T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

HAREKETLİ GÖRÜNTÜ UYGULAMALARI İÇİN SIRÖRTME YAKLAŞIMI İLE VERİ GÖMME ALGORİTMASI TASARIMI

DOKTORA TEZİ

Özdemir ÇETİN

Enstitü Anabilim Dalı : ELEKTRİK ELEKTRONİK MÜH.

Enstitü Bilim Dalı : ELEKTRONİK

Tez Danışmanı : Yrd. Doç Dr. A.Turan ÖZCERİT

Ekim 2008

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

HAREKETLİ GÖRÜNTÜ UYGULAMALARI İÇİN SIRÖRTME YAKLAŞIMI İLE VERİ GÖMME ALGORİTMASI TASARIMI

DOKTORA TEZİ

Özdemir ÇETİN

Enstitü Anabilim Dalı : **ELEKTRİK ELEKTRONİK MÜH.**

Enstitü Bilim Dalı : **ELEKTRONİK**

Bu tez 27/10/2008 tarihinde aşağıdaki jüri tarafından Oybirliği ile kabul edilmiştir.

Prof. Dr. Hüseyin EKİZ
Jüri Başkanı

Yrd. Doç Dr. A. Turan ÖZCERİT
Üye

Prof. Dr. Etem KÖKLÜKAYA
Üye

Prof. Dr. Abdullah ÇAVUŞOĞLU
Üye

Doç. Dr. İsmail ERTÜRK
Üye

TEŞEKKÜR

Bir doktora tez çalışmasının ne kadar meşakkatli bir süreç olduğunu, sanırım bu sürece dâhil olanlar çok daha iyi anlayabilirler. Büyük bir sabır ve azim gerektiren bu süreç aynı zamanda huzurlu bir çalışma ortamı da ister.

Bu zorlu süreci en iyi ve faydalı bir şekilde atlatabilmem için, değerli birikimlerini aktarmaktan kaçınmayan, hertürlü sıkıntı ve sorunlarımı sabırla dinleyerek çok değerli zamanlarını bana ayıran, tezimin bu seviyeye ulaşması için her türlü özveriyi gösteren tez danışmanım Yrd. Doç. Dr. Ahmet Turan ÖZCERİT'e, çalışmalarım süresince hertürlü maddi manevi desteğini benden hiçbir zaman esirgemeyen sayın hocam Prof. Dr. Hüseyin EKİZ'e, değerli görüşleri ile bana yol gösteren ve yakından ilgilenen Dr. Feyzi AKAR ve Doç. Dr. İsmail ERTÜRK'e teşekkürlerimi sunarım. Ayrıca çalışmalarım ve araştırmalarım süresince bana hertürlü desteği veren mesai arkadaşım Barış BORU'ya da teşekkürlerimi sunarım.

Son olarak ise; her zaman yanımda olan öğrenim hayatımdan iş hayatıma benden maddi manevi desteklerini hiçbir zaman esirgemeyen çok değerli annem Melek ÇETİN ve babam Kemal ÇETİN'e de sevgilerimi sunuyorum.

İÇİNDEKİLER

SİMGELER VE KISALTMALAR LİSTESİ

LSB	: Least Significant Bit – En Düşük Değerlikli Bit
DCT	: Discrete Cosine Transform – Ayrık Kosinüs Dönüşümü
DWT	: Discrete Wavelenght Transform – Ayrık Dalgacık 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
MP3	: MPEG-1 Audio Layer 3
HVS	: Human Visual System
İGS	: İnsan Görme Sistemi
HAS	: Human Audio System
İDS	: İnsan Duyma Sistemi
GUI	: Graphical User Interface
SS	: Spread Spectrum
BH	: Benzer Histogramlar Yöntemi
FH	: Farklı Histogramlar Yöntemi
BTBH	: Blok Tabanlı Benzer Histogramlar Yöntemi
BTFH	: Blok Tabanlı Farklı Histogramlar Yöntemi
DB	: Dalgaboyu Yöntemi

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

ÖZET

Anahtar Kelimeler: Video Sırörtme, Sayısal Damgalama, Veri Gömme, Veri Gizleme, Sayısal Video, Ham Video – AVI.

Sırörtme teknikleri, gelişen bilgisayar teknolojisi ile çok büyük ilerleme kaydetmiş, çeşitli matematiksel algoritmalardan oluşan bilgisayar yazılımlarıdır. Günümüze kadar birçok sırörtme tekniği ortaya atılmış ve geliştirilmiştir. Fakat birçok farklı uygulamada olduğu gibi sırörtme teknikleri de mükemmel değildir.

Bu tez çalışmasında, taşıyıcı video içerisine başka bir video dosyası gizlenerek gizli haberleşme sağlanmıştır. Ayrıca algılanabilirliğin azaltılması için daha önce kullanılmamış bir yaklaşıma sahip yeni bir yöntem önerilmiştir. Önerilen yöntem iki işlem adımına sahiptir. İlk işlem olarak taşıyıcı–örtü video dosyası içerisindeki veri gömmeye uygun pikseller bulunur ve ikinci işlem olarak da gömülecek gizli veri en uygun piksellere yeni bir kodlama tekniği ile gömülür.

Veri gömülebilecek uygun pikseller histogramlar yöntemi veya dalgaboyu yönteminden faydalanılarak bulunmaktadır. Histogramlar yönteminde, taşıyıcı-örtü videosunun her bir çerçevesinin histogram değerleri hesaplanır ve daha sonra histogram değerlerinden alınan bilgilere göre video dosyası içerisindeki renk veya hareket bakımından değişkenlik gösteren veya göstermeyen bölgelerin pikselleri veri gömmek için işaretlenir. Dalgaboyu yönteminde ise, insan gözünün algılayamadığı 380nm altındaki (morötesi) veya 780nm üzerindeki (kızılötesi) ışık dalgaboyuna sahip pikseller veri gömme için işaretlenir. Veri gömme için uygun piksellerin bulunmasının ardından yüksek kapasitede veri gizlemeye olanak sağlayan bir kodlama tekniği kullanılarak veri gömme işlemi gerçekleştirilir.

Veri gömme işlemi sonucunda üretilen sırlı videonun algılanabilirliğini ve kalitesini değerlendirmek için Tepe Sinyal Gürültü Oranı (PSNR) kullanılmıştır. Bu çalışmada amaçlanan; algılanabilirliği en düşük seviyede tutarak gömülebilecek gizli veri kapasitesini en yüksek seviyeye çıkartmaktır.

A DATA EMBEDDING ALGORİTHM DESIGN FOR VIDEO APPLICATIONS USING A NEW STEGANOGRAPHY APPROACH

SUMMARY

Keywords: Steganography, Digital Watermarking, Data Embedding, Data Hiding, Digital Video, Raw Video – AVI.

Steganography techniques, which have been recently emerged together with developments in computer technologies, are realized usually using computer softwares consisting of various mathematical algorithms. Many steganography techniques have been developed for the last decade. However, none of them is perfect and yet to be well developed or improved.

In this thesis study, a hidden communication is performed by another video as hidden data is embedded into a cover video. Also, a new method which has a novel approach is suggested to reduce perceptibility of hidden data. This method has two steps. First, pixels appropriate for hiding data are compated in the cover video. And then hidden data replaces these pixels using a new coding technique.

The pixels to embed the data are found using the histograms methods or the wavelength methods. In histograms methods, histogram values are calculated for each frame in the cover video and then, consecutive frame histogram values are compared with each other. As a result, it is decided which pixel is appropriate to hide data. The wavelength method, first finds out pixels near the 380nm or 780nm wavelength values in the cover video. Then, to embed the hidden data into these pixels, a new coding technique providing a large hidden data capacity is used.

Peak Signal to Noise Ratio - (PSNR) parameter is used to assess stego-video quality as a statistical measure during the experimental works. In this thesis, mainly a high hidden data embedding capacity is aimed while keeping the perceptibility as low as possible.

BÖLÜM 1. GİRİŞ

Çoğu teknolojide olduğu gibi Internet teknolojisi de askeri amaçla ortaya çıkmış fakat daha sonra kullanım alanı hızla sivil hayata yayılmıştır. Internet kullanımının bu kadar hızlı yayılması ile her evin içerisinde dünyaya açılan bir kapı bulunmakta ve mesafeler inanılmaz bir biçimde ortadan kalkmaktadır. Bu muazzam büyüklükteki iletişim ortamında güvenliğin tam anlamıyla sağlanması da doğal olarak imkânsızdır. Özellikle bireysel hayatın mahremiyetini korumak, insanların aralarındaki haberleşme güvenliğini sağlamak neredeyse imkânsız hale gelmiştir.

Sayısal medyanın gizli haberleşmede kullanılmaya başlanmasından önce yazılı metinler üzerinde birtakım işlemler yapılarak gizli haberleşme sağlanırdı. Bu gizli haberleşme yöntemi kriptografi (cryptography) olarak adlandırılmaktadır. Kriptografide, yazılı metinler anlaşılması imkânsız olan formlara dönüştürülür ve bu şekilde haberleşme yapılır. Buradaki dezavantaj; yetkisiz kişilerin haberleşmenin içeriğini bilmeseler bile orta da bir haberleşme olduğunu anlayabilmesidir. Sayısal medyanın gelişmesi ile gizli haberleşmede bu ortamları kullanma düşüncesi sayısal damgalama ve sırörtme tekniklerinin gelişmesini sağlamıştır. Her iki teknikte de kullanılan yöntemler benzerlik gösterse de kullanım amaçları itibariyle farklılıklara sahiptirler. Bir sayısal medyanın (sinema filmi, müzik parçası vb.) korunması ve illegal yollarla paylaşılmasını önlemek için sayısal damgalama kullanılır. Farklı coğrafi bölgelerde bulunan insanlar aralarında gizli haberleşme (askeri istihbarat vb.) yapmak için ise sırörtme tekniklerini tercih ederler. İki teknik arasında söylenebilecek en açık fark; sayısal damgalama, bilinen popüler bir medya dosyası üzerinde yapıldığından karşılaştığı saldırılar sırörtme tekniklerinden farklıdır. Çünkü sırörtmede kullanılan taşıyıcı dosya bilinmeyen herhangi bir dosya olacaktır ve saldırıya maruz kalması çok düşük bir ihtimaldir.

Gizli haberleşme teknikleri ilk olarak hareketsiz görüntüler üzerinde uygulanmıştır. Daha sonraki araştırmalarda ise geniş uygulama alanı ve büyük kapasiteye sahip olmasından dolayı hareketli görüntü üzerinde durulmuştur [1]. Dağıtımının kolaylığı ve veri gömme tekniklerinin benzer olması nedeni ile ses dosyaları da veri gizleme tekniklerinde kullanılan diğer taşıyıcı dosyalardır.

1.1. Resim İçerisine Veri Gizleme Çalışmaları

Bilgi gizlemede kullanılan ilk yöntemlerden biri olan LSB (Least Significance Bit) yöntemi, gizli verinin doğrudan LSB düzlemine yerleştirilmesi prensibine dayanır. Schyndel ve Wolfgang çalışmalarında bu tekniği kullanmışlardır [2],[3]. Bu teknikler yüksek bilgi kapasitesi ve düşük algılanabilirlik sağlamalarına rağmen karmaşık bir yapıya sahip olmamaları nedeniyle kötü niyetli kişiler tarafından gizli verinin elde edilmesi oldukça kolaydır. Bu tekniklerin bir başka zayıflığı ise, esnek olmamalarıdır. Yani haberleşme kanalında taşıyıcı resme eklenen bir gürültü gizli verinin geri elde edilmesini engelleyecektir.

LSB tekniğinin zayıflıklarını aşmak için geliştirilmiş diğer çalışmalar [4], [5], [6] ise gizli verinin geri elde edilmesi sırasında taşıyıcı resme ihtiyaç duyarlar. Algılanabilirliği düşürmek için araştırmacılar İGS'nin duyarlılığından faydalanmayı düşünmüşlerdir. Fakat bu sistemin kapasitesi taşıyıcı resme bağlıdır.

Bir başka çalışmada [7] ise araştırmacı, taşıyıcı dosyanın bitlerinde küçük kesirli değişimleri önermektedir. Bu yöntemde, taşıyıcı resmin her yüzüncü bit değeri bir gri seviye ile değiştirilir. Resim gürültüsüne bağlı olarak bu değişiklikler ile uygun karmaşık şüpheler oluşturularak, resmin herhangi bir istatistiksel model ile kolayca anlaşılamaması başarılı bir şekilde sağlanır.

1.2. Video İçerisine Veri Gizleme Çalışmaları

Bir hareketli görüntü içerisine gizli bir bilgi, hareketli görüntünün her bir resim çerçevesi kullanılarak gömülebilir. Var olan birçok hareketli görüntü içerisine bilgi

gömme yöntemi hareketsiz görüntü içerisine bilgi gömme yöntemleri ile tamamen benzer bir işleyişe sahiptir.

Hareketli görüntü üzerinde yapılan damgalama çalışmaları da kullanılan video'ya göre Ham–Video Damgalama (Raw–Video Watermarking) ve Sıkıştırılmış–Video Damgalama (Bit–Stream Watermarking) olarak iki ana sınıfa ayrılmaktadır [8]. Ham Video Damgalama ile ilgili olarak Hartung ve Girod'un çalışmasını [9] ilk yapılan çalışmalardan biri olarak gösterebiliriz. Araştırmacılar çalışmalarında yayılı–izge (spread–spectrum) haberleşmesinden esinlenmişlerdir. Çalışmasında [10] bu mantığı kullanan Hartung, hareketsiz görüntü veri gömme tekniklerini doğrudan ham hareketli görüntüye uygulamıştır. Bu çalışmada, bir (p_i +1 veya -1) rastgele-gürültü dizisi, v_i hareketli görüntüsünün 8×8 boyutunda seçilmiş DCT katsayılarına gömülmüştür.

$$V_{i1} = v_i + p_i \alpha_i \tag{1.1}$$

burada α_i, hareketli görüntünün her çerçevesinde farklı bir değer alan ayarlanabilir genlik faktörüdür. Gizli verinin geri elde edilmesinde alıcı tarafında ilgileşim (korelasyon) metodu uygulanır. Elde edilen deney sonuçlarına göre gizli veri kapasitesi 50 bit/saniye 'dir.

Hartung ham video için önerdiği [10] çalışmasını ayrıca sıkıştırılmış videoya da uygulamıştır. I, P ve B çerçevelerinin her birisine diğer yöntemindeki işleyişin aynısını uygulamıştır. Videoda her bir sıkıştırılmış çerçeve için 8×8 DCT katsayılarına damgayı eklemiştir. Deneylerden elde edilen sonuçlara göre standart sinyal işlemeye karşı daha dayanıklı sonuçlar vermiştir.

Bir başka çalışmada ise Swanson [11],[12], çoklu-ölçek damgalama yöntemini sunmuştur. Bu yöntemde, öncelikle hareketli görüntü çerçevelerine ayrılır. Sonrasında her bir çerçeveye zamansal dalgacık dönüşümü uygulanarak zamansal alçak geçiren ve yüksek geçiren çerçeveler elde edilir. Gizli veri bu çerçevelere gömüldükten sonra ters dönüşüm uygulanarak gizli veri içeren hareketli görüntü elde edilir. Bu çalışmada damganın geri elde edilmesi için orijinal video bilgisine ihtiyaç duyulur.

Hsu ve Wu [13] çalışmalarında ham hareketsiz görüntü için DCT dönüşümünden faydalanılan bir yöntem önermişlerdir. Kalker ise [14] çalışmasında Hartung'a benzer bir düşünce ile hareketli görüntüleri hareketsiz görüntüler olarak kabul ederek veri gömme tekniği uygulamıştır. Bir başka çalışmada [15] Deguillaume 3 boyutlu bir uzamsal-zamansal DFT dönüşümü önermiştir.

Jordan [16] çalışmasında sıkıştırılmış videonun hareket vektörlerine gizli veriyi gömmeyi önermiştir. Gizli veri doğrudan hareket vektöründen geri elde edilir.

1.3. Ses İçerisine Veri Gizleme Çalışmaları

Bazı güncel ses içerisine bilgi gizleme teknikleri yayılı-izge modülasyonunu (SS - Spread Spectrum) kullanmaktadır. Rastgele bir damga dizisi alt-band boyutunda, cepstra boyutunda veya zaman boyutunda ses içerisine gömülür [17], [18], [19].

Bir başka yaklaşımda ise, gizli verinin gömülmesinde insan algılama modeli kullanılır. Bu yöntem duyulabilirliği kontrol edebilmek için uygulanabilecek en etkili yöntemdir [20].

Sıkıştırılmış boyutta ses içerisine sır saklamada kullanılan bir yöntem MP3Stego yöntemidir. Bu yöntemde gizli veri sıkıştırma esnasında üçüncü MPEG katmanına (MP3) gömülür [21].

1.4. Tez Çalışmasının Amacı, İzlenen Çalışma Yöntemi ve Katkıları

Bir ülkenin ulusal güvenliğinin, ticari bir kurumun kurumsal bilgilerinin veya insanların bireysel bilgilerinin korunması gibi problemlere çözüm getirmeyi amaçlayan veri gömme ve gizleme tekniklerinin bu işlemleri en iyi şekilde yerine getirmesi büyük önem arz etmektedir. Gelişen teknolojiyle bilgisayarların hesaplama kabiliyetlerinin artması daha güvenli algoritmaların geliştirilmesine olanak sunmaktadır. Bir yandan bazı araştırmacılar sırörtme tekniklerini geliştirirken diğer yandan bazı araştırmacılar ise bu tekniklerin zayıflıklarını bulmaya çalışmaktadır.

Uygulama alanı yukarıda bahsedildiği gibi bir ülkenin ulusal güvenliği ise amaç en sağlam tekniğin geliştirilmesi olmalıdır.

Bu çalışmada, yapılmış önceki çalışmalardan farklı olarak bilgi gömme (iletişim amaçlı) ve damga ekleme (güvenlik amaçlı) problemleri [22] birbirlerinden ayrılarak sadece bilgi gömme üzerinde durulmuştur. Burada amaç sırlı video ile orijinal video arasında en az bozulmayla bilginin gizlenmesini sağlamaktır. Böylece gizli haberleşme dışarıdan gelebilecek harici saldırılara maruz kalmayacaktır.

Bu çalışmanın var olan sırörtme yöntemlerinden farklılıkları ve katkıları şu şekilde özetlenebilir:

1. Literatürde var olan İGS'ye uygun olarak geliştirilmiş veri gömme tekniklerinden faydalanılarak, video içerisindeki veri gömmeye en uygun pikselleri belirlemek için İGS'ye uygun iki farklı sırörtme yöntemi önerilmiştir.

2. Görüntü içerisindeki veri gömmeye uygun piksellerin belirlenmesinin ardından, gizli verinin en etkin biçimde gömülmesi için, daha önce hareketsiz görüntüler üzeride gerçeklenmiş bir kodlama tekniğinin [87]'de önerilen yönteme uyarlanması gerçekleştirilmiştir.

3. Veri gömme işleminin kullanım amacına ve ihtiyaca göre kapasite ve algılanabilirlik seviyelerinin ayarlanabilmesi, kullanıcılara büyük esneklik sağlamaktadır. Böylece kullanıcı, haberleşme kanalının güvensizliğine göre veya haberleşme bilgilerinin gizliliğine göre algılanabilirlik seviyesini istediği gibi belirleyebilmektedir.

4. Geliştirilen Grafik Kullanıcı Arayüz yazılımı sade bir yapıya sahip olması, hızlı bir şekilde veri gömme ve gizli veriyi geri elde etme performansı, gömme işlemi öncesinde ve sonrasında kullanıcılara sağladığı istatistikî bilgiler sayesinde etkin bir gömme işlemi gerçekleştirmektedir.

5. Daha önce hiçbir veri gömme çalışmasında kullanılmamış olan, belki de İGS'ye en duyarlı olabilecek bir parametre; görülebilir ışığın dalgaboyu parametresi veri gömme için uygun piksellerin belirlenmesi aşamasında kullanılmıştır. Diğer bir parametre olarak ise, video çerçevelerinin histogramlarının kullanılmasıdır. Bu parametre ile bir videonun ne kadar hareketli veya hareketsiz sahneler içerdiği hakkında bilgi sahibi olarak veri gömme yapılacak çerçevelere ve piksellere karar verilmesi hedeflenmiştir.

1.5. Tez Organizasyonu

Tez organizasyonu aşağıda özetlenen sekiz bölümden oluşmaktadır:

Bölüm 1. Giriş: Bu bölümde veri gizleme ile ilgili günümüzde araştırmacıların karşılaştıkları problemler, araştırmacıların bu problemlere getirdiği çözümlerin incelenmesi, tez çalışmasının amacı, karşılaşılan problemlere getirilen öneriler, literatür çalışmalarından farklılıklar ile tez organizasyonu hakkında bilgi sunulmaktadır.

Bölüm 2. Sayısal Görüntü Esasları Ve Görüntü İşleme: Bu bölümde amaçlanan tez konusunun daha iyi anlaşılabilmesi için sayısal görüntü hakkında temel birtakım bilgilerin verilmesidir. İnsan gözünün biyolojik yapısı, ışık bilgisi, sayısal ortamlarda en sık kullanılan renk uzayları, sayısal görüntü ve sayısal görüntü ile ilgili temel kavramlar bu bölümde anlatılan konuları oluşturmaktadır.

Bölüm 3. Veri Gizleme İşlemine Genel Bakış: Veri gizleme işleminin tarihçesi, insanlar için önemi, literatürde veri gizleme için geliştirilmiş teknikler, kullanım alanları hakkında detaylı bilgiler bu bölümde sunulmaktadır.

Bölüm 4. Hareketli Görüntü Uygulamaları İçin Sırörtme Yaklaşımı İle Geliştirilen Veri Gömme Algoritmaları ve Gerçekleştirilmeleri: Tez çalışmasının ana bölümünü oluşturan bu bölümde, geliştirilen yöntemlerin anlatılması, her bir yöntemin blok şeması ile anlatımının detaylandırılması, yazılan kullanıcı arayüz programının kullanılması ile ilgili bilgiler bulunmaktadır.

Bölüm 5. Geliştirilen Uygulamalara Ait Deneysel Sonuçların Değerlendirilmesi: Bu bölümde amaçlanan, geliştirilen yöntemlerin literatürde bir geçerliliklerinin olup olamacağı ile ilgili analizler yapılmasıdır.

Bölüm 6. Sonuçlar ve Öneriler: Son bölüm olan Sonuçlar ve Öneriler bölümünde ise, yapılan deneysel çalışmalardan elde edilen sonuçlar değerlendirilerek çalışmanın katkıları tartışılmıştır. Ayrıca gelecekte yapılması düşünülen, tez çalışmasının devamı niteliğini taşıyabilecek yeni çalışmalar da önerilmiştir.

Ek-A. Geliştirilen Algoritmaların Akış Diyagramları: Bu bölümde, farklı histogramlar yöntemi, blok tabalı farklı histogramlar yöntemi, benzer histogramlar yöntemi, blok tabanlı benzer histogramlar yöntemi, bölgesel histogramlar yöntemi ve dalgaboyu yöntemi algoritmaların akış diyagramlarına yer verilmiştir.

BÖLÜM 2. SAYISAL GÖRÜNTÜ ESASLARI VE GÖRÜNTÜ İŞLEME

2.1. Giriş

Bu bölümde tez çalışmasının ve temellerinin daha iyi anlaşılabilmesi için, sayısal görüntü ve görüntü işleme teknikleri ile ilgili bir takım temel bilgiler sunulmaktadır.

Bilgi teknolojisinin hızla gelişmesi ve çoklu ortam özelliklerine sahip elektronik cihazların artması ile görüntülerin (resim, video gibi) sayısal formatta saklanması bir ihtiyaç halini almıştır. Sayısal görüntü; arşivleme, korunma ve yayımlanma gibi birçok alanda işlem kolaylığına sahip olduğundan, hızla analog görüntülerin yerini almıştır. Bir analog görüntünün yayımlanması için koaksiyel kablo ağına, RF modülatörlere, matris anahtarlayıcılara ve frekans yöneticilerine ihtiyaç vardır. Bu gibi ihtiyaçlar karmaşıklığı ve maliyeti artırdığı için analog görüntü teknolojisinin yerini sayısal görüntü teknolojisine bırakmasını hızlandırmıştır. Durumu örneklendirecek olursak, güvenliğini sağlamak istediğimiz bir binanın güvenlik görüntülerini binanın içerisindeki güvenlik odasından izlemek analog görüntü teknolojisi ile mümkündür. Gerekli olan tek şey kablolama işleminin gerçekleştirilmiş olmasıdır. Fakat aynı binanın güvenlik görüntülerini daha uzak bir mesafeden hatta başka bir şehirden, ülkeden izlemek için aynı sistemin yetersiz kalacağı aşikârdır [23]. Buna karşın sayısal görüntünün gelişmiş Internet ağı sayesinde dünyanın her noktasına çok rahatlıkla iletilebilmesi, sayısal görüntülerin analog görüntülere göre en büyük avantajıdır.

Analog görüntülerin videokasetlere kayıt işlemi, şerit halindeki film üzerinde kimyasal değişiklikler meydana getirilerek gerçekleştirilir. Bu yöntemle kaydedilen videokasetlerin güneş ışınlarına, manyetik alana maruz kalmaları durumunda veri kaybı yaşanmakta ve veriler kurtarılamamaktadır. Sayısal görüntüler ise ışık dalgalarının elektrik sinyallerine dönüştürülmesi ile kaydedilir ve depolama

yöntemine bağlı olarak analog depolamaya göre bazı avantajlara sahiptirler. Görüntülerin kaybedilme riskinin düşük olması, işleme ve dağıtım kolaylığı bunlardan bazılarıdır.

Sayısal ve analog görüntüler arasındaki bazı farklar Tablo 2.1'de özetlenmiştir.

Tablo 2.1. Sayısal görüntü sistemleri ile Analog görüntü sistemleri arasındaki bazı farklar [23].

İşlem	Analog	Sayısal
Video Kaynakları	Analog kameralar, tünerler, uydu yayınları	Analog kameralar, tünerler, uydu yayınları, sayısal kameralar
Erişim	Uydu yayını, RF yayını, kablo yayını olan her yer	Internet, uydu yayını olan her yer
Kalite	Değişken	CD-DVD-HD kalitesi
Ağ girdisi	RF modülatörler	MPEG kodlayıcılar
Ağ çıktısı	TV	Bilgisayar ekranı
Yayın isteği	Sınırlı: RF, frekans yönetimi gerektirir.	Sınırlı: ağ band genişliğine bağlıdır.
Telekonferans	Zor: her iki alıcı ve verici de kendi RF modülatörlerini ve kendi TV kanallarını gerektirirler.	Sınırsız: otomatik işlem gerçekleştirilir.
Kurulum	Maliyet yüksek: her yere koaksiyel kablo hattı gerekli.	Var olan Ethernet kartının kullanılması yeterli.
Maliyet	Düşük	Orta (yeni koaksiyel kablo kurulumu düşünüldüğünde daha ucuz)

Görüntülerin sayısal ortama aktarılması beraberinde birtakım gereksinimleri de getirmiştir. Analog görüntünün hiçbir işlem yapılmaksızın sayısal görüntü olarak ifade edilmesi ciddi anlamda yer gereksinimine sebep olmaktadır. Sayısal ortamda ilk olarak bilinen video formatı VCD; 352×240 çözünürlüğe sahiptir. Basit bir kapasite gereksinimi aşağıdaki Denklem 2.1 ile bulunabilir;

$$\text{Çerçevedeki toplam piksel} \times \text{Sn'deki çerçeve sayısı} \times \ldots$$
$$\text{Piksel için ayrılan hafıza} \times \text{Video Süresi} \qquad (2.1)$$

Denklem 2.1 kullanılarak standart VCD formatındaki 90 dakikalık (5400sn) bir video için gerekli kapasite;

$$(352\times240) \times 25 \times 3 \times 5400 \text{ (sn)} = 34{,}214{,}400{,}000 \text{ bayt} = 34{,}21 \text{ GB}$$

olarak hesaplanır. Yukarıdaki gibi basit bir hesap ile sayısal görüntülere birtakım işlemlerin uygulanması gerekliliği daha açık olarak anlaşılmaktadır. Bahsedilen işlemlere görüntü işleme teknikleri denilmektedir. Temel olarak görüntü işleme teknikleri kullanılarak sayısal görüntü üzerinde kalite, kapasite gibi bir takım iyileştirmeler yapılması düşünülmüş fakat doğan ihtiyaçlar karşısında görüntü işleme

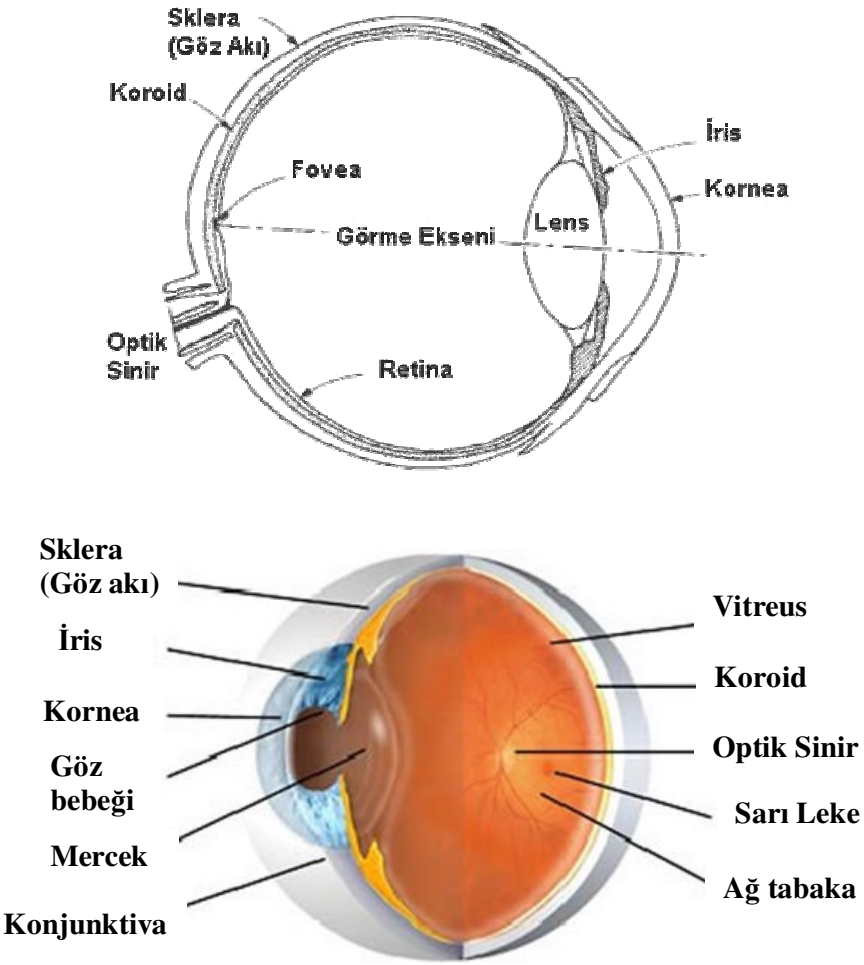
teknikleri daha da geliştirilmiştir. Ortaya çıkan ihtiyaçlardan biri de bu tez çalışmasına konu olan güvenlik ve gizli haberleşmedir.

2.2. Görme Olayı

Görme olayının daha iyi anlaşılabilmesi için, İGS'nin yapısından bahsetmek ve mekanik görme olayının nasıl olduğunu anlamak önemlidir. Görüntü işleme teknikleri yine insanın görsel algılaması doğrultusunda geliştirilmektedir. Bu nedenle İGS yapısının ve sınırlarının bilinmesi birçok noktanın anlaşılmasında faydalı olacaktır. [24]'den İGS ile ilgili daha detaylı bilgi elde edilebilir.

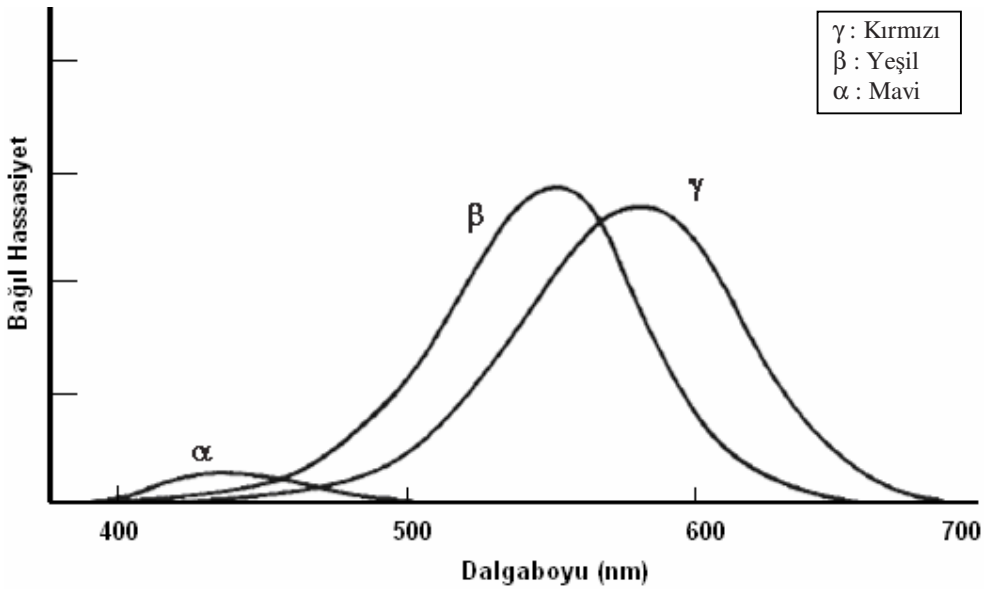
2.2.1. İnsan göz yapısı

Şekil 2.1'de verilen insan göz yapısı temel olarak; kornea, iris, göz bebeği (pupil), göz merceği (lens), ağ tabaka (retina), fovea, koroid (choroid), göz akı (sclera) ve optik sinirlerden oluşmaktadır [25]. Yarı şeffaf bir yapıya sahip olan kornea gözün ön bölümünü kaplamaktadır. Gözün en dışındaki koroidi kaplayan ve lifli bir tabakadan oluşan göz akı (sclera) aynı zamanda kılcal kan damarlarını içeren bir katmandır. Koroidin iç kısmı ise retina yani ağ tabakadır. Ağ tabaka; çubuk (rod) ve koni (cone) adı verilen iki tip algılayıcıdan oluşmaktadır. Ağ tabakanın sinirlerle bağlantısı gözün arka tarafındaki optik sinir yığınları ile sağlanır. Mercek nesnelerin uzaklığına ya da yakınlığına göre şekil değiştirerek odaklanmayı sağlar. Merceğin merkezi ile ağ tabaka arasındaki mesafe yaklaşık olarak 17mm'dir. Göze rengini veren iris, nesneden gelen ışığın şiddetine göre göz bebeğinin genişlemesini ya da küçülmesini sağlayan bir kas dokudan oluşmaktadır. Bu yönüyle iris bir bakıma diyafram vazifesi görmektedir.



Şekil 2.1. İnsan gözünü oluşturan önemli bölümler.

Gözün odaklandığı bir nesneden gelen ışık, korneadan geçerek ağ tabaka üzerine düşer. Bir nesnenin algılanmasında, ağ tabaka üzerinde bulunan çubuksu ve konisel algılayıcıların çok büyük önemi vardır [26]. Koni algılayıcılarına göre ışığa daha hassas olan çubuk algılayıcıları; ağ tabaka içerisinde daha narin ve uzundurlar. Daha kısa ve kalın yapıda olan koni algılayıcıları ise ışığın renk bileşenine hassastırlar. Koni algılayıcıları kırmızı, yeşil ve mavi ışık dalga boylarına duyarlı üç farklı tip hücreden oluşmaktadır. Şekil 2.2'de görüldüğü gibi α koni algılayıcıları mavi rengin algılanmasından sorumludur. Şekildeki konilerin grafiklerine bakıldığında α konisinin algılama hassasiyetinin diğer konilere göre daha az olduğu anlaşılmaktadır. Bu durum mavi rengin algılanma hassasiyetinin kırmızı ve yeşil renklere göre daha düşük olduğu anlamına gelmektedir. Koni görüntüsü 'photopic' veya 'parlak-ışık' görüntüsü olarak adlandırılır.



Şekil 2.2. Kırmızı–Yeşil–Mavi renklerini gösteren koni algılayıcılarının algılama hassasiyetleri [25].

Çubuk algılayıcıları koni algılayıcılarının aksine, nesnenin detaylarını içermeyen genel bir görüntü verir. Çubuk algılayıcıları ışığa karşı hassas fakat renk için hassas değildir. Örneğin güneş ışığı altında görülen parlak renkli bir nesne, ay ışığında renksizmiş gibi görülebilir. Çünkü ay ışığında sadece çubuk algılayıcıları uyarılmaktadır. Elde edilen bu görüntü ise 'scotopic' veya 'sönük-ışık' görüntüsü olarak adlandırılır.

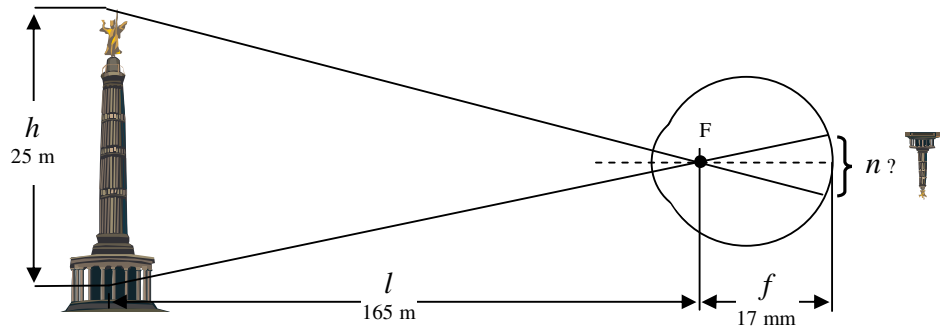
Koni algılayıcılarının en yoğun olduğu ve renk duyarlılığı en yüksek olan nokta fovea'dır. Görüntünün algılanmasında önemli bir yeri olan fovea yaklaşık 1,5mm çapında yuvarlak bir yapıya sahiptir. Benzer şekilde görüntü işleme tekniklerinde bir görüntünün algılanması için 1,5mm × 1,5mm boyutlarında kare veya dikdörtgen dizi yapıları kullanılmaktadır [27]. Fovea'nın boyutlarına göre ağ tabaka'nın merkezindeki koni yoğunluğu mm^2 başına yaklaşık olarak 150,000 elemandır. Fovea merkezinde bulunan en hassas bölgedeki koni sayısı yaklaşık olarak $1{,}5 \times 1{,}5 \times 150{,}000 \cong 337{,}500$ elemandır. Sayısal kameralarda kullanılan görüntü yongasının (CCD–charge-coupled device) çözünürlük hassasiyeti için bu hesaplamalar önemli bir yer tutmaktadır. Örneğin, iyi bir görüntü kalitesi için görüntü yongasının algılayıcı dizisi 5mm × 5mm den büyük olmamalı ve en az yukarıda verilen sayıda eleman içermelidir [27].

2.2.2. Basit olarak görme olayının oluşması

Görme olayının gerçekleşmesi için gerekli olan en önemli şart, ortamda bir ışık kaynağının olmasıdır. Nesnelerden yansıyarak korneadan göze giren ışık görmeye neden olur. Korneanın kavisli bir yapıya sahip olması ile ışık korneadan kırılarak geçer. Gözün bir nesneye ya da noktaya odaklanmasını ise göz merceği sağlar. Göz merceğinin hareketi göz kapağındaki liflerin elektriksel sinyalleri ile kontrol edilir. Göz merceği uzaktaki nesnelere odaklandığında kırma olayını en düşük seviyede gerçekleştirir. Yakın mesafedeki nesnelere odaklandığında ise tam tersi yani en yüksek seviyede kırma yapar. Bu bilgiden faydalanılarak ağ tabaka üzerine düşen nesnenin görüntü boyu hesaplanabilir. Şekil 2.3 matematiksel olarak;

$$\frac{h}{l} = \frac{n}{f} \tag{2.2}$$

ifade edilebilir. Şekil 2.3'de h gerçek nesnenin yüksekliği, l nesne ile göz arasındaki mesafe, f mercek merkezinin ağ tabakaya mesafesi (17 mm), n gözde oluşan görüntünün boyu ve F ise merceğin merkez noktasını göstermektedir.



Şekil 2.3. İnsan gözünde bir görüntünün oluşması.

Örnek olarak şekilde verilen değerler kullanıldığında gözde oluşan görüntünün boyu;

$$\frac{25}{165} = \frac{n}{17} \cong 2.57mm$$

olarak hesaplanır.

2.3. Işık ve Elektromanyetik Tayf

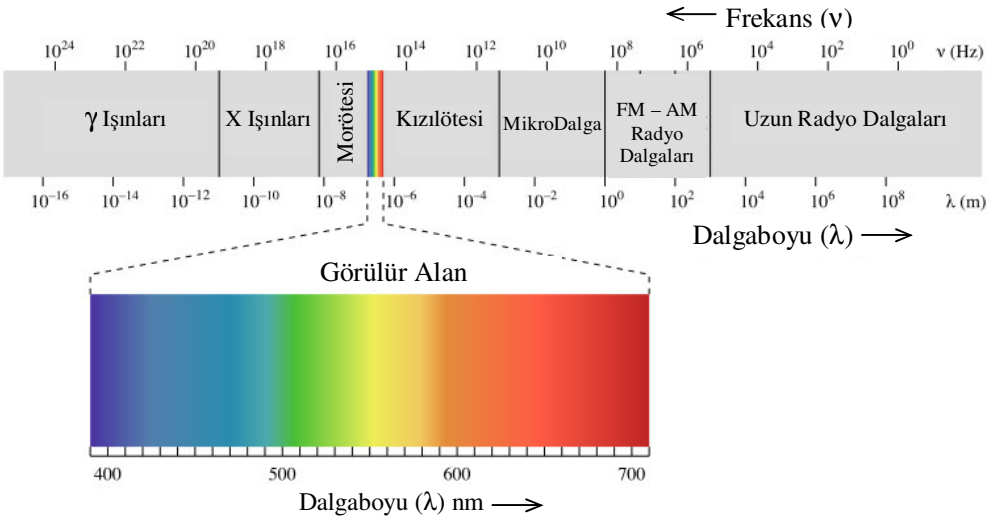
Işık, gözün görme işlemini gerçekleştirmesinde önemli rol oynayan elektromanyetik bir radyasyon türüdür. 1666 yılında Newton, beyaz güneş ışığını cam bir prizmadan geçirerek beyaz ışığı meydana getiren ışık tayfını keşfetti. Newton'un elde ettiği Mor'dan Kırmızı'ya kadar farklı renklerden meydana gelen bu ışık tayfı gökkuşağı renkleri olarak da bilinir. Elektromanyetik tayfa bakıldığında görülebilir ışığın dalgaboyu elektromanyetik tayfın çok küçük bir bölümünde, 350nm – 780nm değerleri arasındadır. Elektromanyetik tayf; dalgaboyu, frekans veya enerji ile ifade edilebilir. Dalgaboyu (λ) ve frekans (v) arasında aşağıda görüldüğü gibi bir bağlantı vardır;

$$\lambda = \frac{c}{v} \tag{2.3}$$

burada c, ışık hızını ($2.998*10^8$ m/s) göstermektedir. Enerji ise şu şekilde hesaplanabilir;

$$E = h \times v \tag{2.4}$$

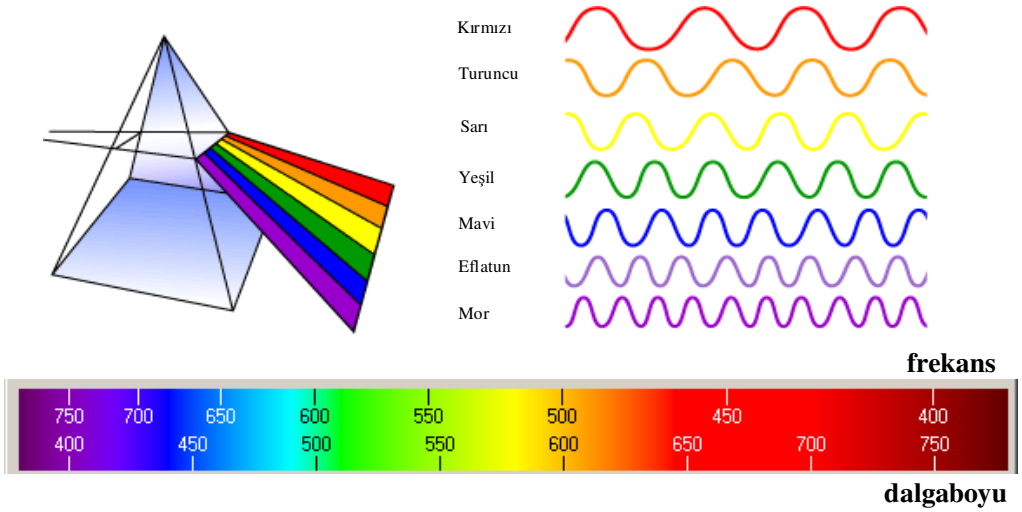
burada h, Planck sabitidir.



Şekil 2.4. Enerji tayfındaki görülebilir ışık alanı.

2.3.1. Görülebilir ışık

Görülebilir tayf ya da optik tayf, elektromanyetik tayfın bir parçasıdır ve görülebilir ışık veya sadece ışık olarak adlandırılır. Bu alanın görülebilir olarak adlandırılmasının sebebi, elektromanyetik tayf üzerindeki diğer enerji formlarından farklı olarak insan gözü tarafından algılanabilmesinden dolayıdır. Görülebilir ışığın sahip olduğu frekans aralığı dışında frekans yayan dalgalar ise İGS tarafından algılanamamaktadır (morötesi, kızılötesi vb.) (Şekil 2.4). Elektromanyetik tayfta görülebilir alanın dalgaboyu değerleri Şekil 2.4'de de görüldüğü gibi 350nm (mor) ile 780nm (kırmızı) arasındadır. Her bir renk farklı bir dalga boyuna sahiptir. Kırmızı renk en uzun dalga boyuna sahip iken mor renk ise en kısa dalga boyuna sahiptir. Bu aralıktaki renkler ise sırasıyla; mor, mavi, yeşil, sarı, turuncu ve kırmızıdır. Görülebilir ışığa ait renk tayfını elde etmenin en yaygın yolu, ışığın bir prizmadan geçirilmesidir (Şekil 2.5) [28].



Şekil 2.5. Görülebilir Işık Dalgaboyu.

2.3.2. Renk teorisi ve renk modelleri

İnsan gözü parlaklık, renk tonu ve doygunluk gibi bileşenlere sahip renkleri fark eder [29]. Kırmızı, Yeşil ve Mavi ana renkler olup bunların belirli oranlarda karıştırılmasıyla diğer renkler elde edilir. Bir renk X, Y ve Z katsayılarının aldığı değerlere göre elde edilir. Bu katsayılar aşağıdaki gibi belirlenmiştir;

$$X = \frac{X}{X+Y+Z},\ Y = \frac{Y}{X+Y+Z},\ Z = \frac{Z}{X+Y+Z} \tag{2.5}$$

Ve bu katsayıların toplamı her zaman 1'e eşittir.

$$X + Y + Z = 1 \tag{2.6}$$

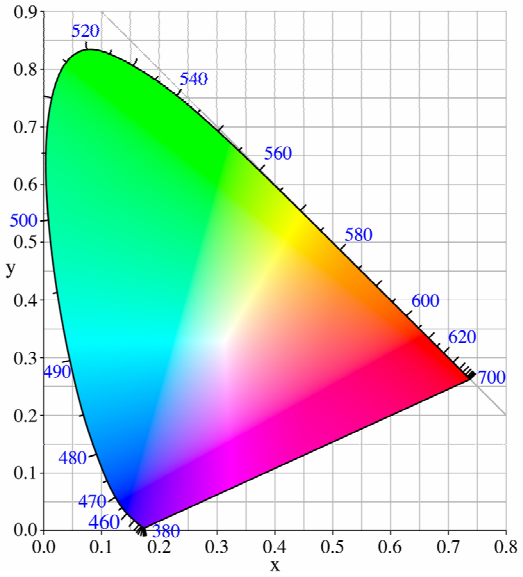
Diğer renkleri elde etmek için kullanılan başka bir yaklaşım ise CIE diyagramıdır. 1931 yılında ana renkleri uluslararası standart haline getirmek için bu diyagram geliştirilmiştir. CIE diyagramında, birbirlerinin karışımlarından diğer bütün renklerin elde edildiği gerçek üç renk yoktur. Bu yüzden CIE diyagramında ana renkler belirlenirken gerçek renkler göz önüne alınmamıştır. Örneğin, gerçek olmayan üç ana renk A, B ve C olsun. Bu renklerden diğer renkleri elde edebilmek için aşağıda verilen denklemlerden faydalanılır.

$$x = \frac{A}{(A+B+C)} \tag{2.7}$$

$$y = \frac{B}{(A+B+C)} \tag{2.8}$$

$$z = \frac{C}{(A+B+C)} \tag{2.9}$$

Burada x ve y biliniyorsa $x + y + z = 1$ eşitliğinin sonucunda z bilgisine ulaşmak mümkündür.



Şekil 2.6. CIE kromatik diyagram.

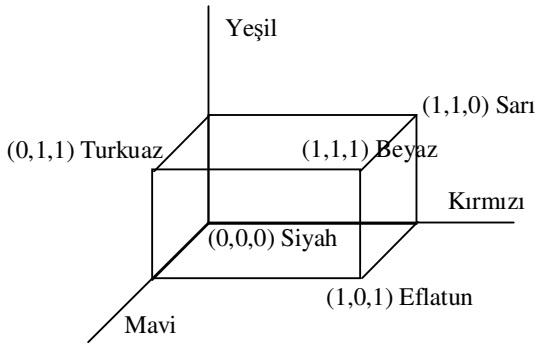
Yukarıdaki CIE diyagramı bütün görülebilir renkler için X değerine karşı Y değerini göstermektedir. Sıfır noktasından beyazı gösteren enerji noktasına doğru doygunluk sıfır değerine giderken, diyagramın sınırlarındaki noktaların tamamen doygun olduğu varsayılır.

Literatürde kullanılan birçok renk modeli şeması vardır. Bunlar; RGB, CMY(K), HSI olarak sınıflandırılabilir.

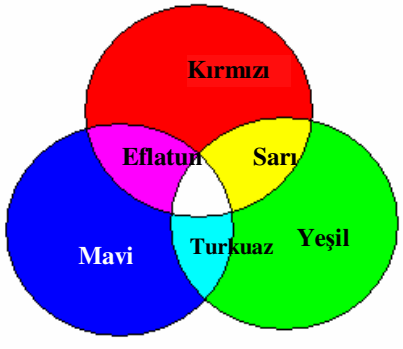
2.3.2.1. RGB renk modeli

RGB renk modeli, fosfor yapıların ışık yayması prensibine dayanarak oluşturulmuş, toplamsal (additive) bir renk modelidir. Bu renk modelinde Kırmızı (Red), Yeşil (Green) ve Mavi (Blue) ana renkler olarak kullanılır. Modelin ismi de bu renklerden gelmektedir. Diğer renkler bu ana renklerin karışımından elde edildiği için bu renk modeli toplamsal renk modeli olarak da ifade edilir. Beyaz renk kırmızı, yeşil ve mavi renklerinin hepsini içermekte, siyah ise hiçbirini içermemektedir. Bu model genellikle televizyon, bilgisayar ekranı gibi aktif göstergelerde kullanılır.

RGB renk modeli Şekil 2.7.a'da gösterilen bir küp ile ifade edilir. Küpün bir köşesi koordinat sisteminin orijinindedir. Koordinat sisteminin orijini (0,0,0) değerine sahip olduğundan siyah renge karşılık gelmektedir. Orijine köşegensel olarak karşılık gelen (1,1,1) noktası ise beyaz renge karşılık gelir. Diğer renkler ise şekilde de görüldüğü gibi ifade edilir.



(a) Küp modeli



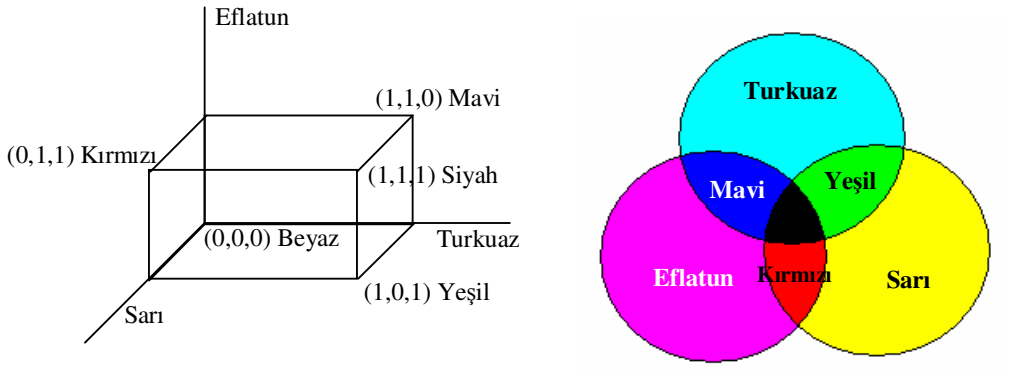
(b) Diyagonal model

Şekil 2.7. RGB renk modelleri

RGB renk modeli yaygın olarak kullanılmasına rağmen, görüntüyü elde etmekte faydalanılan cihazlara bağımlı olması bir dezavantajdır. Bununla birlikte baskı ortamında değil de Internet veya sayısal ortamda yapılan çalışmalarda RGB renk modelinin kullanılması bir avantajdır. Baskı ortamında yapılan çalışmalar için ise CMYK renk modeli geliştirilmiş ve matbaacılıkta da bir standart halini almıştır [30].

2.3.2.2. CMYK renk modeli

Bu renk modelinde Turkuaz (Cyan), Eflatun (Magenta) ve Sarı (Yellow) ana renk olarak kullanılır. Bu renk modelinde RGB renk modelinin tersine diğer renkleri elde etmek için bir nevi çıkarma işlemi uygulanır. Diğer renkleri elde etmek için çıkarma işlemi kullanılması nedeni ile bu renk modeli eksiltici (subtractive) renk modeli olarak da ifade edilir. Diğer renklerin elde edilmesinde, hangi renk için hangi ana renklerin emilmesi veya yansıtılması gerektiği Tablo 2.2'de verilmiştir. Bu işlem için renklere yansıtıcı olmayan bazı pigmentler eklenerek o rengin görülmemesi sağlanır. Bu renk modeli genellikle yazıcılarda, matbaalarda ve yüksek seviyeli baskı gerektiren alanlarda kullanılır.



(a) Küp modeli (b) Diyagonal model

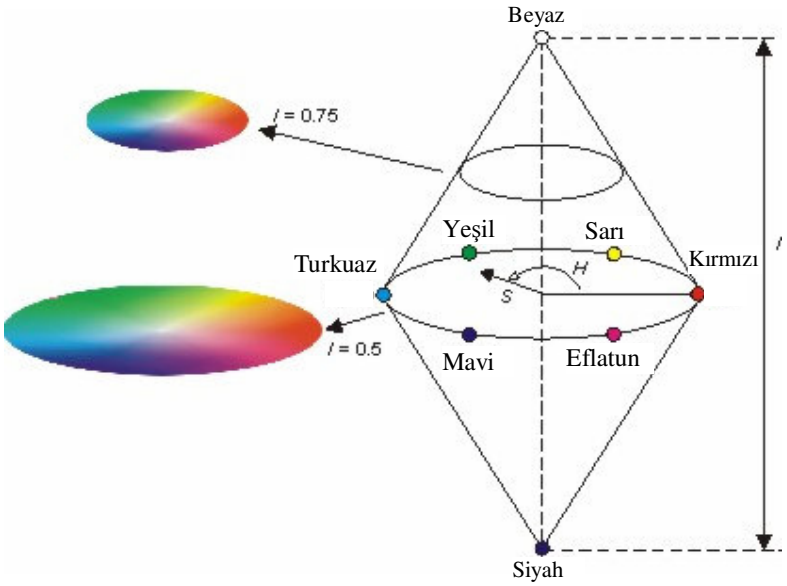
Şekil 2.8. CMYK renk modelleri

Tablo 2.2. CMYK renk modelinde diğer renklerin elde edilmesi.

Ana Renk	Emilme	Yansıtma
Turkuaz	Kırmızı	Mavi ve Yeşil
Eflatun	Yeşil	Mavi ve Kırmızı
Sarı	Mavi	Kırmızı ve Yeşil
Siyah	Hepsi	Hiçbiri

2.3.2.3. HSI renk modeli

HSI (Hue-Saturation-Intensity) renk modelinde ise parlaklık/keskinlik (I), renk bilgisinden ayrıştırılmıştır. Renk bilgisi renk tonu (Hue) kanalı ve doygunluk (Saturation) kanalı ile oluşturulur. HSI renk modeli renkler üzerindeki işlemlerde daha çok sezgisel olması ve yaklaşık olarak insan algılaması ve yorumlamasına yakın olması için geliştirilmiştir. Böylece interaktif uygulamalar sırasında, kullanıcıların beklentilerine cevap verebilecek şekilde renkli resimler üzerinde işlem yapılması uygun hale gelmektedir.



Şekil 2.9. HSI renk modelindeki renklerin gösterimi [31].

Şekil 2.9'da görülen HSI renk modelinde, Ton (H) bileşeni, 0–360 derece arasındaki açılarla rengi belirtir. 0 derece kırmızı, 60 derece sarı, 120 derece yeşil, 240 derece mavi ve 300 derece eflatun rengi göstermektedir.

Doygunluk (S) bileşeni ne kadar rengin beyaz ile birleştirileceğini gösterir. [0,1] arasında değer alır.

Şiddet (I) bileşeni ise [0,1] arasında değer alır. 0 siyah, 1 ise beyaz anlamına gelmektedir.

2.3.3. Renk modelleri arasındaki matematiksel dönüşümler

Uygulamalardaki kullanım alanlarının farklı olması nedeni ile teorik olarak da renk modelleri arasında dönüşüm yapma ihtiyacı doğmuştur. Aşağıda en çok kullanılan renk modelleri arasındaki matematiksel ifadeleri gösteren denklemler verilmiştir. Denklem 2.10 RGB ve CMYK renk modelleri arasındaki dönüşümün denklemini, denklem 2.11 RGB ve YIQ renk modelleri arasındaki dönüşümün denklemini ve denklem 2.12 ise RGB ve HSI renk modelleri arasındaki dönüşümün denklemini göstermektedir.

$$\begin{bmatrix} C \\ M \\ Y \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} - \begin{bmatrix} R \\ G \\ B \end{bmatrix} \tag{2.10}$$

$$\begin{bmatrix} Y \\ I \\ Q \end{bmatrix} = \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ 0.596 & -0.275 & -0.321 \\ 0.212 & -0.523 & 0.311 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix} \tag{2.11}$$

$$\begin{aligned} I &= \frac{1}{3}(R+G+B) \\ H &= \cos\left\{ \frac{\frac{1}{2}\left[(R-G)+(R-B)\right]}{\left[(R-G)^2+(R-B)(G-B)\right]^{1/2}} \right\} \\ S &= 1-\frac{3}{(R+G+B)}\left[\min(R,G,B)\right] \end{aligned} \tag{2.12}$$

2.4. Sayısal Görüntü ve Temel Terminoloji

Bilgisayarların ve sayısal cihazların yaygınlaşması, aynı zamanda sayısal haberleşmenin analog haberleşmeden daha kolay uygulanabilir hale gelmesi ile tüm bilgi türlerinde olduğu gibi sayısal görüntünün de sayısal ortama aktarılması gereksinimini ortaya çıkarmıştır. Sayısal görüntülerin özellikle Internet üzerinden haberleşme amacıyla yoğun bir şekilde kullanılmaya başlanmasından itibaren sayısal görüntüler popüler hale gelmiştir.

2.4.1. Sayısal görüntünün temel taşı: piksel

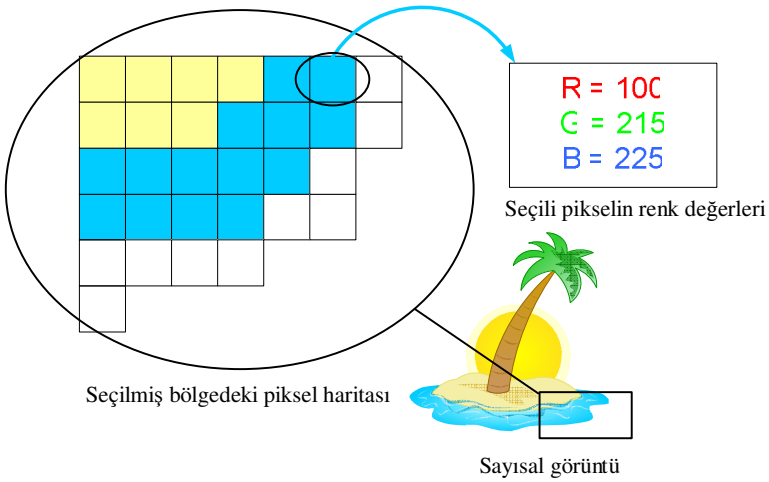
Sayısal görüntüyü oluşturan en küçük yapı taşı piksel olarak isimlendirilir. Bütün sayısal görüntüleme ortamlarında (sayısal televizyon ve monitörler, yansıtım cihazları vs.) kullanılan görüntü alanları bu piksellerin bir araya gelmesi ile oluşturulmaktadır. Bir piksel, piksel başına düşen bit sayısı (bit-per-pixel – bpp) ile ifade edilir. Örneğin, 1 bpp ile ifade edilen bir resim her piksel için 1 bit kullanır. 2 bpp resim 4 renk ve 4 bpp resim ise 16 renge sahiptir.

- 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 bir görüntüyü oluşturan bir piksel, Kırmızı (Red), Yeşil (Green) ve Mavi (Blue) renklerinin birleşmesinden oluşmaktadır. Bu üç ana rengin belirli oranlarda karışımı ile diğer yardımcı renkler elde edilmektedir. Yüksek renk yani 16–bit'lik sayısal görüntülerde, renk bileşenleri için bit dağılımı; 5–bit kırmızı renk, 6–bit yeşil renk ve 5–bit mavi renk şeklindedir (Tablo 2.3). Bunun sebebi ise insan gözünün yeşil renkteki hatalara diğer iki renkten daha çok hassasiyet göstermesidir. Gerçek renk yani 24–bit'lik sayısal görüntülerde ise her bir ana renk 8–bit (1 Bayt) olarak gösterilir. Bu durumda her bir piksel toplam 24–bit'e (3 Bayt) karşılık gelmektedir. Bilgisayar ekranları gibi bazı sistemlerde 32–bit renk derinliği kullanılmaktadır. Buradaki fazla 8–bit ile opaklık yani ışık geçirmezliği gerçekleştirmek için kullanılır [32].

Tablo 2.3. 16–bit sayısal görüntü için bit dağılımı.

Bit	**15**	**14**	**13**	**12**	**11**	**10**	**09**	**08**	**07**	**06**	**05**	**04**	**03**	**02**	**01**	**00**
Renk Bilgisi	R	R	R	R	R	G	G	G	G	G	G	B	B	B	B	B



Şekil 2.10. Örnek bir sayısal görüntünün piksel haritası.

Şekil 2.10'da örnek bir sayısal görüntü görülmektedir. Şekilde görüntünün seçilen belirli bir alanına ait piksel haritası yakınlaştırılarak sunulmuştur. Şekil 2.10 incelendiğinde her bir pikselin R,G,B renk ağırlıklarının birleşmesi ile tek bir renk aldığı görülmektedir. Pikseller görüntü alanını meydana getiren en küçük noktacıklardır ve ekrana bakan insan odaklandığı görüntü alanını bütün bir resim olarak görecektir.

Gerçek görüntüyü temsil edecek nokta (piksel) sayısı ne kadar fazla olursa sayısal görüntü gerçek görüntüye o kadar yakınlaşacaktır. Gerçek görüntü sayısal görüntüye çevrilirken kullanılacak piksel sayısı yeterli seçilmezse içeriğinde farklı renkler bulunan (özellikle görüntüde nesne kenarlarının bulunduğu) küçük alanlar tek bir renk ile ifade edileceğinden net bir görüntü oluşturulamaz. Sayısal görüntüye bakan insan görüntüyü bulanık, nesne kenarlarının net algılanamadığı bir resim olarak görür.

Sayısal görüntü bilgisi içinde bulunan bilgi, piksellerin adreslerine göre renk koyuluk değerleridir. Piksellerin renk koyuluk değerlerini ifade etmek için üç ana rengin (kırmızı, yeşil, mavi) ne oranlarda birbirlerine karıştırıldığı bilgisi verilir. Bu yaklaşım tüm gerçek renkleri üç ana rengin değişik oranlarda karıştırılarak elde edilebileceği bilgisine dayanarak ortaya çıkmıştır. Sayısal görüntüde her bir piksel için üç renk bileşeninin koyuluk değerlerinin verilmesi rengin oluşturulması için

yeterlidir. Örneğin beyazı elde etmek için kırmızı, yeşil, mavi renklerinin hepsi tam koyulukla karıştırılması gerekmektedir. Bu tanımlama bir standart haline gelmiştir ve RGB resim kodlama olarak adlandırılmaktadır.

RGB resim kodlamada; her renk koyuluk değerinin nitelendirileceği en büyük sayı, renk kalitesini belirler. Bunun anlamı; bir piksel ne kadar çok bit ile ifade edilirse kalite o kadar artar. Şekil 2.10'daki örnek resimde her bir piksel 8–bit renk değerine sahiptir. Örneğin renkleri belirtmek için 4–bit seçilirse; her renk için koyuluk ve açıklık 16 farklı şekilde ifade edilecektir ki bu da renkleri ayrıntılı ifade etmekten uzaktır. Bununla birlikte her bir rengi belirtmek için ne kadar az bit kullanılırsa o resim dosyasının boyutu o oranda düşecek ve hafızada o kadar az yer kaplayacaktır.

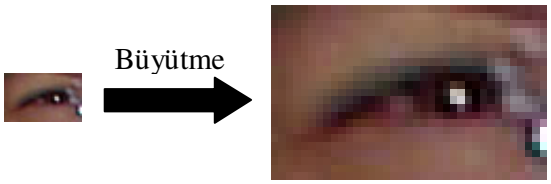
RGB kodlama tekniğinde her renk için 1bayt (8–bit) kullanılması standart haline gelmiştir ve bir pikseli ifade etmek için 3bayt hafıza alanına ihtiyaç vardır. Böylece her bir piksel 24–bit renk değerine sahip olur ve her renk bileşeni 256 koyuluk değeri ile nitelendirilir. Bu durum RGB renkler için, 0 değeri pikselin renk içermediğini, 255 değeri ise pikselin tam koyulukta bir renk içerdiğini belirtir. Bir örnekle bunu açıklayacak olursak, RGB değeri 0,0,0 olan bir piksel siyah, 255,255,255 olan bir piksel ise beyaz renktedir. Şekil 2.10'da RGB kodları gösterilen mavi renkli piksel 100 kırmızı ağırlığına, 215 yeşil ağırlığına, 225 mavi ağırlığına sahiptir.

2.4.2. Çözünürlük ve çözünürlüğün depolanma kapasitesine etkisi

Basit bir ifadeyle çözünürlük; resimdeki detayların iyi bir şekilde ayırt edilebilmesidir [33]. Başka bir ifadeyle çözünürlük, resmin yatay ve dikey olarak kaç piksel ile gösterildiği bilgisidir. Örneğin bir resim için 640×480 çözünürlüğe sahiptir ifadesi kullanıldığında; bu resim alanının dikey olarak 480 piksel, yatay olarak 640 piksel kullanılarak oluşturulduğu (640×480= 307200 piksel içerdiği) anlaşılır. O halde bir sayısal görüntü için çözünürlük ne kadar yüksek ise gerçek görüntüye o kadar yakın bir görüntüdür (o kadar nettir) denilebilir.

Bir sayısal resimde örnekleme yapılan uzamsal frekans değeri (örnekleme frekansı) çözünürlüğü göstermek için kullanılan nesnel bir ölçüttür. Genellikle örnekleme

frekansını artırmak çözünürlüğü de artırır. Bu durum sayısal resimlerin çözünürlüğünden bahsederken neden genellikle her bir inç başına düşen nokta (dpi) veya her bir inç başına düşen piksel (ppi) kullanıldığını göstermektedir. DPI (Dot Per Inch) sayısal görüntülerde çözünürlük bilgisini göstermek için kullanılan bir ölçektir. 1 inç (2.54 cm) uzunluğundaki bölgenin ne kadar noktadan meydana geldiğini gösterir. Örneğin, 600×600 dpi çözünürlüğündeki bir görüntünün eni ve boyu her inç başına 600 nokta uzunluğundadır.



Şekil 2.11. Bir resmin yakınlaştırılması.

Bir sayısal resmin hafızada kapladığı alan; resmin yükseklik bilgisi, genişlik bilgisi ve renk derinliği bilgileri verildiği takdirde denklem 2.13 yardımıyla hesaplanabilir;

$$\text{Dosya Boyutu} = (\text{yükseklik} \times \text{genişlik} \times \text{renk derinliği}) / 8 \qquad (2.13)$$

Formülde 8'e bölme işlemi sonucun bayt (byte) cinsinden ifade edilmesi içindir. Tablo 2.4'de bazı örnek hesaplamalar verilmiştir.

Tablo 2.4. Görüntü boyutu hesaplama tablosu.

Piksel Boyutu	**Renk Derinliği (bit)**	**Resim Boyutu (bayt)**
2,048 × 3,072	24	150,994,944
1,024 × 768	24	18,874,368
800 × 600	24	11,520,000
2,048 × 3,072	16	100,663,296
1,024 × 768	16	12,582,912
800 × 600	16	7,680,000

2.4.3. Görüntü sıkıştırma

Sayısal görüntülerin daha kullanışlı ve paylaşımı kolay olması açısından boyutlarının düşürülmesi gerekmektedir. Bunun için üç farklı yöntem izlenebilir;

1. Çözünürlüğün ve uzunluğun düşürülmesi,

2. Bağımsız piksellerin ve renk derinliğinin düşürülmesi,
3. Sıkıştırma işlemi.

Görüntü sıkıştırma sıklıkla depolama alanından avantaj sağlamak için, dosya transferi yapmak için ve görüntü işleme için uygulanan bir işlemdir. Bütün sıkıştırma teknikleri matematiksel ifadelerle oluşturulmuş algoritmaları kullanır. Kullanılan algoritmaya göre sıkıştırma işlemi kayıplı veya kayıpsız olarak adlandırılabilir. Kayıpsız sıkıştırma tekniklerinde sıkıştırma işlemi sırasında resimden herhangi bir bilgi atılmaz. Örnek olarak ITU-T.6 tekniği dosya uzantısı olarak da bmp uzantılı resimler gösterilebilir. Kayıplı sıkıştırma da ise, sıkıştırma işlemi sırasında resimden insan gözü tarafından algılanamayacağına karar verilen bazı bilgiler atılır. Bu sıkıştırma formatının ismi standardı geliştiren gurubun ismiyle anılır Birleşik Fotoğraf Uzmanları Grubu (Joint Photographic Experts Group–JPEG). Sayısal videolardaki sıkıştırma Hareketli Resimler Uzmanlar Gurubu'nun (Moving Pictures Experts Group–MPEG) geliştirdiği standartlara göre yapılmaktadır. Resim ve video sıkıştırma için belirlenmiş dünya standartları Tablo 2.5'de listelenmiştir.

Tablo 2.5. Sıkıştırma standartları ve uygulama alanları.

Sıkıştırma Standardı	**Uygulama Alanı**
CCITT G3/G4	İkili resimler (uyarlanamayan)
JBIG	İkili resimler
JPEG	Siyah-Beyaz ve renkli hareketsiz görüntüler
H.261	pX64 kbps
MPEG–1	1.5 Mbps
MPEG–2	10–20 Mbps
MPEG–4	4.8–32 kbps (haberleşme ortamında)

CCITT Gurup 3 ve Gurup 4 kodları faks iletişiminde kullanılan sıkıştırma standardıdır. JBIG, CCITT Gurup 3 ve Gurup 4 standardında karşılaşılan problemlere çözüm getirmek için geliştirilmiş bir standarttır. JPEG siyah-beyaz veya renkli hareketsiz görüntülerin sıkıştırılması için geliştirilmiş bir standart olmakla beraber, hareketli görüntülerde de çerçevelerin sıkıştırılması yoluyla kullanılabilmektedir. H.261 video sıkıştırma standardı ISDN hatlarda video konferans uygulamalarında kullanılmaktadır. ISDN hatların desteklediği bit hızı pX64 kbps'dir. Buradaki 'p' sabiti video konferans sırasında kullanılan formata bağlı olarak değişmektedir. Genellikle video konferans uygulamalarında CIF formatı

kullanıldığından p=6 olmaktadır. MPEG–1 sıkıştırma formatı CD-ROM üzerinde depolanan videolar için geliştirilmiştir. MPEG–2 ise yüksek kaliteli televizyon (HDTV–High Definition TV) uygulamalarında kullanılmaktadır. MPEG–4 standardı ise Internet üzerinden gerçek zamanlı video görüşmesi uygulamaları için geliştirilmiştir [34].

2.4.3.1. MPEG video sıkıştırma standardı

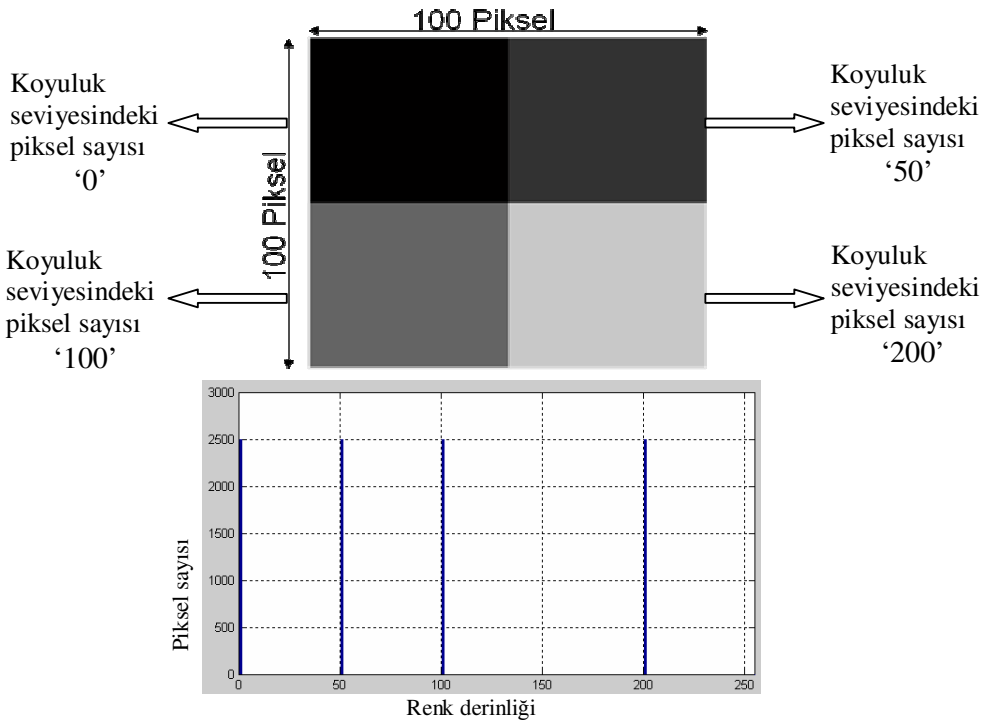
MPEG sıkıştırmada temel fikir video çerçevelerindeki uzamsal fazlalıkları ve çerçeveler arasındaki zamansal fazlalıkları silmektir. Örneğin bir sıkıştırma algoritmasında uzamsal fazlalıkları silmek için ayrık kosinüs dönüşümü (Discrete Cosine Transform–DCT) kullanılır.

MPEG sıkıştırma algoritmasında görüntü renk formatı YUV renk uzayındadır. Eğer RGB renk uzayına sahip bir görüntü varsa MPEG uygulanırken renk uzayı önce YUV formata dönüştürülür. YUV formatında da görüntüler 24–bit olarak ifade edilir. 8–bit parlaklık bilgisi için (Y), geri kalanı ise renklilik (U ve V) için kullanılır.

2.4.4. Görüntünün histogramı ve temel histogram işlemleri

Histogram bir sinyalin sahip olduğu frekans bileşenleri hakkında bilgi veren bir gösterimdir. Analog bir işaret için histogram, analog işaretin hangi frekans değerinde bileşenleri olduğu, her bir frekans değeri için kaç adet bileşen olduğu bilgilerini verir. Analog işaretler için işaretin histogramı sayesinde işaret bileşenlerinin hangi frekanslarda yoğunlaştığı bilgisine ulaşılır. Sayısal resimlerde veya videolarda ise histogram grafikleri resmin renk bileşenleri hakkında bilgi verir. Sayısal resimlerde veya videolarda histogramlar için frekansların yerini renk koyuluk değerleri almaktadır. Bir video çerçevesinin histogramı, 0–255 arası renk ağırlık değerlerine ait kaç tane piksel olduğu konusunda bilgi verir. Örneğin bir resme ait histogram grafiği 255 değerine yakın bir bölgede yoğunlaşıyorsa o resmin neredeyse beyaz bir resim olduğu yorumu yapılabilir. Eğer histogram 0 değerine yakın bölgede yoğunlaşıyorsa resmin neredeyse siyah renk bir resim olduğu yorumu yapılabilir.

Histogram grafiği farklı koyuluk değerlerine dağılmışsa resmin çok renk içeren dolayısıyla farklı objeler içeren bir resim olduğu yorumu yapılabilmektedir.



Şekil 2.12. 100×100 piksel boyutuna sahip örnek bir siyah-beyaz bir resim ve resme ait gri koyuluk değer histogramı.

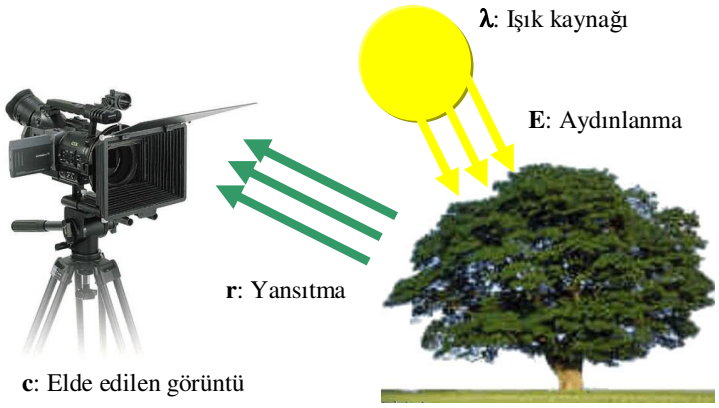
Şekil 2.12'de 100×100 piksel boyutlarına sahip örnek bir siyah-beyaz resim ve resme ait histogram grafiği görülmektedir. Şekildeki resimde toplam 10.000 adet piksel vardır ve bunların 1/4'ü "0" koyuluk değerine, 1/4'ü "50" koyuluk değerine, 1/4'ü "100" koyuluk değerine, 1/4'ü ise "200" koyuluk değerine sahiptir, yani resimde 0, 50, 100, 200 koyuluk değerlerine ait 2500'er adet piksel yer almaktadır. Histogram grafiği incelendiğinde bahsedilen koyuluk değerlerinde bulunan piksel sayılarının histogram grafiğinde yer aldığı görülmektedir.

Renkli resimlere ait histogram grafikleri her bir renk değeri için elde edilmeli ve beraber değerlendirilmelidir. Sayısal resimlerde R,G,B, bileşenleri yer aldığından üç adet ayrı histogram grafiği (kırmızı, yeşil ve mavi histogramları) elde edilmelidir.

2.5. Sayısal Video ve Oluşumu

Hareketsiz sayısal görüntülerin (resimlerin) ardı sıra saniyede 25 kez veya üzerinde oynatılması ile elde edilen hareketli görüntüye sayısal video denir. Bu her bir sayısal görüntüye çerçeve (frame) denilir ve saniyedeki çerçeve sayısına fps (frame per second – saniyedeki çerçeve sayısı) denilmektedir. Hareketsiz resimlerin saniyede 25 kez veya daha fazla oynatılmasının nedeni, insan gözünün 25 Hz üzerindeki frekanslara hassasiyet gösterememesidir. Bu işlemin sonucunda insan gözü resimleri hareketli bir görüntü olarak algılamaktadır.

Sayısal videonun oluşması için gerekli olan şartlar Şekil 2.13'de gösterildiği gibi; bir ışık kaynağı (λ: Dalgaboyu), ışık kaynağının aydınlattığı bir nesne (E(x, y, z, λ), x,y,z: koordinatlar) ve nesnenin ışığı yansıtmasıdır (r(x, y, z, λ), x,y,z: koordinatlar).



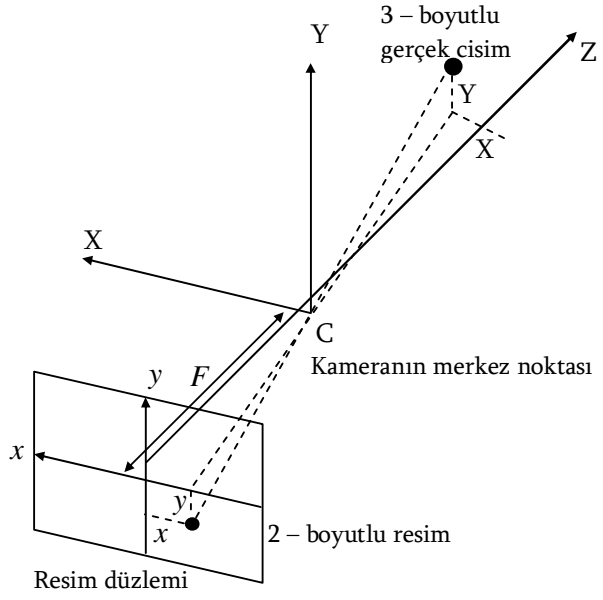
Şekil 2.13. Basit bir görüntünün oluşması.

Şekil 2.13'de görülen hadise matematiksel olarak ifade edildiğinde aşağıdaki gibi bir denklem elde edilir;

$$c(x, y, z, \lambda) = E(x, y, z, \lambda) \times r(x, y, z, \lambda) \qquad (2.14)$$

Kamerada elde edilen sayısal görüntü ise Şekil 2.14'de gösterildiği gibi insan gözünde bir görüntünün oluşması ile tamamen aynıdır. 3–boyutlu gerçek bir görüntü kameradaki resim düzleminde 2–boyutlu olarak ifade edilmektedir. Dikkatle

incelendiğinde Şekil 2.14'de verilen yapının Şekil 2.3'de verilen insan görme olayını ifade eden yapı ile tamamen aynı olduğu anlaşılacaktır.



Şekil 2.14. Sayısal bir görüntünün kamerada elde edilmesi.

$$x = F\left(\frac{X}{Z}\right)$$
$$y = F\left(\frac{Y}{Z}\right) \qquad (2.15)$$

Denklem 2.15'de kullanılan F kameranın odak mesafesidir.

Sayısal videolar sıkıştırılmış video ve sıkıştırılmamış video olarak iki farklı formata sahiptirler. Sayısal medyanın gelişmesi ve kullanımının artması ile sıkıştırılmamış video formatı ilk kullanılan video türüdür. Fakat sıkıştırılmamış video dosyaları hafızada çok büyük yer kapladığından ve paylaşımının zorluklarından dolayı sıkıştırma teknikleri gelişmiş ve buna bağlı olarak da sıkıştırılmış video türleri geliştirilmiştir.

Sıkıştırılmış videolarda kullanılan sıkıştırma tekniklerinin sayısı gün geçtikçe gelişen sıkıştırma teknolojilerindeki hızlı ilerlemeye paralel olarak artmaktadır (MPEG2, MPEG4, H.264 (MPEG–4 AVC), WMV9 (VC–1), M–JPEG (Motion JPEG), SM4).

Geliştirilen standartların birçoğu farklı sıkıştırma yöntemlerini kullanarak yüksek kaliteye sahip hafızada daha az yer kaplayan videoların oluşturulması üzerine yoğunlaşmıştır.

Sıkıştırılmamış dosya türlerinde ise en çok bilineni ve kullanılanı AVI (Audio–Video Interleave) dosya türüdür. AVI formatındaki dosyalar; ses ve görüntünün birleştirilmesi ile oluşturulmuş videolardır. Bu formattaki videolar BMP formatındaki sıkıştırılmamış resim dosyalarının ardı sıra eklenmesi ile oluşturulur. Bu sebeple resim dosyaları üzerindeki kapasite hesabı, çözünürlük hesabı gibi işlemler AVI formatındaki videolar için de geçerlidir. Ayrıca tez çalışması süresince geliştirilen veri gizleme algoritmaları AVI videoları için geliştirilmiştir. Deneysel çalışmalar süresince kullanılacak olan örnek videolardan 'Vipmen.avi' videosunun çerçeve yapısı Şekil 2.15'de görüldüğü gibidir.

Şekil 2.15. Örnek bir video çerçevesi.

Şekil 2.15'de verilen vipmen videosunun örnek çerçevesinin 120 x 160 boyutlarında olduğu görülmektedir. Bu bilgiye dayanarak deneysel çalışmalar esnasında kullanılacak olan 'vipmen.avi' videosunun hafızada kapladığı alan Denklem 2.1 yardımıyla aşağıdaki gibi hesaplanabilir.

$$120 \times 160 \times 30 \times 3 \times 9{,}43 = 16{,}300{,}742 \text{ bayt}$$

Elde edilen sonuca göre vipmen videosu hafızada 16,300,742 bayt yer kaplamaktadır. Vipmen videosunun sadece bir çerçevesi ise hafızada;

$$120 \times 160 \times 3 = 57{,}600 \text{ bayt}$$

yer kaplayacaktır.

2.6. Sonuç

Bu bölümde, İGS ve sayısal görüntü hakkında genel bilgiler verilmiştir. Sayısal görüntülerin gelişim süreçleri, uygulama alanları ve kazandırdıkları avantajları açıklanmıştır. Sayısal görüntü kalitesinin daha da artırılması için günümüzde araştırmacılar yoğun çaba sarf etmektedir. Özellikle daha az yer kaplayan kaliteli görüntüler elde etmek araştırmacıların ilgilendiği konuların başında gelmektedir. Görülebilir alan ışık dalgaboyu tayfında İGS'nin algılama sınırları ve taşıyıcı videonun histogram değerleri, gizli verinin taşıyıcı video içerisinde gömülebileceği en uygun alanları belirlemekte kullanılan en önemli belirleyici unsurdur.

BÖLÜM 3. VERİ GİZLEME İŞLEMİNE GENEL BAKIŞ

3.1. Giriş

Bu bölümde; genel olarak veri gizleme işlemi hakkında temel bilgilerin verilmesi ile yapılan tez çalışmasının amacının daha iyi anlaşılabilmesi amaçlanmıştır.

Özellikle son yıllarda bilgisayar ağları kullanımı olağanüstü derecede gelişmiş ve gelişmeye de devam etmektedir. Neredeyse kurulan tüm ağlar birbirine Internet vasıtasıyla bağlanabilmektedir. Böylece aradaki mesafeler kalkmış ve adeta herkesin evi dünyaya açılan bir pencere halini almıştır. Dünyanın bir ucu olan Çin'den diğer ucu Amerika'ya saniyeler içerisinde bir belge, resim veya video göndermek mümkün hale gelmiştir.

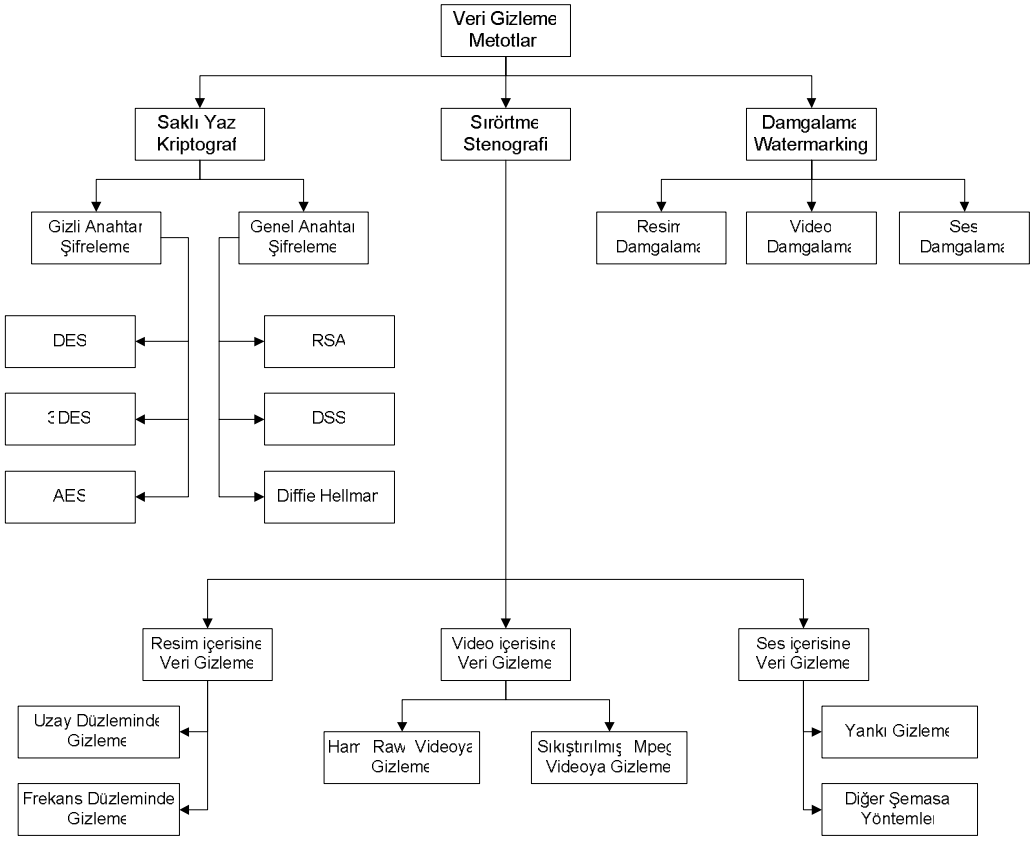
Bilgisayar ve Internet teknolojisindeki gelişmeye paralel olarak, paylaşma kolaylığı, kolay işlenebilirlik, kolay saklanabilirlik gibi özelliklere sahip sayısal medyada da önemli gelişmeler olmuştur. Bu sayede insanlar sadece yazılı metinleri paylaşmakla sınırlı kalmayıp, bir binanın mimari planını, bir ülkenin turistik merkezlerinin resimlerini veya yapılan önemli bir toplantının görüntülerini de paylaşabilme imkânına sahip olmuşlardır.

Teknolojinin bilgi paylaşımında sağlamış olduğu bu kolaylıklar karşısında beraberinde getirdiği en önemli tehdit haberleşmede mahremiyetin sağlanamamasıdır. Bu nedenle haberleşmede gizliliği sağlamak için yeni çalışmalar yapılmıştır. Veri gizleme veya veri gömme olarak bilinen bu çalışmalarda amaç; haberleşme esnasında yetkisiz veya izinsiz kişilerin haberleşme materyallerine ulaşmalarını engellemek ya da ulaşılan materyalleri yetkisiz kişilerce anlaşılmayacak bir forma dönüştürmektir.

Veri gizlemeyi konu edinen bilim dalı kriptolojidir. Kriptoloji, genellikle gizli formda, güvenlikli haberleşme ile ilgilenen matematik biliminin bir dalıdır. Yunanca kryptós (gizli) ve lógos (kelime) kelimelerinden türetilmiştir. Kriptoloji hakkında daha detaylı bilgi için [35], [36] kaynakları faydalı olabilir. Güvenli haberleşme için çözümler sunan birçok geleneksel ya da modern saklı yazı sistemleri yazı formatındaki verileri korumak için tasarlanmışlardır. Orijinal düz metin (plaintext), rasgele olarak anlamsız şifreli metine (ciphertext) dönüştürülmektedir. Şifreli metin alındığında şifre çözme algoritması kullanılarak metin orijinal haline dönüştürülmektedir.

Resimler, metinlerden farklı olduğu için saklı yazı sistemlerinin çoklu ortam dosyaları ile kullanılmasında bazı sıkıntılar meydana gelecektir. Resimleri doğrudan şifrelemek için geleneksel saklı yazı sistemleri (RSA ve DES gibi) kullanabilmemize rağmen bu sistemler iki nedenden dolayı uygun değildir; ilki resimlerin boyutları çoğunlukla metinlerden daha büyüktür. Bu nedenle geleneksel saklı yazı sistemleri resmi doğrudan şifrelemek için daha fazla süreye ihtiyaç duyarlar. İkincisi ise çözülen metnin orijinal metne eş olması zorunluluğudur. Ancak bu zorunluluk resim verisi için geçerli değildir. İnsan algısının karakteristiklerine göre resimdeki ufak bozulmalar genellikle kabul edilebilirdir [37]. Bu gibi nedenlerden dolayı çoklu ortam dosyalarının içerisine veri gizleme için sırörtme yöntemleri geliştirilmiş ve kullanılmıştır.

Sırörtme ve kriptografinin amacı, önemli bilgileri yetkisiz kişilere karşı korumak olduğu için sıklıkla birbirleri ile karıştırılmaktadırlar. Kriptografi; önemli bir bilgiyi karıştırarak anlaşılması imkânsız hale getirmeye çalışırken, sırörtme ise; gizli verinin varlığının anlaşılmasını engellemeye çalışır. Sırörtmenin hedefine ulaşamadığı durumlarda gizli veriyi analiz etmeye çalışan üçüncü kişiler de şüphe uyandırabilir. Bu durumun zayıf yönü her iki yöntemin birlikte kullanılması ile giderilebilir. Sonuç olarak, gizli veriyi bir şekilde algılayan izinsiz üçüncü kişiler, kriptografik yöntemleri kullanmadan orijinal bilgiye ulaşamayacaklardır [38],[39],[40].



Şekil 3.1. Veri gizleme metotları şeması.

Veri gizleme metotları Şekil 3.1'de görüldüğü gibi sınıflandırılmıştır. Şemaya göre veri gizleme metotları üç ana başlığa ayrılmaktadır;

1- Kriptografi (saklı yazı)
2- Stenografi (sırörtme)
3- Watermarking (Damgalama)

Kriptografi yani saklı yazı metodu daha çok yazılı mesajların anlaşılmaz bilgilere dönüştürülmesi esasına dayanarak çalışan bir yöntemdir. Bu yöntemde yetkisiz kişiler haberleşme bilgilerine bakarak gizli verinin varlığından haberdar olabilir fakat içeriği hakkında bilgi sahibi olamazlar.

Sırörtme, gizli verinin maskelenerek haberleşme ortamına gönderilmesi işlemidir ve sırörtmede en önemli amaç haberleşme ile ilgili olarak yetkisiz kişilerde en ufak bir şüphenin bile uyanmasını engellemektir.

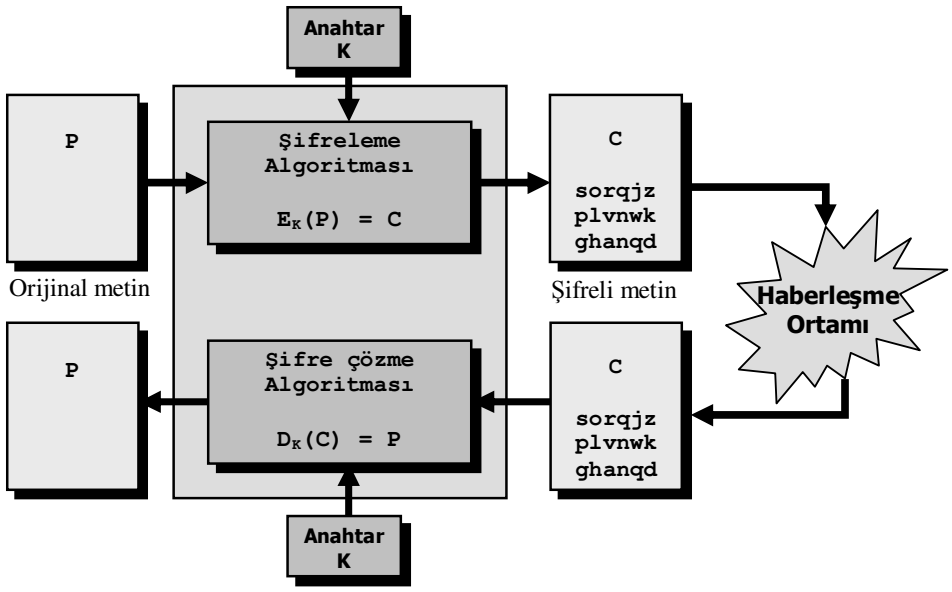
Damgalama metotlarında ise, amaç telif hakkı gibi önemli bilgilerin korunması olduğundan yetkisiz kişiler tarafından gizli veriyi ele geçirme veya yok etme saldırıları kaçınılmazdır. Bu yüzden damgalamada korunan bilginin ele geçirilememesi, yok edilememesi yani saldırılara karşı dayanıklılık en önemli unsurdur.

3.2. Kriptografi Kavramı ve Terminolojisi

Kriptografi terimi çoğu zaman kriptoloji bilim dalı ile aynı anlamda kullanılmaktadır. Bilindiği gibi kriptoloji; veri gizleme sanatı üzerinde çalışan bir matematik bilim dalıdır. Basit olarak kriptografi tanımını şu şekilde yapabiliriz; haberleşme bilgilerinin anlamsız karakter ya da dizilerden oluşturulmasını esas alan matematiksel yöntemler topluluğudur.

Kriptografi, orijinal bilginin doğal yapısını bozmadan elde edilmesi zor bir biçime dönüştürmek ve sonra tekrar eski haline geri döndürmek için çalışır. Farklı bir açıdan kriptografi; bilginin bilinmeyen bir biçime, anlaşılmaz ifadelere dönüştürülmesini sağlayan bir şifreleme yöntemidir. Şifrelenmiş bilgi saklanabildiği gibi başkalarına da gönderilebilir ve 3.kişiler–yetkisiz kişiler (şifrelimetni nasıl çözeceğini bilmeyen) için anlamsızdır.

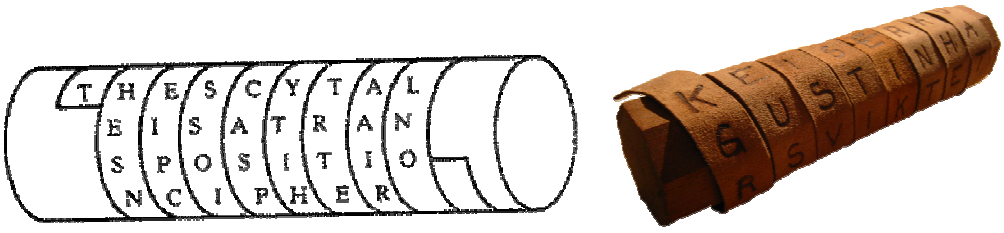
Genel olarak saklı yazı şifreleme yöntemi Şekil 3.2'de gösterildiği gibidir. Burada orijinal metin (P) şifreleme sisteminin giriş bilgisidir. Şifreleme algoritmasına orijinal metin ile birlikte, şifreleme işleminin saldırılara karşı daha dayanıklı olması için anahtar (K) bilgisi de giriş olarak verilir. Şifreleme algoritmasının çıkışında şifreli metin (C) elde edilir. Haberleşme ortamından (Internet, uydu vb.) gizli veri yetkili kişi veya kişilere iletilir. Şifreli bilginin orijinal bilgiye dönüştürülmesi işlemi, şifreleme işleminin tersi olarak çalışmaktadır. Şifreli metin ve anahtar şifre çözme algoritmasına uygulanır. Şifre çözme işlemi sonucunda orijinal metin elde edilir.



Şekil 3.2. Saklı yazı veri gizleme diyagramı.

3.2.1. Kriptografinin tarihçesi

Kriptografinin kökeni muhtemelen insanlığın var oluşunun başlangıçlarına, insanların iletişim kurmayı öğrenmeye başlamalarına kadar gitmektedir. [41], [42]. Mesajları şifrelemek için bilimsel metotların ilk kullanımı eski Yunanlılarla bağdaştırılabilir. Tahminen milattan önce 6 yıllarında gizli haberleşme için "scytale" isimli bir çubuk kullanılmıştır. Gönderici, şerit halindeki kâğıdı çubuk etrafına sarar ve mesajını boylamasına bu kâğıt üzerine yazardı. Daha sonra kâğıdın kıvrımlarını açarak düz hale getirir ve göndereceği adrese yollardı. Çubuğun çapı (gizli anahtar) bilgisi olmaksızın mesaj şifresinin çözülmesi olanaksızdır.



Şekil 3.3. Yunanlıların kullandığı "scytale" isimli çubuk [43].

Daha sonraları Roma orduları iletişimlerinde Sezar (alfabede 3 harf kaydırma) şifrelemesini kullanmışlardır.

Küçük bir örnek ile bu işlemi anlatacak olursak; şifrelenecek bilgi B harfi olsun. Şifreleme anahtarı da 12 ise şifreli metin K olacaktır. B alfabede 2. sırada ve anahtar 12 kullanılınca şifreli metin;

$$(2 +12) \text{ MOD29} =14$$

olarak bulunur ki 14. sayı alfabede K harfidir.

Yukarıdaki şifreleme işlemi matematiksel olarak şu şekilde ifade edilebilir;

$$C_i=(P_i +K) \text{ MOD29} \quad (3.1)$$

Şifre çözme işleminin matematiksel ifadesi ise;

$$P_i=(C_i-K+26) \text{ MOD29} \quad (3.2)$$

olur.

Burada, C: şifreli metin, P: orijinal metin, K: anahtar'dır.

1. ve 2. Dünya savaşları süresince kriptografinin gelişimi:

1. Dünya Savaşı süresince; Şifreleme sistemleri yüksek güvenlik seviyeli ve taktiksel haberleşmelerde kodların korunması için kullanılmıştır. 1920'lerde haberleşmenin telekomünikasyon ihtiyaçları ve elektromekanik teknolojinin olgunlaşması kripto elemanlar hakkında gerçek bir devrim getirmiştir.

2. Dünya savaşı süresince; taktik haberleşmesinde kriptanaliz çok önemli rol oynamıştır. 1930'larda 2. Dünya Savaşı sırasında Naziler tarafından bulunan Enigma makinesi İngilizlere ve Polonyalılara karşı büyük bir başarı göstermiştir. Bir takılabilir bord ve üç tane de birbiriyle değiştirilebilir rotordan oluşan Enigma Simetrik şifreleme kullanır.

Şekil 3.4. Alman ordusunun kullandığı “Enigma” şifreleme cihazı [44].

2. Dünya Savaşından sonra; 1973–1977 yıllarında Data Encryption Standard (DES) şifreleme algoritması geliştirildi. Fakat kullandığı 56-bit anahtar uzunluğu günümüzde kolayca çözülebildiğinden, DES yerini AES şifreleme algoritmasına (Advanced Encryption Standard) bırakmıştır. AES 128,192 veya 256-bit şifreleme anahtarı kullanmaktadır. Bu da bir bilgisayarın çözmesi için bile çok fazla zaman gerektiren bir anahtar uzunluğudur. 1976–1978 yıllarında ise Public Key Cryptography -Genel Anahtar Kriptografi- keşfedildi.

3.2.2. Şifreleme yöntemleri ve kullanılan algoritmalar

Kripto sistemlerde kullanılan şifreleme yöntemleri aşağıdaki gibi sıralanabilir;

1- Simetrik Anahtar Şifreleme
2- Genel Anahtar Şifreleme
3- Tek-Yol Fonksiyonu

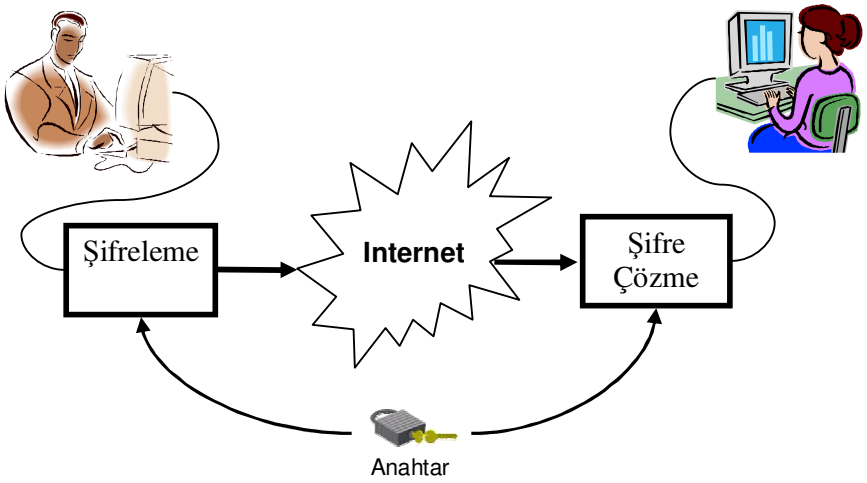
Bu yöntemlerden en çok kullanılanları ise simetrik ve genel anahtar şifreleme yöntemleridir.

3.2.2.1. Simetrik anahtar şifreleme

Kimi zaman bu şifreleme metodu gizli anahtar (secret-key) şifreleme veya tek-anahtar şifreleme olarak da adlandırılır. Simetrik şifrelemede, şifreleme ve şifre çözme işleminde kullanılan anahtarlar aynıdır.

Şifreleme ve şifre çözme işleminde kullanılan anahtar sadece orijinal metine ulaşması istenilen kişilere verilir. Haberleşecek kişiler önceden anahtarı belirlerler. Simetrik şifrelemenin güvenliği anahtarın güvenliğine bağlı olduğundan anahtarın gizli tutulması çok önemlidir.

Orijinal metini şifreleme işlemi için bir gizli anahtar seçilir ve bu gizli anahtar ile metin şifrelenir. Şifrelenmiş metin alıcı kişiye yollanır ve gizli bir şekilde gizli anahtar da alıcı kişiye bildirilir. Şifrelenmiş metini alan kişi bu metini, belirtilen gizli anahtar ile çözüp düz metine çevirir ve gizli veriye ulaşır. Bu şifreleme metodundaki en zayıf yön gizli anahtarın alıcıya bildirilmesidir. Bu bildirme işlemi, üçüncü kişiler tarafından bilinmemelidir. Çünkü gizli anahtarın üçüncü bir kişi tarafından bilinmesi şifrelenmiş metinin kolayca elde edilmesini sağlar. Anlatılan işlemler şekil 3.5'de resmedilmiştir.



Şekil 3.5. Simetrik Anahtar şifreleme.

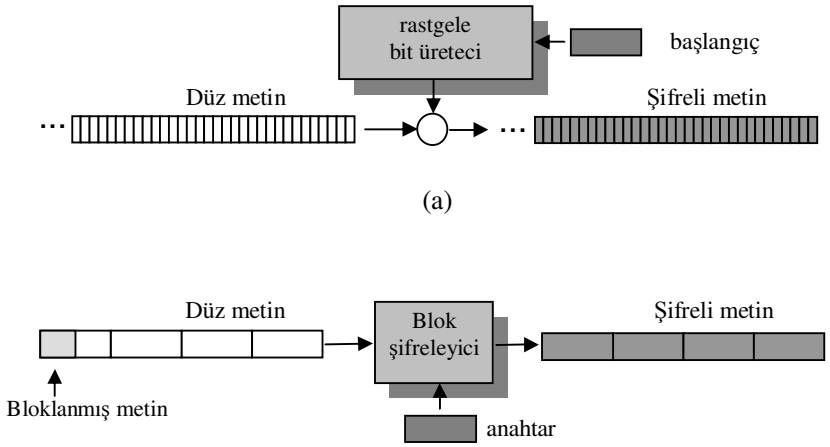
3.2.2.2. Simetrik anahtar şifreleme algoritmaları

Simetrik anahtar şifrelemenin iki temel şifreleme türü vardır:

1- Bit şifreleme (Stream ciphers)
2- Blok şifreleme (Block ciphers)

DES, 3DES ve AES blok şifreleyicidir. Bu algoritmalar düz ve şifreli metini değişmeyen ve eşit genişlikteki bloklar halinde işler [45], [46].

Bit şifrelemede şifrelenecek gizli veri bir kerede şifrelenir. Bit şifreleme aynı zamanda durum şifreleyici (state cipher) olarak da bilinir. Bit şifrelemeyi kullanan algoritmalardan RC4 algoritması, gizlenecek bilgiyi bloklara ayırmadan şifreleme işlemini gerçekleştirir.

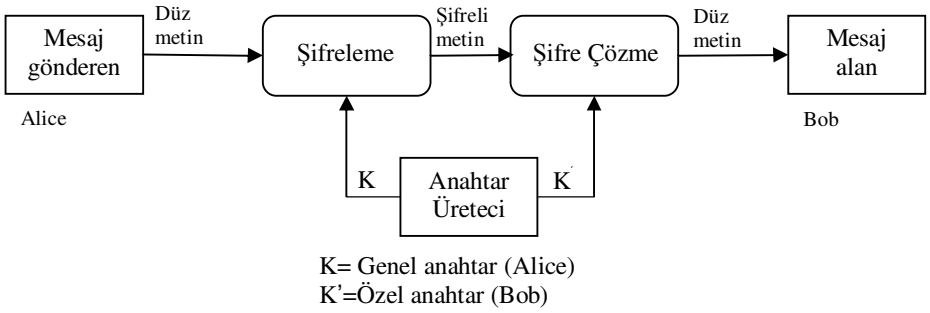


Şekil 3.6. Simetrik anahtar şifreleme yöntemleri.
(a) Simetrik Anahtar Bit şifreleme
(b) Simetrik Anahtar Blok şifreleme.

3.2.2.3. Genel anahtar şifreleme

Genel anahtar şifreleme asimetrik şifreleme olarak da bilinir. Simetrik anahtar şifrelemeye göre çok yavaş olmasına karşın, simetrik şifrelemedeki şifreleme ve şifre çözme anahtarı dağıtımı problemine çözüm getirmektedir. [47], [48], [49]. Asimetrik şifrelemede iki adet anahtar oluşturulur. Bunlar orijinal bilginin şifrelenmesinde

kullanılan genel anahtar ve şifre çözme işleminde kullanılan özel anahtarlardır. Genel anahtar olarak belirtilen anahtar umuma açıktır ve herkes tarafından bilinmesinde herhangi bir sakınca yoktur. Çünkü genel anahtarla sadece bilgiler şifrelenir ve bu şifreli bilgiler sadece genel anahtar kullanılarak üretilmiş özel anahtar kullanılarak çözülebilir. Bu nedenle özel anahtarın gizliliği asimetrik şifrelemede büyük önem taşımaktadır.



Şekil 3.7. Genel Anahtar şifreleme.

Şekil 3.7'de blok diyagramı görülen genel anahtar şifrelemenin çalışması şu şekilde ifade edilebilir;

Ali ve Bora arasında bir veri alışverişi yapıldığını varsayalım. Ali, Boraya şifreli bir mesaj göndermek istemektedir. Bora kendi bilgisayarı üzerinde şifreleme işlemi için bir adet genel anahtar ve şifre çözmek için de bir özel anahtar oluşturur. Daha sonra Bora oluşturmuş olduğu genel anahtarı Aliye gönderir. Ali Boranın gönderdiği genel anahtarı kullanarak mesajını şifreler Boraya yollar. Bora daha önce kendisinin şifre çözmek için ürettiği özel anahtarı kullanarak şifrelenmiş mesajı çözerek gizli veriye ulaşır. Buradaki en önemli nokta özel anahtarın mutlaka gizli kalmasıdır.

3.2.2.4. Genel anahtar şifreleme algoritmaları

En sık kullanılan genel anahtar şifreleme algoritmalarına örnek olarak; RSA, Diffie-Hellman, DSS, ECC verilebilir (daha fazla bilgi için bkz. [50], [51], [52]).

RSA algoritması Amerikalı üç bilim adamı tarafından 1977 yılında geliştirilmiştir ve ismini bu üç kişinin baş harflerinden almıştır; Rivest, Shamir, Adleman. RSA

algoritmasının temelinde asal sayıların kullanılması vardır [53]. Bir örnek ile çalışma prensibini açıklayalım; Önce ‘A’ olarak belirttiğimiz bir asal sayı belirlenir, daha sonra ‘B’ olarak belirttiğimiz ikinci bir asal sayı daha belirlenir.

A=3

B=11

Daha sonra iki sayının çarpımından ‘C’ sayısı elde edilir.

C=(A*B)

C=(3*11)

C=33

Elde edilen ‘C’ sayısı genel ve özel anahtarın üretilmesinde kullanılır.

Daha önce belirlenen ‘A’ ve ‘B’ asal sayılarının bir eksiklerinin çarpımından başka bir sayı üretilir (a).

a = (A -1) * (B -1)

a = (3-1) * (11-1)

a = 2 * 10

a = 20

Böylece ‘a’ sayısı elde edilir. ‘a’ sayısı elde edildikten sonra, ‘a’ sayısı ile herhangi bir ortak böleni olmayan ‘b’ gibi bir sayı belirlenir (b=7 gibi). Bu elde edilen ‘b’ ve ‘C’ sayıları genel anahtarlardır. ‘b’ sayısı kuvvet, ‘a’ sayısı mod olarak kullanılacaktır.

Özel anahtarı üretmek için de, bir ‘d’ sayısı belirlenir. Bu sayının belirlenmesinde dikkat edilecek husus şudur; ‘d’ sayısı, ‘b’ sayısı ile çarpıldıktan sonra ‘a’ sayısı ile modüler aritmetik işlemi yapıldıktan sonra kalanı ‘1’ olacak bir sayı olmalıdır.

d = ? * b mod a => 1

d * b = 1 mod a, yani

d * 7 = 1 mod 20

d = 3

olarak bulunur. Elde edilen bu ‘d’ sayısı ile ‘C’ sayısı da özel anahtarlardır.

Ali ve Bora örneğini kullanarak elde edilen anahtarların nasıl kullanıldığını açıklayacak olursak;

Boranın genel ve özel anahtarları yukarıdaki gibi elde ettiğini varsayalım.

Genel anahtar: b = 7 ve C = 33

Özel anahtar: d = 3 ve C = 33

Bora özel anahtarı saklar ve genel anahtarı Aliye yollar. Ali genel anahtarı kullanarak mesajı şifreler. Örneğin, Ali 'A' harfini şifreleyip göndermek istesin. 'A' harfine karşılık gelen herhangi bir sayı seçilir. 'A' harfinin sayısal değerini 15 olarak seçelim. 15 sayısı, genel anahtarın sahip olduğu 'b' sayısı ile kuvveti alınır ve sonuç 'C' sayısı ile aritmetik işleme tabi tutulur.

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

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

$X = 35831808 \bmod 33$

$X = 27$

Ali elde edilen sonucu (X=27) 'A' harfi olarak Boraya gönderir. Bora almış olduğu mesajı gizli anahtar ile çözer.

$X_ı = X^{d} \bmod C$

$X_ı = 27^{3} \bmod 33$

$X_ı = 19683 \bmod 33$

$X_ı = 15$

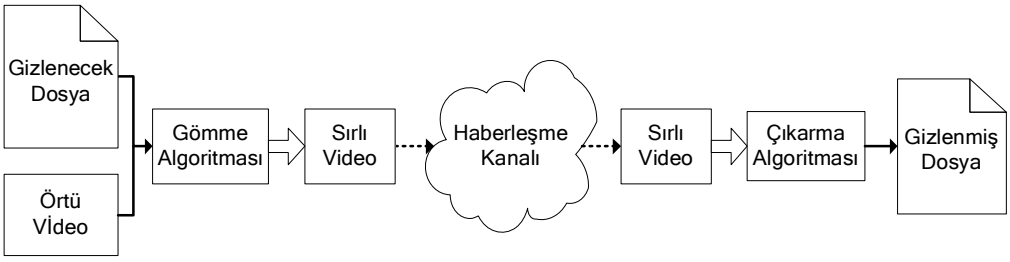
Sonuç olarak Ali 15 sayısını şifreleyip 27'ye çevirmişti. Bora da 27 sayısını çözüp 15 sayısını yani 'A' harfini elde etti.

3.3. Sırörtme

Günümüzde gelişen Internet ve diğer sayısal ağ teknolojileri; sayısal medyayı kalitesini bozmadan, yüksek kalitede paylaşabilme imkânı sunar. Bu durumun teorik olarak düşünüldüğü zaman insanlara inanılmaz bir kolaylık ve fayda sağladığı söylenebilir. Fakat bu muazzam büyüklükteki sanal dünyanın güvenlik yetersizlikleri beraberinde birçok sorunu da getirmiştir. Örneğin sayısal medyanın yasadışı ve korsan dağıtımı yüzünden büyük bir ekonomik kayba yol açtığı acı bir gerçektir [54].

Bir başka sorun ise, insanlar arasındaki haberleşmede mahremiyet hakkının ihlal edilmesidir. Gerek ekonomik anlamda gerekse de güvenlik anlamında meydana gelen bu tür olumsuz gelişmeler sayısal medyanın korunması ve güvenli haberleşme gerekliliklerini ortaya çıkarmıştır.

Özellikle Amerika Birleşik Devletlerinde yaşanan 11 Eylül saldırıları [38],[55], [56],[57] sonrasında araştırmalar, sırörtme üzerinde odaklanmıştır. Yapılan açıklamalarda, teröristlerin eBay, Usenet ve Amazon gibi popüler web sitelerinde hatta porno sitelerinde eylem detaylarını, planlarını bilgi saklı resimler kullanarak paylaştıkları iddia edilmişti. Örneğin terörist saldırı ile ilgili bilgileri (yer, zaman vb.) sırörtümsel yöntemler kullanarak bir resmin içerisine gömmüşler ve bunu Internet üzerinden yayınlamışlardır. Hangi siteden yayın yapıldığını bilen diğer gurup elemanı ilgili resmi ilgili siteden indirerek yine sırörtme yöntemleri ile orijinal bilgiye ulaşmıştır. Bu yöntemle hiçbir şekilde dikkat çekmeksizin istedikleri gibi haberleşme imkânı bulmuşlardır.



Şekil 3.8. Genel olarak veri gizleme blok diyagramı.

Şekil 3.8'de genel olarak bir veri gizleme işleminin blok diyagramı gösterilmektedir. Diyagrama göre, örtü dosyası ve gizli dosya bir gömme algoritmasına uygulanır ve sırlı video elde edilir. Elde edilen sırlı video bir haberleşme kanalından iletilir. Sırlı videoyu alan taraf çıkarma algoritmasını bu videoya uygulayarak gizli dosyayı elde eder.

3.3.1. Sırörtme kavramı ve terminolojisi

Sırörtme, Yunanca kaplamak, örtmek anlamına gelen "stegos" ve yazı anlamına gelen "graphia" kelimelerinden türetilmiştir [58]. Bir nesnenin içerisine bir verinin gizlenmesi olarak da tanımlanan sırörtme [59]; haberleşmede, gizleme bilimi ve sanatı olarak yer alır [38],[60]. Sırörtme kullanarak gizli bir mesajı hiç kimsenin haberi olmadan kuşku uyandırmayacak şekilde bir başkasına göndermek asıl amaçtır.

Haberleşme bilgilerinin anlamsız karakter ya da dizilerden oluşturulmasını esas alan yöntem kriptografidir. Kriptografik bir verinin en zayıf yönü, verilerin gözlemlenmesi sonucunda haberleşmenin şifreli olduğunun anlaşılmasıdır. Haberleşmenin şifreli ya da gizli olduğu kuşkusu yetkisiz kişiler tarafından anlaşıldığında ise gizli veriye yapılacak muhtemel saldırılar gündeme gelecektir. Olası saldırılara mazur kalmamak için haberleşmenin de gizli olarak yapılması gerekliliği ortaya çıkar ki bu durumda haberleşme bilgilerinin maskelenmesi yoluna gidilir. Aynı zamanda bu yöntem sırörtme (nesne içerisine veri gizleme) olarak da bilinir. Bu yöntemde, kriptografinin zayıflığı olan şifreli haberleşme bilgilerinin gözlenerek fark edilmesi ve düzenlenecek saldırıların engellenmesi amaçlanmıştır. Sırörtme yönteminde en kritik nokta, yapılan saldırılardan korunmak değil saldırıların yapılmasını önlemektir. Bu durum bir suçlunun suç işledikten sonra cezalandırılması yerine önceden o suçu işlemesine engel olmak gibi düşünülebilir. Sırörtümsel yöntemler gizli verilerin masum görünümlü taşıyıcılar ile gönderilmesi ilkesine dayanmaktadır. Bahsedilen taşıyıcılar resim, ses, video veya diğer sayısal olarak sunulan kod veya yayımlar olabilir. Görüntü dosyaları üzerinde bilgi gizlemek için çeşitli sırörtmesel yöntemler geliştirilmiştir. Bunlar üç başlık altında sınıflandırılabilmektedir;

- En önemsiz bite ekleme (Least Significant Bit – LSB),
- Maskeleme ve filtreleme,
- Algoritmalar ve dönüşümler [61].

Sırörtme uygulamalarında ilk olarak kullanılan ve en basit yöntem olan en düşük değerlikli bit (LSB–Least Significant Bit) gömme yöntemidir [62],[63],[64]. Bu

yöntem uzay–boyutunda gömme tekniklerini kullanır ve taşıyıcı dosyanın (resim veya video) pikselleri üzerinde değişiklikler yaparak gizli veriyi taşıyıcı dosyanın içerisine gömer. Bu yöntemle veri gizleme yapıldığında, İGS tarafından algılanamayacak ve sıradan bir bilgiymiş gibi normal kullanıcılar tarafından saldırıya maruz kalmayacaktır. Uygulama da birçok basitliğe sahip olmasının yanında LSB kodlamanın bazı zayıf yönleri de vardır. Gizli mesajın doğru bir şekilde elde edilebilmesi için ikili – sayı düzeninin korunması gerekir ki bu önemli bir sorundur. Gürültü eklenmesi, filtreleme, kırpma, renk uzayı dönüşümü ve yeniden örnekleme de önemli eksikliklerdendir. Aynı zamanda bu yöntem kayıplı sıkıştırma algoritmalarından da etkilenerek gizli verinin kaybolmasına neden olabilir.

Maskeleme ve filtreleme yöntemleri İGS'nin sınırlarını kullanarak normal bakmayla anlaşılmayacak bölgeleri bulur ve gizleme işlemini gerçekleştirir. Bu yöntemde gizli veri gürültü kullanılarak gizlenmez ama benzer bir yöntemle örtü dosyasının resim bilgisini oluşturan piksellerinin bulunduğu alana gizlenir. Bu da maskeleme yöntemini kayıplı sıkıştırmalara (JPEG gibi) karşı daha kullanışlı ve dayanıklı hale getirir. Maskeleme ve filtreleme yöntemlerinde genellikle 24 bit resimler veya siyah-beyaz resimler kullanılır. Sıkıştırma, kırpma ve diğer çeşitli resim işleme işlemlerine karşı LSB yöntemine göre daha dayanıklıdır. Bu yöntemler, uzay boyutundan veya dönüşüm boyutundan faydalanarak bilgi gizleme işlemini gerçekleştirirler.

Veri gizleme sırasında kullanılan bütün piksellerin veri gizleme için uygun olabileceği düşünülemez. Ve uygun olmayan bir piksel içerisine veri gizlendiğinde, bu pikselde meydana gelecek olan bozulmalar gizli verinin farkedilmesine neden olabilir. Bu sebeplerden ötürü bazı sırörtme yöntemleri birtakım algoritmalardan oluşur. Bu algoritmalar, içerisine veri gizlenebilecek uygun pikselleri belirlemek için kullanılır [39].

Sırörtümsel yöntemler yukarıda da bahsedildiği gibi farklı başlıklar altında toplansa da bütün hepsinde amaç aynıdır; "algılanamaz olmak". Bu temel amaç doğrultusunda sırörtme üzerinde yapılan birçok çalışmada araştırmacılar insan görme ve ya duyma sisteminin sınırlarını kullanmayı tercih etmişlerdir. Swanson, Zhu, and Tewfik [65]

yaptıkları araştırmalarda, İGS'nin bazı karakteristik özelliklerinden faydalanarak veri gizleme üzerine odaklanmışlardır.

Örtü dosyası içerisine bir mesaj gizlendikten sonra elde edilen gizli veri içeren dosyaya 'sır (stego) nesnesi' denir. Örneğin, bir yazı dosyasının (covertext) içerisine gizli bir işaret veya bilgi eklendiğinde elde edilen yeni dosya sırlı-metin (stegotext), veya bir resim dosyası içerisine (cover-image) gizli bir işaret veya bilgi eklendiğinde elde edilen yeni dosya da sırlı-resim (stego-image) olarak adlandırılır. Bu terminoloji birinci uluslararası bilgi gizleme seminerinde kabul edilmiştir [66],[67].

Örtü Dosyası (Cover–Image): İçerisine gizli verinin gömüleceği dosyadır. Bu dosya resim, video veya ses dosyası olabilir.

Gömü Dosyası (Stego–Image): Gizli veriye sahip dosyadır (resim, video, ses vb).

Örtü Anahtarı (Stego–Key): Gizleme işlemi sırasında kullanılan güvenlik anahtarıdır.

Steganalysis: Gizli verinin bulunması ile ilgili uğraşan bilim dalıdır.

Bir düzyazı (plaintext), bir şifreliyazı (ciphertext), bir resim veya bir bit dizini içerisine gömülmüş herhangi bir bilgi 'gizli veri' olabilir. Örtü dosyası ve gizli veri birlikte gömü dosyasını oluştururlar. Eğer daha fazla güvenlik istenirse ekstra şifre olarak gizli anahtar da kullanılabilir. Tüm bileşenleri tek bir formül altında toplamak gerekirse;

$$\text{Örtü dosyası} + \text{Gizli veri} + \text{Gizli anahtar} = \text{Gömü dosyası} \qquad (3.3)$$

3.3.2. Sırörtmenin tarihçesi

Eski Yunan'da M.Ö. 5. yüzyılda Susa kralı Darius tarafından göz hapsine alınan Histiaeus, Miletus'daki oğlu Aristagoras'a gizli bir mesaj göndermek için kölelerinden birinin saçlarını kazıtır ve mesajını dövme şeklinde kölenin kafa derisine işletir. Kölenin saçları yeterince uzadığında köleyi oğlunun yanına gönderir.

Tarihçi Herodotus'un verdiği bu bilgi ile gizli yazma sanatı sırörtmenin ilk nerede, nasıl ve kimler tarafından kullanıldığı hakkında bilgi sahibi olmaktayız. Bu gizleme sanatı, çağlar boyunca insanların ilgisiyle giderek gelişmiş ve bilgi iletiminde bir bilim dalı haline gelmiştir. Eski Romalılar satırların arasına gözle görünmeyen mürekkepler kullanarak farklı gizleme teknikleri geliştirmişlerdir. Bu mürekkepler doğal maddelerden, meyve özünden (limon gibi), idrar ve de sütten oluşmaktadır. Isıtılınca ortaya çıkan bu gizli mesajlaşma tekniği günümüzde de hala kullanılmaktadır. İkinci Dünya Savaşı sırasında Almanlar mikro-nokta (microdot) olarak adlandırılan farklı bir gizleme tekniği geliştirmişlerdir. Bu teknikte alfabede kullanılan noktalama işaretleri içerisine ebatları küçültülmüş fotoğrafik bir takım gizli mesajlar gömülür. Böylece Almanlar teknik çizimleri de içeren geniş miktarda basılı bilgi göndermeyi başarmışlardır. Savaş sırasında sırörtmenin yaygın kullanımı ve şüphelenme atmosferi içerisindeki İngiltere ve ABD tarafından posta yolu ile her türlü satranç oyunu, örgü işleme resimleri, gazete kupürleri, çocukların çizimleri gibi gizli veri taşıması muhtemel dokümanların gönderilmesi yasaklanmıştır. Yine aynı dönemde Sovyetler Birliği (SSCB) tarafından da tüm uluslararası postalar casusluk aktivitelerine karşı sürekli olarak taranmaktaydı. Bilgisayar teknolojisinin hızlı ilerlemesi ile birlikte bu sınırlamaların tümü geçerliliğini kaybetmiştir. Günümüzde herkes sırörtmenin üstünlüklerini kullanabilir hale gelmiştir.

3.3.3. Sırörtme tekniklerinin gereksinimleri

Sırörtme tekniklerinin başarılı olabilmesi için sağlaması gereken üç önemli gereksinim vardır. Bunlar; gizli haberleşmenin güvenliği, veri gizleme kapasitesi ve kasıtlı veya kasıtsız olarak yapılan saldırılara karşı dayanıklılık olarak sıralanabilir.

Güvenlik: Bir sırörtme tekniğinde, gizli veriyi elde etmek için haberleşme kanalını izleyen kötü niyetli kişilerin algısal ve istatistiksel anlamda dikkatlerinin çekilmemesi en önemli güvenlik gereğidir. Güvenli bir sırörtme tekniğinde kötü niyetli kişiler gizli veriye ulaşamamalıdır.

Kapasite: Sırörtme tekniklerinde asıl amaç gizli haberleşme olduğu için gizli veri kapasitesinin yüksek olması arzulanır. Fakat gizli veri kapasitesinin artması

doğrudan güvenlik zayıflığına neden olmaktadır. Sırörtme tekniklerinde gizli veri kapasitesi ve güvenlik birbirleriyle ters orantılı olan ve araştırmacıların üzerinde yoğunlaştığı iki önemli parametredir [68].

Dayanıklılık: Damgalamada olduğu gibi, sırörtme tekniklerinin saldırılara karşı dayanıklılık sağlaması çok önem teşkil eden bir parametre değildir. Çünkü gizli haberleşme sırasında kullanılan örtü dosyası herkes tarafından bilinen bir dosya değildir. Fakat örtü dosyası JPEG kodlama yöntemi ile oluşturulmuş ise bu durumda sırörtme tekniğinin saldırılara karşı dayanıklı olması gerekecektir [69].

3.3.4. Resim dosyaları için sırörtme teknikleri

Bir resmin görüntüsünde ciddi anlamda bozulmalara neden olmadan önemli bir veriyi bu resmin içerisine gizlemek için, örtü dosyasının piksel değerleri renk değişimleri kullanılarak gürültü ile yer değiştirilebilir. Resim içerisine önemli bir veri gizlemek için kullanılan yöntemler örtü dosyası üzerinde en düşük öneme sahip bit – LSB, maskeleme, algoritma ve dönüşüm tekniklerini kullanırlar.

Resim içerisine veri gizleme yöntemleri iki kategoride sınıflandırılabilir. Bunlardan biri ‘uzay–düzleminde’ veri gizleme, diğeri ise ‘frekans–düzleminde’ veri gizlemedir. Uzay–düzleminde veri gizleme işlemi sırasında [40,70,71], gizli veri resim pikselleri içerisine doğrudan yerleştirilir. Frekans–düzleminde ise, öncelikle örtü dosyası frekans–düzlemine dönüştürülür daha sonra gizlenecek veri taşıyıcı resmin dönüşüm katsayılarına yerleştirilir [72].

3.3.4.1. Uzay-düzleminde sırörtme

Uzay – düzleminde veri gizlemek için en çok kullanılan teknik “en düşük değerlikli bit – LSB” tekniğidir. LSB yönteminin popüler olmasının ve sıklıkla kullanılmasının en önemli nedeni uygulanmasının çok kolay olmasıdır.

Bu yöntemde, içerisine veri gizlenmek istenen örtü dosyası pikselleri ve gizlenmek istenen veri ikili sayı (binary) formatında ifade edilir. Bu işlemden sonra, gizlenmek

istenen verinin her bir bit'i (1 veya 0) taşıyıcı resmin her bir pikselinin en düşük değerlikli bit'i ile değiştirilir. Bu yöntemde bilgi gizlemek için kullanılabilecek en iyi resim formatı 24–bit Bitmap (BMP) resimdir. Bunun başlıca sebebi bu resim formatının yüksek kaliteye sahip olması ve gizlenebilecek veri kapasitesini maksimum seviyeye çıkarmasıdır. Veri gizleme için kullanılacak olan resim formatı yüksek kalitede olduğu zaman, bilginin gizlenmesi ve maskelenmesi daha kolaydır. LSB metoduna göre sırörtme uygulanmış birkaç örnek [2] ve [73]'de gösterilmiştir.

Bu teknikler tamamıyla resim formatına bağladır ve BMP, GIF gibi kayıpsız resim formatları üzerinde kullanılırlar. Bunun sonucunda da büyük miktarda veri gizlemek için oldukça büyük kapasiteye sahip örtü dosyası gereksinimi ortaya çıkar. Günümüzde, Internette 800x600 boyutlarında sıkıştırılmamış bir resmin kullanılması sık karşılaşılan bir durum değildir. Bu boyutlarda bir resmin içerisine bilgi saklamak şüpheleri daha çok çekecektir. Bir başka önemli zayıf yönü ise, içerisinde gizli veri bulunan resmin kayıplı sıkıştırma işlemine tabi tutulmasıdır ki bu işlemden sonra gizli verinin hala resim içerisinde mevcut olması çok güç bir ihtimaldir hatta imkânsızdır denilebilir.

3.3.4.2. Frekans-düzleminde sırörtme

Bir bilgiyi resmin içerisine gizlemenin en karmaşık yolu ayrık kosinüs dönüşümü (DCT), ayrık dalgacık dönüşümü (DWT) gibi dönüşüm yöntemleri kullanmaktır. Bu yöntemler örtü dosyasının önemli bölgelerinde bulunun piksellerinin ayrık kosinüs ve/veya dalgacık dönüşüm katsayılarında değişiklik yaparak gizlenecek bilgiyi frekans düzleminde gömerler. Gerekirse parlaklık gibi örtü dosyasının bazı özelliklerini değiştirerek algılanabilirliği engellemeye çalışırlar. Burada bahsedilen örtü dosyasının önemli bölgelerinden kasıt şudur; bir resme ayrık kosinüs dönüşümü uygulandıktan sonra matematiksel olarak resim bileşenlere ayrılır. Her bir bileşene ait sabit bir katsayı çarpanı bulunur. Bu katsayılardan bazıları matematiksel olarak sıfır değerinde, bazıları ise sıfırdan farklı değerdedir. Bunun anlamı ise sıfır değerine sahip olan bileşenler İGS tarafından algılanamayan bölgelerdir ki bu bölgeler kayıplı sıkıştırma yöntemlerinde resim içerisinden atılarak sıkıştırma işlemi gerçekleştirilir. Sıfırdan farklı değere sahip bileşenler, resim içerisinde İGS'de algılanabilir bölgeleri

temsil etmektedirler. Bu yöntemde bilgi gizleme için bu bölgeler kullanılır. Birçok dönüşüm boyutunu kullanan sırlama yöntemi, örtü dosyası formatından bağımsızdır. Böylelikle kayıplı ve kayıpsız resim formatları arasında yapılacak dönüşümler sırasında gizli veri kaybolmayacaktır. Bu tekniklerde gizlenebilecek bilgi miktarının kapasitesi ile saldırılara karşı dayanıklılık kontrol edilebilir [74].

3.3.5. Video dosyaları için sırörtme teknikleri

Kapasite problemi, sırörtme tekniklerinde sürekli olarak araştırmacıları üzerinde düşündüren, aşılması gereken bir zorluk olmuştur ve olacaktır. Hareketsiz görüntülerin kapasiteleri belli bir sınırın ötesine geçemediğinden dolayı araştırmalar hareketli dosyalar üzerinde yoğunlaşmıştır. Video dosyalarına bilgi gizlemek için genelde resim ve ses içerisine bilgi gizleme yöntemleri birleştirilerek kullanılır. Bilindiği gibi video dosyası hareketsiz resimlerin ardı sıra oynatılmasından meydana gelmektedir. Böylelikle resim dosyaları içerisine veri gizleme için kullanılan yöntemler video dosyaları içinde kullanılabilmektedir. Genellikle video dosyaları içerisine veri gizlemek için dönüşüm–boyutu yöntemleri (Discrete Cosine Transform–DCT, Discrete Wavelenght Transform–DWT gibi) kullanılır. Örneğin DCT yöntemi video dosyasını oluşturan her bir hareketsiz resmin önemsiz miktarlarda değiştirilmesi esasına göre çalışır. DCT resim içerisindeki değişmeyen noktaların değerlerini yukarıya yuvarlayarak değiştirir. Örneğin, 6.667 değerine sahip bir noktanın değeri yuvarlama işleminden sonra 7 olacaktır [57]. Video dosyasındaki ses bilgisi içerisine bilgi gizlemek için de yine ses dosyalarında kullanılan yöntemler kullanılabilir.

Video dosyasının bilgi gizleme için kullanılmasının en büyük yararlarından biri çok büyük miktarda gizli veri kapasitesi sağlamasıdır. Örneğin 30 fps (frame-per-second) ve 10 saniyelik bir video dosyası 300 hareketsiz resimden oluşmaktadır. Böylece bir resim dosyası içerisine gizlenecek gizli veri kapasitesi bu örnek video dosyası için 300 kat daha fazla olacaktır. Diğer bir yarar ise, bilgi gizlemeden kaynaklanabilecek her bir hareketsiz video resmindeki muhtemel bozukluklar İGS tarafından fark edilemeden görüntü akmaya devam edecektir.

İlk olarak video dosyaları üzerinde yapılan veri gizleme çalışmaları ham (raw-video) videolar üzerine odaklanmıştır. Ham videolar üzerinde yapılmış birçok veri gömme uygulaması ve çalışması vardır. Bu çalışmalar video içerisine bilgi gömme çalışmalarının temelini oluşturan çalışmalardır. Sonraları ise gerek ilerleyen sıkıştırma teknikleri ve gerekse büyük kapasiteye sahip videoların Internet üzerinden iletimleri sırasında gerektirdikleri büyük iletim bant genişliği gibi sıkıntılar çalışmaların sıkıştırılmış (bit-stream) videolar üzerine kaymasına neden olmuştur.

3.3.5.1. Ham video (raw-video)

Bir hareketli görüntü içerisine gizli veri, hareketli görüntünün her bir çerçevesi kullanılarak gömülebilir. Var olan birçok hareketli görüntü içerisine bilgi gömme yöntemi hareketsiz görüntü içerisine bilgi gömme yöntemleri ile tamamen benzer bir işleyişe sahiptir.

3.3.5.2. Sıkıştırılmış video (bit-stream)

Günümüzde Internet teknolojisinin büyük bir hızla gelişmesi ve Internet kullanıcısının geçmiş yıllara nazaran hızla artması birçok uygulamanın Internet tabanlı olması gerekliliğini artırmıştır. Ayrıca Internet teknolojisindeki bu hızlı ilerleyiş müzik, resim ve video gibi birçok sayısal dosyanın insanlar arasında kolaylıkla paylaşılabilmesine olanak sağlamıştır. Her ne kadar eskiye göre hızlı bir ilerleme kaydedilmiş olmasına rağmen Internet iletim genişliği yüksek boyutlardaki dosyaların paylaşımı için hala yeterli değildir. Özellikle gerçek zamanlı işlemler sırasında bu yetersizlik daha büyük soruna dönüşmektedir. Bu ve benzeri sorunlar nedeniyle araştırmalar sıkıştırma teknikleri üzerinde yoğunlaşmış ve birçok standart geliştirilmiştir. Görüntü için en çok bilinen sıkıştırma standardı (Moving Pictures Experts Group-Hareketli Görüntüler Uzmanları Gurubu) MPEG'dir. MPEG formatındaki bir videoya gizli veri gömerken DCT yöntemi kullanılır. MPEG formatındaki bir video; I, P ve B çerçevelerinden meydana gelir. I-çerçeve, bir önceki ve sonraki çerçevelerden bağımsız olarak tek bir resimmiş gibi kodlanır. P-çerçeve, bir önceki çerçeveye bağlı olarak kodlanır. B-çerçeve ise, hem önceki hem

de sonraki çerçevelere bağımlı olarak kodlanır. B-çerçeve kodlama, P-çerçeve kodlamaya benzerlik gösterir [75], [76].

Sıkıştırılmış video içerisine bilgi gizleyerek kolay dağıtım ve paylaşım gibi problemlere çözüm aranırken, kapasitenin düşmüş olması ise başka bir problemi ortaya çıkarmaktadır. Sıkıştırma algoritmalarının gereği olarak, sıkıştırılan dosya içerisindeki insan gözünün veya kulağının algılayamadığı bilgiler kalıcı olarak silinir. Bunun anlamı ise bilgi gizleme için kullanılacak olan örtü dosyasının boyutunun azalması ve sonuç olarak gizlenecek bilginin boyutunun azalmasıdır.

3.3.6. Ses dosyaları için sırörtme teknikleri

Internet üzerinde yaygın olarak ve kolaylıkla paylaşılabilmesi ses dosyalarının da gizli veri gömmede kullanılmasına neden olmuştur. Ses dosyaları için birçok sırörtme yöntemi geliştirilmiştir. Bu çalışmalardan önemli olan bazıları şunlardır;

- Düşük Bit Kodlama,
- Yankı Gizleme,
- Yayılı İzge
- Diğer Yöntemler.

3.3.6.1. Düşük bit kodlama

Genellikle ses dosyası içerisine veri gizlemek için LSB metodunda olduğu gibi düşük değerlikli bitler kullanılır. Fakat bu yöntemin kullanılmasında karşılaşılan genel sorun, insan kulağının ses dosyasındaki bozulmaları algılayabilmesidir. Ayrıca bu yöntemde haberleşme kanalında oluşabilecek gürültü nedeniyle gizli verinin kaybedilmesi olasılığı yüksektir [58].

3.3.6.2. Yankı gizleme

Yankı gizleme yeni bir dönüşüm kodlama tekniğidir. İnsan kulağının ses dosyası içerisindeki kısa süreli yankıları (milisaniyeler mertebesinde) algılayamaması özelliğini kullanır. Bu yöntemde, ses dosyası içerisine bilgi gizlemek için ses dosyası

içerisindeki yankılardan faydalanır. Gecikme ve bağıl genlik değerlerine göre ses dosyasının içerisine yankı sinyali eklenir. Gizli veri ise bu yankı sinyali içerisine '0' ve '1' olarak kodlanır. Gecikme zamanı 0.5ms ile 2ms arasında, bağıl genlik ise yaklaşık 0.8 olarak seçilir [77].

3.3.6.3. Yayılı izge

Yayılı izge modülasyonu ses dosyalarında kullanılan bir başka gizleme yöntemidir. Bu yöntem frekans boyutunda ses sinyaline rastgele gürültü ekler. İletişim kanalındaki meydana gelebilecek olası kayıplara ve saldırılara karşı dayanıklı olmakla birlikte insan duyma sistemi tarafından algılanabilecek büyüklükte gürültüye neden olmaktadır.

3.3.6.4. Diğer yöntemler

Bir başka yöntem ise insan duyma sisteminin (İDS) modellenerek gömme işleminin yapılmasıdır. İnsan duyma sisteminin sınırında olmayan frekanslar kullanılarak bir bilginin ses dosyası içerisine gömülmesi mümkündür. Örneğin 20.000 Hz üzerindeki frekansların kullanılarak bilgiler ses dosyaları içerisine gizlenebilir [60].

3.4. Sayısal Damgalama

Yukarıda da açıklandığı gibi sırörtme araştırmaları, gelişen Internet teknolojisi ile ortaya çıkan güvenlik açıklarından haberleşme güvenliği üzerine odaklanmıştır. Sayısal medyanın korunması problemi ile ilgili çalışmalar da damgalama araştırmalarına konu olmuştur. Damgalama tekniklerinde en önemli amaç herkes tarafından bilinen, popüler bir sayısal medyanın kanunsuz yollarla çoğaltılmasını, dağıtılmasını önlemek yani eser sahibinin telif hakkını korumaktır. Aslında, orijinal bir eserin korunmasını önlemek için yapılan koruma yöntemleri daha da öncelere dayanır. Kâğıt banknotlar üzerinde yer alan ve ışığa tutulduğunda görülen filigranlar, kitapların kapaklarında bulunan hologramlar sadece birkaç basit örnektir.

3.4.1. Sayısal damgalama kavramı

Genel bir ifadeyle sayısal damgalama, sayısal formattaki bir eserin korunması amacıyla eserin içerisine gömülen sayısal bir imzadır. Sayısal damgalama değerli sayısal medyanın korunmasında şifreleme ve kopyalama korumalarının yetersiz kaldığı durumlarda son koruma yöntemi olarak önerilmektedir [2],[78].

Sayısal damgalama teknikleri damgalamanın yapılacağı uygulamanın gereksinimine göre iki farklı şekilde gerçekleştirilir.

1- Görülebilir sayısal damgalama,
2- Görülemez sayısal damgalama.

Görülebilir sayısal damgalama uygulamalarında, sayısal medyanın içerisine yerleştirilmiş damga bilgisi İGS tarafından rahatça algılanabilmektedir. Ticari amaçla çekilmiş bir ürünün sayısal resminin hangi kuruma ait olduğunu gösteren damgalar, bir televizyon kanalının yayınlarında kullandığı ekran logosu görülebilir sayısal damgalama uygulamaları için verilebilecek birkaç örnektir.

Görülemez sayısal damgalama uygulamalarında ise, damga bilgisi İGS veya duyma sistemi tarafından algılanamazdır. Piyasaya yeni çıkmış olan bir sinema filminin DVD'sinin veya müzik CD'sinin kopyalamalara karşı korumak amacıyla görülemez sayısal damgalama kullanılır.

Sayısal damgalama ile korunmuş sayısal medya parlaklık ve kontrast ayarlarının değiştirilmesi, özel filtrelerin kullanılması, kağıda baskı veya tarama gibi bir çok saldırıya karşı korunabilmektedir. Ancak StirMark ve UnZign gibi damgalama teknolojisinden hemen sonra ortaya çıkan bazı programlar sayısal damgayı kaldırabiliyor veya etkisiz hale getirebiliyor. Asıl amaçları geliştirilen damgalama tekniklerinin performans değerlendirmelerini yapmak olan bu programlar aynı zamanda sayısal damgayı da yok ederek saldırı amaçlı programlar haline de gelebilmektedirler [79].

3.4.2. Sayısal damgalamanın gereksinimleri

Sayısal damgalamanın sağlaması gereken bir takım gereksinimler vardır. Bu gereksinimler sayısal damgalamanın kullanılacağı uygulamaya göre değişiklik gösterebilir. Genel olarak bir sayısal damganın yerine getirmesi gereken gereksinimler; dayanıklılık, algılanamazlık, güvenlik, hızlı gömme ve geri elde etme, damgalanmamış dosyaya ihtiyaç duymama olarak sıralanabilir.

Dayanıklılık: Sayısal damga, kasıtlı saldırılara karşı korunan bilgilerin zarar görmesini engellemelidir.

Algılanamazlık: Özellikle görülemez sayısal damgalama uygulamalarında, damgalanan sayısal medyanın kalitesinin bozulmaması gerekmektedir.

Güvenlik: Sayısal damga yetkisiz veya kötü niyetli kişiler tarafından fark edilememelidir.

Hızlı gömme ve geri elde etme: Internet üzerinden paylaşılan sayısal medyanın damgalanma işleminin hızlı olması önemlidir.

Damgalanmamış dosyaya ihtiyaç duymama: Bazı uygulamalarda taşıyıcı medyanın orijinali olmadan sayısal damganın geri elde edilmesi gerekmektedir. Aynı zamanda bu durum güvenliği de artıran bir unsurdur.

Uygulama türüne göre değişen bu gereksinimlerden dayanıklılık, algılanamazlık ve güvenlik her uygulamada olması gereken en önemli gereksinimlerdir.

3.4.3. Sayısal damgalama teknikleri

Günümüze kadar birçok sayısal damgalama teknikleri geliştirilmiştir. Bunlardan bazıları uzamsal/zamansal boyutta değişiklik yapmayı önermiş [2],[80], bazıları da dönüşüm katsayıları üzerinde değişiklik yapmayı önermişlerdir [81].

3.4.3.1. Uzamsal ve zamansal boyuttaki teknikler

Hareketsiz görüntüler üzerinde yapılan ilk sayısal damgalama çalışmalarında en düşük değerlikli bit değiştirme yöntemleri kullanılmıştır. Bir çalışmada [2], gizli veri en düşük değerlikli iki bit içerisine gömülmüştür. Bu çalışma gürültü eklemeye dayanıklı değildir.

Bir başka çalışmada ise [82], araştırmacı gizli veriyi geometrik bir şekil olarak sayısal görüntünün algılanamayan parlaklık bilgisine gömmeyi önermiştir.

Fakat bu çalışmalar saldırılara karşı yeterli güvenliği sağlayamamaktadır. Daha dayanıklı bir yöntem olarak sayısal damganın alçak geçiren bir filtre ile desteklenmesi önerilmiştir [83].

3.4.3.2. Dönüşüm boyutu kullanan teknikler

Araştırmacılar daha dayanıklı damgalama yöntemleri geliştirmek için ayrık kosinüs (DCT) ve ayrık dalgacık (DWT) dönüşümleri kullanmayı önermişlerdir.

Cox çalışmasında [84], bir damgalama yönteminin saldırılara karşı dayanıklı olması için, damgayı resmin en önemli algılanabilir bölgelerinin DCT katsayılarına gömmeyi önermektedir. Saldırıların taşıyıcı resme hasar vermeye yönelik değil, damganın silinmesine yönelik olması bu teoriyi desteklemektedir. Fakat bu yöntemin başarısı algılanabilirliğin en alt seviyede tutulmasına bağlıdır.

Bir başka çalışmada [85], araştırmacılar DWT dönüşümüne göre damgalama yöntemi geliştirmişlerdir. Damga Gaussian gürültüsü olarak modellendikten sonra resmin orta ve yüksek frekans bileşenlerine gömülür. Bu teknik DCT [84] tekniğinden daha dayanıklıdır.

3.5. Sırörtme ve Sayısal Damgalama Arasındaki Farklar

Özellikle görünmez sayısal damgalama ile sırörtme yöntemlerinin çok benzer olması birbirleri ile karıştırılmalarına neden olmaktadır. Hâlbuki her iki çalışmanın da öncelikli hedefleri birbirlerinden farklılık gösterir.

Sırörtmenin asıl amacı; haberleşme esnasında kullanılan önemli bir mesajı sırörtme teknikleri ile örterek gizlemeye çalışmaktır. Bir kullanıcının kendisinin oluşturduğu taşıyıcı dosya (resim, video, müzik vb.) içerisine stratejik bir merkezin planını eklemesi örnek olarak verilebilir. Buradaki önemli nokta kullanıcının kendi taşıyıcısını kendisinin oluşturmasıdır. Taşıyıcı dosyasının herkes tarafından bilinen bir dosya olmaması kötü niyetli kişilerin dikkatini çekmemesi açısından önemlidir. Taşıyıcı dosyasının orijinalini bilmeyen kötü niyetli kişiler, taşıyıcı dosyadaki olası bozukluklar hakkında yorum yapamayacaklardır.

Sayısal damgalamanın asıl amacı ise; herkesin ulaşabileceği sayısal bir dosyanın korunmasını sağlamaktır. Sayısal damgalama için verilebilecek en güzel örnek günümüzde yapımcıların yaşadığı korsan baskı sorunudur. Yapımcıların ürettikleri müzik eserlerinin, sinema filmi eserlerinin kendilerine hiçbir ücret ödenmeden korsanlar tarafından kopyalanarak dağıtılması sorununun çözülmesi sayısal damgalamanın en büyük amacıdır. Bu sebepten ötürü damgalama teknikleri sıkıştırma, kırpma ve LSB değişimi yapan bazı sinyal işleme yöntemlerine karşı daha dayanıklı olmalıdır. Bu özelliklerinden ötürü de damgalama teknikleri genellikle, telif hakkı koruması, mülkiyet hakkı koruması ve lisans korumasının önemli olduğu yerlerde kullanılır.

Tablo 3.2'de sırörtme tekniklerinin ve damgalama tekniklerinin kullanım amaçlarına göre birbirleriyle karşılaştırılması özetlenmiştir [69].

Tablo 3.2. Sırörtme ve damgalamanın üstünlükleri zayıflıkları.

	Gereksinimler	Damgalama		Sır Örtme
		Özel	Genel	
Hedefler	IP doğruluğunun korunması	++++		-
	Gizli mesajın şüphe uyandırmadan iletilmesi	-		++++
Özellikler	Görünmezliğin algılanması	++++		+++++
	İstatistiksel veya algoritmik görünmezlik	+		+++++
	Gizli verinin elde edilmesine, zarar görmesine veya değiştirilmesine karşı sağlamlık	+++++		-
	Sinyal işlemeye karşı dayanıklılık	++++		+
	Genel sıkıştırma işlemlerinde gizli verinin korunması	++++		++
	Büyük veri gizleme kapasitesi	++		++++
Algılama/ Geri elde etme	Örtü dosyası olmadan geri elde etme/algılama	-	++++	++++
	Örtü dosyası ile geri elde etme	++++	-	-
	Geri elde etme/algılama sırasında karmaşıklık ihtiyacı	++		+++

+++++: Çok önemli, ++++: Gereksinim, +++: Önemli, ++: Olması gereken, +: Kullanışlı, -: Gereksiz

3.6. Sonuç

Bu bölümde veri gizleme ve şifreleme yöntemleri ile ilgili genel bilgiler verilmiştir. Veri gizleme yöntemlerinin gelişim süreçleri, uygulama alanları ve gizli haberleşmedeki önemleri açıklanmıştır. Günümüzde var olan sırörtme tekniklerinin zayıflıklarının bilinmesi sırörtme tekniklerinin geliştirilmesi için önemli olduğundan, bu zayıflıklar ile ilgili bilgiler burada sunulmuştur.

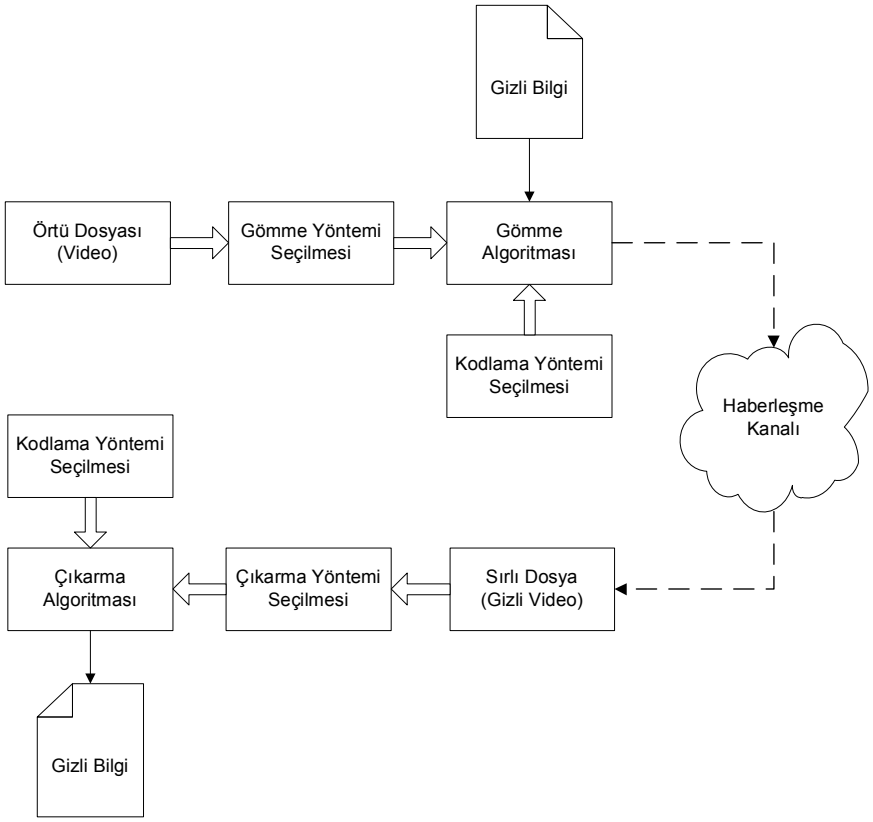
BÖLÜM 4. HAREKETLİ GÖRÜNTÜ UYGULAMALARI İÇİN SIRÖRTME YAKLAŞIMI İLE GELİŞTİRİLEN VERİ GÖMME ALGORİTMALARI VE GERÇEKLEŞTİRİLMELERİ

4.1. Giriş

Sırörtme ile ilgili olarak son yıllarda yapılan çalışmaların büyük çoğunluğu sadece uzay boyutundan faydalanarak yapılan ve hareketsiz görüntüler (resim) içerisine veri gizleme ile ilgilidir. Bu konudaki çok az çalışma veri gizleme işlemini hem uzay boyutunda hem de zaman boyutunda ele almaktadır. Sunulan tez çalışmasında ise bir görüntü içerisine hem uzay boyutunda hem de zaman boyutunda veri gizlemek için yeni yöntemler önerilmektedir.

4.2. Geliştirilen Veri Gizleme İşleminin Genel Çalışma Prensibi

Tez çalışması süresince geliştirilen veri gizleme yöntemlerinin genel blok diyagramı Şekil 4.1'de görülmektedir. Gömü dosyası (gizli veri), gömme yöntemi seçiminden sonra örtü dosyası içerisine gömme ve kodlama algoritmaları vasıtası ile yerleştirilir. Ardından haberleşme kanalına gönderilen gizli veri hedef alıcıya iletilir. Alıcı tarafta öncelikle işlem türü olarak çıkarma yöntemi seçilir. Daha sonra gönderici tarafta kullanılan gömme algoritmasına göre çıkarma algoritması belirlenir. Belirlenen çıkarma algoritması ve gönderici tarafta kullanılan kodlama algoritmasına göre orijinal gizli veri elde edilir.

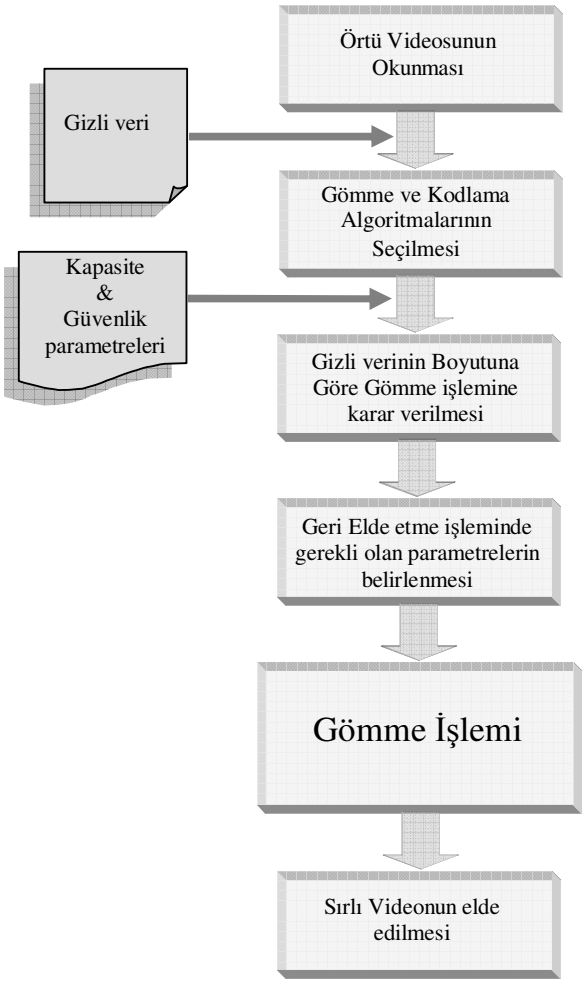


Şekil 4.1. Önerilen sırörtme yaklaşımı ile veri gömme yönteminin genel blok diyagramı.

4.2.1. Veri gizleme işlemi

Veri gizleme işlemi 'avi' video formatındaki herhangi bir örtü videosunun program tarafından okunmasıyla başlar. Bu işlem ile örtü videosunun toplam çerçeve sayısı, süresi, bellekte kapladığı alan bilgileri elde edilir. Örtü videosunun okunmasından sonra veri gizlemede kullanılacak algoritma seçilir. Veri gizleme algoritmasının seçiminden sonra örtü videosuna göre kullanılabilecek en yüksek gizli veri saklama kapasitesi program tarafından hesaplanarak kullanıcıya gösterilir. Böylece kullanıcı seçtiği örtü videosu içerisine ne kadar boyutta bir gizli veri gömebileceği konusunda bilgi sahibi olur. Örneğin veri gizleme işleminde histogramlar yöntemi kullanılacak ise; gömülebilecek gizli veri boyutu, örtü videosunun histogram değeri bulunduktan sonra veri gömmeye uygun piksellerin olduğu çerçevelerin belirlenmesi ile hesaplanır. Aynı zamanda bu özellik kullanıcıya büyük bir zaman tasarrufu da sağlamaktadır. Veri gizleme algoritmasının seçilmesinin ardından gömü dosyasının

örtü dosyasına nasıl kodlanacağını belirleyen kodlama yöntemi seçilir. Seçilen kodlama yöntemi sayesinde veri gizlemeye uygun olarak belirlenen piksellere gömü dosyasının ASCII kodları yerleştirilir. Kodlama işlemi sırasında bir ASCII kodunun bir piksel içerisine gömülmesi esasına dayanan RGB ve R ağırlıklı kodlama yöntemleri veya literatürde sıkça kullanılan en az öneme sahip bit içerisine gömme esasına dayanan LSB kodlama yöntemi kullanılır. Tez çalışması süresince geliştirilen kodlama yöntemlerinin başarımlarını ölçebilmek amacıyla LSB kodlama yöntemi de veri gömme programına eklenmiştir. Program tarafından hesaplanan olabilecek en büyük gömü dosyası boyutuna göre kullanıcı, bir gömü dosyası seçer. Bu aşamadan sonra örtü dosyasının ilk çerçevesi içerisine veri gizleme algoritması, veri kodlama yöntemi, gömü dosyası boyutu, gömü dosyasının türü gibi bilgiler kodlanır. Böylece gizlenmiş veri geri elde edilirken kullanıcının gömü dosyası hakkında herhangi bir bilgiye ve orijinal örtü dosyasına sahip olmasına ihtiyacı olmayacaktır. Seçilen veri gizleme algoritmasına göre örtü dosyasının ilk çerçevesi haricindeki diğer çerçevelerinde veri gizlemeye uygun pikseller belirlenir. Veri gizlemeye uygun olarak belirlenen piksellerin içerisine seçilen veri kodlama yöntemine göre veri gömme işlemi yapılır. Gizli veri boyutuna bağlı olarak veri gizleme işlemi sürer. Gömü dosyasının tamamı örtü videosuna gizlendikten sonra taşıyıcı video (sırlı video) kaydedilir. Gömme işlemine ait istatistiksel veriler kullanıcıya sunularak uygulama sonlandırılır.



Şekil 4.2. Genel Veri Gizleme Akış Diyagramı.

4.2.2. Gizli verinin geri elde edilmesi işlemi

Gizli/gömülü verinin geri elde edilmesi işlemi sırlı videonun program tarafından okunması ile başlar. Bu işlem ile sırlı videonun ilk çerçevesinden gömü dosyasının boyut bilgisi, uzantı bilgisi, veri gizleme algoritması ve veri kodlama yöntemi bilgilerine ulaşılır. Bu bilgiler ışığında veri gizlemede kullanılan gömme algoritması ve kodlama yöntemleri esas alınarak veri geri elde etme işlemi başlar. İçerisine veri gizlenmiş örtü dosyasının çerçeveleri sırayla gezilerek piksellerden gizlenmiş veriler alınır. Bu işlem ilk çerçeveden elde edilen gömü dosyası boyutuna ulaşılıncaya kadar devam eder. Gömü dosyasının boyutuna ulaşıldığı zaman geri elde edilen gömü dosyası (gizli veri) kaydedilir ve veri geri elde etme işlemi sonlandırılır.

Şekil 4.3. Gizli veri Geri Elde Etme Akış Diyagramı.

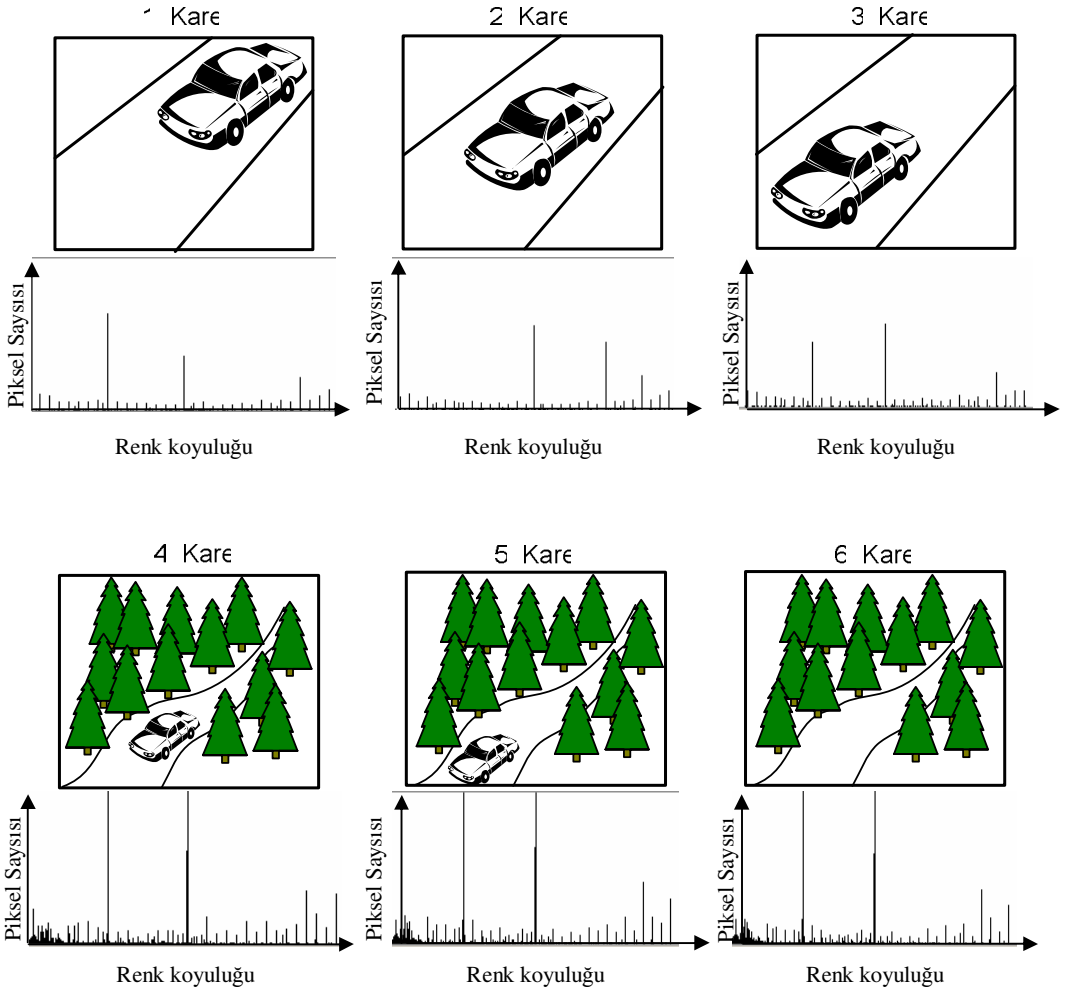
4.3. Geliştirilen Veri Gizleme Yöntemleri

Çalışmamızda öncelikle veri gömülebilecek uygun piksellerin belirlenmesi gerçekleştirilir. Bu işlem için histogramlar ve dalgaboyu yöntemleri geliştirilmiştir. Geliştirilen yöntemler hakkında detaylı bilgilendirme aşağıdaki kısımlarda verilmiştir.

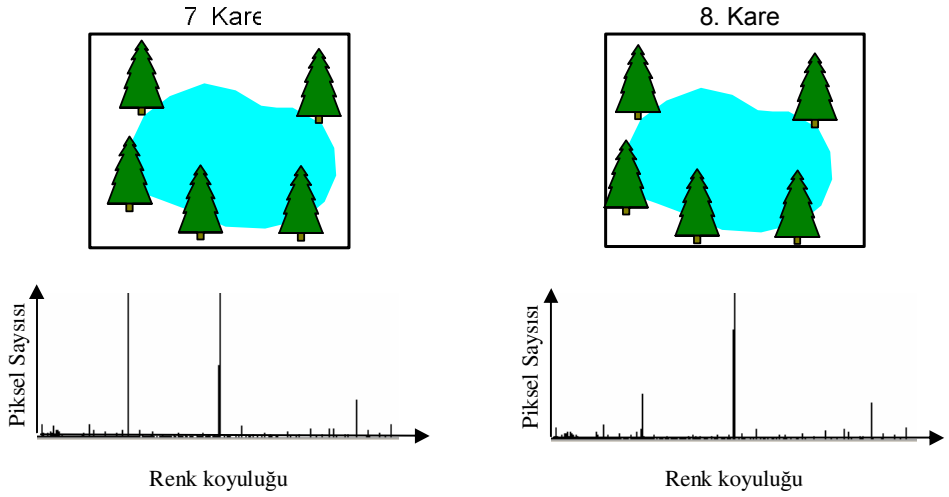
4.3.1. Histogramlar yöntemi

Histogramlar yönteminde ardı sıra gelen her bir video çerçevesinden elde edilen histogram değerleri yorumlanır. Bu yöntemde öncelikle içerisine veri gizlenecek görüntünün çerçeveleri elde edilir. Elde edilen her bir video çerçevesinin histogram değerleri bulunur. Histogram, bir resmi oluşturan piksellerin sahip oldukları renk bileşenlerinin koyuluk bilgilerine göre dağılımlarını gösteren değerler dizisidir (daha fazla bilgi için bkz. Bölüm II). 24 – bit renkli resimler için histogram; tipik olarak 256 elemanlı pozitif tam sayılar dizisidir. Bir resmin histogramı alındığında 0'dan farklı olan değerler ne kadar fazla ise o resim hakkında çok fazla renk ve ton içerdiği söylenebilir. Eğer alınan histogramda 0'dan farklı olan değerler ardışıl olarak bir

aralığa dizilmişse o resmin neredeyse düz bir renk olduğu söylenebilir. Böylelikle her bir video çerçevesini oluşturan renkler hakkında bilgi sahibi olunur. Yapılan çalışmada geliştirilen yöntemlerde, ardışıl video çerçeveleri arasındaki histogram farkları her bir renk bileşeni (R, G, B) için ayrı ayrı elde edildikten sonra bu bileşenlerin ortalaması alınarak ardışıl video çerçevelerindeki renk ve hareket geçişlerini değerlendirme imkânı veren tek bir değer elde edilir. Bu değerin büyük olması iki çerçeve arasında renk ve hareket değişimlerinin fazla olduğunu, bu değerin küçük olması ise sahne içeriğinin hemen hemen hiç değişmediğini ve renk değişiminin olmadığını belirtir. Bu yaklaşım aynı zamanda literatürde video bölümlendirme (segmentation) olarak da bilinen çalışmalarda da kullanılmaktadır [86].



Şekil 4.4. Farklı sahne geçişlerini ve histogramlarını gösteren örnek bir sayısal video.



Şekil 4.4. Farklı sahne geçişlerini ve histogramlarını gösteren örnek bir sayısal video (devam).

Şekil 4.4'de sekiz çerçeveden oluşan örnek bir video verilmiştir. Dikkat edildiğinde video çerçeveleri arasındaki ilk büyük görüntü farkı 4. çerçeve ile başlamaktadır. Bu durumda ilk 3 çerçeve arasında büyük bir değişim göze çarpmamaktadır ki bunun anlamı çerçeveler arasındaki histogram farklarının büyük olmadığıdır. Bu durum çerçevelerin altında verilmiş olan histogram grafiklerinde de görülmektedir. 4. ve 5. çerçeveler arasında da büyük bir fark olmadığı görülmektedir. 6. çerçeve, 5. ve 7. çerçevelerden farklı olduğu için tek başına değerlendirilebilir. Yani bu çerçevede histogram farkı oldukça büyüktür. 7. ve 8. çerçeveler arasında da yine histogram farkları oldukça küçüktür. Ardışıl video çerçeveleri arasındaki bu renk ve hareket geçişlerini algılamak için eşik değeri denen sayısal bir değer kullanılır. Eşik değeri, ardışıl çerçeveler arasında bir değişim veya benzerlik algılanmasında kullanılan, maksimum alabileceği değer video çerçevelerinin boyutu (MxN) ile ifade edilen piksel sayısıdır ve 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 hassasiyetinin artırılmasına karşılık bölümlenebilecek çerçeve sayısında düşme olur. Çerçeve sayısının azalması gizlenmek istenen gömü dosyası boyutunun azalması anlamına gelmektedir. Eşik değerinin düşük seçilmesi durumunda ise hassasiyet azalacak fakat bölümlenen çerçeve sayısı artacaktır. Bu durumda ise gizlenmek istenen gömü dosyası boyutu artacaktır. Bu bilgiler ışığında ardışıl çerçevelerin histogram farkları kullanıcının verdiği bir eşik değeri ile

karşılaştırılarak veri gizlenebilecek video çerçeveleri ve pikselleri belirlenir. Eşik değerinin üzerinde kalan bileşenler seçilirse, ardışıl video çerçevelerinin renk bakımından karışık bir yapıya sahip olduğu anlaşılır ki bunu Farklı Histogramlar (FH) yöntemi olarak adlandıracağız, eşik değerinin altında kalan bileşenlerin seçilmesi durumunda ise ardışıl video çerçevelerinin renk bakımından tekdüze olduğu anlaşılır ki bunu da Benzer Histogramlar (BH) yöntemi olarak adlandıracağız.

Histogramlar yönteminde veri gömmeye uygun alanlar iki farklı yöntemle belirlenir.

A- Çerçeve tabanlı yöntemde; video çerçeveleri bir bütün olarak değerlendirilir. Sahne içeriğinin değiştiği veya değişmediği (kullanılan veri gömme yöntemine göre) durumlar göz önüne alınarak ardışıl video çerçevelerinin tamamına veri gömme yapılır.

B- Blok tabanlı yöntemde ise; öncelikle video çerçeveleri çerçeve boyutları göz önüne alınarak matematiksel ifadelerle bloklara ayrılır. Ardışıl video çerçevelerinde birbirlerine karşılık gelen blokların karşılaştırılması ile veri gömülebilecek bloklar belirlenir. Bu şekilde video çerçeveleri içerisinde belirlenen uygun bloklara veri gömme yapılarak gereksiz piksel bozulmaları ve doğal olarak da algılanabilirlik olabildiğince düşürülmüştür.

4.3.1.1. Farklı histogramlar yöntemi ile veri gizleme

FH yöntemi ile hedeflenen, video çerçeveleri arasındaki uzamsal algılanabilirliğin önlenmesinin yanında zamansal algılanabilirlik sorununa da bir çözüm getirmektir. FH ile veri gizlerken çerçeve tabanlı yöntem kullanıldığında, ardı sıra gelen video çerçevelerinin histogram değerleri birbirleriyle karşılaştırılır. İGS'nin fark edemediği renk ve hareket geçişlerine sahip çerçeveler belirlenir. Bu renk ve hareket geçişlerinin görüldüğü çerçeveler veri gömme işleminde kullanılmak üzere seçilir. Çerçeve tabanlı yöntemde esas olan çerçeveler arasında bu geçişlerin olmasıdır. Şekil 4.4'de verilen örnek video sahnelerine bakıldığında; üçüncü ve dördüncü çerçevelerin histogram değerleri farklıdır. Bunun anlamı üçüncü ve dördüncü çerçevelere veri gizleme yapılabileceğidir. Aynı şekilde beşinci, altıncı ve yedinci

çerçevelerin de farklı histogram değerlerine sahip oldukları görülmektedir. Bu gibi renk ve hareket geçiş anlarında veri gömme işlemi gerçekleştirildiğinde İGS bunu algılayamayacaktır. Çünkü yapılan veri gömme işlemi saniyenin 1/30'unda gerçekleştirildiğinden İGS'nin algılama zamanının çok çok altında olacaktır. FH yöntemine ait işleyişin akış diyagramı blok şema halinde Şekil 4.6'da verildiği gibi olacaktır.

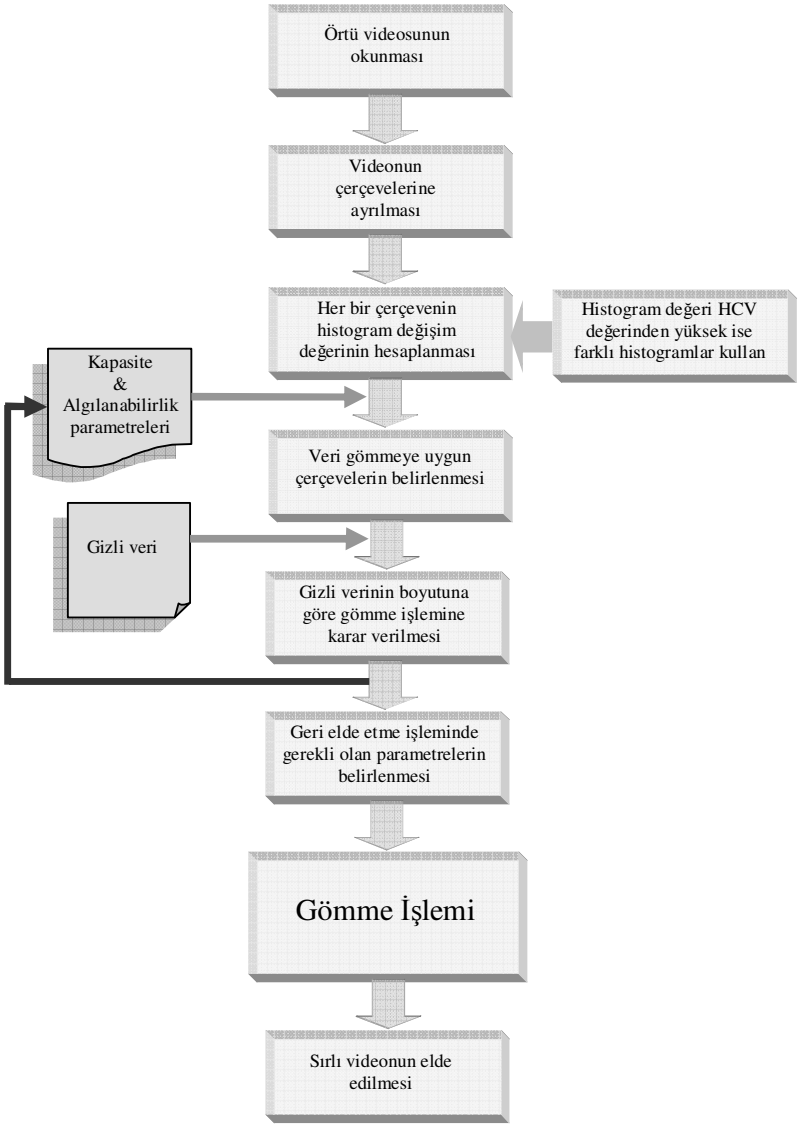
Çerçeve tabanlı FH yönteminde hareket veya renk geçişlerinin olduğu çerçeveler belirlendikten sonra, veri gizleme işlemi tüm çerçevenin piksellerinin içerisine ardışık bir şekilde yapılmaktadır. Her ne kadar İGS'nin bu durumda meydana gelen değişimi algılaması imkânsız gibi görülse de çerçevedeki bütün pikseller ardışık bir şekilde değiştirileceğinden algılanabilirlik de artacaktır. Bu ise istenmeyen bir durumdur.

Çerçeve tabanlı yöntemde ortaya çıkan bu zayıflığın iyileştirilmesi için Blok Tabanlı Farklı Histogramlar (BTFH) yöntemi geliştirilmiştir. Çerçeve tabanlı yöntemde olduğu gibi çerçeveler arasındaki renk ve hareket geçişlerinin algılanması esasına dayanan bu yöntemde farklı olarak veri gömme işlemi çerçevenin tümüne değil hareket veya renk geçişlerinin olduğu bölgelere yapılmaktadır. Veri gömme için belirlenen çerçevelerdeki blokların histogram değerlerinin birbirleriyle karşılaştırılması ile bu bölgeler tespit edilerek veri gömme işlemi gerçekleştirilir. Şekil 4.4'de verilen örnek video sahnelerine bakıldığında; çerçeve tabanlı yöntemden farklı olarak üçüncü ve dördüncü çerçevelerin bloklarının histogram değerleri karşılaştırıldığında üçüncü çerçevede bulunan otomobil veri gizleme için uygun bir bölgedir. Beşinci çerçevedeki otomobilin altıncı çerçevede olmaması otomobilin bu çerçevede de veri gizleme için uygun bir nesne olduğunu gösterir. Altıncı çerçevede bulunan yedinci çerçevede olmayan yol ve bazı ağaçlar da veri gizleme işlemi için çerçeve içindeki uygun bölgelerdir. Böylece çerçevedeki tüm pikseller ardışık olarak değiştirilmediğinden algılanabilirlik daha da düşmektedir. Şekil 4.5'de de görüldüğü gibi bir haber programı görüntüsünde değişen bölge sunucunun ağız ve yüz bölgesidir. Arka platform ve dekor sabit olduğundan buralarda bir değişim söz konusu değildir. Blok tabanlı yöntem kullanılarak veri gizleme işlemi gerçekleştirildiğinde veri gömme işlemi sadece sunucunun ağız ve yüz bölgesine

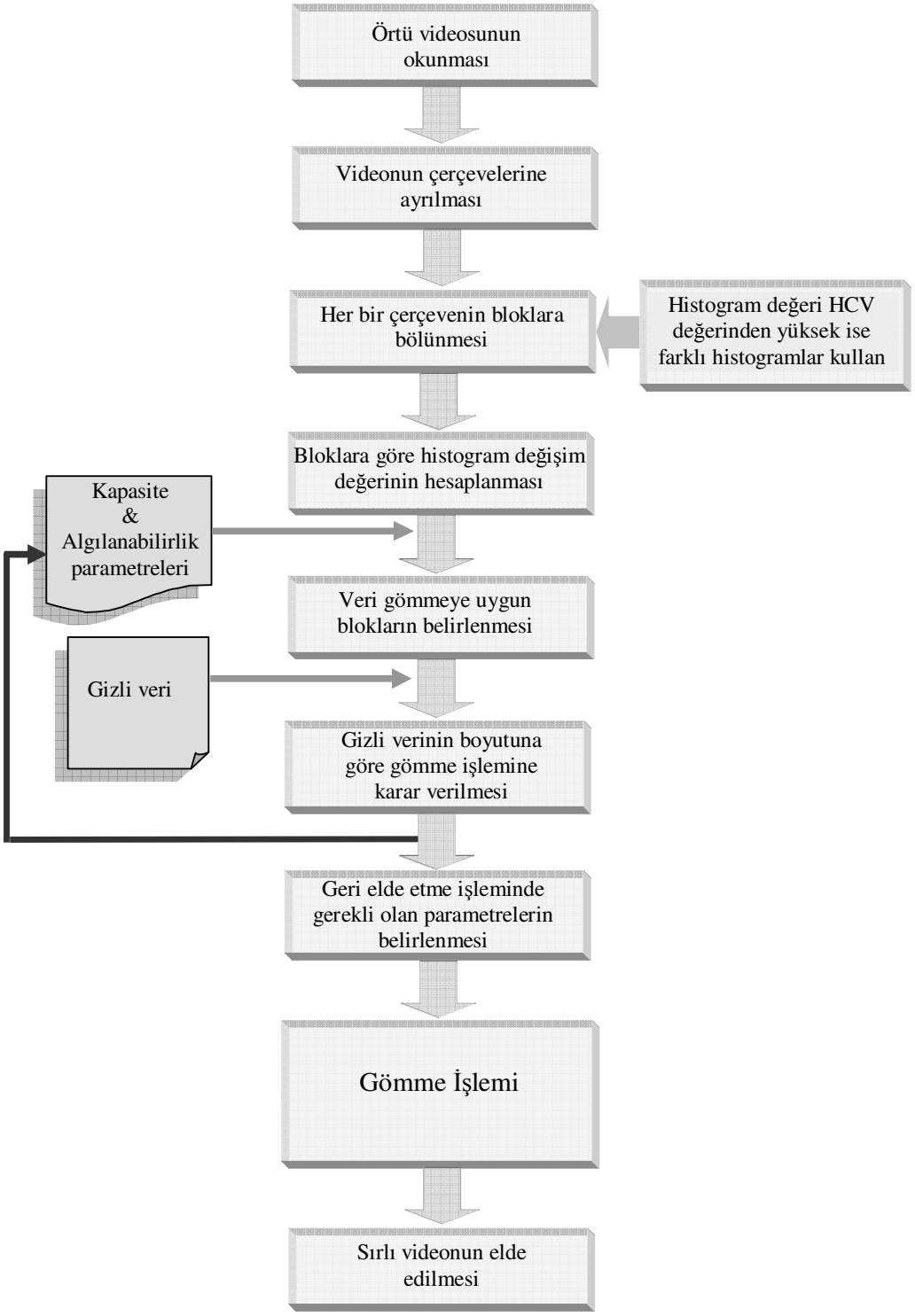
yapılacak ve ilgili çerçevedeki piksellerin değişimleri en aza indirilmiş olacaktır. BTFH yönteminin veri gizleme işleminin akış diyagramı da Şekil 4.7'de blok şema halinde gösterildiği gibi olacaktır.

a) Birinci çerçeve b) İkinci çerçeve c) Üçüncü çerçeve

Şekil 4.5. Bir haber programından örnek sahneler.



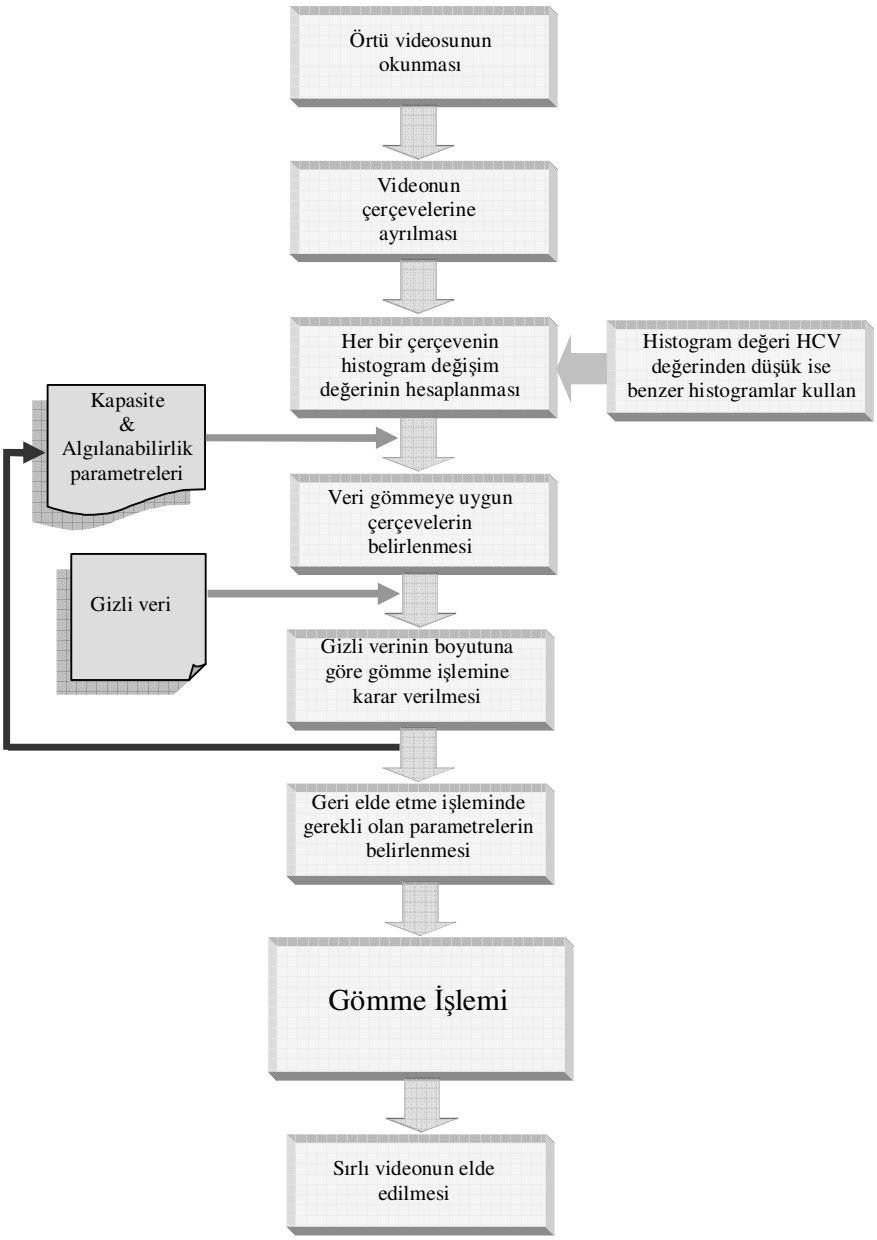
Şekil 4.6. Farklı Histogramlar Yöntemi Akış Diyagramı.



Şekil 4.7. Blok Tabanlı Farklı Histogramlar Yöntemi Akış Diyagramı.

4.3.1.2. Benzer histogramlar yöntemi ile veri gizleme

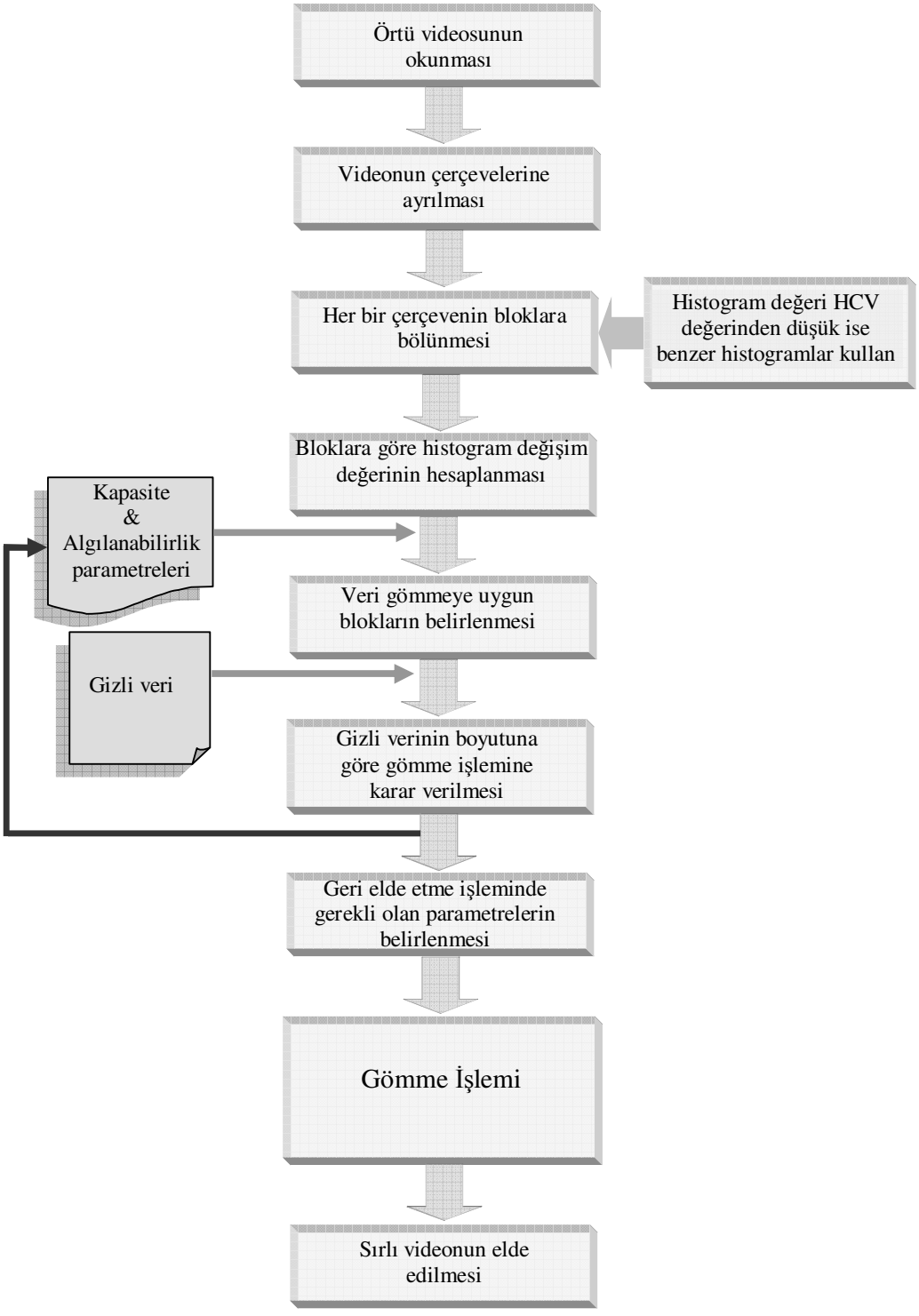
BH yöntemi ile veri gizlerken çerçeve tabanlı yöntem kullanıldığında, ardışık video çerçevelerinin histogram değerlerinin birbirleriyle karşılaştırılmaları ile renk ve hareket geçişlerinin olmadığı çerçeveler belirlenir. Bu çerçevelerin belirlenmesi işlemi FH yönteminde olduğu gibi olacaktır. Çerçeve tabanlı BH yöntemine ait akış diyagramı Şekil 4.8'de blok halinde verilmiştir.



Şekil 4.8. Benzer Histogramlar Yöntemi Akış Diyagramı.

BH yönteminin daha iyi anlaşılması açısından yine Şekil 4.4'de verilen örnek video sahneleri incelenirse; birinci, ikinci ve üçüncü çerçevelerin histogram değerlerinin birbirlerine yakın olduğu görülür. Bu çerçeveler veri gizleme işlemi için uygun olan çerçevelerdir. Dördüncü ve beşinci çerçevelerinde histogram değerlerinin birbirlerine yakın olduğu söylenebilir. Fakat üçüncü ve dördüncü çerçeveler arasındaki histogram değişimi büyük olduğundan BH yöntemine göre bu çerçeveler veri gömme için uygun olmayan çerçevelerdir. Son olarak yedinci ve sekizinci çerçevelerin de histogramları birbirlerine yakın olduğu için bu çerçeveler de veri gömme için uygun çerçevelerdir. Bu renk ve hareket geçişlerinin en az olduğu veya hiç olmadığı çerçeveler veri gömme işleminde kullanılmak üzere seçilir. Çerçeve tabanlı yöntemde esas olan sabit, durağan objelere sahip ardışık iki veya daha fazla çerçevenin olmasıdır. Bu yöntemin en büyük avantajı gömülebilecek gizli veri kapasitesinin yüksek olmasına imkân sağlamasıdır. Fakat aynı oranda da algılanabilirlik artmaktadır. Bunun sebebi ise sabit, durağan bölgelerdeki renk değişimlerinin İGS tarafından daha rahat farkedilebilmesidir. Bu yöntemle yapılan veri gömme işleminde çerçevedeki bütün pikseller kullanılmaktadır. Bunun anlamı veri gömmede sabit, durağan nesnelerin kullanıldığı gibi görüntüdeki değişen nesnelerinde kullanılacağı anlamına gelmektedir. Bu durum algılanabilirlik açısından istenmeyen bir zayıflıktır.

Çerçeve tabanlı yöntem kullanıldığında ortaya çıkan bu zayıflığın giderilmesi için Blok Tabanlı Benzer Histogramlar (BTBH) yöntemi geliştirilmiştir. Çerçeve tabanlı yöntemde olduğu gibi çerçeveler arasındaki renk ve hareket geçişlerinin olmaması esasına dayanan bu yöntemde farklı olarak veri gömme işlemi çerçevedeki tüm piksellere değil sadece sabit, durağan nesnelerin olduğu bölgelere yapılmaktadır. Böylece ilgili çerçevedeki piksellerin tümü değiştirilmediğinden dolayı algılanabilirlik daha da düşük olacaktır. BTBH yönteminin akış diyagramı Şekil 4.9'da görüldüğü gibidir.



Şekil 4.9. Blok Tabanlı Benzer Histogramlar Yöntemi Akış Diyagramı.

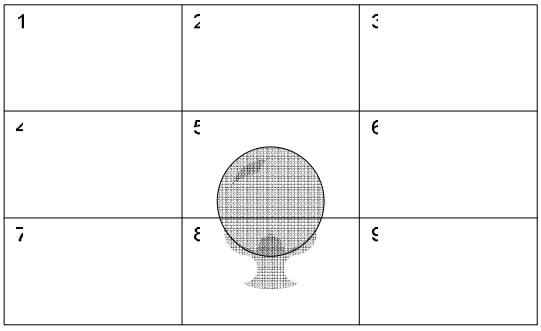
Çerçeve tabanlı yöntem kullanılarak Şekil 4.5'de verilen örnek video içerisine veri gömme yapıldığında, sunucunun ağız ve yüz bölgesi dışında kalan bölgeler veri

gömme için uygun olarak belirlenecektir. Fakat gömme işlemi belirlenen çerçevedeki tüm piksellere ardışık bir şekilde yapılacağından algılanabilirlik yüksek olabilmektedir. Bu zayıflığı iyileştirmek için geliştirilen blok tabanlı yöntemde ise, gömme için belirlenen çerçevelerdeki blokların histogram değerleri birbirleriyle karşılaştırılarak gömme işlemine karar verilir. Şekil 4.4'de verilen örnek video sahnelerine bakıldığında; birinci, ikinci ve üçüncü çerçevelerin histogram değerlerinin birbirlerine yakın olduğu görülür. Bu çerçevelerde veri gizleme işlemi için uygun olan bloklar her üç çerçevede de değişmeyen bölgeler olacaktır. Bunun anlamı, video çerçevesi ilerledikçe hala görüntüde kalan nesnelerin veri gömme için uygun olan bölgeler olmasıdır. Dördüncü ve beşinci çerçevelerinde histogram değerlerinin de birbirlerine yakın olduğu söylenebilir. Bu iki çerçevede de veri gömme işlemi her iki çerçeve arasında değişmeyen nesnelere veya bölgelere yapılacaktır. Son olarak yedinci ve sekizinci çerçevelerde de durum aynıdır. Böylece veri gömme işleminde meydana gelen piksellerdeki değişimler en aza indirilmiş olacak ve algılanabilirlik düşürülmüş olacaktır.

4.3.2. Bölgesel histogramlar optimizasyonu

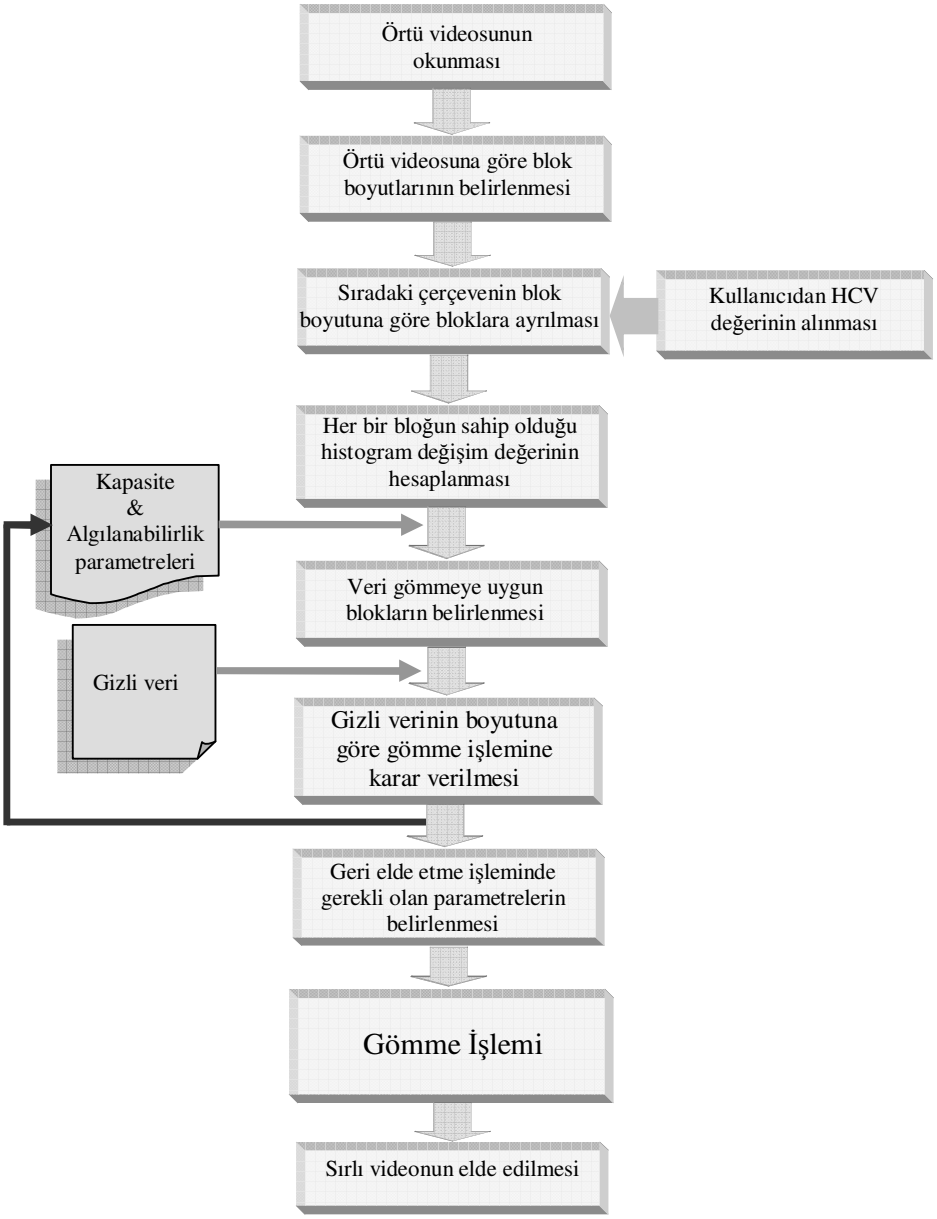
Video çerçevelerine yapılan veri gömme renk bakımından tekdüze olan bölgelere yapıldığında uzamsal ve zamansal algılanabilirlik artmaktadır. Bu algılanabilirliği düşürmek amacıyla geliştirilen bölgesel histogramlar optimizasyonu yönteminde veri gömülecek video çerçeveleri matematiksel ifadelerle belirlenen bloklara bölünür. Her bir bloğun histogram değeri hesaplanarak blokların renk içeriği hakkında bilgi sahibi olunur. Bir bloğun histogram dağılımı belirlenen eşik değerinin altındaysa blok içinde farklı renkler olmadığı yani tekdüze renk ihtiva ettiği ve veri gömme için uygun olmadığı anlaşılır. Bloğun histogram dağılımının belirlenen eşik değerinin üzerinde olması durumunda ise blok içerisinde farklı renklerin olduğu ve veri gömme için uygun olduğu söylenir. Tekdüze bir renk dağılımına sahip zemin önünde bir nesne bulunan video çerçevesinde veri gömme işlemi nesnenin kenarlarının bulunduğu ve nesne üzerindeki renk dağılımlarının yoğun olduğu bölgelere yapılır. Şekil 4.10'da görülen örnek resimde veri gömme işlemi 5. ve 8. bloklar içerisine yapılacak diğer bloklarda herhangi bir renk çeşitliliği olmadığı için bu bloklara veri gömme yapılmayacaktır. Şekil 4.10'da görülen böyle bir video çerçevesinde tekdüz

renge sahip zemine hiçbir şekilde veri gömmesi yapılmaz. Veri gömme için belirlenen 5. ve 8. bloklarda ise gömme işlemi nesneye ait piksellere yapılacaktır.



Şekil 4.10. Bloklara bölünmüş bir video çerçevesi.

Bölgesel histogramlar yöntemini diğer yöntemlerden ayıran en belirgin özellik; veri gömülecek alanların ardışık çerçevelerin histogram değerlerinin birbirleri ile karşılaştırılmaları yerine blokların histogram değerlerinin kendi içlerinde değerlendirilmesi ile bulunurmasıdır. Yani ardışık çerçevelerin histogram değerleri birbirleri ile karşılaştırılmazlar. Bunun yerine her bir çerçevedeki blokların histogram değerleri kullanıcının belirlediği eşik değeri ile karşılaştırılır ve veri gömülecek pikseller belirlenir. Bu yöntemle veri gömme kapasitesinin artırılması amaçlanırken algılanabilirliğin ise düşürülmesi amaçlanmıştır. Her çerçeveye veri gömülmesine imkân verilerek kapasite artırılırken, çerçevedeki bütün pikseller yerine renk değişiminin en çok olduğu piksellere veri gömülerek de algılanabilirlik düşürülmüştür. Bölgesel histogramlar yönteminin akış diyagramı Şekil 4.11'de görüldüğü gibidir.



Şekil 4.11. Bölgesel Histogramlar Yöntemi Akış Diyagramı.

4.3.3. Dalgaboyu yöntemi

Dalgaboyu (DB) yönteminde İGS'nin zaafından faydalanılarak veri gömme işlemi gerçekleştirilir. Enerji tayfındaki İGS'nin algıladığı renk dalgaboyu aralığı, yani görülebilir ışık alanı bilgisinden faydalanarak veri gizlenecek piksellerin belirlenmesi bu yöntemin temelini oluşturmaktadır.

İçerisine veri gömülmek istenen örtü videosunun çerçevelerinde görülebilir ışık aralığının sınır dalgaboyu değerlerine (380nm–750nm) yakın renklere sahip pikseller belirlenir. Bir başka deyişle morötesi ve kızılötesi dalgaboyu değerlerine yakın renklere sahip pikseller belirlenir. Bu sınırlara yakın dalgaboyu değerlerine sahip renkler kullanılarak veri gizleme işlemi gerçekleştirilir. Burada faydalanılan durum İGS'nin morötesi ve kızılötesi ışık dalgalarını algılayamamasıdır. Böylelikle morötesi ve kızılötesi ışınlarına yakın dalgaboyuna sahip renklerin İGS tarafından algılanmasının da daha zor olacağı aşikârdır.

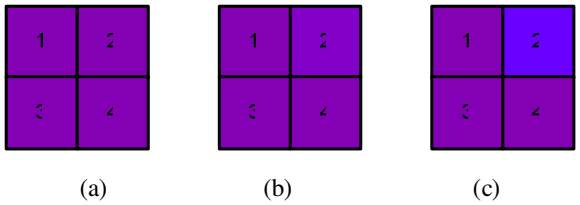
Bu yöntemde de diğerlerinde olduğu gibi örtü videosunun çerçeveleri elde edilir. Her bir ilgili video çerçevesindeki piksellerin ait olduğu renk dalgaboyu değeri geliştirilen algoritma ile bulunur. Bunun için öncelikle mor ve kırmızı renkleri veren RGB renk karışımlarının bir tablosu oluşturulur. Bu tabloyu oluşturmak için herhangi bir resim işleme programından faydalanılabilir. Ayrıca Internette kolayca bulunabilen renk kodlarının listelerinden de faydalanmak mümkündür. Bu çalışmada faydalanılan renklerin listesi ve dalgaboyu değerleri Tablo 4.1'de verilmiştir.

Tablo 4.1. Dalgaboyu değerlerinin tanımlanması.

Dalgaboyu Değeri	**R renk yoğunluğu**	**G renk yoğunluğu**	**B renk yoğunluğu**
Mor renk: 380~400	97~130	0~30	97~175
Kırmızı renk: 730~750	161~200	0~30	0~50

Yukarıdaki tabloya göre, örneğin 100,0,105 RGB değerine sahip bir pikselin kabul edilebilir dalgaboyu aralığında olduğu söylenebilir. Böylelikle, veri gizleme algoritması kullanılarak görülebilir ışığın sınır değerlerine (380nm veya 750nm) yakın dalgaboyuna sahip pikseller veri gömme için belirlenir. Belirlenen her bir pikselin veri gömüldükten sonra da ilk dalgaboyu değerine yakın bir değerde kalıp kalmadığı kontrol edilir. Piksel kabul edilebilir bir renk dalgaboyu değerinde kalıyorsa, bir başka deyişle gömme işlemi sonucunda pikselin sahip olduğu ilk dalgaboyu değerinde çok büyük bir değişim olmuyor ise, bu piksele veri gömme yapılabilir. Şekil 4.12.a'da örnek resimdeki 400nm dalgaboyu değerine sahip mor renkli piksel, veri gömüldükten sonra 400nm ile 410nm aralığında bir dalgaboyu değerinde kalıyorsa bu piksele veri gömme yapılabilir (Şekil 4.12.b). Fakat piksel

veri gömme gerçekleştirildikten sonra örneğin 420nm değerine sahip oluyorsa bu piksel veri gömme için uygun değildir (Şekil 4.12.c). İlk piksel değeri ile sonraki piksel değeri arasında İGS'nin algılayabileceği derecede bir fark söz konusudur.



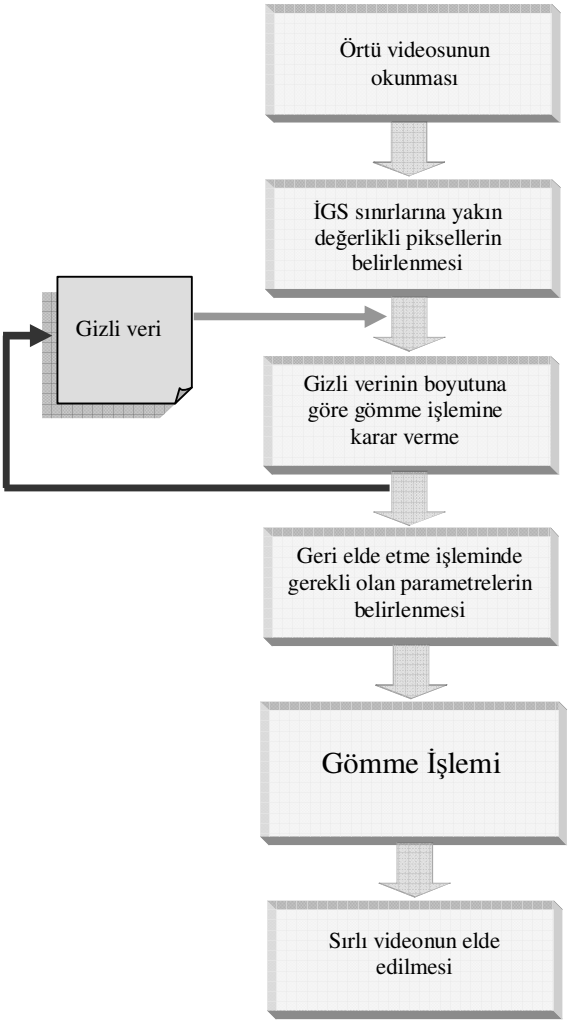
(a) (b) (c)

Şekil 4.12. Mor renk dalgaboyu değerlerine sahip 4 piksellik örnek bloklar.
(a) 4 pikseli de 400nm dalgaboyu olan örnek bir blok.
(b) 2 numaralı pikseli 405nm dalgaboyu olan örnek bir blok.
(c) 2 numaralı pikseli 420nm dalgaboyu olan örnek bir blok.

Standart bir video çerçevesinin 352x288 boyutlarında olduğunu düşünürsek piksel sayısı 101376 olarak hesaplanabilir. Yaklaşık olarak 100 bin piksel içerisinde Şekil 4.12.(a)'da gösterilen orijinal pikselin Şekil 4.12.(b)'deki gibi değişmesinin İGS tarafından algılanması çok zor olacaktır. Fakat Şekil 4.12.(c)'deki gibi bir değişikliğin İGS tarafından algılanma ihtimali daha yüksektir.

DB yönteminde esas olan, gizli verinin içerisine yerleştirildiği pikselin dalga boyu aralığının sahip olduğu orijinal dalga boyu aralığından çıkmaması kıstasıdır ki bu sayede video çerçevelerini oluşturan her bir piksele birbirinden bağımsız olarak veri gömme işlemi gerçekleştirilebilir.

DB yönteminin BH ve FH 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. DB yönteminin akış diyagramı Şekil 4.13'de verildiği gibi olacaktır.



Şekil 4.13. DalgaBoyu Yöntemi Akış Diyagramı.

4.4. Video Ortamında Veri Kodlama Yöntemleri

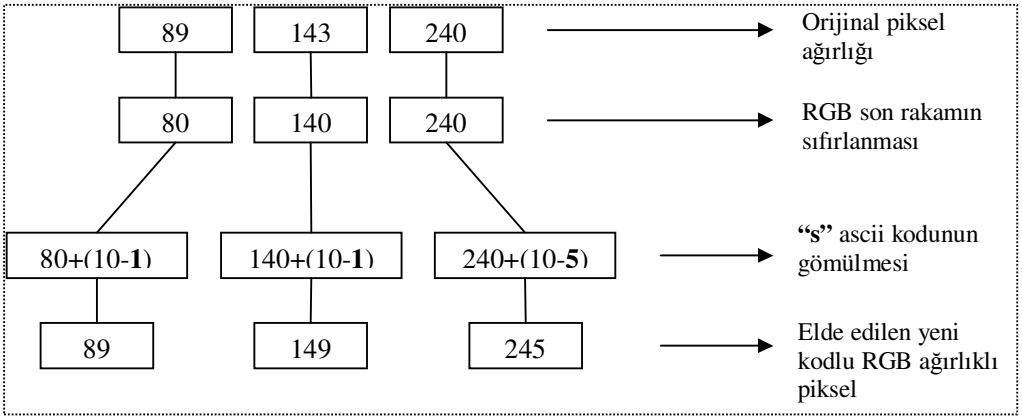
4.4.1. RGB ağırlıklı kodlama tekniği

Örtü videosunda en az bozulma, en fazla veri gizleme kapasitesi sırörtme yöntemlerinde aranan en temel kıstastır. Bunu sağlamak amacıyla resim sırörtme tekniklerinde gizli verinin kodlanması için geliştirilmiş olan RGB ve R ağırlıklı kodlama tekniği bu çalışmada video için uyarlanarak kullanılmıştır [87].

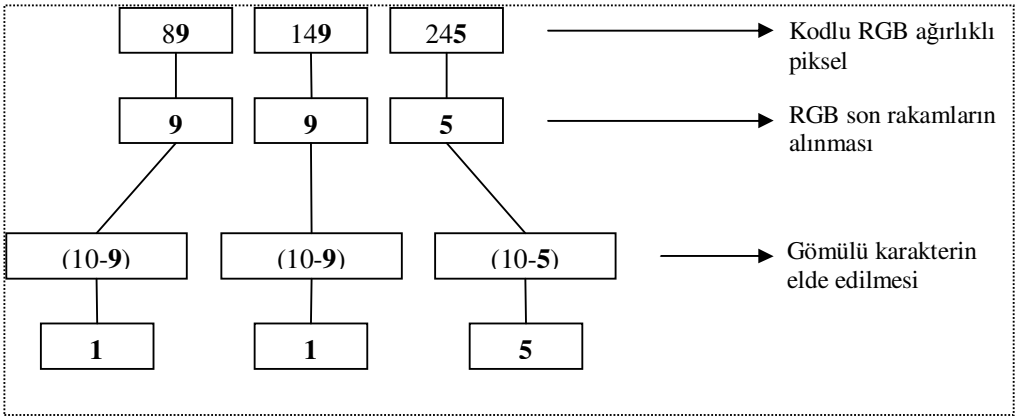
RGB: (89,143,240) olarak üç ana renk dağılımına sahip olan bir pikselin R=89, G=143, B=240 renk ağırlıklarına sahip olduğu söylenebilir. Bu pikselin içerisine "s"

harfinin ASCII karşılığı olan ‘115’ sayısının gömülme işlemi şu şekilde olacaktır (Şekil 4.14); öncelikle R=89, G=143, B=240 gömülen bilginin yeniden elde edilmesi aşamasında sorun yaşamamak için son rakamlar sıfırlanır. Buna göre elimizde R=80, G=140, B=240 değerleri olur. Bir sonraki aşamada “s” harfinin ASCII kodunun her rakamı ‘10’ sayısından çıkarılır (10-1=9, 10-1=9, 10-5=5). Elde edilen bu rakamlar her bir RGB değerlerinin son rakamlarına yerleştirilir. Buyüzden, RGB’nin son rakamlarına bakıldığında anlamlı bir değişikliğin olduğu anlaşılmaması için, gizlenecek bilginin ASCII kodunun her bir rakamı ‘10’ sayısından çıkarılır. Son durumda ise elimizde R=89, G=149, B=245 değerleri bulunur. Gizli verinin elde edilmesi aşamasında (Şekil 4.15) ise pikselin sahip olduğu RGB değerlerinin son rakamları alınır (R=89 G=149 B=245). Bu rakamlar 10 sayısından (10-9=1, 10-9=1, 10-5=5) çıkarılarak tekrar “s” harfinin ASCII kodları elde edilmiş olur.

Veri gömülecek pikselin RGB değeri 250–255 arasında olduğu durumda yukarıda anlatılan işlemlerde hatayla karşılaşılacaktır. Bu durumu engellemek için 250–255 arasındaki değerlere sahip pikseller için RGB değerlerinde 10 azaltma uygulanır. Bir başka istisnai durum da gömülmek istenen karakterin ASCII kodunun 0 ile başlamasıdır (A=065 gibi). Burada R değerinin 10-0=10 çıkması durumunda, sonucun 0 olarak düzeltilmesi gerekmektedir.



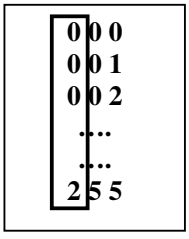
Şekil 4.14. Bir piksel içerisine ASCII kodunun RGB kodlama yöntemi ile gömülmesi işlemi [87].



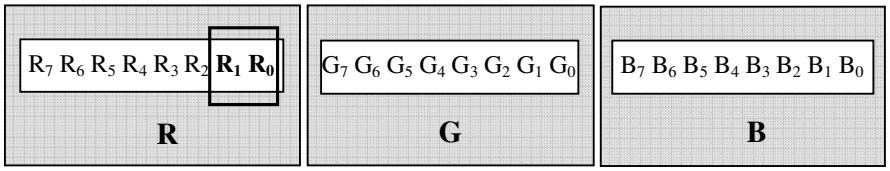
Şekil 4.15. Gömülü ASCII kodunun RGB kodlama yöntemi ile çıkarılması işlemi [87].

4.4.2. R ağırlıklı kodlama tekniği

Yukarıda açıklanan RGB ağırlıklı veri kodlama tekniğinde R-G-B renk ağırlıklarının her üçüne de aynı işlem süreci uygulanarak kodlama gerçekleştirilmiştir. Burada önemli olan orijinal pikselin RGB ağırlıklarının olabildiğince düşük oranlarda değişikliğe uğramasıdır. Bunun doğal bir sonucu olarak da orijinal video ile kodlanmış video arasındaki farklılık azalacaktır. Arzu edilen bu sonuca ulaşmak için "R" ağırlığına gömülen ASCII kodunun ilk bitinin (MSB) sadece 0, 1 ve 2 değerlerini alabilmesi durumundan faydalanılabilir. Böylece "R" ağırlığının kodlama yöntemini diğer iki ağırlığın (G-B) kodlanmasından ayırarak orijinal piksel değerlerinde hedeflenen minimum bozulma elde edilir.

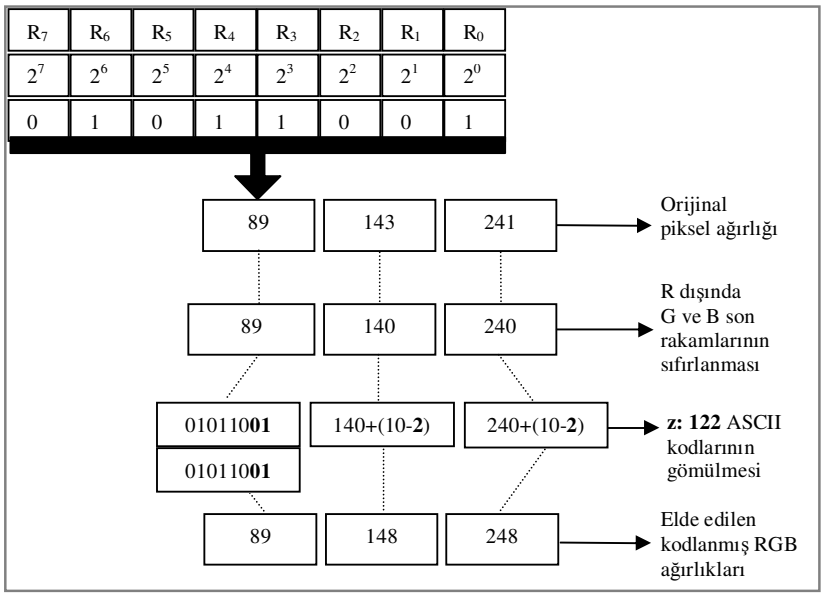


ASCII kod karşılıkları 0–255 arasında değerler aldığından ilk rakam değeri 0, 1 ya da 2 olabilir, 3–9 arası değerler olamaz. Bu durum R ağırlıklı kodlama tekniğinin temelini oluşturur. RGB ağırlıklı kodlama ile veri gizleme uygulamasında 8-bit olarak 3 ayrı renk RGB ağırlıklarını oluşturmaktadır. R ağırlığının ikili karşılığı olan 8–bitin son iki biti bu amaçla kullanılabilir. Bu durum Şekil 4.16'da görülmektedir.

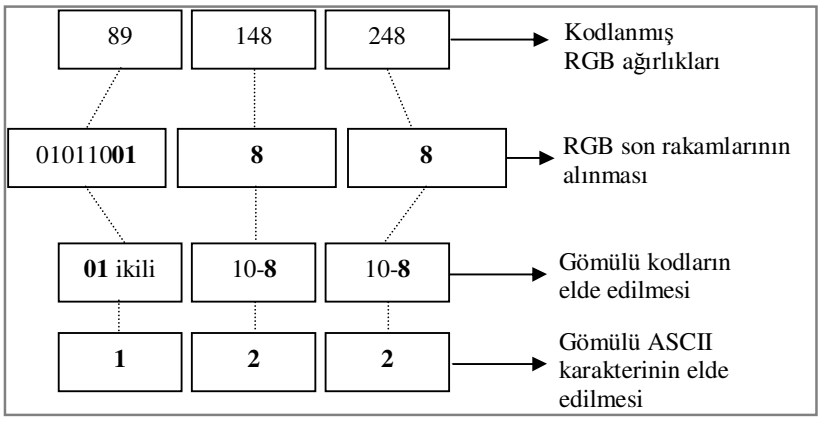


Şekil 4.16. R renk ağırlığının son iki bitinin değiştirilmesi [87].

RGB:(89,143,240) olarak üç ana renk dağılımına sahip olan bir pikselin içerisine "z" harfinin ASCII karşılığı olan 122 sayısının gömülme işlemi Şekil 4.17'de, gömülü bilginin yeniden elde edilmesi işlem süreci ise Şekil 4.18'de görülmektedir.



Şekil 4.17. Bir piksel içerisine ASCII kodunun R kodlama yöntemi ile gömülmesi işlemi [87].

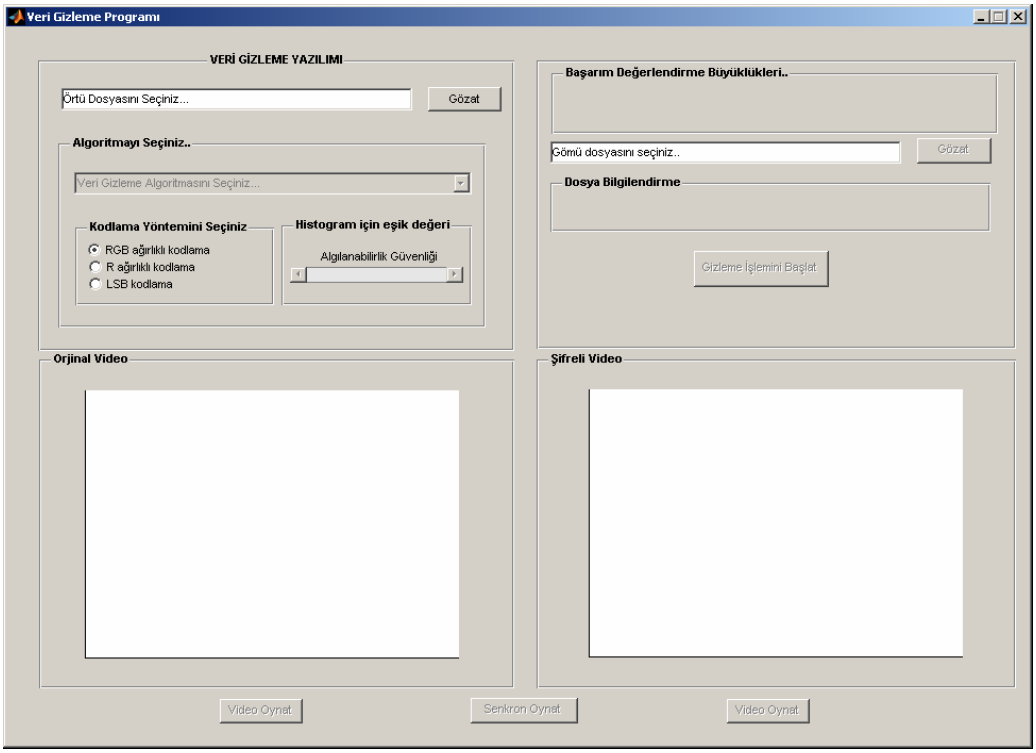


Şekil 4.18. Gömülü ASCII kodunun R kodlama yöntemi ile çıkarılması işlemi [87].

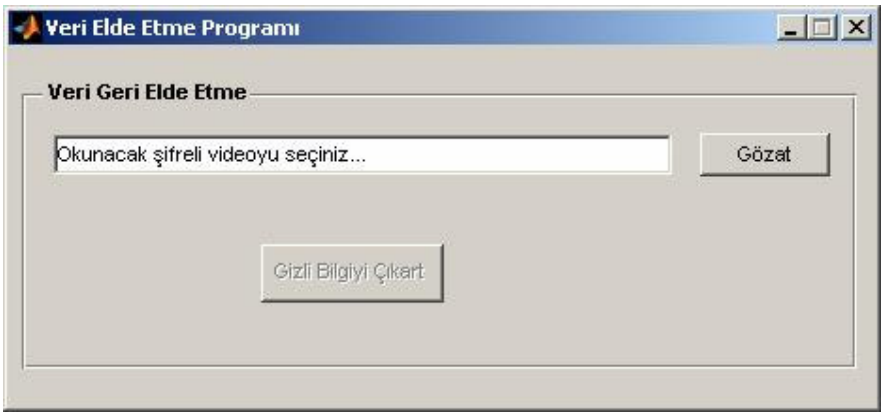
Yukarıda görüldüğü gibi içerisine veri gömülecek pikselin RGB değerleri alınır ve "R" renk değerliği hariç diğer renk değerliklerinin son rakamları aynı RGB kodlama tekniğinde olduğu gibi sıfırlanır. ASCII kodunun alabileceği değer 0–255 arasında değiştiğinden, ASCII kodunun MSB'sine karşılık gelen "R" renk değerinin alabileceği değer en çok 2 olabilir. Bu da ikili sayı olarak '10' değerine karşılık gelir. Bu durum bir avantaj olarak kullanılabilir ve "R" renk değerinin ikili sayı karşılığına ASCII kodunun ilk sayısının ikili karşılığı gömülür.

4.5. Uygulama Yazılımının Tanıtılması

Tasarlanan uygulama yazılımı Matlab 7.3.0.267 R2006b sürümü kullanılarak geliştirilmiştir. Yaklaşık olarak 1595 satırdan oluşan uygulama yazılımı 145 Kbayt büyüklüğündedir. Veri Gizleme işlemi için sekiz yeni algoritma geliştirilmiş olmasına karşın bu algoritmaları iki ana kategoride toplanmaktadır: Histogram tabanlı algoritmalar ve Dalgaboyu tabanlı algoritmalar. Algoritmaları bir önceki bölümde detaylı olarak ele alınan uygulama yazılımının Veri Gizleme adımı dört aşamadan, Gizli Verinin Geri Elde Edilmesi adımı ise sadece bir aşamadan oluşmaktadır. Şekil 4.19'da Veri Gizleme ve Gizli Verinin Geri Elde Edilmesi yazılımlarının ana pencereleri görülmektedir.



(a)



(b)

Şekil 4.19. (a) Veri Gizleme uygulama yazılımı ana penceresi
(b) Gizli Verinin Geri Elde Edilmesi uygulama yazılımı ana penceresi.

4.5.1. Verinin gizlenmesi

Sırörtme olarak adlandırılan veri gizleme bilimi, güvenlik ve gizliliği sağlanmak için haberleşmenin maskelenmesi ilkesini kullanır. Sırörtme tekniklerinde masum görünümlü taşıyıcı (resim, ses, video vb.) dosyaları içerilerine gizli verilerin yerleştirilmesi amacıyla kullanılmaktadır. Tez çalışması sürecinde veri gizleme

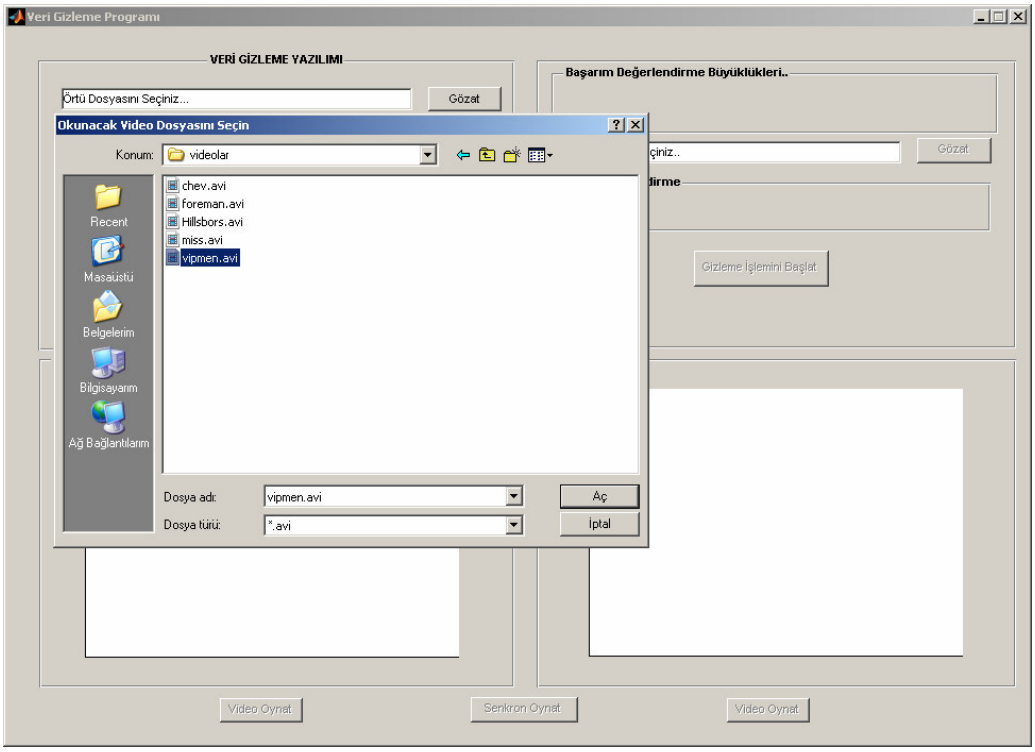
işleminde gizleme nesnesi olarak video kullanılmıştır. Burada önemli bir noktanın bilinmesi gerekmektedir; gömülen ve gömülecek olan dosya türleri birbirinden farklı olabilir. Çalışmada örtü dosyası olarak video dosyaları kullanılırken, gizlenmek istenen veriler; video, ses, resim, metin, html dosyası, ofis dosyaları (doc, xls uzantılı) ya da sıkıştırılmış zip, rar dosyaları olabilir. Gizlenmek istenen nesne türlerinin çeşitliliğinin ve sayısının artırılması uygulama yazılımının kodunda yapılacak birkaç küçük ekleme ile mümkündür.

4.5.1.1. Histogramlar yöntemi ile veri gizleme uygulaması

Histogram tabanlı algoritmaları kullanırken; seçilen algılanabilirlik seviyesine veya gizli verinin boyutuna göre, örtü videosunun histogramına dikkat etmek veri gizleme işleminin kazanımını artıracaktır. Histogram tabanlı yöntemler aşağıda listelenmiştir;

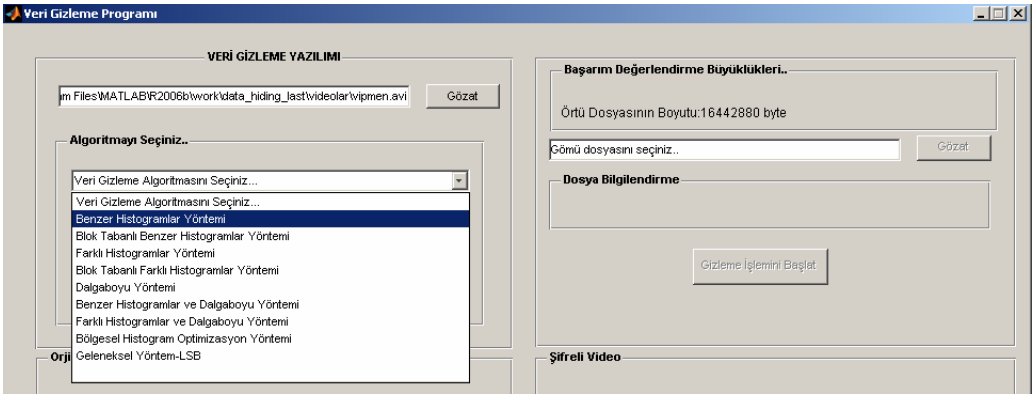
- Benzer Histogramlar Yöntemi
- Blok Tabanlı Benzer Histogramlar Yöntemi
- Farklı Histogramlar Yöntemi
- Blok Tabanlı Farklı Histogramlar Yöntemi
- Bölgesel Histogram Optimizasyon Yöntemi.

Uygulama yazılımı çalıştırıldığında ilk adım gizleme işleminde kullanılacak örtü dosyasının (cover video) seçilmesidir. ‘Örtü Dosyasını Seçiniz’ bilgilendirme kutusunun yanındaki ‘Gözat’ butonuna tıklandığı zaman Şekil 4.20’de görülen iletişim penceresi ekrana gelir.



Şekil 4.20. Video dosyası seçme iletişim penceresi.

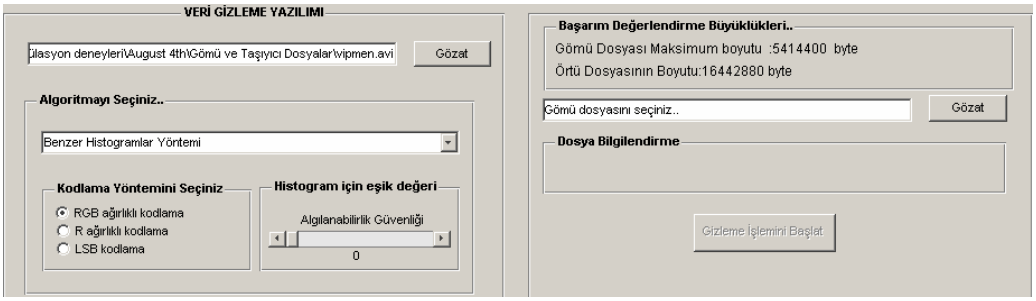
İletişim penceresi kullanılarak bilgisayarda kayıtlı olan '.avi' uzantılı herhangi bir video dosyası (bu uygulama için vipmen.avi) veri gizleme işlemi için seçilir. Video dosyası seçildikten sonra 'Algoritmayı Seçiniz' bölümündeki aşağı açılır menü aktif hale gelecektir. Aşağı açılır menüye tıklandığında Şekil 4.21'de görüldüğü gibi gizleme işleminde kullanılacak algoritmalar listelenir.



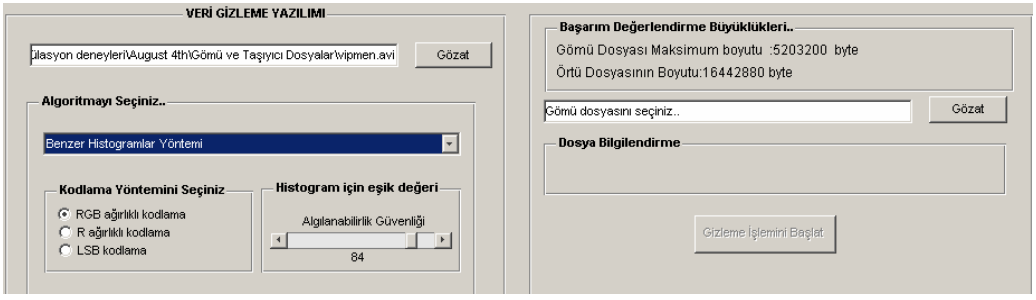
Şekil 4.21. Gizleme işleminde kullanılacak algoritma seçimi.

BH veya FH yöntemlerinden biri seçildikten sonra yazılım otomatik olarak gizleme işlemi için önemli olan bazı bilgileri hesaplayarak yazılım penceresinde sağ üst

köşede bulunan ‘Başarım Değerlendirme Büyüklükleri’ bölümünde gösterir. Bu bilgiler; gömü dosyasının (gizli veri) olabilecek en büyük boyutu ile seçilen örtü dosyasının (seçilen video dosyası) boyut bilgileridir. Gömü dosyasının olabilecek en büyük boyut bilgisine göre gizleyebileceğimiz dosya boyutuna kolayca karar verebilir ve seçimimizi bu bilgiye göre yaparız. Bu bilgi hangi video dosyası içerisine ne kadar büyüklüğünde bir dosya gizleyebileceğimizi açıkça belirtir. Histogram tabanlı veri gizleme işleminde algoritma seçildikten sonra Şekil 4.22.(a)’daki pencerede görülen ‘Histogram İçin Eşik Değeri’ bölümündeki sürgü ile histogram eşik değeri değiştirilebilir. Her bir yeni histogram değerinden sonra gömü dosyasının boyutu tekrar hesaplanarak güncellenir. Sürgünün sağ tarafa doğru hareketi ile algılanabilirlik düşürülürken, doğru orantılı olarak gömme kapasitesi azalacaktır. Sürgünün hareket ettirilmesinden sonra o anki histogram eşik değeri sürgünün hemen altında görülecektir. Şekil 4.22.(a)’da histogram eşik değeri belirlenmemiş ve bu durumda gömü dosyasının olabileceği en büyük boyut 5414400 bayt–5,4 MB olarak hesaplanmıştır. Şekil 4.22.(b)’de ise eşik değeri olarak 84 olarak belirlenmiş ve sonuç olarak gömü dosyasının olabileceği en büyük boyut 5203200 bayt–5,2 MB olarak hesaplanmıştır.



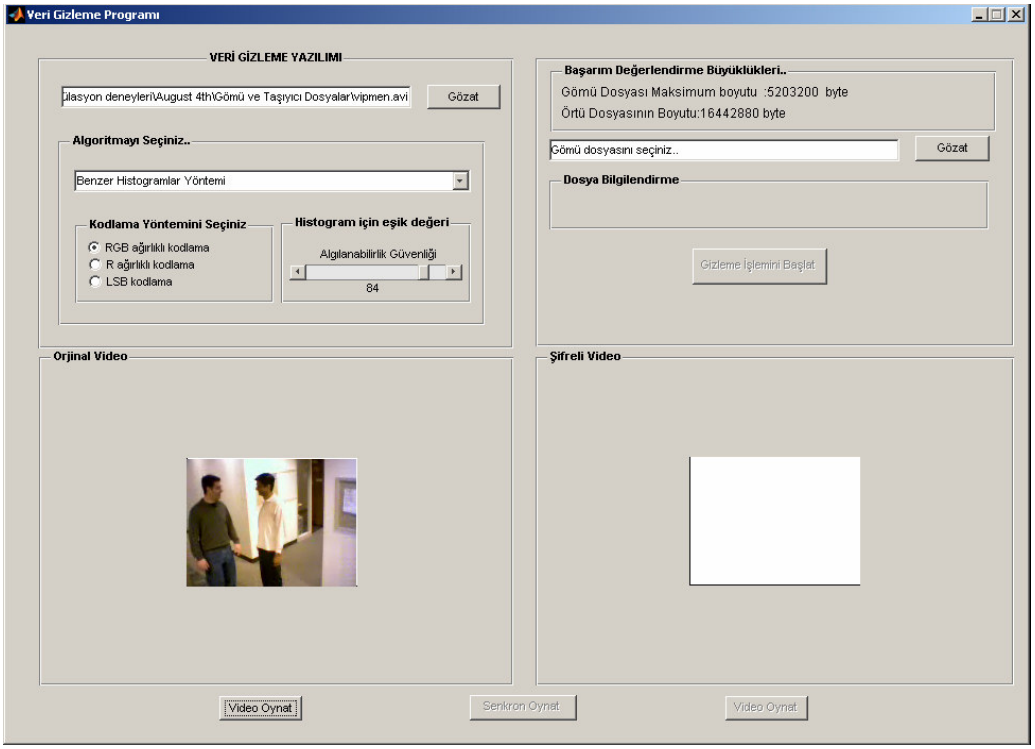
(a)



(b)

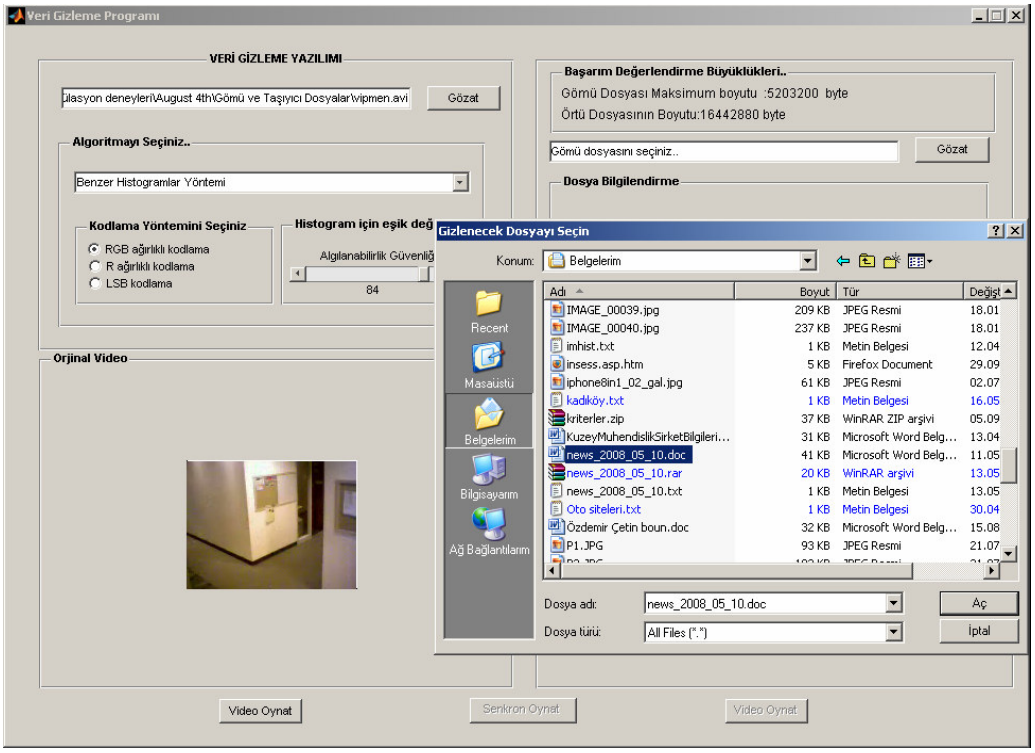
Şekil 4.22. (a) Histogram eşik değeri ‘0’ iken veri gizleme
(b) Histogram eşik değeri ‘84’ iken veri gizleme.

Bir sonraki adım ise kodlama yönteminin seçilmesidir. Şekil 4.23'de görülen pencerede 'Kodlama Yöntemini Seçiniz' bölümünden veri gizleme işleminde kullanılacak kodlama yöntemi seçilir. Bu bölümde görülen LSB kodlama; veri gizleme çalışmalarında ilk kullanılan yöntemdir. LSB kodlamanın uygulama yazılımına eklenmesindeki amaç; geliştirilen yöntemlerin literatürde kabul görmüş bir yöntemle karşılaştırılarak performans ölçme işleminin gerçeklenmesidir. İstenildiği takdirde veri gizleme işleminde kullanılan örtü videosu 'Orijinal Video' bölümünün alt kısmında bulunan 'Video Oynat' butonuna tıklanarak bu bölüm içerisinde izlenebilir (Şekil 4.23).



Şekil 4.23. Kodlama yönteminin seçilmesi ve seçilen örtü dosyasının (orijinal video) oynatılması.

Veri gizleme işlemine başlamadan önceki son adım, gömü dosyasının (gizli veri) seçilmesidir. Uygulama yazılımının sağ kısmında 'Başarım Değerlendirme Büyükleri' bölümünün hemen altında yer alan 'Gömü Dosyasını Seçiniz' bilgilendirme kutusunun yanındaki 'Gözat' butonuna tıklanarak Şekil 4.24'de görülen iletişim penceresi açılır.



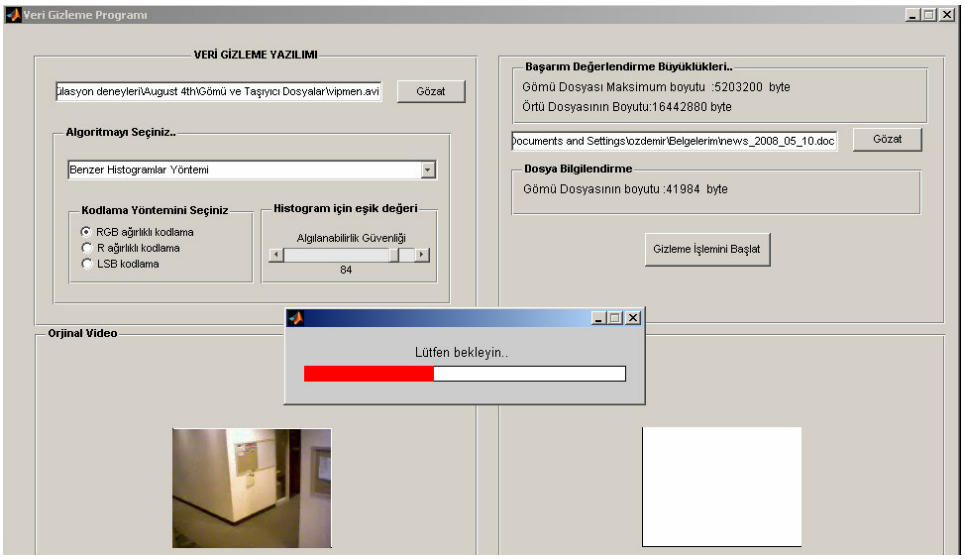
Şekil 4.24. Gömü dosyasının seçilmesi.

Gömü dosyası seçilirken 'Gömü Dosyası Maksimum Boyutu' bilgisi göz önünde tutulmalıdır. Daha büyük boyutta bir gömü dosyası seçilmesi hataya neden olacak ve veri gizleme işlemi başlatılmayacaktır.

Uygulama yazılımının '.rar' uzantısını desteklemesi güvenlik için de bir avantaj olarak kullanılabilir. Gizli veri herhangi bir sıkıştırma programı ile sıkıştırılırken şifreleme yapılarak güvenlik daha da artırılabilir.

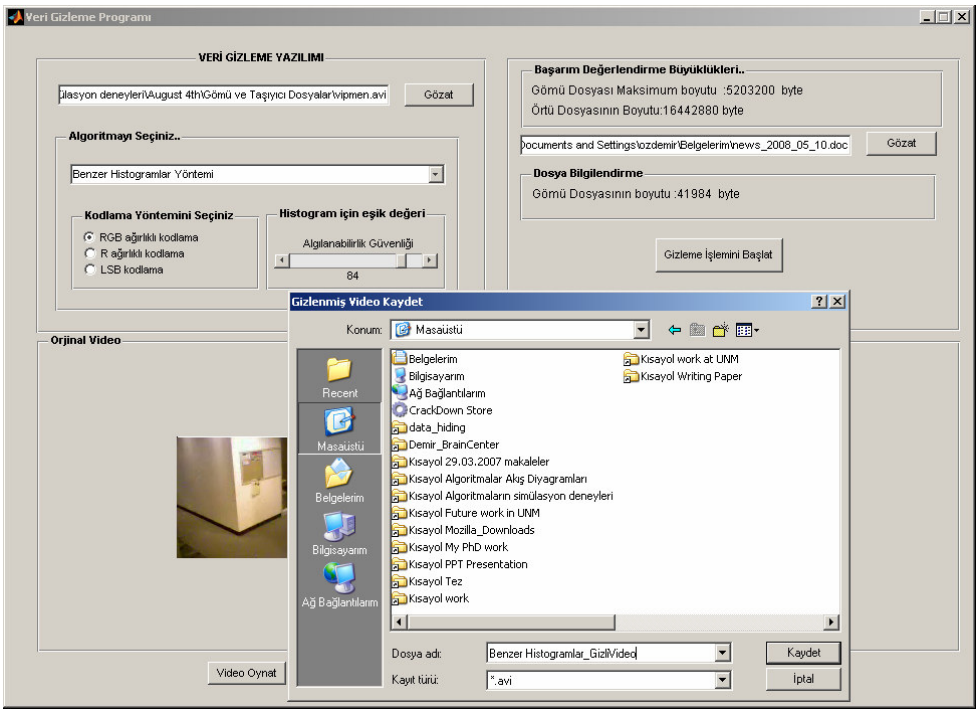
Gömü dosyası seçildikten sonra, seçilen gömü dosyasının boyut bilgisi 'Dosya Bilgilendirme' bölümünde gösterilecektir. Gizleme işlemini başlatmak için 'Gizleme İşlemini Başlat' butonuna basılır. Gömü dosyasının boyutuna göre gizleme işleminin

süresi değişebilir. Gizleme işlemi sürerken Şekil 4.25'deki gibi bir ekran görülecektir.



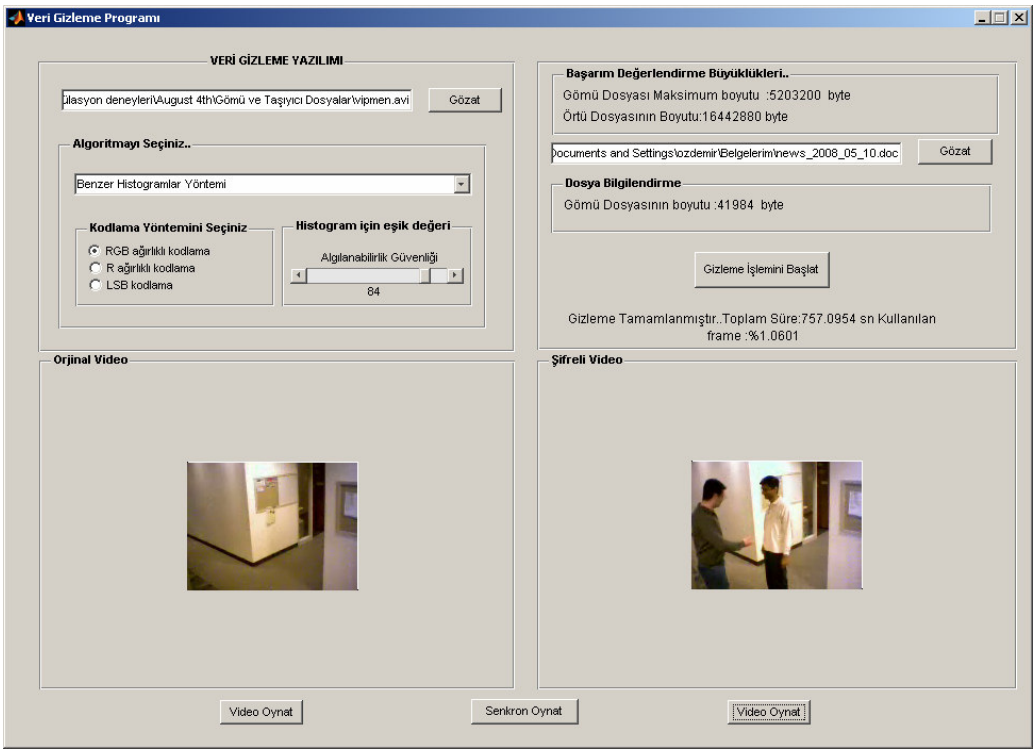
Şekil 4.25. Gizleme işlemi başlatıldıktan sonra görülen bekleme mesajı.

Gizleme işlemi bittiğinde elde edilen sırlı videonun (stego–video) nereye kaydedileceğini soran Şekil 4.26'daki gibi bir iletişim kutusu açılır.



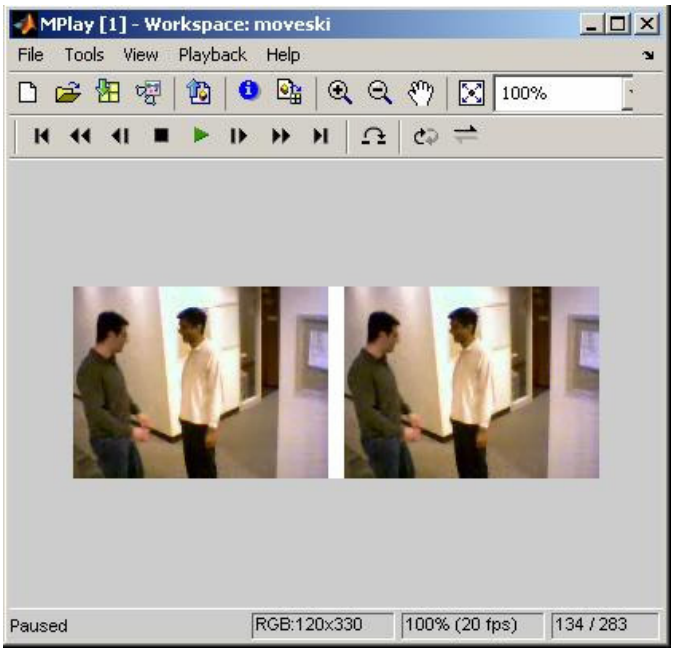
Şekil 4.26. Sırlı video'nun kaydedilmesi.

Arzu edilen bir isim verilerek sırlı video bilgisayarda istenilen bir yere kaydedilir. Kaydetme işleminde sırlı video'nun uzantısını girmeye gerek yoktur. Yazılım otomatik olarak video'yu '.avi' uzantılı olarak kaydedecektir. Gizleme işlemi tamamlandıktan sonra gizleme işlemini başlatan butonun altındaki bölümde gizleme işleminin ne kadar sürdüğü bilgisi ve örtü dosyasının kaçta kaçının kullanıldığı istatistikî bilgileri verilecektir (Şekil 4.27). Gizleme işleminin sona ermesiyle 'Şifreli Video' bölümünün alt kısmında bulunan 'Video Oynat' butonu aktif olur ve istenildiği takdirde elde edilen sırlı video bu bölümde oynatılır (Şekil 4.27).



Şekil 4.27. Sırlı videonun oynatılması ve elde edilen istatistikî bilgiler.

Ayrıca kullanıcının orijinal video ve sırlı videoyu yan yana izleyerek aradaki benzerlikleri veya farklılıkları karşılaştırmaya imkân verecek eşzamanlı izleme özelliği de uygulama yazılımına eklenmiştir. Videoları eşzamanlı olarak izlemek için 'Senkron Oynat' butonuna basıldığında videoların yan yana oynatıldığı bir pencere ekrana gelir (Şekil 4.28).



Şekil 4.28. Orijinal ve sırlı videoların eş zamanlı olarak oynatılması.

4.5.1.2. Dalgaboyu yöntemi ile veri gizleme uygulaması

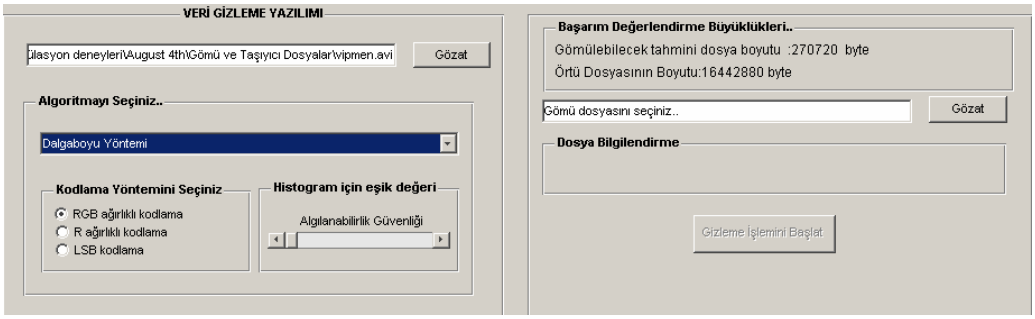
DB yönteminde veri gizleme işlemi için İGS'nin fark edemeyeceği dalgaboyu değerine sahip renkler kullanılmıştır. Bu sebepten dolayı video gizleme için seçilecek video dosyasının bahsedilen renklerden oluşturulmuş olması gizlenebilecek bilgi kapasitesine olumlu yansıyacaktır.

Uygulama yazılımı çalıştırıldığında Histogramlar yöntemi için anlatılan işlem basamakları tekrarlanacaktır. İlk adım olarak örtü dosyası (cover video) seçilir. 'Örtü Dosyasını Seçiniz' bilgilendirme kutusunun yanındaki 'Gözat' butonuna tıklandığı zaman ekrana gelen iletişim penceresinden istenen bir video dosyası seçilir (Şekil 4.20). Örtü dosyası seçildikten sonra 'Algoritmayı Seçiniz' bölümünde aktif hale

gelen aşağı açılır menüden istenen DB yöntemi seçilir (Şekil 4.21). Dalgaboyu kullanılan yöntemler aşağıda listelendiği gibidir;

- Dalgaboyu Yöntemi
- Benzer Histogramlar ve Dalgaboyu Yöntemi
- Farklı Histogramlar ve Dalgaboyu Yöntemi.

DB yöntemi seçildikten sonra gizleme işlemi için önemli olan; gömü dosyasının (gizli veri) en büyük boyutu ile örtü dosyasının (seçilen video dosyası) boyut bilgileri yazılım penceresinin sağ üst köşesindeki 'Başarım Değerlendirme Büyüklükleri' bölümünde gösterilir. Gizleme işlemi için sadece DB yöntemi seçildiyse 'Histogram İçin Eşik Değeri' bölümünden herhangi bir eşik değeri belirlemeye gerek yoktur. Veri gizleme işlemi histogram bilgisi gözetmeksizin gerçekleştirilecektir. Fakat yukarıda listelenen dalgaboyu kullanan yöntemlerden histogram bilgisi de kullanan bir yöntem seçildiğinde, kullanıcının istemesi durumunda eşik değeri belirlenebilir. Şunu unutmamak gerekir ki; eşik değerinin artırılması algılanabilirliği düşüreceği gibi gizlenebilecek bilgi kapasitesini de azaltacaktır. Bu sebepten ötürü; eşik değeri belirlenirken gereken güvelik ihtiyacı iyi belirlenmelidir.

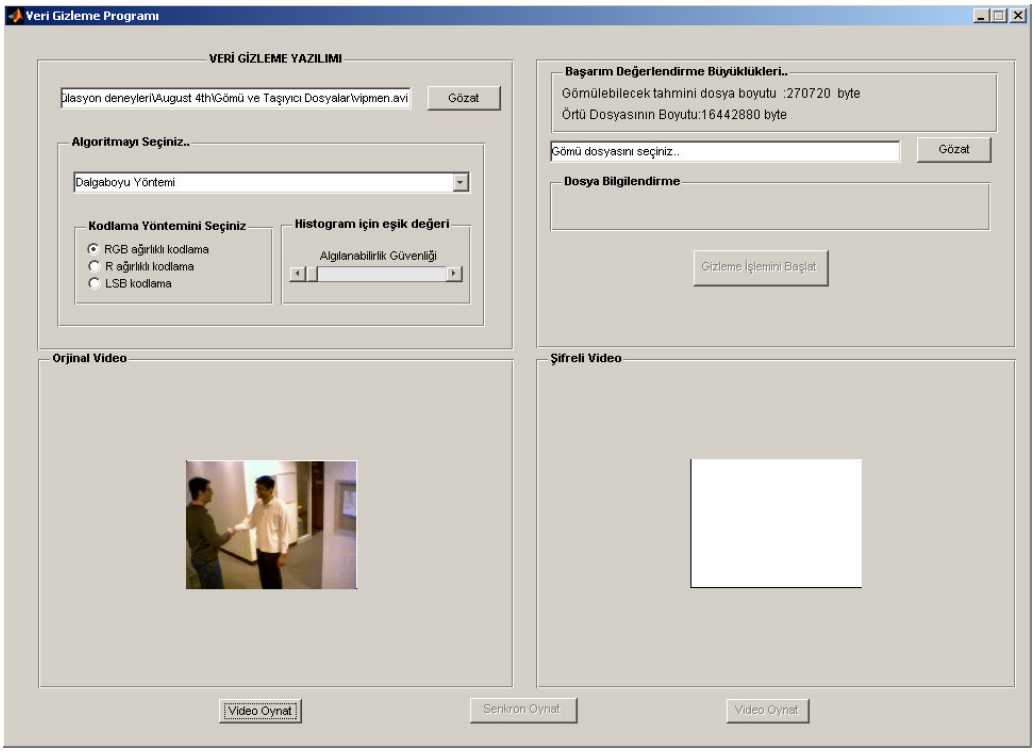


Şekil 4.29. Gizleme işleminde kullanılacak dalgaboyu yönteminin seçilmesi.

Veri gizleme işlemi için DB yöntemi seçildikten sonra uygulama yazılımının hesapladığı 'Gömülebilecek Tahmini Dosya Boyutu' ve 'Örtü Dosyasının Boyutu' Şekil 4.29'da görüldüğü gibidir. Bu değerler seçilen video dosyasına göre farklılık gösterecektir. Histogramlar yöntemi uygulaması için seçilen örnek video dosyası ('vipmen.avi') DB yöntemi için de seçildiğinde, uygulama yazılımı tarafından hesaplanan gömülecek dosyanın boyutunun anlamlı bir şekilde değiştiği görülecektir. Aynı örtü dosyası için histogramlar yönteminde gömü dosyasının en büyük boyutu

5,414,400 bayt iken DB yönteminde bu değer 270,720 bayt olarak hesaplanmıştır (Şekil 4.29).

Bir sonraki adım ise kodlama yönteminin seçilmesidir. Histogramlar yönteminde anlatıldığı gibi Şekil 4.30'da görülen pencerede 'Kodlama Yöntemini Seçiniz' bölümünden veri gizleme işleminde kullanılacak kodlama yöntemi seçilir. Ayrıca kullanıcı örtü videosunu 'Orijinal Video' bölümünün alt kısmında bulunan 'Video Oynat' butonuna tıklayarak bu bölüm içerisinde seyredebilir (Şekil 4.30).



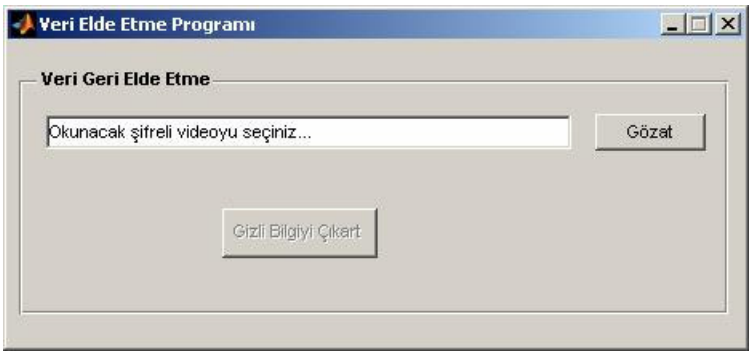
Şekil 4.30. Dalgaboyu yöntemi için seçilen örtü dosyasının (orijinal video) oynatılması.

Kodlama yöntemi seçildikten sonra gizli haberleşme için gerekli olan gömü dosyası (gizli veri) seçilir. Bu noktadan sonra gerçekleşen işlemler histogramlar yöntemi uygulamasında anlatıldığı gibi olacaktır.

4.5.2. Gizli verinin geri elde edilmesi

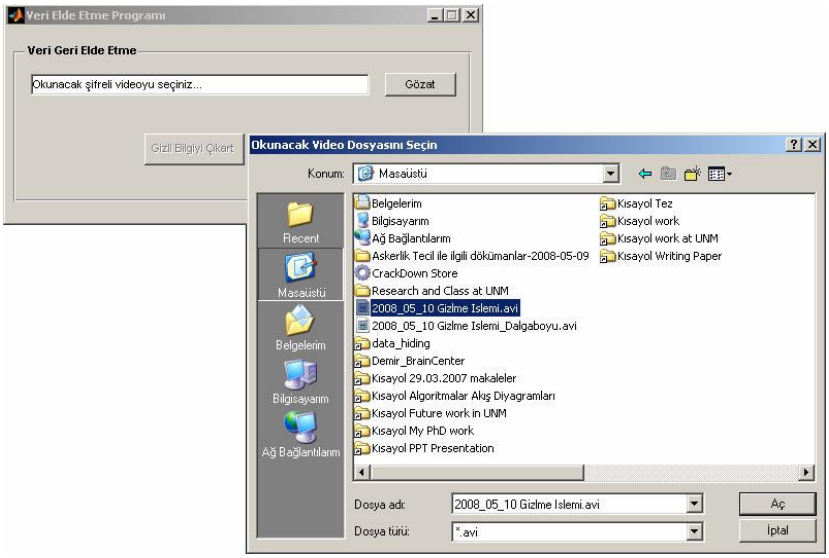
Bir önceki bölümde anlatılan veri gizleme yazlımı kullanılarak elde edilen sırlı videodan gizli veriyi geri elde etmek için basit bir yazılım kullanılmaktadır. Gizleme işlemi sırasında gizli veri dosya türü, boyutu, kodlama ve gizleme yöntemleri örtü videosunun ilk çerçevesine gömülür. Bu sayede veri gizleme işleminde kullanılan veri gizleme yönteminin bilinmesine gerek kalmaksızın gizli verinin geri elde edilmesi gerçekleştirilebilir.

Gizli verinin sırlı video'dan geri elde edilmesi işlemi için Şekil 4.31'de görülen uygulama yazılımı kullanılır. Görüldüğü gibi çok basit olan uygulama yazılımında gerekli olan tek şey içerisinde gizli veri bulunduran sırlı video dosyasıdır.



Şekil 4.31. Gizli veriyi geri elde etme uygulama yazılımı.

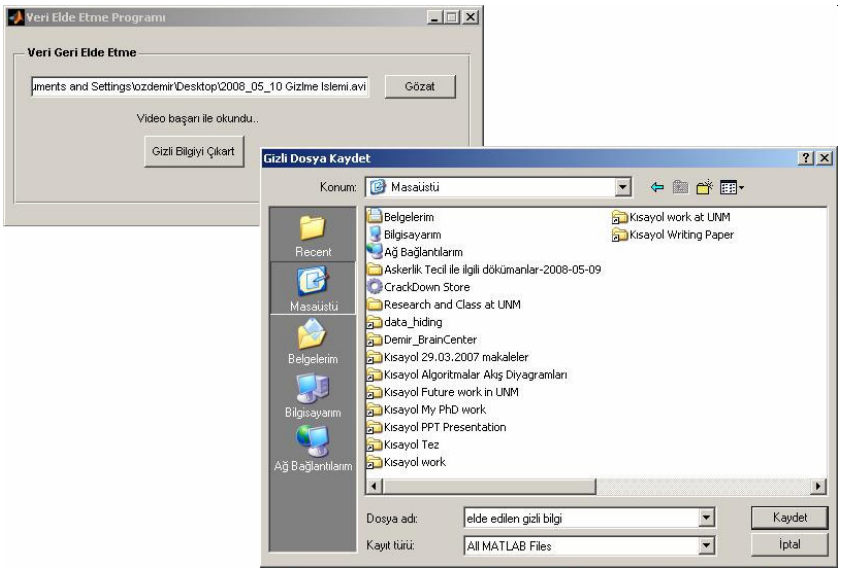
Uygulama yazılımı çalıştırıldığında Şekil 4.31'de görüldüğü gibi uygulama yazılımının ana penceresi ekrana gelecektir. Pencerede görülen 'Okunacak Şifreli Videoyu Seçiniz' bilgilendirme kutusunun yanındaki 'Gözat' butonuna tıklandığında ekranda Şekil 4.32'deki gibi bir iletişim penceresi görülür.



Şekil 4.32. Sırlı videonun seçilmesi.

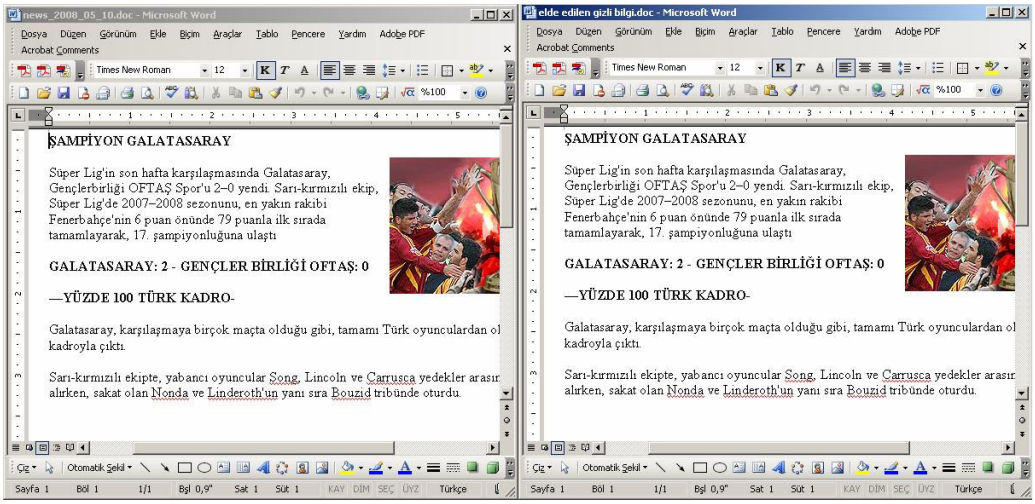
İletişim penceresi kullanılarak bilgisayarda kayıtlı sırlı video seçilir. Sırlı videonun seçilmesi ile aktif hale gelen 'Gizli veriyi Çıkart' butonuna tıklandığında gizli verinin geri elde edilmesi işlemi başlayacaktır.

Gizli verinin çıkarılması işlemi bittiğinde ekrana elde edilen gizli verinin bilgisayarda nereye kaydedileceğini soran bir iletişim penceresi gelir (Şekil 4.33). Bu pencerede elde edilen gizli veriye istenilen bir isim verilerek bilgisayarda istenilen bir yere kaydedilir.



Şekil 4.33. Geri elde edilen gizli verinin kaydedilmesi.

Şekil 4.34'de orijinal gizli veri ile elde edilen gizli veri gösterilmektedir. Şekilde sağ tarafta görülen geri elde edilen bilgi, sol tarafta görülen ise saklanan bilgidir.



Şekil 4.34. Orijinal gizli veri ve elde edilen gizli veri.

4.6. Sonuç

Bu bölümde tez çalışması süresince geliştirilen veri gömme tekniklerine ve veri gömme uygulama yazılımına ait detaylar verilmiştir.

Çalışmada geliştirilen veri gömme yöntemleri temel olarak farklı iki yaklaşım üzerine inşa edilmiştir. Bunlardan birincisi histogramlar yaklaşımı, diğeri görülebilir ışığın dalgaboyu yaklaşımıdır.

Histogramlar yaklaşımı ile oluşturulmuş veri gömme yöntemleri, gizli haberleşmede gizli veri kapasitesinin, gizli verinin algılanabilirliğinden daha önemli olduğu durumlarda tercih edilebilir.

Dalgaboyu yaklaşımına sahip veri gömme yöntemleri ise, gizli verinin algılanabilirliğinin çok önemli olduğu durumlarda, kısaca yüksek haberleşme güvenliği istenen durumlarda tercih edilir.

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. Sıkıştırılmamış formattaki videolar için geliştirilen yöntemlerin deneysel çalışmalarında, literatürde sıklıkla tercih edilen 'Vipmen' videosu kullanılmıştır. Vipmen videosunun çerçeve sayısı 283, çerçeve boyutları ise 160x120'dir.

Deneysel sonuçların değerlendirilmesi aşamasında, sırlı videoların istatistiksel 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 gelmektedir. Aslında PSNR değeri, İGS ile birebir uyuşan bir sonuç vermemektedir. Çünkü insanların renkleri ve tonları algılama davranışı tamamen birbirinden farklıdır. Bu durum göz önüne alınarak bir başka görsel kalite değerlendirme kıstası olan görsel ölçüm yöntemi de geliştirilen tekniklerin başarım değerlendirilmesinde kullanılmıştır.

İki görüntü arasındaki PSNR değerini hesaplamak için öncelikle Ortalama Kare Hatası (Mean Squared Error–MSE) değeri hesaplanmalıdır [88]. MSE değerinin hesaplanması için Denklem 5.1 kullanılabilir. MSE değerinin hesaplanmasının ardından Denklem 5.2'ye göre PSNR hesaplanır [89,90].

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left\|I(i,j) - K(i,j)\right\|^2 \quad \text{veya}$$

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

Burada I ve K birbirleriyle kıyaslanan görüntülerdir. I orijinal görüntüyü K ise yeniden elde edilmiş görüntüyü ifade eder. Görüntü boyutları ise $m \times n$ dir.

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

Denklem 5.2'deki MAX görüntüye ait bir pikselin kaç bit ile ifade edildiğini gösterir. Örneğin bir pikseli ifade etmek için kullanılan bit sayısı 8 olduğunda MAX 255 olacaktır.

Renkli görüntüler için PSNR değerinin hesaplanmasında izlenebilecek iki farklı yol vardır:

1. Renkli görüntüde bir piksel Kırmızı, Yeşil ve Mavi renklerinin birleşmesinden meydana geldiği için MSE hesaplanırken, orijinal ve yeniden elde edilmiş görüntülere ait piksellerin farklarının kareleri, görüntü boyutunun üç katına bölünür [91].

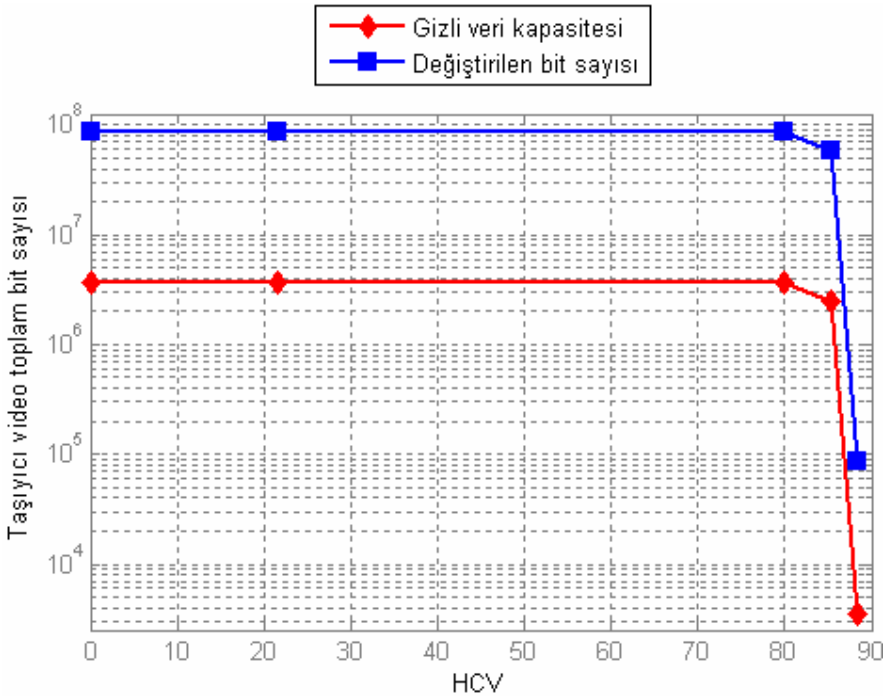
2. Matlab uygulamasına göre ise; renkli görüntünün renk modeli, renk yoğunluğunun ve renk bilgisinin ayrı ayrı ifade edildiği bir modele dönüştürülür. Bu renk modeline en iyi örnek YCbCr renk modeli verilebilir. Dönüşüm işleminden sonra yeni renk modelinin yoğunluk bilgisini içeren parçasının PSNR değeri hesaplanır.

Gizli verinin kapasitesine ve algılanabilirlik parametresine göre bozulan piksel sayılarının elde edilmesi ile istatistikî olarak görüntünün bozulma oranı hakkında bilgi sahibi olmaktayız.

Ayrıca önerilen yöntemler İGS'ne göre düşünüldüğü için, birkaç katılımcının yardımıyla algılanabilirlik başarımı görsel kalite ölçüm yöntemiyle de değerlendirilmiştir.

5.2. Kapasite, Algılanabilirlik ve Gizli Veri Gömme Süresi Başarımlarının Değerlendirilmesi

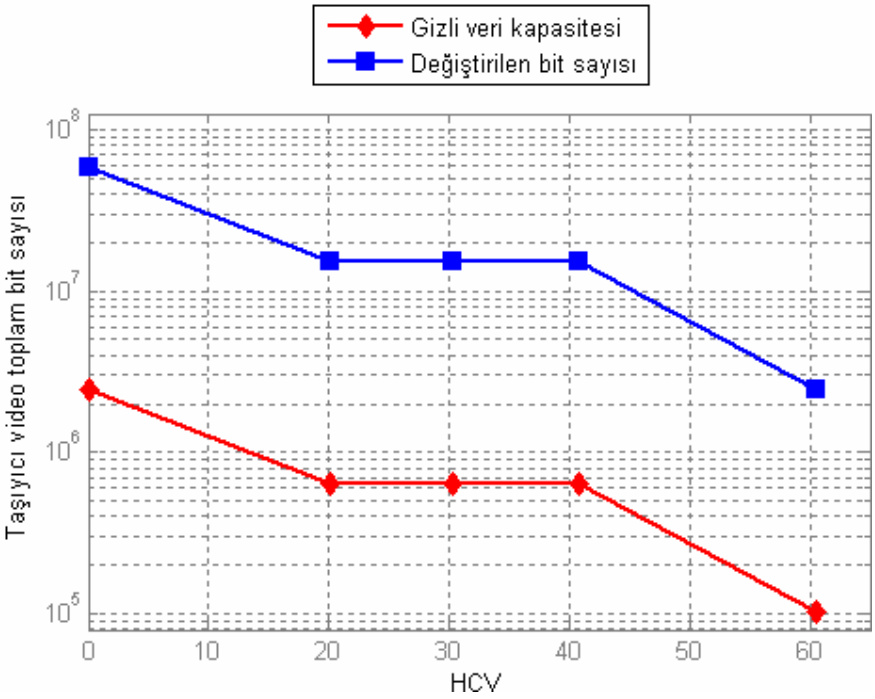
Deney çalışmaları sırasında kullanılan Vipmen örnek videosu için elde edilen deneysel sonuçlar aşağıdaki grafiklerde verilmiştir. Bu grafikler gizli veri kapasitesi, histogram sabiti (HCV) ve gizli veri gömme işleminde kullanılan bit sayısı kriterlerine göre elde edilmiştir.



Şekil 5.1. BH yönteminin HCV–Bit sayısı grafiği.

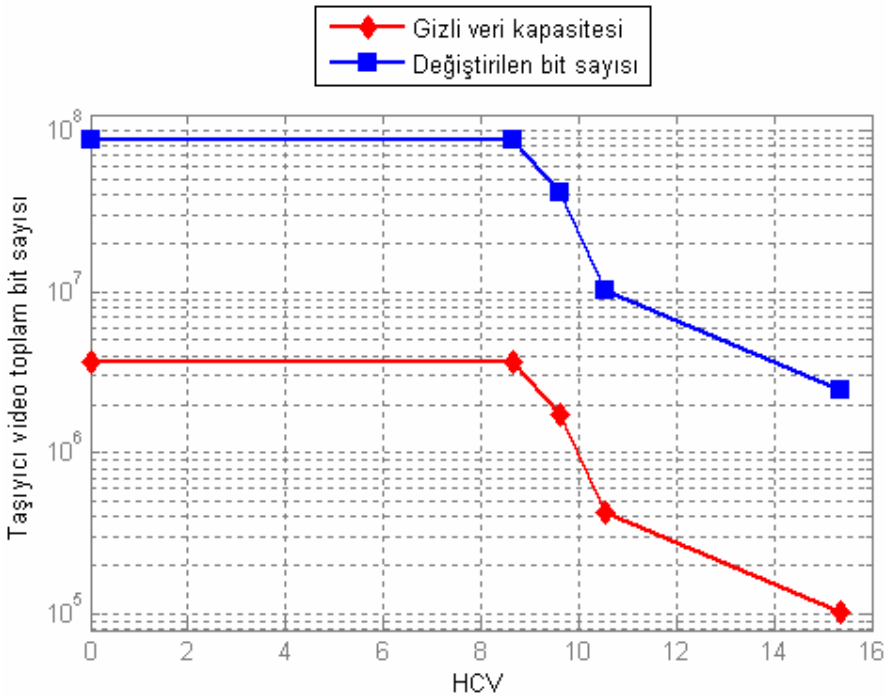
Şekil 5.1'de BH yöntemi için gizli verinin algılanabilirliğini etkileyen HCV değerine göre gizli veri kapasitesini ve taşıyıcı videoda kullanılan bit sayısını gösteren bir grafik verilmiştir. BH yöntemi seçildiğinde; HCV'nin 80 değerine kadar gizli veri gömme için seçilen çerçeveler büyük histogram farkına sahip olmayan çerçevelerdir. Bir başka deyişle, gizli veri gömülen çerçeveler arasında fark edilebilir ölçüde renk ve hareket geçişleri yoktur. Dolayısıyla da gizli veri gömülen çerçevelerdeki piksellerin renk yoğunlukları da birbirlerine yakındır. Bunun sonucu olarak da

yüksek gizli veri kapasitesi elde edilmektedir. HCV'nin 80 – 90 arasında değer aldığı durumda ise, İGS tarafından gizli verinin algılanabilirliğini azaltmak için daha düşük renk ve hareket geçişlerine sahip çerçeveler, kısaca renk yoğunlukları neredeyse aynı olan pikseller tercih edilir. Bunun sonucunda ise, veri gömmeye uygun çerçeve sayısı azalarak gizli veri kapasitesi ve gizli verinin algılanabilirliği oldukça düşmektedir. Sonuç olarak HCV'nin artması gizli veri kapasitesini ve dolayısıyla da algılanabilirliği düşürmektedir.



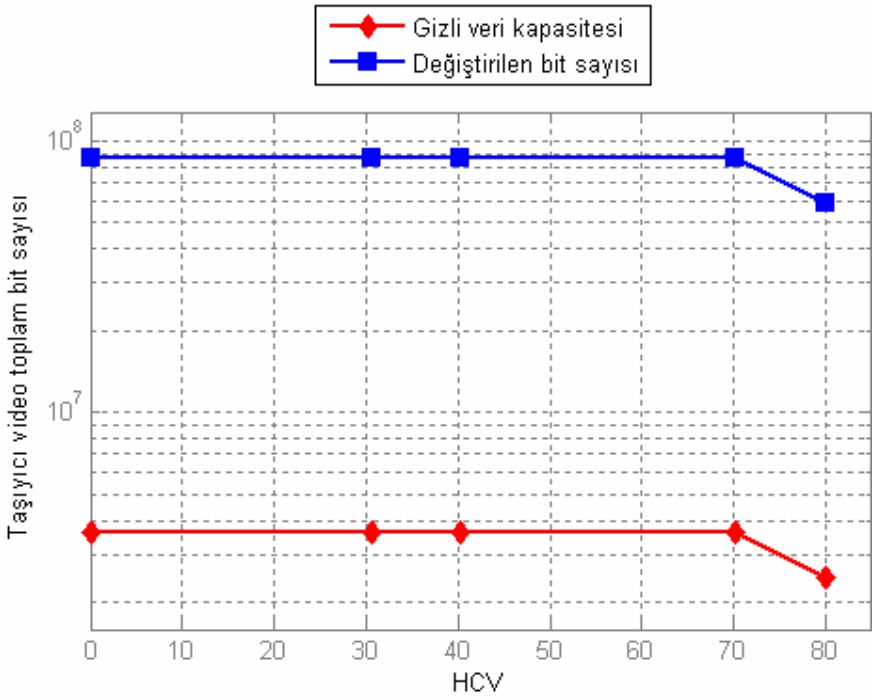
Şekil 5.2. BTBH yönteminin HCV–Bit sayısı grafiği.

Şekil 5.2'de BTBH yöntemi için HCV değerine göre gizli veri kapasitesini ve taşıyıcı videoda kullanılan bit sayısını gösteren grafik verilmiştir. Bu grafiğe göre, gizli veri kapasitesinin HCV'nin 0 – 20 değerleri arasında düştüğü görülmektedir. Bunun nedeni, video çerçevelerinin birbirlerinden oldukça farklı renk yoğunluklarına sahip piksellerden oluşmasıdır. Diğer bir ifadeyle video çerçeveleri yüksek renk geçişleri içeren hareketli sahnelere sahiptir. HCV'nin 20 – 40 arasındaki değerlerinde ise video çerçeveleri renk bakımından tekdüze ve hareketsiz sahnelerden oluşmaktadır. Buradaki önemli nokta, piksellerin renk yoğunluklarının birbirlerine daha yakın olmasıdır. Son olarak HCV'nin 40 – 60 değerleri için de, ilk durumdaki benzer ifadeler geçerlidir.



Şekil 5.3. FH yönteminin HCV–Bit sayısı grafiği.

Şekil 5.3'de FH yöntemi için HCV değerine göre gizli veri kapasitesini ve taşıyıcı videoda kullanılan bit sayısını gösteren grafik verilmiştir. FH yönteminde ise; HCV'nin yaklaşık 8 değerine kadar gizli veri gömme için seçilen video çerçeveleri birbirleri arasında büyük histogram farkı olan çerçevelerdir. Daha açık bir ifadeyle, renk ve hareketlilik bakımından birbirlerinden çok farklı olan çerçevelere gizli veri gömülmektedir. HCV'nin 8 değerinden sonra ise kapasitede büyük miktarda bir düşüşün olduğu gözlemlenmektedir. Bunun anlamı ise, İGS tarafından gizli verinin algılanabilirliğini azaltmak için veri gömülebilecek uygun çerçevelerin belirlenmesinde daha çok hassas davranıldığıdır. Bunun sonucunda, birbirleri arasında renk ve hareket geçişleri çok daha fazla olan çerçeveler veri gömülebilecek uygun çerçeveler olarak belirlenir. Dolayısıyla da veri gömülecek çerçevelerdeki piksellerin renk yoğunlukları da birbirlerinden çok farklı olacaktır. Sonuç olarak gizli veri kapasitesi ve gizli verinin algılanabilirliği oldukça düşmektedir.



Şekil 5.4. BTFH yönteminin HCV–Bit sayısı grafiği.

Şekil 5.4'de BTFH yöntemi için HCV değerine göre gizli veri kapasitesini ve taşıyıcı videoda kullanılan bit sayısını gösteren grafik verilmiştir. BTFH yöntemi veri gizleme için kullanıldığında; HCV'nin 0 – 70 arasındaki değerlerde, birbirleri arasında histogram farkı olan video çerçeveleri veri gömme için kullanılmaktadır. HCV'nin 70 – 80 arasında değer aldığı durumlarda ise, daha yüksek renk ve hareket geçişlerine sahip çerçeveler diğer bir anlatımla renk yoğunlukları birbirlerinden oldukça farklı olan pikseller veri gömme için tercih edilir. Bunun sonucunda ise, gizli veri kapasitesi ve gizli verinin algılanabilirliği oldukça düşmektedir.

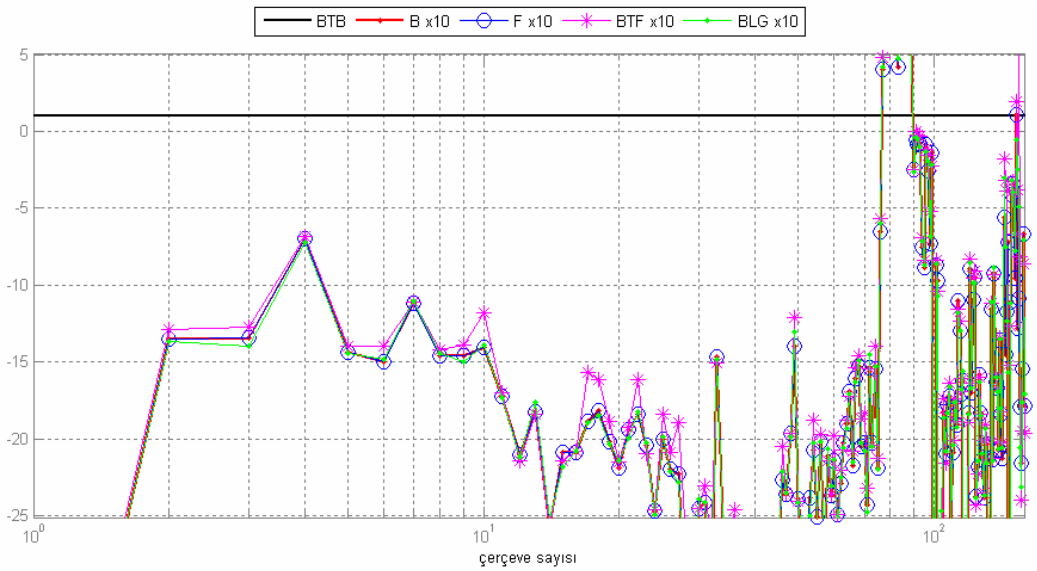
Bu sonuçlar ışığında, algılanabilirlik parametresi olan HCV'nin çok düşük olduğu durumda gizlenen bilgi kapasitesinin maksimum olduğu görülmektedir. Bununla birlikte, gizli veri kapasitesinin yüksek olması gizli veri gömme işlemi süresinin de yüksek olmasına neden olmaktadır.

HCV'nin maksimum olduğu durumda ise gizli veri kapasitesi minimum olmaktadır. Örneğin grafiklerde farklı HCV değerlerine göre gizli veri kapasitesinin nasıl değiştiği açıkça görülmektedir. Grafiklere bakıldığında en yüksek HCV, BH

yönteminde kullanılmıştır. Buna göre; 'Vipmen' örnek videosunda algılanabilirliğin en düşük olduğu gömme algoritmasının BH algoritması olduğu söylenebilir.

İstatistiksel değerlendirmelere göre ise 'Vipmen' uygulama videosu için elde edilen PSNR değerlerinin literatürdeki çalışmalarda elde edilen diğer değerler ile karşılaştırıldığında oldukça tatmin edici olduğu görülmektedir. Kayıplı resim/video sıkıştırma işlemlerinden sonra elde edilen görüntüler için kabul gören PSNR değerleri 30db ile 50db arasındadır [89, 90, 91]. Başka bir ifadeyle, PSNR değeri büyüdükçe sırlı videonun görüntü kalitesi de artacaktır.

Şekil 5.5 ile 5.8 arasında, HCV'nin ve gizli bilgi kapasitesinin en yüksek ve en düşük olduğu durumlarda elde edilen PSNR sonuçlarını gösteren grafikler verilmiştir. Algılanabilirliğin ve gizli bilgi kapasitesinin sınırlarını göstermek için en yüksek ve en düşük değerlerden elde edilen grafikler yorumlanmıştır.

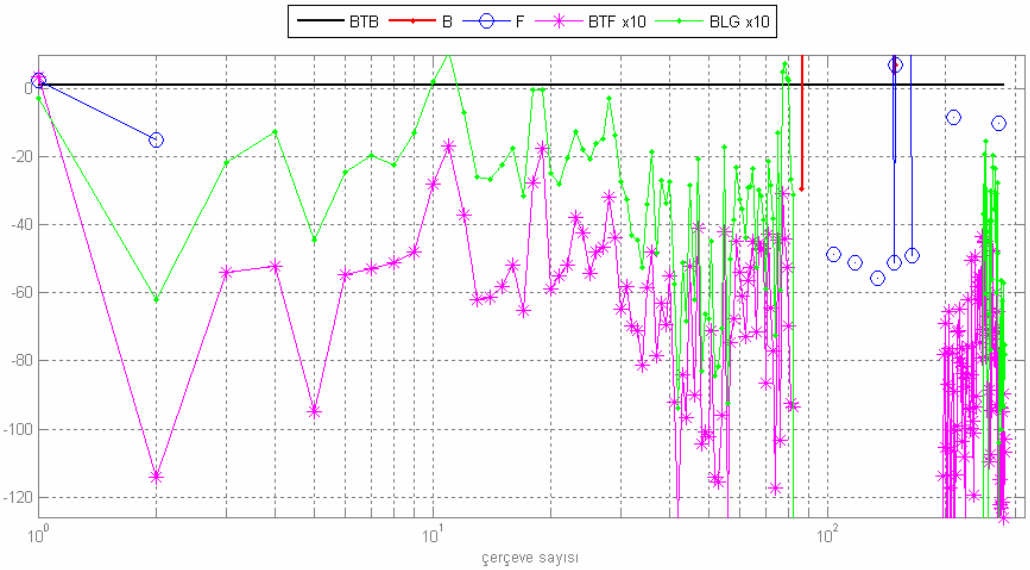


BTB: Blok Tabanlı Benzer Histogram
B: Benzer Histogram
F: Farklı Histogram
BTF: Blok Tabanlı Farklı Histogram
BLG: Bölgesel Histogram

Şekil 5.5. Geliştirilen yöntemlerin en düşük HCV durumundaki PSNR değerleri.

Şekil 5.5'de tez çalışmasında geliştirilen yöntemlerin, HCV'nin en düşük değere sahip olduğu durumdaki PSNR değerlerinin karşılaştırmasını gösteren bir grafik verilmiştir. Geliştirilen yöntemlerden BTBH yöntemi referans alınarak bir normalizasyon işlemi gerçekleştirilmiştir. Grafikte her bir yöntemin ilgili çerçevede veri gömme işlemini gerçekleştirdiğini belirtmek için noktalama işaretleri

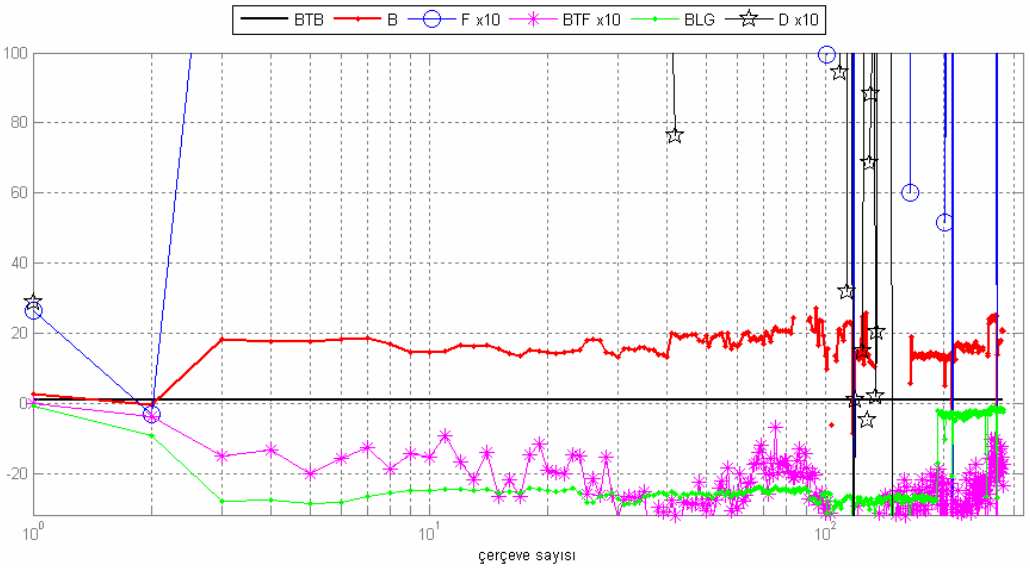
kullanılmıştır. Ayrıca PSNR değerlerinin daha anlaşılır bir şekilde görülebilmesi için her bir yöntemden elde edilen değerlerin 10 katı grafikte gösterilmiştir. Grafiğe göre, genel olarak BTBH yönteminin diğer yöntemlerden daha iyi sonuçlar verdiği görülmektedir.



BTB: Blok Tabanlı Benzer Histogram
B: Benzer Histogram
F: Farklı Histogram
BTF: Blok Tabanlı Farklı Histogram
BLG: Bölgesel Histogram

Şekil 5.6. Geliştirilen yöntemlerin en yüksek HCV durumundaki PSNR değerleri.

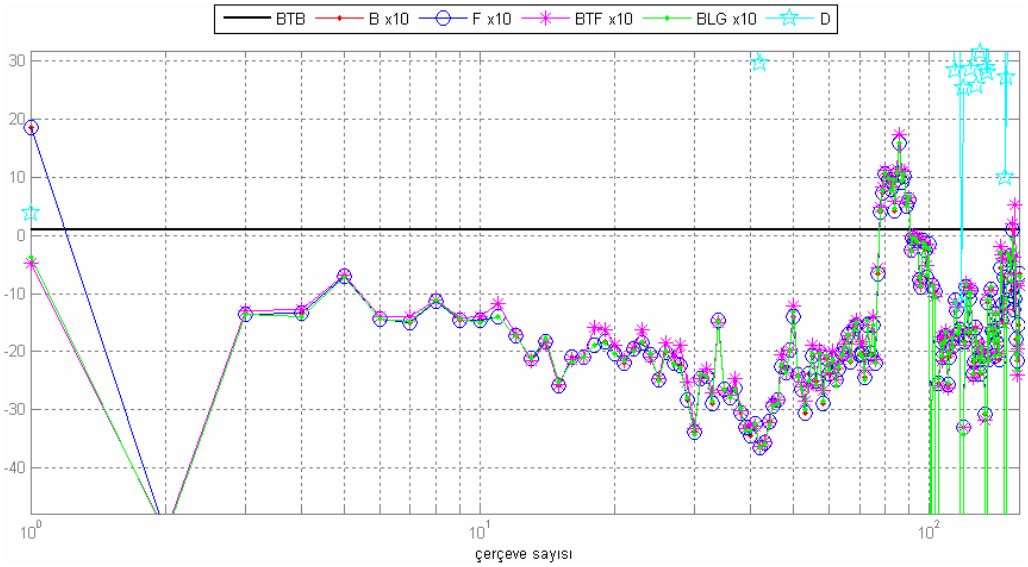
Şekil 5.6'da ise tez çalışmasında geliştirilen yöntemlerin, HCV'nin en yüksek değere sahip olduğu durumdaki PSNR değerlerinin karşılaştırmasını gösteren bir grafik verilmiştir. PSNR değerlerinin daha anlaşılır bir şekilde görülebilmesi için BTFH ve BLG yöntemlerinin değerleri 10 kat büyük olarak grafikte gösterilmiştir. Grafiğe göre, BLG yöntemi HCV'nin en yüksek olduğu durumda yüksek PSNR değerlerine sahiptir. Bununla birlikte, BH ve FH yöntemlerinin veri gömme işlemi sırasında diğer yöntemlere göre daha az sayıda çerçeve kullandığı ve PSNR değerleri de kabul edilebilir sınırlar dahilinde olduğu için, HCV'nin yüksek olduğu durumda veri gizleme için tercih edilebilirler.



BTB: Blok Tabanlı Benzer Histogram
B: Benzer Histogram
F: Farklı Histogram
BTF: Blok Tabanlı Farklı Histogram
BLG: Bölgesel Histogram
D: Dalgaboyu

Şekil 5.7. Geliştirilen yöntemlerin en düşük gizli veri kapasitesine sahipken PSNR değerleri.

Şekil 5.7'de tez çalışmasında geliştirilen yöntemlerin, gizli veri kapasitesinin en düşük olduğu durumdaki PSNR değerlerinin karşılaştırmasını gösteren bir grafik verilmiştir. Burada da PSNR değerlerinin daha anlaşılır bir şekilde görülebilmesi için FH, BTFH ve DB yöntemlerinden elde edilen PSNR değerleri 10 kat büyük olarak grafikte gösterilmiştir. DB ve FH yöntemlerinde, veri gizleme sırasında kullanılan çerçeve sayılarının az olması algılanabilirliğin daha düşük olmasını sağlayacağından bu yöntemlerin yüksek haberleşme güvenliği açısından tercih edilmeleri daha uygun olacaktır. Bununla birlikte BH yöntemininde diğer yöntemlere göre daha başarılı sonuçlar verdiği de grafikten görülmektedir.



BTB: Blok Tabanlı Benzer Histogram
B: Benzer Histogram
F: Farklı Histogram
BTF: Blok Tabanlı Farklı Histogram
BLG: Bölgesel Histogram
D: Dalgaboyu

Şekil 5.8. Geliştirilen yöntemlerin en yüksek gizli veri kapasitesine sahipken PSNR değerleri.

Şekil 5.8'de ise tez çalışmasında geliştirilen yöntemlerin, gizli veri kapasitesinin en yüksek olduğu durumdaki PSNR değerlerinin karşılaştırmasını gösteren bir grafik verilmiştir. PSNR değerlerinin daha anlaşılır bir ifadeye sahip olmaları için BH, FH, BTFH ve BLG yöntemlerinden elde edilen değerler 10 kat büyütülmüş olarak grafikte gösterilmiştir. Grafikten de anlaşıldığı gibi bu durumda DB yöntemi hariç hemen hemen tüm yöntemler aynı sonucu vermektedir. Bu durumda DB yönteminin veri gizleme için en ideal yöntem olduğu aşikârdır.

5.3. Görsel Algılanabilirlik Başarım Değerlendirmesi

Geliştirilen yöntemlerin görsel algılanabilirliklerini ölçmek amacıyla, her bir yöntem kullanılarak gerçekleştirilen gizli veri gömme işlemi sonucunda elde edilen sırlı videolar bir gurup izleyiciye seyrettirildi. İzleyiciler orijinal ve sırlı videoları aynı anda seyrettikten sonra aralarında bir fark olup olmadığı soruldu. İlk gösterimden sonra videolar arasında herhangi bir fark algılayan izleyici olmadı. Aynı videoların ikinci ve üçüncü gösterimlerinden sonra, iki izleyici arada çok küçük bir fark algıladığını ama emin olmadıklarını söyledi. On izleyiciden ikisinin emin olmamakla beraber hataları algılayabildiklerini söylemeleri geliştirilen gizli veri gömme tekniklerinin başarılı olduğunu deneysel olarak göstermektedir.

5.4. Sonuç

Bu tez çalışmasında gizli haberleşmenin güvenliğini artırmak için gizli verinin algılanabilirliğinin en düşük seviyede tutulması amaçlanırken, gizli veri kapasitesinin de yüksek olması hedeflenmiştir.

Gerek deney sonuçlarından elde edilmiş PSNR sonuçlarına göre, gerekse de sırlı videoları izleyen katılımcılardan alınan tepkilere göre gizli verinin algılanabilirliğinin en düşük olduğu veri gizleme yönteminin dalgaboyu yöntemi olduğu görülmüştür.

Deney sonuçlarından elde edilen grafiklere bakıldığında ise, en fazla gizli veri kapasitesi sağlayan yöntemin BTFH yöntemi olduğu görülmektedir.

BÖLÜM 6. SONUÇLAR VE ÖNERİLER

6.1. Sonuçlar

Bu tez çalışmasında, önemli bilgilerin saldırganlardan korunarak haberleşmenin gerçekleştirilebilmesi için yeni sırörtme teknikleri geliştirilmiştir. Geliştirilen yöntemlerin katkılarını üç ana bölümde incelemek mümkündür;

1. Literatürde var olan İGS'ne göre geliştirilmiş yöntemlerden farklı olarak İGS tabanlı yeni bir yöntem geliştirilmiştir.

Sırörtme işleminde birinci ve en önemli gereksinim algılanamazlıktır. Resim, video gibi görsel içerikli taşıyıcı dosyalarda algılanabilirlik kıstası İGS'ye bağlıdır. Bu durumda geliştirilmesi gereken yeni yöntemin İGS özelliklerine, sınırlarına hassas olması gerekmektedir. Video dosyalarında İGS'nin duyarlı olduğu en önemli nokta, renk geçişleri ve video içerisindeki hareketliliktir. Bu düşünce ile taşıyıcı videoların histogram değerleri hesaplanarak renk geçiş noktaları, hareketliliğin bulunduğu çerçeveler belirlenmiştir. Sırörtme yöntemlerinin önde gelen en büyük problemlerinden biri olan kapasite sorununa geliştirilen bu yöntemle çözüm sunulmuştur. Histogram yönteminin kullanıldığı sırörtme işlemlerinde gizli veri kapasitesinin oldukça büyük olduğu görülmektedir. Örneğin 15 MB bir video dosyası içerisine 5 MB'a kadar bilgi gömmek mümkündür. Önerilen diğer yaklaşımda ise görülebilir alan dalgaboyu bilgisinin kullanılması temel alınmaktadır. Burada ana fikir; taşıyıcı video içerisindeki görülebilir ışığın sınırlarına yakın olan dalgaboyu değerlerine sahip piksellerin bulunarak bilgi gömmek için kullanılmasını sağlamaktır. Bilgi gizlemek için kullanılacak olan piksellerin dalgaboyu değerleri kızılötesi (750nm) veya morötesi (380nm) dalgaboyu değerlerine ne kadar yakın olursa, algılama işlemi de o kadar imkânsız olacaktır. Bu yaklaşım ile de, sırörtme

uygulamalarında çözüm bekleyen algılanabilirliğe bağlı güvenlik sorununun iyileştirilmesi amaçlanmıştır.

2. Gizli veri kapasitesini, literatürdeki LSB kodlama tekniğine göre önemli ölçüde artıran resim sırörtme için geliştirilmiş RGB ve R ağırlıklı kodlama teknikleri video sırörtmeye uygulanmıştır.

Daha önce resim dosyaları için kullanılan kodlama teknikleri bu çalışmada video dosyalarına uyarlanmıştır. Kodlama tekniğinin literatürdeki diğer yöntemlere göre karmaşık olmaması ve kolay uygulanabilirliğinin yanında kısa gömme süresi de tekniğin bir diğer avantajıdır. Kodlama tekniğinin önemli bir üstünlüğü olarak, gizli verinin taşıyıcı videoya gömülmesinden sonra video boyutunda bir değişikliğe neden olmaması söylenebilir. Bu durum tez çalışmasını literatürde bulunan birçok çalışmadan ayıran bir diğer önemli üstünlüktür.

3. Video içerisine gizli veri gömme, gizli veriyi geri elde etme uygulamalarının gerçekleştirildiği kullanıcı arayüzü (GUI) Matlab yazılım ortamında tasarlanmıştır.

Tez çalışması kullanıcı arayüzünün Matlab ortamında tasarlanması, sayısal görüntü işleme çalışmalarının hemen hemen hepsinde Matlab yazılımının kullanılmasından kaynaklanmaktadır. Gerçekleştirdiğimiz yöntemlerin var olan diğer yöntemler ile karşılaştırılmaları, zayıflıkları ve üstünlüklerinin ortaya konması gibi söz konusu durumlardan dolayı Matlab kullanıcı arayüz geliştirme ortamı seçilmiştir. Ayrıca, Matlab yazılımının sayısal görüntü işleme, sayısal sinyal işleme gibi konularda sağladığı alt yapı ve kod desteği, tez çalışması sırasında gerekli olan temel sayısal görüntü işleme kodlarını yazarak oyalanmayı engellemiştir.

6.2. Tartışma ve Öneriler

Bu tez çalışmasında Internet gibi güvenliğin son derece düşük olduğu ortamlarda güvenli haberleşme için İGS duyarlı yeni sırörtme yöntemleri geliştirilmiştir. Tez

çalışmasının katkıları ve eksiklikleri göze alınarak çalışmanın geliştirilmesi adına yapılabilecekler aşağıdaki gibi listelenebilir:

1. Bilgi gizlemek için uygun piksellerin seçilmesi aşamasında kullanılmak üzere tasarlanan histogram tabanlı sırörtme yönteminde, uygun piksellerin belirlenmesi için literatürde K-means clustering olarak bilinen sınıflandırma metodundan faydalanılabilir. Böylelikle renk değerlikleri birbirlerine en yakın olan pikseller kümesi elde edilerek veri gömme için uygun bir alan belirlenebilir.

2. Uygun piksellerin belirlenmesi aşamasında kullanılan bir diğer yol olan DB tabanlı sırörtme yönteminde ise, içerisine bilgi gizlenecek taşıyıcı video, görülebilir ışık tayfındaki İGS'nin duyarlı olduğu ışık dalgaboylarına sahip piksellerden oluşturulabilir. Böylece gizli veri kapasitesinin artırılması sağlanabilir. Ayrıca dalgaboyuna duyarlı tasarlanmış bir filtrenin taşıyıcı videoya uygulanması ile video içerisindeki bilgi gizlenebilecek pikseller belirlenebilir ve gömme algoritması bu duruma göre geliştirilebilir.

3. Tez çalışmasında amaç yüksek kapasiteli gizli veri haberleşmesi gerçekleştirmek olduğu için geliştirilen sırörtme yöntemleri ham video dosyaları için tasarlanmıştır. Bununla birlikte gerçeklenen kodlar üzerinde çok fazla değişikliğe gerek kalmadan aynı yöntemlerin sıkıştırılmış videolara uygulanması da mümkündür.

4. Gömme işlemi öncesinde gizli haberleşme bilgilerinin şifrelenmesi güvenliği artıracak bir adımdır. Günümüzde geliştirilmiş dosya sıkıştırma programları sıkıştırma sırasında bir şifre üreterek dosyayı koruma altına almaktadır. Bu sebep ile gerçeklenen tez çalışmasında ayrıca bir şifreleme tekniği üzerinde durma gereksinimi duyulmamıştır. Fakat bir şifreleme yönteminin çalışmaya entegre edilmesi zor olmayan bir uygulamadır ve kolaylıkla gerçeklenebilir.

5. Kullanıcı arayüzü Matlab yazılımından faydalanılarak geliştirilmiş olması yazılımın kullanılacağı bilgisayar üzerinde Matlab programının bulunması gerekliliğine neden olmaktadır. Bu çalışmada amaç akademik bir çalışma

yapmak olduğu için çalışma süresince bu durum göz önüne alınmamıştır. Bu bağımlılığın aşılması için geliştirilen yazılım, farklı programlama dilleri kullanılarak gerçekleştirilebilir.

6. Bu çalışma ile güvenli bilgi haberleşmesinde yeni bir yaklaşım gerçeklenmiştir. Ancak gerçekleştirilen yöntem ile ilgili tüm algoritmaların ve bilgilerin bu çalışma ile duyurulması sonucunda yapılan çalışmaya karşı bir saldırı yönteminin geliştirilmesi kolaylaşmıştır. Tez çalışması ile gerçekleştirilen yöntemler bir akademik çalışmanın amacıdır ve kodlar açıktır.

KAYNAKLAR

[1] KOZ, A., ALATAN, A., Oblivious video watermarking using temporal sensitivity of HVS, Proceedings of the 2005 International Conference on Image Processing (ICIP 2005), Genoa, Italy, 2005.

[2] SCHYNDEL, R., TIRKEL, A., OSBORNE, C., A digital watermark, Proceedings of the IEEE International Conference on Image Processing, 2:86–90, 1994.

[3] WOLFGANG, R.B., DELP, E.J., A watermark for digital images, Proceedings of the IEEE International Conference on Image Processing, Lausanne, Switzerland, 111:219–222, 1996.

[4] COX, I.J., KILIAN J., LEIGHTON, T., SHAMOON, T., Secure spread spectrum watermarking for images, audio and video, Proceedings of the IEEE International Conference on Image Processing, Lausanne, Switzerland, 111:243–246, 1996.

[5] PODILCHUK, C.I., ZENG, W., Digital image watermarking using visual models, Human Vision and Electronic imaging II, volume 3016, pp. 100–111. SPIE, 1997.

[6] SWANSON, M.D., ZHU, B., TEWFIK, A.H., Transparent robust image watermarking, Proceedings of the IEEE International Conference on Image Processing, Lausanne, Switzerland, 111:211–214, 1996.

[7] TUOMAS, A., Invisible Communication, HUT Seminar on Network Security, 1995.

[8] BARNI, M., BARTOLINI, F., CHECCACCI, N., Watermarking of MPEG-4 Video Objects, IEEE Transactions On Multimedia, vol. 7, no. 1, 2005.

[9] HARTUNG, F., GIROD, B., Digital watermarking of raw and compressed video, in Proc. SPIE 2952: Digital Compression Technologies and Systems for Video Communication, Berlin, Germany, pp. 205–213, 1996.

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

[11] SWANSON, M. D., ZHU, B., TEWFIK, A.T., Multiresolution scene-based video watermarking using perceptual models, IEEE J. Select. Areas Commun., vol. 16, pp. 540–550, 1998.

[12] SWANSON, M. D., ZHU, B., TEWFIK, A.T., Data Hiding for Video-in-Video, Proc.ICIP'97, Santa Barbara, CA, 2:676-679, 1997.

[13] HSU, C., WU, J., Digital watermarking for video, in Proc. IEEE Int. Conf. Digital Signal Processing, vol. 1, pp. 217–220, 1997.

[14] KALKER, T., DEPOVERE, G., HAITSMA, J., MAES, M., A video watermarking system for broadcast monitoring, Proc. SPIE, Security and Watermarking of Multimedia Contents, vol. 3657, pp. 103–112, 1999.

[15] DEGUILLAUME, F., CSURCA, G., O'RUANAIDH, J., PUN, T., Robust 3D DFT video watermarking, Proc. SPIE, Security and Watermarking of Multimedia Contents, vol. 3657, pp. 113–124, 1999.

[16] KUTTER, M., JORDAN, F., EBRAHIMI, T., Proposal of a watermarking technique for hiding/retrieving data in compressed and decompressed video, ISO/IEC Jtc1-Sc29-Wg11-Mpeg97, 1997.

[17] IKEDA, M., TAKEDA, K., ITAKURA, F., Audio data hiding by use of band-limited random sequences, Proc. ICASSP'99, pp. 2315-2318, 1999.

[18] BASSIA, P., PITAS, I., Robust audio watermarking in the time domain Proc. EUSIPCO'98, 9th European Signal Processing Conference, pp. 25-28, 1998.

[19] LEE, S., HO, Y., Digital audio watermarking in the cepstrum domain, IEEE Trans. Consumer Electronics, 46(3):334-335, 2000.

[20] ARNOLD, M., KANKA, S., MP3 robust audio watermarking, Proc. DFG VIIDII Watermarking Workshop'99, Erlangen, Germany, 1999.

[21] British Standard, BSI, London, Information technology, Generic coding of moving pictures and associated audio information, ISO/IEC 13818-3:1995.

[22] MIHÇAK, M.K., Watermarking Via Optimization Algorithms For Quantizing Randomized Image Characteristics, Microsoft Research, Cryptography and Anti-Piracy Group WA, USA.

[23] VBrick Systems, inc., Analog Vs. Digital Video, 2002.

[24] BUCHSBAUM, G., An Analytical Derivation of Visual Nonlinearity, IEEE Trans. On Biomedical Engineering, vol.27, pp.237-242, 1980.

[25] PRATT, W.K., Digital Image Processing, ISBN: 978-0-471-76777-0, John Wiley & Sons, Inc., Hoboken, New Jersey, 2007.

[26] www.scienceclarified.com/Ex-Ga/Eye.html
www.lowvisionsolutions.com/resources/vision-anatomy_eye.html.
http://www.sightsavers.org (Erişim Tarihi: Temmuz 2007).

[27] GONZALEZ, R., WOODS, R.E., Digital Image Processing, ISBN 0-201-18075-8 Prentice Hall Upper Saddle River, New Jersey, 2002.

[28] http:// science.hq.nasa.gov (Erişim Tarihi: Haziran 2007).

[29] http://academic.mu.edu/phys/matthysd/web226/L0221.htm
(Erişim Tarihi: May 2007).

[30] http://www.matbaa.org/renkler_hakkinda.asp (Erişim Tarihi:Mayıs 2007).

[31] http://www.blackice.com/colorspaceHSI.htm
(Erişim Tarihi: Temmuz 2007).

[32] http://en.wikipedia.org/wiki/Pixel (Erişim Tarihi: Temmuz 2007).

[33] Digital Imaging Tutorial, Cornell University Library/ Research Department.

[34] TEKALP, A. M., Digital Video Processing, Prentice Hall, 1995.

[35] MENEZES, A., OORSCHOT, P.V., VANSTONE, S., Handbook of Applied Cryptography, CRC Press, 1996.

[36] GOLDWASSER, S., BELLARE, M., Lecture Notes on Cryptography, Cambridge, Massachusetts, August 2001.

[37] CHANG, C., HWANG, M., CHEN, T., A new encription algorithm for image cryptosystems, The Journal of Systems and Software, 2000.

[38] KRENN, J.R., Steganography and Steganalysis,
http://www.krenn.nl/univ/cry/steg/ (Erişim Tarihi: Mart 2007).

[39] ANDERSON, R.J., FABIEN, A.P., On the Limits of Steganography, IEEE Journal on Selected Areas in Communications Vol.16, No.4, 1998.

[40] VENKATRAMAN, S., ABRAHAM, A., PAPRZYCKI, M., Significance of Steganography on Data Security, Proceedings of the International Conference on Information Technology, 2004.

[41] SINGH, S., Histoire des codes secrets, ISBN: 9782709620482, Editor Jean-Claude Lattès, 1999.

[42] KAHN, D., The Codebreakers: the story of secret writing, MacMillan publishing, 1996.

[43] http://e-handel.mm.com.pl/crypto/intro/introduction_to_cryptography.htm
(Erişim Tarihi: Ocak 2007).

[44] http://enigma.wikispaces.com/Enigma (Erişim Tarihi: Ocak 2007).

[45] DAEMEN, J., RIJMEN, V., AES Proposal: Rijndael, 1999.

[46] Federal Information Processing Standards Publication 197, Announcing the Advanced Encryption Standard (AES), 2001.

[47] Article of Anne Canteaut and Fran Lévy-dit-Véhel: http://www-rocq.inria.fr/canteaut/crypto_moderne.pdf (Erişim Tarihi: Ocak 2007).

[48] SCHNEIER, B., Applied Cryptography, John Wiley and Sons, 1996.

[49] VERHEUL, E., KOOPS, B., TILBORG, H.V., Public Key Infrastructure Binding Cryptography-A Fraud-Detectible Alternative To Key-Escrow Proposals Computer Law & Security Report Vol. 13 no. 1, Elsevier Science 1997.

[50] FISCHLIN, R., SCHNORR, C.P., Stronger Security Proofs for RSA and Rabin Bits, Journal of Cryptology 13: 221–244, 2000.

[51] SEROUSSI, G., Elliptic curve cryptography ITW 1999, Metsovo, Greece, 1999.

[52] XIE, R., WU, K., DU, J., LI, C., Survey of Public Key Digital Watermarking Systems, Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing 0-7695-2909-7/07/2007.

[53] VARADHARAJAN, V., NGUYEN, K.Q., MU, Y., On the design of efficient RSA-based on-line electronic cash Schemes Theoretical, Computer Science 226, 173-184, Elsevier, 1999.

[54] ALATTAR, A.M., LIN, E.T., CELIK, M.U., Digital Watermarking of Low Bit-Rate Advanced Simple Profile MPEG-4 Compressed Video, IEEE Transactions On Circuits And Systems For Video Technology, Vol. 13, No. 8, 2003.

[55] SEVGİ, L., 11 Eylül 2001-Değişen Dünya'da Elektronik Savaşlar, Bilgi Güvencesi ve Ulusal Savunma, İTÜV-SAM, Savunma Araştırmaları Merkezi, 2002.

[56] Academic Research Library, Behind the bits Catherine Auer Bulletin of the Atomic Scientists, 2001.

[57] MANGARAE, A., Stego FAQ, http://zone-h.org Zone-H, 2006.

[58] JOHNSON, N.F., JAJODIA, S., Exploring Steganography: Seeing the Unseen, IEEE Computer 1998.

[59] PETITCOLAS, F.A.P., ANDERSON, R.J., KUHN, M.G., Information Hiding–A Survey, Proceedings of the IEEE, Special Issue on Protection of Multimedia Content, 87(7):1062-1078, 1999.

[60] PROVOS, N., HONEYMAN, P., Hide and Seek: An Introduction to Steganography, IEEE Security & Privacy, 2003.

[61] SELLARS, D., An Introduction to Steganography, Student Papers, 1999. http://www.cs.uct.ac.za/courses/CS400/NIS04/papers99/dsellars/index.html

[62] BENDER, W., Gruhl, D., Morimoto, N., Lu, A., 1996. Techniques for data hiding. IBM Syst. J. 35 (3–4), 313–336.

[63] WANG, R.Z., LIN, C.F., LIN, J.C., Image hiding by optimal LSB substitution and genetic algorithm, Pattern Recognition 34, 671–683, 2001.

[64] NODA, H., FURUTA, T., NIIMI, M., KAWAGUCHI, E., Application of BPCS Steganography to wavelet compressed video, International Conf. On Image Processing ICIP, IEEE 0-7803-8554-3, 2004.

[65] SWANSON M.D., ZHU B., TEWFIK, A.H., Robust data hiding FCR images, Proceedings of the IEEE Digital Signal Processing Workshop, Loen, Nor-wag, pages 37-40, 1996.

[66] ANDERSON, R.J., Information Hiding: first international workshop, vol 1174 of Lecture Notes in Computer Science, Isaac Newton Institute, Springer Verlag Berlin Germany, ISBN 3-540-61996-8, 1996.

[67] PFITZMANN, B., Information Hiding Terminology, Information Hiding Workshop, LNCS,Springer-Verlag, Cambridge, UK, 1996.

[68] MARVEL, L., RETTER, C., A Methodology for Data Hiding Using Images, IEEE 0-7803-4902, 1998.

[69] WANG, H., WANG, S., Cyber Warfare: Steganography vs. Steganalysis, Communications Of The Acm, Vol. 47, No. 10, 2004.

[70] JOHNSON, N.F., JAJODIA, S., Steganalysis: the investigation of hidden information, IEEE Information Technology Conference, 113–116, 1998.

[71] JOHNSON, N.F., JAJODIA, S., Steganalysis of images created using current steganography software, in: Proceedings of the Information Hiding Workshop, Portland, Oregon, USA, April, 1998.

[72] COLE, E., Steganography, Information System Security Paper, George Mason University,

[73] WOLFGANG, R.B., DELP, E.J., A watermark for digital images, Proceedings of the IEEE International Conference on Image Processing, Lausanne, Switzerland, 111:219–222, 1996.

[74] VENKATRAMAN, S., ABRAHAM A., PAPRZYCKI, M., Significance of Steganography on Data Security, Proceedings of the International Conference on Information Technology, IEEE 2004.

[75] Video Compression Standards, A Verint Systems Technical Brief, January 2007.

[76] http://www.newmediarepublic.com/dvideo/compression/adv04.html (Erişim Tarihi: Temmuz 2007).

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

[78] COX, I.J., KILIAN, J., LEIGHTON, T., SHAMOON, T., Secure spread spectrum watermarking for images, audio, and video, Proceedings of the IEEE International Conference on Image Processing, pp. 243-256, 1997.

[79] http://www.netpano.com/newsdetail.asp?NewsID=206 (Erişim Tarihi: Mayıs 2006).

[80] TANAKA, K., NAKAMURA, Y., MATSUI, K., Embedding secret information into a dithered multilevel image, in Proc. IEEE Military Commun. Conf., pp. 216–220, 1990.

[81] BENDER, W., GRUHL, D., MORİMOTO, N., Techniques for data hiding, MIT Media Lab, Cambridge, MA, Tech. Rep., 1994.

[82] CARONNI, G., Assuring Ownership Rights for Digital Images, Proceedings of Reliable IT Systems, VIS-95, 1995.

[83] BRAUDAWAY, G.W., Protecting Publicly-Available Images with an Invisible Image Watermark, IEEE International Conference on Image Processing, vol 2, pp 1024-1025,1997.

[84] COX, I., KILIAN, J., LEIGHTON, F., SHAMOON, T., Secure Spread Spectrum Watermarking for Multimedia," IEEE Transactions on Image Processing, vol. 6, no. 12, pp. 1673-1687, Dec. 1997.

[85] XIA, X., BONCELET, C., ARCE, G., A Multiresolution Watermark for Digital Images, Proc. IEEE Int. Conf. on Image Processing, vol. I, pp. 548-551, 1997.

[86] KOPRINSKA, I., CARRATO, S., Temporal Video Segmentation: A Survey, Signal Processing Image Communication, Elsevier Science, 2001.

[87] AKAR, F., VAROL, H.S., A New RGB Weighted Encoding Technique for Efficient Information Hiding in Images, Journal of Naval Science and Engineering, Volume 2, 21–36, July 2004.

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

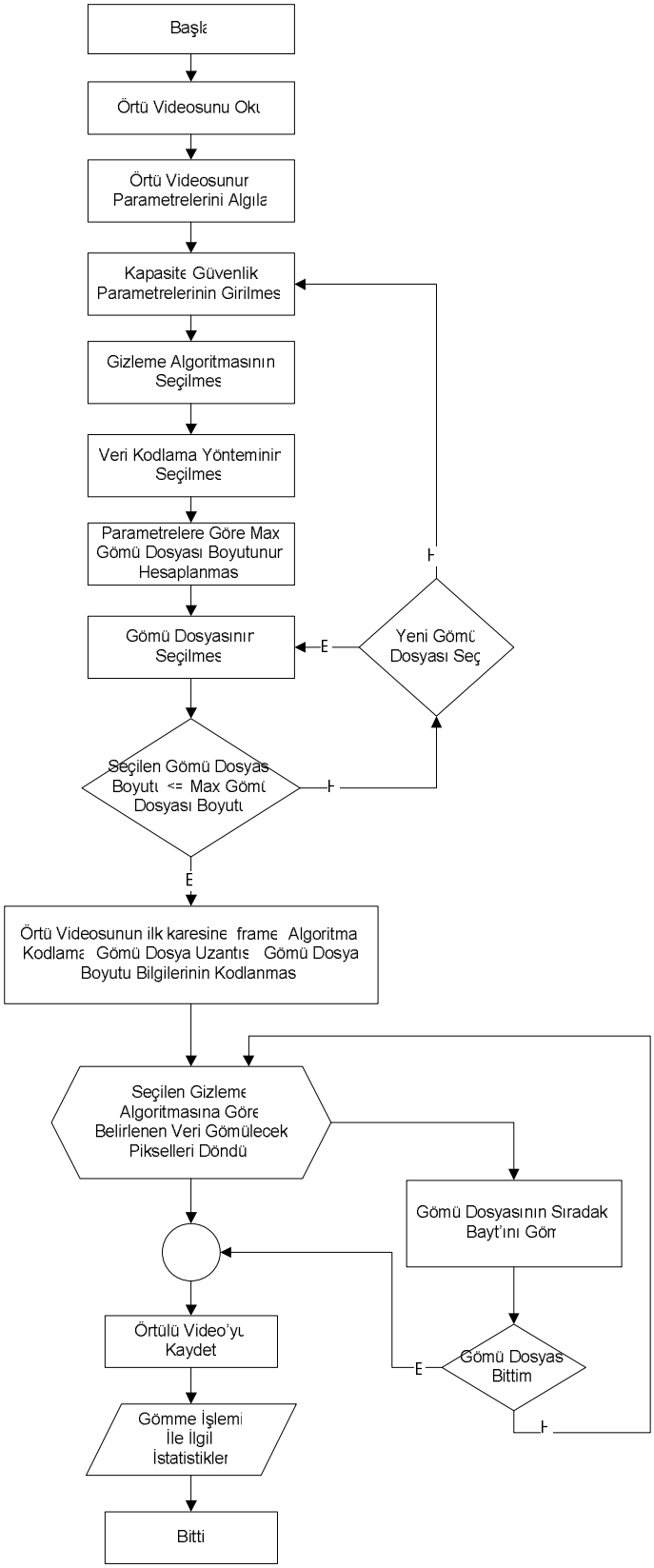
[89] NETRAVALI, A.N., HASKELL, B.G., Digital Pictures: Representation, Compression, and Standards (2nd Ed), Plenum Press, New York, NY 1995.

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

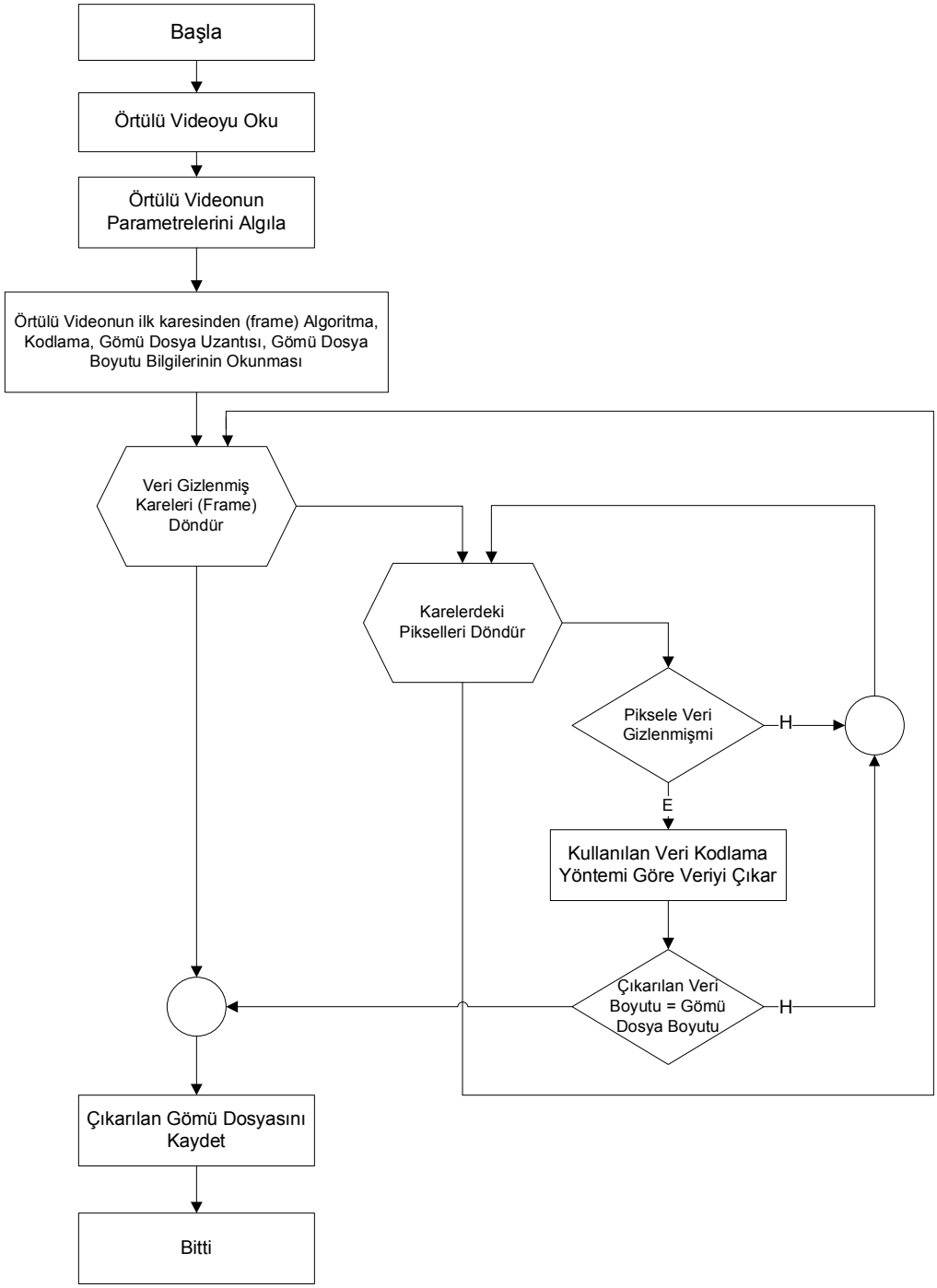
[91] http://en.wikipedia.org/wiki/Peak_signal-to-noise_ratio#searchInput#searchInput (Erişim Tarihi: Haziran 2008).

EKLER

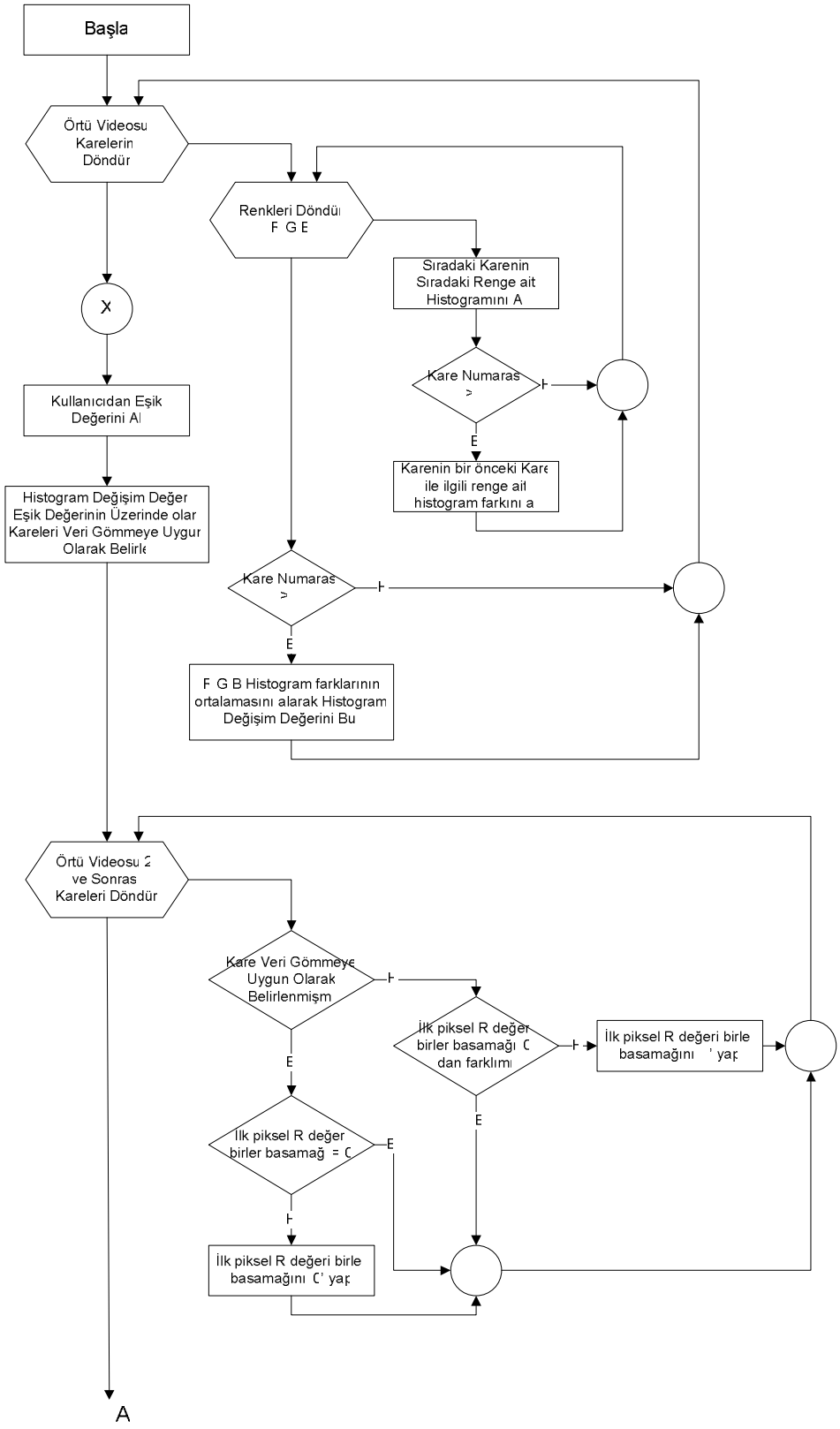
EK-A. Geliştirilen Algoritmaların Akış Diyagramları

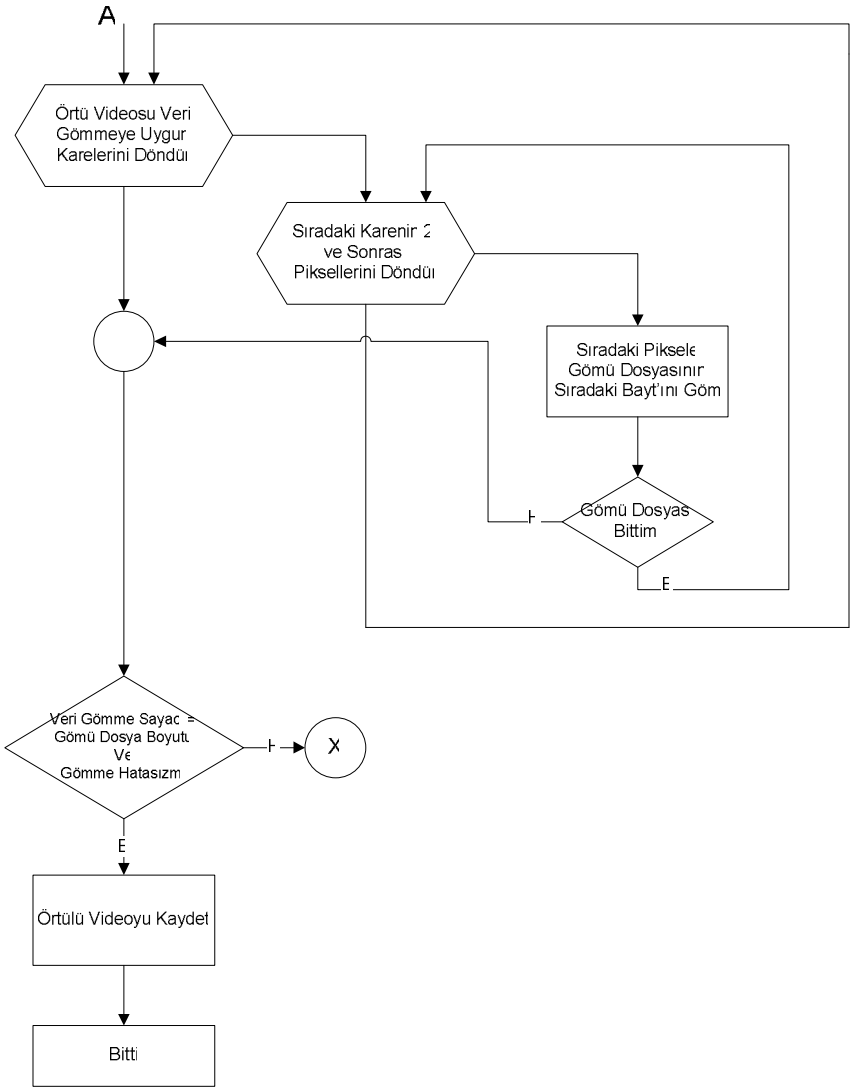


Şekil Ek.1. Genel Veri Gizleme Akış Diyagramı.

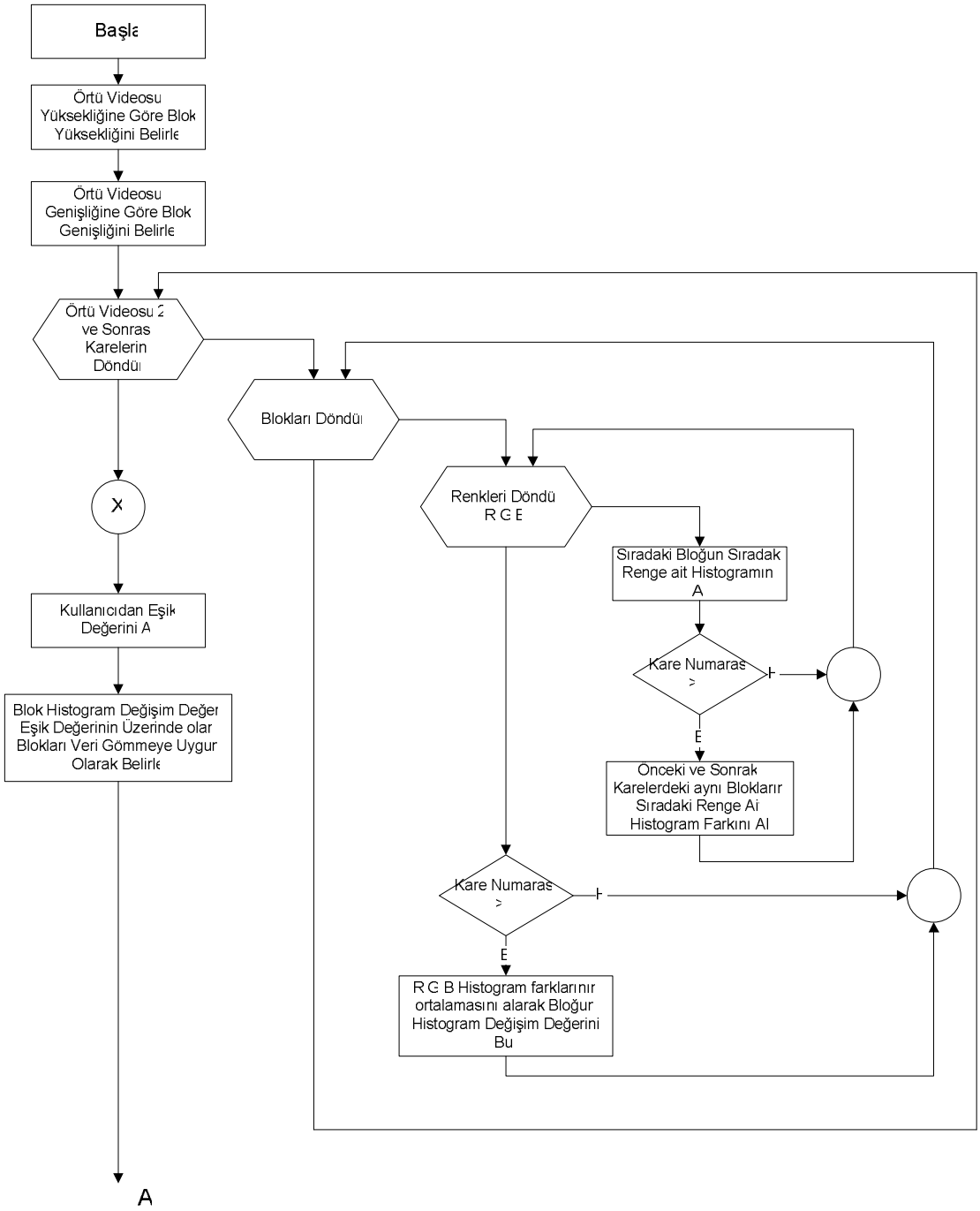


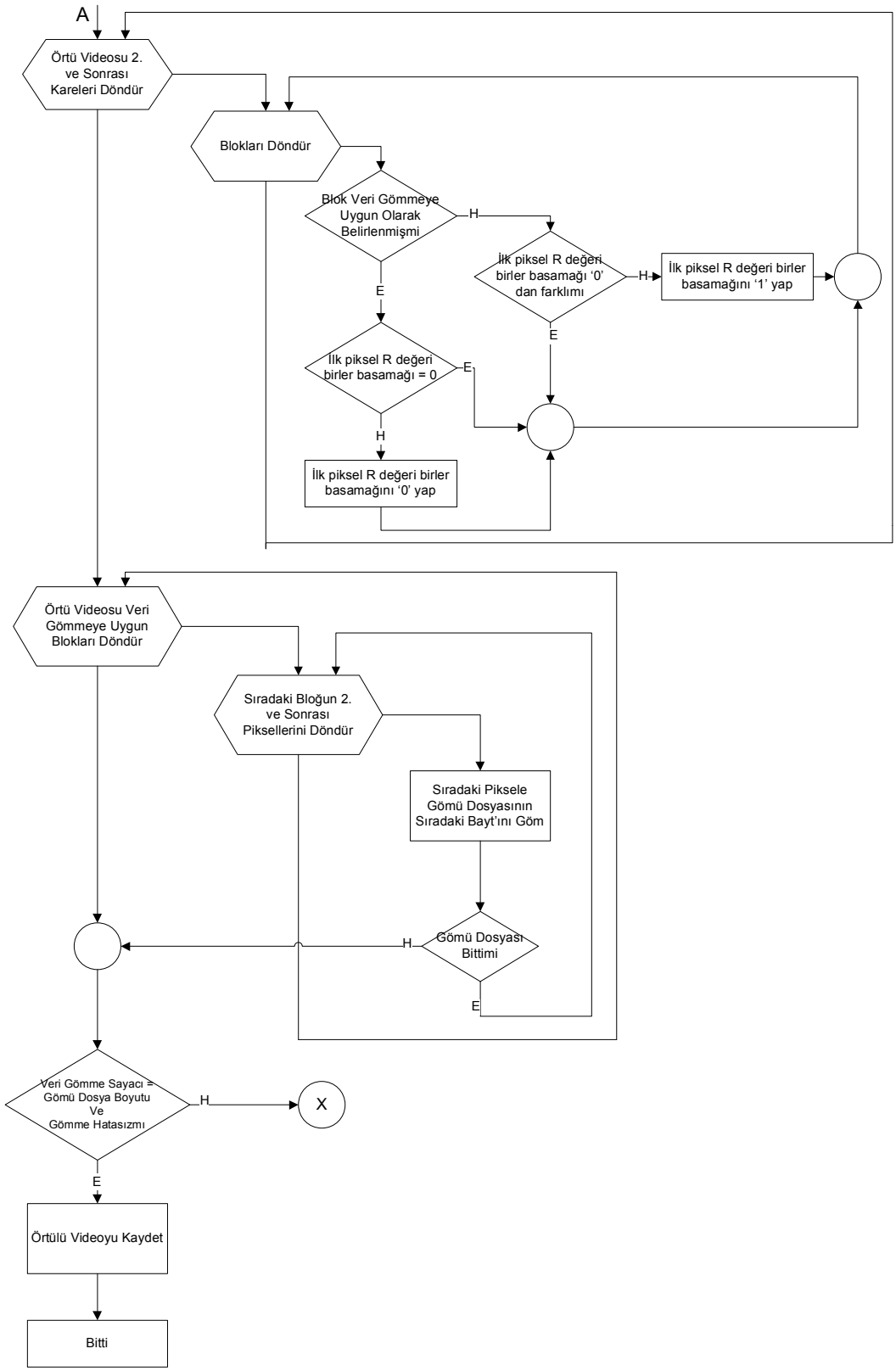
Şekil Ek.2. Genel Veri Geri Elde Etme Akış Diyagramı.


Başla
Örtü Videosu Karelerin Döndür
Renkleri Döndü F G E
Sıradaki Karenin Sıradaki Renge ait Histogramını A
X
Kare Numaras
H
E
Karenin bir önceki Kare ile ilgili renge ait histogram farkını a
Kullanıcıdan Eşik Değerini Al
Histogram Değişim Değer Eşik Değerinin Üzerinde olar Kareleri Veri Gömmeye Uygur Olarak Belirl
Kare Numaras
H
E
F G B Histogram farklarının ortalamasını alarak Histogram Değişim Değerini Bu
Örtü Videosu 2 ve Sonras Kareleri Döndür
Kare Veri Gömmeye Uygun Olarak Belirlenmişm
H
E
İlk piksel R değer birler basamağı C dan farklım
H
İlk piksel R değeri birle basamağını ' yaş
E
İlk piksel R değer birler basamağ = C
E
H
İlk piksel R değeri birle basamağını C' yaş
A

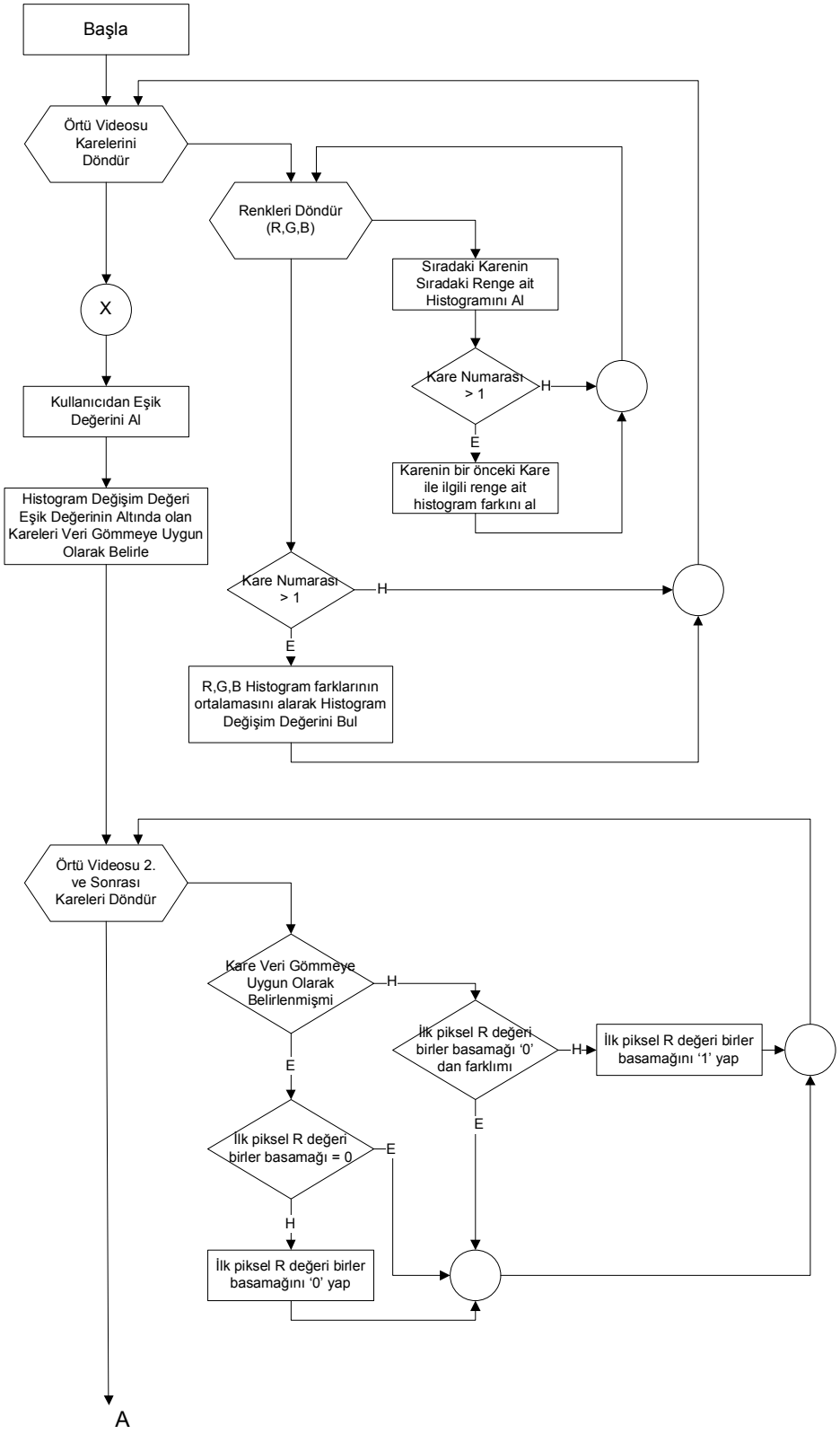


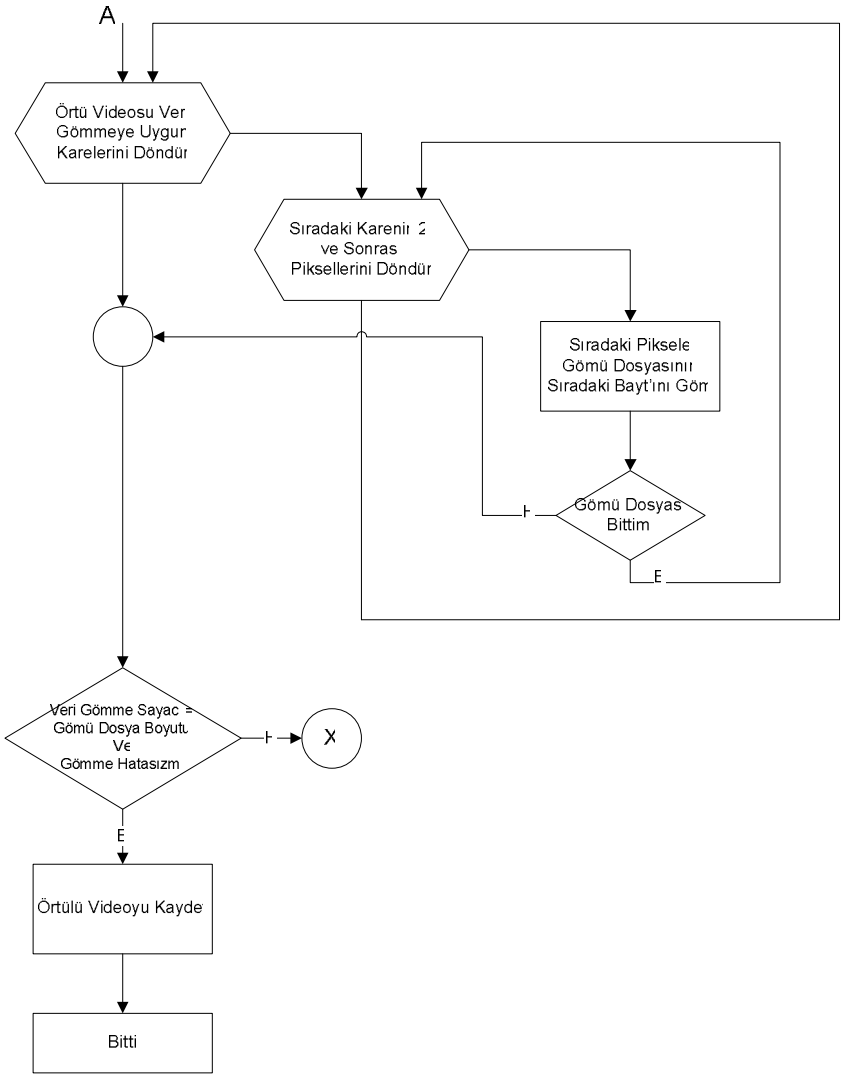
Şekil Ek.3. Farklı Histogramlar Yöntemi Akış Diyagramı.


Başla
Örtü Videosu
Yüksekliğine Göre Blok
Yüksekliğini Belirle
Örtü Videosu
Genişliğine Göre Blok
Genişliğini Belirle
Örtü Videosu 2
ve Sonras
Karelerin
Döndü
Blokları Döndü
X
Renkleri Döndü
R G E
Sıradaki Bloğun Sıradak
Renge ait Histogramın
A
Kare Numaras
>
H
E
Önceki ve Sonrak
Karelerdeki aynı Bloklarır
Sıradaki Renge Ai
Histogram Farkını Al
Kullanıcıdan Eşik
Değerini A
Blok Histogram Değişim Değer
Eşik Değerinin Üzerinde olar
Blokları Veri Gömmeye Uygur
Olarak Belirle
Kare Numaras
>
H
E
R G B Histogram farklarının
ortalamasını alarak Bloğur
Histogram Değişim Değerini
Bu
A

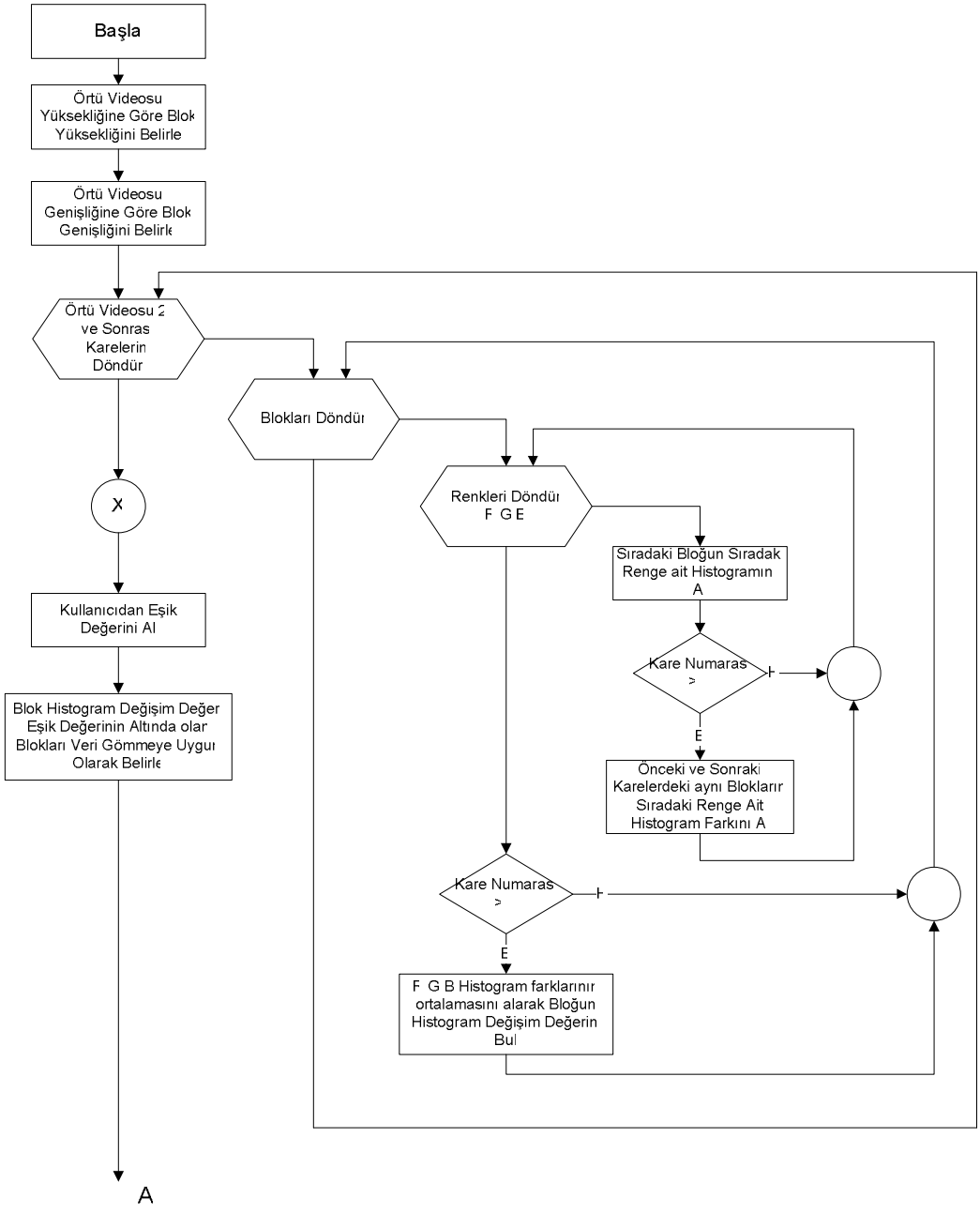


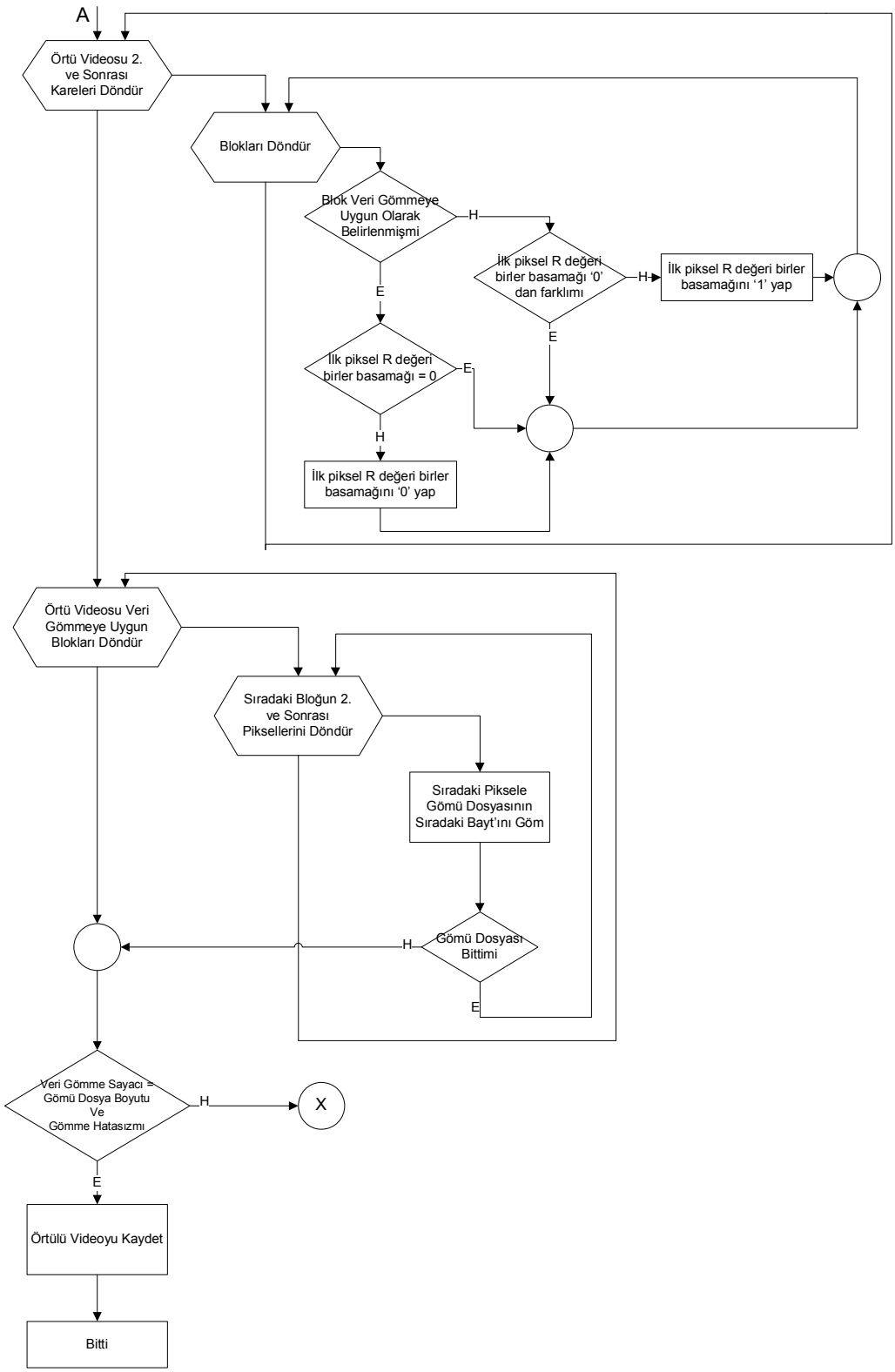
Şekil Ek.4. Blok Tabanlı Farklı Histogramlar Yöntemi Akış Diyagramı.


Başla
Örtü Videosu Karelerini Döndür
Renkleri Döndür (R,G,B)
Sıradaki Karenin Sıradaki Renge ait Histogramını Al
X
Kare Numarası > 1
H
E
Kullanıcıdan Eşik Değerini Al
Karenin bir önceki Kare ile ilgili renge ait histogram farkını al
Histogram Değişim Değeri Eşik Değerinin Altında olan Kareleri Veri Gömmeye Uygun Olarak Belirle
Kare Numarası > 1
H
E
R,G,B Histogram farklarının ortalamasını alarak Histogram Değişim Değerini Bul
Örtü Videosu 2. ve Sonrası Kareleri Döndür
Kare Veri Gömmeye Uygun Olarak Belirlenmişmi
H
İlk piksel R değeri birler basamağı '0' dan farklımı
H
İlk piksel R değeri birler basamağını '1' yap
E
E
İlk piksel R değeri birler basamağı = 0
E
H
İlk piksel R değeri birler basamağını '0' yap
A

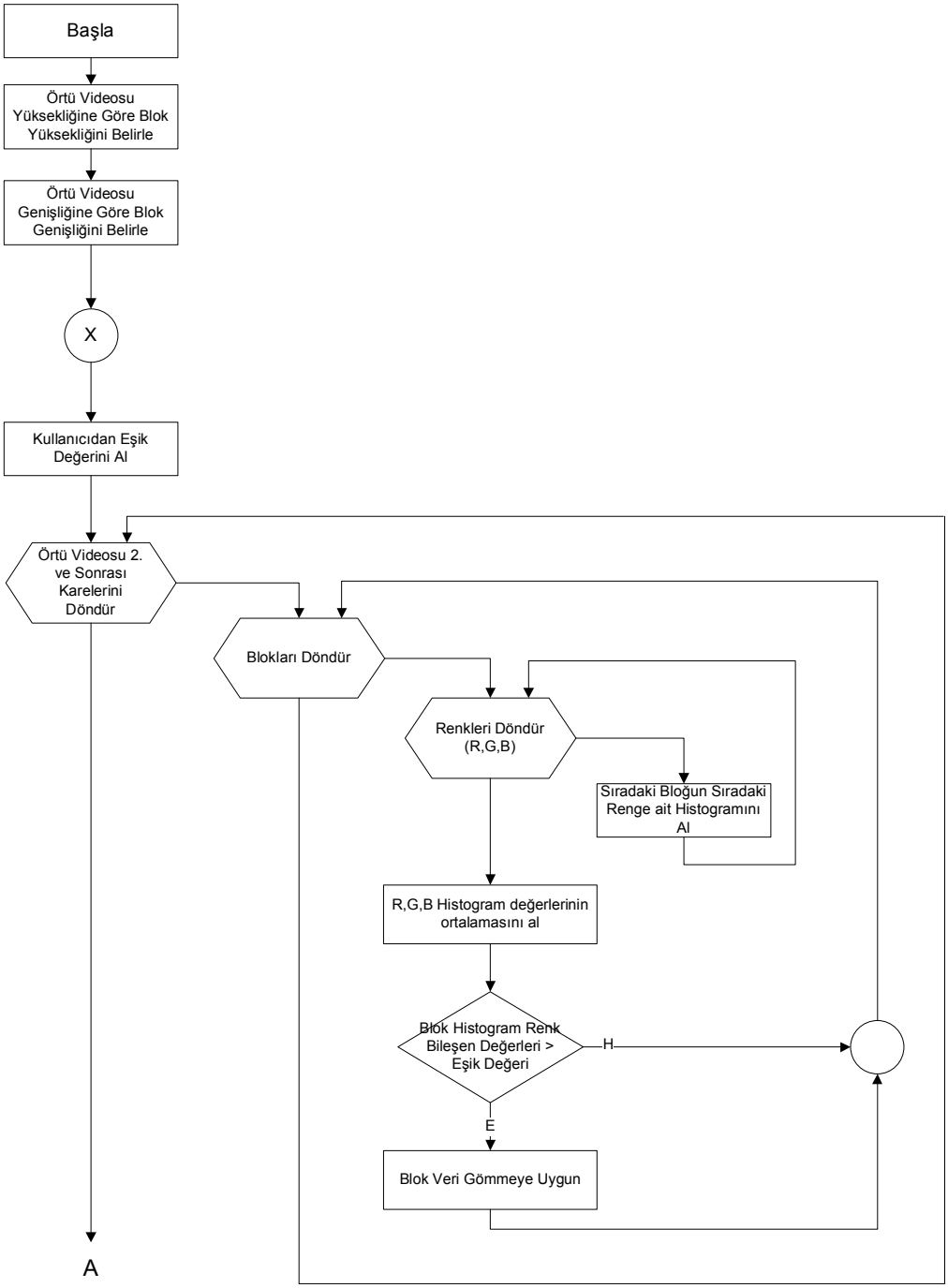


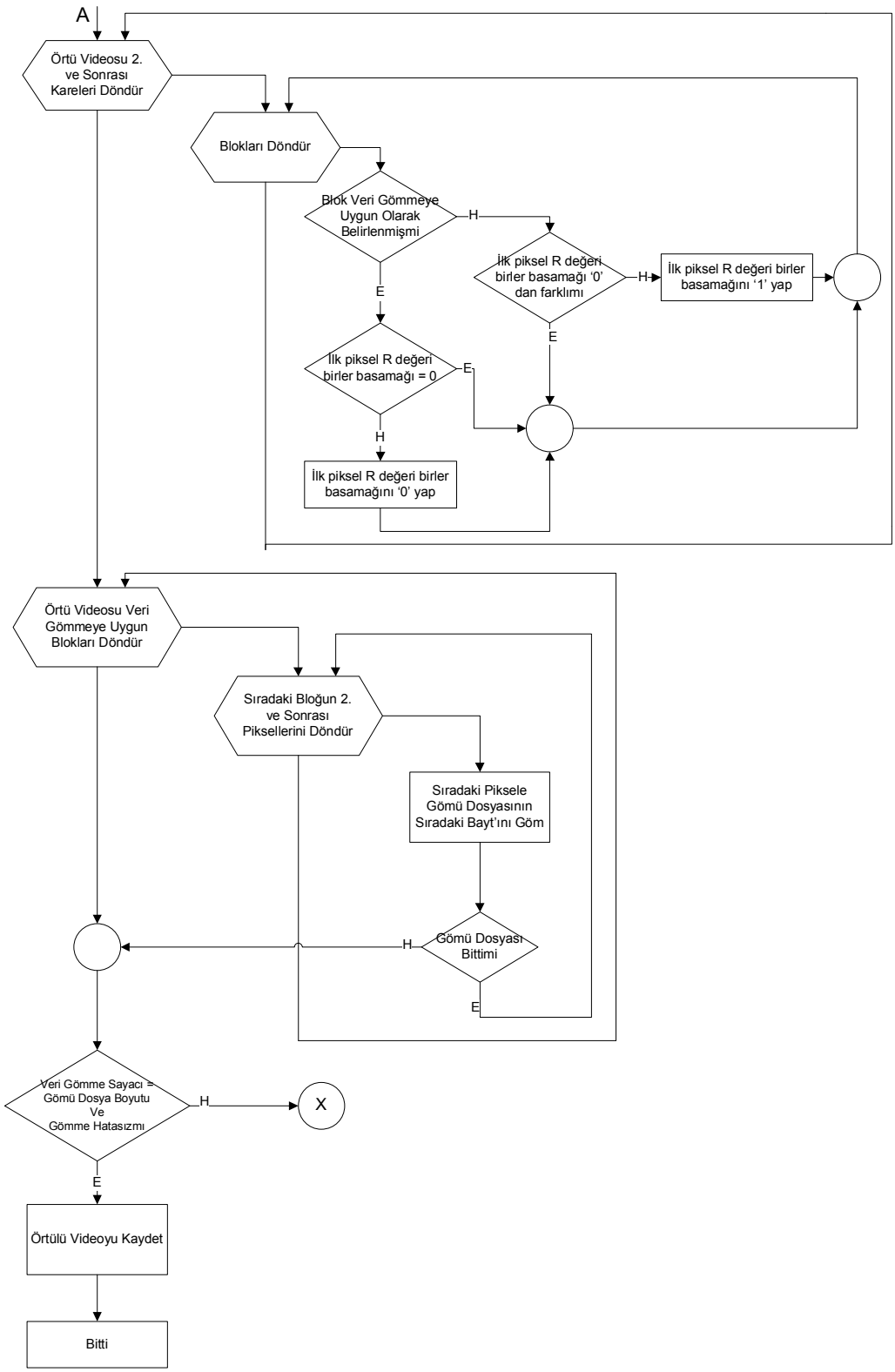
Şekil Ek.5. Benzer Histogramlar Yöntemi Akış Diyagramı.


Başla
Örtü Videosu Yüksekliğine Göre Blok Yüksekliğini Belirle
Örtü Videosu Genişliğine Göre Blok Genişliğini Belirle
Örtü Videosu 2 ve Sonras Karelerin Döndür
Blokları Döndür
Renkleri Döndür F G E
Sıradaki Bloğun Sıradak Renge ait Histogramın A
Kare Numaras >
E
Önceki ve Sonraki Karelerdeki aynı Bloklarır Sıradaki Renge Ait Histogram Farkını A
Kare Numaras >
E
F G B Histogram farklarının ortalamasını alarak Bloğun Histogram Değişim Değerin Bul
X
Kullanıcıdan Eşik Değerini Al
Blok Histogram Değişim Değer Eşik Değerinin Altında olar Blokları Veri Gömmeye Uygur Olarak Belirle
A

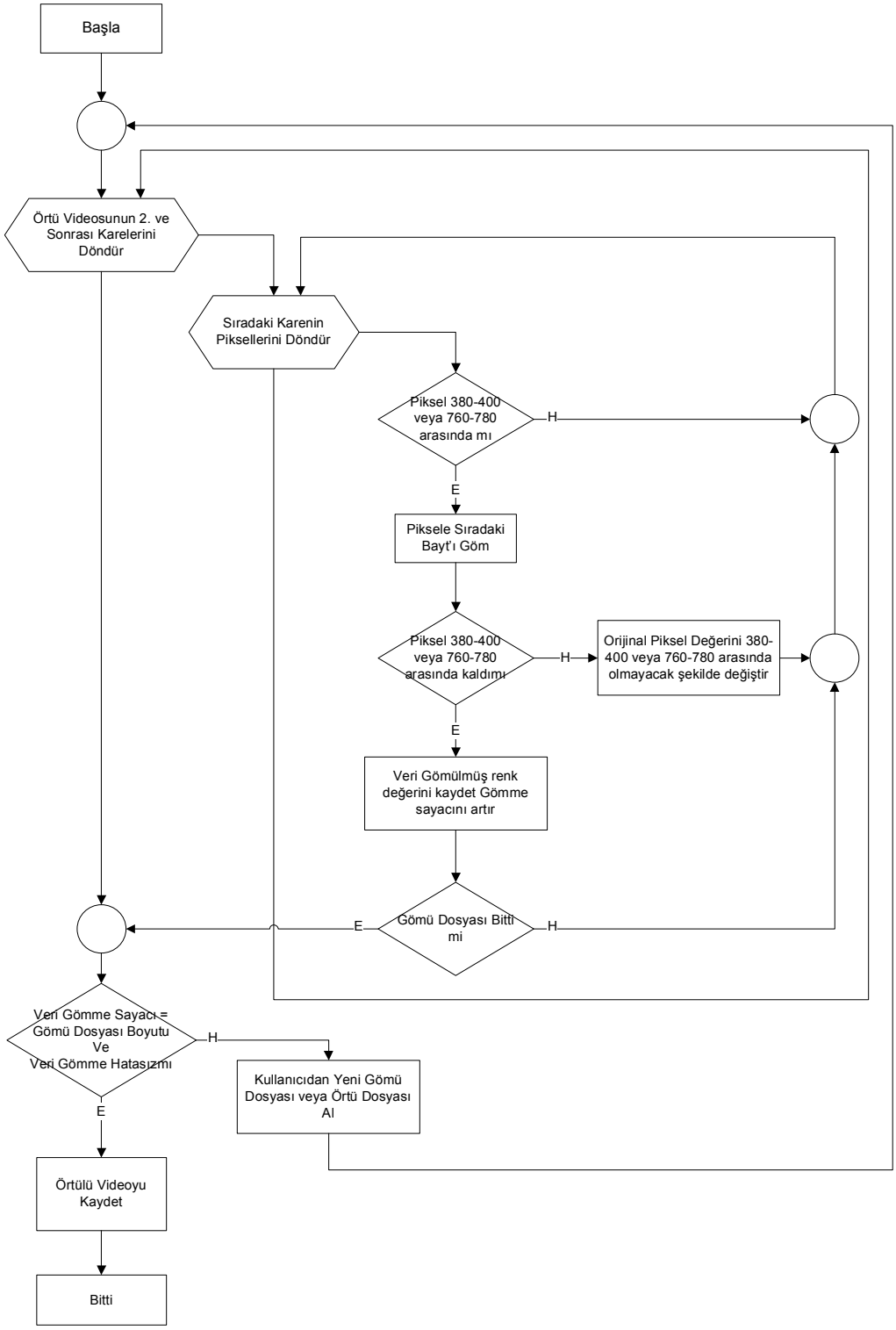


Şekil Ek.6. Blok Tabanlı Benzer Histogramlar Yöntemi Akış Diyagramı.


Başla
Örtü Videosu Yüksekliğine Göre Blok Yüksekliğini Belirle
Örtü Videosu Genişliğine Göre Blok Genişliğini Belirle
X
Kullanıcıdan Eşik Değerini Al
Örtü Videosu 2. ve Sonrası Karelerini Döndür
Blokları Döndür
Renkleri Döndür (R,G,B)
Sıradaki Bloğun Sıradaki Renge ait Histogramını Al
R,G,B Histogram değerlerinin ortalamasını al
Blok Histogram Renk Bileşen Değerleri > Eşik Değeri
H
E
Blok Veri Gömmeye Uygun
A



Şekil Ek.7. Bölgesel Histogramlar Yöntemi Akış Diyagramı.



Şekil Ek.8. DalgaBoyu Yöntemi Akış Diyagramı.

ÖZGEÇMİŞ

Özdemir ÇETİN 1979 yılında İstanbul'da doğdu. İlköğretimini Gazi Osman Paşa ilköğretim okulunda, ortaöğretimini Sağmalcılar Lisesi'nde tamamladı. Lise eğitimine ise Maçka A.T. Teknik Lisesi Elektronik Bölümünde devam etti. Lisans eğitimine 1997 yılında Sakarya Üniversitesi Teknik Eğitim Fakültesi Elektronik–Bilgisayar Eğitimi bölümünde başladı. 2001 yılında lisans eğitimini tamamladı ve aynı yıl Sakarya Üniversitesi Teknik Eğitim Fakültesi Elektronik–Bilgisayar Eğitiminde Araştırma Görevlisi olarak işe başladı. 2001–2003 yılları arasında Teknik Eğitim Fakültesi Elektronik–Bilgisayar Eğitiminde yüksek lisans eğitimini tamamladıktan sonra Mühendislik Fakültesi Elektronik Anabilim dalında doktora eğitimine başladı. Temmuz 2007– Temmuz 2008 tarihleri arasında Amerika'da NewMexico üniversitesinde ziyaretçi araştırmacı olarak görev yaptı. Halen Sakarya Üniversitesi Teknik Eğitim Fakültesi Elektronik-Bilgisayar Eğitimi bölümünde araştırma görevlisi olarak akademik çalışmalarını sürdürmektedir.

ESERLER

- Wenlan Liu, Rohit Sood, Qingchuan Chen, Unal Sakoglu, Jill Hendren, Özdemir Çetin, Ke J. Liu, "Normobaric hyperoxia inhibits NADPH oxidase-mediated matrix metalloproteinase-9 induction in cerebral microvessels in experimental stroke", Journal of Neurochemistry, 16 August 2008.
- Cetin O., Sakoglu U., Sood R., "Software package to calculate permeability based on Patlak method", October 2-4, 2008, 25th Annual Meeting ESMRMB Congress 2008, Valencia/ES.
- Cetin O., Ozcerit A.T, Boru B., "A Novel Blind Video–Steganography Method with High Secret Data Capacity", Network and Information Security National Symposium II, May 16-18,2008, Girne, T.R.Northern Cyprus.

- Cetin,O, Ozcerit,A.T, Cakiroglu,M, "A New Data Embedding Method into Motion Pictures" The 2006 World Congress in Computer Science, Computer Engineering, and Applied Computing, June 26-29, 2006, Las Vegas, USA.
- Cakiroglu,M, Ozcerit,A.T, Cetin,O, "MAC Layer DoS Attacks in Wireless Sensor Networks: A Survey" The 2006 World Congress in Computer Science, Computer Engineering, and Applied Computing, June 26-29, 2006, Las Vegas, USA.
- Cetin,O, Cakiroglu,M, Bayilmis C, Ekiz,H, "Teknolojik Gelişme için Eğitim Önemi ve Internet Destekli Öğretimin Eğitimdeki Yeri", III. International Education Technology Symposium-EGITEK 2003, Gazimagusa, T.R.Northern Cyprus.
- Cakiroglu,M, Ozcerit,A.T, Eskikurt H.I, Cetin,O, "80C51 Mikrodenetleyicilerinde Timer-Counter Yapılarının FPGA Mimarileri Kullanılarak Geliştirilmesi" 3. International Advanced Technologies Symposium, 18-20, 2003 Ankara, TURKEY.
- Cakiroglu,M, Ozcerit,A.T, Cetin,O, Eskikurt H.I, "Integration of Real-Time Counter Unit into a Microcontroller Through Reconfiguration" Proceedings of Twelfth International Symposium on Artificial Intelligence and Neural Networks-TAINN 2003, 02-04 July 2003, Çanakkale, TURKEY.
- Cetin,O, Ozcerit,A.T, Cakiroglu,M, Eskikurt H.I, "Watchdog Timer Biriminin 8051 Mikrodenetleyicisi İçerisine Donanım Tanımlama Dili (HDL) Yardımıyla Entegre Edilmesi", Electric, Electronic, Computer Engineering 10. National Congress, EMO 2003, İstanbul, TURKEY.
- Eskikurt H.I, Cankaya I, Cetin O, "Elektronik Devreler ve Sistemler Laboratuar Kitabı", Sakarya Üniversitesi, 2004.
- Cankaya I, Eskikurt H.I, Cetin O, "Elektronik Devre Elemanları ve Uygulamaları Laboratuar Kitabı", Sakarya Üniversitesi, 2003.