T.C.

TRAKYA ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

HAREKETLİ GÖRÜNTÜ DOSYALARINDA BİLGİ GİZLEMEDE KULLANILAN YÖNTEMLERİN İNCELENMESİ VE EN ÖNEMSİZ BİTE EKLEME YÖNTEMİNİN UYARLANMASI

EGEMEN TEKKANAT

DOKTORA TEZİ

HESAPLAMALI BİLİMLER ANABİLİM DALI

Tez Danışmanı: DR.ÖĞR. ÜYESİ ANDAÇ ŞAHİN MESUT

EDİRNE-2022

EGEMEN TEKKANAT'ın hazırladığı "**HAREKETLİ GÖRÜNTÜ DOSYALARINDA BİLGİ GİZLEMEDE KULLANILAN YÖNTEMLERİN İNCELENMESİ VE EN ÖNEMSİZ BİTE EKLEME YÖNTEMİNİN UYARLANMASI**" başlıklı bu tez, tarafımızca okunmuş, kapsam ve niteliği açısından Hesaplamalı Bilimler Anabilim Dalında bir **Doktora tezi** olarak kabul edilmiştir.

Jüri Üyeleri : İmza

Prof. Dr. Muharrem Tolga SAKALLI ……

Doç. Dr. Vedat TAŞKIN ……

Dr. Öğr. Üyesi Andaç MESUT (Danışman) ……

Doç. Dr. Erdinç UZUN ……

Dr. Öğr. Üyesi Halil Nusret BULUŞ ……

Tez Savunma Tarihi: 04/08/2022

Bu tezin Doktora tezi olarak gerekli şartları sağladığını onaylarım.

İmza

Dr. Öğr. Üyesi Andaç MESUT
Tez Danışmanı ……

Trakya Üniversitesi Fen Bilimleri Enstitüsü onayı

……

Prof. Dr. Hüseyin Rıza Ferhat KARABULUT
Fen Bilimleri Enstitüsü Müdürü

T.Ü.FEN BİLİMLERİ ENSTİTÜSÜ
HESAPLAMALI BİLİMLER ANABİLİM DALI DOKTORA PROGRAMI
DOĞRULUK BEYANI

Trakya Üniversitesi Fen Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında, tüm verilerin bilimsel ve akademik kurallar çerçevesinde elde edildiğini, kullanılan verilerde tahrifat yapılmadığını, tezin akademik ve etik kurallara uygun olarak yazıldığını, kullanılan tüm literatür bilgilerinin bilimsel normlara uygun bir şekilde kaynak gösterilerek ilgili tezde yer aldığını ve bu tezin tamamı ya da herhangi bir bölümünün daha önceden Trakya Üniversitesi ya da farklı bir üniversitede tez çalışması olarak sunulmadığını beyan ederim.

04/08/20202
Egemen TEKKANAT
İmza

Doktora Tezi
Hareketli Görüntü Dosyalarında Bilgi Gizlemede Kullanılan Yöntemlerin İncelenmesi Ve En Önemsiz Bite Ekleme Yönteminin Uyarlanması
T.Ü. Fen Bilimleri Enstitüsü
Hesaplamalı Bilimler Anabilim Dalı

ÖZET

Bilginin gizli kalacak şekilde güvenli iletimi için çeşitli yöntemler kullanılmaktadır. Bilgi gizleme ve şifreleme teknikleri bu amaçla kullanılmaktadır. Bu çalışmada bilgi gizleme yöntemlerinin bir alt dalı olan steganografi hareketli görüntü dosyası olarak ta bilinen video dosyaları üzerinde uygulanmıştır. Gizli bilginin güvenli bir şekilde transfer edilmesi problemine karşı bir algoritma ile birlikte uygulama geliştirilmiştir. Tezin amacı video dosyaları üzerinde steganografi ve kriptoloji kullanarak bilgi gizleme ve veri iletimi için güvenli bir ortam oluşturmaktır. Bu amaç doğrultusunda video dosyaları üzerine En önemsiz bite gizleme yöntemi kullanılarak veriler sıralı ve belirlen bir formül ile birlikte rastgele olarak gizlenmiş ayrıca güvenliği artırmak amacı ile yapılan bu gizleme işleme şifreleme teknikleri ile desteklenmiştir. Geliştirilen algoritmanın taşıyıcıdaki değişim açısından değerlendirmeleri MSE ve PSNR teknikleri ile ve dayanıklılık açısından değerlendirmeleri ise histogram analizi tekniği ile ölçülmektedir. Önerilen yöntem ile gizli iletişim alanında gerçekleştirilebilecek olan çözümlere bir katkı sağlayabileceği düşünülmektedir.

Yıl : 2022

Sayfa Sayısı : 100

Anahtar Kelimeler : Bilgi Gizleme, Steganografi, Video Steganografi, En Önemsiz Bite Ekleme Yöntemi, Steganaliz

Doctorate Thesis
Investigation of Methods Used to Hide Information in Moving Image Files and Adaptation of Least Significant Bit Insertion Method
Trakya University Institute of Natural Sciences
Department of Computational Sciences

ABSTRACT

Various methods are used for the secure transmission of information in a way that remains confidential. Information hiding and encryption techniques are used for this purpose. In this study, steganography, which is a sub-branch of information hiding methods, was applied on video files, also known as moving image files. An application has been developed with an algorithm against the problem of securely transferring confidential information. The aim of the thesis is to create a secure environment for information hiding and data transmission by using steganography and cryptography on video files. For this purpose, by using the least significant bit hiding method on video files, the data is hidden sequentially and randomly with a determined formula, and this hiding process, which is made to increase security, is supported by encryption techniques. Evaluations of the developed algorithm in terms of change in carrier are measured with MSE and PSNR techniques, and evaluations in terms of durability are measured by histogram analysis technique. It is thought that with the proposed method, it can contribute to the solutions that can be realized in the field of confidential communication.

Year : 2022

Number of Pages : 100

Keywords : Information Hiding, Steganography, Video Steganography, Least Significant Bit Insertion Method, Steganalysis

TEŞEKKÜR

Bu çalışmanın hazırlanması esnasında bana yol gösteren, bu alanda çalışmam için beni teşvik eden, yardımlarını ve desteğini benden esirgemeyen değerli danışman hocam Sayın Dr. Öğr. Üyesi Andaç ŞAHİN MESUT'a teşekkür ederim.

Tez izleme komitesinde bulunan ve derin bilgileri ve yapıcı yorumları ile tez çalışmasında bana yaptıkları katkılardan dolayı Sayın Prof. Dr. Muharrem Tolga SAKALLI ve Sayın Doç. Dr. Vedat TAŞKIN'a teşekkürlerimi sunarım.

Çalışmalarım sırasında bana tecrübeleri ile yol gösteren, çalışabilmem için gerekli ortamı sağlayan ve birlikte çalışmalar gerçekleştirdiğimiz mesai arkadaşlarım Sayın Doç.Dr. Murat TOPALOĞLU ve Sayın Dr. Öğr. Üyesi Harun ÖZKİŞİ'ye çok teşekkür ederim.

Son olarak manevi desteğini benden esirgemeyen ve her zaman yanımda olan değerli eşim Gizem TOPALLAR TEKKANAT'a ve aileme teşekkür ederim.

İÇİNDEKİLER

ÖZET iv
ABSTRACT v
TEŞEKKÜR vi
İÇİNDEKİLER vii
KISALTMALAR x
ŞEKİLLER DİZİNİ xi
ÇİZELGELER DİZİNİ xiv
BÖLÜM 1 1
GİRİŞ 1
1.1. Bilgi Güvenliği 1
1.2. Bilgi Gizleme 3
1.3. Bilgi Şifreleme 6
1.4. Tezin Önemi 11
1.5. Tezin Amacı 12
1.6. Tezin Yapısı 12
1.7. Önceki Çalışmalar ve Literatür Taraması 13
BÖLÜM 2 16
STEGANOGRAFİ 16
2.1. Steganografinin Tarihçesi 17
2.2. Steganografik Sistem 19
2.3. Steganografinin Alt Alanları 21
2.4. Steganografinin Kullanım Alanları 22
2.5. Metin Steganografi 23
2.5.1. Açık Alan Yöntemleri 24
2.5.2. Yazımsal Yöntemler 26
2.5.3. Anlamsal Yöntemler 26

2.6. Resim Steganografi 27
2.6.1. Alan Dönüştürme Teknikleri 28
2.6.2. Maskeleme ve Filtreleme Yöntemleri 28
2.6.3. Uzaysal Alan Teknikleri (Spatial Domain Methods) 28
2.6.4. Çarpıtma Teknikleri 29
2.7. Ses Steganografi 29
2.7.1. Taft Yayılması 30
2.7.2. Aşama Kodlaması 30
2.7.3. Düşük Bit Kodlaması 31
2.7.4. Yankı Veri Gizlemesi 31
2.8. HTML Steganografi 31
2.9. Ağ Steganografi 33
BÖLÜM 3 34
VİDEO STEGANOGRAFİ 34
3.1. Video 34
3.1.1. Kodek 35
3.1.2. Kare Hızı 36
3.1.3. Çerçeve Boyutu 36
3.1.4. En-Boy Oranı 36
3.1.5. Video Dosyası Türleri 37
3.2. Video Steganografi 38
3.2.1. Video Steganografi Yöntemleri 41
3.2.2. En Önemsiz Bite Ekleme Yöntemi (LSB) 43
BÖLÜM 4 46
STEGANOGRAFİK YÖNTEMLERİN GEREKSİNİMLERİ 46
4.1. Kapasite 46
4.2. Fark edilmezlik 47
4.3. Dayanıklılık 48
4.3.1. Steganaliz 48
BÖLÜM 5 54
MATERYAL VE METOT 54
5.1. Geliştirilen video steganografi uygulaması 59

5.2. Geliştirilen Uygulamanın Değerlendirilmesi 64
5.2.1. Kapasite Açısından Değerlendirilmesi 65
5.2.2. Taşıyıcıdaki Değişim Açısında Değerlendirilmesi 65
5.2.3. Dayanıklılık Açısından Değerlendirilmesi 72
BÖLÜM 6 78
SONUÇ 78
KAYNAKLAR 80
TEZ İLE İLGİLİ BİLİMSEL FAALİYETLER 85
Ulusal Hakemli Dergi Makaleleri 85
ÖZGEÇMİŞ 86

KISALTMALAR

AES	Advanced Encryption Standard
AVI	Audio Video Interleave
BMP	Windows Bitmap
DCT	Discrete Cosine Transform
DES	Data Encryption Standard
DFT	Discrete Fourier Transform
DWT	Discrete Wavelet Transform
FPS	Frame Per Second
GIF	Graphics Interchange Format
HAS	Human Auditory System
IDEA	International Data Encryption Algorithm
JPEG	Joint Photographic Experts Group
LSB	Least Significant Bit
MD5	Message-Digest Algorithm 5
MPEG	Moving Picture Experts Group
MSE	Mean Squared Error
PNG	Portable Network Graphics
PSNR	Peak SNR (Signal-to-Noise Ratio)
RC4	Rivest Encryption 4
RGB	Red Green Blue
RMSE	Root MSE (Mean Squared Error)
RSA	Rivest–Shamir–Adleman
RQP	Raw Quick Pairs
SHA	Secure Hashing Algorithm
SIFT	The scale-invariant feature transform
SNR	Signal to noise ratio
SSIM	The structural similarity index measure
SURF	Method Speeded Up Robust Features
3DES	Triple DES

ŞEKİLLER DİZİNİ

Şekil 1.1. Bilgi Güvenliği Unsurları 2
Şekil 1.2. Bilgi Güvenliği Sistemi 3
Şekil 1.3. Bilgi Gizleme 4
Şekil 1.4. Bir düz metnin şifrelenmesi ve şifre çözme işlemi 7
Şekil 1.5. Haberleşme Sistemi 9
Şekil 1.6. Simetrik Şifreleme Algoritması 10
Şekil 1.7. Asimetrik Şifreleme Algoritması 11
Şekil 2.1. Stego Nesnesi 16
Şekil 2.2. Steganographia kitabının latince kapağı 18
Şekil 2.3. Mikro Noktalama 18
Şekil 2.4. Steganografik sistemde veri gömme algoritması 20
Şekil 2.5. Steganografik sistemde veri geri elde etme algoritması 21
Şekil 2.6. Steganografi Kullanım Alanları 22
Şekil 2.7. Sayısal Steganografi Alanları 23
Şekil 2.8. Metin Steganografi Algoritması 24
Şekil 2.9. Satır kaydırma kodlaması Örneği 25
Şekil 2.10. Cümle İçi Boşluk Bırakma Örneği 25
Şekil 2.11. Gelecek kodlaması örneği 26
Şekil 2.12. Resim Steganografik Sistem 27
Şekil 2.13. Basit Ses Steganografi Algoritması 30
Şekil 2.14. Örnek HTML kodu 32
Şekil 2.15. HTML koduna gizli mesajın yazılması 32
Şekil 3.1. En çok tercih edilen en-boy oranları 37
Şekil 3.2. Video Steganografi Algoritması 39
Şekil 3.3. Video Steganografi için Gömme Algoritması 40
Şekil 3.4. Video Steganografi için Çıkartma Algoritması 41
Şekil 3.5. LSB yöntemi ile veri gömme 44

Şekil 3.6. LSB uygulaması 45
Şekil 4.1. Steganografi Yöntemlerinin Temel Gereksinimleri 46
Şekil 4.2. MSE Formülü 47
Şekil 4.3. PSNR Formülü 48
Şekil 4.4. Steganaliz Süreci 50
Şekil 4.5. Steganaliz atak türleri 51
Şekil 5.1. Uygulanan Gizleme İşlemi 56
Şekil 5.2. Veriyi geri elde etme işlemi 56
Şekil 5.3. AES algoritması. 58
Şekil 5.4. RSA Algoritması 59
Şekil 5.5. Program Giriş Ekranı 60
Şekil 5.6. Dosya seçim ekranı 61
Şekil 5.7. Gizleme Ekranı 62
Şekil 5.8. Analiz Ekranı 63
Şekil 5.9. Gömme Algoritması 64
Şekil 5.10. Video3 ve Video 4 görselleri 70
Şekil 5.11. Video1 dosyası için **(a)** Veri gizlenmemiş videonun histogram grafiği **(b)** Sıralı şekilde 0,1 KB veri gizlenmesiyle oluşan videonun histogram grafiği **(c)** Rastgele şekilde 0,1 KB veri gizlenmesiyle oluşan videonun histogram grafiği 72
Şekil 5.12. Video1 dosyası için **(a)** Veri gizlenmemiş videonun histogram grafiği **(b)** Sıralı şekilde 30 KB veri gizlenmesiyle oluşan videonun histogram grafiği **(c)** Rastgele şekilde 30 KB veri gizlenmesiyle oluşan videonun histogram grafiği 73
Şekil 5.13. Video1 dosyası için **(a)** Veri gizlenmemiş videonun histogram grafiği **(b)** Sıralı şekilde 120 KB veri gizlenmesiyle oluşan videonun histogram grafiği **(c)** Rastgele şekilde 120 KB veri gizlenmesiyle oluşan videonun histogram grafiği ... 73
Şekil 5.14. Video1 dosyası için **(a)** Veri gizlenmemiş videonun histogram grafiği **(b)** Sıralı şekilde 450 KB veri gizlenmesiyle oluşan videonun histogram grafiği **(c)** Rastgele şekilde 450 KB veri gizlenmesiyle oluşan videonun histogram grafiği ... 74
Şekil 5.15. Video2 dosyası için **(a)** Veri gizlenmemiş videonun histogram grafiği **(b)** Sıralı şekilde 0,1 KB veri gizlenmesiyle oluşan videonun histogram grafiği **(c)** Rastgele şekilde 0,1 KB veri gizlenmesiyle oluşan videonun histogram grafiği 75

Şekil 5.16. Video2 dosyası için **(a)** Veri gizlenmemiş videonun histogram grafiği **(b)** Sıralı şekilde 30 KB veri gizlenmesiyle oluşan videonun histogram grafiği **(c)** Rastgele şekilde 30 KB veri gizlenmesiyle oluşan videonun histogram grafiği **.....** 75
Şekil 5.17. Video2 dosyası için **(a)** Veri gizlenmemiş videonun histogram grafiği **(b)** Sıralı şekilde 120 KB veri gizlenmesiyle oluşan videonun histogram grafiği **(c)** Rastgele şekilde 120 KB veri gizlenmesiyle oluşan videonun histogram grafiğii **..** 76
Şekil 5.18. Video2 dosyası için **(a)** Veri gizlenmemiş videonun histogram grafiği **(b)** Sıralı şekilde 450 KB veri gizlenmesiyle oluşan videonun histogram grafiği **(c)** Rastgele şekilde 450 KB veri gizlenmesiyle oluşan videonun histogram grafiği **...** 76

ÇİZELGELER DİZİNİ

Çizelge 3.1. Video steganografi yöntemlerinin karşılaştırılması 45
Çizelge 5.1. Video 1 değerleri 66
Çizelge 5.2. Video 1 Şifrelenmiş gizleme değerleri 67
Çizelge 5.3. Video 2 Değerleri 68
Çizelge 5.4. Video 2 Şifrelenmiş gizleme değerleri 69
Çizelge 5.5. Video 3 Değerleri 70
Çizelge 5.6. Video 4 Değerleri 71

BÖLÜM 1

GİRİŞ

Tüm dünyada olduğu gibi ülkemizde de bilgi teknolojileri konusunda çağımızdan kaynaklı hızlı bir ilerleme söz konusudur. Özellikle iletim hızındaki artış ve bu hızın oldukça önemli bir hal almasının yanı sıra ağ üzerindeki cihazlarının sayısının artması ile birlikte bilgi ve bilgi iletiminin çağımızda çok önemli bir unsur olduğu bir gerçektir (Şatır, 2013).

Tüm bu unsurlar göz önünde bulundurulduğunda, günümüzde en önemli unsurlardan biri olan bilgiyi tanımlamak, kavramak ve incelemek oldukça önemli bir konu haline gelmiştir. Bu açıdan bakıldığı günümüze kadar geçen süreçte ileriye yönelik gelişimimizi şekillendirmenin en önemli anahtarı bilgidir (Canbek, 2005).

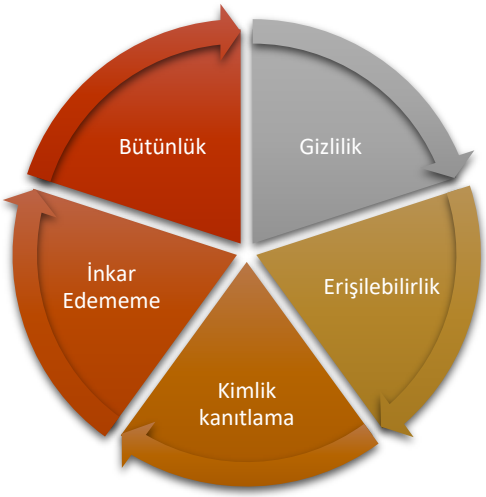
Bilgi ve veri ise birbirinden farklı kavramlardır. Bilgi; toplanmış olan verilerin işlenerek anlamlı hale getirilmiş halidir yani işlenmiş veri olarak da ifade edilebilmektedir. Veriler ise kendi başlarına anlam içermeyen, çeşitli yöntemler kullanılarak elde edilen işlenmemiş bilgilerdir.

1.1. Bilgi Güvenliği

Teknolojinin gelişiminin sürekli ve hızlı bir şekilde ilerlemesi ile birlikte bilgi güvenliği son yıllarda oldukça önemli bir konuma gelmiştir. Bilgiye erişimin kolaylaşması ve bilgi miktarının artması ile birlikte de bilgi güvenliği konusu dünya üzerinde önemli bir sorun haline gelmiştir.

Bilgi güvenliği kavramı, var olan bilgilerin izinsiz veya yetkisiz kişiler tarafından erişilerek bu bilgilerin engellenmesi, değiştirilmesi, dağıtılması, yok edilmesi, kullanılmasını engellemek amacı ile saklanması ya da iletilmesi için yapılması gerekli olan işlemler olarak tanımlanmaktadır (Banupriya, & Suganthi, 2019).

Bilgi güvenliği kavramı, gizlilik, bütünlük, erişilebilirlik, kimlik kanıtlama ve inkâr edememe olarak beş temel unsurdan oluşmaktadır.

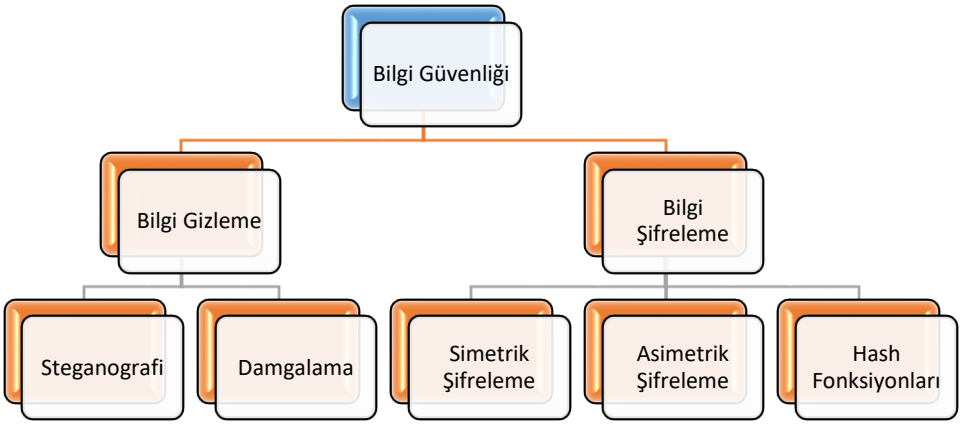


Şekil 1.1. Bilgi güvenliği unsurları

Gizlilik kavramı var olan bilgi ya da kaynakların yetkisiz kişilerden gizlenmesi anlamına gelmektedir. Bütünlük kavramı bilginin bir bütün olarak değerlendirilerek değiştirilmeden saklanması ve korunması demektir. Erişilebilirlik kavramı ise bilginin sadece yetkili kişiler tarafından ihtiyaç duyulduğu durumlarda ulaşılabilmesi ve kullanılabilmesi anlamına gelmektedir. Kimlik kanıtlama kavramı iletişim sırasında gönderici ve alıcının doğru kişiler olması anlamına gelmektedir. İnkâr edememe kavramı ise bilgiyi kullanan kişilerin bu bilgileri kullandığını ret edememesi anlamına gelmektedir.

Bilgi güvenliği kavramındaki bu temel unsurların dışında kullanılan başka sorumluluk, erişim denetimi, güvenilirlik ve emniyet gibi destekleyici unsurlarda mevcuttur.

Bilgi güvenliği sistemini kendi içerisinde bilgi gizleme ve bilgi şifreleme olarak ayırabilmek mümkündür. Bilgi gizleme kavramı içerisinde bilginin gizlenmesi için kullanılan steganografi ve damgalama teknikleri bulunurken bilgi şifreleme kavramında bilginin anlamsız bir forma dönüştürülmesini sağlayan simetrik ve asimetrik şifreleme teknikleri bulunmaktadır.



Şekil 1.2. Bilgi güvenliği sistemi

1.2. Bilgi Gizleme

Antik çağlardan bu yana insanların ihtiyaç duyduğu ve bilgi güvenliği sağlama amacı ile kullanılan gizli haberleşme, teknolojinin değişmesi ve gelişmesi ile birlikte kullanılan yöntemler açısından değişimler göstermiştir (Akbal, 2008).

Teknoloji ve internet kullanımının son yıllarda önemli ölçüde artması ile birlikte bilgi güvenliği kavramı ve bilgisayar sistemlerinin güvenliği oldukça önemli bir konu haline gelmiştir. Özellikle bilgi paylaşımı sırasında resim, video, metin ve ses vb. gibi birçok bilgi ve mesajlar içeren dosyalar, internetin kullanımının iyice yaygınlaşması ile önemli ölçüde artmıştır. Hayatımızı kolaylaştıran bu yapı ciddi güvenlik açıklarına da sebebiyet vermiştir.

Karşılıklı olarak veri alışverişinde bulunan iki taraf arasındaki iletişim hattına dışarıdan bir başka kişi erişebilmekte ve istediği takdirde verileri ele geçirebilmekte, değiştirebilmekte ya da yeni veriler üretebilmektedir. Bu durumda haberleşme sürecinde hatalar oluşmasına neden olmaktadır. Veri iletişiminin güvenli bir şekilde yapılabilmesi için bilgi güvenliği önemli bir konudur. Veri güvenliğinin sağlanması ve yetkisiz erişimlerin engellenebilmesi için koruma ve önleme yöntemleri geliştirilmiştir. Bilgi gizleme ve şifreleme yöntemleri bu sürecin en önemli bileşenleri olarak karşımıza çıkmaktadır.

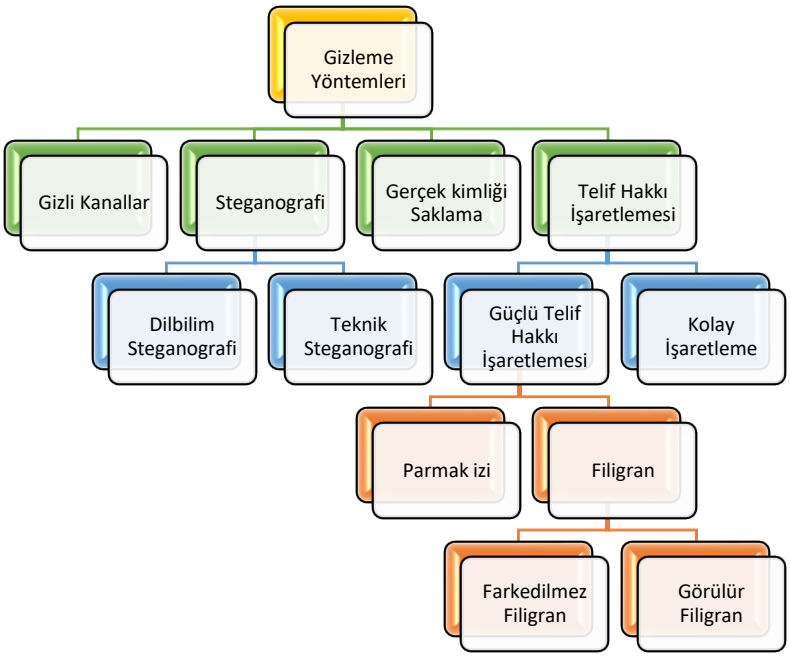
Şifreleme gizlenmesi istenen açık metinlerin anahtarlar vasıtası ile anlaşılmaz hale getirilmesini ifade eder. Bilgi gizleme ise iletişimin varlığını gizlemeyi amaçlamaktadır.

Şifreleme ve steganografi tek başlarına kullanılabilecekleri gibi birlikte kullanıldıklarında daha güçlü ve güvenli bir iletişim sağlayabilirler.

Bilgi gizleme özellikle günümüzde iletişim güvenliği açısından oldukça önemli bir konu haline gelmiştir. Bilgi gizlemedeki amaç bilgiye ulaşmak isteyen üçüncü kişilerin bu bilginin varlığını fark etmemesini sağlamaktır. Bilgi gizleme kavramı, karşı tarafa iletilecek olan bilginin önemli olduğu alanlarda sıklıkla kullanılmaktadır (Şahin, 2007).

Şifreleme ise bilgiye ulaşmak isteyen üçüncü kişiler gizli bir bilginin varlığından haberdardır, bilgi gizleme yöntemlerinin şifrelemeden farkı ise kişiler arasında gerçekleştirilen iletişimin gizli bir şekilde yapılmasını sağlayabilmesidir. Bilgiye ulaşmak isteyen üçüncü kişiler iletişim sırasında gizli bir iletişim olduğunu fark edememektedir (Şahin, 2007).

Antik çağlardan itibaren insanoğlu tarafından kullanılmaya başlanılan bilgi gizleme alanında, teknolojinin hızla ilerlemesi ile günümüzde de birçok yeni teknik geliştirilmiştir ve hala geliştirilmeye devam edilmektedir (Katzenbeisser & Petitcolas, 2000).



Şekil 1.3. Bilgi gizleme

Gizli Kanallar tekniği haberleşen kişiler arasında var olan gizli bilgilerin güvenli bir şekilde el değiştirmesi için gerekli olan iletişimi sağlayan kanallardır. İki kişinin gizli kanalları kurabilmesi için önceden aralarında karşılıklı olarak anlaşması gerektirmektedir. Gizli kanalların kullanılmasındaki amaç ise iletişimin gerçekleşme amacıyla birlikte iletişim sırasındaki veriyi saklamaya çalışmaktır. Bu şekilde yapılan iletişim sonrasında ise iletim yapılan gerçek verilerin transferi normal ve dikkatsiz gözler için zararsız görülebilecektir. Gizli bilgileri gönderecek ve alacak kişiler arasında verileri karıştırabilmek için ayrıca bir şifreleme sistemi yapmalarına gerek kalmamaktadır. Gizli Kanallar, dosya tabanlı steganografi (görüntü, ses, vb.), ağ paket steganografisi ve protokol kapsüllenmesi gibi çeşitli alanlarda kullanılabilmektedir.

Gerçek kimliği saklama tekniği bilginin zarar görmeden gönderebilmesindeki yöntemlerden bir tanesidir. Bu yöntemde veri transferi gönderici ve alıcı arasına gerçek kimlik saklanarak farklı ve bilinmeyen bir kişi üzerinden gönderiliyor gibi gözükmektedir. Bu yöntemdeki olumsuz nokta ise farklı ve bilinmeyen bir kişi üzerinden gönderiliyor gibi gözükmesi ağ üzerinde izleme sırasında fazla dikkat çekmektedir. Bu sebepten dolayı sadece çok gerekli olduğu durumlarda kullanılması önerilmektedir.

Telif hakkı İşaretlemesi steganografi ile kullanılan bir yöntemidir. Aynı zamanda dijital ortam dosyalarında filigran olarak da kullanılabilmektedir. Orijinal dosyaları koruyabilmek amacıyla bazı bilgiler bu dosyaların içine gizlenmektedir. Bu bilgilerin arasında; telif hakkı sahibi, dosyaların üretim tarihi vb. bilgiler bulunmaktadır. Modern steganografi uygulamalarında ise dosyaların kopyalanmasını engellemek amacı ile kullanılmaktadır (Şahin, 2007).

Steganografi bilgi gizleme yöntemlerinin en önemli alt dallarından bir tanesidir. Steganografi kavramı verilerin üçüncü kişiler tarafından fark edilmeyecek ortamlara saklanarak iletişimin gizli bir şekilde yapılmasını sağlayan bir disiplin olarak tanımlanabilir.

Bilgi gizleme yöntemlerinden biride damgalama yöntemidir. Damgalama kavramı, başka kişiler tarafından kullanılması istenilmeyen verilerin damga adı verilen güvenlik amaçlı kullanılan bir bilgi ile birleştirilmesi işlemidir. Damgalama yöntemi kullanıldığında herhangi bir veri kaybına sebep olmamaktadır. Damgalama işlemi şifreleme işlemi ile birleştirildiğinde daha güvenli bir hale gelmektedir. Damgalama

yöntemi kullanıldığında bu işlemin yetkisiz kişiler tarafından tespit edilmesi istenilen bir durum değildir. Gizlenmek istenilen veri damgalandıktan sonra tespit edilip damga kaldırılırsa damgalanmış veri bozulup işe yaramayacak hale gelebilmektedir.

Damgalama yöntemleri kendi içerisinde iki gruba ayrılmaktadır. Bunlar dayanıklı damgalama ve kırılgan damgalama yöntemleridir. Dayanıklı damgalama uygulamalarında gerçekleştirilen saldırılar sonrasında taşıyıcı içerisinde bulunan gizli bilginin bu saldırılar karşısında etkilenmemesi sağlanmalıdır yani taşıyıcıya eklenen veriler koruma altında tutulmaya çalışılmalıdır. Kırılgan damgalama yönteminde ise orijinal dosyaya yerleştirilen damga dosya üzerinde yapılan en ufak bir değişim ile bozulmaya uğramaktadır. Bu sayede eklenen veri aracılığı ile değişiklik yapılıp yapılmadığı tespit edilebilmektedir (Üstübioğlu, Ulutaş & Üstübioğlu, B., 2017).

Bilgi gizleme alanında kullanılmakta olan bu iki kavram aslında birbirlerinden gizlenen verinin kullanım amacı sebebiyle oldukça farklıdır. Steganografi yönteminde gömülecek olan veri taşıyıcı veriden tamamen bağımsızdır. Gizli kanal üzerinden haberleşen kullanıcılarının mesajları içermektedir. Damgalama yönteminde ise gizlenen veri ya telif haklarına dair bir bilgidir ya da bütünlük kontrolü sağlayan bir bilgidir.

Steganografi yöntemlerinde gizleme işlemi için en önemli nokta gizlenecek olan verinin algılanamaz olması ve tespit edilememesidir. Damgalama yöntemlerinde ise algılanamaz olmasının yanı sıra dayanıklılık özelliği oldukça önemlidir. Fark edilmezlik özelliği ise olmazsa olmaz bir unsur değildir. Dayanıklılık özelliği damgalama yöntemlerinde damganın çıkartılamaması anlamına gelmektedir. Hem steganografi hem de damgalama da ki ortak özelliklerden biri olan algılanamaz olması ise insan duyu organları ile algılanamaz olmayı ifade etmektedir (Yargıçoğlu, 2010).

1.3. Bilgi Şifreleme

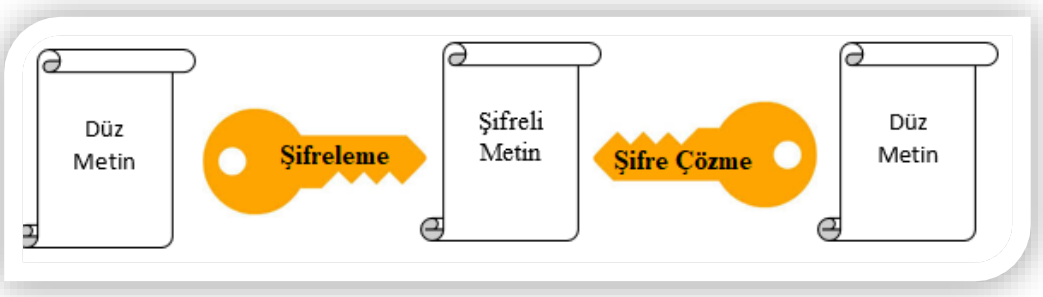
İnsanoğlunun yazıyı icat etmesinden günümüze kadar geçen süreden insanlar haberleşme sırasında gizliliğe her zaman önem vermişlerdir. Bu sebepten dolayı haberleşme sırasında gizleme işlemi için yeni yöntemler geliştirmiştir. Tarih boyunca devletler hayati önem taşıyan bilgilerin düşmanlarının eline geçmesini engelleyebilmek için bu bilgileri kodlama yöntemi uygulamışlardır.

Kriptografi, kökeni Yunanca olan “kryptos” gizli saklı ve “graphein” yazmak anlamına gelen sözcüklerin birleşiminden türetilmiştir. Kriptografinin bilgi güvenliğini sağlamak amacıyla kimlik denetimi, gizlilik ve bütünlük gibi yöntemleri bulunmaktadır ve mevcut olan bu yöntemler sayesinde gönderilecek olan bilgilerin alıcıya ulaşana kadar olası saldırılardan korunmasını sağlamaktadır. Kısaca kriptografi kavramı ele geçirilen bilgilerin anlamsız hale getirilerek istenmeyen kişiler tarafından okunmasını engellemek amacı ile kullanılan tekniklerim tamamıdır (Çimen, Akleylek & Akyıldız, 2007).

Kriptoanaliz yöntemi ise istenmeyen kişiler tarafından ele geçirilmiş şifrelenmiş halde olan yani anlamsız metinlerden gerçek metne ulaşmak için kullanılan yöntemlerdir (Özyılmaz, 2014). Şifreli metine ulaşan kriptoanaliz ile uğraşan kişilerin gerçek metne ulaşmak için kriptografi algoritmalarında kullanılan gizli anahtarın tamamına ya da belli bir kısmına ihtiyaç duymaktadır (Demiröz, 2021).

Kriptoloji, hem kriptografi, hem kriptoanalizi kapsayan bir bilim daldır. Kriptografinin amacı, ileti güvenliğini sağlamak, kriptoanalizin amacı ise var olan şifreleri kırmaktır. Aynı zamanda şifreleme algoritmalarına yapılan saldırılar ile daha güçlü şifreleme algoritmalarının tasarımına yardımcı olmaktır. Şifrelenmiş olan belgeleri ve gizlenmiş yazıları konu edinen bir incelemedir. Kriptolojiye kısaca bir şifre bilimi denebilir (Özyılmaz, 2014).

Kriptolojinin kavramlarından biri olan şifreleme gizlenmek istenen metnin içeriğinin anlamsız hale getirilmesi işlemidir. Şifrelemenin amacı gizlenen metnin başka bir kişi ya da kişiler tarafından okunmasını engellemektir. Şifre çözme işlemi ise anlamsız hale getirilmiş olan metni tekrardan anlamlı hale getirmek için kullanılmaktadır.



Şekil 1.4. Bir düz metnin şifrelenmesi ve şifre çözme işlemi

Şifreleme biliminin temel özellikleri 3 temel kavram altında incelenebilmektedir. Bu kavramlar veri gizliliği, veri bütünlüğü ve kimlik denetimidir. Veri gizliliği kavramı gönderilen verinin yetkisiz kişilerin eline geçse dahi bu kişiler tarafından okunup anlaşılmasını engellemek olarak ifade edilmektedir. Veri bütünlüğü kavramı gönderilen verinin yetkisiz üçüncü kişiler tarafından değiştirilmesini engellemek olarak ifade edilmektedir. Kimlik denetimi kavramı ise gönderilen verinin doğru alıcı tarafından alındığını garanti edilmesi anlamına gelmektedir.

Kriptoloji de kullanılan temel kavramlar ise şu şekildedir;

Düz Metin: Gönderilen mesajın orijinal halidir. Yani şifreleme işleminden geçmemiştir.

Şifreli Metin: Gönderilen mesajın şifreleme işlemlerinden geçmiş halidir.

Anahtar: Mesajı şifreleme ve şifre çözme işlemleri için sadece gönderici ve alıcının bildiği bilgilerdir.

Şifreleme: Bir düz metnin içeriğinin anlamsız hale getirilmesi işlemidir.

Şifre çözme: Şifrelenmiş metnin çözülmesi yani tekrar anlamlı hale getirilmesi işlemidir.

Simetrik Algoritmalar: Şifreleme ve şifre çözme işlemlerinin aynı anahtarın kullanılarak yapıldığı algoritmalardır.

Asimetrik Algoritmalar: Şifreleme ve şifre çözme işlemleri yapılırken farklı anahtarların kullanıldığı algoritmalardır.

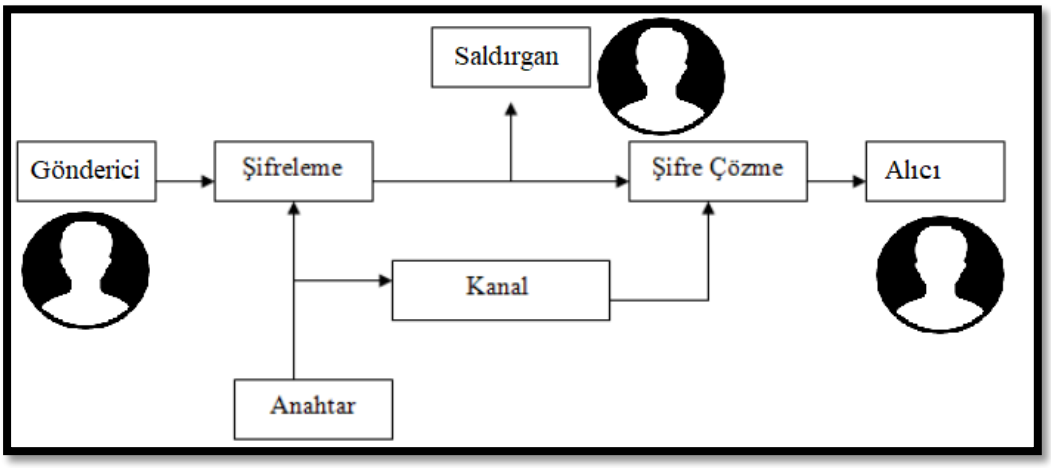
Gönderici: İletişim sırasında bilgiyi alıcıya gönderen kişidir.

Alıcı: İletişim sırasında bilgiyi alan kişidir.

Saldırgan: Gönderici ve alıcı arasındaki iletişimde, mesajı ele geçirerek güvenliği ihlal etmeye çalışan zararlı kişidir.

Saldırı: Bir kriptosistemin tamamını ya da belirli bir kısmını kırmak için yapılan işlemlerdir. Saldırılar sistemi kırmak, şifreli mesajı elde etmek ya da benzersiz anahtarı elde edebilmek anlamında başarılı veya başarısız olabilmektedir.

Kanal: Bilginin göndericiden alıcıya taşınmasına yardımcı olan kişi veya araçtır.



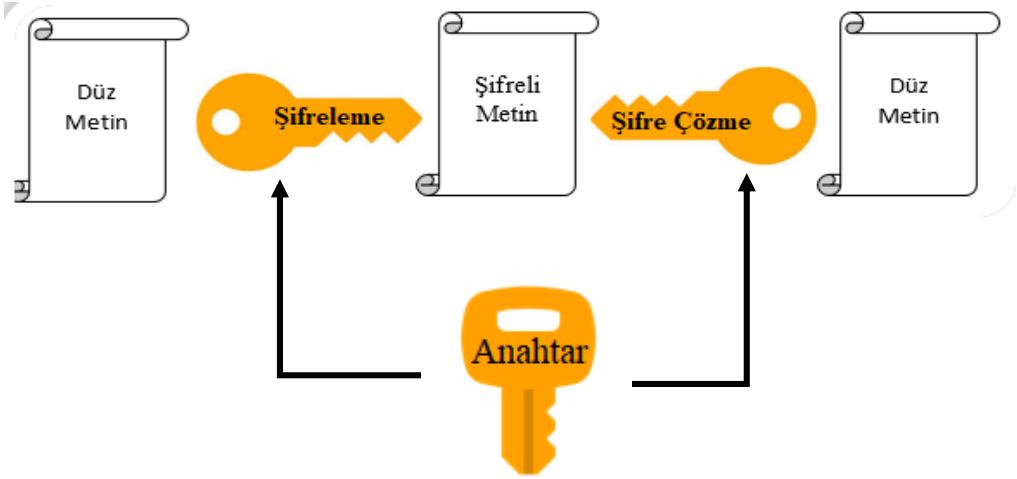
Şekil 1.5. Haberleşme sistemi

Kriptoloji alanında kullanılmakta olan şifreleme algoritmaları kendi içerisinde simetrik şifreleme, asimetrik şifreleme ve hash fonksiyonları olmak üzere kategorilere ayrılmaktadır.

Şifreleme algoritmaları arasında en iyi bilinen ve en eski teknik simetrik şifreleme algoritmalarıdır. Günümüzde şifreleme ve şifre çözmedeki hızından dolayı yaygın bir şekilde kullanılmaktadır.

Simetrik Şifreleme algoritmalarda tek bir anahtar kullanılmaktadır. Bu anahtar hem mesajın şifrelenmesinde hem de çözülmesinde kullanılmaktadır.

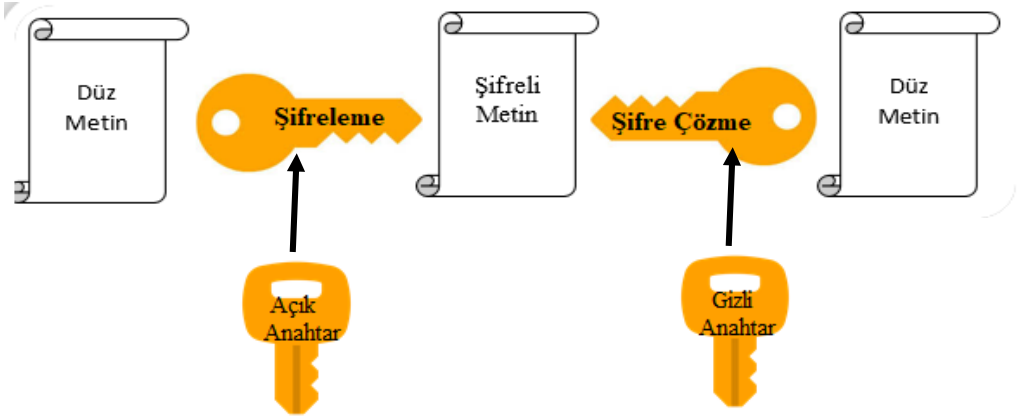
Düz metin üzerinde şifreleme işlemi yapıldıktan sonra şifreli metin ve anahtarı birlikte güvenli bir şekilde alıcıya gönderilmesi gerekmektedir.



Şekil 1.6. Simetrik şifreleme algoritması

Simetrik şifreleme algoritmalarının çeşitli algoritmaları bulunmaktadır. Simetrik şifreleme algoritmaları açık metni nasıl şifrelediklerine göre de blok şifreler ve akış şifreler olarak ikiye ayrılmaktadır. Simetrik şifreleme algoritmalarına örnek olarak DES (Data Encryption Standart - Veri Şifreleme Standardı) (FIPS 46-3, 1999), Blowfish (Schneiner, 1993), AES (Advanced Encryption Standart - Gelişmiş Şifreleme Standardı) (FIPS 197, 2001), RC4 (ARCFOUR) (Rivest R.L.1992) verilebilir. (Demiröz, 2021).

Açık anahtarlı sistemlerde simetrik şifrelemelerden farklı olarak iki anahtar kullanılmaktadır. Bu anahtarlar açık ve gizli anahtarlardır. Bu anahtarlardan açık anahtar herkese açılabilirken, gizli anahtar sadece sahibinde bulunmaktadır. Bu anahtarlardan açık anahtar ile şifreleme işlemi gerçekleştirilirken gizli anahtar ile de şifre çözme işlemleri gerçekleştirilmektedir. Bu iki anahtar çifti birbirleriyle bağlantılıdır. Gizli anahtarın ise sadece bir sahibi vardır. Şifreleme işleminde kullanılan anahtarın gizli olması gerekmez. Bunun sebebi asimetrik şifreleme mantığından kaynaklıdır. Asimetrik şifreleme de açık anahtar verilmesine rağmen şifre çözme anahtarı olarak kullanılan gizli anahtarın bulunmasının zor olmasıdır. Açık anahtarlı sistemler anahtar değişim protokolleri ve sayısal imza gibi uygulamalarda kullanılmaktadır. Asimetrik şifreleme yöntemlerine örnek olarak Diffie-Helman (Diffie & Hellman, 1976) ve RSA (Rivest R.L. vd., 1978) verilebilir.



Şekil 1.7. Asimetrik şifreleme algoritması

Hash fonksiyonları ise mesaj özeti oluşturmak için kullanılırlar. Sayısal imza, mesaj bütünlüğü kontrolü için sıklıkla kullanılmaktadırlar. Hash fonksiyonlarına örnek olarak MD5 (Rivest & Dusse, 1992) ve SHA (FIPS 180-4, 2012) verilebilir.

1.4. Tezin Önemi

İnternet kullanımının gelişen teknolojiyle birlikte hızla ilerlemesi ile internet üzerinden veri paylaşım oranları artış göstermektedir. Resim, metin, video, ses vb. dosyaların internet ağları üzerinden paylaşımı gerek sosyal hayat gerekse iş hayatındaki kullanımlar sebebi ile yaygınlaşmıştır. Bu tür bilgi paylaşımları her ne kadar hayatımıza kolaylıklar getiriyor olsa da bilgi güvenliği açısından ciddi sorunlar ortaya çıkartmaktadır.

Paylaşılan dosyaların üçüncü kişilerin eline geçmesini engellemek ve iletişimdeki güvenliği sağlamak adına bilgi güvenliği konusu altında veri şifreleme ve veri gizleme konuları önem kazanmaktadır. Veri şifreleme bilgileri anlamsız hale getirmek amacı ile işlemler yaparken veri gizleme ise bilgileri gizleme işlemleri gerçekleştirmektedir.

Teknolojinin hızla gelişmeye devam etmesi ile birlikte veri gizleme işlemlerine olan talep her geçen gün arttırmakta ve bu alanda birçok yeni teknik geliştirilmeye devam etmektedir.

Doktora tez çalışması olarak gerçekleştirilen bu çalışmada video steganografi teknikleri incelenmiş ve bilgi güvenliği alanına katkıda bulunarak bu alanda yeni bir yaklaşım ortaya çıkarmak amacı ile bir çalışma gerçekleştirilmiştir.

1.5. Tezin Amacı

Günümüzde teknolojinin gelişmesi ile bilgi güvenliği alanında da sorunlar artış göstermektedir. Verilerin izinsiz kullanılması, ver, hırsızlığı yapılması vb. durumlar ile başa çıkabilmek için veri gizleme ve veri şifreleme tekniklerine ihtiyaç duyulmaktadır.

Özellikle sosyal medya kullanımının giderek yaygınlaşması ile dosya paylaşım oranları artmakladır. Bilgileri gizleme tekniklerine steganografi adı verilmektedir. Steganografi de gizlenen ortamın türüne göre farklı isimler alabilmektedir. Steganografide amaç gizlenen bilginin varlığının tespit edilememesidir.

Video dosyalarının gizleme kapasiteleri yüksek olduğundan dolayı steganografi alanında tercih edilmektedir. Video steganografi de sıkıştırılmış ve ham video dosyalarına bilgi gizleme işlemleri gerçekleştirilebilmektedir.

Gerçekleştirilen doktora tez çalışmasında video dosyaları üzerinde gizlenen verinin varlığının tespit edilememesi amacı ile En Önemsiz Bite Ekleme (Least Significant Bit Insertion - LSB) yöntemi kullanılarak AVI formatındaki video dosyaları üzerine gizlenen sıralı ve rastgele bir şekilde bilgi gizlenmesi yapılmış ve bu gizleme işlemleri şifreleme teknikleri ile güvenliği arttırmak amacı ile desteklenmiştir.

Önerilen gizleme işlemlerin yapılabilmesi ve sonrasında analiz edilebilmesi için bir yazılım geliştirilmiştir.

1.6. Tezin Yapısı

Hareketli görüntü dosyalarında bilgi gizlemede kullanılan yöntemlerin incelenmesi ve yeni bir yöntemin geliştirilmesi adlı doktora tez çalışması altı bölümden oluşmaktadır.

Birinci bölümde bilgi güvenliği, bilgi gizleme ve bilgi şifreleme kavramları ve bu kavramlarının özelliklerinden bahsedilmiştir.

İkinci bölümde steganografi kavramı anlatılmış, özellikler, kullanım alanları ve çeşitlerinden bahsedilmiştir.

Üçüncü bölümde video steganografi kavramı anlatılmış, özellikleri ve yöntemlerinden bahsedilmiştir.

Dördüncü bölümde steganografik sistemin değerlendirilmesi için gerekli yöntemler ile ilgili bilgilendirme yapılmıştır.

Beşinci bölümde En Önemsiz Bite Ekleme yöntemi kullanılarak sıralı veya rastgele bilgi gizleme işlemi yapan ve geliştirilen steganografik sistemin değerlendirilmesini yapabilmek için ölçümler gerçekleştiren program anlatılmıştır.

Son bölümde sonuçların değerlendirmesi yapılmıştır.

1.7. Önceki Çalışmalar ve Literatür Taraması

Akyüz, D. & Kasapbaşı, M. C. tarafından 2021 yılında yapılan çalışmada, video dosyaları üzerinde kaotik yöntem kullanılarak veri gizlenmesi gerçekleştirilmiştir. Gizleme işlemi için LSB yöntemi kullanılmış ve her piksele 1 byte veri gizlenmektedir. Videolar üzerinde çerçeve ve piksel seçimleri kaotik bir yöntem ile seçilmektedir. Gizleme işlemi sonrasında önerilen sistemin başarısı için PSNR, SSIM, SNR, MSE ve entropi yöntemleri tercih edilmiş ve elde edilen sonuçlara göre video üzerindeki bilginin anlaşılamayacak şekilde gizlendiği belirtilmiştir (Akyüz & Kasapbaşı, 2021).

Pehlivanoğlu, M. K., Savaş, B. K., & Duru, N. Tarafından 2015 yılında yapılan çalışmada video dosyaları üzerinde koblitz yöntemi ile birlikte LSB yöntemi kullanılarak veri gizleme işlemi gerçekleşmiştir. Gizlenecek olan bilgi ASCII karakterlerine dönüştürülmekte ve tek indekse sahip karakterler Koblitz Metoduyla şifrelenmektedir. Tek indise sahip bu noktaların ilgili çerçeve üzerindeki piksel değeri, kendinden sonra gelen çift indeksli ASCII karakterin ikilik tabandaki değeri ile LSB metoduyla değiştirilerek gizleme işlemi yapılmaktadır. Steganografi ve kriptolojinin birlikte kullanıldığı bu yöntemde sistemin başarısı için PSNR değeri hesaplanmış ve bu değer sınır değerinin üzerinde bulunmuştur (Pehlivanoğlu, Savaş & Duru, 2015).

Yıldız, Y., & Özcerit, A. T. Tarafından 2015 yılında yapılan çalışmada C# programlama dili kullanılarak video dosyaları üzerinde RGB ağırlık tabanlı veri gizleme

işlemi gerçekleşmiştir. Bu yöntemde gizlenmek istenilen verilerin video içerisindeki en uygun yere gizlenebilmesi video dosyaları üzerinde hareketsiz ya da hareketli, renk yoğunluğunun fazla ya da az olduğu alanların tespit etmek amacı ile histogram yöntemi tercih edilmiştir. Sistemin başarısını ölçmek için PSNR değeri hesaplanmıştır (Yıldız & Özcerit, 2015).

ÇITLAK, S. Tarafından 2020 yılında yapılan çalışmadan Python programı kullanılarak steganografi ve steganaliz işlemleri gerçek zamanlı ham videolar için yapılmış ve ham videolar üzerinde veri gizleme işlemi için SURF ve SIFT algoritmaları kullanılmıştır. Bu algoritmaların performans değerlendirilmesi yapılmıştır. Gerçekleştirilen yöntemde veri gizleme sisteminin başarısı için PSNR değeri hesaplanmış ve yöntemin başarısının yüksek olduğu belirlenmiştir (Çıtlak, 2020).

Dixit, M., Bhide, N., Khankhoje, S., & Ukarande, R. Tarafından 2015 yılında yapılan çalışmadan video dosyalarında bilgi gizleme amacıyla LSB yöntemi kullanılmıştır. Bu yöntemde gizlenilmesi istenilen veriler, taşıyıcı video karesinin piksellerinin LSB konumlarında değiştirilmesi işlemi ile gizlenmiştir. Gerçekleştirilen sistemin başarısını ölçmek için PSNR ve MSE değerleri hesaplanmıştır (Dixit, Bhide, Khankhoje & Ukarande, 2015).

Mstafa, R. J., & Elleithy, K. M. Tarafından 2017 yılında yapılan çalışmada çok sayıda hem sıkıştırılmış hem de ham video steganografi yöntemlerinin incelenmesi ve kapsamlı analizleri yapılmış ve bunların performans değerlendirmelerini sunulmuştur. Yapılan çalışmada İlk olarak, sıkıştırılmış video steganografi teknikleri daha sonra da ham video steganografi teknikleri sınıflandırılarak incelenmiş ve daha sonra her alanın performansları algılanamazlık, gömme kapasitesi, saldırılara karşı sağlamlık olarak değerlendirilmiştir (Mstafa & Elleithy, 2017).

Chandel, B., & Jain, S Tarafından 2016 yılında yapılan çalışmada dijital video steganografi teknikleri için kullanılan yaygın yaklaşımların ve araçların özetlenmesi yapılmıştır. Dijital video dosyaları üzerinde yaygın olarak kullanılan video steganografi yöntemlerinin arasında her yöntemin güçlü ve zayıf yönleri değerlendirilmiş ve bu yöntemleri arasında bir karşılaştırma gerçekleştirilmiştir (Chandel & Jain, 2016).

Rajalakshmi, K., & Mahesh, K. Tarafından 2017 yılında yapılan çalışmada saldırganların gizli bilgileri fark etmesini azaltmak amacı ile Patch wise Kod Oluşturma

tekniklerini kullanarak video dosyasını başka bir video içinde gizlemek için video steganografi yöntemi kullanılmıştır. Gerçekleştirilen sistemin başarısını ölçmek için PSNR ve MSE değerleri hesaplanmıştır (Rajalakshmi & Mahesh, 2017).

Manisha, S., & Sharmila, T. S. Tarafından 2019 yılında yapılan çalışmada Audio Video Interleave videoları için veri gizleme ve çıkarma yöntemi önerilmiştir. Bu yöntemde iki seviyeli bir şifreleme sağlanmaktadır. Görüntü Bitmap dosyası içine gömülmekte ve gömülen gizli görüntünün baytlarını bölünmektedir. Daha sonra da videonun içine yerleştirilmektedir. Böylece daha yüksek düzeyde şifreleme yapma amaçlanmaktadır (Manisha & Sharmila, 2019).

Banupriya, R., Deepa, J., & Suganthi, S. Tarafından 2019 yılında yapılan çalışmada video dosyaları üzerinde kriptografik teknikle uyarlanabilir veri gizleme yöntemi önerilmiştir. bu yöntemde videolar kaos şifreleme algoritması kullanarak şifrelenmektedir. Ayrıca bu yöntemde gizli bir metin verisini şifreli metne şifrelemek için RC7 Şifreleme tekniği kullanılmaktadır. Şifreleme işleminden sonra LSB gömme algoritmasını kullanarak gizli şifreli verileri seçilen çerçeveye gizlemektedir (Banupriya, Deepa, J & Suganthi, 2019).

Ramalingam, M., Isa, N. A. M., & Puviarasi, R Tarafından 2020 yapılan çalışmada, video dosyaları üzerinde afine dönüşüm tekniğini kullanarak verileri gizlemek için steganografi yöntemi önermektedir. Bu yöntemde gizli veriler, video karelerinin tamsayı dalgacık dönüşümünün katsayılarına gömülür. Gömme işlemi sırasında piksel değerleri, Afine dönüşüm tekniği kullanılarak dağıtılmaktadır. Gerçekleştirilen yöntemde veri gizleme sisteminin başarısı için PSNR değeri hesaplanmıştır (Ramalingam, Isa & Puviarasi, 2020).

Abed, S. E., Al-Mutairi, M., Al-Watyan, A., Al-Mutairi, O., AlEnizy, W., & Al-Noori, A. tarafından 2019 yılında yapılan çalışmada video dosyaları üzerinde şifreleme ve steganografi tekniklerini içeren bir yöntem önermektedir. Bu yöntemde şifreleme için AES algoritması ve bilgileri gömmek için de LSB algoritması tercih edilmişidir. Videoların doğruluğunu ve kapasitesini etkilemeden gizli verilerin güvenlik seviyesini artırır. İlk olarak veriler şifrelenmekte ve daha sonra da gizlenmektedir. Gerçekleştirilen yöntemde veri gizleme sisteminin başarısı için PSNR değeri hesaplanmıştır (Abed, Al-Mutairi, Al-Watyan, Al-Mutairi, AlEnizy & Al-Noori, 2019).

BÖLÜM 2

STEGANOGRAFİ

Kimi kaynaklarda Türkçeye "örtülü yazma sanatı" olarak çevrilmiş olan Steganografi tarihi antik çağlara uzanan oldukça eski bir veri gizleme yöntemidir. Kökeni Yunanca olan steganografi kelimesi "örtülmüş yazı" anlamına gelmektedir (Johnson,1998).

Steganografi gizli/örtülü anlamına gelen "Steganos" ve yazım/çizim anlamında gelen "graphy" birleşiminde oluşan Yunanca kökenli bir kelimedir (Cox, Miller & Bloom, 2000).

Steganografide örtü verisi ya da örtü nesnesi olarak adlandırılan kavram içine bilgi gizlenen ortam anlamına gelmektedir. Gizleme sonrası oluşan bu ortama stego- nesnesi veya stego-metin denilmektedir (Kharrazi , Sencar & Memon, 2004) .



Şekil 2.1. Stego nesnesi

Steganografi teknik ve dilbilim steganografi olmak üzere iki alt dala ayrılmaktadır. Bu yaklaşımla resim, video ve ses gibi dijital ortamlar üzerine veri gizleme işlemi yapılabilmektedir.

Bilgi gizleme kavramının içerisinde yer alan steganografi ve şifreleme birbirlerine yakın bir kavram gibi görünse de amaç olarak birbirlerinden faklıdır.

Bu ortamlar içerisine saklanacak olan veri sadece metin olmayabilir Örneğin bir görüntü dosyasının içerisine başka bir görüntü de saklanabilmektedir (Aktaş, 2011).

11 Eylül 2001 yılında Amerika Birleşik Devletleri'nde gerçekleşen olaylardan sonra bir takım haber sitelerinde stenografinin teröristlerin iletişimlerini sırasına kullanıldığına hakkında haberler yer almıştır. İletilecek olan mesajın internet üzerinde paylaşım sitelerinde bulunan resimlere saklandığı ve bu şekilde teröristlerin iletişim kurdukları söylenmiştir (Yıldız, 2012).

Steganografi ve sayısal damgalama teknikleri arasındaki temel fark örtü verisindeki bozulmadan kaynaklanmaktadır. Steganografide veri gizleme işlemi sonrasında örtü veri üzerinde çok az seviyede bozulma oluşabilmektedir. Diğer bir bilgi gizleme yöntemi olan sayısal damgalamada ise gizlenmek istenilen mesaj örtü verisinin bir parçası olarak saklanmakta ve genel olarak örtü verisinin bozulmasına izin verilmemektedir (Kurtuldu & Arıca, 2009).

2.1. Steganografinin Tarihçesi

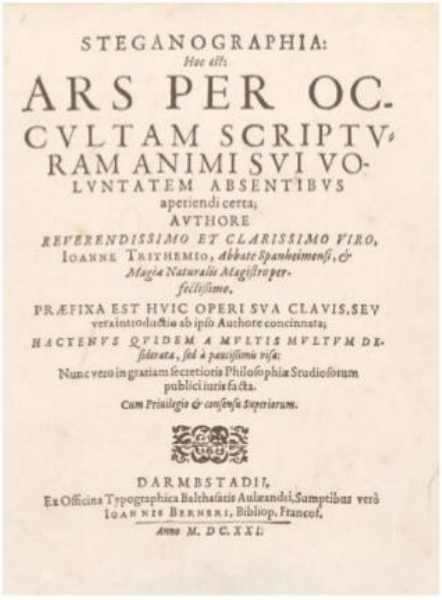
Steganografinin tarihi antik yunan zamanlarına kadar uzanmaktadır. MÖ'den başlamak üzerine tarihte steganografinin çok sayıda örneği bulunmaktadır.

Steganografinin tarihteki örneklerinden bir tanesi, Yunan tiran Histiaeus'un MÖ V. yüzyılda, başka bir yerde hapis durumundayken başka bir şehirde olan damadına gizli bir mesaj göndermek için kölelerinden birinin saçını kazıtıp dövme yaptırması ve fark edilmemesi için kölenin damadının bulunduğu yere yanında hiçbir şey olmadan ve saçı uzayınca göndermesi steganografiye örnektir. Köle damadının bulunduğu yere ulaştığında saçını kazıtarak gizli mesaj ortaya çıkmıştır (Cox vd., 2000).

Antik çağlardaki steganografi kullanımları sadece Yunanlılar üzerinden gerçekleşmemiştir çeşitli milletler de gizli haberleşebilmek için steganografiye başvurmuşlarıdır. Geçmiş zamanlarda kullanılan steganografi teknikleri genel olarak özel mürekkep ya da kimyasal maddeler kullanarak gizli yani görünemeyen yazılar yaratmaya yönelikti. Bu örneklerden bir tanesi eski Romalılar zamanına dayanmaktadır. Bu dönemde eski Romalılar kendi aralarında süt ya da meyve suyu gibi sıvılardan görünmez mürekkep oluşturarak haberleşme yapılabilmekteydi.

Johannes Trithemius'un Rönesans döneminde kriptoloji alanında yazmış olduğu kitaplarının üçleme olarak basılması tarihteki başka bir örnek olarak gösterilmektedir. Trithemius'un oluşturduğu stego metodu "Steganographia" isimli yazısıyla geçerlilik

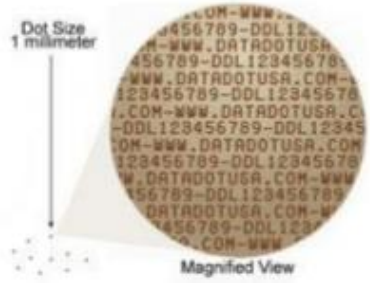
kazanarak o dönem de yaygın olarak kullanılmaya başlanmıştır. Şekil 2.2.'de kapağı gösterilen kitaptaki metot birbirini izleyen sütunlardaki kelimelerin ilk harflerini birleştirmesi yöntemine dayanmaktadır.


STEGANOGRAPHIA:
Hoc eſt:
ARS PER OC.
CVLTAM SCRIPTV-
RAM ANIMI SVI VO-
LVNTATEM ABSENTIBVS
aperiendi certa;
AVTHORE
REVERENDISSIMO ET CLARISSIMO VIRO,
IOANNE TRITHEMIO, Abbate Spanheimenſi, &
Magiæ Naturalis Magiſtro per-
feciſſimo.
PRÆFIXA EST HVIC OPERI SVA CLAVIS, SEV
vera introductio ab ipſo Authore concinnata;
HACTENVS QVIDEM A MVLTIS MVLTVM DE-
ſiderata, ſed à pauciſſimis viſa:
Nunc verò in gratiam ſecretioris Philoſophiæ Studioſorum
publici iuris facta.
Cum Priuilegio & conſenſu Superiorum.
DARMBSTADII,
Ex Officina Typographica Balthaſaris Aulæandi, Sumptibus verò
IOANNIS BERNERI, Bibliop. Francof.
Anno M. DC. XXI.

Şekil 2.2. Steganographia kitabının latince kapağı

Başka bir örnek ise müzik notaları kullanılarak nasıl bilgi gizleme yapılacağı "Schola Steganographica" adlı kitapta bahsedilmiştir. Bu kitap Gaspar Schott (1608–1666) tarafından yazılmıştır (Şahin, 2007).

İkinci Dünya Savaşı sırasında Alman ordusu mikrofilm tekniği kullanarak bir mikro-noktalama kullanmışlardır. Bu yöntemde bir A4 boyutlarında bir kâğıda yazılmış olan mesaj bir nokta kadar küçültülerek gizleme işlemi yapılmaktadır. Böylece masum görünümlü bir mesaj üzerindeki noktalar ile gizli haberleşme yapılabilmekteydi. Bu teknikte herhangi bir şifreleme tekniğine ihtiyaç duyulmamaktadır ve en önemli özelliği de fark edilmez olmasıdır (Yalman & Ertürk, 2009).



Şekil 2.3. Mikro Noktalama

İkinci Dünya Savaşı'nda denenen teknikerden bir tanesi de Boş Şifreleme olarak adlandırılan tekniktir. Boş şifreleme yönteminde gizlenecek olan mesaj sıralı ve tekrarlı olarak taşıyıcı üzerine gizlenmektedir. Bu yöntemin önemli bir başka özelliği ise gizlenecek mesajın hiçbir anlamı olmayan, örnek olarak hava durumu, alışveriş listesi, günlük notları vb. mesajların içerisinde gizlenmesidir. Bu yöntem ile birçok casus ikinci Dünya Savaşı devam ederken çok sayıda bilgi iletilmiştir (Özcan, 2016).

Boş Şifreleme (Null Cipher) Örneği:

İkinci dünya savaşı sırasında kullanılan boş şifreleme örneği şu şekildedir;

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

Çözüm: Cümle içerisinde yer alan her kelimenin sırası ile ikinci harfi alınarak gizli mesaj çıkarılır. Bu örnekteki gizli mesaj "Pershing sails from NY June 1." (Johnson ve Jajodia, 1998).

80'li yıllarda kabinesindeki gizli bilgileri dışarı sızdıran bakının kim olduğunu bulmak amacı ile İngiltere Başbakanı Margaret Thatcher kullanılan kelime işlem programını kabinede yer alan her bakan için ayrı ayrı tanımlayıcı bilgi ekleterek programlatmıştır. Yapılan bu işlem sonucunda bilgileri dışarı sızdıran bakanın kim olduğu ortaya çıkarılmıştır (Anderson & Petitcolas, 1998).

Günümüzde gelişen teknoloji ve artan veri miktarı nedene ile dijital nesneler üzerinde steganografi uygulamaları yapılmaktadır. Ses, görüntü, video ve hatta ip paketleri üzerinde verileri korumak amacıyla steganografi teknikleri sıklıkla kullanılmaktadır.

2.2. Steganografik Sistem

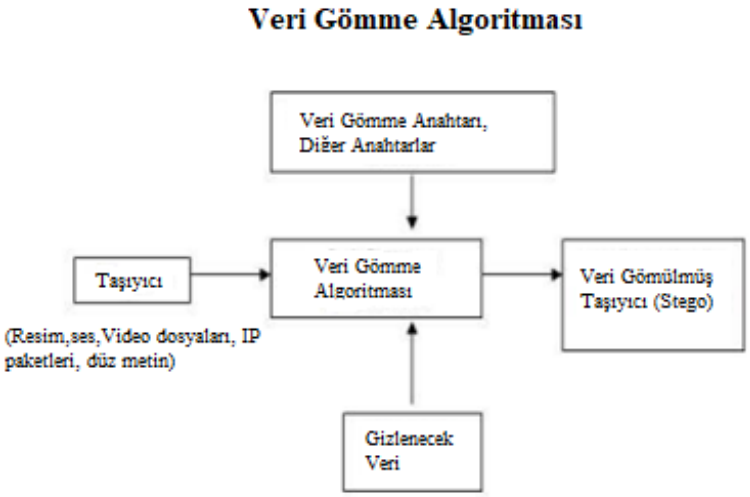
Steganografik sistem modeli (bu stegosistem olarak ta bilinir) veri ve bu veriler arasındaki ilişkileri içeren süreçleri tanımlar.

Bir steganografik sistem bileşenleri şu şekildedir.

- ***Gizli veri:*** gömülecek olan mesajdır.
- ***Taşıyıcı (Cover):*** *gömülecek* verinin başka bir veri içerisine saklanmasıdır.

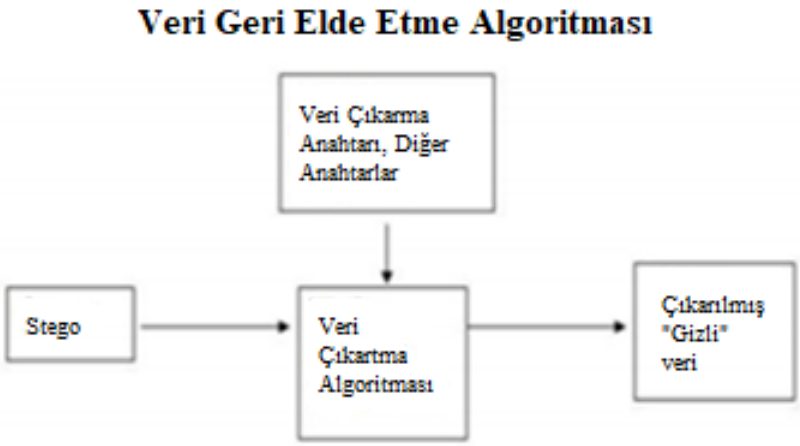
- ***stego:*** gömülmüş olan bir mesajı içeren taşıyıcıların değiştirilmiş bir versiyonudur.
- ***Anahtar (Stego-Key)***: Gönderen ve alan kişiler tarafından gömme ve geri elde etme işlemlerinde kullanılmak için gerekli olan ekstra gizli veridir.
- ***Veri Gömme Algoritması***: Parametre olarak Anahtar, gizli veri ve taşıyıcıya sahip olan ve çıktı olarak stegoyu üreten bir steganografik fonksiyondur.
- ***Veri Çıkarma Algoritması***: Parametre olarak anahtar ile stegoya sahip olan çıktı olarak gizli veriyi üreten bir steganografik fonksiyon. Bu fonksiyon Veri Gömme Algoritmasını ters fonksiyonudur.
- ***İletişim Kanalı:*** *Stego* yu herhangi bir yolla göndericiden alıcıya ulaştıran kanaldır.

Şekil 2.4.'de steganografik sistem içerisinde veri gömme işleminin gerçekleşmesi gösterilmektedir. Taşıyıcı, gizlenecek olan veri ve anahtarlar veri gömme algoritmasına girerek veri gömülmüş taşıyıcı dosya elde edilmektedir.



Şekil 2.4. Steganografik sistemde veri gömme algoritması

Sekil 2.5'de steganografik sistem içerisinde gizlenmiş olan veriyi geri elde etme işleminin gerçekleşmesi gösterilmektedir. Veri gömülmüş taşıyıcı dosya içerisindeki gizli veri, gömme algoritmasının tersi uygulanması ile yani veri çıkarma algoritması uygulanarak çıkartılmaktadır.



Şekil 2.5. Steganografik sistemde veri geri elde etme algoritması

2.3. Steganografinin Alt Alanları

Teknik ve dilbilim steganografi olmak üzere steganografinin iki ayrı alt alanı bulunmaktadır.

Taşıyıcı verinin metin olduğu steganografi alanına dilbilim steganografi denmektedir. Bu alt alanda değişiklik yapabilmek için metnin yapısının değiştirilmesi, grafik kullanılması ve amacı sadece veriyi saklamak olan yeni bir metin yaratma gibi çeşitli yolları mevcuttur.

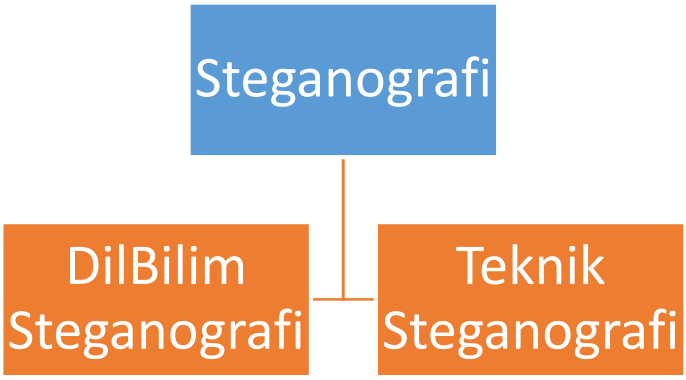
Dilbilim steganografi alanından kullanılan farklı yöntemler arasında açık kodlar ve şemagramlar en çok bilinenlerdir. Şemagram yönteminde gizlenecek olan mesaj açık metin olarak adlandırılan metinin ufak ama gizli detaylarının içerisine gizlenmesidir. Değişiklik yapabilme yolları içerisinde yer alan grafiksel değişiklikler yapılabilmektedir. Boşluk kullanmak, farklı yazıtipi kullanmak bazı yöntemler arasındadır. Açık kodlar yönteminde ise gizli mesaj okunabilir durumdadır. Bu mesaj zararsız bir hal almaktadır, bu işlem için ise boş şifreler, grid ve maskeleme ile yapılabilmektir.

Teknik Steganografi alanından kullanılan farklı yöntemler mevcuttur. Bu yöntemler ise görünmez mürekkeple yazma yöntemine görünmez mürekkep yöntemi denmektedir. Microdot adı verilen bilgiyi noktalar halinde sayfaya gizleme yöntemi de teknik steganografi yöntemlerinden biridir. Bilgiyi kimsenin göremeyeceği yerlere saklama yöntemine ise gizli yerler adı verilmektedir. Bu yöntemde gizleme yerleri olarak kasa bavul vb. yerler kullanılabilmektedir. Video, ses, resim ve metin gibi dosyalar

kullanılarak bilgi gizleme işlemi yapılan yönteme ise Bilgisayar tabanlı yöntemler denmektedir.

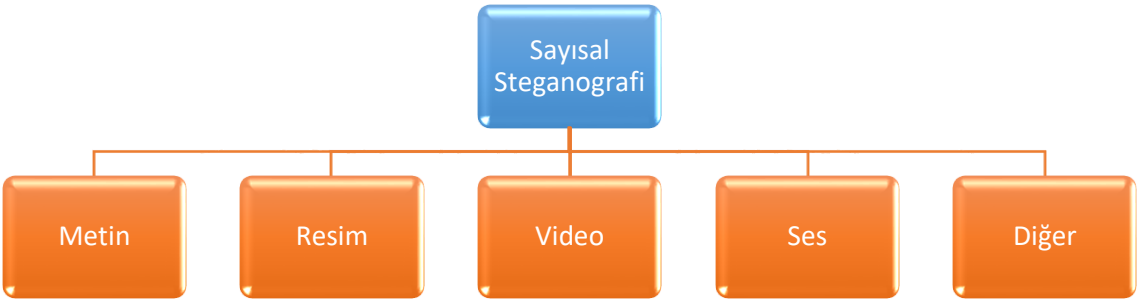
2.4. Steganografinin Kullanım Alanları

Dilbilim steganografisi altında yer alana sözlüksel steganografi kavramı sembolik bir yaklaşımdır ve bu yöntemde yapılan herhangi bir değişiklik anlatılmak istenen konunun farklı bir anlam kazanması ile kabul edilmektedir. Bu yaklaşımda metin içerisinde bulunan kelimelerin yeniden yorumlanması ve ya bu kelimelerin değiştirilmesinin şüpheli bir durum yaratıp yaratmayacağını kontrol edilmektedir. Yine dilbilim steganografisi altında yer alan Bağlam-bağımsız taklit yönteminde ise, cümle yapısı ile kelimelerin aralarındaki bağlılığın da korunarak değiştirilmesini ya da yeniden yorumlanmasını kontrol etmektedir. Dilbilim steganografisi altında yer alan başka bir yöntem olan Varlık bilimsel yöntemi cümleden anlatılmak istenen durumun, cümle içerisindeki kelimelerdeki değişimin ve cümle yapısının bir değişikliğe uğrayıp uğramadığını kontrol edilmesi şeklinde gerçekleşmektedir. Bu yöntemin kabul edilebilmesi için anlam bozulmadan yapılmış olan herhangi bir değişikliğin tüm cümlenin ve hatta metnin anlam bütünlüğünün bozmaması gerekmektedir (Şahin. A).



Şekil 2.6. Steganografi kullanım alanları

Şekil 2.5.'de sayısal steganografi alanları gösterilmektedir. Bu alanlar içerisinde metin, resim, video, ses ve diğer ortam dosyaları üzerinde gerçekleşen teknikler bulunmaktadır



Şekil 2.7. Sayısal steganografi alanları

2.5. Metin Steganografi

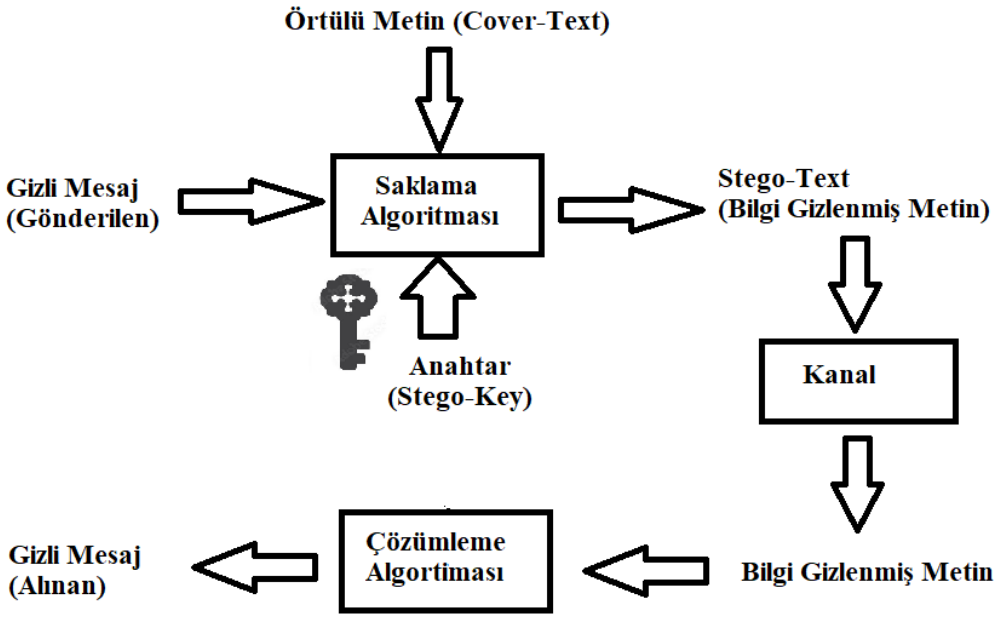
Gizli verilerin metin dosyalarına gizlendiği steganografi koludur. Verileri metin dosyalarına gizlemek için kullanılabilecek bir çok farklı yöntem bulunmaktadır. Genel olarak uygulanması zor olan bu gizleme yöntemlerinin kapasitesi düşük seviyededir çünkü metin içindeki boşluk ve gereksiz metin miktarları oldukça azdır.

Bu yöntemler arasında;

• Format Tabanlı Yöntem: Gizli veriler, metin boşlukları ekleme, kasıtlı yazım hataları, yazı tipi boyutları gibi yöntemlerle kapak verilerinin içine gizlenir. Bu yöntem bir bilgisayar yazılımı tarafından kolaylıkla tespit edilebildiği için daha az tercih edilen bir yöntemdir.

• Rastgele ve İstatistiksel Yöntem: Gizli veriler karakter dizilerinin içinde saklanır. Gizli verilerin saklandığı yerler veriyi elde edecek tarafından bildirilmelidir.

• Dilbilim Yöntemi: Gizli veriler söz dizimsel yapıda saklanır (Macit, Koyun & Güngör).



Şekil 2.8. Metin steganografi algoritması

Metin steganografi yöntemleri, verileri saklanacak yerlerinin özelliklerine göre sınıflandırılmaktadır. Bu yöntemler (Popa, 1998);

- Açık Alan Yöntemleri
  - Satır kaydırma kodlaması,
  - Satır sonu boşluk bırakma,
  - Sağa hizalama,
  - Cümle içi boşluk bırakma,
  - Gelecek kodlaması.
- Yazımsal yöntemler
- Anlamsal yöntemler

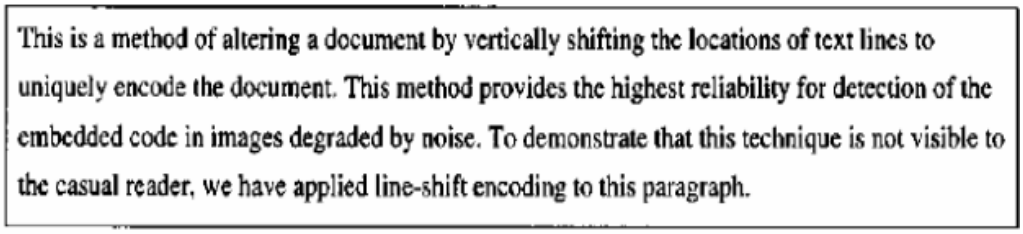
2.5.1. Açık Alan Yöntemleri

Bu yöntemler dikey olarak satırlar arası, kelimeler arası ve satır sonları ekstra boşluklar gibi teknikleri içermektedir.

Satır kaydırma kodlaması yönteminde ise gömülecek olan gizli mesaj, metin içerisindeki satırların kaydırılması işlemi ile kodlanmaktadır. Bu metin kaydırılma

işlemleri ise düşey şekilde kaydırılarak gerçekleşmektedir. Bu yöntemlerde gözle görülür bir fark olmamaktadır. Şekil 2.9.'daki örnekte ikinci satır 1/300 inç yukarıya kaydırılmıştır.

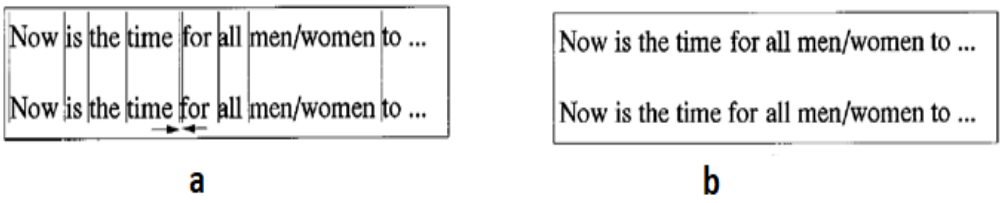
Gizlenmiş ola metinler yine metin dosyası olarak açılabilir.



Şekil 2.9. Satır kaydırma örneği

Cümle içi boşluk bırakma yönteminde veri saklama kapasitesi oldukça azdır. Bu yöntemin işleyiş mantığı kelimeler arası boşluklar ile ilgilidir. Kelimeler arası tek boşluk var ise "0" bitini, iki boşluk var ise "1" bitini saklamaktadır.

Şekil 2.10 (a)'da "for" kelimesinden önce bir boşluk eklenmektedir, Şekil 2.10 (b)'de ise for ile all arasında daha fazla boşluk vardır.



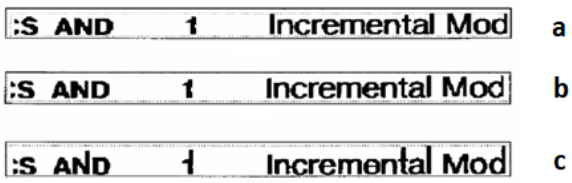
Şekil 2.10. Cümle içi boşluk bırakma örneği

Satır sonu boşluk bırakma yönteminde veri saklama kapasitesi diğer iki yönteme kıyasla daha fazladır. Bunun nedeni ise satır sonundaki boşluklardan faydalanmasıdır. Bu yöntemde gizlenecek olan veriler her bir satırın sonunda olan boşluklara gizlenmektedir.

Bir başka yöntem olan sağa hizalama yönteminde ise gizlenecek olan veri metin içerisinde metinlerin sağa hizalanması ile gerçekleşmektedir. Bu yöntemde kelimeler arasındaki boşluklar hesaplandıktan sonra veri gizleme işleme gerçekleşmektedir. Bu yöntemdeki olumsuz nokta ise çözme işlemi sırasında normal boşluk bırakma yöntemi ile karışmasından dolayı oluşan farkı anlamak zordur ve çözmek zorlaşır. Bu amaçla başka tekniklerden yararlanılmaktadır.

Gelecek kodlaması yönteminde ise metinlerin düşey ve yatay özellikleri değiştirilerek metin içerisine bilgi gizleme işlemi yapılmaktadır. Gelecek kodlaması yöntemi metin belgelerine uygulanabildiği gibi Bitmap türdeki dosyalara da uygulanabilmektedir (Şahin, 2007).

Şekil 2.11' deki örnekte a ile belirtilen metinin bir kodlama yapılmamış orijinal halidir. B ile belirtilen metin de ise seçilen karakterler üzerinde yapılmış gelecek kodlaması örneği gösterilmektedir. C ile gösterilen metinde bu yöntemin yoğun bir şekilde kullanılmış hali gösterilmektedir.



Şekil 2.11. Gelecek kodlaması örneği

2.5.2. Yazımsal Yöntemler

Yazımsal yöntemlerde veri gizlemek için noktalama işaretleri tercih edilmektedir. Gizlenecek metin ile gizlenmiş metinlerden bir tanesi "0" diğeri ise "1" ile belirtilir ve kodlama işlemi bu şekilde gerçekleşir.

Örneğin;

Bilgi ve veri birbirinden farklıdır. ! "0" Bilgi ve ,veri birbirinden farklıdır. ! "1"

2.5.3. Anlamsal Yöntemler

Anlamsal yöntemlerde kodlama işlemi gerçekleştirebilmek için eşanlamlı olan kelimeler için birincil ve ikincil olmak üzere değerlerler atanmaktadır. Sonrasında ise atanan birincil ve ikincil değerler "1" ve "0" olacak şekilde binary'e dönüştürülmektedir.

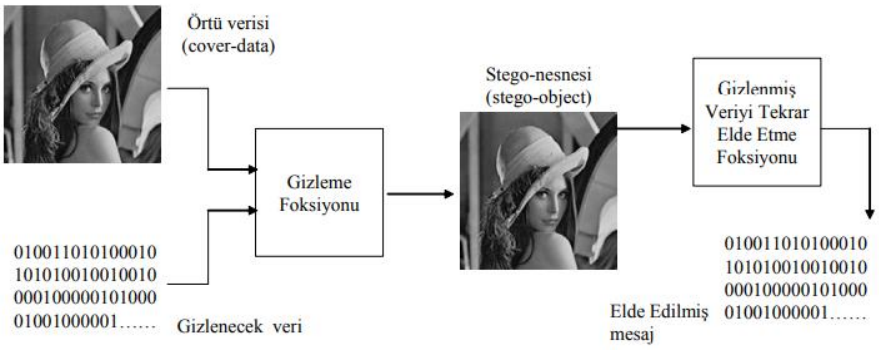
Örneğin; İngilizce de "wonderfull" kelimesi yerine "great" kelimesinin kullanılması.

2.6. Resim Steganografi

Resim steganografi yönteminde veri gizleme işlemi dijital resme bakan bir kişinin anlayamayacağı şekilde gizlenmesi işlemidir. Resim formatı olarak PNG, JPEG, GIFF ve BMP formatları kullanılabilmektedir. Resim dosyaları iletişim ortamlarında fazla kullanıldığı ve internet üzerinden iletimleri çok kolay ve yaygın olduğu için steganografik sistemlerde en sık uygulandığı formatlardır. Bu kadar fazla kullanılmasının en önemli sebeplerinden biri saklanacak veri miktarının çok olmasıdır (Avcı, Tuncer & Ertam, 2014).

Resim dosyalarında steganografi kullanabilmek için öncelikle görüntü dosyasının dijital hale çevrilmesi gerekmektedir. Bu işlemden sonra dijitalleşen görüntü dosyalarının piksel değerleri alınarak seçilen gizleme fonksiyonu uygulanmaktadır.

Resim dosyalarına veri gizleme sırasında kullanılan anahtar kavramı gizlenmesi istenilen mesajın güvenilirliğini sağlamak amacı ile kullanılmaktadır. Kullanılan bu anahtar ile gizlemek istenilen verinin resim içinde hangi piksellerde saklanacağı belirlenmektedir. Eğer istenirse gizlenmek istenen verinin şifrelenmesi amacıyla da bir anahtar kullanılabilir (Şahin Mesut, Mesut & Sakallı, 2010).



Şekil 2.12. Resim steganografik sistem

(Şahin, Buluş & Sakallı, 2006).

Resim steganografide, gizlenmek istenen bilgilerin resim dosyaları içerisine saklanabilmesinin çeşitli yöntemleri vardır. Görüntü dosyaları içerisine bilgi gizleme teknikleri dört ana başlık altında incelenebilmektedir.

Bu yöntemler;

1. Alan dönüştürme teknikleri,
2. Maskeleme ve filtreleme yöntemleri,
3. Uzaysal alanı teknikleri,
4. Çarpıtma teknikleri.

2.6.1. Alan Dönüştürme Teknikleri

Alan dönüştürme yöntemleri bir görüntünün frekans bileşenlerini kullanır. Görüntü önce frekans alanına dönüştürülür ve ardından mesaj gömülür. Resim formatlarından bağımsız çalışan bazı alan dönüştürme teknikleri de mevcuttur. Alan dönüştürme yöntemleri arasında; Ayrık kosinüs dönüşümü (DCT), Ayrık dalgacık dönüşümü (DWT), Ayrık Fourier dönüşümü (DFT), ve Tamsayı Dalgacık Dönüşümü(IWT) bulunmaktadır (Shehzad, 2019).

2.6.2. Maskeleme ve Filtreleme Yöntemleri

Maskeleme ve Filtreleme yönteminde veri gizleme işlemi resmin işaretlenmesi ile sağlanmaktadır. Budan dolayı bu yöntem kullanılırken gizlenmek istenen bilgiler karışık alanlara değil, daha önemli bölgelerde saklanabilmektedir. Örtü nesnesi ile birlikte kullanıldığı takdirde gizli veri daha birleşik ve bütünleşik yapıda olmaktadır. En önemsiz bite gizleme yöntemlerine göre daha sağlamdır ve sadece gri ton paletindeki resimlere uygulanabilmektedirler (Misman,2018).

2.6.3. Uzaysal Alan Teknikleri (Spatial Domain Methods)

Var olan bütün metotlarında veri saklama işlemi sırasında resim piksel değerlerinden bazılarını değiştirebilmektedir. Bu yöntemin avantajları olarak resmin orijinal halinde bozulmanın az olması ve resim dosyası üzerindeki veri saklama kapasitesinin yüksek olması söylenebilir (Misman, 2018).

Kenar tabanlı veri gömme metodu, histogram değiştirme metotları, piksel yoğunluğu metodu, en önemsiz bit, piksel değeri farkı metodu, Rastgele piksel veri gömme metodu, İsimlendirme ya da bağlantı metodu, Doku tabanlı metot ve Eşleme piksel veri saklama metotlar uzay alanı metotlarıdır.

2.6.4. Çarpıtma Teknikleri

Çarpıtma tekniklerinde gizli mesajı doğrulayabilmek için bir değişiklik listesi bulunmaktadır. Bu gizli liste bilgi gizleyen kişi tarafından gizli mesajın ortaya çıkarılabilmesi için örtü resmine eklenmektedir. Gizli mesajın ortaya çıkarılma işlemi için orijinal örtü resmi gerekmektedir. Bunun sebebi ise stego nesnesi ile karşılaştırma yapabilmek için ihtiyaç duyulmasıdır. Böylece gizli bilgi bozulması, çarpıklık olarak tanımlanır (Reddy & Raja, 2009).

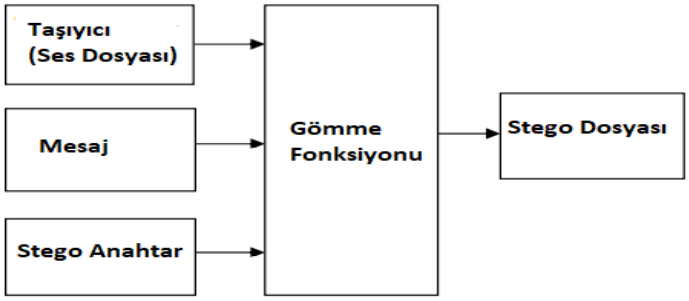
2.7. Ses Steganografi

Bir ses dosyasında bilgi gizlemek için kullanılan yöntem ses Steganografi olarak adlandırılmaktadır. Bilgi gizleme işlemi ses sinyalleri kullanılarak gömülmektedir. Bilgi gizleme işlemi resim steganografi yöntemlerinde olduğu gibi ikilik değerler üzerinde değişiklik yapılarak gerçekleşmektedir. Bu yöntem genellikle, savaş alanı iletişimi ve bankacılık işlemleri gibi bazı uygulamalarda ciddi ve hayati bir öneme sahiptir (Al-Othmani, Manaf & Zeki, 2012).

Ses dosyalarında bilgi gizleme işlemi HAS adı verilen insan işitme sisteminin frekans aralığı yüzünden oldukça dikkatli uygulanması gereken bir konudur (Şahin, 2007).

İnsan kulağı seslerin gücü 109:1'den büyük olduğunda ve frekans aralığı 103:1'den büyük olduğu zaman algılayabilmektedir. İnsan işitme sisteminin, beyaz Gauss gürültüsüne duyarlılığı da yüksektir. Bir ses dosyasındaki bu gürültü ortam seviyesinin 70 dB altında tespit edilebilir (Nosrati, Karimi & Hariri, 2012).

Ses steganografisinin temel modeli Taşıyıcı (Ses dosyası), mesaj ve şifre'den oluşur. Taşıyıcı, gizli bilgileri gizleyen bir örtü dosyası olarak da adlandırılmaktadır.



Şekil 2.13. Basit Ses Steganografi Algoritması

Bilgi gizleme süreci iki adımdan oluşmaktadır.

i. Bir örtü dosyasındaki fazlalık bitlerin tanımlanması aşamasıdır. Fazlalık bitleri, örtü dosyasının kalitesini bozmadan veya bütünlüğünü bozmadan değiştirebilen bitlere verilen isimdir.

ii. Gizli bilgiyi örtü dosyasına gömmek için, örtü dosyasındaki fazlalık bitleri gizli bilginin bitleriyle değiştirilir.

Ses dosyalarında veri gizleme sırasında kullanılan çeşitli yöntemleri mevcuttu, Bu yöntemler;

- Taft yayılması,
- Aşama kodlaması,
- Düşük bit kodlaması,
- Yankı veri gizlemesi.

2.7.1. Taft Yayılması

Ses sinyalinin kullandığı frekans taftı üzerinde gizleme işlemlerinin yapıldığı sistemlerdir. Bu yöntemi kullanılırken gürültü meydana gelmesi sebebiyle güçlü bir yapısı olduğu söylenememektedir (Bender vd.,1996).

2.7.2. Aşama Kodlaması

Bu yöntemde gizleme işlemi sırasında ses dosyaları küçük segmentlere bölünmektedir. Bu segmentlere ait fazlar ile gizlenecek olan verilere ait olan fazların referansları değiştirilerek işlem gerçekleştirilmektedir (Bender vd., 1996).

2.7.3. Düşük Bit Kodlaması

Bu yöntem de de taft yayılması yönteminde olduğu gibi gürültü meydana gelebilmektedir. Dayanıksız bir yapısı olduğu söylenebilmektedir. Ses dosyalarının her baytındaki son bite gizlenecek olan bilgi yazılmaktadır. Aslında bu yöntem aynı resim steganografi tekniğinde kullanılan LSB yöntemine benzemektedir (Kim vd., 2003).

2.7.4. Yankı Veri Gizlemesi

Bu yöntemde bilgi gizleme işlemi, bir yankının taşıyıcı ses sinyali üzerine eklenmesi ile gerçekleşmektedir. Gizlenecek olan bilgiler yankının büyüklüğü, zayıflama oranı ya da gecikme miktarı gibi değerler kullanılarak gizlenir. İnsan kulağının algılayamayacağı düzeyde İki farklı gecikme değeri kullanılarak 0'ın ya da 1'in kodlanabilmesi olasıdır. Sinyaller her bitin kodlanabilmesi amacı ile segmentlere bölünmektedir. Yankı veri gizlemesi yöntemi kayıplı bir kodlama kullanmamaktadır ve ya herhangi bir gürültüye neden olmamaktadır (Gruhl , Lu , Bender, 1996).

2.8. HTML Steganografi

Html dosyaları Zengin Metin işaret dili anlamına gelen internetin en temek unsurlarından bir tanesidir. İnternet kullanımının yaygınlaşması ile birlikte veri paylaşım oranları da artmaktadır. HTML de internet üzerinde veri paylaşmak için kullanılan en yaygın dillerden biridir.

HTML in temel işlevi metin, görüntü, ses, video vb. verileri ve bunları içeren sayfaların düzgün olarak görüntülenmesini sağlamaktır.

HTML steganografi aslen bir çeşit metin steganografi çeşididir.

```
<html>
    <head>
        <title> Bilgi gizleme </title>
    </head>
    <body>

        <p> Html nedir? </p>
        <a href ="http://www.deneme.com.tr"> Deneme </a>
    </body>
</html>
```

Şekil 2.14. Örnek HTML kodu

HTML dili ile kod yazılırken diğer diller de olduğu gibi yapılan işlemleri ifade etmek ve anlatmak amacı ile açıklama satırları yazılabilmektedir. Yazılan bu açıklama satırları internet tarayıcıları tarafından gösterilmez yani pek dikkate alınmaz. Bu şekilde düşünüldüğünde HTML dosyaları üzerine bilgi gizleme işlemi son derece kolay olabilmektedir (Gutub, Fattani, 2007).

```
<html>
    <head>
        <title> Bilgi gizleme </title>
                    <!-- Gizli mesaj buraya yazıldı -->
    </head>
    <body>

        <p> Html nedir? </p>
        <a href ="http://www.deneme.com.tr"> Deneme </a>
    </body>
</html>
```

Şekil 2.15. HTML koduna gizli mesajın yazılması

HTML dilinde <!-- --> etiketleri arasına yazılan her metin açıklama olarak gözükecek ve böylece HTML sayfalarına mesaj gizlenmiş olacaktır.

Yorum satırlarına bilgi gizleme tekniğinden farklı olarak HTML dosyaları üzerine bilgi gizleme de farklı yöntemler de mevcuttur. Bu yöntemler Etiketlerin sırasını değiştirme ve Etiketlerdeki harflerin durumunu değiştirme yöntemleridir.

Etiketlerin sırasını değiştirme

Öğelerin sıralı değişimi, HTML belgesinin çıktısını değiştirmeden verileri gömmek için de kullanılabilmektedir.

Etiketlerdeki harflerin durumunu değiştirme.

HTML etiketleri büyük/küçük harfe duyarsızdır. Dolayısıyla, bu özellik verileri HTML belgesinin içine gömmek için kullanılabilir.

Ancak etiket harflerini farklı durumlarda kullanmak yaygın olmadığı için kolayca tespit edilebilir.

2.9. Ağ Steganografi

Gizli verilerin transferini bilgisayar ağları üzerinde iletişim akışını bozmadan sağlama işlemi olarak bilinen tekniğe ağ steganografi denilmektedir (Karadoğan & Dağ, 2014).

Ağ ortamından gizli bilgi gönderebilme işlemi yapılırken ağ paketlerinin dolgularından, başlık yapılarından, uzunluklarından ve sınıflandırmalarından yararlanarak yapılabilmektedir.

Ağ steganografi tekniğinde kullanılan yöntemleri şu şekilde sınıflandırılabilmektedir;

- Paket başlığı tabanlı steganografi,
- Paket Zamanlama Tabanlı steganografi,
- Paket Uzunluğu Tabanlı steganografi,
- Paket Sıralama Tabanlı steganografi,
- Paket Sınıflandırma Tabanlı steganografi,
- Paket Dolgusu Tabanlı steganografi,
- Karma ve diğer yöntemler.

BÖLÜM 3

VİDEO STEGANOGRAFİ

Bilgi güvenliği içerisinde yer alan verilen korunması kavramı, gelişen teknoloji ve internet kullanımın yaygınlaşması ile oldukça önemli bir konu haline gelmiştir. Özellikle güvenli veri transferi alanında yeni teknikler geliştirilmeye başlanmıştır. Bu yöntemlerden biri olan steganografi kavramı iletilecek olan bilginin gizlenmesi anlamına gelmektedir. Steganografi tekniğinde gizlenecek olan ortamlar çeşitlilik göstermektedir. Video dosyaları üzerine bilgi gizleme işlemlerine video steganografi bu teknikleri denilmektedir. Video dosyalarındaki gizleme işlemleri boyutlarından dolayı gizleme kapasitesi olarak avantaj sağlayabilmektedir.

Bu bölümde video steganografi ve video steganografide uygulanan yöntemler hakkında bilgi verilecektir.

3.1. Video

Bir video, ses ve resim formatlarının birleşiminden oluşmuş bir dosya türüdür. Videoları, sesli ve hareketli fotoğrafların artarda eklenmiş hali olarak kabul edebiliriz. Video dosyası çerçeve olarak adlandırılan verilen resimlerin saniyede ardışık şekilde gösterilmeleriyle oluşturulmaktadır. Peş peşe ekrana gelen bu görüntü kareleri hızlı bir şekilde oynatıldığından dolayı hareketliymiş gibi algılanmaktadır. Bunun sebebi 10 kareden fazla fotoğrafın 1 saniye içinde peş peşe oynatıldığı zaman insan gözü bunu hareketliymiş gibi algılamasıdır. Eğer 1 saniye içerisinde 10 kareden daha az sayıda fotoğraf peş peşe gelirse insan gözü bu görüntüleri kesik kesik görüntüler olarak görmektedir.

Her video görüntüsü, Kırmızı, Yeşil ve Mavi (RGB) veya CMYK Camgöbeği, Macenta, Sarı ve Siyah (CMYK) gibi bir Renk kümesi (üç veya dört) içeren birkaç pikseli kapsayan bir çerçeve olarak adlandırılır. Kalan aracı renkler, bu temel renklerin bir koleksiyonundan yapılır. Genel olarak, insan gözü yeşil renge duyarlıdır, bu nedenle her bir renk karışımının bit sayısı farklı olabilir.

Video dosyalarının özellikleri şu şekildedir;

- Kodek/kompresör,
- Kare hızı,
- Çerçeve boyutu,
- Çerçeve en boy oranı.

3.1.1. Kodek

Bir video kodek bileşeni, dijital videoyu sıkıştıran veya açan bir elektronik devre veya yazılımdır. Video kodekler başlı başına bir yazılım olup, sıkıştırmak ve sıkıştırılan açmak kelimelerinin baş harflerinden doğan bir kelimedir. Sıkıştırma kavramının karşılığı encoder, sıkıştırılanı açmak kavramının karşılığı ise decoder olarak adlandırılmaktır. Kodekler genellikle çok yüksek boyutlara erişen video veya ses dosyalarının boyutunu küçültmek için kullanılan bir algoritmadır. Kodekler görüntüleri veya sesleri aldıktan sonra bunları şifreleyerek sıkıştırmaktadırlar. Bu işlem sayesinde ses ve video dosyaları daha küçük boyutlara ulaşabilmek ve boyut olarak tasarruf sağlanmaktadır. Örneğin; Bir AVI formatındaki video 4,5 GB boyuttan sıkıştırma ve çok az görüntü kaybı yaşanarak 500 MB a kadar düşürülebilmektedir. Sıkıştırılmış olan bu ses veya video türündeki dosyaları açabilmek için ise decodere ihtiyaç duyulmaktadır (Demirkiran, 2008).

Kodekler, herhangi bir veriyi atmadıkları anlamına gelen kayıpsız veya kodlama sırasında verilerin kaybolduğu anlamına gelen kayıplı olabilecek şekilde ikiye ayrılmaktadır. Kayıpsız kodekler, kayıplı kodeklerden daha kalitelidir, ancak daha büyük dosya boyutları üretir.

3.1.2. Kare Hızı

Video dosyalarında 1 saniyede ekrana gelmekte olan kare sayısına “kare hızı” denilmektedir. Kare hızı fps (frame per second) olarak adlandırılan ve saniyeye düşen kare sayısı anlamına gelen bir birim ile ifade edilmektedir.

3.1.3. Çerçeve Boyutu

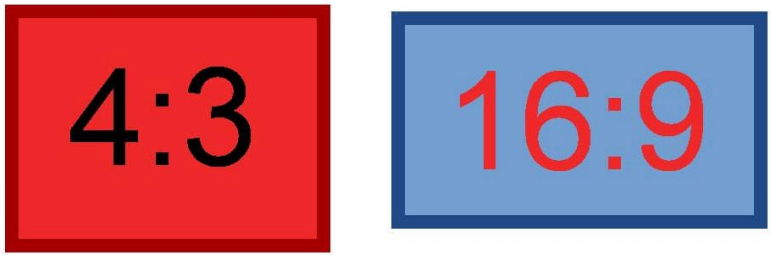
Aynı resim dosyalarında olduğu gibi video dosyaları da bir araya gelen piksellerden oluşmaktadır. Video dosyalarındaki piksellerin sayısı, “çerçeve boyutu” olarak adlandırılmaktadır. Çerçeve Boyutu, tek bir video karesinin boyutunu tanımlar: genişlik × yükseklik, piksel cinsinden ölçülür.

Çerçevenin genişliği, çerçevedeki piksellerin kare piksel veya kare olmayan piksel olmasına bağlı olarak değişebilir.

Örnek: DV-PAL 4:3 karesi 768 piksel genişliğinde (kare piksel) veya 720 piksel genişliğinde (kare olmayan piksel) olur. Bunun nedeni, her bir pikselin daha geniş olması durumunda ekranda aynı boyuttaki kareyi oluşturmak için daha az sayıda pikselin gerekli olmasıdır.

3.1.4. En-Boy Oranı

Videolardaki en-boy oranı özelliği görüntülerin dikey ve yatay eksenlerinin birbirine oranını ifade etmektedir. Farklı ihtiyaçlar için kullanılan birçok en-boy oran standartları bulunmaktadır. Bunlar arasında en yaygın olarak bilinenler arasında 4:3 en boy oranı ve 16:9 en boy orandır. 16:9 oranı yatay eksende uzunlamasına bir görüntü sağladığı için 4:3 oranına göre insan algısına göre daha uygun olmaktadır. Bu yüzden son zamanlarda 4:3 oranı yerine 16:9 oranı daha çok tercih edilmektedir.



Şekil 3.1. En çok tercih edilen en-boy oranları

3.1.5. Video Dosyası Türleri

Dijital yayıncılık ile birlikte kullanıcıların farklı ihtiyaçlarına göre farklı türde video dosyası türleri tercih edilmeye başlanmıştır. Buradaki tercihler ise kullanım amacına bağlı olarak kalite, boyut vb. nedenler ile değişmektedir. Bazı video dosyası türleri az yer kapladığı için bazıları ise görüntü kalitesi iyi olduğu tercih edilmektedirler.

Günümüzde amaçları ve kullanım şekillerine göre farklı video türleri kullanılmaktadır. WEBM video formatı genellikle Youtube vb. gibi video akış siteleri için tercih edilmektedir, dosya boyutları diğer video türlerine göre daha küçük olabilmektedir. Bu sebepten dolayı diğer video türleri kadar yüksek kalite sağlayamamaktadır. OGG video formatını daha çok MPG dosyalarını alternatifi şeklinde kullanılmaktadır ve kalitesi WEBM dosyalarına göre daha yüksektir, açık kaynaklı olmaları sebebi ile farklı uygulamalarda kullanılabilmektedir. Daha çok iletilecek yüksek kalitedeki videolar için tercih edilmektedir. Windows işletim sistemi kullanan bir kullanıcıya video göndermek için tercih edilen bir format olan WMV formatı Microsoft tarafından oluşturulmuştur. Küçük dosya boyutlarına sahip olabilmektedirler fakat kalitesi de bu oranla düşük olmaktadır. Apple şirketi tarafından geliştirilen MOV ve QT video türleri yüksek kalitede ve dosya boyutu olarak büyük video türleridir. Belirli bir video oynatıcısı ile kullanılmak üzere geliştirildiği için diğer programlar ile uyumluluk konusunda çok başarılı değildir. Adobe şirketi tarafından Flash için geliştirilmiş video türleri FLV ce SWF'dir. Günümüzde Flash desteği sona erdiği için popüleritesi ve kullanımı oldukça sınırlanmıştır. MPG video türü sadece ses ya da hem video ve ses içerebilen düşük boyutlu bir türdür. Kaliteleri diğer türlere göre daha düşük olabilmektedir. Kayıplı sıkıştırma sahip olan türlerdir yani tekrar tekrar düzenlendikten

sonra video kalitesi düşebilmektedir. Bu tür için en iyi kullanım şekli ise videoların bir kez kayıt edilip düzenlenmeyeceği şekildedir.MP4 video türü internet üzerinden video akışı için kullanılabilen bir türdür. Aynı MPG türünde olduğu gibi video ve sesi içerebilmeleri ya da yalnızca ses dosyalarını oynatabilmeleri açısından benzemektedir ve kalite olarak da WEBM türlerinden daha kalitelidir. Dosya boyutları ise büyük olabilmektedir. AVCHD video türü dijital video kameralar tarafından oluşturulan bir türdür ve MPG dosya türüne benzemektedirler, bu türler H.264/MPEG-4 video kodek bileşenini kullanmaktadırlar. AVI video türü en uyumlu denilebilecek video türlerinden biridir. Birçok farklı video kodek bileşeni ile birlikte kullanılabilmektedir bu da kalite ve boyut arasında seçim yapma konusunda esneklik sağlamaktadır. Dosya boyutları diğer video türlerinden daha büyük olabilmektedir web kullanımı için pek ideal değildir fakat video depolama vb. işlemler için daha idealdir.

3.2. Video Steganografi

Veri gizleme tekniklerinde araştırmacıların karşısına çıkan kapasite problemi çözülmesi zor bir sorun olarak ortaya çıkmaktadır. Özellikle hareketsiz görüntülerin kapasiteleri belirlenen sınırları aşamadığından steganografi üzerinde çalışan araştırmacılar hareketli görüntü dosyaları yani video üzerinde yoğunlaşmaktadırlar (Yalman, Çetin, Ertürk & Akar, 2014).

Video temel olarak ses ve görüntü türlerinin birleşimi ile oluşmuş bir türdür. Bu yöntem, video dosyaları içerisine her türlü dosya veya veriyi gizlemek amacı ile kullanılmaktadır (Razavi, 2017).

Video dosyası resim ve ses dosyaları içerdiğinden dolayı bu türlere ait olan bilgi gizleme yöntemleri video dosyaları üzerinde de uygulanabilmektedir. Video dosyaları üzerinde bilgi gizleme işlemi yapılaması resim üzerindeki yöntemlere göre avantajlı olabilmektedir. Bunun sebebi ise video dosyalarındaki kare hızından kaynaklanmaktadır. Video dosyalarında kare hızı yüksek olmasından dolayı video üzerinde herhangi bir bilgi gizleme işlemi olup olmadığının anlaşılması oldukça zordur. Böylece gizli mesajın varlığını anlamak zorlaşır.

Video dosyalarının steganografide kullanılma amaçlarının en başında büyük miktarda veri gizleme kapasitesi yer almaktadır. Örneğin 40 fps hızındaki 20 saniyelik

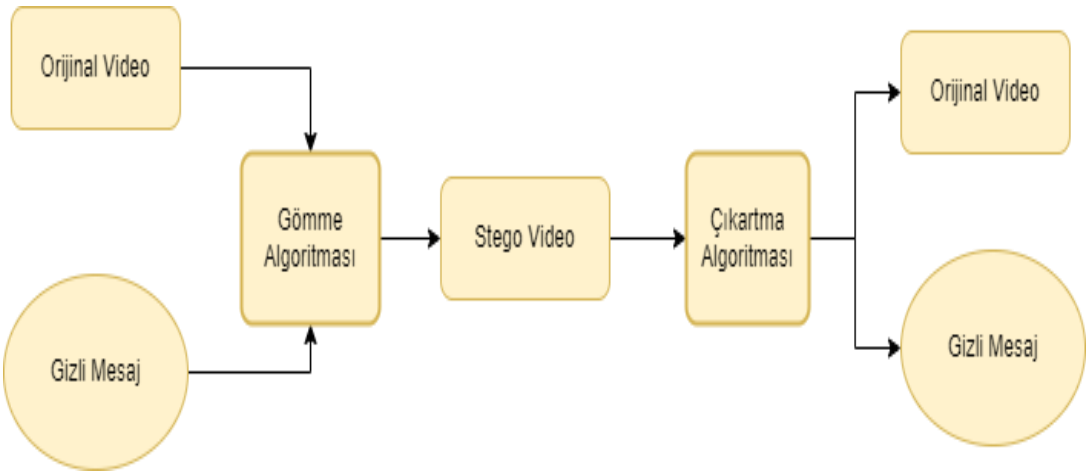
bir video içerisinde 800 hareketsiz resim yer almaktadır. Böylece veri gizleme kapasitesi resimlere oranla oldukça artmaktadır.

Bir video dosyası içerisine bilgi gizleme işlemi, video içerisinde bulunan her bir çerçeveye ayrı ayrı gizlenerek yapılabilmektedir. Video dosyaları içerisinde bilgi gizleme işlemi genellikle resim dosyaları üzerine veri gizleme işlemleri ile benzerlik göstermektedir.

Video stenografin yönteminde kullanılan formatlar MP4, AVI, MPEG, H.264 ve çeşitli formatlar kullanabilmektedir.

Video steganografi de bilgi gizlemek için çeşitli yöntemler mevcuttur. Bu yöntemler en önemsiz bite gömme yöntemi, sıkıştırma video steganografisi, maskeleme ve filtreleme, düzensiz dikdörtgen bölümlemesi ve yaygın Spektrum yöntemidir. Kullanılan yöntemler arasına en çok bilinen yöntem en önemsiz bite ekleme yöntemidir. Bu yöntemde oluşmakta olan veri kaybı diğer yöntemlere göre daha azdır (Demirci, 2016).

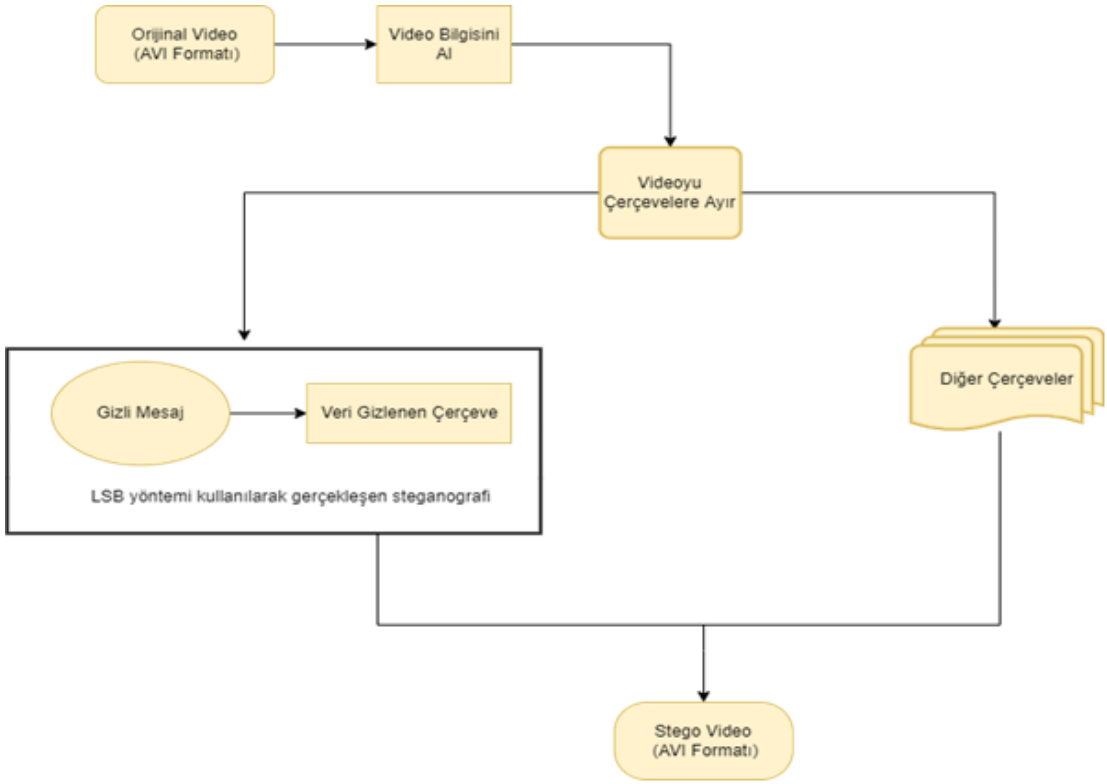
Video Steganografi yöntemlerinde video içerisine veri gömülme işlemi sağlandığında, bu videoları alan kişiler çıplak gözle baktığında video kalitesinde herhangi bir değişiklik fark etmemelidir (Bhaumik, Choi, Robles, & Balitanas, 2009).



Şekil 3.2. Video steganografi algoritması

Gömme Algoritmasında orijinal video dosya içerisindeki çerçevelere gizli mesajı gizleme işlemi yapılmaktadır. Bir iletişim ortamı üzerinden düşünüldüğünde gömme

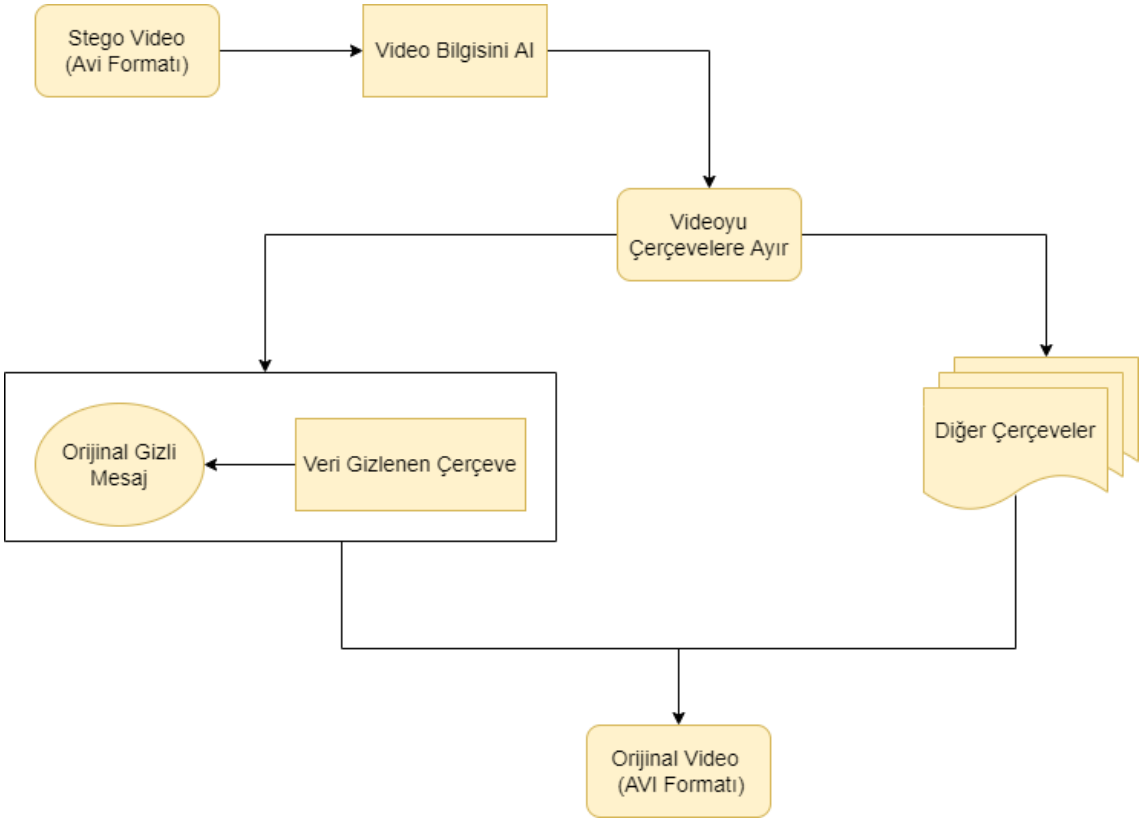
işlemi gönderici tarafından gerçekleşmektedir. Göndericiden alıcıya giden ve gömme işleminden geçmiş olan stego videoyu açıp içerisindeki gizli mesajı alabilmek için alıcının yalnızca gönderici ve alıcı tarafından bilinen stego anahtara ihtiyacı vardır.



Şekil 3.3. Video steganografi için gömme algoritması

Çıkartma algoritmasında alıcı tarafında, gizli bilgileri çevirmek için ters adımlar kullanılır, stego video ve kapak video dosyası okunur ve çerçeve bilgileri toplanır ve ardından bilgilerin gizlendiği çerçeveleri çıkarır.

Daha sonra, çerçeveden ilk mesajı elde etmek için seçilen çerçeve üzerinde gizli anahtar kullanılarak çıkarma algoritması gerçekleştirilir.



Şekil 3.4. Video steganografi için çıkartma algoritması

Video Steganografi Avantajları

Video stenografin yönteminin resim steganografi yöntemine göre avantajları mevcuttur. Bu avantajlar ise çerçeveler yalnızca kısa bir süre için fark edilebilir olduğundan, değişiklikler insan görsel çerçevesi için daha az algılanabilir olması ve çerçeveler tek tek daha az net ve odaklanmış olabilmektedir bu yüzden de küçük renk değişiklikleri fotoğraftaki kadar fark edilebilir olmayabilir.

3.2.1. Video Steganografi Yöntemleri

Video steganografi teknikleri farklı Şekillerde düzenlenebilmektedir:

1. Sıkıştırma ile:

- Sıkıştırılmış video dosyaları için yöntemler,
- Sıkıştırılmamış (ham) video dosyaları için yöntemler.

2. Alanı yerleştirerek:

- Mekânsal alan,
- Dönüştürme alanı.

3. Gömme yöntemiyle:

    - Hareketsiz görüntülere gömme,
    - Video kodeğine dayalı gömme,
    - Video formatına göre gömme.

Video steganografi de farklı stratejilerde kullanılabilmektedir. En uygun olanı, kapak videosunun kalitesinin etkilenmediği ve gizli bilgileri insan gözünün algılayamayacağı şekilde gizleme stratejisidir. Gizlenen video "stego" video olarak göndericiden alıcı tarafına ulaşmaktadır. Bilgileri korumak için şu an için farklı türde video steganografi yöntemleri kullanılmaktadır.

Bu yöntemler;

- En önemsiz bite ekleme yöntemi,
- Tekdüzen olmayan dikdörtgen bölümleme yöntemi,
- Maskeleme ve filtreleme yöntemleri,
- Sıkıştırma Video steganografisi yöntemi,
- Anti-adli yöntemi.

Tekdüzen Olmayan Dikdörtgen Bölümleme Yöntemi

Düzensiz dikdörtgen bölümlemesi yöntemi sıkıştırılmamış videolar için kullanılmaktadır. Bu yöntemde, ana video içerisine sıkıştırılmamış bir video saklanmaktadır. Dikkat edilmesi gereken önemli nokta ise örtü videosu ile gizlenecek videonun aynı boyutlarda olmasıdır. Bu yöntemde resim steganografi tekniklerinden bazıları gizlenecek video ve örtü video dosyalarının her bir karesine uygulanmaktadır. Bu yöntemde düzensiz dikdörtgen ayrıştırması bilgi gizlenecek olan videonun her bir karesine uygulanmaktadır. Bu yöntem uygulanırken ayrıştırma işlemine tabi tutulan kodlar şifrelenerek taşıyıcı ortam olan video dosyasındaki her bir frame'in en düşük değerliğe sahip dört bitine saklanır (Hu, 2011).

Maskeleme ve Filtreleme Yöntemleri

Bu yöntemde 24-bit renk kod yapısına sahip resimler kullanılmaktadır. Maskeleme ve filtreleme yöntemleri kullanılırken resmin var olan nitelikleri değişmemektedir. Hem renkli hem de gri tonlama yapısındaki resimlerde uygulanabilmektedir.

Maskeleme yöntemiyle yapılan gizleme işlemleri üzerine uygulanan steganaliz yöntemleriyle kolay bir şekilde fark edilememektedir. Veri maskeleme işleminde diğer steganografi yöntemlerinden farklı olarak gizli mesaj neredeyse bir multimedya dosyası gibi işlenmektedir (Çimen vd., 2007).

Sıkıştırma Video Steganografisi

İşlemlerin tamamen sıkıştırılan alandan yapılması işlemine Sıkıştırma video steganografisi denilmektedir. Bu yöntemde veriler I çerçevesine P ve B çerçevelerindeki en büyük hareket vektörü ve en yüksek kare değişim değeri ile saklanabilir. Sıkıştırma video steganografisinde AVC kodlama tekniği ile en yüksek performans elde edilmektedir.

Anti-Adli Yöntemi

Bu yöntem, bilgisayar hukuk bilimlerine saldırmak için bilgilere zarar vermek, gizlemek ve işletmek için yapılan alıştırmalardır. Resmi olmayan kişilerden korunmak için güvenlik sağlar. Steganografi, bilgileri ana bilgisayar dosyası altında saklamaya çalıştığımız anti-adli tıpa benzer. Steganografi ve adli tıp aynı anda sistemi yetkisiz erişime karşı daha güvenli hale getirir.

3.2.2. En Önemsiz Bite Ekleme Yöntemi (LSB)

En basit ve en yaygın kullanılan teknik olan En önemsiz bite ekleme yöntemi aynı zamanda uygulaması en kolay yöntemdir. LSB yöntemi kullanılarak gerçekleştirilen veri gizleme işleminde, gizlenmek istenen verinin bitleri sırayla görüntüyü oluşturan her pikselin her byte'nın en önemsiz biti olan son biti ile başlangıçtan itibaren değiştirilerek yapılmaktadır (Şahin vd., 2006).

Veri gizleme işlemi sonrasında gizli mesaj en anlamsız bit veya bitlerde barındırılmaktadır. Bu yöntemde örtü verisi ve gömülü verinin oluşturduğu ortamda meydana gelen değişiklikler duyu organları ile fark edilememektedir. (Şahin vd., 2006).

Avantajları:

- Görsel kalite elde edilmesi,
- Yüksek veri gizleme kapasitesi elde edilmesi,
- Kolay uygulanabilir olması.

Dezavantajları:

- Saldırılara karşı pek dayanıklı olmaması,
- Sıralı yapılmasından dolayı anlaşılabilirliği kolay,
- Veri kayıpları ortaya çıkabilmektedir.

En önemsiz bite ekleme işleminde iki farklı şekilde gizleme işlemi yapılabilmektedir. Bu işlemler sıralı ve rastgele gizleme şeklindedir. Sıralı gizleme işleminde gizlenecek olan bilgi baştan sona doğru olacak şekilde resim dosyası üzerine sıralı olarak gizlenebilmektedir. Rastgele gizleme işleminde gizleme işlemi bir rasgele fonksiyon üreteci kullanılarak yapılmaktadır. Bu fonksiyon kullanımı sonucunda belirlenen pikseller üzerinde gizleme işlemleri yapılmaktadır (Kurtuldu & Arıca, 2009).

LSB Yönteminin Uygulanması

En önemsiz bite ekleme yöntemi yönteminin kullanımı Şekil 3.5'de gösterilmiştir

	Pikselin Renk Değeri	**Renk Sisteminin ikilik karşılığı**
Orijinal Piksel	164	10100100
Veri Gömülmüş Piksel	165	10100101

Şekil 3.5. LSB yöntemi ile veri gömme

Örneğin;

Var olan bir resmin piksel değerlerinin ikilik karşılığı şu şekilde olduğu düşünülürse:

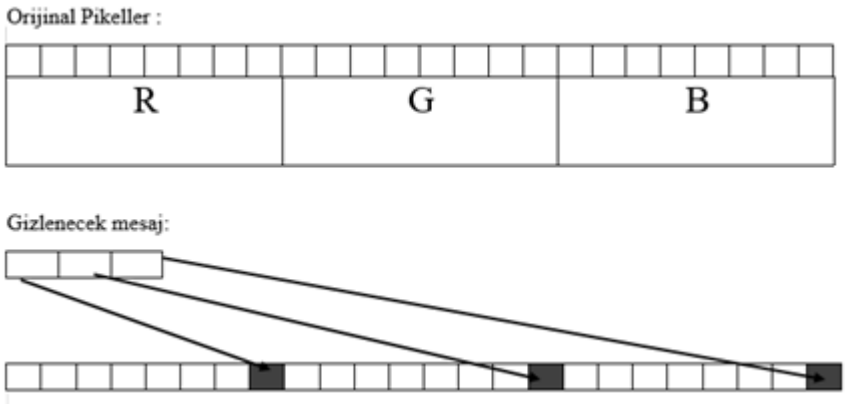
10001001 11101001 11101001 10011011 10011011 10001001 00011111 00011101

Buna T (01010100) karakterini eklersek

Resmin yeni ikilik karşılığı:

10001000 11101001 11101000 10011011 10011010 10001001 00011110 00011100

şeklinde değişecektir.



Şekil 3.6. LSB uygulaması

Video steganografi yöntemlerine ait karşılaştırmaları Çizelge 3.1.' de gösterilmektedir.

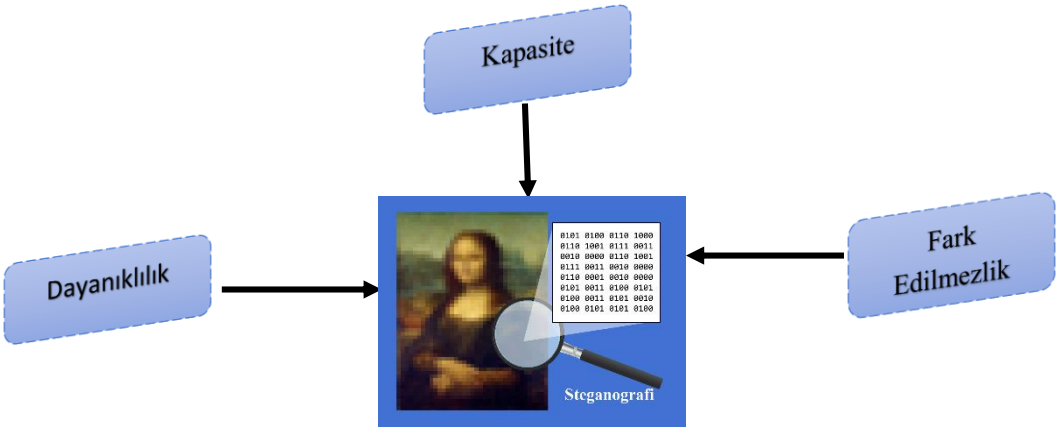
Çizelge 3.1. Video steganografi yöntemlerinin karşılaştırılması

Video steganografi teknikleri	**Avantajı**	**Kısıtlamaları**
LSB Tekniği	Verileri gömmek ve uygulanması kolaydır, yüksek mesaj yükü kapasitesi vardır.	Tespit edilmesi daha kolaydır.
Tekdüzen olmayan dikdörtgen bölümleme Yöntemi	Bilgi gizlenecek videoda herhangi bir değişiklik yapmadan gizleme işlemi yapılabilmektedir.	Gizli ve kapak dosyaları aynı boyutta olmalıdır.
Sıkıştırma video steganografisi	Orijinal video gerektirmeden verilerin çıkarılabilmektedir.	Yalnızca sıkıştırılmış videolar için kullanışlıdır.
Anti-Adli Yöntemi	Verileri yetkisiz erişime karşı korunması.	Temel olarak adli bilişime saldırmak için kullanılır
Maskeleme ve filtreleme	Kolaylıkla tespit edilemez, hem gri hem de renkli ölçekli görüntüler için kullanılabilir. Daha sağlamdır.	Basit istatistiksel analiz ve araçlarla tespit edilebilir

BÖLÜM 4

STEGANOGRAFİK YÖNTEMLERİN GEREKSİNİMLERİ

Steganografi yöntemlerinde kapasite, fark edilemezlik ve dayanıklılık olmak üzere 3 farklı gereksinim bulunmaktadır. Bir steganografi yöntemi geliştirirken bahsedilen gereksinimlere dikkat edilmesi gerçekleştirilecek olan yöntemin amacına uygun olarak yapılması açısında oldukça önem teşkil etmektedir.



Şekil 4.1. Steganografi Yöntemlerinin Temel Gereksinimleri

4.1. Kapasite

Steganografi tekniklerinde amaç bilgiyi gizli bir şekilde iletmek olduğu için gizlenecek veri miktarı önem teşkil etmektedir. Gizlenecek veri kapasitesinin yüksek olması arzulanan bir durumdur. Fakat gizlenen veri miktarının artması ile birlikte bozulmalar meydana gelebilmekte ve güvenlik zafiyetleri ortaya çıkabilmektedir. Bu

sebepten dolayı steganografi yöntemleri ile gizleme yapılırken bu dengenin sağlanması oldukça önemlidir. Kapasite olarak kullanılan dosya formatlarına bağlı olarak bu formatlar arasında da farklılıklar olabilmektedir. Örneğin resim dosyaları için BMP ve JPEG formatları daha iyi sonuçlar verebilmektedir.

4.2. Fark edilmezlik

Örtü verisi üzerinde yapılan değişikliklerin istatistiksel ve insan duyuları tarafından algılanmayacak şekilde olması gerekir. Algılanması durumunda gerçekleştirilen gizli iletişim ortaya çıkabilmektedir. Bu yüzden kapasite gereksinimi ile doğrudan ilişkilidir.

Taşıyıcıdaki değişimin ne kadar olduğu bir steganografik algoritma değerlendirilirken oldukça önemlidir. Verilerdeki bozulma oranı ya da taşıyıcıdaki değişimin belirlenebilmesi amacıyla çeşitli ölçme yöntemleri kullanılmaktadır.

Mevcut yöntemler arasında en bilinenler ise; MSE, RMSE, PSNR yöntemleridir.

Ortalama Kare Hata:

MSE (Mean Squared Error) hataların karelerinin toplamının ortalamasıdır. Resim dosyalarında orijinal ve değişen piksel değerleri arasındaki ortalama kare farkını ölçmek için kullanılmaktadır. MSE σ^2 ile gösterilir. Elde edilen MSE değerinin sıfıra yakın olması resim üzerinde çok değişiklik olmadığını göstermektedir. RMSE (Root Mean Squared Error) ise MSE'nin kareköküdür (Yıldız, 2012).

$$MSE = \frac{1}{n}\sum_{j=1}^{n} e_j^2$$

Şekil 4.2. MSE Formülü

Tepe Sinyali Gürültü Oranı

PSNR (Peak signal-to-noise ratio) yöntemi hatanın büyüklüğünün orijinal piksel değerinin en büyüğü ile olan ilişkisini bulmak için kullanılmaktadır. Bu yöntem bazı durumlarda Ortalama kare hatası yerine kullanılabilmektedir. PSNR, bir işaretin olası

maksimum gücünün işaret üzerindeki gürültünün gücüne oranını gösteren bir ölçme yöntemidir (Sayood, 1996).

$$PSNR(dB) = 10\log_{10}\frac{x_{peak}^2}{\sigma_d^2}$$

Şekil 4.3. PSNR Formülü

Yapısal Benzerlik İndeksi

SSIM yöntemi iki görüntünün yapısal benzerliğini göstermek için kullanılmaktadır. Bu yöntem, işlenmiş görüntü ve orijinal görüntü arasında mevcut olan yapısal benzerliğin karşılaştırmasını yapmaktadır. Yapılan bu karşılaştırmaların sonucu 0–1 arası değerler almaktadır ve elde edilen değerler ’e yaklaştıkça görüntüler arasındaki benzerlik ve kalite artmaktadır. SSIM, analiz işleminde yerel parlaklık ve kontrastı dikkate alır (Sara, Akter, & Uddin, 2019).

4.3. Dayanıklılık

Gizlenen veriyi elde etmek için haberleşme kanalını dinleyen kötü niyetli kişiler olabilmektedir. Bu sebepten dolayı gerçekleştirilen güvenli bir steganografi tekniğinde gizli veriler kötü niyetli kişilerin eline ulaşmamalıdır. Kanalı dinleyen kötü niyetli kişilerin çıkartma algoritmasını bilme ihtimaline karşı gizlenecek olan bilgini şifrelenerek gizlenmesi oldukça önem kazanmaktadır. Bir steganografik sistemin dayanıklılığını ölçmek için Steganaliz yöntemlerine gerek duyulmaktadır.

4.3.1. Steganaliz

Steganografi tekniklerinin kullanımı gelişen teknoloji ile birlikte son yıllarda veri iletişimi açısından oldukça önem kazanmıştır. Bu durum ile birlikte üçüncü kişiler tarafından gönderilen verilerin tespit edilmesi ve geri elde edilmesi konusunda araştırma faaliyetleri oldukça artmaktadır.

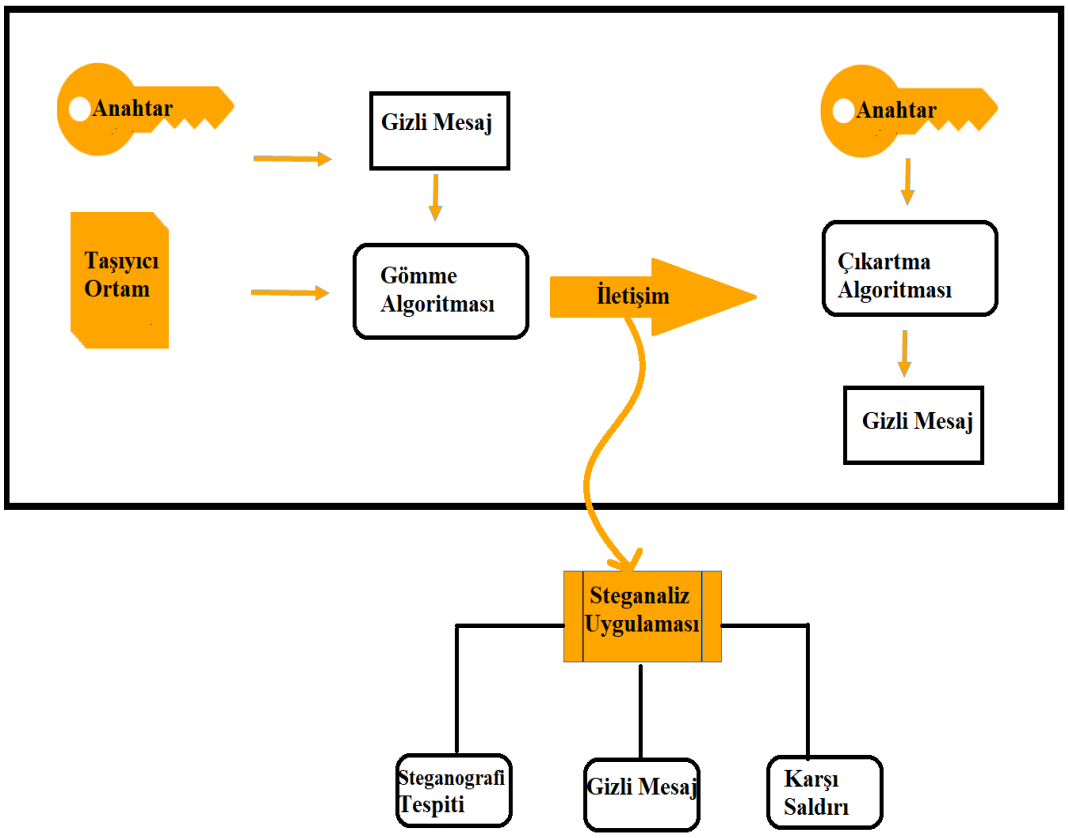
Steganaliz kavramı aslen bir saldırı yöntemdir. Bu kavramda amaç bir stegonagrafik algoritma kullanılmış olan sisteme karşılık örtü veride herhangi bir gizli bilgi olup olmadığını bulmak ve eğer var gizli bilgi var ise bu bilgiyi elde etmektir. Kerchoffs'un prensiplerine göre genelde bir steganalistin yani saldırı yapan kişinin kullanılmış olan steganografik sistemi bildiği varsayılmaktadır (Kerckhoffs A., 1883.).

Steganaliz genel anlamda dijital ortamlarda steganografi teknikleri ile yerleştirilmiş gizli mesaj veya gizli dosyaları tespit etmek ve ortaya çıkarmak için kullanılan bir bilim dalıdır. Steganaliz, sadece gizli mesaj ya da gizli dosyaları tespit etmesi bile steganografi uygulamalarının en önemli amacı engellemektedir.

Saldırı gerçekleştiren steganalistlerin steganografi tekniklerini hakkında detaylı bilgiye sahip olması gerekmektedir. Genellik saldırı yapan steganalistin kullanılan yöntemi bildiği varsayılmaktadır. Şayet kullanılan yöntem hakkında bir bilgiye sahip işi oldukça zorlaşabilmektedir.

Steganografik sisteme saldırı yapabilmek için elinde gerekli olan bilgiler olan steganalist, sahip olduğu bu veriler ışığında saldırı modellerinden birini seçebilir (Şahin, Buluş, Sakallı & Buluş, 2007). Steganografik sistemlere karşı geliştirilen steganaliz saldırılarından bazıları şunlardır;

- Sadece stego saldırısı: Yalnız örtülü nesnenin bilindiği saldırı türüdür.
- Bilinen taşıyıcı saldırısı: mesaj gizlenen ortamın gizlendikten sonraki ve gizlenmeden önceki bilinmektedir.
- Bilinen mesaj saldırısı: Gerçekleşmesi zor olan saldırılardan biridir. Analistin saklanan mesajın bilindiği saldırı türüdür.
- Seçilmiş stego saldırısı: Steganografik algoritma ve örtü-nesnesinin bilindiği saldırı türüdür.
- Seçilmiş mesaj saldırısı: Bu saldırı yönteminde steganalist elinde bulunan stego-nesnesini analiz edebilmek için mesajlar seçerek steganografik araçları kullanarak stego-medyalar elde eder. Böylece algoritmayı bulmaya çalışır (Şahin vd., 2007).



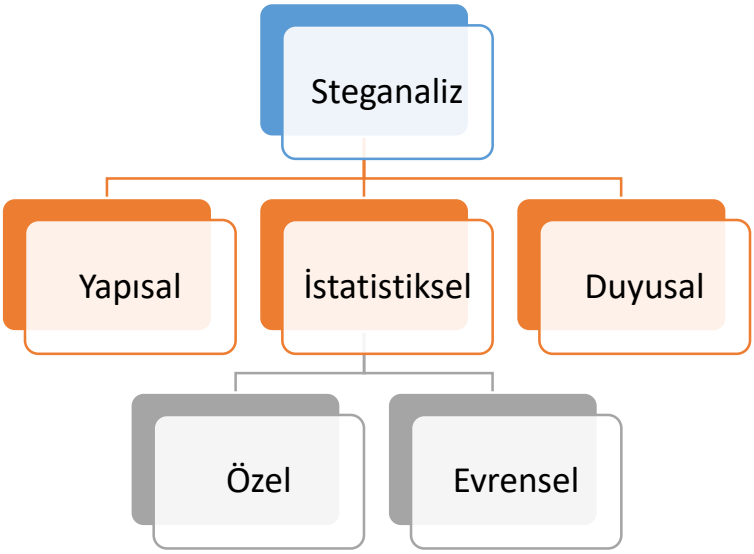
Şekil 4.4. Steganaliz süreci

Steganaliz yöntemlerini kendi içlerinde amaçlarına göre pasif, aktif ve bozucu steganaliz olmak 3 faklı gruba ayrılmaktadır.

Pasif Steganaliz yöntemlerinde gizli bilginin sadece varlığı tespit edilebilmektedir.

Aktif steganaliz yönteminde var olan gizli bilginin bir bölümü ya da tamamının bulunması amaçlanmaktadır.

Bozucu steganaliz yöntemi ise aktif steganaliz yönteminin bir üst seviyesi gibidir, bu yöntemde gizli bilgi bulunduktan sonra ya yok edilir ya da bu bilginin yerine sahte bir mesaj yerleştirilmektedir.



Şekil 4.5. Steganaliz atak türleri

Şekil 4.5.'de görüldüğü üzere literatürde 3 farklı Steganaliz atağı bulunmaktadır.

- **Duyusal Ataklar:** İnsanlar tarafından görsel ve ya işitsel olarak anormallik tespiti yapılmasıdır.
- **Yapısal Ataklar:** Bu oluşum belli bir yapıda, belli bir yoğunlukta ve sıralı, tekrarlayan olağandışı ayırt edici özellik ve örüntülerdir.
- **İstatiksel Ataklar:** Temelini matematiksel yaklaşımların oluşturduğu istatiksel steganaliz uygulamalarıdır. Anlamlı ve izlenebilir farklılıklar istatiksel özelliklerde görülmektedir. Yapısal ataklarla karşılaştırıldığında daha güvenilir ve hassas sonuçlar vermektedir.
    - **Özel:** Yalnız hedef steganografi uygulamasına karşı etkilidir.
    - **Evrensel:** Steganografi uygulamalarının tümüne karşı etkilidir (Çıtlak, 2020).

Geliştirilmiş olan her steganografik yöntem için özel bir analiz yöntemine ihtiyaç duyulmaktadır. Bundan dolayı geliştirilmiş her steganografik yöntem için farklılık gösteren steganaliz yöntemleri geliştirilmiştir ve bu yöntemler de sadece o algoritma üzerinde uygun sonuçlar vermektedir.

Resim dosyaları üzerinde yapılan çalışmalarda steganaliz saldırısı olarak birçok yöntem mevcuttur. Bu yöntemler X^2 testi, histogram analizi, RS steganaliz, RQP yöntemi ve Görsel ataklardır. Gerçekleştirilen saldırılar sonucunda resimler içerisinde gizli veri

tespit edilir ise bu bilgileri elde etmek amacı ile çıkartma saldırıları gerçekleştirilmektedir.

X^2 testi daha çok en önemsiz bite gizleme yöntemiyle veri gizlenen resim dosyalarında kullanılmaktadır. Özellikle sıralı bir biçimde gerçekleştirilen en önemsiz bite gizleme yönteminde başarılı sonuç vermektedir. X^2 testi sonucunda sonuç 1'e yakınsa bu resmin içinde veri saklanmış demektir, eğer sonuç 0 çıkıyorsa içerisine veri saklanmamış demektir. Histogram Analizi yöntemi renklerin dağılımı hakkında bilgi veren bir yöntemdir. Bu yöntemde taşıyıcı içerisine gizlenen bilgi miktarı arttıkça histogramdaki değişim miktarı da artmaktadır. RS steganalizi yöntemi 24 bit renkli (her renk kanalı için ayrı ayrı hesaplanarak) ve 8 bit gri seviye görüntülerde kullanılmaktadır. RQP yöntemi 24 bit renkli resimler üzerinde rastgele LSB yöntemiyle gizlenen veriler için çalışmaktadır. Bu yöntem LSB gizlemesi tarafından yaratılan yakın renk çiftlerini analiz etmeye yöneliktir. Görsel ataklar yöntemi daha çok Bitmap dosyaları üzerinde uygulanan ve amacı resim dosyasındaki değişikliklerin insan gözü ile algılanabilecek hale getirmek olan bir yöntemdir (Şahin, 2007).

Ses dosyaları üzerinde yapılan steganaliz çalışmaları literatürde çok fazla mevcut değildir. Bunun sebebi ses sinyallerinin yüksek kapasiteli veri akışları olmasından dolayı, bilimsel olarak zorlayıcı istatistiksel analiz ihtiyacını gerektirir. Geliştirilen bazı ses steganaliz yöntemlerinden bir tanesi MP3 ses ortamlarının kullanıldığı MP3 ses steganaliz yöntemidir. Bu yöntem nicemleme aşaması farklılık istatistiklerini dikkate almaktadır. Ses steganaliz alanında gerçekleştirilen diğer bir yöntem VOIP konuşmalarındaki steganografiyi tespit eden ve ayrıca gizlenmiş verinin boyutunu hesaplayan bir yöntemdir. Düşük boyutlu gizlenmiş bilgilerin varlığını tespit edebildiği belirlenmiştir. En önemsiz bite gizleme yöntemi ile gizleme işlemi yapılmış ses dosyaları üzerinde gerçek zamanlı ses iletişimine dayalı bir steganaliz yöntemi geliştirilmiştir. Bu yöntemde gerçek zamanlı ses dosyalarının histogramından faydalanılmaktadır. Ses dosyaları üzerinde gerçekleştirilen başka bir steganaliz yöntemi ise türev tabanlı ses steganalizidir. Bu yöntemde bilgi gizlenmiş ses dosyalarının ikinci dereceden türevi ile elde edilen Mel-cepstrum katsayıları ile Markov geçiş özellikler ele alınmaktadır (Yalman, Çetin, Ertürk & Akar, 2014).

Video dosyları üzerinde yapılan steganaliz alanında yapılan çalışmalarda bazı önemli video steganaliz yöntemleride yer almaktadır. Bunlardan bazıları video çerçeveleri kapsamında istatistiksel görünürlük, gömü verini bozucu etkisi ve harektet verktörü gibi teknikler kullanılarak geliştirilen yöntemlerdir.

Geliştirilen video steganaliz yöntemlerindenn bir tanesi bitişik çerçeveler arasında oluşan geçici fazlalık esasına dayanmaktadır. Bu yöntemde video çerçeveleri içeriside ayrık spektrum gizliyazı yöntemi ile saklanan gizlenmiş bilgilerin tespit etmek amacı ile yapılmıştır. Geliştirilen bir başka yöntemde çerçeveler arası bağlantı esasına dayanmaktadır. Bu yöntemde birbirini takip eden video çerçevelerinin hızlı akışını bozulma/hile olarak algılamakta ve kullanılan algoritma ile gizli verinin varlığı tespit edilmektedir. Tespit etme işlemi için çerçeve hızı yavaşlatılarak şüpheli video çerçevelerine karar verilmekte ve daha sonra resim steganaliz yöntemleri kullanılarak çıkartma işlemi gerçekleşmektedir. Gerçekleştirilen bir başka yöntemde ise bozucu etki ve olasılık kütle fonksiyonu temel alınmaktadır. Bu yöntemde video steganografi teknikleri ile veri gömülme işleminden sonra videoların fark işareti ortaya çıkmaktadır ve veri gömülmesi ike oluşan değişiklikler sonucunda orijinal dosya ile veri gömülmüş dosya arasında frekans farkı olduğu ortaya çıkmakta ve Haar dalgacık filtresi kullanılarak gizli bilgi tespiti yapılmaktaıdır. Gerçekleştirilen bir başka video steganaliz tekniğinde hareket vektörleri temel alınmıştır. Uzay ve zaman düzlemlerindeki hareket vektörleri arasındaki bağlantılar değerlendirilerek 12 boyutlu istatistiksel bir özellik vektörü ortaya çıkmakta ve bu vektör makinesi ile eğitilen bu vektör sayesinde gömü verisi ortaya çıkmaktadır (Yalman, Çetin, Ertürk & Akar, 2014)

BÖLÜM 5

MATERYAL VE METOT

Gelişen teknoloji ile birlikte günümüzde tüm iletişim ortamlarında güvenlik kavramına ihtiyaç duyulmaktadır. Dijital imza ve kriptografi gibi oluşabilecek güvenlik sorunlarına çözüm sağlamak amacı ile farklı yöntemler kullanılmaktadır, ancak bu teknikler tek başına yeterli olamazlar. Steganografi kavramı, gizli bilgilerin varlığını gizlediği için karşılaşabilecek sorunlara karşı en iyi çözümdür.

Bu tez çalışmasında geliştirilen steganografi uygulamaları MATLAB programı ile gerçekleştirilmiştir. MATLAB MathWorks şirketi tarafından geliştirilmiş olan yüksek performanslı dördüncü nesil programlama dilidir. Kullanımı basit olan dördüncü nesil programlama dilleri sayesinde uzun kodlar yazmaya gerek kalmadan hazır şablonlar kullanarak belirli ihtiyaçlar için çözümlere geliştirilebilmektedir. MATLAB kullanıcılara Java, C, C++ gibi diller ile geliştirilmiş olan programlar ile çalışma olanağı sağlayabilmektedir. MATLAB kullanarak algoritma geliştirilebilir, matris işlemleri, fonksiyon ve veri çizme işlemlerinin yansıra kullanıcı ara yüzü oluşturulabilmektedir.

Önerilen bu yöntem, LSB ekleme yaklaşımını kullanarak video dosyalarına bilgi yerleştirme ve gömülü verilerin çıkarılması için video steganografi yöntemi sunmaktadır.

Gerçekleştirilen uygulamada bilgileri gizlemek için gizleme yöntemi ve gizli bilgileri çıkartmak için çıkartma yöntemi kullanılmaktadır. Gizlenen bilgilerin güvenliğini arttırmak amacı ile şifreleme teknikleri kullanılmıştır. LSB yönteminin steganalizi için birçok yöntem mevcuttur.

Gizleme işlemleri için olan bölümde gizleme işlemi 2 ayrı şekilde yapılmaktadır. Bu yöntemler sıralı ve rasgele şekildedir. Sıralı gizleme işleminde gizlenecek verinin bitleri her çerçevenin ilk pikselinden başlayarak kaç bit gizlenecek ise kadar piksel kullanılarak saklanır.

Gizlenmek istenen verinin rastgele şekilde saklanması istendiğinde ise bir fonksiyon kullanılmaktadır.

Bu fonksiyon:

f = (ax + b) mod c şeklindedir.

Bu fonksiyonda x değişkeni gizlenecek biti, c veri gizlemek için kullanılabilecek çerçeve sayısını ifade etmektedir. a ve b değerleri ise rastgeleliği sağlamak amacıyla kullanılan asal sayılardır.

Örnek olarak "a" harfi 5 sn'lik ve fps değeri 20 olan bir video içerisine gizlemek istersek. Formüle göre c değerimiz yani çerçeve sayımız 5 x 20 = 100 olarak belirlenmektedir. x değerimiz gizlenecek bit ve a sayımız 7, b sayımız 13 olarak belirlendiğinde gizleme işlemi şu şekilde gerçekleşmektedir:

"a" harfinin ASCII kodu 97 ve ikilik karşılığı "01100001" şeklindedir.

f = (ax + b) mod c formülü uygulandığında a harfinin bitleri

1.bit f = (7x1 + 13) mod 100 = 20. çerçeveye

2.bit: f = (7x2 + 13) mod 100 = 27. çerçeveye

3. bit f = (7x3 + 13) mod 100 = 34. çerçeveye

4.bit f = (7x4 + 13) mod 100 = 41. çerçeveye

5.bit: f = (7x5 + 13) mod 100 = 48. çerçeveye

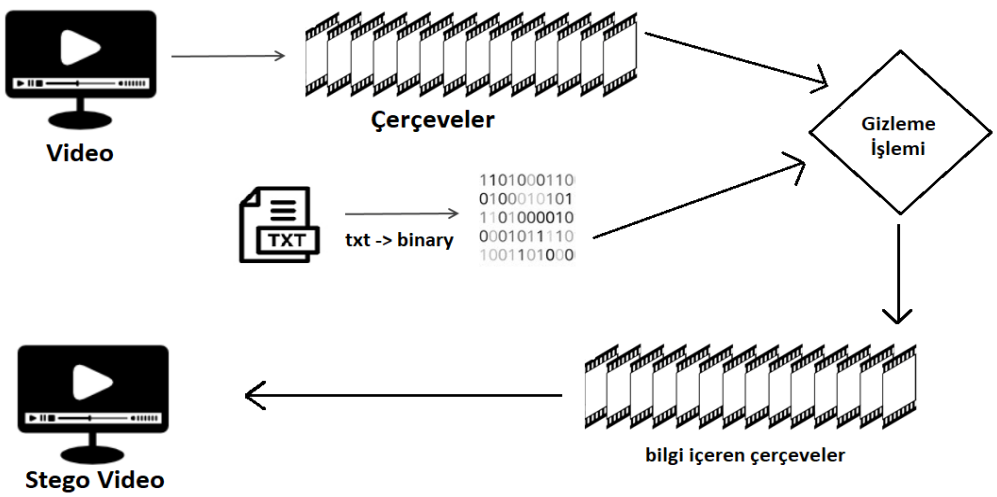
6. bit f = (7x6 + 13) mod 100 = 55. çerçeveye

7.bit: f = (7x7 + 13) mod 100 = 62. çerçeveye

8. bit f = (7x8 + 13) mod 100 = 69. çerçeveye

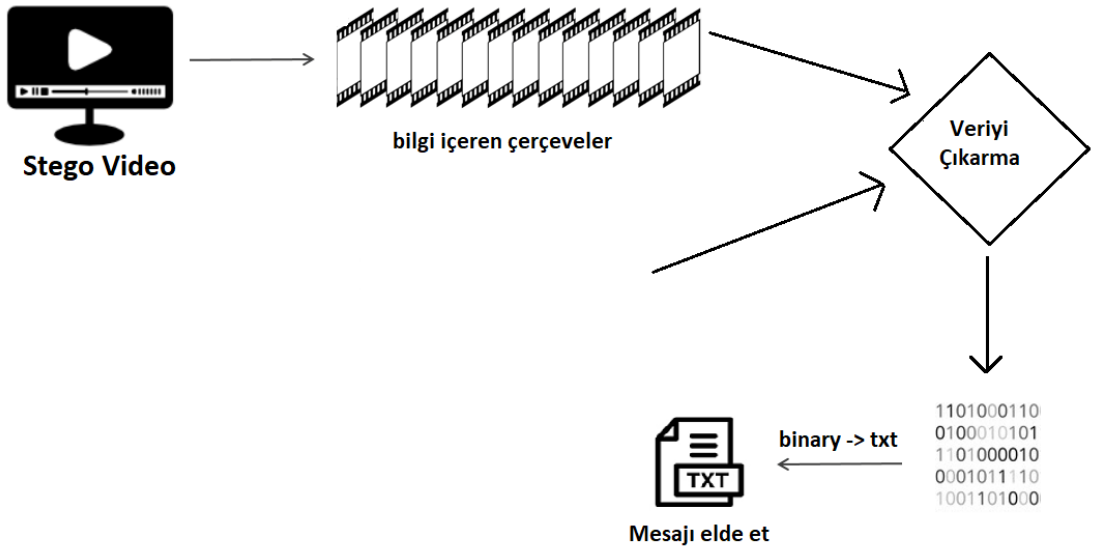
gizlenecek şekilde gerçekleşmektedir.

Şekil 5.1.'de gerçekleştirilen gizleme işlemi gösterilmektedir. Orijinal video çerçevelere ayrılarak sıralı veya rasgele gizleme işlemi yapılmaktadır. Gizlenecek olan veri text den binary e dönüştürüldükten sonra çerçevelerin en önemsiz biti ile yer değiştirilerek gizlenir. Daha sonra bilgi içeren çerçeveler tekrardan birleştirilerek stego video haline getirilmektedir.



Şekil 5.1. Uygulanan gizleme işlemi

Şekil 5.2.'de gizlenen veriyi geri elde etmek için kullanılan işlem gösterilmektedir. Stego video içerisinde yer alan bilgiler sıralı veya rastgele gizleme işleminden hangisi yapıldıysa bu işlemlerin tersi uygulanarak çerçevelerden binary veri olarak elde edildikten sonra dönüştürülerek orijinal mesaj elde edilmektedir.



Şekil 5.2. Veriyi geri elde etme işlemi

Gizleme için kullanılan algoritmanın daha güçlü olmasını sağlamak amacıyla gizlenecek verinin şifrelenmesi ek güvenlik özelliği olarak konulmuştur. Bu çalışmada AES ve RSA şifreleme algoritmaları seçilmiştir. AES bir simetrik şifreleme algoritması

iken RSA asimetrik şifreleme algoritmasıdır. Bu sayede simetrik ya da asimetrik şifreleme yönteminin bilgi gizlemedeki etkisi de incelenmiş olacaktır.

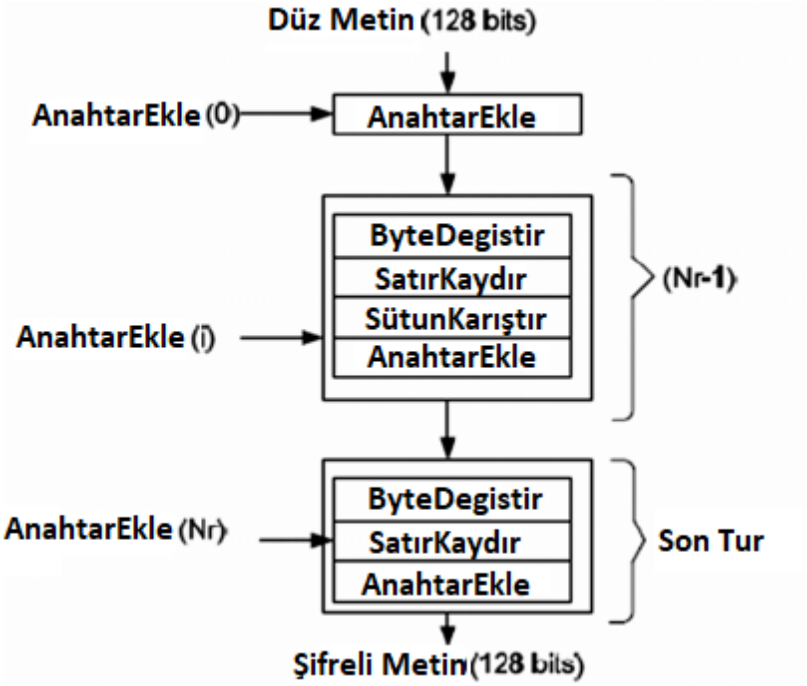
Gizleme işlemleri sırasında örtü verisi ve stego veri arasında boyut farkı oluşmaması çok önemlidir. Bu çalışmada da orijinal ve veri gizlenmiş videoların boyutları aynıdır.

Önerilen yöntemde bilgi gizleme işlemini gerçekleştirebilmek için MATLAB programı ile bir uygulama geliştirilmiştir. Bu uygulamada bilgi gizlemek için bir ekran ve analiz işlemleri için ayrı bir ekran bulunmaktadır.

AES (Gelişmiş Şifreleme Standardı)

Simetrik bir şifreleme algoritması olan AES (Standard A.E., 2001), bir yarışma sonucunda standart olarak kabul edilmiş olan bir blok şifreleme yöntemidir. AES simetrik bir şifreleme yöntemi olduğu için tek anahtar kullanmaktadır, bu anahtar ile hem şifreleme hem de şifre çözme işlemi gerçekleştirilmektedir. AES algoritmasında giriş ve çıkış blokları 128 bit olmak zorundadır. Anahtar uzunlukları döngü sayısına bağlı olarak 128, 192 veya 256 bit olabilmektedir. Algoritma aynı işlemleri içeren birden fazla döngüyü yürütmektedir (Doğan, 2008).

AES algoritmasında yer alan iki bloğun kendi içerisinde çeşitli adımları bulunmaktadır. Tur dönüşüm bloğunun adımları; bayt değiştirme, satır kaydırma, sütun karıştırma ve turdaki anahtar ile toplama adımlarından oluşurken, anahtar üretim bloğunun adımları ise her bir tur dönüşüm bloğu için anahtar üretimi gerçekleştirmektir. Bu iki blok birbiri ile paralel bir şekilde çalışmaktadır (Öztemür, 2012).



Şekil 5.3. AES algoritması.

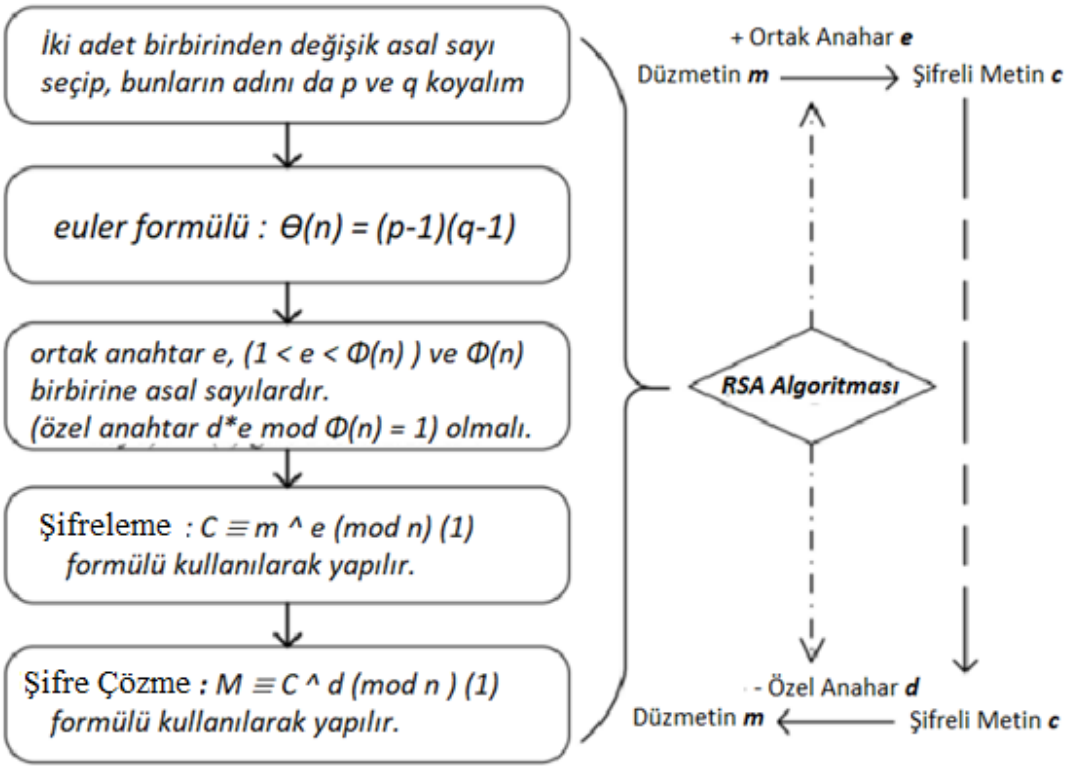
(Mohan & Reddy ,2012)

RSA Algoritması

RSA şifreleme algoritması (Rivest R.L. vd., 1978) iki farklı anahtar kullandığı için asimetrik şifreleme algoritmaları arasında yer almaktadır. Bu anahtarlar genel ve özel anahtar olarak adlandırılmaktadır. Genel anahtar herkes tarafından bilinirken özel anahtar sadece gönderici ve alıcı tarafından bilinmektedir.

RSA çok büyük tam sayıların çarpımı olarak işlem yapmanın zorluğuna dayanan bir algoritmadır ve algoritmanın güvenilirliği buna dayanmaktadır. Algoritmanın güvenilirliği bu tamsayıların büyüklüğü ile doğru orantılıdır. En büyük dezavantajı ise simetrik sistemlere göre daha yavaş çalışmasıdır. Kullanıcı sayısı fazla olan uygulamalar, web siteleri vb. platformlarda güvenli veri paylaşımına olanak sağlamaktadır. Bunun yanı sıra sayısal imza yöntemleri ile birlikte kimlik doğrulama işlemlerinde de kullanılmaktadır.

Şekil 5.4.'te RSA algoritmasının gerçekleşme aşamaları gösterilmektedir.



Şekil 5.4. RSA algoritması

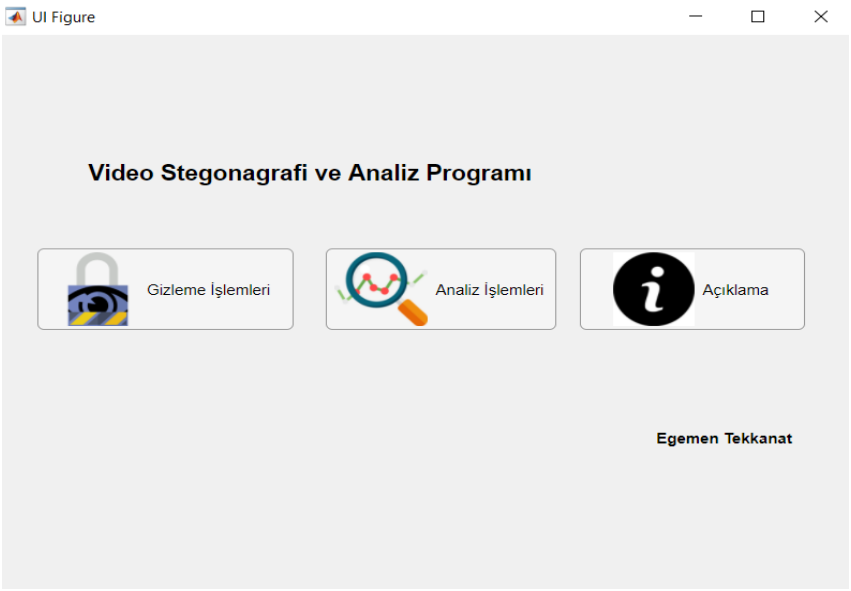
(Yin vd. 2021)

5.1. Geliştirilen video steganografi uygulaması

Önerilen yöntemde video formatı olarak AVI tercih edilmektedir. AVI formatındaki videolar, ses ve görüntünün birleştirilmesi ile oluşmuş ve sıkıştırılmamış BMP formatındaki resimlerin artarda eklenmesi ile oluşmaktadır. AVI dosyaları, farklı veri türlerinin birden çok akışını içerir. Çoğu AVI dizileri hem ses hem de video akışlarını kullanır.

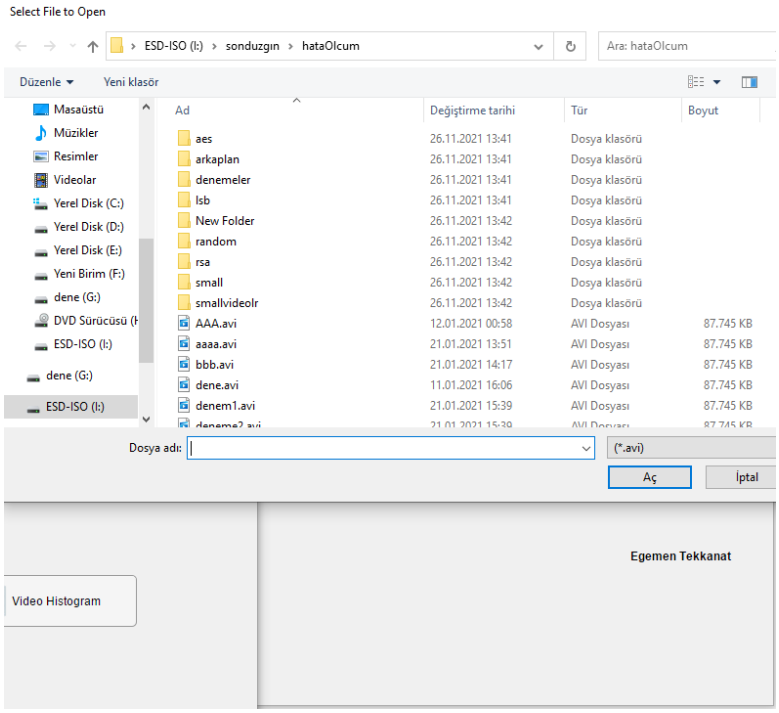
Önerilen yöntemde gömme işlemi için avı formatındaki videonun bilgileri gerçekleştirilen program tarafından alındıktan sonra videonun gömme kapasitesi ile gizli mesajın boyutu karşılaştırılmaktadır. Eğer mesajı boyutu kapasiteyi aşmıyor ise gömme işlemine devam edilmektedir. Gömme yöntemi seçme aşamasında sıralı ve rastgele yöntemlerden biri seçilmektedir. Eğer şifreleme teknikleri ile güvenlik arttırılmak istenirse AES veya RSA tekniklerinden biri seçilerek gömme işlemi şifrelenerek devam etmektedir. Aksi durumda şifreleme uygulanmamaktadır.

Şekil 5.5.'te programın giriş ekranı gözükmektedir. MATLAB ortamında geliştirilen bu ekranda program ile açıklamalar için açıklama adında bir buton, gizleme işlemi ekranına geçmek için gizleme işlemleri adında bir buton ve gizlenen video dosyası ile ilgili işlemlere geçmek için de analiz işlemleri adında ayrı bir buton yer almaktadır.

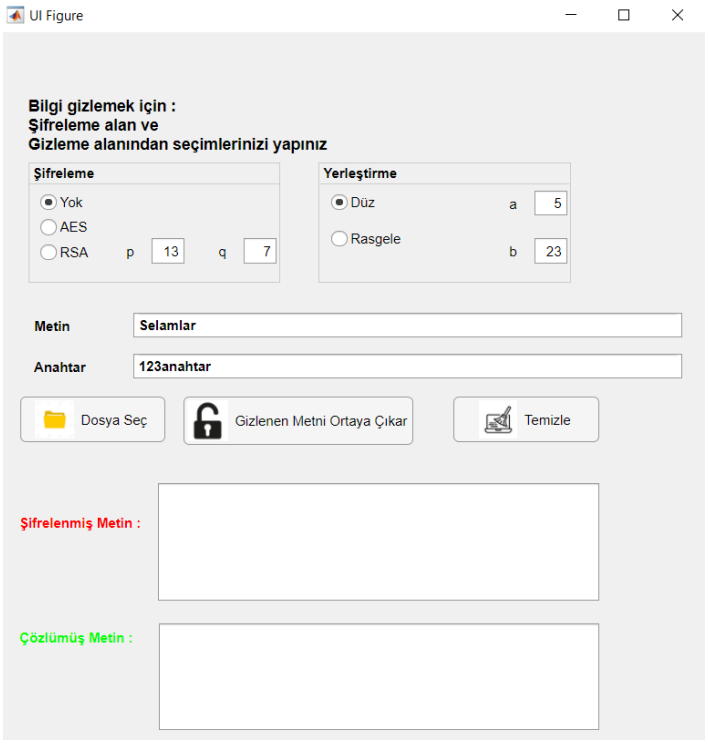


Şekil 5.5. Program giriş ekranı

Şekil 5.6.'da geliştirilen program üzerindeki dosya seçim ekranı gözükmektedir. Şekil 5.7.'de ise gizleme ekranı yer almaktadır. Bu ekranda video dosyaları üzerinde gizleme işlemi gerçekleştirmek için program üzerinden dosya seç butonu ile video dosyasını seçmeden önce sıralı ya da rastgele yöntemlerinden bir tanesi seçerek gizleme yöntemi belirlenmektedir. Eğer bir şifreleme algoritması kullanılmak istenilirse AES veya RSA seçeneklerinden biri seçilerek video üzerinde uygulanmaktadır. Veri gizlenmiş video üzerindeki bilgiyi geri elde etmek için de gizlenen metni ortaya çıkarma işlemi ile video üzerinde gizlenmiş olan veriler ortaya çıkartılmaktadır. Ortaya çıkan gizli bilgiler çözülmüş metin alanında gözükmektedir. Şifreleme Algoritmaları arasından RSA şifreleme algoritmasını tercih edildiğinde asal sayılar kullanıcı tarafından girilmektedir. Aynı şekilde rastgele gizleme algoritması seçildiğinde de formülde belirtildiği gibi asal sayılar seçilebilmektedir.

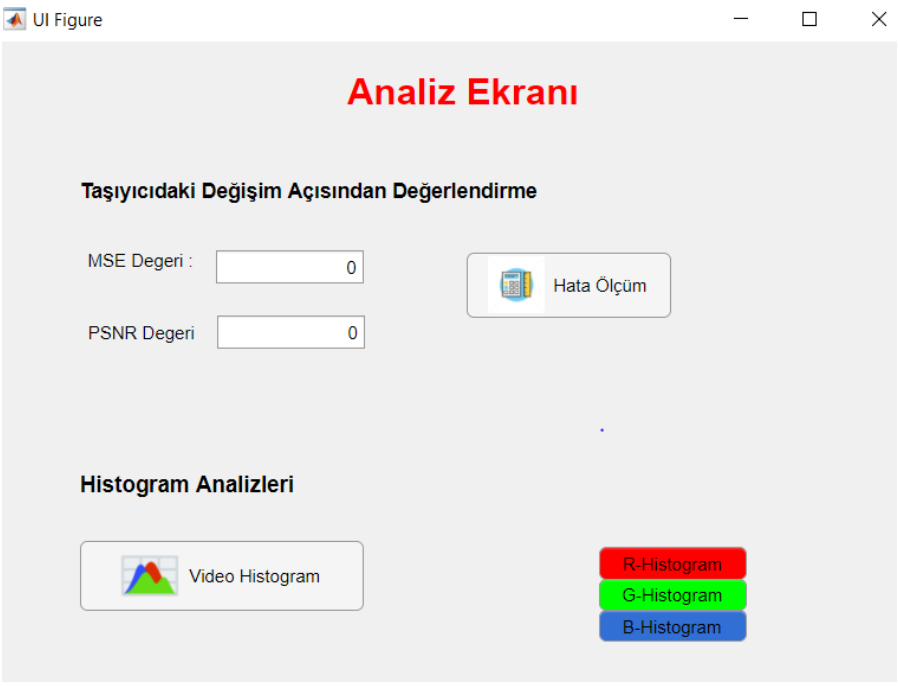


Şekil 5.6. Dosya seçim ekranı



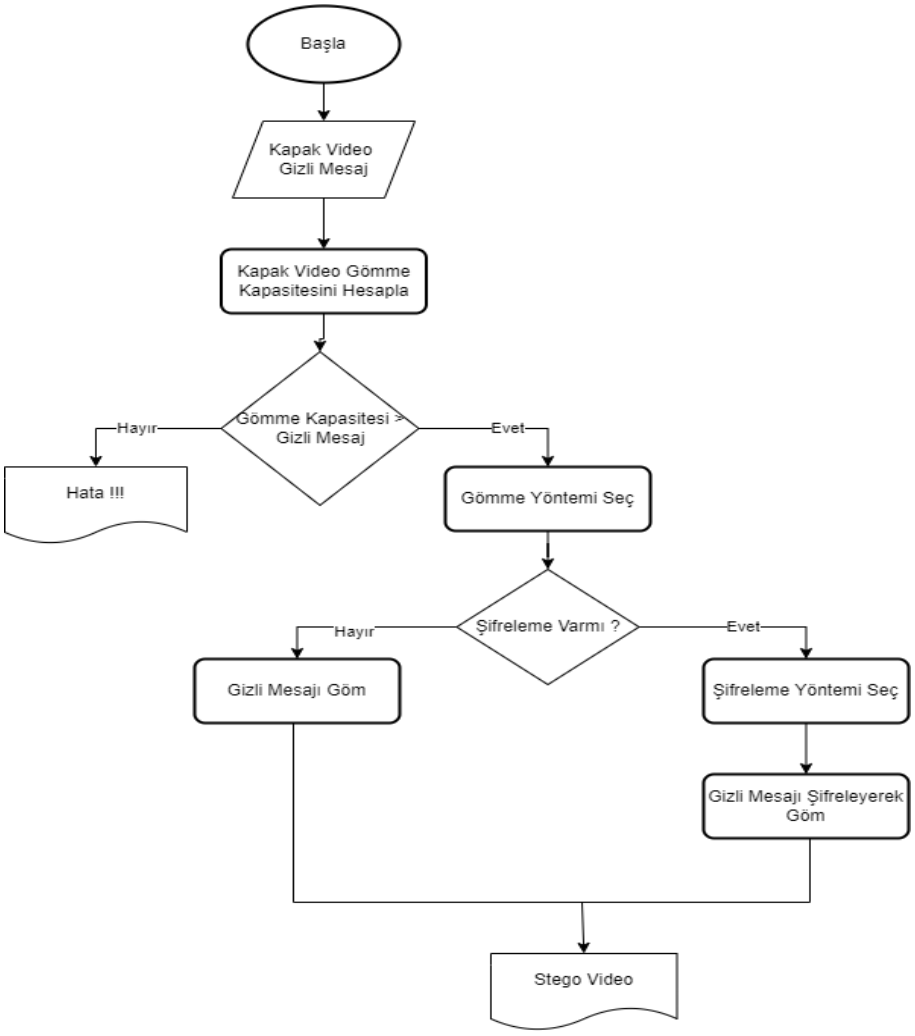
Şekil 5.7. Gizleme ekranı

Şekil 5.8.'de analiz ekranı yer almaktadır. Bu ekranda bilgi gizlenmiş olan videoların analiz işlemleri gerçekleşmektedir. Bu ekranda taşıyıcıdaki değişim ve dayanıklılık analizleri ayrı butonlarda yapılmaktadır. Hata ölçüm adlı butona tıklandığı zaman orijinal dosya ile bilgi gizlenmiş videoların seçilmesi istenmektedir. Gerçekleşen bu işlem sonrasında da iki video arasındaki MSE ve PSNR değerleri hesaplanmaktadır. Video histogram isimli butona tıklandığında ise histogram analizi yapılmak istenilen video seçilerek videoya ait histogram grafiği oluşturulup gösterilmektedir.



Şekil 5.8. Analiz ekranı

Şekil 5.9.'da önerilen yöntem için kullanılan gömme algoritması gözükmektedir. Kaynak video alındıktan sonra bilgiler gömme işlemine geçilmektedir. Bu işlem için öncelikle sırala ya da rastgele yöntemlerden bir tanesi seçilmektedir. Daha sonra isteğe bağlı olarak program üzerinde var olan AES ve RSA şifreleme algoritmalarından biri seçilebilmektedir. Şifreleme algoritması kullanılmamak da alternatifler arasında yer almaktadır. Tüm bu işlemler tamamlandıktan sonra gizlenmek istenen metin program üzerinde eklenerek seçilen kaynak video içerisine bu bilgiler gizlenmektedir.



Şekil 5.9. Gömme algoritması

Önerilen yöntemde bilgileri çıkartma işleminde karşı taraftan gelen stego video alındıktan sonra stego video içerisindeki bilgiler okunmaktadır. Eğer içerisinde bilgi var ise çıkartma işlemi gerçekleştirilir. Çıkan mesaj anlamsız bir mesaj şeklinde çıkmış işe AES veya RSA tekniklerinin şifre çözme adımları gerçekleştirilmektedir. Böylece gizli mesaj ortaya çıkmış olacaktır.

5.2. Geliştirilen Uygulamanın Değerlendirilmesi

Video dosyaları üzerinde gizleme işlemi tamamlandıktan sonra taşıyıcı üzerindeki değişimi hesaplamak için PSNR ve MSE değerlerini hesaplama yapılmaktadır. Orijinal dosya ile veri gizlenmiş dosya seçilerek bu işlemler gerçekleştirilmektedir. Steganaliz için histogram analizi yapılmaktadır.

Bilgi gizleme için avı formatı tercih edilmiştir. Bilgi gizleme işlemi sırasına herhangi bir değişim söz konusu değildir.

5.2.1. Kapasite Açısından Değerlendirilmesi

Geliştirilen uygulama da kullanılan en önemsiz bite uygulama yönteminde kapasite dosya boyutu ile ilgili olmaktadır. Bilgi gizlenmiş video dosyası ile orijinal dosya arasında bu yöntem dışına çıkıldığında kapasitede farklılıklar gözükebilmektedir. Bilgi gizleme işlemi için kullanılan avı formatındaki videolar ile orijinalleri arasında herhangi bir boyut farkı gözükmemektedir.

5.2.2. Taşıyıcıdaki Değişim Açısında Değerlendirilmesi

Taşıyıcıdaki değişimi değerlendirmek amacıyla birçok video dosyası üzerinde ölçümler yapılmıştır. Tezde göstermek amacıyla videolardan iki tanesi seçilmiştir. Taşıyıcıdaki değişimi belirlemek amacıyla PSNR ve MSE ölçümleri yapılmıştır.

Çizelge 5.1.'de Video 1 dosyası üzerine 0.1 KB' den başlanarak 450 KB 'ye kadar yapılan gizleme işlemi sonuçları gösterilmektedir. Geliştirilen uygulama kullanılarak veri gizleme işlemleri sonucunda elde edilen PSNR ve MSE değerleri incelenmiştir. Gizlenen verinin boyutu arttıkça MSE değerlerinin de büyüdüğü buna karşılık PSNR değerlerinin azaldığı gözlenmiştir. Yüksek PSNR değerine karşılık küçük MSE değerleri videonun çok fazla bozulmadığını göstermektedir.

Bilgi gizlenen Video 1 dosyasının boyutu 7.99 MB'dir.

Çizelge 5.1. Video 1 değerleri

Sıralı Gizleme				**Rastgele Gizleme**		
	MSE	**PSNR**			**MSE**	**PSNR**
450 KB	5.553	55,3612		**450 KB**	5.581	55.352
200 KB	5.552	55,3611		**200 KB**	5.580	55.351
116 KB	3.258	57.668		**116 KB**	3,217	57.660
60 KB	1.621	60.687		**60 KB**	1.634	60.672
30 KB	0.7759	63.886		**30 KB**	0.7798	63.881
12 KB	0.4721	66.056		**12 KB**	0.4735	66.055
10 KB	0.2803	68.323		**10 KB**	0.2807	68.331
7.5 KB	0.2196	69.384		**7.5 KB**	0.2195	69.394
6 KB	0.1818	70.200		**6 KB**	0.1825	70.202
4 KB	0.1118	72.306		**4 KB**	0.1116	72.327
3 KB	0.0998	72.794		**3 KB**	0.0999	72.812
2 KB	0.0562	75.264		**2 KB**	0.0565	75.289
1 KB	0.0310	77.836		**1 KB**	0.0321	77.780
0.6 KB	0.0175	80.334		**0.6 KB**	0.1795	80.289
0.3 KB	0.0095	82.961		**0.3 KB**	0.0098	82.942
0.1 KB	0.0035	87.226		**0.1 KB**	0.0035	87.408

Şifreleme işleminin etkisini incelemek amacıyla Video 1 dosyası üzerinde bilgi gizleme işlemleri sıralı, rastgele ve şifrelenerek gerçekleştirilmiştir. Çizelge 5.2.'de bu gizleme işlemleri sonucunda elde edilen MSE ve PSNR değerlerindeki değişimler hesaplanmıştır. RSA şifreleme algoritması kullanılarak yapılan gizleme işlemlerinin AES şifreleme algoritmasına göre daha iyi sonuçlar verdiği gözlemlenmiştir.

Çizelge 5.2. Video 1 Şifrelenmiş gizleme değerleri

	Sıralı Gizleme					**Rastgele Gizleme**			
	RSA		**AES**			**RSA**		**AES**	
	MSE	**PSNR**	**MSE**	**PSNR**		**MSE**	**PSNR**	**MSE**	**PSNR**
450 KB	5.553	55.361	5.530	55,364		5.581	55.352	5.563	55.348
200 KB	5.552	55.361	5.533	55,363		5.580	55.3515	5.563	55.3517
60 KB	1.621	60.687	2.157	59,439		1.634	60.673	2.172	59.425
12 KB	0.4721	66.056	0.6256	64,817		0.4735	66.055	0.6289	64.805
7.5 KB	0.2196	69.384	0.2923	68,136		0.2195	69.394	0.2924	68.135
2 KB	0.0562	75.264	0.0752	74,021		0.0565	75.282	0.0759	73.994
0.6 KB	0.0175	80.334	0.0233	79,054		0.0179	80.289	0.0237	79.039
0.1 KB	0.0035	87.226	0.0048	85,917		0.0035	87.408	0.0048	85.946

Çizelge 5.3.' de Video 2 dosyası üzerine 0.1 KB'den başlanarak 450 KB' ye kadar yapılan gizleme işlemi sonuçları gösterilmektedir. Yine PSNR ve MSE değerleri ölçülmüş ve tabloda verilmiştir.

Bilgi gizlenen Video 2 dosyasının boyutu ise 5.99 MB'dir.

Çizelge 5.3. Video 2 Değerleri

Sıralı Gizleme				**Rastgele Gizleme**		
	MSE	**PSNR**			**MSE**	**PSNR**
450 KB	1.304	55,3824		**450 KB**	1.326	55.344
200 KB	1.303	55,3823		**200 KB**	1.326	55.344
116 KB	1.023	56.431		**116 KB**	1.325	55.356
60 KB	0.5090	59.455		**60 KB**	1.042	56.393
30 KB	0.2432	62.658		**30 KB**	0.5223	59.398
12 KB	0.1486	64.819		**12 KB**	0.2502	62.594
10 KB	0.0864	67.135		**10 KB**	0.1525	64.756
7.5 KB	0.0681	68.182		**7.5 KB**	0.0900	67.042
6 KB	0.0564	68.994		**6 KB**	0.0704	68.116
4 KB	0.0349	71.079		**4 KB**	0.0579	68.945
3 KB	0.0312	71.569		**3 KB**	0.0357	71.042
2 KB	0.0177	74.023		**2 KB**	0.0319	71.535
1 KB	0.0100	76.516		**1 KB**	0.0176	74.045
0.6 KB	0.0058	78.976		**0.6 KB**	0.0098	76.579
0.3 KB	0.0032	81.621		**0.3 KB**	0.0055	79.106
0.1 KB	0.0011	85.907		**0.1 KB**	0.0030	81.755

Video 2 dosyası üzerinde bilgi gizleme işlemleri sıralı, rastgele ve şifrelenerek gerçekleştirilmiştir. Çizelge 5.4.'de bu gizleme işlemleri sonucunda elde edilen MSE ve PSNR değerlerindeki değişimler hesaplanmıştır. Veri boyutu büyüdükçe MSE değeri artmakta PSNR değeri ise azalmaktadır. RSA şifreleme algoritması kullanılarak yapılan gizleme işlemlerinin AES şifreleme algoritmasına göre daha iyi sonuçlar verdiği gözlemlenmiştir.

Çizelge 5.4. Video 2 Şifrelenmiş gizleme değerleri

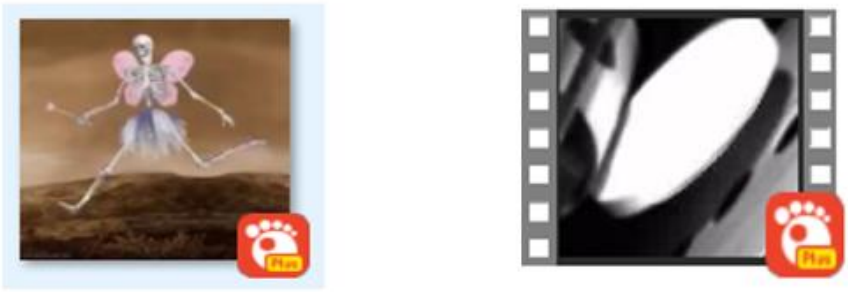
	Sıralı Gizleme					**Rastgele Gizleme**			
	RSA		**AES**			**RSA**		**AES**	
	MSE	**PSNR**	**MSE**	**PSNR**		**MSE**	**PSNR**	**MSE**	**PSNR**
450 KB	1.304	55.382	1.2999	55,382		1.326	55,344	1.322	55.342
200 KB	1.304	55.383	1.2999	55,380		1.325	55,3459	1.321	55.3458
60 KB	0.5089	59.456	0.6784	58,199		0.5223	59,397	0.6944	58.145
12 KB	0.1486	64.819	0.1972	63,570		0.1525	64,756	0.2016	63.519
7.5 KB	0.0681	68.182	0.0898	66,952		0.0704	68,116	0.0938	66.845
2 KB	0.0177	74.023	0.0237	72,759		0.0176	74,045	0.0241	72.707
0.6 KB	0.0058	78.976	0.0076	77,736		0.0055	79,106	0.0073	77.811
0.1 KB	0.0011	85.907	0.0016	84,470		0.0011	85,991	0.0016	84.470

Çizelgelerden da görüldüğü üzere geliştirilen uygulama ile yapılan bilgi gizleme işlemleri taşıyıcıdaki değişim açısından iyi sonuçlar vermektedir. Sıralı ve rastgele yapılan gizleme işlemlerinden rastgele veri gizlemenin daha iyi sonuçlar verdiği gözlemlenmiştir.

Renk dağılımı ve yoğunluğunun bilgi gizlemeye etkisini incelemek amacıyla aynı büyüklükte olan ama farklı renk aralıklarına sahip video dosyalarına veri gizleme işlemi yapılmıştır. Bu videolardan iki tanesi örnek olarak sunulmuştur.

Çizelge 5.5. ve çizelge 5.6.'da birbirine yakın boyutlarda ve farklı renkler içeren videoların MSE ve PSNR analizleri sıralı ve rastgele olarak gerçekleştirilmiş ve aralarındaki farklar incelenmiştir. Çizelge 5.5.'te yer alan video boyutu 18.4 MB olup video içeriği Video 4'e göre daha renklidir. Çizelge 5.6.'da yer alan videonun boyutu 17.9 MB olup video içeriği siyah beyaz ağırlıktadır.

Şekil 5.10.’ da Video 3 ve Video 4 e ait ekran görüntüleri yer almaktadır.



Şekil 5.10. Video3 ve Video 4 görselleri

Çizelge 5.5. Video 3 Değerleri

Sıralı Gizleme				**Rastgele Gizleme**		
	MSE	**PSNR**			**MSE**	**PSNR**
450 KB	8,171904	55,4111		**450 KB**	8,181987	55,4023
200 KB	3,795572	58,7626		**200 KB**	3,767449	58,7734
116 KB	2,070903	61,3823		**116 KB**	2,060353	61,3807
60 KB	1,030039	64,4079		**60 KB**	1,029531	64,3934
30 KB	0.489045	67,6219		**30 KB**	0.490678	67,6063
12kb	0.294604	69,8188		**12 KB**	0.296435	69,7909
7.5kb	0.136668	73,156		**7.5 KB**	0.137179	73,136
6 KB	0.113706	73,9682		**6 KB**	0.113608	73,9573
4kb	0.070274	76,0571		**4 KB**	0.070170	76,0545
3 KB	0.062753	76,5542		**3 KB**	0.062331	76,5513
2 KB	0.035994	78,9724		**2 KB**	0.035540	79,0056
1 KB	0.019773	81,5328		**1 KB**	0.019918	81,5432
0.6 KB	0.011216	84,0117		**0.6 KB**	0.011331	83,9969
0.3 KB	0.006040	86,6948		**0.3 KB**	0.006232	86,6306
0.1 KB	0.002246	91,0136		**0.1 KB**	0.002323	90,9529

Daha renkli olan Video 3'e ait PSNR ve MSE değerlerini gösteren Çizelge 5.5.' ten görüleceği üzere sıralı veya rastgele veri gizleme arasında çok anlamlı farklar olmadığı ortaya çıkmıştır.

Çizelge 5.6. Video 4 Değerleri

Sıralı Gizleme				**Rastgele Gizleme**		
	MSE	**PSNR**			**MSE**	**PSNR**
450 KB	14,89066	55,3612		**450 KB**	15,38314	55,2902
200 KB	6,906542	58,6598		**200 KB**	7,303759	58,5332
116KB	3,7539	61,2834		**116KB**	4,018071	61,1288
60 KB	1,897949	64,2661		**60 KB**	2,035807	64,1094
30 KB	0.908946	67,4602		**30 KB**	0.968549	67,3176
12 KB	0.550368	69,641		**12KB**	0.582378	69,5192
7.5 KB	0.251459	73,019		**7.5 KB**	0.267301	72,8921
6 KB	0.209157	73,8298		**6 KB**	0.221251	73,7116
4KB	0.128553	75,9311		**4 KB**	0.136235	75,821
3 KB	0.113552	76,4493		**3 KB**	0.120757	76,3349
2 KB	0.063964	78,9362		**2 KB**	0.068831	78,7937
1 KB	0.036268	81,4065		**1 KB**	0.038302	81,3122
0.6 KB	0.020806	83,8646		**0.6 KB**	0.020155	83,9445
0.3 KB	0.011393	86,5172		**0.3 KB**	0.010877	86,6597
0.1 KB	0.004286	90,761		**0.1 KB**	0.004220	90,7822

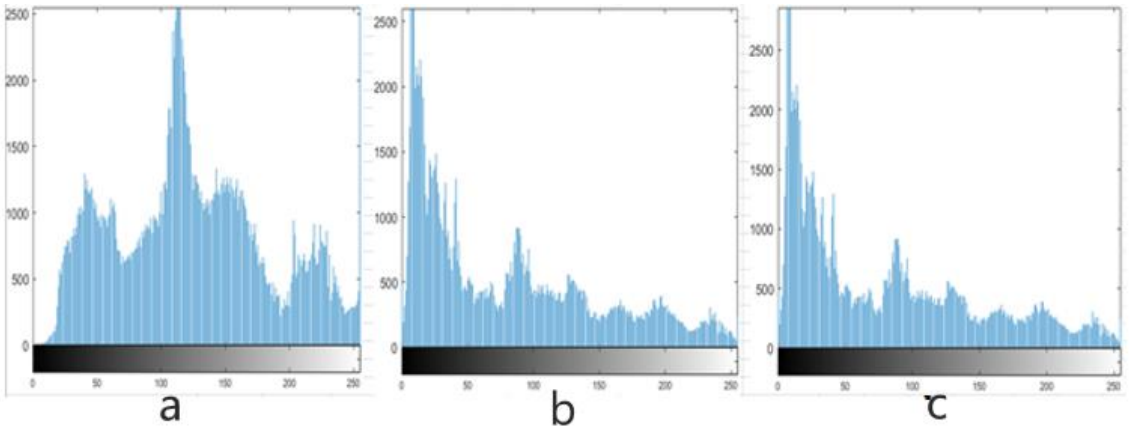
Çizelge 5.6.'da içeriği siyah beyaz olan Video 4 dosyasına ait MSE ve PSNR değerleri bulunmaktadır. Elde edilen ölçümler sonucunda siyah beyaz içeriğe sahip video dosyasında saklanan veri miktarlarında arttıkça bozulma daha belirgin hale gelmektedir.

Birbiri ile benzer uzunlukta ve renk değerleri birbirine farklılık gösteren bu iki video ile gerçekleştirilen PSNR ve MSE analizleri sonrasında video içeriği daha renkli olan Video 3' deki bozulma oranının video içeriği siyah beyaz olan Video 4' e göre daha az olduğu görülmektedir.

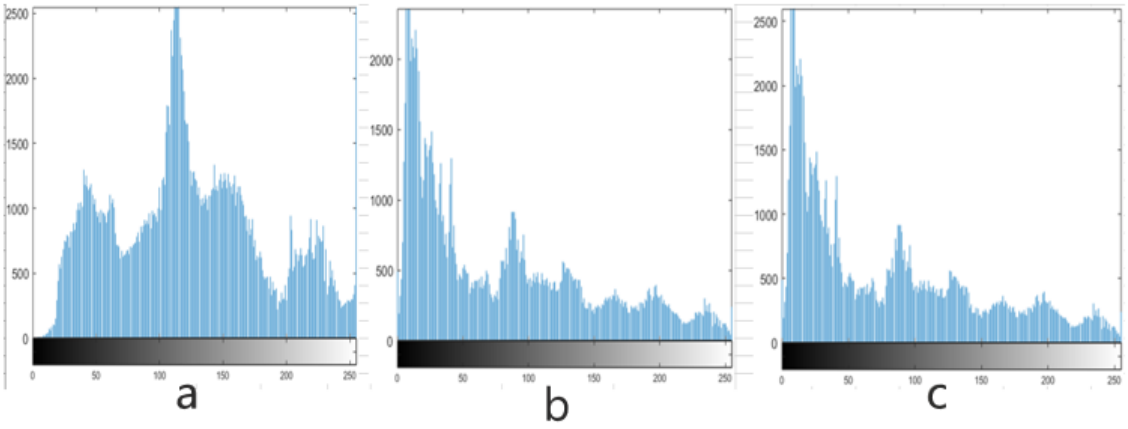
5.2.3. Dayanıklılık Açısından Değerlendirilmesi

Geliştirilen Video Steganografi programının dayanıklılık açısından değerlendirilmesi için histogram analizi yöntemi kullanılmıştır. Histogram analizi yöntemini uygulamak için program içerisinde video histogram ara yüzü tasarlanmıştır.

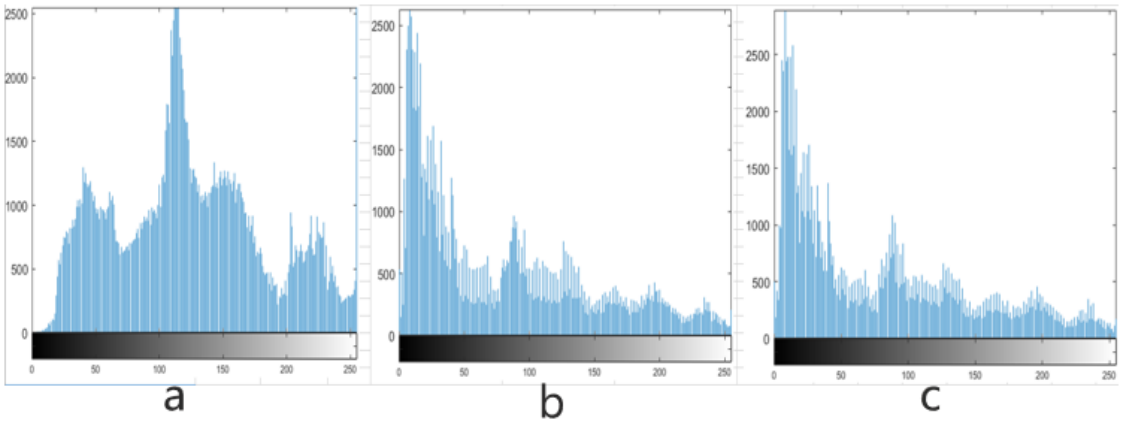
Geliştirilen yöntem video dosyalarındaki renklerin dağılımı hakkında bilgi veren bir yöntemdir. Orijinal dosya ile Bilgi gizlenmiş dosya arasındaki değişim analiz edilmektedir. Orijinal dosyanın elimizde olduğu durumlarda histogram analizi ile gizli verinin varlığı tespit edilebilmektedir. Orijinal video dosyasının video histogram grafiği elde edildikten sonra aynı boyutta olmak şartı ile sıralı ve rastgele bilgi gizlenmiş olan video dosyalarının histogram grafikleri elde edilmekte ve karşılaştırmaları yapılmaktadır.



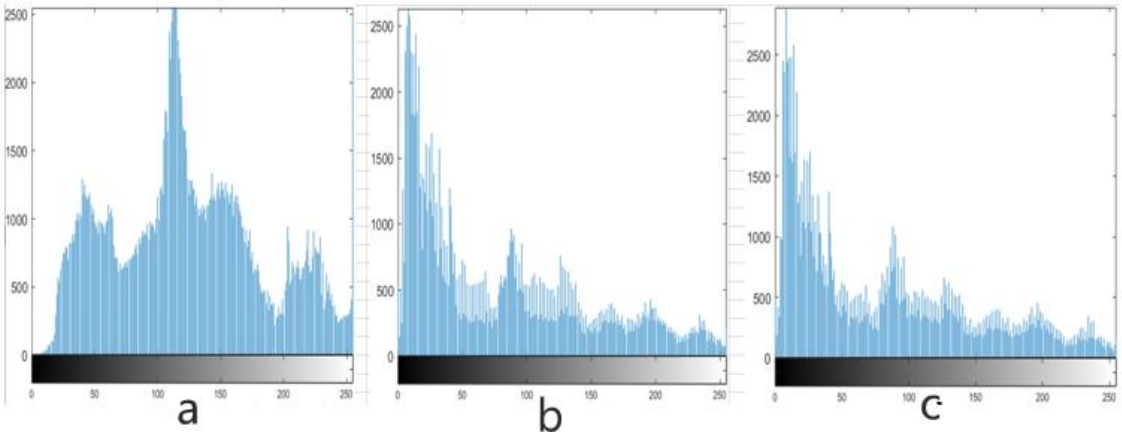
Şekil 5.11. Video1 dosyası için **(a**) Veri gizlenmemiş videonun histogram grafiği **(b)** Sıralı şekilde 0,1 KB veri gizlenmesiyle oluşan videonun histogram grafiği **(c)** Rastgele şekilde 0,1 KB veri gizlenmesiyle oluşan videonun histogram grafiği



Şekil 5.12. Video1 dosyası için **(a**) Veri gizlenmemiş videonun histogram grafiği **(b)** Sıralı şekilde 30 KB veri gizlenmesiyle oluşan videonun histogram grafiği **(c)** Rastgele şekilde 30 KB veri gizlenmesiyle oluşan videonun histogram grafiği



Şekil 5.13. Video1 dosyası için **(a**) Veri gizlenmemiş videonun histogram grafiği **(b)** Sıralı şekilde 120 KB veri gizlenmesiyle oluşan videonun histogram grafiği **(c)** Rastgele şekilde 120 KB veri gizlenmesiyle oluşan videonun histogram grafiği



Şekil 5.14. Video1 dosyası için **(a**) Veri gizlenmemiş videonun histogram grafiği **(b)** Sıralı şekilde 450 KB veri gizlenmesiyle oluşan videonun histogram grafiği **(c)** Rastgele şekilde 450 KB veri gizlenmesiyle oluşan videonun histogram grafiği

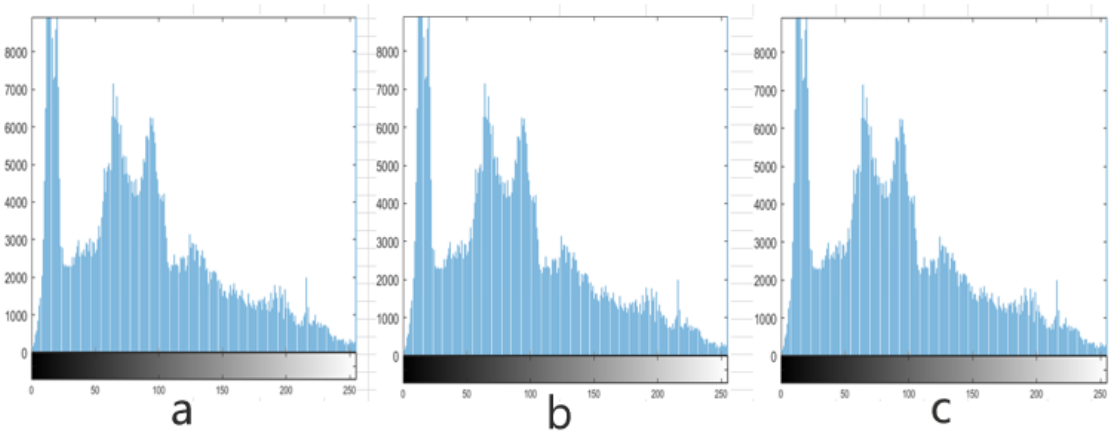
İlk olarak Video1 dosyasına 0,1 KB veri gizlenmiştir. Şekil 5.11.'de orijinal, sıralı gizleme ve rastgele gizleme sonucunda elde edilen histogramlar verilmiştir. Gizlenen veri miktarı çok az olduğunda histogramlar arasında gözle görülebilir bir fark olmadığı sonucuna varılmıştır.

Daha sonra Video1 dosyasına 30 KB büyüklüğünde veri saklanmıştır. Veri gizlenmemiş video dosyası, sıralı ve rastgele gizleme sonucunda elde edilen videoların histogram grafikleri Şekil 5.12.'de verilmiştir. Sıralı veya rastgele gizleme işlemi sonucunda elde edilen histogramlar ile bilgi gizli olmayan dosyanın histogramı arasında fark olduğu gözükmektedir. Orijinal dosyanın elimizde iken bir histogram analizi yapıldığında videonun içinde gizli bilgi olduğu anlaşılabilmektedir. Sıralı ya da rastgele bilgi gizleme işlemleri sonucunda elde edilen histogramlar değerlendirildiğinde gözle görülür fark olmadığı belirlenmiştir.

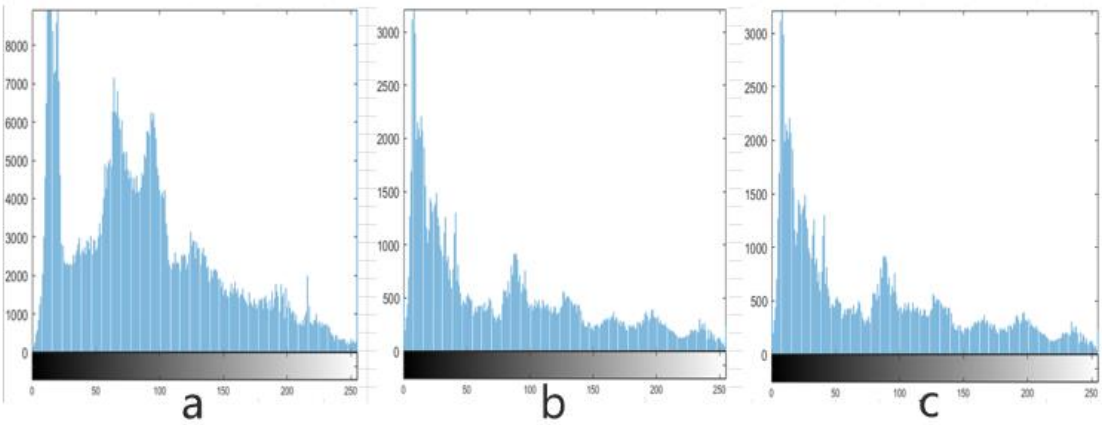
Video1 dosyasına 120 KB veri gizlendiğinde elde edilen histogramlar Şekil 5.13.'te verilmiştir. Saklanan veri miktarı arttığı için orijinal ve veri gizlenmiş videolardan elde edilen histogramlarda gözle görülür farklar oluşmuştur. 120 KB veriyi sıralı ya da rastgele gizledikten sonra elde edilen histogramların grafikleri arasındaki fark ta iyice belirginleşmeye başlamıştır.

Son olarak Video1 dosyasına 450 KB veri gizlenmiş ve oluşan histogramlar incelenmiştir. Bu histogramlar Şekil 5.14'te verilmiştir. Bu büyüklükte bir veri gizlendiğinde histogramlardaki değişimlerin de çok olduğu gözlemlenmiştir.

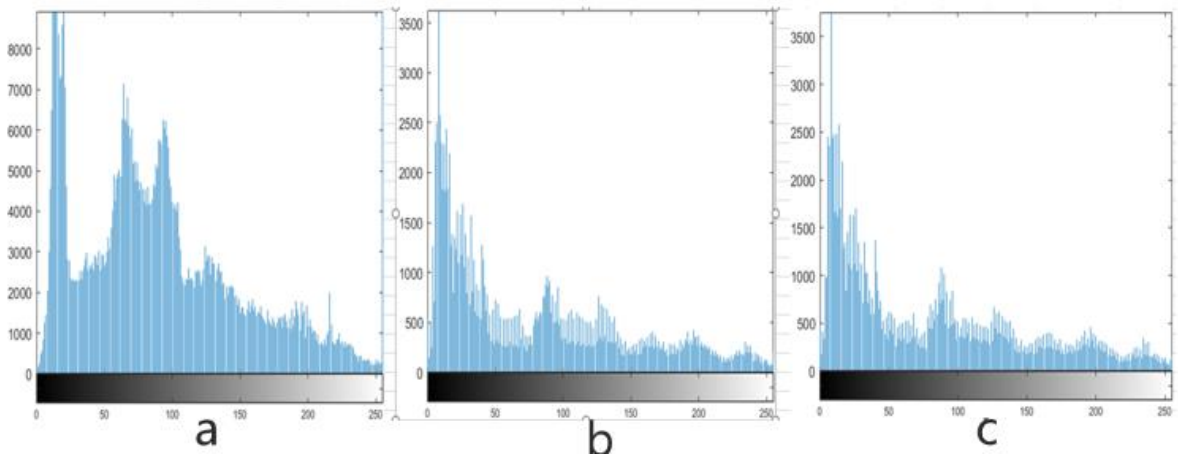
Gizleme işlemlerinde saklanan veri miktarı arttıkça orijinal ve veri gizlenmiş histogramlar arasındaki farklarında belirginleştiği gözlemlenmiştir. 120 KB üstü veri gizlendiğinde histogramlardaki değişimler gözle görülür olmaya başlamıştır. Sıralı ve rastgele gizleme sonrasında ortaya çıkan histogram grafikleri arasındaki farkın daha küçük boyuttaki veri gizleme işlemlerine göre daha fazla olduğu gözlemlenmektedir.



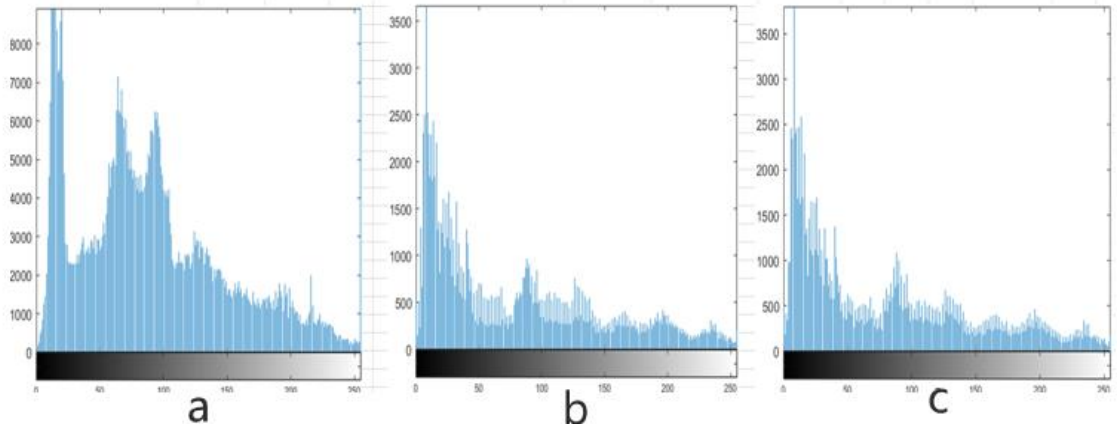
Şekil 5.15. Video2 dosyası için **(a)** Veri gizlenmemiş videonun histogram grafiği **(b)** Sıralı şekilde 0,1 KB veri gizlenmesiyle oluşan videonun histogram grafiği **(c)** Rastgele şekilde 0,1 KB veri gizlenmesiyle oluşan videonun histogram grafiği



Şekil 5.16. Video2 dosyası için **(a)** Veri gizlenmemiş videonun histogram grafiği **(b)** Sıralı şekilde 30 KB veri gizlenmesiyle oluşan videonun histogram grafiği **(c)** Rastgele şekilde 30 KB veri gizlenmesiyle oluşan videonun histogram grafiği



Şekil 5.17. Video2 dosyası için **(a**) Veri gizlenmemiş videonun histogram grafiği **(b)** Sıralı şekilde 120 KB veri gizlenmesiyle oluşan videonun histogram grafiği **(c)** Rastgele şekilde 120 KB veri gizlenmesiyle oluşan videonun histogram grafiği



Şekil 5.18. Video2 dosyası için **(a**) Veri gizlenmemiş videonun histogram grafiği **(b)** Sıralı şekilde 450 KB veri gizlenmesiyle oluşan videonun histogram grafiği **(c)** Rastgele şekilde 450 KB veri gizlenmesiyle oluşan videonun histogram grafiği

Şekil 5.15'te Video2 dosyasına 0,1 KB veri gizlenmesi ile elde edilen histogramlar verilmiştir. Çok az veri gizlendiği için orijinal ve sıralı ya da rastgele gizlenmiş video dosyasının histogramları arasında anlamlı bir fark bulunmadığı görülmüştür.

Sonra Video2 dosyasına 30 KB büyüklüğünde veri saklanmıştır. Orijinal video dosyası, sıralı ve rastgele gizleme sonucunda elde edilen videoların histogram grafikleri

Şekil 5.16.'da verilmiştir. Sıralı veya rastgele gizleme işlemi sonucunda elde edilen histogramlar ile bilgi gizli olmayan dosyanın histogramı arasında fark olduğu gözükmektedir. Orijinal dosyanın elimizde iken bir histogram analizi yapıldığında videonun içinde gizli bilgi olduğu anlaşılabilmektedir. Sıralı ya da rastgele bilgi gizleme işlemleri sonucunda elde edilen histogramlar değerlendirildiğinde gözle görülür fark olmadığı belirlenmiştir.

Video2 dosyasına 120 KB veri gizlendiğinde elde edilen histogramlar ise Şekil 5.17.'te verilmiştir. Saklanan veri miktarı arttığı için orijinal ve veri gizlenmiş videolardan elde edilen histogramlarda gözle görülür farklar oluşmuştur. 120 KB veriyi sıralı ya da rastgele gizledikten sonra elde edilen histogramların grafikleri arasında da gözle görülür farklar ortaya çıkmıştır.

Video2 dosyasına 450 KB veri gizlenmiş ve oluşan histogramlar Şekil 5.18'de verilmiştir. Bu histogramlar incelendiğinde bu büyüklükte bir veri gizlendiğinde değişimlerin de çok olduğu gözlemlenmiştir.

Video1 dosyasında olduğu gibi 120 KB üzeri veri gizlendiğinde orijinal ve veri gizlenmiş videoların histogramları arası farklar artmaktadır.

Sıralı ve rastgele gizleme işlemi açısından bakıldığında ise az miktarda veri gizlemede pek fark olmadığı ama gizlenen veri miktarı arttıkça rastgele veri gizlemenin daha iyi olduğu gözlemlenmektedir.

BÖLÜM 6

SONUÇ

Günümüzde teknolojinin de çok hızlı ilerlemesi ile birlikte bilgi transferi çok yoğun bir şekilde yapılmaktadır. Gerçekleştirilen bu bilgi alışverişi sırasında bilginin güvenliği oldukça önemli bir hal almıştır. Bu tezde hareketli görüntü dosyası olarak bilinen video dosyalarında veri gizleme amacıyla kullanılan En Önemsiz Bit Ekleme yöntemi incelenmiştir. Yapılacak gizleme işleminin sıralı gerçekleştirilmesi ile bir fonksiyon kullanılarak rastgele gerçekleştirilmesinin güvenlik açısından etkili olup olmadığı incelenmiştir. Bu amaçla bir uygulama geliştirilmiştir. Geliştirilen uygulama ile sıralı/rastgele veri gizleme işlemleri ve taşıyıcıdaki değişim ölçümleri ile histogram analizi yapılmıştır. Veri gizleme işleminde güvenliğin arttırılması amacıyla gizlenecek metnin AES yada RSA şifreleme yöntemlerinden biriyle şifrelenmesi seçeneği de eklenmiştir.

Taşıyıcıdaki değişimi PSNR ve MSE değerleri ile ölçülmüştür. Dayanıklılığı değerlendirmek amacıyla da histogram analizi yapılmıştır. Büyüklüğü ve renk dağılımları değişen video dosyalarına farklı büyüklükteki veriler sıralı veya rastgele olarak yerleştirilmiştir. Ayrıca AES yada RSA şifreleme algoritmaları seçilerek sıralı veya rastgele gizleme işlemleri yapılmış ve seçilen şifreleme yönteminin etkisi incelenmiştir. PSNR, MSE değerleri ve histogram grafikleri incelendiğinde düşük miktarda veri gizlendiğinde bilgi varlığının sezilmesinin çok zor olduğu görülmüştür. Bu sonuç uyarlanan yöntem ile az miktarda veri gizlediğimizde güvenli bir iletişim yapılabileceği anlamına gelmektedir.

Gizlenmek istenen veri miktarı arttıkça bir fonksiyona bağlı olarak rastgele olarak yapılan gizleme işlemi sonucunda elde edilen değerlerin daha iyi olduğu görülmüştür. Orijinal dosya ile veri gizlenmiş dosya arasındaki PNSR ve MSE ölçümleri rastgele veri

gizlediğimizde sıralı gizlemeye göre daha başarılı sonuçlar vermiştir. Bu sonuçlar bize rastgele veri gizlemenin sıralıya göre daha iyi olduğunu göstermektedir. Bilgi gizleme işleminin ilk pikselden başlayıp son piksele doğru yapılması nedeniyle sıralı bilgi gizleme işleminin rastgele veri gizlemeye göre daha kolay anlaşılabileceği sonucuna varılmıştır.

Gerçekleştirilen bu çalışma sonrasında benzer başka çalışmalar incelenmiş ve karşılaştırmaları yapılmıştır. Elde edilen sonuçların ışığında video içine bilgi gizleme için önerilen yöntemde gizlenen metinlerin başarılı şekilde çıkarıldığı tespit edilmiş ve rastgele bir şekilde video dosyası üzerine bilgi gizleme işleminin daha sağlıklı sonuçlar verdiği gözlenmiştir. Kalite ölçümlerinden çıkarılan sonuçlara göre video dosyaları üzerindeki gizlenmiş olan verinin anlaşılamayacak şekilde olduğu anlaşılmıştır.

Bilgi güvenliğinin önemimin gittikçe arttığı günümüzde gizli iletişim daha da önem kazanmıştır. Bu sebepten dolayı yapılan bu çalışmada önerilen yöntem ile gizli iletişim alanında gerçekleştirilebilecek olan çözümlere bir katkı sağlayabileceği düşünülmektedir.

KAYNAKLAR

Abed, S. E., Al-Mutairi, M., Al-Watyan, A., Al-Mutairi, O., alenizy, W., & Al-Noori, A. (2019). An Automated Security Approach of Video Steganography–Based LSB Using FPGA Implementation. Journal of Circuits, Systems and Computers, 28(05), 1950083.

Akbal, T. (2008). Ses Verilerine Sıkıştırılmış ve Şifrelenmiş Ham Verilerin Gömülmesi, Yüksek Lisans Tezi, Sakarya Üniversitesi Fen Bilimleri Enstitüsü, Sakarya.

Aktaş, F (2011) Steganaliz Yöntemleri Kullanılarak Resim İçerisindeki Saklı Bilgilerin Tespit Edilmesi, Hacettepe Üniversitesi, Fen Bilimleri Enstitüsü, Elektrik ve Elektronik Mühendisliği Anabilim Dalı, Yüksek Lisans Tezi.

Akyüz, D. & Kasapbaşı, M. C. (2021). Yeni Kaotik Video Steganografi Metodu. Haliç Üniversitesi Fen Bilimleri Dergisi, 4 (1) , 25-40. DOI: 10.46373/hafebid.858834

Al-Othmani, A. Z., Manaf, A. A., & Zeki, A. M. (2012). A Survey on Steganography Techniques in Real Time Audio Signals and Evaluation. International Journal of Computer Science Issues (IJCSI), 9(1), 30.

Anderson, R., J., Petitcolas, F. A. P. (1998). On The Limits of Steganography. IEEE Journal of Selected Areas in Communications, 16 (4), 474–481.

Avcı, E., Tuncer, T., & Ertam, F. (2014). Çok Katmanlı Görüntü Steganografi. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı.

Banupriya, R., Deepa, J., & Suganthi, S. (2019). Video Steganography Using LSB Algorithm for Security Application. International Journal of Mechanical Engineering and Technology, 10(1), 203-211.

Bender W., Gruhl D., Morimoto N., Lu A., "Techniques for Data Hiding", IBM Systems Journal, vol. 35, NOS 3&4, 1996

Bhaumik, A. K., Choi, M., Robles, R. J., & Balitanas, M. O., 2009, Data Hiding in Video. International Journal of Database Theory and Application, 2(2), 9-16.

Canbek, G., (2005) Klavye Dinleme ve Önleme Sistemleri Analiz, Tasarım ve Geliştirme, Yüksek Lisans Tezi, Gazi Üniversitesi, Fen Bilimleri Enstitüsü.

Chandel, B., & Jain, S. (2016). Video Steganography: A Survey. IOSR Journal of Computer Engineering, 18(1), 11-17.

Cox, I. J., Miller, M. L., Bloom, J. A (2000). Watermarking Applications and Their Properties. International Conference on Information Technology, Las Vegas, USA.

Çıtlak, S. (2020). Sıft Anahtar Noktalarını Kullanarak Ham Video Bileşenlerinde Veri Gizleme ve Gizli Verileri Tespit Etme. Doktora Tezi, Ankara Yıldırım Beyazıt Üniversitesi Fen Bilimleri Enstitüsü.

Çimen, C., Akleylek, S. ve Akyıldız, E. , Şifrelerin Matematiği : Kriptografi, ODTÜ Geliştirme Vakfı Yayıncılık ,İstanbul, 2007

Demirci, B., 2016, Görüntü Steganografi Metotları ve Performanslarının Karşılaştırılması, Yüksek Lisans Tezi, Selçuk Üniversitesi Fen Bilimleri Enstitüsü.

Demirkiran, V. (2008). Webe Dayalı Bilgisayar Destekli Uzaktan Eğitim Otomasyon Sistemleri, Yüksek Lisans Tezi, Beykent Üniversitesi, Fen Bilimleri Enstitüsü.

Demiröz. D, (2021). Kriptolojide Yan Kanal Analizleri Ve Uygulamaları, Yüksek Lisans Tezi, Ege Üniversitesi Fen Bilimleri Enstitüsü.

Diffie, W. & Hellman, M. (1976). New Directions in Cryptography. IEEE Transactions on Information Theory, 22(6), 664-654.

Dixit, M., Bhide, N., Khankhoje, S., & Ukarande, R. (2015). Video Steganography. In 2015 International Conference on Pervasive Computing (ICPC) (pp. 1-4). IEEE.

Doğan, A. Y. (2008). AES Algoritmasının FPGA Üzerinde Düşük Güçlü Tasarımı, Doktora Tezi, Yüksek Lisans Tezi, İstanbul Teknik Üniversitesi, Fen Bilimleri Enstitüsü.

FIPS 46-3, Data Encryption Standard (1999). Federal Information Processing Standard (FIPS), Publication 46-3, National Bureau of Standards, U.S. Department of Commerce, Washington D.C., October 25, 1999.

FIPS 180-4 Secure Hash Standarts (2012).s). Federal Information Processing Standart (FIPS) Publication, 180-4. National Bureau of Standarts, US Department Commerce, Washington, DC.

FIPS 197, Advanced Encryption Standard (2001). Federal Information Processing Standart (FIPS) Publication, 197. National Bureau of Standarts, US Department Commerce, Washington, DC.

Gruhl D., Lu A., Bender W., Echo Hiding, In Proceeding of First International Workshop, Springer, Cambridge, UK, May-June, 1996

Gutub, A., Fattani, M., (2007). A novel Arabic text steganography method using letter points and extensions, WASET International Conference on Computer, Information and Systems Science and Engineering (ICCISSE), Vienna, Austria,28–31.

Hu, S. D. (2011). A Novel Video Steganography Based on Non-Uniform Rectangular Partition. In 2011 14th IEEE International Conference on Computational Science and Engineering (pp. 57-61).

Johnson N.F, Jajodia S., (1998) Exploring steganography: Seeing the Unseen, Computer, 31, no 2:26-34.

Karadogan, I. & Das, R. (2014). An Examination on Information Hiding Tools for Steganography. International Journal of Information Security. 3. 200-208.

Katzenbeisser S., Petitcolas F.A.P. (2000) Information Hiding Techniques for Steganography and Digital Watermarking, Artech House, INC. 685 Canton Street Norwood, MA 02062.

Kerckhoffs A. (1883). La cryptographie militaire, Journal des Sciences Militaires.

Kim Y.S., Kim Y.M., Choi J.Y., Baik D.K. (2003). Information Hiding System StegoWaveK for Improving Capacity, International Symposium, ISPA 2003 Aizu-Wakamatsu, Japan, July 2-4, Proceedings, Springer Berlin/ Heidelberg, ISSN 0302-9743, vol. 2745/2003.

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

Kharrazi M., Sencar H.T., Memon N. (2004). Image Steganography: Concepts and Practice, WSPC/Lecture Notes Series, April 22.

Macit, H. B., Koyun, A., & Güngör, O. (2018) A Review and Comparison of Steganography Techniques. INES 2018. Antalya.

Manisha, S., & Sharmila, T. S. (2019). A Two-Level Secure Data Hiding Algorithm for Video Steganography. Multidimensional Systems and Signal Processing, 30(2), 529-542.

Misman, C. (2018). Mobil Haberleşme Güvenliğinin Steganografi ile Arttırılması, Yüksek Lisans Tezi, Necmettin Erbakan Üniversitesi, Fen Bilimleri Enstitüsü.

Mohan, H. S., & Reddy, A. R. (2012). Revised AES and its Modes of Operation. International Journal of Information Technology, 5(1), 31-36.

Mstafa, R. J., & Elleithy, K. M. (2017). Compressed And Raw Video Steganography Techniques: A Comprehensive Survey And Analysis. Multimedia Tools and Applications, 76(20), 21749-21786.

Nosrati, M., Karimi, R., & Hariri, M. (2012). Audio Steganography: A Survey on Recent Approaches. World applied programming, 2(3), 202-205.

Özcan. S., Steganografi Nedir Nasıl Çalışır ve Araçları [PDF Belgesi] 11.03.2022 tarihinde https://www.bgasecurity.com/makale/steganografi-nedir-nasil-calisir-ve-araclari/ adresinden erişildi.

Öztemür, M. (2012). AES Algoritmasının Bir Gerçeklemesine Güç Analizi Saldırıları. Yüksek Lisans Tezi, Yıldız Teknik Üniversitesi, Fen Bilimleri Enstitüsü.

Özyılmaz, Ç. (2014). Kriptolojiye Giriş, Yüksek Lisans Tezi. Karabük Üniversitesi, Fen Bilimleri Enstitüsü, Karabük.

Pehlivanoğlu, M. K., Savaş, B. K., & Duru, N. (2015). LSB Based Steganography over Video Files Using Koblitz's Method. IEEE 23. Sinyal İşleme ve İletişim Uygulamaları Kurultayı, Malatya.

Popa R. (1998). An Analysis of Steganographic Techiques, Ph.D Thesis, The Politehnica University of Timisoara, Faculty of Automatics and Computers, Department of Computer Science and Software Engineering.

Rajalakshmi, K., & Mahesh, K. (2017, February). Video Steganography Based On Embedding The Video Using PCF Technique. In 2017 International Conference on Information Communication and Embedded Systems (ICICES) (pp. 1-4). IEEE.

Ramalingam, M., Isa, N. A. M., & Puviarasi, R. (2020). A Secured Data Hiding Using Affine Transformation İn Video Steganography. Procedia Computer Science, 171, 1147-1156.

Razavi, N. (2017). LSB Steganografi Yönteminde Yüksek Kapasiteli Veri Gizleme, Yüksek Lisans Tezi, Gazi Üniversitesi, Ankara.

Reddy, H. M., & Raja, K. B (2009). High Capacity And Security Steganography Using Discrete Wavelet Transform. International Journal of Computer Science and Security (IJCSS), 3(6), 462.

Rivest R.L. & Dusse S. (1992). The MD5 message-digest algorithm.

Rivest R.L. (1992). The RC4 Encryption Algorithm. RSA Data Security. Inc., March 12, 9-2.

Rivest R.L., Shamir, A. & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM. 21(2), 120-126.

Sara, U., Akter, M., & Uddin, M. S. (2019). Image quality assessment through FSIM, SSIM, MSE and PSNR—a comparative study. Journal of Computer and Communications, 7(3), 8-18.

Sayood, K. (1996). Introduction to data compression. Morgan Kauffman Publishers, Inc. 340 Pine Street, Sixth Floor, San Francisco, CA 94104-3205, USA.

Schneiner B. (1993). Description of a new variable-length key, 64 bit block cipher (Blowfish), International Workshop on Fast Software Encryption, 191-204.

Shehzad, D. (2019). Developing novel techniques for spatial domain LSB image steganography.

Şahin Mesut A., Mesut A., Sakallı M.T., (2010). Görüntü Steganografide Gizlilik Paylaşım Şemalarının Kullanılması ve Güvenliğe Etkileri, III Ağ ve Bilgi Güvenliği Sempozyumu, Ankara-Türkiye.

Şahin, A. (2007). Görüntü Steganografide Kullanılan Yeni Metotlar Ve Bu Metotların Güvenilirlikleri, Doktora Tezi, Trakya Üniversitesi Fen Bilimleri Enstitüsü.

Şahin, A., Buluş, E., Sakallı, M. T., & Buluş, H. N. (2007). Resim İçerisindeki Gizli Bilginin RQP Steganaliz Yöntemiyle Sezilmesi. Akademik Bilişim.

Şahin, A., Buluş, E., & Tolga Sakallı, M. (2006). 24-Bit Renkli Resimler Üzerinde En Önemsiz Bite Ekleme Yöntemini Kullanarak Bilgi Gizleme. Trakya Üniversitesi Fen Bilimleri Dergisi, 7(1), 17-22

Şahin. A, Bilgi Gizleme Teknikleri/Ders-1 [powerpoint slaytı] 10 Eylül 2021 tarihinde http://andacmesut.trakya.edu.tr/bgt/Ders1.ppt adresinden erişildi.

Şatır, E. (2013). Bilgi Güvenliği İçin Metin Steganografisinde Yeni Bir Yaklaşım, Doktora Tezi, Selçuk Üniversitesi Fen Bilimleri Enstitüsü.

Üstübioğlu, A., Ulutaş, G. & Üstübioğlu, B. (2017). Tamper Localization of The Medical Images Based on Fragile Watermarking, 25th Signal Processing and Communications Applications (SIU 2017), Antalya, Türkiye

Yaman, Y., Çetin Ö., Ertürk İ. & Akar, F. (2014). Veri Gizleme. İstanbul: Beta.

Yalman, Y., & Ertürk, İ. (2009). Kişisel Bilgi Güvenliğinin Sağlanmasında Steganografi Biliminin Kullanımı. ÜNAK Bilgi Çağında Varoluş: Fırsatlar Ve Tehditler Sempozyumu, 215.

Yargıçoğlu, A. U. (2010). Düşük Veri Hızlarında Çalışan Konuşma Kodlayıcılarına Gürbüz Bilgi Saklama ve Damgalama, Doktora Tezi, Ankara Üniversitesi Fen Bilimleri Enstitüsü Elektronik Mühendisliği Anabilim Dalı.

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

Yıldız, Y. (2012). Sırörtme yöntemiyle video üzeri şifrelenmiş güvenli iletişim uygulaması, Yüksek Lisans Tezi, Sakarya Üniversitesi, Fen Bilimleri Enstitüsü.

Yin, Z., Xue, F., Liu, P., Luo, J., Zeng, X., Feng, R., & Zhao, X. (2021). Analysis and Test of RSA Algorithm in Smart Electricity Meter Identity Authentication. In Proceedings of 2021 International Top-Level Forum on Engineering Science and Technology Development Strategy: The 6th Purple Mountaın Forum on Smart Grid Protection and Control (2021) (p. 303). Springer Nature.

TEZ İLE İLGİLİ BİLİMSEL FAALİYETLER

Ulusal Hakemli Dergi Makaleleri

E. Tekkanat ve AŞ. Mesut , "Video Dosyaları Üzerinde Lsb Yöntemiyle Bilgi Gizleme İşleminin Sıralı Veya Rastgele Yapılmasının Güvenliğe Etkilerinin İncelenmesi", Trakya Üniversitesi Mühendislik Bilimleri Dergisi, c. 23, sayı. 1, ss. 37-49, Haz. 2022

ÖZGEÇMİŞ

Egemen TEKKANAT, 22 Ocak 1986 tarihinde Edirne/Uzunköprü de doğdu, İlk, Orta ve Lise öğrenimini Edirne'de tamamladıktan sonra 2004 yılında Haliç Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği bölümünü kazandı ve bu bölümden 2009 yılında mezun oldu. 2011 yılında başladığı yüksek lisans eğitimini 2013 yılında bitirdi. 2013 yılında Trakya Üniversitesi Keşan Yusuf Çapraz Uygulamalı Bilimler Yüksekokulu Bilgisayar Teknolojileri ve Bilişim sistemleri bölümünde öğretim görevlisi olarak görev yapmaya başladı. Aynı yıl Trakya üniversitesi Fen Bilimleri Enstitüsü Hesaplamalı Bilimler Anabilim dalında doktora eğitimine başladı. Egemen TEKKANAT halen Keşan Yusuf Çapraz Uygulamalı Bilimler Yüksekokulu Bilgisayar Teknolojileri ve Bilişim sistemleri bölümünde öğretim görevlisi olarak çalışmaktadır.