



**MULTİMEDYA VERİLER ÜZERİNDE  
VERİ GİZLEME İÇİN YENİ YÖNTEMLER**

**Türker TUNCER**

**Doktora Tezi  
Yazılım Mühendisliği Anabilim Dalı  
Danışman: Prof. Dr. Engin AVCI  
HAZİRAN-2016**

**T.C  
FIRAT ÜNİVERSİTESİ  
FEN BİLİMLERİ ENSTİTÜSÜ**

**MULTİMEDYA VERİLER ÜZERİNDE  
VERİ GİZLEME İÇİN YENİ YÖNTEMLER**

**DOKTORA TEZİ**

**Türker TUNCER**

**(121137203)**

**Tezin Enstitüye Verildiği Tarih: 20 Nisan 2016  
Tezin Savunulduğu Tarih: 03 Haziran 2016**

**Tez Danışmanı: Prof. Dr. Engin AVCI (F.Ü)**

**Diğer Jüri Üyeleri: Prof. Dr. İbrahim SOĞUKPINAR (G.T.Ü)**

**Prof. Dr. Mehmet Kemal LEBLEBİCİOĞLU  
(O.D.T.Ü)**

**Doç. Dr. Resul ÇÖTELİ (F.Ü)**

**Yrd. Doç. Dr. Mustafa ULAŞ (F.Ü)**

**HAZİRAN-2016**

## ÖNSÖZ

Bu tez çalışması, Fırat Üniversitesi Fen Bilimleri Enstitüsü Yazılım Mühendisliği Anabilim Dalı Doktora Programı'nda hazırlanmıştır.

Akademik hayatım ve tez çalışmam boyunca benden hiçbir yardımını ve desteğini esirgemeyen değerli büyüğüm ve danışmanım Sayın Prof. Dr. Engin AVCI'ya ve değerli eşi Dr. Derya AVCI'ya minnet ve şükranlarımı sunarım.

Tez çalışmasının tamamlanmasında her türlü desteğini gördüğüm saygıdeğer tez izleme komitesi üyelerinden Sayın Doç. Dr. Resul ÇÖTELİ ve Sayın Yrd. Doç. Dr. Mustafa ULAŞ'a minnetlerimi sunarım.

Tez ve makale yazımında okumalarıyla ve eleştirileriyle bana destek olan dostum Hüseyin Yüce KÜRÜM ve Yrd. Doç. Dr. Fatih ÖZKAYNAK'a teşekkür ediyorum.

Tez çalışmasının her aşamasında yanımda olan sevgili eşim İlknur TUNCER'e ve varlığıyla bana güç katan oğlum Ömer TUNCER'e teşekkürü bir borç bilirim.

Ayrıca yaşamımın tüm safhalarında desteklerini benden esirgemeyen anne ve babama minnet ve şükranlarımı sunarım.

**Türker TUNCER**

ELAZIĞ-2016

## İÇİNDEKİLER

|                                                                       | <u>Sayfa No</u> |
|-----------------------------------------------------------------------|-----------------|
| <b>ÖNSÖZ .....</b>                                                    | <b>I</b>        |
| <b>İÇİNDEKİLER.....</b>                                               | <b>II</b>       |
| <b>ÖZET .....</b>                                                     | <b>V</b>        |
| <b>SUMMARY .....</b>                                                  | <b>VII</b>      |
| <b>ŞEKİLLER LİSTESİ .....</b>                                         | <b>IX</b>       |
| <b>TABLOLAR LİSTESİ .....</b>                                         | <b>XII</b>      |
| <b>KISALTMALAR LİSTESİ .....</b>                                      | <b>XIII</b>     |
| <b>1. GİRİŞ.....</b>                                                  | <b>1</b>        |
| 1.1.Literatür Özeti.....                                              | 2               |
| 1.2.Tezin Amacı .....                                                 | 4               |
| 1.3.Bulgular .....                                                    | 5               |
| 1.4.Tezin Organizasyonu .....                                         | 6               |
| <b>2. BİLGİ GÜVENLİĞİ .....</b>                                       | <b>7</b>        |
| 2.1. Kriptoloji .....                                                 | 7               |
| 2.1.1. Kriptografi .....                                              | 8               |
| 2.1.1.1. Gizlilik .....                                               | 8               |
| 2.1.1.2. Kimlik Doğrulama.....                                        | 8               |
| 2.1.1.3. Bütünlük .....                                               | 9               |
| 2.1.1.4. Erişim Kontrolü .....                                        | 9               |
| 2.1.1.5. İnkâr Edilememe.....                                         | 9               |
| 2.1.2. Kriptografik Güven Modelleri.....                              | 9               |
| 2.1.2.1. Simetrik Güven Modeli .....                                  | 10              |
| 2.1.2.2. Asimetrik Güven Modeli .....                                 | 11              |
| 2.1.2. Kripto Analiz .....                                            | 12              |
| <b>3. SIR PAYLAŞIMI.....</b>                                          | <b>14</b>       |
| 3.1. Shamir'in Sır Paylaşımı Algoritması.....                         | 15              |
| 3.2. Blakley'in Sır Paylaşımı Algoritması.....                        | 17              |
| 3.3. Mignotte'nin Sayı Teorisi Tabanlı Sır Paylaşımı Algoritması..... | 18              |
| 3.4. Asmuth-Bloom Sır Paylaşımı Algoritması.....                      | 19              |
| 3.5. Toplama Tabanlı Sır Paylaşımı Algoritması .....                  | 19              |
| <b>4. GÖRSEL SIR PAYLAŞIMI.....</b>                                   | <b>21</b>       |
| 4.1. Naor ve Shamir'in Görsel Sır Paylaşımı Şeması.....               | 22              |
| 4.2. Wu ve Chen'in Çoklu Görsel Sır Paylaşımı Şeması .....            | 23              |
| 4.3. Rastgele Izgaralar .....                                         | 24              |
| 4.4. Wang'ın Olasılıksal Görsel Sır Paylaşımı Şeması .....            | 25              |
| 4.5. Harf Tabanlı Görsel Sır Paylaşımı Şeması .....                   | 26              |
| <b>5. VERİ GİZLEME .....</b>                                          | <b>29</b>       |
| 5.1. Steganografi.....                                                | 33              |
| 5.1.1. Metin Steganografi .....                                       | 36              |
| 5.1.2. Ses Steganografi .....                                         | 38              |
| 5.1.2.1. Düşük Bit Kodlaması .....                                    | 39              |
| 5.1.2.2. Aşama Kodlaması.....                                         | 39              |
| 5.1.2.3. Tayf Yayılması .....                                         | 40              |
| 5.1.2.4. Yankı Veri Gizlemesi.....                                    | 40              |
| 5.1.3. İmge Steganografi.....                                         | 40              |

|                                                                                                                     |           |
|---------------------------------------------------------------------------------------------------------------------|-----------|
| 5.1.3.1. En Önemsiz Bite Ekleme Yöntemi .....                                                                       | 42        |
| 5.1.3.2. En Etkin Piksel Ayarlama Süreci Yöntemi .....                                                              | 44        |
| 5.1.3.3. Piksel Değer Farklılıkları Yöntemi .....                                                                   | 45        |
| 5.1.3.4. Değişim Yönünü Kullanma Yöntemi .....                                                                      | 46        |
| 5.2. Sayısal Damgalama .....                                                                                        | 47        |
| 5.2.1. Ayırık Dalgacık Dönüşümü Tabanlı Sayısal Damgalama .....                                                     | 48        |
| 5.2.2. Ayırık Kosinüs Dönüşümü Tabanlı Sayısal Damgalama .....                                                      | 50        |
| 5.2.3. Tekil Değer Ayırışımı Tabanlı Sayısal Damgalama .....                                                        | 52        |
| 5.2.4. Kırılğan Damgalama .....                                                                                     | 52        |
| <b>6. VERİ GİZLEME DEĞERLENDİRME PARAMETRELERİ .....</b>                                                            | <b>54</b> |
| 6.1. Optimum Yolla Veri Gizleme .....                                                                               | 54        |
| 6.2. Optimum Yolla Veri Çıkarma .....                                                                               | 55        |
| 6.3. Kapasite .....                                                                                                 | 56        |
| 6.4. Saldırılara Karşı Dayanıklılık/Kırılğanlık .....                                                               | 57        |
| 6.5. Transparanlık .....                                                                                            | 58        |
| 6.5.1. Sinyal Gürültü Oranı .....                                                                                   | 58        |
| 6.5.2. Ortalama Karesel Hata .....                                                                                  | 58        |
| 6.5.3. Tepe Sinyal Gürültü Oranı .....                                                                              | 59        |
| 6.5.4. Bağlı Karesel Fark Yüzdesi .....                                                                             | 59        |
| 6.5.5. Piksel Bozulma Oranı .....                                                                                   | 59        |
| 6.5.6. Yapısal Benzerlik .....                                                                                      | 60        |
| 6.6. Gizlilik .....                                                                                                 | 60        |
| <b>7. GELİŞTİRİLEN UYGULAMALAR .....</b>                                                                            | <b>61</b> |
| 7.1. Sır Paylaşımı Tabanlı Veri Gizleme Uygulamaları .....                                                          | 61        |
| 7.1.1. DNA-XOR Sır Paylaşımı Tabanlı Veri Gizleme Algoritması .....                                                 | 62        |
| 7.1.1.1. Önerilen Algoritma .....                                                                                   | 63        |
| 7.1.1.2. Deneysel Sonuçlar .....                                                                                    | 66        |
| 7.1.1.3. Sonuçlar .....                                                                                             | 69        |
| 7.1.2. Frekans Uzaklığında XOR Sır Paylaşım Tabanlı Veri Gizleme Algoritması .....                                  | 70        |
| 7.1.2.1. Olasılıksal XOR Sır Paylaşımı Yöntemi .....                                                                | 70        |
| 7.1.2.2. Önerilen Algoritma .....                                                                                   | 71        |
| 7.1.2.3. Deneysel Sonuçlar .....                                                                                    | 72        |
| 7.1.2.4. Sonuç .....                                                                                                | 74        |
| 7.2. Görsel Sır Paylaşımı Tabanlı Veri Gizleme Uygulamaları .....                                                   | 75        |
| 7.2.1. Braille Alfabeti Tabanlı Olasılıksal Görsel Sır Paylaşımı Yöntemi .....                                      | 76        |
| 7.2.1.1. Braille Alfabeti .....                                                                                     | 76        |
| 7.2.1.2. Önerilen Yöntem .....                                                                                      | 76        |
| 7.2.1.3. Deneysel Sonuçlar .....                                                                                    | 78        |
| 7.2.1.4. Sonuç .....                                                                                                | 79        |
| 7.2.2. Göktürk Alfabeti Tabanlı Görsel Sır Paylaşımı Yöntemi ile Veri Gizleme Uygulaması .....                      | 79        |
| 7.2.2.1. Motivasyon ve Tasarım .....                                                                                | 80        |
| 7.2.2.2. Önerilen Yöntem .....                                                                                      | 80        |
| 7.2.2.3. Deneysel Sonuçlar .....                                                                                    | 84        |
| 7.2.2.4. Sonuç .....                                                                                                | 86        |
| 7.2.3. Renkli İmgelerde Kimlik Doğrulaması ve Saldırı Tespiti İçin GSP Tabanlı Kırılğan Damgalama Algoritması ..... | 86        |
| 7.2.3.1. Önerilen Yöntem .....                                                                                      | 87        |
| 7.2.3.2. Deneysel Sonuçlar .....                                                                                    | 89        |

|                                                                                    |            |
|------------------------------------------------------------------------------------|------------|
| 7.2.3.3. Sonuç .....                                                               | 93         |
| 7.3. Çok Seviyeli Veri Gizleme Uygulamaları.....                                   | 93         |
| 7.3.1. Çok Katmanlı Görüntü Steganografi.....                                      | 94         |
| 7.3.1.1. Önerilen Yöntem .....                                                     | 94         |
| 7.3.1.2. Deneysel Sonuçlar .....                                                   | 95         |
| 7.3.1.3. Sonuç .....                                                               | 95         |
| 7.3.2. Ses Sinyalleri İçin Çok Seviyeli ADD Tabanlı Veri Gizleme Algoritması ..... | 96         |
| 7.3.2.1. Önerilen Yöntem .....                                                     | 96         |
| 7.3.2.2. Deneysel Sonuçlar .....                                                   | 99         |
| 7.3.2.3. Sonuç .....                                                               | 101        |
| 7.4. Blok Tabanlı Veri Gizleme Uygulamaları.....                                   | 101        |
| 7.4.1. Sayısal Görüntüler İçin Yön Vektörü Tabanlı Veri Gizleme Algoritması.....   | 101        |
| 7.4.1.1. Kenar Çıkarma Algoritmaları.....                                          | 102        |
| 7.4.1.2. Önerilen Yöntem .....                                                     | 103        |
| 7.4.1.3. Deneysel Sonuçlar .....                                                   | 105        |
| 7.4.1.4. Sonuç .....                                                               | 106        |
| 7.4.2. Mayın Tarlası Oyunu Tabanlı Veri Gizleme Algoritması.....                   | 106        |
| 7.4.2.1. Mayın Tarlası Oyunu.....                                                  | 106        |
| 7.4.2.2. Önerilen Yöntem .....                                                     | 107        |
| 7.4.2.3. Deneysel Sonuçlar .....                                                   | 111        |
| 7.4.2.4. Sonuç .....                                                               | 112        |
| <b>8. SONUÇ VE ÖNERİLER .....</b>                                                  | <b>113</b> |
| 8.1. Tez Çıktılarının Literatüre Katkıları.....                                    | 114        |
| 8.2. Öneriler.....                                                                 | 115        |
| <b>KAYNAKLAR.....</b>                                                              | <b>116</b> |
| <b>ÖZGEÇMİŞ .....</b>                                                              | <b>124</b> |

## ÖZET

İnternetin en sık kullanılan iletişim aracı haline gelmesi ve internet bağlantılı cihazların günlük hayatın her alanında kullanılmaya başlamasıyla birlikte, kişisel veriler hızlı bir şekilde sayısallaşmaya başlamıştır. İnternetin yaygın olarak kullanılması bilgi teknolojilerinin gelişmesine neden olmuştur. Bilgi teknolojileri geliştikçe, bilgi güvenliğinin önemi de artmaktadır. Bilgi güvenliğini sağlayabilmek için en sık kullanılan yöntemlerden ikisi şifreleme ve veri gizlemedir. Şifreleme mesajın içeriğini değiştirmeyi hedeflerken, veri gizleme mesajın varlığını gizlemeyi hedeflemektedir.

Modern bilgisayar ve ağ teknolojilerinde sayısal verilerin bilgi güvenliğini sağlayabilmek için şifreleme sıklıkla kullanılmaktadır ancak şifreli mesajlar saldırganların dikkatini çekmektedir ve bu yüzden şifreli mesajlar birçok saldırıya maruz kalmaktadır. Bu problemi çözmek için veri gizleme kullanılmıştır. Veri gizleme ile örtü nesnesine gizli mesaj gömülerek mesajın varlığı gizlenir. Veri gizleme ile iletim hattının gizliliği sağlanırken, telif hakkı ve kimliklendirme gibi uygulamalar da geliştirilebilmektedir.

Bu tez çalışmasında, veri gizleme yöntemlerinde varolan problemleri gidermek için yeni yöntemler geliştirilmiştir. Sır paylaşımı tabanlı veri gizleme yöntemleri, görsel sır paylaşımı tabanlı multimedya veri gizleme ve imge kimliklendirme yöntemleri, çok seviyeli veri gizleme yöntemleri ve blok tabanlı veri gizleme yöntemleri olmak üzere dört ana başlıkta dokuz adet yöntem geliştirilmiştir.

Bu tez çalışmasında önerilen algoritmalar 4 ana kategoride sınıflandırılabilir. Geliştirilen veri gizleme algoritmalarının yüksek başarıma sahip olması amaçlanmaktadır. Önerilen algoritmalar aşağıda verilmiştir.

- XOR sır paylaşımı algoritması geliştirilerek DNA-XOR tabanlı yeni bir sır paylaşımı algoritması önerilmiştir. Bu algoritma veri gizlemede kullanılmış ve başarılı sonuçlar elde edilmiştir. Bu yöntemlerin kapasitesi piksel başına 1.5 ve 2 bittir (bpp). Örtü nesneyi en az bozan elemanlar seçilerek tepe sinyal gürültü oranı (TPGO, PSNR) 51 dB'den yüksek elde edilmiştir.
- Görsel sır paylaşımı algoritmaları genellikle gürültü benzeri sır parçaları üretmektedir ve bu algoritmalar sahtecilik saldırılarına maruz kalmaktadır. Hem sahtecilik hem de ataklardan sır parçalarını korumak için yeni anlamlı görsel sır paylaşımı şemaları oluşturulmuştur ve elde edilen sır parçaları veri gizleme

algoritmaları kullanılarak gizlenmiştir. Bu algoritmaların genişleme katsayısı ve maliyeti diğer görsel sır paylaşımı yöntemlerinden düşük elde edilmiştir.

- Veri gizleme kapasitesini arttırmak için çok seviyeli veri gizleme algoritmaları önerilmiştir. Bu yöntemler kullanılarak yüksek veri gizleme kapasitesi ve yüksek görsel kalite elde edilmiştir.
- Blok tabanlı veri gizleme algoritmaları incelenmiştir. Mayın tarlası oyunu ve yön vektörü tabanlı iki adet veri gizleme algoritması önerilerek veri gizlemenin çok disiplinli bir yapıya sahip olabileceği gösterilmiştir. Bu yöntemler kullanılarak güvenilir, yüksek kapasite ve transparanlığa sahip yeni veri gizleme şemaları oluşturulmuştur.

**Anahtar Kelimeler:** Veri Gizleme, Steganografi, Sayısal Damgalama, Sır Paylaşımı, Görsel Sır Paylaşımı, Şifreleme, Bilgi Güvenliği.

## **SUMMARY**

### **NOVEL METHODS FOR DATA HIDING ON MULTIMEDIA DATA**

As internet became the most popular communication platform and more and more devices with internet connection are used in everyday life, more personal information started to digitize. The widespread use of the internet has led to the development of information technology. As information technology develops, the importance of information security increases as well. Cryptology and data hiding are the most commonly used methods to provide information security. While encryption change the content of the message, data hiding embeds the message.

Cryptographic methods are mostly used to provide information security in modern computer and network technologies. However encrypted messages get the attention of the attackers and thus they are subjected to many attacks. Data hiding is used to solve this problem by embedding the secret message to a cover object. While data hiding provides a secure transmission channel, it can also be used for copyright and authentication purposes.

In this thesis, new methods are developed to solve problems in data hiding methods. There are nine methods in four main topics which are secret sharing based data hiding methods, visual cryptography based multimedia data hiding and image authentication methods, multilayer data hiding methods and block based data hiding methods.

- A new DNA-XOR based secret sharing algorithm is created by building-up on a XOR secret sharing algorithm. This algorithm was used in data hiding and obtained successful results. In this methods, capacities are 1.5 and 2 bpps. Peak Signal-to-Noise Ratio (PSNR) is obtained as higher than 51 dB by selecting values that distort cover object at the very least.
- Visual cryptography algorithms produce noise-like secret components in general and these algorithms are exposed to attacks. In order to secure the secret shares against attacks and forgery, new meaningful visual secret sharing schemas are created. These secret share are hidden with data hiding algorithms. Expansion coefficient and the cost of these algorithms was obtained less than other visual cryptography methods.
- In order to increase data hiding capacity, multi-level data hiding algorithms are suggested. High payload capacity and visual quality was obtained by using these methods.

- Block based data hiding algorithms are examined. Two different data hiding algorithms based on direction vector and Minesweeper game are suggested and it is pointed out that data hiding can have a multi-disciplined field. New data hiding schemes which has secure, high payload capacity and high visual quality were created by using these methods.

**Keywords:** Data Hiding, Steganography, Digital Watermarking, Secret Sharing, Visual Cryptography, Encryption, Information Security.



## ŞEKİLLER LİSTESİ

### Sayfa No

|                                                                                                                                                       |    |
|-------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| Şekil 2. 1. Kriptolojinin Yapısı.....                                                                                                                 | 8  |
| Şekil 2. 2. Simetrik şifrelemenin genel yapısı .....                                                                                                  | 10 |
| Şekil 2. 3. Asimetrik şifrelemenin genel yapısı.....                                                                                                  | 12 |
| Şekil 3. 1. Sır paylaşım algoritmalarının blok diyagramı.....                                                                                         | 15 |
| Şekil 3. 2. Shamir (3,5) sır paylaşımı algoritmasının örnek gösterimi.....                                                                            | 16 |
| Şekil 3. 3. Blakley (2,n) sır paylaşım algoritmasının geometrik gösterimi .....                                                                       | 17 |
| Şekil 3. 4. Blakley (3,3) sır paylaşım algoritmasının 3 boyutlu geometrik düzlemde<br>gösterimi .....                                                 | 18 |
| Şekil 4. 1. Alt piksellerin kodlanması .....                                                                                                          | 22 |
| Şekil 4. 2. Wu ve Chen'in GSP şeması için kullanılan kod tablosu.....                                                                                 | 24 |
| Şekil 4. 3. Rastgele ızgaralar tabanlı GSP örneği.....                                                                                                | 25 |
| Şekil 4. 4. Takizawa vd. (a) ilk şeması (b) ikinci şeması .....                                                                                       | 27 |
| Şekil 4. 5. (a) Sır 1 (b) Sır 2 (c) Yeniden yapılandırılmış imge[11].....                                                                             | 28 |
| Şekil 5. 1. Veri iletişimi blok diyagramı (a) Geleneksel veri iletişim blok diyagramı (b)<br>Veri gizleme tabanlı veri iletişimi blok diyagramı. .... | 29 |
| Şekil 5. 2. Veri gizlemenin tarihsel gelişimi [2].....                                                                                                | 31 |
| Şekil 5. 3. Steganografi kullanılarak oluşturulan veri gizlemenin blok diyagramı .....                                                                | 34 |
| Şekil 5. 4. Steganografi kullanılarak oluşturulan veri çıkarma blok diyagramı .....                                                                   | 35 |
| Şekil 5. 5. Kelime kaydırma yöntemiyle veri gizleme [32].....                                                                                         | 37 |
| Şekil 5. 6. Arapçada kullanılan noktalı ve noktası harfler [30] .....                                                                                 | 38 |
| Şekil 5. 7. İmgeler için kullanılan steganografik sistem diyagramı .....                                                                              | 41 |
| Şekil 5. 8. Amaçlarına göre imge steganografinin sınıflandırılması [95] .....                                                                         | 42 |
| Şekil 5. 9. 24 bitlik imgeye EÖB ile veri gömme[67].....                                                                                              | 43 |
| Şekil 5. 10. (a) Tek seviyeli ADD ile imgenin alt bantlarına ayrılması (b) Üç seviyeli ADD<br>ile imgenin alt bantlarına ayrılması .....              | 49 |
| Şekil 5. 11. AKD ile damgalamanın blok diyagramı .....                                                                                                | 51 |
| Şekil 7. 1. Önerilen veri gizleme algoritmasının blok diyagramı.....                                                                                  | 64 |
| Şekil 7. 2. A (00) verisinin önerilen algoritma kullanılarak imgeye gömülmesi .....                                                                   | 65 |
| Şekil 7. 3. Deneysel sonuçları elde etmek için kullanılan test imgeleri (a) orijinal imge (b)<br>Stego-imge .....                                     | 66 |

|                                                                                                                                                                                                                                                                                         |     |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| Şekil 7. 4. Önerilen algoritmanın ortalama PSNR/ kapasite değişimi.....                                                                                                                                                                                                                 | 68  |
| Şekil 7. 5. Olasılıksal DNA-XOR sır paylaşımı şeması (a) Orijinal imge (b) R katmanına<br>gömülen sır parçası (c) G katmanına gömülen sır parçası (d) B katmanına<br>gömülen sır parçası (e) orijinal imgenin histogramı (f) R katmanına gömülen sır<br>parçasının histogramı (g) ..... | 69  |
| Şekil 7. 6. Test imgeleri (a) Baboon (b) Boat (c) Elaine (d) House (e) Lena (f) Peppers (g)<br>F16 .....                                                                                                                                                                                | 72  |
| Şekil 7. 7. (a) Örtü imgesi (b) Gizli veri (c) Birinci sır parçası (d) İkinci sır parçası (e)<br>Üçüncü sır parçası.....                                                                                                                                                                | 74  |
| Şekil 7. 8. Harflerin Braille kodları [15] .....                                                                                                                                                                                                                                        | 76  |
| Şekil 7. 9. (2,2) BGSP (a) Gizli veri (b) 1. Sır parçası (c) 2. Sır parçası.....                                                                                                                                                                                                        | 78  |
| Şekil 7. 10. Göktrük alfabesine ait harfler .....                                                                                                                                                                                                                                       | 81  |
| Şekil 7. 11. (3,3) sır paylaşımı şeması.....                                                                                                                                                                                                                                            | 82  |
| Şekil 7. 12. Elde edilen değerlerin yeniden yapılandırılmış imgeye yerleştirilmesi .....                                                                                                                                                                                                | 83  |
| Şekil 7. 13. Yeniden yapılandırılmış imgeler (a) Naor ve Shamir'in yöntemi (b) Lin vd.'nin<br>yöntemi (c) Önerilen yöntem.....                                                                                                                                                          | 84  |
| Şekil 7. 14. Harflere ait frekans analizi (a) İlk sır parçası (b) İkinci sır parçası.....                                                                                                                                                                                               | 85  |
| Şekil 7. 15. Wu ve Chang'ın çoklu GSP şemasına ait kodlama tablosu .....                                                                                                                                                                                                                | 87  |
| Şekil 7. 16. Önerilen veri gizleme algoritmasının blok diyagramı.....                                                                                                                                                                                                                   | 88  |
| Şekil 7. 17. Önerilen veri çıkarma algoritmasının blok diyagramı .....                                                                                                                                                                                                                  | 89  |
| Şekil 7. 18. Wu ve Chang'ın görsel sır paylaşımı yönteminin uygulanması (a) Orijinal<br>imge (b) İlk sır parçası (c) ikinci sır parçası (d) üçüncü sır parçası .....                                                                                                                    | 90  |
| Şekil 7. 19. Önerilen veri gizleme algoritmasının blok diyagramı.....                                                                                                                                                                                                                   | 97  |
| Şekil 7. 20. Veri çıkarmanın blok diyagramı.....                                                                                                                                                                                                                                        | 99  |
| Şekil 7. 21. (a) Orjinal görüntü (b) Sobel ile kenar tespiti yapılmış görüntü (c) Canny ile<br>kenar tespiti yapılmış görüntü (d) Roberts ile kenar tespiti yapılmış görüntü (e)<br>Prewitt ile kenar tespiti yapılmış görüntü (f) LOG ile kenar tespiti yapılmış<br>görüntü.....       | 103 |
| Şekil 7. 22. Yön vektörü örnekleri .....                                                                                                                                                                                                                                                | 104 |
| Şekil 7. 23. Mayın tarlası oyunu ekran görüntüsü [18] .....                                                                                                                                                                                                                             | 107 |
| Şekil 7. 24. 3 x 3 komşuluk matrisi .....                                                                                                                                                                                                                                               | 107 |
| Şekil 7. 25. Mayın=1 için komşuluk derecelerinin bulunması .....                                                                                                                                                                                                                        | 108 |
| Şekil 7. 26. Değerlerin histogramları (a) V (b) V (mod 8) (c) V (mod 4) (d) V (mod 2) .                                                                                                                                                                                                 | 109 |

|                                                          |     |
|----------------------------------------------------------|-----|
| Şekil 7. 27. V (mod 2) için veri gizleme diyagramı ..... | 110 |
| Şekil 7. 28. Lena imgesinin bit düzlemleri.....          | 110 |



## TABLÖLAR LİSTESİ

### Sayfa No

|                                                                                                           |     |
|-----------------------------------------------------------------------------------------------------------|-----|
| Tablo 5. 1. Steganografi ve Sayısal Damgalama arasındaki farklılıklar .....                               | 30  |
| Tablo 5. 2. EÖB yöntemiyle veri gömülmesi .....                                                           | 43  |
| Tablo 6. 1. EÖB veri gizleme fonksiyonunun algoritması .....                                              | 54  |
| Tablo 6. 2. EÖB için önerilen optimum veri gizleme algoritması .....                                      | 55  |
| Tablo 6. 3. EÖB veri çıkarma fonksiyonu algoritması .....                                                 | 55  |
| Tablo 6. 4. EÖB optimum veri çıkarma fonksiyonu algoritması .....                                         | 56  |
| Tablo 7. 1. DNA-XOR operatörünün doğruluk tablosu .....                                                   | 62  |
| Tablo 7. 2. Adenin değeri için üçlü DNA-XOR doğruluk tablosu .....                                        | 63  |
| Tablo 7. 3. Önerilen yöntem kullanılarak elde edilen sonuçlar .....                                       | 67  |
| Tablo 7. 4. Önerilen yöntemin literatürde yaygın olarak kullanılan yöntemlerle<br>karşılaştırılması ..... | 67  |
| Tablo 7. 5. Önerilen yöntem ile Yuan'ın yönteminin karşılaştırılması .....                                | 68  |
| Tablo 7. 6. XOR doğruluk tablosu .....                                                                    | 70  |
| Tablo 7. 7. 1.5 bpp kapasitede elde edilen PSNR ve MSSIM değerleri .....                                  | 73  |
| Tablo 7. 8. Elde edilen PSNR değerleri .....                                                              | 79  |
| Tablo 7. 9. Saldırı tespiti ve MD5 özet fonksiyonları .....                                               | 91  |
| Tablo 7. 10. Çok katmanlı steganografi kullanılarak elde edilen kapasiteler .....                         | 95  |
| Tablo 7. 11. Elde edilen PSNR değerleri .....                                                             | 95  |
| Tablo 7. 12. Önerilen yönteme ait SNR değerleri .....                                                     | 100 |
| Tablo 7. 13. Önerilen method ile ADD-HFD [29] yönteminin karşılaştırılması .....                          | 101 |
| Tablo 7. 14. Tablonun test imgeleri üzerinde uygulanması ve elde edilen sonuçlar .....                    | 105 |
| Tablo 7. 15. Elde edilen sonuçların diğer veri gizleme şemalarıyla karşılaştırılması .....                | 112 |

## KISALTMALAR LİSTESİ

|              |                                                                                 |
|--------------|---------------------------------------------------------------------------------|
| <b>ADD</b>   | : Ayrık Dalgacık Dönüşümü                                                       |
| <b>AFD</b>   | : Ayrık Fourier Döşümü                                                          |
| <b>AKD</b>   | : Ayrık Kosinüs Dönüşümü                                                        |
| <b>GSP</b>   | : Görsel Sır Paylaşımı                                                          |
| <b>İİS</b>   | : İnsan İşitme Sistemi                                                          |
| <b>LSB</b>   | : Least Significant Bit embedding method (En anlamsız bite gömme yöntemi )      |
| <b>LSD</b>   | : Least Significant Digit embedding method (En anlamsız basamağa gömme yöntemi) |
| <b>OPAP</b>  | : Kümeleme                                                                      |
| <b>PVD</b>   | : Pixel Value Differences (Piksel Değer Farklılıkları)                          |
| <b>SP</b>    | : Sır Paylaşımı                                                                 |
| <b>VB</b>    | : Vektör Basamaklama                                                            |
| <b>SSIM</b>  | : Yapısal Benzerlik                                                             |
| <b>MSSIM</b> | : Ortalama Yapısal Benzerlik                                                    |

## 1. GİRİŞ

İnternetin yaygın olarak kullanılması ve akıllı cihazların taşınabilir hale gelmesiyle birlikte kişisel veriler hızlı bir şekilde sayısal ortama aktarılmaya başlamıştır. Sayısal ortama aktarılan bu verilerin güvenliğinin sağlanması ise çok önemli bir konu haline gelmiştir. Bilgi güvenliğini sağlayabilmek için veriyi yetkisiz erişimlerden korumak gerekmektedir [1]. Bilgi güvenliğini sağlamanın birçok yolu vardır ancak bilgi güvenliğinin temel bacakları şifreleme ve veri gizlemedir.

Şifreleme bilimi verinin bir protokol aracılığıyla saldırganın erişemeyeceği başka bir forma dönüşümü ile ilgilenmektedir. Bunu sağlamak için simetrik veya asimetrik şifreleme protokolleri kullanılmaktadır. Şifreleme işleminin sağlanabilmesi için karıştırma ve yayılma işlemlerinin gerçekleştirilmesi gerekmektedir.

Verinin varlığını gizleyebilmek amacıyla, birçok veri gizleme uygulaması kullanılmaktadır [2]. Veri gizleme biliminin en sık kullanılan alt dalları ise steganografi ve sayısal damgalamadır. Steganografide gizlenen verinin sezilememesi ve güvenilir veri iletim hattının oluşturulması hedeflenmektedir. Günümüzde birçok firma ve kurum steganografiyi kullanarak bilgi güvenliğini sağlar [3-7]. Sayısal damgalama uygulamalarının temel amacı verinin inkâr edilememesini sağlamaktır. Steganografi ve sayısal damgalama algoritmaları benzer şekilde oluşturulmaktadır. Bu algoritmaları oluşturan öğeler aşağıdaki gibidir [8].

- Örtü nesnesi
- Gizli mesaj
- Veri gizleme fonksiyonu
- Veri gizlenmiş nesne
- Veri gizleme anahtarı
- Veri çıkarma fonksiyonu

Örtü nesnesi metin, ses, imge ve video gibi multimedya verilerden oluşmaktadır [6]. Gizli mesaj, örtü nesnesinin içerisine veri gizleme fonksiyonu kullanılarak gömülür ve çıktı olarak veri gizlenmiş nesne elde edilir. Veri çıkarma aşamasında ise, veri gizleme anahtarı kullanılarak veri gizlenmiş nesnede bulunan veri gizleme indisleri tespit edilir. Veri çıkarma fonksiyonu kullanılarak gizli mesaj elde edilir [9-10]. Veri gizleme algoritmaları veri gizleme alanına göre 3 grupta incelenmektedir. Bunlar uzamsal alan, frekans alanı ve sıkıştırma alanıdır.

**Uzaysal Alan:** Bu grupta geliştirilen algoritmalar, doğrudan sinyali değiştirerek veri gizleme işlemini gerçekleştirirler. Uzamsal alanda yaygın olarak kullanılan algoritmalar En Önemsiz Bit Değiştirme (EÖB) ve En Anlamsız Basamak Değiştirme (EAB-LSD) yöntemleridir [11].

**Frekans Alanı:** Frekans alanında veri gizleme uygulamalarının gerçekleştirilmesinin temel amacı, gizli mesajın saldırılara karşı dayanıklı hale getirilmesidir. Dayanıklılığı arttırmak için Ayırık Kosinüs Dönüşümü (AKD), Ayırık Dalgacık Dönüşümü (ADD), Ayırık Fourier Dönüşümü (AFD) gibi dönüşümler kullanılmaktadır [12-15].

**Sıkıştırma Alanı:** Bu alanda, Vektör Basamaklama (VB), JPEG sıkıştırma vb. yöntemler kullanılarak gizli mesajın sıkıştırma algoritmalarına karşı dayanıklılığının artırılması hedeflenmektedir [16]. Bu yöntemlerin yanı sıra histogram kaydırma gibi yöntemler de kullanılarak veri gizleme işlemi gerçekleştirilmektedir [17].

## 1.1. Literatür Özeti

Bilgi teknolojilerinin gelişmesiyle birlikte veri gizleme önemli bir konu haline gelmiştir. Literatürde sır paylaşımı ve steganografi kullanarak imge kimlik doğrulaması yapan birçok algoritma bulunmaktadır. Bu algoritmaların iki temel amacı vardır. Bu amaçlardan birincisi yüksek görsel kalitede veri gizleme, ikincisi ise gizli verinin güvenilirliğini sağlamaktır. Temel olarak problem bu iki parametrenin ön plana çıkarılmasıdır. Hesapsal maliyet göz ardı edilmiştir. Bu tez çalışmasında literatürde var olan veri gizleme çalışmaları incelenmiş ve aşağıdaki gibi sıralanmıştır. Qi ve ark. [18] imge kimlik doğrulaması için, tekil değer tabanlı yarı kırılğan yeni bir damgalama şeması sunmuşlardır. Bu yöntem içerik bağımlı olarak güvenilir bir damga üretir ve bu damgayı tekil değer dizisine mantıksal operatörler kullanarak gömer. Ancak önerilen algoritma yüksek transparanlığa sahip değildir. Botta ve ark. [19] kendi çalışmalarından önce tespit edilmeyen saldırıları tespit edebilmek ve saldırının lokasyonunu bulabilmek için yeni bir kırılğan damgalama sistemi önermişlerdir fakat elde ettikleri kırılğan damagalama algoritması analiz edilerek güvenilir olmadığı ispat edilmiştir. Yu ve ark. [20] imge kimlik doğrulaması ve saldırı tespiti işlemini gerçekleştirebilmek için yeni bir kırılğan damgalama algoritması geliştirmişlerdir ve yine geliştirilen algoritmanın yüksek transparanlığa sahip olmadığı görülmüştür. Transparanlığı yüksek elde etmek için düşük gömme kapasitesi kullanılarak saldırı tespiti yapılmıştır. Bu sebepten dolayı önerilen algoritma veri gizlemenin tüm başarımlarını parametrelerini

sağlayamamaktadır. Ghosal ve ark. [21] binom dönüşümü tabanlı kırılğan damgalama algoritması önermişlerdir ve elde ettikleri deneysel sonuçlar önerilen algoritmanın başarılı olduğunu göstermiş olsalar da geliştirdikleri yöntemin algoritmik analizini vermemişlerdir. Tong ve ark. [22] kaos tabanlı saldırı tespiti sağlayan ve kendini kurtaran yeni bir kırılğan damgalama algoritması önermişlerdir. Deneysel sonuçlar bu algoritmanın güvenilir, iyi saldırı tespiti yapabilen ve kendini onarabilen bir algoritma olduğunu ortaya koymuştur. Tu ve ark. [23] sayısal dokümanların telif hakkını koruyabilmek için sır paylaşımı ve steganografi tabanlı yeni bir veri gizleme algoritması önermiştir. Önerdikleri yöntemde sadece literatürde varolan sır paylaşımı algoritmaları ve veri gizleme yöntemlerini bir arada kullanmışlardır. Bu sebepten dolayı literatüre orijinal bir katkıda bulunmadıkları gibi hesapsal maliyeti arttırarak veri gizleme algoritmasının performansını düşürmüşlerdir. Lee ve ark. [24] tarafından Shamir'in sır paylaşım modeli tabanlı 4 katmanlı imgeler için kimlik doğrulama algoritması önerilmiştir. Veri gizleme algoritmasında imgenin alfa kanalı kullanılmıştır. Bu veri gizleme algoritması yüksek veri gizleme kapasitesine sahip, güvenilir, verimli ve yüksek görsel kalite değerine sahip olarak görünse de sadece 4 katmanlı imgeler için geliştirildiği için kullanılabilirliği kısıtlıdır. Sır paylaşımı tabanlı veri gizleme algoritmaları kırılğan bir yapıya sahiptir [25-29]. Yuan [30] steganografi ve sır paylaşımı arasındaki ilişkiyi araştırmış ve analiz tabanlı yeni bir steganografik yöntem geliştirmiştir. Geliştirilen yöntem uzamsal alanda  $\pm 1$  veri gizleme fonksiyonunu kullanan bir yöntemdir. Bu yöntemde çoklu örtü nesnesi kullanılmıştır.

Yukarıda bahsedilen yöntemlerin yanı sıra literatürdeki blok tabanlı veri gizleme yöntemleri de incelenmiştir. Nguyen ve Chan [31] sudoku tekniği tabanlı bir tersinir veri gizleme algoritması önermiştir. Bu makale oyun kuralları tabanlı veri gizleme algoritmalarının başarılı sonuçlar elde edebileceğini ortaya koymuştur. Kim ve ark. [32] blok tabanlı tersinir bir veri gizleme algoritması önermiştir. Veri gizleme işlemi yapabilmek için imgenin örtüşmeyen alt bloklara ayrılmaktadır. Bu yöntem alt bloklar histogramla ilişkilendirmektedir ve bu yöneme benzer birçok veri gizleme algoritması da literatürde önerilmiştir [33-35]. Ancak son yıllarda blok tabanlı veri gizleme algoritmalarından en çok atf alan iki algoritma vardır ve bunlar Luo ve ark. [36] tarafından önerilen tersinir blok tabanlı veri gizleme algoritması ve Kamran ve ark. [37] tarafından önerilen tersinir blok tabanlı veri gizleme algoritmasıdır. Bu iki algoritmada da yüksek veri gizleme kapasitesi ve yüksek görsel kalite elde edilmiştir ancak bu yöntemlerin en önemli problemi veri gizleme kapasitesinin örtü nesnesinin yapısal özelliklerine bağımlı olmasıdır. Ayrıca literatürde yer

alan ikili imgeler için önerilen veri gizleme algoritmaları incelenmiş ve blok tabanlı veri gizleme algoritmalarıyla ilişkileri araştırılmıştır [38-47].

Tez süresi boyunca, bilgi güvenliğini sağlayabilmek için anlamlı parçalardan oluşan görsel sır paylaşımı şemaları da incelenmiştir. Görsel sır paylaşımı algoritmaları genellikle gürültü benzeri sır parçaları üretmektedir. Bu durum saldırganların dikkatini çekmektedir. Görsel sır paylaşım şemalarına en sık yapılan saldırı ise sahtecilik saldırısıdır. Bu tip saldırılardan korunmak için saldırganların dikkatinin başka yönlere çekilmesi gerekmektedir. Bu sebepten dolayı, Lin ve ark. [48] doğal dil tabanlı görsel sır paylaşımı şemasını önermişlerdir. Önerilen şemada Latince, Çince, Japonca ve Korecede bulunan harfler kullanılmıştır. Ancak önerilen GSP şeması harflerin morfolojik özelliklerine bağımlı oldukları için tüm harflerin eşit olasılıkla kullanılması sağlanamamaktadır.

Bu tez süresince ses sinyalleri için geliştirilmiş veri gizleme algoritmaları da incelenmiştir. Yapılan analiz sonucunda, frekans alanında yapılan veri gizleme uygulamalarının daha başarılı olduğu gözlemlenmiştir. İnsan işitme sisteminin (İİS) fark edemeyeceği şekilde veri gizlemenin yapılması gerekmektedir [49-57]. Yüksek kapasitede ve yüksek işitsel kalitede veri gizlemek için frekans alanında analiz tabanlı yeni veri gizleme algoritmalarının geliştirilmesinin gerekliliği farkedilmiştir.

Bu tez çalışmasında, yukarıda bahsedilen konularla ilgili geliştirilmiş algoritmalar detaylı bir şekilde incelenmiştir ve analiz tabanlı veri gizleme algoritmalarının daha başarılı olduğu görülmüştür. Sır paylaşımı ve görsel sır paylaşımı gibi kriptolojik protokollerin veri gizleme algoritmalarına adapte edilmesi sonucunda yüksek başarıma sahip veri gizleme ve bilgi güvenliği uygulamalarının geliştirilebileceği gözlemlenmiştir.

## **1.2. Tezin Amacı**

Bu tez çalışmasının altı temel amacı bulunmaktadır. Bunlar:

- Yeni olasılıksal sır paylaşımı şemaları geliştirmek ve olasılıksal sır paylaşımı tabanlı veri gizleme algoritmaları elde ederek bu algoritmaların alandan bağımsız olduğunu göstermek.
- Renkli imgelerde, kimlik doğrulamayı sağlayabilen yüksek görsel kalite ve yüksek kimlik doğrulama yeteneğine sahip kırılğan sayısal damgalama algoritmaları geliştirmek.

- Blok tabanlı veri gizleme algoritmalarını analiz edip, yüksek başarıma sahip blok tabanlı veri gizleme algoritmaları geliştirmek.
- Çok katmanlı steganografik yöntemler kullanarak yüksek kapasitede ve yüksek görsel kalitede veri gizleme şemaları elde etmek. Çok katmanlı yapıların matematiksel özelliklerini ortaya koymak
- Anlamlı alt piksellerden oluşturulan görsel sır paylaşımı şemaları oluşturmak ve bu şemaları veri gizleme algoritmalarıyla birlikte kullanmak. Böylece hem veri gizlemedeki hem de görsel sır paylaşımındaki eksiklikleri gidermek.

### 1.3. Bulgular

Bu tez çalışmasının ilk adımında, veri gizleme algoritmaları ve bu algoritmalar için kullanılan değerlendirme parametreleri incelenmiştir. Literatürde var olan yöntemleri iyileştirmek ve veri gizlemenin temel başarımlarını sağlayabilecek veri gizleme algoritmaları oluşturmak için sır paylaşımı şemaları incelenmiştir. Literatürde veri gizleme ve sır paylaşımının birlikte kullanıldığı yöntemlere rastlanılmıştır. Her iki yöntemin birlikte kullanıldığı şemalara odaklanılmıştır. Son zamanlarda geliştirilen veri gizleme algoritmalarının analiz tabanlı olduğu görülmüş ve sır paylaşımı ile veri gizleme analizi yapılarak optimum veri gizleme algoritmasının oluşturulması için çalışmalar yapılmıştır. Ayrıca oluşturulan veri gizleme algoritmaları hem uzaysal alanda hem de frekans alanında uygulanmıştır.

Sesler için veri gizleme algoritmaları incelendiğinde frekans dönüşümlerinin kullanılmasının uygun olduğu görülmüştür. Veri gizleme kapasitesinin artırılması için çok seviyeli dalgacık dönüşümünün uygulanması gerçekleştirilmiştir. Blok tabanlı veri gizleme yöntemleri analiz edilmiş ve bu yöntemlerin yüksek görsel kalite sağlamadığı gözlemlenmiştir. Blok tabanlı veri gizleme algoritmalarında görsel kaliteyi arttırmaya yönelik çalışmalar yapılmıştır.

Görsel sır paylaşımı yöntemleri incelendiğinde ise, sır parçalarının gürültü benzeri veya dokusal olduğu gözlemlenmiştir. Bu durum saldırganların dikkatini çekmektedir. Gürültü benzeri ve dokusal sır parçalarını analiz etmek veya bu sır parçalarını kullanarak sahtecilik yapabilmek için birçok saldırı geliştirilmiştir. Sır parçalarının saldırganların dikkatini çekmeden alıcı tarafa iletebilmesi için anlamlı alt piksellerden oluşan görsel sır paylaşım yöntemleri oluşturulmuştur ancak bu yöntemler analiz edildiğinde, gizli verinin boyutunu

aşırı derecede arttırdığı ve olasılıksal yapılarda harflerin kullanılma olasılığının hesaplanmadığı farkedilmiştir. Anlamalı görsel sır paylaşımı şemalarının belirtilen eksikliklerini giderebilmek için çalışmalar yapılmıştır.

#### **1.4. Tezin Organizasyonu**

Tez çalışması 8 bölümden oluşmaktadır. Tez çalışmasının ikinci bölümünde bilgi güvenliği ve bilgi güvenliğini oluşturan yöntem bilimlerinden kısaca bahsedilmiştir. Üçüncü bölümde, sır paylaşımı ve sır paylaşımında kullanılan algoritmalarından sunulmuştur. Dördüncü bölümde, görsel sır paylaşımından bahsedilerek deterministik ve olasılıksal yöntemler hakkında bilgiler verilmiştir. Beşinci bölümde, modern veri gizleme algoritmalarıyla ilgili bilgiler verilmiştir. Bu ana başlık altında steganografi ve sayısal damgalama ile ilgili bilgiler sunularak steganografide ve sayısal damgalamada kullanılan yöntemlerden bahsedilmiştir. Altıncı bölümde veri gizlemenin başarımlarından bahsedilmiştir ve bu başarımlar parametreleri 6 ana başlıkta ele alınmıştır. Tezin yedinci bölümünde geliştirilen uygulamalardan bahsedilmiştir. Tez kapsamında 4 ana başlıkta 9 adet yöntem önerilmiştir. Bu ana başlıklar sırasıyla; sır paylaşımı tabanlı veri gizleme uygulamaları, görsel sır paylaşımı tabanlı veri gizleme uygulamaları, çok katmanlı veri gizleme uygulamaları ve blok tabanlı veri gizleme uygulamalarıdır. Bu bölümde, multimedya verileri için veri gizleme algoritmaları önerilmiştir ve önerilen algoritmaların uygulamalarından söz edilmiştir. Tezin sekizinci ve son bölümünde sonuç ve önerilerden bahsedilmiştir.

## 2. BİLGİ GÜVENLİĞİ

Teknolojik gelişmeler ile birlikte bilgi güvenliği giderek önem kazanmaya başlamıştır. Bilgi güvenliği çok yönlü bir konudur. İçerisinde ağ güvenliği, sistem güvenliği ve kişisel veri güvenliği gibi çeşitli alt başlıkları içermektedir. Bilgi güvenliği kavramı iletişim güvenliği için bir çatı kavramı temsil etmektedir. İçerisinde gizlilik, bütünlük, erişilebilirlik, kimlik doğrulama ve inkâr edilememe gibi özellikleri sağlamayı taahhüt etmektedir.

Modern kriptoloji, bilgi güvenliğinin köşe taşlarından biridir. Modern kriptoloji bilimindeki en temel sorun güvensiz bir ortam boyunca iletişim güvenliğinin sağlanmasını garanti edebilmektir. Bunu sağlamak için çeşitli güven modelleri kullanılmaktadır. Güven modelleri genel bir sınıflandırma ile üç kategoriye ayrılabilir. Bunlar simetrik (gizli anahtarlı) güven modeli, asimetrik (açık anahtarlı) güven modeli ve bu iki kategori altında sınıflandırılmayan diğer protokoller olan özet fonksiyonları, mesaj doğrulama kodları ve anahtar değişim protokollerini içermektedir [58]. Bu bölümde güven modelleri ve protokoller kısaca özetlenmiştir.

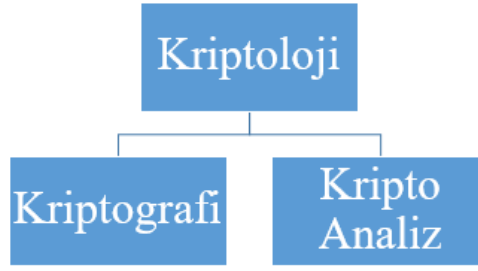
### 2.1. Kriptoloji

Kriptoloji, veri iletim hattı boyunca mesaj içeriğinin korunması için geliştirilen bilim dalıdır. Kriptolojinin tarihi antik çağlara dayanmaktadır. Kriptoloji, Yunanca “Kryptos Logos” kelimelerinden türetilmiştir. “Kryptos” kelimesi gizli dünya, “logos” kelimesi ise neden-sonuç kurma anlamı taşımaktadır. Kriptoloji kelimesinin dünya dillerindeki karşılığı da genellikle bu orijinal halini korumaktadır [59].

Kavram olarak kriptoloji, haberleşen birden fazla sistemin güvenli bilgi alışverişinde bulunabilmeleri için kullandıkları, temeli zor matematiksel problemlere dayalı tekniklerin bütünüdür. 2 farklı ana dalı vardır [60,61]. Bunlar;

- Kriptografi
- Kripto analiz

Şekil 2.1’de kriptolojinin genel bir yapısı verilmektedir.



Şekil 2. 1. Kriptolojinin Yapısı

### 2.1.1. Kriptografi

Kriptografi, şifreleme tekniklerinin tamamını inceleyen bilim dalıdır. Yunanca gizli, saklı anlamına gelen “kript” ve yazı anlamına gelen “graf” kelimelerinden türetilmiştir. Yani şifre yazımı anlamına gelmektedir. Kriptoloji bilmine ilk zamanlarda daha çok askeri alanlarda ihtiyaç duyulmuştur. Ancak günümüz bilgi çağında, şifreleme bilgi güvenliğini sağlayabilmek için her alanda kullanılmaktadır.

Kriptografi, gizlilik, kimlik denetimi, bütünlük, erişilebilirlik ve inkâr edilememe gibi bilgi güvenliği kavramlarını sağlayan ispat edilebilir matematiksel yöntemlerin bütünüdür. Bu yöntemler, iletim hattında karşılaşılabilecek saldırılardan bilgiyi, göndericiyi ve alıcıyı korumayı hedeflemektedir. Diğer bir ifade ile kriptografi, anlamlı bilgiyi yetkisiz taraflar tarafından okunamayacak hale dönüştürülmesi kullanılan yöntemler bütünüdür [62].

#### 2.1.1.1. Gizlilik

Gizlilik, gönderilen mesajın, veri iletim hattında mesajı görme yetkisi olmayan kullanıcılardan saklanmasıdır. Yani bilginin gizli kalması, üçüncü kişiler tarafından okunamamasıdır. Gizlilik, bilgi güvenliği için gerekli olan temel ölçütlerdendir. Bilginin gizliliğini sağlayabilmek için birçok veri gizleme ve şifreleme yöntemleri geliştirilmiştir [62].

#### 2.1.1.2. Kimlik Doğrulama

Kimlik doğrulama, bilgiyi gönderen kişinin gerçekten mesajı gönderen kişi olup olmadığının doğrulanmasıdır. Şifreleme teknikleri ile gönderilen mesajlar üzerine özel imzalar eklenerek, mesajı gönderen kişinin gerçekten doğru kişi olduğundan emin olunması

sağlanmaktadır. Çeşitli algoritmalarla oluşturulan bu özel imzalar, alıcı kişi tarafından belirli tekniklerle doğrulanmaktadır. Bu imza oluşturma ve doğrulama işlemi dijital imza olarak adlandırılmaktadır [63]. Kimlik doğrulamayı sağlayabilmek için özet fonksiyonları, kırılğan damgalama algoritmaları ve sayısal imzalar kullanılmaktadır.

#### **2.1.1.3. Bütünlük**

Bütünlük, bilginin saklanması, iletilmesi vs. süreçlerinde bilginin gönderildiği gibi tekrar elde edilebilmesidir yani üzerinde hiçbir değişiklik yapılmadığının garantisidir. Bilginin içeriğinde meydana gelebilecek değişiklik bazen tamamıyla bilgiyi anlamsızlaştırabilmektedir [62].

#### **2.1.1.4. Erişim Kontrolü**

Erişim kontrolü, yetkisiz kişilerin veriye erişimlerini engellemedir. Erişim kontrolü bir çeşit yetkilendirme olarak da düşünülebilir. Kimlik denetimi yapılan varlıkların yetkisi dâhilindeki kaynaklara erişmesini sağlar [62].

#### **2.1.1.5. İnkâr Edilememe**

İnkâr edilememe, mesaj gönderildiğinde alıcı taraf gönderen tarafın mesajı gönderdiğini, aynı şekilde gönderen tarafta alıcı tarafın mesajı aldığını ispatlayabilme imkânına sahip olmasıdır. İnkâr edilememeyi sağlamak için genellikle kriptolojik özet fonksiyonları, sayısal damgalama ve elektronik imza yöntemleri kullanılmaktadır [62].

### **2.1.2. Kriptografik Güven Modelleri**

Bilgi güvenliğini sağlayabilmek için çeşitli algoritmalara ihtiyaç duyulmaktadır. Kriptoloji algoritmaları, gönderici ve alıcı arasında iletilecek mesajı şifrelemek ve şifreli mesajı deşifre etmek için önerilmiş algoritmalarlardır. Güven modelleri temelli şifreleme algoritmaları kullanılarak mesaj, çeşitli yöntemler yardımı ile kodlanır ve başkasının okuyamayacağı hale getirilir. Kriptografik güven modelleri temel olarak ikiye ayrılmaktadır. Bunlar;

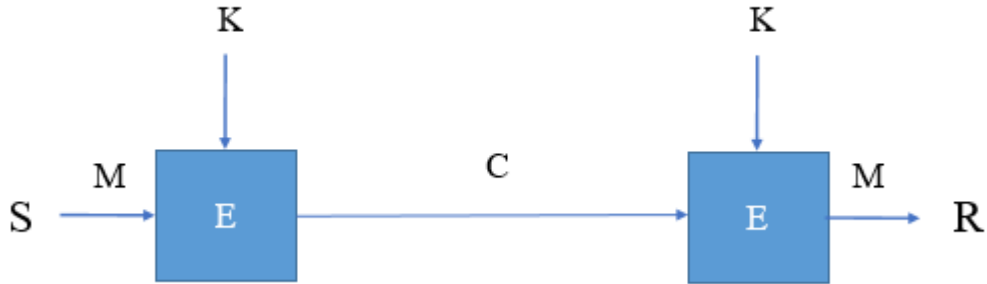
- Simetrik Güven Modeli

- Asimetrik Güven Modeli

olarak sınıflandırılabilir. Bu iki yöntem dışında sınıflandırılmayan protokoller, özet fonksiyonları, mesaj doğrulama kodları ve anahtar dağıtım protokolleri gibi protokoller yer almaktadır. Simetrik şifreleme algoritmalarında gönderici ve alıcı aynı anahtarı kullanarak veri şifreleme ve şifre çözme işlemini gerçekleştirirken, asimetrik şifreleme algoritmalarında ise farklı anahtarlar kullanılarak şifreleme ve deşifreleme işlemleri gerçekleştirilmektedir [58].

### 2.1.2.1. Simetrik Güven Modeli

Simetrik şifreleme algoritmalarında, gönderici taraf ve alıcı taraf şifreleme ve şifre çözme işlemi için aynı anahtarı kullanılmaktadır. Kullanılacak simetrik şifreleme anahtarının genellikle düzgün bir yapıya sahip rastgele karakterlerden olduğu varsayılmaktadır. Simetrik şifreleme algoritmaları; gizli anahtar (K), şifreleme algoritması (E) ve şifre çözme algoritması (D) olmak üzere 3 temel unsurdan oluşmaktadır. Simetrik şifreleme algoritmalarının genel yapısı Şekil 2.2’de verilmiştir.



Şekil 2. 2. Simetrik şifrelemenin genel yapısı

Şekil 2.2’de S gönderici, K şifreleme anahtarı, E şifreleme algoritma ve D ise şifre çözme algoritmasıdır. Denklem 2.1 ve 2.2’de simetrik şifrelemenin yapısı verilmiştir.

$$C = E(M, K) \quad (2.1)$$

$$M = D(C, K) \quad (2.2)$$

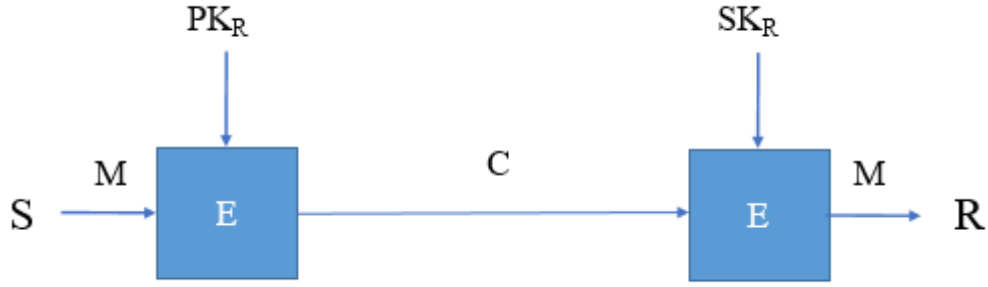
Simetrik şifreleme kendi içerisinde akış ve blok şifreler diye iki temel kategoriye ayrılmaktadır. Akış şifreler veriyi bit bit şifrelerken, blok şifreler veriyi blok blok

şifrelemektedir. Akış şifreler veriyi bit bit şifrelediği ve veri tamamlama işlemine gerek duymadığı için blok şifrelere göre daha hızlıdır. Ancak veri uzunluğu kadar gerçek rasgele anahtarlara ihtiyaç duyması ve bu anahtarların sadece bir defa kullanılabilecek olması bu algoritmaların dezavantajıdır [58].

Yaygın akış şifreleme algoritmaları OTP (One Time Pad – Tek Kullanımlık Şifre), A5/1 ve A5/2 yukarıda sayılan avantajlarından dolayı multimedya verileri ve ses şifreleme için uygundur. Ancak blok şifreler daha genel bir uygulama alanına sahiptir. 1970’li yıllarında ticari amaçlar için blok şifrelerin kullanılması ile birlikte NIST tarafından açık bir yarışma başlatılarak blok şifreleme algoritması standardı olan DES (Data Encryption Standart – Veri Şifreleme Standardı) yayınlanmıştır. Bu algoritmanın hem anahtar uzayının kısa olması hemde diferansiyel ve lineer kriptanalize karşı zayıflıklarının ortaya koyulmasının ardından yeni bir yarışma başlatılarak yeni bir standart belirlenme çalışmalarına gidilmiştir. 2000 yılında AES (Advanced Encryption Standart - Gelişmiş Şifreleme Standartı) olarak adlandırılan yeni bir standart belirlenmiştir. AES şifreleme algoritması, 128, 192, 256 bitlik farklı anahtar uzunlukları kullanarak anahtar uzayının darlığı problemini gidermiş ve tasarımında kullanılan sonlu cisimlerin aritmetiği ile mevcut saldırılara karşı dirençli olduğu gösterilmiştir [64].

#### **2.1.2.2. Asimetrik Güven Modeli**

Simetrik şifreleme algoritmaları asimetrik şifreleme algoritmalarına göre daha hızlıdır. Ancak simetrik şifrelemenin en önemli problemi gönderici ve alıcı tarafların şifreli iletişime başlamadan önce güvenli bir anahtar belirleme gereksinimidir. Asimetrik güven modelinde bu problemi giderebilmek için iletişim taraflarının biri gizli diğeri açık olmak üzere iki anahtarları bulunmaktadır. Bu yolla anahtar değişim problemi çözülmüştür. Asimetrik şifreleme algoritmalarının gelişimi kriptoloji tarihinin en önemli gelişmelerinden birisidir. İlk örnekleri 1976 yılında Martin Hellman ve Whitfield Diffie adlı araştırmacılar tarafından önerilmiştir. Asimetrik şifreleme algoritmalarında anahtarların belirlenmesi çözümü zor matematiksel problemlere dayanmaktadır ve bu durum işlem yükünü artırmaktadır. Şifreleme işlemi açık anahtar kullanılarak yapılmaktadır. Asimetrik şifreleme algoritmalarının genel görünümü Şekil 2.3’te gösterilmiştir [58,64].



Şekil 2. 3. Asimetrik şifrelemenin genel yapısı

Şekil 2.3'te  $PK_R$  açık anahtarı,  $SK_R$  ise gizli anahtarı sembolize etmektedir. Denklem 2.3 ve 2.4'te asimetrik şifrelemenin genel yapısı verilmiştir.

$$C = E(M, PK_R) \quad (2.3)$$

$$M = D(C, SK_R) \quad (2.4)$$

### 2.1.2. Kripto Analiz

Kripto analiz, şifrelenmiş bir metni veya sistemi çözebilmek için yapılan bütün saldırıları inceleyen bilime verilen addır. Yani kripto analiz, şifrelenmiş bir sistemi inceleyerek şifrelenmiş olan mesajın açık halini elde etmeye çalışmaktadır. Kısaca şifre kırma bilimidir. Kripto analiz saldırıları genel olarak sosyal saldırılar, uygulama saldırıları ve klasik saldırılar olarak sınıflandırılabilir. Kriptoloji bilimi içerisinde oldukça önemli bir yere sahiptir [6]. Tezin bu kısmında klasik kripto analiz saldırılarından bahsedilmiştir.

İlk kripto analiz çalışması matematikçi Ebu Yusuf Yakup tarafından 9. yüzyılda önerilmiştir. İkinci Dünya Savaşında şifreleme cihazlarının yaygın olarak kullanılması sebebiyle kripto analiz biliminin önemi daha da artmıştır. İlk blok şifreleme algoritması örneklerinden olan Enigma cihazı, Alan Turing ve ekibi tarafından gerçekleştirilen kripto analiz saldırısı sonucu kırılmıştır [65].

Kripto analiz konusunda devrim yapan olay Kindi'nin yazmış olduğu “Şifreli Mesajların Kırılması Üzerine” adlı eserdir. Bu eserin bir bölümünde Frekans Analizi Yöntemine şöyle açıklık getirilmiştir: “Hangi dilde yazıldığı bilinen şifreli mesajları çözebilmek için; aynı dilde yazılmış bir sayfayı dolduracak uzunlukta farklı bir düz yazı bulmak ve bu yazıda her

bir harfin kaç kere geçtiğini saymak gerekir. En çok geçen harfe “birinci”, sonraki en çok geçen harfe “ikinci”, en çok geçen üçüncü harfe “üçüncü” şeklinde bütün harfler tanımlanarak sıralanmalıdır. Çözölmek istenen şifreli metin örnek metindeki sembollerle aynı şekilde sınıflandırılır. En çok geçen sembolün yerine örnek metindeki “birinci” harf, ikinci en çok geçen sembolün yerine “ikinci” harf konularak tüm harfler tamamlanana kadar devam edilir ve çözüm sağlanmaya çalışılır.”

Kripto analiz çalışması sırasında kriptoanaliz yapan kişinin elinde genellikle çok az bilgi vardır. Bu bilgilerin değişik durumları şunlardır:

**1. Şifrelenmiş Mesajın Analizi:** Kripto analiz yapan kişinin elinde sadece şifrelenmiş mesaj bulunmaktadır. Mesajın açık haliyle ilgili ipucu dahi yoktur.

**2. Tam Bir Açık Mesajın Analizi:** Kripto analiz yapan kişi mesajın hem açık hem de şifreli halinin tamamına sahiptir.

**3. Yarım Olarak Elde Edilmiş Açık Mesajın Analizi:** Kripto analiz yapan kişinin elinde mesajın açık halinin bir kısmı ile şifreli halinin tamamı mevcuttur.

**4. İstenen Açık Mesajın Şifrelenmiş Halinin Analizi:** Kripto analiz yapan kişi istediğinde, açık olan mesajın şifreli halini elde edebilmektedir.

**5. Şifrelenmiş Mesajın Şifreleme Algoritması Bilinerek Yapılan Analizi:** Kripto analiz yapan kişi mesajın hangi yöntemle şifrelendiği bilgisine sahiptir.

**6. Kaba Kuvvet Yöntemi:** Kriptografi bilminde bir şifreyi çözmek için kullanılan en temel saldırı yöntemidir. Bu yöntemde bütün ihtimaller tek tek veya belirli bir mantığa göre deneme yanılma yoluyla denenmektedir. Şifrenin çözölməsi zorluk derecesine göre zaman almaktadır. Eski bir yöntem olsa da günümüzde halen kullanılmaktadır. Günümüzde teknolojinin gelişmesiyle birlikte hesaplama imkânları da gelişmiştir ve şifreleme sistemlerinin kaba kuvvet saldırısına dayanıklı olabilmesi için anahtar uzunluklarının 128 bit ve üzeri olması gerekmektedir.

**7. Diferansiyel Kripto Analiz:** İlk kez 1990 yılında Eli Biham ve Adi Shamir tarafından yayımlanan “Des Benzeri Şifre Sistemlerinin Diferansiyel Kripto analizi (Differential Cryptanalysis of Des Live Cryptosystems)” adlı makalelerinde literatüre sunulan bir saldırı yöntemidir. Bu yöntem bilinen açık ve şifreli mesaj çiftleri arasındaki farkların hesaplanmasına dayanmaktadır [58,64,65].

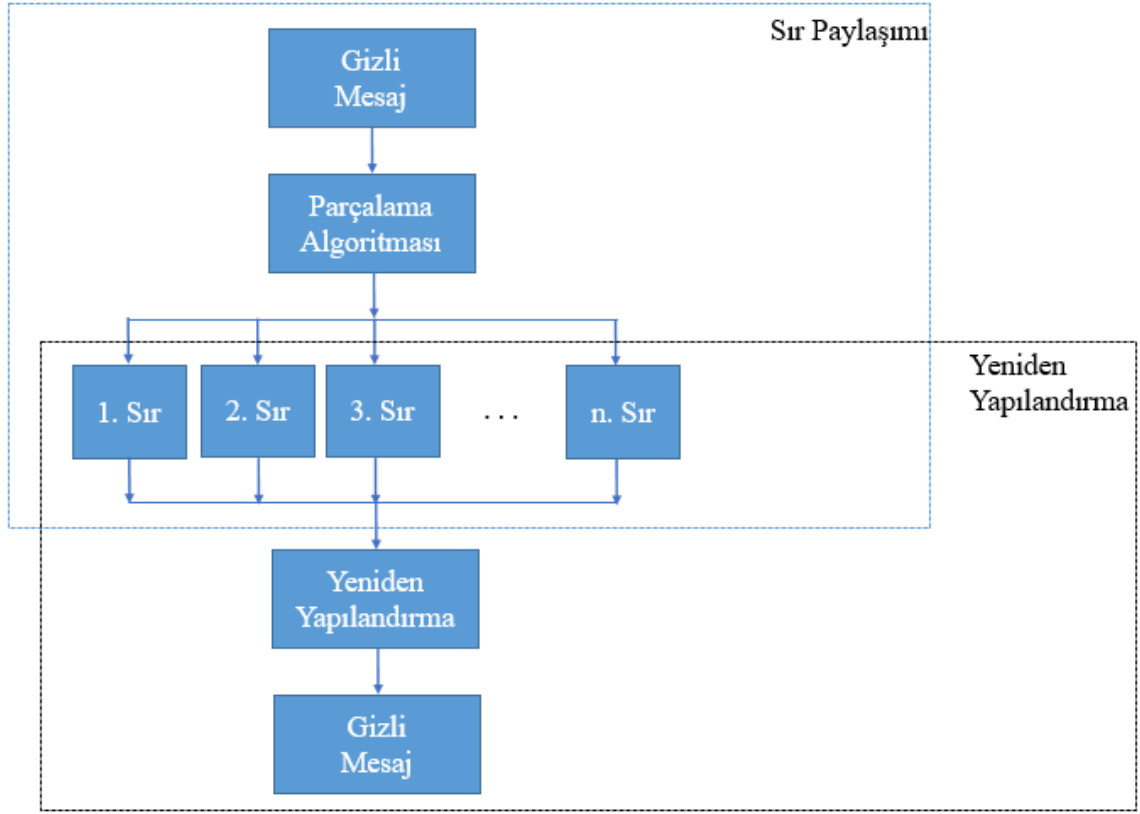
### 3. SIR PAYLAŞIMI

Gizli veriyi  $n$  katılımcı arasında paylaşmak için sır paylaşımı yöntemleri kullanılmaktadır. Sır paylaşımı yöntemlerinde, sır parçalarının dağıtımını yapan mekanizma güvenilir bir dağıtıcı olmalıdır. Gizli veri  $n$  parçaya ayrılır ve bir grup kullanıcı arasında dağıtılır. Bu grupta en az 2 kullanıcı olması gerekmektedir.  $n$  adet sır parçasından istenilen adette sır parçası bir araya gelince gizli veri elde edilmektedir.

Sır paylaşım algoritmaları sır paylaşımı ve yeniden yapılandırma olmak üzere iki adet alt algoritmadan meydana gelmektedir. Sır paylaşımı algoritmalarında gizli verinin paylaşılması ve dağıtılmasından sorumlu olan mekanizmaya dağıtıcı denir ve dağıtıcının güvenilir olması gerekmektedir. Yeniden yapılandırma aşamasında ise önceden belirlenen sayıda sır sahibinin bir araya gelmesi gerekmektedir.  $k$  adet sır sahibi bir araya geldiğinde gizli veri elde edilmektedir.

Shamir ve Blackley, 1979 yılının ayrı zamanlarında eşik tabanlı sır paylaşım şemasını önermiştir [66,67].  $(k,n)$  eşik şeması olarak isimlendirilen yöntemler, gizli verinin  $n$  kişi arasında paylaşılmasına dayanmaktadır. Gizli verinin yeniden elde edilebilmesi için en az  $k$  adet katılımcının bir araya gelmesi gerekmektedir.  $k$ 'dan az katılımcı bir araya geldiğinde ise sır parçası yeniden elde edilemez.

Sır paylaşım algoritmalarının gerçekleştirmesindeki önemli konulardan biri katılımcılara dağıtılacak olan pay değerinin büyüklüğüdür. Gizli tutulması gereken bilgi miktarı arttıkça sistemin güvenliği azalmaktadır. Bu nedenle pay değerlerinin büyüklüğü sır paylaşım şemalarının tasarımındaki anahtar noktalardan biridir. Sır paylaşımındaki önemli parametrelerden biri ortalama bilgi oranı  $\rho$ , katılımcılara gönderilecek olan pay büyüklüklerinin gizli verinin büyüklüğüne oranı olarak hesaplanmaktadır. Sır paylaşım şemalarında, pay bilgileri, hiçbir zaman gizli veriden küçük olamaz. Sır paylaşım algoritmalarının genel blok diyagramı Şekil 3.1'de verilmiştir.



Şekil 3. 1. Sır paylaşım algoritmalarının blok diyagramı

### 3.1. Shamir'in Sır Paylaşımı Algoritması

Sır paylaşımı konusunda yapılan çalışmalar 1979 yılında Adi Shamir ile başlamıştır. Shamir'in yöntemi polinom tabanlı olup rastgele seçilen parametreler üzerine kuruludur. Shamir oluşturduğu sır paylaşım modelinde  $(k,n)$  eşik yöntem kavramını ortaya çıkartmıştır.  $(k,n)$  eşik yönteminde bulunan  $n$  değeri pay sahiplerinin sayısını göstermekte iken  $k$  değeri ise sır değerinin ortaya çıkabilmesi için kaç adet pay sahibinin bir araya gelmesi gerektiğini göstermektedir. Bu tip algoritmalarda  $2 \leq k \leq n$  şartının sağlanması gerekmektedir. Shamir  $(k,n)$  sır paylaşım algoritmasının adımları aşağıdaki gibidir.

**Adım 1:** Sır paylaşımı uygulanacak veri belirlenir ve gizli veri olarak adlandırılır.

**Adım 2:**  $(k,n)$  eşik yönteminde  $k$  ve  $n$  parametreleri belirlenir.

**Adım 3:** Gizli veriyi parçalamak için gerekli fonksiyon oluşturulur.

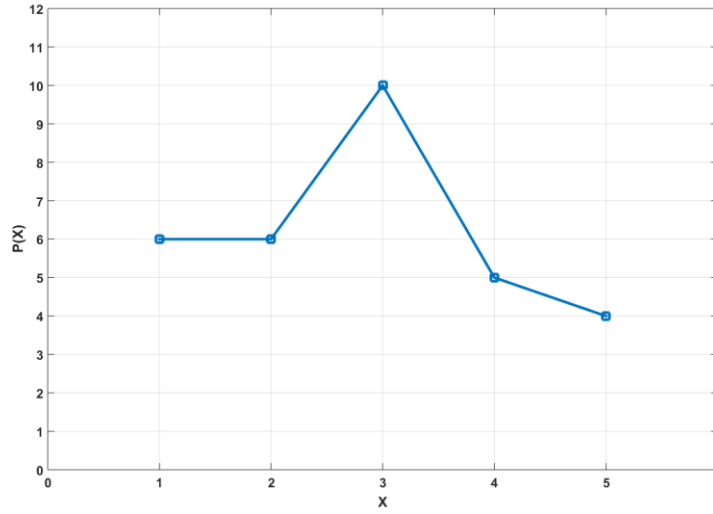
**Adım 4:** Gizli veriyi yeniden elde edebilmek için gerekli fonksiyon oluşturulur.

**Adım 5:** Gizli veri  $n$  adet sır parçasına bölünür.

Shamir'in algoritmasında ifade edilen  $(k,n)$  eşik yönteminde kullanılan polinomun derecesi  $k-1$ 'dir ve bu polinom Denklem 3.1'de verilmiştir [66].

$$P(x) = a_0 + a_1x + a_2x^2 \dots + a_{k-1}x^{k-1} \pmod{p} \quad (3.1)$$

Yukarıdaki denklemde p değeri asal sayı olmak zorundadır. Bunun sebebi ise geri dönüş esnasında tek bir değer üretme ihtimalini garantilemektir. a katsayıları  $[0,p-1]$  arasında rastgele üretilen dizi elemanlarıdır. Polinom ise x değerlerinden üretilmiştir. Örneğin gizli veri 10 sayısını (3,5) eşik şeması kullanılarak paylaştırılması için  $P(x) = 10 + 7x + 2x^2 \pmod{13}$  seçilmiştir.  $Z_{13}$  alanında tanımlı olan bu sır paylaşımı şemasının değerleri Şekil 3.2'deki gibidir.



Şekil 3. 2. Shamir (3,5) sır paylaşımı algoritmasının örnek gösterimi

Şekil 3.2'de gösterilen yöntemde 5 adet sır parçası oluşturulmuştur ve bu sır parçalarının 3 tanesi bir araya geldiğinde gizli veri elde edilecektir. Gizli veriyi yeniden elde etmek için Langrange interpolasyonu kullanılmaktadır. Denklem 3.2'de Langrange interpolasyon formülü verilmiştir.

$$S = \sum_{i \in A} \left( I_i \cdot \prod_{j \in A - \{i\}} \frac{x_j}{x_j - x_i} \right) \pmod{p} \quad (3.2)$$

Denklemde A elde oluşturulan fonksiyona göre elde edilen noktalar kümesini temsil etmektedir.  $A = \{\{1,6\}, \{2,6\}, \{3,10\}, \{4,5\}, \{5,4\}\}$  kümesi elde edilmiştir. A kümesinin 1, 3 ve 4. elemanları seçildiğinde ise gizli veri aşağıdaki gibi elde edilmektedir.

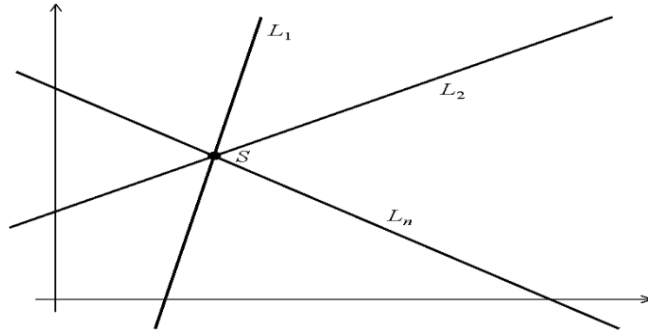
$$S = 6 \cdot \frac{3}{3-1} \cdot \frac{4}{4-1} + 10 \cdot \frac{1}{1-3} \cdot \frac{4}{4-3} + 5 \cdot \frac{1}{1-4} \cdot \frac{3}{4-3} \pmod{13} = 10 \quad (3.3)$$

### 3.2. Blakley'in Sır Paylaşımı Algoritması

Shamir, polinomal interpolasyon kullanarak gizli veriyi sır parçalarına ayırmaktadır. Blackley ise gizli veriyi hiper boyutlu vektör uzayının elemanı olarak tanımlamıştır. Sır sahiplerine dağıtılacak sır parçaları ise  $k-1$  boyutlu bir vektör uzayından türetilen elemanlardır. Galois vektör uzayında Blackley'in sır paylaşım yöntemi Denklem 3.4'te verilmiştir.

$$\{(x_1, x_2, \dots, x_k) \in GF_q^k \mid a_1x_1 + a_2x_2 + \dots + a_kx_k = \beta\} \quad (3.4)$$

$a_1, a_2, \dots, a_n$  ve  $\beta$  değerleri galois uzayının elemanlarıdır ve sır parçalarını tanımlamak için kullanılırlar. Gizli veri  $k$  adet sır parçasının bir araya gelmesi sonucunda oluşmaktadır. Şekil 3.3'te  $(2,n)$  Blackley sır paylaşım algoritmasının geometrik düzlemde tanımlanması gösterilmiştir [67].

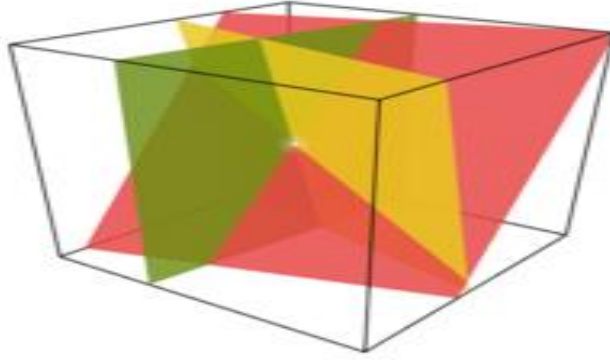


Şekil 3. 3. Blakley (2,n) sır paylaşım algoritmasının geometrik gösterimi

Örneğin gizli veri üç boyutlu uzayda  $(2,5,8)$  koordinatları ile gösterilen bir nokta olsun ve  $(3,3)$  sır paylaşımı algoritması kullanılsın. Denklem  $2a_1 + 5a_2 + 8a_3 = \beta$  olarak elde edilir. Denklemi sağlayacak üç farklı parametre kümesi  $(a_1, a_2, a_3, \beta)$  sır sahiplerine gönderilir. Sır parçaları sırasıyla  $(1, 2, 3, 36)$ ,  $(3, 4, 2, 42)$  ve  $(10, 2, 5, 70)$  şeklinde olsun. Üretilen sır parçaları 3 boyutlu uzayda birbirlerini kesen düzlemlerdir ve Şekil 3.4'te gösterilen düzlemlere benzemektedir. Katsayıları yeniden elde etmek için aşağıdaki Denklem 3.5 kullanılmalıdır.

$$\begin{bmatrix} a_1 \\ a_2 \\ a_3 \end{bmatrix} = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 4 & 2 \\ 10 & 2 & 5 \end{bmatrix}^{-1} \times \begin{bmatrix} 36 \\ 42 \\ 70 \end{bmatrix} = \begin{bmatrix} 2 \\ 5 \\ 8 \end{bmatrix} \quad (3.5)$$

Shamir'in sır paylaşımı şemasına göre, sır parçaları hakkında daha fazla bilgi elde edilebilmekte ve daha basit bir matematiksel temelleri kullandığı için, Shamir'in yöntemine göre kolaylıkla analiz edilebilmektedir.



Şekil 3. 4. Blakley (3,3) sır paylaşım algoritmasının 3 boyutlu geometrik düzlemde gösterimi

### 3.3. Mignotte'nin Sayı Teorisi Tabanlı Sır Paylaşımı Algoritması

Bu algoritmada, Mignotte'nin sırası olarak adlandırılan sayı dizisi kullanılarak  $(k,n)$  sır paylaşımı modeli oluşturulmuş. Sır paylaşımı algoritmasını oluşturmak için birbirleri arasında asal olan  $n$  adet tamsayı kullanılmıştır. Önerilen algoritmanın kuralları Denklem 3.6 ve 3.7'de verilmiştir.

$$p_1 < p_2 < \dots < p_n \quad (3.6)$$

$$\prod_{i=0}^{k-2} p_{n-i} < \prod_{i=1}^k p_i, \quad (3.7)$$

Gizli veri  $S$   $\prod_{i=0}^{k-2} p_{n-i} < S < \prod_{i=1}^k p_i$  şartını sağlamalıdır. Sır parçaları ise Denklem 3.8 kullanılarak hesaplanmaktadır.

$$I_i = S \pmod{p_i}, 1 \leq i \leq n \quad (3.8)$$

Yeniden yapılandırma aşamasında ise  $k$  adet sır parçasının bir araya gelmesi yeterlidir. Yeniden yapılandırma için Çin Kalan Teoremi (ÇKT) uygulanmaktadır [68]. Örneğin (3,5)'lik bir sır paylaşımı yönteminde gizli veri 725 seçilsin. Sayıların aralarında asal olması

için 9, 11, 14, 19 ve 23 mod değerleri seçilsin. Mod değerleri uygulandığında elde edilen değerler sırasıyla 5, 10, 11, 3, 12 değerleridir ve bu değerler sır parçaları olarak kullanılmaktadır. Yeniden yapılandırma aşamasında ise ÇKT kullanılarak 725 değerine ulaşılır. Örneğin ilk üç sır parçasının bir araya getirildiği varsayalım.

$$x = 5 \pmod{9} \tag{3.9}$$

$$x = 10 \pmod{11}$$

$$x = 11 \pmod{14}$$

### 3.4. Asmuth-Bloom Sır Paylaşımı Algoritması

Asmuth-Bloom 1983 yılında Mignotte'nin sır paylaşımı şemasına benzeyen bir algoritma önermiştir [69]. Aralarında  $n+1$  asal sayı Denklem 3.10'da verilen şartı sağlayacak şekilde seçilmelidir.

$$p_0 \cdot \prod_{i=0}^{k-2} p_{n-i} < \prod_{i=0}^k p_i \tag{3.10}$$

Sır sahiplerine gönderilecek sır parçalarıyla ilişkili asal sayıların bilinmesi, algoritmanın düzgün çalışmasını sağlayacaktır. Gizli veri  $S$  tamsayı uzayından seçilecek bir sayı olmalıdır ve sır sahiplerine yollanacak sır parçaları  $I_i = S + \alpha \cdot p_0 \pmod{p_i}$  olarak hesaplanmaktadır. Yeniden yapılandırma aşamasında ise ÇKT kullanılmaktadır.

### 3.5. Toplama Tabanlı Sır Paylaşımı Algoritması

Bu algoritmada gizli veri  $n$  adet kullanıcıya dağıtılmaktadır. Yukarıda sayılan algoritmalara göre daha basit bir matematiksel temele dayanmaktadır.  $(n,n)$  sır paylaşımı şeması olan bu algoritmanın adımları aşağıdaki gibidir.

**Adım 1:**  $q$  adında büyük bir asal sayı seçilir.

**Adım 2:** Güvenilir bir rastgele sayı üretici kullanılarak  $n-1$  adet sır üretilir. Üretilen sır kümesi  $s_1, s_2, \dots, s_{n-1}$  olarak adlandırılır.

**Adım 3:** Son sır parçası Denklem 3.11 kullanılarak elde edilir.

$$s_n = s - \sum_{i=1}^{n-1} s_i \pmod{q} \quad (3.11)$$

**Adım 4:** Tüm sır parçaları sır sahiplerine dağıtılır.

Bu algoritmanın yeniden yapılandırma aşamasında ise sır parçaları biraraya getirilerek toplanır ve  $q$ 'ya göre modu alınır. Yeniden yapılandırma işlemi Denklem 3.12'de verilmiştir [70].

$$s = \sum_{i=1}^n s_i \pmod{q} \quad (3.12)$$

Bu algoritma olasılıksal sır paylaşımının temelini oluşturmaktadır. Bu algorithmada kullanılan toplama işleminin yerine ve (AND), veya (OR), özel veya (XOR) gibi boolean operatörleri de kullanılmaktadır.

#### 4. GÖRSEL SIR PAYLAŞIMI

Güvenilir sayısal görüntülemeyi sağlamak için kriptoloji ve sayısal görüntü işleme tekniklerinin bir arada kullanıldığı hibrit yöntemler geliştirilmiştir. Görsel sır paylaşımı ve gizli görüntü paylaşımı, güvenilir sayısal görüntüleme yöntemlerinin başında gelmektedir.

Görsel Sır Paylaşımı (GSP) sır paylaşımını temel alan bir multimedya güvenlik yöntem bilimidir. GSP, ilk olarak 1994 yılında Naor ve Shamir [71] tarafından sunulmuştur. GSP'nin en önemli özelliklerinden birisi, karmaşık matematiksel işlemlere gereksinim duymadan bilgi güvenliğini sağlamasıdır. GSP deterministik ve olasılıksal olarak ikiye ayrılmaktadır. Deterministik GSP şemalarında, sır parçalarını oluşturacak alt pikseller bellidir. Olasılıksal GSP şemalarında ise alt pikseller olasılık tabanlı seçilir. Deterministik GSP şemalarında mükemmel kontrast ayarı yapılmaya çalışılırken, olasılıksal GSP şemalarında alt piksellerin uniform şekilde kullanılması istenmektedir.

GSP şemalarında da sır paylaşım şemalarında olduğu gibi  $(k,n)$  ve  $(n,n)$  sır paylaşımı şemaları oluşturulmaktadır.  $(k,n)$  GSP şemalarında  $n$  adet sır parçasında  $k$  tanesinin bir araya gelmesiyle gizli veri elde edilmektedir.  $(n,n)$  GSP şemalarında ise gizli veriyi elde edebilmek için tüm sır parçalarının bir araya gelmesi gerekmektedir.

Naor ve Shamir'in GSP şeması siyah beyaz imgelerde uygulanmış ve yıllar geçtikçe bu şemanın eksiklikleri ortaya çıkmıştır. Bu problemleri iyileştirmek için ise literatürde birçok yöntem geliştirilmiştir [72-74].

GSP şemalarının yalnızca siyah beyaz imgelere değil gri seviyeli ve renkli imgelere de uygulanabileceği gösterilmiştir. Ayrıca çoklu GSP şemalarıyla, sır parçalarının bir araya gelmesiyle birden fazla gizli verinin elde edilebileceği gösterilmiştir.

Özellikle Deterministik GSP mükemmel kontrastı sağlamalarına karşın, kullanılan alt piksellerden ötürü sır parçalarının kapasiteleri artmaktadır ve büyüyen sır parçaları veri iletim hattının verimli kullanılmasının önünde en büyük engeldir. Bu problemi çözebilmek için olasılıksal GSP şemaları kullanılmaktadır.

GSP şemalarında karşılaşılan bir diğer problem ise, alt piksellerin gürültü benzeri olmasıdır. Gürültü benzeri oluşan sır parçaları saldırganların dikkatini çekmektedir ve bu sır parçalarına karşı çeşitli ataklar yapılmaktadır. Bu atakların başında gelen atak ise sahtecilik atağıdır. Sahtecilik atağında veri hattındaki bir sır parçası ele geçirilir. Ele geçirilen imge gürültü benzeri mükemmel kontrasta sahip bir imge olduğu için saldırgan bu imgenin sır

parçası olduğunu farkeder. Gönderilecek gizli mesajı değiştirmek için farklı bir mesaj üretir ve bu gizli mesajı sır parçalarına ayırarak alıcıya gönderilir. GSP geliştiricileri bu atağın önüne geçebilmek için, kimlik doğrulama tabanlı GSP şemaları önermiştir. Ancak bu öneri GSP'nin kapsamını daraltmaktadır. Bu sebepten dolayı GSP tabanlı veri gizleme algoritmaları ve anlamlı alt piksellerden oluşmuş GSP şemaları önerilmiştir. Tezin bu bölümünde literatürde sıklıkla kullanılan GSP şemaları anlatılmıştır.

#### 4.1. Naor ve Shamir'in Görsel Sır Paylaşımı Şeması

Literatürde ilk olarak önerilen GSP şeması 1994 yılında Eurocrypt konferansından Naor ve Shamir tarafından önerilen GSP şemasıdır. Bu şema ikili imgeler üzerinde uygulanmaktadır. P imgesini sır parçalarına ayırabilmek için nokta operatörü kullanılır ve tüm pikseller üzerinde işlem yapılır. Alt pikseller seçilirken kontrast ayarının yapılması gerekmektedir. Mükemmel kontrastı sağlamak için seçilen alt piksellerin yarısının 0, yarısının 1 olması gerekmektedir. OR operatörünün kuralları kullanılarak sır paylaşımı işlemleri yapılmaktadır. Alt piksel olarak 1 x 2 veya 2 x 2 boyutunda bloklar kullanılmaktadır. Sır parçası oluşturmak için kullanılan alt pikseller Şekil 4.1'de verilmiştir [71].

| B | Sır 1 | Sır 2 | Sonuç |  | Sır 1 | Sır 2 | Sonuç |
|---|-------|-------|-------|--|-------|-------|-------|
|   |       |       |       |  |       |       |       |
|   |       |       |       |  |       |       |       |
|   |       |       |       |  |       |       |       |
|   |       |       |       |  |       |       |       |
|   |       |       |       |  |       |       |       |
|   |       |       |       |  |       |       |       |

Şekil 4. 1. Alt piksellerin kodlanması [71].

Bu şema, literatürde ki diğer şemalara ilham kaynağı olmuş ve kuralları hala kullanılan bir şemadır ancak birçok problemi bulunmaktadır. Problemlerinden birisi sır parçalarını genişletmesidir. Örneğin gizli veri 100 x 100 boyutunda bir siyah beyaz imge ise bu şema

kullanılarak elde edilecek sır parçaları 200 x 200 boyutunda olacaktır. Bu durum veri iletim hattının verimli kullanılamamasına yol açmaktadır. Ayrıca önerilen bu şema sadece siyah beyaz imgelere uygulanabilmektedir. Gri seviyeli veya renkli imgelere uygulamak için, imgenin bit seviyelerine ayrılması gerekmektedir. Ayrıca oluşturulan sır paylaşımı şeması sadece tek bir gizli veri için sır parçaları üretmektedir.

#### **4.2. Wu ve Chen'in Çoklu Görsel Sır Paylaşımı Şeması**

Naor ve Shamir'in önerdiği GSP şemasının ardından, Wu ve Chen [75] 2 sır parçasında 2 gizli mesaj taşıyabilen bir GSP şeması önermiştir.  $N \times N$  boyutunda 2 adet gizli mesaj için 2 adet sır parçasının üretilmesi önerilmiştir. Alt pikseller ise  $2 \times 2$  boyutundadır. İlk gizli mesajın üretilmesi için sır parçalarının OR işlemine tabi tutulması gerekmektedir. İkinci gizli mesajı elde edebilmek için ise İlk gizli mesajı oluşturan alt piksellerin  $90^\circ$  döndürülüp ikinci sır parçasının alt piksellerine OR operatörünün uygulanması gerekmektedir. Sır parçalarını oluşturabilmek için Şekil 4.2'deki tablonun kullanılması gerekmektedir.

| $P_1$                                                                              | $P_2$                                                                              | Olasılık | $S_1$                                                                               | $S_1^{90}$                                                                          | $S_2$                                                                               | $S_1   S_2$                                                                          | $S_1^{90}   S_2$                                                                      |
|------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|----------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------|
|   |   | 1/4      |    |    |    |    |    |
|                                                                                    |                                                                                    | 1/4      |    |    |    |    |    |
|                                                                                    |                                                                                    | 1/4      |    |    |    |    |    |
|                                                                                    |                                                                                    | 1/4      |    |    |    |    |    |
|   |   | 1/4      |    |    |    |    |    |
|                                                                                    |                                                                                    | 1/4      |    |    |    |    |    |
|                                                                                    |                                                                                    | 1/4      |    |    |    |    |    |
|                                                                                    |                                                                                    | 1/4      |    |    |    |    |    |
|   |   | 1/4      |    |    |    |    |    |
|                                                                                    |                                                                                    | 1/4      |    |    |    |    |    |
|                                                                                    |                                                                                    | 1/4      |    |    |    |    |    |
|                                                                                    |                                                                                    | 1/4      |    |    |    |    |    |
|  |  | 1/4      |    |    |    |    |    |
|                                                                                    |                                                                                    | 1/4      |   |   |   |   |   |
|                                                                                    |                                                                                    | 1/4      |  |  |  |  |  |
|                                                                                    |                                                                                    | 1/4      |  |  |  |  |  |

Şekil 4. 2. Wu ve Chen'in GSP şeması için kullanılan kod tablosu

Bu şemanın önerilmesiyle birlikte literatürde birçok çoklu GSP önerilmiştir ancak Wu ve Chen'nin GSP şeması diğer çoklu GPS şemalarının temelini oluşturmaktadır.

#### 4.3. Rastgele Izgaralar

Rastgele ızgaraları kullanan GSP şemaları diğer GSP şemalarına göre daha farklı bir yapıdadır. Analiz tabanlı yöntemler olup ilk olarak 1987 yılında Kafri ve Karen [76] tarafından önerilmiştir ancak 1987 yılında GSP şemaları önerilmediği için bu yöntem GSP şemaları içerisinde yer almamıştır. 2007 yılında Shyu [77] bu yöntemi yeniden keşfederek GSP şemalarına dâhil etmiştir. Rastgele ızgaralarda piksel genişleme katsayısı 1'dir yani kullanılan alt pikseller piksel boyutundadır. Bir rastgele ızgara R olarak tanımlanan 2 boyutlu bir dizidir. Her piksel yazı tura prosedürüyle veya güvenilir bir rastgele sayı üreticiyle üretilmiş 0 veya 1'lerden oluşmaktadır. Burada önemli olan husus, piksellerin 0 veya 1 olma olasılığının 0.5'e eşit olması gerekmektedir. Eğer kullanılan sözlük boyutu

büyükse, olasılığın 0.5'e yaklaştırılması gerekmektedir. Ayrıca bu yöntem kullanılarak yarıton imgelere sır paylaşımı uygulanabilmektedir. Rastgele ızgaralar kullanılarak oluşturulan sır parçaları ve yeniden yapılandırılmış imge Şekil 4.3'te verilmiştir.



Şekil 4. 3. Rastgele ızgaralar tabanlı GSP örneği

#### 4.4. Wang'ın Olasılıksal Görsel Sır Paylaşımı Şeması

Olasılıksal GSP şemalarında rastgele ızgaralarda olduğu gibi rastgele matrisler oluşturulur ve bu matrisler kullanılarak sır paylaşımı yapılır. Olasılıksal GSP'lerde sır parçaları piksel genişleme katsayısı 1'dir. Sır parçalarının gizli veriyle aynı boyutta olması belleğin ve iletim hattının daha verimli kullanılabileceğini göstermektedir. Bu tip şemalarda uniform özellik gösteren rastgele sayı üreteçlerinin kullanılmasıyla istenilen kontrast değeri de sağlanmaktadır. Olasılıksal GSP'ler  $(k,n)$  ve  $(n,n)$  şemalarını oluşturulma imkanı da sağlamaktadır. Ayrıca olasılıksal GSP şemaları gri seviyeli ve renkli imgelere de uygulanabilmektedir.

Olasılıksal GSP şemalarında literatürde en fazla kullanılan yöntem Wang'ın olasılıksal GSP şemasıdır. Bu şema AND, OR veya XOR gibi mantıksal operatörleri kullanmaktadır. Wang'ın  $(n,n)$  sır paylaşım şemasının adımları aşağıdaki gibidir [78].

**Adım 1:** A adında gizli verinin boyutunu elde et.

**Adım 2:** Gizli veri boyutunda  $n-1$  adet rastgele matris üret  $B_1, B_2 \dots B_{n-1}$ .

**Adım 3:**  $n$  adet sır parçası üret.  $A_1 = B_1$ ,  $A_i = B_i \oplus B_{i-1}$  ve  $A_n = B_{n-1} \oplus A$

**Adım 4:** Elde edilen sır parçalarını sır sahiplerine dağıt.

**Adım 5:** Gizli veriyi yeniden elde edebilmek için tüm sır parçalarına XOR operatörü uygula.

Yukarıda verilen algoritmanın adımları değiştirilerek  $(k,n)$  şemalar elde edilebilmektedir.  $(k,n)$  şemalarının oluşturulabilmesi için kombinasyonların doğru hesaplanması ve bu kombinasyonlara göre kuralların tanımlanması gerekmektedir.

#### **4.5. Harf Tabanlı Görsel Sır Paylaşımı Şeması**

GSP şemalarında alt piksellerin mükemmel kontrastı sağlamak için ayarlanmasından dolayı oluşan sır parçaları gürültü benzeri olmaktadır. Gürültü benzeri sır parçaları saldırganların dikkatini çekmektedir. Saldırganların dikkatini çekmeden gizli veriyi alıcı tarafa göndermek için harf tabanlı GSP şemaları önerilmiştir. Harf tabanlı GSP şemalarında doğal dillerde kullanılan harfler alt piksel olarak kullanılmaktadır. Böylece gürültü benzeri sır parçaları yerine anlamlı parçalardan oluşan sır parçaları oluşturulmuştur.

Takizawa ve ark. Japon harflerini kullanan iki adet sır paylaşımı yöntemi önermiştir. İlk yöntemde bir veritabanı oluşturulmuştur. Oluşturulan veritabanı kullanılarak harflerin morfolojik analizi gerçekleştirilmiştir. Belirlenen harfler döndürülerek, sır parçaları elde edilmiştir. Takizawa vd. İkinci yaklaşımında ise, doğal dillerdeki harfler kullanılarak anlamlı cümleler elde edilmiştir. Anlamlı cümleler sır parçaları olarak kabul edilmiştir. Birden fazla anlamlı cümlelerin bir araya gelmesiyle mesaj elde edilmiştir [79].

磁極盛磁管湯に漸磁磁固本粒計が原対察  
 義高臨難分着駅在電磁磁修煩欄程磁前表  
 波が種種作も産妻るが電会類類業研技係。  
 電電離疎波数磁場磁随磁磁電の茨茅磁で  
 磁す磁離離新城磁重離再重信上

(a)

分散テキスト1 ...方向の臨界周波数目盛の0MHzを示す。...  
 分散テキスト2 ...温秋田電波観測所山岡己雄郵政大臣表彰を...  
 ... 国鉄東北本線古河駅より東、筑波山に向...  
 ...土達により10年程前に紹介されている。...  
 ...いう面で、その施策が不十分であったと認...  
 ...、別に関係する各学会の雑誌もあり、また...  
 ...な研究成果の発表の場としては、別に関係...  
 ...うとの意に出たものである。最近は、本来...  
 ...究所ニュース」と題する一般広報用小冊子...  
 ...行することになった。皆さんは何と聞くで...

(b)

Şekil 4. 4.Takizawa vd. (a) ilk şeması (b) ikinci şeması [79].

Lin ve ark. Çince, Korece, Japonca ve Latince'de bulunan harfleri kullanan bir görsel sır paylaşımı yöntemini önermiştir. Bu yöntem temel olarak Shamir'in (k,n) görsel sır paylaşımını temel almaktadır. Alt pikseller, harflerden oluşmaktadır. Oluşturulan şemanın örneği Şekil 4.5'te verilmiştir [48].

李奧納多·達·芬奇是一位義大利文藝復興時期的多項領域博學專家，同時是建築師、解剖學者、藝術家、工程師、數學家、發明家。他無窮的好奇與創意使得他成為文藝復興時期典型的藝術家，而且也是歷史上最著名的畫家之一。他與米開朗基羅和拉斐爾並稱為文藝復興藝術三傑。達芬奇的父母為地主與農婦，他在義大利佛羅倫斯附近的文西出生。與長大後，達芬奇以其畫作寫實性和極具影響力聞名。前者如蒙娜麗莎最後的晚餐，以寫實著稱；後者像這科魯威人對後世影響深遠。他具有超越當時的廣泛構思，著名的概念性發明比方直昇機、坦克、太陽能飛機等使用計算機模擬造詣基本原理解釋等許多構想。但在他的生平中這麼多的設計只有少數能建造出來或具體可行。現代科學所用的冶金及工程學技術在文藝復興時代方處於萌芽期。他的作品中有極少數畫作流傳下來，加上散佈在形形色色收藏中，包括了繪畫、科學示意圖、筆記的手稿。目前已知最早有日期紀錄的達芬奇作品是以阿莫谷的筆及墨水繪成的畫作，在一四七六年至一四七八年間。達芬奇接受了兩件畫作，由此開始當時他有一間自己的工作室。大約在一四八二年至一四九八年間，米蘭公爵斯福爾扎達·法蘭西斯科·斯福爾扎將他安置在一個位置，就是一四九五年米蘭公爵企圖拯救米蘭免受法國查理八世統治，將七十個銅鑄造成武器，而這些材料原本是達芬奇打算用來製作雕塑。法國回國後，路易十二世統治時，米蘭不戰而降。達芬奇仍在米蘭待了一段時間，直到有一天，當他發現馬蘭卡萊羅的寶物大小粘土模型被法國弓箭手拿來當作標靶練習。達芬奇在威尼西亞，達芬奇被聘為軍事工程師，繼續科學工程領域。就像他的藝術作品般令人難忘，與突出手稿中約一萬三千頁的筆記與繪畫全是混合藝術與科學所組成的紀錄。在科學上，他是一個極細靡遺的觀察家，能以極精細的描述手法表示一個現象，但卻不是透過理論與實驗來驗證。同時期的學者大多未注意到在科學領域中

(a)

李奧納多·達·芬奇是一位義大利文藝復興時期的多項領域博學專家，同時是建築師、解剖學者、藝術家、工程師、數學家、發明家。他無窮的好奇與創意使得他成為文藝復興時期典型的藝術家，而且也是歷史上最著名的畫家之一。他與米開朗基羅和拉斐爾並稱為文藝復興藝術三傑。達芬奇的父母為地主與農婦，他在義大利佛羅倫斯附近的文西出生。與長大後，達芬奇以其畫作寫實性和極具影響力聞名。前者如蒙娜麗莎最後的晚餐，以寫實著稱；後者像這科魯威人對後世影響深遠。他具有超越當時的廣泛構思，著名的概念性發明比方直昇機、坦克、太陽能飛機等使用計算機模擬造詣基本原理解釋等許多構想。但在他的生平中這麼多的設計只有少數能建造出來或具體可行。現代科技所需的冶金及工程技術在文藝復興時代方處於萌芽期。他的作品中有極少數畫作流傳下來，加上散佈在形形色色收藏中，包括了繪畫、科學示意圖、筆記的手稿。統計至今，最早有收藏紀錄的達芬奇作品所採用山谷的筆及墨水繪成的畫作，在一四七六年至一四七八年間。達芬奇接受了兩件畫作，由此開始當時他有一間自己的工作室。大約在一四八二年至一四九八年間，米蘭公爵斯福爾扎達·法蘭西斯科·斯福爾扎將他安置在一個位置，就是一四九五年米蘭公爵企圖拯救米蘭免受法國查理八世統治，將七十個銅鑄造成武器，而這些銅鑄本來是藝術家打算用來製作雕塑。法國回國後，路易十二世統治時，米蘭不戰而降。達芬奇仍在米蘭待了一段時間，直到有一天早上，他在意馬蘭卡萊羅品種蘭花與粘土模型被法國弓箭手拿來當作標靶練習。達芬奇在威尼西亞，達芬奇被聘為軍事工程師，繼續科學工程領域。就像他的繪畫同樣令人難忘，與突出手稿中絕大部份的理論構想與敘述全是混合藝術與科學所組成的紀錄。在科學上，他是一個極細靡遺並且細心的觀察者，其描述手法表示一個現象，但又符合於理論與實驗來驗證。同時期的學者幾乎都忽略了在科學領域中

(b)

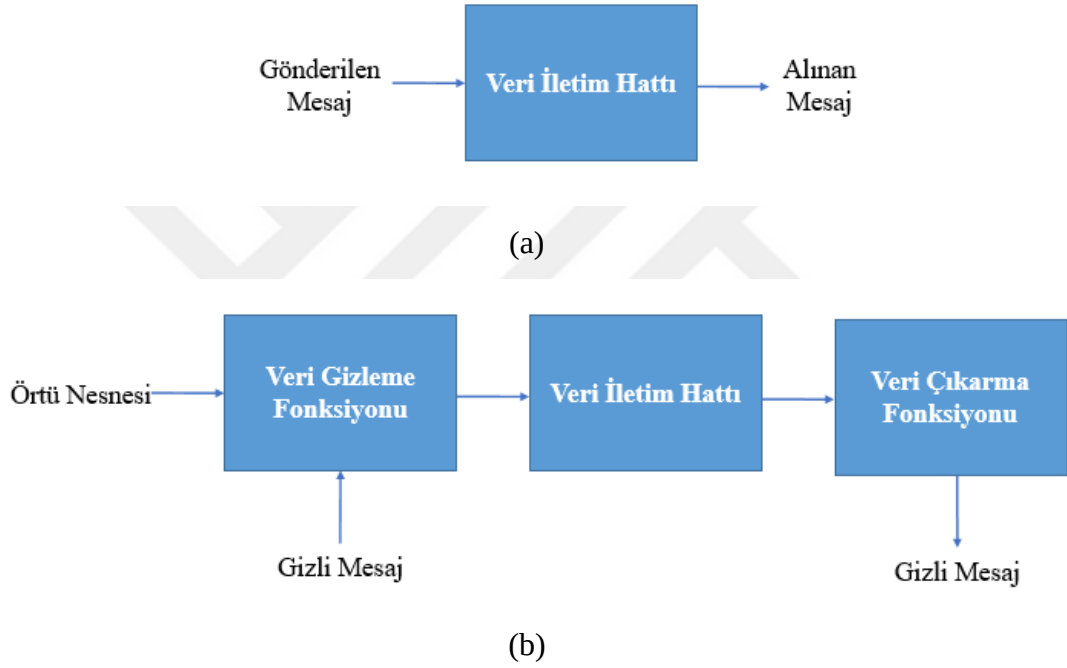
李奧納多·達·芬奇是一位義大利文藝復興時期的多項領域博學專家，同時是建築師、解剖學者、藝術家、工程師、數學家、發明家。他無窮的好奇與創意使得他成為文藝復興時期典型的藝術家，而且也是歷史上最著名的畫家之一。他與米開朗基羅和拉斐爾並稱為文藝復興藝術三傑。達芬奇的父母為地主與農婦，他在義大利佛羅倫斯附近的文西出生。與長大後，達芬奇以其畫作寫實性和極具影響力聞名。前者如蒙娜麗莎最後的晚餐，以寫實著稱；後者像這科魯威人對後世影響深遠。他具有超越當時的廣泛構思，著名的概念性發明比方直昇機、坦克、太陽能飛機等使用計算機模擬造詣基本原理解釋等許多構想。但在他的生平中這麼多的設計只有少數能建造出來或具體可行。現代科學所用的冶金及工程技術在文藝復興時代方處於萌芽期。他的作品中有極少數畫作流傳下來，加上散佈在形形色色收藏中，包括了繪畫、科學示意圖、筆記的手稿。統計至今，最早有收藏紀錄的達芬奇作品所採用山谷的筆及墨水繪成的畫作，在一四七六年至一四七八年間。達芬奇接受了兩件畫作，由此開始當時他有一間自己的工作室。大約在一四八二年至一四九八年間，米蘭公爵斯福爾扎達·法蘭西斯科·斯福爾扎將他安置在一個位置，就是一四九五年米蘭公爵企圖拯救米蘭免受法國查理八世統治，將七十個銅鑄造成武器，而這些銅鑄本來是藝術家打算用來製作雕塑。法國回國後，路易十二世統治時，米蘭不戰而降。達芬奇仍在米蘭待了一段時間，直到有一天早上，他在意馬蘭卡萊羅品種蘭花與粘土模型被法國弓箭手拿來當作標靶練習。達芬奇在威尼西亞，達芬奇被聘為軍事工程師，繼續科學工程領域。就像他的繪畫同樣令人難忘，與突出手稿中絕大部份的理論構想與敘述全是混合藝術與科學所組成的紀錄。在科學上，他是一個極細靡遺並且細心的觀察者，其描述手法表示一個現象，但又符合於理論與實驗來驗證。同時期的學者幾乎都忽略了在科學領域中

(c)

Şekil 4. 5.(a) Sır 1 (b) Sır 2 (c) Yeniden yapılandırılmış imge [48].

## 5. VERİ GİZLEME

Veri gizleme, gizleme sanatının sayısal ortama aktarılmış halidir. Gizli bir mesajı örtü nesnesi içerisine fark edilmeyecek şekilde gizlenmesi işlemidir. Veri gizlenmiş sinyale stego-sinyal denilmektedir. Veri gizleme, subliminal iletişimin olmazsa olmazlarından biridir. Veri gizlemedeki temel amaç, güvenilir olmayan bir veri iletim hattında güvenilir bir kanal açarak, saldırganların dikkatini çekmeden mesajı alıcı tarafa göndermektir. Geleneksel iletişim ve veri gizleme tabanlı iletişimin blok diyagramı Şekil 5.1’de verilmiştir.



**Şekil 5. 1.** Veri iletişimi blok diyagramı (a) Geleneksel veri iletişim blok diyagramı (b) Veri gizleme tabanlı veri iletişimi blok diyagramı.

Veri gizleme işlemlerinde genellikle multimedya veriler kullanılmaktadır. Multimedya verileri metin, ses, imge ve video verileridir. Gizli veri, örtü nesnesine, İGS ve İİS’nin algılamayacağı şekilde gizlenmektedir. Veri gizlemeye ait bileşenler ise aşağıdaki gibidir.

- Örtü nesnesi
- Gizli mesaj
- Veri gizleme fonksiyonu
- Veri gizleme anahtarı
- Veri gizlenmiş nesne

- Veri çıkarma fonksiyonu

Veri gizleme fonksiyonu örtü nesnede gizli mesajın nasıl gizleneceğini, veri gizleme anahtarı ise gizli mesajın örtü nesnesinin hangi konumlarına gizleneceğini belirlemektedir. Veri gizleme fonksiyonu ve veri gizleme anahtarı kullanılarak gizli mesaj örtü nesnesine gömülür. İçerisine veri gizlenmiş nesne veri gizlenmiş nesne olarak adlandırılır. Veri gizlenmiş nesnede gizli mesajı çıkarabilmek için ise veri çıkarma fonksiyonu ve veri gizleme anahtarı kullanılır.

Veri gizlemeyi kullanan 2 temel yöntem bilimi vardır. Bunlar;

- Steganografi
- Sayısal Damgalama

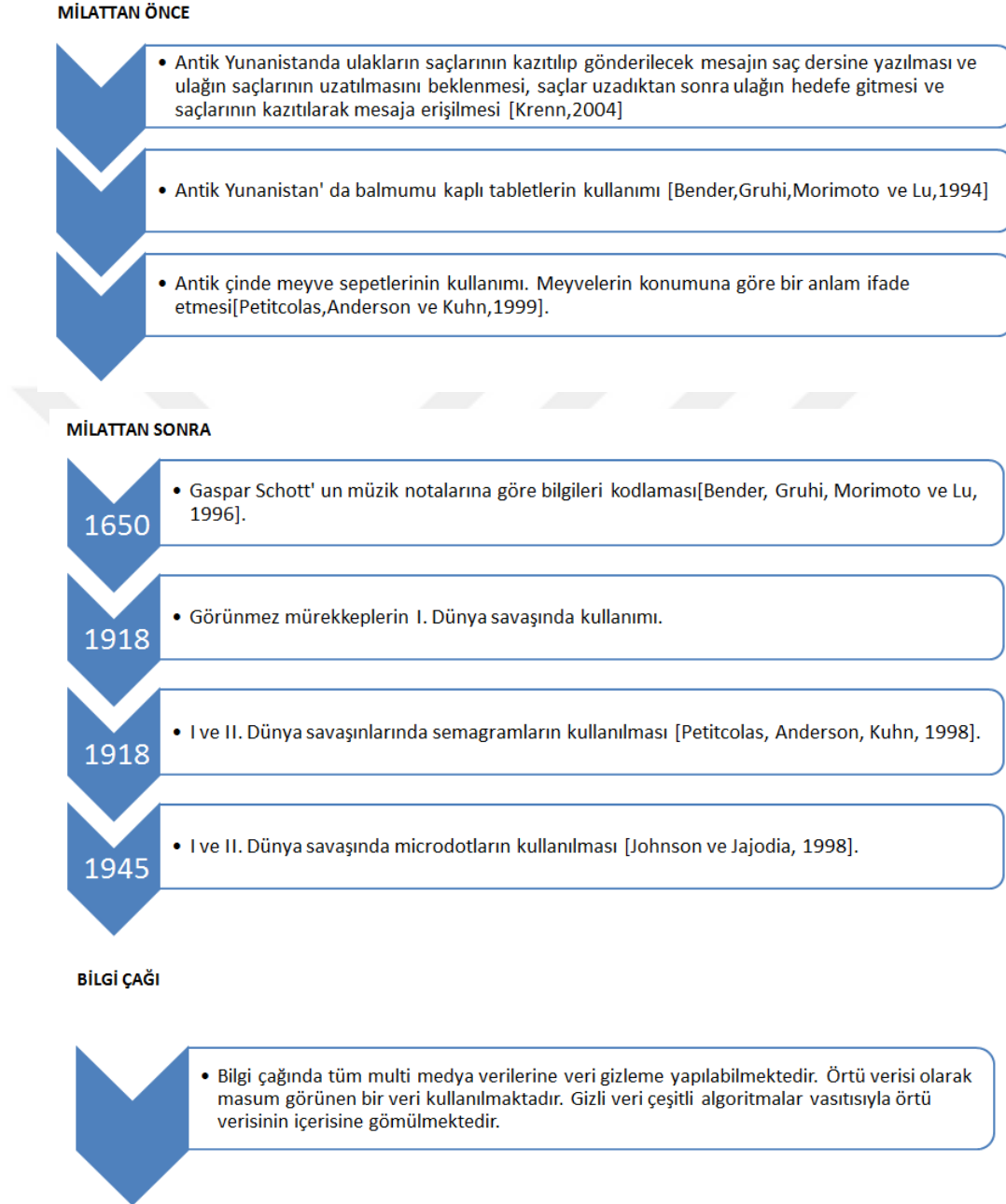
Bu iki yöntem bilim ilk bakışta aynı gibi görünse de veri gizlemeyi kullanma amaçları farklıdır. Steganografide temel amaç gizli mesajı başkalarının farketmesini engellemektir. Sayısal damgalama yöntemlerinin temel amacı ise verinin telif hakkını korumaktır. Bu yöntem bilimler kullanılarak bilgi güvenliği sağlanmaktadır. Steganografi ile sayısal damgalama arasındaki farklılıklar Tablo 5.1’de verilmiştir.

**Tablo 5. 1.** Steganografi ve Sayısal Damgalama arasındaki farklılıklar

| <b>Steganografi</b>                                                         | <b>Sayısal Damgalama</b>                                                         |
|-----------------------------------------------------------------------------|----------------------------------------------------------------------------------|
| Veri iletim hattının gizliliğini sağlamayı amaçlamaktadır.                  | Verinin telif hakkı ve orijinalliğinin korunması amaçlamaktadır.                 |
| Gizli verinin örtü nesnesiyle ilişkilendirilmesine gerek yoktur.            | Gizli veri örtü nesnesi ile ilişkilendirilmelidir.                               |
| Gizli verinin saldırılara karşı dayanıklı/kırılgan olması beklenmemektedir. | Gizli verinin saldırılara karşı dayanıklı/kırılgan olması beklenmektedir.        |
| Multimedya mesajların yanı sıra IP, exe gibi veriler de kullanılmaktadır.   | Genel olarak multimedya mesajlarında kullanılmaktadır.                           |
| Mesajın görünmemesi ve algılanmaması gerekmektedir.                         | Mesaj görünür veya yarı saydam olabilmektedir.                                   |
| Karşı adli bilişim uygulamalarında kullanılabilir.                          | Adli bilişim uygulamalarında özet fonksiyonuna alternatif olarak kullanılabilir. |

Veri gizleme antik çağlardan beri kullanılan hem bir bilim hem de bir sanattır. İlk bilinen veri gizleme uygulaması antik Yunanistan da gerçekleşmiştir ve bunun gerçekleştiği Herodot

tarafından nakledilmiştir ve günümüzde halen veri gizleme ile ilgili çalışmalar devam etmektedir. Veri gizlemenin tarihsel gelişimi Şekil 5.2’de verilmiştir.



Şekil 5. 2. Veri gizlemenin tarihsel gelişimi [80].

İran’da bulunan Yunan casusunun, Pers savaş planlarını Yunanistan’a veri gizleme kullanarak ilettiğinden bahsedilmektedir. Yazıya göre, casus kölenin kestirmiş ve savaş planlarını kölenin kafa derisine dövme olarak yazdırmıştır. Daha sonra yapılacak olan, kölenin saçının yazıyı kapatacak kadar uzamasını beklemek ve bu köleyi Yunanistan’a

göndermektir. Kölenin bilmesi gereken tek bilgi “*saçlarımı kesin*”olacaktır. Yine aynı devirde avcı kılığındaki bir ulağın, avladığı hayvanın karnına parşömen saklayarak Yunanistan’a girmesi anlatılmaktadır. Antik çağda veri gizleme uygulamalarının kullanımı yalnızca Yunanistan ile sınırlı değildir. Çin kaynaklarında ise gizli veri iletişiminin ilk uygulamasında meyve sepetinin kullanıldığından bahsedilmektedir. Bu uygulamada meyvelerin pozisyonuna göre veri gizlendiği bilinmektedir. Bu uygulamalar veri gizleme tarihinin çok eski olduğunu göstermektedir. 15. yüzyılda yazılan “Steganographiæ” adlı kitap veri gizleme hakkında yazılmış ilk eser olarak bilinmektedir. Schola Steganographica adlı eser Gaspar Schott tarafından 17. yy’de yazılmıştır. Bu eserde notalar kullanılarak veri gizleme uygulamaları gerçekleştirilmiştir ve birçok veri gizleme yöntemine de temel oluşturmuştur. Sonraki yıllarda ise veri gizleme uygulamaları, harf frekansları, görünmez mürekkep ve mors kodları gibi kodlar kullanılarak gerçekleştirilmiştir [81].

Ancak, veri gizleme uygulamalarının en ilginç uygulaması II. Dünya Savaşı yıllarında gözlemlenmektedir. Bu yöntem gizli mesajları bir kimyasal madde kullanarak gerçekleştirilmiştir. Kimyasal maddeyle gizli mesaj bir mendile yazılmakta ve bu mendil önceden belirlenen çöp kutularına atılmaktaydı. Alıcı taraf ise çöp kutusundaki mendili alıp yine bir kimyasal karışım kullanarak gizli mesajı elde etmekteydi. [82].

Yine II. Dünya Savaşı döneminde Almanlar “mikrofilm” teknolojisi kullanarak mikro noktalara veri gizleme uygulamaları gerçekleştirmiştir. Bu yöntemde harfler nokta boyutunda küçültülüp bir A4 belgesine yazılmaktaydı. Bu yöntem kullanılarak A4 büyüklüğündeki bir kağı da çok yüksek kapasitede veri gizlemek mümkün hale gelmiştir ve günümüzde bazı yazıcı firmaları tarafından damgalama amaçlı kullanılmaktadır.

Aşağıda, ikinci dünya savaşında kullanılan bir steganografi örneği verilmiştir [80].

“Apparently neutrals protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils.”

Yukarıda verilen paragrafta her kelimenin ikinci harfleri yan yana getirildiğinde “Pershing sails from NY June 1.” Mesajı ortaya çıkmaktadır.

Günümüzde multimedya veriler için veri gizleme uygulamaları yapılmaktadır ve veri gizleme yöntemleri bilgi güvenliğinin en önemli unsurlarından birisi haline gelmiştir.

Bir mesajı gizlemek için örtü nesnesi kullanılmalıdır. Örtü nesnesi veri iletim hattında masum görünümlü ve dikkat çekmeyen bir nesne olmalıdır. Veri gizleme için en sık kullanılanları multimedya verileridir ve multimedya verileri içerisinde en sık kullanılan veri

tipi ise imgelerdir. Veri gizleme kullanılarak sadece multimedya verilerine veri gizlenmez. Multimedya verilerine veri gizlemeyle paralel olarak sabit diskte kullanılmayan alanlara, IP paketlerine, html dosyalarına, exe vb. uzantılı dosyalara da veri gizlemek mümkündür [80].

Veri gizlemenin tarihi incelediğinde dijital ortamda kullanılan veri gizlemeyle, kölenin kafası kullanılarak yapılan veri gizlemenin çalışma prensibinin aynı olduğu görülmektedir. Günümüzde veri gizlemenin 5 temel ögesi vardır ve bunlar; gizlenecek mesaj, örtü verisi, Stego anahtar, veri gizleme fonksiyonu ve Stego nesnesidir. Heredot'un MÖ 430 naklettiği ilk örneği incelendiğinde gizlenecek mesaj karşı tarafa gönderilmesi istenen mesajdır, örtü verisi kölenin kafası, anahtar ise kölenin alıcıya saçlarını kes demesidir. Veri gizleme işlemi için kullanılan algoritma saçların uzamasını beklemek ve Stego nesnesi saç uzamış kölenin kafasıdır. Günümüzde ise veri gizleme şeması hala aynı prensiple çalışır, gizlenecek mesaj ne olursa olsun bir Stego anahtar, bir örtü nesnesi ve bir veri gizleme algoritmasının var olması sonucunda stego nesnesi oluşmaktadır.

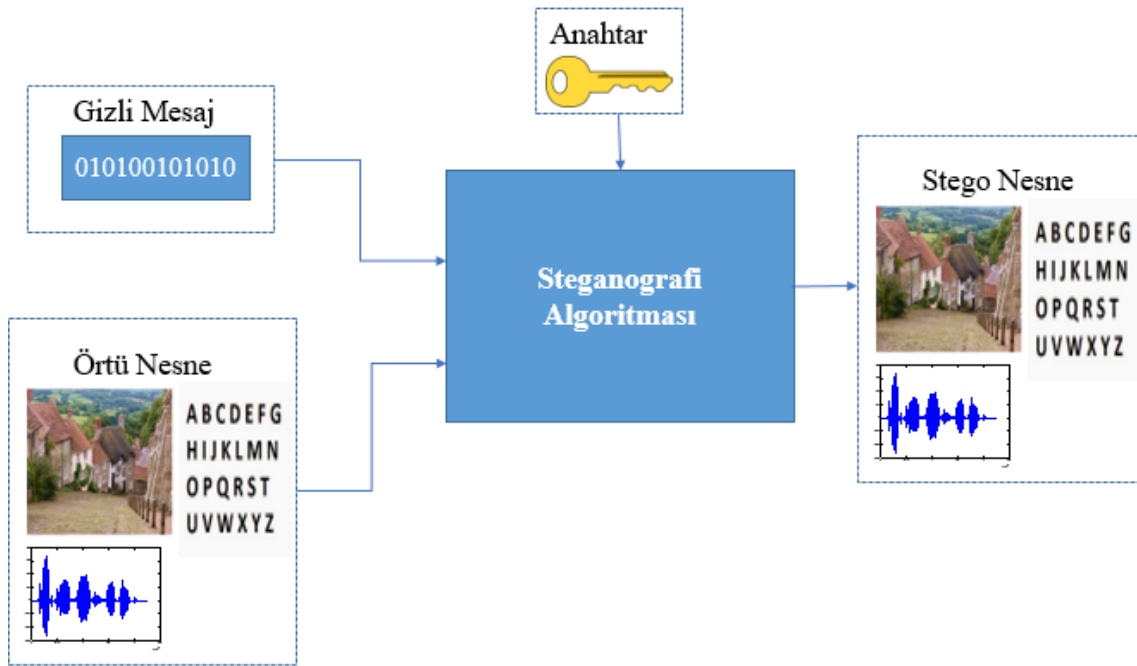
### 5.1. Steganografi

Steganografi gizi iletişim bilimi olarak literatürde yerini almıştır ve günümüzde sıkça kullanılmaktadır. Steganografi eski bir veri gizleme sanatıdır [81]. Steganografi kelimesi kökleri “στεγανος” ve “γραφειν”den gelen Yunan alfabesinden türetilmiştir. Tam olarak anlamı “*kaplanmış yazı*” (covered writing) demektir [83]. Kriptografide alıcı şifrenin varlığından haberdardır ancak uygun anahtar veya algoritmayı bilmeden gizli mesajı elde edemez ancak steganografide mesajı çözmek çok zor olmamasına rağmen, mesajın varlığının bilinmesi veya sezilmesi oldukça zordur. Kriptografi ve steganografinin birlikte kullanılmasıyla çok seviyeli bir güvenlik mekanizmaları elde edilebilir. Çok seviyeli güvenlik uygulamalarında öncelikle gizli mesaj şifrelenir ve şifreli mesaj veri gizleme fonksiyonu kullanılarak örtü nesnesine gömülür ancak homomorfik sistemlerin gelişimiyle beraber öncelikle örtü nesnesi şifrelenip ve gizli mesaj şifreli örtü nesnesine gömülmektedir. Homomorfik şifreleme algoritmasına ait anahtar bilinmezse gizli veriyi elde etmek imkânsızdır ve bu konu çok yeni ve güncel bir çalışma konusudur. Günümüzde şifrelenmiş bilgiyi, metin dosyaları, imge dosyaları, ses dosyaları, videolar, IP paketleri, exe uzantılı çalıştırılabilir dosyalar, scriptler veya e-posta gibi dijital verilerin içerisinde gömülü olarak alıcı tarafa göndermek mümkündür. Bu sayede güvenilir olmayan veri iletişim hattında güvenilir bir kanal oluşturulmaktadır [84].

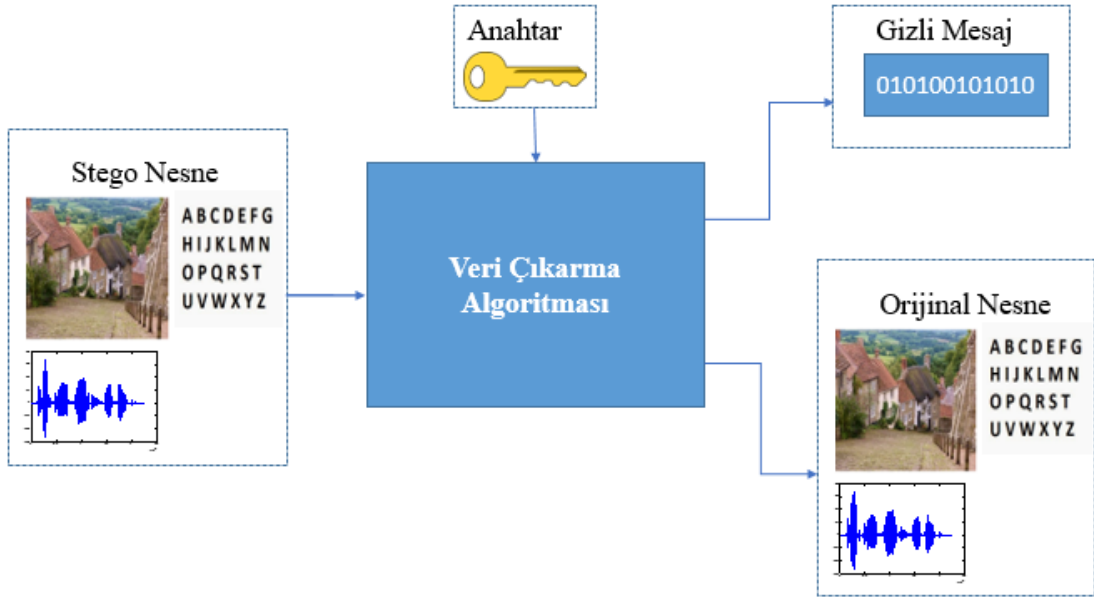
Metin, ses, sayısal imge ve video gibi multimedya dosyalarının üzerinde steganografi kullanılarak veri gizlenebilmektedir. Bu tür veri gizleme uygulamalarına multimedya veri gizleme denmektedir. Gizli mesaj genellikle metin formatında bulunmaktadır ancak gizlenen veri imge, ses veya video gibi multimedya mesajlardan da oluşabilmektedir [85,86].

Bilim çevrelerinde ilk Steganografi çalışmaları 1983 yılında Simmons tarafından tanımlanan hapishane problemidir. Bu problemde iki mahkûmun gardiyana farketirmeden kaçış planlarını birbirlerine yollamaları gerekmektedir. Eğer gardiyan iki mahkûm arasındaki iletişimi farkedirse mahkûmlar hapishaneden kaçamayacaklardır. Mahkûmların kendi aralarında gizli iletişimi sağlamaları gerekmektedir [87].

Problemın çözümünde ise steganografi kullanılmaktadır. Veri gizleme ortamı, örtü verisi veya örtü nesnesi, oluşan ortama da stego nesnesi denilmektedir [88]. Steganografik sistemin blok diyagramı Şekil 5.3 ve Şekil 5.4'te verilmiştir.



Şekil 5. 3. Steganografi kullanılarak oluşturulan veri gizlemenin blok diyagramı



Şekil 5. 4. Steganografi kullanılarak oluşturulan veri çıkarma blok diyagramı

Steganografi, kriptografi gibi bilgi güvenliği sağlamak için geliştirilmiş bir yöntemler bilimidir ancak kriptografi ve steganografi birbirinden farklıdır. Kriptografi, çeşitli matematiksel ve mantıksal operatörler kullanarak gizli mesajın içeriğini değiştiren ve istendiğinde bu mesajı yeniden elde edebilmeyi sağlayan bir yöntemler topluluğudur ancak steganografi gizli mesajı zararsız görünen örtü nesnelerinin içerisine çeşitli fonksiyonlar yardımıyla gizleyerek mesajın varlığının saldırganlar tarafından sezilememesini sağlayan yöntemler topluluğudur. Bu sebepten dolayı steganografi, kriptolojiyle yakından ilişkili olmasına rağmen kriptolojinin bir alt dalı değildir [89].

Steganografide metin, ses, imge ve video gibi multimedya mesajlar kullanılmaktadır. Kullanılan multimedya ortamlarına göre steganografi çeşitleri aşağıdaki gibidir.

- Metin steganografi
- Ses steganografi
- İmge steganografi

İmge steganografide kullanılan yöntemlerin tümü videolara da uygulanabilmektedir. Bu nedenden dolayı her iki ortamda gerçekleştirilen steganografi imge steganografisi olarak değerlendirilmektedir ancak video steganografinin kendine özel yöntemleri de bulunmaktadır.

### **5.1.1. Metin Steganografi**

Metin içerisine bilgi gizleme esasına dayanan steganografik bir yöntemdir. Kelimedeki özel karakterler, HTML dokümanları, satır ve kelime kaydırma, kısaltmalar ve boşluklar ile semantik ve karakter özellik yöntemleri bulunmaktadır [90].

#### **5.1.1.1. Ayrılmış Karakterler**

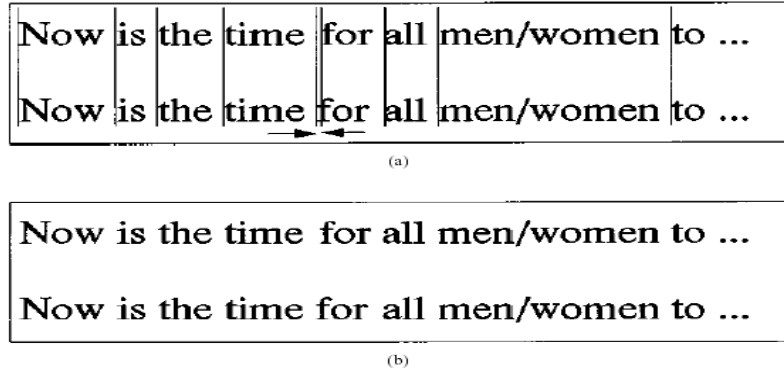
Ayrılmış karakterler yöntemi metin steganografide kullanılan en basit yöntemlerden biridir. Temel olarak metnin içerisinde özel karakterler ve belirli kelimeler seçilerek gizleme yapılabilir. Örneğin referans kelimeler “kış” ve “ilkbahar” olarak kabul edilsin. Cümle içerisinde kış kelimesi kullanılınc “0” ilkbahar kelimesi kullanılınc “1” i ifade ettiğini varsayalım. Referans kelimeler kullanılarak gizlenmek istenen mesaj metnin içerisine gizlenir [90].

#### **5.1.1.2. HTML Dokümanları**

Gizli veri HTML etiketleri kullanılarak gizlenebilmektedir [90]. Örneğin <body bgcolor=”red”> ve <body BGcolor=”red”> etiketleri aynı görevi yapmaktadır. Eğer arka planda HTML tagları bu şekilde kullanılırsa, web sayfasında herhangi bir değişiklik gözlenmeyecek ve web sayfasından şüphelenilmeyecektir. Ancak taglar bu şekilde yazılarak gizli bir mesajı sembolize etmektedir. HTML dokümanları kullanılarak yapılan steganografide güvenlik üst düzeydedir ve ilgili web sitesine bakılarak gizli mesaj hiçbir şekilde algılanamamaktadır. Gizli mesajın anlaşılabilmesi için sitenin kaynak kodlarına bakmak gerekmektedir.

#### **5.1.1.3. Satır ve Kelime Kaydırma**

Satırları dikey ve kelimeleri yatay olarak kaydırmak en temel metin steganografisi yöntemlerinden biridir. Kelimeler veya harfler arasında boşluklar insan görme sisteminin algılamayacağı şekilde değiştirilerek veri gizleme işlemi gerçekleştirilir.



Şekil 5. 5. Kelime kaydırma yöntemiyle veri gizleme [91].

Şekil 5.5'teki çizgilerden anlaşıldığı gibi for'dan önce fazladan boşluk bırakılmıştır ve bu boşluklar gizli veriyi ifade etmektedir. Bu yöntemle barkodlara da veri gizlenebilir. Barkodlardaki çizgilerin arasındaki mesafe sabittir. Bu mesafelerin 0.03 inç artırılıp azaltılmasıyla gizli veri kodlanmaktadır. Gizlenen veri özel bir programla entegre edilmiş bir OCR tarafından okunabilir. Bu yöntem tam boşluk bırakmaz, boşluğun yarısı ve çeyreği kadar mesafe bırakarak mesajı gizler.

#### 5.1.1.4. Kısaltmalar ve Boşluklar

Kısaltmalar ve boşluklar kullanılarak metne çok az miktarda veri gizlenmektedir ve bu yöntem İngilizce metinlerde sıkça kullanılmaktadır. Örneğin noktadan sonra boşluk bırakmak "0"ı temsil ederken çift boşluk "1"i temsil etmektedir. Bu işlem kullanışlı bir yöntemdir ancak bu yöntemle çok küçük kapasitelerdeki veriler saklanabilir. Kısaltmalar ve boşluklar yönteminin editörler tarafından kullanılması zordur çünkü metin editörlerinde TRIM ve benzeri komutlar otomatik olarak devreye girerek fazla boşluklar silinmektedir. Boşlukların otomatik düzeltmeyle silinmesi ise gizli mesajın silinmesi anlamına gelmektedir [80,91].

#### 5.1.1.5. Anlamsal ve Karakter Özellikleri Yöntemi

Anlamsal yöntemler gizli verinin varlığını korumak için geliştirilen yöntemlerdir. Anlamsal yöntemler genelde eş anlamlı kelimeleri kullanarak veri gizleme yapmaktadır [33]. Örneğin cümlede "al" ve "kırmızı" kelimeler geçmektedir. "al" kelimesi 0'ı "kırmızı"

kelimesi ise 1'i temsil etmektedir ve böylece veri gizleme işlemi gerçekleştirilmektedir. Bu tip veri gizleme yöntemine anlamsal Steganografi denmektedir.

Karakter özelliği Steganografi de karakterlerin bazı özellikleri değiştirilir. Örneğin metin içerisinde kullanılan bazı karakterler uzatılır veya kısaltılır. Bu karakterlerin en anlamlı bitleri kullanarak veri gizleme işlemi yapılabilir. Örneğin a harfi 1 ile ifade edilirken @ karakteri 0 ile ifade edilebilir. Bu kullanım en çok Arapça, Japonca ve Çince gibi özel karakterlerin yoğun olduğu dillerde kullanılmaktadır. Seçilen noktalı ve noktasız harfler herhangi bir biti temsil etmektedir. Metnin içerisinde ki kullanımlarına göre gizli mesaj ifade edilmektedir. Şekil 5.6'da Arapça harflerin steganografik kullanımıyla ilgili bir örnek gösterilmektedir.

| Noktasız Harfler | Noktalı Harfler |
|------------------|-----------------|
| ا ح د ر          | ب ت ث           |
| س ص              | ج خ ذ ز         |
| ط ع ك            | ش ض             |
| ل م ه و          | ظ غ ف           |
|                  | ق ن ي           |

Şekil 5. 6. Arapçada kullanılan noktalı ve noktasız harfler [90].

### 5.1.2. Ses Steganografi

Örtü nesnesi olarak ses sinyallerinin kullanıldığı steganografi çeşidine ses steganografi denilmektedir. Ses steganografinin en temel başarımlı parametresi İİS'dir. Oluşturulacak ses steganografi yönteminin İİS tarafından farkedilmemesi gerekmektedir. Ses sinyallerine veri gizleme işlemi yapmadan önce o ses sinyalinin hangi karakteristikte olduğunun bilinmesi gerekmektedir. Ses sinyalleri iki temel özelliğe sahiptir.

- I) Basit niceleme yöntemi
- II) Geçici seçme oranı

Basit niceleme yöntemi önemli olan unsur sesin kaç bit ile kodlandığıdır. Genel olarak WAV ve AIIF uzantılı ses dosyalarında bu yöntem kullanılmaktadır. Geçici seçme oranı yönteminde ise önemli olan sesin frekansının ne olduğudur.

Ses analog bir sinyal olduđu için, sesin dijitalleştirilmesi gerekmektedir. Analog sinyal dijital hale dönüştürüldükten sonra veri gizleme işlemi kolaylıkla yapılabilir. Ses steganografide kullanılan yöntemler ise düşük bit kodlaması, aşama kodlaması, tayf yayılması ve yankı veri gizlemesidir [80].

#### 5.1.2.1. Düşük Bit Kodlaması

Analog ses sinyalleri sayısal hale çevrildikten sonra gizli veri ses sinyalinin en anlamsız bitine gömülür. Ses sinyalleri için düşük bit kodlaması olarak adlandırılan bu yöntem imge dosyalarında kullanıldığında ise en önemsiz bit (EÖB) yöntemi olarak adlandırılmaktadır. Temel olarak aynı işlevi gerçekleştirerek veri gömen bu iki yöntem literatürde farklı isimlerle anılmaktadır. Farklı isimlendirmenin temel olarak iki sebebi vardır bunlardan ilki örtü nesnesinin birinde ses verisi diğesinde ise imge verisi olmasıdır, diğere sebep ise ses dosyalarında analogdan sayısal hale çevirme işlemi kullanılırken, imge dosyalarında böyle bir çevrimin kullanılmasına gerek yoktur. Düşük bit kodlaması yöntemi ses dosyalarına veri gizleme için kullanılan başarılı bir yöntem değildir. Veri gizleme sonucunda elde edilen ses dosyalarında İİS tarafından algılanabilen gürültülere rastlanmaktadır ve bu yöntem saldırılara karşı kırılğan bir karakteristik göstermektedir [92]. Bu yöntemde yüksel işitsel kalite elde edebilmek için frekans dönüşümlerinin kullanılması önerilmektedir.

#### 5.1.2.2. Aşama Kodlaması

Bu yöntem JPEG sıkıştırma algoritmasına benzemektedir. Veri gizleme işlemi yapılacak örtü ses dosyası küçük bloklara ayrılır ve her bloğa ait aşama gizli verinin aşama referansı ile değiştirilir. Yöntemin adımları aşağıda verilmiştir [93].

**Adım 1:** Ses verisi  $N$  adet bloğa bölünür.

**Adım 2:** Her bloğa Ayırık Fourier Dönüşümü (AFT) uygulanarak aşama ve büyüklük matrisleri elde edilir.

**Adım 3:** Komşu blokların farkı hesaplanır.

**Adım 4:** Her blok için yeni bir aşama değerine bilgi gizlenerek oluşturulur.

**Adım 5:** Veri gizlenmiş aşama matrisleri büyüklük matrisleriyle birleştirilerek veri gizlenmiş bloklar elde edilir.

**Adım 6:** Veri gizlenmiş bloklar birleştirilerek, stego ses elde edilir.

### 5.1.2.3. Tayf Yayılması

Veri gizleme işlemini ses sinyalinin frekans taftı üzerinden gerçekleştiren ve ses dosyaları için özelleşmiş bir veri gizleme yöntemidir. Güçlü bir yapısı ve yüksek işitsel kalitesi bulunmamaktadır [80].

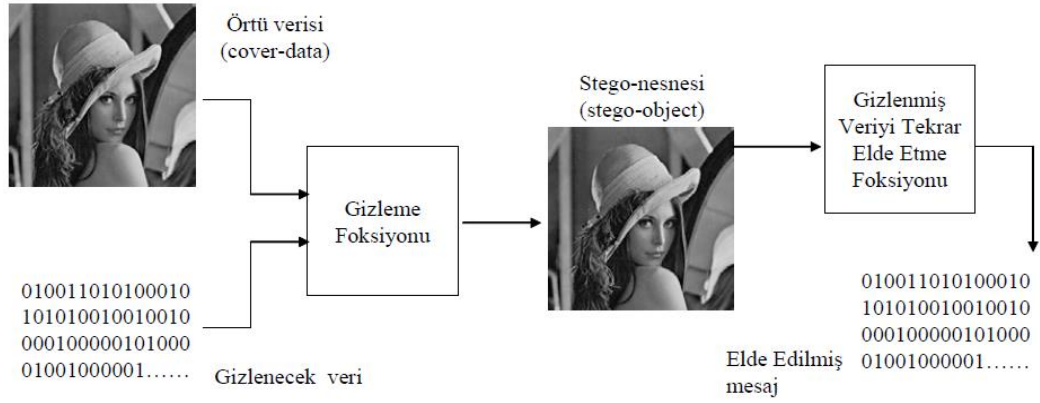
### 5.1.2.4. Yankı Veri Gizlemesi

Ses verisine veri gizlemek için, örtü verisi olan ses dosyasına yankı eklenmesi işleminin gerçekleştirilmesidir. Veri gizleme için yankının 3 adet parametresi kullanılmaktadır ve bunlar, gecikme miktarı, zayıflama oranı veya büyüklüğü gibi değerleridir.  $N$  farklı değer kullanılarak işitsel olarak algılanamayacak  $\log_2 N$  adet bitin kodlanması mümkündür. Her bitin kodlanması için sinyal segmentlere bölünür. Yankı veri gizlemesi yöntemi herhangi bir gürültüye neden olmamakta veya kayıplı bir kodlama kullanmamaktadır [80].

### 5.1.3. İmge Steganografi

Örtü nesnesi olarak imgenin kullanıldığı steganografi türüne imge steganografi denilmektedir. Steganografi tekniğinin en sık uygulandığı medya formatları imge formatlarıdır ve günümüzde yaygın şekilde kullanılmaktadır. Yaygın kullanılmasının en önemli sebeplerden biri görüntü formatlarının veri gizleme işlemine uygun olmasıdır.

Dijital imgelerin dağıtımı kolay ve internette hemen hemen her sayfada bulundukları için steganografik iletişim açısından sıkça kullanılabilecek dosyalardır. İmge dosyalarına steganografinin uygulanabilmesi için ön şart imgenin sayısallaştırılmasıdır. Piksel değerleri alındıktan sonra hangi gizleme fonksiyonun kullanılacağı seçilir. Gizleme fonksiyonu seçildikten sonra gömülecek verinin boyutu, tipi ve örtü nesnesinin hangi bölgesine gömüleceği hakkındaki bilgiler alınarak steganografi anahtarı oluşturulmalıdır. Anahtar istenilirse şifrelenir veya anahtar kullanılarak gizli mesaj şifrelenir. Ardından gömülecek veri gizleme fonksiyonu kullanılarak örtü nesnesine gizlenir ve Stego-imge veya steganogram oluşturulur. Şekil 5.7’de imgeler için steganografik sistemin yapısı verilmiştir.



Şekil 5. 7. İmgeler için kullanılan steganografik sistem diyagramı

Herhangi bir steganografik sistemin kabul edilebilmesi üç temel şartın sağlanması gerekmektedir. Bunlar görsel kalite, saldırılara karşı dayanıklılık ve kapasitedir. Görsel kalite; taşıyıcı nesnenin içerisinde bilgi olup olmadığının sezilmesidir. Bir sistemde bilgi varlığı ne kadar az sezilirse, sistem o kadar güvenilirdir. Sağlamlık koşulu gizli verinin ne kadarlık kısmı iletim hattında bozulmadan alıcı tarafa iletilmiş olduğunun ölçütüdür. Gizli veri iletim kanalındaki gürültü ve saldırılardan ne kadar az etkilenmişse sistem o kadar sağlamdır. Kapasite ise örtü verisinin ne kadarlık bilgi taşıyabileceğiyle ilgilidir. Örtü verisi ne kadar çok bilgi taşırsa o kadarlık kapasiteye sahip demektir. 1 bpp veri gizleme kapasitesine sahip veri gizleme fonksiyonuna ait kapasiteyi hesaplamak için gerekli denklemler Denklem 5.1 – 5.3’te verilmiştir.

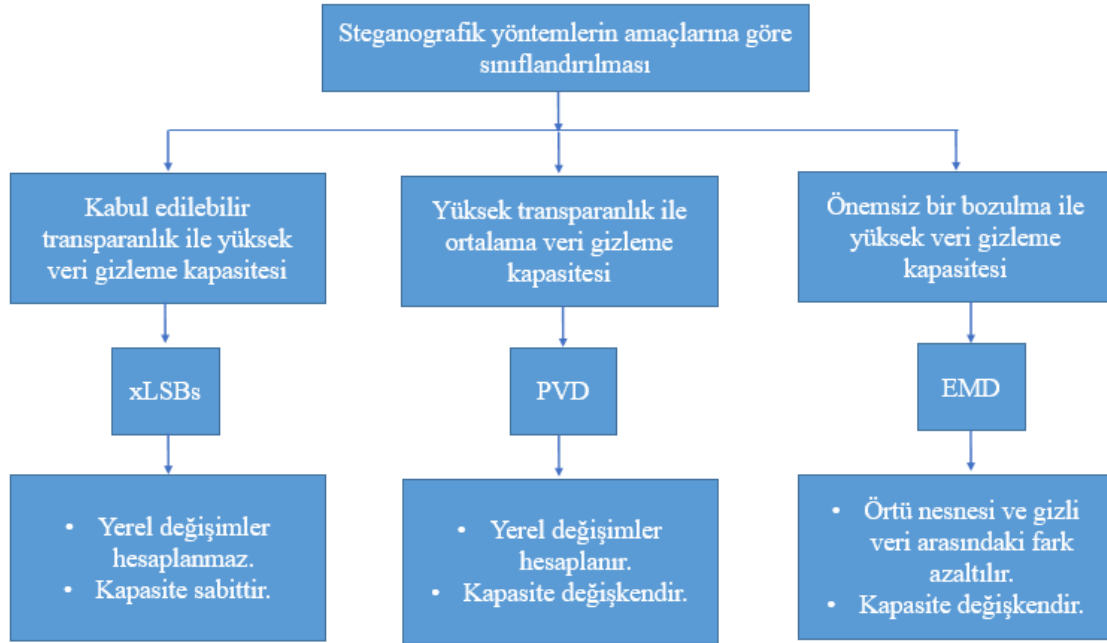
$$S = mnk \quad (5.1)$$

$$B = 8b \quad (5.2)$$

$$K = \frac{mnk}{8} \quad (5.3)$$

Burada S imgenin piksel sayısı temsil etmektedir. m satır sayısı, n sütun sayısı ve k ise katman sayılarını sembolize etmektedir. Her pikselin bir byte kapasitede bilgi taşıdığı düşünülecek olursa Denklem 5.1. imgenin kapasite bilgisi verilmektedir. Eğer imge RGB formatında ise k 3 değerini alacaktır, gri seviyeli bir imge ise k değeri 1 olacaktır. 1 byte’ın 8 bit olduğu Denklem 5.2’te gösterilmiştir. Gizleme fonksiyonun özelliği ve eldeki bilgilerden yola çıkılarak Denklem 5.3’teki kapasite denklemi elde edilmiş olur [94].

Kusursuz bir steganografik sistemin oluşturulması için transparanlık, gizlilik ve kapasite ölçütlerinin maksimum düzeye taşınması gerekmektedir fakat taşıyıcının kapasitesi arttıkça transparanlığı düşmekte ve bu nedenden dolayı algılanabilirliği artmaktadır. Algılanabilen bir veri gizleme algoritması ise kabul edilmezdir. Aynı zamanda kapasitesi arttırılan bir steganografik sistemde sağlamlıktan bahsetmekte zor olacaktır. Çünkü taşınan veri iletim kanalında gerçekleşen kayıp ve saldırılardan doğrudan etkilenecektir. Bu 3 ölçütü mükemmel kullanabilen bir veri gizleme fonksiyonunun geliştirilmesi için çalışmalar halen devam etmektedir. Bu ölçütlerin en iyi sağlandığı veriler imge verileri (durağan ve hareketli) olduğu için İmge Steganografi çok sık kullanılmaktadır. Amaçlarına göre imge steganografinin sınıflandırılması Şekil 5.8’de verilmiştir.



Şekil 5. 8. Amaçlarına göre imge steganografinin sınıflandırılması [95].

#### 5.1.3.1. En Önemsiz Bite Ekleme Yöntemi

En önemsiz bite ekleme yöntemi (EÖB) [96] matematiksel olarak yalın bir ifadeye sahip, yaygın kullanılan ve uygulanabilir bir veri gizleme yöntemidir ancak yöntem kayıplı sıkıştırma algoritmaları veya dönüşümlerle birlikte kullanılırsa veri kayıplarına sebep olmaktadır. Bu sebepten dolayı EÖB kırılgan bir yapıya sahiptir.

EÖB yönteminde örtü nesnesinin en anlamsız bitleri değişikliğe uğratıldığı için bu yöntem yüksek görsel kalitede ve yüksek kapasitede veri gizleme imkanı sağlamaktadır. 8

bitlik imgenin soldan sağa ilk 4 biti anlamlı bit dizisinin oluştururken son 4 biti ise önemsiz bit dizisini oluşturmaktadır. Örneğin en önemsiz 2 bite veri gizlemek için örtü imgesinin 7. ve 8. bitleri kullanılır. Kullanılan önemsiz bit sayısı arttıkça kapasite artar ancak görsel kalite düşer.

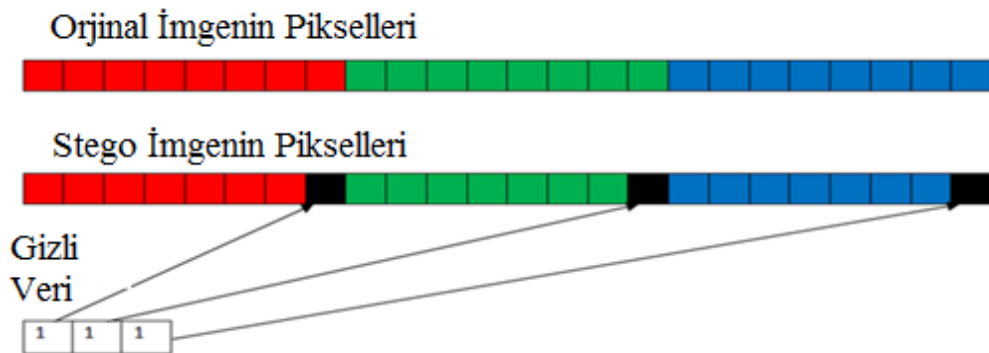
EÖB yöntemi gri ve renkli görüntülerde uygulanabilen bir yöntemdir. 8 bitlik gri bir imgede piksel değerleri 0-255 arasında değişmektedir. Bu yöntemin uygulanışının en basit yolu ise öncelikle piksel değerleri ikilik sayı sistemine dönüştürülür ve veri pikselin en anlamsız bitine yerleştirilir [97].

**Tablo 5. 2.** EÖB yöntemiyle veri gömülmesi

| Değerler             | Pikselin Renk Değeri | Renk Değerinin İkilik Sistemdeki Karşılığı |
|----------------------|----------------------|--------------------------------------------|
| Orijinal Piksel      | 158                  | 1001110                                    |
| Veri gömülmüş Piksel | 159                  | 1001111                                    |

EÖB yöntemi kullanılarak yapılan veri gizlemeler uygulamalarında, ilgili pikselin değeri  $\pm 2^{n-1}$  değişir veya hiçbir değişikliğe uğramaz.

24 bitlik imgelede her katmanın son bitini değiştirmek suretiyle her bir piksele 3 bit gizli veri saklanabilmektedir. Bu işlem 8 bitlik gri seviyeli imgelede veri gizlemeye benzemektedir. EÖB yöntemi 24 bit renk derinliğine sahip 800 x 600 boyutundaki bir imgeye uygulanacak olursa, veri gizlemek için kullanılabilir alan 1.440.000 bit (180.000 byte) olarak hesaplanır. Eğer gizli veri, veri gizleme işleminden önce sıkıştırılırsa, örtü nesneye daha yüksek miktarda bilgi gömülebilir.



**Şekil 5. 9.** 24 bitlik imgeye EÖB ile veri gizleme [97].

EÖB yöntemi hem basit hem de kolay uygulanabilir bir yöntemdir. Bu sebepten dolayı EÖB yöntemini kullanan birçok algoritma bulunmaktadır. Günümüzde geliştirilen yeni nesil veri gizleme algoritmalarının çoğunda halen veri gizleme fonksiyonu olarak EÖB kullanılmaktadır. Ayrıca bu yöntemle birlikte bir anahtar kullanılarak, gömülen mesajın gizliliğini koruyabilmek için anahtar tabanlı EÖB yöntemi de kullanılmaktadır. EÖB yönteminin saldırılara karşı dayanıklılığını arttırmak için AKD, ADD, AFD gibi dönüşümler kullanılmaktadır.

### 5.1.3.2. En Etkin Piksel Ayarlama Süreci Yöntemi

EÖB yönteminin görsel kalitesini arttırmak ve daha yüksek görsel kaliteye sahip steganografik yöntemler geliştirebilmek için En Etkin Piksel Ayarlama Süreci (OPAP) yöntemi Chan ve Cheng tarafından önerilmiştir [98]. EÖB'yi temel alan bu yöntem belirli bir prosedüre dayanmaktadır. Bu prosedürü daha iyi anlayabilmek için aşağıda belirtilen sembolleri tanımlamak gerekmektedir.

$C$ : Örtü imge

$C'$ : EÖB yöntemi uygulanmış Stego-imge.

$C''$ : OPAP yöntemi uygulanmış Stego-imge.

$p_i$ : Örtü imgenin  $i$ . indisindeki piksel değeri.

$p'_i$ : EÖB uygulanmış Stego-imgenin  $i$ . indisindeki piksel değeri.

$p''_i$ : OPAP uygulanmış Stego-imgenin  $i$ . indisindeki piksel değeri.

Örtü imgesiyle EÖB uygulanmış Stego-imgenin arasındaki fark hesaplanır. Denklem 5.4 kullanılarak pikseller arasındaki fark değeri hesaplanır.

$$f_i = p'_i - p_i \quad (5.4)$$

$$-2^k < f_i < 2^k \quad (5.5)$$

OPAP yöntemi hata oranlarını kullanarak veri gizleme işlemini gerçekleştiren bir yöntemdir. Aşağıdaki denklemler kullanılarak  $p''_i$  hesaplanmaktadır.

$$(2^{k-1} < f_i < 2^k) \wedge (p'_i \geq 2^k) \Rightarrow p''_i = p'_i - 2^k \quad (5.6)$$

$$(2^{k-1} < f_i < 2^k) \wedge \sim(p'_i \geq 2^k) \Rightarrow p''_i = p'_i \quad (5.7)$$

$$(-2^{k-1} \leq f_i \leq 2^{k-1}) \Rightarrow p''_i = p'_i \quad (5.8)$$

$$(-2^k < f_i < -2^{k-1}) \wedge (p'_i < 256 - 2^k) \Rightarrow p''_i = p'_i + 2^k \quad (5.9)$$

$$(-2^k < f_i < -2^{k-1}) \wedge \sim(p'_i < 256 - 2^k) \Rightarrow p''_i = p'_i \quad (5.10)$$

Bu yöntem bir bitlik veri gizleme için görsel kaliteyi iyileştirmez fakat 2, 3 ve 4 bitlik veri gizlemeler için görsel kaliteyi yaklaşık 2 dB iyileştirmektedir.

### 5.1.3.3. Piksel Değer Farklılıkları Yöntemi

Gri seviyeli imgelere veri gizlemek için Wu ve Tsai tarafından 2003 yılında önerilmiştir [99]. Örtü imge ikili gruplara ayrılarak farkları alınır ve alınan farklar belirlenen aralıklara denk gelmektedir. Aralıklar, insan görme sistemi baz alınarak hesaplanmaktadır. Bu aralıklarda yapılacak değişikliklerin insan görme sistemi tarafından algılanmaması istenmektedir. Bu yöntem kullanılarak yapılan veri gizlemelerde kapasite imgenin yapısına göre değişmektedir.

Önerilen yöntem gri seviyeli imgeler için tasarlanmıştır. Gri seviyeli imgeler genellikle 8 bitlik oldukları için 256 farklı renk seviyesinden oluşmaktadır. Piksel çiftleri yukardan aşağı, aşağıdan yukarı, soldan sağa, sağdan sola veya daha değişik tarama yöntemleri kullanılarak belirlenmektedir. Piksel çiftleri arasındaki fark  $d$  olarak adlandırılmaktadır. Bu yöntemde gizli mesaj bit olarak kodlanmaktadır. İlgili bloğa gizlenecek maksimum kapasite logaritmik olarak hesaplanmaktadır. Yöntemin adımları aşağıdaki gibi verilmiştir.

**Adım 1:** Denklem 5.11 kullanılarak fark değer olan  $d$  hesaplanır.

$$d_i = p_{i+1} - p_i \quad (5.11)$$

**Adım 2:** Fark değeri kullanılarak optimal değer aralığı hesaplanır.

$$R_i = \min(u_k - d_i), u_k \geq d_i, 1 \leq k \leq n \quad (5.12)$$

**Adım 3:** Bloğa gizlenecek bit sayısı logaritma 2 tabanına göre hesaplanır.

**Adım 4:** Bloğa gizlenecek bit sayısı ondalık tabana çevrilir.

**Adım 5:** Yeni fark değeri Denklem 5.13'e göre hesaplanır.

$$d'_i = I_k + b \quad (5.13)$$

**Adım 6:** m değeri Denklem 5.14 kullanılarak hesaplanır.

$$m = \frac{d_i + d'_i}{2} \quad (5.14)$$

**Adım 7:** Yeni  $p_i$  ve  $p_{i+1}$  değerleri Denklem 5.15 kullanılarak hesaplanır.

$$(p'_i, p'_{i+1}) = \begin{cases} p_i + [m], p_{i+1} - [m], & \text{if } p_i \geq p_{i+1} \text{ and } d'_i > d_i \\ p_{i+1} + [m], p_i - [m], & \text{if } p_i < p_{i+1} \text{ and } d'_i > d_i \\ p_i - [m], p_{i+1} + [m], & \text{if } p_i \geq p_{i+1} \text{ and } d'_i \leq d_i \\ p_{i+1} + [m], p_i - [m], & \text{if } p_i < p_{i+1} \text{ and } d'_i \leq d_i \end{cases} \quad (5.15)$$

**Adım 8:** Gizli veri boyutunca adım 2-6'yı tekrarla.

#### 5.1.3.4. Değişim Yönünü Kullanma Yöntemi

Değişim yönünü kullanma (EMD) yöntemi Zhang ve Wang tarafından 2006 yılında önerilmiştir. Bu yöntemde, gizli veriyi temsil eden rakamların  $(2n + 1)$  tabanında olması durumunda, n adet örtü imge pikselinin saklamada kullanılması prensibine dayanmaktadır [100]. Veri gizleme yapılırken örtü imgesi piksellerinin değerleri  $\pm 1$  değişecektir. n pikselden oluşan bir grup için, piksellerin değiştirilmeme durumu da göz önüne alınırsa  $2n+1$  farklı durum oluşturulabilir. Veri gizleme prosedüründe, gizli mesaj  $(2n+1)$  sayı tabanına çevrilir. Eğer gizli mesaj ikilik tabanda ise, L bitten oluşan parçalara ayrılır. Her bir parçanın onluk değeri  $(2n + 1)$ 'lik sistemdeki K adet sayı tarafından temsil edilir. Denklem 5.16'da L değerine ait denklem verilmiştir.

$$L = \lfloor K \log_2(2n + 1) \rfloor \quad (5.16)$$

Örneğin (1101 0110 1001) ikili kod dizisi 5 sayı tabanında (23 11 14) olarak ifade edilmektedir ve  $K=2$  ve  $L=4$  olarak hesaplanmaktadır. Veri gizlenecek grupta tek bir sayının artırılması veya azaltılması gizli mesajın ifade edilmesi için yeterli olacaktır. Piksellerin ağırlıkları Denklem 5.17’de ifade edilmektedir.

$$f(p_1, p_2 \dots p_n) = \left[ \sum_{i=1}^n (p_i i) \right] \text{mod}(2n + 1) \quad (5.17)$$

Eğer hesaplanan  $d$  değeri  $f$  değerine eşit ise piksel grubunda herhangi bir değişme olmamaktadır. Eğer  $d \neq f$  olması durumunda ise Denklem 5.18’deki denklem kullanılır.

$$s = d - f \text{mod}(2n + 1) \quad (5.18)$$

$s$  değeri  $n$ ’den büyük değilse  $p_s$  değeri bir arttırılır, değilse  $p_{2n+1-s}$  değeri bir azaltılır.

## 5.2. Sayısal Damgalama

Bilişim teknolojilerinin gelişmesiyle birlikte, verilerin dağıtılması ve değiştirilmesi kolaylaşmıştır. Tezin bu kısmına veri gizlemenin alt dallarından olan görünmez damgalama sistemlerinden bahsedilecektir. Sayısal damgalamanın temel amacı genellikle multimedya verisinin kimlik doğrulamasını yaparak telif haklarının korunmasını sağlamaktır. Bilgi güvenliğini ve telif haklarını sağlayabilmek için damgalamanın kullanılması gerekmektedir. Sayısal damgalama ile ilgili çalışmalar 1990’lı yıllarda hız kazanmaya başlamıştır. İki tür sayısal damgalama tipi vardır bunlar;

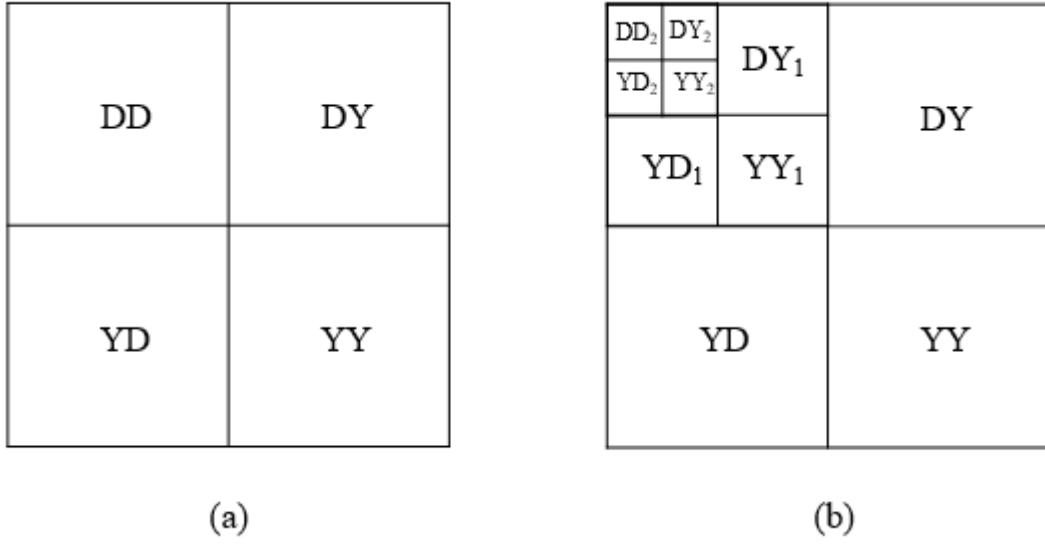
- Görünür damgalama
- Görünmez damgalama

Bilimsel çalışmaların büyük çoğunluğu görünmez damgalama ile ilgilidir. Görünmez damgalama uygulamalarında steganografik yöntemlerin kullanmasına rağmen verinin uçtan uca iletişim sağlamasına gerek yoktur. Damgalamada gerçekleştirilmek istenen bir diğer özellik, damgalama yönteminin saldırılara karşı dayanıklı veya saldırılara karşı kırılğan olmasıdır. Kırılğan damgalama yöntemleri genellikle adli bilişim ve imge kimliklendirme uygulamalarında kullanılmaktadır. Adli bilişim uygulamalarında multimedya mesajlarının değişikliğe uğrayıp uğramadığının tespiti için kullanılmaktadır. Adli bilişim uygulamalarında bu tespiti yapabilmek için kriptografik özet fonksiyonları kullanılmaktadır

ancak kriptografik özet fonksiyonları saldırının multimedya mesajın hangi bölgesine yapıldığını tespit edememektedir. Bu sebepten dolayı kırılğan damgalama teknikleri kullanılmaktadır. Kırılğan damgalama teknikleri sayesinde multimedya mesajda değiştirilen bölge tespit edilebilmektedir. Dayanıklı damgalar oluşturabilmek için ise Ayrık Kosinüs Dönüşümü (AKD), Ayrık Dalgacık Dönüşümü (ADD) ve Tekil Değer Ayrışımı (TDA) gibi yöntemlerin kullanılması gerekmektedir [101,102].

### **5.2.1. Ayrık Dalgacık Dönüşümü Tabanlı Sayısal Damgalama**

ADD verilen sinyali yüksek ve düşük geçiren filtrelerden geçirerek alt frekans bantlarına ayırmasını sağlamaktadır. Bu dönüşüm temelini Joseph Fourier tarafından geliştirilen Fourier dönüşümünden almaktadır. ADD imge ve ses işleme uygulamalarında da sıklıkla kullanılan frekans dönüşüm yöntemidir. Ses sinyalleri tek boyutlu olduğu için, bu tür sinyallerde tek boyutlu ADD kullanılmaktadır. İmgeler ise iki boyutlu olduğu için, imgenin frekans bantlarını elde etmek için 2 boyutlu ADD kullanılmaktadır. Bir multimedya veriye tek seviyeli veya çok seviyeli ADD uygulanabilmektedir. 2 boyutlu ADD kullanılarak 4 adet alt bant elde edilmektedir. Elde edilen altbantlar DD (Düşük Düşük), DY (Düşük Yüksek), YD (Yüksek Düşük) ve YY (Yüksek Yüksek) olarak adlandırılmaktadır. Bu bantlar sırasıyla DD yaklaşık imge, DY imgenin dikey detay bandı, YD imgenin yatay detay bandı ve YY ise imgenin köşegen bandı olarak adlandırılmaktadır. İkinci seviye de ADD için DD alt bandı kullanılır. Şekil 5.10'da tek seviyeli ve çok seviyeli ADD örneği verilmiştir [103].



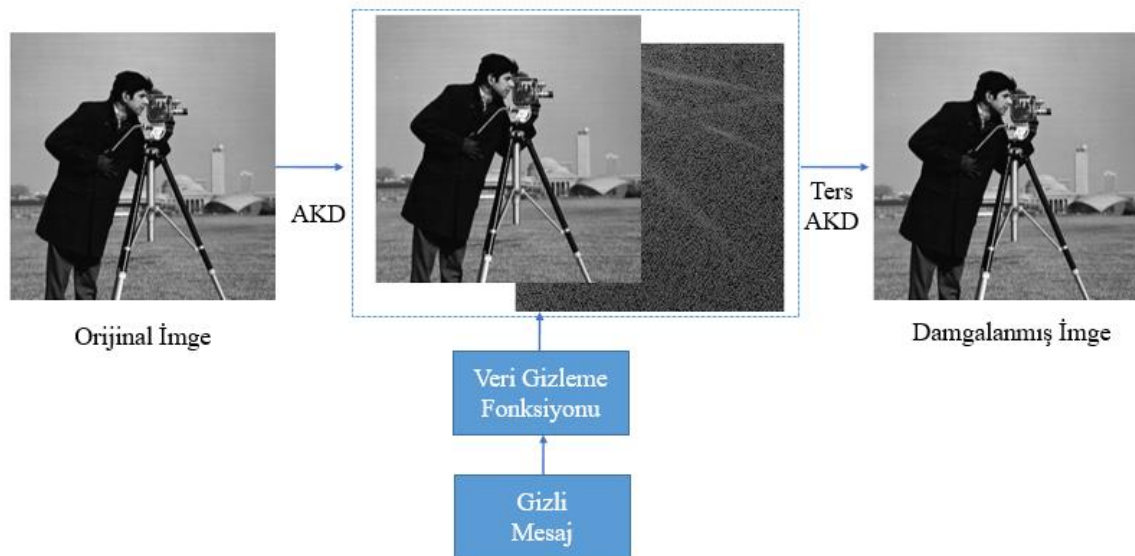
**Şekil 5. 10.** (a) Tek seviyeli ADD ile imgenin alt bantlarına ayrılması (b) Üç seviyeli ADD ile imgenin alt bantlarına ayrılması

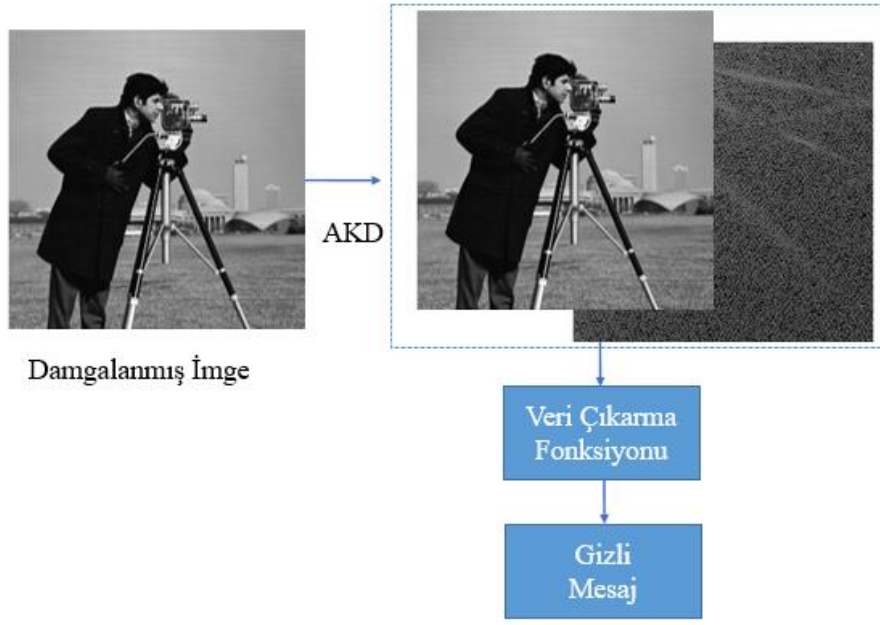
Elde edilen ADD alt bantlarına ait katsayılar kullanılarak damgalama işlemi gerçekleştirilmektedir. Günümüzde 37 farklı ADD tipi kullanılmaktadır. Genellikle DY, YD ve YY alt bantlarına damga eklenerek damgalı imge elde edilmektedir. Bu yöntemlerde damga alt bantlara ya doğrudan eklenmekte ya da EÖB gibi veri gizleme yöntemleri kullanılarak damga eklenmektedir. Bu yöntemin kullanılmasının en büyük avantajı saldırılara karşı dayanıklı damgalama modelleri elde edebilmektir. Literatürde, dayanıklı damgalama modelleri oluşturmak için  $DD_2$  alt bandının frekans katsayılarının kullanılması önerilmiştir. Yüksek geçirgen bantlardan elde edilen katsayılar kullanılarak veri gizleme işlemleri de yapılabilmektedir. DY, YD ve YY gibi frekans alt bantlarında bulunan katsayılar kullanılır. Bu katsayılar imgenin ayrıntı bilgilerini vermektedir ve burada yapılacak büyük değişiklikler imgeyi çok fazla bozmamaktadır.

ADD'nin veri gizleme açısından en olumsuz yanı ise veri kayıplarına sebep olmasıdır. Veri kayıplarının önüne geçebilmek için katsayıları tamsayı olarak üretebilen ikinci nesil ADD'ler kullanılmaktadır. Bu dönüşümlerden en çok bilineni ise Kaldırma Dalgacık Dönüşümüdür (KDD). KDD 1998 yılında Swelden tarafından önerilmiştir. Bu dönüşümün 3 aşaması vardır bu aşamalar bölme, tahmin ve güncelleştirme aşamalarıdır [104]. KDD tüm dalgacık filtre tiplerine uygulanabilmektedir.

### 5.2.2. Ayırık Kosinüs Dönüşümü Tabanlı Sayısal Damgalama

AKD, özellikle örüntü tanıma, özellik çıkarma, veri gizleme ve veri sıkıştırma algoritmalarında yaygın olarak kullanılan bir dönüşümdür. 2 boyutlu AKD (2B AKD) genellikle imgeler için kullanılmaktadır ve JPEG sıkıştırma algoritmasının temelini oluşturmaktadır. İmgeyi 8 x 8 boyutunda bloklara ayırarak piksel değerlerini frekans düzlemine taşır [105]. Ayırık Fourier Dönüşümü (AFD), karmaşık işareti karmaşık uzayda dönüştürür. Ancak işaret gerçel sayılardan oluşuyorsa yani sanal kısmı sıfır ise spektrumda gerçel ve sanal kısımlar birbirinin aynısı olur. Bu da elde edilen dönüşümün yarısının kendisini tekrar edeceği anlamına gelir. AKD, gerçel işareti gerçel spektruma dönüştürerek AFD'nin tekrar problemini çözer. AKD sinyalleri değişken frekanslardaki sinüslerin toplamına dönüştürür. İmgeler için 2B AKD kullanılır ve imgenin bir matris denklemi elde edilir.  $N \times M$  boyutundaki bir imgeye 2B AKD uygulanarak  $N \times M$  boyutunda AKD katsayıları elde edilir. Elde edilen bu matrisin sol üst köşesinde bulunan katsayılar enerjinin çok büyük bir kısmını tutarlar. Dolayısıyla bilginin büyük bir kısmı da bu alandadır. Uygun tarama yöntemleri ile matris tek boyutlu dizilere taşınır ve geliştirilen algoritmalarla bu bilgiler daha ayrıntılı, sağlam ve güvenli olarak işlenebilir [106]. AKD imgenin tamamına uygulanırsa bu tür dönüşüme Global AKD denir. Bu durumda imgenin tüm noktaları arasındaki ilişki kodlanmaya çalışılır. İmgenin belirli bölgesi ile ilgili ayrıntı elde edilmek istenirse imgenin tümüne AKD uygulanması istenen sonucu vermeyebilir. İmgenin tümüne AKD uygulanmasının yerine imgenin alt bloklarına AKD uygulanması daha uygun olacaktır. AKD'nin işlem basamakları Şekil 5.11'de verilmiştir [107].





Şekil 5. 11. AKD ile damgalamanın blok diyagramı

AKD tabanlı sayısal damgalama tekniğinin işlem adımları aşağıdaki gibi verilmiştir.

**Adım 1:** Örtü imge 8 x 8 boyutunda bloklara ayrılır.

**Adım 2:** Her bloğa 2B AKD uygulanır.

**Adım 3:** Orta frekans bandında iki adet  $ind_1$  ve  $ind_2$  adında indis seçilir. Örneğin (4,3) ve (5,3) indisindeki değerler seçilir.

**Adım 4:** Frekans bileşenleri arasındaki fark az olduğu için  $k$  adında bir toplama sabit seçilir.

**Adım 5:** Eğer gizli veri 0 ise  $ind_1 > ind_2$  şartının sağlanması gerekmektedir. Bu şart sağlanmıyorsa  $ind_1$  indisine  $k$  değeri eklenerek şart sağlanır.

**Adım 6:** Eğer gizli veri 0 ise  $ind_2 \geq ind_1$  şartının sağlanması gerekmektedir. Bu şart sağlanmıyorsa  $ind_2$  indisine  $k$  değeri eklenerek şart sağlanır.

**Adım 7:** Gizli veri uzunluğunca Adım 1- 6 tekrarlanır.

**Adım 8:** Her bir bloğa ters 2B AKD uygulanarak damgalanmış imge elde edilir.

**Adım 9:** Damgalanmış imgeden gizli veriyi elde etmek için alt bloklara AKD uygulanır ve Adım 4 ve 5'teki şartlar kullanılarak gizli veri elde edilir.

$k$  sabitiyle toplama yerine seçilen indisler yer değiştirilerek de veri gizleme işlemi uygulanır.

### 5.2.3. Tekil Değer Ayırışımı Tabanlı Sayısal Damgalama

Tekil Değer Ayırışımı (TDA) doğrusal matematik yöntemlerini kullanarak matrisleri çarpanlarına ayıran bir yöntemdir. Verilen bir matristeki problemleri belirleyip sayısal cevaplar bulmaya yarar [108]. Bir K matrisi  $K = USV^T$  olmak üzere üç ayrı matrisin çarpımına ayrıştırılabilir. Burada U, MxN ve  $V^T$ , NxN boyutunda ortagonal matrislerdir. S ise NxN boyutlarında bir köşegen matristir. S matrisinin sıfıra karşılık gelmeyen köşegen elemanları A matrisinin tekil değerleri olarak adlandırılır ve aşağıdaki gibi ifade edilebilir [109].

$$TDA(K) = \begin{bmatrix} u_1 & u_2 & u_3 \\ u_4 & u_5 & u_6 \\ u_7 & u_8 & u_9 \end{bmatrix} \times \begin{bmatrix} s_1 & 0 & 0 \\ 0 & s_2 & 0 \\ 0 & 0 & s_3 \end{bmatrix} \times \begin{bmatrix} v_1 & v_2 & v_3 \\ v_4 & v_5 & v_6 \\ v_7 & v_8 & v_9 \end{bmatrix} \quad (5.19)$$

K matrisinin aralığı r ise  $S = \text{diag} (s_1, s_2, \dots, s_n)$  değeri  $s_1 \geq s_2 \dots \geq s_{r+1} = s_n = 0$  özelliği sağlanmış olur. TDA yönteminde sayısal damgalama işlemi yapılırken damga imgenin köşegen matrisine eklenmektedir. TDA'nın en önemli özelliklerinden birisi AKD, AFD ve ADD gibi dönüşümlere göre daha dayanıklı sayısal damgalar oluşturulmasına olanak sağlamaktadır ve diğer dönüşümlerle birlikte kullanılabilir.

### 5.2.4. Kırılğan Damgalama

Kırılğan damgalama algoritmalarının temel amacı, multimedya veriye saldırıyı tespit edebilmek için kullanılmaktadır. Kırılğan damgalama yöntemleri genellikle parite biti kullanılır. Parite ve hamming ağırlığı hesaplanarak kırılğan damgalama işlemi gerçekleştirilir. Litetürde bulunan birçok yöntem ise kırılğanlığın sağlanması için doğrusal olmayan fonksiyonları kullanmaktadır [110]. Kırılğan damgalar telif hakkı sağlamak için uygun değildir çünkü en küçük saldırıda damga bozula bilmektedir. Bir kırılğan damgalama şemasının özellikleri ise aşağıdaki gibidir.

- Saldırı yapılan bölgeyi tespit edebilme imkânı sağlamalıdır.
- Yüksek görsel/işitsel kaliteye sahip olmalıdır.
- Damga kolaylıkla tahmin edilememelidir.
- Damga alıcı tarafından elde edilmeli ve doğrulanmalıdır.
- Eğer anahtar kullanılıyorsa damgalama anahtar uzayı yeterince geniş olmalıdır.

- Eđer 6zet fonksiyonu kullanılıyorsa, g6venilirlięi ispatlanmış bir 6zet fonksiyonu kullanılmalıdır.
- Eđer doęrusal olmayan bir denklem kullanılıyorsa, bu denklemin tohum deęerlerinde yapılacak k66k deęişimler ıktıda kabul edilebilir farklılıklar oluřturmalıdır.



## 6. VERİ GİZLEME DEĞERLENDİRME PARAMETRELERİ

Bir veri gizleme algoritmasını değerlendirebilmek için temel olarak 3 parametre bulunmaktadır ancak bu tez çalışmasında değerlendirme parametrelerinin sayısı 6'ya çıkarılmıştır. Bunlar ise aşağıdaki gibidir [111,112].

- Optimum yolla veri gizleme
- Optimum yolla veri çıkartılması
- Veri gizleme kapasitesi
- Saldırılara karşı dayanıklılık/kırılganlık
- Transparanlık (Görsel/ İşitsel Kalite)
- Gizlilik

Bu parametreler aşağıdaki bölümlerde tek tek ele alınmıştır.

### 6.1. Optimum Yolla Veri Gizleme

Bu parametrede veri gizleme algoritması çalışma zamanı göz önüne alınmaktadır. Amaç hızlı bir veri gizleme fonksiyonu kullanmaktır. Örneğin EÖB yöntemi değerlendirilirse aşağıdaki algoritmanın kullanılması gerekmektedir.

**Tablo 6. 1.** EÖB veri gizleme fonksiyonunun algoritması

---

**Algoritma 6.1.** EÖB veri gizleme fonksiyonunun algoritması

---

**Girdi:** W x H boyutunda örtü imge  $\tilde{O}$ , W x H bitlik gizli veri SD

```
1: for i= 1 to W do
2:   for j=1 to H do
3:     bits(1:8)=dec2bin( $\tilde{O}(i,j)$ ,8); // Örtü imgenin piksellerinin ikilik tabana dönüştürülmesi
4:     bits(8)=SD(i,j);
5:     kk=0;
6:      $S\tilde{I}(i,j)=0$ ;
7:     for kk=1 to 8 do
8:        $S\tilde{I}(i,j)=S\tilde{I}(i,j)+bits(kk) \cdot 2^{kk-1}$ 
9:     endfor
10:   endfor
11: endfor
```

**Çıktı:** : W x H boyutunda stego imge  $S\tilde{I}$

---

Yukarıdaki algoritmada görüldüğü gibi örtü imgenin veri gizlenecek piksellerini ikili tabana dönüştürüldükten sonra, elde edilen en anlamsız bit gizli verinin bitleriyle değiştirilmektedir. Yukarıdaki algoritmanın karmaşıklığı ise  $O(n^3)$ 'dür ve kullanılan bu algoritma EÖB veri gizleme fonksiyonu için optimum veri gizleme fonksiyonu değildir. EÖB için optimum veri gizleme fonksiyonu aşağıda Tablo 6.2'deki algoritmada verilmiştir.

**Tablo 6. 2.** EÖB için önerilen optimum veri gizleme algoritması

| <b>Algoritma 6.2.</b> EÖB optimum veri gizleme fonksiyonunun algoritması        |                                                                |
|---------------------------------------------------------------------------------|----------------------------------------------------------------|
| <b>Girdi:</b> W x H boyutunda örtü imge $\hat{O}I$ , W x H bitlik gizli veri SD |                                                                |
| 1:                                                                              | <b>for</b> i= 1 to W <b>do</b>                                 |
| 2:                                                                              | <b>for</b> j=1 to H <b>do</b>                                  |
| 3:                                                                              | <b>if</b> SD(i,j)=0 and $\hat{O}I(i,j) \pmod{2}=1$ <b>then</b> |
| 4:                                                                              | $S\hat{I}(i,j)=\hat{O}I(i,j)-1$ ;                              |
| 5:                                                                              | <b>endif</b>                                                   |
| 6:                                                                              | <b>if</b> SD(i,j)=1 and $\hat{O}I(i,j) \pmod{2}=0$ <b>then</b> |
| 7:                                                                              | $S\hat{I}(i,j)=\hat{O}I(i,j)+1$ ;                              |
| 8:                                                                              | <b>endif</b>                                                   |
| 9:                                                                              | <b>endfor</b>                                                  |
| 10:                                                                             | <b>endfor</b>                                                  |
| <b>Çıktı:</b> : W x H boyutunda stego imge $S\hat{I}$                           |                                                                |

Tablo 6.2'de gösterilen algoritma Tablo 6.1'de gösterilen algoritmaya göre daha hızlı çalışmaktadır. Çünkü Tablo 6.1'de verilen algoritmanın karmaşıklığı  $O(n^3)$ 'dür. Tablo 6.2'de bu algoritma optimize edilmiştir ve karmaşıklık  $O(n^2)$ 'ye düşürülmüştür. Karmaşıklığın  $O(n^2)$  olmasının sebebi ise imgede nokta operatörünün kullanılmasıdır.

## 6.2. Optimum Yolla Veri Çıkarma

Bu değerlendirme parametresinde ise veri çıkarma algoritmasının çalışma zamanı göz önüne alınmaktadır. Amaç hızlı bir veri çıkarma fonksiyonu kullanmaktır. Örneğin EÖB yöntemi değerlendirilirse Tablo 6.3'deki algoritmanın kullanılması gerekmektedir.

**Tablo 6. 3.** EÖB veri çıkarma fonksiyonu algoritması

| <b>Algoritma 6.3.</b> EÖB veri çıkarma fonksiyonu algoritması |  |
|---------------------------------------------------------------|--|
| <b>Girdi:</b> W x H boyutunda stego imge $S\hat{I}$           |  |

---

```

1: for i= 1 to W do
2:   for j=1 to H do
3:     bits(1:8)=dec2bin(Öİ(i,j),8); // Stego imgenin piksellerinin ikilik tabana dönüştürülmesi
4:     SD(i,j)= bits(8);
5:   endfor
6:endfor
Çıktı: : W x H boyutunda gizli veri SD

```

---

Yukarıdaki algoritmanın 3. satırının kullanılan *dec2bin* fonksiyonu piksel değerini onluk tabandan ikili tabana çevirmeyi sağlamaktadır ancak bu fonksiyon maliyetli bir fonksiyondur. Bu fonksiyonu gerçekleştirmek için döngü kullanılması gerekmektedir. Kullanılacak döngü ise bu algoritmanın karmaşıklığını  $O(n^3)$ 'e çıkarmaktadır ve bu da istenmeyen bir durumdur. Bu durumu gidermek için ve optimum veri çıkarma algoritmasını oluşturmak için gerçekleştirilen sözde kod Tablo 6.4'deki verilmiştir.

**Tablo 6. 4.** EÖB optimum veri çıkarma fonksiyonu algoritması

---

**Algoritma 6.4.** EÖB optimum veri çıkarma fonksiyonu algoritması

---

**Girdi:** W x H boyutunda stego imge Sİ

```

1: for i= 1 to W do
2:   for j=1 to H do
3:     SD(i,j)= Sİ (mod 2);
4:   endfor
5: endfor

```

**Çıktı:** : W x H boyutunda gizli veri SD

---

Tablo 6.4'de verilen algoritmanın karmaşıklığı  $O(n^2)$ 'dir. Bitlere ayırma işleminin yerine mod fonksiyonu kullanılmıştır. Böylece veri çıkarma fonksiyonu hem daha hızlı çalışır hale getirilmiştir hem de algoritmanın okunabilirliği iyileştirilmiştir.

### 6.3. Kapasite

Bir veri gizleme algoritmasını değerlendirirken olmazsa olmaz başarımlar parametrelerinin başında kapasite gelmektedir. Literatür incelendiğinde, veri gizlemeyle ilgili yapılan çalışmaların hepsinde veri gizleme kapasitesi verilmiştir. Veri gizleme kapasitesi ses dosyaları için kpbs (kilo bit per second- saniyede kilo bit) belirtilirken, imge dosyalarında

bpp (bit per pixel – piksel başına bit) olarak verilmektedir ancak genel olarak veri gizleme kapasitesi bit olarak adlandırılmaktadır. Örneğin 512 x 512 boyutundaki 8 bitlik bir gri seviyeli imgeli 512 x 512 bitlik veri gömüldüğünde kapasite 1 bpp olmaktadır. Gizli verinin boyutu 1024 x 1024 bit olduğunda ise kapasite 4 bpp olmaktadır [113].

EÖB, EAB (en anlamsız basamağa veri gizleme) gibi bit veya basamak değerini referans alan veri gizleme yöntemlerinde kapasite sabitken, PDF ve EMD gibi blok veya kural tabanlı yöntemlerde ise kapasite değişmektedir. Literatürdeki önerilen veri gizleme yöntemleri multimedya verisi olarak genellikle imgeleri kullanmaktadır ve referans olarak kullanılan yöntemlerin kapasitesi genellikle piksel başına 2 bittir.

#### 6.4. Saldırlara Karşı Dayanıklılık/Kırılabilirlik

Veri gizleme algoritmalarında özellikle sayısal damgalama uygulamalarında gizli verinin saldırılara karşı dayanıklı olması istenmektedir ancak kırılabilir damgalama ve multimedya mesajları kimliklendirme uygulamalarında ise gizli verinin kırılabilir olması istenmektedir. Bir veri gizleme algoritmasının dayanıklılığının test edilmesi için aşağıdaki saldırılar kullanılmaktadır.

- Kesme saldırısı,
- Kolaj saldırısı,
- Döndürme saldırısı,
- JPEG sıkıştırma saldırısı,
- Medyan filtre saldırısı,
- Boyutlandırma saldırısı.

Stego nesneye yukarıdaki ataklar uygulandıktan sonra gizli veri çıkarılır ve gizli veriye verdiği zararı belirlemek için ise BER (Bit Error Rate) kullanılmaktadır. BER'in formülü Denklem 6.1'de verilmiştir.

$$BER = \frac{\text{toplam bit değişimi}}{\text{toplam bit sayısı}} \quad (6.1)$$

Dayanıklı veri gizleme algoritmalarında BER değerinin düşük kırılabilir veri gizleme algoritmalarında ise yüksek çıkması istenir. Literatürdeki birçok örnekte ise BER yerine görsel gizli veriler kullanılmaktadır ve gizli verideki değişim görsel olarak gösterilmektedir[114].

## 6.5. Transparanlık

Veri gizleme uygulamalarının değerlendirilmesinde kullanılan en önemli parametrelerden birisi de transparanlıktır. Veri gizlemenin temel amacını ortaya koyan başarımlar parametresi olarak da adlandırılmaktadır ve bu başarımlar parametresini test etmek için birçok değerlendirme kriteri önerilmiştir ancak transparanlığı ifade etmek için en yaygın olarak kullanılan istatistiksel özellik SNR ve PSNR'dir. Aşağıdaki alt bölümlerde transparanlığı ölçmek için kullanılan istatistiksel özellikler verilmiştir[115].

### 6.5.1. Sinyal Gürültü Oranı

Bu istatistiksel özellik genellikle ses veya EKG sinyallerini kullanan veri gizleme yöntemlerinin başarımlarını ölçmek için kullanılmaktadır. Aşağıdaki denklemde SNR'ye ait denklem verilmiştir.

$$SNR = 10 \log_{10} \frac{\sum_{i=1}^N cs^2(i)}{\sum_{i=1}^N (cs(i) - ss(i))^2} \quad (6.2)$$

Yukarıdaki denklemde  $cs$  örtü sinyali,  $ss$  stego sinyal,  $N$  sinyalin uzunluğu ve  $i$  ise indisleri temsil etmektedir. SNR'nin yüksek elde edilmesi veri gizleme algoritmasının transparanlığın yüksek olduğunu, düşük elde edilmesi ise transparanlığın kötü olduğunu ifade etmektedir [116].

### 6.5.2. Ortalama Karesel Hata

Veri gizleme algoritmalarının görsel kalitesini ölçmek için en sık kullanılan istatistiksel özelliklerden biridir ortalama karesel hatadır (mean square error - MSE). MSE'nin formülü Denklem 6.3'te verilmiştir.

$$MSE = \frac{1}{WH} \sum_{i=1}^W \sum_{j=1}^H (\mathcal{O}i_{i,j} - S\mathcal{I}_{i,j})^2 \quad (6.3)$$

$\mathcal{O}i$  örtü imge,  $S\mathcal{I}$  stego imge,  $W$  imgenin genişliği,  $H$  imgenin uzunluğu,  $i$  ve  $j$  ise indislerdir [115].

MSE ile transparanlık ters orantılıdır. Özellikle 2 bpp kapasiteli veri gizlemelerde mükemmel MSE 1 olarak kabul edilmektedir. 1'in altında elde edilen MSE değerleri çok başarılı olarak kabul edilmektedir.

### 6.5.3. Tepe Sinyal Gürültü Oranı

Tepe sinyal gürültü oranı (Peak Signal to Noise Ratio – PSNR) parametresi özellikle imge ve video verisi kullanan veri gizleme algoritmalarının transparanlığını ölçmek için kullanılmaktadır. Literatürde en sık rastlanan ölçüm metriğidir. 8 bitlik imgeler için kabul edilebilir PSNR değerinin 30 ve üzerinde olması beklenmektedir. PSNR'nin formülü Denklem 6.4'te verilmiştir [115].

$$PSNR = 10 \log \frac{Max(\hat{O}_{i,j}^2)}{MSE} \quad (6.4)$$

### 6.5.4. Bağlı Karesel Fark Yüzdesi

Bağlı karesel fark yüzdesi orijinal sinyal ve stego sinyal arasındaki bağlı karesel farkı ifade etmektedir. İki sinyal arasındaki fark arttıkça bağlı karesel fark yüzdesi lineer olarak artmaktadır. Bağlı karesel fark yüzdesinin formülü Denklem 6.5'te verilmiştir [117].

$$BFK = \sqrt{\frac{\sum_{i=1}^N (cs_i - ss_i)^2}{\sum_{i=1}^N cs_i^2}} \quad (6.5)$$

### 6.5.5. Piksel Bozulma Oranı

Piksel bozulma oranı parametresi genellikle ikili imgeler için kullanılan bir veri gizleme başarımlı parametresidir. Piksellerdeki bozulma oranını hesaplamak için kullanılmaktadır. Bozulma oranı arttıkça PD oranı artmaktadır. Teorik olarak olması gereken en yüksek PD oranı 0.45'tir. PD'nin formülü Denklem 6.6'te verilmiştir.

$$PD = \frac{\text{değişime uğramış toplam bit sayısı}}{\text{gömülen toplam bit sayısı}} \quad (6.6)$$

### 6.5.6. Yapısal Benzerlik

Yapısal benzerlik, özellik olarak PSNR'ye benzemektedir ve -1 ile 1 arasında değer almaktadır. SSIM değerinin 1'e yaklaşması, veri gizleme algoritmasının başarılı olduğunu göstermektedir.

$$SSIM(\ddot{O}i, Si) = \frac{(2\mu_{\ddot{O}i}\mu_{Si})(2\sigma_{\ddot{O}iSi} + c_2)}{(\mu_{\ddot{O}i}^2 + \mu_{Si}^2 + c_1)(\sigma_{\ddot{O}i}^2 + \sigma_{Si}^2 + c_2)} \quad (6.7)$$

$\mu_{\ddot{O}i}$  Örtü imgenin ortalaması,  $\mu_{Si}$  stego imgenin ortalaması,  $\sigma_{\ddot{O}i}^2$  örtü imgenin varyansı,  $\sigma_{Si}^2$  stego imgenin varyansı,  $\sigma_{\ddot{O}iSi}$  örtü imge ve stego imgenin kovaryansı,  $c_1 = (k_1L)^2$  ve  $c_2 = (k_2L)^2$ ,  $L$  piksel aralığıdır ve  $2^{bit} - 1$  olarak ifade edilmektedir.  $k_1 = 0.01$  ve  $k_2 = 0.03$  olarak seçilmektedir [118].

Yukarıda sayılan parametreler transparanlık veya görsel/işitsel kalite parametresi olarak kullanılmaktadır. Bu parametrelerin dışında tüm istatistiksel özellikler de kullanılabilir. Literatürde kurtosis, skewness vb. gibi istatistiksel özellikler de kullanılmaktadır. Ayrıca ki-kare ve RS (ölçeklenmiş aralık) gibi istatistiksel analizlerde kullanılmaktadır.

### 6.6. Gizlilik

Bu başarıım metriğinde istenen gizli verinin güvenliğinin sağlanmasıdır. Bu sebepten dolayı stego anahtarı kullanılmaktadır. Stego anahtarı kullanılarak gizli verinin örtü nesnesinde gizleneceği indisler belirlenir veya gizli veri şifrelenir. Bu tez çalışmasında sır paylaşımı tabanlı algoritmalar kullanılarak gizlilik ve transparanlık sağlanmıştır.

## 7. GELİŞTİRİLEN UYGULAMALAR

Bu tez çalışması süresi boyunca veri gizlemeyle ilgili birçok uygulama geliştirilmiştir. Bu uygulamalar geliştirilirken diğer yöntem-bilimlerden de faydalanılmıştır. Bu tez çalışmasının İkinci Bölümünde kriptoloji, Üçüncü Bölümünde Sır Paylaşımı ve Dördüncü Bölümünde görsel sır paylaşımı anlatılmıştır. Amaca uygun multimedya veri gizleme algoritmaları oluşturabilmek için kriptolojinin protokollerinden sır paylaşımı ve görsel sır paylaşımı yöntemlerinden faydalanılmıştır. Ayrıca blok ve kural tabanlı yeni multimedya veri gizleme algoritmaları geliştirilmiştir. Geliştirilen uygulamalar aşağıdaki gibidir.

- a) Sır paylaşımı tabanlı veri gizleme uygulamaları
  - DNA-XOR sır paylaşımı tabanlı veri gizleme algoritması
  - Frekans uzayında XOR sır paylaşım tabanlı veri gizleme algoritması
- b) Görsel sır paylaşımı tabanlı multimedya veri gizleme ve imge kimliklendirme uygulamaları
  - Braille alfabesi tabanlı olasılıksal görsel sır paylaşımı yöntemi
  - Göktürk Alfabesi tabanlı görsel sır paylaşımı yöntemi ile veri gizleme uygulaması
  - Renkli imgelerde kimlik doğrulaması ve saldırı tespiti için GSP tabanlı kırılğan damgalama algoritması.
- c) Çok Seviyeli Veri Gizleme Uygulamaları
  - Çok katmanlı görüntü steganografi
  - Ses sinyalleri için çok seviyeli ADD tabanlı veri gizleme algoritması
- d) Blok tabanlı veri gizleme uygulamaları
  - Mayın tarlası oyunu tabanlı veri gizleme algoritması.
  - Sayısal görüntüler için yön vektörü tabanlı veri gizleme algoritması

### 7.1. Sır PaylaşımıTabanlı Veri Gizleme Uygulamaları

(k,n) sır paylaşımı şemaları ilk kez 1979 yılında farklı iki uygulamayla Shamir ve Blackley tarafından önerilmiştir. Sır paylaşımının temel özelliği, karmaşık matematiksel işlemler kullanmadan veri gizliliğinin sağlanması ve gizli verinin birden fazla sır parçasına ayrılmasıdır. Veri gizlemenin temel değerlendirme parametrelerinden birisi de veri gizliliğidir. Veri gizliliğini sağlayabilmek için kullanılan en temel yöntem şifrelemedir

ancak multimedya mesajları şifreleme yöntemleri karmaşık matematiksel ve iteratif işlemler içerdiği için maliyetleri yüksektir. Ayrıca şifrelemenin görsel kaliteye herhangi bir etkisi bulunmamaktadır. Hem görsel kaliteyi arttırmak hem de veri gizliliğini sağlayabilmek için sır paylaşımı tabanlı veri gizleme uygulamaları geliştirilmiştir.

#### 7.1.1. DNA-XOR Sır Paylaşımı Tabanlı Veri Gizleme Algoritması

Önerilen yöntem Wang'ın sır paylaşımı yöntemine benzemektedir. Wang'ın (n,n) sır paylaşımı yönteminde rastgele n-1 adet matris üretilir ve n matris bu matrislere göre hesaplanır. Bu yöntem olasılıksal sır paylaşımı ve görsel sır paylaşımı yöntemlerinde kullanılmasına rağmen, veri gizleme açısından bir artı sağlamamaktadır. Bu yöntemde sır paylaşımıyla veri gizleme bir arada kullanılarak optimum veri gizleme algoritması elde edilmiştir. Bu yöntemin sır paylaşımı aşamasında DNA-XOR mantıksal operatörü kullanılarak olasılıksal sır paylaşımı şeması elde edilmiştir. Elde edilen sır parçaları 2EÖB veri gizleme fonksiyonu kullanılarak renkli imgenin katmanlarına gizlenmiştir. DNA-XOR 2 bitlik özel bir XOR operatörüdür ve bu operatör genellikle imge şifreleme işlemlerinde kullanılmaktadır. DNA-XOR operatörünün doğruluk tablosu aşağıdaki gibidir.

**Tablo 7. 1.** DNA-XOR operatörünün doğruluk tablosu

| XOR | A | G | C | T |
|-----|---|---|---|---|
| A   | A | G | C | T |
| G   | G | A | T | C |
| C   | C | T | A | G |
| T   | T | C | G | A |

DNA-XOR operatörünün doğruluk tablosu kullanılarak sır paylaşımı işlemi gerçekleştirilmiştir. Bu çalışmada kullanılan sır paylaşımı yöntemi Wang ve ark.'nın [78] sır paylaşımı yöntemine benzemektedir ancak bu yöntemde gizli veriyi elde edebilecek tüm olasılıklar değerlendirilir ve örtü nesneyi en az bozan değerler sır parçası olarak seçilir. Bozulmayı hesaplamak için MSE kullanılmaktadır [119].

### 7.1.1.1. Önerilen Algoritma

Yuan'ın makalesinin sonuç kısmında sır paylaşımı tabanlı veri gizleme algoritmalarının RGB imgelere veri gizlemede kullanılabileceğinden bahsedilmiştir [30]. Yüksek görsel kalitede, yüksek kapasiteli, güvenilir bir veri gizleme algoritması elde edebilmek için Yuan'ın sonuç kısmında önerdiği yöntem yeni bir sır paylaşımı kullanılarak elde edilmiştir. Gizli veri her bir katmana gömülmek üzere 3 adet sır parçasına ayrılmıştır. 2 bit işlemde 3 adet sır parçası elde edildiği için her bir veriyi oluşturabilecek 16 adet olasılık bulunmaktadır. Örneğin Adenin verisini elde edebilmek için gerekli olan üçlü kombinasyonlar Tablo 7.2'de verilmiştir.

**Tablo 7. 2.** Adenin değeri için üçlü DNA-XOR doğruluk tablosu

|   |   |   |   |   |   |   |    |   |   |   |   |   |   |
|---|---|---|---|---|---|---|----|---|---|---|---|---|---|
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 9  | 1 | 0 | 0 | 0 | 1 | 1 |
|   | A |   | A |   | A |   |    | C |   | A |   | T |   |
| 2 | 0 | 0 | 0 | 1 | 0 | 1 | 10 | 1 | 0 | 0 | 1 | 1 | 0 |
|   | A |   | G |   | G |   |    | C |   | G |   | C |   |
| 3 | 0 | 0 | 1 | 0 | 1 | 0 | 11 | 1 | 0 | 1 | 0 | 0 | 1 |
|   | A |   | C |   | C |   |    | C |   | C |   | G |   |
| 4 | 0 | 0 | 1 | 1 | 1 | 1 | 12 | 1 | 0 | 1 | 1 | 0 | 0 |
|   | A |   | T |   | T |   |    | C |   | T |   | A |   |
| 5 | 0 | 1 | 0 | 0 | 0 | 1 | 13 | 1 | 1 | 0 | 0 | 1 | 0 |
|   | G |   | A |   | G |   |    | T |   | A |   | C |   |
| 6 | 0 | 1 | 0 | 1 | 0 | 0 | 14 | 1 | 1 | 0 | 1 | 1 | 1 |
|   | G |   | G |   | A |   |    | T |   | G |   | T |   |
| 7 | 0 | 1 | 1 | 0 | 1 | 1 | 15 | 1 | 1 | 1 | 0 | 0 | 0 |
|   | G |   | C |   | T |   |    | T |   | C |   | A |   |
| 8 | 0 | 1 | 1 | 1 | 1 | 0 | 16 | 1 | 1 | 1 | 1 | 0 | 1 |
|   | G |   | T |   | C |   |    | T |   | T |   | G |   |

Tablo 7.2'de görüldüğü gibi A verisini elde edebilecek 16 adet farklı olasılık elde edilmektedir. Elde edilen 16 farklı olasılık A'yı oluşturan veri kümesidir. Önerilen algoritmada örtü imgesini en az bozacak üçlü kombinasyon sırasıyla imgenin R, G ve B katmanlarına gömülmektedir. Önerilen algoritmanın adımları aşağıdaki gibidir.

**Adım 1:** Örtü imgenin R,G ve B katmanları elde edilir.

**Adım 2:** Gizli veri DNA formuna çevrilir.

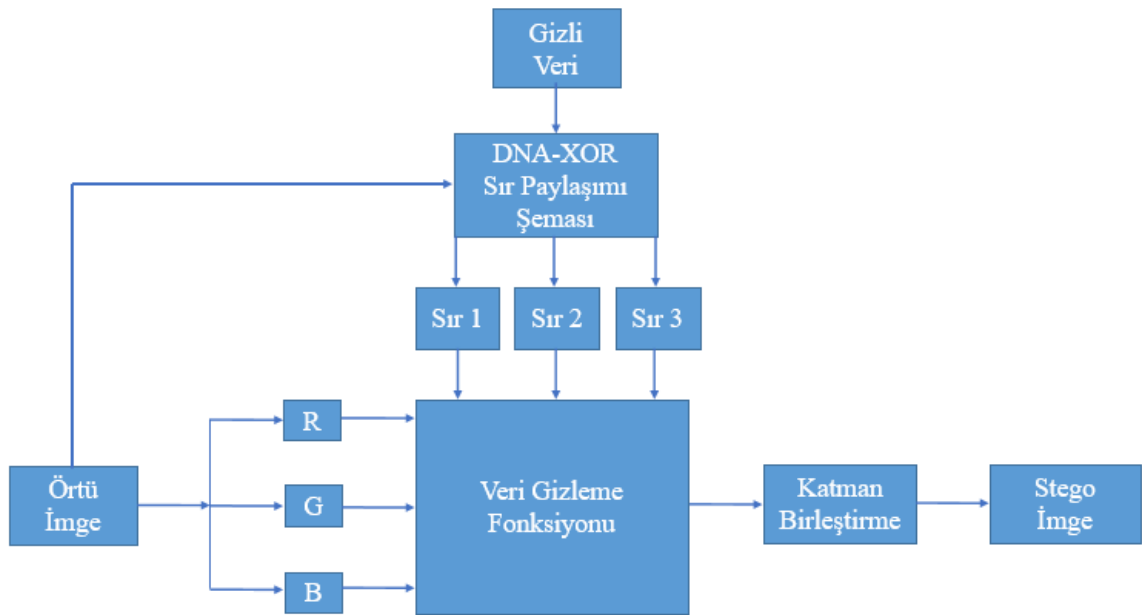
**Adım 3:** Her bir DNA kodu için olasılık tablosu oluşturulur.

**Adım 4:** Olasılık tablosunun her bir elemanı ile örtü imgenin elemanları arasındaki yerel MSE değerleri hesaplanır.

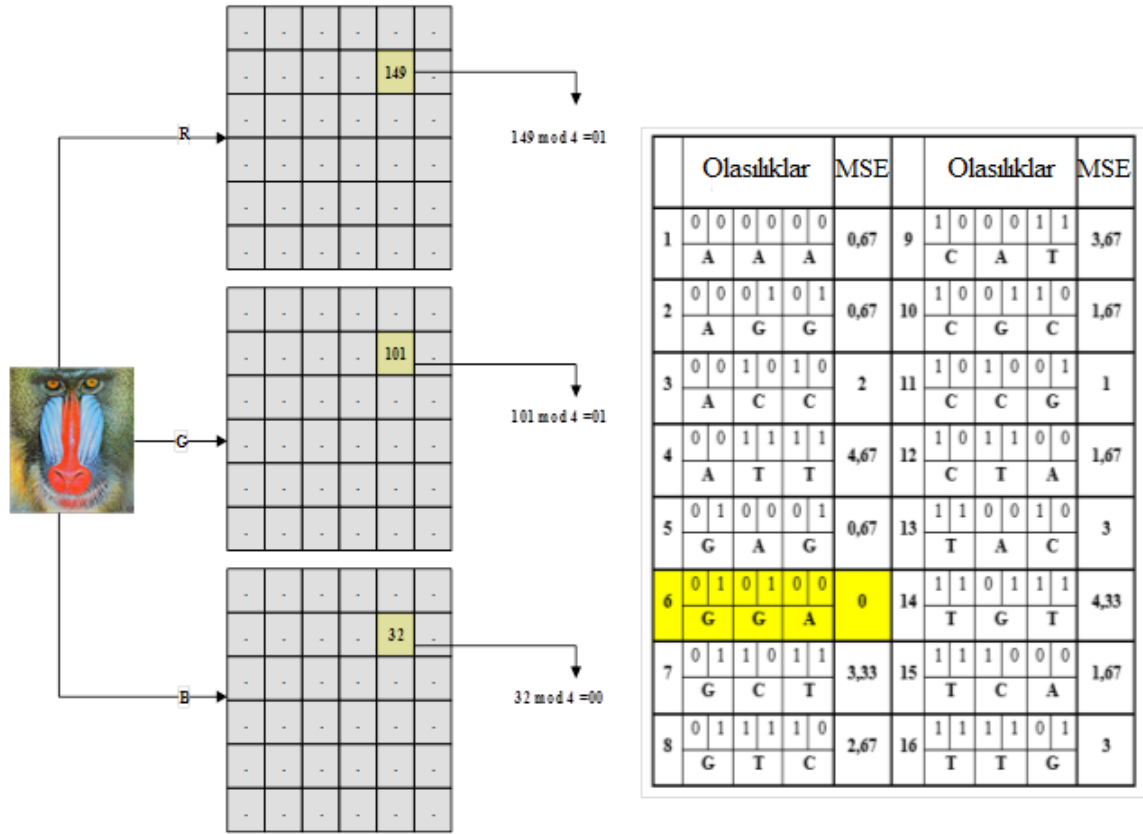
**Adım 5:** Minimum yerel MSE'ye sahip üçlü kombinasyon imgeye 2 EÖBs veri gizleme fonksiyonu kullanılarak gömülür.

**Adım 6:** Bu işlem gizli veri boyutunca devam eder.

Şekil 7.1'de önerilen veri gizleme algoritmasının blok diyagramı gösterilmiştir.



**Şekil 7. 1.** Önerilen veri gizleme algoritmasının blok diyagramı



Şekil 7. 2. A (00) verisinin önerilen algoritma kullanılarak imgeye gömülmesi

Şekil 7.2’de önerilen veri gizleme algoritmasının bir örneği verilmektedir [116]. Şekil 7.2’de görüldüğü gibi imgeyi en az bozacak üçlü kombinasyon G,G ve A’dır.

Önerilen algoritmanın veri çıkarma adımları aşağıdaki gibi verilmiştir.

**Adım 1:** Stego imgenin R,G ve B katmanları elde edilir.

**Adım 2:** Stego-anahtar kullanarak veri gizlenmiş indisler tespit edilir.

**Adım 3:** Veri gizlenmiş piksellere mod 4 işlemini uygulanır.

**Adım 4:** Kullanılan DNA tablosuna göre elde edilen değeri A,T,G veya C’ye çevir.

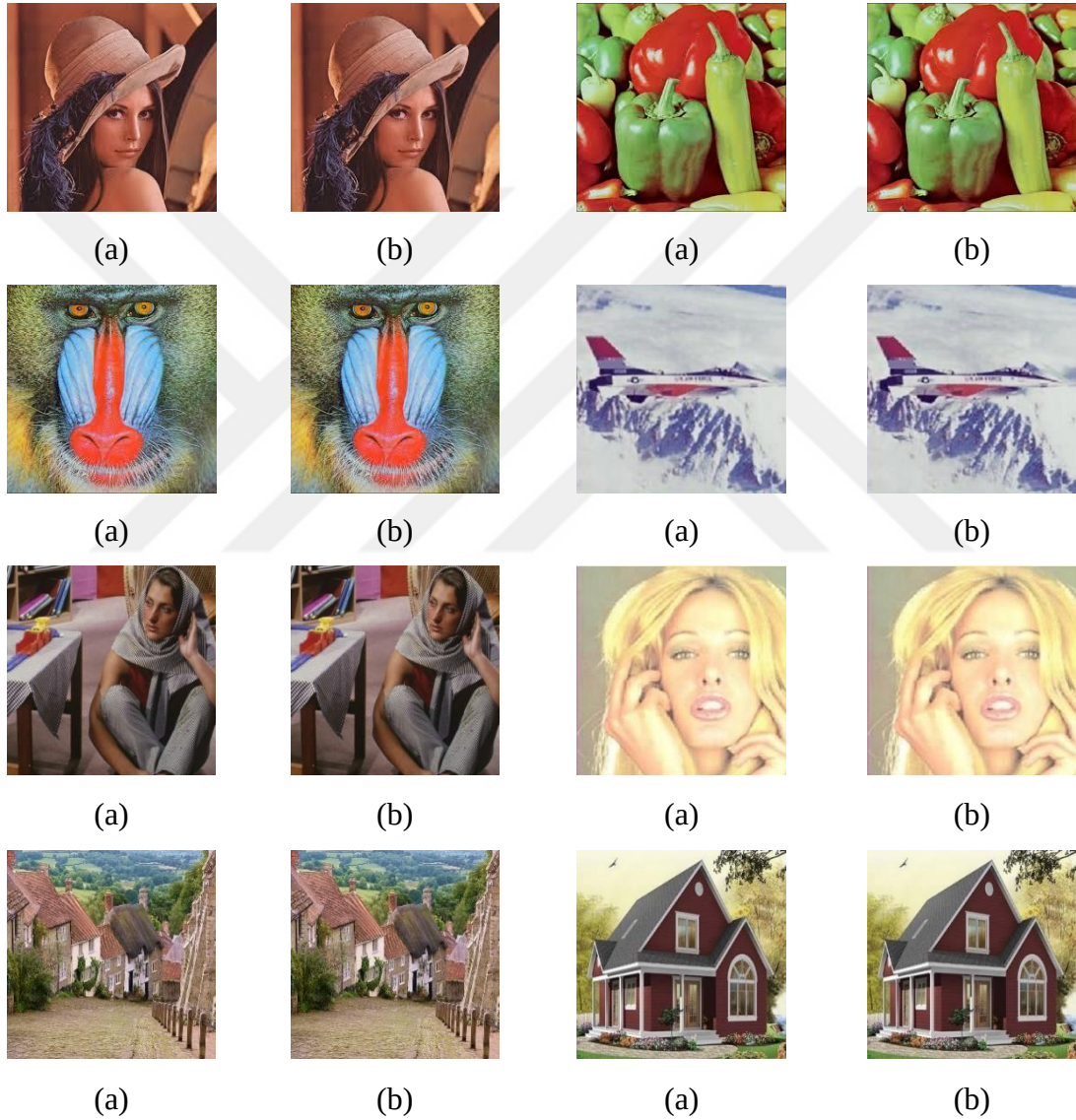
**Adım 5:** Elde edilen DNA kodlarına DNA-XOR operatörünü uygula.

**Adım 6:** Gizli veri boyutunca işlemleri tekrarla.

**Adım 7:** Elde edilen DNA kod yapısındaki gizli veriyi DNA kod tablosunu kullanarak istenilen formata çevir.

### 7.1.1.2. Deneysel Sonuçlar

Önerilen algoritmanın performansını test edebilmek için SIPI imge veritabanından seçilmiş 512 x 512 boyutunda 8 adet RGB imge kullanılmıştır. Bu imgeler sırasıyla Lena, Peppers, Tiffany, Goldhill, Baboon, Jet, Barbara ve House imgeleridir. Kullanılan imgeler Şekil 7.3'te gösterilmiştir [120].



Şekil 7. 3. Deneysel sonuçları elde etmek için kullanılan test imgeleri (a) orijinal imge (b) Stego-imge

Şekil 7.3'de gösterilen test imgelerine 2 bpp kapasitede veri gizlenmiştir. Elde edilen PSNR, BER, PD ve SSIM değerleri Tablo 7.3'de gösterilmiştir.

**Tablo 7. 3.** Önerilen yöntem kullanılarak elde edilen sonuçlar

| İmge     | PSNR  | BER    | PD     | SSIM   |
|----------|-------|--------|--------|--------|
| Lena     | 52.24 | 0.0272 | 0.1636 | 0.9996 |
| Peppers  | 52.12 | 0.0273 | 0.1632 | 0.9999 |
| Baboon   | 52.18 | 0.0273 | 0.1641 | 0.9996 |
| Jet      | 52.18 | 0.0269 | 0.1619 | 0.9890 |
| Barbara  | 52.31 | 0.0273 | 0.1638 | 0.9986 |
| Tiffany  | 52.11 | 0.0274 | 0.1646 | 0.9997 |
| Goldhill | 52.27 | 0.0273 | 0.1643 | 0.9998 |
| House    | 52.11 | 0.0268 | 0.1605 | 0.9991 |

Önerilen yöntemin performansının diğer veri gizleme yöntemleriyle karşılaştırılması da gerekmektedir. Önerilen yöntemin diğer yöntemlerle karşılaştırılması ise Tablo 7.4’de verilmiştir.

**Tablo 7. 4.** Önerilen yöntemin literatürde yaygın olarak kullanılan yöntemlerle karşılaştırılması

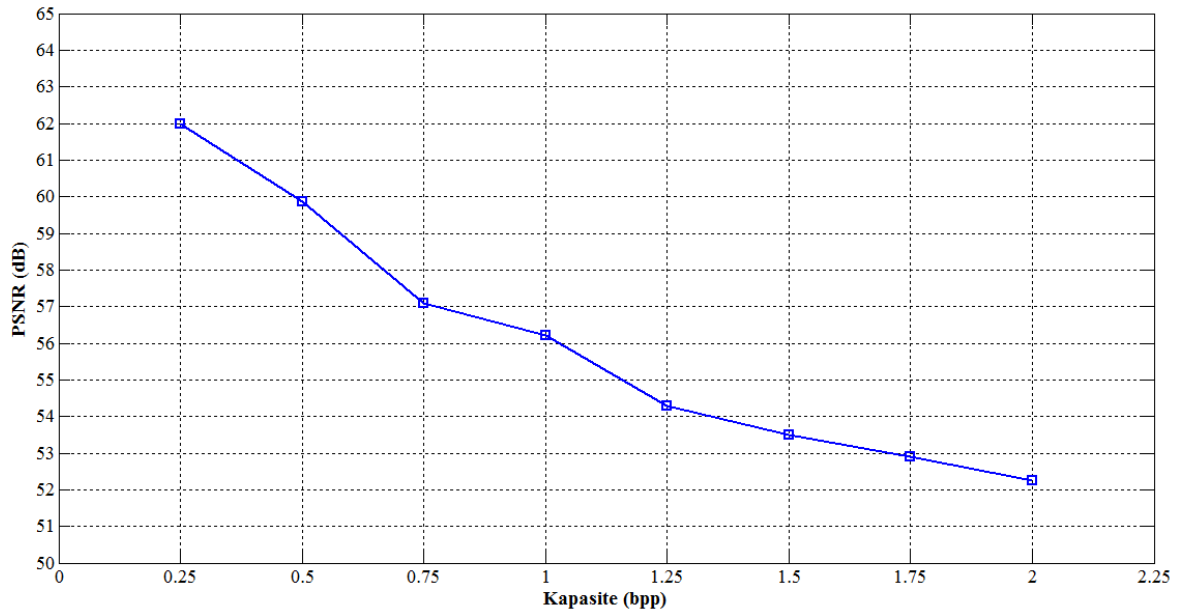
| Stego image | PSNR(dB)                     |                               |                                |                              |                                   |                       |
|-------------|------------------------------|-------------------------------|--------------------------------|------------------------------|-----------------------------------|-----------------------|
|             | Lin ve Tsai’nin yöntemi [25] | Yang ve ark.’nin yöntemi [26] | Chang ve ark.’nin yöntemi [27] | Wu ve ark.’nin yöntemi [121] | Kanan ve Nazeri’nin yöntemi [122] | Önerilen yöntem [119] |
| Lena        | 39.20                        | 41.60                         | 40.37                          | 43.54                        | 45.12                             | 52.24                 |
| Jet         | 39.25                        | 41.66                         | 40.73                          | 43.53                        | 45.18                             | 52.18                 |
| Peppers     | 39.17                        | 41.56                         | 39.30                          | 43.56                        | 45.13                             | 52.12                 |
| Baboon      | 39.18                        | 41.55                         | 39.94                          | 43.54                        | 45.12                             | 52.18                 |
| Average     | 39.2                         | 41.59                         | 40.08                          | 43.54                        | 45.14                             | 52.18                 |

Ayrıca önerilen yönteme ilham kaynağı olan ve veri gizlemeyle sır paylaşımını bir arada kullanıp başarılı sonuçlar elde eden Yuan’ın yöntemiyle önerilen veri gizleme algoritması karşılaştırılmıştır. Bu iki yöntemi karşılaştırmak için test imgelerine 131,072 bit veri gizlenmiştir. Elde edilen sonuçlar Tablo 7.5’de gösterilmiştir.

**Tablo 7. 5.** Önerilen yöntem ile Yuan'ın yönteminin karşılaştırılması

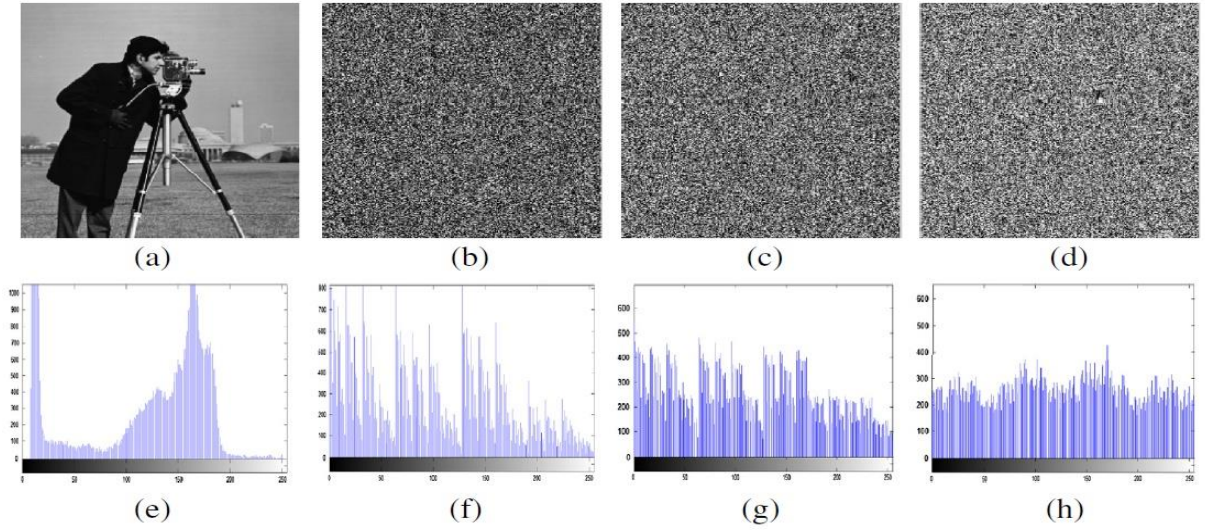
| Image   | Yuan'nın Yöntemi [30] |        | Önerilen Yöntem |        |
|---------|-----------------------|--------|-----------------|--------|
|         | PSNR                  | MSSIM  | PSNR            | MSSIM  |
| Lena    | 55.46                 | 0.9993 | 59.85           | 0.9999 |
| Jet     | 55.70                 | 0.9995 | 59.90           | 0.9999 |
| Peppers | 55.64                 | 0.9993 | 59.81           | 0.9999 |
| Bridge  | 51.46                 | 0.9991 | 59.89           | 0.9999 |
| Average | 54.56                 | 0.9993 | 59.86           | 0.9999 |

Önerilen algoritmanın PSNR/kapasite değişim oranı Şekil 7.4'da verilmiştir.



**Şekil 7. 4.** Önerilen algoritmanın ortalama PSNR/ kapasite değişimi

Yukarıdaki tablolar göz önüne alındığında, önerilen yöntemin yüksek görsel kalitede yüksek veri gizleme kapasitesine sahip olduğu görülmektedir. Yüksek görsel kalite hedeflenirken, gizli verinin güvenilirliği de sağlanmıştır. Şekil 7.5'de Baboon imgesine gömülen 256 x 256 boyutunda "cameraman" imgesi ve bu imgeye ait sır parçaları gösterilmektedir.



**Şekil 7. 5.** Olasılıksal DNA-XOR sır paylaşımı şeması (a) Orijinal imge (b) R katmanına gömülen sır parçası (c) G katmanına gömülen sır parçası (d) B katmanına gömülen sır parçası (e) orijinal imgenin histogramı (f) R katmanına gömülen sır parçasının histogramı (g)

Bu yöntemde, örtü imge şifreleme anahtarı gibi kullanılmaktadır. Örtü imgeyi en az bozacak olasılıklar sır parçası olarak seçilmekte ve imgeye gömülmektedir. Ayrıca önerilen algoritmada mod tabanlı veya EÖB gibi veri gizleme fonksiyonları kullanılmaktadır. Önerilen sır paylaşımı algoritmasının maliyeti  $O(n^2)$  iken veri gizleme fonksiyonunun maliyeti  $O(1)$ ' dir.

### 7.1.1.3. Sonuçlar

Bu yöntemde güvenilir, yüksek görsel kalite ve veri gizleme kapasitesine sahip, tersinir, basit ve uygulanabilir bir veri gizleme algoritması önerilmiştir. Toplama tabanlı sır paylaşımı algoritmasında toplama işlemi yerine DNA-XOR operatörü kullanılarak yeni bir sır paylaşımı yöntemi geliştirilmiştir. Genellikle imge şifreleme yöntemlerinde kullanılan DNA-XOR operatörü literatürde ilk kez sır paylaşımı tabanlı veri gizleme algoritmasında kullanılmıştır. Oluşturulan sır parçaları rastgele değil, örtü imgenin özelliklerine göre üretilmiştir. Örtü imgenin özellikleri kullanıldığı için en az değişimi gerçekleştirecek olasılıklar sır parçası olarak kabul edilir ve bu sebepten dolayı önerilen algoritmanın görsel kalitesi yüksektir.

Önerilen yöntem, literatürdeki diğer yöntemlerle karşılaştırılmış ve daha başarılı sonuçlar elde edilmiştir. 2 bpp kapasitede elde edilen PSNR 52 dB'den yüksektir. Bu değer  $48.13 \text{ dB}(10\log_{10} 255^2 / 1)$  büyüktür.

### 7.1.2. Frekans Uzayında XOR Sır Paylaşım Tabanlı Veri Gizleme Algoritması

Bu algoritmada XOR sır paylaşımı şeması kullanılarak sır paylaşımı yapılmıştır ve sır parçaları ADD katsayılarına gömülmüştür. Tek bir gri seviyeli imgeye sır paylaşımı kullanarak veri gizlemek için ADD'den faydalanılmıştır. Örtü imgeye ADD uygulanıp DD, DY, YD, YY bantlar elde edilmiştir. Gizli veri XOR sır paylaşım şeması uygulanıp 3 adet sır parçasına bölünmüştür. Elde edilen sır parçaları ise sırasıyla DY, YD ve YY altbantlarına gömülmüştür. Literatürde önerilen sır paylaşımı tabanlı veri gizleme algoritmalarında genellikle çok sayıda örtü imge kullanılmaktadır ve veri gizleme işlemi uzaysal alanda yapılmaktadır. Bu yöntemde tek bir örtü imgesi kullanılarak veri gizleme işlemi frekans alanında yapılmaktadır [123].

#### 7.1.2.1. Olasılıksal XOR Sır Paylaşımı Yöntemi

Olasılıksal XOR sır paylaşımı yöntemi XOR doğruluk tablosunu kullanmaktadır ve Tablo 7.6'de XOR doğruluk tablosu verilmiştir.

**Tablo 7. 6.** XOR doğruluk tablosu

| Sır 1 | Sır 2 | Sonuç |
|-------|-------|-------|
| 0     | 0     | 0     |
| 0     | 1     | 1     |
| 1     | 0     | 1     |
| 1     | 1     | 0     |

Tablo 7.6'de iki adet çıkış bulunmaktadır ve bu çıkışlar 0 ve 1'dir Bu çıkışları oluşturan kümeler ise  $S^0$  ve  $S^1$  olarak adlandırılmaktadır.  $S^0 = \{\{0,0\}, \{1,1\}\}$  ve  $S^1 = \{\{0,1\}, \{1,0\}\}$  dir. Her iki kümede de 2 adet 2'li kombinasyon bulunmaktadır. Eğer 0 bitini 2 adet sır parçasına ayırmak istenirse  $S^0$ 'da bulunan ikililerden birinin kullanılması gerekmektedir. Eğer 1 biti 2 adet sır parçasına ayırmak istenirse  $S^1$ 'de bulunan ikililerden birisinin kullanılması gerekmektedir. Kümelerin eleman sayısını hesaplayabilmek için ise Denklem 7.1 kullanılmaktadır.

$$n = 2^{b(s-1)} \quad (7.1)$$

n eleman sayısı, s sır parçası sayısını ve b ise çıkış bitlerini ifade etmektedir. Örneğin 2 bitlik 3 adet sır paylaşımı oluşturulursa, oluşacak kümeler  $S^{00}$ ,  $S^{01}$ ,  $S^{10}$  ve  $S^{11}$  olacaktır ve her bir küme 16 elemana sahip olacaktır. Bu ölçümü yapabilmek için tüm elemanlar imgeye gömülür ve yerel MSE değerleri elde edilir. Minimum değere sahip değer ise sır parçası olarak imgeye gömülmektedir. Yani seçme anahtarı olarak örtü imge veya örtü imgeye ait ADD katsayıları kullanılmaktadır. Gizli veriyi yeniden elde etmek için sır parçalarına XOR operatörü uygulanmaktadır [123].

#### 7.1.2.2. Önerilen Algoritma

Önerilen algoritmada örtü imgesi olarak gri seviyeli imgeler kullanılmaktadır. Örtü imgeye ADD uygulanarak alt bantlar elde edilmektedir. Eğer gizli veri 4 veya daha az sır parçasına bölünecek ise, tek seviyede iki boyutlu ADD uygulanması gerekmektedir. Eğer gizli veri daha fazla sır parçasına bölünecekse, örtü imgesine çok seviyeli ADD uygulanması gerekmektedir. Önerilen veri gizleme algoritmasının adımları aşağıdaki gibidir.

**Adım 1:** Örtü imgeye 2 boyutlu tam sayı ADD uygulanarak DD, DY, YD ve YY alt bantları elde edilir.

$$[DD, DY, YD, YY] = ADD(\text{Öİ}) \quad (7.2)$$

**Adım 2:** Gizli veriye olasılıksal XOR sır paylaşımı algoritması uygulanarak, olasılık kümeleri elde edilir.

**Adım 3:** Elde edilen olasılıklardan, DY, YD ve YY frekans katsayılarını en az bozan parçalar seçilir ve sır parçaları oluşturulur.

**Adım 4:** Oluşturulan sır parçaları sırasıyla DY, YD ve YY alt bantlarına 2EÖB kullanılarak gömülür.

**Adım 5:** Gizli veri boyutunca işlemleri tekrarlanır.

**Adım 6:** Veri gizlenmiş alt bantları DD alt bandına ters ADD uygulayarak Stego imge elde edilir.

$$Sİ = TADD(DD, sDY, sYD, sYY) \quad (7.3)$$

Önerilen yöntemin veri çıkarma algoritması ise aşağıdaki gibi verilmiştir.

**Adım 1:** Stego imgeye 2 boyutlu tam sayı ADD uygulanarak DD, DY, YD ve YY alt bantları elde edilir.

**Adım 2:** Elde edilen Stego DY, YD ve YY alt bantlarına mod 4 işlemi uygulanır.

**Adım 3:** Elde edilen değerlere XOR işlemi uygulanır.

$$GV_{i,j} = 2LSBs(LH_{i,j}) \oplus 2LSBs(HL_{i,j}) \oplus 2LSBs(HH_{i,j}) \quad (7.4)$$

GV gizli veri, 2EÖB fonksiyonu ise  $2EÖB(sayı) = sayı \pmod{4}$ .

**Adım 4:** Gizli veri boyutunca işlemler tekrarlanır.

### 7.1.2.3. DeneySEL Sonuçlar

DeneySEL sonuçları elde edebilmek için SIPI imge veritabanından seçilmiş 9 adet 512 x 512 boyutunda gri seviyeli imge kullanılmıştır. Test için kullanılan imgeler Şekil 7.6’da verilmiştir [120].



**Şekil 7. 6.** Test imgeleri (a) Baboon (b) Boat (c) Elaine (d) House (e) Lena (f) Peppers (g) F16 (h)Tiffany (f) Barbara

Gizli verinin boyutu ise 131, 072 bittir ve gizli veri rastgele üretilmiştir. Bu algoritmayı test edebilmek için 4 adet performans metriği kullanılmıştır. Bu metrikler kapasite, görsel kalite, gizlilik ve dayanıklılıktır.

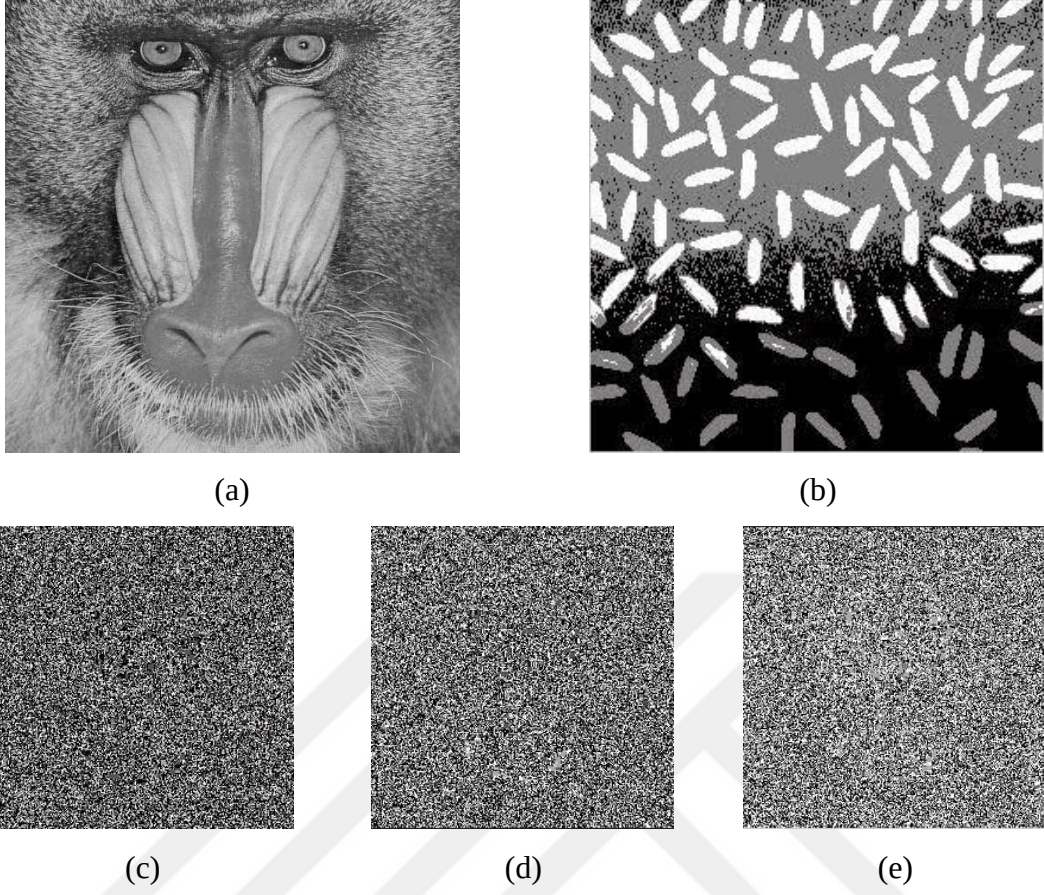
**Kapasite:** Gizli veri 131,072 bittir ve bu veri olasılıksal XOR sır paylaşımı yöntemi kullanılarak 3 adet sır parçasına ayrılmıştır. Her bir sır parçasının boyutu 131,072 bit olduğu için toplamda imgeye gömülen veri boyutu  $3 \times 131,072 = 393,216$  bittir ve toplamda imgelere 1.5 bpp kapasite veri gizlenmiştir.

**Görsel Kalite:** Görsel kaliteyi hesaplayabilmek için PSNR ve ortalama SSIM (MSSIM) görsel kalite ölçüm metrikleri kullanılmıştır. Elde edilen değerler Tablo 7.7’de verilmiştir.

**Tablo 7. 7.** 1.5 bpp kapasitede elde edilen PSNR ve MSSIM değerleri

| İmge    | PSNR  | MSSIM  | Kapasite |
|---------|-------|--------|----------|
| Baboon  | 51.67 | 0.9964 | 1.5 bpp  |
| Boat    | 51.58 | 0.9964 | 1.5 bpp  |
| Elaine  | 51.75 | 0.9965 | 1.5 bpp  |
| House   | 51.80 | 0.9965 | 1.5 bpp  |
| Lena    | 51.51 | 0.9964 | 1.5 bpp  |
| Peppers | 51.59 | 0.9964 | 1.5 bpp  |
| F16     | 51.63 | 0.9964 | 1.5 bpp  |
| Tiffany | 51.93 | 0.9966 | 1.5 bpp  |
| Barbara | 51.46 | 0.9962 | 1.5 bpp  |

**Gizlilik:** Olasılıksal XOR sır paylaşımı algoritması kullanılarak gizli veri 3 adet sır parçasına ayrılmıştır. Önerilen yöntemde bu sır paylaşımı algoritması kullanılarak olasılık kümeleri oluşturulmakta ve oluşan kümelerin imgeyi en az bozan elemanları sır parçası olarak seçilmektedir. Bu durumda imgenin ADD frekans katsayıları şifreleme anahtarı olarak kullanılmaktadır. Şekil 7.7’de gri seviyeli Baboon imgesine Rice imgesinin önerilen yöntemle gömülmesi ve elde edilen sır parçaları gösterilmiştir.



Şekil 7. 7. (a) Örtü imgesi (b) Gizli veri (c) Birinci sır parçası (d) İkinci sır parçası (e) Üçüncü sır parçası

**Dayanıklılık:** Sır paylaşım tabanlı veri gizleme algoritmaları ataklara karşı kırılgan bir davranış sergilemektedir ancak önerilen yöntem ile ADD katsayılarına veri gizlenmiştir. ADD'nin veri gizleme uygulamalarında kullanılmasının temel amaçlarından birisi de dayanıklılıktır. Bu sebepten dolayı önerilen yöntem yarı kırılgandır.

#### 7.1.2.4. Sonuç

Önerilen yöntem ile sır paylaşımı tabanlı veri gizleme uygulamalarının frekans alanında uygulanabileceği gösterilmiş ve tatmin edici sonuçlar elde edilmiştir. Ayrıca önerilen algoritma kullanılarak, gri seviyeli imgelerin kimlik doğrulamasının yapılabileceği de gösterilmiştir. 1.5 bpp kapasitede 51 dB'den yüksek PSNR elde edilmiştir. Bu da yöntemin görsel kalitesinin yüksek olduğunu göstermiştir. Veri gizleme fonksiyonu olarak 2EÖB veri gizleme fonksiyonu kullanılmıştır. Kullanılan sır paylaşımı algoritması sayesinde gizlilik sağlanmıştır. Ayrıca önerilen sır paylaşımı algoritmasının maliyeti  $O(n^2)$  iken veri gizleme

fonksiyonunun maliyeti  $O(1)$ 'dir. Önerilen algoritmanın sonuçları tatmin edicidir ve gelecekteki çalışmalarda alıcı ve satıcı damgalama protokollerinde de bu algoritmanın kullanılabileceği gösterilmiştir.

## 7.2. Görsel Sır Paylaşımı Tabanlı Veri Gizleme Uygulamaları

GSP şemaları, karmaşık matematiksel işlemler kullanmadan veri güvenliğini garanti eden algoritmalarlardır ancak bu algoritmaların en büyük problemi sahtecilik saldırılarıdır. Sır parçalarından herhangi birinin saldırganların eline geçmesi büyük bir problemdir. Bu durumda saldırgan mesajı bozabilmektedir. Bu durumu ortadan kaldırmak için güvenilir bir veri iletim hattının oluşturulması gerekmektedir ve bu sebepten dolayı veri gizleme algoritmalarının kullanılması önerilmiştir.

Tez süresince GSP şemaları detaylı olarak incelenmiştir. GSP şemalarında var olan problemler aşağıdaki gibidir.

- Gürültü benzeri veya dokusal imgeler üretildiği için saldırganların dikkatini çekmektedir.
- Sır parçalarının biri veya bir kaç ele geçirildiğinde saldırgan mesajı değiştirmek için yeni sır parçaları üretebilmektedir.
- Literatürde, saldırganların dikkatini çekmeyen anlamlı alt piksellerden oluşmuş GSP şemaları önerilmiştir ancak bu şemalarda Naor ve Shamir'in GSP şemasını kullanmaktadır.
- Anlamlı alt piksellerden oluşan GSP şemalarının çoğunun en büyük problemi, sözlükte harfleri eşit oranda kullanamamaları ve kontrast değerini ayarlayamamalarıdır.

Sayılan bu problemlerinin yanı sıra GSP şemalarının sağladığı en büyük avantaj ise, karmaşık matematiksel işlemler yapmaksızın veri güvenliği sağlayabilmeleri ve gizli mesaja kırılğan bir yapı kazandırıp multimedya veriye yapılan saldırıları kolayca tespit etme imkânı sağlayabilmeleridir. Bu bulgular ışığında 4 adet yeni yöntem geliştirilmiştir.

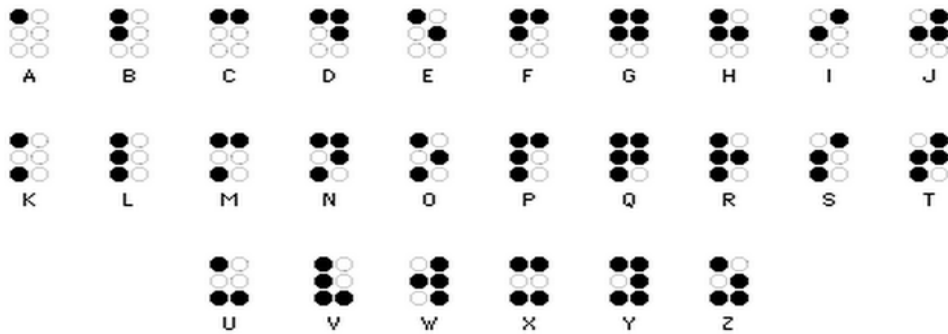
### 7.2.1. Braille Alfabeti Tabanlı Olasılıksal Görsel Sır Paylaşımı Yöntemi

Naor ve Shamir, imgelerin ve şifreleme anahtarlarının gizliliğinin korumak için  $(k,n)$  görsel sır paylaşımı (GSP) yöntemini önermiştir. Bu yöntem kullanılarak, gizli veri karmaşık hesaplamalar yapılmaksızın veri sır parçalarına ayrılabilir. Gürültü benzeri imgeler saldırganların dikkatini çekmektedir. Bu yöntemde alt pikseller, braille alfabesindeki harflerden oluşmaktadır yani sır parçaları anlamlı parçalardan oluşmaktadır. Bu çalışmada, olasılıksal bir yaklaşım kullanılarak yeni bir GSP önerilmiştir. Gizli mesajı yeniden elde etme aşamasında XOR operatörü kullanılmıştır. Ayrıca, önerilen braille tabanlı GSP (BGSP) kullanılarak veri gizleme yapılmıştır [124].

#### 7.2.1.1. Braille Alfabeti

Görme engelli kişilerin kullanması için, 1829 yılında Louis Braille tarafından önerilmiştir. Louis Braille bu alfabeye adını vermiştir ve bu alfabe literatürde Braille alfabesi olarak anılmaktadır. Braille alfabesi 6 adet noktadan oluşmaktadır ve bu noktalar  $3 \times 2$  boyutundaki bir matrise yerleştirilmiştir. Alfabede yer alan işaretlerin tamamı bu 6 noktanın pozisyonuna göre oluşturulmuştur [125]

Harflerin Braille alfabesine göre kodlanması Şekil 7.8’de verilmiştir.



Şekil 7. 8. Harflerin Braille kodları [126]

#### 7.2.1.2. Önerilen Yöntem

Bu yöntemde sır parçaları olarak, Şekil 7.10’da gösterilen Braille harfleri kullanılmıştır. Önerilen yöntem Naor ve Shamir’in  $(k,n)$  GSP şeması [71] ve Wang’ın OGSP şemasından esinlenerek ileri sürülmüştür [78]. Olasılıksal BGSP oluşturulduğu için rastgele sayı

üreteçleri kullanılmıştır. Sır paylaşımı gerçekleştirmek için XOR operatörü kullanılmıştır. Bu operatörün kullanılmasının en temel sebebi ise 0 ve 1'in oluşmasından 0.5'e en yakın olasılığın oluşmasıdır. (2,2) BGSP şemasında, 26 adet harf kullanıldığı için toplam olasılık sayısı  $26^2=676$ 'dır. Bir bloğun siyah piksele eşit olması için en az 4 adet siyah pikselin olması gerekmektedir. Diğer durumlarda o blok beyaz (1) olarak ifade edilecektir. Bu koşullar altında 362 çift Braille koda XOR işlemi uygulanması sonucu 1, 314 çift Braille kodun XOR işlemi uygulanması sonucu 0 elde edilecektir. Bu makalede önerilen olasılıksal yöntemin, Yang'ın [127] sunduğu OGSP'ye göre en temel farkı alt piksellerin anlamlı olmasıdır. Yang'ın şemasında imgenin kontrastı söz konusuysa, önerilen yöntemde harflerin eşit gelme olasılığı hesaplanmalıdır ve bu harfler biraraya geldiğinde 0 ve 1'i elde etme olasılıklarının hesaplanması gerekmektedir. Sözde rastgele sayı üreteçleri kullanılarak harflerin gelme olasılıkları uniform olarak ayarlanabilir. Kullanılan sözde rastgele sayı üreteçlerinin büyük bir kısmı üniform özellik gösterdiği için, bu yöntemde kullanılan rastgele sayı üreticinin türünün pek bir önemi yoktur.  $P(0)=314/676=0.4645$  ve  $P(1)=362/676=0.5355$  olacaktır. Olasılıkların 0.5'e yakın olmasından dolayı XOR operatörü kullanılmıştır. Önerilen olasılıksal BGSP'nin algoritması aşağıdaki gibidir. Ayrıca sır parçalarını gizlemek için veri gizleme algoritmalarından faydalanılmıştır. Önerilen BGSP tabanlı veri gizleme algoritmasının adımları aşağıdaki gibidir.

**Adım 1:** 0 ve 1 kombinasyonlarını iki ayrı listeye kaydet.

**Adım 2:** İkili imgeyi gir.

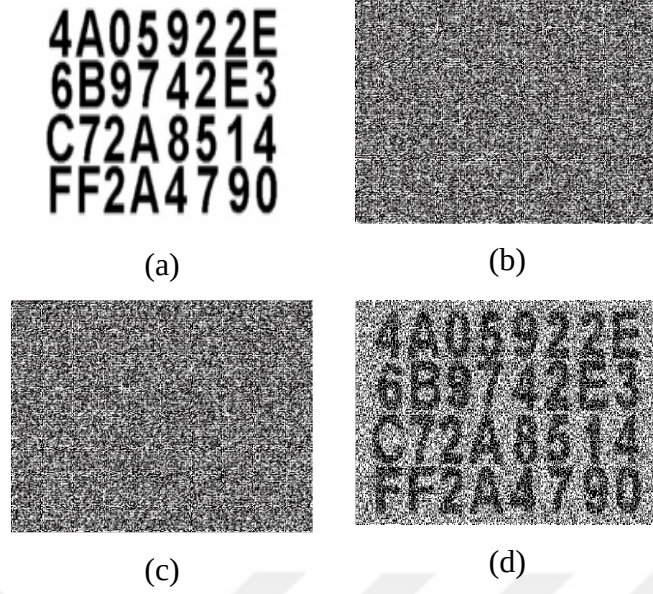
**Adım 3:** İkili imgenin piksel değeri 0 ise sıfırlar listesinden rastgele Braille kodları seç.

**Adım 4:** İkili imgenin piksel değeri 1 ise birler listesinden rastgele Braille kodları seç.

**Adım 5:** Braille kodlarını sır parçası olan imgelere yerleştir.

**Adım 6:** İkili imgenin boyutu kadar adım 3-5'i tekrarla.

**Adım 7:** Elde edilen sır parçalarını örtü imgelerine veri gizleme fonksiyonunu kullanarak gizle.



**Şekil 7. 9.** (2,2) BGSP (a) Gizli veri (b) 1. Sır parçası (c) 2. Sır parçası (d) Yeniden elde edilmiş imge

Şekil 7.9’da (2,2) BGSP kullanılarak yapılan sır paylaşımı işlemi gösterilmiştir. İmgeyi yeniden elde etmek için, XOR operatörü kullanılmaktadır. Sır parçalarını gizlemek için kullanılan veri gizleme algoritması ise 2EÖB algoritmasıdır. Bu algoritma kullanılarak, sır parçaları örtü nesnesinin en anlamsız iki bitine gömülmüştür. Böylece sır parçalarını alıcı tarafa güvenilir bir veri hattı üzerinden iletilmektedir [124].

### 7.2.1.3. Deneysel Sonuçlar

Bu algoritma kurallar değiştirilerek kontrast ayarlanabilir veya bu çalışmada yapıldığı gibi 0 ve 1 gelme olasılıkları ayarlanabilir. Veri gizlemenin performansını analiz etmek için Şekil 7.8’de bulunana imgeler örtü imgesi olarak kullanılmıştır ve elde edilen PSNR değerleri Tablo 7.8’de verilmiştir.

**Tablo 7. 8.** Elde edilen PSNR deęerleri

| Örtü İmgesi | PSNR (dB) |       |
|-------------|-----------|-------|
|             | Sır 1     | Sır 2 |
| Baboon      | 44.65     | 44.93 |
| Boat        | 44.99     | 44.37 |
| Elaine      | 45.52     | 45.11 |
| House       | 45.36     | 45.54 |
| Lena        | 44.01     | 44.75 |
| Peppers     | 44.88     | 44.16 |
| Airplane    | 43.97     | 44.61 |
| Tiffany     | 45.32     | 45.88 |
| Barbara     | 45.36     | 44.93 |

#### 7.2.1.4. Sonuç

Bu yöntemde Braille alfabesinde bulunan harfler kullanılarak, yeni bir anlamlı sır paylaşımı yöntemi önerilmiştir. Önerilen yöntem kullanılarak veri gizleme uygulaması gerçekleştirilmiştir. Önerilen BGSP algoritması olasılıksal yöntem ve XOR operatörünü kullanmıştır. Bu yöntemde XOR kullanılarak olasılıklar 0.5'e yaklaştırılmıştır. Rastgele sayı üretici kullanılarak, Braille kodların sır parçası üzerinde uniform dağılımı sağlanmıştır. Kamuflej aşamasında ise veri gizleme algoritmalarından faydalanılmış ve başarılı sonuçlar elde edilmiştir. Gelecekteki çalışmalarda, görsel anlamlı şifreli görüntüler oluşturmak için bu yöntem kullanılacaktır [124].

#### 7.2.2. Göktürk Alfabesi Tabanlı Görsel Sır Paylaşımı Yöntemi ile Veri Gizleme Uygulaması

Günümüzde birçok sır paylaşımı ve (GSP) tabanlı veri gizleme yöntemi önerilmiştir. GSP karmaşık matematiksel işlemler kullanmadan bilgi güvenliğini sağlayan bir yöntemdir ancak GSP yöntemleri gürültü benzeri veriler ürettiği için, saldırganların dikkatini çekmektedir. Bu problemi çözebilmek için harf tabanlı GSP yöntemleri önerilmiştir. Harf tabanlı GSP yöntemleri, harflerin morfolojik özelliklerine bağımlı oldukları için istenilen performansı sağlayamamaktadır. Bu problemi çözmek için toplama tabanlı sır paylaşımı yöntemini

kullanan yeni bir harf tabanlı GSP yöntemi geliştirilmiştir. Önerilen harf tabanlı GSP yöntemi harflerin morfolojik özelliklerinden bağımsızdır ve tüm doğal diller için kullanılabilir. Bu makalede önerilen harf tabanlı GSP yöntemi, Göktürk alfabesinde bulunan harfler kullanılarak gerçekleştirilmiştir. Gizli veri önerilen Göktürk alfabesi tabanlı GSP yöntemi kullanılarak sır parçalarına ayrılmış ve RGB imgelerinin katmanlarına gömülmüştür. Deneysel sonuçlar, önerilen GSP tabanlı veri gizleme uygulamasının başarılı olduğunu göstermiştir [128].

#### **7.2.2.1. Motivasyon ve Tasarım**

Literatürde önerilen harf tabanlı görsel sır paylaşımı şemaları incelendiğinde, oluşturulan sır paylaşım şemalarının harflerin morfolojik özelliklerini kullandığı gözlemlenmiştir. Doğal dillerde kullanılan harflerin morfolojik özelliklerinin farklı olmasından dolayı harf tabanlı görsel sır paylaşım şemalarının tüm alfabelerde uygulanamadığı, uygulansa dahi belirli bir harf kümesinin kullanıldığı gözlemlenmiştir [48].

Bu yöntemde, tüm doğal dillerde bulunan harfleri kullanılabilecek yeni bir görsel sır paylaşımı önerilmiştir. Önerilen görsel sır paylaşımı yönteminin hesapsal karmaşıklığı diğer yöntemlere göre düşüktür. Ayrıca bu yöntemde veri gizleme kullanılarak elde edilen sır parçaları gizlenmiş ve sır parçalarının hilecilik saldırılarından korunması hedeflenmiştir.

#### **7.2.2.2. Önerilen Yöntem**

Bu çalışmada Göktürk alfabesine ait 38 adet harf anlamlı sır parçalarının oluşturulması hedeflenmektedir. Göktürkçe'nin harfleri Şekil 7.10'da verilmiştir [129].

|   |   |   |   |   |
|---|---|---|---|---|
| Ѕ | Ѣ | Ѧ | Ѧ | Ч |
| Љ | Д | Ѧ | Ѧ | ☺ |
| Ѧ | Ѧ | Ѧ | Ѧ | Ѧ |
| Ѧ | Ѧ | Ѧ | Ѧ | Ѧ |
| Ѧ | Ѧ | Ѧ | Ѧ | Ѧ |
| Ѧ | Ѧ | Ѧ | Ѧ | Ѧ |
| Ѧ | Ѧ | Ѧ | Ѧ | Ѧ |
| Ѧ | Ѧ | Ѧ | Ѧ | Ѧ |
| Ѧ | Ѧ | Ѧ | Ѧ | Ѧ |

Şekil 7. 10. Göktrük alfabesine ait harfler [129].

Önerilen yöntem kullanılarak gizli veri, anlamlı alt piksellerden oluşan sır parçalarına ayrılmaktadır. Bu yöntem kullanılarak hem anlamlı görsel sır parçaları elde edilmektedir hem de elde edilen sır parçaları kullanılarak RGB imgelerin kimlik doğrulaması yapılabilmektedir.

**Adım 1:** Harflere ID numarası atanır. Harflere ID numarası atamak için çevrimsel asal döngüsü kullanılır.

$$CG = a^i \bmod p, \quad p > 38, \quad i = \{1, 2, \dots, p\} \quad (7.5)$$

**Adım 2:** Gizli veri 3 x 2 boyutundaki bloklara ayrılır ve her blok için hedef değeri hesaplanır  $\lceil \log_2 38 \rceil = 6$ . Harf setinin büyüklüğüne bağımlı blokların oluşturulması sayesinde, önerilen GSP’de meydana gelecek piksel genişleme oranı azaltılmıştır. Örneğin Liu ve arkadaşları’nın önerdiği görsel sır paylaşımı yönteminde kullanılan alt piksellerin boyutu 9 x 9’dur [11]. Bu durumda piksel genişleme değeri 81 olarak elde edilmektedir. Ancak Denklem 7.6 kullanılarak elde edilecek piksel genişleme değeri  $\frac{9 \times 9}{6} = 13.5$  olarak elde edilmektedir.

$$T = WI_{i,j}2^5 + WI_{i,j+1}2^4 + \dots + WI_{i+2,j+1}2^0 \pmod{38} \quad (7.6)$$

**Adım 3:** Oluşturulan (n,n)’lik görsel sır paylaşımı şemasının n-1 adet parçası rastgele sayı üretici kullanılarak oluşturulmaktadır. Denklem 7.7 ve 7.8’de doğrusal eşiksel rastgele sayı üretici ve lojistik harita tabanlı rastgele sayı üreticinin denklemleri verilmiştir.

$$x_{i+1} = [(cx_i + d \bmod p) \bmod 38] \quad (7.7)$$

$$x_{i+1} = \text{round}(37rx_i(1 - x_i)), 3.5 \leq r \leq 4, x \neq 0.5, x \in [0,1] \quad (7.8)$$

$c$ , rastgele sayı üretici çarpanı  $d$ , artım miktarı  $r$ , kaos katsayısı ve  $x$  ise elde edilen rastgele sayı dizisidir.

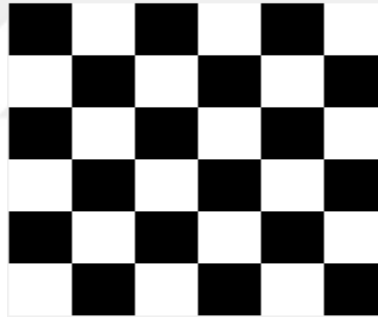
**Adım 4:**  $n$ . sır parçasının üretebilmek için aşağıdaki formül kullanılmaktadır.

$$\text{sum} = \sum_{i=1}^{n-1} id_i \quad (7.9)$$

$$id_n = T, \quad 1 \leq id_n \leq 38 \quad (7.10)$$

**Adım 5:** Oluşturulan sır parçaları örtü nesnesinin katmanlarına gizlenir.

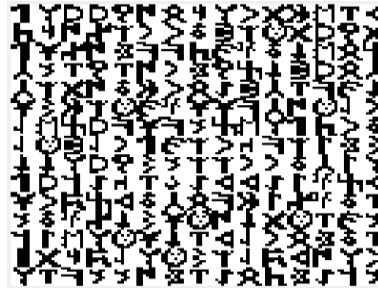
Aşağıdaki imgenin önerilen yöntem kullanılarak sır parçalarına ayrılması Şekil 7.11’de verilmiştir.



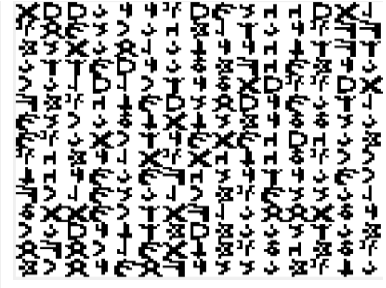
(a) Gizli veri



(b) Sır 1



(c) Sır 2



(d) Sır 3

Şekil 7. 11. (3,3) sır paylaşımı şeması

Şekil 7.11’de dama tahtası imgesi ve bu imgeye ait 3 adet sır parçası verilmektedir Dama tahtası imgesinin özelliği, her bir blokta bulunan piksel değerlerinin birbirine eşit olmasıdır.

Bu imgeye ait bloklar aynı özellikte olmasına rağmen üretilen sır parçaları Şekil 7.11’de görüldüğü gibi farklı özellikler göstermektedir [128].

Önerilen veri çıkarma ve yeniden yapılandırma algoritmasının adımları aşağıda verilmiştir.

**Adım 1:** Çevrimsel asal döngüsünün parametreleri kullanılarak harflere ait kimlik numaraları elde edilir.

**Adım 2:** Örtü imge R, G ve B katmanlarına ayrılır.

**Adım 3:** Veri çıkarma algoritması uygulanarak sır parçaları elde edilir.

**Adım 4:** Harfler elde edilir ve örüntü eşleştirme kullanılarak harflere ait id değerleri elde edilir.

**Adım 5:** Denklem 7.11, 7.12 ve 7.13 kullanılarak orjinal piksel değerleri hesaplanır.

$$T = \sum_{i=1}^n id_i(mod 38) \quad (7.11)$$

$$value = dec2bin(T, 6) \quad (7.12)$$

$$WI_{i,j} = value_1, WI_{i,j+1} = value_2, WI_{i+1,j} = value_3 \quad (7.13)$$

$$WI_{i+1,j+1} = value_4, WI_{i+2,j} = value_5, WI_{i+2,j+1} = value_6$$

$$i = \{1,3,5, \dots, m-1\}, j = \{1,3,5, \dots, n-1\}$$

*Value* elde edilen değerler dizisi olarak nitelendirilmektedir.

**Adım 6:** Hesaplanan değerler Şekil 7.12’de gösterildiği gibi yerleştirilerek gizli veri elde edilir [128 ].

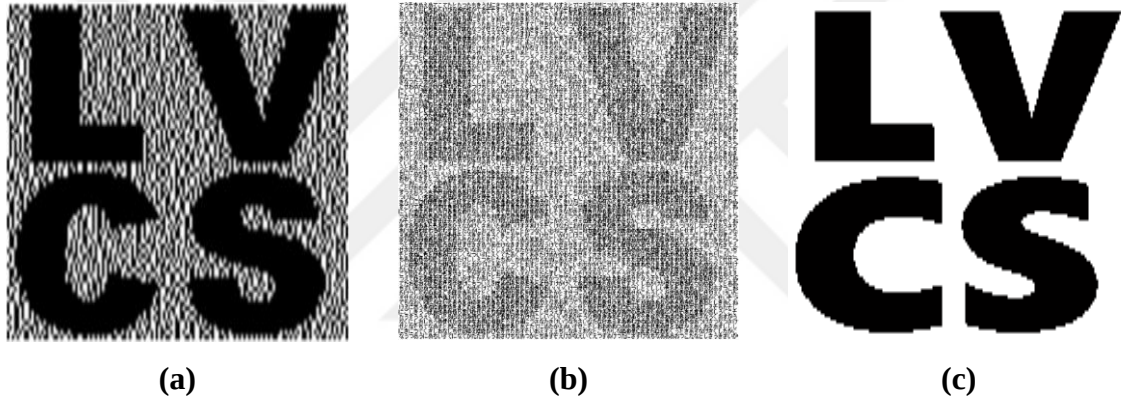
|           |           |
|-----------|-----------|
| $value_1$ | $value_2$ |
| $value_3$ | $value_4$ |
| $value_5$ | $value_6$ |

**Şekil 7. 12.** Elde edilen değerlerin yeniden yapılandırılmış imgeye yerleştirilmesi

### 7.2.2.3. Deneysel Sonuçlar

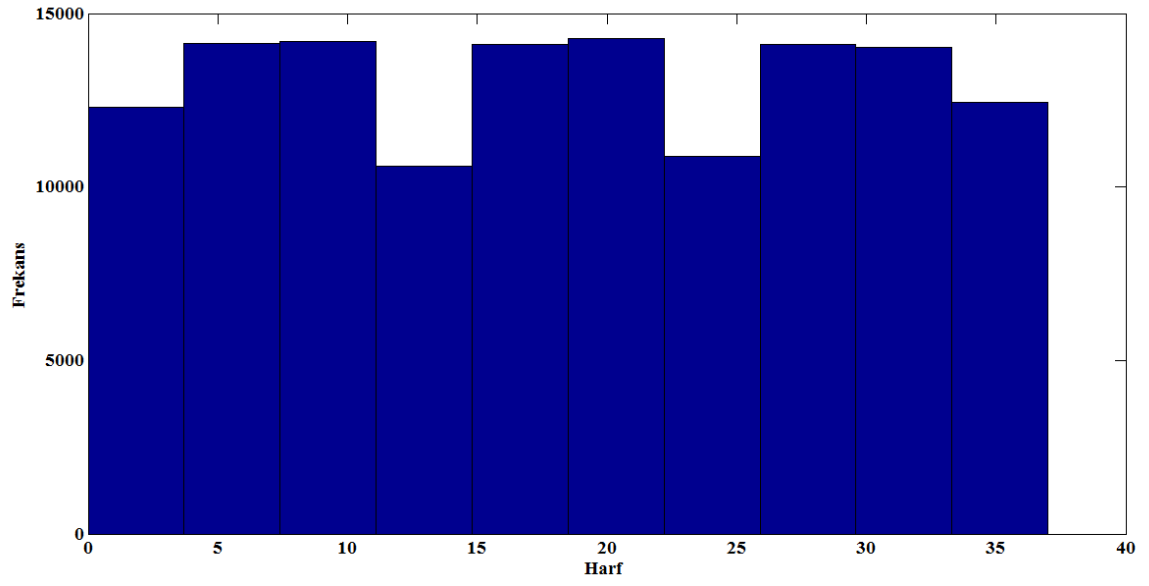
Önerilen algoritmada Şekil 7.6’da gösterilen imgeler kullanılmıştır ve gizli veri 3 adet sır parçasına ayrılmıştır. Veri gizleme fonksiyonu olarak 2EÖB kullanılmıştır ve elde edilen PSNR değeri ortalama 43.57 dB’dir.

Önerilen yöntemin yeniden yapılandırma aşaması Naor ve Shamir [71] ve Lin ve arkadaşlarının [48] yöntemleriyle karşılaştırılmıştır. Toplama tabanlı olan bu yöntemin yeniden yapılandırmasında, gürültüye rastlanmamıştır. Yeniden yapılandırma örnekleri Şekil 7.13’te verilmiştir.

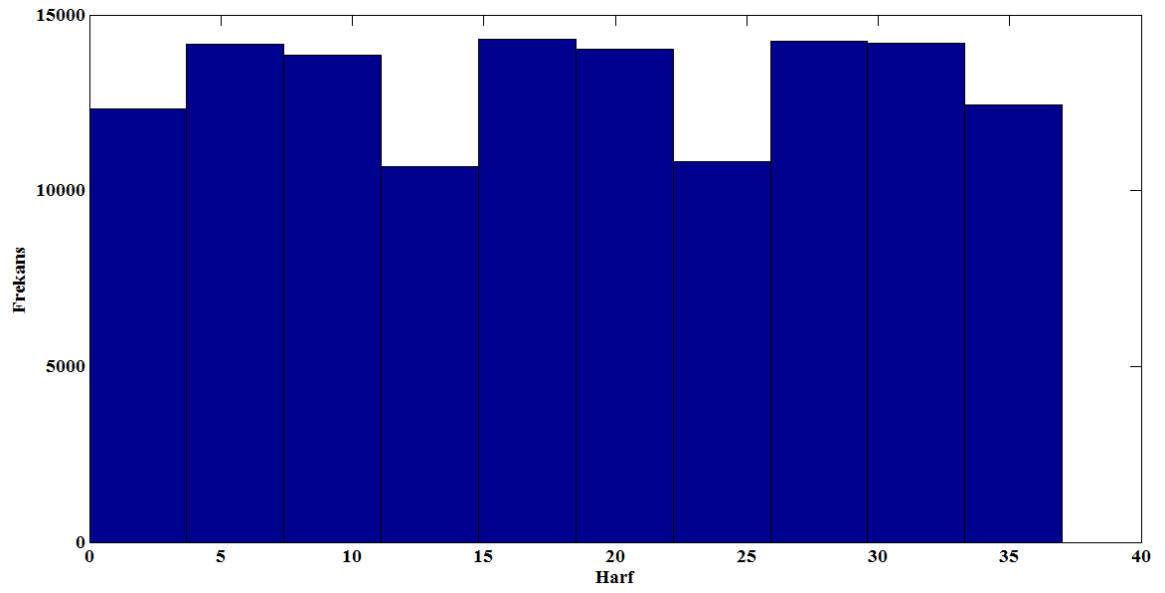


**Şekil 7. 13.** Yeniden yapılandırılmış imgeler (a) Naor ve Shamir’in yöntemi (b) Lin ve ark.’nın yöntemi (c) Önerilen yöntem

Önerilen harf tabanlı GSP yönteminde alfabede bulunan harflerin kullanılma olasılığının birbirine yakın olması gerekmektedir. Harflerin kullanılma olasılıklarının hesaplanması için frekans analizi yapılmıştır. Frekans analizini yapabilmek için “Fırat” imgesi (2,2) GSP yöntemi kullanılarak sır parçalarına ayrılmıştır. Sır parçalarına ayırma işleminde Matlab R2013a yazılımının rand fonksiyonu kullanılmıştır. Elde edilen sır parçalarının harf frekans analiz sonuçları Şekil 7.14’de verilmiştir.



(a)



(b)

Şekil 7. 14. Harflere ait frekans analizi (a) İlk sır parçası (b) İkinci sır parçası

Şekil 7.14’de gösterildiği gibi, alfabede bulunan tüm harfler kullanılmıştır ve harflerin kullanılma olasılıkları birbirine yakındır. Harflerin kullanılma olasılıkları, GSP şemasında kullanılan rastgele sayı üreticine bağlıdır.

#### 7.2.2.4. Sonuç

Bu yöntemde yeni bir harf tabanlı GSP yöntemi önerilmiştir ve önerilen yöntem veri gizleme ile birlikte kullanılarak çok katmanlı güvenlik uygulaması oluşturulmuştur. Literatürdeki harf tabanlı GSP yöntemlerinde bulunan problemleri çözmek için toplama tabanlı sır paylaşımı yöntemini kullanan yeni bir harf tabanlı GSP yöntemi geliştirilmiştir. Önerilen yöntemde lojik toplama operatörü olan OR'un yerine cebirsel toplama ve mod operatörü kullanılmıştır. Gizli veri gürültüsüz ve genişlemesiz olarak yeniden yapılandırılmıştır. Önerilen yöntemin hesapsal karmaşıklığı  $O(1)$ 'dir.

Bu yöntemde harf tabanlı GSP ile veri gizleme yöntemleri birlikte kullanılarak imgeler için kimlik doğrulama yapılabileceği gösterilmiştir. Deneysel çalışmaların ilk bölümünde veri gizleme sonuçları analiz edilmiştir. Elde edilen veri gizleme sonuçları literatürdeki diğer yöntemlerle karşılaştırılmış ve önerilen yöntemin sonuçları başarılı bulunmuştur. Ayrıca deneysel çalışmaların 2. bölümünde ise önerilen harf tabanlı GSP şeması incelenmiş ve istenilen başarımlar parametreleri elde edilmiştir. Gelecekteki çalışmalarda, anlamlı görsel şifreli görüntüler oluşturmak için bu yöntem kullanılacaktır. Ayrıca veri tabanında bulunan harf ve karakter sayısı genişletilip, yeni bir GSP tabanlı imge kimliklendirme algoritmasının önerilmesi planlanmaktadır [128].

#### 7.2.3. Renkli İmgelerde Kimlik Doğrulaması ve Saldırı Tespiti İçin GSP Tabanlı Kırılğan Damgalama Algoritması

Adli bilişim, bilişim sistemleri üzerinden genellikle veri olarak elde edilen delillerin toplanması, saklanması, derlenmesi ve analizi konusunda standartları oluşturulan çok disiplinli bir yapıdır. Adli bilişim sanılanın aksine özel bir alan değil, geniş alan disiplindir. Bu yöntemde adli bilişim uygulamalarında sıklıkla kullanılan özet fonksiyonlarının yerine kırılğan damgaların kullanılması önerilmiştir. Özet fonksiyonları saldırının yapıldığı bölgeyi tespit edemez. Multimedya verilerde saldırının yapıldığı bölgeyi tespit edebilmek için kırılğan damgalama yöntemlerinin kullanılması önerilmiştir. Bir damgayı kırılğan hale getirebilmenin en iyi yolu sır paylaşım tabanlı algoritmaları kullanmaktır. Bu yöntemde Wu ve Chen'in çoklu GSP algoritması kullanılarak, RGB imgeler için kimlik doğrulama ve saldırı tespiti yapılmıştır. Önerilen kırılğan damgalama algoritması yüksek görsel kaliteye sahip, kırılğan, güvenilir ve yüksek veri gizleme kapasitesine sahip bir algoritmadır. Wu ve

Chen görsel sır paylaşımı algoritması kullanılarak kimliklendirme yeteneği yüksek, yeni bir kırılğan damgalama algoritması önermiştir.

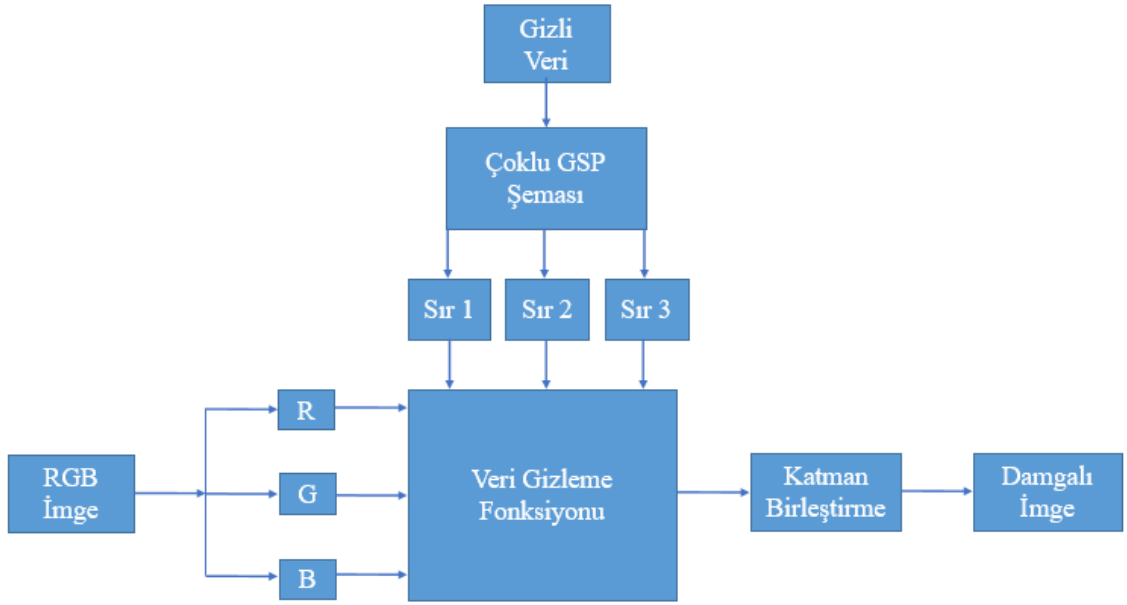
### 7.2.3.1. Önerilen Yöntem

Önerilen veri gizleme uygulamasında çoklu GSP şemaları kullanılarak kırılğan damgalama algoritmalarının elde edilmesi amaçlanmıştır. Veri gizleme fonksiyonu olarak 2EÖBs ve GSP şeması olarak da Wu ve Chang'in yöntemi kullanılmıştır. Şekil 7.15'de kodlama tablosu verilen GSP şeması Wu ve Chang tarafından 2005 yılında önerilmiştir. Önerilen algoritmada 3 adet sır parçası ve 2 bitlik veri gizleme fonksiyonu kullanılacağı için Wu ve Chang'in modelinin kullanılması öngörülmüştür [130]. Wu ve Chang'in GSP şemasına ait kodlama tablosu Şekil 7.15'de verilmiştir.

| P <sub>1</sub> | P <sub>2</sub> | Olasılık | S <sub>1</sub> | S <sub>1</sub> <sup>a</sup> | S <sub>2</sub> | S <sub>1</sub>   S <sub>2</sub> | S <sub>1</sub> <sup>a</sup>   S <sub>2</sub> |
|----------------|----------------|----------|----------------|-----------------------------|----------------|---------------------------------|----------------------------------------------|
| □              | □              | 1/4      |                |                             |                |                                 |                                              |
|                |                | 1/4      |                |                             |                |                                 |                                              |
|                |                | 1/4      |                |                             |                |                                 |                                              |
|                |                | 1/4      |                |                             |                |                                 |                                              |
| □              | ■              | 1/4      |                |                             |                |                                 |                                              |
|                |                | 1/4      |                |                             |                |                                 |                                              |
|                |                | 1/4      |                |                             |                |                                 |                                              |
|                |                | 1/4      |                |                             |                |                                 |                                              |
| ■              | □              | 1/4      |                |                             |                |                                 |                                              |
|                |                | 1/4      |                |                             |                |                                 |                                              |
|                |                | 1/4      |                |                             |                |                                 |                                              |
|                |                | 1/4      |                |                             |                |                                 |                                              |
| ■              | ■              | 1/4      |                |                             |                |                                 |                                              |
|                |                | 1/4      |                |                             |                |                                 |                                              |
|                |                | 1/4      |                |                             |                |                                 |                                              |
|                |                | 1/4      |                |                             |                |                                 |                                              |

Şekil 7. 15. Wu ve Chang'in çoklu GSP şemasına ait kodlama tablosu [130].

Bu yöntemin temel amacı, adli bilişimde sıklıkla kullanılan özet fonksiyonlarının yetersiz kaldığı yerlerde kırılğan damgaları kullanmaktır. Önerilen yöntem ile öncelikle damga GSP şeması kullanılarak parçalarına ayrılacak ve ardından damga 2EÖBs veri gizleme fonksiyonu kullanılarak veri gizlenecektir. Önerilen veri gizleme algoritmasında görsel sır paylaşımı algoritması olarak Wu ve Chen'in görsel sır paylaşımı algoritmasının kullanılması önerilmiştir. Şekil 7.18'de verilen tablo kullanılarak damga gürültüsüz olarak elde edilmektedir. Önerilen veri gizleme algoritmasının blok diyagramı Şekil 7.16'da verilmiştir.



Şekil 7. 16. Önerilen veri gizleme algoritmasının blok diyagramı

Önerilen veri gizleme algoritmasının adımları da aşağıdaki gibidir.

**Adım 1:** Renkli RGB imge sırasıyla R, G ve B kanallarına ayrılır.

**Adım 2:** Wu-Chang GSP algoritması kullanılarak damga 3 sır parçasına ayrılmıştır.

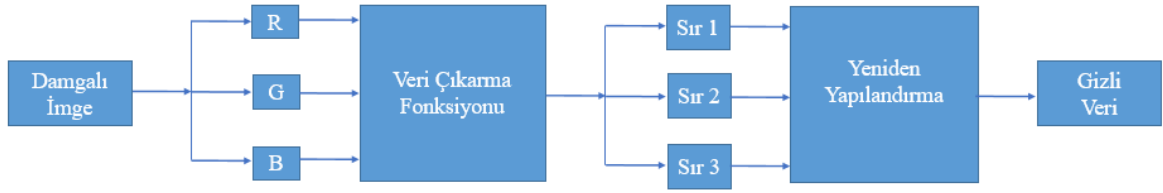
**Adım 3:** Sır parçası olacak elemanları seçebilmek için ise sözde rastgele sayı üreticileri kullanılmıştır. Bu yöntemde lineer eşiksel sayı üretici kullanılmıştır.

$$X_{i+1} = (aX_i + c) \bmod m \quad (7.14)$$

$X$  rastgele sayı dizisi,  $a$  çarpan,  $c$  artım ve  $m$  modül katsayılarıdır. Bu formül kullanılarak istenilen uzunlukta 0 ile  $m-1$  arasında rastgele sayı üretilebilmektedir.

**Adım 4:** Elde edilen 3 sır parçası 2EÖB veri gizleme algoritması kullanılarak örtü imgesine gömülür.

Yukarıdaki adımlar gerçekleştirildikten sonra damgalanmış imge elde edilir. Damgalanmış imgeden, damgayı elde etmek için ise kullanılacak adımların blok diyagramı Şekil 7.17’de verilmiştir.



**Şekil 7.17.** Önerilen veri çıkarma algoritmasının blok diyagramı

Önerilen algoritma kullanılarak damgayı yeniden elde etmek için aşağıdaki adımlar kullanılır.

**Adım 1:** Damgalanmış imge katmanlarına ayrılır.

**Adım 2:** Veri çıkarma fonksiyonu kullanılarak S1, S2 ve S3 kümeleri oluşturulur. Bu çalışmada 2EÖBs veri gizleme algoritması kullanıldığı için aşağıdaki formüller kullanılarak veri çıkarma işlemi gerçekleştirilir.

$$S_{1i,j} = R_{i,j}(\text{mod } 4), i = \{1,2, \dots, m\}, j = \{1,2, \dots, n\} \quad (7.15)$$

$$S_{2i,j} = G_{i,j}(\text{mod } 4), i = \{1,2, \dots, m\}, j = \{1,2, \dots, n\} \quad (7.16)$$

$$S_{3i,j} = B_{i,j}(\text{mod } 4), i = \{1,2, \dots, m\}, j = \{1,2, \dots, n\} \quad (7.17)$$

**Adım 3:** Şekil 7.17’deki kurallar kullanılarak sır parçalarından damga elde edilir.

### 7.2.3.2. Deneysel Sonuçlar

Bu çalışmada kullanılan yöntemi değerlendirebilmek için 6 adet veri gizleme başarımlı kriteri kullanılmıştır. Bahsedilen değerlendirme kriterleri aşağıdaki gibi verilmiştir.

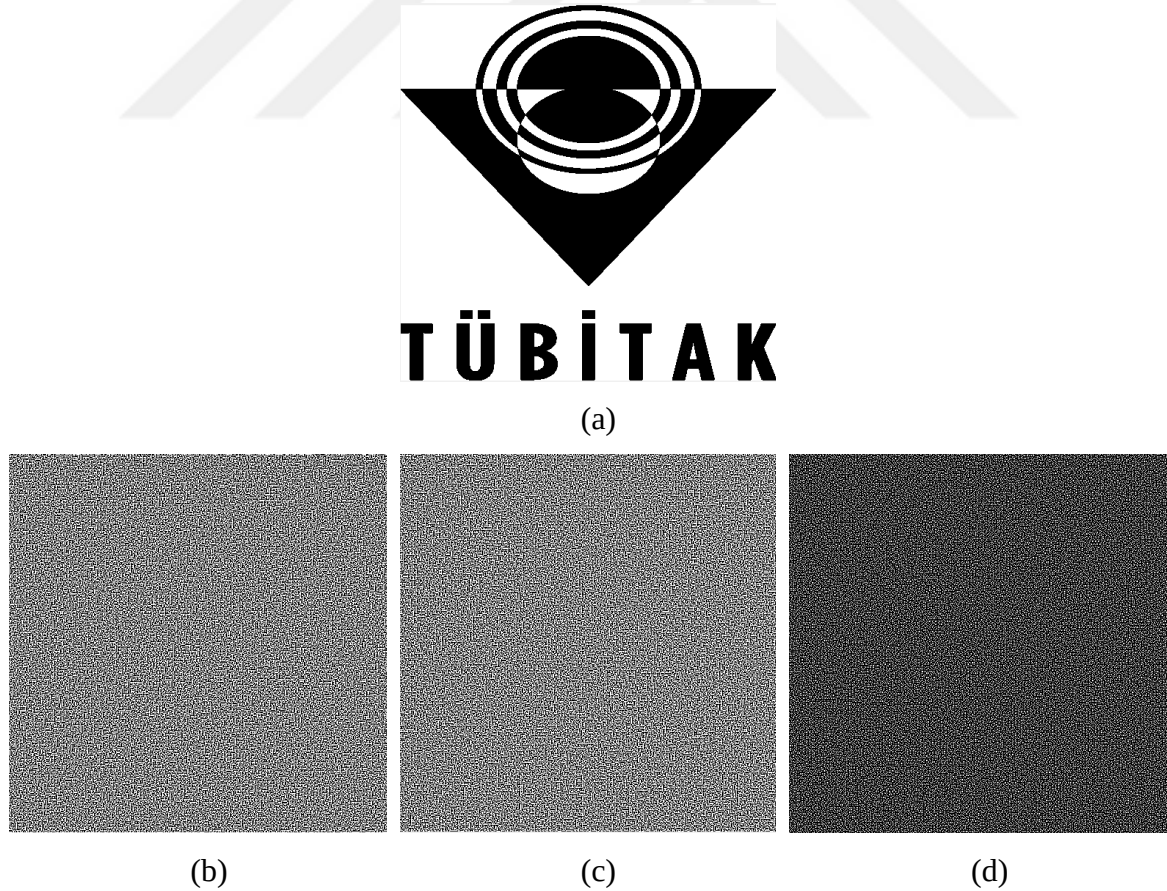
**Optimum Veri Gizleme Fonksiyonu:** Bu yöntemde veri gizleme fonksiyonu olarak 2EÖB kullanılmıştır. EÖB veri gizleme algoritmalarında en sık kullanılan ve en çok bilinen

veri gizleme fonksiyonlarıdır. Bu fonksiyonların uygulaması kolaydır ve bu fonksiyonlar kullanılarak veri gizleme işlemi hızlı bir şekilde yapılmaktadır. Şekil 7.17’de verilen tablo kullanılarak damga sır parçalarına ayrılır ve 2EÖB fonksiyonu kullanılarak renkli imgeye gömülür.

**Optimum Veri Çıkarma Fonksiyonu:** Önerilen yöntemler veri çıkarabilmek için (mod 4) işlemi kullanılarak sır parçaları elde edilmektedir. Sır parçaları elde edildikten sonra mantıksal VEYA işlemi Şekil 7.17’de verilen Wu ve Chang’in kodlama tablosu kullanılarak damga elde edilir.

**Kapasite:** Önerilen algoritma kullanılarak renkli imgenin her bir katmanına 2bpp (bit per pixel – piksel başına bit) kapasitede veri gizlenmektedir.

**Gizlilik:** Wu ve Chen’in görsel sır paylaşımı yöntemi kullanılarak damganın gizliliği sağlanmaktadır. Aynı zamanda sır parçalarının rastgele seçimi sayesinde güvenilir bir dağılım sağlanacaktır. Rastgele sayı üreticinin sağladığı en büyük avantajlardan biriside yayılma özelliğini sağlamasıdır. Şekil 7.18’de, ikili bir imge ve imgeye önerilen görsel sır paylaşım şemasının uygulanmasının ardından elde edilen sır parçaları verilmiştir.



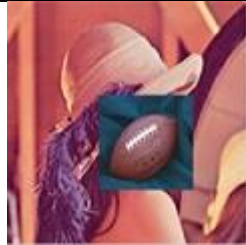
**Şekil 7. 18.** Wu ve Chang’ın görsel sır paylaşımı yönteminin uygulanması (a) Orijinal imge (b) ilk sır parçası (c) ikinci sır parçası (d) üçüncü sır parçası

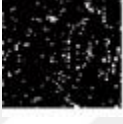
Elde edilen 3 adet sır parçası sırasıyla R, G ve B katmanlarına gömülmektedir. Veri çıkarma fonksiyonu bilinse de damgaya doğrudan ulaşamayacaktır. Wu ve Chen'in görsel sır paylaşımı yöntemi kullanılarak damganın gizliliği sağlanmaktadır.

**Ataklara Karşı Dayanıklılık:** Bu yöntemde, kırılğan ve atağın hangi bölgeye yapıldığını tespit edebilen yeni bir algoritma önerilmiştir. Test imgeleri olarak Şekil 7.18'de gösterilen renkli imgeler kullanılmıştır. Bu imgelerin 100 x 100'lük kısmına aşağıdaki ataklar uygulanmıştır [28-30]. Saldırıları tespit edebilmek için tüm elemanları 1 olan beyaz damganın gömülmesi öngörülmüştür.

- Kesme saldırısı
- Kolaj saldırısı
- Döndürme saldırısı
- JPEG sıkıştırma saldırısı
- Medyan filtre saldırısı
- Boyutlandırma saldırısı

**Tablo 7. 9.** Saldırı tespiti ve MD5 özet fonksiyonları

| Saldırı              | Saldırı Yapılan İmge                                                                | Elde Edilen Damga                                                                   | Özet Fonksiyonları (MD5)                                                                                                                   |
|----------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Kesme Saldırısı      |  |  | <p>Orijinal imge:<br/>CB18648237B3DA26440D7F233AC503FE</p> <p>Kesme saldırısı uygulanmış imge:<br/>7623195870C23B9E6AC11A0E947666B7</p>    |
| Kolaj Saldırısı      |  |  | <p>Orijinal imge:<br/>CB18648237B3DA26440D7F233AC503FE</p> <p>Kolaj saldırısı uygulanmış imge:<br/>45385D2B552542C7A72DB42B0AD5D61D</p>    |
| Döndürme (90 derece) |  |  | <p>Orijinal imge:<br/>CB18648237B3DA26440D7F233AC503FE</p> <p>Döndürme saldırısı uygulanmış imge:<br/>31E01399DCB3C56904815AB7F377E663</p> |

|                                                      |                                                                                     |                                                                                     |                                                                                                                                      |
|------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| <b>Gaussian<br/>Gürültü<br/>(M=0.01,<br/>V=0.01)</b> |    |    | Orijinal imge:<br>CB18648237B3DA26440D7F233AC503FE<br>Gürültü saldırısı uygulanmış imge:<br>FC6FD9D3D494D0873907A9CA0D747A34         |
| <b>JPEG<br/>Sıkıştırma<br/>(%90)</b>                 |    |    | Orijinal imge:<br>CB18648237B3DA26440D7F233AC503FE<br>JPEG sıkıştırma saldırısı uygulanmış imge:<br>0075BE44A271BE390B844504AB74BEB8 |
| <b>Medyan<br/>Filtre Saldırısı<br/>(3 x 3)</b>       |   |    | Orijinal imge:<br>CB18648237B3DA26440D7F233AC503FE<br>Medyan filtre saldırısı uygulanmış imge:<br>91EB75A75852D15BAF97E8E476BA601C   |
| <b>Wiener Filtre<br/>Saldırısı<br/>(3 x 3)</b>       |  |  | Orijinal imge:<br>CB18648237B3DA26440D7F233AC503FE<br>Wiener Filtre uygulanmış imge:<br>D8375C73852E20756471A5EEAB624C79             |
| <b>Boyutlandırma<br/>Saldırısı<br/>(150 x 150)</b>   |  |  | Orijinal imge:<br>CB18648237B3DA26440D7F233AC503FE<br>Boyutlandırma saldırısı uygulanmış imge:<br>40DDD296B5B7C7ACF8624F776AC8311E   |

Tablo 7.9’da gösterildiği gibi özet fonksiyonlar kullanılarak saldırı tespiti yapılamamaktadır. Saldırının, imgenin hangi bölgesine yapıldığını tespit edebilmek için önerilen yöntem kullanılmalıdır. Elde edilen sonuçlar, önerilen yöntemin yüksek kırılma dayanıklılığına sahip olduğunu göstermektedir.

**Yüksek Görsel Kalite:** Bir veri gizleme algoritmasının sağlaması gereken en önemli özelliklerden birisi de yüksek görsel kalitedir. Gizlenen verinin gözle fark edilememesi gerekmektedir.

Önerilen algoritmada elde edilen PSNR sonuçları 0.25 bpp için 53.18 dB civarında elde edilirken 2 bpp kapasitede 44.15 dB civarında elde edilmektedir. Elde edilen PSNR oranları yüksek olduğu için önerilen veri gizleme algoritması yüksek görsel kaliteye sahiptir.

### 7.2.3.3. Sonuç

Bu yöntemde, toplanan verileri doğrulama ve bu verilere yapılan saldırıları tespit edebilmek için rastgele sayı üreteçleri, özet fonksiyonları, görsel sır paylaşım algoritmaları ve veri gizleme algoritmaları kullanılmıştır. Elde edilen deneysel sonuçlar, bu algoritmanın adli bilişim uygulamalarında da kullanılabileceğini göstermiştir. Birbirinden ayrı 3 disiplin kullanılarak veri doğrulama yapılmıştır. Özet fonksiyonları değiştirilen verileri tespit edebilmektedir ancak verinin hangi bölgesinin saldırıya uğradığını tespit edememektedir. Bu sebepten dolayı görsel sır paylaşımı tabanlı yeni bir kırılğan damgalama önerilmiştir. Wu-Chang GSP modeli ve 2EÖBs veri gizleme fonksiyonu kullanılarak oluşturulan bu algoritma, veri gizleme ölçütlerinin tümünü sağladığı gibi, saldırı tespiti yapabilmede de yüksek performansa sahiptir. Özellikle açışal saldırılara karşı oldukça hassas bir damgalama yöntemi önerilmiştir. Bu işlem adli bilişimde sadece toplanan verilerin doğrulanması kısmında kullanılacaktır. Bu yöntemde, adli bilişimin geniş alan bilgisine sahip olduğunu göstermekle beraber, veri gizlemenin tüm başarımlı ölçütlerini sağlamış, kırılğan ve adli bilişimde uygulanabilir bir damgalama sistemi önerilmiştir.

### 7.3. Çok Seviyeli Veri Gizleme Uygulamaları

Bilindiği üzere, veri gizleme uygulamalarında kapasite ve görsel kalite arasında ters orantı vardır. Kapasitesi arttıkça görsel kalite düşmekte ve kapasite arttıkça görsel kalite azalmaktadır. Çok seviyeli veri gizleme uygulamalarında temel amaç, görsel kaliteyi düşürmeden veri gizleme kapasitesini arttırmaktır.

Bu tez çalışması süresince, görsel kaliteyi düşürmeden veri gizleme kapasitesini arttırmak için iki adet yöntem önerilmiştir ve bu yöntemler imge ve ses dosyalarına uygulanmıştır. Çok seviyeli veri gizleme uygulaması hem uzaysal alanda hem de frekans alanında gerçekleştirilmiştir.

### 7.3.1. Çok Katmanlı Görüntü Steganografi

Bir steganografik yöntemi değerlendirebilmek için örtü verideki değişim ve örtü verinin taşıma kapasitesi ele alınmalıdır. Steganografik yöntemlerde en temel amaç kapasiteyi arttırmak ve örtü verideki değişimi azaltmaktır. Ancak kapasiteyle örtü verisindeki değişim ters orantılı olduğu için bu iki amaç aynı anda gerçekleşemez. Örtü verideki değişimi sabit tutup kapasiteyi arttırmak için çok katmanlı steganografi kullanılmaktadır. Bu çalışmada çok katmanlı görüntü steganografi ele alınacak ve çok katmanlı olmayan yöntemlerle karşılaştırılacaktır.

#### 7.3.1.1. Önerilen Yöntem

Çok katmanlı steganografik yöntemler taşıyıcının kapasitesini ve güvenliğini arttırmak amacıyla ortaya atılmıştır [131]. Örneğin taşıma kapasitesi 10 Kb olan bir örtü verisinin kapasitesini 12 Kb'e çıkarmak amaçlanmıştır. Çok katmanlı steganografinin bir diğer avantajı ise kapasiteyi artırırken taşıyıcıdaki değişim yok denecek şekilde artmaktadır veya hiç artmamaktadır [131]. Çok katmanlı steganografinin matematiksel modeli aşağıdaki gibidir.

$$S = \log_{\frac{b}{e}}(W.H.k) \quad (7.18)$$

$$C = \sum_{n=1}^s \frac{W.H.k}{\frac{b}{e}^n} \quad (7.19)$$

$$C' = \frac{W.H.k}{\frac{b}{e}} \quad (7.20)$$

$$K = \frac{C - C'}{C'} 100 \quad (7.21)$$

$$R = \frac{C}{W.H.k} 100 \quad (7.22)$$

S seviye sayısı, b imgenin kaç bitle kodlandığının sayısıdır. Örneğin gri seviyeli imgeler genellikle 8 bitle kodlanır ve b=8 olmaktadır. W imgenin genişliği, H imgenin yüksekliği ve k imgenin katman sayısıdır, C'tek katmanlı veri gizlemenin maksimum kapasitesi, K kazanç, R ise kapasitenin imgeye olan oranını temsil etmektedir [94].

### 7.3.1.2. Deneysel Sonuçlar

Algoritmanın performansını test edebilmek için görsel kalite parametresi olan PSNR ve kapasite parametresi olan bpp ölçülmüştür. Elde edilen sonuçlar Tablo 7.10’da verilmiştir.

**Tablo 7. 10.** Çok katmanlı steganografi kullanılarak elde edilen kapasiteler

| Çok katmanlı görüntü steganografi kazanç tablosu $b=8$ , $e=1$ |         |           |           |             |
|----------------------------------------------------------------|---------|-----------|-----------|-------------|
| Boyut                                                          | 64 X 64 | 256 X 256 | 512 X 512 | 1536 X 1536 |
| Seviye                                                         | 4       | 5         | 6         | 7           |
| Kazanç (%)                                                     | 14.2578 | 14.2822   | 14.2853   | 14.2857     |

Yukarıdaki tabloda EÖB tekniği çok katmanlı görüntü steganografi açısından ele alınmıştır. Sadece 2 seviyeli EÖB uygulamasında bant genişliğinde kazanç % 12.5 olarak gerçekleşmiştir. Çok katmanlı steganografi yapısı karmaşık olmasına rağmen kapasiteyi ciddi şekilde artırdığı gözlemlenmiştir. Kapasite artarken, görsel kalite düşmemektedir. Tablo 7.11’de PSNR sonuçları verilmiştir.

**Tablo 7. 11.** Elde edilen PSNR değerleri

| Çok katmanlı görüntü steganografi kazanç tablosu $b=8$ , $e=1$ |             |                |                                    |
|----------------------------------------------------------------|-------------|----------------|------------------------------------|
| İmge                                                           | EÖB (1 bpp) | EÖB (1.14 bpp) | 4 katmanlı steganografi (1.14 bpp) |
| Lena                                                           | 51.1440     | 48.3568        | 51.1392                            |
| Baboon                                                         | 51.1449     | 48.8845        | 51.1444                            |
| Barbara                                                        | 51.1444     | 49.0012        | 51.1423                            |
| Goldhill                                                       | 51.1504     | 48.3374        | 51.1486                            |
| Peppers                                                        | 51.1539     | 48.3126        | 51.1343                            |

### 7.3.1.3. Sonuç

Bu çalışmada çok katmanlı steganografinin tek katmanlı steganografiye göre sağladığı avantajlardan bahsedilmiştir. Özellikle bant genişliğinin taşıyıcı kapasitesini artırması önemli bir özellik olarak görülmüştür. Örneğin tek katmanlı steganografik bir modelin karmaşıklığını  $O(n)$  olarak kabul edersek, aynı modelin 2 katmanlı uygulamasının karmaşıklığı  $O(n \log n)$  olarak karşımıza çıkacaktır. Ancak kapasite arttıkça örtü verisindeki bozulma artmaktadır. Çok katmanlı yöntemler kullanılarak örtü verisindeki değişim sabit tutularak kapasite artırılabilir. Bu yöntem özellikle soğan yönlendirme (onion routing) ve

çok seviyeli güvenlik uygulamalarında da kullanılabilir. Soğan yönlendirme de taşıyıcı (soğan) birden fazla mesaj taşımaktadır ve bu mesajlar çeşitli anahtarlarla şifrelenmiştir. İlgili anahtara sahip olan kullanıcı soğanı deşifre ederek ilgili mesajı elde edebilmektedir. Soğanın oluşturulabilmesi için çok katmanlı steganografi kullanılabilir. Örtü verinin altında gizlenecek alt örtü veriler sayesinde, birden fazla mesaj taşınabilir. Ayrıca çok seviyeli güvenlik uygulamalarında da bu yöntem kullanılabilir.

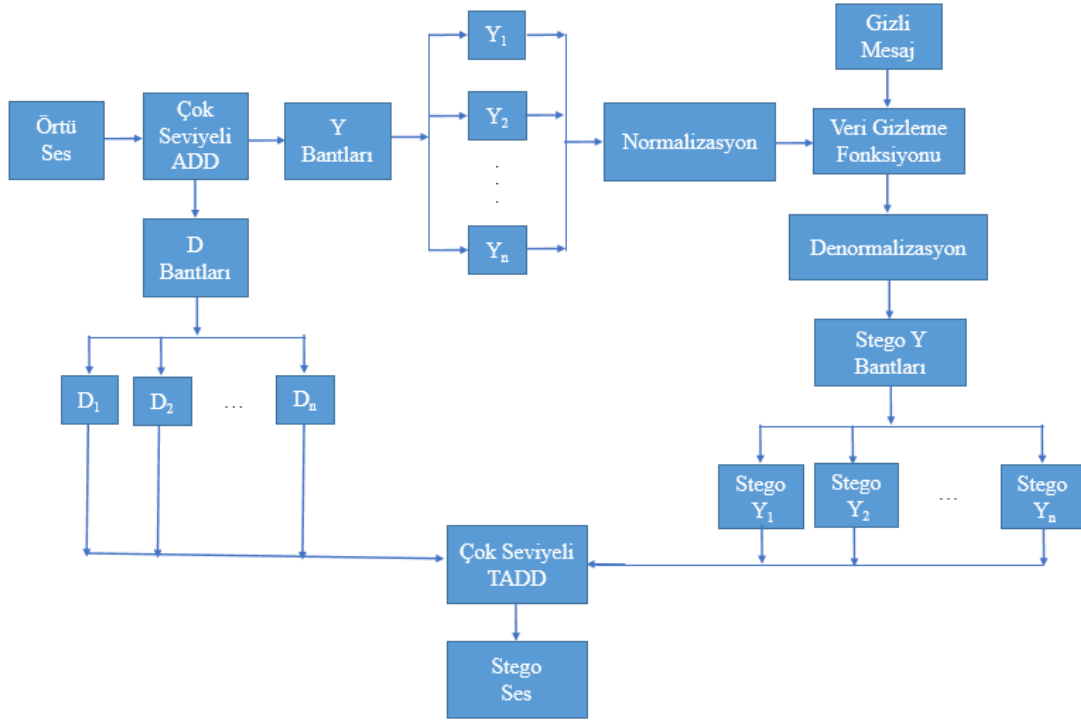
Modelin performansını arttırmak için paralel programlama yöntemlerine başvurulabilir. Örneğin threadler kullanılarak modelin performansı artırılabilir. Ayrıca gömülü sistemlerde uygulaması yapılarak analiz edilebilir.

### **7.3.2. Ses Sinyalleri İçin Çok Seviyeli ADD Tabanlı Veri Gizleme Algoritması**

Ses sinyallerine veri gizleme günümüzde yaygın olarak kullanılmaktadır. Ses kalitesi, dayanıklılık ve kapasite veri gizleme algoritmalarının başarımlarını ölçütlerindendir. Veri gizleme yöntemlerinin en popülerleri ise EÖB'dir. Bu çalışmada ses verilerine frekans alanında veri gizleme işlemi yapılmaktadır. Frekans dönüşümlerden en çok bilineni ve veri gizlemede en yaygın kullanılan dönüşüm ADD'dir. Bu çalışmada ses sinyallerine, çok seviyeli ADD uygulanarak yüksek geçirgen filtre katsayılarına EÖB kullanılarak veri gizleme işlemi gerçekleştirilmiştir. Ayrıca önerilen yöntemin başarımlarını ölçmek için istatistiksel analizler yapılmıştır.

#### **7.3.2.1. Önerilen Yöntem**

Bu çalışmada ses sinyallerine veri gizlemek için çok katmanlı bir veri gizleme yöntemi önerilmiştir. Önerilen yöntemin temel amacı gürültü oranı az, yüksek kapasiteli ve dayanıklı bir veri gizleme şeması oluşturmaktır. Bu şemayı oluşturabilmek için ADD'nin yüksek geçirgen filtre katsayıları kullanılmaktadır. Örtü verisi olan ses verisine çok seviyeli ADD uygulandıktan sonra her bir H bandı için normalizasyon işlemi yapılmalıdır. Normalizasyon işleminin temel amacı ise katsayıları daha az bitle kodlayıp algoritmanın hızını arttırmaktır. Normalizasyon işleminin ardından veri gizleme fonksiyonu kullanılarak, gizli veri ses verisine gömülmektedir. Çok seviyeli ADD'nin kullanılmasındaki temel amaç kapasite ve dayanıklılığın artırılmasıdır. Önerilen yöntemin veri gizleme blok diyagramı Şekil 7.19'da verilmiştir.



Şekil 7. 19. Önerilen veri gizleme algoritmasının blok diyagramı

Önerilen yöntemin veri gizleme adımları aşağıdaki gibidir.

**Adım 1:** İçerisine veri gizlenecek ses verisine çok seviyeli ADD uygulanarak yüksek geçirgen filtre katsayıları elde edilir.

$$[L, H] = ADD(CS) \quad (7.23)$$

$$[L_1, H_1] = ADD(L) \quad (7.24)$$

$$[L_2, H_2] = ADD(L_1) \quad (7.25)$$

$$[L_n, H_n] = ADD(L_{n-1}) \quad (7.26)$$

$L$  alçak geçirgen filtre katsayısı,  $H$  yüksek geçirgen filter katsayısı ve  $ADD$  ise ayrık dalgacık dönüşümünü ifade etmektedir.

**Adım 2:** Yüksek geçirgen filtre katsayılarının kaç bitle kodlanacağı belirlenir ve bu değer stego anahtarına kaydedilir.

**Adım 3:** Yüksek geçirgen filter katsayıları kodlanacak bit sayısına göre normalize edilir. Normalizasyon formülü Denklem 7.27’de verilmiştir.

$$H'_i = \frac{H_i - \min(H)}{\max(H) - \min(H)} (2^b - 1), \quad i = \{0,1,2 \dots, n\} \quad (7.27)$$

Yukarıdaki formülde  $H'_i$  normalize edilmiş yüksek geçirgen filter katsayıları,  $H_i$  yüksek geçirgen filtre katsayıları,  $\min(H)$  yüksek geçirgen filter katsayılarının en küçüğü,  $\max(H)$  yüksek geçirgen filter katsayılarının en büyüğü ve  $b$  ise katsayıların kaç bitte kodlanacağını ifade etmektedir.

**Adım 4:** Gizli veri ikili olarak kodlanır ve gizli veri normalize edilmiş H katsayılarına, EÖBs veya başka bir veri gizleme fonksiyonu kullanılarak gizlenir. Örneğin kEÖB bitlerini elde etmek için aşağıdaki formül kullanılmaktadır.

$$kEÖBs(H'_i) = H'_i \bmod 2^k, k \leq \frac{b}{2}, \quad i = \{0,1,2 \dots, n\} \quad (7.28)$$

**Adım 5:** Veri gizlenmiş ve normalize edilmiş H bantları katsayıları denormalize edilir. Denormalizasyon işleminin formülü aşağıdaki gibidir.

$$H_i = \frac{H'_i \cdot (\max(H) - \min(H))}{2^b - 1} + \min(H), \quad i = \{0,1,2 \dots, n\} \quad (7.29)$$

**Adım 6:** Veri gizlenmiş ve denormalize edilmiş H bantları L bantları inverse DWT edilerek stego ses elde edilir.

$$SS = TADD(H, L) \quad (7.30)$$

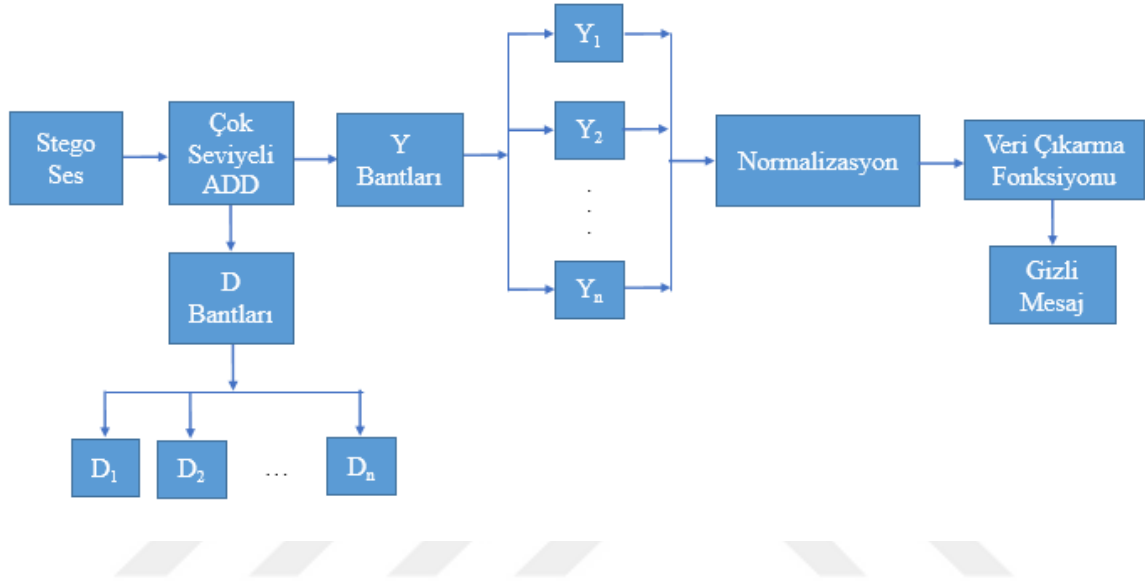
Her seviye ADD için aynı işlem tekrarlanır. Çok seviyeli ADD kullanmanın en büyük avantajı veri gizleme kapasitesini arttırmasıdır. Çok seviyeli ADD’nin kapasiteye etkisi aşağıdaki denklemler ile ifade edilmiştir.

$$l = \text{length}(CS) \quad (7.31)$$

$$s = \lfloor \log_2 l \rfloor \quad (7.32)$$

$$c = \sum_{i=1}^s l_i \frac{k}{2^i}, \quad i = \{1, 2, 3, \dots, s\} \quad (7.33)$$

Yukarıdaki formüllerde  $l$  örtü ses uzunluğu,  $s$  ADD için seviye sayısı ve  $c$  ise çok seviyeli ADD için maksimum kapasiteyi vermektedir. Veri çıkarma algoritmasının blok diyagramı ise Şekil 7.20’de verilmiştir.



Şekil 7. 20. Veri çıkarmanın blok diyagramı

Veri çıkarma adımları ise aşağıdaki gibidir.

**Adım 1:** Stego ses sinyaline çok seviyeli ADD uygulanır.

**Adım 2:** Elde edilen H katsayıları normalize edilir.

**Adım 3:** Stego anahtarı kullanılarak veri gizlenmiş indisler elde edilir.

**Adım 4:** H bantlarına veri çıkarma fonksiyonu uygulanarak gizli veri elde edilir.

### 7.3.2.2. Deneysel Sonuçlar

Algoritmanın performansını test edebilmek için NOIZEUS ses veritabanında bulunan 30 adet ses verisi kullanılmıştır. Veri gizleme işleminde sırasıyla 1, 2, 3 ve 4 seviyede ADD uygulanmıştır ve sese 4, 6, 7 ve 7.5 KB veri boyutunda veri gizlenmiştir. Elde edilen SNR değerler Tablo 7.12’de verilmiştir.

**Tablo 7. 12.** Önerilen yönteme ait SNR değerleri

| Ses<br>Verisi | SNR (dB) |         |         |         | Ses<br>Verisi | SNR (dB) |         |         |         |
|---------------|----------|---------|---------|---------|---------------|----------|---------|---------|---------|
|               | s=1      | s=2     | s=3     | s=4     |               | s=1      | s=2     | s=3     | s=4     |
| sp01          | 35.7923  | 31.4201 | 29.8022 | 28.5629 | sp16          | 29.2015  | 26.4634 | 25.7600 | 25.4996 |
| sp02          | 34.5353  | 31.5760 | 29.7797 | 28.9339 | sp17          | 32.0500  | 28.6129 | 27.7534 | 27.4294 |
| sp03          | 32.5873  | 27.7921 | 26.4667 | 25.9264 | sp18          | 34.6020  | 32.3684 | 31.2051 | 30.1594 |
| sp04          | 34.7568  | 31.1085 | 29.7940 | 29.2996 | sp19          | 31.6565  | 27.2621 | 25.8590 | 25.7706 |
| sp05          | 33.6823  | 29.5896 | 28.5500 | 28.1218 | sp20          | 31.6780  | 28.0886 | 27.0874 | 26.8710 |
| sp06          | 33.3834  | 28.4787 | 26.8064 | 26.4453 | sp21          | 35.2257  | 30.8622 | 28.7716 | 28.1218 |
| sp07          | 34.4272  | 29.7645 | 27.5139 | 26.9369 | sp22          | 36.4719  | 32.1969 | 30.9941 | 29.7094 |
| sp08          | 33.3309  | 29.3403 | 27.9036 | 26.9918 | sp23          | 35.7650  | 30.1840 | 28.7408 | 27.9168 |
| sp09          | 36.8823  | 31.4855 | 30.1129 | 29.2892 | sp24          | 38.8007  | 33.2238 | 31.5256 | 29.9268 |
| sp10          | 33.4459  | 29.0621 | 27.7270 | 27.3728 | sp25          | 37.5362  | 31.9931 | 28.9045 | 27.5473 |
| sp11          | 32.1079  | 27.8763 | 26.6446 | 26.3391 | sp26          | 31.3344  | 26.8194 | 25.8216 | 25.6758 |
| sp12          | 35.0596  | 31.4425 | 30.1642 | 29.2361 | sp27          | 32.3628  | 29.0879 | 28.3186 | 27.9373 |
| sp13          | 34.9731  | 29.9935 | 29.0152 | 28.6487 | sp28          | 33.0732  | 28.3776 | 26.7511 | 26.4327 |
| sp14          | 30.1665  | 25.9960 | 25.1295 | 25.0098 | sp29          | 30.8390  | 26.3363 | 25.3162 | 25.1294 |
| sp15          | 36.2698  | 31.2375 | 29.9614 | 29.4870 | sp30          | 32.9675  | 28.6470 | 27.1310 | 26.8253 |

Aynı zamanda önerilen algoritma Rekik ve ark.'nin [116] önerdiği yöntemle karşılaştırılmıştır. Elde edilen sonuçlar Tablo 7.13'de gösterilmiştir.

**Tablo 7. 13.** Önerilen yöntem ile ADD-AFD [116] yönteminin karşılaştırılması

| Rekik ve ark.'nin Yöntemi [116] |              |             | Önerilen Yöntem |              |             |
|---------------------------------|--------------|-------------|-----------------|--------------|-------------|
| Örtü Sinyal                     | Gizli Sinyal | SegSNR (dB) | Örtü Sinyal     | Gizli Sinyal | SegSNR (dB) |
| Kadın                           | Erkek        | 31.86       | Kadın           | Erkek        | 34.53       |
| Erkek                           | Kadın        | 32.70       | Erkek           | Kadın        | 35.79       |
| Kadın                           | Erkek        | 34.45       | Kadın           | Erkek        | 36.88       |
| Erkek                           | Kadın        | 31.13       | Erkek           | Kadın        | 35.05       |

### 7.3.2.3. Sonuç

Bu çalışmada, ses verileri için çok seviyeli ADD kullanılarak veri gizleme uygulaması gerçekleştirilmiştir. Her seviyeden elde edilen yüksek geçirgen filtre katsayılarına EÖB yöntemi kullanılarak veri gizlenmiş ve ses verisini 8 bitte ifade edebilmek için normalizasyon işlemi uygulanmıştır. Çok seviyeli ADD-EÖB'nin başarımı kapasite ve gürültü parametreleri kullanılarak değerlendirilmiştir. Tek seviyeli ADD- EÖB'nin ortalama SNR değeri 33.83 dB ve kapasitesi 4 kbps elde edilirken, 4 seviyeli ADD-EÖB yönteminde ortalama SNR değeri 27.5851 ve kapasitesi 7.5 kbps olarak elde edilmiştir. Bu çalışma, ses verisine daha yüksek kapasitede ve kabul edilebilir miktarda veri gizlemek için çok seviyeli ADD-EÖB yönteminin kullanılabileceği gösterilmiştir.

## 7.4. Blok Tabanlı Veri Gizleme Uygulamaları

Blok tabanlı veri gizleme uygulamalarının en çok bilineni PDF veri gizleme algoritmasıdır. Bu tür veri gizleme algoritmalarında multimedya verisi eşit boyutlu bloklara ayrılarak veri gizleme işlemi gerçekleştirilir. Bu tür veri gizleme algoritmaları EÖB ve EAB yöntemleri gibi çalışmamaktadır. Blok tabanlı veri gizleme algoritmaları genellikle örtü multimedya verisinin yapısına göre çalışmaktadır ve veri gizleme kapasitesi değişkendir.

Tez süresi boyunca blok tabanlı veri gizleme algoritmaları incelenmiş ve yeni yöntemler önerilmiştir.

### 7.4.1. Sayısal Görüntüler İçin Yön Vektörü Tabanlı Veri Gizleme Algoritması

Günümüzde, veri gizleme algoritmaları yaygın olarak kullanılmaktadır. Bu algoritmaların başarımları ölçütleri güvenilirlik, kapasite, taşıyıcıdaki değişim ve dayanıklılıktır. Yaygın olarak kullanılan veri gizleme algoritmalarının güvenilirlikleri

tartışma konusu haline gelmiştir. Bu çalışmada yön vektörü tabanlı yüksek veri gizleme kapasitesine sahip bir veri gizleme algoritması kullanılmıştır. Bu algoritma kullanılarak, imge 3 x 3 boyutundaki bloklara bölünür ve her bir bloğa 4 bit gömülmektedir. Taşıyıcıdaki değişimi azaltmak için kenar çıkarma algoritmalarından faydalanılmıştır. Kullanılan algoritma güvenilir, taşıyıcıdaki değişimi az ve yüksek kapasiteli bir veri gizleme algoritmasıdır [132].

#### 7.4.1.1. Kenar Çıkarma Algoritmaları

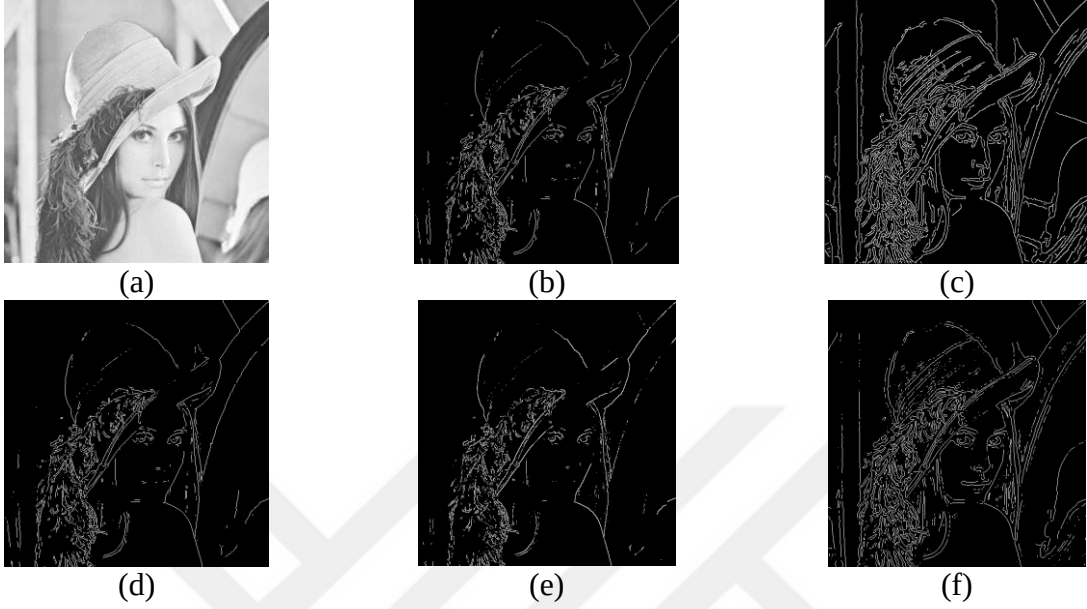
İmgedeki ani ve sürekli renk değiştiren bölgelere kenar adı verilmektedir. Görüntüye ilişkin kenarların belirlenmesi birçok durumda kullanışlıdır. Nesne tanıma problemi buna bir örnek olarak verilebilir. Nesne tanımda temel adım, bir görüntüyü farklı nesnelere karşı düşen farklı bölgelere bölütlemektir. Kenar belirleme işleminin kullanışlı olduğu diğer bir örnek, sadece görüntüye ilişkin kenarların kodlandığı düşük bit oranlarında görüntü kodlama uygulamasıdır [133].

Kenar belirlemenin önemli uygulamalarından biriside, görüntü içerisindeki belirli nesnelerin boyutunun doğru bir şekilde ölçülmesi işlemidir. Cisimlerin fiziksel özellikleri ile kenarları arasında doğrudan bir ilişki söz konusudur. Dolayısıyla görüntünün birçok fiziksel özelliği kenar bilgisinden ortaya çıkarılabilir. Dolayısıyla kenar belirleme konusu, görüntü analizinde ki önemli konulardan birisidir [134].

Kenar belirleme işlemi birçok yerde kullanıldığı gibi veri gizleme algoritmalarında da kullanılmaktadır. Yaygın olarak kullanılan kenar çıkarma algoritmaları aşağıdaki gibidir [135].

- Sobel
- Canny
- Roberts
- Prewitt
- Laplacian of Gauss (LOG)

Bu kenar çıkarma algoritmaları kullanılarak veri gizleme işlemi gerçekleştirilecektir. Şekil 7. 21’de kenar yukarıda belirtilen kenar çıkarma operatörlerinin lena görüntüsüne uygulanması gösterilmiştir.



**Şekil 7. 21.** (a) Orjinal görüntü (b) Sobel ile kenar tespiti yapılmış görüntü (c) Canny ile kenar tespiti yapılmış görüntü (d) Roberts ile kenar tespiti yapılmış görüntü (e) Prewitt ile kenar tespiti yapılmış görüntü (f) LOG ile kenar tespiti yapılmış görüntü

#### 7.4.1.2. Önerilen Yöntem

Önerilen yöntem veri gizleme fonksiyonunu güvenilir ve hızlı bir hale getirmeyi planlamaktadır. Bu algoritma matris tabanlı bir algoritma olup veri gizleme kapasitesini arttırmak için matris indislerinden faydalanmaktadır. Önerilen veri gizleme algoritması tersinir olup yüksek veri gizleme kapasitesine sahiptir. Bu çalışmada 3X3 boyutunda pencereler kullanılarak veri gizleme işlemi yapılmıştır ve her bir pencere 4 bit veri gizlenmiştir. Böylece veri gizleme kapasitesi 0.44 bpp (bit per pixel) olarak gerçekleşmiştir ancak görüntünün kenar verilerinde gürültüler oluştuğu için kenar verilerine veri gizleme işlemi yapılmamasına karar verilmiştir. Önerilen veri gizleme algoritmasının adımları aşağıdaki gibidir.

**Adım 1:** Örtü verisi olan imge alınarak 3 x 3 boyutundaki bloklara ayrılır.

**Adım 2:** Gizli veri 4 bit olarak kodlanır.

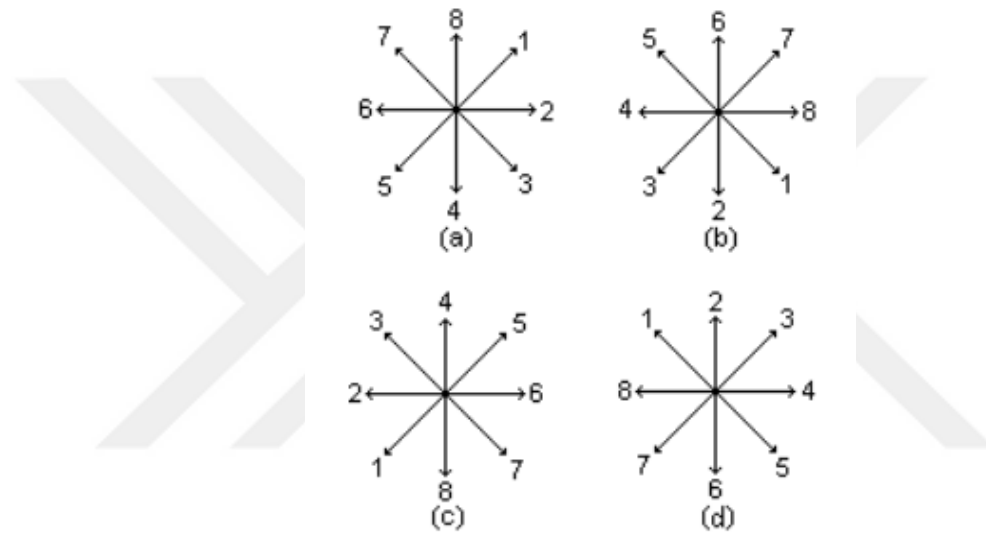
**Adım 3:** Bloкта bulunan piksellerden herhangi biri referans piksel olarak belirlenir. Gerçekleştirilen uygulamada referans pikseli bloğun merkez pikseli kabul edilmiştir.

**Adım 4:** Herhangi bir kenar çıkarma algoritması kullanılarak örtü nesnenin kenarları çıkarılır ve kaydedilir.

**Adım 5:** Eğer ilgili bloğun herhangi bir elemanı kenar verisine denk gelmişse sonraki bloğa geçilir o blokla ilgili herhangi bir işlem yapılmaz. Eğer ilgili bloğun herhangi bir elemanı kenar verisi değilse blok referans değerine göre düzenlenir.

**Adım 6:** Eğer bloktaki elemanların herhangi biri referans değere eşitse o elemana 1 eklenir, referans değerinden 1 küçükse o elemana 2 eklenir ve böylece veri gizleme işleminin tersinir olabilmesi sağlanır.

**Adım 7:** Kodlama işlemi Şekil 7. 22’de belirtilen sekizli zincir kod düzenine göre yapılır.



**Şekil 7. 22.** Yön vektörü örnekleri

**Adım 8:** Gizli verinin en anlamlı 3 biti verinin hangi yöne gömüleceği bilgisini ve gizli verinin en anlamsız biti o yönde bulunan piksele yapılacak işlemi belirtmektedir (GV=gizli veri). Kod tablolarının seçimi için PRNG (Pseudo Random Number Generator – Sözde Rastgele Sayı Üretici) kullanılmaktadır. Örneğin  $x_{i+1}=ax_i+b$  gibi bir denklem kullanılarak rastgele sayıları üretilebilir ve bu denklemde yer alan a,b,x<sub>i</sub> tohum değerleri kabul edilerek stego anahtarına yazılır. Örneğin (a) kod düzeni seçildi ve gizli veri 2, referans değer 2 ile gösterilen piksel değerine atanır. Gizli veri 10 olsaydı referans değer 1 eksiği 2 ile gösterilen piksel değerine atanmaktadır. Bu şekilde veri gizleme işlemi gerçekleştirilir. Referans değer ve diğer 8 yön değerinin diziliş sayısı 9!’dir.

**Adım 9:** Gizli verinin uzunluğu kadar 3-8. adımlar tekrarlanır.

Veri çıkarma algoritması ise aşağıda verildiği gibidir.

**Adım 1:** Stego imge 3 x 3 boyutundaki bloklara ayrılır.

**Adım 2:** Referans pikseli dışındaki piksellerde referans değeri veya referans değerinin 1 eksiği aranır.

**Adım 3:** İstenilen değerler bulunduğu anda, bulunduğu indis değerine göre kod tablosunda karşılığı kaydedilir ve veri elde edilir. Yukarıda belirtilen işlemler kenar verisi üzerinde bulunan bloklara uygulanmaz [132].

#### 7.4.1.3. Deneysel Sonuçlar

Önerilen algoritmanın performansını ölçmek için PSNR ve kapasite parametreleri kullanılmıştır. Elde edilen sonuçlar Tablo 7.14’de verilmiştir.

**Tablo 7. 14.** Tablonun test imgeleri üzerinde uygulanması ve elde edilen sonuçlar

| İmge    | Kenar Tespit Alg. | Kapasite (bit) | PSNR (dB) |
|---------|-------------------|----------------|-----------|
| Lena    | Sobel             | 101148         | 42.01     |
|         | Canny             | 81436          | 43.61     |
|         | Roberts           | 102836         | 41.36     |
|         | Prewit            | 101300         | 42.05     |
|         | LOG               | 90468          | 42.54     |
| Peppers | Sobel             | 105508         | 43.80     |
|         | Canny             | 78852          | 45.88     |
|         | Roberts           | 107404         | 43.21     |
|         | Prewit            | 105588         | 43.84     |
|         | LOG               | 86104          | 44.71     |
| Jet     | Sobel             | 100456         | 42.22     |
|         | Canny             | 85212          | 43.13     |
|         | Roberts           | 101440         | 41.28     |
|         | Prewit            | 100456         | 42.22     |
|         | LOG               | 90816          | 42.67     |
| Boat    | Sobel             | 98772          | 38.62     |
|         | Canny             | 71248          | 40.70     |
|         | Roberts           | 102532         | 37.65     |
|         | Prewit            | 98960          | 38.60     |
|         | LOG               | 79484          | 39.13     |

Ayrıca önerilen algoritma Intel Core i5 – 4300 işlemcili, 4 GB RAM ve Windows 8.1. işletim sistemine sahip bir dizüstü bilgisayarda gerçekleştirilmiştir. Uygulamanın kodları MATLAB R2013a programında yazılmıştır ve algoritmanın veri gömme işlemi için harcadığı ortalama süre 0.21 saniye olarak gerçekleşmiştir. Önerilen algoritma güvenilir bir algoritmadır. Yani kaba kuvvet saldırısı uygulanırsa  $9! \cdot 2^4$  kez sistemin denenmesi

gerekmektedir. Bir imgede 2000'den fazla bloğun olduğu düşünülürse, veri çıkarma işleminin tek başına hayli zaman alacağı öngörülmektedir  $(9! \cdot 16)^{2000}$ . Bu algoritma güvenilirlik, düşük gürültü oranı, yüksek kapasite parametrelerini sağlamıştır. Yarı kırılğan yapıyla dayanıklılık başarımlar ölçütünü de kısmen sağlamıştır [132].

#### **7.4.1.4. Sonuç**

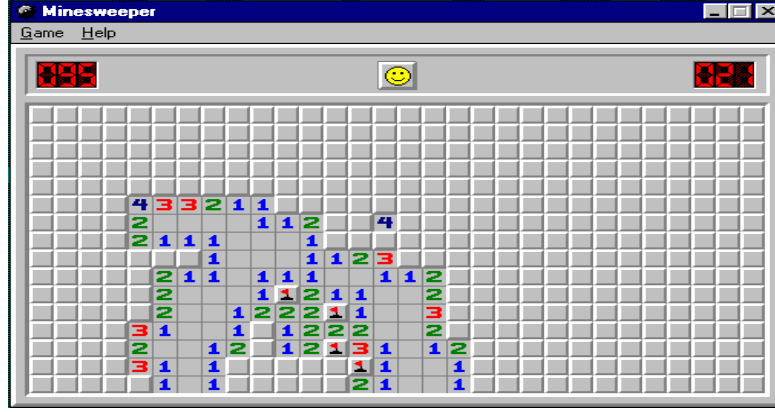
Algoritmanın hem hızlı çalışması hem güvenilir olması hem de PSNR değerlerinin yüksek çıkması, başarılı bir veri gizleme algoritması olduğunun göstergesidir. Bloktaki referans değere göre işlem yapıldığı için kontrast saldırılarına karşı dayanıklı olduğu ortaya çıkmaktadır. Parlaklık saldırılarına karşı yerel ikili örüntüler gibi davranabilmektedir [132].

#### **7.4.2. Mayın Tarlası Oyunu Tabanlı Veri Gizleme Algoritması**

Günümüzde ikili imgeler için birçok veri gizleme algoritması önerilmektedir. Önerilen algoritmaların temel amacı yüksek kapasitede ve yüksek görsel kalitede veri gizlemeyi sağlamaktır. Bu amacı gerçekleştirmek için genellikle örüntü tabanlı veri gizleme algoritmaları kullanılmaktadır. Bu çalışmada, ikili imgeler için mayın tarlası oyunu tabanlı yeni bir veri gizleme algoritması önerilmiştir. Mayın değeri 0 veya 1 seçilerek komşuluk dereceleri hesaplanmaktadır. Komşuluk derecelerini belirlemek için 3 x 3 boyutundaki örtüşmeyen bloklar kullanılmıştır. Elde edilen komşuluk derecelerini değiştirerek veri gizleme işlemi gerçekleştirilmektedir. Bozulmanın minimum seviyede olması için hamming uzaklığı hesaplanmıştır. Komşuluk dereceleri farklı, benzer blokların seçiminde ise rastgele sayı üreteçleri kullanılarak algoritmanın gizliliği sağlanmıştır. Deneysel sonuçlar, önerilen veri gizleme algoritmasının başarılı sonuçlar elde ettiğini göstermiştir.

##### **7.4.2.1. Mayın Tarlası Oyunu**

Mayın tarlası oyununun ilk örnekleri 1960 ve 1970'li yılların başlarında ortaya çıkmıştır. Mayın tarlası oyunu günümüzdeki haliyle 1983 yılında piyasaya sürülmüştür. Mayın tarlası tek kullanıcı bir video oyunudur. Oyunun amacı mayına rastlamadan tüm boş alanları bulmaktır [17]. Mayınsız alanlara tıklayınca karşımıza gelen sayılar ise, o alan etrafında bulunan mayın sayısını vermektedir. Şekil 7.23'de oyunun ekran görüntüsü verilmiştir.



Şekil 7. 23.Mayın tarlası oyunu ekran görüntüsü [136]

Günümüzde windows işletim sistemleriyle birlikte gelen oyun basit bir hafıza ve mantık testidir ve tüm zamanların en yaygın Windows oyunlarından biridir [137]. Oyunun amacı, mayınlardan kaçmak ve boş alanları bulmaktır.

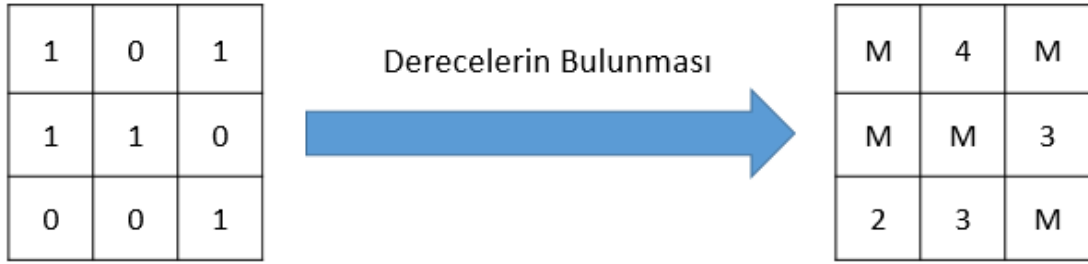
#### 7.4.2.2. Önerilen Yöntem

Önerilen veri gizleme algoritması gri görüntüler için geliştirilmiştir. Komşuluk analizi yapabilmek için 3 x 3 boyutunda komşuluk matrisi kullanılmıştır. Komşuluk matrisi Şekil 7.24’de verilmiştir.

|             |               |               |
|-------------|---------------|---------------|
| $P_{i,j}$   | $P_{i,j+1}$   | $P_{i,j+2}$   |
| $P_{i+1,j}$ | $P_{i+1,j+1}$ | $P_{i+1,j+2}$ |
| $P_{i+2,j}$ | $P_{i+2,j+1}$ | $P_{i+2,j+2}$ |

Şekil 7. 24. 3 x 3 komşuluk matrisi

Önerilen metot ile mayınların belirlenmesi gerekmektedir. 0 veya 1 değerindeki pikseller mayın olarak seçilmektedir. Eğer 1 değeri mayın olarak seçilirse, 0 değerinde bulunan piksellerin dereceleri hesaplanmaktadır. Tüm değerleri 0 veya 1 olan 3 x 3 boyutundaki örtüşmeyen alt bloklar veri gizleme işlemi için kullanılmamaktadır. Şekil 7.25’de mayın komşuluk derecelerinin bulunması ile ilgili örnek verilmiştir.



Şekil 7. 25. Mayın=1 için komşuluk derecelerin bulunması

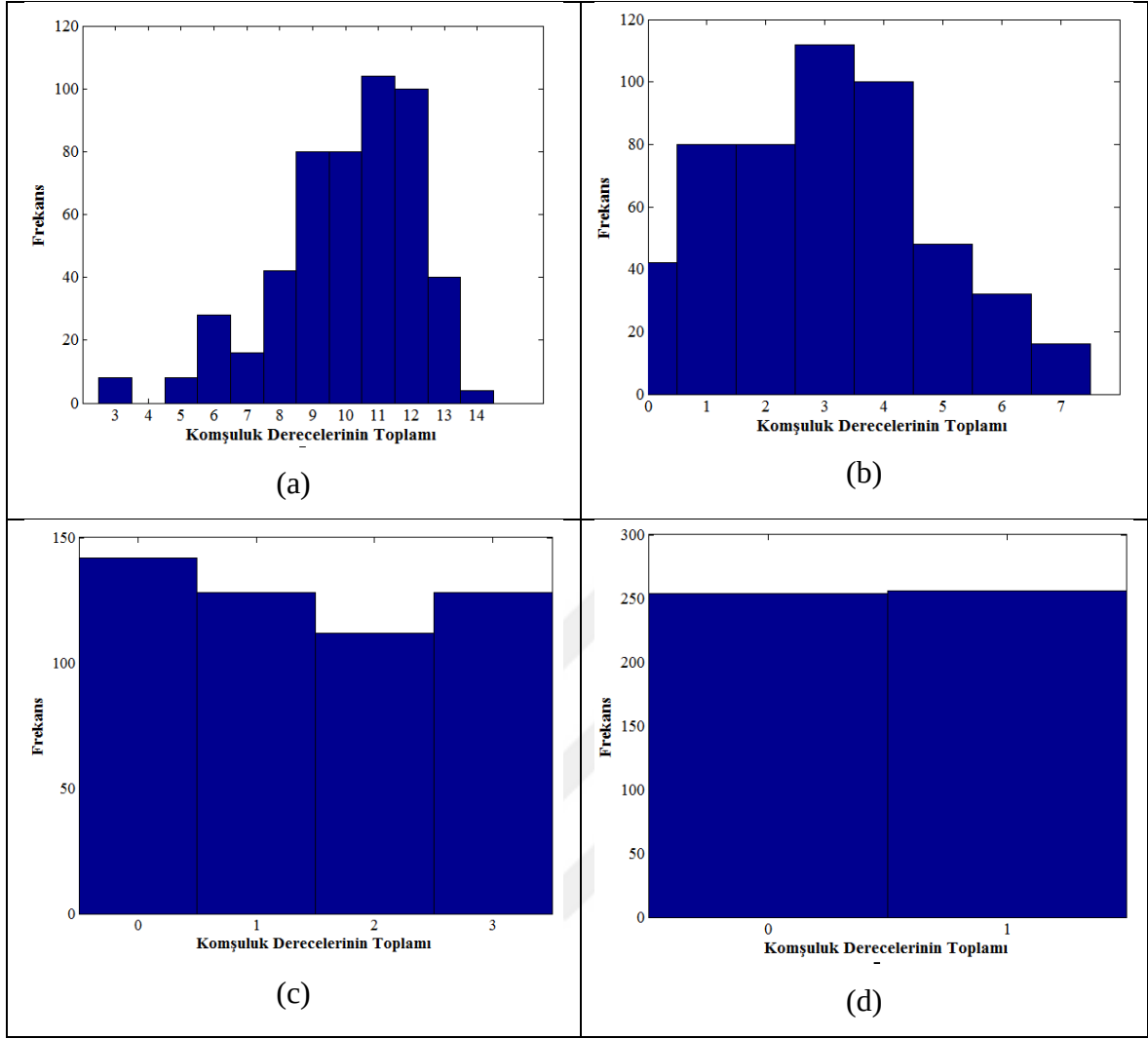
Yukarıdaki örnekte 1 pikseli mayın olarak seçilmiştir ve 0 olan piksellerin dereceleri bulunmuştur. Elde edilen dereceler toplanarak matrisin değeri elde edilmektedir. Şekil 7.25’deki matrisin değeri  $4+3+3+2=12$ ’dir. Matrisin mayın komşuluk değerini hesaplamak için Denklem 7.34 kullanılmaktadır.

$$V = \sum_{i=1}^n der_i \quad (7.34)$$

V matrisin komşuluk derecelerinin toplamı, *der* ise matristeki mayın olmayan elemanların derecesidir. 3 x 3 boyutunda matrisin alabileceği tüm değerler hesaplanmıştır ve en yüksek değer 14 olarak elde edilmiştir. Hesaplanan değerler ise [1,510]’dur. Önerilen algoritma tüm elemanları 0 veya 1 olan alt bloklara veri gizleyememektedir. Bu sebepten dolayı onluk değeri 1 ile 510 arasında olan matrislere veri gizlenmektedir. 3 x 3 boyutundaki alt bloğun onluk değerinin hesaplanması için Denklem 7.35 kullanılmaktadır.

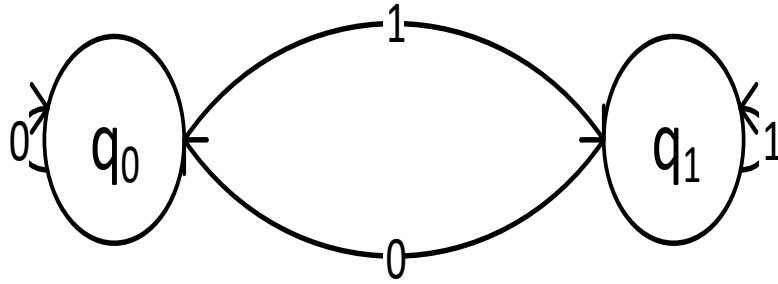
$$deger = p_{i-1,j-1} \times 2^8 + p_{i-1,j} \times 2^7 + \dots + p_{i+1,j+1} \times 2^0 \quad (7.35)$$

Ancak bu değerlerin dağılımı eş değildir. Bu sebepten dolayı, mod fonksiyonu kullanılmıştır. Değerlerin dağılım histogramları Şekil 7.26’da verilmiştir.



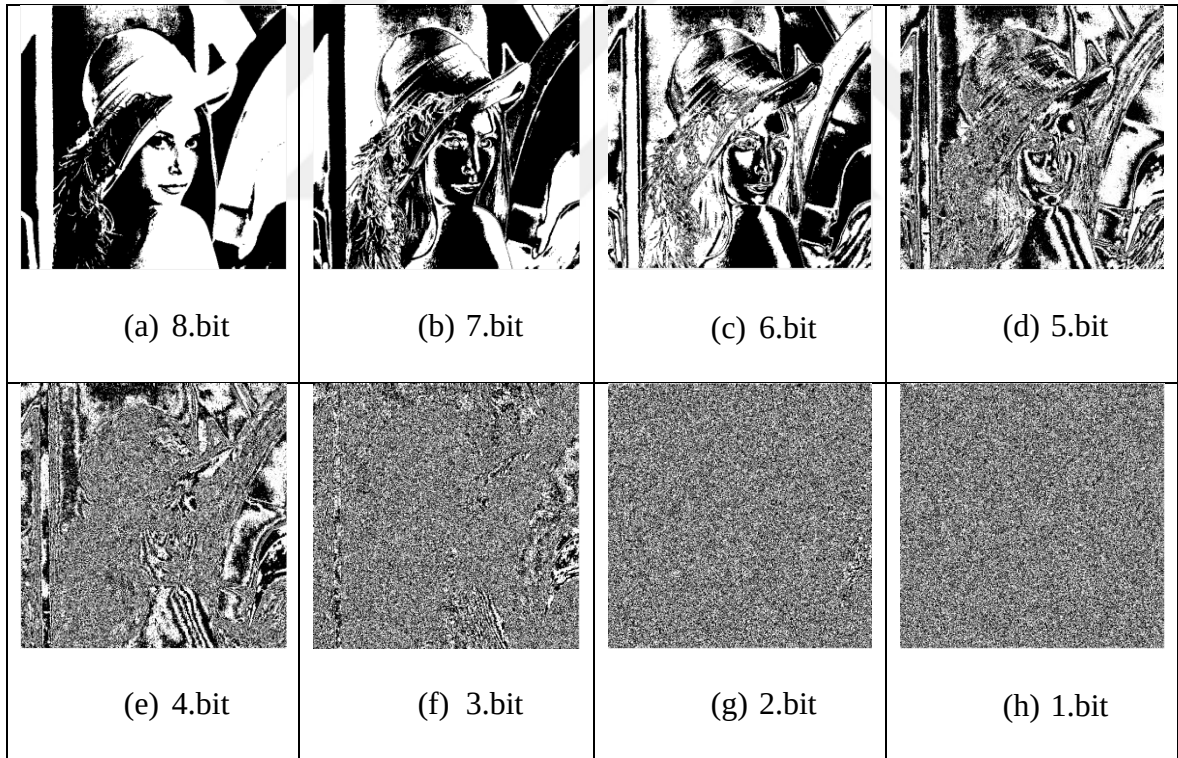
Şekil 7. 26. Değerlerin histogramları (a) V (b) V (mod 8) (c) V (mod 4) (d) V (mod 2)

Şekil 7.26'da görüldüğü gibi en iyi dağılım V (mod 2) işleminde görülmektedir. Komşuluk değerleri V (mod 2) işlemine göre hesaplanmaktadır. Matrisler arasındaki benzerlikler hesaplanır ve benzer matrisler adına bir listede tutulur. Benzerlik hesaplanırken, bit değişimi dikkate alınır ve minimum bit değişimine sahip değer benzer değer olarak kabul edilir. Farklı bit sayısı toplamı bir olan elemanlar benzer adındaki bir listeye kaydedilir. Örneğin 4 sayısı 9 bitte (000000100) olarak ifade edilmektedir. 4 sayısının benzerleri ise 5 (000000101), 6 (000000110), 12 (000001100), 36 (000100100), 68 (001000100), 132 (010000100) ve 260 (10000100)dir. Bu benzerler arasından V (mod 2) işleminin sonucu 4 ün V (mod 2) sonucuna eşit olmayanlar benzer adlı tabloya kaydedilir ve veri gizleme işleminde bu elemanlar rastgele seçim yöntemi kullanılarak mevcut matrisin yerine yerleştirilir. Bu işlem matrisler için bir kereliğine yapılacaktır. Veri gizleme işlemi Şekil 7.27'de verilen otomataya göre yapılacaktır.



Şekil 7. 27. V (mod 2) için veri gizleme diyagramı

Bu yöntem kullanılarak ikili imgelere doğrudan veri gizlenebilir. Gri ve renkli imgelere veri gizlemek için ise imgenin bit düzlemlerini elde etmek gerekmektedir. Şekil 7.28’de Lena adlı imgeye ait bit düzlemleri verilmiştir.



Şekil 7. 28. Lena imgesinin bit düzlemleri

Önerilen veri gizleme algoritmasının adımları aşağıda verilmiştir.

**Adım 1:** Mayın olarak 0 veya 1 seç.

**Adım 2:** İmgeyi bit düzlemlerine ayır.

**Adım 3:** Seçilen  $3 \times 3$  matrisine ait değer  $[1,510]$  aralığında ise 4. adıma geç, değilse pencereyi bir sonraki piksellere kaydır.

**Adım 4:** Seçilen mayına göre komşuluk derecelerini hesapla.

**Adım 5:** Denklem 7.34 'ü kullanarak  $V$  değerini hesapla.

**Adım 6:** Eğer  $V \pmod{2} = 1$  ve  $SD_{i,j}=0$  ise  $V \pmod{2} = 0$  olan ve matrise en yakın benzerlikte olan matrisi, seçili matrisin yerine yerleştir ve 2. adıma git.

**Adım 7:** Eğer  $V \pmod{2} = 0$  ve  $SD_{i,j}=1$  ise  $V \pmod{2} = 1$  olan ve matrise en yakın benzerlikte olan matrisi seçili matrisin yerine yerleştir ve 2. adıma git.

**Adım 8:** Adım 3-7'yi gizli veri boyutunca tekrarla.

Önerilen yöntemin veri çıkarma algoritmasının adımları aşağıda verilmiştir.

**Adım 1:** Stego imgeyi bit düzlemlerine ayır ve veri gömülen bit düzlemlerini elde et.

**Adım 2:** Mayın olan piksel değerini elde et.

**Adım 3:** Seçilen  $3 \times 3$  matrisine ait değer  $[1,510]$  aralığında ise 4. adıma geç, değilse pencereyi bir sonraki  $3 \times 3$  boyutundaki piksellere kaydır.

**Adım 4:** Seçilen mayına göre komşuluk derecelerini hesapla.

**Adım 5:** Denklem 7.34'ü kullanarak  $V$  değerini hesapla.

**Adım 6:**  $SD_{i,j}=V \pmod{2}$  bir sonraki  $3 \times 3$  boyutundaki matrisi seç ve adım 3'e git.

**Adım 7:** Adım 3-6'yı gizli veri boyutunca tekrarla.

#### 7.4.2.3. Deneysel Sonuçlar

Önerilen yöntemin başarımını test etmek PSNR ve kapasite parametreleri kullanılmıştır. Elde edilen sonuçlar literatürde yaygın olarak kullanılan blok tabanlı veri gizleme algoritmalarının sonuçlarıyla karşılaştırılmıştır ve elde edilen sonuçlar Tablo 7.15'de gösterilmiştir.

**Tablo 7. 15.** Elde edilen sonuçların diğer veri gizleme şemalarıyla karşılaştırılması

| Şema                   | Lena    |      | Airplane |      | Baboon  |      |
|------------------------|---------|------|----------|------|---------|------|
|                        | C (bpp) | PSNR | C (bpp)  | PSNR | C (bpp) | PSNR |
| Ni ve ark.[35]         | 0.02    | 48.2 | 0.06     | 48.2 | 0.02    | 48.2 |
| Hwang ve ark. [33]     | 0.02    | 48.2 | 0.06     | 48.3 | 0.02    | 48.2 |
| Kuo ve ark. [34]       | 0.02    | 48.2 | 0.06     | 48.3 | 0.02    | 48.2 |
| Kim ve ark. [32]       | 0.09    | 48.9 | 0.12     | 49.0 | 0.02    | 48.7 |
| Luo ve ark.[36]        | 0.11    | 48.9 | 0.15     | 49.0 | 0.03    | 48.7 |
| Kamran ve ark.<br>[37] | 0.09    | 57.8 | 0.12     | 56.4 | 0.11    | 56.9 |
| Önerilen yöntem        | 0.11    | 60.7 | 0.19     | 54.1 | 0.11    | 60.7 |

Önerilen yöntemde mayın dereceleri ve komşu matrislerin bulunması işlemi bir defaya mahsus gerçekleştirilmektedir. Liste tabanlı yöntem olması nedeniyle veri gizleme algoritmasının zamansal karmaşıklığı  $O(1)$  olarak elde edilmiştir. Listenin oluşturulması ise  $O(n^2)$  karmaşıklığındadır.

#### 7.4.2.4. Sonuç

Bu çalışmada, blok tabanlı yeni bir veri gizleme algoritması önerilmiştir. Önerilen algoritma mayın tarlası oyunundaki kuralları kullanarak veri gizleme yapmaktadır. Veri gizleme yapabilmek için mayın olmayan piksellerin dereceleri değiştirilmektedir. 3 x 3 boyutundaki bloklar kullanılarak mayın dereceleri bulunmuştur. Yüksek görsel kalitede veri gizlemek için, en yakın benzerlikteki ve farklı derecedeki bloklar seçilmektedir.

Deneyisel sonuçlarında gösterdiği gibi, önerilen algoritma yüksek veri gizleme kapasitesi ve yüksek görsel kaliteye sahiptir. Literatürde daha önceden önerilmiş yöntemlerle karşılaştırılmış ve tatmin edici sonuçlar elde edilmiştir. Ayrıca üniform dağılım ve benzer eleman seçiminde kullanılan rastgele sayı üretici sayesinde veri güvenliği sağlanmıştır. Önerilen veri gizleme ve veri çıkarma algoritmaları hızlı çalışmaktadır.

## 8. SONUÇ VE ÖNERİLER

Bu tez çalışmasında multimedya verileri için veri gizleme algoritmaları incelenmiş ve yeni veri gizleme uygulamaları geliştirilmiştir. Geliştirilen veri gizleme uygulamalarının veri gizlemenin performans kriterlerine göre değerlendirilmiş ve literatürdeki diğer yöntemlerle karşılaştırılarak başarılı sonuçlar elde edilmiştir. Literatürde yer alan veri gizleme uygulamaları genellikle kapasite, transparanlık ve dayanıklılık başarımlarını kullanmaktadırlar ancak bu tez çalışmasında 6 adet değerlendirme varlığı ortaya konulmuş ve geliştirilen uygulamalar bu parametrelere göre değerlendirilmiştir. Bu tez çalışmasında, veri gizleme kriptolojik protokollerden olan sır paylaşımı ve görsel sır paylaşımı yöntemleri ile birlikte kullanılarak yüksek başarımla sahip yöntemler elde edilmiştir. Geniş bir uygulama alanına sahip olan veri gizleme uygulamaları sır paylaşımı, görsel sır paylaşımı yöntemleriyle ilişkilendirilmiş ve yüksek başarımla sahip veri gizleme algoritmaları elde edilmiştir. Ayrıca sır paylaşımı ve görsel sır paylaşımı şemalarında var olan problemler tartışılmıştır. Bu problemleri giderebilmek için veri gizleme fonksiyonları kullanılmıştır.

Bu tez çalışmasında sır paylaşımı şemaları irdelenmiş ve veri gizlemeyle olan ilişkisi OR kural tabanlı olasılıksal sır paylaşımı şemaları elde etmek için bool cebri mantıksal operatörlerinden olan XOR'dan faydalanılmıştır. XOR operatörünün en önemli özelliği 0 ve 1'lerin oluşma olasılığının eşit olmasıdır. Bu özellik kullanılarak sır paylaşım şeması oluşturulmuştur. Oluşan olasılık kümesinden örtü nesneyi en az bozacak elemanlar sır parçası olarak seçilerek örtü nesnesine gizlenmektedir ve böylece yüksek başarımlı veri gizleme algoritmaları elde edilmektedir. Bu tez çalışmasında veri gizleme ve sır paylaşımında ilk kez DNA-XOR operatörü kullanılmıştır ve uzaysal alanda 2EÖB veri gizleme fonksiyonu kullanılarak veri gizleme işlemi gerçekleştirilmiştir.

Özellikle görsel sır paylaşımı şemalarında meydana gelen en büyük problem gürültü benzeri imgelerin üretilmesidir. Gürültü benzeri imgeler saldırganların dikkatini çekmekte ve bu imgelere birçok saldırı tekniği uygulanmaktadır. Veri gizlemenin temel amaçlarından birisi de saldırganların dikkatini çekmeden gizli veriyi göndericiden alıcıya göndermektir. Bu sebepten dolayı görsel anlamlı sır paylaşımı şemaları önerilmiştir. Çok katmanlı bilgi güvenliği modelleri oluşturabilmek için, görsel anlamlı GSP şemaları veri gizlemeyle

birlikte kullanılmıştır. Ayrıca çoklu görsel sır paylaşımı şemaları kullanılarak imge kimliklendirme ve saldırı tespiti uygulamaları da gerçekleştirilmiştir.

Veri gizleme uygulamalarında karşılaşılan bir diğer paradoks ise kapasite arttıkça transparanlığın azalmasıdır. Bu paradoksun üstesinden gelebilmek için çok seviyeli veri gizleme uygulamaları gerçekleştirilmiştir. Bu uygulamalar ses ve imge verisine uygulanmıştır.

Blok tabanlı veri gizleme uygulamaları incelenmiş ve kural tabanlı yeni veri gizleme uygulamaları geliştirilerek hem ikili imgelere hem de gri ve renkli imgelere veri gizleme işlemi gerçekleştirilmiştir. Elde edilen blok tabanlı algoritmalar literatürdeki diğer blok tabanlı veri gizleme algoritmalarına göre yüksek başarımlarına sahiptir.

Özet olarak bu tez çalışmasında veri gizleme algoritmalarının başarımlarını iyileştirmek için diğer disiplinlerden faydalanılmıştır ve elde edilen bulgular ışığında yeni veri gizleme algoritmaları önerilmiştir.

### **8.1. Tez Çıktılarının Literatüre Katkıları**

Bu tez çalışmasının literatüre kattıkları aşağıdaki gibi sıralanmıştır.

- XOR ve DNA-XOR tabanlı yeni sır paylaşımı algoritmaları geliştirilmiştir. Geliştirilen algoritmalar olasılık tabanlıdır. Elde edilen olasılık kümesi elemanları kullanılarak yüksek başarımla sahip veri gizleme algoritması oluşturulmuştur.
- Elde edilen sır paylaşımı tabanlı veri gizleme algoritmalarının uzaysal ve frekans alanlarında veri gizleme yeteneğine sahip oldukları gösterilmiştir.
- Görsel sır paylaşımı şemalarında problemler irdelenmiş ve Braille alfabesini kullanan yeni bir olasılıksal görsel sır paylaşımı şeması geliştirilmiştir. Bu şema  $(n,n)$  ve  $(k,n)$  eşikleme yeteneğine sahiptir. Ayrıca veri gizleme kullanılarak çok katmanlı bilgi güvenliği uygulaması gerçekleştirilmiştir. Bu algorithmada Naor ve Shamir'in görsel sır paylaşımı şemasının olasılıksal olarak nasıl kullanılacağı, alt piksellerin anlamlı verilerden oluşturulabileceği ve sahtecilik atağından korunmak için veri gizleme kullanılmıştır.
- Harf tabanlı görsel sır paylaşımı şemaları incelenerek Göktürk alfabesi tabanlı yeni bir görsel sır paylaşımı şeması oluşturulup veri gizleme algoritmalarıyla birlikte kullanılmıştır. Bu algorithmada toplama tabanlı sır paylaşımı şemasının harf tabanlı görsel sır paylaşım şemalarında kullanılabileceği gösterilmiştir.

- Çoklu görsel sır paylaşımı şemalarının veri gizleme uygulamalarında kullanılarak imge kimliklendirme algoritması geliştirilmiştir ve çoklu görsel sır paylaşımı şemalarıyla veri gizleme uygulamalarının multimedya verileri için adli bilişimde özet fonksiyonuna alternatif olarak kullanılabileceği gösterilmiştir.
- Çok seviyeli veri gizleme uygulamaları kullanılarak ses ve imge verilerinin kapasiteleri arttırılırken transparanlıklarının değişiminin minimum olması sağlanmıştır.
- Blok tabanlı veri gizleme algoritmaları incelenmiştir. Mayın tarlası oyunu kurallarını kullanan ve yön vektörlerini kullanan iki adet blok tabanlı veri gizleme algoritması geliştirilmiştir.

## 8.2. Öneriler

Gelecekteki çalışmalarda, bu tez çalışmasında elde edilen bulgular kullanılarak yeni veri gizleme tasarımları geliştirilebileceği gösterilmiştir. Ayrıca veri gizleme algoritmalarının değerlendirme parametrelerinin standartlaşması için çalışmaların yapılmasının gereksinimi belirtilmiştir. Veri gizleme başarımlarından en ayrıntılı inceleneni transparanlıktır. Diğer başarımların ölçümünü standartlaştırmak için yeni çalışmaların yapılması gerekmektedir.

Yeni nesil veri gizleme uygulamaları geliştirilebilir. Mobil cihazlar için hafif sıklet veri gizleme algoritmaları oluşturulabilir. Ayrıca gerçek zamanlı damgalama ve kimliklendirme yapabilmek için veri gizleme cihazı tasarlanabileceği gösterilmiştir.

## KAYNAKLAR

- [1] **Ni, Z., Shi, Y.-Q., Ansari, N., Su, W.,** (2006). Reversible Data Hiding, IEEE Transactions On Circuits And Systems For Video Technology, 16 (3).
- [2] **Begum, M. B., Venkataramani, Y.,** (2012). LSB Based Audio Steganography Based On Text Compression, Procedia Engineering, 30, 703-710.
- [3] **Perez-Gonzalez, F., Balado, F.,** (2002). Quantized projection data hiding, IEEE Int. Conf. Image Process., 2, 889–892.
- [4] **Shi, Y. Q., Ni, Z., Zou, D., Liang, C.,** (2004). Lossless data hiding: fundamentals, algorithms and applications, IEEE Int. Symp. Circuits Syst., 33–36.
- [5] **Mao, Q.,** (2014). A fast algorithm for matrix embedding steganography, Digital Signal Processing, 25, 248-254.
- [6] **Von Ahn, L. and Hopper, N. J.,** (2004). Public-key steganography, in Advances in Cryptology-Eurocrypt, Berlin, Germany: Springer-Verlag, 3027, 323–341.
- [7] **Lin, G.S., Chang, Y.T., Lie, W.N.,** (2010). A framework of enhancing image steganography with picture quality optimization and anti-steganalysis based on simulated annealing algorithm, IEEE Trans. Multimedia, 12 (5), 345–357.
- [8] **Cachin, C.,** (2004). An information-theoretic model for steganography, Information and Computation, 192 (1), 41-56.
- [9] **Yu, Y.-H., Chang, C.-C.,** (2006). A new edge detection approach based on image context analysis, Image and Vision Computing, 24 (10), 1090–1102.
- [10] **Westfeld, A.,** (2003). Detecting low embedding rates, In: Proceedings of information hiding workshop. LNCS, 2578, 324-339.
- [11] **Miller, A. (2012).** Least Significant Bit Embeddings Implementation and Detection, <http://www.aaronmiller.in/thesis/>.
- [12] **Noda, H., Niimi, M., Kawaguchi, E.,** (2006). High-performance JPEG steganography using quantization index modulation in DCT domain, Pattern Recognition Letters, Volume 27, Issue 5, pp. 455-461.
- [13] **Chang, P.C., Chung, K.L., Chen, J. J., Lin, C. H., Lin, T. J.,** (2014). A DCT/DST-based error propagation-free data hiding algorithm for HEVC intra-coded frames, Journal of Visual Communication and Image Representation, Volume 25, Issue 2, pp. 239-253.
- [14] **Lee, S. H.,** (2014). DWT based coding DNA watermarking for DNA copyright protection, Information Sciences, Volume 273, pp. 263-286.
- [15] **Chen, B., Coatrieux, G., Chen, G., Sun, X., Coatrieux, J. L., Shu, H.,** (2014). Full 4-D quaternion discrete Fourier transform based watermarking for color images, Digital Signal Processing, 28, 106-119.
- [16] **Qin, C., Chang, C.-C., Chen, Y.-C.,** (2013). Efficient Reversible Data Hiding for VQ-Compressed Images Based on Index Mapping Mechanism, Signal Processing, vol. 93, no. 9, pp. 2687-2695.
- [17] **Qin, C., Chang, C.C., Huang, Y.H., Liao, L.-T.,** (2013). An Inpainting-Assisted Reversible Steganographic Scheme Using a Histogram Shifting Mechanism, IEEE Transactions on Circuits and Systems.
- [18] **Qi, X., Xin, X.,** (2015). A singular-value-based semi-fragile watermarking scheme for image content authentication with tamper localization, Journal of Visual Communication and Image Representation, 30, 312-327.

- [19] **Botta, M., Cavagnino, D., Pomponiu, V.,** (2015). A successful attack and revision of a chaotic system based fragile watermarking scheme for image tamper detection, *International Journal of Electronics and Communications (AEÜ)*, 69 (1), 242-245.
- [20] **Yu, M., Wang, J., Jiang, G., Peng, Z., Shao, F., Luo, T.,** (2015). New fragile watermarking method for stereo image authentication with localization and recovery, *International Journal of Electronics and Communications*, (69), 1, 361-370.
- [21] **Ghosal, S.K., Mandal, J.K.,** (2014). Binomial transform based fragile watermarking for image authentication, *Journal of Information Security and Applications*, 19 (4&5), 272-281.
- [22] **Tong, X., Liu, Y., Zhang, M., Chen, Y.,** (2013). A novel chaos-based fragile watermarking for image tampering detection and self-recovery, *Signal Processing: Image Communication*, 28 (3), 301-308.
- [23] **Tu, S., Hsu, C.,** (2014). Protecting secret documents via a sharing and hiding scheme, *Information Sciences*, 279 (20), 52-59.
- [24] **Lee, C., Tsai, W. H.,** (2013). A data hiding method based on information sharing via PNG images for applications of color image authentication and metadata embedding, *Signal Processing*, 93 (7), 2010-2025.
- [25] **Lin, C.C., Tsai, W.H.,** (2004). Secret image sharing steganography and authentication, *Journal of Systems and Software*, 73, 405.
- [26] **Yang, C.N., Chen, T.S., Yu, K.H., Wang, C.C.,** (2007). Improvements of image sharing with steganography and authentication, *Journal of Systems and Software*, 80, 1070-1076.
- [27] **Chang, C.C., Hsieh, Y.P., Lin, C.H.,** (2008). Sharing secrets in stego images with authentication, *Pattern Recognition*, 41, 3130-3137.
- [28] **Eslami, Z., Razzaghi, S.H., Ahmadabadi, J. Z.,** (2010). Secret image sharing based on cellular automata and steganography, *Pattern Recognition*, 43, 397-404.
- [29] **Yang, C.N., Ouyang, J.F., Harn, L.,** (2012). Steganography and authentication in image sharing without parity bits, *Optics Communications*, 285, 1725-1735.
- [30] **Yuan, H. D.,** (2014). Secret sharing with multi-cover adaptive steganography, *Information Sciences* 254, pp. 197–212.
- [31] **Nguyen, T.S., Chang, C.C.,** (2015). A reversible data hiding scheme based on the Sudoku technique, *Displays*, 39, 109-116.
- [32] **Kim, K.S., Lee, M.J., Lee, H.Y., Lee, H.K.,** (2009). Reversible data hiding exploiting spatial correlation between sub-sampled images, *Pattern Recognition*, 42,3083-3096.
- [33] **Hwang, J., Kim, J.W., Choi, J.U.,** (2006). A reversible watermarking based on histogram shifting, in: *International Workshop on Digital Watermarking, Lecture Notes in Computer Science*, vol. 4283, 348–361.
- [34] **Kuo, W.C., Jiang, D.J., Huang, Y.C.,** (2007). Reversible data hiding based on histogram, in: *International Conference on Intelligent Computing, Lecture Notes in Artificial Intelligence*, vol. 4682, 1152–1161.
- [35] **Lu, T.-C., Tseng, C.-Y., Wu, J.-H.,** (2016). Asymmetric-histogram based reversible information hiding scheme using edge sensitivity detection, *Journal of Systems and Software*, 116, 2-21.
- [36] **Luo, H., Yu, F.X., Chen, H., Huang, Z.L., Li, H., Wang, P.H.,** (2010). Reversible data hiding based on block median preservation, *Information Sciences* 181, 308– 328.

- [37] **Kamran, Khan, A., Malik, S.A.,** (2014). A high capacity reversible watermarking approach for authenticating images: Exploiting down-sampling, histogram processing, and block selection, *Information Sciences*, 256, 162-183.
- [38] **Wu, M.,** (2001). *Multimedia Data Hiding*, Thesis of Doctor of Philosophy, University of Maryland, [http://www.ece.umd.edu/~minwu/public\\_paper/thesis/wm\\_thesis\\_all.pdf](http://www.ece.umd.edu/~minwu/public_paper/thesis/wm_thesis_all.pdf).
- [39] **Low, S.H., Maxemchuk, N.F., Lapone, A.M.,** (1998). Document identification for copyright protection using centroid detection, *IEEE Trans. Commun.* 372–383.
- [40] **Brassil, J.T., Low, S.H., Maxemchuk, N.F.,** (1999). Copyright protection for the electronic distribution of text documents, in: *Proc. of IEEE*, pp. 1181-1196.
- [41] **Koch, E., Zhao, J.,** (1995). Embedding robust labels into images for copyright protection, in: *Proc. of the International Congress on Intellectual Property Rights for Specialized Information, Knowledge & New Technologies*, pp. 242–251.
- [42] **Wu, M., Tang, E., Liu, B.,** (2000). Data hiding in digital binary images, in: *IEEE Inter. Conf. on Multimedia & Expo*, pp. 393–396.
- [43] **Jung, K.-H., Yoo, K.-Y.,** (2009). Data Hiding Method with Quality Control for Binary Images, *J. Software Engineering & Applications*, 2, 20-24.
- [44] **Wu, M., Liu, B.,** (2004). Data hiding in binary image for authentication and annotation, *IEEE Trans. Multimedia* 528–538.
- [45] **Venkatesan, M., Meenakshidevi, P., Duraiswamy, K., Thiagarajah, K.,** (2007). A new data hiding scheme with quality control for binary images using block parity, in: *3rd Inter. Symposium on Information Assurance and Security*, pp. 468–471.
- [46] **Yung, K.H., Yoo, K.Y.,** (2014). Data hiding method in binary images based on block masking for key authentication, *Information Sciences*, 277, pp. 188-196.
- [47] **Tseng, H.W., Wu, F.R., Hsieh, C.P.,** (2007). Data hiding for binary images using weight mechanism, *IIHMSP* 307–310.
- [48] **Lin, H.C., Yang, C.N., Lai, C.S., Lin, H.T.,** (2013). Natural language letter based visual cryptography scheme, *Journal of Visual Communication and Image Representation*, 24 (3), 318-331.
- [49] **Hu, H. T., Hsu, L. Y., Chou, H. H.,** (2014). Variable-dimensional vector modulation for perceptual-based DWT blind audio watermarking with adjustable payload capacity, *Digital Signal Processing*, 31, 115-123.
- [50] **Nematollahi, M. A., Al Haddad, S. A. R., Zarafshan, F.,** (2015). Blind digital speech watermarking based on Eigen-value quantization in DWT, *Journal of King Saud University - Computer and Information Sciences*, 27 (1), 58-67.
- [51] **Yan, D., Wang, R., Yu, X., Zhu, J.,** (2012). Steganography for MP3 audio by exploiting the rule of window switching, *Computers & Security*, 31 (5), 704-716.
- [52] **Ballesteros, D. M., Moreno, J. M.,** (2012). Highly transparent steganography model of speech signals using Efficient Wavelet Masking, *Expert Systems with Applications*, 39 (10), 9141-9149.
- [53] **Yan, D., Wang, R.,** (2011). Huffman table swapping-based steganography for MP3 audio, *Multimedia Tools and Applications*, 52 (2&3), 291–305.
- [54] **Kar, D.C., Mulkey, C.J.,** (2015). A multi-threshold based audio steganography scheme, *Journal of information security and applications*, 23, pp. 54-67.

- [55] **Bassia, P., Pitas, I., Nikolaidis, N.,** (2001). Robust audio watermarking in the time domain, *IEEE Trans. Multimedia*, 3 (2), 232–241.
- [56] **Mazurczyk, W.,** (2012). Lost audio packets steganography: The first practical evaluation, *Security Commun. Netw.*, 5 (12), 1394–1403.
- [57] **Qiao, M., Sung, A. H., Liu, Q.,** (2013). MP3 audio steganalysis, *Information Sciences*, 231, 123-134.
- [58] **Özkaynak, F.,** (2013). Kaos Tabanlı Şimetrik Şifreleme Sistemlerinin Tasarımı ve Analizi, Doktora Tezi, Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.
- [59] **Dinçer, Ö.,** (2007). Açık Anahtar Altyapısı (AAA) Sistemindeki Sertifikasyon Problemleri ve Diğer Güvenlik Sorunları, <http://bilmuh.gyte.edu.tr/~ispinar/BIL571/>
- [60] **Arslan, G.,** (2009). Kriptoloji Kavramları ve Kripto Analiz Merkezi, <http://www.bilgiguvenligi.gov.tr/>
- [61] **Yıldırım, H. M.,** (2014). Bilgi Güvenliği ve Kriptoloji, Uluslararası Adli Bilişim Sempozyumu.
- [62] **Güngör, M.,** (2015). Ulusal Bilgi Güvenliği: Strateji ve Kurumsal Yapılanma, T.C. Kalkınma Bakanlığı.
- [63] **Menezes, A., Van Oorschot, P., C., Vanstone, S., A.,** (1996). *Handbook of Applied Cryptography*, CRC Press.
- [64] **Paar, C. ve Pelzl, J.,** (2010). *Understanding Cryptography A Textbook for Student and Practitioners*, Springer.
- [65] **Sakallı, M. T.,** (2006). Modern Şifreleme Yöntemlerinin Gücünün İncelenmesi, Doktora Tezi, Trakya Üniversitesi Fen Bilimleri Enstitüsü, Edirne, Türkiye.
- [66] **Shamir, A.,** (1979). How to share a secret, *Communications of the Association for Computing Machinery* 22 (11), 612–613.
- [67] **Blakley, G.,** (1979). Safeguarding cryptographic keys. In *Proc. of AFIPS National Computer Conference*.
- [68] **Mignotte, M.,** (1983). How to Share a Secret, *Lecture Notes in Computer Science*, 149, 371–375.
- [69] **Asmuth, C., Bloom, J.,** (1983). A Modular Approach to Key Safeguarding, *IEEE Transactions on Information Theory*, 29, 208–210.
- [70] **Karaoğlu, D.,** (2009). A Key Establishment Scheme for Wireless Mesh Networks using Identity-based Cryptography and Threshold Secret Sharing, Master of science thesis, Sabanci University, Turkey.
- [71] **Naor, M., Shamir, A.,** (1994). Visual cryptography, in: A. DeSantis (Ed.), *Advances in Cryptology – EUROCRYPT’94, Lecture Notes in Computer Science*, Perugia, Italy, vol. 950, pp. 1–12.
- [72] **Verheul, E. R., Van Tilborg, H. C. A.,** (1997). Constructions and Properties of k Out of n Visual Secret Sharing Schemes, *Designs, Codes and Cryptography*, 11, 2 179–196.
- [73] **Blundo, C., De Santis, A., Stinson, D. R.,** (1999). On the Contrast in Visual Cryptography Schemes, *Journal of Cryptology*, 12, 261–289.
- [74] **Lin, P.-Y., Wang, R.-Z., Chang, Y.-J., Fang, W.-P.,** (2015). Prevention of cheating in visual cryptography by using coherent patterns, *Information Sciences*, 301, 61-74.
- [75] **Wu, C.C., Chen, L.H.,** (1998). A study on visual cryptography, Master Thesis, Institute of Computer and Information Science, National Chiao Tung University, Taiwan, R.O.C..

- [76] **Kafri O., Keren E.,** (1987). Encryption of pictures and shapes by random grids. *Optics Letters*, vol. 12, n. 6, pp. 377-379.
- [77] **Shyu, S. J.,** (2007). Image encryption by random grids, *Pattern recognition*, vol. 40, no. 3, pp. 1014-1031.
- [78] **Wang, D., Li, X., Yi, F.,** (2007). Probabilistic (n,n) visual secret Sharing scheme for grayscale images, in: *Information Security and Cryptology, Lecture Notes in Computer Science*, vol. 4990, Springer-Verlag, Berlin, , pp. 192–200.
- [79] **Takizawa, O., Yamamura, A.,** (2001). A proposal of secret sharing using natural language text, in: *IPSJ Computer Security Symposium*, 343–348.
- [80] **Şahin, A.,** (2007). Görüntü Steganografide Kullanılan Yeni Metotlar ve Bu Metotların Güvenilirlikleri, Doktora Tezi, Trakya Üniversitesi Fen Bilimleri Enstitüsü, Edirne.
- [81] **Katzenbeisser, S., Petitcolas, F.A.P.,** (2000)., *Information Hiding Techniques for Steganography and Digital Watermarking*, Artech House, INC. 685 Canton Street Norwood, MA 02062.
- [82] **Ünlü, O.,** (2012), Ortam ve Yöntem Bağımsız Steganografik Kütüphane Tasarımı, Yüksek Lisans Tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara.
- [83] [http://www.oxforddictionaries.com/definition/american\\_english/steganography](http://www.oxforddictionaries.com/definition/american_english/steganography) (Son Erişim Tarihi: 21.04.2016)
- [84] <https://www.bilgiguvenligi.gov.tr/guvenlik-teknolojileri/uygulamalarla-steganografi-3.html>, 7 Haziran 2014
- [85] **Memon, N., Wong, P.,** (1998) ,Protecting digital media content, *Communications of the ACM*, vol 41, no. 7 , pp. 34–43.
- [86] **Bateman, P., Schaathun, H. G.,** (2008), *Image Steganography and Steganalysis*, Master of Science Thesis, Department of Computing Faculty of Engineering and Physical Sciences University of Surrey.
- [87] **Simmons G.,** (1984) The Prisoners'Problem and the Subliminal Channel, *CRYPTO83 Advances in Cryptology*, pp. 51-67, Aug 22 -24.
- [88] **Kharrazi M., Sencar H.T., Memon N.,** (2004). *Image Steganography: Concepts and Practice*, WSPC/Lecture Notes Series.
- [89] **Anderson, R.J, Petitcolas, F.A.P.,** (1998). On the Limits of Steganography, *IEEE Journal of Selected Areas in Communications*, 16(4):474-481, Special Issue on Copyright & Privacy Protection.
- [90] **Gutub, A.A., Fattani, M.M.,** (2007). A Novel Arabic Text Steganography Method Using Letter Points and Extensions, *World Academy of Science, Engineering and Technology International Journal of Computer, Information Science and Engineering* Vol:1 No:3.
- [91] <http://andacmesut.trakya.edu.tr/bgt/Ders1.ppt>, (Son Erişim Tarihi: 8 Nisan 2015) .
- [92] **Phan, R.C.W., Ling, H.C.,** (2003). Steganalysis of Random LSB Insertion Using Discrete Logarithms Proposed At Cıta03, M2USIC03, PJ, Malaysia.
- [93] **Pitas I., Nikolaidis N.,** (1996). Copyright Protection of Images using Robust Digital Signatures, *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP-96)*, vol. 4, pp. 2168-2171.
- [94] **Avcı, E., Tuncer, T., Ertam, F.,** (2014). Çok Katmanlı Görüntü Steganografi, 7. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı.
- [95] **Ulutaş, G.,** (2012). Gizli Görüntü Paylaşım Şemalarının İyileştirilmesi ve Geometri Tabanlı Yeni Bir Yöntemin Tasarımı, Doktora Tezi, Karadeniz Teknik Üniversitesi Fen Bilimleri Enstitüsü, Trabzon.

- [96] **Liu, J.-F., Tian, Y.-G., Han, T., Yang, C.-F., Liu, W.-B.,** (2015). LSB steganographic payload location for JPEG-decompressed images, *Digital Signal Processing*, 38, 66-76.
- [97] **Tuncer, T., Ertam, F., Avcı, E.,** (2013). A Watermarking Application For Authentication Of Holy Quran, *Taibah University International Conference on Advances in Information Technology for the Holy Quran and Its Sciences (NOORITC)*, Medinah.
- [98] **Chan, C. K., Cheng, L. M.,** (2001). Improved Hiding Data in Images by Optimal Moderately Significant-Bit Replacement, *IEE Electron. Letters*, 37, 16, 1017–1018.
- [99] **Wu, D. C. ve Tsai, W. H.,** (2003). A Steganographic Method for Images by Pixel-Value Differencing, *Pattern Recognition Letters*, 24, 1613–1626.
- [100] **Zhang, X., Wang, S.,** (2006). Efficient Steganographic Embedding by Exploiting Modification Direction, *IEEE Communications Letters*, 10, 11, 781-783.
- [101] **Shih, F. Y., Wu, Y.,** (2003). Combinational image watermarking in the spatial and frequency domains, *Pattern Recognition*, 969 – 975.
- [102] **Shieh, C., Huang, H., Wang F., Pan, J.,** (2004). Genetic watermarking based on transform-domain techniques, *Pattern Recognition*, pp. 555-565.
- [103] **Regentova, E., Latifi, S., Deng, S.,** (2001). Images Similarity Estimation by Processing Compressed Data, *Image and Vision Computing*, 19 (7), 485-500.
- [104] **Sweldens, W.,** (1998). The lifting scheme: a construction of second generation wavelets. *SIAM J. Math. Anal.* 29(2), 511–546.
- [105] **Watson, A. B.,** (1994). Image Compression Using the Discrete Cosine Transform, *Mathematica Journal*, 4, 81-88.
- [106] **Barni, M., Bartolini, F., Cappellini, V. and Piva, A.** (1998). A DCT-Domain System for Robust Image Watermarking. *Signal Processing*, 66, 357-372.
- [107] **Parah, S. A., Sheikh, J. A., Loan, N. A., Bhat, G. M.,** (2016). Robust and blind watermarking technique in DCT domain using inter-block coefficient differencing, *Digital Signal Processing*, 53,11-24.
- [108] **Aslantas, V.,** (2008). A Singular-Value Decomposition-based Image Watermarking using Genetic Algorithm, *AEU - International Journal of Electronics and Communications*, 62 (5), 386-394.
- [109] **Fan, M.-Q., Wang, H.-X., Li, S.-K.,** (2008). Restudy on SVD-Based Watermarking Scheme, *Applied Mathematics and Computation*, 203(2), 926-930.
- [110] **Yeung, M., Mintzer, F.,** (1998). Invisible watermarking for image verification, *Journal of Electronic Imaging*, vol. 7, no. 3, pp. 578-591.
- [111] **Cox, I.J., Killian, J., Leighton, T., Shamoon, T.,** (1997). A secure robust watermark for multimedia, *IEEE Trans. Image Process.* 6 (12), 1673–1687.
- [112] **Phadikar, A., Maity, S.P.,** (2012). On protection of compressed image in fading channel using data hiding, *Comput. Electr. Eng.* 38 (5), 1278–1298.
- [113] **Rad, R. M., Wong, K., Guo, J.-M.,** (2016). Reversible data hiding by adaptive group modification on histogram of prediction errors, *Signal Processing*, 125, 315-328.
- [114] **Tokur, Y., Erçelebi, E.,** (2005). Spread Spectrum Audio Watermarking Scheme Based On Psychoacoustic Model, *The International Conference on Electrical and Electronics Eng.*, 143-147, Bursa/Türkiye.
- [115] **Tanchenko, A.,** (2014). Visual-PSNR measure of image quality, *J. Vis. Commun. Image R.* 25,874–878.

- [116] **Rekik, S., Guerchi, D., Selouani, S. A., Hamam, H.,** (2012). Speech steganography using wavelet and Fourier transforms, *EURASIP Journal on Audio, Speech, and Music Processing*.
- [117] **Jeroa, S. E., Ramua, P., Ramakrishnan, S.,** (2015). ECG steganography using curvelet Transform, *Biomedical Signal Processing and Control*, 22, 161–169.
- [118] **Wu, C.-C., Kao, S.-J., Hwang, M.-S.,** (2011). A high quality image sharing with steganography and adaptive authentication scheme, *J. Syst. Software* 84 (12), 2196–2207.
- [119] **Tuncer, T., Avci, E.,** (2016). A reversible data hiding algorithm based on probabilistic DNA-XOR secret sharing scheme for color images, *Displays*, 41, 1-8.
- [120] University of Southern California, Signal and Image Processing Institute, SIPI Image Dataset, <http://sipi.usc.edu/database/> (05.01.2015)
- [121] **Wu, C.-C., Kao, S.-J., Hwang, M.-S.,** (2011). A high quality image sharing with steganography and adaptive authentication scheme, *J. Syst. Software* 84 (12), 2196–2207.
- [122] **Kanan, H.R., Nazeri, B.,** (2014). A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm, *Exp. Syst. Appl.* 41, 6123-6130.
- [123] **Avci, E., Tuncer T., Avci, D.,** (2016). A Novel Reversible Data Hiding Algorithm Based on Probabilistic XOR Secret Sharing in Wavelet Transform Domain, *Arab J Sci Eng.*, DOI 10.1007/s13369-016-2124-4.
- [124] **Tuncer, T., Avci, E.,** (2015). Braille Alfabeti Tabanlı Olasılıksal Görsel Sır Paylaşımı Yöntemi, 8. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, Ankara, Türkiye.
- [125] **MEB,** (1991). Özel eğitim okulları için Braille kabartma yazı kılavuzu, [http://orgm.meb.gov.tr/alt\\_sayfalar/yayimlar/ozelegitim/blair/blair.pdf](http://orgm.meb.gov.tr/alt_sayfalar/yayimlar/ozelegitim/blair/blair.pdf), MEB Devlet Kitapları, pp. 4.
- [126] **Braille,** (2015). <http://sanlitarihim.blogcu.com/braille-alfabesini-dunyada-ilkkez-osmanli-kullandi/6593257> (Son Erişim Tarihi: 16/08/2015)
- [127] **Yang, C. -N.,** (2004). New visual secret sharing schemes using Probabilistic method, *Pattern Recognition Letters*, 25, pp. 481-494.
- [128] **Tuncer, T., Avci. E.,** (2016). Göktürk Alfabeti Tabanlı Sır Paylaşımı Yöntemi ile Veri Gizleme Uygulaması, *Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi*, Kabul Edildi.
- [129] **Göktürk Alfabeti,** (2015). <http://turkcesivarken.com/gokturkce/> (Son Erişim Tarihi: 28/08/2015).
- [130] **Wu, H.-C., Chang, C.-C.,** (2005). Sharing visual multi-secrets using circle shares, *Comput. Stand. Interfaces*, 134, (28), 123–135.
- [131] **Fraczek, W., Mazurczyk, W., Szczypiorski, K.,** (2011). Multi-Level Steganography: Improving Hidden Communication, *Computing Research Repository (CoRR)*, abs/1101.4789:, arXiv.org E-print Archive, Cornell University, Ithaca, NY (USA).
- [132] **Tuncer, T., Avci, E.,** (2015). A new data hiding algorithm based on direction vector for Digital images, *23rd Signal Processing and Communications Applications Conference (SIU)*, pp. 1753-1756.
- [133] **Yu, Y.-H., Chang, C.-C.,** (2006). A new edge detection approach based on image context analysis, *Image and Vision Computing*, 24 (10), pp. 1090–1102, 2006.

- [134] **Heath, M., Sarkar, S., Sanocki, T., Bowyer, K.,** (1998). Comparison of edge detectors: a methodology and initial study, *Computer Vision and Image Understanding*, 69 (1), pp. 38–54.
- [135] **Ziou, D., Tabbone, S.,** (1998). Edge detection techniques—an overview, *Pattern Recognition and Image Analysis*, 8 (4), pp. 537–559.
- [136] **Minesweeper,** (2015). <http://www.bilgisayamiyorum.com/question/252.aspx> (Son Erişim Tarihi: 07.08.2015).
- [137] **Minesweeper,** (2016). <http://windows.microsoft.com/tr-tr/windows/minesweeper-how-to#1TC=windows-7> (Son Erişim Tarihi: 12.04.2016).



## ÖZGEÇMİŞ

**Türker TUNCER**

Teknoloji Fakültesi

Yazılım Mühendisliği Bölümü

GSM: +90 531 669 30 70

E- mail: turkertuncer@firat.edu.tr

### Eğitim

**DOKTORA (2012– ) Fırat Üniversitesi /Elazığ, Türkiye**

*Fırat üniversitesi Fen Bilimleri Ens. Yazılım Mühendisliği Ana  
Bilim Dalı.*

**YÜKSEK LİSANS (2009–2011) Fırat Üniversitesi /Elazığ, Türkiye**

*Teknik Eğitim Fakültesi Elektronik ve Bilgisayar Eğitimi  
Bölümü, Telekomünikasyon ABD*

**LİSANS (2005–2009) Fırat Üniversitesi /Elazığ, Türkiye**

*Teknik Eğitim Fakültesi Elektronik ve Bilgisayar Eğitimi  
Bölümü, Bilgisayar Öğretmenliği*