

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

RESİMLER İÇİN VERİ GİZLEME TABANLI
BİLGİ GÜVENLİĞİ UYGULAMALARI

YÜKSEK LİSANS TEZİ

Türker TUNCER

Anabilim Dalı: Elektronik Bilgisayar Eğitimi

Danışman: Doç. Dr. Engin AVCI

T.C.
FIRAT ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

RESİMLER İÇİN VERİ GİZLEME TABANLI
BİLGİ GÜVENLİĞİ UYGULAMALARI

YÜKSEK LİSANS TEZİ

Türker TUNCER
091131107

Tezin Enstitüye Verildiği Tarih: 03.05.2011
Tezin Savunulduğu Tarih: 27.05.2011

Tez Danışmanı: Doç. Dr. Engin AVCI (F.Ü)
Diğer Jüri Üyeleri: Doç. Dr. Sami EKİCİ (F.Ü)
Yrd. Doç. Dr. Davut HANBAY (F.Ü)

MAYIS-2011

ÖNSÖZ

Bu tez çalışması Fırat Üniversitesi Rektörlüğü Bilimsel Araştırma Projeleri (FÜBAP) Biriminin 2091 nolu Sayısal Resimler İçin Veri Gizleme Teknikleri başlıklı projesi tarafından desteklenmiştir. Bu tez çalışması veri gizleme uygulamaları üzerine hazırlanmıştır. Günlük hayata uygulanmak istenirse askeri güvenlik sistemlerinde, telekomünikasyon v.b. alanlarda kullanılabilmesi amaçlanmaktadır. Bu çalışmadaki genel amaç, gizliliğin teknolojiyle bütünleştiği, bilginin her şeyden üstün hale geldiği çağımızda bilgi gizliliğinin en üst düzeye ulaşmasını sağlamaktır.

Çalışmam esnasında her türlü hoşgörü, destek ve bilgisiyle bana katkıda bulunan değerli danışmanım Doç Dr. Engin AVCI' ya, uygulama geliştirme esnasında yardımını esirgemeyen Arş. Gör. Şengül DOĞAN' a, her daim bana destek veren ve yanımda olan çok kıymetli aileme, arkadaşlarıma ve özellikle anneme teşekkürü bir borç bilirim.

Türker TUNCER

ELAZIĞ- 2011

İÇİNDEKİLER

	<u>Sayfa No</u>
ÖNSÖZ	II
İÇİNDEKİLER.....	III
ÖZET	VI
SUMMARY	VII
ŞEKİLLER LİSTESİ	VIII
TABLOLAR LİSTESİ	XI
KISALTMALAR LİSTESİ	XII
1. GİRİŞ.....	1
2. SAYISAL RESİM VE GÖRÜNTÜ FORMATLARI	3
2.1. Temel Kavramlar	3
2.1.1. Piksel	3
2.1.2. Nokta ve Nokta Aralığı (Dot ve Dot Pitch).....	3
2.1.3. Çözünürlük	4
2.1.4. Rezolasyon	4
2.1.5. LPI (Line Per Inch).....	4
2.1.6. DPI (Dot Per Inc).....	4
2.2. Görüntü Formatları	5
2.2.1. PICT	5
2.2.2. EPS	5
2.2.3. TIFF	5
2.2.4. JPG	6
2.2.5. BMP	6
2.2.6. GIF	6
2.2.7. PNG	7
2.2.8. PSD.....	7
3. VERİ GİZLEME YÖNTEMLERİ VE TARİHÇESİ	8
3.1. Steganografi.....	8
3.2. Kriptoloji	9
3.3. Sayısal Damgalama	10
3.4. Parmak İzi Ekleme ve Etiketleme	10
3.5. Sayısal İmzalama	10

4.	STEGANOĞRAFI.....	12
4.1.	Bilgi Gizlemenin Alt Alanları	12
4.1.1.	Gizli Kanallar (Covered Channels)	13
4.1.2.	Gerçek Kimlięi Saklama (Anonymity).....	13
4.1.3.	Telif Hakkı İşaretleme (Copyright Marking).....	14
4.1.4.	Steganografi (Steganography)	15
4.2.	Steganografi.....	15
4.2.1.	Steganografi Nedir?	15
4.3.	Steganografinin Alt Alanları	17
4.4.	Steganografinin Kullanım Alanları	17
4.4.1.	Metin (text) Steganografi.....	18
4.4.1.1.	Açık Alan Yöntemleri	19
4.4.1.2.	Yazımsal Yöntemler	19
4.4.1.3.	Anlamsal Yöntemler.....	20
4.4.2.	Görüntü (Image) Steganografi.....	20
4.4.2.1.	Görüntü Dosyalarında Steganografik Yöntemler	21
4.4.2.1.1.	Patchwork Algoritması	22
4.4.2.1.2.	Amplitude (Genlik) Modülasyonu Kullanılarak Bilgi Gizleme	23
4.4.2.1.3.	SSIS (Spread Spectrum Image Steganography) Yöntemi	23
4.4.2.1.4.	Frekans Domaini İçine Veri Saklanması	24
4.4.2.1.5.	Son Bite Ekleme (Least Significant Bit Insertion-LSB) Yöntemi	24
4.4.2.1.5.1.	Gri seviye imgeler üzerinde LSB yönteminin uygulanması.....	25
4.4.2.1.5.2.	8-bit Renkli İmgeler ve LSB yönteminin uygulanması.....	25
4.4.2.1.5.3.	24-bit Renkli İmgeler ve LSB yönteminin uygulanması.....	26
4.5.	Ses (Audio) Steganografi	27
4.5.1.	Düşük Bit Kodlaması	28
4.5.2.	Aşama Kodlaması.....	28
4.5.3.	Taft Yayılması	28
4.5.4.	Yankı Veri Gizlemesi	28
4.6.	Kullanılan Diğer Ortamlar.....	29
5.	STEGANOĞRAFI UYGULAMALARINDA KULLANILAN YÖNTEMLER.....	30
5.1.	Ayrık Dalgacık Dönüşümü.....	30

5.1.1.	DWT'nin Karakteristikleri	31
5.2.	Ayrık Kosinüs Dönüşümü	33
5.3.	Ayrık Fourier Dönüşümü (DFT)	34
5.4.	EÖB Yer Değiştirme Yöntemi (LSB Replacement).....	35
6.	RENKLİ İMGELER İÇİN GERÇEKLEŞTİRİLEN VERİ GİZLEME	
	UYGULAMALARI	42
6.1.	En Önemsiz Bite Ekleme (LSB) Metoduyla Veri Gizleme Uygulaması	42
6.2.	Ayrık Kosinüs Dönüşümü (DCT) Metoduyla Veri Gizleme Uygulaması	47
6.3.	Ayrık Dalgacık Dönüşümü (DWT) Metoduyla Veri Gizleme Uygulaması..	53
6.4.	Çerçeve Metoduyla Veri Gizleme Uygulaması.....	58
6.5.	Geliştirilen Metotla Veri Gizleme Uygulaması.....	63
7.	SONUÇ	69
	KAYNAKLAR	71
	ÖZGEÇMİŞ	80

ÖZET

Bu tez bilgi gizlemenin önemli bir alt dalı olan steganografi ile ilgilidir. Tezin amacı, görüntü dosyaları içerisine bilgi gizlemek için kullanılan steganografik metotların incelenmesi ve bu yöntemlerin güvenilirliklerinin ölçülmesidir. Bu amaç doğrultusunda görüntü steganografide kullanılan yöntemler ayrıntılı bir biçimde incelenmiş ve yaygın olarak kullanılan Son Bite Ekleme Yöntemine göre sayısal resmin içerisine sıralı bir şekilde bilgi gizleyen bir uygulama geliştirilmiştir. Bu uygulama, steganografik sistem değerlendirme kriterleri olan taşıyıcıdaki değişim, kapasite ve dayanıklılık ölçütlerine göre değerlendirilmiştir. Uygulamanın dayanıklılık kriterine göre test edilebilmesi amacıyla bir steganaliz uygulaması geliştirilerek programın güvenilirliği incelenmiştir.

Anahtar Kelimeler: Bilgi Gizleme, Steganografi, Görüntü Steganografi, Son Bite Ekleme Yöntemi

SUMMARY

This thesis is related with one of the important branch of information hiding technique known as Steganography. The aim of the thesis to examine steganographic techniques used for hiding information on image files and to measure reliability of these techniques. To realize our aim, we examined the techniques used in hiding information on image files in detail. Moreover, we developed an application hiding information in arranged order on images according to commonly used LSB method. This application is evaluated according to the evaluation criteria in steganographic systems like change on cover object, capacity and robustness. To test our application according to the robustness criterion, we developed a steganalysis application to examine the reliability of our computer program.

Keywords: Information Hiding, Steganography, Image Steganography, Least Significant Bit Insertion Method

ŞEKİLLER LİSTESİ

Sayfa No

Şekil 2.1 Normal boyuttaki bir imge de piksellerin kare olduğu belirgin değildir.....	3
Şekil 2.2. İmge büyütüldüğünde (32 Kat) piksellerin kare olduğu anlaşılır. Her bir piksel tek renkten oluşur.	3
Şekil 3.1 Steganografik sistem	9
Şekil 4.1. Bilgi gizleme yöntemlerinin sınıflandırılması.....	13
Şekil 4.2. Resmin tamamına filigran gömülmüş örnek.	15
Şekil 4.3. Sayısal Steganografi yöntemlerinin sınıflandırılması	18
Şekil 4.4. Yama çeşitleri.....	23
Şekil 5.1. Filtreleme işleminden sonra sinyalin spektrum ayrışımı.....	31
Şekil 5.2. Lena resmi üzerinde Haar DWT birinci ve ikinci seviye ayrıştırma işlemi.....	33
Şekil 5.3. Kenar steganografisi.....	37
Şekil 5.4. Orijinal imge ve imgenin bpcs kırmızı 3, 4, 5 nci bit katmanları.....	39
Şekil 5.5. Renk paletleri (a) gerçek renk paleti (b) düzenlenmiş renk paleti	40
Şekil 5.6. EzStego algoritması ile veri gizleme yöntemi.....	41
Şekil 6.1. Veri gizleme şeması.	43
Şekil 6.2. Gizlenen verinin yeniden elde edilmesi.	43
Şekil 6.3: Orijinal imge	44
Şekil 6.4: Veri gizlenen imge	44
Şekil 6.5: Keskinleştirilmiş veri gömülen imge	45
Şekil 6.6: Keskinleştirilmiş orijinal imge	45
Şekil 6.7: Bulanıklaştırılmış veri gömülen imge	45
Şekil 6.8: Bulanıklaştırılmış orijinal imge.....	45
Şekil 6.9: 0.4 Oranında küçültülmüş veri gömülen imge	45
Şekil 6.10: 0.4 Oranında küçültülmüş orijinal imge.....	45
Şekil 6.13. Veri gizleme şeması.	48
Şekil 6.14. Gizlenen verinin yeniden elde edilmesi.	49
Şekil 6.15: Orijinal imge	49
Şekil 6.16: Veri gizlenen İmge	49
Şekil 6.17: Keskinleştirilmiş veri gömülen imge	50
Şekil 6.18: Keskinleştirilmiş orijinal imge	50
Şekil 6.19: Bulanıklaştırılmış veri gömülen imge	51

Şekil 6.20: Bulanıklaştırılmış orijinal imge.....	51
Şekil 6.21: 0.4 Oranında küçültülmüş veri gömülen imge	51
Şekil 6.22: 0.4 Oranında küçültülmüş orijinal imge.....	51
Şekil 6.23: -45° Döndürülmüş veri gömülen imge	51
Şekil 6.24: -45° Döndürülen orijinal imge	51
Şekil 6.25. Veri gizleme şeması.	53
Şekil 6.26. Gizlenen verinin yeniden elde edilmesi.	54
Şekil 6.27: Orijinal imge	54
Şekil 6.28: Veri gizlenen imge	54
Şekil 6.29: Keskinleştirilmiş veri gömülen imge	55
Şekil 6.30: Keskinleştirilmiş orijinal imge	55
Şekil 6.31: Bulanıklaştırılmış veri gömülen imge	56
Şekil 6.32: Bulanıklaştırılmış orijinal imge.....	56
Şekil 6.33: 0.4 Oranında küçültülmüş veri gömülen imge	56
Şekil 6.34: 0.4 Oranında küçültülmüş orijinal imge.....	56
Şekil 6.35: -45° Döndürülmüş veri gömülen imge	56
Şekil 6.36: -45° Döndürülen orijinal imge	56
Şekil 6.37. Veri gizleme şeması.	58
Şekil 6.38. Gizlenen verinin yeniden elde edilmesi.	59
Şekil 6.39: Orijinal imge	59
Şekil 6.40: Veri Gizlenen imge	59
Şekil 6.41: Keskinleştirilmiş veri gömülen imge	60
Şekil 6.42: Keskinleştirilmiş orijinal imge	60
Şekil 6.43: Bulanıklaştırılmış veri gömülen imge	60
Şekil 6.44: Bulanıklaştırılmış orijinal imge.....	60
Şekil 6.45: 0.4 Oranında küçültülmüş veri gömülen imge	61
Şekil 6.46: 0.4 Oranında küçültülmüş orijinal imge.....	61
Şekil 6.47: -45° Döndürülmüş veri gömülen imge	61
Şekil 6.48: -45° Döndürülen orijinal imge	61
Şekil 6.49. Veri gizleme şeması.	64
Şekil 6.50. Gizlenen verinin yeniden elde edilmesi.	64
Şekil 6.51: Orijinal imge	65
Şekil 6.52: Veri Gizlenen imge	65

Şekil 6.53: Keskinleştirilmiş veri gömülen imge	66
Şekil 6.54: Keskinleştirilmiş orijinal imge	66
Şekil 6.55: Bulanıklaştırılmış veri gömülen imge	66
Şekil 6.56: Bulanıklaştırılmış orijinal imge.....	66
Şekil 6.57: 0.4 Oranında küçültülmüş veri gömülen imge	67
Şekil 6.58: 0.4 Oranında küçültülmüş orijinal imge.....	67
Şekil 6.59: -45° Döndürülmüş veri gömülen imge	67
Şekil 6.60: -45° Döndürülen orijinal imge	67

TABLOLAR LİSTESİ

Tablo 6.1. LSB metoduyla ile veri gizlenmiş imgelerin PSNR değerleri.	437
Tablo 6.2. DCT metoduyla ile veri gizlenmiş imgelerin PSNR değerleri.....	52
Tablo 6.3: DWT metoduyla ile veri gizlenmiş imgelerin PSNR değerleri	57
Tablo 6.4: Çerçeve metoduyla ile veri gizlenmiş imgelerin PSNR değerleri	62
Tablo 6.5: Geliştirilen metotla ile veri gizlenmiş imgelerin PSNR değerleri	68

KISALTMALAR LİSTESİ

LSB	: En Önemsiz Bite Ekleme
DWT	: Ayrık Dalgacık Dönüşümü
DCT	: Ayrık Kosinüs Dönüşümü
AFD	: Ayrık Fourier Dönüşümü
BMP	: Windows Bitmap
GIF	: Grafik Değiştirme Biçimi
JPEG	: Birleşik Fotoğraf Uzmanları Grubu
PNG	: Taşınabilir Ağ Grafiği
PSNR	: İşaret-Gürültü Oranı

1. GİRİŞ

Son yıllarda bilgisayar sistemlerinin güvenliği ve özellikle bilgi güvenliği oldukça önemli bir konu olarak karşımıza çıkmaktadır [1]. Özellikle son 10 yılda internetin yaygınlaşmasıyla veri alışverişi ve paylaşımı da artmıştır. Metin, imge, ses vb. gibi birçok veriyi içeren dosyalar, etkin bir şekilde dünyanın birçok yerindeki insanlar tarafından paylaşılabilir hale gelmiştir. Fakat hayatı kolaylaştıran bu iletişim ağı çok ciddi güvenlik açıklarını da beraberinde getirmiştir. Birbiriyle haberleşen iki kişi arasındaki iletişim bir üçüncü kişi tarafından erişilebilir ve değiştirilebilir hale gelmiştir. Bunu engellemek amacıyla çeşitli koruma mekanizmaları geliştirilmiş ve yeni teknolojiler ve yeni uygulamalar ortaya çıkmıştır. Bu teknolojilerden biri şifrelemedir (kriptoloji). Şifrelemede gönderilecek ve korunması istenen sayısal veri şifreleme algoritmalarıyla bir anahtar yardımıyla anlaşılabilir bir hale dönüştürülür ve bu şekilde gönderilir. Ancak şifrelerin de zaman içinde kırılabilmesi şifrelemenin güvenli iletişim için tek başına yeterli olmadığını göstermektedir [2].

Bilgisayar ortamında bilginin gizli bir şekilde gönderilmesi için önerilen yöntemlerden diğeri Steganografi'dir. Steganografi, herhangi bir sayısal ortama; sese, videoya, görüntüye ya da yazıya, bu bilginin görünmez bir şekilde gizlenmesi ve bilginin taşıyıcı aracılığıyla yollanmasıdır [3]. Gönderilecek bilgi, seçilen sayısal ortama fark edilebilir bir değişikliğe sebep olmayan bir yöntem kullanılarak eklenir. Böylece gönderilen sayısal ortam içinde herhangi bir bilginin bulunduğu dair herhangi bir ize rastlanmaz. Diğer bir yöntem olan kriptolojiden farklı olarak bilgi, üzerinde herhangi bir deşifre işlemine gerek duyulmadan anlaşılır bir şekilde geri elde edilir [4]. Kriptoloji de ise, bilginin kendisi bir algoritma ile şifrelenir. Şifrelenmiş bilgi, herhangi bir taşıyıcı olmaksızın iletilir. İletim tamamlanıncaya kadar bilgi şifrelidir. İletimin sonunda alıcı, deşifre algoritmasını kullanarak şifrelenmiş bilgiyi çözer. Böylece sayısal içeriğe erişime yetkisiz bir kişi iletimin herhangi bir aşamasında şifrelenmiş bilgiyi elde etse bile, şifreyi çözmek için deşifre algoritmasını bilmediğinden asıl bilgiye ulaşamaz [5].

Bilgi gizleme iletişim güvenliği için oldukça önemli bir konudur. Bilgi gizlemede amaç iletişimin bir üçüncü kişinin fark edemeyeceği şekilde yapılmasıdır. Şifrelemede üçüncü kişi gizli bir bilginin gönderildiğinden haberdardır, fakat bilgi gizleme yöntemleriyle iki kişi arasındaki iletişimin gizli bir şekilde yapılması mümkün olmaktadır. Üçüncü kişi arada gizli bir iletişim olduğunu fark edememektedir [6].

Bilgi gizleme çok eski yıllardan beri kullanılmaktadır. Günümüzde teknolojinin gelişmesiyle birlikte birçok yeni teknik geliştirilmiştir ve hala geliştirilmeye devam edilmektedir. Bilgi gizlemenin çok önemli bir alt disiplini olan Steganografi, sayısal (dijital) ortamdaki verilerin (metin, ses ve görüntü dosyaları) korunması için son yıllarda sıklıkla kullanılmaktadır. Steganaliz ise gizli yapılan iletişimin ele geçirilmesi için yapılan saldırıları içermektedir [7].

Bir steganografik sistemin güvenilirliği çeşitli açılardan değerlendirilmektedir. Bunlar bilgi gizlemenin örtü verisini (cover object) ne kadar değiştirdiği, bilgi saklama kapasitesinin ne kadar olduğu ve dayanıklılığının ne kadar olduğudur. Dayanıklılık ölçütü steganalitik yöntemlere karşı ne kadar başarılı olduğu ile ölçülmektedir [8].

Teknolojinin gelişmesiyle birlikte birçok steganografik yöntem ortaya çıkmıştır, bu gelişmeyle birlikte birçok steganalitik yöntemin de geliştirilmesi gerekmiştir. Her steganografik yöntem farklı bir metot izlediği için bunları sezmede kullanılacak steganalitik yöntemler de çeşitlidir [9]. Bir steganografik yöntem için geliştirilen steganaliz yöntemi bir diğeri için çalışmamaktadır. Her steganografik yöntemin kendine özgü bir steganaliz yöntemi bulunmaktadır. Son otuz yıldır teknolojiye paralel olarak; internetin giderek yaygınlaşması, sayısal veri saklama ve kaydetme cihazlarının (CD, DVD gibi depolama araçlarının) ortaya çıkması, yüksek bant genişliği ve kalitesi gibi yaşanan teknolojik gelişmeler sayısal içeriğin oluşturulmasını, kopyalanmasını ve iletimini daha ucuz ve kolay hale getirmiştir [10].

Bu çalışma ile bilgisayar ortamındaki görüntülere gizli bir bilgi gizlenmesi amaçlanmıştır. Bu amaçla bilgi içeren bit dizisi seçilmiştir. Bilgi eklenecek taşıyıcı görüntü üç boyutlu görüntü olup, ekleme işlemi sonunda görüntüdeki bozulmanın en az olması ve eklenecek bilginin çeşitli görüntü işleme saldırılarına karşı tanınabilir şekilde geri elde edilmesi amaçlanmıştır. Tez düzeni genel hatlarıyla şu şekildedir; 2. bölümde sayısal görüntü özellikleri, 3. bölümde veri gizleme yöntemleri ve tarihçesi, 4. bölümde Steganografi kavramı, 5. bölümde Steganografi uygulamalarında kullanılan yöntemler, 6. bölümde uygulamalar ve 7. bölümde sonuç kısmına yer verilmiştir.

2. SAYISAL RESİM VE GÖRÜNTÜ FORMATLARI

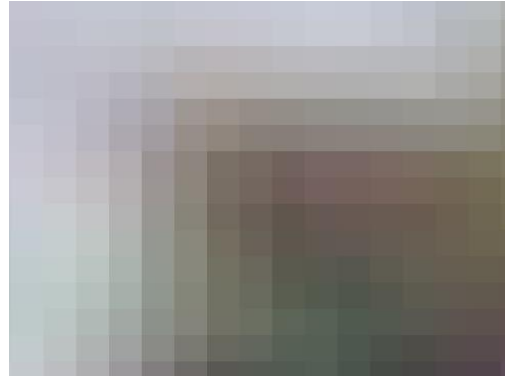
2.1. Temel Kavramlar

2.1.1. Piksel

Ekranda oluşan görüntüler noktalardan oluşur. Noktalar kare şeklindedir. Çok yakından bakıldığı zaman veya imge büyütüldüğünde bu noktalar fark edilebilir. Ekranda kontrol edilebilen en küçük noktalara piksel denir. Bir piksel kırmızı, yeşil ve mavi renklerin karışımından oluşur. Bitmap (piksel tabanlı) imge programları, ölçü birimi olarak piksel kullanırlar. Piksel yoğunluğu arttırılırsa görüntü netleşir. Çok fazla arttırıldığında ise dosyanın kapasitesinin artmasına, ayrıca yazdırılırken zaman kaybına ve mürekkep sarfiyatına neden olur.



Şekil 2.1 Normal boyuttaki bir imge de piksellerin kare olduğu belirgin değildir



Şekil 2.2. İmge büyütüldüğünde (32 Kat) piksellerin kare olduğu anlaşılır.

Piksel tek başına bir ölçüyü ifade etmez. Verilen piksel sayısı, belirtilen alan içerisindeki piksel sayısıdır. Verilen alan içerisindeki piksel sayısına göre piksellerin boyutu değişir. Piksel boyutu sabit bir değer değildir.

2.1.2. Nokta ve Nokta Aralığı (Dot ve Dot Pitch)

Pikselli oluşturan kırmızı, mavi veya yeşil renklerinden her birine ise nokta (dot) denir. Bir pikseldeki renklerin birbirine olan mesafesine nokta aralığı (dot pitch) denir.

2.1.3. Çözünürlük

Bir defa da ekranda görüntülenebilen piksel sayısına çözünürlük denir.

2.1.4. Rezolasyon

Bir resmin piksel yoğunluğu yani PPI (Pixel Per Inches) 1 inç karede (1 inç = 2.54 cm) bulunan piksel sayısıdır. Ofset baskı için en önemli etken, baskının yapılacağı kâğıt cinsidir. Gazete kâğıdı ile kuşe kâğıda yapılacak baskı arasında fark vardır. Gazete kâğıdına baskı 40'lık tramla basılırken, kuşe için 70 ya da 80'lik tram kullanılması gerekir. Tramlar, birbirine özel açılar ile dizilmiş noktacıklardır ve sonuçta aralarında belli bir miktar boşluk vardır.

2.1.5. LPI (Line Per Inch)

Film pozlanırken 1 inç yüksekliğindeki (2.54 cm) alana atılan satır sayısına LPI adı verilir. Ofset baskıda tramlarla iş basılır. Paralel çizgiler halinde sıralandıklarını düşünebiliriz. Tramlar yardımı ile mavi, kırmızı, sarı ve siyah mürekkepleri kâğıda aktarılır. Bu çizgilerin yoğunluğu ve aralığı baskı kalitesini belirler. En çok kullanılan tram aralıkları 175, 150, 133, 120, 110, 100, 85 ve 65 LPI'dir.

2.1.6. DPI (Dot Per Inc)

Çıkış cihazlarında 1 inç'te (2.54 cm x 2.54 cm) noktalanın (yani basılan) ya da pozlanan piksel sayısına DPI adı verilir. Renkli/siyah-beyaz çıkış yapan yazıcılar baskılarını nokta vuruşları ile yapar. Her inç'te noktalanın piksel sayısı makinenizin özelliğine göre değişir. Çünkü her yazıcının kullanabileceği en yüksek nokta yoğunluğu farklıdır. 300 DPI, 600 DPI, 1200 DPI gibi... CMYK adı verilen “Cyan, Magenta, Yellow ve Black” ile kâğıdın üzerinde küçük mürekkep noktacıklarını basar, bunlar da bildiğimiz renkleri oluşturur. Film çıkış cihazları çözünürlüğü, DPI'e, yani bir Inch başına vurduğu nokta sayısına göre hesaplar.

2.2. Görüntü Formatları

Masaüstü yayıncılıkta kullanılan yazılımlar birbirleri ile dosya alışverişinde bulunarak çalışırlar. Bir resmi veya vektörel çizimi oluşturduğumuz uygulama programından bağımsız hale getirip sayfa düzenleme programına ya da vektörel programlara aktarmak için farklı bir formatta kaydetmemiz gerekir. Yaygın kullanılan görüntü formatlarından bazıları şunlardır.

2.2.1. PICT

PICT formatı bütün programların ortak kullandığı dosya formatıdır. Bu format herhangi bir uygulama programına aktarıldığında imge bilgisi sayfaya dâhil olur. Görüntü diskinizden silinse dahi baskı aracı sayfayı basarken PICT dosyasını aramaz.

2.2.2. EPS

EPS formatı hemen hemen bütün çizim ve sayfa düzenleme programları tarafından desteklenir. Photoshop programında, doküman Bitmap modunda kaydedilirken Transparent (Şeffaf) + Whites (beyazları saydam yap) seçeneği işaretlenerek kaydedilirse, dosyada beyaz alanlar şeffaf olarak tanımlanır. Renkli bir doküman EPS olarak kaydedilecekse olası baskı problemlerini önlemek için CMYK moduna geçirilmiş olmalıdır.

2.2.3. TIFF

TIFF formatı bilgisayarlar arası ortak bir dosya formatıdır. Tüm programlar tarafından desteklenir. Bu formatta kayıtlı dosyalar, herhangi bir uygulama programında sayfa içine alındığında görüntünün ve zeminin renk değerlerini azaltma ve değiştirme olanağı verir. Örneğin, farklı renklerde kullanacağımız bir görüntü ya da logoyu TIFF formatla kaydedip sayfaya yapıştırdığımızda renklerini değiştirebilirsiniz. Bu yolla her renk değişikliğinde onu oluşturan uygulama programında açıp yeniden renk verip yeni dosyalar yaratmamış oluruz.

2.2.4. JPG

JPG formatı, imge işleme programlarının yüksek MB'lı dosyaları sıkıştırarak disk üzerinde kayıt edebileceğiniz bir formattır. JPEG veya JPG formatının özelliği gerçek renk değerlerini içermesidir. Bu nedenle fotoğrafik (çizgisel/grafiksel olmayan) görüntüleme için kullanılmalıdır. JPEG sıkıştırma yöntemi görüntünün algılanması için zorunlu olmayan detayları bulup atan ve dosyayı bu şekilde sıkıştıran bir format olduğundan kayıplı formatlar arasında yer alır. Kaybolan ayrıntılar ve sıkıştırma oranı arasında bağlantı bulunduğundan bu dengeyi iyi korumak gerekmektedir. Daha fazla sıkıştırma daha fazla detay kaybı, daha az sıkıştırma daha büyük dosya demektir.

2.2.5. BMP

BMP, Windows ve Microsoft'un PCX formatını değiştirerek geliştirdiği bir formattır. Windows 3.1 ve 95 ile birlikte gelen MSPaint programı görüntüleri bu formatta işler. BMP formatı 1-24 bit arasında değişen bir piksel derinliğini içerebilir. Sıkıştırma seçeneği başlangıçta bulunmamakta idi. Opsiyon olan bu sıkıştırma görüntüde detay kaybına yol açmaz, yani kayıpsız sıkıştırma yöntemlerindendir. BMP formatı alıcı bilgisayarında Paint'den başka görüntü programı bulunmadığı durumlarda kullanılır.

2.2.6. GIF

CompuServe firmasının Graphics Interchange Format (GIF) dosyaları internet üzerinde oldukça yaygın kullanılan bir formattır. Az sayıda renk içeren (1 ila 8 bitlik) dokümanlarda oldukça iyi sıkıştırma sağlaması, animasyonlarda zamanlama ve farklı boyutlardaki imgeleri bir arada tutma desteği, saydam renk tanımlanması bu format'ı popüler yapan nedenlerden sadece bir kaçıdır. Ancak "Adobe Photoshop" gibi imge işleme programlarının çoğu GIF formatının tüm özelliklerini kullanamamaktadır. Bu nedenle bu format ile çalışırken sıklıkla başka programlara gereksinim duyulmaktadır. GIF dosyaları Bitmap, gri skala ve indekslenmiş renk sisteminde olabilmektedir. Gerçek renk desteği yoktur. GIF imgeleri sıralı (interlaced) veya sırasız kaydedilebilmektedir. Sıralı GIF dosyaları yükleme esnasında satır satır gelerek imge bitiminden önce neye benzeyeceğine

dair bir ipucu verirler. Saydamlık tanımlanması için GIF89a Export komutu kullanılarak saydam olacak renk belirlenebilir.

2.2.7. PNG

PNG (Portable Network Graphics) formatı patentsizdir. PNG kayıpsız Wave Table sıkıştırma yöntemini kullanır. Şu anda mevcut olmayan kayıpsız gerçek renk ve saydamlık bilgilerini içeren imge kalitesini internet'e taşımayı amaçlamaktadır. PNG dosyalarındaki saydamlık bilgileri alfa kanalı içerisinde saklanmaktadır. Sıralı yükleme de olanaklıdır. Ayrıca sıkıştırma için değişik filtreleme algoritmaları sıkıştırma öncesi kullanılabilir.

2.2.8. PSD

PSD (Photoshop Document) Photoshop uygulamasına özel bir formattır. PSD çok sayıda alfa kanalını, yolu ve katmanı desteklemektedir. PSD dosyaları ikili dosya, indekslenmiş renk, gerçek renk RGB, CMYK, Lab biçimlerini destekler. Çalışma yaptığınız işlerin PSD'sini saklamayı alışkanlık haline getirmeniz, daha sonra yapılacak düzeltmelerde çok işinize yarayacaktır [11].

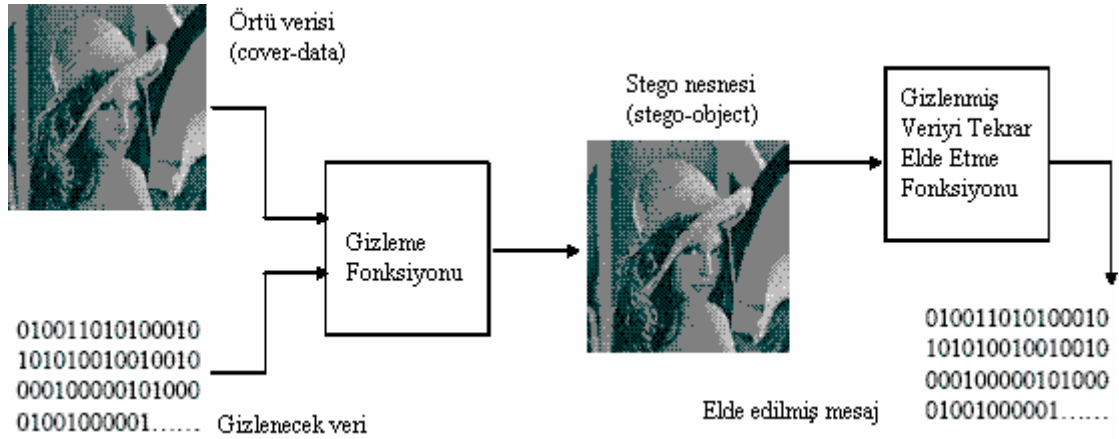
3. VERİ GİZLEME YÖNTEMLERİ VE TARİHÇESİ

Veri gizleme yöntemlerinin tarihi, veri iletişimi kadar eskilere dayanır. İlk Yunan tarihçisi Heredot'un bir çalışmasında anlattığı gizli mesaj yollama tekniği şu şekildedir. Sahibi tarafından Pers işgali altındaki İyonya şehri Milet'e yollanan bir köleyle gizli olarak mesaj yollanır. Histiaüs, kölesinin kafa derisine bir mesajı dövmelettirir. Zamanla kölesinin saçları uzar ve mesaj saçın altında gizli kalır ve köle Milet'e, Milet'in valisi Aristogoras'a yollanır. Aristogoras, kölenin saçını traşlatır ve gizli mesaj olan "Persliler'e karşı ayaklanma başlatın. " diyerek bir ayaklanma çıkartır. Bu yöntem damgalamadan farklı olarak steganografik veri gizleme olarak adlandırılır. Eğer mesaj "Bu köle Histiaüs'undur" şeklinde köle ve sahibi hakkında bilgi içermiş olsaydı bir damgalama tekniği uygulanmış olacaktı. İnternet gibi sayısal sistem ağlarının yaygınlaşmasıyla ortaya çıkan güvenlik ve telif hakları sorunu için sayısal damgalama düşüncesi ilk olarak 1990 yılının başında ortaya atılmıştır. O günden beri konu üzerinde araştırmalar yapılmaktadır. Sayısal görüntülerin damgalanması konusundaki ilk yayınlar TANAKA ve çalışma grubu tarafından 1990, CARONNI ve çalışma grubu tarafından 1993 yılında yapılmıştır. Sayısal görüntülerdeki damgalama çalışmaları, sonradan, ses ve video görüntüleri üzerine de yapılarak genişleyerek artmıştır [12-15] Sayısal görüntüler üzerinde yapılan bilgi gizleme işlemleri amacına uygun olarak farklı yöntemlerle yapılmaktadır. Bu bölümde veri gizleme terminolojisi kısaca anlatılacak ve ardından literatürde karşılaşılan veri gizleme çalışmaları hakkında bir özet sunulacaktır.

3.1. Steganografi

"Steganografi", örtülü yazı anlamına gelip, bir taşıyıcıya gizli mesajın eklenmesi ile yapılan iletişim türüdür. Gizli mesaj doğrudan ya da şifrelenerek değil, taşıyıcı aracılığı ile karşı tarafa iletilir. Mesajın taşıyıcı üzerinde yapılacak değişikliklere karşı dayanıklı olması beklenmez. Buradaki amaç, taşıyıcıya fark edilmeyecek bir yöntem ile mesajı saklamak ve iletmeğdir [16]. Mesaj, taşıyıcı içinde küçük bir değişiklikle yok olabilecek kırılgan bir yapıya sahiptir. Steganografi kullanım alanları açısından üçe ayrılmaktadır. Bunlar aşağıdaki gibidir [17]:

- Metin (text) steganografi
- Görüntü (image) steganografi
- Ses (audio) steganografi.



Şekil 3.1 Steganografik Sistem

Görüntü steganografide, bilgilerin görüntü dosyaları içerisine saklanması için çeşitli yöntemleri vardır. Şekil 1’de Gizleme Fonksiyonu olarak adlandırılan ve bilgi gizlemede en çok kullanılan yöntemler aşağıdaki gibidir.

- En önemsiz bite ekleme
- Maskeleye ve filtreleme
- Algoritmalar ve dönüşümler [18]

3.2. Kriptoloji

Veri gizleme yöntemi olan kriptolojide, steganografiden farklı olarak herhangi bir taşıyıcı kullanılmaz. Gizlenmesi gereken mesaj, bir algoritma kullanılarak şifrelenir ve şifreli mesajın kendisi herhangi bir taşıyıcı kullanılmadan gönderilir. Alıcı, aldığı mesajı deşifre ederek asıl mesaja ulaşır [19]. Sayısal içeriğe erişimi yetkisiz kişiler şifrelenmiş mesajı elde etse bile deşifre algoritmasını bilmedikçe mesajın aslını elde edemezler [20].

3.3. Sayısal Damgalama

Bilgisayarların ve bilgisayar ağlarının gelişmeye başlaması ile birlikte, güvenlik ve telif haklarının korunması amacıyla ortaya atılan sayısal damgalama yöntemleri de steganografi uygulamalarına benzer. Ancak amaç bakımından sayısal damgalamada, çalışma ile birlikte çalışmaya damgalanan bilginin taşınması da istenir. Bu nedenle bilgisayar ortamındaki çalışmalara telif hakkı, lisans, logo vb. bilgiler damgalanır. Damgalama yöntemlerinin geliştirilmesinde, sayısal çalışmalara damgalanan bilginin çeşitli saldırılara (gürültü, sıkıştırma, kesme, yeniden boyutlandırma... gibi işaret işleme işlemlerine) karşı dayanıklı olması öncelikli amaç olarak göz önünde tutulur. Steganografi uygulamalarında böyle bir beklenti yoktur [21].

3.4. Parmak İzi Ekleme ve Etiketleme

Parmak izi, diğer bir adıyla etiketleme, sayısal bir çalışmanın belli bir tüketiciye dağıtılma öncesinde, telif haklarının korunması amacıyla, yalnızca o tüketiciyi temsil eden bilginin çalışmaya görünmez bir şekilde damgalanması işlemidir. Etiketlemede kullanılan yöntemde bilgi, dışardan yapılan çeşitli saldırılara karşı dayanıklıdır. Böylece her tüketiciye, içinde kendisine özel bir bilginin saklandığı bir ürün verilir [22]. Parmak izi ekleme, amaç bakımından sayısal damgalamadan farklı ancak yöntem olarak sayısal damgalama ile aynı özellikler gösterir.

3.5. Sayısal İmzalama

Sayısal imzalama, doküman sahibinin kendi kişisel anahtarı ile dokümanı imzalaması yani şifrelemesidir. Bu kişisel anahtardan üretilen kamusal anahtar, dokümanın gönderileceği alıcı tarafında bulunur ve dokümanı açmakta kullanılır. Sayısal imzalama, kişisel ve kamusal anahtarın kullanıldığı damgalama olarak tanımlanabilir. Kişisel bir anahtar ile imzalanan doküman, sahibi hakkındaki bilgiyi de birlikte taşımış olur. Sayısal damgalama ile sayısal imzalamanın eş anlamlı olduğuna dair görüşlere karşın bunları birbirinden ayrı tutan görüşler de vardır [23].

Sayısal dokümanların imzalanması için uygulamada çeşitli yazılımlar vardır. Herhangi birisi için oluşturulan kamusal ve kişisel imzalar, kendisine elektronik kartlarda

verilir. Ancak birçok yerde yasal düzenlemelerin ve teknik altyapının tamamen sağlanmamış olmasından dolayı kullanımı yaygın değildir. Sayısal imza kullanılarak, gönderilecek dokümanın bütünlüğü sağlanır, göndericinin kişisel imzası kullanılarak şifrelendiğinden gönderici tarafından inkar edilemez ve göndericinin imzası taklit edilemeyeceğinden belirtilen göndericiden geldiği kesindir. Alıcı kendisine ait kamusal anahtarı kullanarak bu dokümanı açar, ancak göndericinin kişisel anahtarı olmadan doküman üzerinde değişiklik yapamaz.

4. STEGANOGRAFI

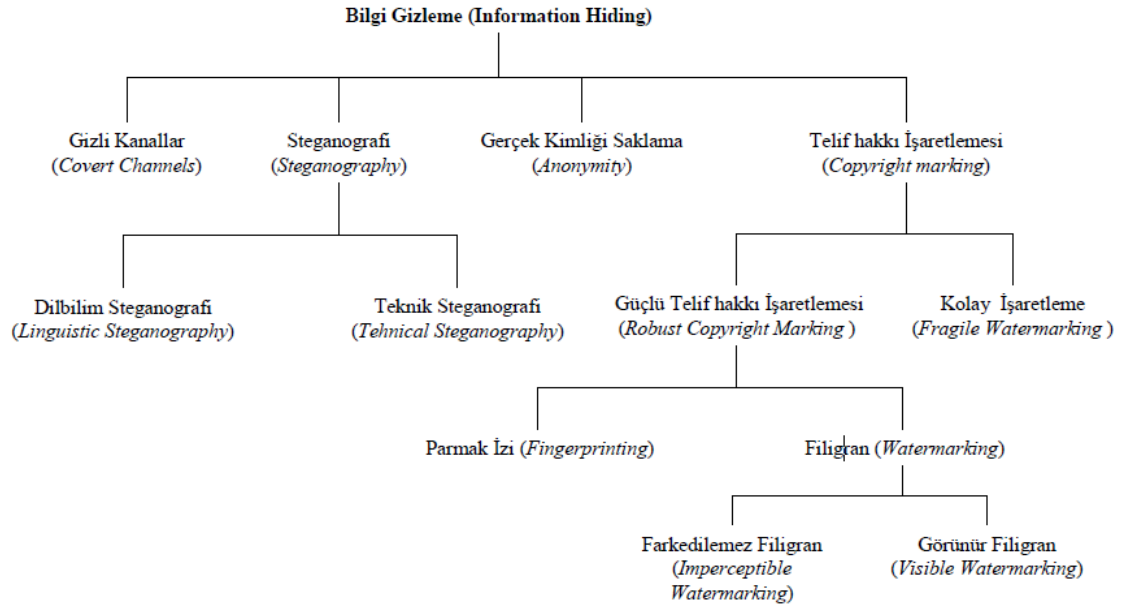
Bilgi gizleme iki kiři arasında yapılan iletiřimin bir üçüncü kiři tarafından fark edilmeyecek řekilde gerekleřtirilmesidir. Bilgi gizlenmenin amacı, iletiřimimizdeki veriyi veya iletiřiminin amacını saklamaktır. Bilgi gizleme, gönderilecek bilginin önemli olduđu birçok alanda sıklıkla kullanılmaktadır [24].

Askeri ve istihbarat birimleri, aralarındaki iletiřimin güvenli olmasını, gönderdikleri gizli verilere başka kiřilerinin erişmemesini isterler. İçerik řifrelense bile, modern savaş sahalarında bir sinyalin yakalanmasıyla saldırgan bu sinyale saldırabilir ve bilgiyi ele geçirebilir[25]. Bu nedenle, askeri iletiřimlerde sinyalin düşman tarafından bulunmasını zorlařtıran çeřitli bilgi gizleme teknikleri kullanılmaktadır.

Suçlular da kendi aralarındaki iletiřimin güvenlik güçleri tarafından anlařılmaması için çeřitli yöntemler kullanmaktadırlar. Örneğin cep telefonları frekanslarını kendi aralarındaki iletiřim için düzenleyebilmekte ve diđer kiřiler bunları duyamamasını sađlamaktadırlar. Buna karşılık olarak güvenlik güçleri de bu iletiřimi ele geçirebilmek için karşı yöntemler geliřtirmiřtir [26].

4.1. Bilgi Gizlemenin Alt Alanları

İletiřimin gizli bir řekilde gerekleřtirilebilmesi için çeřitli yöntemler geliřtirilmiřtir. Bilgi gizlemenin sınıflandırılması Şekil 1.1.'de gösterilmektedir [27]. Bu sınıflandırma, bilgi gizleme konusunda yapılan ilk alıřtay'da üzerinde alışılarak kabul edilmiřtir [28].



Şekil 4.1. Bilgi gizleme yöntemlerinin sınıflandırılması

4.1.1. Gizli Kanallar (Covered Channels)

Bilgi gizlemenin ilk alt basamağı olan gizli kanallar tanımlanmıştır. Gizli kanallar iki kişi arasında gizli bilgilerin el değiştirmesi için iletişimi sağlayan kanaldır [29].

Gizli kanal kurulması iki kişinin karşılıklı anlaşmasını gerektirmektedir. Gizli kanalların amaçları, iletişimimizdeki veriyi saklamaya çalışmak ve iletişiminin amacını saklamaktır. Böylece; gerçek veri transferi, dikkatsiz gözlerle zararsız ve kanuna uygunmuş gibi gözükecek ve veriyi karıştırmak için ayrı bir şifreleme yapılmasına gerek kalmayacaktır [30].

4.1.2. Gerçek Kimliği Saklama (Anonymity)

Diğer bir alt alan olan gerçek kimliği saklama, veri gönderimi sırasında gerçek kimliği saklayarak, bilginin bilinmeyen ya da anlaşılamayan biri üzerinden gidiyor olduğunu izlenimi verilerek gönderilmesidir. Bu şekilde bilgi zarar görmeden gönderilebilmektedir. Fakat ağlar üzerinde bilinmeyen kullanıcı olayı ağ yöneticilerinin daha fazla dikkatini çekmekte ve bilgi güvenliği tehlikeye girmektedir. Bu yüzden sadece çok gerektiği durumlarda kullanılması uygundur [31,32].

4.1.3. Telif Hakkı İşaretlemesi (Copyright Marking)

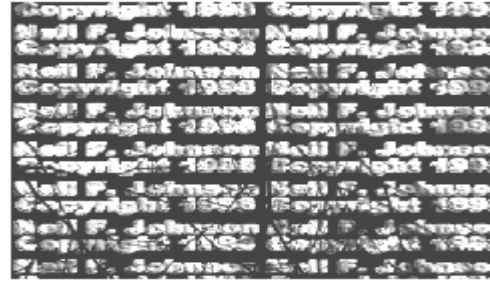
Telif hakkı işaretlemesinde ise orijinal dosyanın korunması amacıyla dosyanın içine bazı bilgiler gizlenmektedir. Bunlar; dosyaların üretildiği tarih, telif hakkı sahibi, üreticiye nasıl ulaşılabilceği gibi bilgileri içermektedir. Bu yöntemler steganografi ile beraber kullanılmaktadır. Telif hakkı işaretlemesi, sayısal görüntülerde sayısal filigran olarak kullanılmaktadır [33]. Filigran, bir çeşit gizli damga baskısıdır. Kâğıt banknotlar üzerindeki gizli damgalar buna örnek olarak gösterilebilir. Bunlar ancak ışığa tutularak bakıldıklarında görülebilmektedirler.

Modern steganografi uygulamalarında kullanılan filigranlar ise görüntü ve ses dosyalarında kopyalamayı önlemek amacıyla damgalar bırakmaktadırlar [34]. Bu damgalar özel programlar tarafından okunabilmekte ve dosyaların üretildiği tarih, telif hakkı sahibi, üreticiye nasıl ulaşılabilceği gibi bilgileri içermektedir.

Filigran ile korunmuş görüntüler parlaklık ve zıtlık (kontrast) ayarlarının değiştirilmesi, özel filtrelerin kullanılması, kâğıda baskı ve tarama gibi birçok yöntemle karşı koyabilmektedir. Fakat gelişen teknolojiyle birlikte ortaya çıkartılan bazı yeni programlar kullanılarak bu filigran aşılabilmektedir. Sayısal filigranlar ikiye ayrılır. Bunlar;

- Görünür filigran (visible watermark)
- Görünmez filigran (invisible watermark)

Görünen filigranlar insan gözünün rahatlıkla görebileceği izlerdir. Örneğin paralar da bulunan ışığa tutunca görünen imgeler (TL. deki Atatürk resmi gibi), bir başka örnek ise televizyon kanallarında o görüntünün hangi kanal yada ajans tarafından çekildiğini gösteren ekranın köşesinde bulunan bir logodur. Bir görünür filigrana saldırı, ancak o kısmın kesilerek çıkarılmasıyla yapılabilir. Görünmeyen filigrana bir örnek ise; pasaportlarda bulunan kişiye ait seri numarasının fotoğrafın içerisine de gömülmesidir. Herhangi biri elde ettiği bir pasaporta kendi resmini yapıştırdığı zaman özel tarayıcılarla fotoğrafı tarandığında seri numarasının tutmadığı ya da olmadığı gözükcektir. Görünmeyen filigranların görünen filigranlara göre bazı avantajları vardır. Filigran yerleri belli değildir ya da filigran olup olmadığı fark edilmeyebilir. Filigranı tüm imge içine dağıtmak genel bir uygulamadır [35].



Şekil 4.2. Resmin tamamına filigran gömülmüş örnek.

Bu durum resmi kesme saldırılarına (cropping attacks) karşı biraz olsun koruma sağlar. Fakat dosya içerisine gömülecek olan bilgi ne kadar az ise saldırılara karşı o kadar güçlü ve güvenli olur. Bu, dosya içerisindeki tekrarlılığın (redundancy) azalması için gereklidir [36].

4.1.4. Steganografi (Steganography)

Steganografi bilgi gizleme yöntemlerinin en önemli alt dalıdır [37]. Bu yaklaşım, bir nesnenin içerisine bir verinin gizlenmesi olarak tanımlanabilir. Dilbilim ve teknik steganografi olarak ikiye ayrılmaktadır. Bu yaklaşımla ses, sayısal imge, video görüntüleri üzerine veri saklanabilir. Görüntü dosyaları içerisine saklanacak veriler metin dosyası olabileceği gibi, herhangi bir görüntü içerisine gizlenmiş başka bir görüntü dosyası da olabilir [38].

4.2. Steganografi

4.2.1. Steganografi Nedir?

Steganografi eski bir bilgi gizleme sanatıdır [39]. Steganografi kelimesi kökleri “στεγανος” ve “γραφειν”den gelen Yunan alfabesinden türetilmiştir. Tam olarak anlamı “kaplanmış yazı” (covered writing) demektir [40].

Steganografi’nin amacı gizli mesaj ya da bilginin varlığını saklamaktır. Taşınmak istenen mesaj bir başka masum görünüşlü ortamda saklanarak, üçüncü şahısların iletilen mesajın varlığından haberdar olması engellenir. Metin, ses, sayısal imge, video dosyaları üzerine veri saklanabilir. Bu veriler metin dosyası olabileceği gibi, herhangi bir görüntü

içerisine başka bir görüntüyü gizlemekte olasıdır. Yine aynı şekilde bir ses dosyasının içine bir metin dosyası da saklanabilmektedir [41,42].

Steganografi gizli bir iletişim sağlamaktadır. Amacı iki kişi arasındaki iletişimin bir üçüncü şahıs tarafından fark edilememesidir. Bilimsel ortamda Steganografi çalışmaları 1983 yılında Simmons tarafından “Prisoner Problem”’in [43] tanımlanması ile başlamaktadır. Bu problemde Alice ve Bob hapisanededir ve hapisaneden kaçmak için planlar yapmaktadırlar. Fakat bu planların gardiyan Willie’ye fark ettirilmeden yapılması gerekmektedir. Eğer Willie bunu fark ederse kaçma planları suya düşecektir. Bu nedenle de çeşitli gizli haberleşme yöntemleri geliştirilmesi gerekmektedir.

Bu yaklaşımda içine bilgi gizlenen ortama örtü verisi (cover-data) veya örtü nesnesi (cover-object), oluşan ortama da stego-metin (stego-text) veya stego-nesnesi (stego-object) denmektedir [44].

$$\text{Gizlenecek Mesaj} + \text{Örtü Nesnesi} = \text{Stego Nesnesi}$$

Steganografi şifrelemeye yakın olmasına rağmen şifrelemeden farklıdır. Şifreleme mesajın içeriğinin korunması ile ilgilenirken steganografi mesajın varlığının gizlenmesi ile ilgilenmektedir. Dolayısıyla steganografi bir şifreleme yöntemi değil şifrelemeyi tamamlayıcı bir öğedir [45]. Steganografi birçok alanda ve çeşitli amaçlar için kullanılmaktadır. Bunlar şöyle belirtilebilir [46,47]:

– **Askeri:** Askeri durumlarda iletişimin şifrelenmesi her zaman yeterli olmamaktadır. Şifrelenmiş bir bilginin gönderildiği düşman tarafından fark edilebilir. Buna karşılık iletişim steganografik yöntemlerle yapılırsa çok daha başarılı olacaktır. Bu nedenle şifrelemeye alternatif olarak kullanılabilir.

– **Filigran ve parmak izi:** Hem filigranlar hem de parmak izleri gizlendiğinde bunun belli olmamasına ve güvenli olmasına ihtiyaç duyarlar. Bu nedenle, bu işlemde steganografiden yararlanılmaktadır.

– **Sağlık alanı:** Bazı sağlık sistemleri görüntüleri ve bunlar hakkındaki açıklamaları bir yere gönderebilir ve orada saklayabilir. Bazen bu görüntüler ve açıklamalar birbirinden ayrılabilir ve bu da tehlikeli sonuçlara yol açabilir. Eğer açıklama bilgileri görüntünün içine saklanırsa böyle bir durum ortadan kaldırılır. Bu işlem için de steganografi kullanılmaktadır.

4.3. Steganografinin Alt Alanları

Steganografi, Dilbilim Steganografi (Linguistic Steganography) ve Teknik Steganografi (Technical Steganography) olmak üzere kendi içerisinde ikiye ayrılmaktadır [48]. Dilbilim Steganografi, taşıyıcı verinin metin olduğu steganografi koludur. Burada değişiklik yapmanın çeşitli yolları vardır. Bunlardan bazıları şöyledir:

- Grafik kullanılarak yapılabilir,
- Metnin yapısı değiştirilerek yapılabilir
- Ya da amacı sadece veriyi saklamak olan yeni bir metin yaratılabilir.

Dilbilim Steganografi’de kullanılan yöntemler ise şunlardır [49]:

– **Açık kodlar:** Gizli mesaj, açıkça okunabilir fakat zararsız bir mesaj haline gelir. Bu işlem; maskeleye, boş şifreler ve grid (ızgara) ile yapılmaktadır.

– **Şemagramlar:** Gizli mesaj, açık metnin ufak fakat gizli bir detayının içine gizlenmektedir. Bunun için grafiksel değişiklikler yapılmaktadır. Kullanılan yöntemler ise; farklı yazı tipleri kullanmak, eski daktilo yazılarını kullanmak, imgeler içinde boşluklar kullanmak vb’dir.

Teknik Steganografi, birçok konuyu içine almaktadır. Bunları bazı başlıklar altında toplayabiliriz;

– **Görünmez mürekkep:** Geleneksel hale gelmiş olan görünmez mürekkeple yazma yöntemidir.

– **Gizli yerler:** Kimsenin göremeyeceği gizli yerlere saklama (bavul, kasa vb.)

– **Microdot’lar:** Bilgiyi noktalar halinde sayfaya gizleme

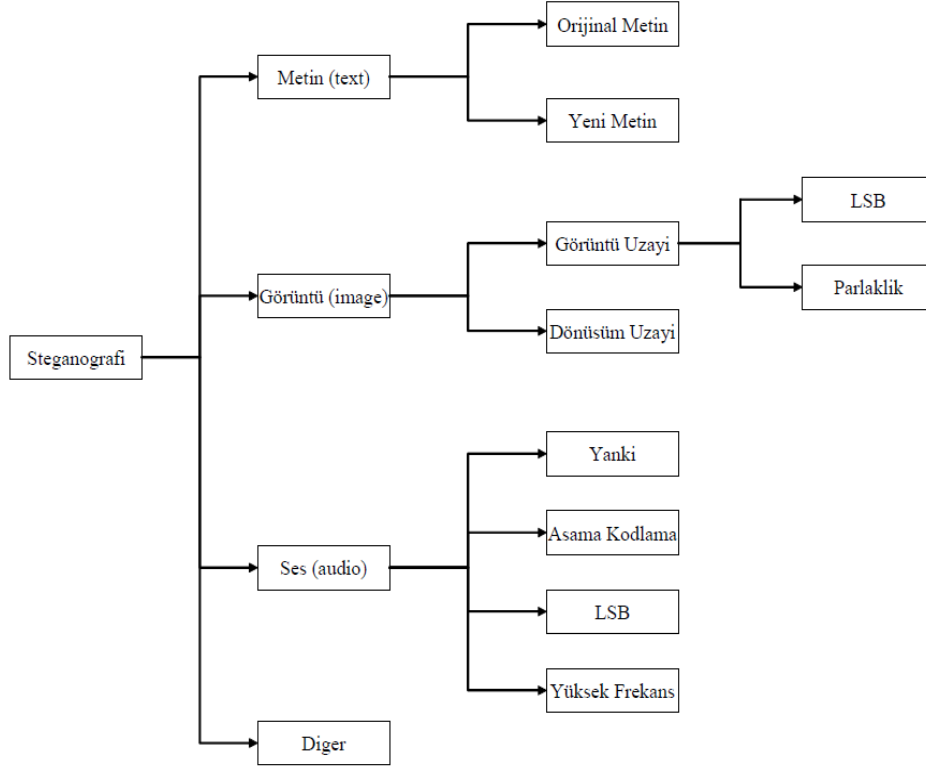
– **Bilgisayar tabanlı yöntemler:** Metin, ses, görüntü, imge dosyalarını kullanarak veri gizleme yöntemleridir.

4.4. Steganografinin Kullanım Alanları

Sayısal steganografi kullanım alanları açısından genel olarak üçe ayrılmaktadır. Bunlar aşağıdaki gibidir [50]:

- Metin (text) steganografi
- Görüntü (image) steganografi
- Ses (audio) steganografi

Yaygın olarak kullanılan sayısal steganografi yöntemlerinin sınıflandırılması Şekil 4.3’de verilmektedir.



Şekil 4.3. Sayısal Steganografi yöntemlerinin sınıflandırılması

4.4.1. Metin (text) Steganografi

Metin steganografi bilgi gizlenecek ortamın metin (text) olduğu steganografi koludur. Metin steganografinin uygulanabilmesi için çeşitli yöntemler vardır. Bunlar şu şekilde sınıflandırılabilir [51];

1. Açık Alan Yöntemleri (Open Space Methods)
 - ✓ Satır Kaydırma Kodlaması
 - ✓ Kelime Kaydırma Kodlaması
 - ✓ Gelecek Kodlaması
2. Yazımsal Yöntemler (Syntactic Methods)
3. Anlamsal Yöntemler (Semantic Methods)

4.4.1.1. Açık alan yöntemleri

Bu yöntemler, anormal gözükmeyen iki kelime arasında ekstra boşluklar ve satır sonu boşlukları ile çalışmaktadır. Bununla birlikte açık alan yöntemlerinin ASCII kodları ile kullanılması daha uygundur. Açık alan yöntemlerinde kullanılan kodlama yöntemleri şu şekildedir.

- **Satır kaydırma kodlaması**

Bu yöntemde metin satırları düşey olarak kaydırılarak gömülecek mesajın kodlanması sağlanır. Gömülmüş kelime yine metin dosyası ya da Windows Bitmap (BMP) [52] dosya olarak açılabilir. Aşağıdaki metinde ikinci satır 1/300 inch yukarıya kaydırılmıştır. Fakat gözle anlaşılır bir fark yoktur. Bu yapılan “0” ya da “1” ile tanımlanarak kodlama işlemi gerçekleştirilir.

- **Kelime kaydırma kodlaması**

Bu yöntemde metnin satırları yatay olarak kaydırılarak dokümanın tek olarak kodlanması sağlanır. Gömülmüş kelime yine metin dosyası ya da BMP dosyası olarak açılabilir. Bu yöntem, dokümana uygulandığında yakın kelimeler arasında çok ta fark edilmeyen boşluklar ortaya çıkmaktadır. Bu oluşan boşluklardan dolayı dokümanın kodunun çözülmesi için eski belgeye de ihtiyaç vardır.

- **Gelecek kodlaması**

Bu kodlama tekniği hem metin belgelerine hem de bitmap dosyalara uygulanabilmektedir. Burada kelimelerin yerleri ve bazı harflerin boylarıyla oynanmakta ve ASCII kodlarında değişiklik yapılmaktadır.

4.4.1.2. Yazımsal yöntemler

Bu yöntem, dokümanı kodlamak için noktalama işaretlerini kullanır [53]. Örneğin aşağıdaki iki cümle ilk bakışta aynıymış gibi gözükmektedir, fakat dikkatlice bakıldığında ilk cümlelerin fazladan bir ‘,’ işareti içerdiği görülmektedir. Bu yapıların biri “1”, diğeri de “0” olarak belirlenmekte ve kodlama işlemi bu şekilde gerçekleştirilmektedir.

“bread, butter, and milk”

“bread, butter and milk”

4.4.1.3. Anlamsal yöntemler

Bu yöntem W. Bender tarafından ortaya atılmıştır. Bu yöntemde eşanlamlı kelimelere birincil ve ikincil değerler atanmaktadır. Sonra bu değerler “1” ve “0” olarak binary’e dönüştürülmektedir. Örneğin *“big”* kelimesi birincil, *“large”* kelimesi de ikincil olarak işaretlenmiş olsun. Birincil “1”, ikincil de “0” olarak binary’e çevrilmiştir [54].

4.4.2. Görüntü (Image) Steganografi

Sayısal imgeler dağıtımı en kolay ve internette hemen her sayfada karşılaşılabilecek dosyalardır. Kullanıldıkları formatlara göre farklılık göstermekle birlikte steganografi uygulamalarında en yaygın kullanılan ortamlar imge dosyalarıdır. Bu nedenle steganografi konusunda yapılan çalışmalar ve geliştirilen teknikler ağırlıklı olarak imge steganografi çerçevesinde yer almaktadır. Görüntü dosyalarının içerisine bir metin gizlenebileceği gibi bir imge dosyasının içine bir başka resmi de gizlemek mümkündür. Gizli bilgiyi bir resme gömme (yada gizleme) işleminde iki dosya söz konusudur [55]. Kapak imge ya da örtü verisi (cover image) olarak adlandırılan ilk dosya, gizli bilgiyi saklayacak imge dosyasıdır. İkinci dosya ise gizlenecek bilgi olan mesajdır. Bu mesaj da stego olarak isimlendirilmektedir. Mesaj, açık metin (plain text), şifreli metin (chipher text), başka imgeler veya bit dizisi içinde saklanabilecek başka bir şey olabilir. Gömme işlemi sonucunda kapak imge ve gömülü mesajın oluşturduğu dosyaya “stego imge” adı verilir. Birçok farklı yöntem kullanılarak imgelerde bilgi gizlenebilmektedir.

Kullanılan yöntemler, gömme işlemi sırasında kullandıkları veri dikkate alınarak iki başlık altında toplanabilmektedir [56].

1. Uzaysal / Görüntü Alan Tekniği (Spatial / Image Domain Technique)
2. Frekans / Dönüşüm Alan Tekniği (Frequency / Transform Domain Technique)

Uzaysal Alan veya Görüntü Alan olarak adlandırılan teknik, gömme işleminde imge dosyasındaki veriyi doğrudan kullanılır. Gömme işlemin de bilgiyi gizlediği veri kümesi piksel değerlerini temsil eden kısımdır. Bu tekniğe örnek olarak yaygın olarak kullanılan En Önemsiz Bite Ekleme (Least Significant Bit Insertion - LSB) yöntemi gösterilebilir.

Frekans Alan veya Dönüşüm Alan olarak bilinen teknik ise kapak verideki değişimler üzerinde gömme işlemini uygular. Dönüşüm Alan tekniğine örnek olarak ise JPEG formatlı imge dosyalarına veri gömme işleminde kullanılan algoritmaları verebiliriz. Bu algoritmalar JPEG sıkıştırma sırasında kullanılan DCT katsayıları üzerinde veri gömme işlemini uygular [57].

4.4.2.1. Görüntü Dosyalarında Steganografik Yöntemler

Görüntü Dosyalarında bilgiyi gizlemek için kullanılan çeşitli yöntemler vardır. Bu yöntemler 3 gruba ayrılabilir [58];

Değiştirmeye dayalı yöntemler: Bu grup yöntemlere LSB Yöntemi ya da Amplitude (Genlik) Modülasyonu kullanılarak bilgi gizleme verilebilir. Burada bilgi gizlemek için renk değerleriyle oynanabilir ya da palet değiştirilebilir. Renk değerleriyle oynama en basit yöntemdir. Renk değerlerinin düşük anlamlı bitleri ile gizli verinin bitleri değiştirilir. Değişim, insan gözü tarafından algılanmaz. Gizli veri, “*gürültü (noise)*” olarak resme eklenir. Bu yöntem yüksek oranda veri gömme şansı verir, fakat imge üzerinde yapılacak değişimlere karşı oldukça hassastır. Palet ile oynamada ise, renk bilgilerinin palet üzerinde tutulduğu imge dosyaları kullanılır. Paletteki sıralama değiştirilir. Bunun sonucunda imge bozulabilir. Ayrıca imge türü değiştirildiğinde tüm yapılanlar yok edilir

İşaret işlemeye dayalı yöntemler: Bu yöntemler çeşitli dönüşümlerin kullanıldığı yöntemlerdir. DCT, DFT gibi dönüşümler kullanılabilir. İşaret işlemeye dayalı yöntemler imge üzerinde yapılan değişikliklere karşı da dayanıklıdır fakat resmi bozabilirler. İmgede bozulma olup olmayacağı da ancak işlem sonrası anlaşılabilir. Ayrıca, her 64 adetlik bloklara 1 bit gömülebilmesi, saklanabilecek veri miktarını önemli oranda düşürmektedir.

Spektrum yayılmasına dayalı yöntemler: Tayf (Spektrum) yayılmasına dayalı yöntemler de son yıllarda oldukça fazla kullanılmaya başlanmıştır. Tayf yayılması askeri iletişimde oldukça yoğun kullanılmaktadır. Bu yöntemde gönderilmek istenen mesaj ihtiyaç duyduğu frekans bandından çok daha fazlasına dağıtılır. Üçüncü bir kişi araya girip bir ya da birden fazla frekans bandında bozulmalara neden olsa bile, alıcı geri kalan frekans bantlarındaki bilgiler ile asıl mesajı elde edebilmektedir. Gizli mesaj birden fazla bantta yayılarak resme gürültü olarak eklenebilir.

Yukarıdaki yöntemleri kullanarak bilgi gizleyen steganografik algoritmalarından en yaygın olarak kullanılanları şunlardır [59];

- Patchwork Algoritması
- Amplitude (Genlik) Modülasyonu kullanılarak bilgi gizleme
- SSIS (Spread Spectrum Image Steganography) Yöntemi
- Frekans Domaini İçine Veri Saklanması
- Son Bite Ekleme (LSB-Least Significant Bit Insertion) yöntemi

4.4.2.1.1. Patchwork Algoritması

Bender tarafından ortaya atılan ve halen sıklıkla kullanılan algoritmadır. Bu algoritma, bilgiyi Gauss dağılımı gösteren bir istatistiğe sahip örtü verisinin içine gizlemeyi amaçlayan bir istatistiksel yöntemle dayanır [60,61]. Bu algoritma genelde filigran (watermarking) uygulamalarında kullanılmaktadır. Bu algoritma genellikle 256 bit gri-seviye (gray-scale) için kullanılmaktadır.

İmge içinde rasgele olarak iki nokta seçilir (A ve B). i a , A noktasının parlaklığı, i b ise B noktasının parlaklığıdır. Bir resmi şifrelemek için 4 adımda işlem yapılır.

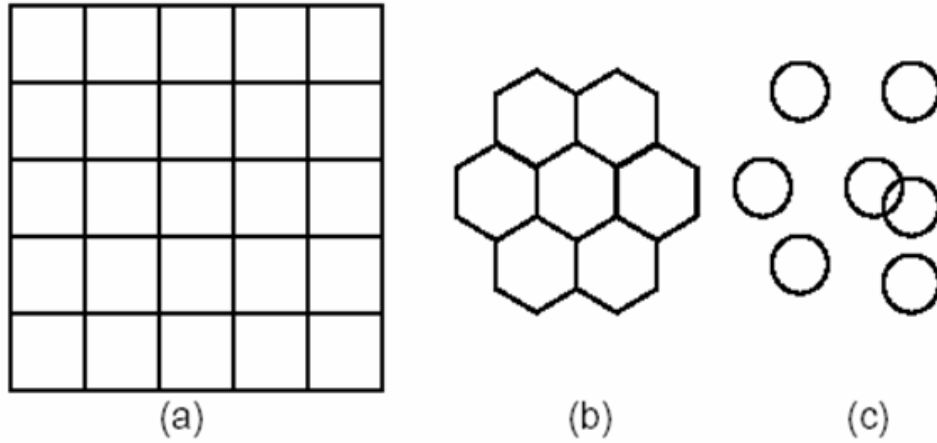
Adım 1: (a , b) i a b çiftini seçmek için sahte rasgele (pseudo random) numara üretici ile bir belirli anahtarın kullanılmasını gerektirir.

Adım 2: a parçasının parlaklığı δ 1 kadar artırılır.

Adım 3: b parçasının parlaklığı ise aynı δ kadar azaltılır.

Adım 4: Son adımda ilk üç adım n için tekrarlanır (n 'in değeri 10.000 civarındadır)

Burada yama (patch) şekilleri de oldukça önem kazanmaktadır. Olası üç adet tek boyutlu yama şekli vardır. Eğer keskin kenar içeren küçük yamalar seçersek, yamanın enerjisi görüntü analizinin yüksek frekanslı kısmı içerisinde yoğunlaşacaktır. Fark edilmesi oldukça zordur fakat filtreleme sonucunda kolaylıkla elde edilebilir. Diğer bir olasılık yumuşatılmış kenarlar içeren yamalar kullanılmasıdır. Bu durumda bilgiler düşük-frekans analizi içinde kalacaktır. Üçüncü olasılık ise ilk iki olasılığın birleştirilmesidir. Bu şekilde yamanın enerjisi dağıtılmaktadır. Şekil 3.5. (a)'da doğrusal bir kafes biçimi kullanılmıştır. Fakat bu pek tercih edilen bir yöntem değildir. Şekil 3.5. (b) a'ya alternatif olarak gösterilmiştir. Fakat en tercih edilir çözüm Şekil 3.5. (c)'de verilmektedir. Buradaki yamalar rasgele olarak dağılmakta ve seçilebilmektedir. Akıllıca bir dağılımla her türlü çözünürlükte iyi sonuç verebilecektir [62].



Şekil 4.4. Yama çeşitleri

4.4.2.1.2. Amplitude (Genlik) Modülasyonu Kullanılarak Bilgi Gizleme

Genlik modülasyonu kullanılarak işaret bitleri mavi kanaldaki piksel değerleri değiştirilerek gömülür. Bu değişimler ışığın oranına ve bitin değerine bağlı olarak artırma ya da eksiltme yoluyla yapılmaktadır [63].

s ; saklanacak tek bir bit;

$I = \{R, B, G\}$ görüntü;

$p(i, j)$; I görüntüsü içerisinde sahte rasgele (pseudorandom) olarak seçilmiş bir pozisyon; K 'da üretilen anahtar olarak tanımlanmaktadır. Gizlenecek bit $L = 0.299R + 0.587G + 0.114B$ olmak üzere B mavi kanal (blue channel)'ın değiştirilmesiyle p pozisyonuna saklanır. Gizlenen bitleri sırasıyla geri getirmek için, örtü verisinin (cover data) ilk renk değerlerinin tahmin edilmesi gerekmektedir. Bu tahmin, $p(i, j)$ 'nin komşularının mavi kanal (B) değerlerinin lineer kombinasyonuna dayanmaktadır. En iyi performansın çapraz komşular kullanılarak elde edileceği düşünülmektedir. Tahmini değer şu şekilde hesaplanmaktadır. Burada c değeri, çapraz şekilde olan komşuların uzunluğudur. Gizlenen bitleri geri getirmek için tahmini değer ile pikselin şu anki değeri arasındaki fark alınır [64].

4.4.2.1.3. SSIS (Spread Spectrum Image Steganography) Yöntemi

SSIS yöntemi, sayısal görüntünün içindeki bilgi bitlerinin işaretleme kalitesini, saklama ve geri getirme işlemlerinin gözlemleyen biri tarafından fark edilemeyecek şekilde

yapılması yeteneđi sađlar [65]. Gizli bitlerin elde edilmesi iin orijinal grntye ihtiyaı yoktur. SSIS yntemi tayf (spectrum) yayılım iletiřimi, hata kontrol kodlaması, grnt iřleme gibi tekniklerle birleřtirilebilmektedir. Bu dřnce tarzıyla saklanacak bilgi bir grlt (noise) iine konularak grnt ierisine yerleřtirilir. Grltnn dřk gte olmasından ve kod-zme iřleminden dolayı mkemmel deđildir [66].

Adım 1: Mesaj seime bađlı olarak $key1$ ile řifrelenmekte

Adım 2: Sonra dřk oranlı hata kontrol kodu (error control code-ecc) ile kodlanarak, m kodlanmış mesajı retilmektedir.

Adım 3: Gnderici; aynı zamanda n sıralamasına sahip bir yayılım retmek iin $key2$ 'yi sađlar.

Adım 4: Daha sonra bu iki deđer (m ve n) bir modlasyon iřlemine girer ve s gml sinyali elde edilir.

Adım 5: Bu gml sinyal bir $key3$ ile birleřtirme (interleaving) iřlemine tabi tutulur.

Adım 6: Daha sonra rt verimiz (cover data) olan f ile iřleme girerler.

Adım 7: Sinyal orijinal rt verimizin (f) iine yerleřtirilerek stegoimage elde edilir.

Adım 8: Son olarak ta bu řekilde alıcıya gnderilir.

4.4.2.1.4. Frekans Domaini İine Veri Saklanması

Yine filigran (watermark) teknolojileri iin kullanılan bu yntem grntlerin dnřtrlmesi (transform) temeline dayanmaktadır. Grnt dnřtrlmesi iin genellikle ayrık kosins dnřm (Discrete Cosine Transform- DCT) kullanılmaktadır. Bunun dıřında kullanılan dnřm algoritmaları ise; Ayrık Fourier Dnřm (DFT), Walsh dnřm ya da Wavelet (dalga) dnřmdr [67]. Bu teknik grnt zerinde bazı DCT katsayıları hesaplanarak bilgiye eklenip gizlenmesi iin kullanılır.

4.4.2.1.5. Son Bite Ekleme (Least Significant Bit Insertion-LSB) Yntemi

En nemsiz bite ekleme yntemi (Least Significant Bit Insertion Methods) [68] yaygın olarak kullanılan ve uygulaması basit bir yntemdir. Fakat yntemin dikkatsizce uygulanması durumunda veri kayıpları ortaya ıkmaktadır. Bu yntemde; resmi oluřturan

her pikselin her byte'nın en önemsiz biti olan son biti değiştirilerek o bitin yerine gizlenmesini istediğimiz verinin bitleri sırasıyla verinin başlangıcından itibaren birer birer yerleştirilmektedir. Burada her sekiz bitin en fazla bir biti değişikliğe uğratıldığından ve eğer değişiklik olmuşsa da değişiklik yapılan bitin byte'ın en az anlamlı biti olmasından dolayı, ortaya çıkan steganogramdaki (= örtü verisi + gömülü veri) değişimler insan tarafından algılanamaz boyutta olmaktadır. İmgelerin özelliklerine göre son bite ekleme yönteminin çalışma şekilleri aşağıda verilmiştir.

4.4.2.1.5.1. Gri seviye imgeler üzerinde LSB yönteminin uygulanması

Gri-seviye imgelerde her piksel, 0 (siyah) ile 255 (beyaz) arasında tam sayı değer alabilen 1 byte ile temsil edilmektedir. 0-255 arasındaki değerler gri'dir ve bundan dolayı bir resme ait tam sayı "*gri ton seviye*" (gray level) olarak isimlendirilmektedir [69].

Örneğin, renk değeri 182 olan bir pikselin içine ikilik sayı sistemindeki 1 değeri saklandığında oluşan piksel ve renk değeri yukarıda gösterilmektedir. Yukarıdaki renklerden de görüleceği gibi iki renk arasında gözle fark edilemeyecek kadar az bir değişim vardır. Son bitin 1 ya da 0 olması gözle görülebilir bir fark yaratmamaktadır [70].

4.4.2.1.5.2. 8-bit Renkli İmgeler ve LSB yönteminin uygulanması

8 bitlik görüntülerde piksel başına 1 byte kullanılmaktadır. 8 bitlik görüntüler renk sınırlaması yüzünden çok iyi bir sonuç vermemektedir. Saklanacak bilgi, saklama ortamını çok fazla değiştirmeyecek şekilde dikkatlice seçilmelidir. Orijinal görüntüde son bite ekleme işlemi yapıldığında, renk girişi göstergeleri değişmektedir. 8 bitlik görüntülerde 4 basit renk (WRBG) kullanılmaktadır. Bunlar; beyaz (White-W), kırmızı (Red-R), mavi (Blue-B) ve yeşildir (Green-G). Bu renklerin renk paletinde karşılık gelen girişleri ise sırasıyla

0 (00)

1 (01)

2 (10)

3 (11) şeklindedir.

Örnek olarak verilen orijinal görüntü pikselleri “Beyaz, beyaz, mavi, mavi” (00 00 10 10) ise 10 sayısının ikilik (binary) tabandaki karşılığı olan 1010 değeri bu piksellere gizlendiğinde, yapılan değişiklikler sonucunda görüntünün yeni piksel değerleri aşağıdaki gibi elde edilmektedir.

01 00 11 10

Bu değerler de renk paletinde sırasıyla kırmızı, beyaz, yeşil ve mavi değerlerine karşılık gelmektedir [71]. Piksellerin renk değerleri oldukça değiştiğinden, gözle fark edilebilecektir ve bu kabul edilemez bir durumdur. Veri gizleme uzmanları bu nedenle 8 bitlik renkli görüntüler yerine gri-seviye görüntülerin kullanılmasını daha uygun bulmaktadırlar [72].

4.4.2.1.5.3. 24-bit Renkli İmgeler ve LSB yönteminin uygulanması

24 bit imgeler bir piksel başına 3 byte kullanmaktadır. Her pikselin rengi “Kırmızı (red), Yeşil (green), Mavi (blue)” olmak üzere üç ana renkten elde edilmektedir. Buna pikselin RGB değeri denmektedir. Her byte’ta son biti değiştirmek suretiyle bir piksel’de 3 bitlik bilgi saklanabilir. Yani 24 bit derinliğine sahip 1024x768 piksel boyutundaki bir imge, bilgi saklamak için kullanılabilir 2.359.296 bit (294.912 byte)’e sahiptir. Gizlenmek istenen mesaj, saklama işleminden önce sıkıştırılırsa çok daha fazla sayıda bilgi resmin içine gizlenebilir.

10010101 00001101 11001001 (149,13,201)

10010110 00001111 11001010 (150,15,202)

10011111 00010000 11001011 (159,16,234)

Orijinal görüntü bitleri yukarıdaki gibi verilen 3 pikselin içine “101101101” bilgisi gizlendiğinde oluşan yeni piksel değerleri aşağıdaki gibi olmaktadır.

10010101 0000110**0** 11001001 (149,12,201)

1001011**1** 0000111**0** 1100101**1** (151,14,203)

10011111 00010000 11001011 (159,16,234)

Yukarıdaki örnekte sadece 4 bitte değişiklik yaparak bilgi gizlenmektedir. Bu yöntemde en az değişikliği yaparak sonuca gitmek ve gizlenecek bilgi 9 bitten az ise hangi bitlerin yok sayılacağını belirlemek oldukça önemlidir [73].

4.5. Ses (Audio) Steganografi

İnsan işitme sistemi (Human auditory system-HAS) frekans aralığı yüzünden, ses sinyalleri içerisine bilgi gizleme oldukça uğraş gerektiren bir konudur. HAS 1/1.000'den daha büyük frekans aralığını fark edebilir. Aynı zamanda HAS nereden geldiği belli olmayan gürültülere de oldukça duyarlıdır. Ses sinyalleri üzerinde uğraşırken ses dosyalarının hangi karakteristiklere sahip olduklarını bilmemiz gerekmektedir. Ses dosyaları iki ana özelliğe sahiptirler:

- Basit nicelendirme metodu: Yüksek kaliteli sayısal seslerin 16-bit doğrusal nicelendirme ile ifadesinde en çok kullanılan yöntemdir. Bazı sinyal bozulmaları bu formatta ortaya çıkabilir.

- Geçici seçme oranı: Ses için en çok kullanılan oranlar 8 kHz, 9.6 kHz, 10 kHz, 12 kHz, 16 kHz, 22.05 kHz ve 44.1 kHz 'dir. Bu değer frekans aralığının kullanılabilecek en üst seviyesidir.

Bir diğer sayısal gösterim ise ISO MPEG-Audio formatıdır. Bu algılama ile ilgili bir formattır. Bu yöntemde sinyal istatistiği değiştirilir. Böylece ses korunur fakat sinyal değiştirilmiş olur. Ses dosyalarında veri gizleme yöntemleri ise şunlardır:

- Düşük bit kodlaması (Low-bit encoding)
- Aşama kodlaması (Phase coding)
- Taft yayılması (Spread spectrum)
- Yankı veri gizlemesi (Echo data hiding)

4.5.1. Düşük bit kodlaması

Görüntü steganografide kullanılan LSB ekleme yöntemiyle aynı şekilde gerçekleştirilir. Ses dosyasındaki verinin her baytının son bitine gizlenecek bilginin bir biti yazılır. Sonuçta oluşan değişiklik ses dosyasında gürültüye neden olmaktadır. Ayrıca dayanıksız bir yapısı vardır. Tekrar örnekleme veya kanalda oluşabilecek gürültü ile mesaj zarar görebilir veya yok edilebilir [74].

4.5.2. Aşama kodlaması

Aşama kodlaması yöntemi de imge dosyalarında uygulanan JPEG algoritması benzeri bir yapı taşımaktadır. Gömme işleminde ses dosyası küçük segmentlere bölünür ve her segmente ait aşama (faz) gizlenecek veriye ait aşama referansı ile değiştirilir. Aşama kodlaması prosedürü aşağıdaki gibidir [75].

- Ses verisi N adet kısa segmente bölünür.
- Her segmente Discrete Fourier Transform (DFT) uygulanarak aşama ve büyüklük (magnitude) matrisleri yaratılır.
- Komşu segmentler arasındaki aşama farklılıkları hesaplanır.
- Her segment için yeni bir aşama değeri bilgi gizlenerek oluşturulur.
- Yeni aşama matrisleri ile büyüklük matrisleri birleştirilerek yeni segmentler elde edilir.
- Yeni segmentler birleştirilerek kodlanmış çıkış elde edilir.

4.5.3. Taft yayılması

Gizleme işlemini ses sinyalinin kullandığı frekans taftı üzerinde yapmaktadır. Güçlü bir yapısı olamamakla birlikte seste gürültü meydana getirmektedir [76].

4.5.4. Yankı veri gizlemesi

Bilginin gizlenmesi taşıyıcı ses sinyali üzerine bir yankı eklenmesi ile sağlanmaktadır. Bilgi yankının gecikme miktarı, zayıflama oranı veya büyüklüğü gibi değerler kullanılarak gizlenir. İki farklı gecikme değeri kullanılarak insan kulağının

algılamayacağı düzeyde 0 veya 1'in kodlanması mümkündür. Her bitin kodlanması için sinyal segmentlere bölünür. Yankı veri gizlemesi yöntemi herhangi bir gürültüye neden olmamakta veya kayıplı bir kodlama kullanmamaktadır [77].

4.6. Kullanılan Diğer Ortamlar

Steganografi uygulamalarında yaygın olarak kullanılan text, görüntü ve ses dosyaları haricinde, sabit disklerdeki kullanılmayan alanlar, IP (Internet Protocol) paketlerinin ileride kullanmak üzere ayrılmış bölümleri gizli verinin saklanması için kullanılabilir. Yine aynı şekilde Html dosyaları, exe dosyaları vb. gibi dosyalar da içlerine veri saklamada kullanılabilir. İmge ve ses dosyalarına veri saklama yöntemleri insanın görme ve işitme sisteminin fark edemeyeceği ufak değişikliklerle bilgi gizleme mantığını temel almaktadır. Html ve exe gibi dosyala veri saklama yöntemleri ise bu dosyaların kendi formatlarındaki esneklikleri temel alarak çalışırlar.

Örneğin html dosyalarında etiketler (tag) kullanılmaktadır. Bu etiketlerin açma ve kapama şekilleri vardır. Bir metni şekillendiren iki etiket olduğunda bunları kaparken hangisinin daha önce kapandığı hangisinin daha önce açıldığı sayfanın görünümünde fark oluşturmaz. Örneğin:

`<tr><b>deneme</tr></b>` ile

`<tr><b>deneme</b></tr>` satırları aynı görüntüyü sağlamaktadır.

Ayrıca html dosyasında arada bırakılan boş satırların sayısı görüntüyü değiştirmemektedir. Bu durumda, bu alanlar veri saklama amacıyla kullanılabilir. Ancak bu yöntemlerin saklama kapasitesi düşüktür ve steganalitik yöntemlere karşı dayanıklılığı azdır. Exe dosyalarında da benzer mantıkla hareket edilmektedir. Komut setlerinde aynı işlevi gören farklı komutlar olabilmekte ve bunlardan hangisinin kullanıldığı oluşan exe dosyasının çalışmasında değişikliğe neden olmamaktadır. Bu durum veri saklama amacıyla kodlanabilir. Ancak yine burada da saklama kapasitesindeki düşüklük gündeme gelmektedir [78].

5. STEGANOGRAFI UYGULAMALARINDA KULLANILAN YÖNTEMLER

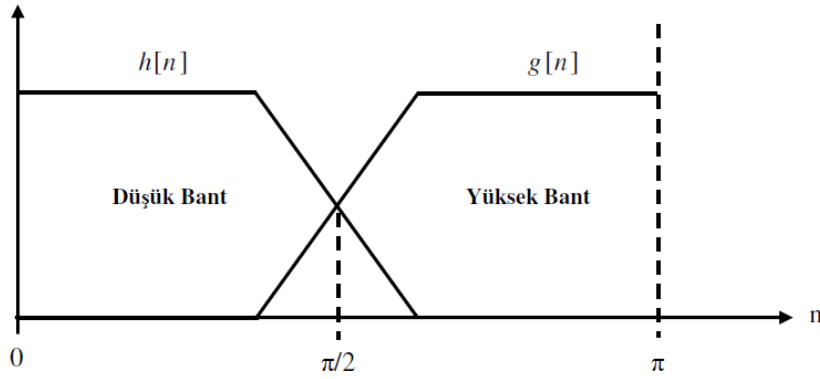
5.1. Ayrık Dalgacık Dönüşümü

Ayrık Dalgacık Dönüşümünün (DWT) temel fikri, tek boyutlu sinyaller üzerine uygulandığında daha kolay anlaşılabilir [79-82]. DWT, verilen sinyali iki alt-banda böler ve bunlar genellikle *yüksek frekans* ve *düşük frekans* alt-bantlarıdır. Bu bölme işlemine *ayrıştırma* denilir. Sinyalin kenar bileşenleri, büyük ölçüde yüksek frekans alt bandına ayrıştırılır. Sinyalin yüksek ve düşük frekans alt-bantlarına ayrıştırılması için sinyal sırasıyla bir dizi *yüksek-geçiren (YGF)* ve *düşük-geçiren(DGF)* filtrelerden geçirilir. Sinyalin farklı çözünürlükler üzerinde analiz edilmesi için farklı kesik frekans filtreleri kullanılır. Orijinal $x[n]$ sinyali yüksek-geçiren $g[n]$ ve düşük-geçiren $h[n]$ filtrelerinden geçirilir ve iki ile aşağı örneklenir. Aşağı örnekleme sonunda alt sinyallerin örnek sayıları yarıya düşer. Böylece, sinyalin en yüksek frekans bandı $\pi/2$ olur. Birinci seviyeli ayrıştırmayı oluşturur ve elde edilen yüksek-geçiren sinyalle düşük-geçiren sinyaller matematiksel olarak sırasıyla şu şekilde ifade edilebilirler:

$$Y_{Yüksek}[n] = \sum_k x[k]g[2n - k] \quad 5.1$$

$$Y_{Düşük}[n] = \sum_k x[k]h[2n - k]$$

Sinyal üzerinde birden fazla ayrıştırma yapılmak istenirse, yukarıdaki işlem alt-sinyaller üzerinde tekrarlanır. Yüksek-geçiren filtre ve düşük-geçiren filtrenin çıktılarına, *DWT katsayıları* denir ve bu DWT katsayıları kullanılarak orijinal sinyal yeniden geri elde edilebilir. Yeniden elde etme işlemine *Ters Ayrık Dalgacık Dönüşümü (TDWT)* denir.



Şekil 5.1. Filtreleme işleminden sonra sinyalin spektrum ayrışımı

TDWT işlemi, sinyali geri çatmak için ters bir sırada çalışır. Sinyaller her seviyede iki ile yukarı örneklenir ve yüksek-geçiren $g[n]$ ve düşük-geçiren $h[n]$ sentez filtrelerinden geçirilir ve sonra elde edilen her iki sinyal toplanır. Analiz ve sentez filtreleri birbirleriyle uyumlu bir *filtre bankası* oluştururlar. Bundan dolayı, her katman için geri çatma formülü şu şekilde olur:

$$x[n] = \sum_{k=-\infty}^{\infty} (Y_{Düşük}[k]h[2n-k] + Y_{Yüksek}[k]g[2n-k]) \quad 5.2$$

Filtre bankasını oluşturan $h[n]$ ve $g[n]$ filtrelerinin Fourier dönüşümleri olan $H(\omega)$ ve $G(\omega)$ fonksiyonları, dikgenlik koşulunu sağlamalıdır:

$$|H(\omega)|^2 + |G(\omega)|^2 = 1 \quad 5.3$$

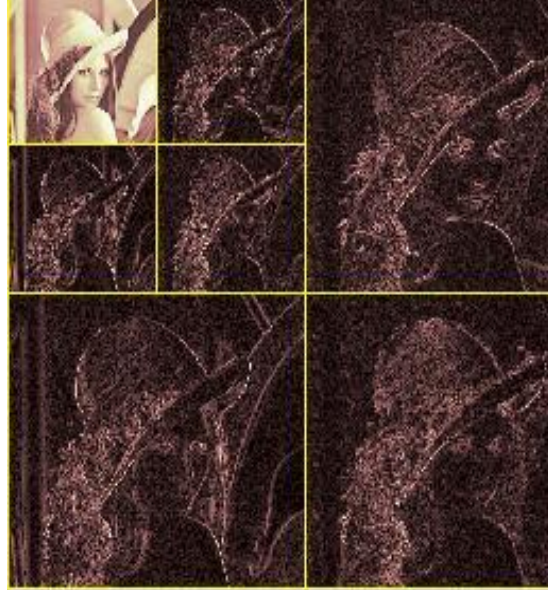
5.1.1. DWT'nin Karakteristikleri

Dalgacık ayrışımı resmi üç yönlü –yatay, dikey ve diyagonal– uzamsala ayrıştırır. Bundan dolayı, dalgacıklar insan görsel sisteminin (IGS) yön bağımlı özelliklerini çok dikkatli bir şekilde yansıtır [83]. Çoklu çözünürlük özeliğinden dolayı, ölçeklenebilirlik ve alçaltmaya dayanıklılık gerektiren uygulamalar için uygun olur. Bu yüzden, imgelerin aşamalı iletimine izin verir. Yüksek çözünürlük alt-bantları, resmin içindeki kenar ve doku örüntülerinin kolay bir şekilde bulunmalarını sağlar.

Dalgacık dönüşümü hesaplama yönünden etkindir ve basit evrişim filtresi kullanılarak uygulanabilir. Ayrıca dayanıklılık yönünden, iletme ve kod çözme hatalarına

karsı daha dayanıklıdır. Her ayrıştırma seviyesindeki düşük (DD) alt-bantların DWT genlik katsayıları daha büyük olur. DWT'nin genlik katsayıları diğer (DY, YD, YY) alt-bantlarda daha küçük olur. DWT'nin hesaplama karmaşıklığı doğrusaldır. Yani DWT algoritması $O(n)$ zamanda çalışır [84,85]. DWT resmin hem uzamsal hem de frekans bilgilerini içerir.





Şekil 5.2. Lena resmi üzerinde Haar DWT birinci ve ikinci seviye ayrıştırma işlemi

5.2. Ayrık Kosinüs Dönüşümü

Tipik bir kodlayıcı da blok bazlı Ayrık Kosinüs Dönüşümü kullanılır. 8x8 boyutundaki görüntü parçası bire bir dönüşüm kullanılarak frekans boyutuna taşınır. Bu dönüşüm sonucunda toplam enerjinin büyük bir bölümü az miktarda dönüşüm katsayısında toplanır. Dönüşüm katsayıları genelde sıkıştırma veya daha özel olarak damgalama ve farklı bir çok amaçla saklanır, kuvantalanır ve kodlanır. Basitlik ve hesaplama karmaşıklığını azaltmak için ayrık dönüşümler kullanılır. İki boyutlu DCT'nin taban vektörleri aşağıdaki gibi verilir.

$$c(k, l) = \alpha(k) \cos \frac{\pi(2l+1)k}{2N} \quad \begin{matrix} 0 \leq k \leq N-1 \\ 0 \leq l \leq N-1 \end{matrix}$$

5.4

$$\alpha(0) = \sqrt{\frac{1}{N}}, \quad \alpha(k) = \sqrt{\frac{2}{N}} \quad 1 \leq k \leq N-1$$

İki boyutlu DCT çifti, $C = \{c(k, l)\}$ olmak üzere reel değerli görüntü matrisi için $\mathbf{V} = \mathbf{CUC}^T$ ve $\mathbf{U} = \mathbf{C}^T \mathbf{VC}$ çözümünden elde edilir (86, 88). DWT kullanılarak dördüncü seviyeye kadar alt bant ayrışımından elde edilen alt bantların C matrisi yardımıyla DCT

dönüşümlerinin matematiksel gösterimi $IBl(k,l) = DCT\{IBl(u,v), B \in \{T,D,Y,K\}, 1 < l < 4\}$ şeklindedir [89].

5.3. Ayırık Fourier Dönüşümü (DFT)

Ayrık Fourier Dönüşümü aşağıdaki eşitlikteki gibi ifade edilir.

$$X_m = \sum_{k=0}^{N-1} x_k e^{\frac{-j2\pi mk}{N}} \quad 5.5$$

- Zamanın sürekli fonksiyonu olan sinyelimiz $f(t)$ zaman dizisi k ya dönüşmüştür.
- Sürekli zaman olan t , zaman indeksi veya örnek numarası olan k ya dönüşmüştür. ($k:0,1,2,\dots,N-1$ değerlerini alır).

Sinyalin uzunluğu N adet örneğe çevrilmiştir

- İntegral işlemi Toplam işlemiyle yer değiştirmiştir.
- Frekans fonksiyonu olan $F(\omega)$ frekans dizisi olan k X halini almıştır.
- Sürekli f frekans fonksiyonu $0,1,2,\dots,N-1$ değerlerini alan m frekans indeksi olmuştur [90,91]..

Frekans domeninden zaman domenine geri dönüşü sağlayan Ters Ayırık Fourier Dönüşümü de aşağıdaki gibi ifade edilir.

$$x_k = \frac{1}{N} \sum_{m=0}^{N-1} X_m e^{\frac{j2\pi mk}{N}} \quad 5.6$$

Ayrık Fourier dönüşümünde N adet örnek için Gerçel ve Sanal olmak üzere iki çeşit veri elde edilir. her birisinin sayısı $(N/2)+1$ dir. Bu iki kısım elde edilen Sinüs ve Kosinüs lerin genlik bilgilerini içerir ve bunlara frekans bileşenleri adı verilir. Gerçel kısımlar (**Re X []**) kosinüs bileşenlerin genliklerini, Sanal kısımlar (**Im X []**) ise Sinüs bileşenlerin genliklerini gösterir. Frekans bölgesi de zaman bölgesiyle aynı sinyali ifade eder ancak farklı bir biçimde gösterir. Bu şekilde fourier dönüşümü kullanarak zaman bölgesinden frekans bölgesine geçiş ayrıştırma, analiz veya ileri fourier dönüşümü olarak adlandırılır.

Frekans bölgesinden, zaman bölgesine geçiş ise sentez veya Ters Ayırık Fourier Dönüşümü olarak adlandırılır. Yukarıdaki formülden de hesaplanabilmesine rağmen daha anlaşılır olduğu için gerçel ve sanal kısımlar aşağıdaki gibi ayrı ayrı hesaplanabilir [92,93].

$$\text{Re } X[k] = \sum_{i=0}^{N-1} x[i] * \text{Cos}(2\pi ki / N)$$

$$\text{Im } X[k] = -\sum_{i=0}^{N-1} x[i] * \text{Sin}(2\pi ki / N)$$

5.7

5.4. EÖB Yer Değiştirme Yöntemi (LSB Replacement)

İmgelere veri gizlemenin en basit yaklaşımı EÖB yer değiştirme yöntemidir. Bu yöntemde imgenin EÖB'nin değiştirilmesi ile veri gömülebilmektedir. Yöntem ortalama olarak gizlenecek verinin yarısı kadar örtü imgesinin piksel değerinin değiştirilmesine neden olmaktadır. Örnek olarak gizli verimizin [0 0 1 1] olduğunu varsayalım. Gri seviyeli imge içerisinde seçilen 4 pikselin değeri aşağıdaki gibi olsun.

		<u>İkili Değeri</u>	<u>Onluk Değeri</u>
1 nci piksel	:	[0 1 0 1 0 1 1 0]	86
2 nci piksel	:	[1 0 0 0 1 1 0 0]	140
3 ncü piksel	:	[0 1 0 1 0 1 0 <u>0</u>]	84
4 ncü piksel	:	[1 0 1 1 0 0 1 <u>0</u>]	178

Yukarıdaki verilen piksellerin ikili değerinin EÖB ile gizli verinin bit değerleri karşılaştırıldığında sadece 3 ncü ve 4 ncü pikselin değerlerinin uyuşmadığı görülmektedir. Gizli veriyi gömmek için sadece 3 ncü ve 4 ncü piksel değerlerini 1 arttırarak 85 ve 179 yapmamız yeterli olacaktır. Bu durumda örtü imgemiz aşağıdaki gibi olacaktır.

		<u>İkili Değeri</u>	<u>Onluk Değeri</u>
1 nci piksel	:	[0 1 0 1 0 1 1 0]	86
2 nci piksel	:	[1 0 0 0 1 1 0 0]	140
3 ncü piksel	:	[0 1 0 1 0 1 1 1]	85
4 ncü piksel	:	[1 0 1 1 0 1 0 1]	179

Yukarıdaki örnekte gösterildiği üzere 4 gizli veri biti için örtü imgesi üzerinde 2 piksel değerinin değiştirilmesi ile saklanabilmektedir. Örtü imgesinde daha az piksel değişikliği ile gizli veri gizlenebilmektedir.

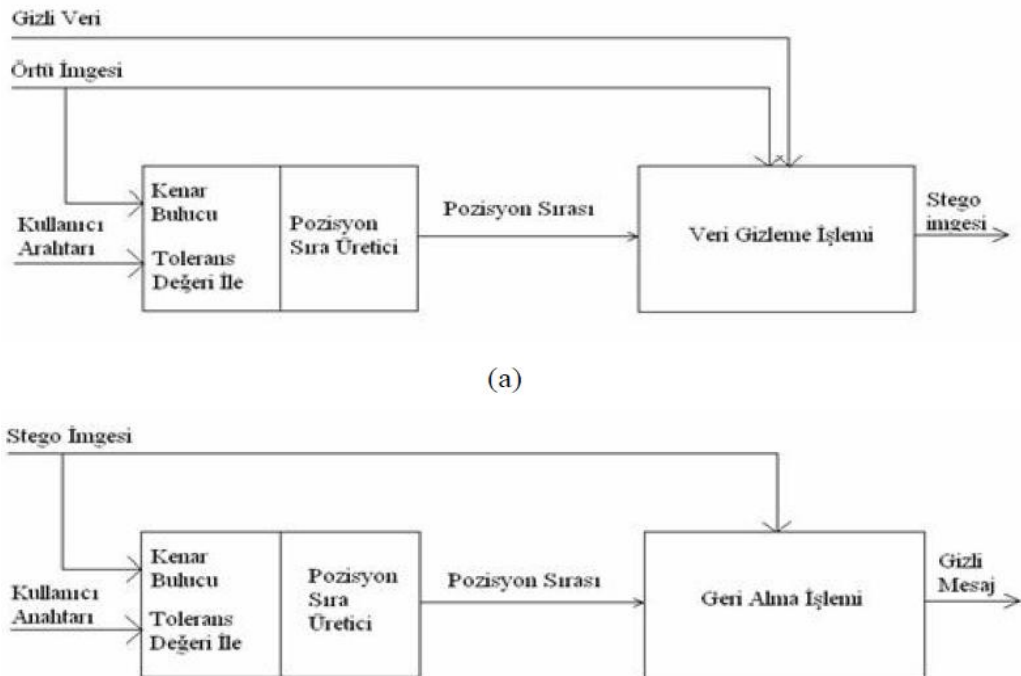
EÖB yer değiştirme yönteminin basitliğinin yanında örtü imgesinin kalitesinin bozulması insan görsel sistemi (HVS) tarafından da kolayca fark edilememektedir. Ancak EÖB yer değiştirme yöntemi kesme-yapıştırma, döndürme, sıkıştırma vb. basit saldırılara karşı çok hassastır. Ayrıca EÖB yer değiştirme yöntemi sonucu oluşan değişimler imge piksellerinin bağlantılı olmasından dolayı basit analizler ile tespit edilebilmektedir. Eğer gizlenecek veri, imge içerisinde bağlantısız yerlere gömülürse analizci tarafından daha az dikkat çekecektir. Bu nedenle EÖB yer değiştirme yönteminin zayıf yanlarını azaltmak için değişik çalışmalar yapılmıştır. Bunlardan birisi piksel steganografi yöntemidir. Piksel steganografi yönteminde yapılan araştırmalarda gizli verinin örtü imgesinde gömülebileceği en güvenli yerlerin başında en az benzer piksellerin; yani çizgilerin sonları, köşeler, ince çizgiler ve piksel değerlerinin çok süratli değiştiği alanlar gelmektedir [94].

Kenar piksel tabanlı steganografi yöntemlerinde gizli verinin, örtü imgesinde en fazla gürültüye maruz kalan bu bölgelere gömülmesi ile gizli verinin insan görme sistemi veya stegoanaliz yöntemleri ile tespit edilmesi zorlaştırılmıştır. Kenar piksel steganografisinde veri gömme işlemi θ (eşik seviyesi)'ne karşın kenar piksellerinin seçimi ile başlar. Seçilen piksellere veri gömme işlemi belirli bir sıra ile yapılır. Eşik seviyesine göre yapılan veri gömme işlemi:

$$OCB = \begin{cases} CB+1, & \text{Eğer } D \geq \theta \text{ \& CB tek ise \& SMB = 0} \\ CB+1, & \text{Eğer } D \geq \theta \text{ \& CB çift ise \& SMB = 1} \\ CB-1, & \text{Eğer } D \leq -\theta \text{ \& CB tek ise \& SMB = 0} \\ CB-1, & \text{Eğer } D \leq -\theta \text{ \& CB çift ise \& SMB = 1} \\ CB & \text{diğer durumlarda} \end{cases}$$

Formülde geçen OCB (çıkış örtü biti-output cover bit) değişim sonucu elde edilen stego imgesini, CB (örtü biti-cover bit) örtü imgesinin piksel değerini, D (uzaklık-distance) kenar piksellerin bulunmasında kullanılan dedektörün değeri ve SMB (gizli mesaj biti-secure message bit) gizli biti ifade etmektedir. Veri gömme işlemi yukarıdaki şartlara göre yapılmaktadır.

Stego imgesinde gizli veri seçilen piksellere belirli bir sıraya göre gömülmekte ve gizli veri alıcı tarafından seçilen piksellerin sıralaması yapıldıktan sonra tek mi çift mi olduğuna bakılarak geri alınabilmektedir. Örtü imgesine veri gizleme ve veriyi geri elde etme işleminin akış şeması Şekil-5.3 (a) ve Şekil-5.3 (b)'de gösterilmiştir [95].



Şekil 5.3. Kenar Steganografisi

(a) Gizli Veri Gömme İşlemi (b) Gizli Veriyi Elde Etme İşlemi

Kenar steganografisini en önemli avantajı belirlenen tolerans (eşik) değeri ile ikinci bir güvenlik oluşturmaları [96] ve gradyen (gradient) enerji EÖB analiz yönteminde gizli verinin uzunluğunun doğru olarak tespit edilememesidir [97]. Ancak örtü imgesinde mevcut kenar piksellerin sayısından dolayı fazla miktarda veri gömülememesi en büyük dezavantajıdır.

Örtü imgesinin bozulmasının en az seviyede tutulması maksadıyla yapılan çalışmalardan bir diğeri imge blokları içerisinde en benzer piksellerin değişimi ile sağlanmasıdır. Bu yöntem genellikle imge içine imge gizleme amacıyla kullanılır. Yapılan çalışmalarda örtü imgesinin bloklara ayrılarak blok içerisinde gizlenecek imge pikselleri ile blok pikselleri arasında yüksek oranda benzerlik sağlandığı görülmüştür. Bu işlem tüm gizli piksellerin gömülmesine kadar devam eder [98].

Örnek olarak 98 değerindeki gizlenecek piksel değerimiz bulunsun. Örtü imgesinin ilgili bloğunda gizlenecek piksele en yakın değerde pikselin arandığını ve 100 değerinde pikselin bulunduğunu varsayalım. 100 değeri 98 yapılarak gizlenecek imgenin bir pikseli örtü imgesine gizlenmiş olur. Gizlenen piksellerinin geri alma işlemi seçilen piksel değerlerinin bulunmasıyla elde edilmektedir.

Yapılan çalışmalarda bloklar içerisindeki arama uzayının çeşitliliğinden dolayı örtü imgesinin % 2-3 oranlarında bozulması ile gizli verinin gömülebileceği tespit edilmiştir [99]. Ancak gizlenecek verinin çok olduğu durumlarda arama uzayı azalacaktır. Ayrıca gizlenecek imge ile seçilen örtü imgesinin de uyumlu olması gerekmektedir. Eğer gizlenecek veri, imge yerine yazı dosyalarına gömülmek istediğinde kötü sonuçlar elde edilebilmektedir. Bir diğer hususta benzerliğin sağlanabilmesi için örtü imgesinin bloklarının kullanılması ile gömülecek verinin sınırlı kalmasıdır. EÖB yöntemlerinin örtü imgesinde yaptığı hasarın azaltılmasının yanı sıra ayrıca bir güvenliğin kazandırılmasına yönelik çalışmalar da mevcuttur. M.A.Khan, V.Potdar ve E.Chang [100] tarafından yapılan çalışmalarda gizlenecek veri matematiksel bir fonksiyona göre seçilmekte ve gizli veri ile ilişkilendirilmektedir. Seçilen pikseller ön aşamadan geçirilerek hepsinin çift yapılması sağlanmakta daha sonra veri bitleri ile uyuşmayan kısımlarda piksellerin tek olarak değiştirilmesi ile veri örtü imgesine gömülmektedir.

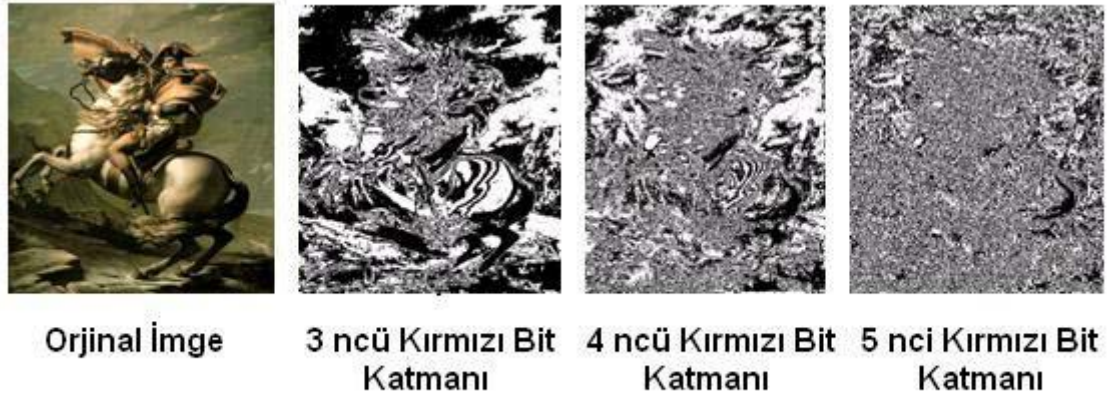
Örtü imgesinin ön işleme tabi tutulmasıyla örtü imgesinin bozulması azaltılmakta ve birlikte fazladan güvenlik elde edilebilmektedir. Ancak kesme, kırpma, yapıştırma gibi basit işlemler sonucunda gizli veride kayıplar olabilmektedir.

Sıradan EÖB yöntemlerinin dayanıklılığının geliştirilmesi amacıyla veri gizleme işlemi esnasında Fibonacci serileri de kullanılmıştır. Bu yöntemde seçilen pikseler ilk önce fibonacci değerlerine dönüştürülmekte ve gizli veri bu dönüşüm sonucunda ilgili piksele saklanmaktadır [101]. Geliştirilen yöntemde gizli verinin saklanması esnasında insan görsel sisteminin algılayamadığı hızlı değişen yerlerin kullanılması [102] yerine değişik bir strateji kullanılarak yerel varyans değerleri uygun olan bölgeler seçilmiştir.

Genel olarak imgeler içerisinde imge kapasitesinin yaklaşık %15'i kadar veri gizlenebilmektedir. Bit Katmanı Karmaşıklık Bölümleri (BPCS) yöntemi ile renkli imgeler içerisinde gizlenen veri oranının %50'ye kadar arttırılmaktadır. BPCS yönteminde renkli imgeler bit katmanlarına ayrılmaktadır. 24 bitlik BMP dosyaları için bu yöntemi uygularsak imge Kırmızı Yeşil Mavi (RGB) uzayında her bir renk için 8 bit katmana ayrılmış olmaktadır.

İmge = (İ-kırmızı-1, ..., İ-kırmızı-8, İ-Yeşil-1,..., İ-Yeşil-8, İ-Mavi-1, ...,İ-Mavi-8)

Şekil-5.4'te örtü imgesinin kırmızı bit katmanlarına ayrılmış durumu görülmektedir.

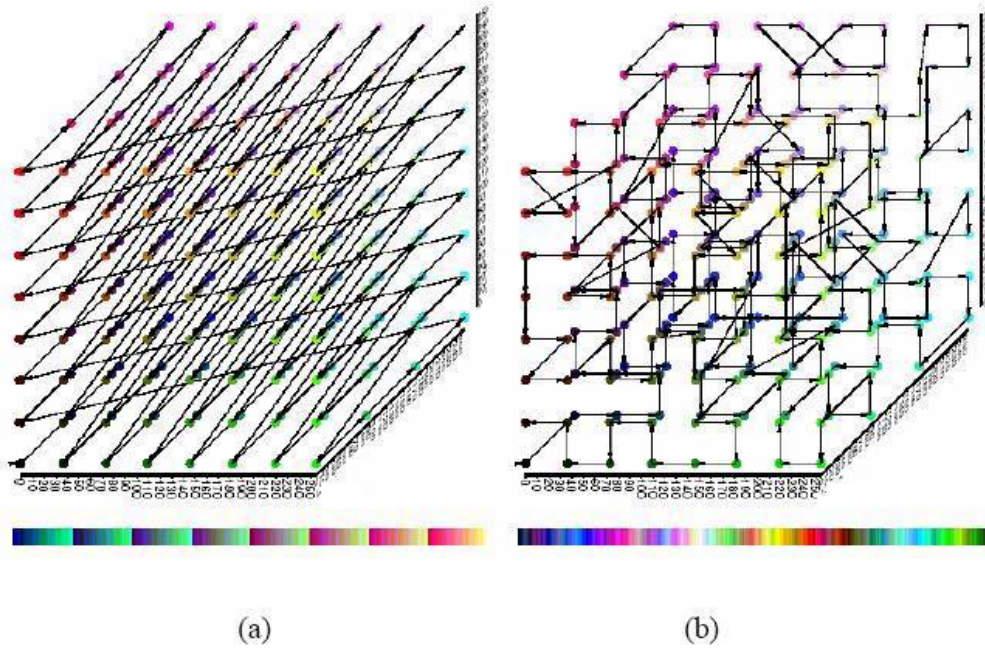


Şekil 5.4. Orijinal İmge ve İmgenin BPCS Kırmızı 3, 4, 5 nci Bit Katmanları

Şekil-5.4'te görüldüğü üzere bit katmanları önemliden önemsiz doğru arttıkça imgenin özelliğinden çok gürültüye benzer şekiller ortaya çıkmaktadır. Sıradan yöntemlerin yerine bozulmanın insan gözünün algılayamayacağı katmanlarda yaparak imgelerde gizlenecek bit oranının da arttırılması sağlanmaktadır.

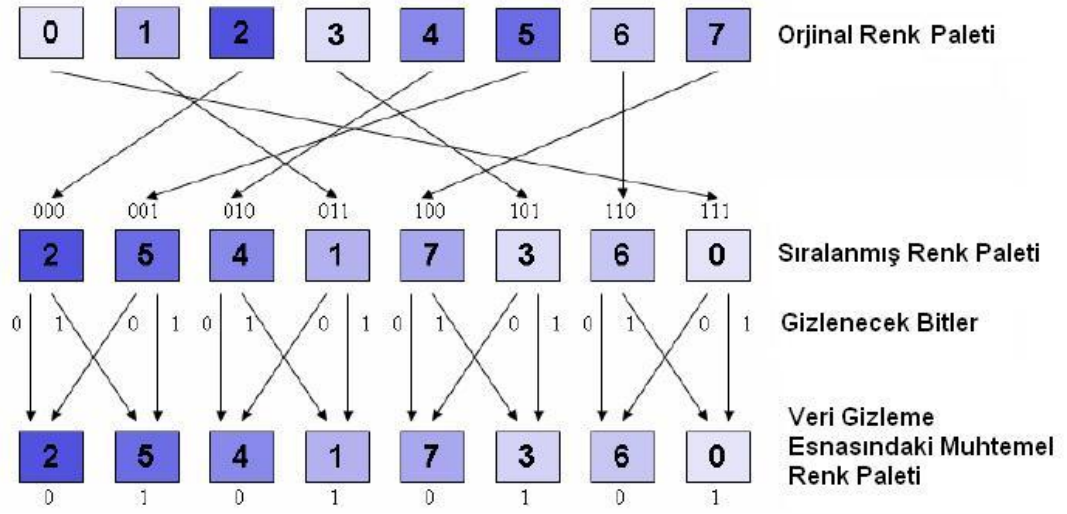
Veri gizleme işlemi gürültünün fazla olduğu düşük seviyeli katmanlarda uygulanır. Her bir katman eşit boyutlu bölümlere ayrılmaktadır ve her bir bölümün karmaşıklığı hesaplanır. Bölümlerin karmaşıklık seviyelerinin bir eşik değerinde olup olmadığı kontrol edilir. Eğer karmaşıklık istenilen düzeyde ise ilgili katmanın seçilen bölümüne gizli veri

gizlenmiş olmaktadır. Bu yöntemde uygulanan eşik seviyesinin her bir katman için ayrı uygulandığında ya da imgelerin değişik katmanlarında belli şartlar altında kullanılmasıyla gizlenecek veri sayısında da artış sağlanmaktadır. Renkli imgelerde geliştirilen diğer bir yöntem ise EzStego algoritmasıdır [103]. Bu yöntemde renk paletleri birbirine en yakın olacak şekilde yeniden düzenlenmektedir. Bu şekilde verinin gömülmesinden sonra imgede çok az renk değişimi olmakta ve insan gözü ile bu fark ayırt edilememektedir. Renkli imgelerin normal renk paleti Şekil 5.5. (a)'da, EzStego algoritması sonucu yeniden düzenlenen renk paleti Şekil 5.5 (b)'de gösterilmiştir.



Şekil 5.5. Renk Paletleri (a) Gerçek Renk Paleti (b) Düzenlenmiş Renk Paleti

İmgelere veri gizleme işlemi renk paletinin düzenlenmesinden sonra yapılmaktadır. Eğer veri biti ile imge pikselin renk paletindeki değeri uyuşuyorsa herhangi bir değişiklik olmaz diğer durumlarda renk paletinde en yakın renk gizli seçilen piksel değerinin yerine veriyi saklamak için kullanılır. Renkli imgelere veri gizleme örneği Şekil 5.6.'te gösterilmiştir.



Şekil 5.6. EzStego Algoritması İle Veri Gizleme Yöntemi

Sıradan EÖB yer değiştirme yöntemlerinde anlatılan gelişmelerin hepsi temelde EÖB'in gizli veriye karşın değiştirilmesi temeline dayandığından basit saldırılara çok hassastırlar. Yapılan çalışmaların bir kısmı analizcinin dikkatini en az seviyede çekmek diğer bir kısmı ise nicemlendirme (quantize) özelliklerini kullanarak veri gizleme de fazladan güvenlik sağlamak üzerine odaklanmıştır. İmge uzayında yapılan değişimlerin dönüşüm uzayındaki etkileri dikkate alınmamıştır. Böylece tüm çalışmaların sonuçları yine aynı uzayda elde edilmektedir. Eğer bu çalışmaların uzantıları başka uzaylarda da mantıklı sonuç elde edilebilirse fazladan güvenliğinin yanında basit saldırılara karşı da dayanıklılık kazandırılabilceği düşünülmektedir.

6. RENKLİ İMGELER İÇİN GERÇEKLEŞTİRİLEN VERİ GİZLEME UYGULAMALARI

Bu tez çalışmasında renkli imgeye veri gizleme uygulaması yapılmaktadır. Hazırlanılan sistemde 256x256 boyutunda 20 farklı imgeye LSB, DCT, DWT ve Çerçeve metotları uygulanmıştır. Kendi geliştirdiğimiz yeni bir yöntemle diğer metotlar karşılaştırılmaktadır. Aynı zamanda görsel ataklardan bulanıklaştırma, keskinleştirme, ölçeklendirme ve döndürme saldırılarına karşı orijinal imgeye oranla değişimi kontrol edilmektedir. Kriter olarak işaret-gürültü oranı değerleri (Peak-Signal-to-noise Ratio, PSNR) baz alınmıştır. Orijinal imge ile veri gizlenmiş imge ve orijinal veri arasındaki PSNR değeri aşağıdaki denkleme göre hesaplanmıştır.

$$PSNR = 10 \times \log_{10} \left(\frac{255^2}{\frac{1}{N \times N} \sum_{i=1}^N \sum_{j=1}^N [I_1(i, j) - I_2(i, j)]^2} \right)$$

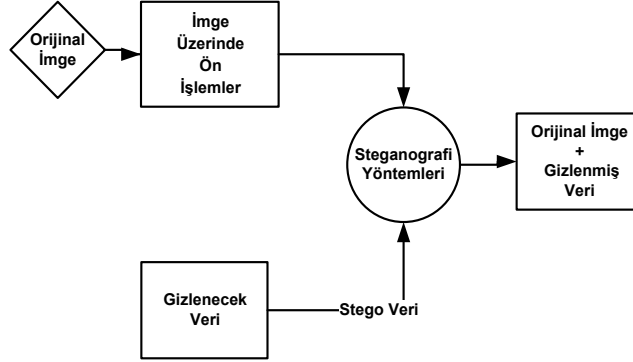
Tez çalışmasında kullanılan yöntemler ve elde edilen sonuçlar alt başlıklar halinde aşağıda verilmektedir.

6.1. En Önemsiz Bite Ekleme (LSB) Metoduyla Veri Gizleme Uygulaması

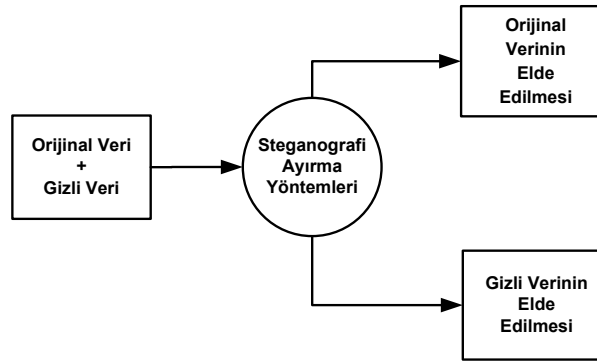
Sistem 20 imge üzerinde denenmiştir. 256x256 boyutunda 20 farklı resme LSB yöntemi ile aşağıdaki metin gömülmüştür.

“Ey Gönül! Damlayı anlayan deryayı nasıl aramasın, Deryayı bulansa damlayı nasıl bırakmasın? Ey fâni sevgili! Sen, Bâki Sevgilinin (c.c.) pırıltısını aksettiren bir damla nispetindesin, lakin görevin bitti artık perdeyi yırtma vaktidir. Zira perdenin ardından Derya bize göz kırpmada Üzülme! Dert etme can! Görebiliyorsan, dokunabiliyorsan, nefes alabiliyorsan, yürüyebiliyorsan... Ne mutlu sana! Elinde olmayanları söyleme bana... Elinde olanlardan bahset can! Üzülme! Geceler hep kimsesiz mi geçecek? Gidenler dönmeyecek mi? Yitirdiğin her ne ise; bir bakarsın yağmurlu bir gecede. Veya bir bahar sabahında karşına çıkmış... Bil ki! Güzellikler de var bu hayatta... Gel Git’lerin olmadığı bir hayat düşünebilir misin? “Hüzün olgunlaştırır” ...’Kaybetmek sabrı öğretir’... (Hz. Mevlana)”

Sistemde imge üzerine veri gömülmesi işleminin blok şeması Şekil 6.1’de, gömülen verilerin çözülmesi işlemi için blok şeması ise Şekil 6.2’de verilmiştir.



Şekil 6.1. Veri gizleme şeması.

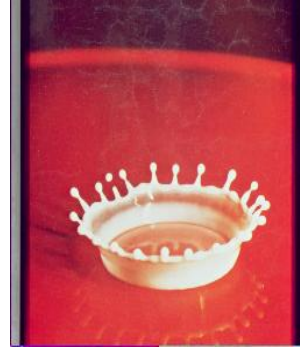


Şekil 6.2. Gizlenen verinin yeniden elde edilmesi.

Geliştirilen metotta öncelikle eldeki orijinal imgeye LSB metodu ile yukarıda verilen metin gömülmüştür. Orijinal imge [104] ve veri gömüldükten sonra elde edilen yeni imgeler Şekil 6.3 ve Şekil 6.4’de gösterilmiştir. Veri gömülmüş imge ile orijinal imgeden elde edilen PSNR oranı: 50.4485’dir.



Şekil 6.3. Orijinal İmge

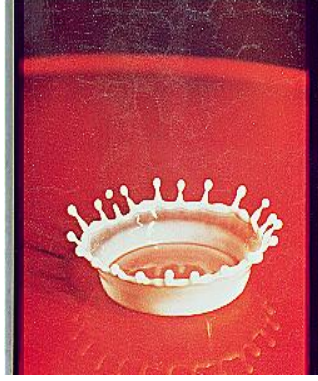


Şekil 6.4. Veri Gizlenen İmge

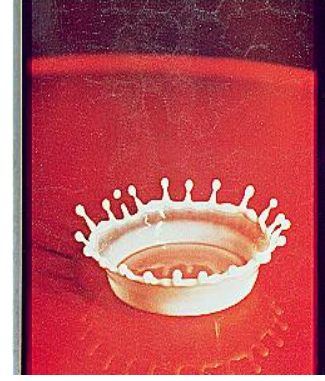
Şekil 6.4'deki veri gizlenmiş imge içerisinde çıkarılan veri aşağıdaki gibidir ve gömülen veri ile aynıdır.

“Ey Gönül! Damlayı anlayan deryayı nasıl aramasın, Deryayı bulansa damlayı nasıl bırakmasın? Ey fâni sevgili! Sen, Bâki Sevgilinin (c.c.) pırıltısını aksettiren bir damla nispetindesin, lakin görevin bitti artık perdeyi yırtma vaktidir. Zira perdenin ardından Derya bize göz kırpmada Üzülme! Dert etme can! Görebiliyorsan, dokunabiliyorsan, nefes alabiliyorsan, yürüyebiliyorsan... Ne mutlu sana! Elinde olmayanları söyleme bana... Elinde olanlardan bahset can! Üzülme! Geceler hep kimsesiz mi geçecek? Gidenler dönmeyecek mi? Yitirdiğin her ne ise; bir bakarsın yağmurlu bir gecede. Veya bir bahar sabahında karşına çıkmış... Bil ki! Güzellikler de var bu hayatta... Gel Git'lerin olmadığı bir hayat düşünebilir misin? “Hüzün olgunlaştırır” ...'Kaybetmek sabrı öğretir'... (Hz. Mevlana)”

Veri gömülmüş imgelere 4 farklı saldırı (keskinleştirme, bulanıklaştırma, imge ölçekleme ve imge döndürme) uygulanmıştır. Orijinal imge ile veri gömülmüş imge keskinleştirilme işleminden geçirildikten sonra elde edilen yeni imgeler Şekil 6.5 ve 6.6'da verilmiştir. Bu iki imge kullanılarak elde edilen PSNR oranı 48.5736 olarak bulunmuştur.



Şekil 6.5. Keskinleştirilmiş Veri Gömülen
İmge



Şekil 6.6. Keskinleştirilmiş Orijinal
İmge

Aynı şekilde bulanıklaştırma işlemi ile elde edilen imgeler Şekil 6.7 ve 6.8’de verilmiştir. PSNR değeri 53.7336’tür.



Şekil 6.7. Bulanıklaştırılmış Veri Gömülen
İmge



Şekil 6.8. Bulanıklaştırılmış Orijinal
İmge

0.4 katsayısı ile ölçeklendirilen imgeler Şekil 6.9 ve 6.10 ile temsil edilmektedir. Bu iki imge arasındaki PSNR oranı 43.3809 olarak bulunmuştur.

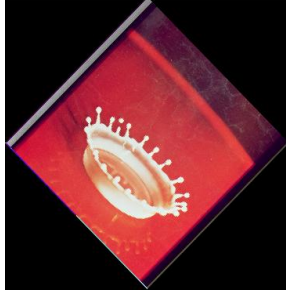


Şekil 6.9. 0.4 Oranında Küçültülmüş Veri
Gömülen İmge



Şekil 6.10. 0.4 Oranında Küçültülmüş
Orijinal İmge

Son olarak -45° döndürülen imgeler Şekil 6.11 ve 6.12’de gösterilmektedir. İşlem sonucunda elde edilen PSNR oranı 67.1594’dir.



Şekil 6.11. -45° Döndürülmüş Veri Gömülen İmge



Şekil 6.12. -45° Döndürülen Orijinal İmge

Sistem 256X256 boyutunda 20 imge için uygulanmış ve LSB yöntemi ile gömülen verinin herhangi bir saldırı sırasında çözümünü zorlaştırmak için kullanılan 3 boyutlu resmin her bir boyutuna veri gömülmüştür. Gömme işlemi sırasında 3 boyutlu imge ve veri ikili kodlara dönüştürüldükten sonra, veri oluşturduğumuz algoritma paralelinde 3 boyutlu resme sırayla değil rastgele indislerle gömülmüştür. Oluşturulan veri tabanında ortalama PSNR değeri 57.1022 olarak bulunmuştur.

Yukarıdaki örnekte anlatılan tüm işlemler 20 imge için uygulanmıştır. Elde edilen PSNR değerleri Tablo 6.1’de gösterilmiştir.

Tablo 6.1. LSB metoduyla ile veri gizlenmiş imgelerin PSNR değerleri

Resmin Adı	Orijinal Veri gömülmüş imge	Keskinleştirilmiş veri gömülmüş imge	Bulanıklaştırılmış veri gömülmüş imge	-45 derece döndürülmüş veri gömülmüş imge	0.4 oranında ölçeklendirilmiş veri gömülmüş imge
1.BMP	50.4485	50.4485	53.7336	67.1594	43.3809
2.BMP	49.7842	49.7812	49.7485	67.4594	41.8709
3.BMP	64.4991	63.8175	64.7690	67.4603	56.5170
4.BMP	51.5166	51.4346	48.7156	67.4612	40.8776
5.BMP	58.2090	57.1022	56.5390	67.4566	49.5118
6.BMP	64.6749	64.7524	64.4881	67.4724	56.7331
7.BMP	55.6044	55.4556	55.4904	67.4640	47.6141
8.BMP	52.1136	52.1475	50.5252	67.4659	43.0992
9.BMP	52.1566	51.6819	52.0299	67.4519	44.1817
10.BMP	63.732	63.9860	63.3290	67.4715	55.6560
11.BMP	56.919	56.4219	58.5891	67.4603	49.9059
12.BMP	51.794	51.9881	51.1225	67.4510	43.0546
13.BMP	48.7900	49.1437	48.8512	67.4631	40.7956
14.BMP	64.6136	63.7052	48.8664	67.4566	56.8474
15.BMP	54.5344	54.5547	54.0581	67.4584	46.4756
16.BMP	64.6899	64.6819	61.0170	67.4640	55.6022
17.BMP	48.5744	48.5719	48.6077	67.4491	40.6783
18.BMP	49.3465	49.6059	48.9343	67.4528	41.2019
19.BMP	62.7622	62.7360	62.7341	67.4752	54.7917
20.BMP	53.9239	51.8194	54.4543	67.4752	46.4309

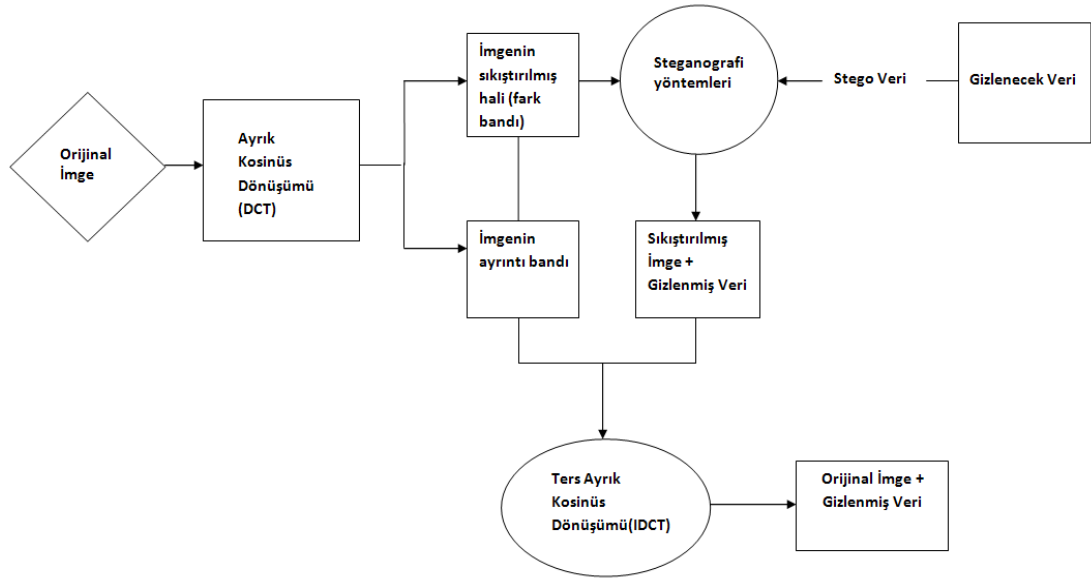
6.2. Ayrık Kosinüs Dönüşümü (DCT) Metoduyla Veri Gizleme Uygulaması

Sistem 20 imge üzerinde denenmiştir. boyutunda 20 farklı resme DCT yöntemi ile aşağıdaki metin gömülmüştür.

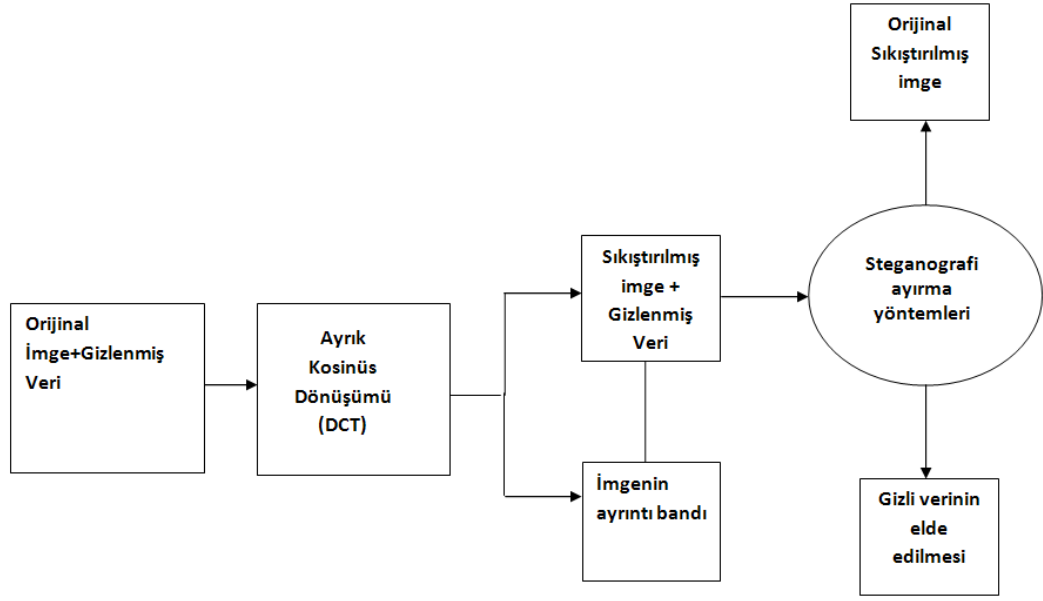
“Ey Gönül! Damlayı anlayan deryayı nasıl aramasın, Deryayı bulansa damlayı nasıl bırakmasın? Ey fâni sevgili! Sen, Bâki Sevgilinin (c.c.) pırıltısını aksettiren bir damla nispetindesin, lakin görevin bitti artık perdeyi yırtma vaktidir. Zira perdenin ardından

Derya bize göz kırpmada Üzülme! Dert etme can! Görebiliyorsan, dokunabiliyorsan, nefes alabiliyorsan, yürüyebiliyorsan... Ne mutlu sana! Elinde olmayanları söyleme bana... Elinde olanlardan bahset can! Üzülme! Geceler hep kimsesiz mi geçecek? Gidenler dönmeyecek mi? Yitirdiğin her ne ise; bir bakarsın yağmurlu bir gecede. Veya bir bahar sabahında karşına çıkmış... Bil ki! Güzellikler de var bu hayatta... Gel Git'lerin olmadığı bir hayat düşünebilir misin? “Hüzün olgunlaştırır” ...'Kaybetmek sabrı öğretir'... (Hz. Mevlana)”

Sistemde imge üzerine veri gömülmesi işleminin blok şeması Şekil 6.13’de, gömülen verilerin çözülmesi işlemi için blok şeması ise Şekil 6.14’de verilmiştir.



Şekil 6.13. Veri gizleme şeması.

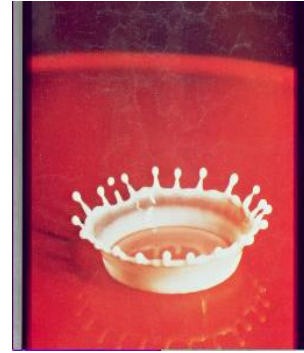


Şekil 6.14. Gizlenen verinin yeniden elde edilmesi.

Geliştirilen metotta öncelikle eldeki orijinal imgeye DCT metodu ile yukarıda verilen metin gömülmüştür. Orijinal imge ve veri gömüldükten sonra elde edilen yeni imgeler Şekil 6.15 ve Şekil 6.16’ de gösterilmiştir. Veri gömülmüş imge ile orijinal imgeden elde edilen PSNR oranı: 46.2504’ dır.



Şekil 6.15. Orijinal İmge



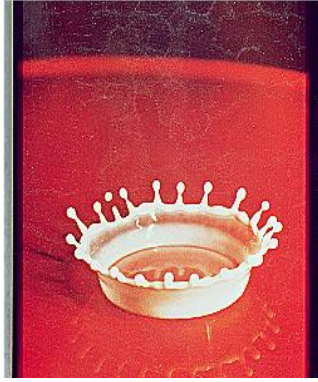
Şekil 6.16. Veri Gizlenen İmge

Şekil 6.16’daki veri gizlenmiş imge içerisinde çıkarılan veri aşağıdaki gibidir ve gömülen veri ile aynıdır.

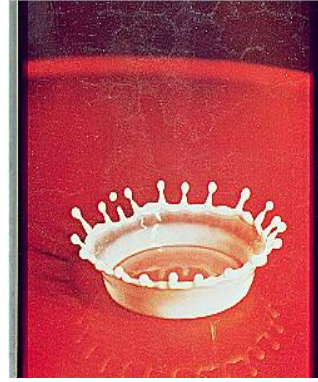
“Ey Gönül! Damlayı anlayan deryayı nasıl aramasın, Deryayı bulansa damlayı nasıl bırakmasın? Ey fâni sevgili! Sen, Bâki Sevgilinin (c.c.) pırıltısını aksettiren bir damla nispetindesin, lakin görevin bitti artık perdeyi yırtma vaktidir. Zira perdenin ardından

Derya bize göz kırpmada Üzülme! Dert etme can! Görebiliyorsan, dokunabiliyorsan, nefes alabiliyorsan, yürüyebiliyorsan... Ne mutlu sana! Elinde olmayanları söyleme bana... Elinde olanlardan bahset can! Üzülme! Geceler hep kimsesiz mi geçecek? Gidenler dönmeyecek mi? Yitirdiğin her ne ise; bir bakarsın yağmurlu bir gecede. Veya bir bahar sabahında karşına çıkmış... Bil ki! Güzellikler de var bu hayatta... Gel Git'lerin olmadığı bir hayat düşünebilir misin? “Hüzün olgunlaştırır” ...'Kaybetmek sabrı öğretir'... (Hz. Mevlana)”

Veri gömülmüş imgelere 4 farklı saldırı (keskinleştirme, bulanıklaştırma, imge ölçekleme ve imge döndürme) uygulanmıştır. Orijinal imge ile veri gömülmüş imge keskinleştirilme işleminden geçirildikten sonra elde edilen yeni imgeler Şekil 6.17 ve 6.18’de verilmiştir. Bu iki imge kullanılarak elde edilen PSNR oranı 42.4917 olarak bulunmuştur.



Şekil 6.17. Keskinleştirilmiş Veri Gömülen İmge



Şekil 6.18. Keskinleştirilmiş Orijinal İmge

Aynı şekilde bulanıklaştırma işlemi ile elde edilen imgeler Şekil 6.19 ve 6.20’ de verilmiştir. PSNR değeri 42.4282’tür.



Şekil 6.19. Bulanıklaştırılmış Veri Gömülen
İmge



Şekil 6.20. Bulanıklaştırılmış Orijinal
İmge

0.4 katsayısı ile ölçeklendirilen imgeler Şekil 6.21 ve 6.22 ile temsil edilmektedir. Bu iki imge arasındaki PSNR oranı 36.3600 olarak bulunmuştur.



Şekil 6.21. 0.4 Oranında Küçültülmüş Veri
Gömülen İmge



Şekil 6.22. 0.4 Oranında Küçültülmüş
Orijinal İmge

Son olarak -45° döndürülen imgeler Şekil 6.23 ve 6.24' de gösterilmektedir. İşlem sonucunda elde edilen PSNR oranı 47.0366'dır.



Şekil 6.23. -45° Döndürülmüş Veri Gömülen
İmge



Şekil 6.24. -45° Döndürülen Orijinal
İmge

Sistem 256X256 boyutunda 20 imge için uygulanmış ve DCT yöntemi ile gömülen verinin herhangi bir saldırı sırasında çözümünü zorlaştırmak için kullanılan 3 boyutlu resmin her bir boyutuna veri gömülmüştür. Gömme işlemi sırasında 3 boyutlu imge katmanlarına ayrılıp her bir katmana teker teker DCT uygulanmış ve veri ikili kodlara dönüştürüldükten sonra, veri oluşturduğumuz algoritma paralelinde 3 boyutlu resme sırayla değil rastgele indislerle gömülmüştür. Oluşturulan veri tabanında ortalama PSNR değeri 46.2504 olarak bulunmuştur.

Yukarıdaki örnekte anlatılan tüm işlemler 20 imge için uygulanmıştır. Elde edilen PSNR değerleri Tablo 6.2’de gösterilmiştir.

Tablo 6.2. DCT metoduyla veri gizlenmiş imgelerin PSNR değerleri

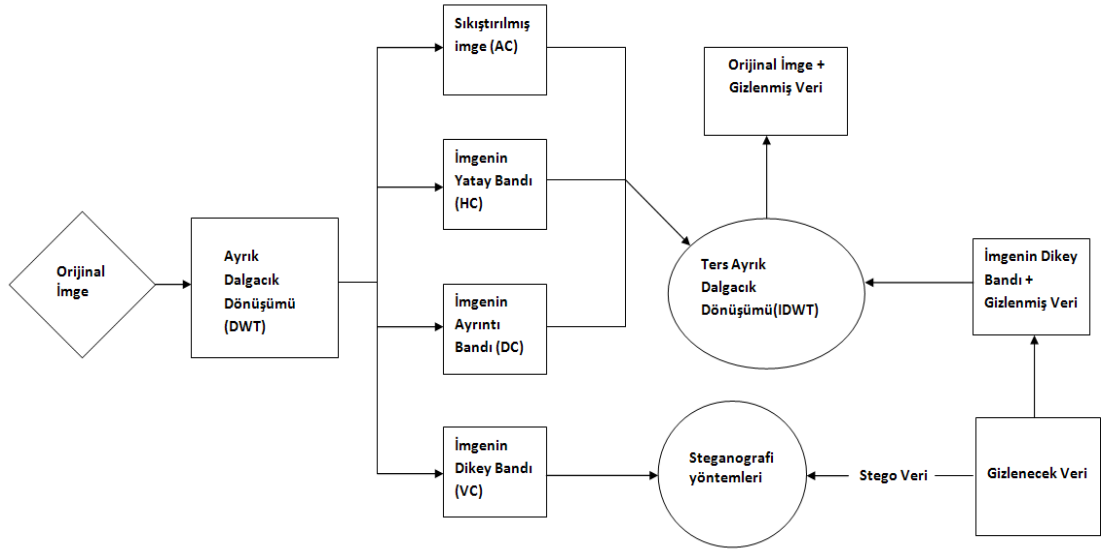
İmge İsmi	Orijinal veri gömülmüş imge	Keskinleştirilmiş veri gömülmüş imge	Bulanıklaştırılmış veri gömülmüş imge	-45 derece döndürülmüş veri gömülmüş imge	0.4 oranında ölçeklendirilmiş veri gömülmüş imge
1.BMP	46.2504	42.4917	42.4282	47.0366	36.3600
2.BMP	46.5558	44.2657	44.2340	47.3441	36.3441
3.BMP	46.5622	44.2607	44.1997	47.3480	36.6282
4.BMP	46.5635	44.2666	41.3387	47.3490	33.6195
5.BMP	46.5633	44.6152	43.7415	47.3489	36.6941
6.BMP	45.1441	44.6230	44.1308	47.3450	36.7256
7.BMP	45.4814	44.6205	44.1997	47.3480	36.7264
8.BMP	45.0750	44.2673	42.9462	47.3490	35.3879
9.BMP	45.4383	44.6095	44.1308	47.3456	36.5618
10.BMP	45.4407	44.6151	44.1653	47.3477	36.3600
11.BMP	49.0708	44.6211	44.3360	47.3452	36.7260
12.BMP	48.8231	44.3518	43.5587	47.3468	36.2571
13.BMP	48.9502	44.5983	44.1997	47.4784	36.5276
14.BMP	44.6457	44.2633	44.2340	47.3488	36.7267
15.BMP	44.6240	44.2663	43.7777	47.3490	36.3258
16.BMP	44.4689	44.2633	44.2340	47.3488	36.7267
17.BMP	44.6333	44.6279	44.5694	47.7139	36.7265
18.BMP	45.6233	44.6123	44.2340	47.7043	36.7265
19.BMP	44.6238	44.6276	44.2681	47.3346	36.7251
20.BMP	44.2664	44.2508	44.1308	47.3472	36.3599

6.3. Ayırık Dalgacık Dönüşümü (DWT) Metoduyla Veri Gizleme Uygulaması

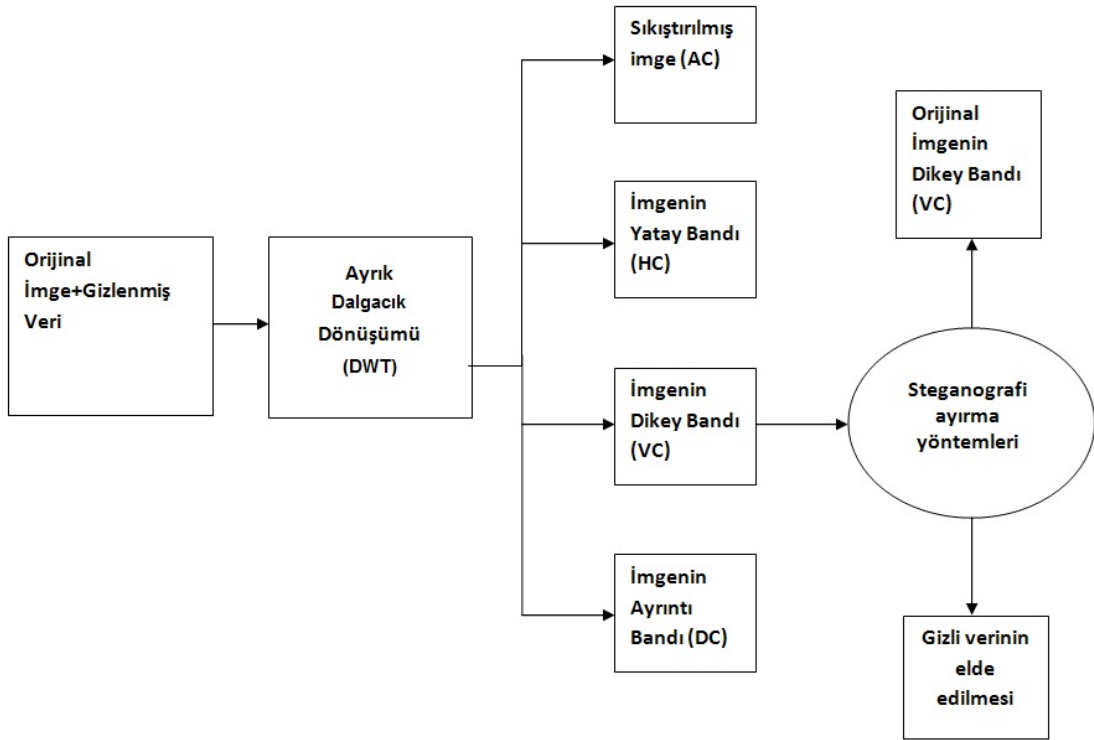
Sistem 20 imge üzerinde denenmiştir. 256x256 boyutunda 20 farklı resme LSB yöntemi ile aşağıdaki metin gömülmüştür.

“Ey Gönül! Damlayı anlayan deryayı nasıl aramasın, Deryayı bulansa damlayı nasıl bırakmasın? Ey fâni sevgili! Sen, Bâki Sevgilinin (c.c.) pırıltısını aksettiren bir damla nispetindesin, lakin görevin bitti artık perdeyi yırtma vaktidir. Zira perdenin ardından Derya bize göz kırpmada Üzülme! Dert etme can! Görebiliyorsan, dokunabiliyorsan, nefes alabiliyorsan, yürüyebiliyorsan... Ne mutlu sana! Elinde olmayanları söyleme bana... Elinde olanlardan bahset can! Üzülme! Geceler hep kimsesiz mi geçecek? Gidenler dönmeyecek mi? Yitirdiğin her ne ise; bir bakarsın yağmurlu bir gecede. Veya bir bahar sabahında karşına çıkmış... Bil ki! Güzellikler de var bu hayatta... Gel Git’lerin olmadığı bir hayat düşünebilir misin? “Hüzün olgunlaştırır” ...’Kaybetmek sabrı öğretir’... (Hz. Mevlana)”

Sistemde imge üzerine veri gömülmesi işleminin blok şeması Şekil 6.25’de, gömülen verilerin çözülmesi işlemi için blok şeması ise Şekil 6.26’de verilmiştir.

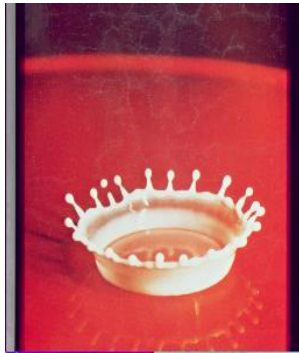


Şekil 6.25. Veri gizleme şeması.

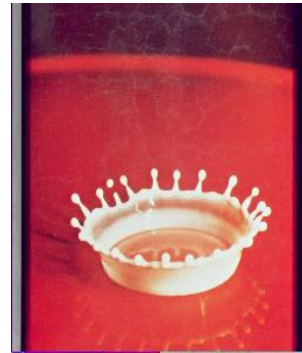


Şekil 6.26. Gizlenen verinin yeniden elde edilmesi.

Geliştirilen metotta öncelikle eldeki orijinal imgeye DWT metodu ile yukarıda verilen metin gömülmüştür. Orijinal imge ve veri gömüldükten sonra elde edilen yeni imgeler Şekil 6.27 ve Şekil 6.28’de gösterilmiştir. Veri gömülmüş imge ile orijinal imgeden elde edilen PSNR oranı: 58.6640’dır.



Şekil 6.27. Orijinal İmge



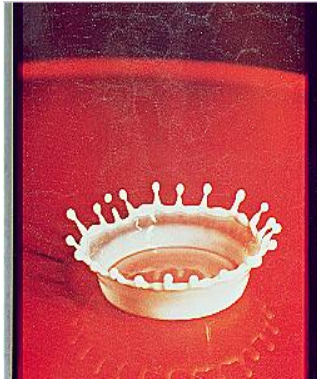
Şekil 6.28. Veri Gizlenen İmge

Şekil 6.28’deki veri gizlenmiş imge içerisinden çıkarılan veri aşağıdaki gibidir ve gömülen veri ile aynıdır.

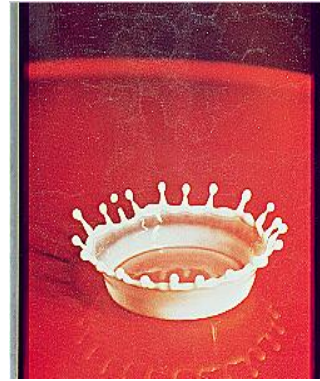
“Ey Gönül! Damlayı anlayan deryayı nasıl aramasın, Deryayı bulansa damlayı nasıl

bırakmasın? Ey fâni sevgili! Sen, Bâki Sevgilinin (c.c.) pırıltısını aksettiren bir damla nispetindesin, lakin görevin bitti artık perdeyi yırtma vaktidir. Zira perdenin ardından Derya bize göz kırpmada Üzülme! Dert etme can! Görebiliyorsan, dokunabiliyorsan, nefes alabiliyorsan, yürüyebiliyorsan... Ne mutlu sana! Elinde olmayanları söyleme bana... Elinde olanlardan bahset can! Üzülme! Geceler hep kimsesiz mi geçecek? Gidenler dönmeyecek mi? Yitirdiğin her ne ise; bir bakarsın yağmurlu bir gecede. Veya bir bahar sabahında karşına çıkmış... Bil ki! Güzellikler de var bu hayatta... Gel Git'lerin olmadığı bir hayat düşünebilir misin? “Hüzün olgunlaştırır” ...'Kaybetmek sabrı öğretir'... (Hz. Mevlana)”

Veri gömülmüş imgelere 4 farklı saldırı (keskinleştirme, bulanıklaştırma, imge ölçekleme ve imge döndürme) uygulanmıştır. Orijinal imge ile veri gömülmüş imge keskinleştirilme işleminden geçirildikten sonra elde edilen yeni imgeler Şekil 6.29 ve 6.30'da verilmiştir. Bu iki imge kullanılarak elde edilen PSNR oranı 59.0216 olarak bulunmuştur.



Şekil 6.29. Keskinleştirilmiş Veri Gömülen İmge



Şekil 6.30. Keskinleştirilmiş Orijinal İmge

Aynı şekilde bulanıklaştırma işlemi ile elde edilen imgeler Şekil 6.31 ve 6.32'de verilmiştir. PSNR değeri 58.5415'tür.



Şekil 6.31. Bulanıklaştırılmış Veri Gömülen İmge



Şekil 6.32. Bulanıklaştırılmış Orijinal İmge

0.4 katsayısı ile ölçeklendirilen imgeler Şekil 6.33 ve 6.34 ile temsil edilmektedir. Bu iki imge arasındaki PSNR oranı 58.3983 olarak bulunmuştur.

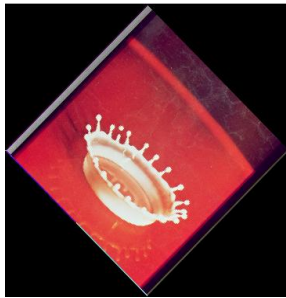


Şekil 6.33. 0.4 Oranında Küçültülmüş Veri Gömülen İmge



Şekil 6.34. 0.4 Oranında Küçültülmüş Orijinal İmge

Son olarak -45° döndürülen imgeler Şekil 6.35 ve 6.36'de gösterilmektedir. İşlem sonucunda elde edilen PSNR oranı 61.5896'dır.



Şekil 6.35. -45° Döndürülmüş Veri Gömülen İmge



Şekil 6.36. -45° Döndürülen Orijinal İmge

Sistem 256X256 boyutunda 20 imge için uygulanmış ve DWT yöntemi ile gömülen verinin herhangi bir saldırı sırasında çözümünü zorlaştırmak için kullanılan 3 boyutlu

resmin her bir boyutuna veri gömülmüştür. Gömme işlemi sırasında 3 boyutlu imgeye DWT uygulandıktan sonra imgenin dikey bandı (VC) ve veri ikili kodlara dönüştürülmüştür, veri oluşturduğumuz algoritma paralelinde 3 boyutlu resme sırayla değil rastgele indislerle gömülmüştür. Oluşturulan veri tabanında ortalama PSNR değeri 58.3768 olarak bulunmuştur.

Yukarıdaki örnekte anlatılan tüm işlemler 20 imge için uygulanmıştır. Elde edilen PSNR değerleri Tablo 6.3' de gösterilmiştir.

Tablo 6.3: DWT metodu ile veri gizlenmiş imgelerin PSNR değerleri

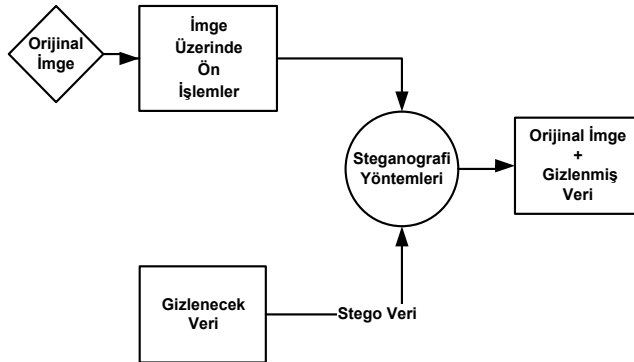
İmgenin İsmi	Orijinal Veri gömülmüş imge	Keskinleştirilmiş veri gömülmüş imge	Bulanıklaştırılmış veri gömülmüş imge	-45 derece döndürülmüş veri gömülmüş imge	0.4 oranında ölçeklendirilmiş veri gömülmüş imge
1.BMP	58.6640	59.0216	58.5415	61.5896	58.9156
2.BMP	58.9827	58.9491	60.8762	61.9114	58.9572
3.BMP	58.9355	58.9540	58.9172	61.8416	58.9343
4.BMP	58.9319	58.9354	60.3048	61.8312	56.1059
5.BMP	58.9222	58.9269	58.3768	61.8274	58.9866
6.BMP	58.9481	58.9615	59.9455	61.8086	59.0008
7.BMP	58.9724	58.9268	58.8402	61.8345	59.0353
8.BMP	59.5630	59.1749	59.7324	62.3285	58.2600
9.BMP	58.9358	58.9306	58.8601	61.8494	58.9137
10.BMP	58.9327	58.9211	58.9613	61.8775	58.9674
11.BMP	58.9301	58.9349	59.1419	61.9103	58.9676
12.BMP	59.0303	58.9675	59.6301	61.9709	58.8904
13.BMP	58.9072	58.9421	58.9049	61.8108	59.0079
14.BMP	58.9356	59.0455	59.2080	61.9322	59.0034
15.BMP	58.6224	59.0645	59.4312	62.1158	58.9054
16.BMP	58.9155	58.9046	55.7673	61.8331	57.7836
17.BMP	58.1515	59.1706	59.5847	62.1089	59.1218
18.BMP	58.8951	59.3420	58.9347	62.1069	59.0263
19.BMP	59.8472	59.7736	59.7201	62.5559	59.5414
20.BMP	60.0320	60.0042	59.7755	62.8881	59.8915

6.4. Çerçeve Metoduyla Veri Gizleme Uygulaması

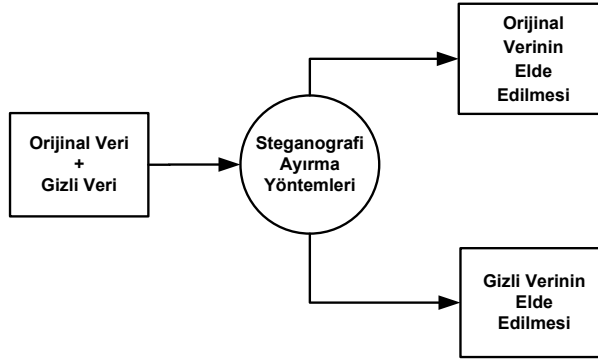
Sistem 20 imge üzerinde denenmiştir. 256x256 boyutunda 20 farklı resme Çerçeve yöntemi ile aşağıdaki metin gömülmüştür.

“Ey Gönül! Damlayı anlayan deryayı nasıl aramasın, Deryayı bulansa damlayı nasıl bırakmasın? Ey fâni sevgili! Sen, Bâki Sevgilinin (c.c.) pırıltısını aksettiren bir damla nispetindesin, lakin görevin bitti artık perdeyi yırtma vaktidir. Zira perdenin ardından Derya bize göz kırpmada Üzülme! Dert etme can! Görebiliyorsan, dokunabiliyorsan, nefes alabiliyorsan, yürüyebiliyorsan... Ne mutlu sana! Elinde olmayanları söyleme bana... Elinde olanlardan bahset can! Üzülme! Geceler hep kimsesiz mi geçecek? Gidenler dönmeyecek mi? Yitirdiğin her ne ise; bir bakarsın yağmurlu bir gecede. Veya bir bahar sabahında karşına çıkmış... Bil ki! Güzellikler de var bu hayatta... Gel Git’lerin olmadığı bir hayat düşünebilir misin? “Hüzün olgunlaştırır” ...’Kaybetmek sabrı öğretir’... (Hz. Mevlana)”

Sistemde imge üzerine veri gömülmesi işleminin blok şeması Şekil 6.37’de, gömülen verilerin çözülmesi işlemi için blok şeması ise Şekil 6.38’de verilmiştir.

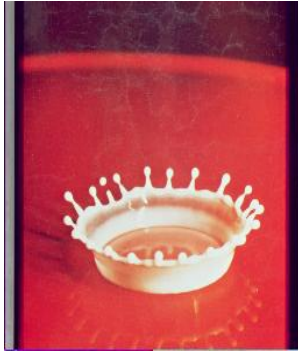


Şekil 6.37. Veri gizleme şeması.

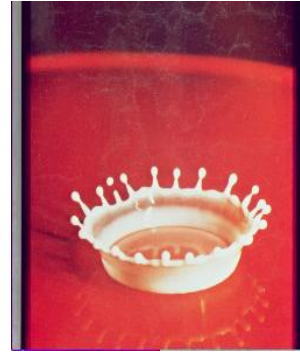


Şekil 6.38. Gizlenen verinin yeniden elde edilmesi.

Geliştirilen metotta öncelikle eldeki orijinal imgeye Çerçeve metodu ile yukarıda verilen metin gömülmüştür. Orijinal imge ve veri gömüldükten sonra elde edilen yeni imgeler Şekil 6.39ve Şekil 6.40’de gösterilmiştir. Veri gömülmüş imge ile orijinal imgeden elde edilen PSNR oranı: 46.0249’ dır.



Şekil 6.39. Orijinal İmge



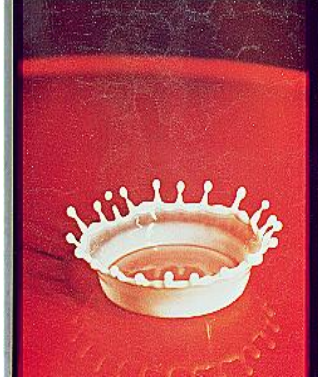
Şekil 6.40. Veri Gizlenen İmge

Şekil 6.40’daki veri gizlenmiş imge içerisinde çıkarılan veri aşağıdaki gibidir ve gömülen veri ile aynıdır.

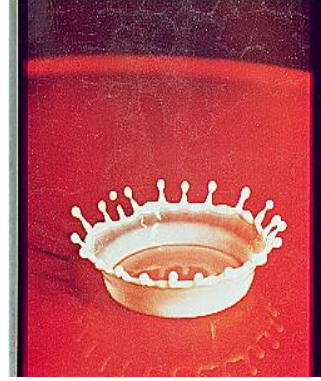
“Ey Gönül! Damlayı anlayan deryayı nasıl aramasın, Deryayı bulansa damlayı nasıl bırakmasın? Ey fâni sevgili! Sen, Bâki Sevgilinin (c.c.) pırıltısını aksettiren bir damla nispetindesin, lakin görevin bitti artık perdeyi yırtma vaktidir. Zira perdenin ardından Derya bize göz kırpmada Üzülme! Dert etme can! Görebiliyorsan, dokunabiliyorsan, nefes alabiliyorsan, yürüyebiliyorsan... Ne mutlu sana! Elinde olmayanları söyleme bana... Elinde olanlardan bahset can! Üzülme! Geceler hep kimsesiz mi geçecek? Gidenler dönmeyecek mi? Yitirdiğin her ne ise; bir bakarsın yağmurlu bir gecede. Veya bir bahar sabahında karşına çıkmış... Bil ki! Güzellikler de var bu hayatta... Gel Git’lerin olmadığı

bir hayat düşünebilir misin? “Hüzün olgunlaştırır” ...’Kaybetmek sabrı öğretir’... (Hz. Mevlana)”

Veri gömülmüş imgelere 4 farklı saldırı (keskinleştirme, bulanıklaştırma, imge ölçekleme ve imge döndürme) uygulanmıştır. Orijinal imge ile veri gömülmüş imge keskinleştirilme işleminden geçirildikten sonra elde edilen yeni imgeler Şekil 6.41 ve 6.42’de verilmiştir. Bu iki imge kullanılarak elde edilen PSNR oranı 45.9344 olarak bulunmuştur.



Şekil 6.41. Keskinleştirilmiş Veri Gömülen İmge



Şekil 6.42. Keskinleştirilmiş Orijinal İmge

Aynı şekilde bulanıklaştırma işlemi ile elde edilen imgeler Şekil 6.43 ve 6.44’de verilmiştir. PSNR değeri 46.0282’tür.



Şekil 6.43. Bulanıklaştırılmış Veri Gömülen İmge



Şekil 6.44. Bulanıklaştırılmış Orijinal İmge

0.4 katsayısı ile ölçeklendirilen imgeler Şekil 6.45 ve 6.46 ile temsil edilmektedir. Bu iki imge arasındaki PSNR oranı 37.2836 olarak bulunmuştur.



Şekil 6.45. 0.4 Oranında Küçültülmüş Veri Gömülen İmge



Şekil 6.46. 0.4 Oranında Küçültülmüş Orijinal İmge

Son olarak -45° döndürülen imgeler Şekil 6.47 ve 6.48’de gösterilmektedir. İşlem sonucunda elde edilen PSNR oranı 48.1229’dır.



Şekil 6.47. -45° Döndürülmüş Veri Gömülen İmge



Şekil 6.48. -45° Döndürülen Orijinal İmge

Sistem 256X256 boyutunda 20 imge için uygulanmış ve Çerçeve yöntemi ile gömülen verinin herhangi bir saldırı sırasında çözümünü zorlaştırmak için kullanılan 3 boyutlu resmin her bir boyutuna veri gömülmüştür. Gömme işlemi sırasında 3 boyutlu imge ve veri ikili kodlara dönüştürüldükten sonra, veri imgenin etrafındaki 1 piksel kalınlığındaki çerçeveye yerleştirilmiştir. 3 boyutlu resme veri sırasıyla yerleştirilmiştir. Oluşturulan veri tabanında ortalama PSNR değeri 44.5257 olarak bulunmuştur.

Yukarıdaki örnekte anlatılan tüm işlemler 20 imge için uygulanmıştır. Elde edilen PSNR değerleri Tablo 6.4’ de gösterilmiştir.

Tablo 6.4: Çerçeve metodu ile veri gizlenmiş imgelerin PSNR değerleri

İmgenin İsmi	Orijinal Veri gömülmüş imge	Keskinleştirilmiş veri gömülmüş imge	Bulanıklaştırılmış veri gömülmüş imge	-45 derece döndürülmüş veri gömülmüş imge	0.4 oranında ölçeklendirilmiş veri gömülmüş imge
1.BMP	46.0249	45.9344	46.0282	48.1229	37.2836
2.BMP	46.0189	46.0184	46.0193	48.1125	37.3532
3.BMP	45.1240	45.9114	45.9079	48.8229	37.2347
4.BMP	45.2306	46.0163	46.0198	48.5681	37.3658
5.BMP	45.2350	45.9634	45.9905	48.0012	37.3495
6.BMP	44.6636	45.8398	45.8356	48.1358	37.1543
7.BMP	44.5257	46.0205	46.0276	48.9982	37.3821
8.BMP	44.6904	45.8229	45.8229	47.5233	37.3378
9.BMP	44.5142	45.9927	46.0308	48.2358	37.2881
10.BMP	44.6993	45.9196	45.9964	49.2555	37.2718
11.BMP	44.5764	45.9019	45.9300	48.5622	37.2309
12.BMP	44.5361	45.8458	45.8459	48.1229	37.3000
13.BMP	44.6400	45.9101	45.9685	48.2589	37.1928
14.BMP	44.5758	45.9013	45.9086	48.9521	37.2833
15.BMP	44.5089	45.8133	45.8118	48.1229	37.2059
16.BMP	44.6702	46.0060	45.9846	48.4525	37.3588
17.BMP	45.1795	46.0312	46.0404	48.0101	37.1351
18.BMP	45.2932	46.0354	46.0210	48.1012	37.3276
19.BMP	45.2965	46.0191	46.0356	49.1512	37.2202
20.BMP	45.1142	45.9586	45.9752	47.9221	37.3349

6.5. Geliştirilen Metotla Veri Gizleme Uygulaması

Bu tez çalışmasında geliştirilen metotla veri gizleme algoritması aşağıdaki adımlar takip edilerek yapılmıştır.

1.Adım: Başla

2.Adım: İmgeyi al ve boyutunu kaydet.

3.Adım: Metni al ve ikilik kodlara çevir ve şifre adındaki matrise ata.

4.Adım: Şifrenin boyutunu al anahtar olarak kaydet.

5.Adım: Eğer şifrenin boyutu imgenin boyutundan büyük ise programı sonlandır.

6.Adım: Eğer şifrenin boyutu imgenin boyutundan küçük ise şifrenin tüm elemanlarını, imgenin şifrenin boyutu kadar olan elemanlarını tara

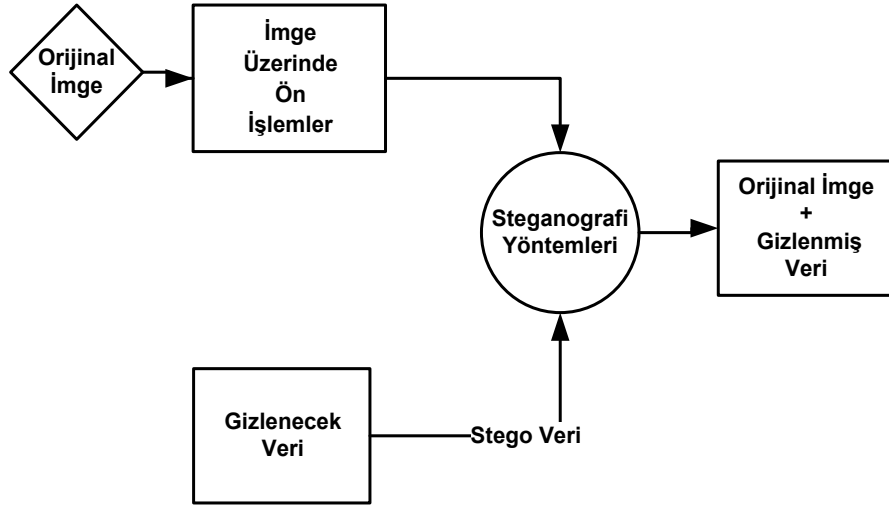
7.Adım: Eğer şifrenin herhangi bir elemanı 1 ise, imgenin elemanını bir artır.

8.Adım: Bitir

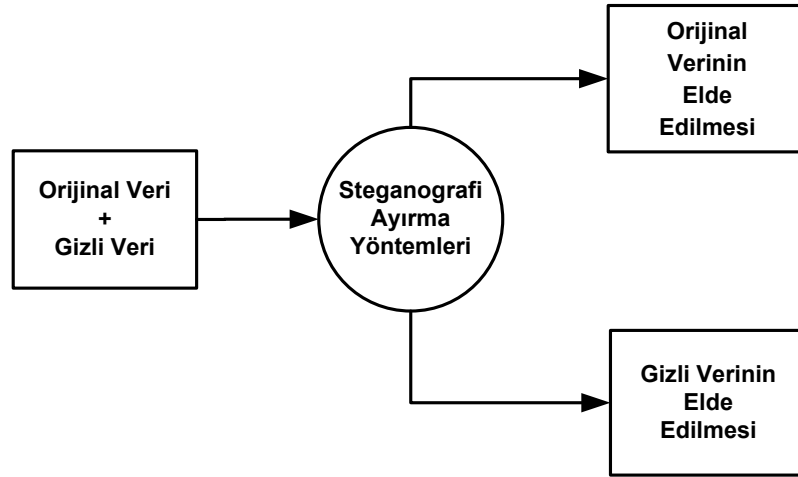
Sistem 20 imge üzerinde denenmiştir. 256X256 boyutunda 20 farklı resme geliştirilen metot ile aşağıdaki metin gömülmüştür.

“Ey Gönül! Damlayı anlayan deryayı nasıl aramasın, Deryayı bulansa damlayı nasıl bırakmasın? Ey fâni sevgili! Sen, Bâki Sevgilinin (c.c.) pırıltısını aksettiren bir damla nispetindesin, lakin görevin bitti artık perdeyi yırtma vaktidir. Zira perdenin ardından Derya bize göz kırpmada Üzülme! Dert etme can! Görebiliyorsan, dokunabiliyorsan, nefes alabiliyorsan, yürüyebiliyorsan... Ne mutlu sana! Elinde olmayanları söyleme bana... Elinde olanlardan bahset can! Üzülme! Geceler hep kimsesiz mi geçecek? Gidenler dönmeyecek mi? Yitirdiğin her ne ise; bir bakarsın yağmurlu bir gecede. Veya bir bahar sabahında karşına çıkmış... Bil ki! Güzellikler de var bu hayatta... Gel Git’lerin olmadığı bir hayat düşünebilir misin? “Hüzün olgunlaştırır” ...’Kaybetmek sabrı öğretir’... (Hz. Mevlana)”

Sistemde imge üzerine veri gömülmesi işleminin blok şeması Şekil 6.49’de, gömülen verilerin çözülmesi işlemi için blok şeması ise Şekil 6.50’de verilmiştir.

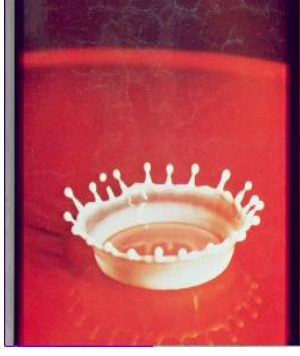


Şekil 6.49. Veri gizleme şeması.

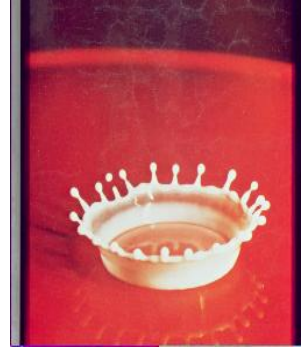


Şekil 6.50. Gizlenen verinin yeniden elde edilmesi.

Geliştirilen metotta öncelikle eldeki orijinal imgeye kendi geliştirdiğimiz yöntem ile yukarıda verilen metin gömülmüştür. Orijinal imge ve veri gömüldükten sonra elde edilen yeni imgeler Şekil 6.51 ve Şekil 6.52’de gösterilmiştir. Veri gömülmüş imge ile orijinal imgeden elde edilen PSNR oranı: 66.0447’ dir.



Şekil 6.51. Orijinal İmge



Şekil 6.52. Veri Gizlenen İmge

Şifreyi çözme algoritması ise aşağıdaki adımlar takip edilerek yapılmıştır.

1.Adım: Başla

2.Adım: Anahtarı al.

3.Adım: Anahtarı çöz ve boş matrisi oluştur.

4.Adım: Orijinal imge ve veri gömülmüş imgeyi anahtardaki boyut kadar tara.

5.Adım: Orijinal imge ve veri gömülmüş imgeyi karşılaştır. Farklı olan bitler için boş matrise 1 aynı olan bitler için 0 ata.

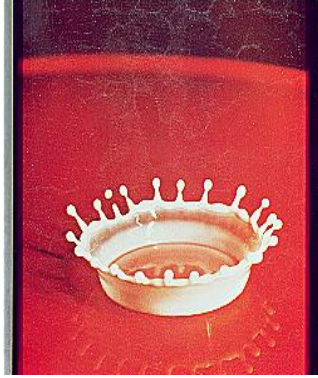
6.Adım: Boş matrisi 10'luk sayı sistemine çevir. Şifreyi elde et

7.Adım: Bitir.

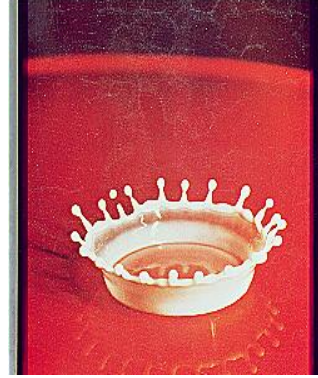
Şekil 6.52'deki veri gizlenmiş imge içerisinde çıkarılan veri aşağıdaki gibidir ve gömülen veri ile aynıdır.

“Ey Gönül! Damlayı anlayan deryayı nasıl aramasın, Deryayı bulansa damlayı nasıl bırakmasın? Ey fâni sevgili! Sen, Bâki Sevgilinin (c.c.) pırıltısını aksettiren bir damla nispetindesin, lakin görevin bitti artık perdeyi yırtma vaktidir. Zira perdenin ardından Derya bize göz kırpmada Üzülme! Dert etme can! Görebiliyorsan, dokunabiliyorsan, nefes alabiliyorsan, yürüyebiliyorsan... Ne mutlu sana! Elinde olmayanları söyleme bana... Elinde olanlardan bahset can! Üzülme! Geceler hep kimsesiz mi geçecek? Gidenler dönmeyecek mi? Yitirdiğin her ne ise; bir bakarsın yağmurlu bir gecede. Veya bir bahar sabahında karşına çıkmış... Bil ki! Güzellikler de var bu hayatta... Gel Git’lerin olmadığı bir hayat düşünebilir misin? “Hüzün olgunlaştırır” ...’Kaybetmek sabrı öğretir’... (Hz. Mevlana)”

Veri gömülmüş imgelere 4 farklı saldırı (keskinleştirme, bulanıklaştırma, imge ölçekleme ve imge döndürme) uygulanmıştır. Orijinal imge ile veri gömülmüş imge keskinleştirilme işleminden geçirildikten sonra elde edilen yeni imgeler Şekil 6.53 ve 6.54’da verilmiştir. Bu iki imge kullanılarak elde edilen PSNR oranı 66.3908 olarak bulunmuştur.



Şekil 6.53. Keskinleştirilmiş Veri Gömülen İmge

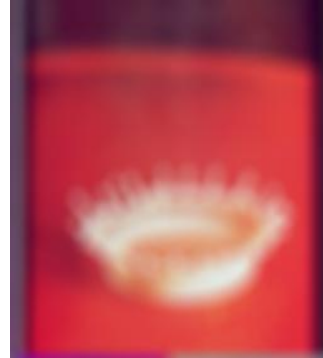


Şekil 6.54. Keskinleştirilmiş Orijinal İmge

Aynı şekilde bulanıklaştırma işlemi ile elde edilen imgeler Şekil 6.55 ve 6.56’de verilmiştir. PSNR değeri 65.6103’ tür.



Şekil 6.55. Bulanıklaştırılmış Veri Gömülen İmge



Şekil 6.56. Bulanıklaştırılmış Orijinal İmge

0.4 katsayısı ile ölçeklendirilen imgeler Şekil 6.57 ve 6.58 ile temsil edilmektedir. Bu iki imge arasındaki PSNR oranı 66.7045 olarak bulunmuştur.

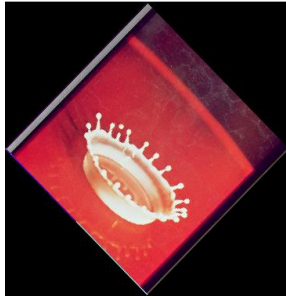


Şekil 6.57. 0.4 Oranında Küçültülmüş Veri Gömülen İmge



Şekil 6.58. 0.4 Oranında Küçültülmüş Orijinal İmge

Son olarak -45° döndürülen imgeler Şekil 6.59 ve 6.60'de gösterilmektedir. İşlem sonucunda elde edilen PSNR oranı 77.3815' tir.



Şekil 6.59. -45° Döndürülmüş Veri Gömülen İmge



Şekil 6.60. -45° Döndürülen Orijinal İmge

Sistem 256X256 boyutunda 20 imge için uygulanmış ve kendi geliştirdiğimiz yöntem ile gömülen verinin herhangi bir saldırı sırasında çözümünü zorlaştırmak için kullanılan 3 boyutlu resmin her bir boyutuna veri gömülmüştür. Gömme işlemi sırasında veri ikili kodlara dönüştürüldükten sonra, 8' er piksellik aralıklarla imge taranmaya başlanmıştır. İkili kodlara çevrilen verinin eğer bir elemanı 1 ise imgede taranan pikseli 1 arttırmaktadır. 0 olduğu durumlarda ise imgede taranan pikseli olduğu gibi bırakılmaktadır. Veri oluşturduğumuz algoritma paralelinde 3 boyutlu resme sırayla değil rastgele indislerle gömülmüştür. Oluşturulan veri tabanında ortalama PSNR değeri 68,3659 olarak bulunmuştur.

Yukarıdaki örnekte anlatılan tüm işlemler 20 imge için uygulanmıştır. Elde edilen PSNR değerleri Tablo 6.5.'de gösterilmiştir.

Tablo 6.5: Geliştirilen metot ile veri gizlenmiş imgelerin PSNR değerleri

İmgenin İsmi	Orijinal Veri gömülmüş imge	Keskinleştirilmiş veri gömülmüş imge	Bulanıklaştırılmış veri gömülmüş imge	-45 derece döndürülmüş veri gömülmüş imge	0.4 oranında ölçeklendirilmiş veri gömülmüş imge
1.BMP	65.7428	66.3908	65.6103	77.3815	66.7045
2.BMP	65.7428	66.3908	65.6103	77.3815	66.7045
3.BMP	65.7428	66.3908	65.6103	77.3815	66.7045
4.BMP	65.7428	66.3908	65.6103	77.3815	66.7045
5.BMP	65.7428	66.3908	65.6103	77.3815	66.7045
6.BMP	65.7428	66.3908	65.6103	77.3815	66.7045
7.BMP	65.7428	66.3908	65.6103	77.3815	66.7045
8.BMP	65.7428	66.3908	65.6103	77.3815	66.7045
9.BMP	65.7428	66.3908	65.6103	77.3815	66.7045
10.BMP	65.7428	66.3908	65.6103	77.3815	66.7045
11.BMP	65.7428	66.3908	65.6103	77.3815	66.7045
12.BMP	65.7428	66.3908	65.6103	77.3815	66.7045
13.BMP	65.7428	66.3908	65.6103	77.3815	66.7045
14.BMP	65.7428	66.3908	65.6103	77.3815	66.7045
15.BMP	65.7428	66.3908	65.6103	77.3815	66.7045
16.BMP	65.7428	66.3908	65.6103	77.3815	66.7045
17.BMP	65.7428	66.3908	65.6103	77.3815	66.7045
18.BMP	65.7428	66.3908	65.6103	77.3815	66.7045
19.BMP	65.7428	66.3908	65.6103	77.3815	66.7045
20.BMP	65.7428	66.3908	65.6103	77.3815	66.7045

7. SONUÇ

Bu tezde sayısal imgelere bilgi gizlemek için kullanılan steganografik yöntemler ve bu yöntemlerin güvenilirlikleri incelenmiştir. Bir steganografik sistem sağlamlık ve şeffaflık ölçütlerini sağlamalıdır. Şeffaflık saklanan verinin tespit edilememesi ve fark edilememesini ifade ederken sağlamlık saklanan verinin çıkartma işleminde düzgün bir şekilde geri getirilmesini anlatmaktadır.

Bir steganografik sistemin değerlendirilmesinde kullanılan etmenler ise taşıyıcıyı ne kadar değiştirdiği, saklayabileceği bilgi miktarı ve steganalitik saldırılara karşı ne kadar dayanıklı olduğunun incelenmesidir.

Taşıyıcıdaki değişimleri ölçebilmek amacıyla PSNR ve MSE değerleri hesaplanmaktadır. Burada yüksek PSNR değerlerine karşılık düşük MSE değerlerinin elde edilmesi imgenin fazla bozulmadığını yani taşıyıcıdaki değişimin fazla olmadığını göstermektedir. JPEG ve GIF formatındaki imge dosyaları özelliklerinden dolayı taşıyıcıdaki değişime daha duyarlıdır. Taşıyıcıdaki değişim açısından BMP dosyalar daha iyi sonuçlar vermektedir [105].

Steganografi’ de uygulanmış olan metotlar, temel olarak iki alt başlıkta incelenmektedir. Birincisi imge bandında yapılan uygulamalar, ikincisi ise frekans bandında yapılan uygulamalardır. İmge bandında yapılan uygulamalar genel olarak LSB tabanlıdır.

Bu tez çalışmasında ise yukarıda belirtilen amaçlar doğrultusunda renkli imgelerde veri gizleme için kullanılan yöntemler ayrıntılı bir biçimde incelenmiş ve yaygın olarak kullanılan LSB metoduna göre sayısal imgenin içerisine sıralı bir şekilde bilgi gizleyen bir uygulama geliştirilmiştir. Bu uygulama, steganografik sistem değerlendirme kriterleri olan taşıyıcıdaki değişim, kapasite ve dayanıklılık ölçütlerine göre değerlendirilmiştir. Değerlendirme sonuçları Bölüm 6’da sırasıyla Tablo 6.1-6.5’de verilmiştir. Uygulamanın dayanıklılık kriterine göre test edilebilmesi amacıyla bir steganaliz uygulaması geliştirilerek programın güvenilirliği incelenmiştir.

Geliştirilen bu metodun literatüre kattığı en büyük kazanım olarak, daha önce bu alanda LSB metodu kullanılarak yapılmış diğer çalışmalardan farklı olarak, imgenin piksel yapısı v.b. özelliklerine bağlı kalmaksızın, imge içerisine yerleştirilecek verinin PSNR oranının yüksek çıkması ve ayrıca bu yüksek PSNR oranının farklı imgelerde de aynı metin için değişmemesidir.

Bu kullanılan yöntemin dezavantajı olarak ta orijinal imge olmaksızın, içerisine veri gömülmüş imgeden verinin tekrar aslına uygun olarak çıkarılması çok zordur.

İleride bu alanda yapılacak çalışmalarda daha çok bu dezavantajı giderecek metotlar üzerine yoğunlaşılabilir.

KAYNAKLAR

- [1] Alwan R.H., Kadhim F.J., Al-Taani A.T., "Data Embedding Based on Better Use of Bits in Image Pixels", International Journal of Signal Processing Volume 2, Number 2, ISSN 1304-4494, 2005.
- [2] Adli, A.; Nakao, Z., "Three steganography algorithms for MIDI files," Machine Learning and Cybernetics, 2005. Proceedings of 2005 International Conference , Guangzhou, China, 4 : 2401- 2404 (2005).
- [3] Akleylek, S. Nuriyev, U., "Steganography and new implementation of steganography", Signal Processing and Communications Applications Conference, 2005. Proceedings of the IEEE 13th, Kayseri, TURKEY, 64-67 (2005).
- [4] Amin M. M., Salleh M., Ibrahim S., Katmin M. R., "Steganography: Random LSB Insertion Using Discrete Logarithm," Proceedings of 3rd International Conference on Information Technology in Asia (CTA03), pp. 234–238, 2003.
- [5] Anderson R.J, Petitcolas F.A.P., "On the Limits of Steganography", IEEE Journal of Selected Areas in Communications, 16(4):474-481, Special Issue on Copyright & Privacy Protection. ISSN 0733–8716, May 1998.
- [6] Al-Hamami, A.H., Al-Ani, S.A., "A New Aproach for Authentication Technique", Journal Of Computer Science Science Publications, 1 (1): 103- 106 (2005).
- [7] Amin, M.M., Salleh, M., Ibrahim, S., Katmin, M.R., Shamsuddin, M.Z.I., "Information hiding using steganography," Telecommunication Technology, 2003. NCTT 2003 Proceedings. 4th National Conference, Shah Alam, MALAYSIA, 21- 25 (2003).
- [8] Anderson,R.J., Petitcolas, F.A.P., "On The Limits of Steganography", IEEE Journal of Selected Areas in Communications, 16(4):474-481 (1998).
- [9] Aura, T., "Practical Invisibility in Digital Communication", First Workshop of Information Hiding Proceedings, Cambridge, pp 14 (1996).
- [10] Avcıbas, I., "Audio Steganalysis With Content Independent Distortion Measures," IEEE Signal Processing Letters, 13(2): 92-95 (2006).
- [11] Avcıbas, I., M. Kharrazi, N. Memon, B. Sankur, "Image Steganalysis With Binary Similarity Measures," EURASIP Journal on Applied Signal Processing, 2005(17): 2749-2757 (2005).

- [12] Avcıbas, I., N. Memon, B. Sankur, "Steganalysis Using Image Quality Metrics," IEEE Transactions on Image Processing, 12(2): 221-229 (2003).
- [13] Bender, W., Gruhl, D., Morimoto, N., and Lu, A. "Techniques for data hiding". IBM Syst. J., 35(3&4):313-336 (1996).
- [14] Brisbane, G., Safavi-Naini, R., Ogunbona, P., "High-capacity steganography using a shared colour palette," Vision, Image and Signal Processing, IEE Proceedings, 152: 787- 792 (2005).
- [15] Caldwell, 2nd Lt. J., "Steganography", CROSSTALK The Journal of Defense Software Engineering, 25-27 (2003).
- [16] Canbek, G., Sağiroğlu, S., "Bilgi ve Bilgisayar Güvenliği Casus Yazılımlar ve Korunma Yöntemleri", Grafiker, Ankara, 1-50 (2006).
- [17] Chou, J., Ramchandran, K., Ortega, A., "High capacity audio data hiding for noisy channels," Information Technology: Coding and Computing, 2001. Proceedings. International Conference, Las Vegas, 108-112 (2001).
- [18] Cvejic, N., Seppanen, T., "Increasing the capacity of LSB-based audio steganography," Multimedia Signal Processing, 2002 IEEE Workshop , St. Thomas, Virgin Islands, USA , 336- 338 (2002).
- [19] Farid, H., "Detecting steganographic message in digital images". Technical Report TR2001-412, Dartmouth College, 1-9 (2001).
- [20] Fridrich, J., Goljan, M., "Practical steganalysis of digital images state of the art.", Proc. SPIE Photonics West, 4675:1–13 (2002).
- [21] Fridrich, J., Goljan, M., Rui Du, "Detecting LSB steganography in color, and gray-scale images," Multimedia, IEEE , 8(4):22-28 (2001).
- [22] Fridrich, J., Du, R., Long, M., "Steganalysis of LSB encoding in color images," Multimedia and Expo, 2000. ICME 2000. 2000 IEEE International Conference , New York, USA , 3:1279-1282 (2000).
- [23] Fridrich, J., "Minimizing the embedding impact in steganography", Proceeding of the 8th Workshop on Multimedia and Security, Geneva- Switzerland, 2-10 (2006).
- [24] Gopalan, K., "Audio steganography using bit modification," , 2003 International Conference on Multimedia and Expo, Baltimore, Maryland, 629-632 (2003).

- [25] Johnson, N.F., Jajodia, S., "Exploring Steganography: Seeing the Unseen", IEEE Computer, 31(2):26-34 (1998).
- [26] Kaufman, C., Perlman, R., Speciner, M., "Network Security Private Communication in a Public World 2nd ed.", Prentice Hall, New Jersey, 62- 65, 81-84, 109, 140-141 (2002).
- [27] Kessler, G.C., "An Overview of Steganography for the Computer Forensics Examiner", Forensic Science Communications , 6(3):1-29 (2004).
- [28] Lee, Y.K., Chen, L.H., "High capacity image steganographic model," Vision, Image and Signal Processing, IEE Proceedings- , 147(3):288-294 (2000).
- [29] Paulson, L.D., "New System Fights Steganography.", IEEE Computer Society, 39(8):25 (2006).
- [30] Niimi, M., Noda, H., Kawaguchi, E., Eason, R.O., "High capacity and secure digital steganography to palette-based images," Image Processing 2002. Proceedings 2002 International Conference , Rochester, New York, USA, 2: 917-920 (2002).
- [31] Noda, H., Spaulding, J., Shirazi, M.N., Kawaguchi, E., "Application of bitplane decomposition steganography to JPEG2000 encoded images" Signal Processing Letters, IEEE 9(12):410-413 (2002).
- [32] Özer, H., Sankur, B., Memon, N., Avcibas, D., "Detection Of Audio Covert Channels Using Statistical Footprints Of Hidden Messages.", Digital Signal Processing 16 (4): 389-401 (2006).
- [33] Provos, N., Honeyman, P., "Detecting steganographic content on the internet," Tech. Rep. CITI 01-1a, University of Michigan, 1-14 (2001).
- [34] Rabah, K., "Steganography-The Art of Hiding Data.", Information Technology Journal, 3 (3):245-269 (2004).
- [35] Ru et al., "Audio Steganalysis Based On 'Negative Resonance Phenomenon' Caused By Steganographic Tools.", Journal of Zhejiang University Science A, 7(4):577-583 (2006).
- [36] Sağiroğlu, S., Alkan, M., "Her Yönüyle Elektronik Imza (e-imza)", Grafiker, Ankara, 3, 5, 33 (2005).
- [37] Sağiroğlu, S., Tunçkanat, M., "A Secure Internet Communication Tool", Turkish Journal of Telecommunications, 1(1):40-46 (2002).

- [38] Sankur B., N. Memon, I. Avcibas, "Automatic Detection of the Presence of Stegosignals and Watermarks in Images," European Conference on Visual Perception, Antalya,38 (2001).
- [39] Shahreza, S., "Stealth steganography in SMS" Wireless and Optical Communications Networks, 2006 IFIP International Conference, Bangalore, 5- (2006).
- [40] Srinivasan, Y., Nutter, B., Mitra, S., Phillips, B., Ferris, D., 2004. "Secure Transmission of Medical Records Using High Capacity Steganography". Proceedings of the 17th IEEE Symposium on Computer-Based Medical Systems (CBMS'04), Bethesda, Maryland, 122-127 (2004).
- [41] Sui, X.G., Luo, H., "A new steganography method based on hypertext" Radio Science Conference, 2004. Proceedings. 2004 Asia-Pacific, Qingdao, China , 181-184 (2004).
- [42] Swanson, M.D., Zhu, B., Tewfik, A.H., "Robust Data Hiding For Images", In 7th Digital Signal Processing Workshop (DSP 96), Loen Norway, 37-40 (1996).
- [43] Tseng, H.W., Chang, C.C., "Steganography using JPEG-compressed images" Computer and Information Technology, 2004. CIT '04. The Fourth International Conference , Wuhan, China ,12- 17 (2004).
- [44] Atıcı M.A., "Steganografik Yaklaşımlar ve Uygulamaları", Gazi Üniversitesi, Bilgisayar Mühendisliği Bölümü Yüksek Lisans Semineri, 2005.
- [45] Bender W., Gruhl D., Morimoto N., Lu A., "Techniques for data hiding", IBM Systems Journal, vol. 35, NOS 3&4, 1996.
- [46] Biryukov A., "Methods of Cryptanalysis", PHd Thesis, 1999.
- [47] Chaum D., "Untraceable Electronic Mail, Return DWTTresses and Digital Pseudonyms", Communications of the ACM, vol. 24, no. 2, pp. 84-88, February 1981.
- [48] CompuServe, "Graphics Interchange Format(sm), Version 89a", CompuServe Incorporated, Columbus, Ohio, 1990.
- [49] Cox I.J., Kilian J, Leighton T., Shamoon T., "A Secure, Robust Watermark for Multimedia", Proc. First Int'l Workshop Information Hiding, Lecture Notes in Computer Science No. 1, 174, Springer-Verlag, Berlin, 1996, pp. 185-206.
- [50] Erkin Z., Örencik B., "Steganografik Kütüphane", Ağ ve Bilgi Güvenliği Ulusal Semp. (ABG 2005) Bildiriler Kitabı, ISBN 975-395-885-4, s. 98-102, İstanbul, 9-11 Haziran, 2005.

- [51] Fridrich J., Goljan M., “Practical Steganalysis of Digital Images – State of the Art”, Proc. SPIE Photonics West, Vol. 4675, Electronic Imaging 2002, Security and Watermarking of Multimedia Contents, pp. 1-13, San Jose, California, January 2002.
- [52] Fridrich J., Du R., Meng L., “Steganalysis of LSB Encoding in Color Images”, Proceedings IEEE International Conference on Multimedia and Expo, New York City, NY, July 30–August 2, 2000.
- [53] Fridrich J., Goljan M., Hoge D., “Steganalysis of JPEG Images: Breaking the F5 Algorithm”, 5th Information Hiding Workshop, Noordwijkerhout, The Netherlands, pp. 310-323, 7–9 October 2002.
- [54] Gruhl D., Lu A., Bender W., “Echo Hiding”, in Proceeding of First International Workshop, Springer, Cambridge, UK, May-June, 1996.
- [55] Hartung F., Kutter M., “Multimedia watermarking techniques,” Proc. of the IEEE, vol. 87, pp. 1079–1107, July 1999.
- [56] Herodotus, “The Histories”, First Published in Greek 430 B.C.E., Translated by Selincourt A., Penguin Classics, Hammondsworth, 1971.
- [57] Johnson N.F., Duric Z., Jajodia S., “Information Hiding: Steganography and Watermarking - Attacks and Countermeasures”, Kluwer Academic Publishers, ISBN: 0-79237-204-2, 2000.
- [58] Johnson N.F., Jajodia S., “Exploring steganography: Seeing the Unseen”, Computer, 31, no 2:26-34, February 1998.
- [59] Johnson N. F., Jajodia S., “Stegananalysis of Images Created Using Current Steganography Software”, Second Information Hiding Workshop held in Portland, Oregon, USA, April 15-17, 1998. Proceedings LNCS 1525, 273-289, Springer-Verlag, 1998.
- [60] Johnson N.F., Rude T., “Introduction to Steganography Hidden Information”, Regional Computer Forensic Group (RCFG) and Mid-Atlantic Chapter of High- Technology Crime Investigation Association (HTCIA) George Mason University Computer Forensics Symposium (GMU 2001), Fairfax, VA, August 13-17, 2001.
- [61] Kahn D., “The Codebreakers”, Macmillan, New York, 1967.

- [62] Katzenbeisser S., Petitcolas F.A.P., "Information Hiding Techniques for Steganography and Digital Watermarking", Artech House, INC. 685 Canton Street Norwood, MA 02062, 2000.
- [63] Kharrazi M., Sencar H.T., Memon N, "Image Steganography: Concepts and Practice", WSPC/Lecture Notes Series, April 22, 2004.
- [64] Kim Y.S., Kim Y.M., Choi J.Y., Baik D.K., "Information Hiding System StegoWaveK for Improving Capacity", International Symposium, ISPA 2003 Aizu-Wakamatsu, Japan, July 2-4, Proceedings, Springer Berlin/ Heidelberg, ISSN 0302-9743, vol. 2745/2003, 2003.
- [65] Kutter M., Jordan F., Bossen F., "Digital Signature of Color Images using Amplitude Modulation", in Proceedings of SPIE storage and retrieval for image and video databases, San Jose, USA, February 13-14, 1997
- [66] Lai X., "On the Design and Security of Block Ciphers", ETH Series in Information Processing, v. 1, Konstanz: Hartung-Gorre Verlag, 1992.
- [67] Marvel L.M., Boncelet C.G., Jr. Retter C.T., "Reliable Blind Information Hiding for Images", in Proceedings of 2nd Workshop on Information Hiding (D.Aucsmith, editor), Lecture Notes in Computer Science, Springer, 1998.
- [68] Moerland T, "Steganography and Steganalysis", Universiteit Leiden, Rhone- Alpes, 2003.
- [69] Morkel T., Eloff J.H.P., Olivier M.S., "An Overview of Image Steganography", in Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, June/July 2005 (Published electronically)
- [70] Murray A.H., Burchfield R.W (eds.), "The Oxford English Dictionary: Being a Corrected Re-issue", Oxford, England: Clarendon Pres, 1933.
- [71] Newman B., "Secrets of German Espionage", London: Robert Hale Ltd., 1940.
- [72] Petitcolas F.A.P., Anderson R.J., Kuhn M.G., "Information Hiding—A Survey", Proceedings of the IEEE, Special Issue on Protection of Multimedia Content, 87(7):1062-1078, July 1999.
- [73] Pfitzmann B., "Information Hiding Terminology", In Anderson [3], pp. 347-350, ISBN 3-540-61996-8, 1996.

- [74] Phan R.C.W., Ling H.C., "Steganalysis of Random LSB Insertion Using Discrete Logarithms Proposed At Cita03", M2USIC03, PJ, Malaysia, 2-3 October 2003.
- [75] Pitas I., Nikolaidis N., "Copyright Protection of Images using Robust Digital Signatures", in IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP-96), vol. 4, pp. 2168-2171, May 1996.
- [76] Rivest R.L., "The MD5 Message Digest Algorithm", Request for Comments (RFC) 1321, Internet Activities Board, Internet PrivacZ Task Force, 3RIPEDM-1281, April 1992.
- [77] Popa R., "An Analysis of Steganographic Techniques", Ph.D Thesis, 1998.
- [78] Potdar V.M., Chang E., "Grey Level Modification Steganography for Secret Communication", Industrial Informatics, INDIN '04. 2004 2nd IEEE International Conference, pp. 223-228, ISBN: 0-7803-8513-6, 24-26 June 2004.
- [79] Terzija, N., Repges, M., Luck, K. and Geisselhardt, W., "Digital Image Watermarking Using Discrete Wavelet Transform: Performance Comparison of Error Correction Codes", *2nd IASTED International Conference, Visualization, Imaging and Image Processing*, Benalmadena, Malaga, Spain, 2002.
- [80] Talukder, K. H and Harada, K., "Haar Wavelet Based Approach for Image Compression and Quality Assessment of Compressed Image", *IAENG International Journal of Applied Mathematics*, 36 (1), 2007.
- [81] Chen, P. Y. and Lin, H. J., "A DWT Based Approach for Image Steganography", *International Journal of Applied Science and Engineering*. 4 (3), 275-290, 2006.
- [82] Delp, E. J., Saenz, M. and Salama, P., "Block Truncation Coding (BTC)", *Handbook of Image and Video Processing: BTC*.
- [83] Tu, S. F. and Hsu, Ch. Sh., "BTC-Based Watermarking Scheme for Digital Images", *Information and Security, An International Journal*, 15 (2), 216- 228, 2004.
- [84] Franti, P., Nevalinen, O. and Kaukoranta T., "Compression of Digital Images By Blok Truncation Coding: Survey", *The Computer Journal*, 37 (4), 308-332, 1994.

- [85] Wang, H. and Wang, S., "Cyber Warfare: Steganography vs. Steganalysis", *Communications of the ACM*, 47 (10), 76-82, 2004.
- [86] Barni, M., Bartolini, F., Cappellini, V. and Piva, A. 1998. A DCT-domain system for robust image watermarking. *Signal Processing*, 66, 357-372.
- [87] Huang, J., and Shi, Y.Q. 1999. Embedding strategy for image watermarking in DCT domain. *Proceedings of APCC/OECC'99*, pp. 981-984.
- [88] Liu, F. and Liu, Y. 2008. A watermarking algorithm for digital image based on DCT and SVD. *Congress on Image and Signal Processing*, pp. 380-383.
- [89] Lu, Z-M., Zheng, H-Y. and Huang, J-W. 2007. A digital watermarking scheme based on DCT and SVD. *Third International Conference on International Information Hiding and Multimedia Signal Processing*, pp. 241-244.
- [90] Gonzalez, R.C., Woods, R.E., *Digital Image Processing*, DWTison Wesley, 2002, (ISBN: 0-20-118075-8), 124.
- [91] Ruanaidh, J.O., Dowling, W.J., Boland, F.M., Phase Watermarking of Digital Images, *Proc. IEEE Int. Conf. Image Processing (ICIP)*, 239-242, 1996.
- [92] Herrigel, A., et al., Secure Copyright Protection Techniques for Digital Images, in *Information Hiding*, LNCS 1525, 169-190, 1998.
- [93] Pereira, S., et al., Template Based Recovery of Fourier-Based Watermarks Using Log-Polar and Log-Log Maps, *Proc. IEEE Multimedia Systems 99, Int. Conf. Multimedia Computing and Systems*, Florence, Italy, 870-874, 1999.
- [94] Schott G., "Schola steganographica: in classes octo distributa....", Jobus Hertz, printer, 1680, bound with: Gasparis Schotti...Technica curiosa... Herbipoli, [Courtesy of Whipple Science Museum, Cambridge.], 1665.
- [95] Sellars D., "An Introduction to Steganography", Online book, 1999.
- [96] Simmons G., "The Prisoners' Problem and the Subliminal Channel", *CRYPTO83 Advances in Cryptology*, pp. 51-67, Aug 22 -24, 1984.
- [97] Stinson D.R., "Cryptography: Theory and Practice, Second Edition", CRC Press, 2002.
- [98] Swanson M., Kobayashi M., Tewfik A., "Multimedia Data Embedding and Watermarking Technologies", *Proc. of IEEE*, vol. 86, no. 6, pp. 1064-1087, June 1998.

- [99] Şahin A., Buluş E., Sakallı M.T., “24-Bit Renkli İmgeler Üzerinde En Önemsiz Bite Ekleme Yöntemini Kullanarak Bilgi Gizleme”, Trakya Üniversitesi Fen Bilimleri Dergisi, Edirne-Türkiye, 2006.
- [100]Şahin A., Buluş E., Sakallı M.T., “Gri Seviye İmgeler Üzerinde Rasgele LSB Yöntemini ve Sayı Teorisini Kullanarak Bilgi Gizleme ve Steganaliz”, Akademik Bilişim Konferansları 2006-AB2006, Denizli-TÜRKİYE, Şubat-2006.
- [101]Tunçkanat M., Sağıroğlu Ş., “Güvenli İletişim İçin Yeni Bir Yaklaşım: İmge İçerisine Döküman Gizleme”, GAP IV. Mühendislik Kongresi (Uluslar arası Katılımlı), Şanlıurfa, vol.1, s.665-668, 6-8 Haziran 2002.
- [102]Wang H., Wang S., “Cyber Warfare: Steganography vs. Steganalysis”, Communications of the ACM, vol. 47, no. 10, October 2004.
- [103]Westfeld, A., “High Capacity despite Better Steganalysis (F5–A Steganographic Algorithm)”, In: Moskowitz, I.S. (eds.): Information Hiding. 4th International Workshop. Lecture Notes in Computer Science, Vol.2137. Springer-Verlag, Berlin Heidelberg New York, 289–302, 2001.
- [104]<http://www.grafikerler.org/sanat-fotograflari/27388-dali-atomicus-photoshop-kullanilmayan-saheser.html>, 28.12.2010.
- [105]Şahin A., “Görüntü Steganografide Kullanılan Yeni Metodlar ve Bu Metodların Güvenilirlikleri”, Doktora Tezi 93-94, Edirne 2007.

ÖZGEÇMİŞ

1986 yılında Tunceli’de doğdu. İlk, orta ve lise öğrenimini Elazığ’da tamamladıktan sonra 2005 yılında Fırat Üniversitesi, Teknik Eğitim Fakültesi, Elektronik Bilgisayar Eğitimi Bölümü, Bilgisayar Öğretmenliğini kazandı. 2009 yılında bu bölümden mezun oldu. Yine 2009 yılında Fırat Üniversitesi, Fen Bilimleri Enstitüsü, Elektronik Bilgisayar Eğitimi Bölümü, Telekomünikasyon Anabilim Dalında yüksek lisans eğitimine hak kazandı. 2010 yılında Tunceli ilinin Pertek ilçesinde Cumhuriyet İlköğretim Okulunda sözleşmeli bilgisayar öğretmeni olarak göreve başladı. Halen Cumhuriyet İlköğretim Okulundaki görevini sürdürmektedir. Yabancı dili İngilizce’dir.