FEN BİLİMLERİ ENSTİTÜSÜ

CEBİRSEL ŞİFRELENMİŞ LSB YÖNETİMİ

Ali KARADURAN

Danışman
Dr. Öğr. Üyesi Metin TURAN

YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
İSTANBUL - 2020

KABUL VE ONAY SAYFASI

Ali KARADURAN tarafından hazırlanan **"Cebirsel Şifrelenmiş LSB Yöntemi"** adlı tez çalışması 08/09/2020 tarihinde aşağıdaki jüri üyeleri önünde başarı ile savunularak, İstanbul Ticaret Üniversitesi Bilgisayar Mühendisliği **Anabilim Dalı**'nda **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Danışman	**Dr. Öğr. Üyesi Metin TURAN** İstanbul Ticaret Üniversitesi	.....
Jüri Üyesi	**Dr. Öğr. Üyesi Ali BOYACI** İstanbul Ticaret Üniversitesi	.....
Jüri Üyesi	**Dr. Öğr. Üyesi Zeynep TURGUT** Haliç Üniversitesi	.....

Onay Tarihi : 18.09.2020

İstanbul Ticaret Üniversitesi, Fen Bilimleri Enstitüsünün 18 09.2020 tarih ve 2020/290 numaralı Yönetim Kurulu Kararının 2. maddesi gereğince, ders yüklerini ve tez yükümlülüğünü yerine getirdiği belirlenen "Ali KARADURAN" (TC:14198113862) adlı öğrencinin mezun olmasına oy birliği ile karar verilmiştir.

Prof. Dr. Necip ŞİMŞEK
Enstitü Müdürü

AKADEMİK VE ETİK KURALLARA UYGUNLUK BEYANI

İstanbul Ticaret Üniversitesi, Fen Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında,

- tez içindeki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,
- görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu,
- başkalarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunduğumu,
- atıfta bulunduğum eserlerin tümünü kaynak olarak gösterdiğimi,
- kullanılan verilerde herhangi bir tahrifat yapmadığımı,
- ve bu tezin herhangi bir bölümünü bu üniversitede veya başka bir üniversitede başka bir tez çalışması olarak sunmadığımı

beyan ederim.

18/09/2020

Ali KARADURAN

İÇİNDEKİLER

ÖZET

Yüksek Lisans Tezi

CEBİRSEL ŞİFRELENMİŞ LSB YÖNTEMİ

Ali KARADURAN

İstanbul Ticaret Üniversitesi
Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı

Danışman: Dr. Öğr. Üyesi Metin TURAN

2020, 52 sayfa

Teknolojinin gelişmesiyle ile birlikte bilgi güvenliğine olan ihtiyaç da önemli hale gelmiştir. Veri güvenliğinin amacı veride gizlenen mesajın üçüncü kişinin eline geçse bile anlayamayacağı formata getirilerek hedefe gönderilmesidir. Veri güvenliği ile alakalı kriptografi ve steganografi teknikleri kullanılmaktadır.

Bu tez çalışmasında stenografi bilim dalının en az ağırlıklı bit şifreleme tekniği olarak bilinen LSB algoritmasının veri güvenliğinin cebirsel ifadeler ile iyileştirerek, belli oranda daha fazla sıkıştırma sağlarken resim üzerinde oluşan değişim hata oranını da çok artırmamak amaçlanmıştır. Geliştirilen algoritmada mesajın 24 bit renkli resimlere şifrelenmesi sağlanmıştır. Mesajda yer alan her karakter, şifrelenmek istenen resmin 2 pikseline kodlanır. Modelin başarımını ölçmek üzere (orijinal resim ile şifreli resmin değişim oranı) MSE ve PSNR metrikleri kullanılmış, LSB algoritması ile önerilen çalışma yaygın olarak kullanılan bazı model resimler üzerinde farklı uzunluktaki mesajlar için karşılaştırılmışlardır. Elde edilen sonuçlara göre, çalışmada önerilen algoritmanın sıkıştırma oranı %33 daha iyi olmasına rağmen, yapılan sınamalarda elde edilen değerlerin ortalamasına göre beklendiği üzere MSE hata oranı %29 artmış ve PSNR ise %2,5 azalmıştır. Her ne kadar metrik değerleri negatif gözükse de, orijinal resimdeki bu değişimler çok ufak ve gözle algılanabilir olmaktan uzaktır. Kazanılan sıkıştırma oranı ve ayrıca verinin gizlenme güvenliği göz önünde bulundurulduğunda, güvenliğin önemli olduğu uygulamalara hitap ettiği düşünülmelidir.

Araştırmada verinin gizliliğini sağlayan LSB ve cebirsel ifadeler ile iyileştirilen yöntemlerin geliştirilmesi C# yazılım dili kullanılarak gerçekleştirilmiştir. Resmin piksellerine veri gizleme işlemleri yapıldıktan sonra, MSE ve PSNR metrik değerlerinin hesaplanması için Matlab programı kullanılmıştır.

Anahtar Kelimeler: En az ağırlıklı bit, kriptoloji, metin şifreleme, stenografi.

ABSTRACT

M.Sc. Thesis

ALGEBRAIC ENCRYPTIONED LSB METHOD

Ali KARADURAN

İstanbul Commerce University
Graduate School of Applied and Natural Sciences
Department of Computer Engineering

Supervisor: Assist. Prof. Dr. Metin TURAN

2020, 52 pages

With the development of technology, the need for information security has also become important. The purpose of data security is to send the message hidden in the data to the destination, which it cannot understand even if it is received by the third person. Cryptography and steganography techniques related to data security are used.

In this thesis, it is aimed to improve the data security of LSB algorithm, which is known as the least weighted bit encryption technique of the shorthand discipline by algebraic expressions, while providing a certain amount of compression, and not to increase the error rate of the change on the picture. In the developed algorithm, the message is encrypted into 24-bit color images. Each character in the message is encoded into 2 pixels of the picture that you want to encrypt. MSE and PSNR metrics were used to measure the performance of the model (the rate of change of the original picture and the encrypted picture). The proposed study with the LSB algorithm was compared for messages of different lengths on some commonly used model pictures. According to the results obtained, although the compression rate of the algorithm proposed in the study was 33% better, the MSE error rate increased by 29% and PSNR decreased by 2.5% as expected compared to the average of the values obtained in the tests. Although the metric values seem negative, these changes in the original image are very small and far from perceptible. Considering the compression rate gained and also the security of data hiding, it should be considered that it addresses applications where security is important.

LSB and algebraic expressions that ensure the confidentiality of the data in the research were developed using C # software language. After data hiding operations were done on the pixels of the image, Matlab program was used to calculate MSE and PSNR metric values.

Keywords: Cryptology, least significant bit, steganography, text encryption.

TEŞEKKÜR

Bu araştırma için beni yönlendiren, karşılaştığım zorlukları bilgi ve tecrübesi ile aşmamda yardımcı olan değerli Danışman Hocam Dr. Öğr. Üyesi Metin TURAN'a teşekkürlerimi sunarım. Literatür araştırmalarımda yardımcı olan değerli hocam Dr. Öğr. Üyesi Metin TURAN'a, teşekkür ederim.

Tezimin her aşamasında beni yalnız bırakmayan aileme sonsuz sevgi ve saygılarımı sunarım.

Ali KARADURAN
İSTANBUL, 2020

ŞEKİLLER

ÇİZELGELER

Sayfa

SİMGELER VE KISALTMALAR

ASCII	American Standard Code for Information Interchange
BPCS	Bit Plane Complexity Segmantation
CMYK	Cyan, Magenta, Yellow, Key
dB	Desibel
DCT	Ayrık Cosinus Dönüşümü
DES	Data Encryption Standart
DFT	Ayrık Fourier Dönüşümü
DPI	2.54cm x 2.54cm 'lik kare alanın içindeki nokta sayısı
GIF	Graphichs Interchange Format
ICMP	Internet Control Message Protocol
IDEA	International Data Encryption Algorithm
IP	Internet Protocol
JPEG	Joint Photographic Expert Groups
LPI	2.54 cm 'lik alana düşen satır sayısı
LSB	Least Significant Bit
MSE	Mean Squared Error
OSI	Open System Interconnection
PNG	Portable Network Graphichs
PSNR	Peak Signal to Noise Ratio
RGB	Red Green Blue
RSA	Rivest-Shamir-Adleman Cryptosystem
SHA	Secure Hash Algorithm
SSIS	Spread Spectrum Image Steganography
TCP	Transmission Control Protocol
TIFF	Taggged Image File Format
UDP	User Datagram Protocol
XOR	Exclusive OR

1. GİRİŞ

Teknolojinin gelişmesiyle bilgisayar dünyasında sayısal verilerin paylaşımı ve güvenliği önem kazanmıştır (Özbilgin ve Durmuş, 2018). Bu veriler resim, ses, metin ve video formatlarında olabilir. Teknolojinin gelişmesi ile verilerin güvenliği konusunda ciddi problemler çıkmaktadır. Elektronik ortamda saklanan sayısal verilerin alıcıya gönderilirken bu verilerin korunması gereklidir. Alınan önemlere rağmen değişik tipte tehdit yöntemleri ortaya çıkmaktadır. İletişim gizliliğinde ve verinin güvenli biçimde iletilmesinde en çok bilinen yöntem Kriptografidir (Sevindir ve Sayın, 2018). Kriptografi verinin algoritma ile biçim değiştirilmesiyle karşı tarafa gönderilme işlemidir. Veriyi alan kişi verinin şifrelenmiş olduğunu biliyorsa, şifre çözme algoritması ile mesajı geri elde edebilir. Kriptografi yönteminin özel bir uygulama alanı steganografi yöntemidir (Şahin vd., 2005).

Kriptolojinin bir uygulama alanı olan Steganografi resime veri gizleme bilimidir. Mesaj resimin piksellerine şifrelenir. Dışarıdan resime bakıldığında göz ile ayrıntılar normal resimden ayırt edilemez. Son zamanlarda kriptoloji ve steganografi beraber kullanılmaya başlanmıştır. Veri gizleme işleminden önce mesaj şifrelenir ve bu şifreli bilgiler resime gizlenir.

2. LİTERATÜR ÖZETİ

2.1. Temel Kavramlar

Sayısal görüntü, bilgisayar ortamındaki görüntü dosyalarına verilen isimdir. Sayısal görüntü farklı dosya türleri olarak elektronik ortamda saklanmaktadır. Sayısal görüntüler ile ilgili piksel, çözünürlük, LPI, DPI ve nokta aralığı gibi kavramların bilinmesi gerekmektedir (Özbilgin vd., 2018).

2.1.1. Piksel

Sayısal görüntüler noktalardan oluşmaktadır. Görüntü yakınlaştırıldığında veya büyütüldüğünde noktaların kare olduğu görülmektedir. Bu karelere piksel denilir. Bir piksel, RGB (Red, Green, Blue) değerlerinden oluşmaktadır. Resim ne kadar çok piksel içeriyorsa resim netliği de o kadar iyi olmaktadır (Özbilgin vd., 2018).

2.1.2. Çözünürlük

Görüntü dosyalarında görüntüyü oluşturan piksel sayısının tamamına çözünürlük denilmektedir. Çözünürlük yüksek olduğunda resim kalitesi de o kadar iyidir (Belenli, 2015).

2.1.3. Nokta ve nokta aralığı

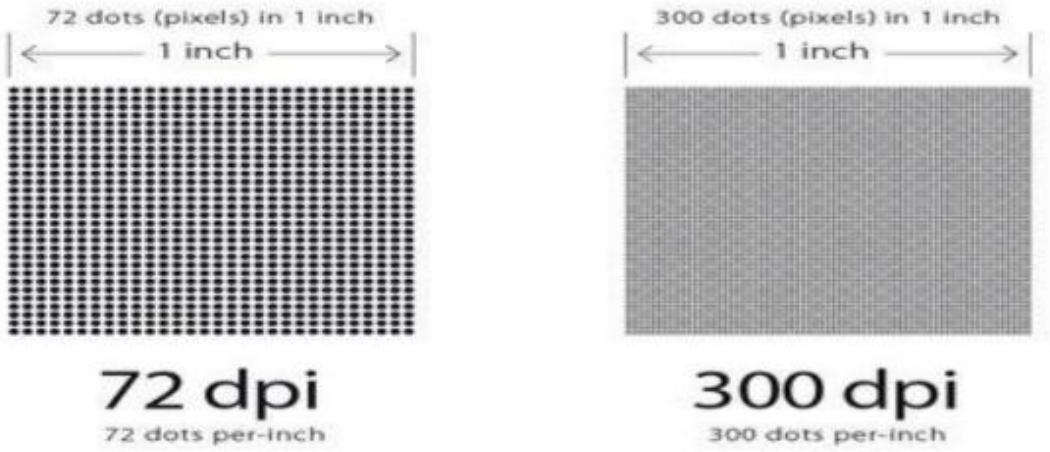
Pikseli oluşturan RGB renklerinin her birine nokta denilmektedir. Pikseli oluşturan RGB renklerinin arasındaki mesafeye nokta aralığı denilmektedir. Bu nokta aralığı değeri ne kadar az ise resim o kadar iyi denilir (Belenli, 2015).

2.1.4. İnç başına düşen çizgi sayısı

Bir inç 2.54 cm den oluşmaktadır. 2.54 cm 'lik alana düşen satır sayısına LPI denilir. Bu satırlar noktalardan oluşmaktadır. Satırları oluşturan nokta dizilerine tram denilir. LPI çözünürlüğü tram sıklığını elde etmemizi sağlamaktadır (Belenli, 2015).

2.1.5. İnç başına düşen nokta sayısı

Bir inç olarak adlandırılan 2.54 cm x 2.54cm kare içinde nokta sayısına DPI denir. 1 inç alana daha fazla kare sıkıştırmak için noktaların küçülmesi gerekmektedir. Bir inç kareye ne kadar çok nokta girerse baskı da o kadar kaliteli olur. İki farklı DPI arasındaki fark Şekil 2.1'de gösterilmiştir (Belenli, 2015).



Şekil 2.1. 72 Dpi ile 300 dpi görüntü arasındaki fark

2.2. Sayısal Görüntü Formatları

Görüntü dosyaları eğriler, alanlar ve doldurdukları renkler veya noktalar topluluğu olarak iki türde saklanabilmektedir. İlk yöntem eğriler, alanlar ve doldurdukları renkler metoduna vektör tabanlı resim, ikinci yöntem ise noktalar topluluğu metoduna da piksel tabanlı resim denilmektedir. Bu

çalışmada görüntü formatı, çalışmanın vektörel grafik formatlarına ihtiyaç duyulması sebebiyle piksel tabanlı resim formatları olacaktır. En popüler görüntü dosya türleri GIF, BMP, PNG, JPEG, TIFF 'dir.

2.2.1. Gif

Bu fotoğraf türünün açılımı 'Graphichs Interchange Format' dır. Bu dosya türü internet alanında sıkça kullanılmaktadır. Az sayıda renk içeren dosyalarda iyi sıkıştırma sağlaması, animasyonlarda zamanlama bu formatı popüler yapan nedenlerdir (Belenli, 2015).

2.2.2. Bmp

Windows 3.1 ve Windows 95 ile beraber gelen Paint uygulamasının işlediği, 1-24 bit renk derinliği içeren dosya tipidir. BMP dosya tipinde ilk zamanlarda sıkıştırma özelliği bulunmamaktaydı. Fakat daha sonra opsiyonel kayıpsız sıkıştırma özelliği eklenmiştir. Bu sıkıştırma işleminde veri kaybı olmamaktadır. BMP formatı Paint'ten başka görüntüleme uygulaması olmayan cihazlarda kullanılır (Gürel, 2006).

2.2.3. Png

Bu fotoğraf türünün açılımı "Taşınabilir Ağ Grafiği" 'dir. PNG dosya türünde kayıpsız sıkıştırarak görüntü saklama biçimidir. Resmi katmanlar halinde saklamaya izin verir. PNG dosya türünün kayıpsız format olmasından dolayı grafik ve metin içeren dosyalarda iyi sonuç vermektedir (Belenli, 2015).

2.2.4. Jpeg

Dünyada en çok kullanılan fotoğraf dosya türüdür. JPEG dosya türü, Joint Photographic Experts Group tarafından standartlaştırılmış sayısal görüntü kodlama türüdür. Bu görüntü dosyasının uzantısı ".jpg"dir (Eskiçırak, 2012).

Bu dosya türü sıkıştırma yöntemini kullanmaktadır. JPEG dosya türü zorunlu olmayan detayları atan ve dosyayı son haliyle sıkıştıran bir dosya türü olduğu için görüntüde kayıp alanlar olmaktadır. JPEG dosya türünde renk değerlerinde değişiklik olmaz. JPEG formatın özelliği görüntünün gerçek renk değerlerini içermesidir. Bundan dolayı fotoğrafik görüntüleme için kullanılır.

2.2.5. Tiff

Bu fotoğraf türünün açılımı 'Tagged Image File Format'tır. TIFF türünün 1, 8, 24 bitlik formatları bulunmaktadır. Bu formatlar sıkıştırılmış ve sıkıştırılmamış 2 farklı tipe sahiptir. 1 bit fakslarda dosya iletiminde kullanılır. Çok fazla renkle işlem yapıldığında ve zaman önemli fakat yer önemli değil ise, TIFF dosya türünün kullanılması fayda sağlamaktadır (Gürel, 2006).

TIFF formatı farklı işletim sistemleri ve uygulamalar arasında kayıpsız ve esnek dosya değişimi sağlaması sebebiyle tüm çalışmalar için uygun bir formattır. TIFF dosya türü LZW, RGB, CMYK, Lab sıkıştırma ve dosya biçimlerini desteklemektedir.

2.2.6. Pict

PICT dosya türünü bilgisayar ortamında her program kullanabilmektedir. Herhangi bir programa gönderildiği zaman, imge bilgisi imgeyle birlikte sayfaya dâhil olmaktadır (Yiğit, 2018).

3. VERİ GİZLEME YÖNTEMLERİ

Steganografi, bir örtü verinin içine veri gizlemek için kullanılan yöntemdir. Bu yöntemde şifrelenen verinin çözülebilmesi için kod çözme algoritmasının olması gerekmektedir. Steganografi yönteminde verinin gizlendiğinden haberiniz yoktur. Bu yöntemde resimler, video ve ses dosyaları üzerine işlem yapılmaktadır (Yürüklü, 2013).

Gizlenecek mesaj şifrelenmiş, düz metin veya bitler halinde kaydedilmektedir. Görüntü dosyalarında gizlenecek mesajlar metin dosyası veya herhangi bir resim içerisine şifrelenmiş başka resim dosyası da olabilir (Şahin vd., 2016).

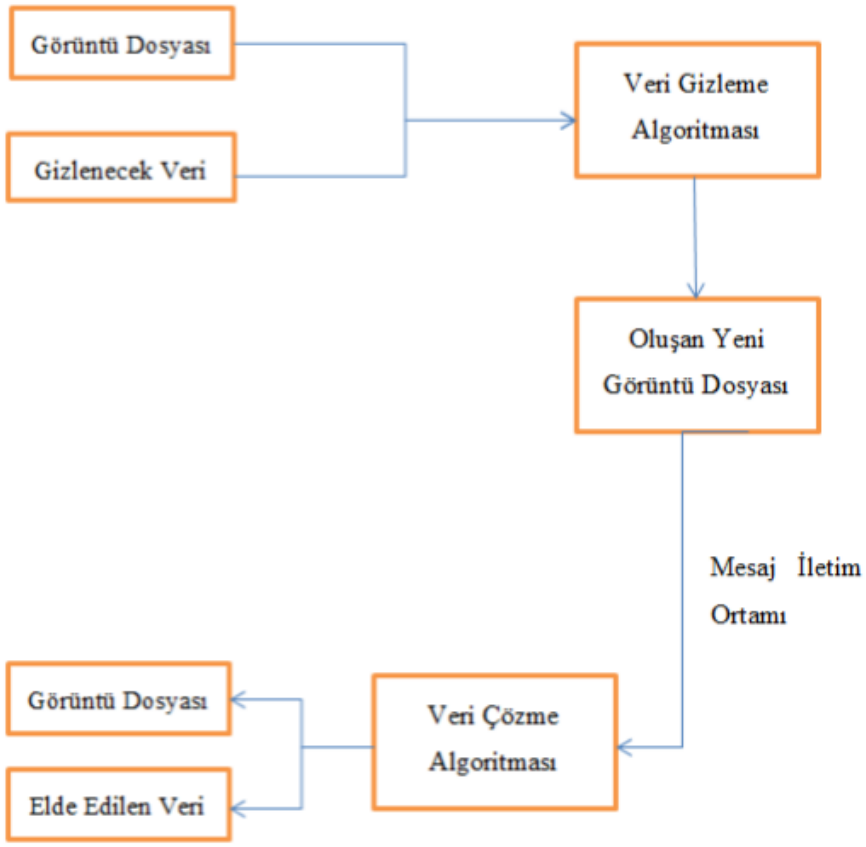
3.1. Steganografinin Tanımı

Steganografinin tarihi ilk şifreleme yapıldığı zamandan da öncesine gitmektedir. Eski Yunanistan'da mesajlar tahtalara yazılıp üzerine mum kaplanarak, cisim kullanılmamış tablete benzetilirdi. Mesajın okunabilmesi için mumum eritilmesi gerekmekteydi. Başka bir uygulamada, 1960' lı yıllarda mor ötesi ile yazı yazılan sprey ve kalemlerdir. Bu kalemle yazılan yazılan sadece mor ötesi ışık altında görünmekteydi (Tuncer, 2016).

Steganografi, çok eskiye dayanan bilgi gizleme tekniklerinden bir tanesidir. Latincede "steganos" kelimesi "görünmeyen" demektir. Steganografi kelimesi "gizlenmiş yazı" anlamına gelmektedir. Steganografinin amacı; mesajın dijital ortamda bulunan dosyalara gizlenerek anlaşılmamasını sağlamaktır (Solak ve Altınışık, 2018).

Steganografi bilgi gizleme tekniklerinden bir tanesidir. Bu teknik ile ses, video ve resim nesnelerinin içine veri gizlenebilmektedir. Görüntü dosyaları içerisine saklanacak veriler metin dosyası olabileceği gibi başka bir görüntü dosyası da olabilir.

Steganografinin sistem yapısı; gizlenecek verinin veri gizleme algoritması ile resim nesnesinin içine saklanmasıdır. Daha sonra veri gizlenmiş resmin üzerinde, veri çözme algoritması ile verinin çözme işlemi yapılmaktadır (Yaşar ve Özteriş, 2015). Steganografinin sistem yapısı Şekil 3.1 'deki gibidir.



Şekil 3.1. Steganografi sistem yapısı

Steganografi biliminde temel amaç bilgiyi saklamaktır. Bundan dolayı steganografi kriptolojinin bir parçasıdır. Kriptoloji ve steganografi beraber kullanıldığında verinin güvenliği artmaktadır. Mesaj kriptoloji ile şifrelenir daha sonra şifrelenen mesaj veri gizleme işlemi yapılarak görüntüye kaydedilir (Aydoğan, 2014). Görüntü üzerinde değişimin fark edilmemesi, görüntüde saklanacak verinin uzunluğu, dayanıklık olmak üzere 3 temel amaca dikkat edilmelidir (Esin ve Güvenoğlu, 2011).

- Görüntü üzerinde değişimin fark edilmemesi

Değişimin fark edilmeme amacı, görüntü üzerinde yapılan değişikliklerin insan duyuları tarafından fark edilmemesidir. Aksi takdirde görüntü içerisinde gizli veri olduğu anlaşılır ve üçüncü kişinin içerisinde gizli veri bulunan nesnede işlem yapma ihtimali ortaya çıkmaktadır.

- Görüntüde saklanacak verinin uzunluğu

Görüntü içerisinde gizlenecek veri miktarı önemli bir etkendir. Fakat gizlenen veri miktarı arttıkça resim üzerindeki değişim de arttığından dolayı insan gözüyle algılanabilecek duruma gelmektedir. Bu durum değişimin fark edilmeme amacıyla çelişmektedir.

- Dayanıklık

Gizlenen verinin saldırılara rağmen hedefteki kişi tarafından başarılı biçimde çıkartılabilmesi için düşünülmüş dayanıklılığı artırıcı önlemler, yapılması gereken işlem düzeyini artırmaktadır. Dolayısıyla dosya üzerinde yapılan değişim algılanabilecek seviyeye gelebilmektedir.

Yukarıda belirtilen steganografinin amaçlarının avantaj ve dezavantaj karşılaştırılması Hussain ve Hussain (2013) tarafından Tablo 3.1'de verilmiştir.

Çizelge 3.1. Steganografi algoritmasının kalitesini belirleyen ölçütler ve bu ölçütlerin avantaj ve dezavantajları

Ölçü	**Açıklama**	**Avantaj**	**Dezavantaj**
Yüksek Kapasite	Resim içerisine gizlenecek azami veri miktarı	Yüksek	Düşük
Algısal Şeffaflık	Veri gizleme işlemi tamamlandıktan sonra insan tarafından farkın algılanıp veri saklama işleminden şüphelenmesi	Yüksek	Düşük
Sağlamlık	Gizleme işlemi gerçekleştirildikten sonra resimde meydana gelen döndürme uzaklaştırma, küçültme, büyütme gibi işlemler sonunda gizlenen verinin orijinal haliyle yani kayıpsız olarak korunup korunamaması.	Yüksek	Düşük
Tavlama Direnci	Resmin içerisine metin gizlendikten sonra metinde değişiklik veya güncelleme yapılması.	Yüksek	Düşük
Hesaplama Karmaşıklığı	Resim içerisine veri gizlemenin ve gizlenen veriyi geri getirmenin hesaplama maliyeti	Düşük	Yüksek

3.2. Steganografi Alt Alanları

Steganografi kendi içerisinde Teknik Steganografi ve Dilbilim Steganografi olmak üzere ikiye ayrılmaktadır. Dilbilim Steganografide text, taşıyıcı veridir. Teknik Steganografi ise birçok alt metinden oluşmaktadır. Bunlar; gizli yerler, microdotlar, görünmez mürekkep ve bilgisayar tabanlı yöntemler başlıkları altında yer almaktadır. Bilgisayar tabanlı yöntemler görüntü, resim, ses ve metin dosyalarını kullanarak veri gizleme işlemidir. Görüntü steganografisinde görüntü uzayı ve dönüşüm uzayı tabanlı yöntemler kullanılmaktadır. İmge uzayında ise kullanılan yöntem LSB (Least Significant Bit) yöntemidir. Dönüşüm uzay tabanlı metotlar imge verisini frekans uzayını dönüştürdükten sonra saklama işlemini dönüşüm uzayında yapmaktadır (Kurtuldu, 2009).

3.2.1 Dilbilim steganografi

Steganografide verinin gizlenecek yerinin metin (text) olduğu durumdur. Burada mesaj text (metin) içine yazı tipinin değiştirilmesi ile gizlenmektedir. Bu steganografi yönteminde değişiklik yapmanın birkaç yolu vardır. Bu yollar aşağıda sıralanmıştır.

- Grafik kullanma yoluyla yapılabilir.
- Metin yapısının değiştirilmesiyle yapılabilir.
- Gizlenecek veriyi saklamak amacı ile yeni bir metin oluşturulması yapılabilir.

Dilbilim steganografisinde, açık kod ve şemagram olmak üzere iki yöntem bulunmaktadır. Açık kodda, şifrelenmek istenilen mesaj açıkça görülebilir ama bu mesaj zararsız hale gelir. Açık kod işleminde maskeleme boş şifre ve grid metoduyla yapılmaktadır. Şemagram, gizlenecek olan mesajın görünen metnin içinde saklanılmasıdır. Gizlenecek mesajın şemagram metodu ile gizlenmesi için grafiksel değişiklikler yapılmalıdır. Yapılması gereken bu değişiklikler için kullanılan bu yöntemler daktilo yazılarını kullanmak, farklı tipte yazı türleri kullanmak, resim içinde boşluk kullanmaktır (Aydoğan, 2014).

3.2.2 Teknik steganografi

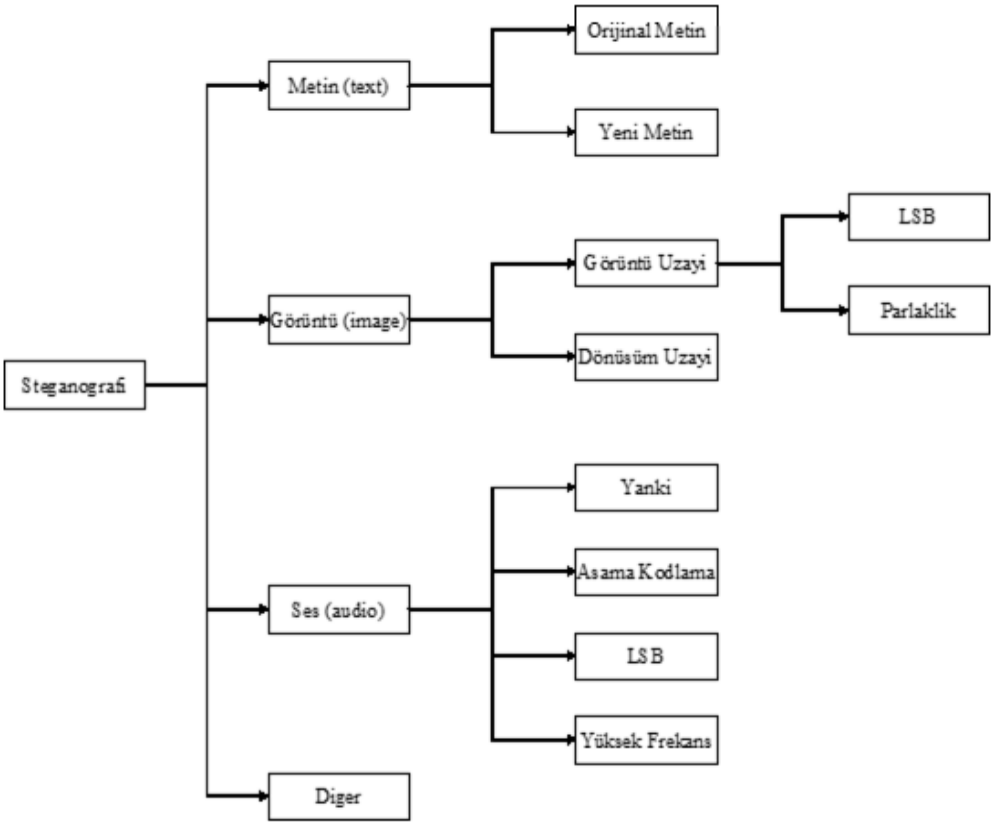
Teknik steganografi; görünmez mürekkep, gizli yerler, microdot ve bilgisayar tabanlı yöntemler olmak üzere birçok konuyu içermektedir. Görünmez mürekkep, geleneksel hale gelmiş görünmez mürekkep ile yazılan yazılar yöntemidir. Gizli yerler, gizlenecek olan mesajın çanta veya dolap gibi eşyaların içine saklanmasıdır. Microdot, bilgiyi noktalar halinde sayfaya gizleme işlemidir. Bilgisayar tabanlı yöntemler ise ses, resim, text resim dosyalarını kullanarak veri gizleme yöntemleridir (Badem ve Güneş, 2011).

3.3. Steganografinin Uygulama Alanları

Ortamlara göre steganografinin farklı kullanımları bulunmaktadır. Bunlar aşağıdaki gibi verilebilir.

- Ses üzerinde steganografi
- Video üzerinde steganografi
- Network steganografi
- Metin steganografi
- Resim üzerinde steganografi

Steganografi biliminde sıkça kullanılan yöntemlerin sınıflandırılması Şekil 3.2'de gösterilmektedir.

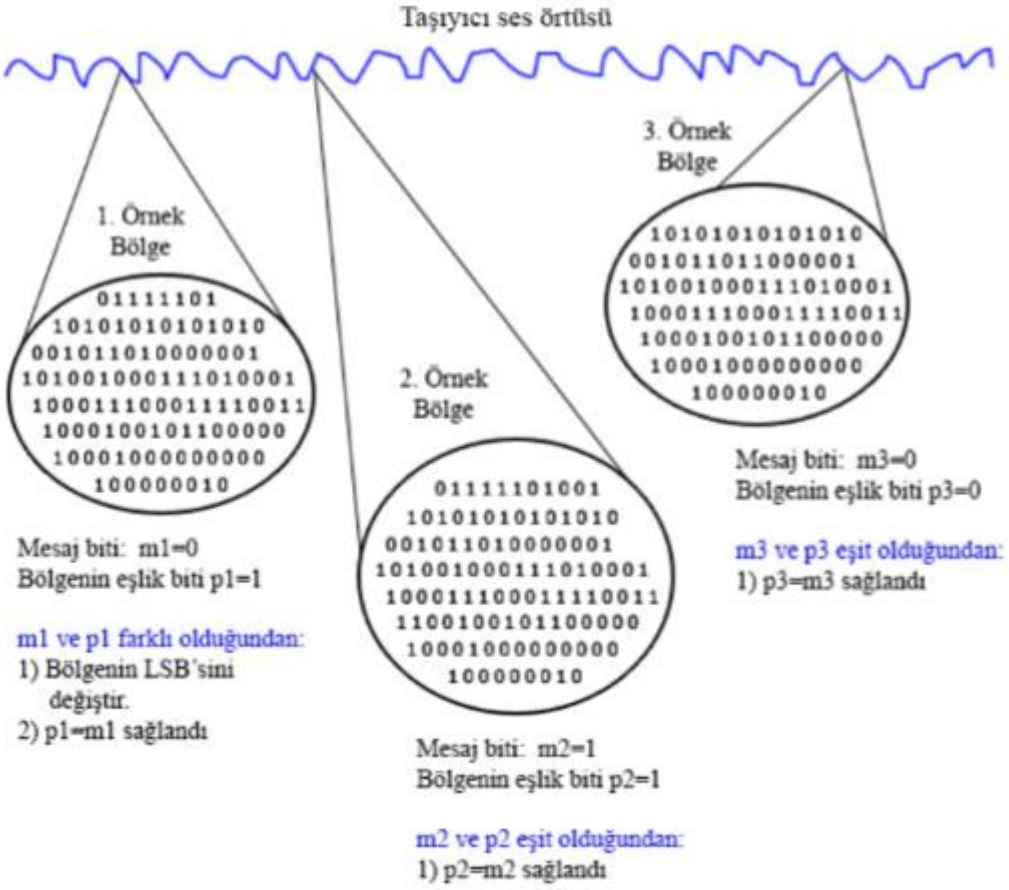


Şekil 3.2. Steganografi veri gizleme yöntemleri (Yiğit, 2018)

3.3.1. Ses üzerinde steganografi

Ses steganografisi ses sinyallerine veri gizlenmesi işlemidir. Ses sinyalleri resim sinyallerine benzer bir görünümde olduğundan dolayı ses steganografisinde kullanılan metotlar resim steganografisinde kullanılan yöntemlerle benzerlikler içerir (Karadoğan, 2016). Ses steganografisinde LSB, faz kodlama, eşlik kodlama, yaygın spektrum ve yankı saklama yöntemleri uygulanır (Demirci, 2016).

Eşlik kodlama; ses sinyalini ayrık örneklere pay edip, iletinin her bitini eşlik bitine saklar. Eşlik, diğer adıyla parite, örnek bir veri dizisindeki 1 bitlerinin sayısıdır. Dizideki 1 bitlerinin toplamı tek ise dizinin eşliği tek, toplamı çift ise eşliği çifttir. Şekil 3.3'te gösterilen bölgelerin eşlik bitleri, seçilen bölgelerdeki 1 bitlerin toplamı çift ise 0, toplamı tek ise 1 olarak alınmıştır (Tekeli, 2017).

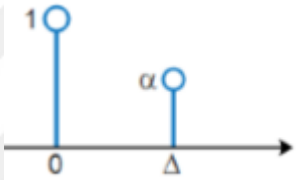


Şekil 3.3. Eşlik kodlama ile veri gizleme işlemi (Tekeli, 2017)

Faz kodlama; başlangıçtaki ses segmentinin fazını saklı bilgiyi gösteren referans fazla yer değiştirir. Ses örtüsü parçalara ayrılıp, ayrık Fourier dönüşümü yardımı ile bölünen ses örtülerinin faz açıları hesaplanarak gizleme işlemi ilk bölütün faz açıları üzerinde yapılmaktadır (Tekeli, 2017).

Yaygın spektrum; LSB yöntemine yakın bir şekilde saklı bilgiyi ses frekans spektrumu boyunca yayar (Tekeli, 2017).

Yankı saklama; gizli mesajı ses dosyasınn içerisine ayrık sinyal olacak biçimde yankı formunda gizlenir. Tekli yankı veri saklamada kullanılan yankı çekirdeğinin görseli Şekil 3.4'te gösterilmektedir (Tekeli, 2017).



Şekil 3.4. Tekli yankı gizlemede kullanılan yankı çekirdeği (Tekeli, 2017)

Resim steganografisinde olduğu gibi, ses dosyasına kaydedilen veri insan kulağıyla fark edilememektedir.

3.3.2. Video üzerinde steganografi

Video steganografi, mesajın akış esnasındaki videonun sinyallerine gizlenmesi ile oluşmaktadır. Video dosyası resim dizisinden oluşmaktadır. Bundan dolayı da resimde kullanılan steganografik metotlar bir miktar değişiklik yapılarak uygulanmaktadır (Karadoğan, 2016).

Videoda steganografi sesteki steganografi mantığına benzemektedir. Buradaki mantık en önemsiz bite gizleme işlemidir. Bu alanda 1999 yılında Chale ve Manjunath çalışmalar yapmıştır (Demirci, 2016).

3.3.3. Network steganografi

Network steganografi, iletişimde akış bozulmadan bilgisayar ağlarında gizli mesajın iletilmesi olarak tanımlanmaktadır. Örtü nesnesinde TCP, UDP, ICMP, IP gibi protokollerin gizli mesajı taşıyıcı olarak kullanması ile ağ steganografisi yapılmaktadır. OSI modelinde örtü olarak kullanılan kanallar bulunmaktadır (Demirci, 2016).

Ağ steganografisinde gönderilen paketlerin başlık yapılarından, sıralandırılmalarından, dolgularından, sınıflandırılmalarından, uzunluklarından yararlanılarak network ortamında gizli mesaj gönderilebilir (Karadoğan, 2016).

3.3.4. Metin steganografi

Metin steganografisi, metin dosyalarında metin tiplerinin içine veri gizlenmesi işlemidir. Bu yöntem resim, ses ve video steganografisine göre daha zor bir işlemdir. Bu yöntemde gizlenecek verinin kapasitesinin daha az olduğu görülmektedir. Bu kapasitenin az olması dezavantaj olmasına rağmen metinler her yerde bulunduğundan dikkate değer veri gizleme işlemleri yapılabilir.

Metin steganografisinde birçok yaklaşım bulunmaktadır. Bunlar; sözdizimsel değişiklik, metin kısaltma, anlamsal değişiklik, satır kaydırma yaklaşımlardır. Bu yaklaşımlar, metin biçimini değiştirme ve metnin anlamını değiştirme şeklinde iki grup altında toplanabilir (Karadoğan, 2016).

3.3.5. Resim üzerinde steganografi

Steganografi dünyasında en çok resim üzerinde veri gizleme işlemleri yapılmaktadır. Bunun nedeni ise veri gizlendikten sonra resim üzerinde değişikliklerin insan gözüyle fark edilmemesi ve resim dosyasında gizlenecek veri miktarının da fazla olmasıdır (Karadoğan, 2016).

Resimde bulunan RGB değerlerinin çok az farkla değiştirilmesi, sayısal ifadeyle o noktanın renk kodunun en düşük değerli bitlerinin değiştirilmesi ile mesaj gizlenmektedir.

Aşağıda yer alan Şekil 3.3'te sol taraftaki resim orijinal hali olup, bu resime mesaj şifrelendikten sonra oluşan görüntünün son hali ise sağ taraftaki görüntüdür. Her iki resim arasında insan gözüyle fark edebilecek farklılık bulunmamaktadır.

Orijinal Resim *Veri Gizlenmiş Resim*

Şekil 3.5. Orijinal bir resim ve aynı resmin veri gizlenmiş hali

3.4. Steganografi Alanında Yapılan Çalışmalar

2000'li yıllardan itibaren, LSB ve Bit Plane Complexity Segmantation (BPCS) yöntemiyle, dönüştürme ve permütasyon teknikleri ile resim içerisine veri gizleme çalışmaları gerçekleştirilmiştir (Bilgin, 2013).

Koçak (2015) Erciyes Üniversitesinde yayınlandığı makalesinde kriptoloji ve steganografi üzerine bir çalışma yapmıştır. Yapılan bu çalışmada 2 bit LSB yöntemi kullanılmıştır. Bu çalışmada RGB değerlerinden R ve G değerleri

kullanılmıştır. Yöntemde 4 bit değiştirilerek veri gizleme işlemi yapılmıştır (Koçak, 2015).

Yıldız, Özcerit (2015) steganografi üzerine yaptıkları çalışmada 24 bit renkli hareketli videoların RGB değerlerinde cebirsel işlemler uygulandıktan sonra, yeni oluşan değerleri Red Green Blue değerlerine kaydetmektedir. Çalışmada gizlenen veri uzunluğu arttıkça piksel sayısında bozulmaların da arttığı görülmüştür. Fakat bu artış diğer veri gizleme algoritmalarına göre çok küçüktür (Yıldız ve Özcerit, 2015).

3.5. Steganografi Yöntemleri

Steganografide mesajı görüntünün içine saklamak için çeşitli yöntemler mevcuttur. Bu yöntemler aşağıdaki gibidir.

1. Patchwork Algoritması
2. Amplitude (Genlik) Modülasyonu Kullanılarak Bilgi Gizleme
3. Toplamsallık Algoritması
4. SSIS (Spread Spectrum Image Steganography) Yöntemi
5. Frekans Alanına Veri Saklanması
6. Son Bite Saklama Yöntemi

3.5.1. Patchwork algoritması

Bu algoritma Bender tarafından geliştirilmiştir. Patchwork Algoritması halen kullanılan bir yöntemdir. Bu algoritma, mesajı Gauss dağılımı gösteren bir istitatistiğe sahip örtü verisinin içine gizlemeyi hedefleyen tahminleme yöntemidir. Bu algoritma filigran uygulamalarda sıkça kullanılmaktadır (Belenli, 2015).

3.5.2. Amplitude (Genlik) modülasyonu kullanılarak bilgi gizleme

Bu yöntem işaret bitleri ile mavi kanaldaki pikselin sayısal değerleri yer değiştirilerek oluşan yeni değerlerin resim içerisine gizlenmesidir. Bu yer değişimleri ışığın oranına ve bit değerine bağlıdır. Işığın oranına ve bit değerine bağlı olarak renk tonunun arttırılması veya azaltılması yoluyla yapılmaktadır (Belenli, 2015).

3.5.3. Toplamsallık algoritması

Bu algoritmayı 1996 tarihinde Pitas ve Nikolaidis yaptığı çalışmalarda bulmuştur. Toplamsallık algoritması filigran uygulamalarında kullanılmaktadır. NxM çözünürlük içeren görüntü eşitlik Formül 3.1'de verilmektedir (Yıldırım, 2014).

$$\boldsymbol{I = \{X_{mn}, n \in \{0, \dots, N-1\}, m \in \{0, \dots, M-1\}\}} \quad (3.1)$$

Bu ifade Xmn, n ∈ {0, …, N-1}, (n, m) pikselinin koyuluk seviyesini göstermektedir. Gizlenecek Bitler, 1 ya da 0 değeri almaktadır. Formül 3.2'te verilmektedir.

$$\boldsymbol{S = S_{mn}, n \in \{0, \dots, N-1\}, m \in \{0, \dots, M-1\}, S_{mn} \in \{0, 1\}}$$
(3.2)

Bu işlemden sonra I, S kullanılarak iki eş alt kümeye bölünmektedir. Formül 3.3'te verilmektedir.

$$\mathbf{A = X_{mn} \in I, S_{mn} = 1}$$
$$\mathbf{B = X_{mn} \in I, S_{mn} = 0} \quad (3.3)$$
$$\boldsymbol{|A| = |B| = \frac{|I|}{2} = \frac{|NxM|}{2} = P}$$
$$\boldsymbol{I = A \cup B}$$

Filigran' ın görüntü üzerine eklenmesi C = {Xmn ⊗ k, Xmn ∈ A} işlem ile ilave edilmektedir. Bu ifade deki ⊗ işlem Toplamsallık kuralıdır. Filigranlanmış resim formülü Formül 3.4'teki gibidir (Yıldırım, 2014).

$$\mathbf{I_s = C \cup B} \tag{3.4}$$

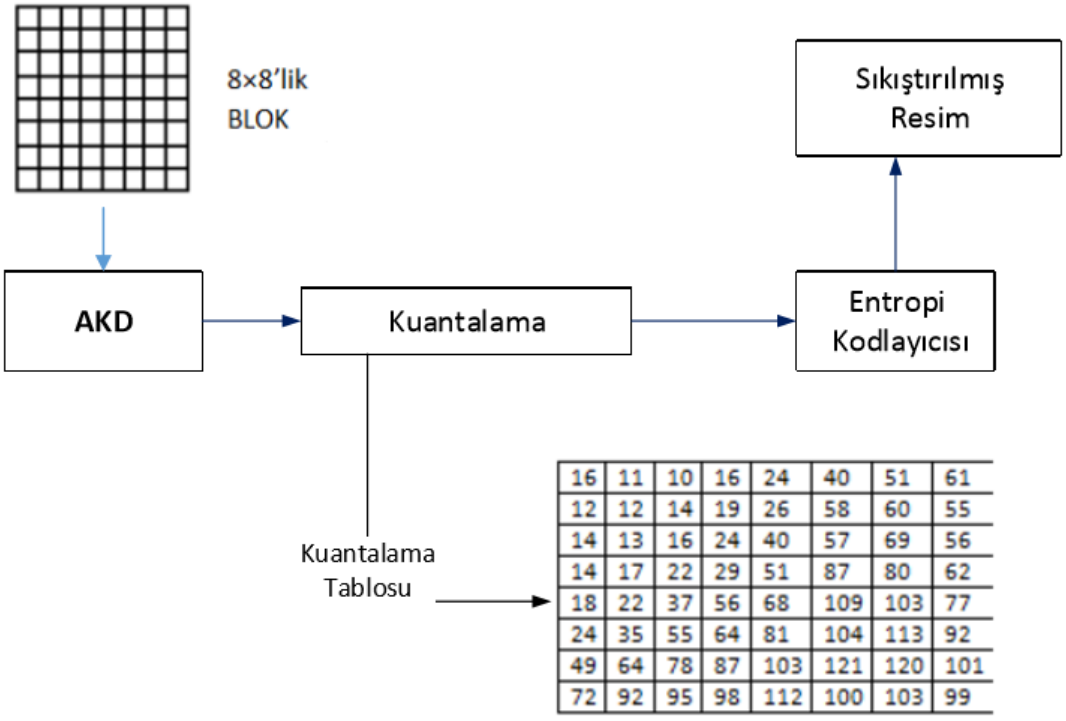
3.5.4. Ssis (Spread spectrum image steganography) yöntemi

Spread-Spectrum şifreleme tekniği, mesajı (dar-bantlı bir sinyali) daha geniş bantlı sinyal içerisine gizlemek için kullanılmaktadır. Bu şifreleme tekniği gürültü kaynağından elde edilen gürültüyü ses sinyaline eklemektedir. Literatürde bu teknik Bender ve arkadaşlarının 1996 yılındaki çalışması ile hız kazanmıştır (Yıldırım, 2014).

3.5.5. Frekans alanına veri saklanması

Bu yöntem filigran teknolojileri için görüntünün dönüştürülmesi temeline dayanmaktadır. Görüntünün dönüştürülebilmesi için ayrık cosinus dönüşümü (DCT) kullanılmaktadır. Bunun dışında kullanılan algoritmalar Ayrık Fourier Dönüşümü (DFT), Waish dönüşümü ve Wavelet dönüşümüdür (Yıldırım, 2014).

Ayrık kosinüs dönüşümü steganografisi en çok JPEG dosyalarında kullanılmaktadır. JPEG dosyasında kosinüs dönüşümü uygulandıktan sonra kuantalama ve yuvarlama yapıldıktan sonraki sonuç üzerinde LSB yöntemi uygulanır. JPEG sıkıştırma algoritma şeması Şekil 3.4'te gösterilmektedir. Bir değer üzerinde yapılan değişiklik tüm bloğu etkileyeceğinden, bilginin hangi değerlere saklanacağı önemlidir.



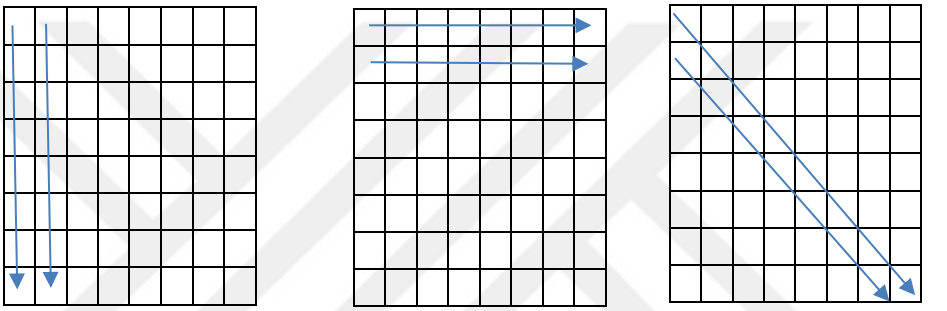
Şekil 3.6. Jpeg sıkıştırma algoritma şeması (Yıldırım, 2014)

3.5.6. En önemsiz bite ekleme (Lsb)

En önemsiz bite ekleme yöntemi (LSB) günümüzde yaygın olarak kullanılmaktadır ve uygulanması basit bir yöntemdir. Fakat yöntem dikkatsizce uygulandığında veri kayıpları ortaya çıkabilmektedir. Gizlenecek olan mesajın bitleri örtü imgenin piksellerin en önemsiz bitleri ile yer değiştirilir. Mesajın bitleri resmin sütun veya satır olmak üzere istenilen biçiminde gizlenilebilir. Bu yöntemde resmin piksellerine birçok teknik uygulanabilmektedir. Bu tekniklere ayrık logaritma fonksiyonu ve Laplacian kenar bulma algoritması örnek olarak verilebilir (Olcay ve Saran, 2013).

Sayısal değeri düşük olan bit üzerinde yapılan değişim, resim üzerindeki etkisi göz ile fark edilemeyecektir. LSB yöntemi ile, genellikle yüksek kalitedeki resim dosyalarında, yüksek miktarda veri gizleme işlemi yapılmaktadır. Fakat LSB yönteminin uygulanmasının yaygınlığı ve bilinmesinden dolayı bu yöntem saldırılara karşı dayanıksızdır (Tuncer ve Avcı, 2017).

Görüntü içerisine veri sütun, satır veya köşegene sıralı olarak görüntünün piksellerine gizlenebilmektedir (Güvenoğlu, 2016). Bu yöntemler Şekil 3.4'te görülmektedir. Şeklin b şıkkında satıra veri gizleme işlemi ilk satırdan itibaren soldan sağa doğru ilerlemektedir. Şeklin a şıkkında sütuna veri gizleme işlemi de benzer biçimde ilk sütündan itibaren yukarıdan aşağıya doğru ilerlemektedir. Şeklin c şıkkında ise, köşegen uygulamasında veri gizleme işlemi görülmektedir. Bu projedeki LSB yönteminin veri gizleme işlemi satır sıralı olarak soldan sağa doğru olacak Şekil 3.4'te uygulanmıştır.



(a) Sütun yöntemi (b) Satır yöntemi (c) Köşegen yöntemi

Şekil 3.7. Lsb yönteminin resim üzerinde piksellere uygulanma yöntemleri

24-bit renkli resimde en önemsiz bite ekleme yönteminin uygulanması basittir. Resimdeki her piksel 3 bayt ile temsil edilmektedir. Bu durum, bir pikselin rengini belirleyen R(Kırmızı), G(Yeşil), B(Mavi) değerlerinden oluşmaktadır. Bu durumda her baytın son bitini değiştirmek amacıyla bir pikselde 3 bitlik mesaj saklanabilmektedir. Gizlenmek istenen mesaj, saklama işleminden önce sıkıştırılırsa, çok daha fazla sayıda bilgi resmin içine gizlenebilir. Örneğin, bir resmin orijinal halinin 3 pikseline ait RGB değerleri aşağıdaki gibidir.

1. piksel : 10010101 00001101 11001001 (149,13,201)
2. piksel : 10010110 00001111 11001010 (150,15,202)
3. piksel : 10011111 00010000 11001011 (159,16,234)

Yukarıda resime ait 3 piksele ait RGB değerlerinin içine 'a' karakterini gizleyeceğimizi düşünelim. 'a' karakterinin ASCII kodu karşılığı olan 97

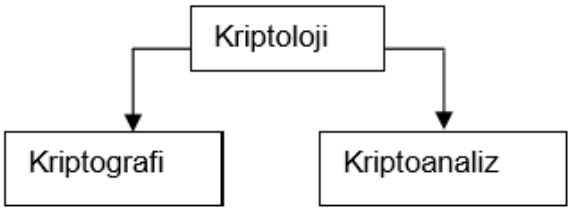
değerinin bit karşılığı dizisi “01100001’ olacaktır. Bu 8 bit toplamda 8 bayt veri üzerine gizlendiğinde oluşan yeni piksel değerleri aşağıdaki yer almaktadır. Buradaki örnekte orijinal değerlerden sadece 4 bitte değişiklik olmuştur.

1. piksel : 1001010**0** 00001101 11001001 (149,12,201)
2. piksel : 10010110 0000111**0** 11001010 (151,14,203)
3. piksel : 1001111**0** 0001000**1** 11001011 (159,16,234)

Resmin RGB değerlerine mesaj gizleme işleminden sonra oluşan yeni RGB değerleri çok ufak değişimlere uğradığından, bu değişiklik göz ile fark edilemeyecek düzeydedir. LSB yönteminin çıkış noktası, en az değerlikli bite uygulanmak üzere olsa da en az ağırlıklı farklı sayıda bite uygulanacak çeşitli yöntemler de önerilmiştir (Doğan ve Daş, 2016).

4. KRİPTOLOJİ

Kriptoloji mesajın şifrelenmesi bilimine denilmektedir. Kriptoloji Şekil 4.1'de görüldüğü gibi "kriptografi" ve "kriptoanaliz" olmak üzere iki alt bilim dalından oluşmaktadır.



Şekil 4.1 Kriptoloji bilimi alt bilim dalları

Kriptoloji biliminin alt bilim dalından olan kriptografi, açık olan bilgiyi anlaşılmaz hale getirmek için kullanılan şifreleme bilimidir. Kriptoanaliz ise şifrelenmiş metnin analiz süreçleri üzerinde duran ve açık metni elde etmek için kullanılan metot ve yöntemleri içeren kriptolojinin alt bilim dalıdır.

Kriptoloji biliminde şifreleme algoritmalarında bulunan temel özellikler aşağıdaki gibidir (Çoşkun ve Ülker, 2013).

- Gizlilik: Mesaj sadece istenen kişi veya kişiler tarafından anlaşılmalıdır.
- Bütünlük: Şifrelemeyi yapan kişi veya kişiler dışında kimse mesajı değiştirememelidir.
- Reddedilememezlik: Mesajı şifreleyen kişinin daha sonrasında bunu inkâr edememesidir.
- Erişilebilirlik: Yetkili kişi veya kişilerin ihtiyaç duyduğu anda gerekli bilgiye erişmesidir.
- Kimlik denetimi: Mesajı gönderen ve mesajı alan tarafların birbirlerinin kimliklerini doğrulamasıdır.

4.1. Kriptografi

4.1.1. Kriptografi tanımı

Kriptografi matematiksel yöntemler kullanılarak mesajın gizlenmesidir. Şifreleme işlemi, mesajı belirli kişilerden saklama amacını taşır. Mesajın şifrelenmesi ile mesaj istenmeyen kişilerin eline geçse bile anlaşılamaması için mesajın şifrelenmesi amaçlanmaktadır. Şifrelenen mesaj doğru kişi tarafından çözme algoritması ile kolaylıkla çözülür (Akleylek ve Yıldırım, 2011).

4.1.2. Kriptografi tarihçesi

Kriptoloji, geçmiş zamanlarda askeri ve diplomatik haberleşme alanında bilgi güvenliğini sağlamak için kullanılmıştır. Şimdilerde ise bilgisayar sistemleri ve cep telefonları gibi alanlarda kullanılmaktadır (Yaşar ve Ceylan, 2014).

Bilinen en ilkel şifreleme algoritması şifreleme metodunun sadece alıcı ve gönderen kişi arasında bilindiği algoritmalardır. Bu algoritma ile mesaj çözümlenmesi yapılır. Roma İmparatorluğu'nda Sezar, askerlerine gönderdiği gizli mesajlarda, her bir karakteri belirli miktar kaydırma işlemi yaparak göndermektedir (Yeşilbaş, 2016).

M.Ö. 480 yılında Yunanlılar ve Persler arasında geçen savaşta steganografi tekniği kullanılmıştır. İran'da bulunan bir Yunanlı, kölesinin saçını kazıtarak Yunanlılara karşı düzenlenmesi planlanan Pers istilasını onun kafa derisine dövme ile yazmıştır. Saçları uzadıktan sonra kölesini Atina'ya göndermiştir. Köle, İran'a yakalanmadan Atina'ya gitmiş ve saçını kazıtıp mesajı iletmiştir.

4.1.3. Kriptolojinin önemi

Günümüzde bilgi giderek daha önemli bir hale gelmiştir. İletişim alanındaki gelişmeler bilgiyi saklama ve iletme açısından işleri zorlaştırmakta ve yeni metotları geliştirmeye sevk etmektedir. Uydu ve internet üzerinden yapılan

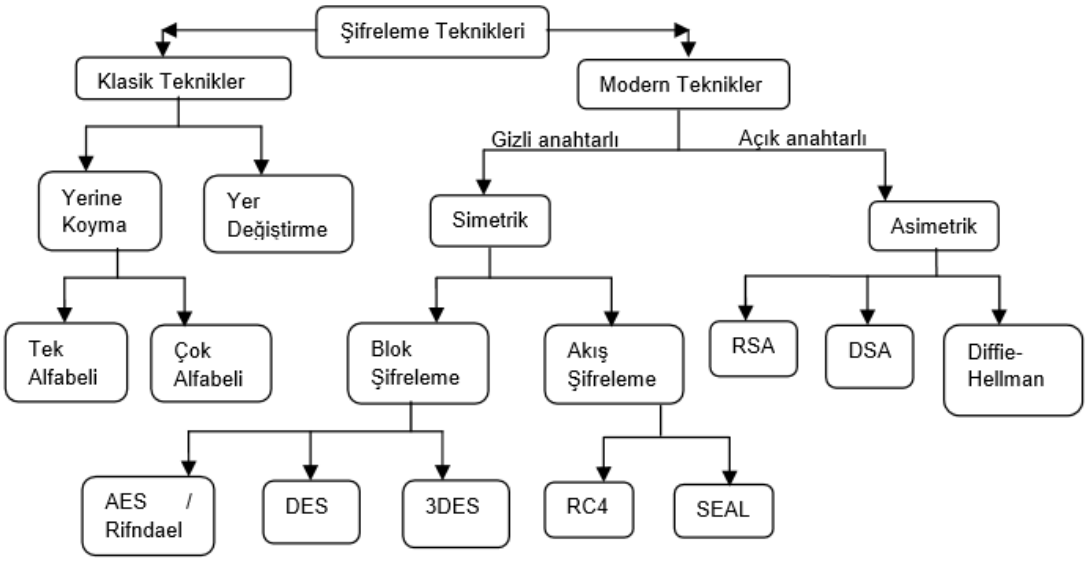
iletişim ve haberleşmenin dinlenme olasılığı bulunmaktadır. Gizliliği önemli olan belgelerin elektronik ortamda taşınması ve gönderilmesi kriptografinin önemini artırmaktadır. İnternetin yaygınlaşması ile teknolojik kullanımın oldukça geniş bir kitleye hitap etmesi sağlanmıştır. Bu durum bilgi güvenliği açısından büyük tehdit oluşturmaktadır.

Kriptografi günümüzde bankamatikler, e-posta iletileri, telefon bankacılığı gibi birçok alanda kullanılmaktadır.

Günlük hayatta işlemlerimizi kendimiz yaparken duyduğumuz güven duygusu sanal ortamda kriptoloji bilimi ile sağlanabilir. Kişiler sahtekarlık ve aldatılma kaygısı taşımadan elektronik ortamda tüm işlemlerini yapmaktadır. Günlük hayatımızın her alanına giren kriptolojinin en önemli noktası ulusal bilgi güvenliğini sağlaması, siber saldırılarda bilgi hırsızlığı girişimlerini karşılıksız çıkarmasıdır.

4.1.4. Kriptografi algoritmalarının sınıflandırılması

Teknolojinin gelişmesi ile şifreleme yöntemleri de gelişmiştir. Kriptografi algoritmaları klasik ve modern diye iki ana başlığa ayrılmaktadır. Şifreleme algoritmasının sınıflandırılmalarını Şekil 4.2'de gösterilmektedir.



Şekil 4.2. Şifreleme algoritmalarının sınıflandırılması

4.1.4.1. Klasik teknikler

Bu şifreleme tekniği, klasik şifreleme yöntemi olan kâğıt-kalem kullanılarak yapılan şifreleme algoritmalarıdır. 2. Dünya Savaşı zamanında Enigma tekniği kullanılmıştır (Ülker, 2014).

Klasik kriptografi askeri işlemlerde ve akademik yerlerde kullanılmıştır. Klasik teknikler, algoritması gizli şifreleme teknikleri içermektedir. Klasik tekniğe Sezar ve Enigma sistemleri örnek verilebilir.

Sezar Şifreleme; Alfabede bulunan harflerin sıra numaraları belirli bir algoritma ile kaydırılarak şifreli karşılıkları elde edilir. Tek alfabeli şifreleme tekniği veya öteleme şifrelemesi olarak da geçmektedir. Örnek olarak harflerin ötelenme miktarı 3 olursa Sezar Şifreleme Yöntemi olarak geçmektedir. Matematiksel ifadesi Formül 4.1 bağıntısı ile ifade edilmektedir (Yeşilbaş, 2016).

$$Ek(m) = (m + k) \bmod 26 \qquad (4.1)$$

m= açık metindeki sıradaki harfin sıra numarası
k= harflerin ötelenme miktarı

mod 26'daki 26 değeri ingiliz alfabesindeki toplam karakter sayısını (bu karakter sayısı ülkenin alfabesindeki karakter sayısına göre değişebilmektedir) ifade etmektedir.

Enigma; 2. Dünya Savaşı'nda Almanlar tarafından kullanılmıştır. Düz metinleri mekanik ortamda şifreleyen makine geliştirilmiştir. Enigma'da 26 harften oluşan klavye bulunmaktadır. Tuş yatağının arkasına tuşları aydınlatıcı lambalar vardır. Şifreleme işlemini 3 adet şifreleme çarkı ve hareketsiz olan 1 adet çark yapmaktadır. Hareketsiz olan çark yansıtıcı olarak adlandırılır. Hareketli çarklarda ise ters düz eden bir mil kullanılır.

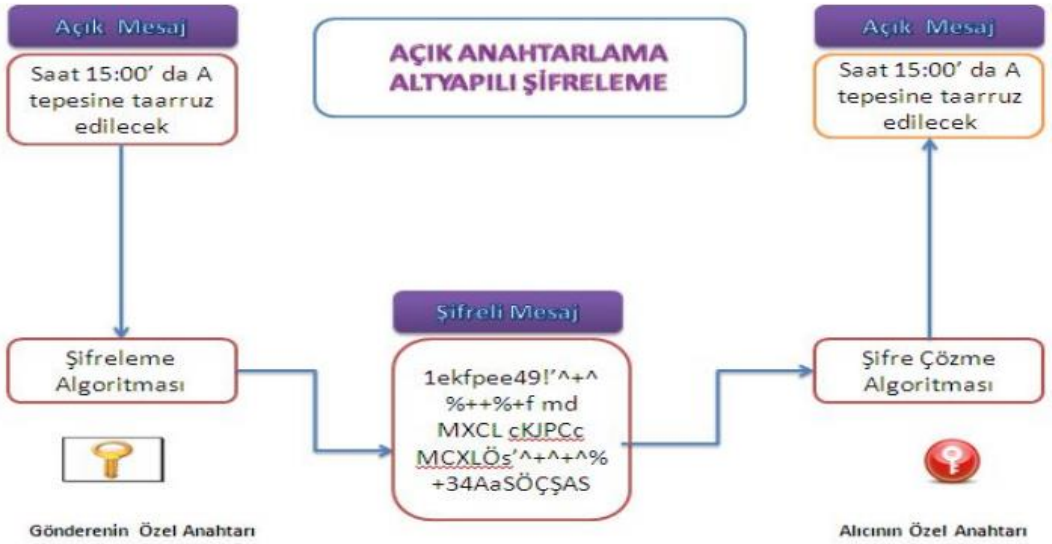
4.1.4.2. Modern teknikler

Teknolojinin gelişmesi ile şifreleme sistemleri bilgisayar programları ile gerçekleştirilmeye başlanmıştır. Harfler bilgisayar ortamında bitlerden oluştuğundan şifreleme işlemleri de bitler ile yapılmaktadır. Modern teknikler simetrik algoritmalar, asimetrik algoritmalar ve hash algoritmalar olmak üzere üç gruba ayrılmaktadır (Ülker, 2014).

Simetrik Algoritmalar: Simetrik algoritmalarda tek bir anahtar kullanılır. Bu anahtarla hem şifreleme işlemi hemde şifreyi çözme işlemi yapılır. Simetrik şifreleme ve deşifreleme algoritması çözüm işlerimlerini Şekil 4.3'te gösterilmektedir. Bundan dolayı şifreleme işleminde kullanılan anahtar gizlidir. Anahtar bilgisi gönderici ve alıcıda bulunmalıdır. Anahtarı elde eden kişi şifreyi çözebilmektedir (Yayık, 2013). Simetrik şifreleme algoritmasına XOR, DES, 3DES, IDEA gibi algoritmalar örnektir.

Şekil 4.3. Gizli anahtarlama altyapısı

Asimetrik Algoritma: Asimetrik algoritma tekniğinde iki farklı anahtar vardır. İlk anahtar şifreleme aşamasında kullanılır ve herkes görebilir. İkinci anahtar şifre çözme aşamasında kullanılır. Bu anahtar metni çözmesi gereken kişiye özeldir. Asimetrik şifreleme algoritmasına RSA, DSA gibi algoritmalar örnektir. Asimetrik şifreleme simetrik şifrelemeye göre oldukça zordur. Açık anahtarlamanın uygulanması Şekil 4.4'te gösterilmektedir (Yayık, 2013).



Şekil 4.4. Açık anahtarlama altyapısı

Hash Algoritması: Hash algoritması özetleme işlemi yapmaktadır. Mesajdan sabit uzunlukta dizi üretilir. Üretilen bu diziye mesajın özeti denir. Üretilen bu özet metnin karakterini taşır. Şifrelenecek metindeki tek bir karakter değişikliği üretilecek özette büyük değişimlere yol açar. Bu algoritmalarda özetleme tek yönlü olduğundan özetten asıl metine dönüş yapılamamaktadır. Hash şifreleme algoritmasına MD4, MD5, SHA-1 gibi algoritmalar örnektir.

4.1.5. Kriptoanaliz tekniklerinin sınıflandırılması

Kriptolu metin üzerinde düz metine ulaşmak için yapılan çalışmalar kriptoanaliz atağı olarak değerlendirilmektedir. Bu saldırı tekniklerinden bazıları aşağıdaki gibidir.

4.1.5.1. Sadece şifreli metin saldırısı

Saldırı yapan kişi mesajın içeriğini bilmemektedir. Sadece şifreli metini kullanarak mesajı elde etmeye çalışır. Uygulamada düz metine dair tahminler yapar. Klasik saldırılarda bu yöntem kullanılmaktadır (Ülker, 2014).

4.1.5.2. Bilinen düz metin saldırısı

Şifreli metini çözmek isteyen kişi, düz metnin bazı kısımlarına ya da tamamına karşılık gelen şifreli metine sahiptir. Elindeki bilgi ile şifreli metinleri çözebilmektedir. Bu yöntemde en çok kullanılan saldırı blok şifrelemeye karşı lineer kriptoanaliz tekniğidir (Ülker, 2014).

4.1.5.3. Seçilmiş düz metin saldırısı

Seçilmiş düz metin saldırısındaki amaç şifreleme için kullanılan anahtarı bilmektir. 3. kişinin şifreleme algoritmasını bildiği düşünülürse, yapılabilecek muhtemel saldırıdan biri kaba kuvvet saldırısıdır. Kaba kuvvet saldırısında tüm anahtarların denemesi yapılır (Ülker, 2014).

4.1.5.4. Seçilen şifreli metin saldırısı

Şecilen şifreli metin saldırısında kriptoanalist, şifreli metin seçip şifreli metinle örtüşen düz metini bulmaya çalışır. Bu teknik deşifreleme için kullanılan özel bir cihazla şifreleme anahtarı olmadan da yapılabilmektedir (Ülker, 2014).

4.1.5.5. Uyarlanır seçili düz metin / şifreli metin saldırısı

Seçilen düz metin ya da seçilen şifreli metin saldırısıyla benzerdir. Bunlar arasındaki fark, uyarlanabilir seçili düz metin veya şifreli metin saldırısındaki metnin rastgele seçilmemesidir. Ancak daha önceki şifre çözme işlemlerinde elde edilen bilgiler üzerinden seçilmesidir.

4.1.5.6. İlişkili anahtar atağı

Farklı anahtarlar ile şifrelenmiş açık metinlerin sonuçlarını değerlendirebilmeye bağlı saldırı tekniğidir (Ülker, 2014).

4.2. Kriptoanaliz

Kriptoanalizin amacı kriptografik bir plandaki bazı zayıflıkları bulmaktır. Kriptoanaliz; belirli bir sistemi yıkmaya çalışan saldırgan tarafından, sistemin savunmasızlıklarının olup olmadığını değerlendiren sistem tasarımcısı tarafından üstlenebilir. Her şifreleme yöntemi kırılamamaktadır (Tuncal, 2008).

5. LEAST SİGNİFİCANT BİT (LSB) ALGORİTMASININ GELİŞTİRİLMESİ VE UYGULAMASI

5.1. Cebirsel Şifreleme Tanımı

Bu çalışmada stenografi bilim dalının en az ağırlıklı bit şifreleme tekniği olarak bilinen LSB algoritmasının veri güvenliğini cebirsel ifadeler ile iyileştirmek, belli oranda daha fazla sıkıştırma sağlarken, resim üzerinde oluşan değişim hata oranını da çok arttırmamak amaçlanmıştır. Geliştirilen bu yöntemde, mesajın 1 karakteri 24 bit renkli görüntünün 2 pikselinin R(Red), G(Green), B(Blue) değerlerine gizlenmiştir. Mesaj, resim içerisinde soldan sağa olacak şekilde satır olarak, yukarıdan aşağıya dikey olacak şekilde sütün veya diagonel şekilde gizlenebilmektedir. Bu çalışmada mesaj resim içerisine soldan sağa olacak şekilde satır olarak gizlenmiştir. Resmin toplam piksel sayısının yarısı kadar karakter mesaj içine şifrelenebilmektedir.

5.2. Cebirsel Şifreleme Yöntemi

Geliştirilen cebirsel şifreleme yöntemi, cebirsel matematik işlemlerinden sonra elde edilen toplam değerlerin 24 bit renkli resmin piksellerine dağıtılmaktadır. Geliştirilen bu yöntem cebirsel işlemler olmasından dolayı LSB yönteminden daha güvenlidir.

Önerilen cebirsel şifreleme yönteminin algoritması aşağıdaki gibidir.

Öncelikle, mesajın her bir karakterinin ASCII kod değerinin basamak değerlerinin üç farklı toplamı elde edilir. Bu üç farklı toplam, sayısal değerlerin sırasıyla resmin piksellerindeki RGB renk değerlerine dağıtılmaktadır. Böylece piksel bazında tahmin edilebilirlik ortadan kalktığı için, cebirsel şifreleme yönteminin getirdiği güvenlik daha fazla olmaktadır. Bu cebirsel işlemler daha sonra ters aritmetik işlemler biçiminde kullanılarak, orijinal basamak değerlerinin kolayca tekrardan elde edilmesi mümkün olmaktadır.

Teori:

3 basamaklı bir sayının (karakterin ASCII değeri) yüzler basamağını x, onlar basamağını y ve birler basamağını z ile gösterelim. Bu durumda aşağıdaki gibi 3 cebirsel toplam yazılarak elde edilecek değerlerden;

xy = x+y (1. Toplam) yz = y+z (2. Toplam) xyz = x+y+z (3. Toplam)

Aşağıda yer alan 3 cebirsel fark işlem ile tekrar orjinal değerlere ulaşmak mümkündür.

x=xyz-yz z=xyz-xy y=xyz-(x+z)

Örnek 5.1.:

Basit bir "ab" mesajının, çalışmada önerilen yöntemle şifreleme ve çözme algoritmalarının nasıl uygulandığı aşağıda örneklenmiştir.

(a karakteri için)

097 ➔ xy=yüzler basamak değeri + onlar basamak değeri (0 + 9) = 09

yz=onlar basamak değeri + birler basamak değeri (9 + 7) =16

xyz=yüzler basamak değeri + onlar basamak değeri + birler basamak değeri (0 + 9 + 7) =16

(b karakteri için)

098 ➔ xy=yüzler basamak değeri + onlar basamak değeri (0 + 9) = 09

yz=onlar basamak değeri + birler basamak değeri (9 + 8) =17

xyz=yüzler basamak değeri + onlar basamak değeri + birler basamak değeri (0 + 9 + 8) =17

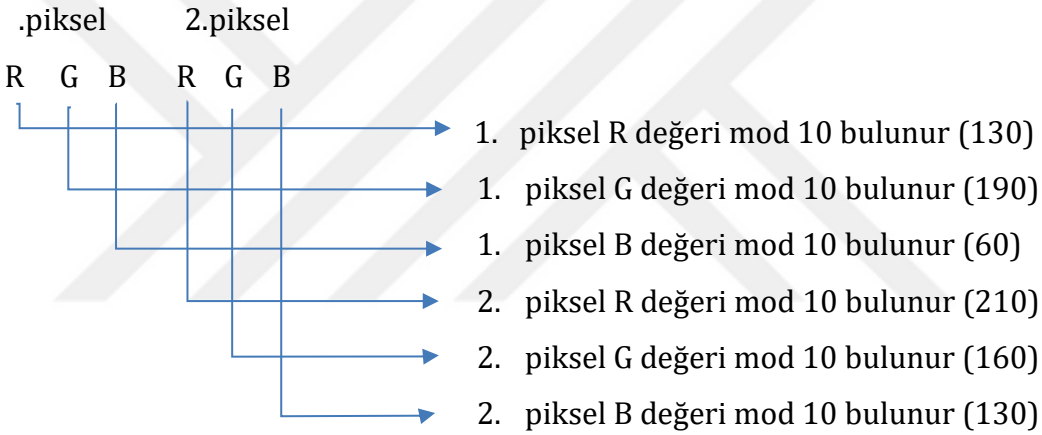
Elde edilen bu toplamlar, daha sonra ilgili resimde yer alan piksellerin RGB baytlarına aşağıdaki gibi kodlanmaktadır. Her renk değeri 0 ile 255 arasında bir yoğunluk değeriyle belirlendiğinden, yöntemde her renk değerine mod 10 uygulanır ve sıfırlanan birler basamak değerine şifrelenecek mesaja ait toplam

değerlerin rakamları (sıfır ile başlasa bile iki basamak olarak düşünülürek) sırasıyla yerleştirilir. İşlemin nasıl uygulandığı aşağıda örneklenmektedir.

Orijinal resime ait ilk satır ilk 4 piksel değerinin aşağıdaki gibi olduğunu varsayalım.

Çizelge 5.1. Orjinal resimdeki ilk 4 pikselin rgb değerleri

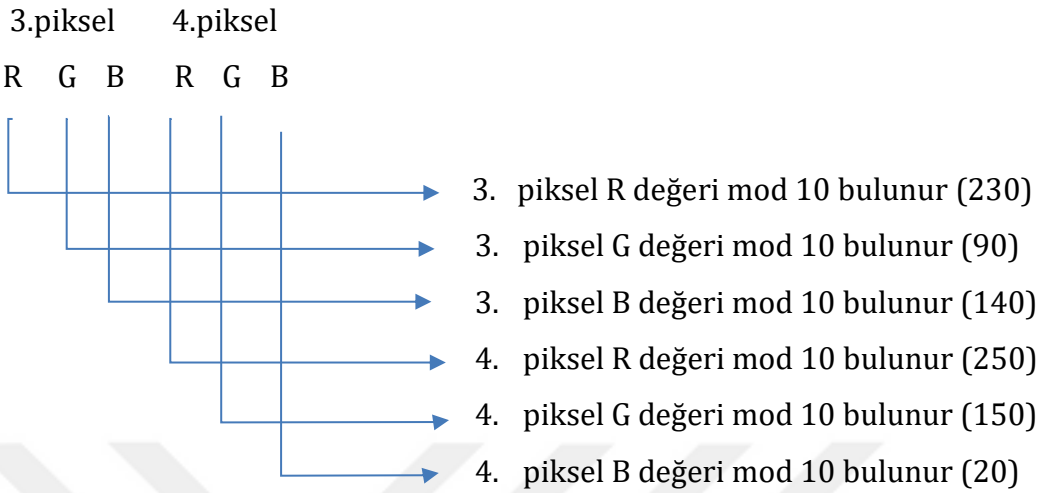
1. piksel			2. piksel			3. piksel			4. piksel			…….
R	G	B	R	G	B	R	G	B	R	G	B	…..
135	197	63	215	167	133	234	97	145	253	155	28	……



Daha sonra, gizlenecek mesajın ‘a’ karakteri cebirsel toplamlarının rakamları, resmin mod işlemine tabî tutulmuş renk sayısal değerlerine 1. pikselin R değerinden başlanarak, 2. Pikselin B değerine kadar sırasıyla aşağıdaki gibi eklenir (6 rakam).

130 + xy’nin onlar basamağı= 130 + 0 =130
190 + xy’nin birler basamağı= 190 + 9 =199
60 + yz’nin onlar basamağı= 60 + 1 =61
210 + yz’nin birler basamağı= 210 + 6 =216
160 + yz’nin onlar basamağı= 160 + 1 =161
130 + yz’nin birler basamağı= 130 + 6 =136

Benzer işlem gizlenecek mesajın ‘b’ karakteri için uygulanacak olursa aşağıdaki değerler elde edilecektir.



230 + xy’nin onlar basamağı= 230 + 0 =230

90 + xy’nin birler basamağı= 90 + 9 =99

140 + yz’nin onlar basamağı= 140 + 1 =141

250 + yz’nin birler basamağı= 250 + 7 =247 (>255, toplam sonucun onluk basamak değeri 1 eksiltilir → 247 olur)

150 + yz’nin onlar basamağı= 150 + 1 =151

20 + yz’nin birler basamağı= 20 + 7 =27

Bu işlemler sonucunda artık resim üzerinde ‘ab’ mesajının şifrelenmiş piksel değerleri aşağıdaki gibi olacaktır.

Çizelge 5.2. Şifrelenmiş resimdeki ilk 4 pikselin RGB değerleri

1. piksel			2. piksel			3. piksel			4. piksel			…….
R	G	B	R	G	B	R	G	B	R	G	B	…..
130	199	61	216	161	136	230	99	141	247	151	27	……

Yeni piksel değerlerinden görüleceği üzere, renk kodlarının sayısal değerlerinin değişimi sınırlı olduğundan, gözle görünür bir biçimde resim üzerinde bir fark yaratmayacaktır. Şifreleme işleminin çözülme algoritması ise aşağıdaki gibidir.

5.3. Cebirsel Şifreleme Çözme Yöntemi

Şifreleme yapılan piksellerin R G ve B değerlerinin mod 10 değeri alınarak, piksele hangi rakamın eklendiği bulunur. Bu rakamlar aşağıdaki gibi ağırlıklandırılarak;

(1.piksel R *10) + (1.piksel G) işleminin sonucu (x+y) değeri bulunur.
(1.piksel B *10) + (2.piksel R) işleminin sonucu (y+z) değeri bulunur.
(2.piksel G *10) + (2.piksel B) işleminin sonucu (x+y+z) değeri bulunur.

Teoride verilen 3 bilinmeyenli bu 3 farklı denklem kullanılarak, x, y ve z değerleri bulunabilir. Nihai olarak;

(x*100) + (y*10) + (z)

Cebirsel işlemi bize mesajdaki orijinal karakterin ASCIII değerini verir. Bu değer ile orijinal karakter ASCII tablosundan bulunabilir. Bu işlem, mesaj uzunluğunda metin elde edilene kadar uygulanmaktadır. Bu algoritmayı sadece ilk mesaj karakteri ‘a’ için uygularsak;

130%10=0 ve 199%10=9 değerlerinin ağırlıklı toplamı (0*10+9) xy’yi verir, yani 9’dur.

61%10=1 ve 216%10=6 değerlerinin ağırlıklı toplamı (1*10+6) yz’yi verir, yani 16’dır.

161%10=1 ve 136%10=6 değerlerinin ağırlıklı toplamı (1*10+6) xyz’yi verir, yani 16’dır.

Buradan x, y ve z değişkenleri (basamak rakamları) bulunur.

x=xyz-yz cebirsel işleminden, x=16-16=0 olarak bulunur.
z=xyz-xy cebirsel işleminden, z=16-9=7 olarak bulunur.

y=xyz-(x+y) cebirsel işleminden, y=16-(0+7)=9 olarak bulunur.

Ağırlıklar kullanılırsa;

Karakter ASCII değeri = (x*100) + (y*10) + (z)= 97

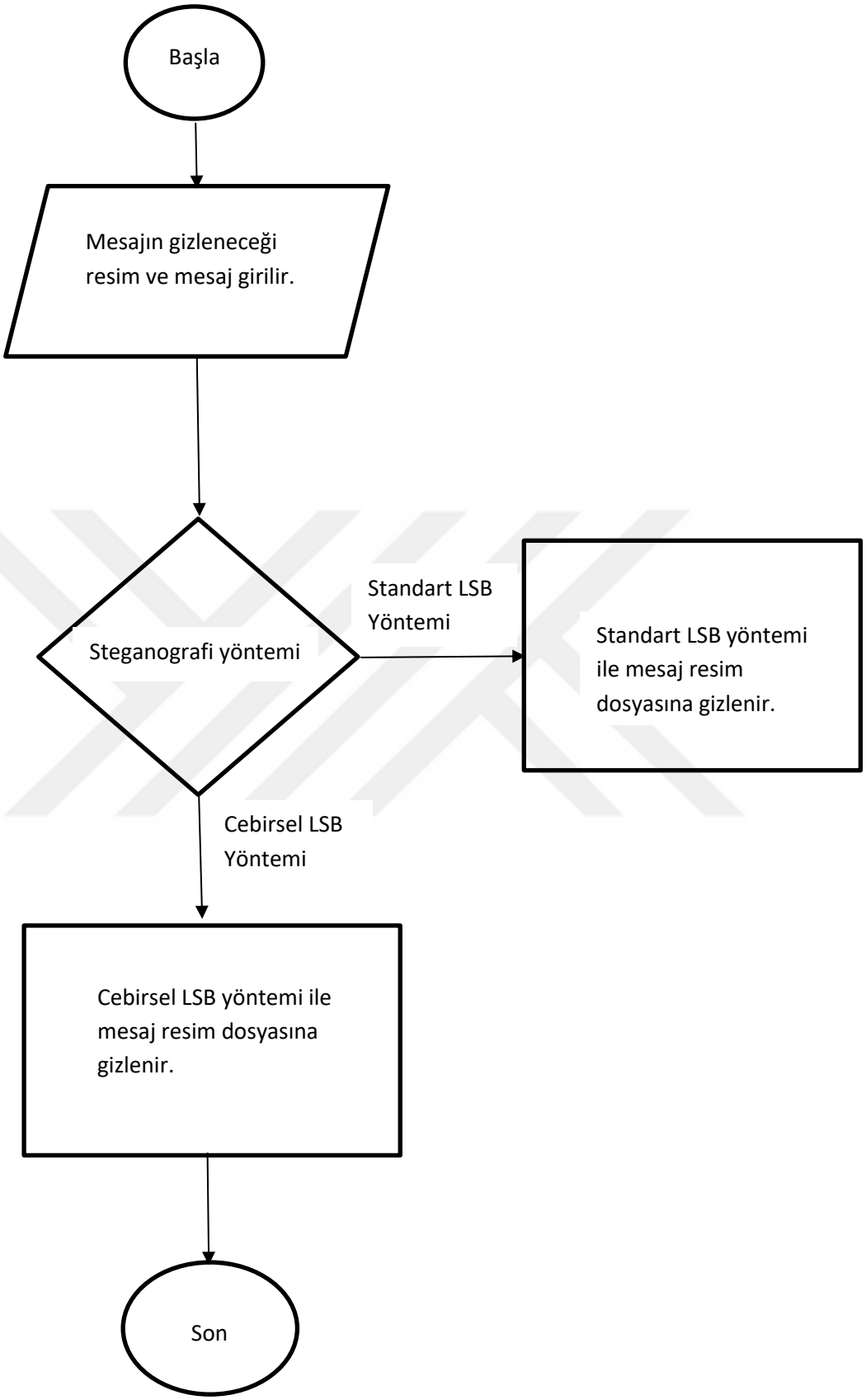
olarak bulunur. ASCII tablosunda 97 değeri ‘a’ karakterine karşılık gelmektedir.

5.4. Cebirsel LSB Yönteminin Uygulanmasının Geliştirilmesi

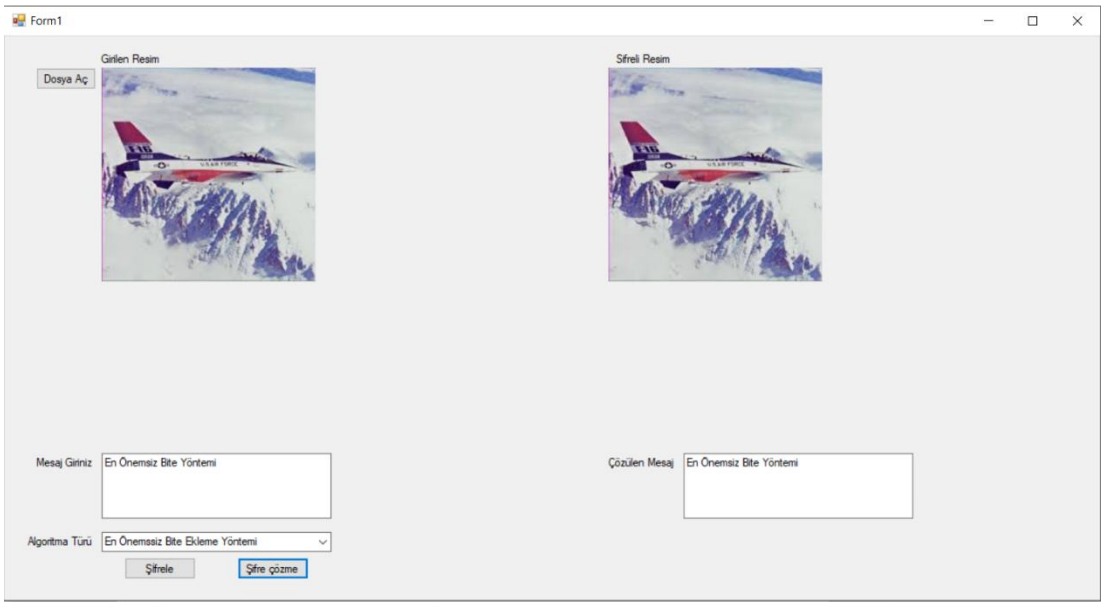
Bu çalışma C# programlama dilinde geliştirilmiştir. Uygulama veriyi gizlemek üzere 24 bit Tiffany, Baboon, Airplane ve Peppers resimlerini veri gizleme amacı ile kullanmaktadır. Kullanıcı standart LSB ve cebirsel LSB yöntemlerinden birini seçebilir. Uygulama hem veri gizleme hem de veri şifre çözme işlemi yapmaktadır. Veri gizlendikten sonra gizlenmiş resim yeni bir dosya olarak kaydedilmektedir. Bu işlemden sonra orijinal resim ile stego resim arasındaki görüntü kalitesini değerlendirmek için Matlab uygulaması geliştirilmiştir. Bu uygulamada consol terminalinde görüntü kalite değerlerinin sonuçları hesaplanıp gösterilmektedir. C# programlama dili ile geliştirilen programın LSB kodları Ek A’da, cebirsel LSB kodları Ek B’de verilmiştir. Matlab’de yazılan komutlar Ek C’de görülmektedir.

Uygulamada şu adımlar sırasıyla uygulanmaktadır. Şifrelenecek resim seçilir. Ardından gizlenmek istenilen mesaj alınır ve mesaj şifrelenir. Görüntü belirtilen dosya konumuna kaydedilir.

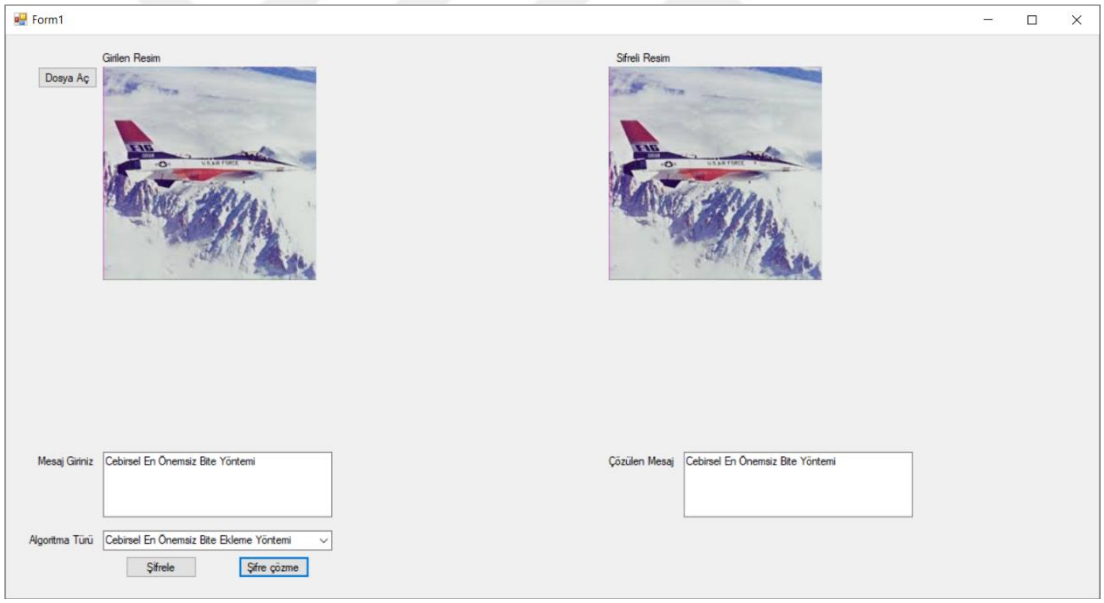
Şifre çözme talebinde bulunulduğunda, seçilen şifreli resimdeki mesaj çözülür ve görüntülenir. Standart LSB ve cebirsel LSB yöntemlerinin akış algoritması Şekil 5.1‘de ve uygulamanın ekran görüntüleri ise Şekil 5.2 ve Şekil 5.3’te görülmektedir.



Şekil 5.1. Cebirsel lsb ve standart lsb yöntemlerinin akış algoritması



Şekil 5.2. Standart lsb yönteminin uygulanması



Şekil 5.3. Cebirsel lsb yönteminin uygulanması

Uygulamada mesaj gizlenme aşamasında RGB değerleri 255 değerinden büyük bir değer alırsa, değer 10 azaltılarak kaydedilir.

6. GÖRÜNTÜ KALİTE TESPİTİ

Standart en az ağırlıklı bit ve cebirsel şifreleme modeli tarafından şifrelenmiş resimlerin orijinal halleri ile karşılaştırılma yapılmaktadır. Görüntü kalitesi değerlerini hesaplamak için tepe sinyali gürültü oranı değeri ve ortalama karesel hata metrikleri kullanılmıştır (Tuncer, 2011). Bu metrikler Matlab uygulamasında fonksiyonlar tarafından yapılmıştır.

6.1. Ortalama Karesel Hata (Mean- Squared Error – MSE)

Bir görüntüde farklı tipte işlemler yaptıktan sonra orijinal görüntü ile işlem yapılan görüntüyü karşılaştırmak için bu yöntem kullanılır. Resimde oluşabilecek farklılıkları karşılaştırmak için kullanılan ortalama karesel hata tahminidir (Tunver ve Avcı, 2016). Bu yöntemin hesaplanması oldukça basittir ama insanın kalite algısına uygun değildir. Ortalama karesel hata ne kadar az ise aslına o kadar yakındır. Bu metrik Matlab uygulamasında "immse" komutu ile hesaplanmaktadır. Ortalama karesel hata performans değerini ölçer ve her zaman pozitif değerdir. Ortalama karesel hata değeri sıfıra yakın olan tahminleyicilerin daha iyi bir performans gösterdiğini söylemektedir. Ortalama karesel hatanın matematiksel karşılığı Formül 6.1 ile ifade edilmektedir.

$$\text{MSE} = \frac{1}{n}\sum_{i=1}^{n}(y_i - \tilde{y}_i)^2 \qquad (6.1)$$

6.2. Tepe Sinyali Gürültü Oranı (Peak Signal to Noise Ratio – PSNR)

Sayısal görüntülerde görüntüler arasındaki benzerliği gösterebilmek için tepe sinyali gürültü oranı değeri metriği kullanılmaktadır. Metin resime şifrelendikten sonra görüntü üzerindeki bozulmaları tepe sinyali gürültü oranı değeri ile bulunur. Tepe sinyali gürültü oranı değerinin yüksek olması resmin kalitesini ve resimin üzerindeki bozulmaların daha minimum olduğunu söylemektedir (Kaş ve Tanyıldızı, 2017). Metnin içindeki gizlenmiş görüntünün bozulmalarını hesaplayan tepe sinyali gürültü oranı değerinin matematiksel

karşılığı Formül 6.2'de görülmektedir. Tepe sinyali gürültü oranı değeri dB(desibel) cinsinden hesaplanmaktadır. Tepe sinyali gürültü oranı değeri matlab uygulamasında "psnr" komutu ile hesaplanmaktadır.

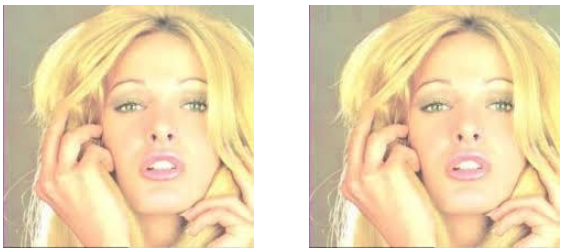
$$\text{PSNR} = 10*\mathbf{log_{10}}\left(\frac{MAX_I^2}{MSE}\right) \text{ (dB)} \qquad (6.2)$$

7. ARAŞTIRMA BULGULARI VE TARTIŞMA

Steganografide verinin gizliği önemlidir. LSB algoritmasında mesajın 1 karakteri resmin 8 baytına kopyalanmaktadır. Önerilen cebirsel şifreleme yaklaşımında ise 1 karakter resmin 2 pikseline (yani toplam 6 bayta) eklenmektedir. Böylelikle veri güvenliğinin arttırılmasının yanı sıra, yaklaşık %33 oranında (8 / 6 ≅%33) veri sıkıştırması da sağlanmaktadır.

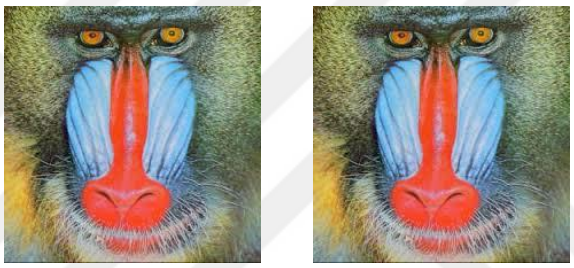
Veri gizleme işlemi resmin piksellerine satır öncelikli uygulanmıştır. Piksellerin renk değerlerine, cebirsel işlem sonucunun rakamları en ağırlıklıdan başlayarak sırasıyla yerleştirilir. Örneğin cebirsel toplam 18 ise, ilk piksele 1 sonraki piksele 8 eklenir. Doğal olarak en büyük rakam 9 olabileceğinden, her renk baytının en az ağırlıklı son 4 biti değiştirilebilir. Fakat öncesinde renk değerinin son rakamı mod işlemi ile atıldığından, sonuç olarak değişim olmamaktadır. Sadece renk değeri >250 ise bu durumda eklenecek yeni rakam değeri ASCII kod sınırını aşmasına neden olmaktadır. Böyle durumlarda renk değerinin onlar basamağı, bir eksiltilerek uygulanmaktadır. Renk değerinin son rakamı çıkartılarak, yerine cebirsel ifadenin yeni rakamı eklendiğinden MSE hatalarının çok olmaması beklenmektedir. Fakat bahsedildiği üzere renk değeri çok canlı olan resimlerde, modelde hata oranı büyüme eğilimindedir. Yapılan denemelerde benzer sonuçlar elde edilmiştir. Veri güvenliği ve sıkıştırmadan kaynaklı MSE hata oranının artması kabul edilebilir düzeydedir. Elde edilen şifrelenmiş resimler orijinallerinden çıplak gözle fark edilememektedir.

Genel olarak sınamalarda kullanılan 24 bitlik Tiffany, Peppers, Airplane, Baboon resimlerine 25, 251 ve 2070 karakter uzunluğunda hem standart LSB, hem de cebirsel LSB yöntemi uygulanarak veri gizleme işlemi yapılmıştır. Orijinal resimler ve cebirsel şifrelenmiş resimler Şekil 7.1'de görülmektedir. Her iki yöntemle şifrelenen resimlerin kalite karşılaştırma metrik değerleri (MSE ve PSNR), Tablo 7.1 ve Tablo 7.2'de verilmiştir.



(a) (b)

(a) (b)



(a) (b)

(a) (b)

Şekil 7.1. Çalışmada kullanılan görüntüler (a) Orijinal Resim (b) Stego Resim

Çizelge 7.1. Standart lsb yönteminin uygulanmasının görüntü kalite değerlikleri

Resim Adı	Karakter Uzunluk	MSE	PSNR(db)
Airplane	25	2,13	44,88
Baboon	25	2,36	44,43
Tiffany	25	0,98	48,26
Peppers	25	1,41	46,66
Airplane	251	2,13	44,88
Baboon	251	2,36	44,43
Tiffany	251	0,98	48,24
Peppers	251	1,40	46,71
Airplane	2070	2,13	44,87
Baboon	2070	2,35	44,45
Tiffany	2070	0,98	48,26
Peppers	2070	1,41	46,67

Çizelge 7.2. Cebirsel şifrelenmiş lsb yönteminin uygulanmasının görüntü kalite değerlikleri

Resim Adı	Karakter Uzunluk	MSE	PSNR(db)
Airplane	25	2,14	44,85
Baboon	25	2,36	44,43
Tiffany	25	0,99	48,22
Peppers	25	1,43	46,62
Airplane	251	2,26	44,61
Baboon	251	2,47	44,24
Tiffany	251	1,66	45,95
Peppers	251	2,07	45,01
Airplane	2070	3,17	43,15
Baboon	2070	3,65	42,53
Tiffany	2070	1,95	45,25
Peppers	2070	2,44	44,29

25 karakter şifrelenmiş olan resimlerde standart LSB yönteminin MSE metrik değeri, cebirsel LSB yöntemi ile şifrelenmiş olanlarla hemen hemen aynı bulunmaktadır. Bununla birlikte beklendiği üzere karakter sayısı arttıkça cebirsel yöntemin MSE değeri artmaktadır. Yapılan sınamalarda elde edilen değerlerin ortalamasına göre MSE hata oranı %29 artmakta ve PSNR %2,5 azalmaktadır. Her ne kadar metrik değerleri cebirsel LSB için negatif gözükse de orijinal resimdeki bu değişimler çok ufak ve gözle algılanabilir olmaktan uzaktır.

8. SONUÇ VE ÖNERİLER

Çalışmada C# programlama dili kullanılmıştır. Resmin piksellerine veri gizleme işlemleri yapıldıktan sonra, MSE ve PSNR metrik değerlerinin hesaplanması için Matlab programı kullanılmaktadır.

25, 251 ve 2070 karakterlik veriler kullanılarak LSB ve cebirsel LSB yöntemleri ile şifrelenen veriler görüntülerin içerisine satır olarak gizlenmektedir. Karakter sayısı arttıkça cebirsel LSB yöntemi ile şifrelenmiş resimlerdeki MSE metrik değerinin arttığı görülmektedir. Metrik değerleri cebirsel LSB yöntemi için olumsuz görünse de orijinal resimlerdeki bu değişimler çok ufak ve gözle algılanamamaktadır. Kazanılan sıkıştırma oranı ve ayrıca verinin gizlenme güvenliği göz önünde bulundurulduğunda bu yöntem, güvenliğin önemli olduğu uygulamalara hitap etmektedir.

Gizlenen mesajın güvenliğini daha da arttırmak üzere, şifrelenmek istenen mesajın ilk önce şifreleme algoritması yardımı ile şifrelenmesi, daha sonra cebirsel LSB yöntemi ile görüntünün içine gizlenmesi sağlanabilir.

KAYNAKLAR

Akdemir, B., 2009. Tahmin Uygulamalarında Performans Geliştirmek İçin Kullanılan Normalizasyon Metotlarına Yeni Bir Yaklaşım, Selçuk Üniversitesi, Fen Bilimleri Enstitüsü, Doktora Tezi, 156, Konya.

Akleylek, S., Yıldırım, H.M., Tok, Z.Y., 2011. Kriptoloji ve Uygulama Alanları: Açık Anahtar Altyapısı ve Kayıtlı Elektronik Posta, Akademik Bilişim, Şubat 2011.

Aydoğan, M., 2014. Adli Bilişimde Görüntü Üzerine Kriptografi Uygulamaları, Fırat Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, 88, Elazığ.

Badem, H., Güneş, M., 2011. Video Formatına Veri Gizleme Amacıyla Gömülmüş Bir Steganografi Uygulamasının Geliştirilmesi, KSU Mühendislik Bilimleri Dergisi, 2(14), 1-10.

Belenli, İ.L., 2015. Sır Paylaşımı Tabanlı Elektronik Görsel Şifreleme Sistemi, Fırat Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, 64, Elazığ.

Bilgin, M., 2013. Steganografi, Akademik Bilişim 2013 – XV. Akademik Bilişim Konferansı Bildirileri, Ocak 2013.

Çoşkun, A., Ülker, Ü., 2013. Ulusal Bilgi Güvenliğine Yönelik Bir Kriptografi Algoritması Geliştirilmesi ve Harf Frekans Analizine Karşı Güvenirlik Tespiti, Bilişim Teknolojileri Dergisi, 2(6), 31-39.

Demirci, B., 2016. Görüntü Steganografi Medotları Ve Performanslarının Karşılaştırılması, Selçuk Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, 83, Konya.

Doğan, F., Daş, R., Türkoğlu, İ., 2016. İmgeler İçin Farklı Bir Veri Gizleme Yaklaşımı, Dicle Üniversitesi Mühendislik Dergisi, 3(7), 501-514.

Esin, E. M., Güvenoğlu, E., 2011. Resim İçerisine Yazı Gizlenmesi Amacıyla Kullanılan LSB Ekleme Yönteminin Shuffle Algoritmasıyla İyileştirilmesi, Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi, 1(2), 1-6.

Eskiçırak, F., 2012. Çoklu Ortamlarda Bilgi Gizleme Uygulaması Tasarımı ve Geliştirilmesi, Haliç Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, 98, İstanbul.

Gürel, H., 2006. Sayısal Resim İçerisine Veri Gizleme Uygulamaları, Kocaeli Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, 99, Kocaeli.

Güvenoğlu, E., 2016. Resim Şifreleme Amacıyla Dinamik S Kutusu Tasarımı İçin Bir Yöntem, El-Cezeri Fen ve Mühendislik Dergisi, 2(3), 179-191.

Karadoğan, I., 2016. Ağ İletişiminde Veri Gizleme Tabanlı Bilgi Güvenliği Uygulamaları, Fırat Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, 82, Elazığ.

Kaş, Ü., Tanyıldızı, E., 2017. Euler Renk ve Hareket Büyütme Yöntemlerinin Performans Analizi, Afyon Kocatepe Üniversitesi Fen ve Mühendislik Bilimleri Dergisi, 17(506), 506-515.

Koçak, C., 2015. Kriptografi ve Stenografi Yöntemlerini Birlikte Kullanarak Yüksek Güvenlikli Veri Gizleme, Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 2(31), 115-123.

Kurtuldu, Ö., 2009. İmge Kareleri Kullanan Yeni Bir Steganografi Yöntemi, Journal of Naval Science and Engineering,1(5), 107-118.

Olcay, C., Saran, N., 2013. İmge İçine Bilgi Gizlemede Kullanılan LSB Yöntemlerinin Karşılaştırılması, Çankaya University Journal of Science and Engineering, 1(10), 17-32.

Özbilgin, F., Durmuş, F., Karagöl, S., 2018. Yazılı Metni Şifreleyip LSB Yöntemi ile Gizleme, Düzce Üniversitesi Bilim ve Teknoloji Dergisi,6, 676-685.

Sevindir, H. K., Sayın, N., 2018. Dalgacık Dönüşümü Tabanlı Görsel Kriptoloji, Afyon Kocatepe Üniversitesi Fen ve Mühendislik Bilimleri Dergisi, 15101(67746), 888-894.

Solak, S., Altınışık, U., 2018. En Düşük Anlamlı Son Üç Bitin Değiştirilmesi Yöntemi Kullanılarak Renkli Görüntülere Verilerin Gizlenmesi, Uluslararası Marmara Fen ve Sosyal Bilimler Kongresi, Kasım 2018.

Şahin, A., Buluş, E., Sakallı, M. T., 2005. 24-bit Renkli Resimler Üzerinde En Önemsiz Bite Ekleme Yöntemini Kullanarak Bilgi Gizleme, Trakya Üniversitesi, 1(7), 17-22.

Şahin, A., Buluş, E., Sakallı, M. T., 2016. Gri Seviye Resimler Üzerinde Rasgele LSB Yöntemini ve Sayı Teorisini Kullanarak Bilgi Gizleme ve Steganaliz, Trakya Üniversitesi Dergisi, Şubat 2014.

Tekeli, K., 2017. Ses Steganografi Ve Metotlarının Karşılaştırılması, Adnan Mendres Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, 111, Aydın.

Tuncal, T., 2008. Bilgisayar Güvenliği Üzerine Bir Araştırma Ve Şifreleme-Deşifreleme Üzerine Uygulama, Maltepe Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, 181, İstanbul.

Tuncer, T., 2011. Tekil Değer Ayrışımı Tabanlı Yeni Bir İmge Kimliklendirme Yöntemi, Fırat Üniversitesi Teknoloji Fakültesi Adli Bilişim Mühendisliği, 32(3), 877-886.

Tuncer, T., 2016. İkili İmgeler İçin Kaos Tabanlı Yeni Bir Steganografik Yöntem, Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi, 1(9), 29-36.

Tuncer, T., 2017. İkili İmgeler İçin Blok Tabanlı Yeni Bir Kimlik Doğrulama Yöntemi, Dicle Üniversitesi Mühendislik Dergisi, 3(8), 525-534.

Tuncer, T., Avcı, E., 2016. Göktürk Alfabesi Tabanlı Görsel Sır Paylaşımı Metodu ile Veri Gizleme Uygulaması, Gazi Üniversitesi Mühendislik ve Mimarlık Dergisi, 3(31), 781-789.

Tuncer, T., Avcı, E., 2017. Yerel İkili Örüntü Tabanlı Veri Gizleme Algoritması: LBP-LSB, Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendislik Dergisi, 1(10), 48-53.

Ülker, Ü., 2014. Klasik Teknikler Kullanılarak Bir Kriptografi Algoritması Geliştirilmesi ve DES Algoritması İle Performans Analizlerinin Karşılaştırılması, Gazi Üniversitesi, Bilişim Enstitüsü, Yüksek Lisans Tezi, 171, Ankara.

Yaşar, H., Ceylan, M., 2014. RGB Görüntülerin Bit Değişimi ve Ripplet-I Dönüşümü Tabanlı Şifreleme ile Filigranlanması, 7. Uluslararası Bilgi Güvenliği ve Kriptoloji Konfreransı, Ekim 2014.

Yaşar, H., Özteriş, G. H., Ceylan, M., 2015. Renkli Taşıyıcı ve Renkli Gizli Görüntülerin Görüntü Özellik Tabanlı İki Katmanlı Şifreleme ve En Önemsiz Bit Yöntemi Kullanılarak Filigranlanması, Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, 2(1), 6-14.

Yayık, A., 2013. Yapay Sinir Ağı ile Kriptoloji Uygulamaları, Mustafa Kemal Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, 82, Hatay.

Yeşilbaş, E., 2016. Cebirsel Kriptoloji Yöntemleri Ve Bazı Uygulamaları, Recep Tayyip Erdoğan Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, 78, Rize.

Yıldırım, E. O., 2014. Kaotik Haritaların Steganografi İle Birlikte Kullanımı, Karadeniz Teknik Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, 90, Trabzon.

Yıldız, Y., Özcerit, A. T., 2015. 24 Bit Renkli Hareketli Resimler (Video) Üzerinde Geliştirilen Sır Örtme Yöntemi, Sakarya Üniversitesi Fen Bilimleri Dergisi, 1, 1-6.

Yiğit, Y., 2018. Sayısal İmgelerde Güvenli Veri Gizlemeye Yönelik Uygun Maske Belirleme, Fırat Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, 60, Elazığ.

Yürüklü, E., 2013. Kaotik Özelliklerin Konuşma Sesleri Steganalizinde Kullanımı, Uludağ Üniversitesi, Fen Bilimleri Enstitüsü, Doktora Tezi, 106, Bursa.

EKLER

EK A. Standart LSB yönteminin uygulanmasının görüntü kalite değerlikleri

EK B. Cebirsel LSB yönteminin uygulanmasının görüntü kalite değerlikleri

EK C. Çalışmada kullanılan görüntüler

EK A. Standart LSB yönteminin uygulanmasının görüntü kalite değerlikleri

Çizelge A.1. Standart LSB yönteminin uygulanmasının görüntü kalite değerlikleri

Resim Adı	Karakter Uzunluk	MSE	PSNR(db)
Airplane	25	2,13	44,88
Baboon	25	2,36	44,43
Tiffany	25	0,98	48,26
Peppers	25	1,41	46,66
Airplane	251	2,13	44,88
Baboon	251	2,36	44,43
Tiffany	251	0,98	48,24
Peppers	251	1,40	46,71
Airplane	2070	2,13	44,87
Baboon	2070	2,35	44,45
Tiffany	2070	0,98	48,26
Peppers	2070	1,41	46,67

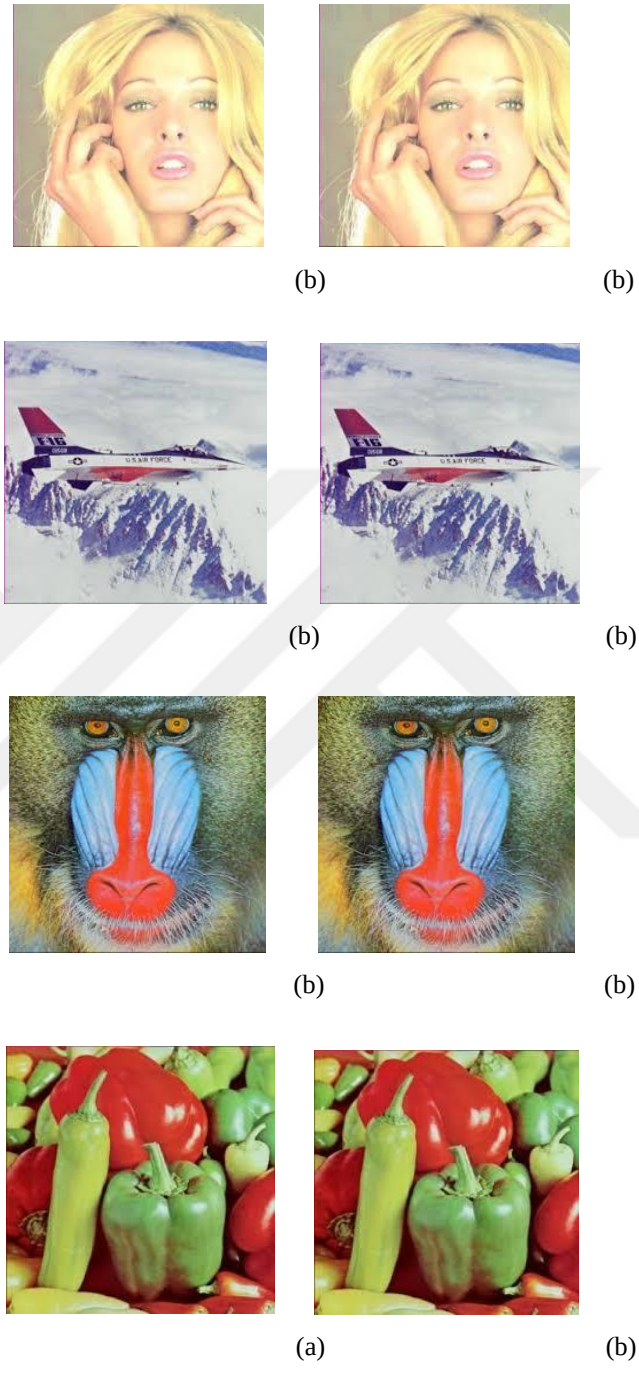
,

EK B. Cebirsel LSB yönteminin uygulanmasının görüntü kalite değerlikleri

Çizelge B.1. Cebirsel Şifrelenmiş LSB yönteminin uygulanmasının görüntü kalite değerlikleri

Resim Adı	Karakter Uzunluk	MSE	PSNR(db)
Airplane	25	2,14	44,85
Baboon	25	2,36	44,43
Tiffany	25	0,99	48,22
Peppers	25	1,43	46,62
Airplane	251	2,26	44,61
Baboon	251	2,47	44,24
Tiffany	251	1,66	45,95
Peppers	251	2,07	45,01
Airplane	2070	3,17	43,15
Baboon	2070	3,65	42,53
Tiffany	2070	1,95	45,25
Peppers	2070	2,44	44,29

EK C. Çalışmada kullanılan görüntüler



(b) (b)

(b) (b)

(b) (b)

(a) (b)

Şekil C.1. Çalışmada kullanılan görüntüler (a) Orijinal Resim (b) Stego Resim

ÖZGEÇMİŞ

Adı Soyadı : Ali KARADURAN

Doğum Yeri ve Yılı : ERZURUM, 08/11/1988

Medeni Hali : Evli

Yabancı Dili : İngilizce

E-posta : ali.karaduran@istanbulticaret.edu.tr

Eğitim Durumu

Lise : Ereğli Lisesi, 2005

Lisans :Haliç Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, 2013

Yüksek Lisans :İstanbul Ticaret Üniversitesi, Bilgisayar Mühendisliği Anabilim Dalı, Bilgisayar Mühendisliği Bölümü, 2020

Mesleki Deneyim

Korvus Bilişim,
Bilgisayar Mühendisi 2013 - 2015

Optiim Yazılım Hizmetleri A.Ş.,
Yazılım Test Mühendisi 2015

İstanbul Ulaşım Hizmetleri ve Araç Kiralama A.Ş.,
Bilgisayar Mühendisi 2017 - Devam Ediyor

Yayınları

Karaduran, A., Turan, M., 2020. Cebirsel LSB Yöntemi, Avrupa Bilim ve Teknoloji Dergisi, Özel Sayı, 73-80.