SIR PAYLAŞIMI TABANLI ELEKTRONİK GÖRSEL ŞİFRELEME SİSTEMİ

İbrahim Levent Belenli

Yüksek Lisans Tezi

Yazılım Mühendisliği Anabilim Dalı

Danışman: Doç. Dr. Engin AVCI

NİSAN-2015

T.C

FIRAT ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

SIR PAYLAŞIMI TABANLI ELEKTRONİK GÖRSEL ŞİFRELEME SİSTEMİ

YÜKSEK LİSANS TEZİ

İbrahim Levent BELENLİ

121137106

Tezin Enstitüye Verildiği Tarih: 10.04.2015

Tezin Savunulduğu Tarih: 24.04.2015

Tez Danışmanı : Doç. Dr. Engin AVCI (F.Ü.)

Diğer Jüri Üyeleri : Doç. Dr. Ali KARCI (İnönü Üniversitesi)

Yrd. Doç. Dr. Mustafa ULAŞ (F.Ü.)

NİSAN-2015

ÖNSÖZ

"Sır Paylaşımı Tabanlı Elektronik Görsel Şifreleme Sistemi" adlı çalışma, günümüzde hızla gelişmekte olan ve geliştikçe saldırılara daha çok maruz kalan web teknolojilerinin güvenlik seviyelerine katkı sağlayabileceği düşünülerek, Fırat Üniversitesi Fen Bilimler Enstitüsü Yazılım Mühendisliği Anabilim Dalında, Yüksek Lisans Tezi olarak hazırlanmıştır.

Çalışmalarım esnasında bilgisi, tecrübesi ve önerileriyle hep yanımda olan ve üzerimde büyük emeği bulunan danışman hocam sayın Doç. Dr. Engin AVCI'ya teşekkürü bir borç bilirim.

Hayatımın her aşamasında bana sonsuz destek olan sevgili anneme ve babama saygılarımı ve teşekkürlerimi sunarım.

Bu çalışma kapsamında hazırlamış olduğumuz 2130120 numaralı ve *"SIR PAYLAŞIMI TABANLI ELEKTRONİK GÖRSEL ŞİFRELEME SİSTEMİ"* adlı projemize, 1512 kodlu Girişimcilik Aşamalı Destek Programı kapsamında sağlamış oldukları desteklerden dolayı TÜBİTAK'a teşekkür ederim.

Ayrıca yine aynı çalışma kapsamında hazırlamış olduğumuz *"A SECURE WEB APPLICATION BASED VISUAL CRYPTOGRAPHY AND SECRET SHARING"* adlı makaleyi titizlikle inceleyip, dergilerinde JMESTN42350539 numarası ile yayınlayan Journal of Multidisciplinary Engineering Science and Technology (JMEST) editörlerine teşekkür ederim.

İbrahim Levent BELENLİ

Elazığ - 2015

İÇİNDEKİLER

ÖZET

Günümüzde bilgiye sürekli erişimi sağlamak ve bu bilginin son kullanıcıya kadar bozulmadan, değişikliğe uğramadan ve başkaları tarafından ele geçirilmeden güvenli bir şekilde sunulması zorunluluk haline gelmiştir. Siber dünyada barış ve savaş durumunun zaman ve mekân sınırları belirsizleşmiştir. Genellikle bilgi güvenliği sağlamak için kullanılan ve en çok bilinen metot şifrelemedir. Şifrelemede ise metin şifreleme algoritmaları yaygın bir şekilde kullanılmaktadır.

Bu çalışmada ise metin verisi yerine resim verisi kullanılmaktadır. Çünkü resim verisi metin verisine göre daha büyük bir veri olduğundan ve oluşturulacak şifre resimlerinin birden fazla kişiye dağıtılması ve şifrenin meydana gelebilmesi için bu resimlerin bir araya gelmesi gerektiğinden, oluşturulacak şifrelemenin daha güçlü ve çözülmesi çok daha zor olacağı ön görülmektedir. Yukarıda sayılan sebeplerden dolayı bilgi güvenliğinin önemi hızla artmaktadır. Bilgi güvenliği sağlamak için en sık kullanılan yöntem kriptolojidir.

Kriptoloji çok geniş bir bilim dalı olup iki ana başlık altında incelenmektedir. Bu başlıklar kriptografi ve kriptoanalizdir. Kriptografi bir veriyi şifreleme sanatıdır. Kriptoanaliz ise kullanılan şifreleme algoritmasının ne kadar kullanışlı olduğunu tespit eden bilim dalıdır.

Sır paylaşımı teknikleri kriptografi de kullanılan tekniklerden birisidir ve şifrelenecek veriyi parçalara bölüp sır sahiplerine dağıtmayı amaçlamaktadır. Bu amacı gerçekleştirmek için birçok çalışma yapılmıştır. Son yıllarda yapılan çalışmalarla beraber sır paylaşımı teknikleri yeni özelliklerle desteklenmiştir. Bu özellikler; bilgi güvenliğinin daha da artırılması, gizlenen verilerin bellekte kapladığı alanın azaltılması ve kullanılan parametrelerin değişmesini içermektedir.

Bu tez çalışmasında kriptoloji teknikleri ve sır paylaşım teknikleri derinlemesine ele alınmış ve bu teknikler kullanılarak web tabanlı bir güvenlik uygulaması geliştirilmiştir. Ayrıca yöntemlerin birbirlerine karşı avantaj ve dezavantajları belirlenmiş ve hangi durumlarda hangi yöntemin kullanılmasının daha doğru olacağı hakkında da fikirler sunulmuştur.

Anahtar Kelimeler: Sır paylaşımı, Sır resim paylaşımı, Genetik algoritma, Eşik yöntem, Bilgi güvenliği, Görüntü işleme

SUMMARY

ELECTRONİC VİSUAL CRYPTOGRAPHY SYSTEM BASED ON SECRET SHARİNG

Nowadays, provide continuous access to information which is unchanged and safely without being seized by others submission has become a necessity. In the cyber world, the peace and war has blurred in terms of the boundaries of time and space. Generally, encryption is the most widely known method in order to ensure information security. Text encryption algorithms is are widely used ones.

In this study, the image data is intended to be used instead of text data. The fact that the image data is larger than text data. Photos of passwords will be distributed to more than one person and in order to occur the password in these images is a need to come together. In conclusıon, encryption is more potent and to be much more difficult to be solved. For the reasons stated above, importance of information security is rapidly increasing.In order to ensure information security, cryptography is the most commonly used method.

Cryptology is a wide branch of science and is studied in two main branches. This is divided into two main branches, cryptography and cryptoanalisis. Cryptography is the art of data encryption. Cryptoanalisis determines how useful is encryption algorithm used.

Secrets of sharing techniques in cryptography is one of the techniques used and aims the data to be encrypted divide and distribute to secret owner. To accomplish this goal, many studies is complited. In recent years, together with the study of secret sharing technique is supplemented with new features. These features comprises to enhance further the security of information, to reduct space of hidden data stored in the memory and the change of the parameters used.

In this thesis study, cryptography methods and the secret sharing methods will be discussed in deeply. Using these techniques, a web-based security application is developed. Methods determine the advantages and disadvantages against each other and in which cases it would be more accurate idea about which method will be used.

Keywords: Secret sharing, Secrets image sharing, Genetic algorithm, Threshold method, Information security, Image processing.

ŞEKİLLER LİSTESİ

Sayfa No

KISALTMALAR LİSTESİ

DSA : Digital Signature Algorithm
SHA : Secure Hashing Algorithm
RSA : Rivest, **S**hamir, **A**dleman
ECC : Elliptic Curve Criptography
3DES : Triple Data Encryption Standard
AES : Advanced Encryption Standard
BMP : Windows Bitmap
DES : Data Encryption Standard
GIF : Graphics Interchange Format
HTML : HyperText Markup Language
IDEA : International Data Encryption Algorithm
IP : Internet Protocol
JPEG : Joint Photographic Experts Group
LSB : Least Significant Bit
MD5 : Message-Digest Algorithm 5
MPEG : Moving Picture Experts Group
PAE : Peak Absolute Error
PNG : Portable Network Graphics

1. GİRİŞ

Naor ve Pinkas'ın makalelerinde, görsel şifrelemenin online sistemlerde transparan uygulamasının yapılabileceğini öngörülmüştür. İleri sürülen uygulamadaki temel amaç kimlik doğrulama ve kimliklendirme olarak belirlenmiştir [1].

Üzerinde çalıştığım Sır Paylaşımı Tabanlı Elektronik Görsel Şifreleme sistemi, mevcut şifreleme yöntemlerinin içerdiği birçok dezavantajı avantaja çevirmektedir. Bu dezavantajlardan en büyüğü yapılan saldırılar ile kullanıcıların şifrelerinin çalınmasıdır. Bu saldırılardan en çok kullanılanları trojan, keylogger veya screenlogger'lardır. Sır paylaşım tabanlı elektronik şifreleme sistemi bu ihtimali ortadan kaldırmayı hedeflemektedir. Şifreyi görselleştirip, elimizdeki görseli istenilen mik

tarda parçaya bölerek şifrenin güvenliğini sağlamak ve arttırmak amaçlanmaktadır.

Örneğin bir define haritası düşünelim bu haritayı 8 ayrı parçaya bölelim ve her bir parçayı 8 ayrı kişiye verelim. Bu işlemi gerçekleştirdikten sonra definenin yerinin bulunması için bu 8 kişinin bir araya gelmesi gerekmektedir. Böylelikle definenin yerinin bulunması daha zor hale getirilerek güvenlik artırılmış olacaktır. Bu prensiple çalışan sır paylaşımı tabanlı güvenlik sistemi kullanılarak sistem daha güvenilir hale getirilmektedir. Çalışmalar sonucunda yapılmak istenen, şifreyi görselleştirip parçalara bölmek ve parçalar bir araya geldiği zaman şifrenin ortaya çıkmasını sağlamaktır.

Görsellerin (resim ve video) boyutları kullanılan klasik şifrelerin boyutlarından büyük olduğu için klasik metin şifrelerden daha güçlü olacağı öngörülmektedir. Microsoft, garanti bankası internet bankacılığı, mobil uygulamalar ve daha birçok sistem artık görsel şifreleme uygulamalarına geçmiş bulunmaktadır. Örneğin 40 karakterlik hex kod olan mobil imzanın 16 üzeri 40, yani 2 üzeri 160 adet kombinasyonu vardır ancak 100X100'lük resim shamir (k,n) eşikleme algoritmasına göre şifrelendiğinde 2 üzeri 10000 adet kombinasyon elde edilecektir. Ayrıca bu şifre parçaları n adet parçaya bölündüğünde bu ihtimal daha çok artacak ve şifreyi çözmek bir o kadar zorlaşacaktır. Banka zarflarında görülen sır paylaşım tabanlı görsel şifreleri tamamen elektronik ortamda taşımak amaçlanmaktadır. Ayrıca şifre parçalarının iletişimini güvenlik altına alabilmek için

steganografik teknikler kullanılarak bilgi güvenliği bir kademe daha ileri seviyeye taşınacaktır.

E- imza ve güvenlik işiyle dünyanın en saygın firmaları ilgilenmektedir. Türkiye'de tübitak, e-tuğra vb. firmalar elektronik imzada söz sahibidir.

E- imza oluşturma algoritmaları aşağıda verilmiştir.

1.DSA: El gammal şifreleme yöntemi tabanlıdır. Modüler artimetik kullanan deterministik bir sistemdir.

2.RSA: Sık kullanılan bir algoritmadır. Asal sayı tabanlıdır. Güvenilir bir sistemdir.

3.SHA: Günümüzde e- imzalarda en çok kullanılan algoritmadır. Özetleme fonksiyonları kullanılır. 2013 yılında SHA-3 kabul edildi.

4.ECC: Elliptic Curve Criptography eliptik polinomal sistemlerden üretilen şifrelerdir. Herhangi bir eliptik polinom seçilerek oluşturulur [2].

Günümüzde e-imza üretmek için yukarıdaki algoritmalar kullanılır. Bu algoritmalardan en yaygını SHA tabanlı e-imza üreteçleridir. Ancak son yıllarda ECC algoritmasıyla ilgili çalışmalarda yoğunlaşmıştır. ECC algoritmasının en büyük avantajlarından biri ise anahtar boyutunun küçük olmasıdır. Anahtar boyutu küçüldükçe şifreleme hızı ve şifrelemenin kullanışlılığı artmaktadır. Sır paylaşım tabanlı elektronik görsel şifreleme sistemi de polinomal bir sistemdir [2].

Sır paylaşım yöntemleri ve eşikli şifreleme, şifreleme anahtarının yönetimini sağlamayı hedeflerler. Temel fikir anahtarın hiç bir alt grup veya tarafın tek başına elde edilemeyeceği şekilde bir gruba dağıtılmasıdır. Etkin olarak, bu şifreleme ve şifre çözme işlemi için grubun bir araya gelmesini gerektirir. Sır paylaşım yöntemleri bir sırrı parçalara bölerek grup üyelerine dağıtılmasını öngören ve sadece belirlenmiş alt grupların sırrı yeniden oluşturmasına olanak sağlayan, diğerlerine ise hiç bir bilgi sızdırmayan yöntemlerdir.

(k,n) eşikli şifreleme ise paylaşılan sırrın oluşturulması için toplam n grup üyesiden k'sının bir arada olmasını gerektiren ve k-1 veya daha az kişinin sır hakkında hiç bir bilgi edinemediği yöntemdir. Paylaşılmış sır oluşturulması, herhangi bir hesaplama ile değil doğrudan göz ile gerçekleştirilmektedir. İki slaytın üst üste konmasıyla şifre çözülmektedir. İki resmin bitleri VEYA işlemine tabi tutulur. 0 ve 1'in pixel gösterimi bir çok şekilde yapılabilir. Her bir pixel, iki yarım pixel'in bileşeni olarak gösterilir. İki resmin (sır parçasının) her bir pixeli rassal bir şekilde ya yarı-siyah yarı-beyaz yada yarı-beyaz

yarı-siyah'tır. Sır parçaları, sır olan resim üstündeki siyah pixeller siyah, beyaz pixellerde yarı-siyah yarı-beyaz olacak şekilde oluşturulmaktadır. Temel Fikir: y=f(x)=a0+a1x+a2x 2+...+ak-1xk-1 şeklinde ifade edilen k-1 dereceli polinom farklı x değerleri alan k nokta ile eşsiz bir şekilde tanımlanabilir.

Lagrange İnterpolasyon Teoremi: İki boyutlu bir düzlem üstünde verilen k farklı (x1,y1), (x2,y2)...,(xk,yk) noktası için yi=f(xi)?i sağlayan k-1 veya daha düşük dereceli f(x) polinomu şu şekilde yazılabilir. Shamir reel aritmetik kullanmak yerine, polinom interpolasyonunu modüler aritmetik kullanarak Zp sınırlı alanında gerçekleştirmiştir. Paylaşılan sırrın oluşturulması veya daha fazla kişiden oluşan bir grup bir araya gelip parçalarını birleştirirlerse, Langrange polinom interpolasyonu ile ai, 1'i k-1, katsayılarını ve hesaplayabilir. k-1 veya daha az kişiden oluşan gruplar sır hakkında hiç bir bilgi edinemez [3].

Tüm S'ler için verilen k-1 noktayı içeren eşit olasılıklık bir polinom bulunabilir (mükemmel gizlilik). Parçaları dağıtan kişinin güvenilir olduğu kabul edilmektedir. Parçaların doğruluğunu kontrol etmek için doğrulanabilir metotlar kullanılır. Gerçekleştirilmesi planlanan sır paylaşımı tabanlı elektronik görsel şifrenin çalışma adımları aşağıdaki gibidir.

1. Şifre Üret.

2. Şifreyi görselleştir.

3. Herhangi bir sır paylaşımı metodu seç.

4. Sırrın kaç parçaya bölüneceği ve kaç adet parça bir araya gelirse sırrın ortaya çıkacağını belirle (örneğin (2,8) sır 8 parçaya bölünecek ve herhangi iki parça bir araya gelince sır meydana çıkacak.).

5. Sırrı oluşturan parçalardan birini veri tabanına kaydet, diğer parçayı ise kullanıcı veya kullanıcılara ver.

6. Sırrın iletişim yolunda güvenliğini sağlamak için steganografik metotlar kullan.

2. YAPILMIŞ ÇALIŞMALAR

Korunması gereken verilerin güvenliğinin sağlanabilmesi için, sır paylaşımı tabanlı güvenlik yöntemleri kullanılmadan önce farklı güvenlik yöntemleri kullanılmıştır. Bu yöntemlerden en bilindik olanları RSA ve DES şifreleme yöntemleridir. Bu yöntemler bilinen bazı dezavantajlarından dolayı ya tam anlamıyla kullanılamamış yada DES'in 3DES'e dönüşmesi gibi evrimleşerek başka şekiller ile kullanılmaya devam edilmiştir. Bu yöntemlerin dezavantajlarından bazıları şunlardır; anahtarın korunması esnasındaki güvenlik problemleri, anahtarın kime verileceği, bilgilerin nasıl depolanacağı vb. Ortaya çıkan bu ve bunun gibi problemler sonucunda mevcut yöntemlere olan güvenin azalmasından dolayı sır paylaşımı tabanlı güvenlik yöntemleri önerilmiştir [4].

Sır paylaşımı tabanlı güvenlik yöntemlerinin geliştirilmesi konusunda yapılan ilk çalışmalar lisans derecesini matematik alanında almış olan İsrail'li bilim adamı Adi Shamir tarafından gerçekleştirilmiştir. Shamir seçtiği rasgele parametreleri kullanarak polinom tabanlı bir sır paylaşım yöntemi geliştirmiştir. Geliştirdiği bu eşik yöntem, bilginin n parçaya bölündükten sonra, bu n parçadan t tanesinin bir araya gelmesiyle sırrın yeniden elde edilmesini içermektedir [5].

Shamir'in çalışmalarını sürdürdüğü esnada Amerikalı matematikçi George Blakley'de benzer çalışmalar gerçekleştirmiştir. Shamir ve Blakley'in önermiş olduğu sır paylaşım modelleri, bu alanda yapılan ilk çalışmalar olarak tarihe geçmiştir [6].

Bu çalışmaların ardından Chin-Chen Chang adlı bilim adamı ekibiyle birlikte Blakley'in modelinin üzerine kurulu olduğu gelişmiş şifreleme yöntemini çözebilmek adına bir takım çalışmalar yapmışlardır. Yaptıkları bu çalışmalar sonucunda kullandıkları geometri tabanlı yöntem ile Blakley'in geliştirmiş olduğu sır paylaşım yöntemini çözmeyi başarmışlardır [7].

Ardından Noar ve Shamir, bu tez çalışmasına da konu olan, görsel sır paylaşımı adı verilen şifreleme yöntemi üzerinde çalışmaya başlamıştır. Yapılan bu çalışmalar kapsamında elde bulunan orjinal resmi, n adet gürültülü resim elde edilecek şekilde parçalanmıştır. Elde edilen bu parçaların her biri orijinal resim hakkında veri bulunduran gürültüden ibarettir. Bu parçaların gürültülerden ibaret olması sır parçalarının okunabilirliğini imkansız kılmaktadır. Bu parçalar pay sahiplerine dağıtıldıktan sonra, bu parçalardan t tanesi bir araya geldiğinde orijinal resim elde edilmektedir [8].

Cheng, Tsai, Harn ve Lin adlı bir grup bilim adamı, 1993 yılında sır paylaşım yöntemi üzerinde yaptıkları bir çalışma sonucunda, görsel şifreleme yönteminin 3. kişilere karşı olan güvenlik seviyesini bir miktar daha arttırmayı başarmışlardır [9,10].

Günümüzde internet hızının artması sonucu, internet üzerinden yapılan resim aktarımı ve resim dosyalarının kullanımı bir hayli artmıştır. Bu artışın sonucunda sır paylaşımı yönteminde görsel nesnelerin kullanılması daha fazla ilgi çekmeye başlamıştır. Huang ve Chang vektör niceleme tekniğini kullanarak resimleri şifrelemiş ve eşik yöntem kullanarak sır parçasını yeniden ortaya çıkarmışlardır [11]. Tsai'de benzer bir çalışma yaparak en az anlamlı biti birleştirerek pay sahipleri tabanlı çoklu sır paylaşım yöntemini önermiştir [12].

Plataniotis ve Lukac ise sır paylaşımı için kullanılacak sır parçalarını oluştururken diğerlerinden farklı bir yöntem olan bit seviyeli ayrıştırma yöntemini kullanmışlardır. Bu yöntem dahilinde resim bit düzeyinden ayrıştırılarak, bit düzleminde paylaştırma işlemi yapılmaktadır Sır parçaları birleştirilerek orijinal resmin kayıpsız şekilde elde edilebilmesi için ise renk vektörleri üzerinde ikili şifreleme işlemi uygulanmıştır [13,14].

3. KRİPTOLOJİ

Kriptoloji kelimesi Yunanca, “kryptos”(gizli) ve “logos” (bilim) kelimelerinin bir araya gelmesi ile meydana gelmiştir. Kriptoloji kelimesinin en temel anlamı şifreli belgeler, gizli yazılar olarak tanımlanabilir. Kriptoloji genel olarak “Kriptografi” ve “Kriptoanaliz” olmak üzere iki ana dala ayrılmaktadır [15].

Kriptografi; Yunanca, “kryptos” ve “graphein” (yazmak) kelimelerinin bir araya gelmesiyle ortaya çıkmıştır. Kriptografi, Belgelerin şifrelenmesi ve şifrelenen belgelerin şifrelerinin çözülerek okunabilir hale getirilebilmesi için kullanılan yöntemlere verilen addır. Kriptoloji hem şifreleme ve hem de bu şifrelerin çözülmesinde kullanılan tekniklerin tümünü incelemektedir.

Kriptoanaliz ise; hali hazırda oluşturulmuş olan bir şifreleme sistemini veya şifrelenmiş bir mesajı inceleyen ve şifreli mesajı çözerek orijinal halini elde etmeye çalışan kriptoloji disiplinidir. Temel manada, kriptografi bilimi ile daha önceden şifrelenmiş olan metinler, kriptoanaliz bilimi ile çözülmeye çalışılmaktadır.

Kriptoloji, insanoğlunun birbiriyle iletişim ihtiyacı hissettiği andan itibaren giderek büyük bir önem kazanmaya başlamıştır. Kriptoloji bilimine verilen önemin giderek artması ve kullanımının da giderek yaygınlaşmasıyla kriptoloji bilimi hayatımızın her alanında aktif rol almaya başlamıştır. Yüzlerce yıl önce; dünya üzerindeki devletler, düşmanın eline geçmemesi gereken önemli bilgileri iletmek istedikleri hedefe iletebilmek için güvercinler, ulaklar vs. kullanmışlardır. Fakat kullandıkları bu yöntemler mesajın istenmeyen kişilerin eline geçmesine engel olamamıştır. Kriptoloji biliminin ortaya çıkmasının yegane nedeni, iletilmesi hedeflenen bilginin gizli tutulmak istenmesidir.

Binlerce yıl önce, bilgilerin kodlaması (kelimelerin başka kelimelerle veya sayı yada sembollerin yerlerinin değiştirilerek) ile ortaya çıkan kriptoloji, o dönem için mesajın istenmeyen kişiler tarafından anlaşılmasını engellemek için yeterli olmuştur. Fakat geçen süre boyunca gelişen teknoloji ile birlikte bu yöntemler artık işe yaramamaya başlamış ve hızla tarih sayfalarındaki yerlerini almışlardır. Kriptoloji biliminde günümüzde matematik temellerine ve bilgisayarların işlem güçlerine dayalı olan elektronik sistemler hâkimiyet sürmektedir.

3.1. Kriptolojinin Tarihi

Kriptolojinin tarihi incelenmek istendiğinde, kriptoloji ile ilgili ilk kayıtlara M.Ö. 2000'li yıllarda Nil nehri kıyısında küçük bir şehir olan Menet Khufu'da rastlanmaktadır. Menet Khufu'daki bir kâtibin, efendisinin hayatını anlatırken kullandığı hiyeroglifler kriptoloji tarihinin ilk kayıtları olarak kabul edilmektedir. Bu hiyeroglifler üzerinde kullanılan simgeler sadece ilgili kişiler tarafından anlaşılabilmekte ve yapılan çalışmalar sonucunda bu hiyeroglifleri ilgili kişiler dışındakilerin anlamasının istenmediği sonucuna varılmaktadır. Bu hiyeroglifler üzerinde kullanılan simgelerin daha önce hiç kullanılmadığı düşünülmektedir. Bu durumun bilgi güvenliğini arttırmak amacıyla uygulanmış olan bir kriptoteknik olduğu kabul edilmektedir [16].

Kriptografi tekniklerini askeri haberleşme alanında kullanan ilk ulus ise Ispartalılardır. Ispartalılar'ın M.Ö. 5.yüzyılda geliştirdikleri Şekil 3.1'deki cihaz, tarihin ilk yer değiştirme sistemi olarak Isparta askeri birlikleri tarafından kullanılmıştır. Bu cihaz belli kalınlıkta bir tahta silindirden ve silindirin etrafına eğik biçimde sarılmış papirüs ya da ince, deri bir şeritten oluşmaktadır. Bu teknik ile gizli mesaj silindir üzerinde sarılı vaziyette bulunan şerit üzerine yazılmakta ve daha sonra şerit silindirden çözülerek mesajın okunabilirliği ortadan kaldırılmaktadır. Şeridin tahtadan ayrılmasıyla birbirinden ayrılan karakterler yeniden aynı kalınlıkta bir tahta silindire sarılmadıkça hiçbir anlam ifade etmemektedir.

Şekil 3.1 Ispartalıların Kullandıkları Kripto Cihazı

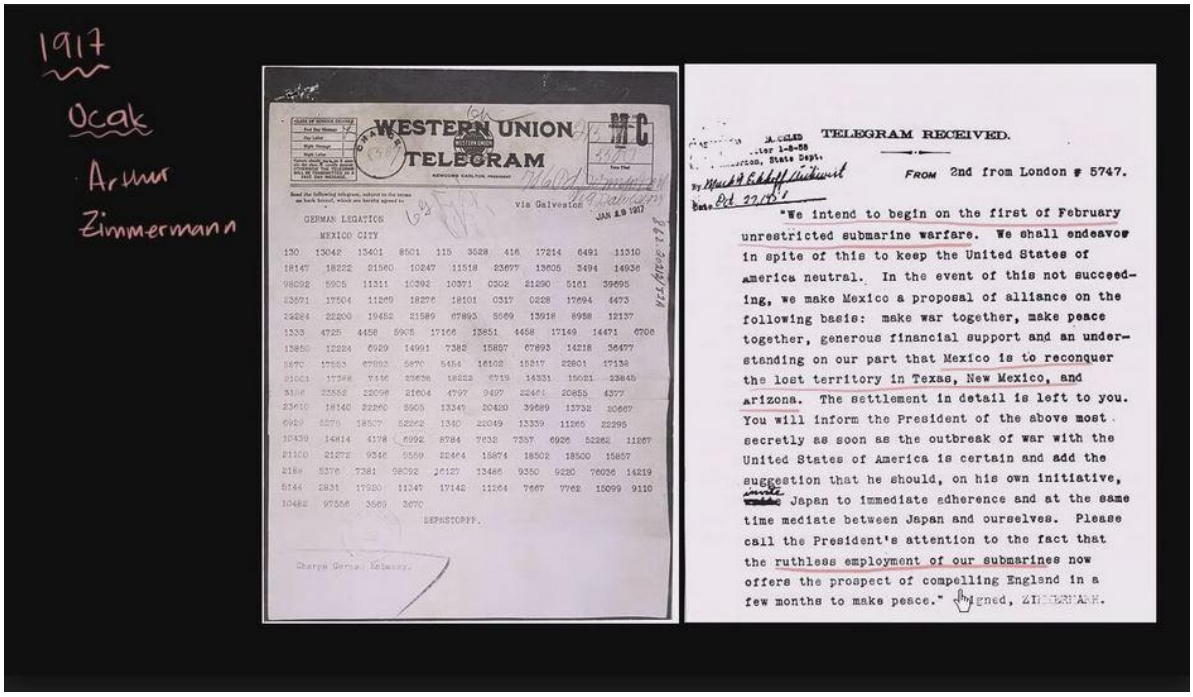
Tarihte kripto analiz çalışmaları ilk olarak Araplar tarafından yapılmıştır. Araplar tarafından kripto analiz faaliyetleri gerçekleştirilene kadar kriptoloji çalışmaları dahi yaygın şekilde gerçekleştirilmemiştir. Edebiyat ve matematik alanlarında çağın ötesinde olan Araplar kriptoloji çalışmalarına milattan sonra 600'lü yıllarda başlamışlardır. İngilizce "cipher" ve Fransızca "chiffre" kelimeleri şifre kelimesinin Arapça karşılığı olan "cifr" kelimesinden türeyerek bu dillere geçmiştir. Milattan sonra 718 yılında "Kitab-ül muamma" adlı kitap, Abdurrahman el-Halil tarafından yayınlanarak, kriptoloji alanında yazılan ilk eser olarak kayıtlara geçmiştir. Bu kitap Bizans imparatoru tarafından Yunanca yazılmış şifreli mektubun çözülmesi aşamalarını içermektedir [4].

Günümüzde kullanılan kriptoloji tekniklerine olan gereksinimin hissedilmesi ise ilk olarak birinci dünya savaşı olmuştur. Savaş esnasında kriptoloji yöntemlerinin haberleşme sistemlerine olan katkıları ve bu katkılardan dolayı çok sık kullanılması, savaş sona erdikten sonra hızla gelişen teknolojinin, kriptolojinin geliştirilmesinde daha fazla kullanılmasını sağlamıştır.

Fakat kriptolojinin öneminin artmasının asıl nedeni birinci dünya savaşı döneminde telsiz haberleşmenin icat edilmesidir. Telsiz haberleşmenin mantığı mesajın radyo dalgaları ile karşı tarafa iletilmesidir. Fakat bu radyo dalgalarının, bu dalgalara erişebilen herkes tarafından dinlenebilmesi mümkündür. Bu yüzden bu dalgalara erişebilen üçüncü kişilerin bertaraf edilebilmesi için yeni teknikler geliştirilmesi kaçınılmaz olmuştur.

Almanlar gönderilen mesajların üçüncü kişiler tarafından kolayca anlaşılmasını engellemek için "ADFGVX" ve "Kod Kitabı" yöntemlerini geliştirerek mesajlarını bu yöntemle şifrelemişler ve daha sonra mesajı iletme yolunu seçmişlerdir. Geliştirdikleri bu yöntemler metinlerin sayılar ile eşleştirilmeleri esasına dayanmaktadır. Örnek verecek olursak Almanların Zimmermann telgrafı olarak kayıtlara geçen mesajlarında "Fest" kelimesi 13732 sayısı ile "Februar" kelimesi ise 13605 sayısı ile kodlanmıştır. Fakat her ne kadar kriptoloji yöntemleri gelişse ve Almanlar bu yöntemleri kullanmış olsalarda, bu yıllarda kripto analiz yöntemleri de oldukça gelişmiş durumdadır. İngilizler yaptıkları analizler sonucunda Almanların geliştirmiş oldukları şifreleme sistemini çözerek savaşın seyrini değiştirmişlerdir (Şekil 3.2). Bu yüzden daha güçlü şifreleme sistemlerine ihtiyaç olduğu gün yüzüne çıkmıştır.

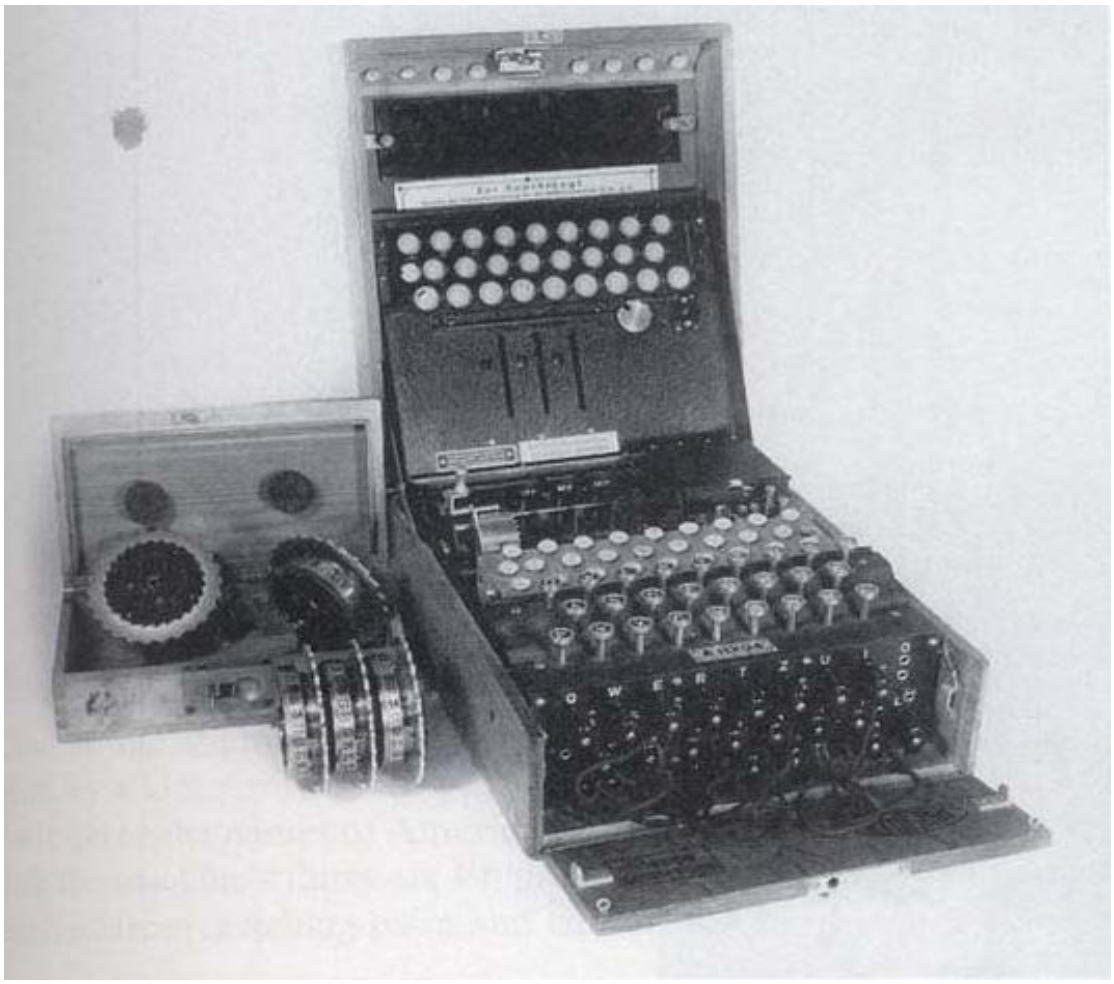
Sonuç olarak kriptografik yöntemler geliştirilmiş ve bu yöntemleri kullanan cihazlar gizli haberleşmelere yön vermeye başlamışlardır.



Şekil 3.2 Birinci Dünya Savaşında Almanların gönderdiği telgraf

İkinci dünya savaşında ise kriptolojinin savaşa olan etkisi çok daha büyük olmuştur. Kriptoloji yöntemlerini kullanan devletler, birliklerine göndermek istedikleri mesajı, üçüncü kişilerin anlamasının önüne geçerek istedikleri şekilde hedefe ulaştırabilmişlerdir. Almanların geliştirmiş ve kullanmış oldukları Enigma adlı şifreleme makinesi savaşın adeta seyrini değiştirmiştir (Şekil 3.3). Enigma elektronik bir cihaz olmasına karşın mekanik ayarlar ile yönlendirilmektedir. Geliştiricisi olan Arthur Scherbius bu cihazı ilk olarak bankalar arasındaki haberleşmeleri güvenli bir şekilde gerçekleştirmek amacıyla kullanmıştır. Fakat daha sonra Alman ordusunun bu cihazı kullanma kararı alması ile birlikte yüzbin adet Enigma üretilmiştir. 21. yy'a kadar bu kadar yüksek miktarda kripto cihazı üretilmemiştir.

Savaşın başlarında Almanların kazanmış oldukları büyük başarıların nedeni Enigma'nın şifresinin düşman tarafından henüz çözülememiş olmasıdır. Mesajlar telsiz haberleşme yoluyla radyo dalgaları kullanılarak karşı tarafa iletilse de öncesinde Enigma cihazı üzerinden yazılmış ve yazılan mesaj cihaz içerisinde şifrelenmiştir (Şekil 3.4).



Şekil 3.3 Enigma Kripto Cihazı

İngiliz ve Polonya'lı matematikçiler uzun süren kripto analiz çalışmaları sonucunda Enigma'nın ürettiği mesajların şifresini çözmüşlerdir. Bu çalışmalar sonucunda aslında Enigma'nın çokta güvenli bir cihaz olmadığı ortaya çıkmıştır. Bu gelişmelerden sonra savaşın seyri değişmiş ve Almanların elde ettikleri başarılar son bulmuştur. Fakat geliştirilen kripto analiz yöntemlerini zamanında uygulayabilmek için işlem gücü yüksek cihazlara olan ihtiyaç ortaya çıkmıştır. Böylece ilk bilgisayarlar geliştirilmiş ve kriptoloji biliminde yeni bir dönem başlamıştır.

Şekil 3.4 Enigma cihazı Alman muhabere birliği tarafından kullanılırken

3.2. Kriptografi Prensipleri

3.2.1. Gizlilik

Gizlilik prensibine bilginin üçüncü kişilerin eline geçmesinin engellenmesi için ihtiyaç duyulmaktadır. Gizlilik, hem kalıcı ortamlarda (hard disk vb.) tutulan veriler, hem de ağ üzerinde bir göndericiden bir alıcıya iletilmek istenen veriler için geçerlidir. Saldırganların, yetkili olmadıkları verilere erişebilmelerinin birçok yolu bulunmaktadır. Dosyalarda tutulan parolaların ele geçirilmesi ve sosyal mühendislik gibi yöntemler kullanılarak bir bilgisayar kullanıcının bilgileri, ona fark ettirmeden ele geçirilebilmektedir. Bunun yanında trafik analizinin, yani hangi gönderici ile hangi alıcı arası haberleşmenin olduğunun belirlenmesine karsı alınan önlemler de gizlilik hizmeti çerçevesinde ele alınmalıdır [17,18].

3.2.2. Süreklilik

Bilişim sistemleri kendisinden istenen görevleri ifa ederken, verilen bu görevi bitirdiğinde ulaşması gereken bir başarım değeri vardır. Bu başarım değerinin mümkün olduğunca yüksek tutulması gerekmektedir. Başarım değeri ne kadar yüksek olursa müşteri memnuniyeti o kadar artar ve süreç o kadar hızlanır. Süreklilik hizmeti, bilişim sistemlerini, kurum içinden ve dışından gelebilecek ve başarım değerlerini düşürebilecek tehditlere karşı korumayı hedeflemektedir. Süreklilik hizmeti sayesinde kullanıcılar, erişim yetkileri dâhilinde olan verilere, veri güncelliğini yitirmeden, zamanında ve güvenilir bir şekilde ulaşabilmektedir. Sistem sürekliliğinin güvenilirliği, yalnızca kötü amaçlı bir kullanıcının, sistem başarım değerini düşürmeye yönelik bir saldırısı sonucu zedelenmemektedir. Bilgisayar yazılımlarının geliştirme sürecinde yapılan hatalar, geliştirilen sistemin bilinçsiz ve eğitimsiz personeller tarafından kullanılması, ortam şartlarındaki değişimler (nem, ısı, yıldırım düşmesi, topraklama eksikliği) gibi faktörler de sistem sürekliliğini etkileyebilmektedir [17,18].

3.2.3. Veri Bütünlüğü

Kriptografi prensiplerinden veri bütünlüğünün amacı, veriyi, göndericiden çıktığı yani orijinal haliyle alıcıya ulaştırmaktır. Bu amacın gerçekleştirilebilmesi durumunda veri, haberleşme sırasında izlediği yollarda değiştirilmemiş, araya yeni veriler eklenmemiş, belli bir kısmı ya da tamamı tekrar edilmemiş ve sırası değiştirilmemiş şekilde alıcısına ulaştırılmış olmaktadır. Bu prensibin sağlanamaması durumunda bozulma, geri dönüşümü olan ve olmayan şeklinde sınıflandırılmaktadır. Veri alıcıya ulaştırıldıktan sonra alıcıda iki tür bütünlük sınaması yapılmaktadır. Bu sınıflandırmalar bozulma sınaması ve düzeltme sınamasıdır. Bozulma sınaması ile verinin göndericiden alıcıya ulaştırılması esnasında değiştirilip değiştirilmediğinin tespitinin yapılması hedeflenmektedir. Düzeltme sınamasında ise, bozulma sınamasına ek olarak eğer veride bir değişiklik tespit edilirse, bu veriyi göndericiden çıktığı orijinal haline döndürmek hedeflenmektedir [17,18].

3.2.4. İzlenebilirlik

Kriptografi prensiplerinden izlenebilirliğin amacı, sistemde gerçeklesen olayları, daha sonra analiz edilmek üzere kayıt altına almaktır. Burada olay olarak tanımlanan ifade, bilgisayar sistemi ya da ağı üzerinde olan herhangi bir faaliyeti anlatmaktadır. Sistem üzerinde yaşanabilecek olaylara: kullanıcının parolasını yazarak sisteme girmesi, bir web sayfasına bağlanması, e-posta alması veya göndermesi ya da facebook üzerinden mesaj yollaması gibi örnekler verilebilmektedir. Tüm bu olaylar gerçekleşirken toplanan kayıtlar üzerinde yapılacak analizler sonucunda, bilinen saldırı türlerinin örüntülerine rastlanırsa ya da bulanık mantık kullanılarak önce rastlanmayan ve saldırı olasılığı yüksek bir aktivite tespit edilirse sistem tarafından uyarı mesajları üretilerek sistem yöneticileri uyarılmaktadır [17,18].

3.2.5. Kimlik Sınaması

Kriptografi prensiplerinden kimlik sınamasının ağ güvenliği açısından tanımı, alıcının, göndericinin iddia ettiği kişi olduğundan emin olabilecek duruma gelebilmesidir. Ayrıca, bir bilgisayar programını kullanırken bir parola girmek de kimlik sınaması çerçevesinde değerlendirilmektedir. Günümüzde kimlik sınaması, sadece bilgisayar ağları ve sistemleri için değil, fiziksel sistemler için de çok önemli bir hizmet halini almıştır. Akıllı karta ya da biyometrik doğrulama teknolojilere dayalı kimlik sınama sistemleri hayatımızın neredeyse her alanında yaygın olarak kullanmaya başlanmıştır [17,18].

3.2.6. Güvenilirlik

Kriptografi prensiplerinden güvenilirlik, sistemin beklenen davranışı ile elde edilen sonuçlar arasındaki tutarlılık durumudur. Kısacası güvenilirlik prensibi, sistemden ne yapmasını bekliyorsak, sistemin de eksiksiz ve fazlasız olarak tam olarak istenilen şeyi yapması ve her çalıştırıldığında da tutarlı olarak aynı şekilde davranması olarak tanımlanabilmektedir [17,18].

3.2.7. İnkar Edememe

Kriptografi prensiplerinden inkar edememe prensibi sayesinde, ne gönderici alıcıya bir mesajı gönderdiğini ne de alıcı göndericiden bir mesajı aldığını inkâr edememektedir. Bu prensip, özellikle gerçek zamanlı işlem gerektiren finans sistemlerinde kullanım alanı bulmaktadır. Gönderici ile alıcı arasında ortaya çıkabilecek anlaşmazlıkların en aza indirilmesini sağlamaya yardımcı olmaktadır. Zaman içinde bilgisayar sistemlerine karsı ortaya çıkmış tehditler ve yaşanan bazı olaylar sonucunda bu prensinim gerekliliği anlaşılmıştır. Yani her bir prensip, belli bir grup potansiyel tehdide karsı sistemi korumaya yöneliktir, denilebilmektedir [17,18].

3.3. Kriptografik Algoritmalar

Şifreleme işleminin güvenli bir şekilde gerçekleştirilmesi şifreleme sırasında kullanılan tüm yöntem ve bilgilerin gizli tutulabilmesi prensibine dayanmaktadır. Ancak herhangi bir nedenle şifreleme esnasında kullanılan yöntem veya bilgilerden herhangi birinin açığa çıkabileceği düşünülerek iletişim güvenliği, şifreleme anahtarı denen bir ek yöntem kullanılarak arttırılmaktadır. Bu durumda şifreleme işlemi sırasında açık mesaj, şifre anahtarı kullanılarak şifrelenmektedir. Yani açık mesaj ile şifrelenmiş mesaj arasındaki geçişler şifreleme algoritmasına bağlı olduğu gibi aynı zamanda kullanılan anahtar bilgisine de bağlıdır. Günümüzde kullanılan kriptografik algoritmalar ikiye ayrılmaktadır. Bunlar, kullandıkları anahtar biçimine göre simetrik veya asimetrik olarak adlandırılmaktadır [19].

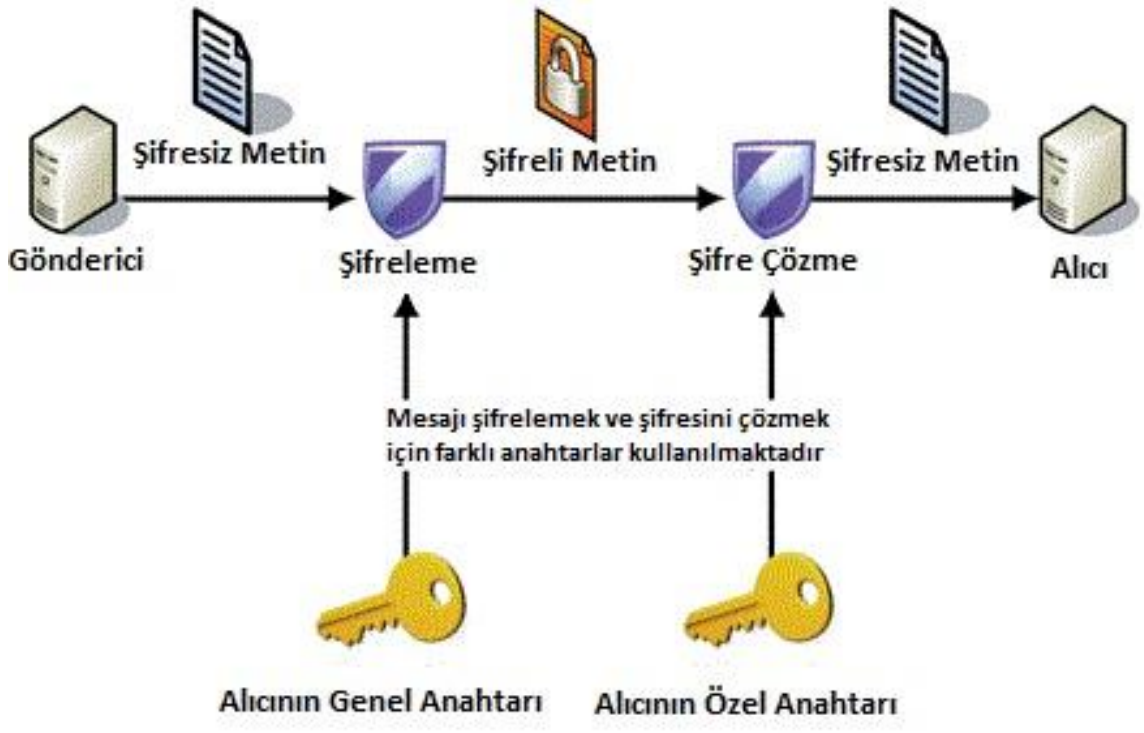
3.3.1. Simetrik Şifreleme Algoritmaları

Simetrik şifreleme algoritmaları kapsamında şifreleme ve şifre çözme işlemleri için tek bir anahtar kullanılmaktadır. Bu anahtar herkesin göremeyeceği gizli bir anahtardır. Simetrik şifreleme algoritması kullanılarak şifreleme işlemi gerçekleştirilmektedir. Daha sonra elde edilen şifreli metin gizli anahtar ile birlikte güvenli bir yol izlenerek alıcıya iletilmektedir [20,21]. Simetrik şifreleme algoritmaları şifreleme ve şifre çözme işlemlerini çok hızlı bir şekilde gerçekleştirebildiği için günümüzde yaygın bir şekilde

kullanılmaktadır. AES ve DES şifreleme algoritmaları simetrik şifreleme algoritmalarına örnek olarak verilebilir [22].

3.3.2. Asimetrik Şifreleme Algoritmaları

Simetrik şifreleme tekniğinin uygulanması esnasında karşılaşılan en büyük problem anahtar dağıtımının nasıl yapılacağıdır. Bu problemin giderilebilmesi için şifreleme ve şifrelenen verinin çözülmesi işlemlerinin her ikisi için farklı anahtarların kullanıldığı bir şifreleme sistemi tasarlanmıştır (Şekil 3.5) [23,24]. Tasarlanan sistemde şifreleme işlemi açık anahtar kullanılarak yapılmaktadır. Bu anahtar herkes tarafından bilinmektedir. Sistemin asimetrik şifreleme sistemi olarak bilinmesinin temel sebebi, şifreleme ve şifre çözme işlemlerinin birbirinin simetriği olmayan yani asimetrik algoritmalar kullanılarak gerçekleştirilmesidir [25].



Şekil 3.5 Asimetrik Şifreleme algoritmalarının yapıları

3.3.3. Şifreleme Algoritmalarının Performans Kriterleri

Bir şifreleme algoritmasının performansını değerlendirirken yaygın olarak şu kriterler kullanılmaktadır [26].

- Kırılabilme süresinin uzunluğu
- Şifreleme ve çözme işlemlerine harcanan zaman (Zaman Karmaşıklığı)
- Şifreleme ve çözme işleminde ihtiyaç duyulan bellek miktarı (Bellek Karmaşıklığı)
- Bu algoritmaya dayalı şifreleme uygulamalarının esnekliği.
- Bu uygulamaların dağıtımındaki kolaylık ya da algoritmaların standart hale getirilebilmesi
- Algoritmanın kurulacak sisteme uygunluğu

3.4. Kripto Analiz Çeşitleri

Kripto analiz; şifrelenmiş bir mesajı veya şifrelenmiş bir sistemi detaylı bir şekilde inceleyerek, şifrelenmiş bu mesaj veya sistemin şifrelenmeden önceki açık halini tespit etmeye çalışan kriptoloji disiplinidir.

3.4.1. Lineer Kripto Analiz

1993 yılında Matsui, bir sisteme yapılan saldırıyı teorik olarak keşfetmiştir. Daha sonra DES algoritmasına karşı lineer kripto analiz yöntemini başarı ile uygulamıştır. Lineer kripto analiz, şifreli metin bitleri ile, açık metin bitleri arasındaki yüksek olasılıkta lineer ifadelerin meydana gelme avantajını kullanmaktadır. Bunun yolu da S kutularından geçmektedir. Bu analiz yönteminde saldırganın algoritmayı bildiği ve belli sayıda açık metin ve şifreli metinlere sahip olduğu varsayılmaktadır. Fakat S kutularının büyük olması, aktif S kutularındaki artış, lineer sapma ve küçük S kutularının tasarımı lineer kripto analizin uygulanmasını engelleyici faktörler olarak öne çıkmaktadır [27].

3.4.2. Diferansiyel Kripto Analiz

Diferansiyel kripto analiz, metin şifrelenmeden önce metni oluşturan karakter değişikliklerinin, metnin şifrelenmesi sonucunda ortaya çıkan şifreli metin üzerine yapmış olduğu etkiyi analiz etmektedir. Bu etkiler mümkün olan anahtarların olasılıklarını ve mümkün olan en büyük anahtarı ortaya koymak için tayin edilmektedir [28].

3.4.3. İmkansız Diferansiyel Kripto Analiz

İmkansız diferansiyel kripto analiz yöntemi kesik diferansiyel kripto analiz yönteminin bir alt çeşididir. Önceden bir diferansiyel öngörülmektedir. Bu öngörüye göre bazı özel farklar asla meydana gelmeyecektir. Kripto analizde imkânsız durumların kullanılabileceği fikri çok eski bir fikirdir. Ortada ıskalama saldırısı ya da imkânsız diferansiyel saldırısı olarak isimlendirilen bu saldırılar, bir blok şifrede imkânsız bir davranışın nasıl belirleneceği ve bunun nasıl anahtarı elde etmek için kullanılacağı ile ilişkili sistematik bir analiz olarak tanımlanmaktadır [29].

3.4.4. Çoklu Set Saldırıları (Square Saldırısı)

Çoklu set saldırıları ilk olarak square algoritmasını geliştiren J. Daemen, V. Rijmen ve L. Knudsen tarafından kullanılmıştır. Dolayısıyla bir diğer ismi square (kare) saldırısı olarak bilinmektedir. O zamandan beri diğer birçok algoritmaya uygulanmıştır. Bir açık metin saldırısıdır ve iyi seçilmiş açık metin setleri ile şifrenin ileri doğru incelenmesiyle gerçekleştirilmektedir. Bu saldırı tipinde lineer ve diferansiyel kripto analizden farklı olarak açık metin grubunun tümü dikkate alınarak şifre hakkında bilgi toplanmaktadır [30].

4. STEGANOGRAFİ

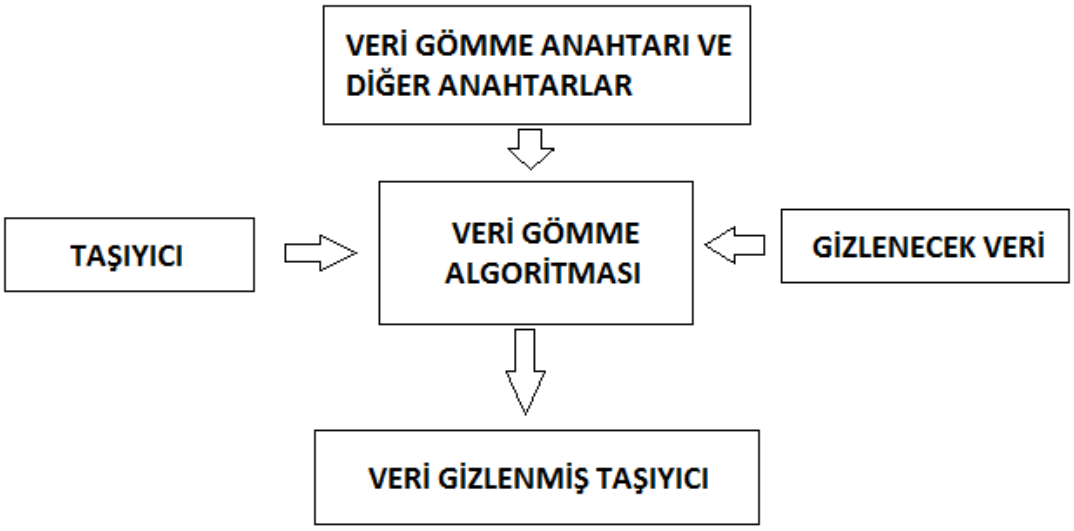
4.1. Steganografi Nedir?

Steganografi, bir mesajın veya bilginin, herhangi bir dijital ortam içerisine saklanarak, bir bilginin veya mesajın varlığı üçüncü kişilere belli edilmeden, bilginin ulaştırılması istenen yere ulaştırılmasıdır [31].

Steganografi, içinde gizli mesaj veya bilgiler bulunan bir veriyi, aktarılmak istenen hedeften başka kimsenin fark edemeyeceği bir biçimde, hedefe gönderme sanatıdır. Latincede 'steganos' kelimesi 'görünmeyen', steganografi de 'gizlenmiş yazı' anlamına gelmektedir. Kısaca steganografi 'veri gizleme sanatı' olarak tanımlanabilir. Amaç, iletilmek istenen bilgiyi ve bu bilginin varlığını başkalarının fark etmesini engelleyecek kadar iyi saklamaktır. Steganografi'de kendisine bilgi gönderilen kişi bile ancak anahtar bilgisini bilmesi durumunda gizli veriyi elde edebilir [32].

Kriptografiden farklı olarak steganografide önemli olan bilginin şifrelenmesi değildir. Kriptografi, gücünü şifreleme algoritmasından alır ve iletilmek istenen verinin varlığının bilinmesinden çekinilmeyen bir bilimdir. Bu nedenle, kriptografide verinin hangi kanalla taşınacağının önemsenmesi gerekmez, fakat ne kadar sağlam olursa olsun hiçbir algoritma çözülemez olmadığı için kriptografiden farklı olarak steganografide, verinin nasıl taşınacağı saklanmak zorundadır [33].

Steganografide önemli olan, verinin varlığının gizlenebilmesidir. Verinin varlığı ne kadar iyi gizlenebilirse, aktarılan veri o kadar güvenli iletilir. Aslında pek önemsenmeyen bir resim veya müzik dosyası, farkedilmeden çok gizli bilgiler taşıyor olabilir. Anahtar bilgi olmadan ve dosyanın içeriği anahtar veri ile incelenmeden alıcı dahil hiç kimse dosyadan kuşkulanmaz ve içeriğini anlayamaz. Bu yüzden steganografide, alıcının elinde, verinin hangi kanalla taşınacağı ve mesajın nasıl çözülebileceği bilgileri olmadan verinin karşı tarafa iletilmesi hiçbir önem taşımaz. Şekil 4.1 ve Şekil 4.2'de veri gömme ve çıkarma haritaları görülmektedir [33].



Şekil 4. 1 Steganografi'de veri gizleme haritası

Şekil 4. 2 Steganografi'de veri çıkarma haritası

4.2. Steganografi'nin Tarihi

Günümüzde yaygın olarak birçok alanda kullanılan steganografinin tarihte ilk ortaya çıkışı M.Ö. 400'lü yıllarda olmuştur. Herodot tarafından anlatılan ve steganografinin tarihteki bilinen ilk örneği, M.Ö.440 yılında Demaratus'un Yunanistan'a yaklaşan bir saldırı tehlikesini, tahta bir tabletin üzerine kazıdıktan sonra üzerini balmumu ile kaplamasıdır. Üzeri balmumu ile örtülü tablet hiçbir şekilde dikkat çekmezken, ısıtılarak mumun eritilmesi sonrasında, tabletteki saldırı uyarısı ortaya çıkmıştır. Bu ilk

örnek olmakla birlikte Eski Yunan'da balmumuyla kaplanan tahta tabletlerin kullanımına birçok örnek vardır [32].

Bir başka eski örnek de bir kölenin saçlarının kesilerek verilmek istenen bilgini dövme şeklinde yapılışı ve kölenin saçları uzadıktan sonra mesajın ulaştırılması gereken yere gönderilmesidir. Köle mesajın gideceği yere ulaştıktan sonra saçları tekrar kesilmiş ve böylece mesaj güvenli olarak karşı tarafa ulaştırılmıştır [33].

Bilinen ilk örnekleri bunlar olan steganografi, ikinci dünya savaşında da sıkça kullanılmıştır. Amerika'da yaşayan bir Japon ajanının, oyuncak bebek siparişi gibi görünen mesajlarla diğer ajanlarla ve hükümetiyle gizli bir şekilde mesajlaşması, Fransızların görünmez mürekkep kullanarak gönderilen postaların üzerine bir takım notlar saklaması, mektup pullarının arka yüzeylerine yazılan bir takım notlar da steganografinin 20nci yüzyıldaki yaygın kullanımına örnek olarak gösterilebilir. Bir diğer örnekse ikinci dünya savaşı sırasında Alman bir casus tarafından gönderilen bir telgraftır [33].

4.3. Steganografi'nin Alt Dalları

Steganografi, Dilbilim Steganografi (Linguistic Steganography) ve Teknik Steganografi (Technical Steganography) olmak üzere kendi içerisinde ikiye ayrılmaktadır [34]. Dilbilim Steganografi, taşıyıcı verinin metin olduğu steganografi koludur. Burada değişiklik yapmanın çeşitli yolları vardır. Bunlardan bazıları şöyledir:

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

Dilbilim Steganografi"de kullanılan yöntemler ise şunlardır [35].

- Açık kodlar: Gizli mesaj, açıkça okunabilir fakat zararsız bir mesaj haline gelir. Bu işlem; maskeleme, boş şifreler ve grid (ızgara) ile yapılmaktadır.
- Şemagramlar: Gizli mesaj, açık metinin 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 [36].

4.4. Görüntü 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 [37]. 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 [38].

- Uzaysal / Görüntü Alan Tekniği (Spatial / Image Domain Technique)
- 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.

4.4.1. Sayısal Resmin Yapısı

Sayısal (dijital) resim N satır ve M sütunluk diziler ile ifade edilmektedir. Bu dizilerin satır ve sütun sayıları x - y veya r - c olarak tanımlanmaktadır. Bu resim dizisindeki her bir elemana piksel adı verilmektedir. En yalın hal olarak siyah beyaz bir resim düşünecek olursak pikseller 1 veya 0 değerlerinden oluşurlar. Bu piksellerin bir araya gelmesiyle oluşan resimlere binary resim adı verilmektedir. [39,44].

Resimlerdeki karanlık ve aydınlık değerleri sırasıyla 0 ve 1 değerleri ifade etmektedirler. Bu karanlık ve aydınlık bölgeler nesne ve zeminin ayırt edilmesinde kullanılmaktadır [40]. Sayısal resim dosyaları renkli olarak ifade edilmek istenirse 8 yada 24 bit ile, gri seviye renkler ile ifade edilmek istenirse ise 1,2,4,6 veya 8 bit ile tanımlanmaktadır

Gri-seviye resimlerde her bir piksel, 0 (siyah) ile 255 (beyaz) arasında tam sayı değer alabilen 1 byte ile ifade edilmektedir. 0 ile 255 arasındaki değerlere karşılık gelen tüm renkler grinin tonları olduğu için bu tip resimler gri ton seviye (gray level) olarak adlandırılmaktadır [41].

Gri-seviye resimlerde olduğu gibi 8 bitlik renkli resimlerdede her piksel 1 bytelık yer kaplamaktadır. 8 bitlik resimler, 24 bitlik bir resme göre çok daha az sayıda renk içerdiği için çok iyi görüntüler vermemektedir. 8 bitlik bir resme bilgi saklanmak istenirse, saklanacak bilgi, saklama ortamını çok fazla değiştirmeyecek şekilde çok dikkatli bir şekilde 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) şeklinde ifade edilmektedir [42].

Gri-seviye ve 8 bitlik resimlerin aksine 24 bitlik resimler ise her bir piksel başına 3 bytelık alan kaplamaktadır. 24 bitlik resimlerdeki pikselin rengi; Kırmızı (red), Yeşil (green), Mavi (blue) olmak üzere üç ana renkten oluşmaktadır. Bu renkler genel olara RGB değeri olarak adlandırılmaktadır [43].

4.4.1.1. Veri Gizleme İşlemi

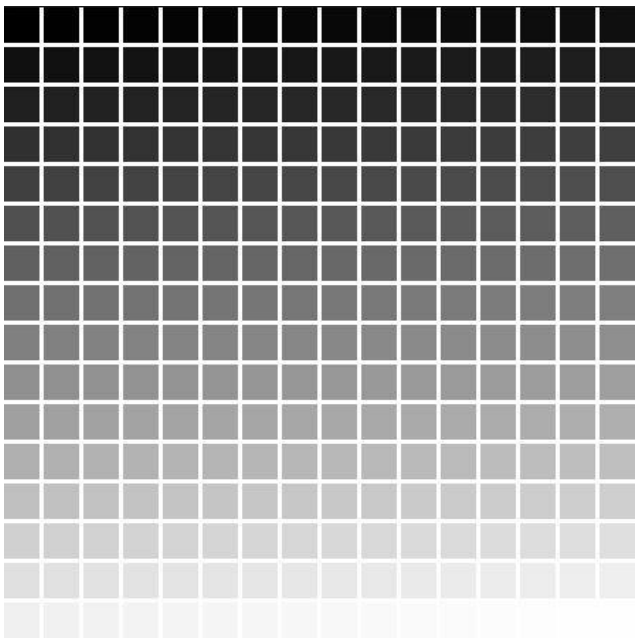
Veri gizleme işlemleri esnasında üzerinden işlem yapılacak iki dosya bulunmaktadır. Bu dosyalardan ilki cover image olarak adlandırılmakta olan ve gizli bilgiyi saklayacak olan resim dosyasıdır. Bu dosyalardan ikincisi ise gizlenecek bilgiyi içeren dosyadır. İkinci dosya plain text veya chipher text içerebileceği gibi başka dosyalar veya bit dizisi vs. de içerebilmektedir.

Veri gizleme işlemi tamamlandıktan sonra elde edilen ve hem gizleyen hem de gizlenen dosyayı içeren resme stegoresim adı verilmektedir. Steganografi yazılımlarında jpeg resimlerinin kullanılmaması tercih edilmemektedir. Genellikle 24 bitlik bmp formatlı resim dosyaları kullanılmaktadır. Ayrıca gri tonlamalı ve 256 renk resimlerde kullanılabilmektedir. 256 renk resim ismi ile tabir edilen resim formatı sıkça kullanılmakta olan gif formatıdır. Gif formatlı resim dosyaları ve 8 bit bmp resimlerde bulunan her bir piksel 1 byte ile ifade edilmektedir. Bu tip resimlerde bulunan her bir renk 256 renk paletinden seçilmektedir. Bu tip resimlerdeki her bir piksel 256 renk paletindeki renge karşılık gelen 1 byte'lık bir alan kaplamaktadır.

Gömme işlemi sonucunda kapak resim ve gömülü mesajın oluşturduğu dosyaya "stego resim" adı verilmektedir. Birçok steganografi yazılımı JPEG formatını desteklemez veya kullanımını tavsiye etmezken, 24 bit BMP resimlerin kullanılmasını tercih etmektedir. Diğer alternatifler ise gri tonlamalı ve 256 renk resimlerdir. Söz edilen 256 renk resimlerin en yaygın kullanılanı GIF formatıdır. GIF formatlı resim dosyaları ve 8 bit BMP resimlerde her piksel bir byte ile gösterilir. Bu tip resimler resimde kullanılan renkleri içeren 256 renkli bir palet taşırlar. Her piksel bu palette bir renge karşılık gelen 1 byte'lık değeri taşımaktadır (Şekil 4.3).

Şekil 4.3 Renk Paleti ve bu Palet ile oluşturulmuş resim

Steganografi alanında çalışmalar yapmakta olan bir çok bilim adamı 256 gri tonlamalı resimlerin kullanılmasını önermektedir. Gri tonlamalı resimlerin kullanılmasını önermelerinin en önemli sebebi, resmi oluşturan renklerin her bir piksel için çok küçük farklar ile renk tonunun değişmesidir. Bu tip resimlerde kullanılan renklerde 256 renk paletinde bulunan renklerden meydana gelmektedir (Şekil 4.4). bu palet üzerindeki renkler üzerindeki her bir ton değişimi insan gözünün fark edemeyeceği kadar küçüktür. Bazı gri tonlamalı resimler 4 bitlik olabilmektedir ve 16 farklı gri ton içerebilmektedir. Bu tipteki resimlerde bulunan piksel renkleri üzerindeki değişimler çok daha belirgin bir şekilde gerçekleşmektedir.



Şekil 4. 4 256 Gri Renk Paleti

Gri tonlamalı resimler, steganografik çalışmalar için iyi sonuçlar verdiğine göre küçük renk değişimlerini çok miktarda içeren resimler de steganografik çalışmalar açısından oldukça etkili demektir. Benzer renkli büyük kısımlar içeren resimler ise steganografik çalışmalar açısından iyi bir seçenek değildir. Çünkü resmin benzer renklerden oluşan kısımlarda gizlenecek mesajın oluşturacağı değişimler çok daha fazla dikkat çekici olacaktır [44].

4.4.1.2. Veri Gizleme Yöntemleri

Birçok farklı yöntem kullanılarak resim dosyaları içerisinde bilgiler gizlenebilmektedir. Veri gizleme işlemleri esnasında kullanılan yöntemler, gizleme işlemi sırasında kullandıkları veri dikkate alınarak iki başlık altında incelenebilmektedir [44].

- Uzaysal / Görüntü Alan Tekniği (Spatial / Image Domain Technique)
- Frekans / Dönüşüm Alan Tekniği (Frequency / Transform Domain Technique)

Uzaysal Alan veya Görüntü Alan olarak adlandırılan teknik, gizleme işleminde resim dosyasındaki veriyi doğrudan kullanmaktadır. Gizleme işleminde bilgiyi gizlediği veri kümesi, piksel değerlerini temsil eden kısımdır. Bu tekniğe örnek olarak

steganografik çalışmalar kapsamında yaygın olarak kullanılmakta olan En Önemsiz Bite Ekleme (Least Significant Bit Insertion - LSB) yöntemi gösterilebilmektedir.

Frekans Alan veya Dönüşüm Alan olarak bilinen teknik ise kapak verideki değişimler üzerinde gizleme işlemini uygulamaktadır. Dönüşüm Alan tekniğine örnek olarak ise, JPEG formatlı resim dosyalarına veri gömme işleminde kullanılan algoritmalar verilebilmektedir. Bu algoritmalar JPEG sıkıştırma sırasında kullanılan DCT katsayıları üzerinde veri gömme işlemini uygulamaktadır [42,44].

4.4.2. Görüntü Dosyalarında Steganografik Yöntemler

Görüntü dosyalarında bilgi gizleyebilmek için çeşitli yöntemler kullanılmaktadır. Bu yöntemler ana başlıklar altında incelenmek istenilirse 3 gruba ayrılabilir [47];

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 dayanıklıdırlar 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 algoritmalardan en yaygın olarak kullanılanları şunlardır [48];

- 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. Patchwork Algoritması

Patchwork algoritması, Bender tarafından ortaya atılmış olan ve halen sıklıkla kullanılmakta olan bir algoritmadır. Bu algoritma, bilgiyi Gauss dağılımı gösteren bir istatistiğe sahip örtü verisinin içine gizlemeyi amaçlayan istatistiksel bir yönteme dayanmaktadır [45]. Bu algoritma genellikle filigran (watermarking) uygulamalarında kullanılmaktadır [44].

4.4.2.2. Amplitude (Genlik) Modülasyonu Yöntemi

Amplitude (Genlik) modülasyonu yöntemi kullanılarak işaret bitleri ile mavi kanaldaki piksel değerleri değiştirilerek resim içerisine gizlenmektedir. Bu değişimler ışığın oranına ve bitin değerine bağlı olarak rengin tonunun arttırılması veya eksiltilmesi yoluyla yapılmaktadır [44,46].

4.4.2.3. SSIS (Spread Spectrum Image Steganography) Yöntemi

SSIS (Spread Spectrum Image Steganography) yöntemi, sayısal görüntünün içindeki bilgi bitlerinin işaretleme kalitesinin, saklama ve geri getirme işlemlerini gözlemleyen birinin farkedemeyeceği şekilde değiştirilmesiyle gizleme işlemini

gerçekleştirmektedir [49]. Bu yöntem ile gizlenmiş bir metnin tekrar elde edilebilmesi için orijinal görüntüye ihtiyaç bulunmamaktadır.

4.4.2.4. Frekans Domaini İçine Veri Saklanması Yöntemi

Frekans Domaini İçine Veri Saklanması Yöntemi filigran (watermark) teknolojileri için kullanılmaktadır. Bu yöntem görüntülerin dönüştürülmesi (transform) temeline dayanmaktadır. Görüntü dönüştürülmesi için genellikle ayrık kosinüs dönüşümü (Discrete Cosine Transform- DCT) kullanılmaktadır. Bunun dışında kullanılan dönüşüm algoritmaları ise; Ayrık Fourier Dönüşümü (DFT), Walsh dönüşümü ya da Wavelet (dalga) dönüşümüdür [50].

4.4.2.5. Son Bite Ekleme (LSB-Least Significant Bit Insertion) Yöntemi

En önemsiz bite ekleme yöntemi (Least Significant Bit Insertion Methods) en yaygın olarak kullanılmakta olan ve uygulaması basit bir yöntemdir [51]. Fakat yöntemin dikkatsizce uygulanması durumunda veri kayıpları ortaya çıkabilmektedir.

5. GÖRÜNTÜ FORMATLARI

Görüntü dosyaları eğriler, alanlar, doldurudukları renkler veya noktalar topluluğu olarak iki şekilde depolanabilmektedirler. İlk yöntem olan eğriler, alanlar ve doldurudukları renkler yöntemine vektör tabanlı görüntü, ikinci yöntem olan noktalar topluluğu yöntemine ise piksel tabanlı görüntü denilmektedir. Vektör tabanlı görüntülerin avantajı istenilen ölçülere kayıpsız bir şekilde ve dosyanın boyutunu arttırmadan büyütme yapabilmesidir. Piksel tabanlı görüntülerin dosya boyutu büyütme oranı arttıkça artmaktadır. Vektör grafikleri sorunsuz bir şekilde piksel tabanlı grafiklere dönüştürülebilmektedir. Fakat piksel tabanlı grafiklerin vektör tabanlı grafiklere dönüştürülmesi her zaman mümkün değildir. Vektör grafikleri içerisinde pikselli grafik kullanmak mümkündür ancak tersi mümkün değildir. Ancak bu çalışmada kullanılacak görüntü formatı, çalışmanın vektörel grafik formatlarına gereksinim duymaması nedeniyle piksel tabanlı görüntü formatları olacaktır. Yaygın olarak kullanılmakta olan ve bu çalışmada da kullanılması planlanan görüntü formatlarından bazıları şunlardır.

5.1. Joint Photographic Experts Group (JPEG)

En yaygın kullanılan fotoğraf dosyası türü olan JPEG, Joint Photographic Experts Group (Birleşik Fotoğraf Uzmanları Grubu) tarafından standartlaştırılmış bir sayısal görüntü kodlama biçimidir. Bu dosya türündeki fotoğraflar jpg, jpe ya da jfif uzantılıdırlar.

JPEG sıkıştırma yöntemi görüntünün algılanması için zorunlu olmayan detayları bulup atan ve dosyayı bu şekilde sıkıştıran bir format olduğundan "kayıplı formatlar" arasında yer alır. JPEG sıkıştırmasında renk değerlerinde bozulma olmaz ancak çizgisel-grafiksel şekillerde bozulmalara sebep olabilir. JPG formatı, resim 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 [52].

5.2. Portable Network Graphics (PNG)

PNG, "Taşınabilir Ağ Grafiği" anlamındaki “Portable Network Graphics”in kısaltmasıdır ve kayıpsız sıkıştırarak görüntü saklamak için kullanılan bir saklama biçimidir. Görüntüyü katmanlar halinde saklamaya imkân tanır. Hazırladığımız bir afişi PNG formatında kaydettiğimizde, sonradan katmanlar üzerinde işlem yapabilir, örneğin yazıyı, görüntü üzerinde başka bir noktaya kaydedebiliriz.

PNG, kayıpsız bir format olduğu için özellikle grafik ve metin içeren dosyalarda kullanıldığında iyi sonuç verir [52].

5.3. Graphics Interchange Format (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 [52].

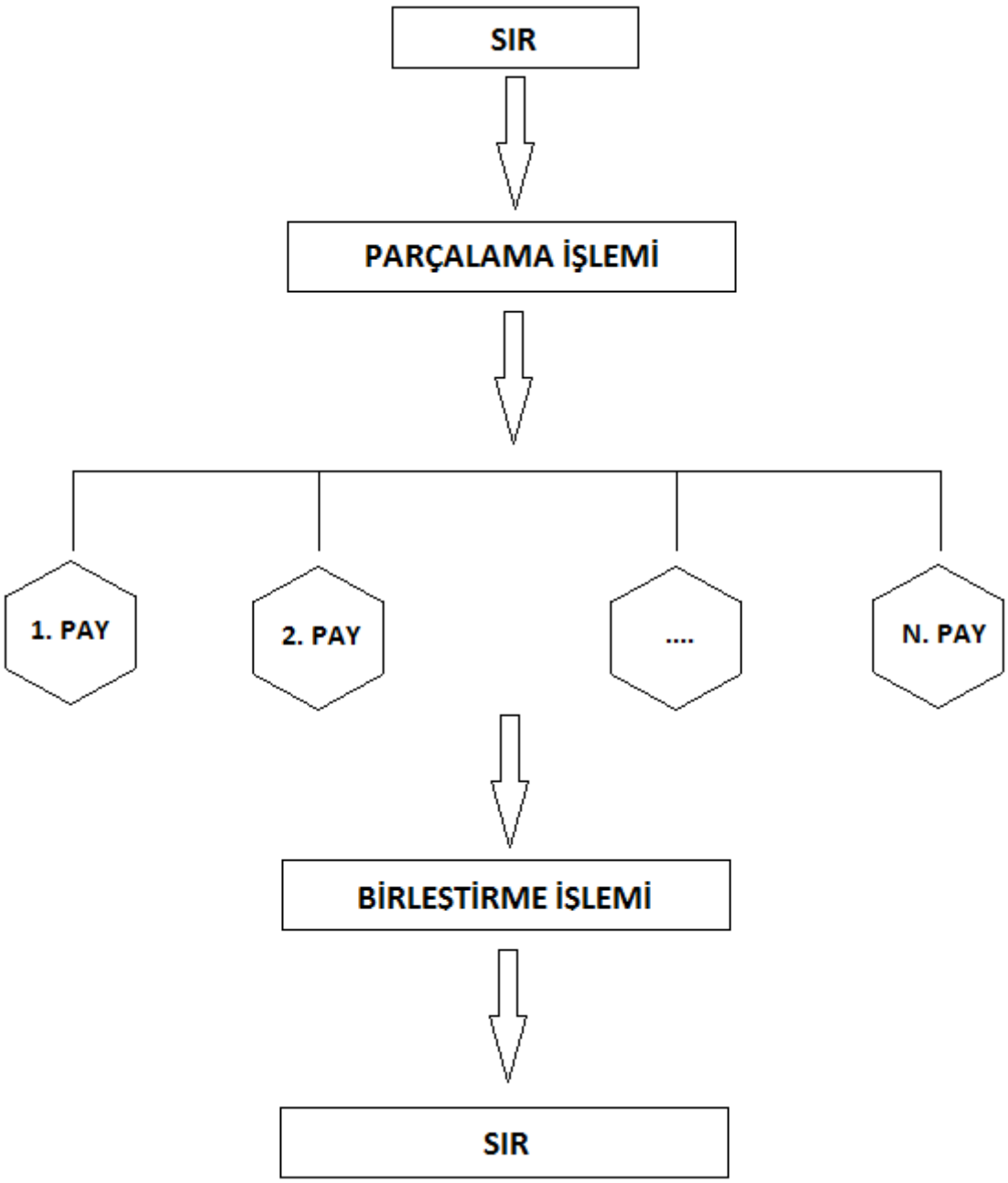
6. SIR PAYLAŞIM YÖNTEMLERİ

6.1. Shamir'in Sır Paylaşımı Yöntemi

Sır paylaşımı konusunda yapılan çalışmalar 1979 yılında Adi Shamir ile başlamıştır. Shamir'in yöntemi polinom tabanlı olup rastgele seçilen parametreler üzerine kuruludur. Shamir oluşturduğu sır paylaşım modelinde (t,n) eşik yöntem kavramını ortaya çıkartmıştır. (t,n) eşik yönteminde bulunan n değeri pay sahiplerinin sayısını göstermekte iken t değeri ise sır değerinin ortaya çıkabilmesi için kaç adet pay sahibinin bir araya gelmesi gerektiğini göstermektedir. Shamir'in (t,n) eşik yöntemine ait blok şema Şekil 6.1'de verilmiştir.

Blok şeması verilen Shamir'in sır paylaşım yönteminin gerçekleştirilir iken izlenen algoritma adımları aşağıda belirtilmiştir.

- Sır paylaşımı yöntemi uygulanacak veri belirlenir,
- (t,n) eşik yöntemi belirlenir,
- Sır nesnesinin parçalama işlemi için gerekli fonksiyon oluşturulur,
- n adet pay değeri oluşturulur,
- Birleştirme işlemi için gerekli fonksiyon oluşturulur,
- m tane sır değeri elde edilir.



Şekil 6.1. Sır paylaşımı yönteminin blok şeması

Shamir'in modelini ifade eden ve (t,n) eşik yöntemini kullanan polinomun derecesi t-1'dir ve bu polinom Formül (6.1)'de gösterilmiştir.

$$q(x) = a_0 + a_1 x + \ldots\ldots + a_{k-1} x^{k-1} \ (mod\ p) \tag{6.1}$$

Formül (6.1)'de belirtilen q(x), a1 ile ak-1 arası rastgele seçilen parametrelerden oluşmaktadır. a0 parametresi ise sır değerini yani anahtarı ifade etmektedir. Sır değerin parçalanması ile elde edilen pay değerleri Formül (6.2)'deki gibi elde edilebilmektedir.

$$D_1 = q(1), \ldots\ldots\ldots, D_i = q(i), \ldots\ldots\ldots, D_n = q(n) \tag{6.2}$$

Elde edilen 1'den n'e kadar olan D değerleri Shamir'in sır paylaşımı yöntemindeki pay değerlerini temsil etmektedir. Eşik yöntemi olarak (t,n) eşik değeri kullanılıyor ise n tane pay değeri olduğu anlaşılmaktadır. n adet pay değeri ise q(x) polinomu ile Formül (6.3)'te gösterildiği şekilde bulunabilir.

1 ile k-1 arasında rastgele seçilen a parametreleri ile a0 sır değeri [0,p) aralığında olmalıdır. [0,p) aralığındaki p değeri ise elde edilen değerin alabileceği en büyük değerdir. Örneğin gri resimlerde her bir pikselin alabileceği en büyük değer 255 olduğu için gri resimlerde p değeri 256 olmalıdır. Eğer q(n) polinomunun sonucu p değerinden büyük ise mod p işlemi uygulanmalı ve D değerleri bu yöntem ile yeniden hesaplanmalıdır.

$$D_n = q(n) mod\ p \tag{6.3}$$

Shamir'in sır paylaşım tekniğine göre parçalanarak elde edilen pay değerleri kullanılarak yeniden sır değeri yani anahtar ortaya çıkarılmak istenirse Lagrange Enterpolasyonu uygulanmalıdır. Lagrange Denklemi Denklem (6.4)'te gösterilmiştir.

$$f(x) = \sum_{i=1}^{k} D_i \prod_{j=1, j\neq i}^{k} \frac{(x - x_j)}{(x_i - x_j)} (mod\ p) \tag{6.4}$$

Lagrange Denkleminde belirtilen f(x) fonksiyonunda sabit değer gerekmektedir. Formül (6.4) üzerinde gerekli sadeleştirmeler yapıldıktan sonra Denklem (6.5) elde edilmektedir.

$$s = f(0) = \sum_{i=1}^{k} D_i \prod_{i=1, j \neq i}^{k} \frac{-x_j}{(x_i - x_j)} \ (mod\ p) \tag{6.5}$$

Shamir'in sır paylaşımı yöntemini, gerekli parametreler belirlendikten sonra bir sayı üzerinde uygulayarak gerçekleştirebiliriz. Aşağıda belirtilen değişkenlerden (S) sır değerini, (n) pay sahibi sayısını, (t) eşik değerini belirtmektedir. Ayrıca (a) ve (b) olarak adlandırılan rastgele iki sayı seçilmiştir.

$$\begin{aligned} S &= 500 \\ n &= 5 \\ t &= 3 \\ a &= 300 \\ b &= 150 \end{aligned} \tag{6.6}$$

Yukarıda tanımlanan uygulama da S ile gösterilen değer n değeri ile belirtildiği gibi 5 paya ayrılmaktadır. Ayrılan bu paylar, t değerinde belirtildiği gibi 3'lü kombinasyonlar şeklinde bir araya geldiği zaman tekrardan parçalanmadan önceki haline yani S değerine ulaşılmaktadır. Yukarıda belirtilen uygulamanın sonucunda ortaya çıkacak pay değerlerini belirleme fonksiyonu Formül (6.7)'da gösterilmiştir.

$$q(x) = 500 + 300 * x + 150 * x^2 \tag{6.7}$$

Yukarıda n değişkeni ile belirtilen 5 tane pay değeri A, B, C, D ve E ile ifade edildiği takdirde Formül (6.8) elde edilmektedir.

$$
\begin{aligned}
A &= q(1) = 500 + 300 * 1 + 150 * 1^2 = 950 \\
B &= q(2) = 500 + 300 * 2 + 150 * 2^2 = 1700 \\
C &= q(3) = 500 + 300 * 3 + 150 * 3^2 = 2750 \\
D &= q(4) = 500 + 300 * 4 + 150 * 4^2 = 4100 \\
E &= q(5) = 500 + 300 * 5 + 150 * 5^2 = 5750
\end{aligned} \tag{6.8}
$$

Formül (6.8) ile elde edilen bu değerler S anahtarının pay değerleridir. Pay değerini elde ederken elde ettiğimiz bu değerler S anahtarının pay değerleridir. Bu örnekte pay değerini elde ederken bir değer sınırlaması bulunmamaktadır. Bu yüzden denkleme mod işleminin uygulanması gerekmemektedir. Eğer S anahtarının bilinmediğini varsayar isek, yeniden S değerini elde etmek için bu değerler kullanılmalıdır.

S değeri, 5'in 3'lü kombinasyonu kadar farklı şekilde Formül (6.9) kullanılarak yeniden elde edilebilir. Bu kombinasyonlardan birkaçı şunlardır:

A, B, C kombinasyonu için,

$$S_{ABC} = 950 * 3 - 1700 * 3 + 2750 = 2850 - 5100 + 2750 = 500 \tag{6.9}$$

C, D, E kombinasyonu için,

$$S_{CDE} = 2750 * 10 - 4100 * 15 + 5750 * 6 = 27500 - 61500 + 34500 = 500 \tag{6.10}$$

A, C, E kombinasyonu için,

$$S_{ACE} = 950 * \left(\frac{15}{8}\right) - 2750 * \left(\frac{5}{4}\right) + 5750 * \left(\frac{3}{8}\right) = 1781{,}25 - 3437{,}50 + 2156{,}25 = 500 \tag{6.11}$$

B, C, D kombinasyonu için,

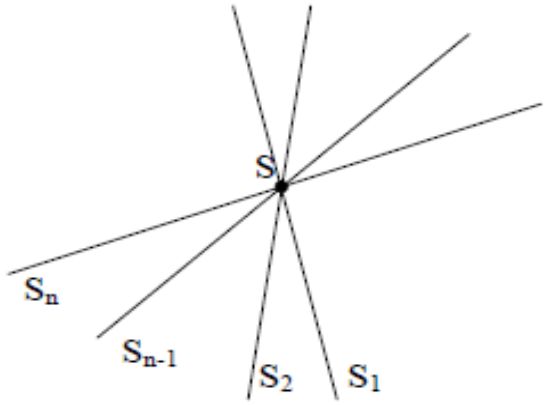
$$S_{BCD} = 1700 * 6 - 2750 * 8 - 4100 * 3 = 10200 - 22000 + 12300 = 500 \qquad (6.12)$$

denklemleri kullanılmıştır [4].

6.2. Blakley'in Sır Paylaşımı Yöntemi

Blakley, Shamir'in yönteminde kullandığı polinomial interpolasyon yerine, t boyutlu uzaydaki hiper düzlemlere dayanan geometriyi kullanmaktadır. (t,n) eşik şemasını uygulayabilmek için n adet katılımcının her birine GF(q) sonlu alan üzerinde t boyutlu uzayda bir hiper düzlem denklemi verilir.

Hiper düzlemler a1x1 + ……. + atxt = b şeklinde olan denklemi tanımlamaktadır. x = (x1, …… , xt) değerleri pay değerlerini tanımlamada kullanılır. Her bir hiper düzlem belli bir noktadan geçmektedir. Hiper düzlemlerin kesişme noktaları sır olarak tanımlanmaktadır. T adet katılımcının bir araya gelmesiyle sırrı yeniden elde etmek için denklem sisteminin çözülmesi gerekmektedir. Şekil 6.2'de Blakley'in sır paylaşım şemasının nasıl gerçekleştirilebileceğinin bir örneği gösterilmiştir. Burada t = 2'dir. Yani her hiper düzlem denklemi bir doğru denklemiyle ifade edilmektedir. n sayıda katılımcı için dağıtıcı tarafından gizli verinin temsil ettiği noktayı kesen n adet doğru denklemi üretilmektedir. Herhangi t sayıda katılımcının doğrusunun kesiştirilmesi sonucu gizli veri yeniden elde edilebilmektedir.



Şekil 6.2 Blakley sır paylaşım şeması, t = 2

Blakley'in sır paylaşımı yöntemine göre, gizli veri üc boyutlu uzayda bir noktanın koordinatlarıyla (2,4,9) olarak verilmiş ise (3,4) şeması için 2x1 + 4x2 + 9x3 = b denklemi GF(11) alan üzerinde üretilir. Her bir katılımcıya gönderilecek olan 4 farklı değerler kümesi (x1, x2, x3, b) pay değerlerini oluşturur. Pay değerleri aşağıdaki şekilde hesaplanarak elde edilmektedir.

$$\left(\begin{bmatrix}2 & 3 & 1\\ 3 & 2 & 6\\ 4 & 2 & 1\\ 5 & 1 & 10\end{bmatrix} * \begin{bmatrix}2\\4\\9\end{bmatrix}\right) \Big/ 11 = \begin{bmatrix}3\\2\\3\\5\end{bmatrix} \tag{6.13}$$

Pay değerleri sırasıyla (2,3,1,3), (3,2,6,2), (4,2,1,3), (5,1,10,5) olacaktır. Bu katılımcılardan herhangi üç katılımcı bir araya gelerek, düzlemlerinin kesişme noktası olan (2,4,9) yeniden elde edilir. Gizli veri aşağıda ki sistemi çözerek yeniden elde edilir [53].

$$\begin{bmatrix}a_1\\a_2\\a_3\end{bmatrix} = \left(\begin{bmatrix}23\ 1\\42\ 1\\5110\end{bmatrix}^{-1} * \begin{bmatrix}3\\3\\5\end{bmatrix}\right) \Big/ 11 = \begin{bmatrix}2\\4\\9\end{bmatrix} \tag{6.14}$$

6.3. Mignotte'nin Sır Paylaşımı Yöntemi

Mignotte'nin eşik sır paylaşım şeması, Mignotte'nin sırası olarak adlandırılan sıralı tamsayıları kullanmıştır. (t, n)eşik şeması için Mignotte'nin sırası, aralarında asal olan tamsayılar m1 < m2 < ⋯ < mn sırasıdır ve Formül (6.15)'deki koşulu sağlayacak şekilde belirlenir.

$$\prod_{i=0}^{t-2} m_{n-i} < \prod_{i=1}^{t} m_i \tag{6.15}$$

Formül (6.15)'de verilen denklem, Formül (6.16)'da verilen denkleme eşittir.

$$max_{1 \le i_1 \le \ldots \le i_{t-1} \le n}\left(m_{i_1} m_{i_2} \ldots m_{i_{t-1}}\right) < min_{1 \le i_1 \le \ldots \le i_t \le n}\left(m_{i_1} m_{i_2} \ldots m_{i_t}\right) \tag{6.16}$$

(t, n) Mignotte'nin sır paylaşım şeması aşağıdaki adımları halinde verilmektedir:

- Gizli veri S, $\beta < S < \alpha$ koşulu sağlanacak şekilde rastgele tamsayı olarak seçilir. $\alpha = \Pi^{t}_{i=1} m_i$ ve $\beta = \Pi^{t-i}_{i=0} m_{n-i}$'dir.

- Pay değeri si=S mod mi, 1<= i <= n denklik ifadesi yardımıyla belirlenir.
- Herhangi t adet pay değeri si1, … , sit ele alınır, Çinli Kalan Teoremi kullanılarak, Formül (6.17)'deki denklik sisteminin tek çözümü olarak yeniden gizli veri S, elde edilir.

$$\begin{aligned} x &\equiv s_{i_1} \, mod \, m_{i_1} \\ &\vdots \\ x &\equiv s_{i_t} \, mod \, m_{i_t} \end{aligned} \qquad (6.17)$$

Yeniden yapılandırma aşamasında, sadece t-1 pay değerinden s_{i1}, … , s_{it-1}, elde edilen denklik ifadesi $S \equiv x_0 \bmod m_{i1} \ldots m_{it-1}$ şeklinde olur.

x_0 değeri mod $m_{i1} \ldots m_{it-1}$ tabanındaki tek çözümdür.

Örneğin Mignotte'nin (3,5) eşik şeması kullanılarak, S = 135 gizli veriyi katılımcılar arasında paylaştıralım. Her katılımcıya karşılıklı olan, Mignotte'nin koşulunu sağlayarak, modül değerleri sırasıyla 7,11,13,17,19 olsun. Katılımcılara gönderilecek olan pay değerleri

$$\begin{cases} s_1 = 135 \, mod \, 7 = 2 \\ s_2 = 135 \, mod \, 11 = 3 \\ s_3 = 135 \, mod \, 13 = 5 \\ s_4 = 135 \, mod \, 17 = 16 \\ s_5 = 135 \, mod \, 19 = 2 \end{cases} \qquad (6.18)$$

olarak hesaplanır. Yeniden yapılandırma aşamasında, en az üç katılımcının bir araya gelmesi gerekir. $s_2 = 3$, $s_3 = 5$, $s_4 = 16$ pay değerleri seçilir. Çinli Kalan Teoremi kullanılarak, aşağıda verilen denklik sisteminin çözülmesi sonucu gizli veri yeniden elde edilir [53].

$$\begin{cases} S \equiv 3 \, mod \, 11 \\ S \equiv 5 \, mod \, 13 \\ S \equiv 16 \, mod \, 17 \end{cases} \qquad (6.19)$$

$$\begin{aligned} S &= (221 * 3 * 1 + 187 * 5 * 8 + 143 * 16 * 5) mod \, 2431 = 19583 \, mod \, 2431 \\ &= 135 \qquad (6.20) \end{aligned}$$

6.4. Asmuth-Bloom'un Sır Paylaşımı Yöntemi

Asmuth-Bloom eşik sır paylaşım şeması, Mignotte sır paylaşım şemasına benzer niteliktedir ve bu yöntemde de, özel sıralı tamsayılar (aralarında asal olan $m_0 < m_1 < \cdots < m_n$) kullanılmaktadır. Sıra tamsayılar Formül (6.21)'deki koşulu sağlayacak şekilde seçilmektedir.

$$m_0 \prod_{i=0}^{t-2} m_{n-i} < \prod_{i=1}^{t} m_i \tag{6.21}$$

Genelde m_0, sır olarak saklanır ve $m_1, \ldots, m_n$ aleni olarak belli olur. Asmuth-Bloom sır paylaşım şeması aşağıdaki adımları halinde verilmektedir:

- Gizli veri S , $\mathbb{Z}_{m0}$ kümesinin bir elemanı olarak seçilir.
- y , $y = S + A.m_0$ denkleminden hesaplanır. Burada A bir rastgele sayıdır ve $y \in \mathbb{Z}_{m1 \ldots mt}$ 'dir.
- Pay değerleri olan s_i'ler , $s_i = y \bmod m_i$, $1 \leq i \leq n$ denkleminden hesaplanır.
- Herhangi t tane pay değeri $s_{i1}, \ldots, s_{it}$ ele alınarak, gizli veri S, $S = x_0 \bmod m_0$ denklemi sayesinde elde edilir. x_0 verisi farklı standart Çinli kalan teoremi kullanılarak, Formül (6.22)'deki denklik sisteminden, $m_{i1} \ldots m_{it}$ modülünün tek çözümü olarak hesaplanır [53].

$$\begin{aligned} x &\equiv d_{i_1} \bmod m_{i_1} \\ &\vdots \\ x &\equiv d_{i_1} \bmod m_{i_1} \end{aligned} \tag{6.22}$$

6.5. Çinli Kalan Teoremine Dayalı Sır Paylaşımı Yöntemi

Çinli kalan teoremine göre Formül (6.23)'deki denklem sistemi verilsin:

$$\begin{aligned} x &\equiv a_1 \bmod p_1 \\ x &\equiv a_2 \bmod p_2 \\ &\vdots \\ x &\equiv a_n \bmod p_n \end{aligned} \tag{6.23}$$

Taban değerleri $p_1, p_2, \dots, p_n$ arasında asal olsun yani ebob(p_i,p_j) = 1, $i \neq j$

$$P = \prod_{i=1}^{n} P_i \tag{6.24}$$

Tüm $i \in \mathbb{N}$ $(1 \leq i \leq n)$ için y_i bir tamsayı olsun ki

$$y_i * \frac{p}{p_i} \equiv 1 \; mod \; p_i$$

Burada oluşacak tek çözüm $x_0 = \Sigma^{n}_{i-1} a_i y_i \; p/p_i$ ve $x \equiv x_0 \pmod{p}$ şeklinde elde edilebilir.

Örneğin aşağıdaki sistemi ele alırsak,

$$\begin{aligned} x &\equiv 4 \; mod \; 5 \\ x &\equiv 5 \; mod \; 7 \\ x &\equiv 8 \; mod \; 11 \end{aligned} \tag{6.25}$$

$$P = 5 * 7 * 11 = 385 \, , n_1 = \frac{p}{p_1} = 77 \, , n_2 = 55 \, , n_3 = 35 \tag{6.26}$$

y_i'ler aşağıdaki gibi bulunur:

$$77 \; y_1 \equiv 1 \; (mod \; 5) 55 y_2 \equiv 1 \; (mod \; 7) 35 y_3 \equiv 1 \; (mod \; 11) \tag{6.27}$$

$$y_1 = 3, y_2 = 6, y_3 = 6 \tag{6.28}$$

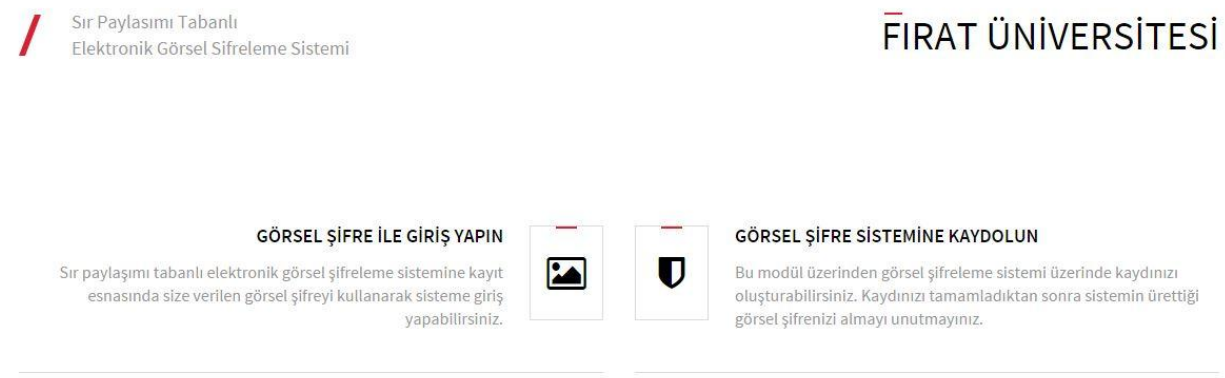
$$x = (3 * 4 * 77 + 5 * 6 * 55 + 6 * 8 * 35) \; mod \; 385 = 19 \; (mod \; 385) \tag{6.29}$$

x değeri 19 olarak hesaplanır [53].

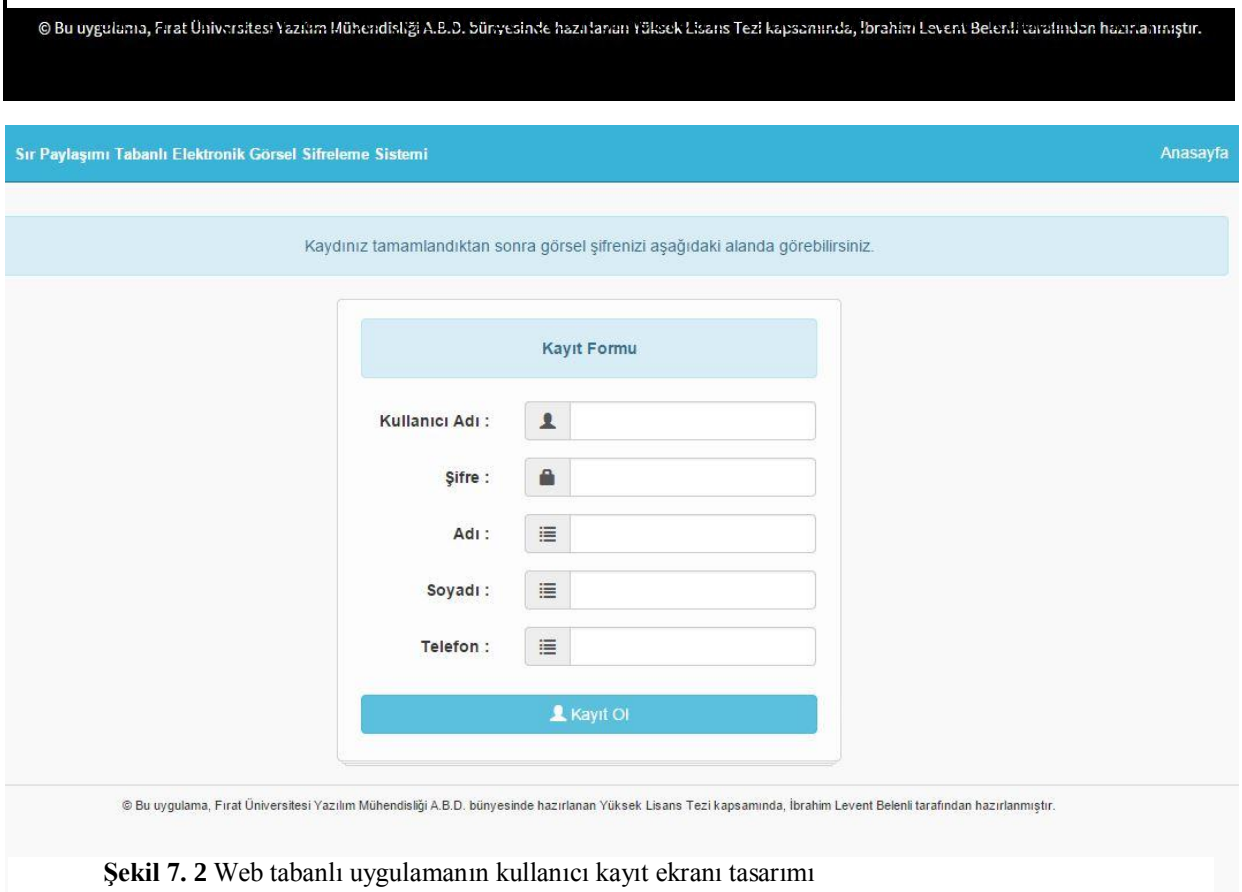
7. YÖNTEM VE WEB TABANLI UYGULAMA

Günümüzdeki en büyük problem casus yazılımlarla mücadele etmek konusunda yaşanmaktadır. Trojan, keylogger, screenlogger ve benzeri zararlı yazılımlar kullanan üçüncü kişilerin müdahaleleriyle internet şifrelerimizin bu kişilerin eline geçmesi hiçte zor değildir. Örnek vermek gerekirse, internet bankacılığını kullanarak başka bir hesaba belli bir miktar para transferi gerçekleştirmek istiyoruz. Sisteme giriş yapıldığı esnada şifreler klavye vasıtasıyla sisteme girildiği için, keylogger veya spyware yazılımları vasıtasıyla şifrelerin çalınması olağandır. Güvenlik sistemleri alanında çalışmalar yapan uzmanlar, kullanıcı şifrelerini keyloggerlardan koruyabilmek için ekran klavyesi modelini geliştirmişlerdir. Ancak ekran klavyesi modeline karşıda screenloggerlar ortaya çıkmıştır. Ardından sistemlerin güvenliklerinin arttırılması için sisteme giriş olayının son aşamasında tek kullanımlık şifreler kullanılmaya başlanmıştır. Fakat tek kullanımlık şifrelerin firmalara olan sms maliyetlerinden dolayı firmalar tek kullanımlık şifrelere soğuk bakmaktadır. Ayrıca sürekli şifre girme işlemleri vakit kaybı olup kullanılmakta olan uygulamaların kullanışlılığı olumsuz yönde etkilenmektedir. Geliştirilen sır paylaşım tabanlı görsel şifreleme sisteminde bahsedilen mevcut problemlerin giderilmesi amaçlanmaktadır.

Geliştirilmiş olan web tabanlı uygulama Visual Studio 2012 geliştirme ortamında ASP.NET MVC projesi olarak hazırlanmıştır. Script dili olarak ise C# kullanılmıştır. Veri tabanı olarak MS SQL Server kullanılmıştır. Sistemin kullanımı çok kolay olup oluşturulan görsel şifreyle sistemin güvenliğinin sağlanması amaçlanmaktadır. Geliştirilmiş olan sistemin anasayfa tasarımı (Şekil 7.1)'de gösterilmektedir.



Şekil 7. 1 Web tabanlı uygulamanın anasayfa tasarımı

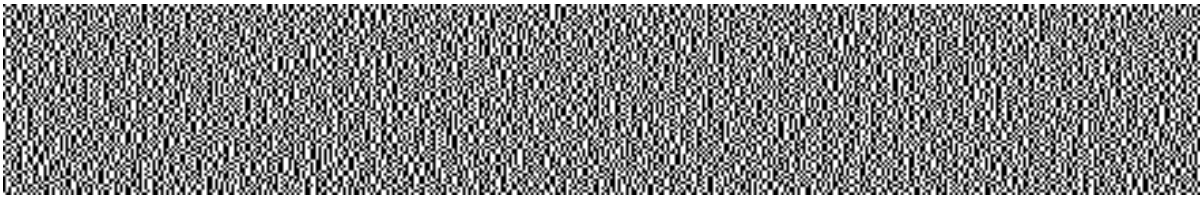


Şekil 7. 2 Web tabanlı uygulamanın kullanıcı kayıt ekranı tasarımı

Kullanıcı kayıt formu üzerindeki gerekli alanlar doldurulduktan sonra kayıt ol butonuna tıklanarak kayıt formu sunucuya gönderilmektedir. Sunucuda ise belirlemiş olduğunuz şifre bir resim haline getirilmektedir (Şekil 7.3).

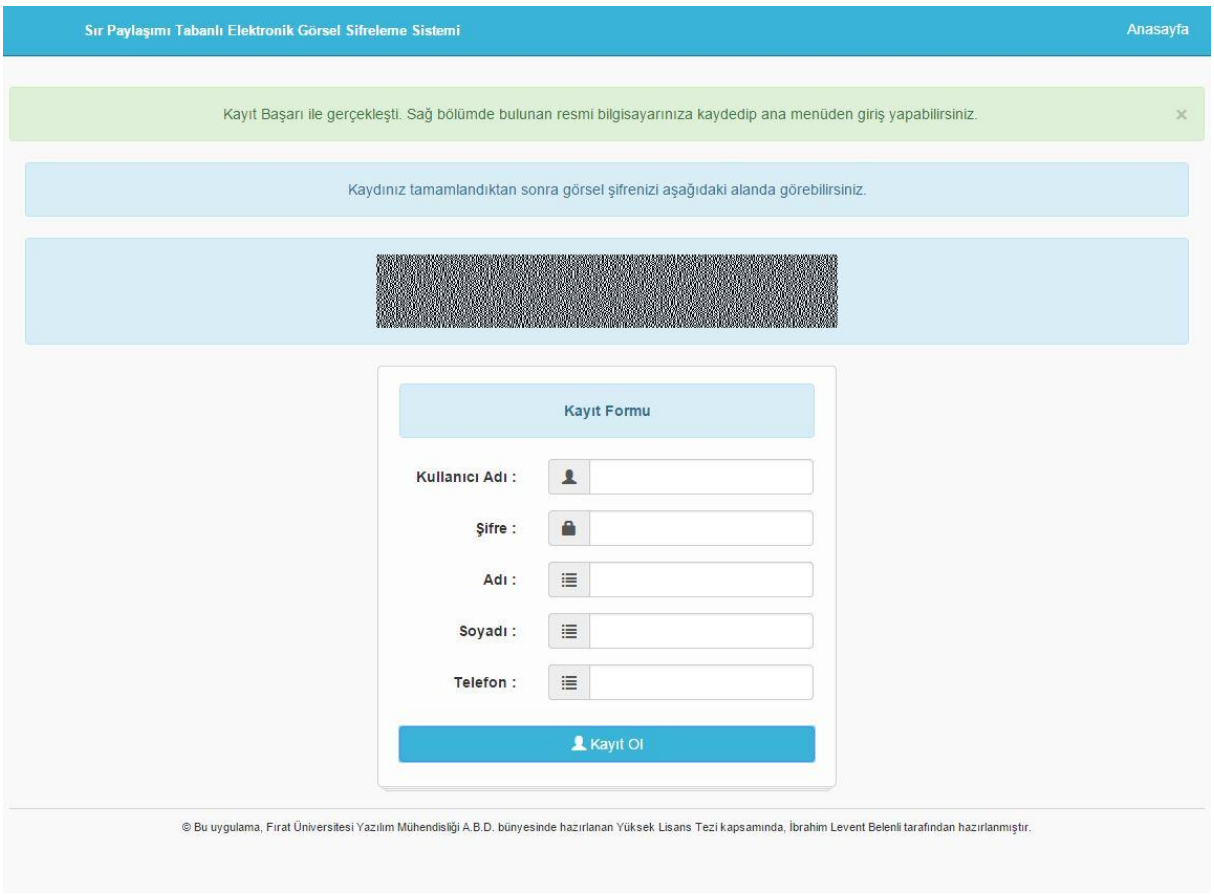
Şekil 7. 3 Resim haline getirilmiş olan şifre

Oluşturulmuş olan bu resim Shamir' in eşikli sır paylaşımı şeması kullanılarak 2 parçaya ayrılır (2 sayısı isteğe bağlıdır. İstenirse görsel daha fazla parçaya ayrılabilir). Elde edilen şifrenin parçalarından ilki veri tabanına kaydedilmektedir. Elde edilen diğer parça ise sisteme giriş esnasında kullanabilmesi için kullanıcıya verilmektedir (Şekil 7.4.)



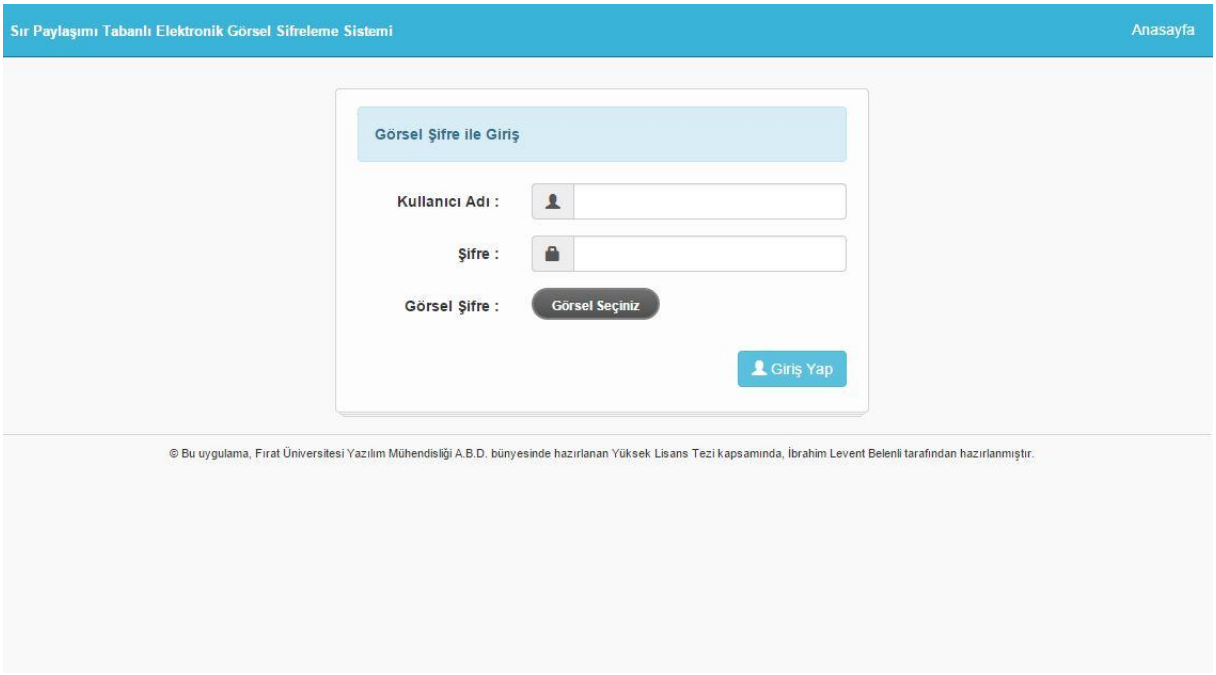
Şekil 7. 4 Kullanıcıya verilen sır parçası

Gerçekleştirilen bu aşamaların ardından kullanıcı kaydı başarıyla tamamlanmış demektir (Şekil 7.5).



Şekil 7. 5 Web tabanlı uygulamanın kayıt başarılı ekranı tasarımı

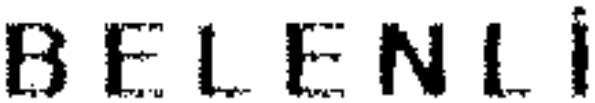
Elektronik görsel şifreleme sistemin web tabanlı uygulamasına kayıt olma işleminin tamamlanmasının ardından sisteme giriş yapılabilmektedir. Sisteme giriş yapılması esnasında klasik kullanıcı giriş ekranlarından farklı olarak kullanıcı adı ve şifreye ek olarak birde görsel şifre gerekmektedir (Şekil 7.6). Bu şifre kullanıcı kaydı tamamlandığı esnada kullanıcıya verilen görseldir.



Şekil 7. 6 Web tabanlı uygulamanın kullanıcı giriş ekranı tasarımı

Kullanıcı adı, şifre alanları doldurulup görsel şifre sisteme yüklendikten sonra giriş yap butonuna tıklanarak form sunucuya gönderilmektedir. Sunucuya gönderilen form bilgilerinden öncelikle kullanıcı adı ve metin şifre alanları veritabanında sorgulanarak böyle bir kullanıcı olup olmadığı teyit edilmektedir. Eğer veritabanında böyle bir kullanıcı bulunabilirse görsel şifre devreye girmektedir. Kullanıcıya ait görsel şifre veritabanından çekilerek kullanıcının sisteme giriş esnasında yüklediği görsel şifre ile birleştirilmektedir. Bu birleşme ile ortaya çıkan görsel şifreden (Şekil 7.7) OCR yazılımı kullanılarak şifrenin elde edilebilmesi için öncelikle gürültünün temizlenmesi gerekmektedir. Gürültü temizlendikten sonra Şekil 7.8'de gösterilmiş olan resim elde edilmektedir. Elde edilen bu görsel üzerinde OCR yöntemi uygulanarak görsel üzerindeki karakterler metin olarak elde edilir. Bu metin ile veritabanında metin halinde bulunan şifre eşleşir ise sisteme giriş yapılmaktadır (Şekil 7.9).

Şekil 7. 7 Görsel şifrenin gürültülü hali



Şekil 7. 8 Görsel şifrenin gürültüden arındırılmış hali

Şekil 7. 9 Web tabanlı uygulamanın giriş başarılı ekranı tasarımı

8. KORELASYON ANALİZİ

Korelasyon analizi ki adet vektör ya da matris arasındaki ilişkiyi incelemek amacıyla kullanılmaktadır. Korelasyon analizi ile vektör veya matrisler üzerinde yapılan işlemlerin temel amacı aynı koordinatlara karşılık gelen pikseller arasındaki benzerliği incelemektir. İmgelere ait korelasyon katsayısının hesaplanması sonucunda, iki imgenin birbirine maksimum benzerlik göstermesi durumunda 1, minimum benzerlik göstermesi durumunda ise -1 olacak şekilde hesaplanmaktadır [54]. Korelasyon analizi imgelere ait piksellerin benzerliğinin tespiti esnasında sıkça kullanılan bir analiz yöntemidir. (bkz. Formül (8.1)). Bu denklemde verilen eşitlikte, A ve B imgelerine ait piksellerin ortalama değerleri gösterilmektedir [55].

$$\rho_{kor} = \frac{\sum_m \sum_n (A_{mn} - \bar{A})\,(B_{mn} - \bar{B})}{\sqrt{\sum_m \sum_n (A_{mn} - \bar{A})^2 \; \sum_m \sum_n (B_{mn} - \bar{B})^2}} \tag{8.1}$$

Korelasyon katsayısı kullanılarak görsel şifreleme uygulamasında kullanılan resimler arasındaki ilişki tespit edilecektir ve korelasyon katsayısının formülü Formül (8.2)'te gösterildiği gibidir.

$$r = \frac{\sum x_i y_i}{\sqrt{\sum x_i^2 \sum y_i^2}}$$

$$= \frac{\sum (X_i - \bar{X})(Y_i - \bar{Y})}{\sqrt{\sum (X_i - \bar{X})^2 \sum (Y_i - \bar{Y})^2}} \tag{8.2}$$

Korelasyon katsayısı hesaplanırken kullanılacak olan formül Formül (8.22)'te gösterilmiştir. Bu formülün hesaplanması sonucu elde edilecek olan değer, web tabanlı şifreleme sisteminden üretilen resimler arasındaki ilişkinin yorumlanmasında kullanılacaktır. Bu değerin yorumlanabilmesi için Tablo 8.1'e bakmamız gerekmektedir [43].

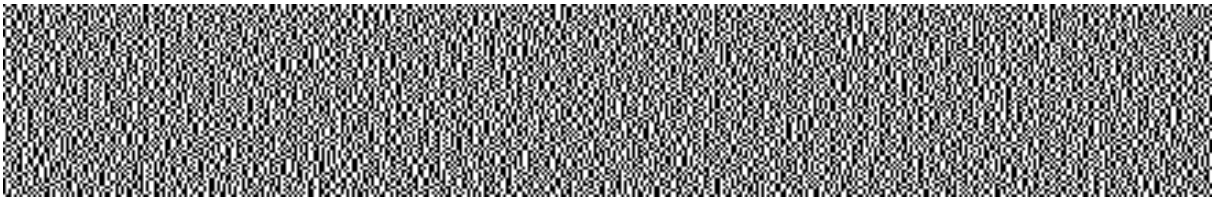
Tablo 8. 1 Pearson Korelasyon Katsayısının Yorumlanması

r	İlişki
0-0,25	Çok Zayıf
0,25-0,50	Zayıf
0,50-0,70	Orta
0,70-0,90	Yüksek
0,90-1,00	Çok Yüksek

Şifrenin görselleştirilmiş haliyle (Şekil 8.1) birinci sır parçası arasındaki korelasyon katsayısı 0,001 olarak hesaplanmıştır. Ayrıca görsel şifre ile ikinci sır parçası arasındaki korelasyon katsayısı da 0,002 olarak hesaplanmıştır. Elde edilen bu değerler Pearson korelasyon katsayısının yorumlanması tablosu üzerinden değerlendirildiğinde, sır parçaları ile şifrenin görselleştirilmiş hali arasındaki ilişkinin çok zayıf ve hatta yok denilecek kadar az olduğu görülmektedir.

Şekil 8. 1 Şifrenin görselleştirilmiş hali

Şekil 8. 2 Birinci sır parçası



Şekil 8. 3 İkinci sır parçası

9. SONUÇ VE ÖNERİLER

Bu bölümde, bu tez çalışması kapsamında yapılmış olan çalışmalar değerlendirilecek ve bu değerlendirmeler sonucunda çalışmanın nasıl daha da geliştirilebileceği hakkında öneriler yapılacaktır.

Bu tez çalışmasında yeni bir dijital şifreleme yöntemi geliştirebilmek için kullanılması gereken yöntem ve teknolojiler incelenmiş ve bu yöntem ile teknolojiler içerisinden uygun olanlar tespit edilerek sır paylaşımı tabanlı elektronik görsel şifreleme sisteminin web tabanlı uygulaması geliştirilmiştir.

Bu çalışma ile gerçekleştirilen dijital şifreleme yönteminin temeli kriptoloji ve sır paylaşımının harmanlanmasına dayanmaktadır. Bu nedenle kötü niyetli bir kişi oluşturulan görsel şifreyi ele geçirse ve bu resmin bir şifre olduğunu anlasa ve hatta bu resmi hangi sistem üzerinde kullanabileceğini anlasa bile elde ettiği görsel şifre sadece bir sır parçası olduğu için sisteme giriş yapabilmesi mümkün olmamaktadır. Tek bir görsel şifrenin anlamlı hale gelebilmesi mümkün değildir. Görsel şifreler ancak bir araya geldiklerinde anlamlı hale gelmektedir. İki resim bir araya geldiğinde çalışma kapsamında anlatılmış olan piksel tabanlı algoritma ile anlamlandırılmakta ve tek bir resim haline dönüşmektedir. Elde edilmek istenen asıl gizli bilgi bu aşamalar sonucunda ortaya çıkacak olan üçüncü görselin içerisindedir. Bu nedenle geliştirilen bu sistemin kullanıcı doğrulama sistemlerinde kullanılması, kullanılacak sistemin güvenlik seviyesini daha üst bir düzeye taşıyacaktır.

Sistemin önemli getirilerinden bir tanesi de basit şifrelerin çok daha etkili bir hale getirilebilmesidir. Böylelikle kullanıcıları, şifrelerini belirlerken karmaşık şifreler belirlemeleri yönünde zorlamalar anlamsız hale gelmiştir. Çünkü geliştirilen sistemde kullanıcı tek karakterlik bir şifre belirlese bile, bu şifre piksel tabanlı bir algoritma kullanılıp farklı iki resim içerisine dağıtıldığı için, bu basit şifre bile kırılması zor bir hal almaktadır.

Görsel şifrenin yaygın olarak kullanılmaya başlamasıyla, üretilen görsellerin birer şifre oldukları herkes tarafından bilinmeye başlanacaktır. Her ne kadar şifrenin çözülebilmesi için diğer sır parçasına ihtiyaç olsa da, üretilen görselin bir şifreleme sisteminin parçası olduğunun bilinmesi, sistemi üzerinde analiz çalışmaları yapılacak bir hale getirecektir. Bu yüzden çalışma kapsamında kriptoloji yöntemleri ve sır paylaşım yöntemlerinin yanı sıra steganografi yöntemlerinden de detaylıca bahsedilmiştir. Üretilen bu görseller steganografik yöntemler kullanılarak dikkat çekmeyecek şekilde alakasız resimlerin içerisinde tutularak, bu görsellerin şifre olduğunun anlaşılmasının önüne geçilebilecektir. Böylece sistemin güvenlik seviyesi daha üst seviyelere çıkartılabilecek ve sistemin çözülebilmesi ihtimali çok daha azaltılabilecektir.

KAYNAKÇA

[1] **Naor, M., Pinkas, B., "**Efficient oblivious transfer protocols", SODA, pp 448–457, 2001.

[2] **ISO/IEC 15946-1-2008**, "Cryptographic techniques based on elliptic curves", Information Technology, 2008.

[3] **Berrut J. P., Trefethen L. N.,** "Barycentric Lagrange Interpolation", SIAM Review Vol. 46, No. 3, pp. 501–517, 2004.

[4] **Kaya E.,** "Optimal Sır Resim Paylaşımı", Yüksek Lisans Tezi, Erciyes Üniversitesi, 2010.

[5] **Rivest, R., Shamir, A., Adleman, L.,** "A method for obtaining digital signatures and public-key cryptosystems", Communications of the Association for Computing Machinery pp 120-126, 1978.

[6] **Shamir, A., "**How to share a secret", Communications of the ACM, pp 612-613, 1979.

[7] **Chen. C. C., Fu. W. Y., Chen. C. C.,** "A Geometry Based Secret Image Sharing Approach", Proceedings IVCNZ (Image and Vision Computing, Newzeland), 2005.

[8] **Noar, N., Shamir, A.,** "Visual Cryptography", Advances in Cryptography, pp 1-12, 1995.

[9] **Chang. C.C., Tsai, H. M.,** "A Generalized Secret Sharing Scheme", Journal of System and Software pp 267-272, 1997.

[10] **Lin, H. Y., Harn, L.,** "A Generalized Secret Sharing Scheme with Cheater Detection", Lecture Notes in Computer Science, Advances in Cryptology Berlin, pp 149-158, 1993.

[11] **Chang, C.C., Huang, R.J.,** "Sharing secret images using shadow codebooks", Information Science pp 335-345, 1998.

[12] **Tsai, C.S., Chang, C.C., Chen, T.S.,** "Sharing multiple secrets in digital images", J. Syst. Software pp 163-170, 2002.

[13] **Lukac, R., Plataniotis, K.N.,** "A cost-effective encryption scheme for color images", Real-Time Imag. pp 454-464, 2005.

[14] **Lukac, R., Plataniotis, K.N.,** "Bit-level based secret sharing for image encryption", Pattern Recognition pp 767-772, 2005.

[15] **Ulutürk A., "**Gelişmiş Şifreleme Standardı", Yüksek Lisans Tezi, Gazi Üniversitesi, 2010.

[16] **Aksuoğlu A.,** "Rsa Algoritmasının İyileştirilmesi İçin Yeni Bir Yaklaşım", Yüksek Lisans Tezi, Anadolu Üniversitesi, 2010.

[17] **İnternet, Pro-G ve Oracle,** "Bilişim Güvenliği Sürüm 1.1", http://www.prog.com.tr/whitepapers/bilisim-guvenligi-v1.pdf (Son Erişim Tarihi: 15.03.2015), 2003.

[18] **Baskök, M. D.,** "AES Sifreleme Algoritmasının Modellenmesi", Yüksek lisans, Gazi Üniversitesi Fen Bilimleri Enstitüsü, Ankara, 9-13, 2007

[19] **Koblitz, N.,** "A course in Number theory and Cryptography", Springer Verlag, 1994.

[20] **Tsunoo Y., Tsujihara E., Minematsu K., Miyauchi H.,** "Cryptanalysis of Block Ciphers Implemented on Computers with Cache", ISITA, 2002.

[21] **NBS FIPS PUB 46,** "Data Encryption Standard" , National Bureau of Standarts, U.S. Departman of Commerce, 1977.

[22] **Diffie, W., Hellman, M.,** "New directions in cryptography." IEEE Trans. Inform. Theory IT-22, pp 644-654, 1976.

[23] **Rivest R.,. Shamir A., Adleman L.,** "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of the ACM, v. 21, n. 2 pp. 120-126, 1978.

[24] **Ellison C., Schneier B.,** "Ten Risks of PKI: What You're Not Being Told About Public Key Infrastructure", Computer Security Journal, vol. 16, no. 1, pp. 1-7, 2000.

[25] **Yerlikaya T., Buluş E., Arda D.,** "Asimetrik Kripto Sistemler Ve Uygulamaları", II. Mühendislik Bilimleri Genç Araştırmacılar Kongresi İstanbul, 2005.

[26] **Atay S.,** "Eliptik Eğri Tabanlı Kriptografik Protokol ve Akıllı Kart Üzerinde Bir Uygulama", Ağ ve Bilgi Güvenliği Sempozyumu, 2005.

[27] **Matsui, M.,** "Linear Cryptanalysis Method for DES Cipher", Advances in Cryptology- Eurocrypt '93, Springer-Verlag, pp 386-397, 1994.

[28] **Biham, E. , Shamir, A. ,** "Differential Cryptanalysis of the full 16-round Data Encryption Standard", Advances in Cryptology: Proceedings of CRYPTO'92, Springer-Verlag, Berlin, pp 487–496, 1993.

[29] **Knudsen, L. R.** , "Truncated and Higher Order Differentials", Fast Software Encryption, Springer-Verlag, pp 196–211, 1995.

[30] **Daemen, J. , Knudsen, L. R. , Rijmen, V.** , "The Block cipher Square", Fast Software Encryption, Springer Verlag, New York, pp 149–165, 1997.

[31] **Mesut A.,** "Bilgi Gizleme Teknikleri", http://andacmesut.trakya.edu.tr/bgt (Son Erişim Tarihi, 27.12.2014), 2013.

[32] **Dereli Ç.,** "Dilbilimsel Steganografi Yöntemleri üzerine bir Araştırma", Yüksek Lisans Tezi, Ege Üniversitesi, 2010.

[33] **Bilgin M.,** "Steganografi", 2012.

[34] **CompuServe Incorporated Columbus,** "Graphics Interchange Format(sm), Version 89a", Ohio, 1990.

[35] **Cox I.J., Kilian J, Leighton T., Shamoon T.,** "A Secure, Robust Watermark for Multimedia", Proceedings First International Workshop Information Hiding, Lecture Notes in Computer Science No. 1, 174, pp. 185-206, Berlin, 1996.

[36] **Tuncer T.,** "Resimler için Veri Gizleme Tabanlı Bilgi Güvenliği Uygulamaları", Yüksek Lisans Tezi, Fırat Üniversitesi, 2011.

[37] **Hartung F., Kutter M.,** "Multimedia watermarking techniques,", Proceedings of the IEEE, vol. 87, pp. 1079–1107., 1999

[38] **Heredotus,** "The Histories", First Published in Greek 430 B.C.E., Translated by Selincourt A., Penguin Classics, Hammondsworth, 1971.

[39] **Ş. Doğan, T. Tuncer, E. Avci, A. Gulten,** "A New Watermarking System based on Discrete Cosine Transform (DCT) in Color Biometric Images", Journal of Medical Systems, 2011.

[40] **Tunçkanat M., Sağıroğlu Ş.,** "Güvenli İletişim İçin Yeni Bir Yaklaşım: Resim İçerisine Döküman Gizleme", GAP IV. Mühendislik Kongresi (Uluslararası Katılımlı) Şanlıurfa, 2002.

[41] **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: 7803-8513, 2004.

[42] **Johnson N.F., Duric Z., Jajodia S.,** "Information Hiding: Steganography and Watermarking - Attacks and Countermeasures", Kluwer Academic Publishers, ISBN: 0-79237-204-2, 2000.

[43] **Morkel T., Eloff J.H.P., Olivier M.S.,** "An Overview of Image Steganography", Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton South Africa, 2005.

[44] **Şahin A.,** "Görüntü Steganografide Kullanılan Yeni Metodlar Ve Bu Metodların Güvenilirlikleri", Trakya Üniversitesi, 2007.

[45] **Bender W., Gruhl D., Morimoto N., Lu A.,** "Techniques for data hiding", IBM Systems Journal, vol. 35, 1996.

[46] **Hartung F., Kutter M.,** "Multimedia watermarking techniques", Proceedings Of the IEEE, vol. 87, pp. 1079–1107, 1999.

[47] **Johnson N.F, Jajodia S.,** "Exploring steganography: Seeing the Unseen", Computer, 31 pp 2:26-34, 1998

[48] **Johnson N. F., Jajodia S.,** 1999, "Stegananalysis of Images Created Using Current Steganography Software", Second Information Hiding Workshop held in Portland, Oregon, USA, 1998.

[49] **Marvel L.M., Boncelet C.G., Jr. Retter C.T.,** "Reliable Blind Information Hiding for Images", Proceedings of 2nd Workshop on Information Hiding (D. Aucsmith, editor), Lecture Notes in Computer Science, Springer, 1998.

[50] **Barni M., Bartolini F., Cappellini V., Piva A.,** "Robust Watermarking of Stil Images for Copyright Protection", Proceedings of DSP'97, International Conference on Digital Signal Processing, Santorini, Greece, pp.499-502, 2-4, 1997.

[51] **Cox I.J., Kilian J, Leighton T., Shamoon T.,** "A Secure, Robust Watermark for Multimedia", Proc. First International Workshop Information Hiding, Lecture Notes in Computer Science No. 1, 174, Springer-Verlag, Berlin, 1996.

[52] **Milli Eğitim Bakanlığı**, "Radyo-Televizyon Fotoğraf, Ses ve Video Formatları", 2011

[53] **Zadeh S.,** "Çok Parçalı Sır Paylaşım Şemaları ve Uygulamaları", Yüksek Lisans Tezi, Karadeniz Teknik Üniversitesi, 2012

[54] **Mark Hoemmen,** "Computing the standard deviation efficiently", http://www.cs.berkeley.edu/~mhoemmen/cs194/Tutorials/variance.pdf (Son erişim 10/03/2015), 2007.

[55] **Big Pan**, "Two-dimensional digital image correlation for in-plane displacement and strain measurement: a review, Measurement Science and Technology", 2009.

ÖZGEÇMİŞ

İbrahim Levent BELENLİ

Kişisel Bilgileri

Uyruğu: T.C.

Doğum Tarihi: 01.01.1989

Doğum Yeri: Silifke/MERSİN

Telefon: 05056303989

E-mail: ibrahim.belenli @inonu.edu.tr

Eğitim Bilgileri

Öğrenim Dönemi	Okul	Öğrenim Türü
2002 - 2007	Silifke Anadolu Teknik Lisesi, Bilgisayar Yazılımı Bölümü	Lise
2008 - 2012	Fırat Üniversitesi, Teknik Eğitim Fakültesi, Elektronik ve Bilgisayar Eğitimi Bölümü	Lisans
2012 - 2015	Fırat Üniversitesi, Fen Bilimleri Enstitüsü, Yazılım Mühendisliği A.B.D.	Yüksek Lisans

Çalıştığı Projeler

Sır Paylaşımı Tabanlı Elektronik Görsel Şifreleme Sistemi – Tübitak 1512 (2013 - 2015) FPGA Tabanlı Kan Sayım Cihazı – Tübitak 1001 (2013 - 2015)