T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

SIRÖRTME YÖNTEMİYLE VİDEO ÜZERİ ŞİFRELENMİŞ GÜVENLİ İLETİŞİM UYGULAMASI

YÜKSEK LİSANS TEZİ

Yasemin YILDIZ

Enstitü Anabilim Dalı	**:**	**ELEKRONİK VE BİLGİSAYAR EĞİTİMİ**
Enstitü Bilim Dalı	**:**	**ELEKRONİK VE BİLGİSAYAR EĞİTİMİ**
Tez Danışmanı	**:**	**Doç. Dr. A.Turan ÖZCERİT**

Haziran 2012

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

SIRÖRTME YÖNTEMİYLE VİDEO ÜZERİ ŞİFRELENMİŞ GÜVENLİ İLETİŞİM UYGULAMASI

YÜKSEK LİSANS TEZİ

Yasemin YILDIZ

Enstitü Anabilim Dalı : ELEKRONİK VE BİLGİSAYAR EĞİTİMİ

Bu tez 13/06/2012 tarihinde aşağıdaki jüri tarafından Oybirliği ile kabul edilmiştir.

Doç. Dr.	**Doç. Dr.**	**Doç. Dr.**
A. Turan ÖZCERİT	**Murat ÇAKIROĞLU**	**Ahmet ÖZMEN**
Jüri Başkanı	**Üye**	**Üye**

TEŞEKKÜR

Kablosuz haberleşmede veri güvenliğinin son derece azaldığı günümüzde, kaybedilen güvenliğin yeniden sağlanabilmesi için geliştirilen veri gizleme tekniklerinin önemi giderek artmaktadır. Sırörtüsü (Steganography) yöntemleri geliştirilen algoritmalarla veri gizliliği için güçlü yazılımlar geliştirmektedir. Bu noktadan hareketle, kablosuz ortamlarda sayısal video içerisine gizlenmek istenen mesaj önce şifrelenerek ardından gömme işlemini gerçekleştirildikten sonra gönderilmesi üzerine tez çalışmaları yapılmış olup, geliştirilen yazılımlar sunulmaktadır.

Yüksek lisans eğitimim süresince değerli birikimlerini bana aktaran, tezimin başlangıcından bitimine kadar her aşamasında sorunlarımı dinleyen, çalışmalarıma yön veren ve değerli zamanını sorunlarımın çözümüne ayıran tez danışmanım Sayın Doç. Dr. A. Turan ÖZCERİT'e ve danışmanım kadar da çalışmama katkısı bulunan Sayın Doç. Dr. Özdemir ÇETİN'e, teşekkürlerimi sunarım.

Bugünlere gelmemi sağlayan annem Arife TİYRAKİ'ye ve babam Ahmet TİYRAKİ'ye, tez çalışmam sürecinde sabırları ve yardımları için ise eşim Cihan YILDIZ 'a teşekkür ederim.

İÇİNDEKİLER

TEŞEKKÜR ii
İÇİNDEKİLER iii
SİMGELER VE KISALTMALAR LİSTESİ vi
ŞEKİLLER LİSTESİ vii
TABLOLAR LİSTESİ ix
ÖZET x
SUMMARY xi
BÖLÜM 1. GİRİŞ 1
1.1. Literatürde Yapılan Çalışmaların Özetleri 2
1.2. Tez Çalışmasının Amacı ve Motivasyonu 4
1.3. Tez Organizasyonu 5
BÖLÜM 2. SAYISAL GÖRÜNTÜ ESASLARI VE GÖRÜNTÜ İŞLEME 7
2.1. Giriş 7
2.2. Görme ve Görüntü İşleme Arasındaki İlişki 8
2.2.1. Göz ve görme 9
2.2.2. Renk teorisi ve renk modelleri 12
2.2.3.1. RGB renk modeli 13
2.2.3.2. CMYK renk modeli 14
2.2.3.3. Renk modelleri arasındaki dönüşümler 16
2.3. Sayısal Görüntü 16
2.3.1. Sayısal görüntünün oluşumu 17
2.4. Sayısal Videonun Yapısı ve Oluşumu 18
2.5. Sonuç 19
BÖLÜM 3. ŞİFREMELE TEKNOLOJİLERİ 20
3.1. Giriş 20
3.2. Şifrelemenin Amacı 22

3.2.1. Veri güvenliği 22
3.2.2. Veri bütünlüğü 22
3.2.3. Kimlik denetimi 23
3.3. Şifreleme Algoritmaları 23
3.3.1. Açık anahtarlı şifreleme sistemleri(Asimetrik şifreleyiciler) 24
3.3.1.1. RSA Şifreleme Sistemi 26
3.3.2. Gizli anahtarlı şifreleme sistemleri(Simetrik şifreleyiciler) 28
3.3.2.1. Kaydırma şifrelemesi(Shiftchipher) 28
3.3.2.2. One Time Pad(OTP) 29
3.4. Veri Gizleme ve Gömme Teknikleri 31
3.4.1. Şifeleme kavramı ve terminolojisi 33
3.4.1.1. Kriptografinin tarihçesi 34
3.4.2. Sırörtme 36
3.4.2.1.Sırörtme kavramı ve terminolojisi 38
3.4.2.2. Sırörtmenin tarihçesi 40
3.4.2.3. Resim dosyaları için sırörtme teknikleri 41
3.4.2.3.1. Uzay düzleminde sırörtme 41
3.4.2.3.2. Frekans düzleminde sırörtme 42
3.4.2.4. Video dosyaları için sırörtme teknikleri 42
3.4.2.5. Ses dosyaları için sırörtme teknikleri 43
3.4.3. Sayısal Damgalama 44
3.4.3.1. Uzamsal ve zamansal boyuttaki damgalama teknikleri 46
3.4.3.2. Dönüşüm boyutu kullanan damgalama teknikleri 46
3.4.4. Sayısal Damgalama ve Sırörtme Arasındaki Farklar 46
3.5. Veri Gömme Teknikleri 47
3.5.1. Histogramlar Yöntemi 47
3.5.2. LSB Yöntemi 48
3.5.3. Dalgaboyu Yöntemi 50
3.6. Sıraçma (Steganaliz) 51
3.6.1. χ^2 Testi 53
3.6.2. Histogram Analizi 56
3.6.3. RQP Yöntemi 57
3.7. Sonuç 58

BÖLÜM 4. VİDEOLAR İÇİN SIRÖRTME YAKLAŞIMI İLE GELİŞTİRİLEN VERİ GÖMME ALGORİTMALARI 59
4.1. Giriş 59
4.2. Geliştirilen Veri Gizleme İşleminin Genel Çalışma Prensibi 59
4.2.1. Veri şifreleme işlemi 60
4.2.2. Veri gizleme işlemi 61
4.2.3. Gizli verinin geri elde edilmesi ve şifre çözme işlemi 63
4.3. Geliştirilen Veri Gizleme ve Şifreleme Yöntemleri 65
4.3.1. Kullanılan Şifreleme Yöntemi 65
4.3.2. Kullanılan Veri gömme yöntemi 66
4.3.2.1 Histogramlar yöntemi 66
4.3.2.1.1. Benzer histogramlar yöntemi 70
4.4. Video Ortamında Veri Kodlama Yöntemleri 73
4.4.1. RGB ağırlıklı kodlama yöntemleri 73
4.5. Uygulama Yazılımının Tanıtılması 75
4.5.1.Verinin şifrelenmesi 78
4.5.2. Verinin gizlenmesi 79
4.5.2.1.Histogramlar yöntemi ile veri gizleme uygulaması 80
4.5.3. Sırlı Videodan şifreli mesajın okunması ve şifrenin çözülmesi 84
BÖLÜM 5. GELİŞTİRİLEN UYGULAMALARA AİT DENEYSEL SONUÇLARIN DEĞERLENDİRİLMESİ 88
5.1. Giriş 88
5.2. Bozulan piksel sayısı, Kapasite ve Algılanabilirlik Başarımlarının Değerlendirilmesi 90
5.3. Görsel Algılanabilirlik Başarım Değerlendirilmesi 92
5.4. Sonuç 92
5.5. TARTIŞMA VE DEĞERLENDİRMELER 93
KAYNAKLAR 96
EKLER 101
EK- A. Geliştirilen Algoritmaların Akış Diyagramları 101
EK- B. Sayısal Video İçerisinde Şifrelenmiş Gizli Verilerin Kablosuz Transferi için Geliştirilen Yazılımın Program Kodları CD İçerisinde Sunulmuştur (EK-A klasörü) 108
EK- C. Tez pdf Dosyası CD İçerisinde Sunulmuştur (Tez.pdf). 109
ÖZGEÇMİŞ 110

SİMGELER VE KISALTMALAR LİSTESİ

LSB	:	Least Significant Bit – En Düşük Değerlikli Bit
DCT	:	Discrete Cosine Transform – Ayrık Kosinüs Dönüşümü
DWT	:	Discrete Wavelenght Transform – Ayrık DAlagacık Dönüşümü
RGB	:	Red Green Blue – Kırmızı Yeşil Mavi
ASCII	:	American Standard Code for Information Interchange
BMP	:	Bit Map
JPEG	:	Joint Photographic Experts Group
AVI	:	Audio/ Video Interleaved
MPEG	:	Moving Pictures Experts Group
HAS	:	Human Audio System
BH	:	Benzer Histogramlar Yöntemi
DB	:	Dalgaboyu Yöntemi

ŞEKİLLER LİSTESİ

Şekil 2.1 İnsan gözünü oluşturan önemli bölümler ve görülebilir ışık. 10
Şekil 2. 2. Görülebilir ışık dalga boyu. 10
Şekil 2. 3. RGB renk modelleri. 14
Şekil 2. 4. CMYK renk modelleri. 15
Şekil 2. 5. Sayısal görüntüde piksel. 17
Şekil 3.1. Genel şifreleme ve şifre çözme yol haritası. 21
Şekil 3.2. Asimetrik .Anahtarlı Şifreleme. 24
Şekil 3.3. Simetrik Anahtarlı Şifreleme. 28
Şekil 3.4. Veri gizleme metotları şeması. 32
Şekil 3.5. Veri gizleme ve çözme diyagramı. 34
Şekil 3.6. Yunanlıların veri gizlemede kullandığı ”scytale” isimli çubuk. 35
Şekil 3.7. Genel olarak veri gizleme blok diyagramı. 37
Şekil 3.8. Damgalama teknikleri. 45
Şekil 3.9. LSB ile veri gömme. 49
Şekil 3.10. İnsan görme sisteminin görebileceği ışık değer aralıkları. 51
Şekil 3.11. χ^2 Testi için kullanılan orijinal resim. 54
Şekil 3.12. Resmin veri gömülmeden önceki χ^2 Testi sonuçları. 54
Şekil 3.13. Resmin içerisine 1KB’lık veri gömüldükten sonraki χ^2 Testi sonuçları. 54
Şekil 3.14. Resmin içerisine 2,7 KB’lık veri gömüldükten sonraki χ^2 Testi sonuçları. 55
Şekil 3.15. Orijinal resim. 56
Şekil 3.16. Orijinal resim için Histogram değerleri. 56
..... 57
Şekil 4.1. Sunulan tez çalışmasının genel çalışma prensibi blok diyagramı..... 60
Şekil 4.2. RSA şifreleme ile iletişim. 61
Şekil 4.3. Genel veri gizleme akış diyagramı. 63
Şekil 4.4. Gizli veriyi geri elde etme ve şifre çözme akış diyagramı..... 64
Şekil 4.5. Farklı sahne geçişlerini ve histogramlarını gösteren örnek bir sayısal video. 68
Şekil 4.6. Benzer Histogram Yöntemi Akış Diyagramı..... 71
Şekil 4.7. Blok Tabanlı Benzer Histogramlar Yöntemi Akış Diyagramı. 72
Şekil 4.8. RGB veri kodlama yöntemi ile veri gömme işlemi. 74
Şekil 4.9. RGB veri kodlama yöntemi ile veri geri elde etme işlemi..... 75

Şekil 4.10. (a).Veri gizleme uygulama yazılımının ana pencere 77
(b).Gizli veriyi şifreleme uygulama yazılımının ana penceresi. 77
(c).Verinin elde edilmesi ve şifre çözümü yazılımının ana penceresi..... 77
Şekil 4.11. Kablosuz bağlantı için server'ın çalışması. 78
Şekil 4.12. Girilen metnin şifrelenmesi ve bağlantılar..... 79
Şekil 4.13. Gizlenmek istenen şifreli mesaj için örtü dosyasının seçilmesi..... 81
Şekil 4.14. Veriyi gömebilmek için uygun algoritmanın seçimi. 81
Şekil 4.15. Örtü dosyası hakkında bilgi verilmesi. 82
Şekil 4.16. Kodlama yönteminin seçimi ve eşik değerin belirlenmesi. 83
Şekil 4.17. Orijinal dosya ve resimlerin, Veri gömülmüş halleriyle karşılaştırılması. 84
Şekil 4.18. Sırlı videonun kaydedilen dosyadan alınması..... 84
Şekil 4.19. Sırlı videonun adresinin gösterilmesi..... 85
Şekil 4.20. Sırlı videodan okunan şifreli metin..... 86
Şekil 4.21. Şifreli metnin doğru bir şekilde çözülme mesajı. 86
Şekil 4.22. Orijinal mesaj..... 87
Şekil 5.1. Hata Analizi. 90
Şekil 5.2. Orijinal görüntü ve sırlı görüntü arasındaki Histogram farkının gösterilmesi. 91
Şekil Ek.1. Şifreleme Algoritması. 102
Şekil Ek.2. Şifre Çözme Algoritması..... 103
ekil Ek.3. Genel Veri Gizleme Akış Diyagramı 104
Şekil Ek.4. Genel Veri Geri Elde Etme Akış Diyagramı..... 105
Şekil Ek.5. Benzer Histogramlar Yöntemi ile Veri Gömme Akış Diyagramı 107

TABLOLAR LİSTESİ

Tablo 5.1. Elde edilen sırlı görüntüler için hesaplanan görüntü kalite ölçütleri…….90

Tablo 5.2. RGB kodlama ve değişen piksel sayısı……..92

ÖZET

Anahtar kelimeler: Sayısal Video, Veri Gizleme, Şifreleme, Sırörtüsü, Kablosuz Haberleşme

Gelişen teknoloji ve iletişim koşulları haberleşmede veri güvenliğini zorlaştırmıştır. Verinin güvenli bir şekilde göndericiden alıcıya ulaşması için insanoğlu birçok yöntem geliştirmiştir. Veri gizleme(steganography), Veri şifreleme (Cryptography) ve geliştirilen diğer yöntemlerin tümü veri güvenliği ve güvenli iletişim de giderek artan bir öneme sahiptir.

Bu tezde sunulan projenin temel amacı; sayısal hareketli resimler yani videolar içerisinde gönderilecek verinin daha güvenli iletimi için şifreleme ve sırörtme yöntemleri kullanarak gizli veri transferinin kablosuz ortamda gerçekleştirilmesidir. Bu amaçla kablosuz ortamda sayısal video içerisine gizli veri şifrelenerek gömme algoritmaları tasarlanmıştır.

Tez çalışmasında tasarlanan algoritmalar, C# programlama dili ve Microsoft Visual Studio 2010 programında gerçekleştirilmiştir. Kablosuz haberleşmeyi sağlamak için ise değişik özelliklere sahip iki adet kablosuz haberleşme yapabilen bilgisayar kullanılmıştır.

Yapılan çalışmaların sonucunda, elde edilen sonuçlar sunularak başarım değerlendirmeleri yapılmıştır.

SUMMARY

Key Words: Digital Video, Data Hiding, Steganography, Data Embedding, Digital Watermarking, Raw Video-AVI.

Techniques for Steganography, Cryptography have nowadays become increasingly more sophisticated and widespread. Researches on information embedding, have received considerable attention for a decade due to its potential applications in multimedia and information security.

The main objective of this thesis presented is to design and implement encrypted and compressed hidden data transfer within digital video for wirless communications. Fort his reason, the appl,cat,on is used for file embedding within digital video. Furthermore, this application also enables conventional wireless images communication.

In this thesis, two different computers and an access point are utilized. The software is developed by Microsoft Visual Studio 2010.

The result of the application software developed are presented and their performances are evaluated.

BÖLÜM 1. GİRİŞ

İnsanlar yaratılışları itibariyle sosyal varlıklardır. Bu sosyallik sürekli olarak iletişim halinde olmayı gerektirmektedir. Gelişen ve değişen dünyada her geçen zaman içerisinde farklı ihtiyaçlar ve bu farklılıkların doğurduğu gereksinimlerle iletişim şekilleri geliştirilmektedir. Örneğin savaş zamanı haberleşme, şirket içi haberleşme vb. bu gibi durumlarda haberleşmenin şeklide değişmektedir. İlk çağlarda dumanla haberleşme, güvercinle haberleşme, elçi ile haberleşme, günümüze de ise tüm bunları geride bırakan Internetle haberleşme insanoğlunun geçmişten bu güne kullanmış olduğu haberleşme çeşitlerindendir.

Kullanılan haberleşme yolu hangisi olursa olsun neticesinde güvenlik sorunu ortaya çıkmıştır. Bu sorunu ortadan kaldırmak için tarih içerisinde birçok yöntem geliştirilmiştir. İletişimde güvenlik için kullanılan ilk yöntemler gönderilecek olan mesajı şifrelemek üzerine olmuştur. Bu yönteme kriptografi denir. Mesajın anlaşılmaz hale getirilmesidir.

Tarihte bilinen ilk kriptografi yöntemi yer değiştirme ve harf değiştirme yöntemidir. Bu yöntemlerden ilki mesaj içerisindeki harflerin birbiri ile yer değiştirmesidir, ikincisi ise harflerin başka harflerle yer değiştirmesidir. Bu yöntemi kullanarak yapılan en ünlü yöntem Sezar Şifresi'dir. Bu teknikle her bir harf kendisinden birkaç sonraki harfle temsil edilir.

MÖ.1900 dolaylarında bir Mısırlı katip yazdığı kitabelerde standart dışı hiyeroglif işaretleri kullandı. 1000 – 1200 Gazneliler den günümüze kalan bazı dokümanlarda şifreli metinlere rastlanmıştır. Bir tarihçinin dönemle ilgili yazdıklarına göre yüksek makamlardaki devlet görevlilerine yeni görev yerlerine giderken şahsa özel şifreleme

bilgileri (belki şifreleme anahtarları)veriliyordu.1623 Sir Francis Bacon, 5-bit ikili kodlamayla karakter tipi değişikliğine dayanan stenografı buldu.
Teknolojinin baş döndüren bir hızla gelişmesi neticesinde değişen haberleşme yolları olarak en son internet kullanılmaktadır. Internet ilk olarak, geliştirilen çoğu teknoloji gibi, askeri amaçlarla kullanılmaya başlanmıştır. Hızlı gelişmelerin ardından tüm insanlığın hizmetine sunulmuştur. Gerek genel gerekse özel olsun hemen hemen tüm haberleşmeler internet üzerinden yapıldığı için iletişimde güvenirlik sorunları ortaya çıkmıştır. Kullanılan kriptoloji yöntemleri mesajı iyi bir şekilde şifrelemekte fakat dezavantajı ise ortada bir şifreli metnin olduğu üçüncü kişiler tarafından bilinmektedir. Bu sorunu ortadan kaldırmak için sırörtme(steganography)yöntemi geliştirilmiştir.

Steganography mesajı bir görüntü, ses veya video içerisine yerleştirerek saklama yöntemidir. Böylelikle üçüncü kişiler tarafından gönderilen bir gizli mesajın varlığı anlaşılması imkânsızlaştırılmıştır.İlk sır örtme tek bir görüntü(resim) üzerine LSB (LeastSignificant Bit embedding) yöntemiyle yapılmıştır.

1.1. Literatürde Yapılan Çalışmaların Özetleri

Bir müzik şirketinin 1954 yılında yapmış olduğu kayıtların içerisine sahiplik bilgisini içeren kod yerleştirmek için almış olduğu patentle birlikte, telif haklarının korunmasına yönelik ses bilgilerinin içerisine veri gömme tekniği üzerindeki çalışmalar yoğunlaşmıştır.

Lisa M. Marvel, Charles T. Retter ve Charles G. Bencelet’ in 1998 yılında birlikte yapmış olduğu çalışmada resim içerisine hata kontrol kodu ile veri gömme çalışmaları yapmış, çalışma sonucunda oluşan hataları tespit ve giderilmesi konusunda bilgiler vermişlerdir.

XiaohangZhang ve LequenMin'nin 1998 yılında yapmış oldukları gerçek zamanlı videoya LSB yöntemi ile veri gömme çalışması ile sırörtme alanında oldukça kapsamlı veriler elde etmişlerdir.
KennethBarr ve KrsteAsanovi'c 2003 yılındaki yayınladıkları "EnergyAwareLossless Data Compression" adlı makalede kablosuz haberleşme yapılırken veri gönderilmeden önce sıkıştırma işleminin yapılmasının enerji boyutundan getireceği kazançları göstermişlerdir.

MohammadShirali'nin 2007 yılında yayınlamış olduğu "Steganography in MMS" adlı makalesi ile mobil telefon üzerinden kablosuz olarak video ile gizli veri iletimi ve gizli verinin geri elde edilmesi hakkında çalışmalarını ortaya koymuştur.

NedeljkoCvejic'in 2002 yılında yayınlamış olduğu "Increasing the capacity of LSB-based audio steganagraphy" adlı makalesindeki çalışması ile LSB tekniğinin veri gömme kapasitesini geliştirmiş olduğu algoritma ile %30 oranında arttırmıştır.

Christian Kratzer, Jana Dittmann, Thomas Vogel ve ReykHillert 2008 yılında yayınladıkları makalede iki kullanıcı arasında sesli görüşme yapılırken sessizlik algılanması, şifreleme ve sır örtüsü yöntemlerini kullanarak gizli bilgi gönderme işlemini gerçekleştirmişlerdir. Gönderilecek bilgiler, ses bilgilerinin son bitlerine(LSB) gömülmüştür.

Kurniawan Wibowo ve Ihsan Jatnika 2008 yılında yayınlamış oldukları "Insert Messages into Digital Images Using steganography Technique in Visual C# 2005" adlı makalesindeki çalışması ile LSB yöntemini kullanarak Visual C# ortamında veri gizleme algoritması geliştirilmiştir.

Yıldıray Yalman ve İsmail Ertürk'ün 2009 yılında yayınladıkları "İmge Histogramı Kullanılarak Geometrik Ataklara Dayanıklı Yeni Bir Veri Gizleme Tekniği Tasarımı ve Uygulaması" adlı makalede histogramlar yöntemi ile LSB tekniğini birleştirmiş ve sonuç imgelerinin döndürme, görüntüleme oranını değiştirme ve eğme gibi geometrik ataklara karşı oldukça dayanıklı, esnek ve maliyeti düşük uygulamalar geliştirilmiştir.

Arup Kumar Bhaumik, Minkyu Choi, Rosslin J. Robles ve Maricel O. Balitanas ‘ın 2009 yılında yayınladık “Data Hiding in Video” adlı makalede ham videolarda (.avi) DCT tekniğini kullanarak veri gömmeye uygun alanları tespit ederek LSB tekniği ile bu alanlara verileri gömme algoritmaları geliştirmişlerdir.

1.2. Tez Çalışmasının Amacı ve Motivasyonu

Gelişen teknoloji ile birlikte büyük devletler savaş zamanlarında değişik yöntemler kullanarak mesajları şifrelemeyi başarmışlardır. Şifrelenmiş anlaşılması zor fakat varlığı belli mesajlar üçüncü kişiler tarafından bilinmekte fakat geri elde edilmesi konusunda zorluk çekmekteydiler.

Almanlar II. Dünya savaşı sırasında bir mikro noktalama aleti geliştirmişlerdir. Bu araç sayesinde bir metinde bulunan noktalı harflerin noktalarına gizli veriyi çok küçülterek yerleştirmekteydi. Daha sonra metni alan kişi bu noktalar birleştirilerek anlamlı mesaj elde etmiş olurdu.

Şifreleme yöntemi mesajın içeriğini saklamış olsa bile gizli bir haberleşmenin olduğunu gizleyememektedir. Bu eksikliğin giderilmesi ile ilgili çalışmalar neticesinde masum gibi görülen taşıyıcı (resim, ses, video vb.) içerisine gömülmeye başlanmıştır. Hatta veri taşıyıcı dosyaya gömülmeden önce şifrelenebilmektedir. Bu geliştirilen teknikle mesajın varlığını sadece gönderen ve alıcı bilmekte, iletişim yolunu dinleyen üçüncü kişiler mesajın varlığından bile haberdar olmamaktadır.

Özellikle Internet ortamında kullanılan gizli haberleşme yöntemleri milli güvenliğin sağlanması açısından önem taşımaktadır. 11 Eylül’de yaşanan saldırı olaylarında teröristlerin Internette sır örtüsü tekniği ile haberleştikleri saptandıktan sonra gizli haberleşme tekniklerinin popülerliği artmıştır.

Oluşan tüm bu gelişmeler göz önüne alınarak, özellikle Internet üzerinden yapılan haberleşmelerde zararsız görünen dosyaların(metin, resim, ses, video vb.) içerisine

gizli bilginin gömülebileceği ve bu gizli verinin gömülmüş olduğu dosyanın kablolu veya kablosuz ortamda güvenli bir şekilde haberleşebileceği, verinin taşıyıcı dosyaya gömülürken sır örtüsünün kullanılabileceği, gömülmeden önce seçilen bir yöntemle şifrelenebileceği, bu yolla daha güvenli iletişimin sağlanabileceği gerçeği bu tezin temel motivasyonunu oluşturmaktadır.

1.3. Tez Organizasyonu

Yapılan çalışmaların sunulduğu bu tez 5 ana bölümden oluşmaktadır.

Bölüm 1 Giriş: Bu bölümde tez çalışmasına konu olan problemin tanımı, çalışmanın amacı, literatürdeki ilgi problemle ilgili yapılan çalışmaların özetleri ve tez çalışmasının amacı ve motivasyonu hakkında bilgi sunulmaktadır.

Bölüm 2 Sayısal görüntü Esasları ve Görüntü İşleme: Bu bölümde insan görme sistemi hakkında, görme olayı, renkli görmeyi sağlayan etkenler, gözün yapısı gibi görme olayı ile ilgili sistemler incelenmiştir. Ayrıca sayısal görüntü, özellikleri, en küçük yapısına kadar incelenerek sayısal görüntünün tanımı yapılmıştır. Sayısal görüntüde de kullanılan renk modelleri, özellikleri ve birbirine dönüşümleri anlatılmıştır. Sayısal görüntü ile analog görüntü arasındaki farklar ve sayısal görüntüye geçişin sebepleri ayrıntılı bir şekilde sunulmuştur.

Bölüm 3 Şifreleme Teknolojileri: Gelişen iletişim yollarının ve teknolojilerin kötü niyetli kişilerce başkaları arasında gerçekleşen iletişimi dinlemede kullanması üzerine geliştirilen şifreleme yöntemi, şifrelemenin tarihi gelişimi, amacı ve çeşitleri konuları incelenmiştir.

Bölüm 4 Videolar İçin Sırörtme Yaklaşımı ile Geliştirilen Veri Gömme Algoritmaları: Güvensiz iletişim yollarının güvenliğini arttırmak amacıyla tasarlanan sırörtme(steganography) veri kapasitesi, algılanabilirlik vb. gibi sebeplerden dolayı çeşitli algoritmalar tasarlanmıştır. Bu algoritmalardan tez çalışmamız için

geliştirdiklerimiz bu bölümde anlatılmıştır. Algoritmaların amacı, blok diyagramları, özellikleri anlatılmıştır. Ayrıca gizlenecek olan veriyi hareketli görüntülere gömebilmek için geliştirilen kodlama yöntemi(RGB) hakkında da bilgiler verilmiştir. Geliştirilen arayüz tasarımı ve programların çalışması sunulmuştur.

Bölüm 5 Geliştirilen Uygulamalara Ait Deneysel Sonuçların Değerlendirilmesi: Geliştirilen algoritmalarla ilgili yapılan performans değerlendirmeleri, bozulan bit sayıları PSNR ve MSE değerleri ve bu değerlerin yorumları bu bölümde bulunmaktadır.

BÖLÜM 2. SAYISAL GÖRÜNTÜ ESASLARI VE GÖRÜNTÜ İŞLEME

2.1. Giriş

Bu bölümde görüntü işlemenin daha iyi anlaşılması için bazı temel kavramlar ve bilgiler verilmektedir.

Sayısal görüntü temel anlamda, piksel öğelerinden oluşan görüntüdür. Başka bir deyişle dijital görüntü, piksel öğelerden oluşan elektronik bir fotoğraftır. Her piksel öğe, resmin bir kısmını siyah, beyaz, grinin bir tonu ya da bir rengi içeren bir renk tonu değeri ile temsil eder. İki rakamlı(0 ve 1) kodlar bu dijital görüntüleri bilgisayar ortamında karakterize eder.

Gelişen teknoloji ve yöntemler sayısal görüntünün kullanım alanlarını arttırmıştır. Değişen teknolojinin yanı sıra kolay yayılımı, kolay elde edilmesi, kolay saklanması veya kolay geri elde edilmesi vb. özellikleri sayesinde analog görüntünün önüne geçmiştir. Analog görüntünün yayılımı uydu yayını, RF yayını ve koaksiyel kablo ağına ihtiyaç duyarken, sayısal görüntünün ise her türlü yolla iletimi sağlanabilir. Analog görüntünün kalitesi değişkenken sayısal görüntününki CD-DVD-HD kalitesindedir. Tüm bu ve buna benzer daha birçok özellik neticesinde analog görüntünün sayısal görüntüye oranla daha maliyetli oluşu yine sayısal görüntünün bir avantajı olmuştur.

Analog görüntülerin kayıt işlemleri şerit halindeki film üzerine kimyasal değişiklikler meydana getirerek gerçekleştirilir. Bu yüzden filmler güneş ışınlarına ve manyetik alana maruz kaldıklarında geri dönüşü mümkün olmayan bozulmalar

gerçekleşmektedir. Sayısal görüntü ise ışık dalgalarının elektrik sinyallerine dönüştürülmesiyle kaydedilir. Dolayısıyla veri bozulmaları veya kayıpları analog görüntülerinkine oranla daha zordur.

Analog görüntülerin kaydedilmesi ve saklanması için çok büyük hafıza alanlarına ihtiyaç duyulurken sayısal görüntüde ise bu ihtiyaç aşağıdaki Denklem 2.1 ile bulunabilir;

Çerçevedeki toplam piksel x saniyedeki çerçeve sayısı x ..
Piksel için ayrılan hafıza x video süresi (2.1)

Denklem 2.1 kullanılarak standart VCD formatındaki 30 dakikalık(2700sn) bir video için gerekli kapasite;

(352 x 240) x 25 x 3 x 2700=17,107,200,000 bayt=17,10 GB

olarak bulunur. Sayısal görüntünün yukarıda saymış olduğumuz avantajlarının dışında kullanımında bazı ihtiyaçlara gerek duyulmuştur. Bu önemli ihtiyaçlardan bazıları da bu teze konu olan haberleşmede güvenlik ve verinin gizliliğidir.

2.2. Görme ve Görüntü İşleme Arasındaki İlişki

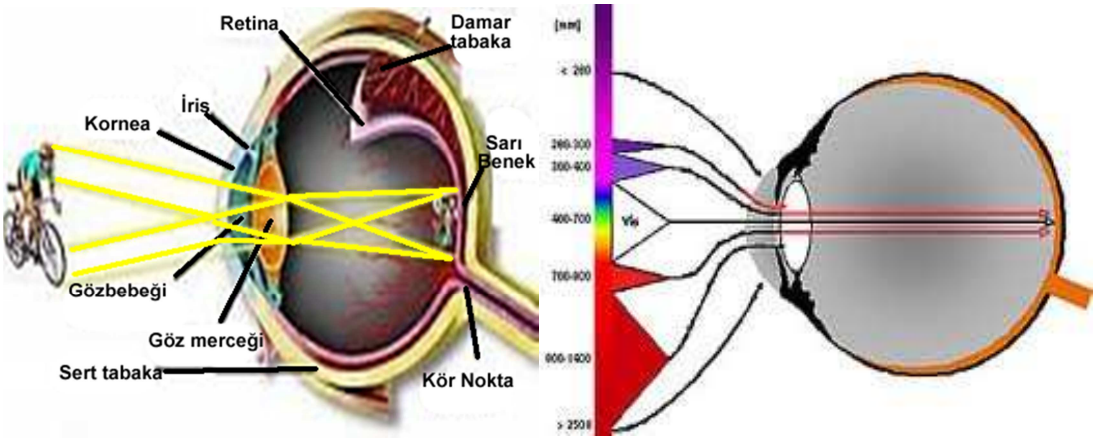
Video, saniyede en az 25 resim çerçevesinin peşi sıra akışı ile oluşur. Bu oluş esasında sıralı resim slaytı gibidir. Fakat insan bunu fark etmez ve video olarak izler. Videonun oluşumunun temelinde insan göz sisteminin bazı durumlarından yararlanılmaktadır. Yani göz 25 FPS(Frame per Second) ‘de ve üzerindeki resim akışlarını fark edemez ve video olarak izler.

Görüntü işlemede de insan göz sisteminin özelliklerinden faydalanılır. Göz her ışın dalgasındaki ışıkları göremez. 350nm ve 780nm arasındaki ışınları görebilir. Bu aralıktaki ışınlara görülebilir ışın denir. Bu alanın dışındakiler insan göz sistemi

tarafından fark edilemez. Görüntü işlemede de bu aralıktaki ışınların değerlerinin insan göz sisteminde algılanmayacak şekilde değişiklikler yapılmaktadır. Tezimizin kapsamında olan görüntü işlemeyi anlayabilmek için göz ve görme olayı hakkında biraz daha bilgi edinmek gerekmektedir.

2.2.1. Göz ve görme

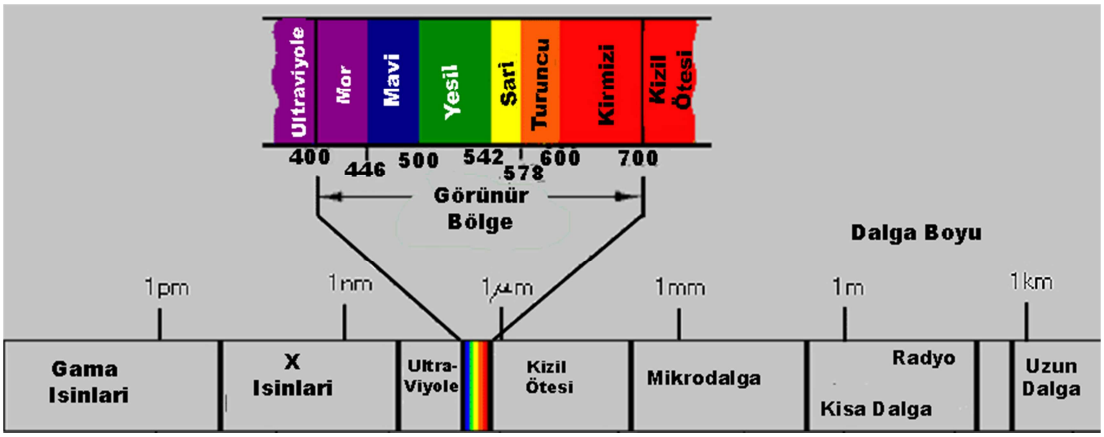
Görme, ortamdaki ışık ve cisimlerin duyusal retinadaki fotoreseptör hücreleri tarafından algılanmasıdır. Bu işlem fotoreseptör dış segmentlerindeki görme pigmentleri tarafından yapılır. Görme pigmentleri retinal ve opsin'den oluşur. Rod reseptörlerindeki görme pigmenti rodopsin, koni reseptörlerindeki pigment, ise iodopsindir. Işığın etkisiyle retinal ve opsinin birbirinden ayrılması membran potansiyelde değişikliğe yol açar ve bir impuls oluşur. Bu fotoşimik olaylarla elektriksel impuls olarak optik sinire, oradan da oksipital korteksteki görme merkezlerine gönderilir. Olay üç nöronlu ve iki sinapslıdır. Birinci nöron, koni ve bipolur hücreler olup ganglion hücrelerle sinaps yapar. İkinci nöron olan ganglion hücreleri optik sinir aracılığı ile lateralgenikulate cisme ulaşır. İkinci sinaps buradadır. Sinaps sonrası üçüncü nöron olarak optik radyasyo lifleriyle korteksteki görme merkezine ulaşır. Gözün bütün diğer yapıları bu işleme yardım etmekle görevlidir. Kornea ve lensin kırıcılığı, uveanın besleyici rolü, skleranın koruyuculuğu, gözdışı kaslar yardımı ile ilgi noktasına fiksasyon hep bu fotoreseptör işlevine yöneliktir ve görsel dünyadaki hayaller sürekli bir şekilde alınır ve iletilir. Bu işlevi yapan asıl nokta özellikle retinadaki makuladır. Dolayısıyla, görme kavramı makulanın görevi olan; görme keskinliği, kontrast görme, renkli görme, karanlık adaptasyonu ile görme alanı ve sonucu binoküler görme ile stereopsis (derinlik hissi) gibi birçok nitelik ve nicelik özelliklere sahiptir. Normal görme için tüm bunların fizyolojik sınır içinde olması gerekir. Bunlar;



Şekil 2.1 İnsan gözünü oluşturan önemli bölümler ve görülebilir ışık.

Görme Keskinliği: çevreden göze 1 dakikalık açıyla gelen cismi fark edebilme yeteneğidir.

Kontrast Görme: zemindeki aydınlık ile üzerindeki cismin aydınlık farkını, zıtlığını fark edebilme yeteneğidir (örneğin sisli havada sürücünün bir yayayı fark etmesi gibi).



Şekil 2. 2. Görülebilir ışık dalga boyu.

Renkli Görme: 350-780 nm dalga boyundaki ışık insan gözü için algılanabilir yani görünebilir ışıktır. Detayı ve rengi görmeye yarayan kon reseptörleri üç ayrı dalga boyundaki ışığı algılayabilecek biçimde farklılaşmıştır. Uzun dalga boyu algılayan konlar kırmızıya, orta dalga boyu algılayan konlar yeşile, kısa dalga boyu algılayan konları da mavi ışığa maksimum emilimle cevap verir.

Görme Alanı: Retinanın tüm periferi ile cevap verebildiği uzaysal alandır. Bir gözün belli bir noktaya fikse olduğu sırada çevrede algılayabildiği alanın tümüdür. Genişliği derece, derinliği ise duyarlılık olarak ifade edilir. Retina periferinde duyarlık özellikle karanlığa adapte gözlerde artmıştır. Bu rod reseptörlerinin alacakaranlıkta görmeye programlı oluşu nedeniyledir ve fonksiyonları karanlık adaptasyonu ile incelenir.

Binoküler Görme ve Derinlik Hissi: Her iki gözde foveaların algıladıkları görüntüler, oksipital korteks tarafından birleştirilir ve tek görüntüye çevrilir (füzyon). Cisimlerin kenarları, gölgeler iki ayrı gözün algıladığı görüntülerde küçük detay, farkı oluştur. Bu da stereoskopik yani derinlik hissi diğer anlamda da üç boyutlu görmeyi oluşturur.

Tüm bu görsel işlevler için gerekli olan enerji kaynağı ışıktır.Güneş bitmeyen ışık kaynağıdır. Görme olayının meydana gelebilmesi için de elektromanyetik bir dalga olan ışığın algılanması gerekir.

Bilindiği gibi atom, ortada bir çekirdek etrafında enerjilerine bağlı olarak belli uzaklıkta yerleşmiş yörüngelerde dönen elektronlardan oluşur (BOHR Atomu). Düşük enerji durumunda alt yörüngelerde bulunan elektronlar atomun enerjisi arttığında üst yörüngeye çıkar. Enerjisi uzun süre yetmeyeceğinden bir müddet sonra alt yörüngeye düşer. Aradaki enerji farkı bir ışık taneciği (foton) yaratır. Bu olay komşu atomdaki dış elektronun düşmesine ve diğer atomların da bu etkileşim sonucu sinüzoidal seyreden ışık dalgalarına dönüşerek saçılıma uğrar. Yayılma anında birbirlerine ve dalganın ilerleme yönüne dik bir elektriksel ve manyetik alan ortaya çıkarırlar (elektromanyetik dalgalar). Bu şekilde de maddenin görünmesi sağlanır.

Elektromanyetik dalgalar yayılır, yansır ve emilir. Işığın boşluktaki yayılma hızı 186.000 mil/sn'dir. Dalga boyu ise binlerce metreden (radyo dalgaları) çok ufak uzaklıklara (gamma ışınları) kadar olabilir. Geçtikleri ortamın atom yapısına bağlı olarak hızları yavaşlar, emilir veya yansır. Ancak elektromanyetik boyutun 350-780 nm dalga boyuna sahip olan kısmı görülebilen ışıktır. Göz tarafından algılanma nedeni ise bu dalga boylarının rod ve konilerdeki pigment tarafından emilmesi ve

sonucunda kimyasal reaksiyonların başlamasıdır (görme olayı). Daha yüksek veya daha düşük dalga boylarında bu olay olmadığı için bu ışınlar var oldukları halde görünmezler (görünmeyen ışınlar).

Elektromanyetik dalganın enerjisi dalga boyu ile ters orantılıdır. Bu nedenle dalga boyu kısaldıkça enerjisi artar. Örneğin 400 nm dalga boyundaki foton enerjisi 800 nm dalga boyuna göre iki kat enerji yüklüdür. Dolayısıyla X ışınları ağır doku harabiyeti, ultraviyole ışınları (UV) yanık yaparken, kırmızı ışık zararsızdır.

2.2.2. Renk teorisi ve renk modelleri

Erken dönem filozof, fizikçi ve sanatçıları, renk nedir, onları nasıl görürüz sorularına yanıt aramışlar ve çevrelerini kuşatan görsel dünyanın açıklamasına yardım etmek için teoriler geliştirmişlerdir.

Aristoteles, renkler arasındaki benzerlikleri güneş ışığı, alev, hava ve suyun farklı kuvvetlerdeki karışımına bağlamış, “karanlık, ışığın yoksunluğu sebebiyledir” demiştir.

Büyük Rönesans sanatçısı Leonardo da Vinci beyaz ve siyahı da ana renkler arasına katmış, tamamlayıcı kontrast olarak bilinen fenomeni gözlemlemiştir. Da Vinci, renk kombinasyonlarının optik etkilerine dikkat çekmiş, perspektif ve gölge etkilerini tanımlamıştır.

İngiliz fizikçi Newton, tüm spektral renklerin beyaz ışıkta var olduğunu labrotuvar ortamında ispatlamış, renk ilişkilerini gösteren ilk renk halkasının onlardan yapıldığını açığa çıkarmıştır.

İngiliz etimolog ve gravür sanatçısı Moses Haris ışıktan çok pigmentler ile çalışmış birincil (kırmızı-mavi-sarı) ve ikincil renk (turuncu-mor-yeşil) renk pigmentlerini elde etmiştir.

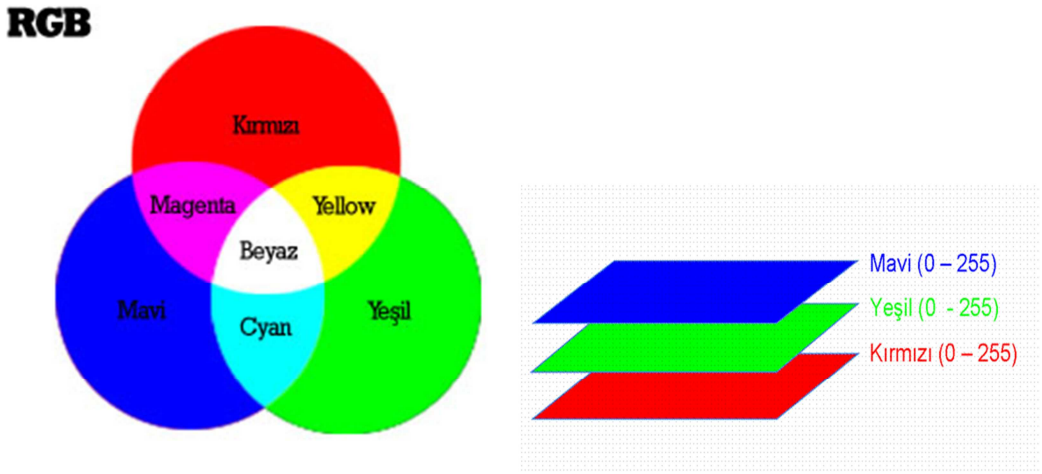
Ünlü Alman şairi Goethe “renklerin teorisi” (1810) adlı kitabında rengi gözde oluşan görsel bir fenomen olarak ele almıştır.

Alman ressam OttoRunge rengin üç boyutlu modeli üzerinde çalışarak renk küresini yayınlamış ve renk ilişkilerini göstermiştir.

2.2.3.1. RGB renk modeli

Fosfor yapılarının ışık yayma prensibine dayalı olarak oluşturulmuş bir renk modelidir. Kırmızı(Red), yeşil(Green) ve mavi(Blue) renklerinin farklı değerlerde karıştırılmasıyla oluşur. Adını da bu üç rengin İngilizce isimlerinden almıştır. Renk oluşumu için kırmızı, yeşil ve mavi renklerin değişken değerlerinin birleşimiyle oluşur. Beyaz renk için bu üç renk bulunurken, siyah renk için üçü de yok demektir. RGB modeli televizyon, bilgisayar, kameralar, fotoğraf makineleri, tarayıcılar vb. aktif göstergelerde kullanılır.

RGB renk modeli Şekil 2. 3 ‘de gösterilen renklerle ifade edilir. RGB modelini oluşturan her bir renk 0 - 255 arasında bir renk değerine sahiptir. Bu değerlerin değişmesiyle diğer renkler oluşur. Örneğin RGB değerlerinin (0,0,0) olması siyah renk olduğunu, (255,255,255) olması ise beyaz renk olduğunu gösterir.



Şekil 2. 3. RGB renk modelleri.

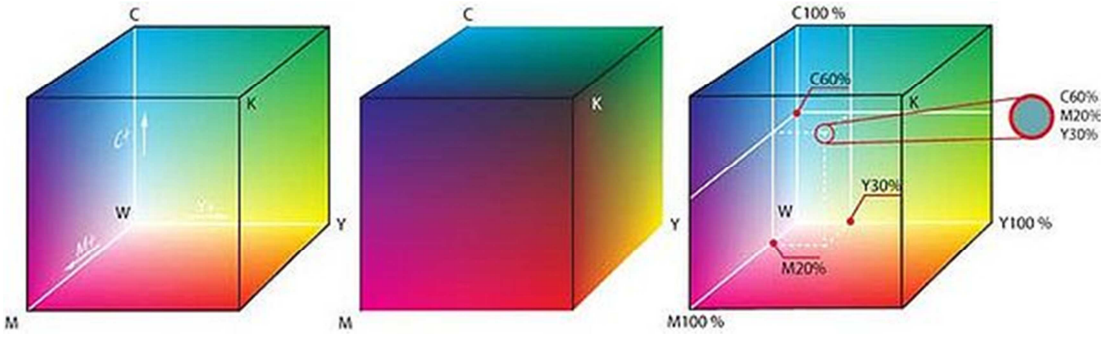
RGB renk modeli aygıta bağımlı renk modelidir. Internet ve sayısal ortamda kullanılmasına karşın baskı ortamında kullanılamaması dezavantajlarından biridir. Kullanım alanlarının Internet ve sayısal ortamlar olduğu için tez çalışmamızda RGB renk modeli kullanıldı.

2.2.3.2. CMYK renk modeli

CMYK basılı ortamlar için kullanılan renk uzayının ismidir ve farksal bir renk modelidir, yani mürekkep kâğıdın üzerine uygulandığında, bu renkler ışığı emer. Bu renk modeli, diğer renkleri oluşturmak için CMYK pigmentlerini karıştırma üzerine kuruludur. Bu renkler tram yöntemi ile baskıda kullanılan renkleri oluştururlar. Aslında temel renk sayısı üçtür. Siyah bu renklere zorunlu olarak ilave edilmiştir. Kuramda üç rengin karışımının siyahı oluşturması gerekirken, pratikte bu durum böyle değildir. Bu üç pigmentin birleşiminden koyu, çamur rengi gibi bir renk çıkar. Bu yüzden gerçek siyah renklere sahip bir renk paleti için siyah eklenir. CMYK ışığı emerek çalışır. Görülen renkler, ışığın üzerine düştüğü nesne tarafından emilen değil, nesneden yansıyan renklerdir. Hem üç rengin mürekkepleri yeterli renk şiddetini sağlamadıklarından hem de üç renkli mürekkebin karışımı yerine siyah mürekkep kullanmanın maliyetinin daha düşük olması nedeniyle siyah renk sisteme ilave edilmiştir.

CMYK tram yöntemiyle dört renk birbirini tamamlayarak elde edilmek istenen renk oluşturulur. Bir başka deyişle basılı medya gözlerimiz RGB deki gibi direk ışıkları değil basılı medya üzerinde yansıma yapan güneş ışığını görür. Bu bağlamda CMYK gerçek, RGB zahiri görüntü anlamına gelebilir.

Şekil 2.4 ‘de görüldüğü gibi CMYK renk modelinde üç temel renk vardır. Bu renklerin birleşimiyle gerçek siyah renginin elde edilmesi imkansız olduğundan dördüncü bir renk olarak siyah renk sonradan bu modele eklenmiştir. Dört rengin belirli yüzdelerle birleşmesiyle farklı renkler oluşmaktadır. Bu oluşum gerçek renge en yakın olan renklerdir. Bu yüzden CMYK modeli yüksek seviyeli baskılarda ve matbaalarda yaygın olarak kullanılır.



Şekil 2. 4. CMYK renk modelleri.

CMYK modelinde kullanılan dört temel renk;
Cyan(Cam göbeği), Magenta(Galibarda), Yellow (Sarı), Key (black - Siyah) olmak üzere oluşur.

Daha birçok renk modeli bulunmaktadır. Bu bölümde, tez çalışması içerisinde en çok kullanılan renk modelleri ayrıntılı olarak işlenmiştir.

2.2.3.3. Renk modelleri arasındaki dönüşümler

Tüm renk modellerinin kullanım alanlarının farklı olması ortak uygulamalarda bazı sorunlar çıkarmaktadır. Bu uyum sorunlarının aşılabilmesi için renk modelleri arasında dönüşümler yapma gereği duyulmuştur. Denklem 2.2 ‘de CMYK ve RGB renk modellerinin birbirine dönüşümü, denklem 2.3 ‘de RGB ve YIQ renk modelleri arasındaki dönüşümü, Denklem 2.4 ‘de ise RGB ve HSI renk modelleri arasındaki dönüşümü göstermektedir.

$$\begin{bmatrix} C \\ M \\ Y \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} - \begin{bmatrix} R \\ G \\ B \end{bmatrix} \tag{2.2}$$

$$\begin{bmatrix} Y \\ I \\ Q \end{bmatrix} = \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ 0.596 & -0.275 & -0.321 \\ 0.212 & -0.523 & 0.311 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix} \tag{2.3}$$

$$\mathrm{I} = \frac{1}{3}(R + G + B)$$

$$\mathrm{S} = 1 - \frac{3}{(R + G + B)}[\min(R, G, B)] \tag{2.4}$$

$$H = cos\left\{\frac{\frac{1}{2}[(R - G) + (R - B)]}{[(R - G)^2 + (R - B)(G - B)]^{1/2}}\right\}$$

2.3. Sayısal Görüntü

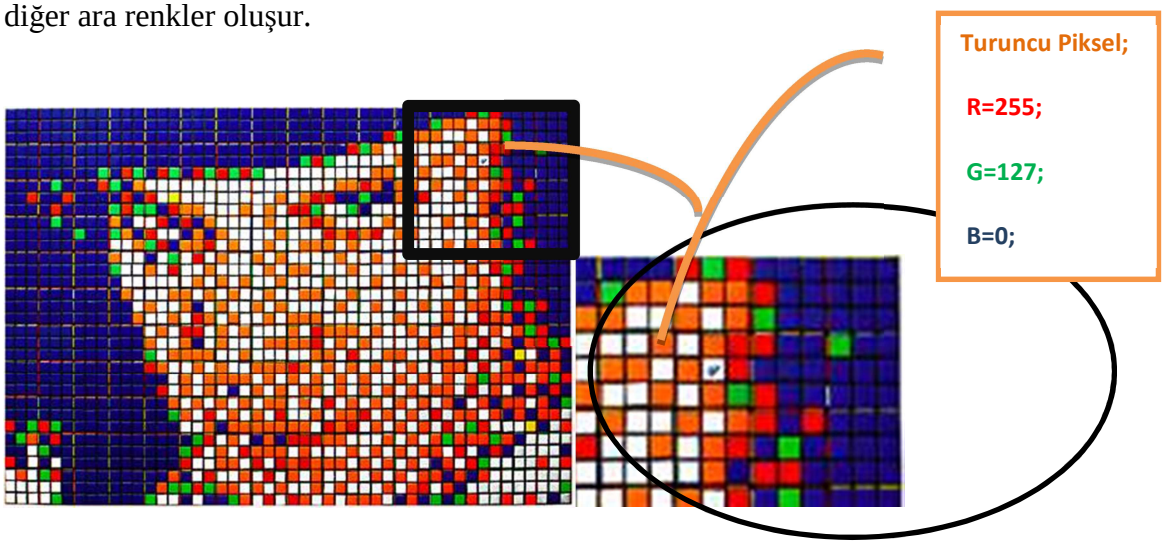
Teknolojinin hızlı gelişimi ve analog görüntünün önemini kaybetmesiyle sayısal görüntünün değeri hızla artmıştır. Gerek işleme ve kullanma kolaylığı, gerek kaydetme ve saklama kolaylığı, gerekse maliyetinin hesaplılığı gibi özellikleriyle sayısal görüntü, analog görüntünün yerine hızla geçmiştir.

2.3.1. Sayısal görüntünün oluşumu

Sayısal görüntüyü oluşturan en küçük yapı taşına piksel denir. Piksel İngilizce "Picture cell" resim hücresi anlamına gelen kavramın kısaltılmasıyla oluşmuştur. Bir piksel ilgili resmin tüm renk özelliklerini taşır. Bu sebeple sayısal görüntünün temel yapı taşı denilmektedir. Bir piksel, piksel başına düşen bit sayısı (bit-per-pixel--bpp) ile ifade edilir.

-- 1 bpp, 2^1 = 2 renk(tek renkli)
-- 2 bpp, 2^2 = 4 renk
-- ...
-- 8 bpp, 2^8 = 256 renk
-- 16 bpp, 2^{16} = 65,536 renk(yüksek renk)
-- 24 bpp, 2^{24} = 16,7 milyon renk(gerçek renk)

Renkli görüntüyü oluşturan her piksel Kırmızı(Red), Yeşil(Green) ve Mavi(Blue) renklerinin birleşmesiyle oluşur. Bu üç temel rengin değişik oranlarda birleşmesiyle diğer ara renkler oluşur.



Pikselleri belirgin görüntü Piksellerin daha büyük görüntüsü

Şekil 2. 5. Sayısal görüntüde piksel.

İnsan gözü bir renkli görüntü içerisindeki pikselleri fark edemez. Onları bir bütün(resim) olarak algılar. Şekil 2.5. 'de pikselleri belirginleştirilmiş bir görüntü

verilmiştir. Bu görüntünün bir bölümünden parça ayrılıp ayrıntılı incelemek için büyütülmüştür. Büyütülen görüntüde pikseller daha rahat bir şekilde görülmektedir. İçinden bir piksel seçilerek o pikseli oluşturan RGB değerleri gösterilmiştir. Örnek piksel olarak turuncu renkteki piksel seçilmiştir. Turuncu pikseli oluşturan RGB renk değerleri, (255, 127, 0) 'dır. Bu örnekten de anlaşıldığı üzere her bir rengi temsil eden piksel, aslında kırmızı, yeşil ve mavi renklerin değişik oranlarda bir araya getirilmesiyle farklı renklere sahip olabilir.

Bir görüntüyü oluşturan piksel sayısı ne kadar fazla ise görüntü gerçek rengine o kadar yakın olur. Piksel sayısı azaldıkça bulanık, donuk, rengi bozuk görüntüler oluşur. Bir görüntüde kaç piksel olduğu bilgisi ise çözünürlüğü ifade eder. Çözünürlük bir görüntüdeki yatay ve dikey olarak toplam kaç pikselin olduğunu veren değerdir. Çözünürlük ne kadar fazla ise görüntü gerçek rengine o kadar yakındır denilebilir. Örneğin bir görüntünün yatayda 640, dikeyde 480 pikseli var ise bu görüntü 640 x 480 çözünürlüğe sahiptir denir.
Bir görüntünün hafızada kapladığı alan, resmin yüksekliği, genişliği ve derinliği bilindiği takdirde Denklem 2.5' deki gibi hesaplanabilir.

$$\text{Dosya boyutu} = (\text{yükseklik} \times \text{genişlik} \times \text{renk derinliği})/8 \qquad (2.5)$$

Örneğin; 240 x 300 piksel boyutlarına sahip ve 24 bit renk derinliği olan bir resmin boyutu;

Dosya boyutu=240 x 300 x 24 =1728000(bayt) olur.

2.4. Sayısal Videonun Yapısı ve Oluşumu

Videolar, hareketsiz sayısal görüntülerin ardı sıra saniyede en az 25 kez oynatılmasıyla oluşur[1]. İnsan göz sistemi bu hareketsiz resimlerin akışını anlayamaz ve video olarak izler.

Sayısal bir videonun oluşması için, bir ışık kaynağına, bir nesneye ve nesnenin ışığı yansıtmasına gerek vardır. Tüm bu şartlar oluştuğunda önce görüntü ve ardından sayısal video oluşur.

2.5. Sonuç

Bu bölümde, insan görme sistemi ve görme olayı hakkında bilgi verilmiştir. Sayısal ve baskı ortamlarında kullanılan renkler, renk modelleri ve bu modellerin birbirine dönüşümü incelenmiştir. Çalışmamızda hangi renk modelinin kullanılabileceği hakkında bilgi sahibi olundu. Bir sayısal görüntü en küçük parçasına kadar incelendi. Pikselin yapısı ve renk bileşenleri değerlendirildi. Çözünürlüğün resim ve depolama kapasitesi üzerindeki etsini denklemler yardımıyla incelendi. Tezimizin içeriğinde yer alan videonun oluşumu ve tüm incelenen konularla bağlantılar sunuldu.

BÖLÜM 3. ŞİFREMELE TEKNOLOJİLERİ

3.1. Giriş

Büyük bir hızla gelişen teknoloji, insanoğlunun refah düzeyini oldukça yükseltmiştir. Önce bilgisayarın ebatlarının küçültülüp maliyetinin azaltılması ve evlere girmesi, ardından da Internetin hızlı bir şekilde yaygınlaşması haberleşmede ve iletişimde çığır açmıştır.

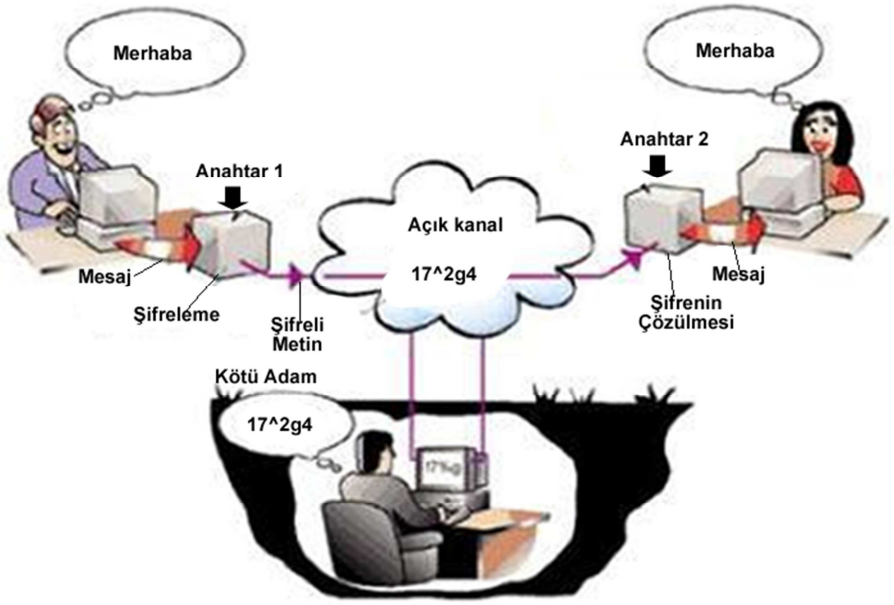
Tüm teknoloji insanoğlunun bazı ihtiyaçları üzerine geliştirilmektedir. Karşılanan her ihtiyaç, ardından yeni bir ihtiyaç doğurmaktadır. Gelişen haberleşme teknikleri ve yolları tüm insanlığın Interneti yaygın bir şekilde kullanmaya başlamasıyla eski güvenirliliğini kaybetmiştir. Artık mesajlar sadece alıcı tarafından değil üçüncü kişiler tarafından da elde edilebilir oldu. İletişimin güvenirliğini tekrar kazanmak için birçok çalışmalar gerçekleştirilmektedir. Bunlardan biri de göndericiden alıcıya iletilen mesajı şifreleme tekniğidir. Bir mesajı şifrelemek, alıcı dışındaki kişilerin göndericiden gönderilen mesajı ele geçirseler de onu anlaşılmayacak hala getirmektir.

Şifreleme bilimi mesajların gizli tutulma sanatıdır. Şifre çözme ise şifreli metnin şifresini kırma sanatıdır. Şifreleme bilimi ile uğraşanlara kriptograf, şifre çözümü uygulamacılarına ise kriptanalist denir.

Şifreleme işlemi, çeşitli şifre algoritmaları kullanarak orijinal metni gizleme işlemidir. Şifreleme için gizlenmesi gereken bir mesaj ve genellikle anahtar denilen ek bilgiler olmalıdır. Mesaj ve anahtar birleşerek bir kriptogram üretilir. Bir

kriptosisteme güvenli denilebilmesi için şifreli metnin anahtar olmadan başka kişiler tarafından çözülememesi gereklidir. Metni şifrelemeye encryption, şifre çözme işine ise decryption denir.

Hemen hemen her teknolojik gelişimde olduğu gibi şifreleme ve şifre çözme algoritmaları ilk olarak askeri ve diplomatik alanlarında kullanılmaya başlanmıştır. Teknoloji geliştikçe ve ihtiyaçlar arttıkça güvenlik sivil toplum ve ticari kuruluşlar içinde önem kazanmış, şifreleme tekniği hemen her sektörde kullanılmaya başlanmıştır.



Şekil 3.1. Genel şifreleme ve şifre çözme yol haritası.

Şekil 3.1’ de genel bir şifreleme ve şifre çözme de izlenecek yollar gösterilmektedir. Gönderici ve alıcı arasındaki bir mesaj üçüncü bir kişi tarafından fark edilmekte fakat mesajın içeriği anlaşılmamaktadır.

3.2. Şifrelemenin Amacı

İletişim yolunu dinleyen eden kötü niyetli kişi ya da hacker elde ettiği mesajı üç amaçla müdahale edebilir. Verinin gitmesini engelleme(intercept), veriyi sadece okuma(read), veriyi değiştirme(modify). Bu tip müdahaleleri engellemek amacıyla şifreleme bir bilim olarak çalışmaktadır ve üç temel görevi üstlenmektedir.

3.2.1. Veri güvenliği

Gönderici ve alıcı arasında gönderilen verinin üçüncü kişiler tarafından okunmasını engellemedir. Göndericiden çıkan mesaj alıcıya giderken iletişim yolu üzerinde başka kişiler tarafından ele geçirilebilir. Mesajın içeriği diğer kişiler tarafından öğrenildiği için verinin güvenirliği olmaz. Şifreleme tekniği ile mesaj kimin eline geçerse geçsin anahtar olmadan anlamsız bir metin parçası olmaktan başka bir duruma geçemez. Şifreli metin, orijinal metin halinde olmadığı için veri güvenliği sağlanmış olur.

3.2.2. Veri bütünlüğü

Gönderici ve alıcı arasında gönderilen verinin üçüncü kişiler tarafından değiştirilmesini engellemedir. Veriler üçüncü kişiler tarafından sadece okunmakla kalmayabilir. Veri değiştirilebilir. Bu sebepten dolayı iletilmek istenen veri ilgili kişiye doğru bir şekilde (olması gerektiği gibi) gitmeyebilir. Şifreleme algoritmalarıyla bu veri bütünlüğünün bozulması durumu da engellenmiş olur. Alıcı mesajı aldığında istenilen sonuçların çıkmadığını fark eder ve mesaja dışarıdan müdahale edildiği anlaşılır.

3.2.3. Kimlik denetimi

Gönderici taraf veri paketinin üzerine kendi bilgilerini ekleyerek yollar. Alıcı tarafta aldığı verinin doğru kişiden gelip gelmediğine bakar. Doğru ise mesaja müdahale edilmediği, yanlışsa üçüncü kişilerin saldırıları olduğu anlaşılır.

3.3. Şifreleme Algoritmaları

İletişimdeki veri özelleştikçe ve transfer için kullanılan yollar kötü niyetli kişilerce dinlenmeye devam ettikçe veri güvenliği sorun olmuş ve bu sorunun çözümü için çeşitli teknikler geliştirilmiştir. Şifreleme de veri gizliliği için geliştirilmiş bir tekniktir.

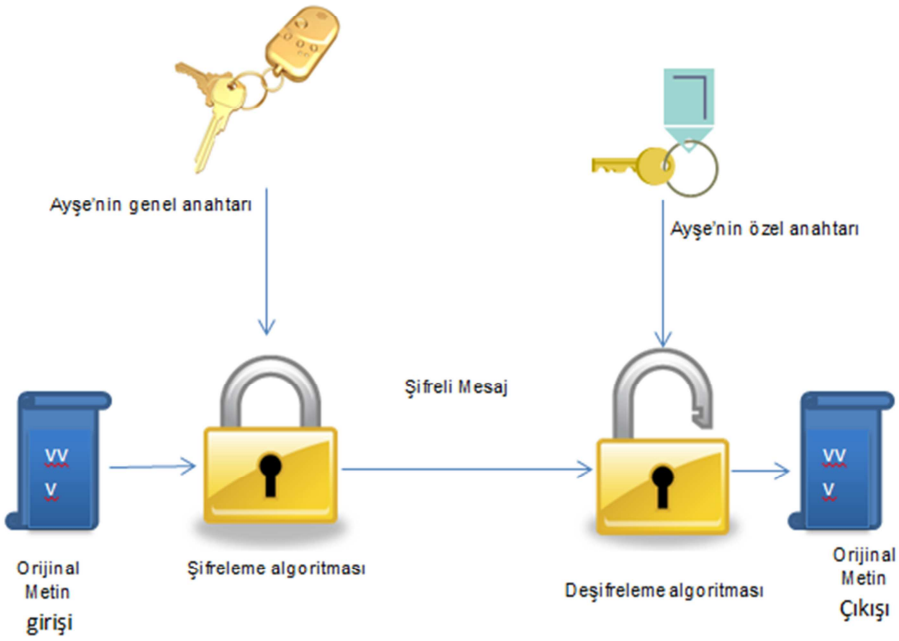
Şifreleme, iki ya da daha fazla nokta arasında, mesajın gönderildiği ortamdan bağımsız olarak güvenli bir şekilde iletilmesini sağlar. Bu iletimi sağlarken gönderilen veriyi sadece göndericinin ve alıcının bildiği bir anahtar yardımıyla üçüncü kişilerin anlayamayacağı bir şekle sokar. Alıcı taraf bu veriyi çözmek için yine anahtara ihtiyaç duymaktadır. Aksi halde verinin orijinal halinin elde edilmesi zor ya da imkânsızdır.

Gönderilecek mesajı şifreleme işi, bu iş için geliştirilen algoritmalar yardımıyla yapılır. Algoritmalar amaca uygun tasarlandıkları için çok çeşitlilik gösterir. Anahtar temelli algoritmaların iki çeşidi vardır. Bunlar; simetrik (gizli anahtar) ve asimetrik (açık anahtar)'tır.

Simetrik anahtarlı ve asimetrik anahtarlı şifrelemeyi birbirinden ayıran en temel özellik; simetrik anahtarlı şifrelemede verinin şifrelenmesi ve çözümü için aynı anahtar kullanılırken, asimetrik anahtarlı şifreleme de verinin şifrelenmesi ve çözümü için farklı anahtarlar kullanılır.

3.3.1. Açık anahtarlı şifreleme sistemleri(Asimetrik şifreleyiciler)

Açık anahtar şifreleme tekniğinde veriyi şifrelemek ve çözmek için ayrı ayrı anahtarlar kullanma mantığıyla tasarlanmıştır. Gönderilmek istenen veri genel bir anahtarla şifrelenir. Şifreli veriyi alan taraf kendinde bulunan özel anahtarla şifreyi çözer. Böylelikle dış müdahalelerde özel şifre bilinmediği için mesaj çözülemez.



Şekil 3.2. Asimetrik .Anahtarlı Şifreleme.

Şekil 3.2. ‘de Çınar, Ayşe’ye bir mesaj göndermek istiyor. Çınar, Ayşe’den daha önceden aldığı genel anahtar ile mesajı şifreleme algoritması yardımıyla şifrelemektedir. Şifreli mesajı iletim yoluna koyar ve Ayşe’ye yollar. Mesajı alan Ayşe kendinde bulunan ve kimsede olmayan özel anahtarı ile şifreli mesajı çözer. Böylece Ayşe Çınar’dan mesajı güvenli bir şekilde almış olur.

Örnekten de anlaşıldığı üzere kişilerin sahip oldukları genel anahtarlar herkeste bulunabilir. Bu anahtar sayesinde metin şifrelenir. Fakat özel şifre sadece alıcı tarafta bulunur ve başka kimse bu mesajı çözemez.

Asimetrik şifreleme sistemlerinde her kullanıcının sadece kendi anahtarını gizli tutması yeterlidir. Bunun aksine (n) tane kullanıcının bulunduğu bir simetrik şifreleme sisteminde gizli tutulması gereken anahtar sayısı her kullanıcı için (n-1) tanedir. Bu da sistem için büyük bir depolama yükü oluşturur.

Ayrıca simetrik sistemlerde anahtarların kesinlikle güvenli yollardan kullanıcılara ulaştırılması gerekmektedir. Örneğin değişik kıtalarda yaşayan kişilerin Internet gibi herkese açık (güvensiz) bir ortam üzerinden güvenli bir şekilde haberleşmesi ya da alışveriş yapması için gizli anahtarlarını değiş-tokuş etmeleri pratikte mümkün değildir. Açık sistemlerdeyse anahtar değiş-tokuşu güvensiz kanallar üzerinde belli önlemleri almak şartıyla güvenli bir şekilde yapılabilir.

Simetrik şifreleme sistemleriyle karşılaştırıldığında, asimetrik sistemler çok daha yavaştır. Bu, şifrelemede kullanılan anahtarların uzunluğu ve yapılan işlemlerin yavaşlığından kaynaklanmaktadır.

Asimetrik şifreleme yöntemiyle şifrelenmiş bir bilgiyi aynı anda değişik kullanıcılara gönderebilmek için aynı bilginin her alıcı için ayrı ayrı şifrelenmesi gerekmektedir. Bu da şifreleme için ayrı bir yük getirmektedir.

Bu amaçla asimetrik ve simetrik şifreleme sistemlerinin avantajlı yönlerini bir arada kullanan hibrid sistemler kullanılmaktadır. Hibrid sistemlerde şifreleme için simetrik anahtarlar kullanılırken, bu anahtarların iki taraf arasında taşınması için asimetrik yöntemler kullanılmaktadır.

Bir diğer sorun ise, asimetrik sistemlerin güvenliğinin henüz daha ispatlanmamış varsayımlara dayandırılmasıdır. Asimetrik sistemlerde güvenlik tek-yönlü-fonksiyonlara dayandırılmaktadır. Bu fonksiyonların kendisinin hesaplanması "kolay", tersinin hesaplanması "imkânsız" dır. İmkânsızdan kasıt, fonksiyonun tersinin hesaplanmasının polinomial süre içerisinde imkânsız olmasıdır. Ancak ters alma işlemini hızlandıracak yöntemlerin var olmadığı henüz ispatlanmış değildir.

3.3.1.1. RSA Şifreleme Sistemi

Diffie ve Hellman tasarlamış oldukları algoritma ile simetrik şifrelemede sorun olan anahtarın gizliliği ve dağıtımı önemli ölçüde çözülmüştür. 1977 yılında R.Rivest, A.Shamir ve L.Adleman isminde üç bilim adamı tarafından tasarlanmış olan RSA asimetrik anahtarlı şifreleme algoritması, anahtar dağıtımının yanı sıra mesajı şifreleme ve deşifreleme işlemlerini de gerçekleştirmektedir. RSA'nın tasarlanmasıyla asimetrik anahtar şifreleme yönteminin kullanımı artmıştır.

RSA şifreleme sistemi, hem gizlilik hem de sayısal imza sağlamak amacıyla kullanılabilir. Bu sistemin güvenliği tamsayılarda çarpanlara ayırma probleminin kolaylıkla olmaması temeline dayanır. RSA kripto sisteminde kişilere şifreli mesaj gönderilebilmesi için o kişilerin açık anahtarlarına ihtiyacı vardır. Mesajı alan kişinin de mesajı okuyabilmesi için gizli bir anahtarın olması gerekir. [2]

RSA şifreleme algoritmasına göre anahtar üretmeyi ve şifrelemeyi daha iyi anlamak için ;

A ve B olmak üzere iki asal sayı seçilir.

A = 3; B = 11

Hem özel anahtarı hem de genel anahtarın üretiminde kullanılacak olan bir C sayısı türetilir. Bu sayı A ve B'nin birbiriyle çarpımı kadardır.

C = A*B; C=3*11 C=33

Daha önce üretilen A ve B sayılarının 1 eksiğinin birbiriyle çarpımlarından yeni bir sayı türetilir.

a = (A-1)*(B-1) a=(3-1)*(11-1)=20

a sayısıyla ortak böleni olmayan bir "b" sayısı türetilir.

b = 7

Bu elde edilen “b” ve “C” sayıları genel anahtar olarak kullanılacaktır.

Özel anahtar üretmek için ise bir “d” sayısı belirlenir. “d” sayısı, “b” sayısı ile çarpıldıktan sonra “a” sayısı ile modüler aritmetik işleminden sonra kalan 1 olan bir sayı olmalıdır.

d*b mod (a) = 1 olmalıdır. d*7 mod(20)=1 ise d=3 olabilir.

Bu elde edilen “d” sayısı ile “C” sayısı ise özel anahtar için kullanılır. Böylelikle genel ve özel anahtarlar türetilmiş olur.

Örneğin; “A” harfi şifrelensin ve A harfine karşılık gelen değer 15 olsun,

Şifrelemek için;

$X=15^{b} \bmod C$

$X=15^{7} \bmod 33$

$X=35831808 \bmod 33$

X=27 şifreli sayı.

Şifre çözümü için;

$X_1=27^{d} \bmod C$

$X_1=27^{3} \bmod 33$

$X_1=19683 \bmod 33$

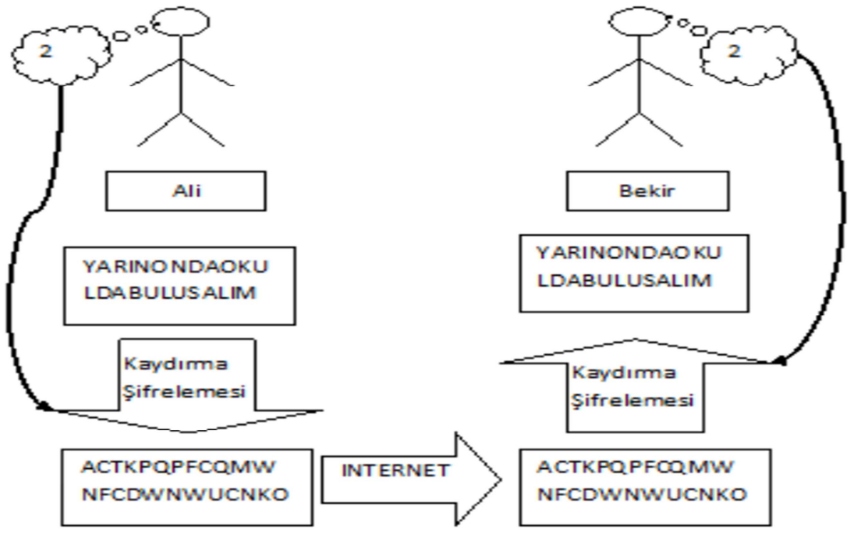
$X_1=15$ orijinal sayı.

3.3.2. Gizli anahtarlı şifreleme sistemleri(Simetrik şifreleyiciler)

Gizli anahtarlı şifreleme sistemlerinde, şifreleme ve şifre çözmede sadece bir tane anahtar kullanılır. Gönderici ve alıcı tarafların her ikisi de daha önceden bildikleri anahtar yardımıyla güvenli haberleşmeyi sağlarlar.

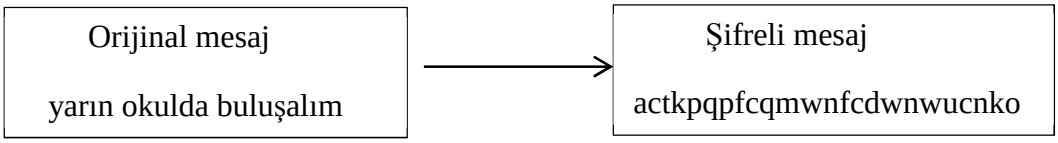
3.3.2.1. Kaydırma şifrelemesi(Shiftchipher)

Algoritma simetrik anahtar şifreleme tekniğine göre tasarlanmıştır. Birbirine mesaj göndermek isteyen her iki tarafta daha önceden belirledikleri şifre ile mesajı şifrelerler veya deşifrelerler.



Şekil 3.3. Simetrik Anahtarlı Şifreleme.

Kaydırma yöntemine göre mesaj, anahtara göre alfabedeki sıraya uygun kaydırma yapılır. Örneğin birbirine mesaj göndermek isteyen iki kişi Ali ile Bekir anahtar olarak iki(2) sayısını belirlediler. Ali “yarın okulda buluşalım” mesajının her bir harfini alfabedeki sıraya göre iki kaydırarak şifreler.



“actkpqpfcqmwnfcdwnwucnko” şeklini alan mesaj iletişim yoluna yani Internete koyulur ve Bekir’e gönderilir. Mesajı alan Bekir şifrenin iki olduğunu bildiği için şifre çözme algoritmasını kullanarak şifreyi çözer ve böylece iletişim güvenli bir şekilde sonlanmış olur.

3.3.2.2. One Time Pad(OTP)

1917 yılında Josep Mauborgne ve Gilbert Vernam birlikte geliştirdikleri şifreleme sistemi olan “on time pad”’i buldular. Bu şifreleme tekniği oldukça basit tasarlanmıştır. Öncelikle şifrelenecek metin girilir ve metin uzunluğu hesaplanır. Hesaplamanın sonucuna göre metinle aynı uzunlukta bir anahtar seçilir. Fakat anahtarın bir bölümü asla tekrarlanmaz. Aksi halde şifre kolaylıkla çözülebilir. Daha sonra şifrelenecek metin ile anahtar XOR işlemine tabi tutulur. İşlemin sonucunda şifreli metin elde edilmiş olur.

ÖRNEK:
Gönderilecek mesaj=”sonunda bitiyor” olsun.

Bu ifadenin ASCII kodundaki sayısal karşılığı:

115 111 110 117 110 100 97 32

98 105 116 105 121 111 114

şeklindedir.

Anahtar =” B4K89IPELDRT67* “ olarak belirlenmiş olsun.

Anahtarın ASCII kodu karşılığı:

66 52 75 56 57 73 80 69

76 68 82 84 54 55 42

şeklindedir.

Anahtar ile metin son alarak özelveya(XOR) işlemine tabi tutulur. Aşağıdaki şifreli metin elde edilir.

Şifreli metinin ASCII kod karşılığı:

49	91	37	77	87	45	49	101
46	45	38	63	77	88	88	

Şifreli metinin karakter karşılığı:

1[%MW-1e.-&?MXX şeklini alır.

Şeklini alır. Alıcı nokta şifreli mesajı aldıktan sonra anahtar yardımıyla mesajı tekrar orijinal haline çevirir. Şimdi şifreli metnin iletişim yolunda üçüncü şahıslar tarafından elde geçirildiğini düşünelim. Kişi ya da kişiler metnin uzunluğunda bir anahtar düşüneceklerdir. ASCII kodlarında 256 farklı karakter bulunmaktadır. Her bir karakteri deneyerek şifreyi elde etmeye çalışacaklardır. Metin boyu 15^{256}'den 1,2005004253118409429987471605189e+301 olası anahtar var demektir. Bu olasılıkların hepsi denenmiş olsa bile neticede çok sayıda anlamlı kelime grupları çıkacağı için arasından hangisinin doğru metin olduğunu bulmak oldukça zor ve tahmin edilmesi güçtür. Bu da sistemin üstünlüklerindendir.

Sistemin dezavantajı ise, çok uzun metinler olsa bile metin boyu kadar uzunlukta anahtar üretmek gereklidir. Ayrıca bu uzunluktaki bir anahtarı alıcı tarafa güvenli bir şekilde göndermekte sorun teşkil etmektedir. Bu durumda uzun metinlerin gönderilmesi ve anahtarın seçimi oldukça güçtür.

3.4. Veri Gizleme ve Gömme Teknikleri

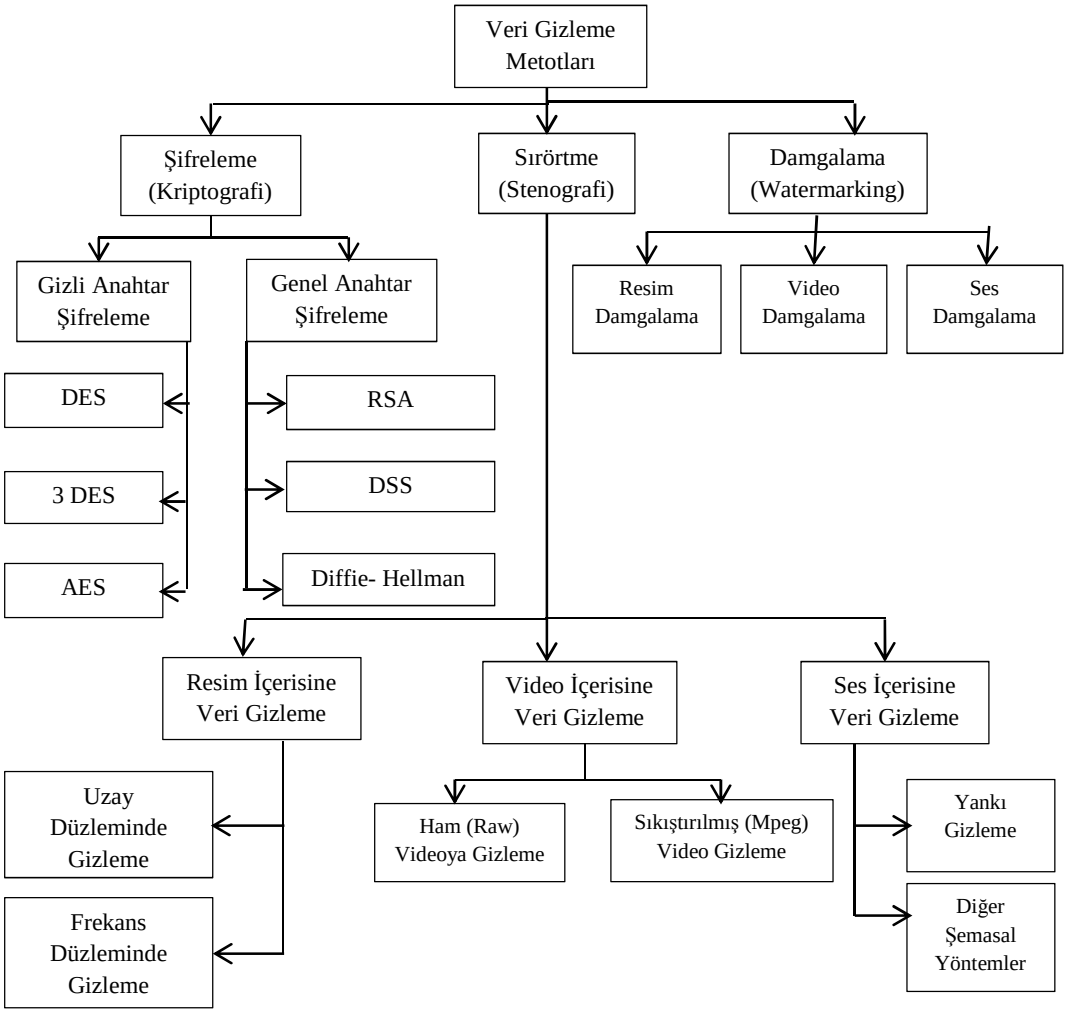
Teknolojik gelişmelerden en fazla yararlanan alanlardan biri de şüphesiz haberleşme alanıdır. Hemen hemen her insanın kullandığı Internet, geliştirilen en iyi iletişim aracıdır. İnternet sayesinden dünyanın bir ucundan diğer ucuna sadece saniyeler içerisinde video, resim, metin vb. olgular paylaşılabilir.

İnternet geliştikçe dosya aktarımı, paylaşımı, saklanması, kaydedilmesi gibi eylemlerin rahatlıkla yapılabilmesi daha da kolaylaşmıştır. Teknoloji ilerledikçe sadece metin, resim, video değil özel tasarımlar, özel veriler, devlet sırları gibi çok özel bilgiler de paylaşılabilmektedir. Haberleşmede kullanılan verilerin gizliliği arttıkça üçüncü kişilerin saldırıları da artmıştır. Bu yüzden güvenlik ihtiyacı daha da artmıştır. Güvenlik gereksinimlerini giderebilmek için çeşitli yöntemler geliştirilmiştir.

Yetkisiz kişilerin izni olmadan bir haberleşmeye dahil olmamasını sağlamak için eski tarihlerden buyana çalışmalar sürmektedir. Amaç, gizli verinin üçüncü kişilerin anlayamayacağı şekle büründürmekse bununla uğraşan bilim dalına şifreleme denir. Şifreleme, gizli mesajın sadece alıcı tarafın anlayabileceği özel bir forma sokar. Metin gönderici tarafından bir anahtar vasıtasıyla şifrelenir ve İnternet gibi bir iletişim ortamı aracılığıyla alıcı tarafa gönderir. Mesajı alan taraf, şifre çözme algoritmasını çalıştırarak orijinal mesajı elde eder.

Gizlenecek olan bir metin değil de resim veya video ise o zaman metin için kullanılan şifreleme yöntemlerini kullanmamız tasarlanan algoritma açısından biraz daha zor olacaktır. Boyutu küçük resim veya videolarda kullanılabilirken, boyut arttıkça şifreleme yöntemleri yetersiz kalmaktadır. Bu tür uygulamalar içinse sırörtme (steganography) yöntemleri geliştirilmiştir. Sırörtme tekniklerine göre gizlenecek metin resim içerisine saklanır. Bu yöntem insan göz sisteminin bazı renk değişimlerini algılayamamasından faydalanır.

Şifreleme ve sırörtme arasındaki en temel fark:: şifrelemede yetkisiz kişiler bir gizli haberleşmeden haberdardır, ancak mesajın anlamını elde etmek zordur. Sırörtmede ise üçüncü kişiler gizli haberleşmeden haberdar değildir. Masum görünümlü resim ya da videolar üzerinden gizli haberleşmenin yapıldığı anlaşılamaz. Şifreleme ve sırörtmenin ortak amacı ise gizli verinin üçüncü kişilerin eline geçmeden ilgili alıcıya gönderebilmektir.



Şekil 3.4. Veri gizleme metotları şeması.

Şekil 3.4'deki veri gizleme metotları şemasına göre veri gizleme tekniklerini üç ana başlığa ayrılmaktadır;

a) Şifreleme (Kriptografi)
b) Sırörtme (Stenografi)
c) Damgalama (Watermarking)

Şifreleme, veri gizleme tekniğinde, gizlenecek veri yetkisiz kişilerin eline ulaştığında onların anlayamayacağı forma sokmaktır. Üçüncü şahıslar gizli bir haberleşmenin olduğundan haberdardır.

Sırörtme tekniğinde resim, video gibi dosyaların içerisine gizlenecek veriyi gömerek güvenli haberleşmeyi sağlar. Yetkisiz kişiler gizli bir haberleşmenin olduğundan habersizdir. Bu yüzden haberleşme oldukça güvenlidir.

Damgalama metotlarında ise daha çok telif hakkı gibi önemli bilgilerin korunması olduğundan yetkisiz kişiler tarafından gizli veriyi ele geçirme veya yok etme kaçınılmazdır. Bu gibi durumları engellemek için ise damgalama tekniği kullanılır.

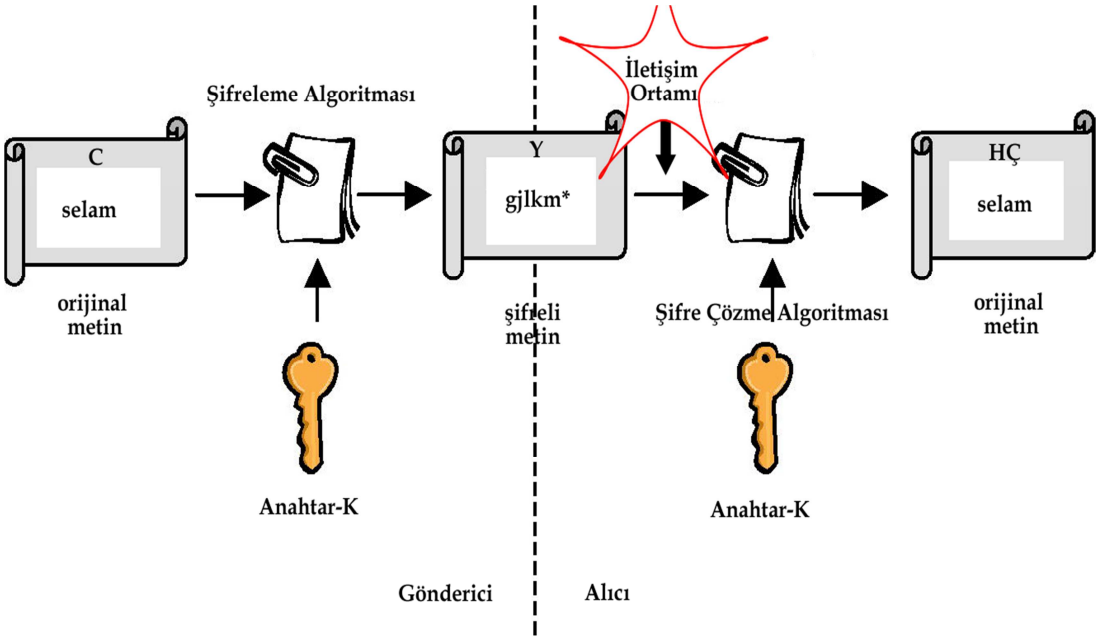
3.4.1. Şifeleme kavramı ve terminolojisi

Şifreleme terimi çoğu zaman kriptoloji bilim dalı ile aynı anlamda kullanılmaktadır. Şifreleme; veri gizleme üzerine çalışan bir matematik bilim dalıdır. Amacı haberleşmede güvenliği sağlamaktır. Bunu yaparken de gönderilecek olan veriyi matematiksel yöntemlerle anlaşılmaz ifadelere dönüştürür.

Şifreleme, gönderilecek olan verinin orijinalliğine bozmadan üçüncü kişiler tarafından elde edilmesi zor bir şekle dönüştürür. Diğer bir değişle şifreleme bilginin, anlaşılması zor, anlamsız bir yapıya dönüştürülmesi ve tekrar orijinal metnin elde edilmesiyle ilgilenir. Etkisiz kişiler iletişime ne kadar müdahale ederlerse etsinler anahtar olmadan orijinal veriyi geri elde edemezler.

Genel olarak veri gizleme ve gizli veriyi tekrar elde etme yöntemi Şekil 3.5’ gösterildiği gibidir. Yetkisiz kişilerce yapılabilecek olan olası saldırılara karşı şifrelenmek istenen orijinal metin, şifreleme algoritması ve sadece göndericinin

bildiği (alıcıda biliyor olabilir) anahtar ile şifrelenir. Şifreleme algoritması sonucunda oluşan şifreli metin bir iletişim yoluna (Internet) koyulur. Yol boyunca yetkisiz kişilerce de elde edilebilecek olan şifreli metin sadece alıcıya ulaştığı zaman anlamlı hale gelebilir. Alıcı şifreli metni iletişim yolundan alır, şifre çözme algoritması ve anahtar vasıtasıyla orijinal metin elde edilir.



Şekil 3.5. Veri gizleme ve çözme diyagramı.

3.4.1.1. Kriptografinin tarihçesi

Kriptografinin Türkçe adı saklı yazıdır. Kriptografi yunanca gizli anlamına gelen “kriptos” ve yazı anlamına gelen “graphi” dan türetilmiştir. Kriptoloji ise şifre bilimidir. Kriptografi bilgi güvenliği ile uğraşır, Kriptoanaliz güvenli bilginin kırılması başka bir deyişle kriptografinin tam karşıtıdır. Kriptoanalistler genelde şifre çözmeye dayalı çalışırlar.

İlk kriptolog, 4000 yıl önce yaşamış Mısırlı bir kâtiptir. Efendisinin hayatını anlatırken hiyeroglifleri şifrelenmiş bir şekilde oluşturmuştu ve bazı hiyeroglifler daha önce hiç kullanılmamıştı.

Kriptografi, bu şekilde başlamasına karşın, hayatının ilk 3000 yılında neredeyse hiç gelişemedi. Dünyanın farklı farklı yerlerinde bağlantısız bir şekilde en temel biçimde kullanılmıştı ancak medeniyetlerin yıkılışıyla sonraki adımlara geçilememişti.
Dönemin en önde uygarlığı olan Çin'de ise yazının şifresiz yazılmasının bile çok zor olması nedeniyle kriptografi hiç gelişemedi.
Daha sonraları (M.Ö 5. - 6. yüzyıl) askeri istihbaratta gizliliğin gerekmesi nedeniyle, kriptografi askeri alana girdi. Askeri alandaki ilk kriptograflar Spartalılardır.

Şifrelemeye verilebilecek ilk örnek, eski Yunanlılara ait “scytale” isimli bir çubuktur. Sarmal şifrelemesi, simetrik bir şifreleme yöntemidir. Şifrelenecek bir metin ince uzun bir kağıda harf harf yazılır. Burada anahtar gizli metinin sarılacağı çubuğun çapıdır. Farklı çaplardaki çubuklarla şifreyi çözmek imkansızdır. Çubuğun çapı ise sadece gönderen ve alıcı tarafından bilinmektedir.

Şekil 3.6. Yunanlıların veri gizlemede kullandığı ”scytale” isimli çubuk.

1917’de Edward Hugh Hebern tarafından Rotor machine adı verilen bir şifreleme aracı geliştirilmiştir. 1971’de de IBM tarafından Lucifer adı verilen şifreleme şeması oluşturulmuştur. 1975’te DES, 1976’da da Diffieand Hellman şifreleme teknikleri geliştirilmiştir. 1976-1978 yıllarında ise PublicKeyCryptography- Genel Anahtar Kriptografi- keşfedilmiştir.

Kriptografi’de kullanılan şifreleme algoritmaları aşağıdaki gibi sıralanabilir;

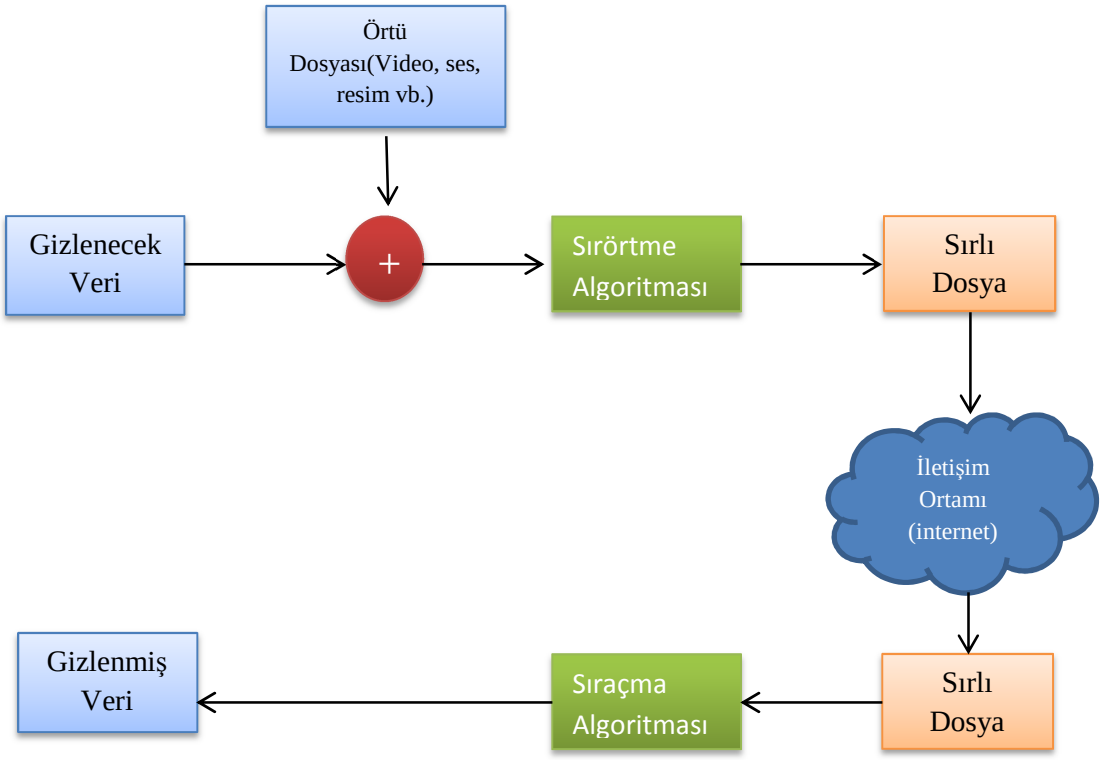
a) Simetrik Anahtar Şifreleme
b) Genel Anahtar Şifreleme
c) Tek- Yol Fonksiyonu

Uygulama alnında en çok kullanılan simetrik ve genel anahtar şifreleme algoritmalarıdır.

3.4.2. Sırörtme

Hızla gelişen Internet ve diğer sayısal iletişim yolları sayısal dosyaları orijinalliğini bozmadan saklayabilmekte veya çok uzak mesafelere bile saniyeler içinde gönderebilmektedir. Bu muazzam iletişim ağları kullanıcı sayılarının ve verilerin gizliliğinin artmasıyla güvenlik sorunları ortaya çıkmıştır. İletişimde sadece masum metinler, resimler, videolar veya ses dosyaları gönderilmemekte, aynı zamanda bir devletin gizli sırları, bir şirketin özel verileri veya herhangi bir saldırı planı bu masum görünüşlü dosyaların içinde gizlenmiş halde bulunuyor olabilmekte. Tüm bu gereksinimler neticesinde güvenli haberleşmek için çeşitli çalışmalar gerçekleştirilmiştir.

Özellikle son dönemlerde yaşanan terör saldırılarından sonra sırörtme tekniğinin önemi ve kullanımı artmıştır. Amerika Birleşik Devletleri'nde yaşanan 11 Eylül saldırıları buna büyük bir örnek teşkil etmektedir. Yaşanan bu felaket için hazırlıklar Internet üzerinden gerçekleştirildiği düşünülmektedir. Teröristler bazı ünlü web sitelerde eylem detaylarını anlatan bilgileri resimlere gizleyerek yayınlamışlardır. Aslında masum görünüşlü bu resimlerde büyük bir yıkımın detayları gizlenmişti. Bu vahim olayın ardından sırörtme ve veri gizleme teknikleri büyük önem kazanmış ve bu yönde gelişmeleri sağlayacak çalışmalar hızlanmıştır.



Şekil 3.7. Genel olarak veri gizleme blok diyagramı.

Şekil 3.7.'de genel olarak bir veri gömme ve gömülü veriyi geri elde etme tekniği anlatılmaktadır. Öncelikle gizlenecek dosya belirlendikten sonra gömülecek veriyi tümüyle saklayabilecek bir örtü dosyası seçilecektir(video, ses, resim vb.). Daha önce belirlenen bir gömme algoritmasıyla veri, örtü dosyasının içerisine gömülecektir. İletişimi sağlayacak olan ağa(internet) sırlı dosya yerleştirilir ve alıcı tarafa gönderilir. Alıcı nokta sırlı dosyayı aldıktan sonra gömme algoritmasına ters mantıkla çalışan çıkarma algoritmasını çalıştıracaktır. Bu işlem sonucunda orijinal veri geri elde edilmiş olacaktır.

3.4.2.1.Sırörtme kavramı ve terminolojisi

Sırörtme, Yunanca örtmek anlamına gelen “stegos” ve yazı anlamına gelen “graphia” kelimelerinden türetilmiştir. Anlamı gizlenmiş yazı olarak Türkçe ’ye çevrilmiştir. Haberleşmede, gizleme bilimi ve sanatıdır[3].

Gönderilecek olan veriyi anlaşılması zor bir biçime dönüştürmekle uğraşan bilime kriptografi denir. Kriptografinin en büyük dezavantajı, yetkisiz kişiler ortamda bir gizli haberleşme olduğunu anlayabilmesidir. Orijinal metni elde edemeseler de veriyi yok etme, silme ya da veriyi bozma gibi çeşitli saldırılarda bulunabilirler. Bu tür saldırılara maruz kalmamak ve üçüncü kişileri gizli haberleşmeden haberdar etmemek için sırörtme (steganography) tekniği geliştirilmiştir. Bu yöntem, veriyi bir taşıyıcı dosya içine gömer. Taşıyıcı içerisine gömülen mesaj dışardan anlaşılamaz ve böylelikle kimse gizli haberleşmeden haberdar olmaz. Sırörtme yönteminin amacı, sadece veriyi çeşitli dış müdahalelerden korumak değil, müdahalelerin yapılmasını engellemektir. Yani yetkisiz kişilerin gizli haberleşme yapıldığından bile haberi olmamasını sağlamaktır. Bu teknik, saldırı yaşanıp bittikten sonra değil, saldırı olmadan önlemini alır. Bu amaçla çeşitli sırörtme tekniği geliştirilmiştir.

a) En önemsiz bite ekleme (LeastSignificant-LSB),
b) Maskeleme ve filtreleme,
c) Algoritmalar ve dönüşümler [4].

Sırörtme uygulamalarında ilk olarak kullanılan yöntem en düşük değerlikli bite (LSB) gömme yöntemidir [5],[6]. Uygulamada çok basit bir yöntem olmasına karşın dikkatsizce kullanıldığında veri kayıplarına sebep olur. Bu yöntemde, gizlenecek verinin her biti, resim verisinin bir baytının son bitine yazılır. Gizli verinin elde edilebilmesi için ikilik sayı düzeninde bulunması ve bu düzenin korunması gerekir. LSB tekniğine kayıplı sıkıştırma algoritmalarından da eklenerek gizli verinin kaybolmasına neden olabilir. Ayrıca bu yöntem, uzay boyutunda gömme tekniklerini kullanır.

Maskeleme ve filtreleme, insan göz sisteminin sınırlarını kullanarak veri gömme yapan bir tekniktir. Yani normal bakmayla anlaşılamayan bölgeleri bulur ve bu bölgelere gizleme işlemini gerçekleştirir. Maskeleme ve filtreleme görünür damgalama uygulamalarında kullanılan bir tekniktir. Uygulama alanı gri tonlamalı resimler ve 24 bit BMP formatı ile sınırlıdır. Resimde görülebilir işaretleme yapmak için kullanılır. Kayıplı sıkıştırmalara karşı LSB'ye oranla daha kullanışlı ve daha az veri kaybı meydana getirir.

Tüm bu sırörtme teknikleriyle veri gömülecek olan resmin ya da videonun tüm pikselleri içerisine veri gömülme işlemi gerçekleştirilemez. Veri gömme işleminin tam anlamıyla yapılabilmesi için veri gömmeye uygun piksellerin seçilmesi gerekir. Uygun pikselleri bulmak için ise geliştirilmiş olan algoritmalar vardır.

Sırörtme ile ilgili bazı önemli terimler aşağıda verilmiştir.

Örtü Dosyası (Cover - Image): İçerisine gizli verinin gömüleceği dosyadır. Bu dosya resim, video ya da ses olabilir.

Gömü Dosyası (Stego - Image): Gizli verinin gömülü olduğu dosyadır (ses, video, resim vb.).

Örtü Anahtarı (stego- key): Gizleme işlemi sırasında kullanılan güvenlik anahtarıdır.

Steganalysis: Gizli verinin bulunmasıyla uğraşan bilim dalıdır.

Tüm bu terminoloji birinci uluslar arası bilgi gizleme seminerinde kabul edilmiştir.

$$\text{Örtü dosyası} + \text{Gizli veri} + \text{Gizli anahtar} = \text{Gömü dosyası} \qquad (3.1)$$

3.4.2.2. Sırörtmenin tarihçesi

Eski Yunan'da, insanlar mesajları tahtaya yazıp üzerini mumla kaplarlardı. Böylece cisim kullanılmamış bir tablete benzerdi öte yandan mumun eritilmesiyle birlikte içindeki gizli mesaj okunabilirdi.

Herodotos'un bir hikâyesine göre Pers saldırısının öncesinde saçları traşlanan bir kölenin kafasına yazılan uyarı mesajı, saçlarının uzaması sayesinde saklanmıştır. Bu sayede, mesaj dikkat çekmeden gerekli yere ulaşabilmiş, ulaştığında da kölenin saçları tekrar kesilerek uyarı okunabilmiştir.

Kızıl Derelilerin dumanlı mesajları da bir çeşit sırörtme tekniği olarak kullanımıştır.

İkinci Dünya Savaşı sırasında, New York'taki bir Japon ajanı (Velvalee Dickinson) oyuncak bebek pazarlamacısı kılığı altında saklanmaktaydı. Bu ajan, Amerikan ordusunun hareketlerini bebek siparişi içeren mektuplar içine saklayarak Güney Amerika'daki adreslere gönderiyordu.

Özellikle 1960′larda mor ötesi boya ile yazı yazabilen sprey ve kalemler moda idi. Bu kalemlerin yazdığı yazılar, sadece bir mor ötesi ışıkla görülebiliyordu. RonHoward'ın Akıl Oyunları (A BeautifulMind) filminde, John Nash gazete ve dergilerde gizli mesajlar aramaktadır. Günümüzde ise sırörtme tekniği herkes tarafından ve her alan tarafından kullanılabilir hale gelmiştir.

3.4.2.3. Resim dosyaları için sırörtme teknikleri

Bir resim dosyası içerisine görme sisteminin anlayamayacağı, bozulmalara neden olmadan önemli bir veriyi, renk değerlerinde küçük değişikliklerle gömmek mümkündür. Bir resim dosyası içerisine LSB, maskeleme, algoritma ve dönüşüm teknikleriyle veri gömme yapılabilir.

Resim içerisine veri gömme tekniklerini iki ana kategoride inceleyebiliriz. Bunlardan biri “uzay düzleminde”, diğeri ise “frekans düzleminde” veri gizlemedir.

3.4.2.3.1. Uzay düzleminde sırörtme

Uzay düzleminde veri gizlemede kullanılan en yaygın teknik LSB ’ye (En Düşük Değerlikli Bit) veri gömme tekniğidir. Bu tekniğin yaygın bir şekilde kullanılmasının sebebi kolay uygulanabilir olmasıdır.

Bu yöntemde, gömü yapılacak resim dosyası ve gömülecek veri ikilik sayı sistemine çevrilmelidir. Ardından gömülecek verinin her bir biti resim dosyasının her bir pikselinin en düşük değerlikli bitinin yerine koyulur. Bu teknik yüksek kaliteli resimlerde kullanıldığında yüksek performans sağlar. Yani yüksek kalitedeki resimlerde bilginin şifrelenmesi veya maskelenmesi daha kolaydır. 24 bit BMP uzantılı resimlerde en ideal şekilde veri gizleme yapılabilir.

Küçük boyutlu resimlerin içine veri gömme tercih edilir. Aksi halde internetten yayınlarken sıkıştırma yapmak gerekebilir. Böyle durumlarda veri kaybı yaşanması engellenemez. Ayrıca çok büyük boyuta sahip resimler internette daha çok dikkat çeker ve gizli haberleşme olduğu konusunda şüpheleri üzerine toplar.

3.4.2.3.2. Frekans düzleminde sırörtme

Ayrık kosinüs dönüşümü (DCT) ve ayrık dalgacık dönüşümü (DWT) gibi dönüşümlerin kullanıldığı bir yöntemdir. Bu yöntemler kullanım bakımından oldukça zor fakat kaybı en az olan yöntemlerden biridir. Gömü yapılacak dosya (resim, video, ses vb.) ayrık kosinüs veya ayrık dalgacık dönüşümleriyle bölgelere ayrılır. Her bir bölgenin, bölgelere ayrılma işleminden sonra katsayıları olur. Oluşan bu katsayılarda değişiklikler yapılarak veri gömme işlemi gerçekleştirilir. Bu katsayıların bazıları sıfır bazıları da sıfırdan farklı değerlerdir. Bu katsayıların sıfır olması piksellerin insan görme sistemi tarafından algılanamayacağını belirtir. Bu pikseller kayıplı sıkıştırma ile sıkıştırıldığında silinebilen piksellerdir. Yani varlıkları da yoklukları da insan görme sistemi tarafından algılanamazlar. Bu durumdan faydalanmak için katsayıları sıfır olan piksellerin matematiksel işlemlerle değerleri değiştirilir ve veriler gömülür. Böylece kayıplı ya da kayıpsız sıkıştırma yapılsa bile artık veri gömülen pikseller silinmez. Bu da bu tekniğin avantajlarındandır.

3.4.2.4. Video dosyaları için sırörtme teknikleri

Bir resim dosyasına sınırlı kapasitede veri gömme yapılabilir. Bu resimlerin Internet vb. gibi bir iletişim yolu kullanıldığı düşünüldüğünde ise çok büyük boyutlarda olmaması gereklidir. Örneğin 450 x 500 boyutundaki bir resmi 225000 piksele sahiptir. Sahip olduğu her piksele veri gömme yapılamadığından örneğin 18850 pikseline veri gömülebilir olsun. O zaman kullanılacak veri gömme tekniğine göre maksimum 18850 piksellik veri gömülümü gerçekleşebilir. Bu sınırları aşma çalışmaları ve çabaları mevcuttur.

Video, kendisini oluşturan birçok resmin bir biri sıra sürekli akmasıyla oluşur. Yani video da resim dosyalarından oluşur. Örneğin saniyede 35 (35 fps)hareketsiz resim geçebilen 15 saniyelik bir video içerisinde 525 adet hareketli resim var demektir. Böylelikle bir hareketsiz resmin içine gömülebilecek verinin 525 katı daha

büyüklüğünde veri gömülmesi yapılabilir. Böylece veri gömmenin sınırlarını önemli ölçüde genişletilmiş olunur.

Video, hareketsiz resimlerden ve sesten oluştuğuna göre resim ve ses dosyalarına veri gömmede kullanılan tüm yöntem ve teknikler video için de kullanılabilir. Genellikle ayrık kosinüs dönüşümü (DCT) ile ayrık dalgacık dönüşümü(DWT) yöntemleri kullanılır.

Video üzerine veri gömmede yapılan ilk çalışmalar ham video (raw- video) üzerinde olmuştur. Ham video içerisine gömülecek olan veri, videonun her bir çerçevesine gömülebilir. Bunun için ise hareketsiz resme veri gömmede kullanılan yöntemler kullanılabilir.

İlerleyen zamanlarda Internetin kullanılması ve video kapasitelerinin yüksek olması fakat veri yolu bant genişliğinin yeterli derecede büyük olmaması gibi sebeplerden dolayı videoları sıkıştırma işlemine başvurulmuştur. Bu sebeple de çalışmalar sıkıştırılmış videolar üzerinde devam etmiştir. Videoları sıkıştırmak için birçok yöntem vardır (Mpeg, Mpeg4 vb.). Bu sıkıştırma yöntemlerinden hangisi kullanılıyorsa o yönteme en uygun teknikle veri gömme işlemi gerçekleştirilir.

3.4.2.5. Ses dosyaları için sırörtme teknikleri

Resim, video gibi Internetten rahatlıkla gönderilebilen, yayılabilen ses dosyalarına da veri gömme işlemi rahatlıkla gerçekleştirilebilir. Ses dosyaları içinde birçok veri gömme tekniği geliştirilmiştir. Bunlardan bazıları;

a) Düşük Bit Kodlama,
b) Yankı Gizleme,
c) Yayılı İzge,
d) Diğer Yöntemler.

Düşük bit kodlama, resim dosyalarında ve videolarda da kullanılan LSB metodunun kullanıldığı bir yöntemdir. Ses dosyalarının en düşük değerlikli bitine veri gömülür. Fakat bu yöntemin getirdiği bazı sıkıntılar bulunmaktadır. İnsan görme sistemi resim üzerindeki LSB değişikliklerini zor algıladığı halde kulak bu değişiklikleri daha kolay algılayabilir. Ayrıca iletişim sırasında oluşabilecek gürültüler de gömülü verinin bozulmasına sebep olabilir.

Yankı gizleme metodunda, insan kulağı ses içerisinde oluşan kısa süreli(milisaniyeler) yankıları algılayamamaktadır. Bu özellikten faydalanarak veri gömme işlemi yapılır. Veri gömmek için, bir ses dosyasına önce insan kulak sisteminin algılayamayacağı gecikme ve bağıl genlik değerlerine uygun olarak yankı eklenir. Daha sonra eklenen bu yankı üzerine gizlenecek veri ‘0’ ve ‘1’ olarak eklenir. İşitme sisteminin algılamayacağı yankı için gecikme yaklaşık 0.5ms ile 2 ms arasında ve bağıl genlik ise 0.8 olarak seçilir[7].

Yayılı izge metodunda ses dosyalarının içerisine rastgele gürültü eklenir. İletişim ortamında oluşabilecek saldırılara karşı dayanıklı olmakla birlikte insan kulağının duyabileceği büyüklükte gürültüler ekler.

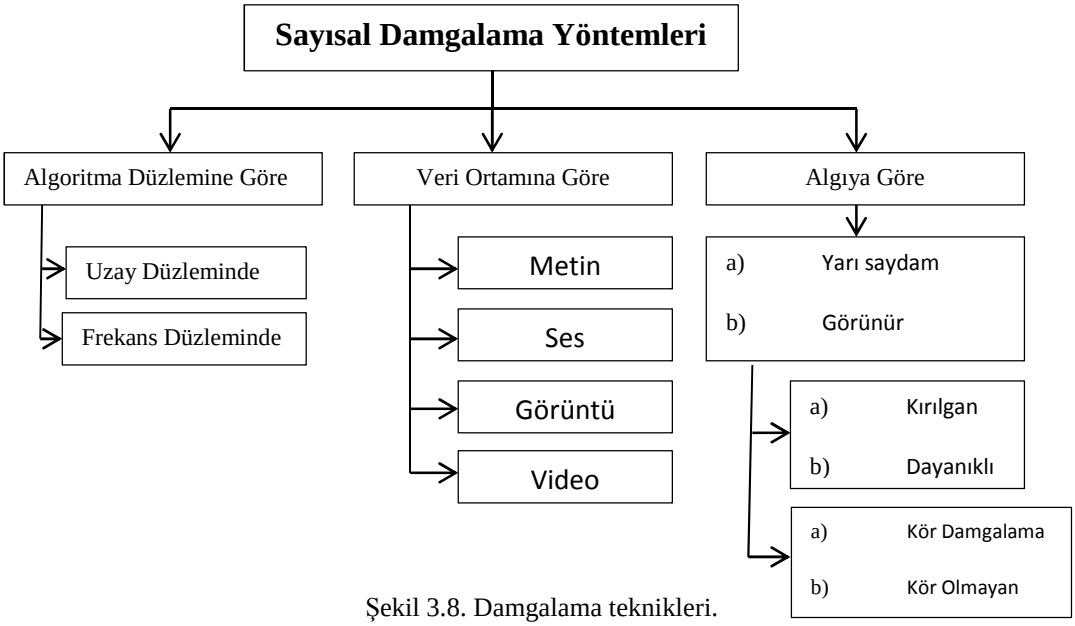
Diğer ses dosyasına veri gömme tekniği olarak, insan işitme sisteminin ses sınırlarından faydalanılır. Bu işitme sınırlarının dışına veri gömme işlemi gerçekleştirilir. Bu yöntem insan görme sisteminin göremediği ışık dalgaları aralığına veri gömme ile aynı mantıkta çalışmaktadır.

3.4.3. Sayısal Damgalama

Sayısal damgalama tekniği diğer veri gömme tekniklerinden bazı konularda farklılık göstermektedir. Burada amaç sadece gizli haberleşme ya da mesajı gizleme değildir. Hızlı gelişen teknolojinin yararlarının yanında zararlarıyla da var olmaktadırlar. Özellikle filmlerin, CD ya da DVD ‘lerin, kasetlerin vb. kopyalarını oluşturulması gelişen teknolojinin dezavantajlarındandır. Bu tür kopyalama, sahtecilik veya telif

hakkı gibi konuların çözüme kavuşturulabilmesi için sayısal damgalama tekniği geliştirilmiştir.

Sayısal damgalama, bir televizyon programının, bir filmin, bir paranın vb. kişiye veya devlete özel evrakların kopyalanıp çoğaltılmasını ve saldırıları önlemek amacıyla geliştirilmiştir. Sayısal damgalama teknikleri Şekil 3.8'de gösterilmiştir.



Şekil 3.8. Damgalama teknikleri.

Görünür Damgalama, İnsan görme sisteminin görebildiği, farkına varabildiği damgalama türüdür. Televizyon kanallarındaki logo, bazı kitap kapaklarının filigranları gibi gözün algılayabileceği damgalamalardır.

Görünmez damgalama, insan görme sisteminin göremediği, farkına varamadığı damgalamalardır. Film kasetlerinin kopyalanmasını engellemek amacıyla yapılan damgalama görünmez damgalamaya örnek olarak verilebilir.

3.4.3.1. Uzamsal ve zamansal boyuttaki damgalama teknikleri

Hareketsiz resimler üzerinde yapılan ilk damgalama en düşük değerlikli bite veriyi gömme tekniğidir. İlerleyen çalışmalarda ise parlaklık içine veri gömme tekniği de geliştirilmiştir. Fakat bu yöntem saldırılara karşı dayanıksız olduğu için damganın alçak geçiren bir filtre ile desteklenmesi gerekir.

3.4.3.2. Dönüşüm boyutu kullanan damgalama teknikleri

Bu damgalama tekniğinde ise dönüşüm yöntemlerinden yararlanılmıştır. Ayrık kosinüs dönüşümü ve ayrık dalgacık dönüşümü yöntemleri dönüşüm boyutunu kullanan damgalama tekniklerinde kullanılmıştır.

Dönüşüm teknikleriyle, resim ya da video gibi veri gömülmek istenen taşıyıcı dosya parçalara ayrılır. Ayrılan parçalar değerlendirilir ve insan görme sisteminin algılamasının en düşük olduğu parçalar bulunur. Bu parçalara veri gömme işlemi yapılabilir. Bu yöntem yetkisiz kişilerce yapılan saldırılara karşı oldukça dayanıklıdır.

3.4.4. Sayısal Damgalama ve Sırörtme Arasındaki Farklar

Görünmez damgalama tekniği ile sırörtme tekniği birbirine benzerlik göstermelerine rağmen iki teknik karıştırılmamalıdır. Damgalama tekniği bir bilginin gizliliğinden çok sayısal dosyaların korunmasını sağlar. Amacı kopya oluşumuna karşı bilgileri korumaktır. Örtü dosyası olarak herkesin bildiği ve kullandığı taşıyıcı dosyaları(resim, video, ses vb.) tercih edilir. Sayısal damgalamaya verilebilecek çok sayıda örnek mevcuttur. Örneğin paranın üzerine basılan, sadece mavi ışık altında görülebilen filigranlar, televizyon kanallarının logoları vb. Filmlerin kopyalanıp çoğaltılmasını önlemek damgalamanın en büyük uygulama alanlarındandır.

Sırörtme tekniği ise gizli bir haberleşmenin sağlanabilmesi için mesajın taşıyıcı bir dosyaya (resim, video, ses vb.) gömülmesidir. Amaç kimse tarafından bilinmeyen bir taşıyıcı üzerinde, dikkat çekmeden gizli haberleşmeyi sağlamaktadır. Sırörtme tekniğinde, taşıyıcı dosya gönderici tarafından seçilir ve diğer kişiler bunu bilemezler. Böylece taşıyıcı dosya dikkat çekmeyecek ve olası saldırılar önlenmiş olacaktır.

3.5. Veri Gömme Teknikleri

Gizlenecek olan mesajı örtü dosyası içerisine (resim, ses, video vb.) gömebilmek için çeşitli gömme algoritmaları geliştirilmiştir. Kimi yöntemle renk üzerine veri gömülürken kimi yöntemle de parlaklık gibi özellikler üzerine veri gömme işlemi gerçekleştirilebilir. Veri gömme tekniklerinden bazıları;

a) Histogramlar Yöntemi
   1. Benzer histogramlar yöntemi
   2. Farklı histogramlar yöntemi

b) Dalgaboyu Yöntemi

c) LSB Yöntemi

3.5.1. Histogramlar Yöntemi

Göndericinin kendisi tarafından seçilmiş olan bir örtü dosyasına (ses, resim, video vb.) gizlemek istediği mesajı en güvenli yöntemlerden biri olan histogramlar yöntemiyle gömebilir. Her algoritmanın farklı bir işleyişi vardır. Histogramlar yöntemi de taşıyıcı dosyayı oluşturan renklerin ve renk tonlarının üzerinde işlemler yaparak veri gömme işini gerçekleştirir.

Histogramlar yöntemi, örtü dosyası olan videoyu çerçevelere ayırır. Ayrılan her çerçevenin pikselleri için RGB (kırmızı, yeşil, mavi) renk bileşenlerinin değerlerini bulur. Bulduğu renk tonlarının değerlerinin ortalamasını alarak her bir piksel için tek bir histogram değeri hesaplanır. Ardışık çerçevelerdeki piksellerin karşılıklı olarak

değerlendirmesi yapılır. Bu değerlendirme aşamasında histogramlar yöntemi, Benzer Histogramlar ve Farklı Histogramlar yöntemi olarak iki farklı algoritmaya ayrılır. Değerlendirme neticesinde bulunan veri gömmeye uygun pikseller gömme algoritması aracılığıyla gömme işlemi yapılır.

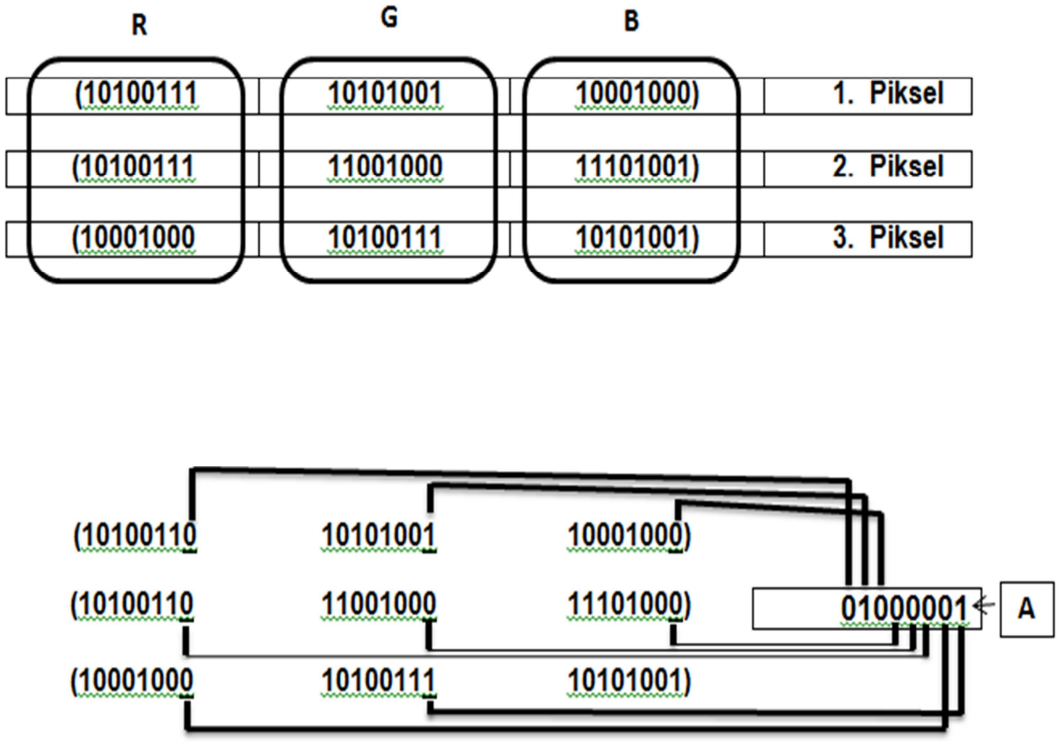
Histogramlar yöntemi veri gömme alanlarını seçerken iki farklı yol kullanır;

a) Blok tabanlı histogramlar yöntemi; video çerçevelere ayrılır. Her bir çerçeve belli katsayılarla bloklara ayrılır. Blokların içindeki piksellerin histogramları hesaplanır ve ardışık gelen çerçevedeki blokların histogram değerleriyle karşılaştırılır. Şarta uygun bloklara veri gömülür.

b) Çerçeve tabanlı yöntem de ise video çerçevelere ayrılır ve çerçevelerde bulunan piksellerin histogramları hesaplanarak ardışık gelen çerçevedeki histogram değerleriyle karşılaştırılır. Veri gömmeye elverişli olan pikseller veri gömme işlemi yapılır.

3.5.2. LSB Yöntemi

8 bitlik bir resmin her pikseli 1 ve 0 bitlerinden oluşmaktadır ve bu bitlerin 2^8 yani 256 renk meydana getirdiği bilinmektedir. İkili sayı sistemine göre 10110111 sayısı ele alınırsa: Bu sayının onluk sistemdeki karşılığı hesaplandığında 183 sayısı elde edilir. Sondaki bitin 1 veya 0 olması bu değeri çok fazla değiştirmeyecektir. Sondaki bit değeri 0 olduğu takdirde yeni oluşan kodlu ifadenin değeri 182 olacak ve renk üzerinde gözle görülecek büyük bir değişikliğe yol açmayacaktır. İşte bu en sonda yer alan bit, LSB olarak adlandırılır. Bu bitler yerine gizlenecek olan veriler yerleştirilerek veri gizleme işlemi yapılabilmektedir.



Şekil 3.9. LSB ile veri gömme.

Örneğin, 24 bitlik bir resim içerisine A harfini yerleştirilsin. 24 bitlik resim Şekil 3.9 ’da görülmektedir. A harfinin ASCII karşılığı 065 olup ikili karşılığı $(01000001)_2$’dir. Pikseldeki LSB’nin yerine A harfine ait sekiz bitin yerleştirilmesi işlemi Şekil 3.9’da görülmektedir. Dağıtım sonucunda değişen bitlerin altı çizili olarak verilmiştir. Orijinal resimle içerisine veri gizlenen resim arasında gözle görülür bir fark oluşmayacaktır. Bunun sebebi ise değişim 8-bit renk hücre biriminin en düşük değerlikli biti olan 2^0 yani 1 ağırlığına sahip olan bitinde yapılmasıdır. Dolayısıyla kırmızı-yeşil-mavi (Red, Green, Blue, RGB) ağırlıklarının her biri en fazla ±1 değişime uğrayacak olup bazı durumlarda da aynı kalmaktadır.

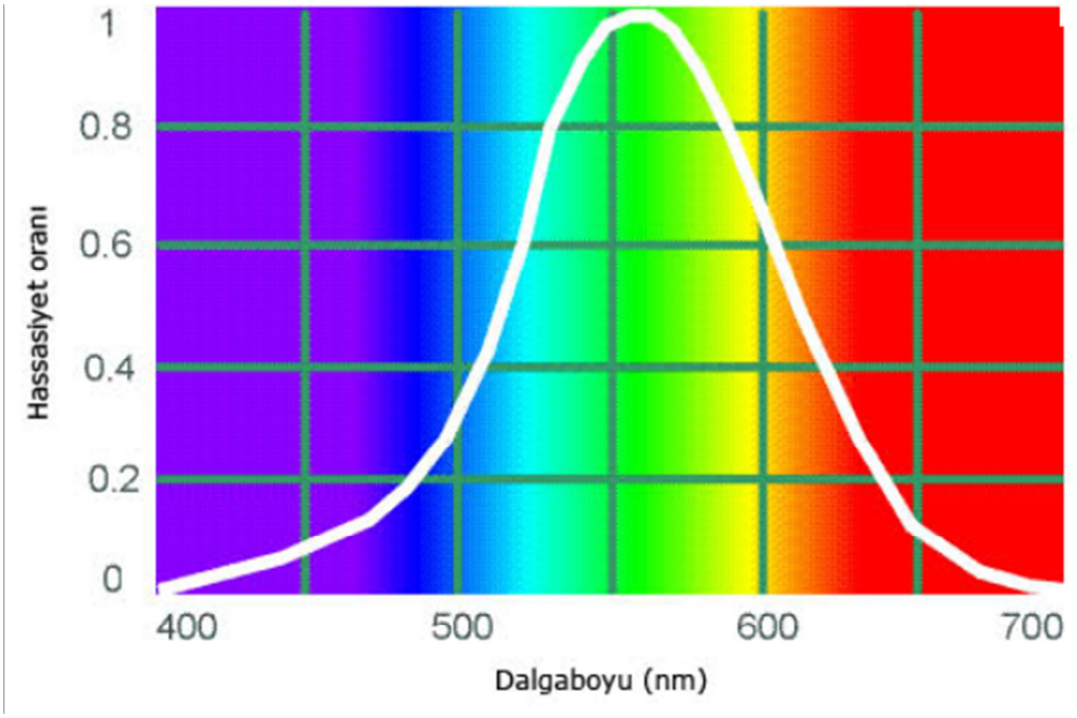
3.5.3. Dalgaboyu Yöntemi

Dalgaboyu yaklaşımı da diğer yaklaşımlar gibi insan görme sisteminin zayıflıklarından faydalanma üzerine kurulmuştur. İnsan gözü belli dalgaboyu aralığındaki değerlerde görebilir (350 nm ile 750nm). Bu aralığın dışındaki dalga değerleri morötesi ve kızılötesi ışık dalgalarıdır ve insan görme sistemi bu dalgaları göremez. Dalgaboyu yaklaşımı da bu durumdan faydalanır. İnsan görme sisteminin göremediği dalga sınırlarına yakın pikseller seçilir ve bu aralığa veriler gömülür.

Öncelikle örtü dosyası bir video ise çerçevelere ayrılır. Ayrılan çerçevelerdeki piksellerin dalgaboyu değer aralığı bulunur. Bunun için öncelikle mor ve kırmızı renkleri veren RGB renk karışımlarının bir tablosu oluşturulur. Bu tabloyu oluşturmak için herhangi bir resim işleme programından faydalanılabilir. Ayrıca İnternette kolayca bulunabilen renk kodlarının listelerinden de faydalanmak mümkündür. Piksellerin dalga boylarının değerleri bulunduktan sonra elde edilen tablodan veri gömmeye uygun olup olmadığına bakılır. Eğer pikselin dalga değerleri sınır değerlerine yakın ise (380 nm ile 750nm) veri gömme işlemi bu pikseller üzerine yapılır. Gömme işleminin en önemli kısmı ise veri gömüldükten sonra pikselin dalgaboyu değeri ilk durumundakine yakın ise veri tam olarak o piksele gömülür. Yakın değil ise bu değişimi insan görme sistemi tarafından algılanacağından bu piksele veri gömme işleminin uygulanması tercih edilmez. Örneğin resimdeki 520 nm dalgaboyu değerine sahip mor renkli piksel, veri gömüldükten sonra 520nm ile 530nm aralığında bir dalgaboyu değerinde kalıyorsa bu piksele veri gömme yapılabilir. Fakat piksel veri gömme gerçekleştirildikten sonra 540nm değerine sahip oluyorsa bu piksel veri gömme için uygun değildir ve veri gömülmez.

Dalga boyu yönteminde önemli olan, gizli verinin içerisine yerleştirildiği pikselin dalga boyu aralığının sahip olduğu orijinal dalga boyu aralığından çıkmamasıdır ve bu sayede video çerçevelerini oluşturan her bir piksele birbirinden bağımsız olarak veri gömme işlemi gerçekleştirilebilir. Dalgaboyu yönteminin benzer ve farklı histogramlar yöntemleri ile birlikte kullanılması sayesinde gizli verinin

algılanabilirliği daha da düşürülerek haberleşme güvenliği en üst seviyeye çıkarılabilir. Fakat bu durumun gizli veri kapasitesini önemli ölçüde düşüreceği unutulmamalıdır.



Şekil 3.10. İnsan görme sisteminin görebileceği ışık değer aralıkları.

3.6. Sıraçma (Steganaliz)

Bir sıraçılımsal algoritma değerlendirilirken üç temel özelliği dikkate alınır. Bunlar;

1. Taşıyıcıdaki Değişim
2. Kapasite
3. Dayanıklılık

Bir sıraçılımsal algoritma değerlendirilirken taşıyıcıda (cover object) ne kadar değişim olduğu çok önemlidir. Taşıyıcıdaki değişimi ya da resimdeki bozulma oranının belirlenmesi için çeşitli ölçme yöntemleri vardır. Bunlar arasında en bilinenleri; MSE, RMSE, PSNR'dır. MSE (mean squared error) hataların kareleri

toplamının ortalamasıdır. MSE genellikle σ^2 olarak gösterilir. RMSE (root mean squared error) ise MSE'nin kareköküdür.

$$\sigma^2 = \frac{1}{N}\sum_{n=1}^{N}(x_n - y_n)^2$$

Bazen MSE yerine, hatanın büyüklüğünün orijinal piksel değerinin en büyüğü (peak-tepe) ile olan ilişkisi önem kazanır. Bu gibi durumlarda PSNR (peak signal-to-noise ratio) yöntemi kullanılır.

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

sıraçma, bir örtü verisi (cover data) içerisinde herhangi bir bilgi olup olmadığını bulmayı ve eğer var ise bu bilgiyi elde etmek amacıyla steganografik algoritma kullanılan sisteme karşı yapılan saldırı yöntemleridir. Genelde saldırı yapan kişinin sıraçıcı (steganalist) kullanılan sıraçımsal sistemi bildiği varsayılır (Kerchoffs'un prensibi). Eğer sıraçıcı kullanılan sistemi bilmiyorsa, bu onun işini zorlaştıracaktır. Sıraçıcının bir sıraçılımsal sisteme saldırabilmesi için sahip olması gereken veriler vardır. Bu sahip olduğu verilere göre saldırı modellerinden birini seçebilir. Bu saldırı modellerinden en yaygın olanları şunlardır:

- Sadece sır saldırısı: Analiz için sadece sır-nesnesi (Stego-object) bilinmektedir.

- Bilinen örtü (cover) saldırısı*:* Görüntünün mesaj gizlenmeden önceki ve sonraki hali bilinmektedir.

- Bilinen mesaj saldırısı: Saklanan mesaj bilinmektedir.

- Seçilmiş sır saldırısı: Sıraçımsal algoritma ve sır-nesnesi bilinmektedir.

- Seçilmiş mesaj saldırısı: Sıraçıcı bu yöntemde sır-nesnesini analiz edebilmek için çeşitli mesajlar seçer, sıraçımsal araçlar kullanır ve algoritmayı bulmaya çalışır

- Bilinen sır saldırısı: Örtü nesnesi, sır nesnesi ve sıraçımsal araçlar bilinmektedir.

Her sıraçımsal yöntem özel bir analiz yöntemine ihtiyaç duyar. Yani her yöntem için birçok farklı sıraçma yöntemi geliştirilmiştir ve sadece o algoritma üzerinde uygun sonuçlar vermektedir. Küçük bir bilgiyi büyük boyuttaki bir resmin içine gömmemiz halinde hiç kimse tarafından sezilemeyecektir.
Sıraçmada sezme saldırısı olarak kullanılan birçok yöntem vardır. En yaygın olarak kullanılanlar şunlardır:

1. χ^2 Testi
2. Histogram Analizi (PoVs'lerin Analizi)
3. RS Steganaliz (İkili İstatistik Yöntemi)
4. RQP Yöntemi (Raw Quick Pairs)
5. Görsel Ataklar

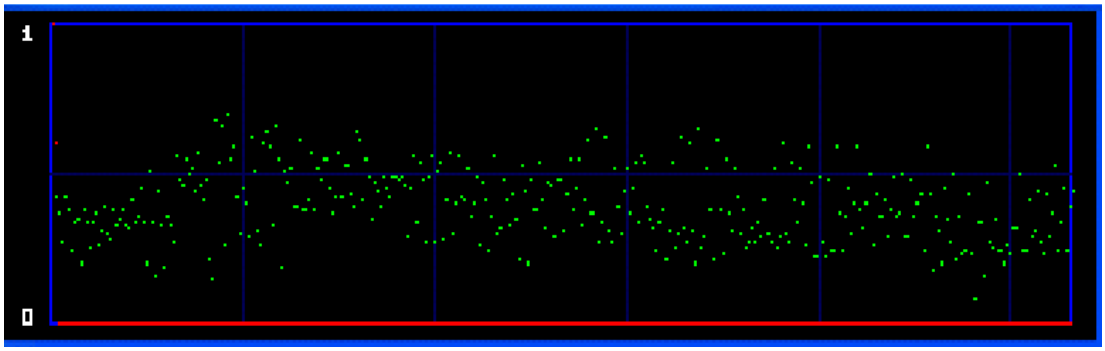
3.6.1. χ^2 Testi

LSB yöntemiyle veri gizlenen resim dosyalarında kullanılmaktadır. Özellikle sıralı LSB gömme sırörtmede başarılı sonuç vermiştir. PoVs (pair of values) değerlerinde istatistiksel analizde temelli olan χ^2 istatistik testi, Westfeld tarafından sunulan bir sıraçma yöntemidir. İçine veri gizlenmemiş görüntüler için PoVs'lerin frekansları düz bir şekilde dağılmamaktadır, fakat LSB gizleme sırörtme söz konusu olunca her PoVs' in frekansları eşit olmaktadır. Her baytın 8 bit ile temsil edildiğini düşünürsek 256 değerimiz ve 128 PoV çiftimiz olacaktır. χ^2 Testi sonucu 1'e yakınsa bu resmin içinde veri saklanmış demektir. Eğer 0 çıkıyorsa veri gizlenmemiştir[8].

Örnek resim: 130x110 boyutunda bir bmp resim.

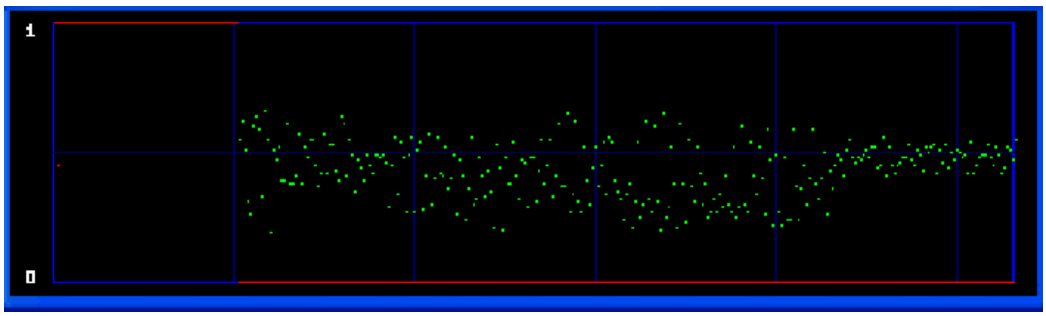
Şekil 3.11. χ^2 Testi için kullanılan orijinal resim.

Resmin içinde bilgi yokken yapılan χ^2 Testi sonucu şöyledir.

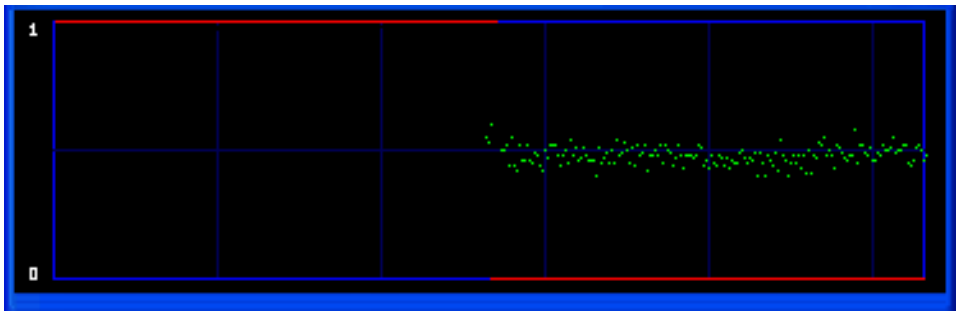


Şekil 3.12. Resmin veri gömülmeden önceki χ^2 Testi sonuçları.

Resmin içine sırasıyla 1 KB ve 2,7 KB gizlediğimizde ise oluşan test sonuçları şöyledir.



Şekil 3.13. Resmin içerisine 1KB'lık veri gömüldükten sonraki χ^2 Testi sonuçları.



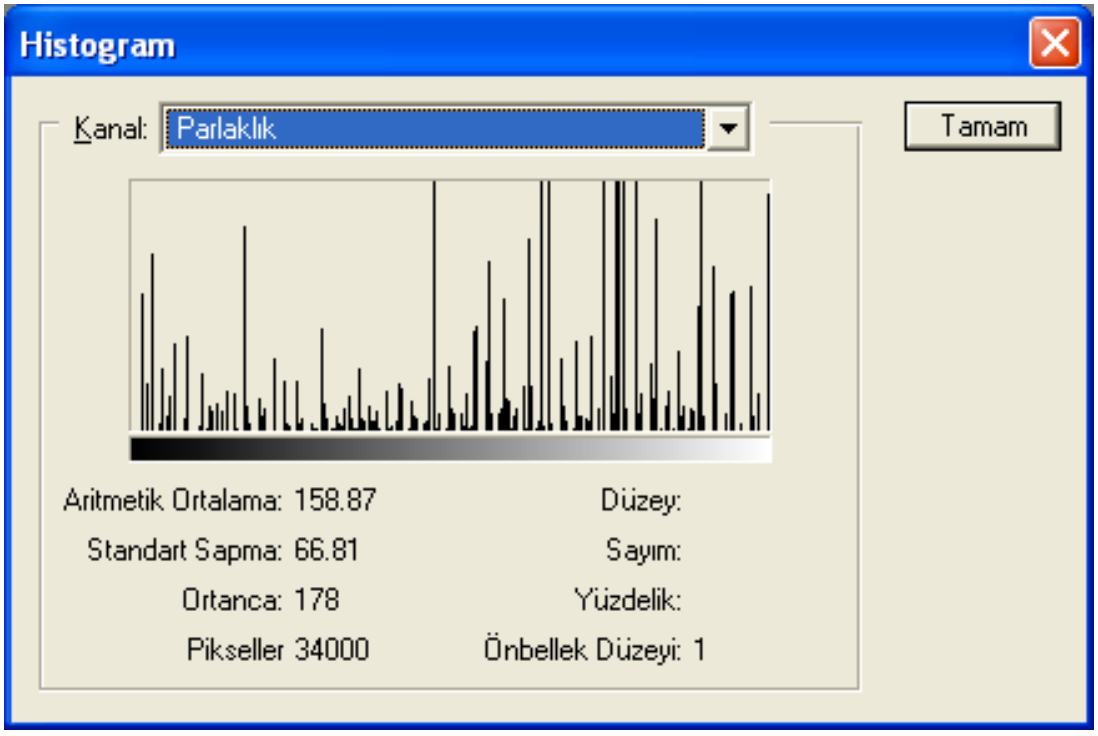
Şekil 3.14. Resmin içerisine 2,7 KB'lık veri gömüldükten sonraki χ^2 Testi sonuçları.

Şekil 3.12'de görüldüğü gibi resim için hesaplanan PoVs değerleri tek düze olarak görünmemektedir. Değerler 0 ile 1 arasında değişik değerler almıştır. Şekil 3.13'de ise içerisine 1 KB'lık veri gömülmüş ve PoVs değerleri ilk peiyotta 1 değerini almıştır. Bu da resmin bu alanında veri gömülmesi olmuş demektir. Diğer periyotlar da ise PoVs değerleri 0 değerindedir ve bu da bu alanlara veri gömülümü olmamış demektir. Şekil 3.14' de ise gömülen verinin boyutu arttırılınca oluşan PoVs değerleri sonuçlarını göstermektedir.

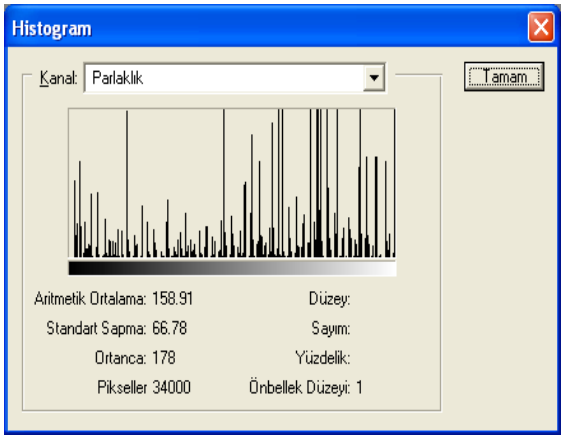
3.6.2. Histogram Analizi

Histogram Analizi renklerin dağılımı hakkında bilgi vermektedir. İçine 1 KB, 5 KB saklanmış olan 200x170 boyutlarındaki resmimiz için histogram sonuçları aşağıda verilmiştir[8].

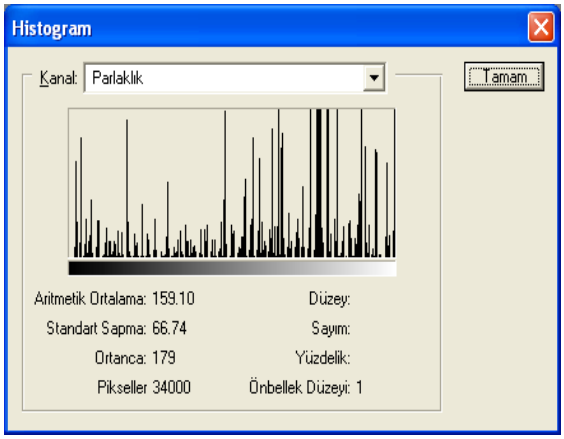
Şekil 3.15. Orijinal resim.



Şekil 3.16. Orijinal resim için Histogram değerleri.



Şekil 3.16. 1 KB veri gizlenmiş resim için histogram



Şekil 3.17. 1 KB veri gizlenmiş resim için histogram

Bu yöntemde gizlenen veri miktarı arttıkça histogramdaki değişim miktarı artmaktadır. Çok az miktarda saklanan verilerin tespitinde pek güvenilir sonuçlar vermemektedir.

.

3.6.3. RQP Yöntemi

Fridrich, RQP (Raw Quick Pairs) metodunu da geliştirmiştir. RQP yöntemi 24 bit renkli resimler üzerinde rastgele LSB yöntemiyle gizlenen veriler için çalışmaktadır. Bu metod LSB gizlemesi tarafından oluşturulan yakın renk çiftlerini analiz etmeye yöneliktir. Yakın renk çiftleri ile tüm renk çiftleri arasındaki oran hesaplanır. Elimizde bulunan içinde veri olup olmadığını anlamak istediğimiz resim için bu oran (O_1) hesaplanır. Daha sonra bu resmin içine bir test mesajı gizlenir. Oran tekrar hesaplanır (O_2). O_1 ile O_2 arasındaki fark çok farklı ise elimizde bulunan resimde gizlenmiş veri yoktur. Bu oran birbirine çok yakın ise resmin içinde gizlenmiş veri var demektir. RQP, cover-görüntüde yakın renk çiftlerinin sayısı, piksel çiftlerinin sayısının %30'undan küçük olduğu sürece gayet iyi sonuçlar vermektedir. %50'sini geçerse, verilen sonuçlar giderek güvensiz olmaktadır[8].

3.7. Sonuç

Gelişen teknoloji ile birlikte iletişimde bazı sorunlar ortaya çıkmıştır. Bu sorunların en başında güvenlik gelmektedir. Yetkisiz kişilerce düzenlenen saldırılarda kişiye ya da devlete özel mesajlar deşifre olmakta ve kötü niyetli kişilerce de mesajın içeriği bilinmektedir. Güvenlik sorunlarının aşılabilmesi için insanlar tarih öncesi çağlardan bu yana çalışmalar sürdürmüştür. Her gösterilen gelişme bir önceki yöntemden daha üstün ve daha başarılı olmuştur.

Son zamanlarda yapılan çalışmalarda ise şifreleme teknikleri geliştirilmiştir. Şifreleme verileri üçüncü kişilerin eline geçtiğinde bir anlamı olmayan bir biçime dönüştürür. Bu sayede de mesaj başkalarının eline geçmiş olsa dahi anlamsız simgeler olmaktan başka bir anlam ifade etmez.

Şifrelemenin bir dezavantajı varsa o da üçüncü kişilerinde gizli bir haberleşmenin varlığından haberdar olmalarıdır. Bu durumu aşabilmek için ise sırörtme (staganography) tekniği geliştirildi. Bu teknik sayesinde gönderici ve alıcıdan başka kimse gizli bir haberleşmenin varlığından haberdar değildir.

Bu bölümde şifreleme ve sırörtme teknikleri incelenmiştir. Şifrelemenin ve sırörtmenin güvenli haberleşmede ne kadar önemli olduğu açıklanmıştır. Hangi tür amaçlar için hangi tür tekniklerin kullanılması gerektiği konusunda fikirler sunulmuştur. Tekniklerin üstünlükleri ve zayıflıkları da yine bu bölümde incelenmiştir.

BÖLÜM 4. VİDEOLAR İÇİN SIRÖRTME YAKLAŞIMI İLE GELİŞTİRİLEN VERİ GÖMME ALGORİTMALARI

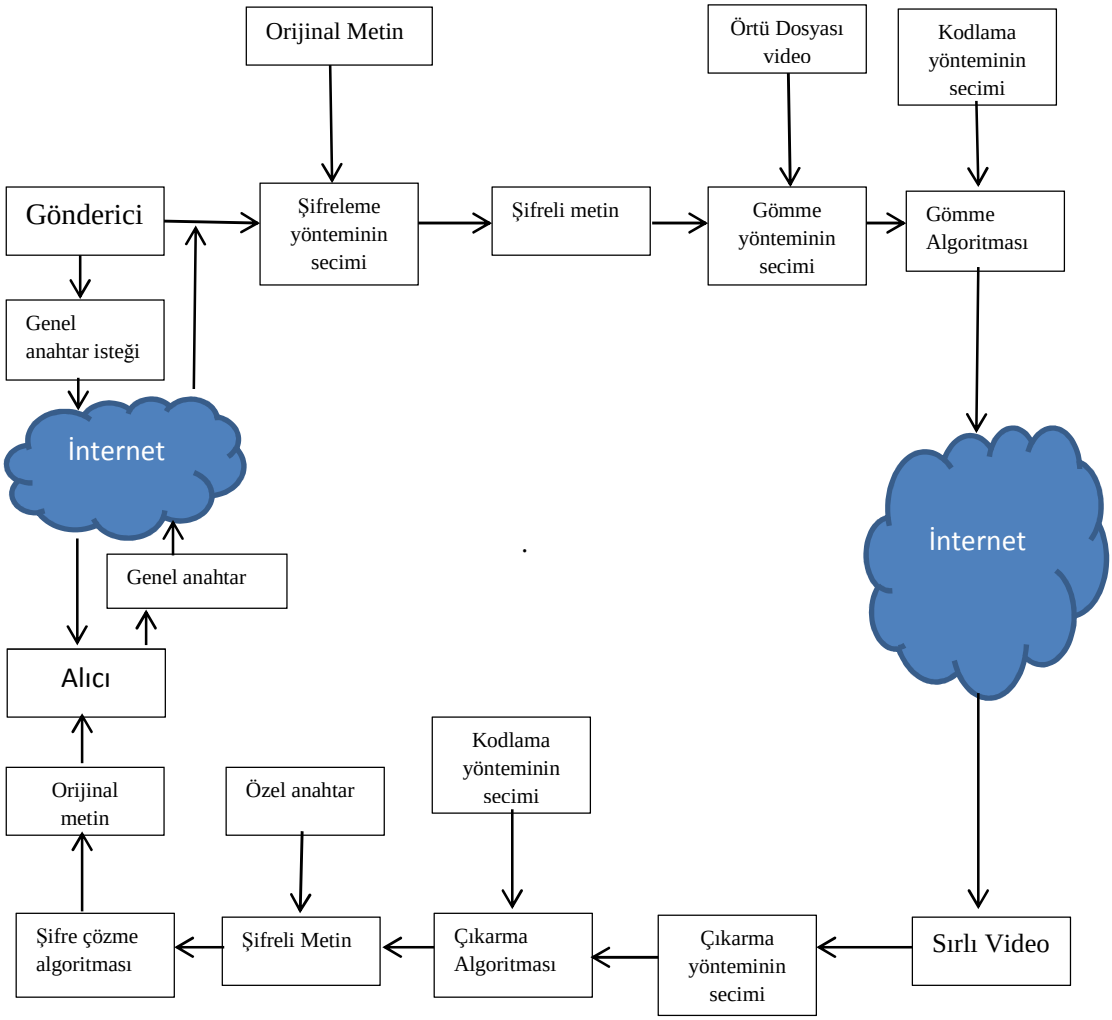
4.1. Giriş

Son yıllarda yapılan çalışmalar da sadece uzay boyutunda hareketsiz görüntülere gizli veriyi gömme üzerine ağırlık verilmiştir. Çok az sayıdaki çalışmalarda hem uzay düzleminde hem de zaman düzleminde taşıyıcı dosyaya veri gömme ele alınmaktadır. Ayrıca daha önceden yapılmış çalışmalar ya şifreleme ya da veri gömme üzerine olmuştur. Sunulan tez çalışmasında önce şifrelenen veriyi hem uzay boyutunda hem de zaman boyutunda gömmek için bazı yöntemler önerilmektedir.

4.2. Geliştirilen Veri Gizleme İşleminin Genel Çalışma Prensibi

Tez çalışması sürecinde gizlenecek veriyi şifreleme ve gizleme sürecinde izlenecek olan yöntemlerin genel blok diyagramı Şekil 4. 1.‘de gösterilmektedir. Süreç gönderici tarafın, alıcı taraftan, veriyi şifrelemekte kullanılacak olan genel anahtarı istemesi ile başlar. Alıcı bu isteği değerlendirir ve kendisi için özel anahtar gönderici için ise genel anahtar üretir. Genel anahtarı gönderici noktaya iletir. Gönderici genel anahtarı almıştır. Aldığı genel anahtar sayesinde girmiş olduğu gizli mesajı seçmiş olduğu şifreleme yöntemiyle şifreler. Oluşan şifreli metin önceden belirlenmiş olan bir taşıyıcı dosyaya(video) seçilmiş olan gömme tekniği, gömme algoritması ve kodlama yönteminin seçimiyle gizli metin örtü dosyasına gömülmüş olur. İletişim hattı üzerinden gönderilen sırlı video alıcı tarafından alınır. Ardından çıkarma yöntemi, çıkarma algoritması ve kodlama tekniği seçilerek sırlı videodan şifreli bilgi

çıkarılmış olur. Ardından şifre çözme algoritması uygulanarak şifresi çözülür ve orjinal metin elde edilmiş olur.

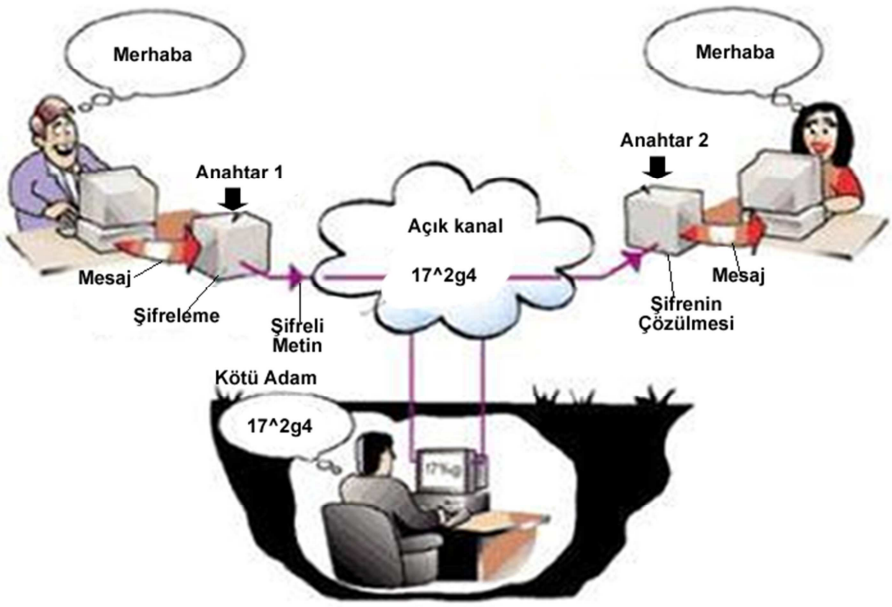


Şekil 4.1. Sunulan tez çalışmasının genel çalışma prensibi blok diyagramı

4.2.1. Veri şifreleme işlemi

Gizli veriyi gönderen nokta ile alacak olan nokta birbirine kablosuz Internet ağı üzerinden bağlanır. Bağlantının kurulmasının ardından gönderici, alıcıdan anahtar üretmesi için istekte bulunur. Alıcı bu istediği aldığına dair bir geri bildirimde bulunur. Ardından genel ve özel anahtarları üretir. Genel anahtarı göndericiye yollar. Genel anahtarı alan gönderici dışarıdan girilen gizlenecek olan mesajı alır ve genel

anahtar aracılığıyla RSA açık anahtar şifreleme tekniği ile şifreler. Şifrelenmiş metin gönderilmeye hazırdır.



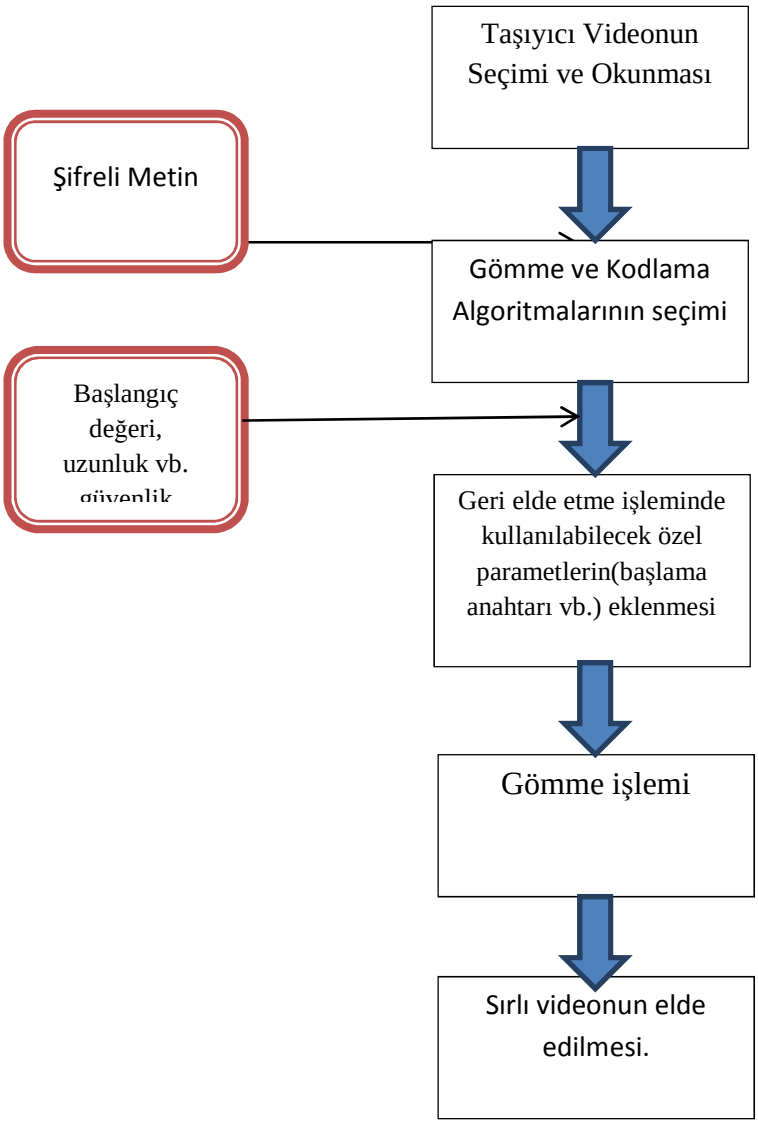
Şekil 4.2. RSA şifreleme ile iletişim.

Şekil 4.2.'de gösterildiği üzere gizli haberleşmeyi gerçekleştirecek iki nokta arasında kurulan iletişim yolunu yetkisiz kişiler tarafından dinlenilmektedir. Gönderici genel anahtarla (herkesin bildiği anahtar) şifrelemiş olduğu mesajı iletişim yoluna koyar. Kötü niyetli kişiler gizli haberleşme olduğunu anlar fakat anlamsız biçimlere büründürülmüş olan metni çözemezler. Alıcı nokta mesajı aldığında özel anahtarla (sadece alıcının bildiği anahtar) şifreli mesajı çözer ve orijinal metni elde eder.

4.2.2. Veri gizleme işlemi

Şifreli metin elde edildikten sonra, veri gizleme işlemine başlanacaktır. Veri gizleme "avi" video formatında herhangi bir videonun seçilmesiyle başlar. Bu seçilen video örtü (taşıyıcı) videodur. Seçim işlemi gerçekleştikten sonra videodaki toplam çerçeve sayısı, videonun süresi ve bellekte kapladığı alan gibi birkaç özelliği hesaplanır. Yapılan bu hesaplamaların ardından veri gizlemede kullanılacak algoritma seçilir. Seçilen veri gizleme algoritmasına göre kaç adet piksel var ve maksimum ne kadarlık

veri gömme yapılabilir hesaplanır. Örneğin benzer histogramlar yöntemine göre veri gizlenecek ise; önce her bir çerçevedeki veri gömmeye uygun pikseller bulunur ve kullanıcı bu doğrultu da bilgilendirilir. Veri gizleme yöntemi seçiminin ardından verinin örtü dosyasına nasıl kodlanacağını belirleyen kodlama yöntemi seçilir. Belirlenen kodlama tekniğiyle veri gömmeye elverişli piksellere gizlenecek verinin ASCII kodları yerleştirilir. Kodlama işlemi sırasında kodlamanın nasıl olacağını belirleyen yöntem için RGB ve R ağırlıklı kodlamaların yanı sıra LSB kodlama tekniği de kullanılabilir. Tez çalışmamızda RGB ağırlıklı kodlama tekniğinin kullanılması tercih edilmiştir. Tüm bu kodlama tekniklerinin seçiminden sonra daha önceden şifrelenmiş olan mesajı paketinin içine, başlangıç değeri olarak adlandırdığımız ve verinin bu değerden hemen sonra gelmeye başlayacağını gösteren değer, ardından mesajın boyu ve gizli mesajın içeriği yerleştirilmeye başlanır. Bu aşamadan sonra her bir çerçeve içerisinde veri gömmeye elverişli piksellere oluşturulmuş veri paketi gömülmeye başlanır. Veri paketinin oluşturulması alıcı tarafın paket hakkında hiçbir şey bilmemesine rağmen üzerinde rahatlıkla işlemler yapabilmeyi sağlar. Gizlenecek verinin uzunluğuna göre veri gömme süresi değişir. Gömü dosyasının tamamı taşıyıcı videoya gömüldükten sonra oluşan sırlı video kaydedilir. Böylece veri gömme uygulaması sonlandırılır.



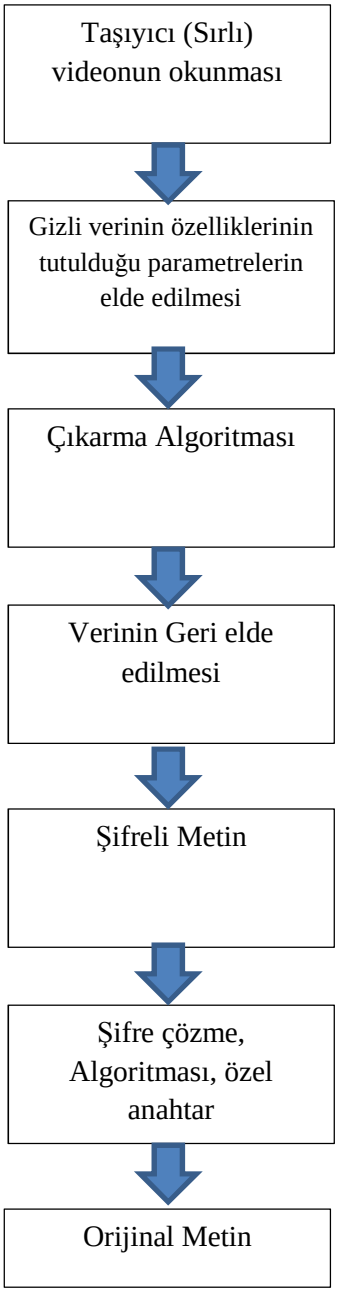
Şekil 4.3. Genel veri gizleme akış diyagramı.

4.2.3. Gizli verinin geri elde edilmesi ve şifre çözme işlemi

Sırlı videodan gizli verinin elde edilmesi işlemi, sırlı videonun alıcı tarafa ulaşması ve okunmasıyla başlar. Gömme işleminde kullanılan gömme ve kodlama algoritmaları doğrultusunda tasarlanmış olan çıkarma algoritması sayesinde videonun veri gömülmüş olabileceği pikselleri araştırılır. Belirlemiş olduğumuz başlangıç değerini elde ettiğimizde veri gömme kodumuza göre artık veri gelmeye başlayacaktır. Her bir çerçevenin piksellerine bakılır. Veri parçaları toplanır ve en

son olarak verinin boyuna eş veri toplanıldığında ise gizli mesajı geri elde etmiş oluruz.

Elde edilen metin şifreli metindir. Öncelikle alıcı tarafta bulunan özel anahtar ve şifre çözme algoritması ile birlikte şifreli metin çözülmüş olur. Bu yolla orijinal mesaj elde edilir.



Şekil 4.4. Gizli veriyi geri elde etme ve şifre çözme akış diyagramı.

4.3. Geliştirilen Veri Gizleme ve Şifreleme Yöntemleri

Çalışmalarımız, öncelikle gizli veri girilmesi ve girilen mesajın şifrelenmesiyle başlar. Şifreleme işlemini gerçekleştirebilmek için geliştirilen algoritma açık anahtar şifreleme yöntemlerinden biri olan RSA algoritmasıdır. RSA şifreleme ile ilgili verilen aşağıdaki kısımlarda verilmiştir.

4.3.1. Kullanılan Şifreleme Yöntemi

İlk defa 1977 yılında RonRivest, Adi Shamir ve LeonardAdleman tarafından oluşturulan RSA algoritması geliştiricilerinin soyadlarının ilk harfleriyle anılmaktadır.

Bir genel anahtarlı şifreleme tekniği olan RSA, çok büyük tamsayıları oluşturma ve bu sayıları işleminin zorluğu üzerine düşünülmüştür. Anahtar oluşturma işlemi için asal sayılar kullanılarak daha güvenli bir yapı oluşturulmuştur. Anahtar oluşturma algoritması şu şekildedir:

a) P ve Q gibi çok büyük iki asal sayı seçilir.

b) Bu iki asal sayının çarpımı N = P.Q ve bu bir eksiklerinin $\varphi(N)=(P-1)(Q-1)$ hesaplanır.

c) 1'den büyük $\varphi(N)$'den küçük $\varphi(N)$ ile aralarında asal bir E tamsayısı seçilir.

d) Seçilen E tamsayısının mod $\varphi(N)$'de tersi alınır, sonuç D gibi bir tamsayıdır.

e) E ve N tamsayıları genel anahtarı, D ve N tamsayıları ise özel anahtarı oluşturur.

Genel ve özel anahtarları oluşturduktan sonra gönderilmek istenen bilgi genel anahtar ile şifrelenir. Şifreleme işlemi şu şekilde yapılmaktadır: Şifrelenecek bilginin sayısal karşılığının E'ninci kuvveti alınır ve bunun mod N deki karşılığı şifrelenmiş metni oluşturmaktadır. Genel anahtar ile şifrelenmiş bir metin ancak özel anahtar ile açılabilir. Bu yüzden şifrelenmiş metin, yine aynı yolla, şifrelenmiş metnin sayısal karşılığının D'ninci kuvveti alınır ve bunun mod N'deki karşılığı orijinal metni oluşturur.

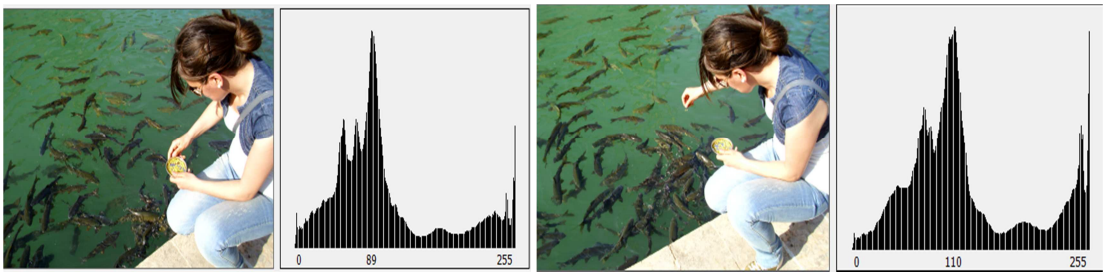
4.3.2. Kullanılan Veri gömme yöntemi

Çalışmamız, öncelikle örtü dosyasında bulunan piksellerin veri gömmeye elverişli olup olmadığının belirlenmesiyle devam etmektedir. Veri gömmeye uygun piksellerin bulunması için geliştirilen yöntem histogramlar yöntemidir. Geliştirilen bu yöntem ile ilgili detaylı bilgi aşağıdaki kısımlarda verilmiştir.

4.3.2.1 Histogramlar yöntemi

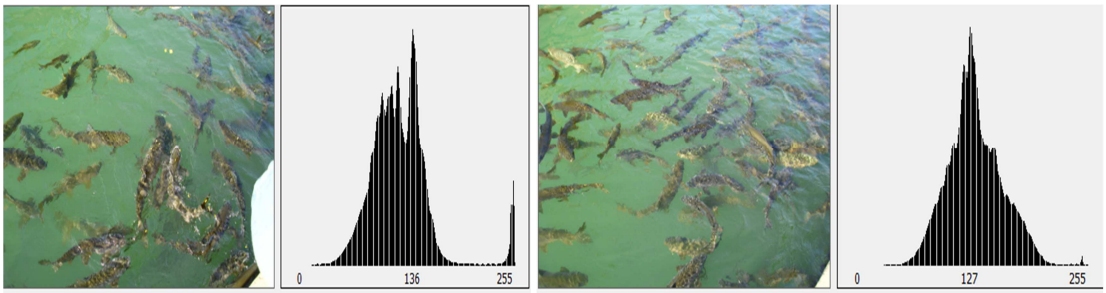
Histogramlar yönteminde ardı sıra gelen video çerçevelerinin her bir pikselinin ayrı ayrı histogram değerleri hesaplanır ve olay bu değerler üzerinde yorumlanır. Bu yöntemde öncelikle içerisine veri gömülebilecek piksellere sahip olan çerçeveler belirlenir. Elde edilen bu çerçevelerde bulunan piksellerin histogram değerleri bulunur. Histogram, bir videoyu oluşturan her bir hareketsiz görüntüyü (resim) oluşturan piksellerinin sahip oldukları renk bileşenlerinin koyuluk bilgilerine göre dağılımlarını gösteren değerler dizisidir. Genel olarak 24-bit renkli resimler için histogram 256 elemanlı pozitif tam sayılar dizisidir. Yani resmi oluşturan her bir pikselin 0 ile 255 arasında bir renk koyuluk değerine sahiptir. Bir resim ele alındığında, piksellerin sahip oldukları histogram değerleri '0' dan farklı olan değerler ne kadar farklı ise resim hakkında o kadar çok fazla renk ve ton sahibi olduğunu söyleyebiliriz. Histogram değerleri '0' olan ne kadar çok pikseli var ise o resimde resim o kadar beyaz ve tonsuzdur denilir. Yine resim içerisinde piksellerin sahip oldukları '0 'dan farklı histogram değerleri, birbirini takip eden pikseller

arasında yakın değerler aralığına düşüyor ise o resim neredeyse düz bir renkte olduğu söylenebilir. Böylelikle her bir video çerçevesini oluşturan renkler ve tonları hakkında bilgi sahibi olmuş oluruz. Geliştirilmiş olan histogramlar yönteminde, öncelikle video kendisini oluşturan hareketsiz görüntülere ayrılıyor. Bunların her biri genel olarak çerçeve (frame) olarak adlandırılıyor. Videoyu oluşturan çerçevelerin her bir pikseli için o pikselin renk tonunu oluşturan renk bileşenleri (R,G,B) için ayrı ayrı bulunduktan sonra bulunan bu değerin ortalaması alınır. Örneğin; n. pikselin R=255, G=24, B=45 bulunmuş olsun bu n. pikselin histogramı,(R+G+B)/3 ‘den bulunur. Ardışık çerçevelerde de bu işlem gerçekleştirildikten sonra birbirini takip eden her bir çerçevenin aynı pikseli için bulunan histogramlar arasındaki fark hesaplanır. Böylece değerlendirilecek olan tek bir değer elde etmiş olunur. Örneğin; birinci çerçevedeki üçüncü pikselin histogramı 156 bulunmuş olsun, bir sonraki çerçeve olan ikinci çerçevenin yine aynı pikseli yani üçüncü pikselinin histogram değeri 147 hesaplanmış olsun. Bu iki histogram arasındaki farkın mutlak değeri alınır ve değerlendirme yapmak için tek bir değer elde etmiş oluruz. Elde edilen bu değer ne kadar az ise resim çerçeveleri arasındaki fark o kadar azdır, ne kadar fazla ise de resimler arasındaki renk ve ton o kadar birbirinden farklıdır denilir. Böylece hangi çerçevenin hangi pikseline veri gömüldüğünde insan göz sisteminin bu değişimi algılamasının en az olacağını yorumlayabiliriz.



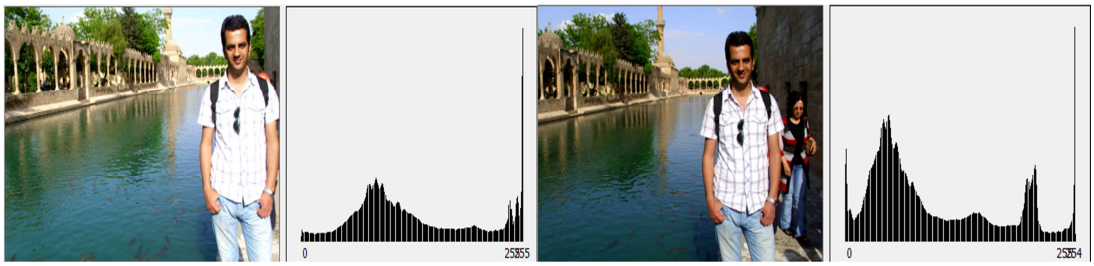
1.Kare Resim ve Histogram Değerleri

2.Kare Resim ve Histogram Değerleri



3.Kare Resim ve Histogram Değerleri

4.Kare Resim ve Histogram Değerleri



5.Kare Resim ve Histogram Değerleri

6.Kare Resim ve Histogram Değerleri

Şekil 4.5. Farklı sahne geçişlerini ve histogramlarını gösteren örnek bir sayısal video.

Şekil 4.5 ‘de altı çerçeveden oluşan örnek bir video verilmiştir. Her bir çerçevenin histogram değerleri yanlarında bulunan grafiklerde gösterilmektedir. Resimlerde büyük farklılık 3.kare ile başlamaktadır. Bunu yanlarında verilen histogram değerlerini gösteren grafikten rahatlıkla görebilmekteyiz. 1. ve 2. karelerde fazla bir farklılık yoktur. Histogram grafikleri bu çıkarımı doğrulamaktadır. 2. kare ile 3. kare arasında fazlasıyla fark bulunmaktadır. Yani iki çerçeve arasındaki histogram farkı

büyüktür. 3.kare ile 4.kare arasında da fazla bir histogram farkı yoktur. Fakat 4.kare ile 5.kare arasında fazlasıyla fark bulunmaktadır. 5.kare ile 6.kare arasında da benzerlik çoktur. Ardışık video çerçeveleri arasındaki bu renk ve hareket geçişlerini algılamak için eşik değeri denen sayısal bir değer kullanılır. Eşik değeri ardışık çerçeveler arasında bir değişim veya benzerlik algılanmasında kullanılan, alabileceği en büyük değer histogramın alabileceği en büyük değerle aynıdır. Yani en çok 255 değerini alabilir. Eşik değer aslında kullanıcı tanımlı bir algılama kıstasıdır. Tez çalışmasında geliştirilen veri gizleme programında bu eşik değeri algılanabilirlik – kapasite parametresi ile kullanıcı tarafından ayarlanabilmektedir. Bununla kullanıcıya bir esneklik sağlamak amaçlanmıştır. Eşik değerinin yüksek seçilmesi ile çerçeve geçişlerindeki algılama hassasiyetin arttırılmasına karşılık bölümlenebilecek çerçeve sayısında düşme olur. Çerçeve sayısının azalması ise gömülebilecek veri uzunluğunun azalması anlamına gelmektedir. Eşik değerinin düşük seçilmesi durumunda ise hassasiyet azalacak fakat bölümlenebilecek çerçeve sayısı artacaktır. Dolayısıyla gömülebilecek veri uzunluğu da artacaktır. Bu bilgiler ışığında kullanıcı tarafından girilecek bir eşik değer ile ardışık çerçevelerin histogram farkları karşılaştırılarak veri gizlenebilecek video çerçeveleri ve pikselleri belirlenir. Eşik değerin üzerinde kalan pikselleri seçilirse, ardışıl video çerçevelerinin renk bakımından karışık bir yapıya sahip olduğu anlaşılır ki bu Farklı Histogramlar yöntemi olarak adlandırılır. Eşik değerin altında kalan bileşenlerin seçilmesi durumunda ise ardışıl video çerçevelerinin renk bakımından tekdüze olduğu anlaşılır ki bu da Benzer Histogramlar yöntemi olarak adlandırılır.

Histogramlar yönteminde veri gömülecek olan uygun alanlar iki farklı teknikle bulunur.

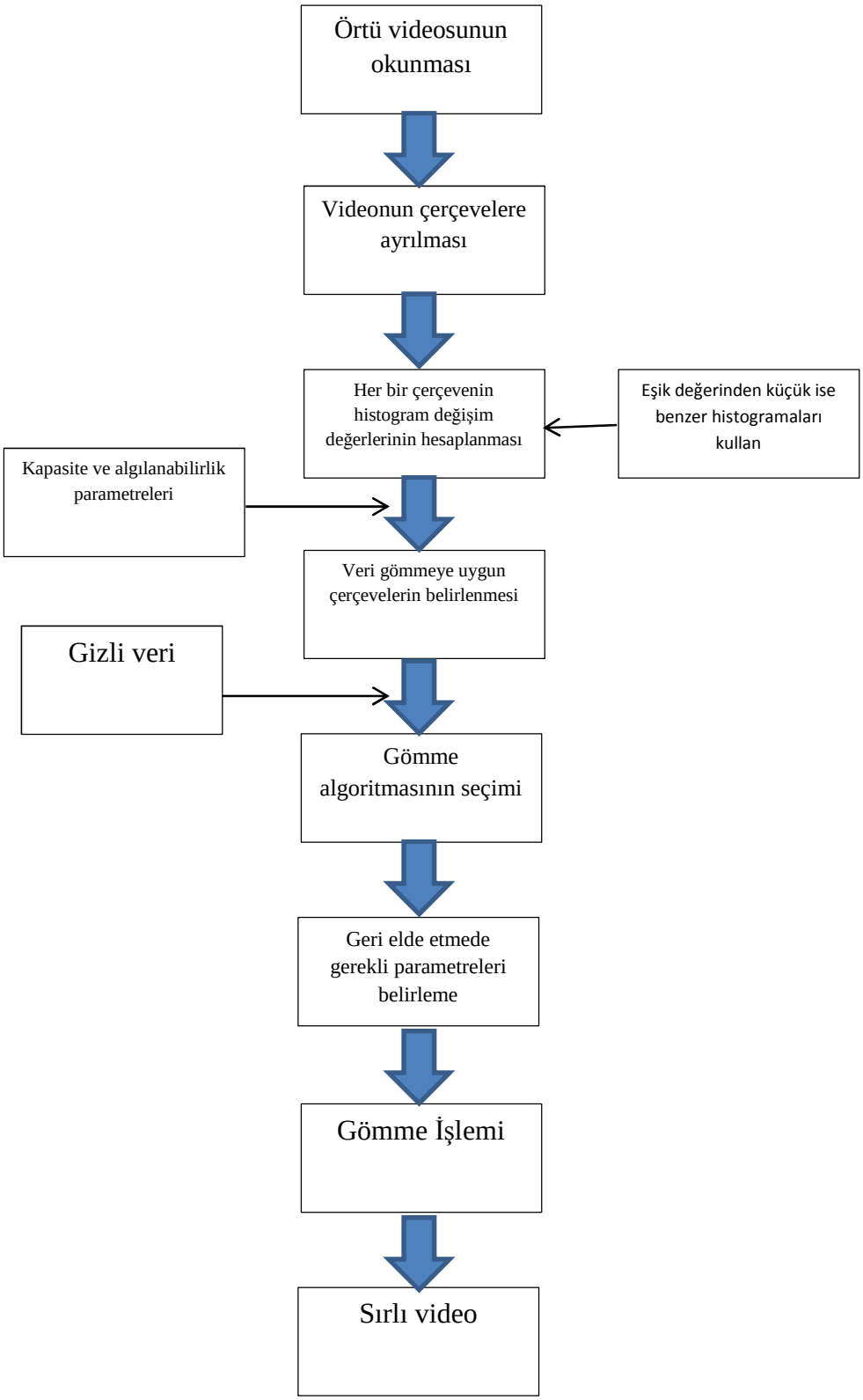
a) Çerçeve tabanlı yöntemde; videoyu oluşturan her bir çerçeve bir bütün olarak ele alınır ve bu çerçeveyi oluşturan pikseller ayrı ayrı incelenerek veri gömmeye uygun olan alanlar bulunur.

b) Blok tabanlı yöntemde; videoyu oluşturan her bir çerçeve belli ölçüler çevresinde küçük bloklara ayrılır. Ardışıl çerçevelerde bulunan birbirine denk düşen bloklar karşılaştırılır ve buna göre veri gömülecek olan alan seçilir.

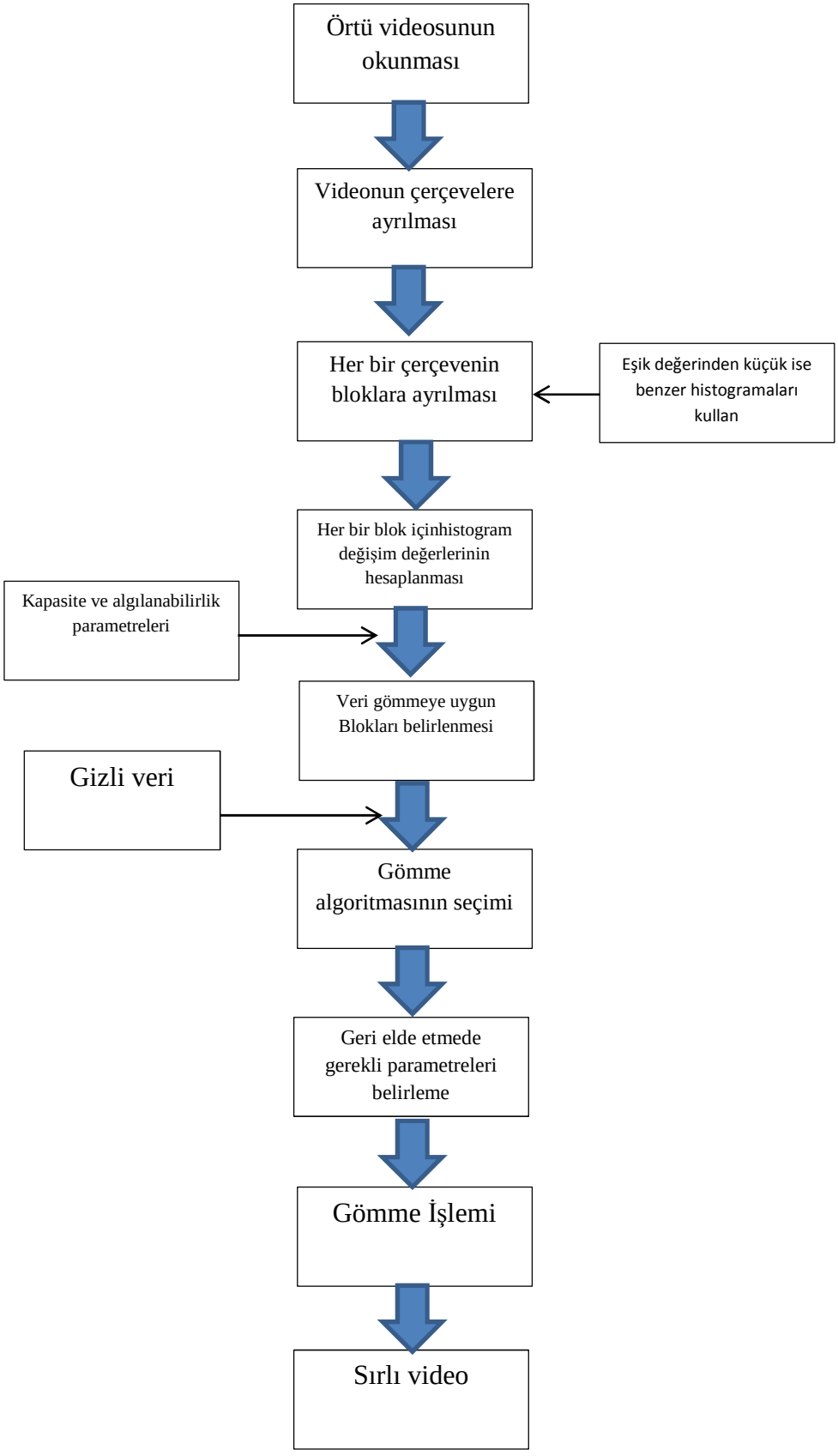
4.3.2.1.1. Benzer histogramlar yöntemi

Çerçeve tabanlı benzer histogramlar yöntemi ile veri gömme amaçlanmış ise, ardışık video çerçevelerinin histogram değerlerinin birbirleriyle karşılaştırılmaları ile renk ve hareket bakımından fazla farkların olmadığı çerçeveler belirlenir.

Video, kendini oluşturan çerçevelere ayrıldıktan sonra çerçeveyi oluşturan piksellerin tek tek histogram değerleri hesaplanır. Bu işlem ardışık çerçevelerin tüm pikselleri için ayrı ayrı yapılır. Ardından birbirini takip eden çerçeveler arasındaki pikseller karşılaştırılır. Histogram farkları elde edilir. Bu farklar kullanıcı tarafından girilen eşik değerle karşılaştırılır. Eşik değerinden küçük histogramlar seçilirse benzer histogramlar yöntemi ile veri gömme yapmış olunur. Yani Benzer Histogramlar yöntemi seçilmiş ise Şekil 4.5' deki resimlerden 1. kare ve 2. kare arasındaki benzerlikten yararlanarak değişme az olan ya da hiç olmayan piksellere rahatlıkla veri gömme işlemi gerçekleştirebiliriz. Benzer Histogramlar yöntemi ile veri gömme işlemi yapılacak ise durağan, fazla değişken olmayan alanlar tercih edilir. Bu da bir resim içerisinde genellikle arkaplan resmi, dekorlar, dağ, tepe vb. hareket etmeyen cisimler tercih edilir. Fakat bunun da bir zayıf tarafı vardır: Durağan cisimlerde değişikliğin insan göz sistemi tarafından hemen algılanabilir olmasıdır. Bu zayıflığı gidermek için ise Blok Tabanlı Benzer Histogramlar (BTBH) yöntemi seçilir. BTBH yöntemi ile hareketli cisimler bloklara ayırılır ve benzer bloklara veri gömme işlemi gerçekleştirilir.



Şekil 4.6. Benzer Histogram Yöntemi Akış Diyagramı



Şekil 4.7. Blok Tabanlı Benzer Histogramlar Yöntemi Akış Diyagramı.

4.4. Video Ortamında Veri Kodlama Yöntemleri

Örtü dosyasının türüne, kapasitesine vb. özelliklerine göre uygun veri kodlama teknikleri geliştirilmiştir. Çalışmamızda geliştirilen veri kodlama yöntemi RGB ağırlıklı kodlamadır. Detaylı bilgi aşağıdaki kısımlarda verilmiştir.

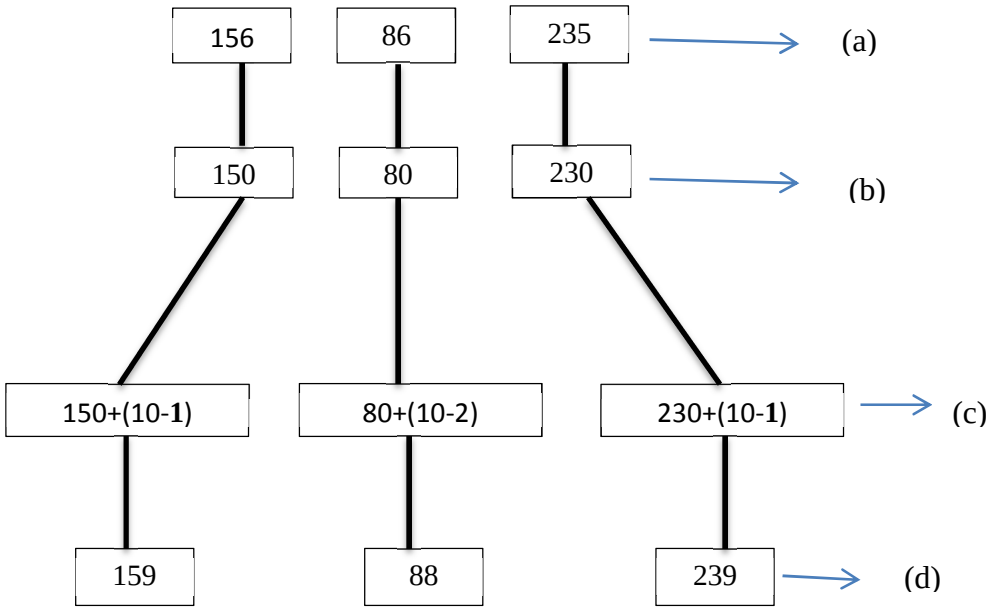
4.4.1. RGB ağırlıklı kodlama yöntemleri

Veri gizleme işlemi sırasında orijinal videoda en az bozulmayla ve en yüksek veri gömme kapasitesine erişmek temel amaçların başında gelir. Bu amaçla tasarlanan birçok veri kodlama yöntemi bulunmaktadır. Bu konuda ise çalışmamızda geliştirmiş olduğumuz yöntem olan RGB hakkında detaylı bilgi sunulmuştur.

Videolar çerçevelerden, çerçevelerde piksellerden oluşmaktadır. Bu aşamada mevcut veri gömmeye uygun olan piksellerin belirlenmesinden sonra bu piksellere veri gömme işlemini gerçekleştirmek gerekecektir. Her piksel RGB olarak bilinen üç rengin bileşiminden oluşmaktadır. R; resimdeki kırmızı rengin tonlarını, G; resimdeki yeşil rengin tonlarını, B; resimdeki mavi rengin tonlarını temsil etmektedir. Bu üç renk değerinin farklı değerlerde birleşmesiyle diğer renk tonları oluşmaktadır. Örneğin RGB değeri, (255,255,0) olan renk sarı renk, (255,127,0) olan renk ise turuncu renktir.

RGB değerleri için; R=156, G=86, B=235 rengine sahip olan piksele “y” harfini gömmek istersek; Öncelikle “y” harfini ASCII kod değerine çevirmemiz gereklidir. “y” harfinin ASCII kodu ‘121’dir. R=156, G=86, B=235 gömülen bilginin yeniden elde edilmesi aşamasında sorun yaşamamak için son rakamlar sıfırlanır. Buna göre elimizde R=150, G=80, B=230 değerleri oluşur. Bir sonraki aşama ise “y” harfinin ASCII kodunun her bir rakamı ‘10’ sayısından çıkarılır (10-1=9, 10-2=8, 10-1=9). Elde edilen bu rakamlar her bir RGB değerlerinin son basamağına yerleştirilir. Bu yüzden RGB’nin rakamlarına bakıldığında anlamlı bir değişikliğin olduğu anlaşılmaması için, gizlenecek bilginin ASCII kodunun her bir rakamı ‘10’

sayısından çıkarılır. Son aşamada ise R=150+9=159, G=80+8=88, B=230+9=239 değerleri elde edilir. Böylelikle gizlenecek olan veri örtü dosyasının uygun pikseline gömülmüş olur. Gizli verinin çıkarılması evresinde ise yapılan işlemlerin sağlaması yapılır. Yani pikselin RGB değerleri alınır (159, 88, 239). Son basamaklarındaki sayıları ‘10’’dan çıkarılır. (10-9=1, 10-8=2, 10-9=1). Böylece “y” harfinin tekrar ASCII kod karşılığını bulmuş oluruz.



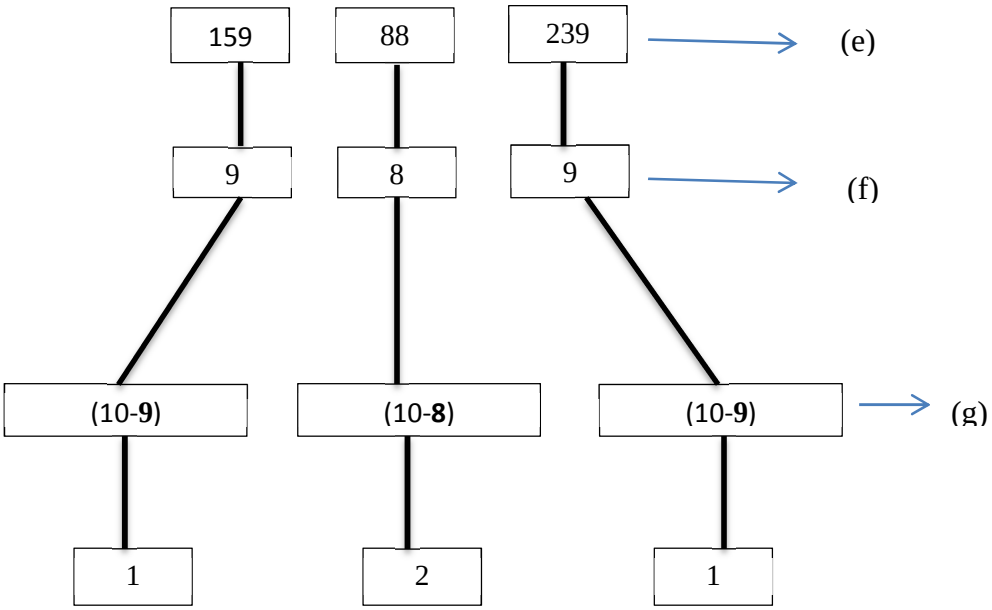
Şekil 4.8. RGB veri kodlama yöntemi ile veri gömme işlemi.

a) orijinal piksel ağırlığı,

b) RGB son rakamlarının sıfırlanması,

c) “y” kodunun gömülmesi,

d) Elde edilen yeni RGB ağırlıklı piksel



Şekil 4.9. RGB veri kodlama yöntemi ile veri geri elde etme işlemi.

e) Kodlu RGB ağırlıklı,

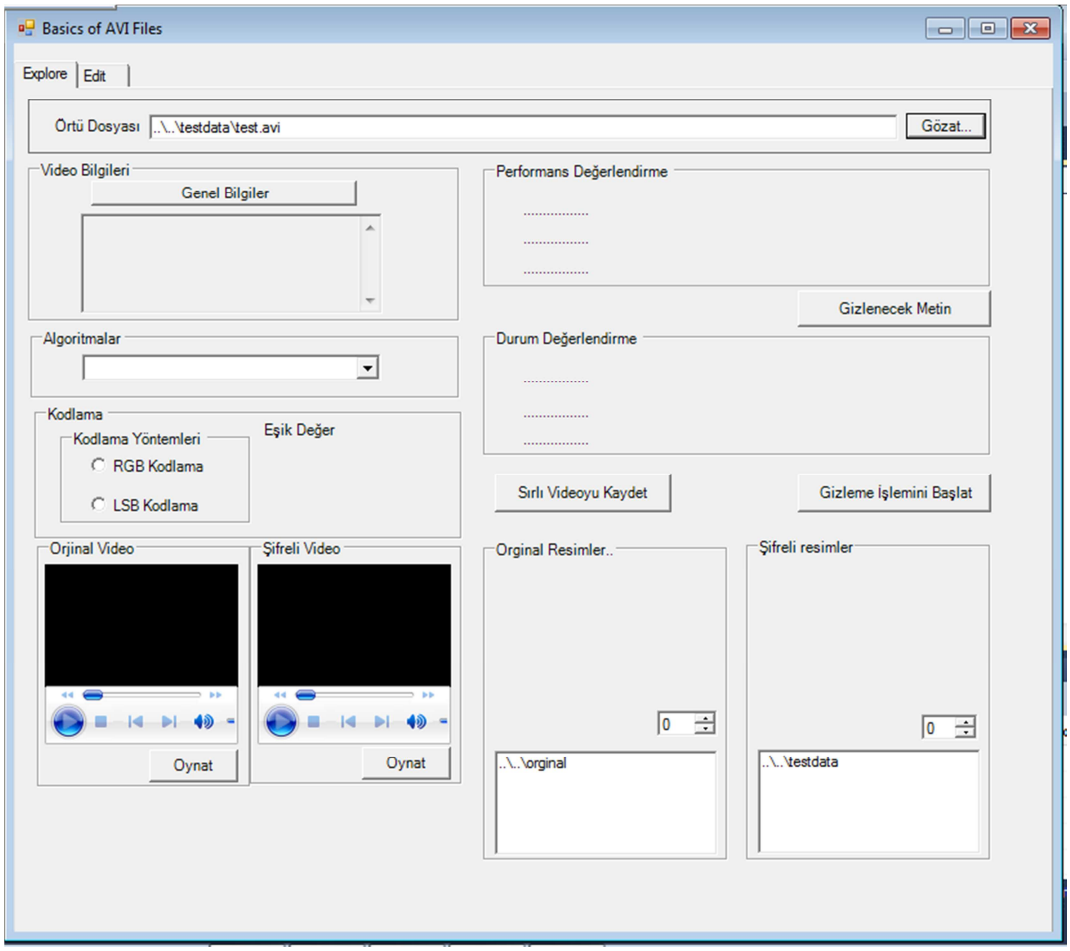
f) RGB son rakamlarının alınması,

g) “y” gömülü karakterin elde edilmesi.

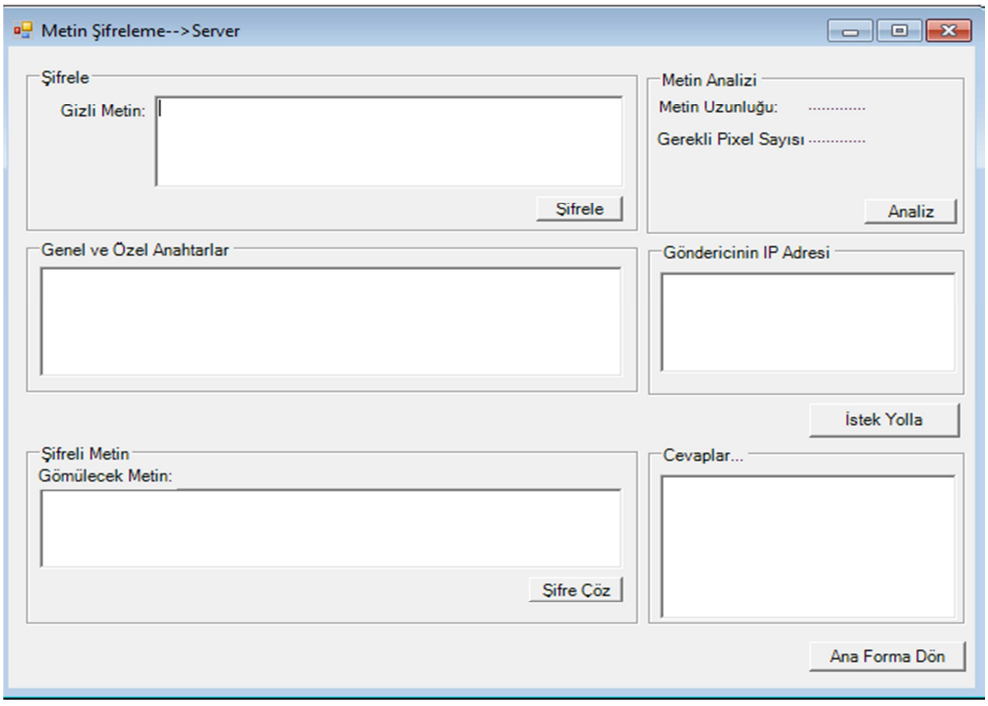
4.5. Uygulama Yazılımının Tanıtılması

Uygulama Microsoft Visual Studio 2010 sürümü kullanılarak tasarlanmıştır. Tasarlanan sistem için 1500 yakın satır kod yazılmıştır. Yazılım fazla yer kaplamaması sayesinde oldukça kullanışlıdır. Veri şifrelemek için RSA algoritması kullanılmıştır. Bu algoritmanın en ideal bir biçimde kullanılabilmesi için iki bilgisayar arasında kablosuz iletişim kurulmuştur. İki bilgisayar Internet üzerinden IP adresleri aracılıyla birbirine bağlanmıştır. Kablosuz haberleşme için fazladan bir donanım vb. devre elemanı kullanılmamıştır. Veriyi örtü dosyasının içerisine gömebilmek için histogram yöntemi ile algoritma tasarlanmıştır. Geliştirilen algoritmaları daha önceki konularda ayrıntılı bir şekilde sunulmuş olduğundan bu

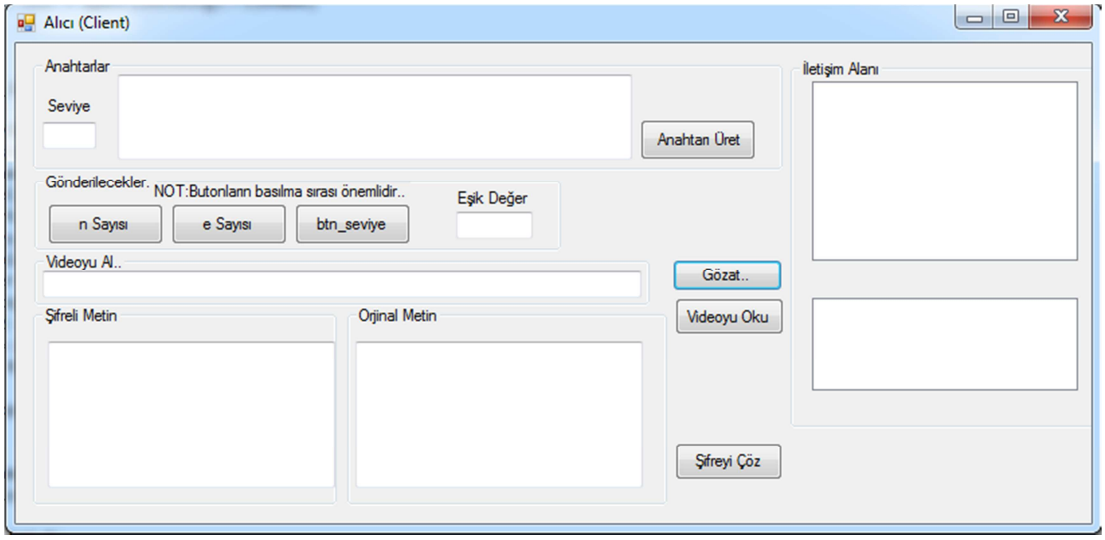
bölümde iki bilgisayar arasında kablosuz bağlantı kurma, veriyi şifreleme, şifreli veriyi örtü dosyası olan videoya gömme, sırlı videoyu alıcı tarafa gönderme, sırlı videonun alınması ve okunması, şifreli verinin elde edilmesi ve son olarak da şifrenin çözülerek orijinal mesajın elde edilmesi anlatılacaktır. Şekil 4.10'da verinin gizlenmesi, verinin şifreleme ve verinin geri elde edilmesini sağlayan yazılımların ana pencereleri görülmektedir.



(a)



(b)



(c)

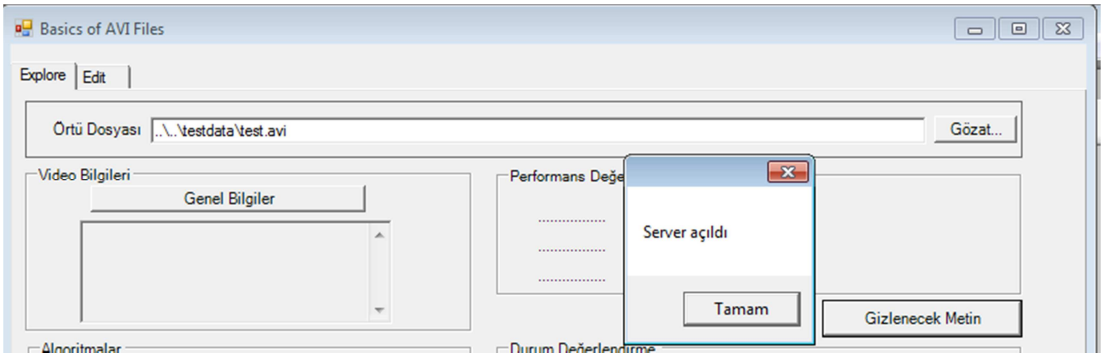
Şekil 4.10. (a).Veri gizleme uygulama yazılımının ana pencere

(b).Gizli veriyi şifreleme uygulama yazılımının ana penceresi.

(c).Verinin elde edilmesi ve şifre çözümü yazılımının ana penceresi.

4.5.1.Verinin şifrelenmesi

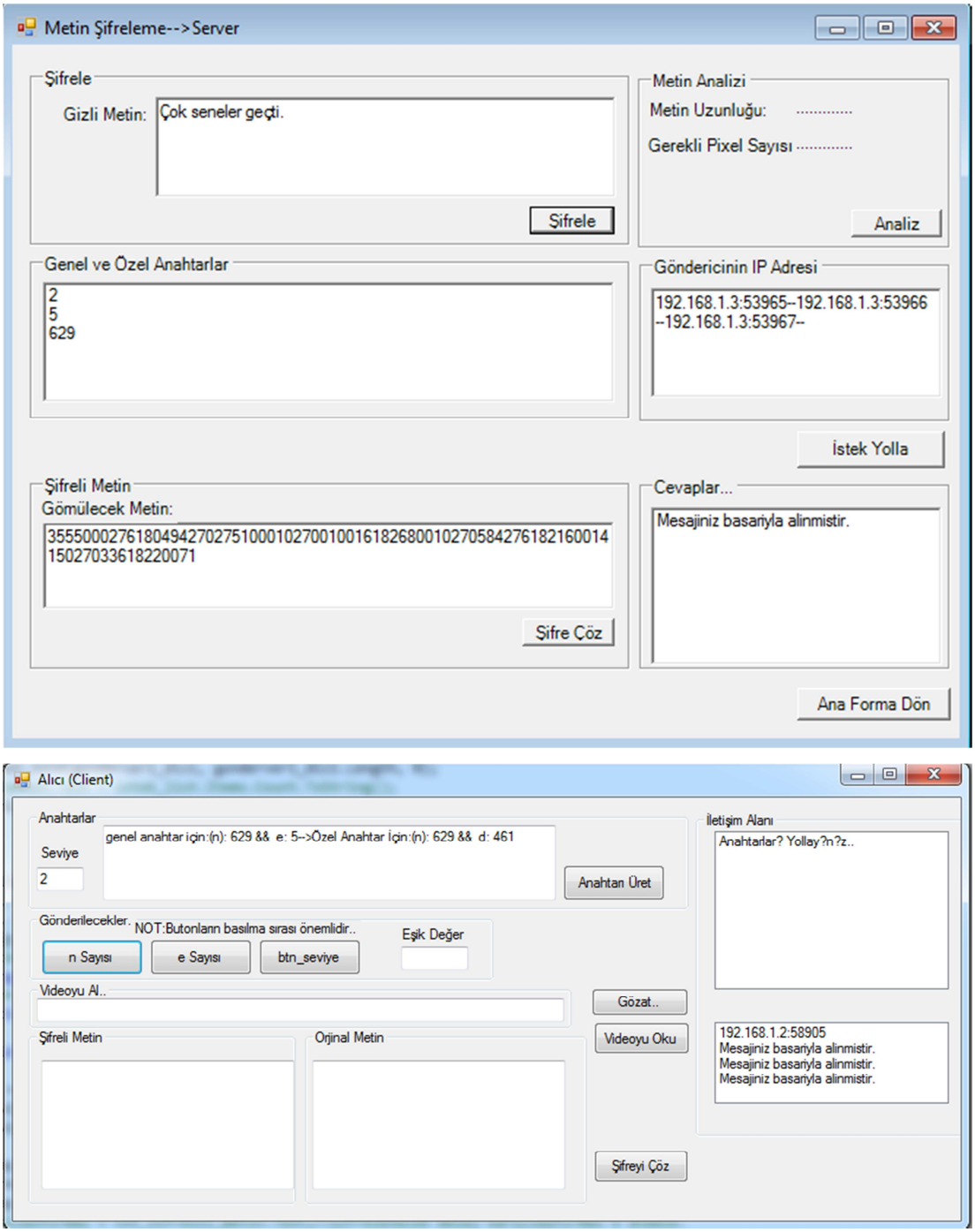
Veri gizlemek için tasarlanan ana pencerede bulunan “Gizlenecek metin” butonuna tıklandığında önce “server açıldı” diye bir mesaj penceresi açılır. Bu pencere kablosuz bağlantı kurulacak olan server’ın çalışmaya başladığını gösterir. Şekil 4.11’ da bu açılan pencere gösterilmiştir.



Şekil 4.11. Kablosuz bağlantı için server’ın çalışması.

Mesaj kutusunda “tamam” butonu tıklandığında ana server açılmış olur. Bu pencere şifrelenecek olan metnin girildiği bölümdür. Pencere açılır açılmaz diğer bilgisayar ile iletişime geçer. Bunu kod bölümüne girdiğimiz IP adresi yardımıyla yapar. Şifrelemek istediğimiz mesaj girildikten sonra “istek yolla” butonu ile diğer bilgisayardan genel anahtarı yollaması istenir. Eğer istek diğer kullanıcıya doğru bir şekilde gitmiş ise bilgisayardan isteğin alındığına dair doğruluk mesajı yollanır. Ardından genel anahtarın gelmesi beklenir. Gelen genel anahtar aracılıyla mesaj RSA algoritmasına uygun olarak şifrelenir. “Şifrele” butonuna basılarak şifrelenen metin “şifreli metin” alanına yazılır. Ardından “Ana Forma Dön” butonuyla veri gömmek için tasarlanan ana forma dönülür. Dönerken de şifreli metin bir değişkene atanarak ana forma taşınır.

Şekil 4.12’ da bilgisayarlar arasındaki bağlantılar. İstekte bulunması vb. gerçekleşen olaylar gösterilmektedir.



Şekil 4.12. Girilen metnin şifrelenmesi ve bağlantılar.

4.5.2. Verinin gizlenmesi

İletişimin güvenli bir şekilde gerçekleşmesini sağlamak amacıyla tasarlanmış olan sırörtme tekniği haberleşmenin şifrelenmesi ilkesine dayanır. Veriyi gömmek için bir

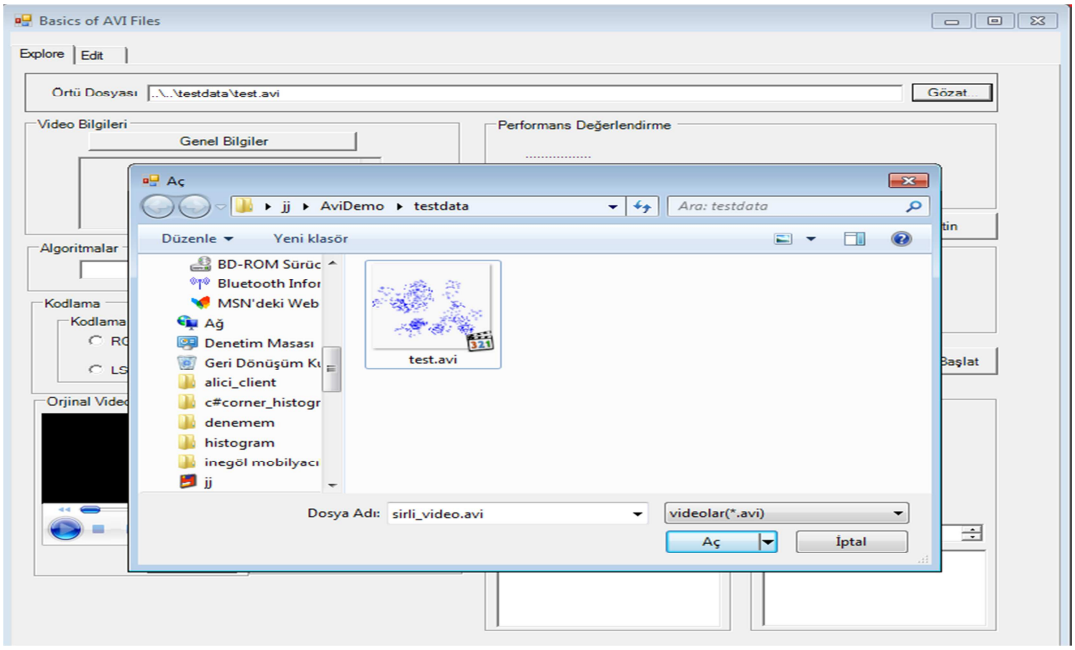
örtü dosyası (video, ses, resim) kullanır. Tez çalışması sürecinde örtü dosyası olarak ".avi" uzantılı 100 x 100 boyutlarında video kullanılmıştır. Gizlemek istenilen mesaj dosyası istenilen uzantıda olabilir. Fakat çalışmamızda sadece metin kutusundaki mesaj gizlenebilmektedir.

4.5.2.1.Histogramlar yöntemi ile veri gizleme uygulaması

Histogram tabanlı veri gömme algoritmaları kullanılırken; seçilen algılanabilirlik (eşik değer) ve gizli verinin boyutuna göre örtü videosunun histogramına dikkat etmek veri gizleme işleminin kazanımını artıracaktır. Histogram tabanlı yöntemler aşağıda listelenmiştir.

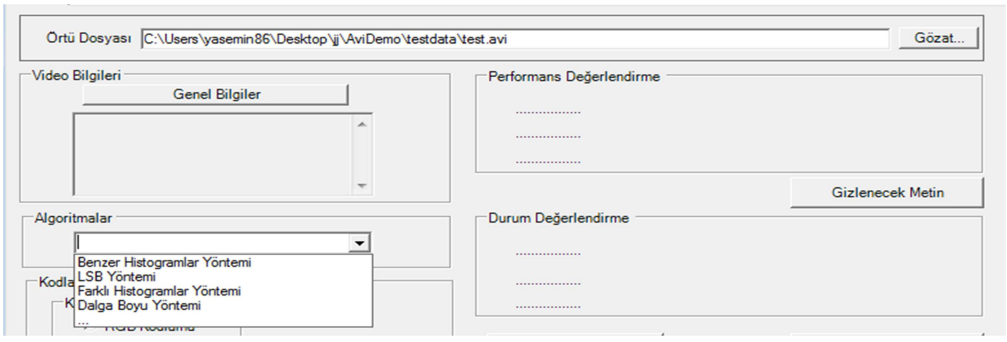
a) Benzer Histogram Yöntemi
b) Blok Tabanlı Benzer Histogram Yöntemi
c) Farklı Histogram Yöntemi
d) Blok Tabanlı Farklı Histogram Yöntemi
e) Bölgesel Histogram Optimizasyon Yöntemi.

Uygulama da veri gömme işlemine başlamadan önce ilk iş olarak örtü dosyasının seçilmesi gereklidir. "Gözat" butonu tıklandığında Şekil 4.13' de görülen iletişim penceresi ekrana gelir.



Şekil 4.13. Gizlenmek istenen şifreli mesaj için örtü dosyasının seçilmesi.

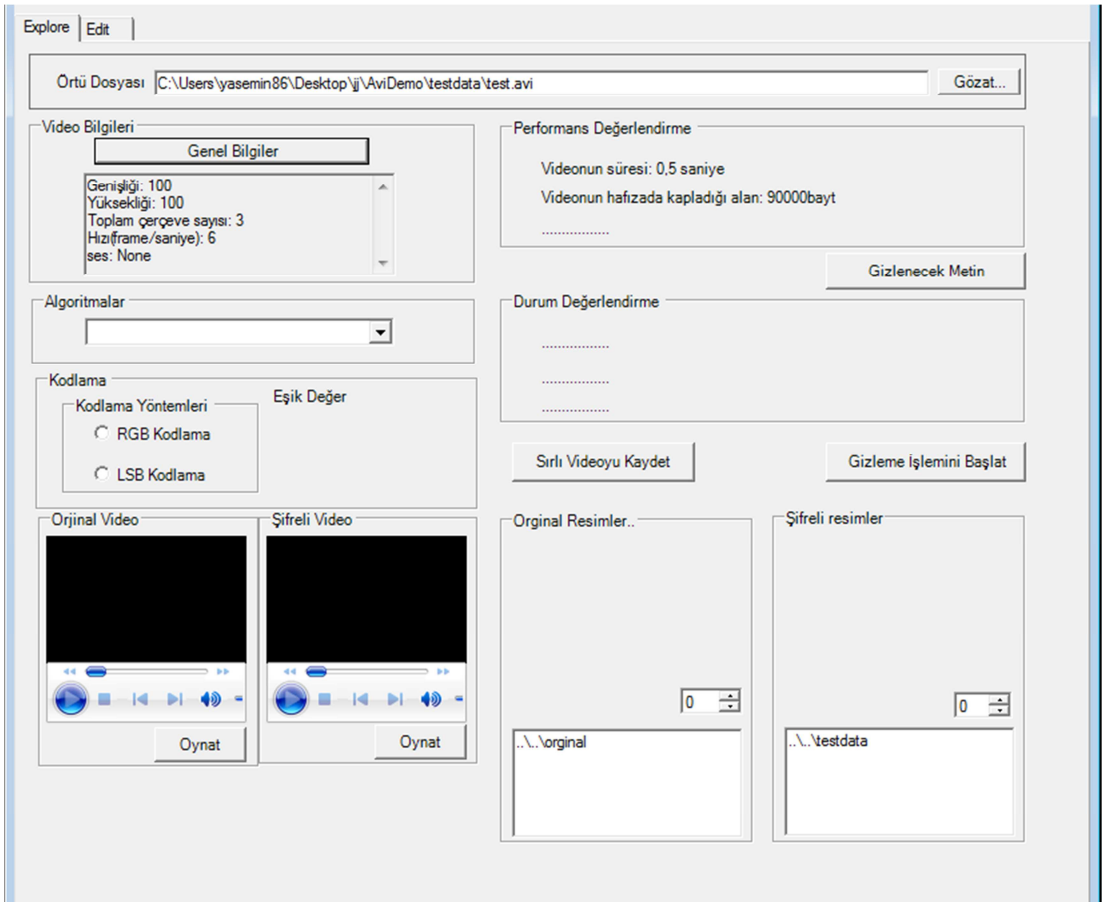
Açılan iletişim penceresi kullanılarak bilgisayarda bulunan ".avi" uzantılı herhangi bir örtü dosyası seçilebilir (bu uygulama için test.avi). Örtü dosyasının seçiminin hemen ardından "Algoritmalar" alanındaki açılır menüden veri gömmede kullanılacak olan algoritma seçilir (Bu uygulama için Benzer Histogramlar Yöntemi). Şekil 4.14 'de görüldüğü gibi açılır menüde işlem yapılabilecek algoritmalar gözükür.



Şekil 4.14. Veriyi gömebilmek için uygun algoritmanın seçimi.

Veri gömebilmek için kullanılacak olan algoritmayı seçtikten sonra, örtü dosyası hakkında bazı istatiksel bilgilerin hesaplanması gerekmektedir. Bunun için "Genel Bilgiler" butonuna tıklanması gereklidir. Tıklandıktan sonra videonun, toplam

çerçeve sayısı, boyu, eni, videoda sesin olup olmadığı, saniyede akan çerçeve sayısı, videonun süresi ve bellekte kapladığı alan vb. bilgiler kullanıcının bilgilendirilmesi amacıyla hesaplanarak ekrana yansıtılır. Şekil 4. 15'de seçilen örtü dosyası hakkında yapılan istatiksel hesaplamaları göstermektedir. Bu hesaplar kullanıcının ne kadar uzunlukta veri gömmesi gerektiği ya da hangi kodlama yöntemini seçmesi gerektiği gibi konularda bilgiler verir.

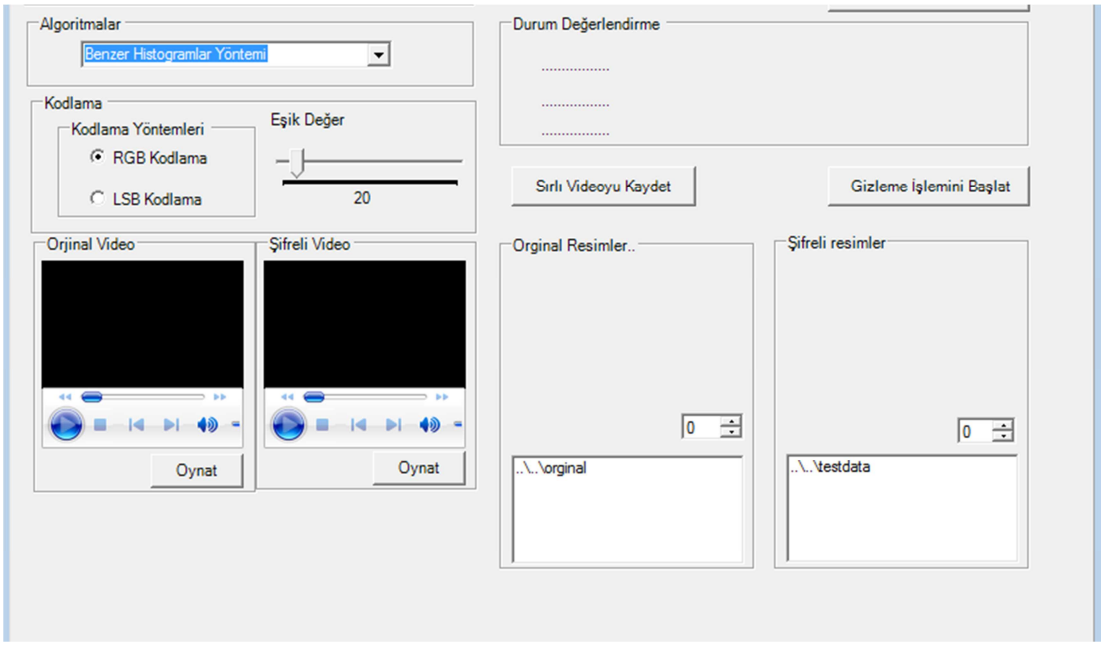


Şekil 4.15. Örtü dosyası hakkında bilgi verilmesi.

Tez çalışmasında örtü dosyası olarak düşük kapasiteli bir video seçilmiştir. Örtü dosyasında toplam üç çerçeve bulunmaktadır. Videoda saniyede altı çerçeve akmakta ve ses bulunmamaktadır. Ayrıca çerçeve bellekte de çok yer kaplamamakta sadece 90000 baytlık alan yeterli olmaktadır.

Tüm bu tercih ve işlemlerin ardından veriyi en uygun kodlamayı yapabilmek için kodlama algoritması seçilmelidir. RGB kodlama, R kodlama veya LSB kodlamalardan herhangi biri tercih edilerek gömme işlemine başlanabilir. Fakat tez

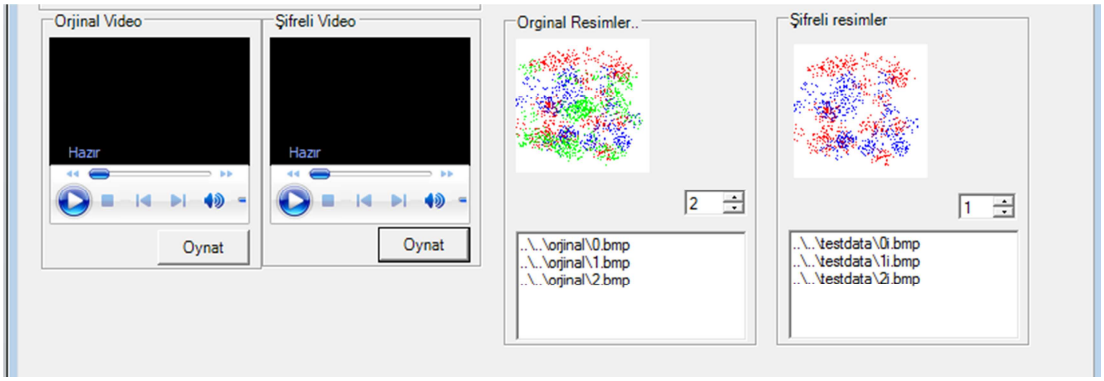
çalışmasında kodlamanın en performanslı bir şekilde yapılabilmesi için RGB algoritması tercih edilmiştir. Şekil 4. 16'da gösterildiği üzere RGB kodlama yönteminin seçilmesiyle eşik değer alanı aktif olmaktadır. Buradan istendiği büyüklükte bir eşik değer seçilerek veri gömme işlemine başlanabilir.



Şekil 4.16. Kodlama yönteminin seçimi ve eşik değerin belirlenmesi.

Bundan sonraki aşama ise Şekil 4. 16' da görüldüğü "Gizleme İşlemini Başlat" butonuna tıklamaktır. İşlem süresi verinin ve örtü dosyasının boyutuna göre değişmektedir. İşlem bittikten sonra işlemin sonlandığını belirten bir yazı çıkacaktır.

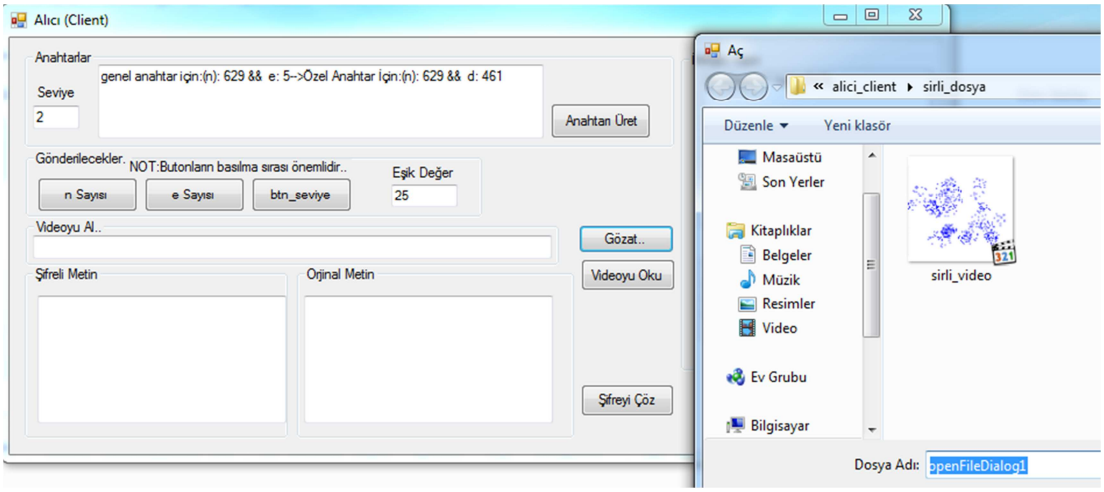
Veri gizleme işleminin sonlanmasında hemen sonra "Sırlı Videoyu Kaydet" butonu ile daha önceden belirttiğimiz dosya içerisine sırlı videoyu "sirli_video.avi" adında kaydeder. Kayıt işlemlerinin bitiminde Şekil 4. 17'de görülen video alanlarından hem sırlı dosya hem de orijinal dosya seyredilebilir. Aynı şekilde Orijinal resimler bölümünden çerçevelerin veri gömülmeden önceki halleri ve şifreli resimler bölümünden ise çerçevelerin veri gömüldükten sonraki halleri numara kutularının sayesinde görülebilir. Bu resim alanlarının altında bulunan metin alanlarında resim dosyalarının bulundukları dosyaların adresleri görülmektedir.



Şekil 4.17. Orijinal dosya ve resimlerin, Veri gömülmüş halleriyle karşılaştırılması.

4.5.3. Sırlı Videodan şifreli mesajın okunması ve şifrenin çözülmesi

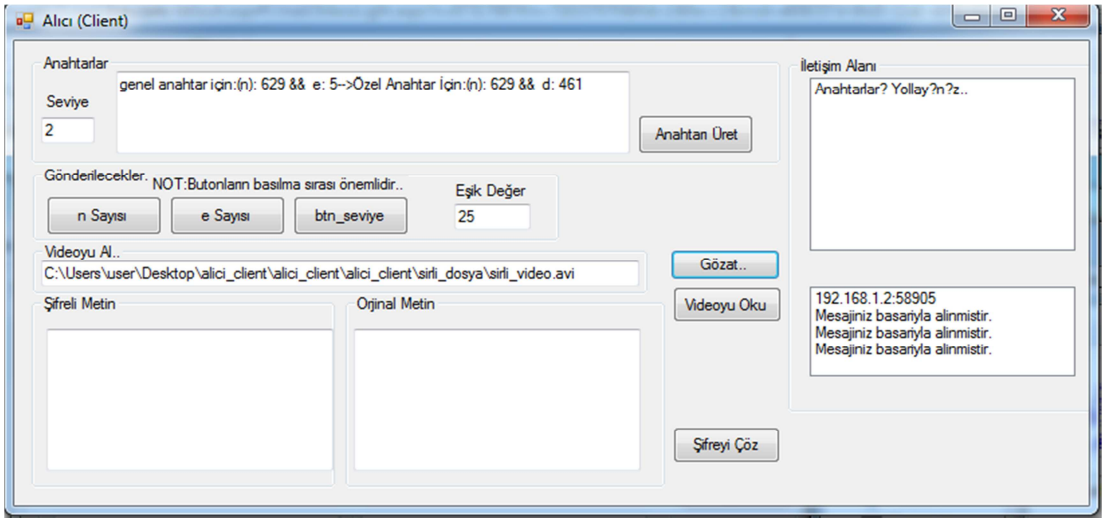
Veri gömme işlemin gerçekleşmesinin ardından sırlı video bir Internet ortamı aracılığıyla alıcı noktaya gönderir. Alıcı bu dosyayı bir web sitesinden, bir sosyal paylaşım ağından ya da video paylaşımı sağlayan herhangi bir alandan elde edebilir. Çalışmamızda sırlı video uygulaması üzerinden alıcı bilgisayara gönderilmektedir. Alıcı nokta sırlı dosyayı aldığında önce videoyu okuyup şifreli mesajı alacak, daha sonra ise şifreyi çözme algoritmasını çalıştırarak şifreyi çözecektir.



Şekil 4.18. Sırlı videonun kaydedilen dosyadan alınması.

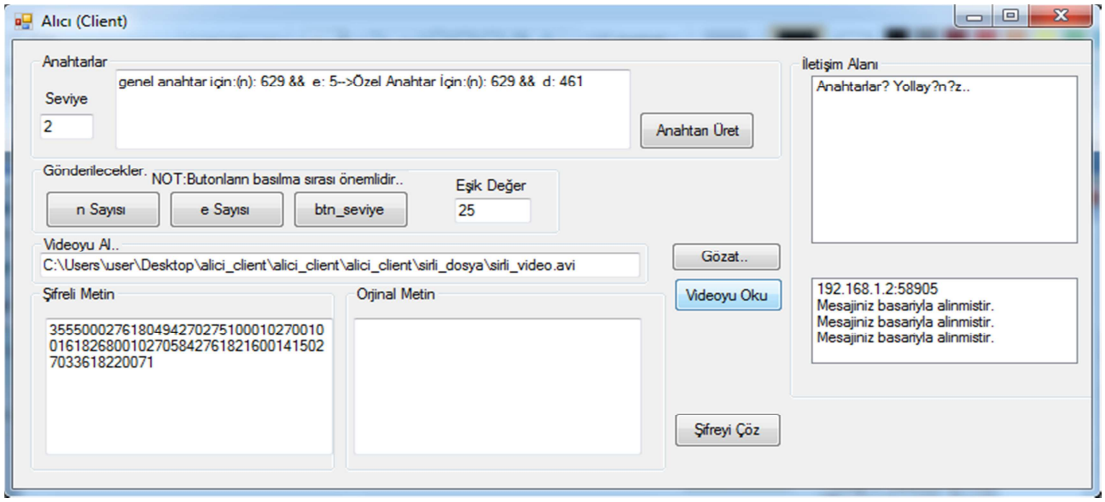
Şekil 4. 18'de görüldüğü üzere veri şifrelenmeden önce göndericinin isteğiyle üretilen genel ve özel anahtarlar hala kullanılmak için aktif durumdadır. Üretilen özel anahtar ilerleyen zamanlar içerisinde şifre çözmek amaçlı kullanılacaktır.

Eşik değer bölümüne şifrelerken seçilmiş olan değer girilir. Girilmez ise veriyi okuma işlemi gerçekleşmez. Daha sonra “gözat” butonu tıklanarak sırlı videonun kaydedildiği yerden alınması sağlanır. “Gözat” butonun hemen yanındaki metin alanına videonun adresi eklenir. Şekil 4. 19 ‘ da gösterilmiştir.



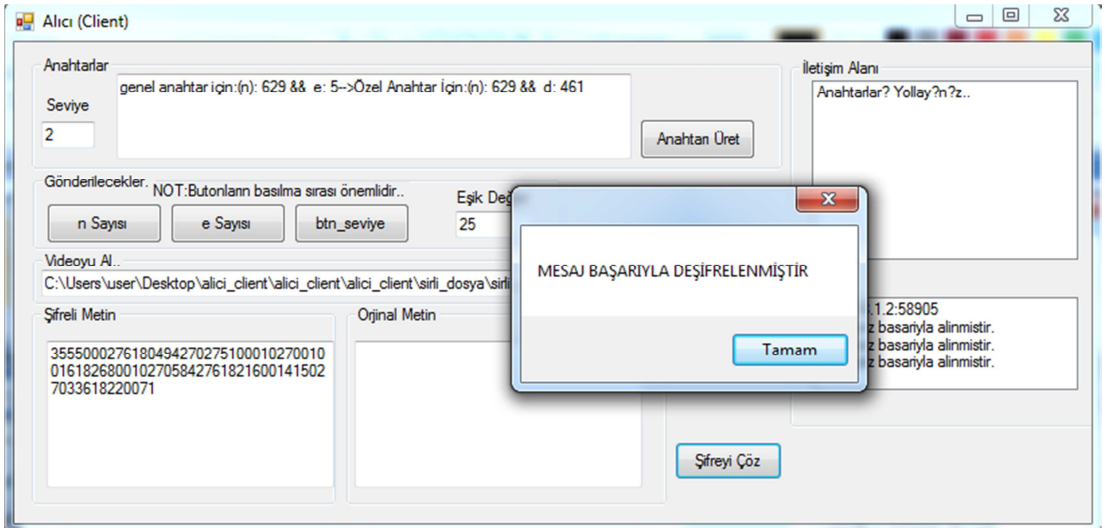
Şekil 4.19. Sırlı videonun adresinin gösterilmesi.

“Video Oku” butonuna basıldığında video çerçevelere ayrılır ve her bir çerçeve için çıkarma algoritması çalıştırılır. Çıkarma algoritması Benzer Histogramlar Yöntemine göre standart olarak tasarlanmıştır. Başlangıç değeri bulunduktan hemen sonra önce veri boyu okunur, ardından veri okunmaya başlar. Okuma işlemi bitince şifreli mesaj “Şifreli metin” alanına yazılır. Burada anlamsız sayılardan oluşan bir metin oluşacaktır. Metin anlamlı hale ancak şifre çözme algoritması çalıştırılınca dönecektir. Şekil 4. 20’de şifreli metin gösterilmektedir.

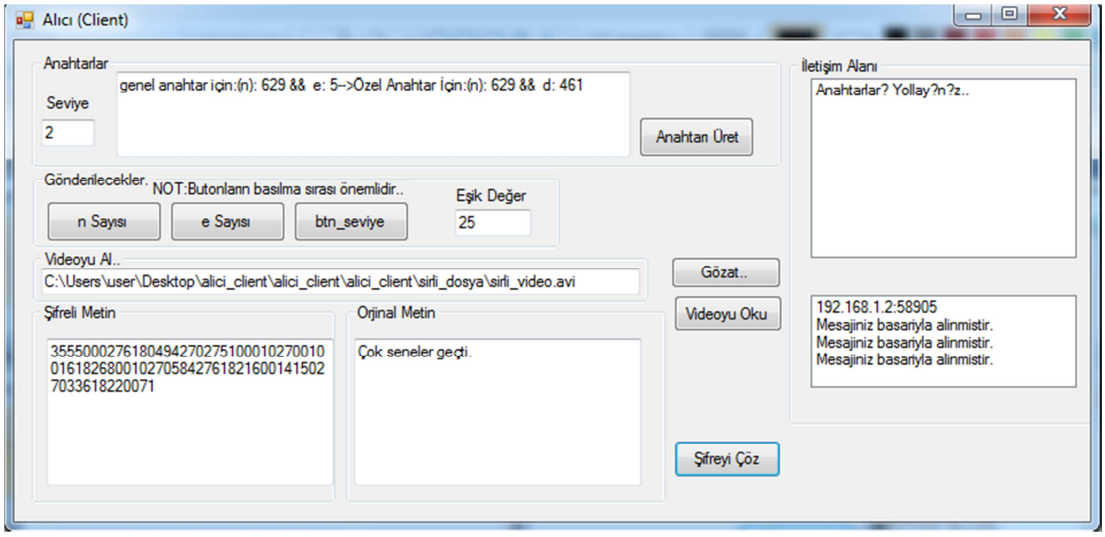


Şekil 4.20. Sırlı videodan okunan şifreli metin.

Şekil 4.22'de görüldüğü üzere "Şifreyi Çöz" butonuna tıklandığında şifre çözme algoritması çalışacaktır. Şifreli metin alanından mesajı alarak şifre çözme algoritması ile orijinal metin elde edilecektir. Eğer şifre doğru bir şekilde çözüldü ise bir mesaj penceresi ile bu mesajın doğru bir şekilde deşifre edildiği belirtilmektedir. Orijinal mesajımız "Çok seneler geçti." İdi. Son olarak algoritmanın doğru işlediğini Şekil 4.22'den görebiliriz.



Şekil 4.21. Şifreli metnin doğru bir şekilde çözülme mesajı.



Şekil 4.22. Orijinal mesaj.

BÖLÜM 5. GELİŞTİRİLEN UYGULAMALARA AİT DENEYSEL SONUÇLARIN DEĞERLENDİRİLMESİ

5.1. Giriş

Bu bölümde, değişik uygulama örnekleri için önerilen sırörtme tekniklerinin kapasite, algılanabilirlik ve gizli veri gömme süreleri gibi kriterlere bağlı başarımları değerlendirilmektedir.

Deneysel çalışmaların değerlendirilmesi aşamasında, sırlı videoların istatiksel kalitelerini ölçmek için Tepe Sinyal Gürültü Oranı (Peak Signal to Noise Ratio-PSNR) kriteri kullanılmıştır. PSNR, orijinal görüntü ile sırlı görüntü arasındaki benzerlik kalitesini hesaplar. Hesaplama sonucunda PSNR tek bir değer üretir. Bu değerin yüksek olması kalitenin de yüksek olduğu anlamına gelir. Aslında PSNR değeri, insan görme sistemi ile birebir uyuşan bir sonuç vermemektedir. Çünkü insanların renkleri ve tonları algılama davranışı tamamen birbirlerinden farklıdır. Bu durum göz önüne alınarak bir başka görsel kalite değerlendirme kıstası olan görsel ölçüm yöntemi de geliştirilen tekniklerin başarım değerlendirmesinde kullanılmıştır.

İki görüntü arasındaki PSNR değerini hesaplamak için öncelikle Ortalama Kare Hatası (Mean Squared Eror- MSE) değeri hesaplanmalıdır[9]. MSE değerinin hesaplanması için Denklem 5.1 kullanılabilir. MSE değerinin hesaplanmasının ardından Denklem 5.2 ‘ye göre PSNR hesaplanır[10,11].

$$MSE = \frac{\sum_{M,N}[I(i,j) - K(i,j)]^2}{MxN} \tag{5.1}$$

Denklem 5.1 ‘de kullanılan I ve K birbiriyle kıyaslanan görüntülerdir. I veri gömülmeden önceki yani orijinal görüntüdür. K ise veri gömüldükten sonraki orijinal görüntüdür. M x N ile temsil edilen ise videonun görüntü boyutlarıdır.

$$PSNR = 10\log_{10}\left(\frac{MAX^2}{MSE}\right) \tag{5.2}$$

Denklem 5.2’de kullanılan MAX görüntüye ait bir pikselin kaç bit ile ifade edildiğini gösterir. Örneğin bir pikseli ifade etmek için 8 bit kullanılıyorsa o zaman MAX 255’tir. Genellikle de işlemlerde sabitliği sağlamak için 255 değeri kullanılır.

Renkli görüntüler de PSNR değerinin hesaplanabilmesi için iki farklı yol kullanılır:

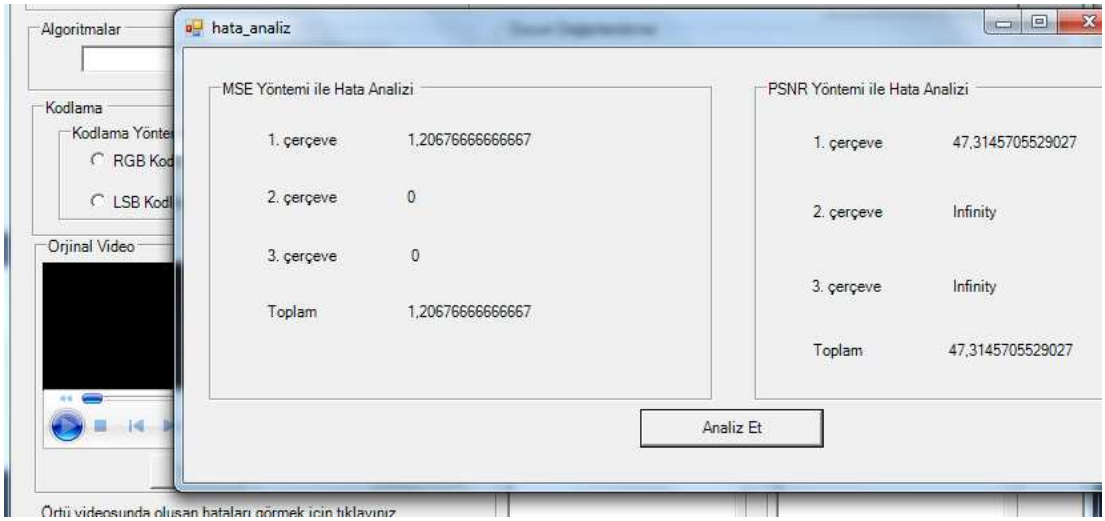
1. Renkli görüntüde renkleri oluşturabilmek için Kırmızı, Yeşil ve Mavi renklerinin farklı değerlerde birleşmesinden meydana gelir. Bu yüzden MSE hesaplanırken, orijinal ve yeniden elde edilmiş görüntülere ait piksellerin farklarının karelerinin boyutlarının üç katına bölünür.

2. Diğer bir yola olarak da renkli görüntünün renk modeli, renk yoğunluğunun ve renk bilgisinin ayrı ayrı ifade edildiği bir başka renk modeline dönüştürülür. Örneğin mevcut görüntünün renk modeli YCbCr renk modeline dönüştürülebilir. Bu dönüşüm sonrasında oluşan renk modelinin yoğunluk bilgisini içeren kısmı ile PSNR değeri hesaplanabilir.

Gizli veride MSE ve PSNR gibi değerlendirme kıstaslarıyla örtü dosyasında oluşun hatalı bitler bulunabilir. İnsan görme sistemi ile algılanabilecek değişiklikler tahmin edilebilir.

5.2. Bozulan piksel sayısı, Kapasite ve Algılanabilirlik Başarımlarının Değerlendirilmesi

Çalışmada orijinal video ve sırlı video arasında değerlendirme yapılmıştır. Farklı uzunlukta ve farklı veri boylarında değerlendirmeler yapılmıştır. Her seferinde hatalı bit sayıları hesaplanmıştır. Orijinal video ile sırlı video arasında gözle görülebilecek hiçbir fark oluşmamıştır. Tablo 5.1 'de yapılan çalışmalar ve sonuçları gösterilmiştir. Bu değerlendirme işlemini yapabilmek için veri gömme ana penceresine bazı ekler yapılmıştır. Şekil 5.1 'de bu değişiklikler görülmektedir.



Şekil 5.1. Hata Analizi.

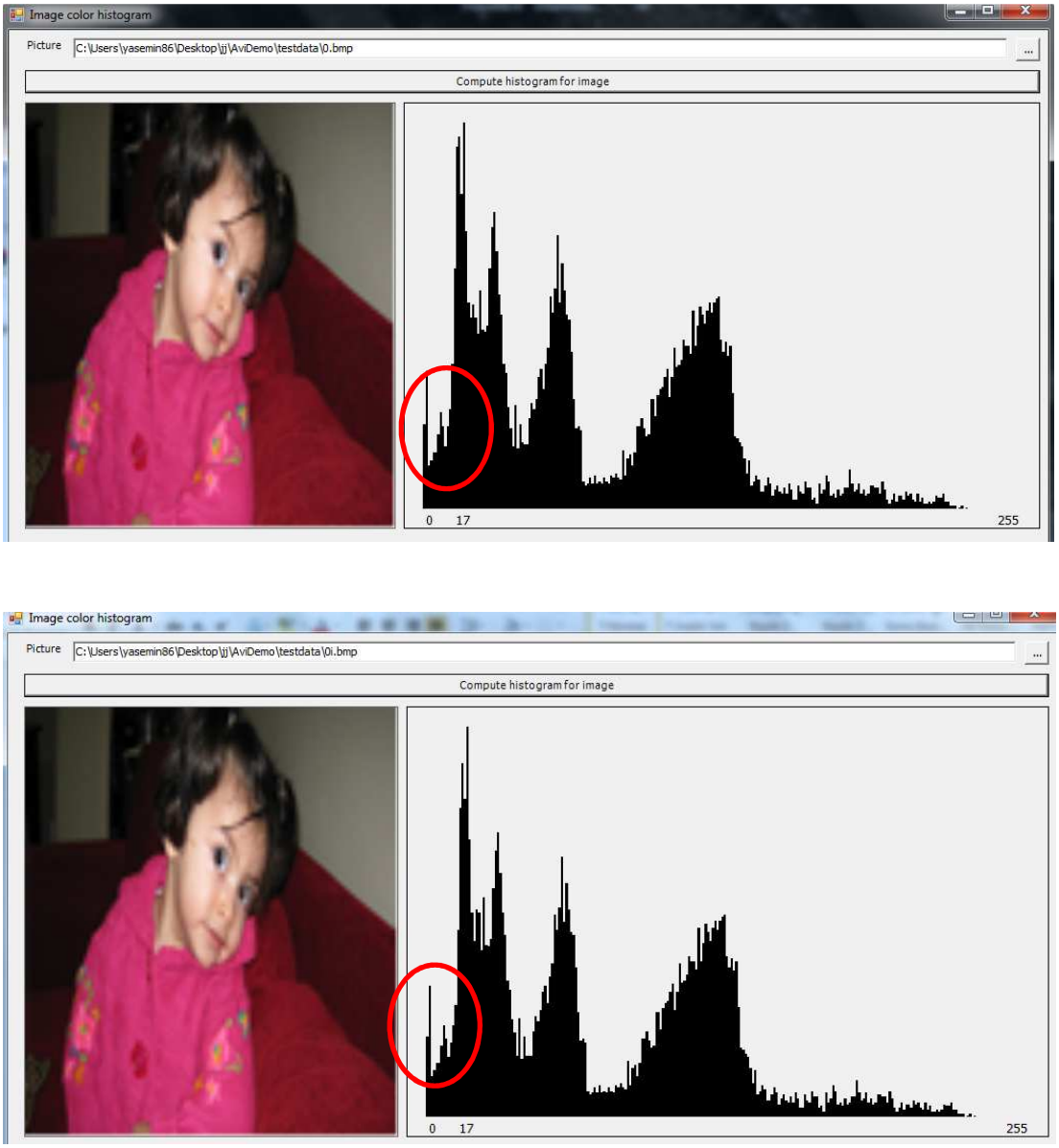
Tablo 5.1. Elde edilen sırlı görüntüler için hesaplanan görüntü kalite ölçütleri

Video boyutu (bayt)	Veri boyutu (bayt)	MSE	PSNR
90000	12.711	3.08796	43,234077
90000	16.384	10.2063	38.04212
90000	20.455	14.244	36.011

Tablo 5.1 'de görüldüğü üzere videonun boyutunun ya da süresinin artması, verinin uzunluğunun artması MSE ve PSNR etkilemiştir. Orijinal video ile sırlı video

arasında gözle görülebilir bir fark olmamasına rağmen bozulan bitleri bulunmaktadır. Bu da RGB kodlama tekniğinin üstün yönlerinden bir tanesini göstermektedir.

Şekil 5.2 ‘de orijinal görüntü ile veri gömülmüş iki görüntünün değişen Histogram değerleri gösterilmiştir.



Şekil 5.2. Orijinal görüntü ve sırlı görüntü arasındaki Histogram farkının gösterilmesi.

Şekil 5.2’de görüldüğü gibi orijinal görüntü ve sırlı görüntünün histogram değerleri yanlarında verilmiştir. Daire içine alınmış olan alanda çok az bir farkın olduğu biraz dikkatli bakıldığında anlaşılmaktadır. Görüntülerde ise insan görme sisteminin algılayabileceği bir fark olmadığı görülmektedir.

Tablo 5.2. RGB kodlama ve değişen piksel sayısı.

	Değişen Piksel Sayısı
Gizli dosya boyutu	RGB kodlama
54(bayt)	54 piksel

RGB kodlama ile değişen piksel sayısını gösterilmiştir. Değişen piksel sayısı LSB kodlama tekniğine göre daha azdır.

5.3. Görsel Algılanabilirlik Başarım Değerlendirilmesi

Geliştirilen yöntemin görsel algılanabilirliğini ölçmek amacıyla, bu yöntemle içerisine veri gömülmüş olan sırlı videolar bir grup izleyiciye seyrettirildi. Grubun yaş aralığı 20 ile 35 arasında değişmektedir. Video izleyicilere aydınlık ortamda, 1 metre mesafe ile 15.4 inch ekran büyüklüğünde ve 1366 x 768 ekran çözünürlüğünde izletildi. Hem orijinal hem de sırlı videolar aynı anda seyrettirildikten sonra onlar arasında fark olup olmadığı soruldu. İlk izlemeden sonra hiç kimse farkları algılayamadı ve iki video da aynı diye yanıt verildi. Ardından ikinci, üçüncü ve dördüncü izlemeden sonra videoları seyreden 12 kişi arasından sadece 2 kişi çok küçük farklar olabilir diye yanıt verdi. On iki kişiden sadece ikisi izledikleri videoların aynı olduklarından emin olamadılar. Bu da geliştirilen yöntemle veri gömmenin gayet güvenli ve farklılıkların algılanabilirliği düşük olduğunu gösterir.

5.4. Sonuç

Bu tez çalışmasında gönderilecek olan mesajın dışarıdan gelebilecek saldırılara karşı korunması amacıyla şifreleme ve veri kodlama yöntemleri geliştirilmiştir. Amaç yetkisiz kişilerin mesaja ulaşamaması, ulaşsa dahi şifreli metni çözememesini sağlamaktır. Bunu yaparken de şifrelemede kullanılan anahtarların gizliliğini maksimum seviyede tutulması, gizli verinin algılanabilirliğini en düşük seviyede tutulması ve gizli veri kapasitesinin en yüksek olması hedeflenmiştir.

Yapılan deney sonuçlarından ve PSNR sonuçlarından anlaşıldığı üzere, veri şifrelemede en iyi yöntemlerden biri RSA'dır. Şifrelenme mantığı, şifrelemek için izlenen yolun geri dönüş şekli yani sağlamasının olmamasıdır.

Benzer histogramlar yönteminin algılanabilirliğinin en düşük olmasa da yine de iyi sayılabileceği ve veri gizleme kapasitesinin yüksek olduğu görülmüştür.

5.5. TARTIŞMA VE DEĞERLENDİRMELER

Güvenli iletişimin zorlaştığı haberleşme ortamlarında daha güvenli bir iletişim kurulabilmesi için insan görme sisteminin çalışma mekanizmasına uygun sayısal video içerisine şifrelenmiş dosya gömme ve çıkarma algoritmaları ile bu algoritmaların uygulanabilmesini sağlayan arayüzlerin geliştirildiği bu tez çalışması kapsamında elde edilen sonuçlar ışığında, konuya ilgi duyan araştırmacılara ve bilim camiasına aşağıdaki öneri/tartışma ve değerlendirmelerin sunulması uygun görülmektedir.

1. Uygulamalar yapılırken haberleşmede kullanılacak olan bilgisayarlar arasındaki bağlantı Internet üzerinden sağlanmaktadır. Bağlantı sorunsuz bir şekilde kurulurken veri gönderiminde bazı sorunlar oluşmaktadır. Bu sorunları ortadan kaldırabilmek için yeni algoritmalar tasarlanabilir.
2. Uygulamalar yapılırken RF etkisinin söz konusu olduğu ortamlarda videoda bazı bozulmalar meydana geldiği gözlemlenmiştir. Bu bozulmaların en aza indirgenmesi için çeşitli algoritmalar geliştirilebilir.
3. Bilgi gizlemek için uygun piksellerin seçilmesi evresinde kullanılmak üzere tasarlanan histogram tabanlı sırörtme yönteminde, veri gömmeye uygun piksellerin belirlenmesi için literatürde K-means clustering olarak bilinen sınıflandırma metodundan faydalanılabilir. Bu yöntemle renk değerleri birbirine en yakın olan pikselleri belirlenerek veri gömmeye uygun alanlar belirlenebilir.

4. Tez çalışmasında amaç yüksek kapasiteli gizli veri haberleşmesi gerçekleştirmek olduğu için geliştirilen sırörtme yöntemleri ham videolar üzerine tasarlanmıştır. Tasarlanan algoritmalar üzerinde fazla bir değişikliğe gerek kalmadan küçük değişiklerle sıkıştırılmış videolar üzerine de rahatlıkla uygulanabilir.
5. Gömü dosyasının gömülmesi ve gönderilme süresi, ilgili dosyanın boyutu ile doğru orantılı olarak arttığından gömülecek olan bit sayısını azaltmak için sıkıştırma algoritmalarından faydalanılabilir. Böylelikle sıkıştırılmış büyük boyutlu dosyalarda sadece sırörtüsü uygulanan dosyalara oranla daha hızlı veri gömülümü ve gönderimi gerçekleşebilir.
6. Tasarlanan algoritmalar ve arayüz Microsoft Visual Studio 2010 ortamında tasarlandığı için ortamdan bağımsız çalışabilir. Tasarlanan program rahatlıkla diğer kodlama dillerine de uyarlanabilir.
7. Tasarlanan uygulama sadece o anda yazılan metini şifreleyip video içerisine gömme üzerine çalışılmıştır. Fakat bu tasarı ile .txt, .doc, .bmp vb. uzantılı dosyalar da kod kısmında birkaç değişiklikle rahatlıkla şifrelenerek video içerisine gömülebilir. Bu tez akademik amaçlı olduğu için geliştirilen algoritmaların çalışabilirliğini test etmek amacıyla sadece düz metin üzerine geliştirilmiştir. Diğer uzantıları da aynı işleme tabi tutmak oldukça kolay ve kısa süreli bir çalışma olacaktır.
8. Dosya gönderimi yapılırken gönderilen video verilerini dinleyen yetkisiz kişiler gizlenen veriyi elde edebilmek için şu aşamalardan geçmesi gereklidir.
    a) Yapılan sırörtüsü videosunun hangi gömme ve kodlama algoritmasıyla nasıl yapıldığını bilmeleri gerekir.(RGB, histogramlar yöntemi vb.)
    b) Gönderilen dosya paketinin yapısını(başlat bitleri, uzunluk, veri vb,) bilmeleri gerekir.
    c) Videoyu dinleyen yetkisiz kişilerin elde ettikleri gizli veri şifreli olacağından öncelikle hangi şifreleme yönteminin (RSA) kullanıldığını, şifreyi çözecek olan özel anahtarın ne olduğunu bilmeleri gerekmektedir. Anahtarı bilmeden çeşitli yöntemlerle anahtar üretseler bile çok sayıda anlamlı veri oluşacağı için doğru mesajı tahmin etmeleri gerekmektedir.

d) Tüm yukarıdaki aşamalara sahip olan dışarıdan birinin ancak iki kişi dosya gönderimini başlatır başlatmaz paketleri ele geçirmelidir. Bu paketlerden herhangi birini dinleyemez ise verinin elde edilmesi mümkün olmayabilir.

9. Bilgisayar donanım özellikleri iyileştikçe uygulamanın daha sorunsuz çalıştığı tespit edilmiştir. Gelecekteki donanım birimlerinin çok daha gelişmiş olacağı göz önüne alındığında gömme ve gömülü veriyi elde etme süreleri daha da kısalacaktır.

KAYNAKLAR

[1] ÇETİN Ö., "Hareketli Görüntü Uygulamaları İçin Sırörtme Yaklaşımı ile Veri Gömme Algoritması Tasarımı", Doktora Tezi, Sakarya Üniversitesi 2008

[2] YERLİKAYA T. , BULUŞ E. , ARDA D. , "Asimetrik Kripto Sistemler ve Uygulamaları ", II. Mühendislik Bilimleri Genç Araştırmacılar Kongresi, İstanbul, MBGAK 2005.

[3] KRENN J. R. , "Steganography and Steganalysist," (Erişim Tarihi 2011).

[4] NEDELJKO C. , TAPIK S. , "Incresing the cappacity of LSB based audio steganography" (Erişim Tarihi 2010).

[5] AMIN M. F. , MOHAMMAD R., AKBARZADEH T. , FARSHAD V. A. , "A New Genetic Algorithm Approach for Scure JPEG Stagenography" , 2006.

[6] SHALI M., "Steganography in MMS" , 2007.

[7] GRUHL, D., BENDER, W., LU A., "Echo Hiding" , ISBN 3-540-61996-8, 1996.

[8] KURTULDU Ö.,"İmge Steganografisi İçin Yeni Yöntemler", 2008.

[9] JONATHAN, K. S. ,HARTUNG, F.,GIRID, B., "Digital Watermarking Of Text, Image, And Video Documents Comput. & Graphics", Vol. 22, No. 6, pp. 687±695, Elsevier Science, 1999.

[10] NETRAVALI, A.N., HASKELL, B. G. ,"Digital Pictures: Representation, Compression, and Standards(2nd Ed)," Plenum Press, New York, NY, 1995.

[11] RABBANI, M., JONES, P.W., "Digital Image Compression Techniques", Vol TT7, SPIE Optical Engineering Press, Bellvue, Washington 1991.

[12] HARTUNG, F., GIROD, B., “Digital watermarking of uncompressed and compressed video, Trans. Of Signal Processsing- Sprecial Issue on Copyright protection and Access Control for Multimedia Services”, 66(3):283-301,1998.

[13] KURTULDU Ö., ARICA N., “İmge Kareli Kullanan Yeni Bir Stegnografi Yöntemi”, Vol.5, No.1, pp.67-48(2009)

[14] ŞAHİN A, BULUŞ E, SAKALL T.N., “24-Bit Renkli Resimler Üzerinde En Önemsiz Bite Ekleme Yöntemini Kullanarak Bilgi Gizleme”, Trakya Üniversitesi, Mühendislik Mimarlık Fakültesi, Bilgisayar Mühendisliği Bölümü, EDİRNE (2006)

[15] Ingemear J. COX, LAWRENCEVİLLE, N.J. MATTHEW L. MİLLER, KAZUYOSHİ T., “DIJITAL WATER MARKING”, App1. No.:081746,022, (1996)

[16] BRETT S. , “Dijital Video Processing”, pn:4024179 (2000)

[17] AĞAOĞLU S. , “Sıkıştırılmış Sayısal Görüntü ve Video için Hata Gizleme”, Yüksek Lisans Tezi, Sakarya Üniversitesi , (2005)

[18] AKBAL T. , “Ses Verilerine Sıkıştırılmış ve Şifrelenmiş Ham Verilerin Gömülmesi”, Yüksek Lisans Tezi, Sakarya Üniversitesi, (2008)

[19] ÇİVİCİOĞLU P. , ALÇI N. , “Güvenli İletişim İçin Veri Gizleme Tekniklerinin Kullanımı” , Erciyes Üniversitesi, Erişim Tarihi (2011)

[20] MESUT A. “Veri Sıkıştırmada Yeni Yöntemler”, Doktora Tezi, Trakya Üniversitesi, (2006)

[21] ANIN M. M., İBRAHİM S., SALLEH M., KATMIN N. R., “Infirmation Hiding Using Stegonografphy”, Department Of Computer System & Communication Faculty Of Computer Science and Information System, University Teknology Malansia, 2003

[22] ANDERSON R. J., “On The Limits of Stegonography”, Erişim Tarihi, 2011

[23] ATICI M. A., “Stegonografik Yaklaşımların İncelenmesi, Tasarımı ve Geliştirilmesi”, Yüksek Lisans Tezi, Gazi Üniversitesi, Bilgisayar Mühendisliği, (2007)

[24] RAHMANA B., ELÇİ A., “Güvenli Kimlik Hizmetinde Yeni Bir Yaklaşım”, Bilgisayar Mühendisliği Bölümü ve İnternet Teknolojileri Araştırma Merkezi, Doğu Akdeniz Üniversitesi, Erişim Tarihi 2011

[25] KOK-BENG N., THIA S., “Digital Stegonography for Information Security”, Erişim Tarihi 2010

[26] ELÇİ B., “Stegonografi”, İstanbul Teknik Üniversitesi, Elektronik Mühendisliği, Erişim Tarihi 2011

[27] BHAMMİK A. K., CHOI M., ROBLES R.J., BALITAMAS M. O., “Data Hiding in Viideo”, Heitage Institute of Tecnology, Kalkata-70017, Indıa Hannam Universty Vol.2, No.2, 2009

[28] GUTUB A., AL-QAHTANI A., TABAKH A., “Secure RQB Image Stegonography Based on Randomization”, Computer Engineering Department, KFUPN, Dhahron 31261, Saudi Arabia, Erişim Tarihi 2010

[29] CACHIN C., “An Information-theoritic Model for Stegonography”, IBM Zurich Laboratory, Ctl-8803 Rüschlikon, Switzerland, 2004

[30] CHEN M., AGAIN S.S., CHEN C.L.P., “Generalized Collage Stegonography on Images”, Departmant of Electricaland Computer Engineering The University of Texas, USA, IEE 2008

[31] LU C.-SHEIN, “Multimedia Securty:Stegonography and Digital Watermarking Techniques for Protection of Intellectual Property”, Institute of Information Science Acedemia Sinica, Taiwan, ROC, Erişim Tarihi 2011

[32] CUEJIC N., SEPPANEN T., “Increasing the Capacity of LSB-Based Audio Stegonography”, Media Team Oulu Information Processing Laboratory FIN-90014 University of Oulu, Finland, IEE 2002

[33] ÇAYIRLI M., “Yanma Olayının Modellenmesi ve Görüntü İşleme Yoluyla Yanma Performansının Optimizasyonu”, Yüksek Lisans Tezi, Makine Eğitimi Anabilim Dalı Isparta, 2006

[34] TAŞKIN D., SUÇSUZ N., “Sıkıştırılmış Ortamda Çerçeve Tipine Dayalı Gerçek Zamanlı Sahne Değişimi Belirleme”, Trakya Üniversitesi, Bilgisayar Mühendisliği Bölümü, Erişim Tarihi 2010

[35] ORAL M., “Veri Saklama Yöntemleri: Sayısal Görüntülerin Damgalanması, Amaçları ve Uygulama Alanları”, Elektrik Elektronik Mühendisliği Bölümü, Mustafa Kemal Üniversitesi, Hatay, Çukurova Üniversitesi, Adana, Erişim Tarihi 2011

[36] KAHN D., “The History of Stegonography”, 120 Wooleys Lone Greak Neck, NewYork 11023, Erişim Tarihi 2012

[37] JAHNE B., “Digital İmage Processing”, ISBN 3-540-67754-2, 2002

[38] ARTZ D., “Digital Stegonography: Hiding Data Within Data”, Los National Laboratory, 2001

[39] ERKİN Z., “Bilgisayar Ağlarında Güvenlik”, Bilgisayar Mühendisliği Anabilim Dalı, İstanbul Teknik Üniversitesi, Erişim Tarihi 2012

[40] ERKİN Z., ÖRENCİK B., “Stegonografik Kütüphane”, Bilgisayar Mühendisliği, İstanbul Teknik Üniversitesi, Erişim Tarihi, 2002

[41] PETITCOLAS F.A.P., ANDERSON R.J., KUHN M.G., “Information Hiding-A Survey”, IEE 87(7):1062-1078, 1999

[42] FARD A.M., AKBARZADEH M., VARASTED F., “A New Genetic Algorithm Approach for Secure Jpeg Stegonography”, IEE, 2006

[43] FURAT M., “Sayısal Ortamlarda Veri Damgalanması ve Geri Elde Edilmesi”, Yüksek Lisans Tezi, Mustafa Kemal Üniversitesi, Elektrik-Elektronik Mühendisliği Anabilim Dalı, Antakya, 2006

[44] GONZALEZ R.C., WOODS R.E., “Digital İmage Processing”, ISBN:0-201-18075-8, 2001 (Kitap)

[45] GÜREL H., “Sayısal Resim Üzerine Veri Gizleme Uygulamaları”, Yüksek Lisans Tezi, Elektronik ve Bilgisayar Eğitimi, Kocaeli Üniversitesi, 2006

[46] BULUŞ H.M., “Temel Şifreleme Algoritmaları ve Kriptonalizlerinin İncelenmesi”, Yüksek Lisans Tezi, Trakya Üniversitesi, 2006

[47] HANAFY A.A., SALAMA G.I., MOHASSED Y.Z., “A Secure Convert Communication Model Based on Video Stegonography”, The Military Technical Collegei Egypt. 11331

[48] FARID M., “Dedecting Stegonographic Messages in Digital Images”, Department of Computer Science Dartmouth College, Erişim Tarihi 2012

[49] KHALIL M.I., “Image Stegonography: Hiding Short Audio Messages Within Digital Images”, Reactor Physics Department, Nuclear Research Center, Atomic Energy Authority, Cairo, Egypt Vol. 11 N.2

[50] KURTULDU Ö., “İmge Stegonografisi için Yeni Yöntemler”, Yüksek Lisans Tezi, Gazi Üniversitesi, ANKARA, 2007

[51] ATICI M.A., “Stegonografik Yaklaşımların İncelenmesi, Tasarımı ve Geliştirilmesi”, Yüksek Lisans Tezi, Bilgisayar Mühendisliği, Anabilim Dalı, 2008

[52] DALKILIÇ M., “Cryptography and Network Securiity: Steganography”, Ege Üniversitesi, 2002

[53] AMIN M.M., IBRAHIM S., SALLEH M., KATMIN M.R., “Infırmatıon Hiding Using Steganography”, Universiti Teknolji Malaysia, 2003

[54] OĞUZ C., “Görüntü İşaretleri İçin Yeni Bir sayısal Damgalama Yöntemi”, Elektrik-Elektronik Mühendisliği Anabilim Dalı, İstanbul Üniversitesi, 2006

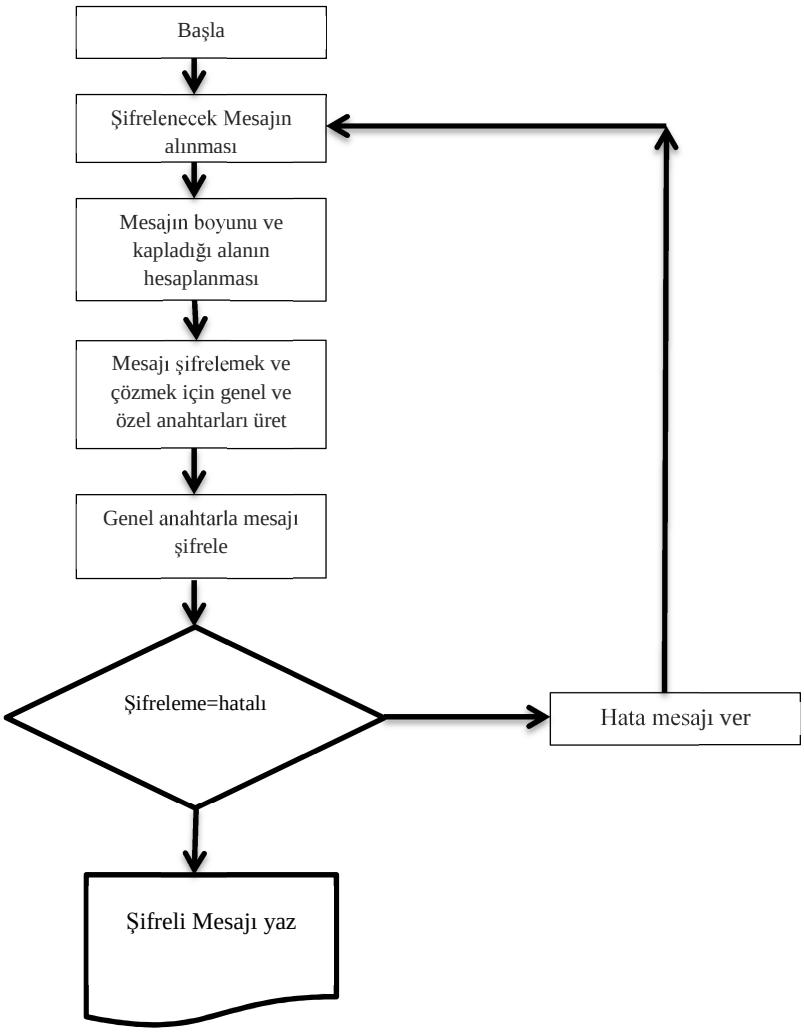
[55] ŞAHİN A., “Görüntü Steganografide Kullanılan Yeni Metodlar ve Bu Metodların Güvenilirlikleri”, Doktora Tezi, Bilgisayar Mühendisliği Anabilim Dalı, Trakya Üniversitei, 2007

[56] AKBAL T., YALMAN Y., ÖZCERİT A.T., ”Gerçek Zamanlı Sayısal Ses İçerisinde Sıkıştırılmış ve Şifrelenmiş Veri Transferi”, Elektrinik ve Bilgisayar Eğitimi Bölümü, Sakarya Üniversitesi, Sakarya, Kocaeli Üniversitesi, Kocaeli, Erişim Tarihi 2011

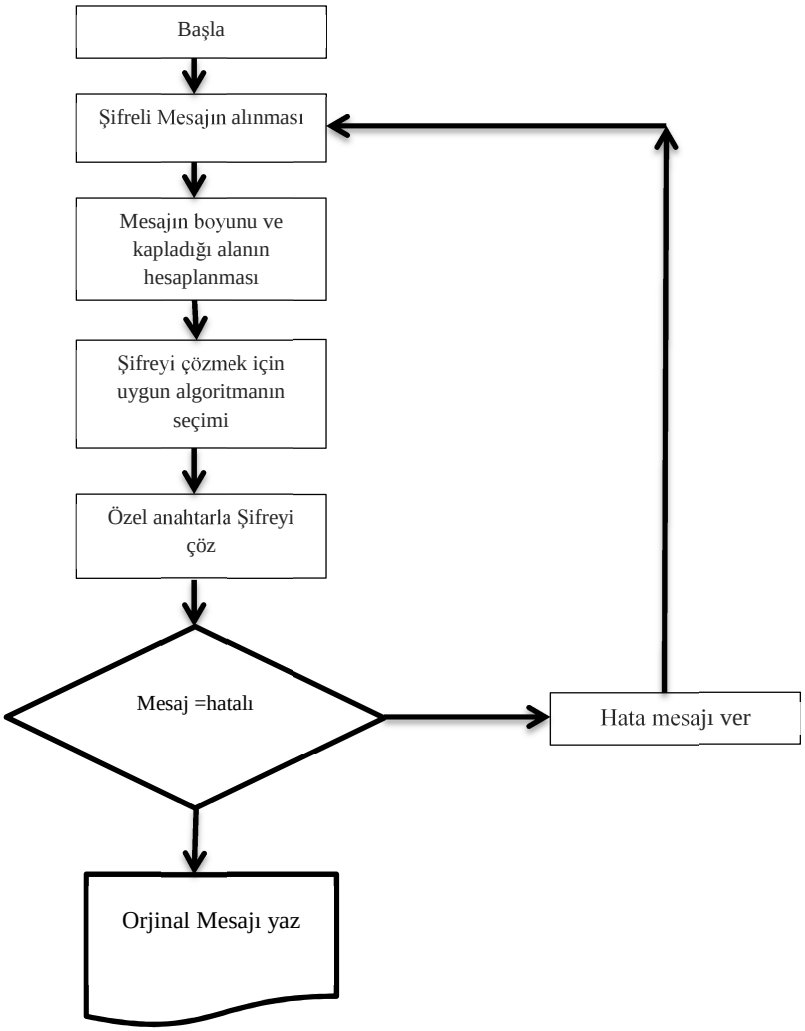
[57] ZHANG X., MIN L., “Steganography of Multimedia Information Based on Generallized Chaos Synchronization System”, Applied Science School and Information School University of Science and Technology Beijing 100083, PR Chinna, 2006

EKLER

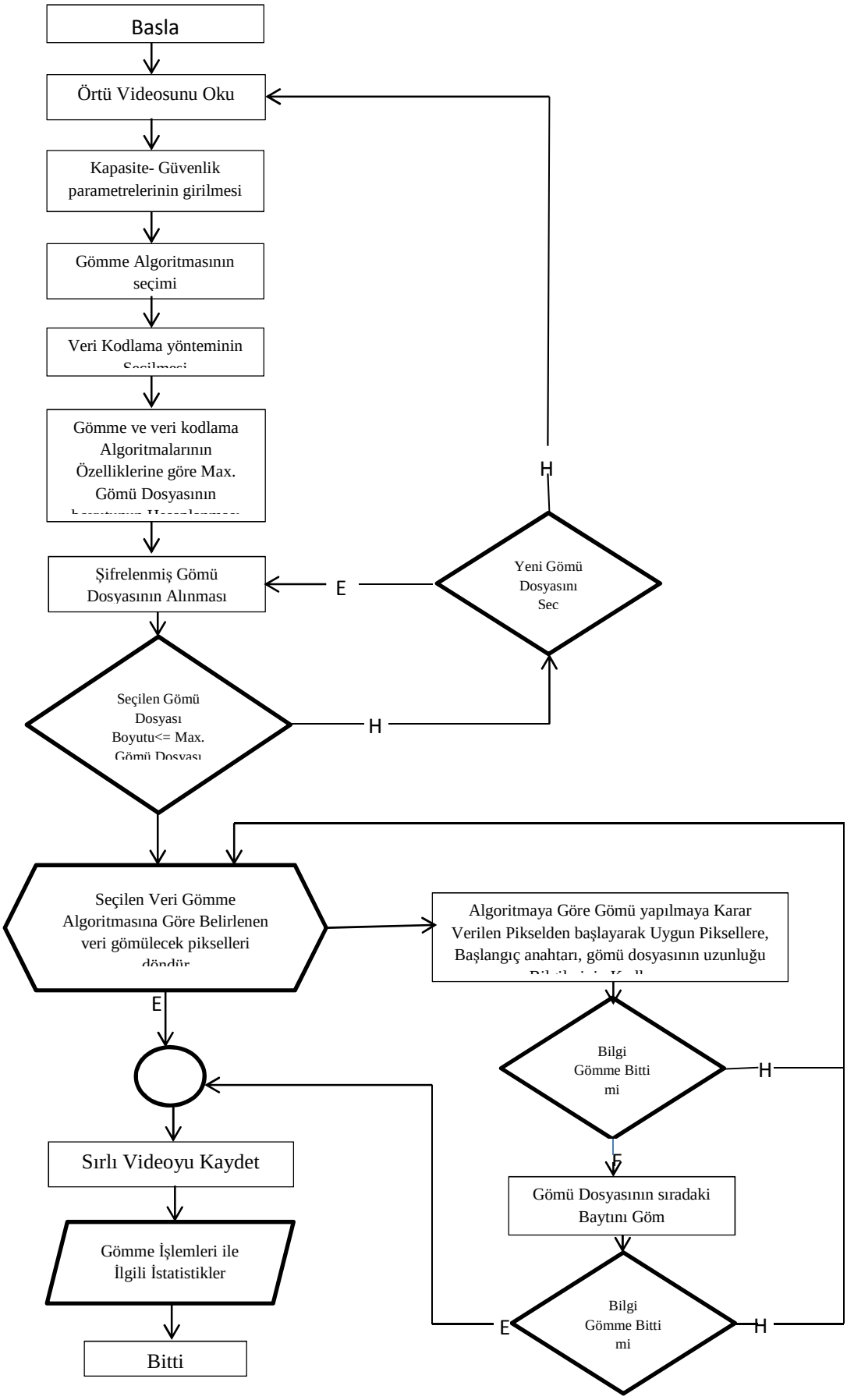
EK- A. Geliştirilen Algoritmaların Akış Diyagramları



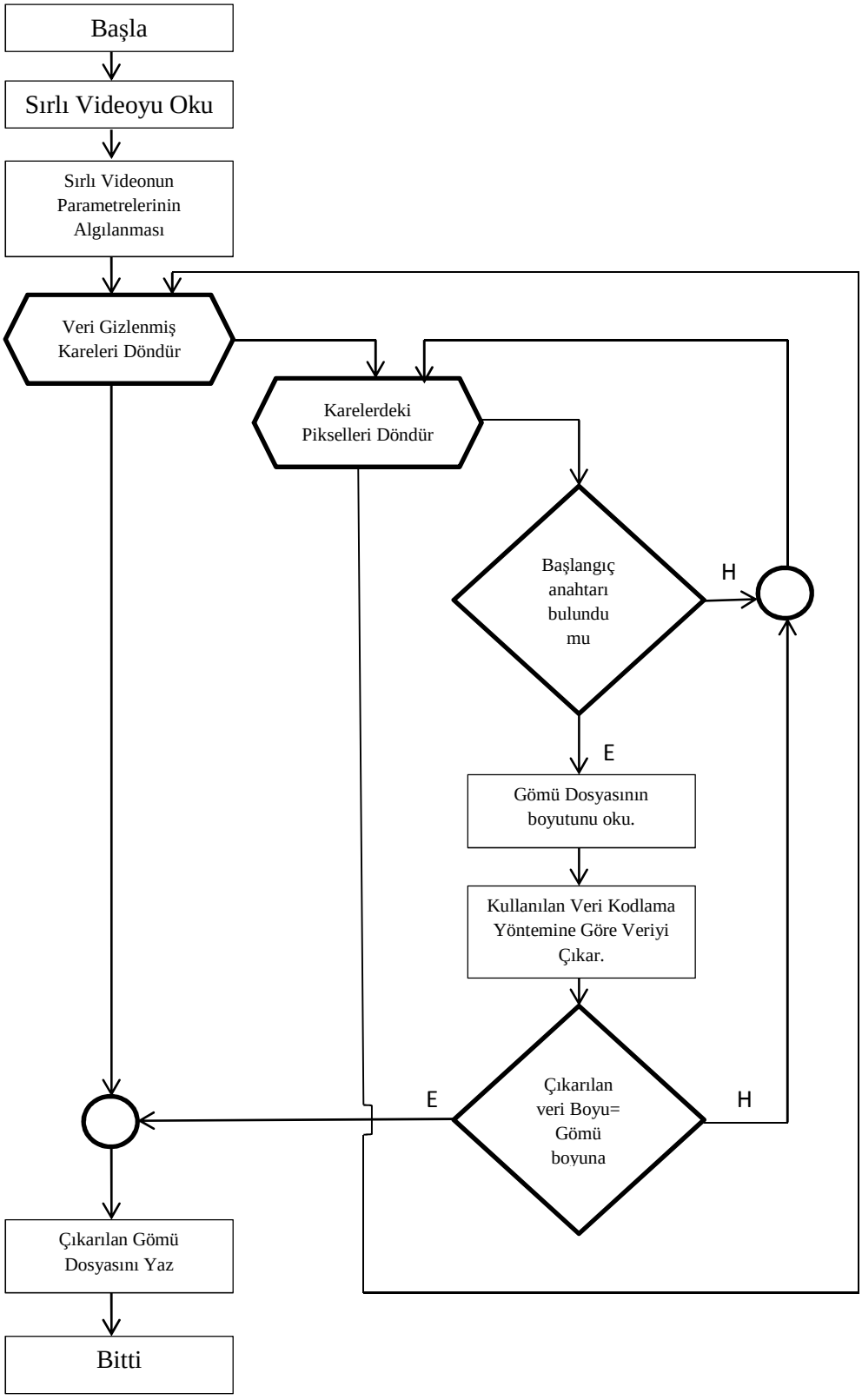
Şekil Ek.1. Şifreleme Algoritması.



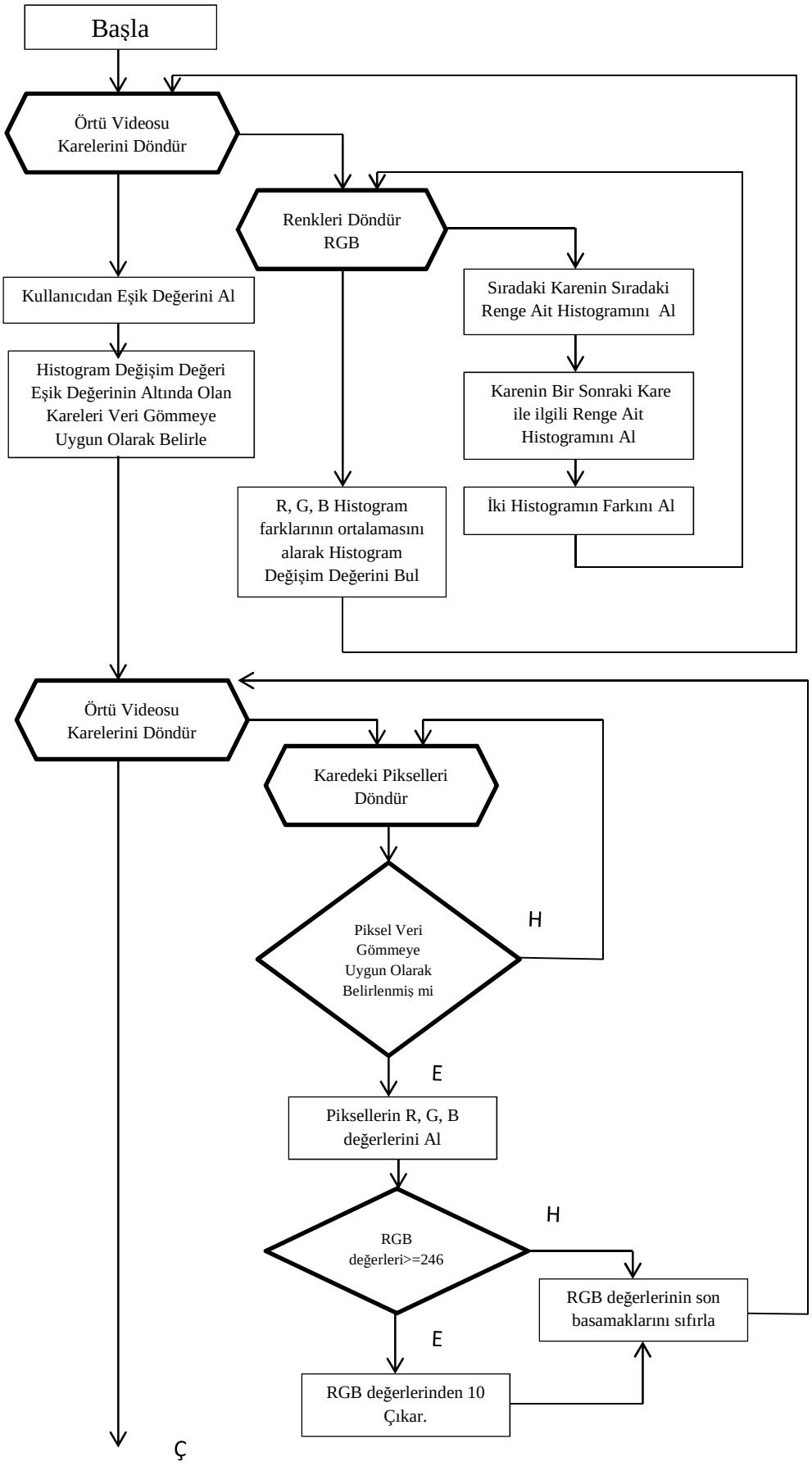
Şekil Ek.2. Şifre Çözme Algoritması.

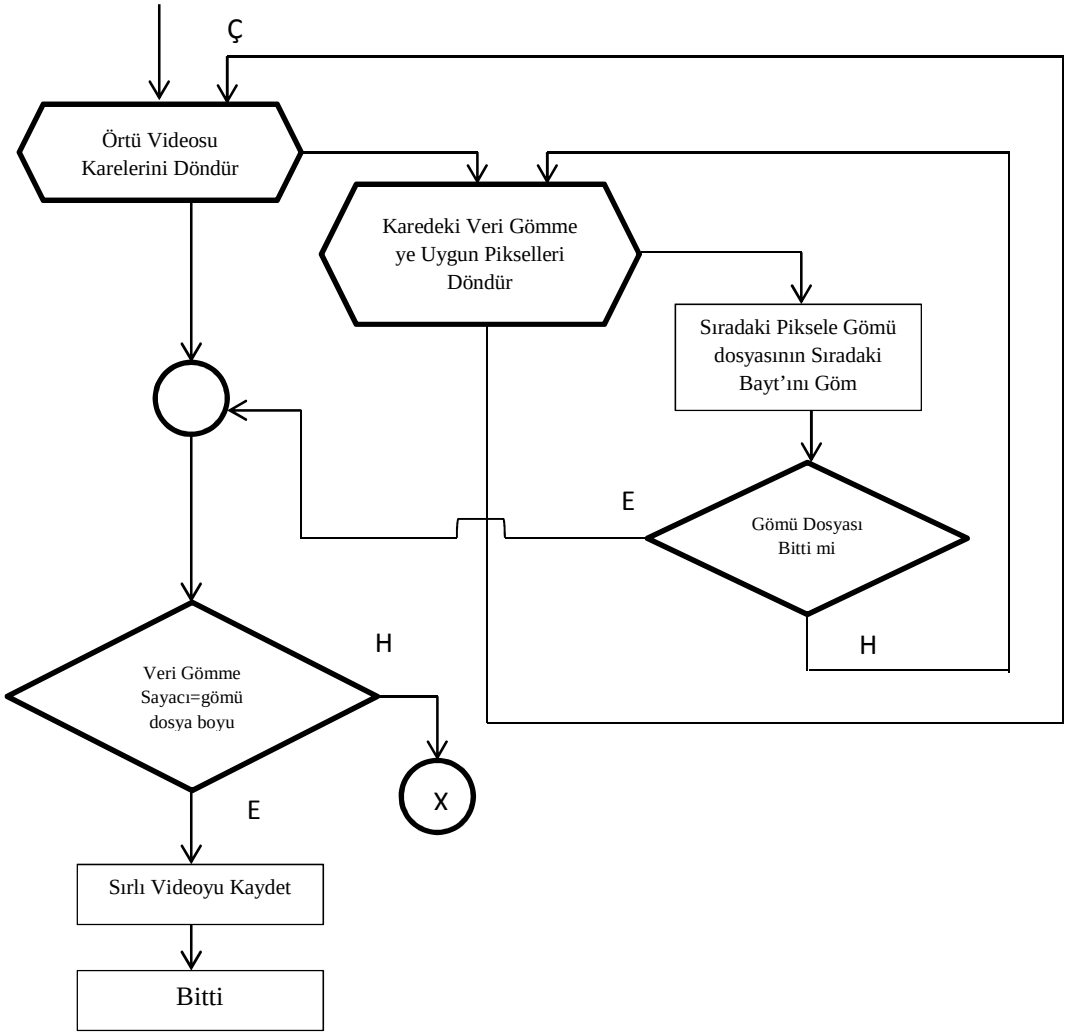


ekil Ek.3. Genel Veri Gizleme Akış Diyagramı



Şekil Ek.4. Genel Veri Geri Elde Etme Akış Diyagramı


Başla
Örtü Videosu Karelerini Döndür
Renkleri Döndür RGB
Kullanıcıdan Eşik Değerini Al
Sıradaki Karenin Sıradaki Renge Ait Histogramını Al
Histogram Değişim Değeri Eşik Değerinin Altında Olan Kareleri Veri Gömmeye Uygun Olarak Belirle
Karenin Bir Sonraki Kare ile ilgili Renge Ait Histogramını Al
R, G, B Histogram farklarının ortalamasını alarak Histogram Değişim Değerini Bul
İki Histogramın Farkını Al
Örtü Videosu Karelerini Döndür
Karedeki Pikselleri Döndür
Piksel Veri Gömmeye Uygun Olarak Belirlenmiş mi
H
E
Piksellerin R, G, B değerlerini Al
RGB değerleri>=246
H
E
RGB değerlerinin son basamaklarını sıfırla
RGB değerlerinden 10 Çıkar.
Ç



Şekil Ek.5. Benzer Histogramlar Yöntemi ile Veri Gömme Akış Diyagramı

EK- B. Sayısal Video İçerisinde Şifrelenmiş Gizli Verilerin Kablosuz Transferi için Geliştirilen Yazılımın Program Kodları CD İçerisinde Sunulmuştur (EK-A klasörü).

EK- C. Tez pdf Dosyası CD İçerisinde Sunulmuştur (Tez.pdf).

ÖZGEÇMİŞ

1986 yılında Kastamonu'da doğdu. Cide Atatürk İlköğretim Okulu'nu bitirdikten sonra 2004 yılında Kastamonu Mustafa Kemal Anadolu Lisesi'nden mezun oldu. 2005 yılında girmiş olduğu ÖSS sonucunda Sakarya Üniversitesi Teknik Eğitim Fakültesi Elektronik ve Bilgisayar Eğitimi Bölümü Bilişim Sistemleri Öğretmenliğinde okumaya hak kazandı. Buradan 2009 yılında mezun oldu ve aynı yıl Pamukova Teknik ve Endüstri Meslek Lisesi'nde Bilgisayar öğretmeni olarak göreve başladı. Yine aynı yıl Sakarya Üniversitesi'nde Yüksek Lisans öğrenimi görmeye başladı. 2010 yılında Mardin Mazıdağı Teknik ve Endüstri Meslek Lisesi'nde doğu görevine başladı. 2011 yılında ise evlenerek Kırşehir Kaman Kız Meslek Lisesi'nde bilgisayar öğretmeni olarak tayin oldu. 2012 yılında ise Kaman Teknik ve Endüstri Meslek Lisesi'nde çalışma hayatına başladı ve halan burada görevine devam etmektedir.