T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

SAYISAL GÖRÜNTÜLERDE İNSAN GÖRME SİSTEMİ MERKEZLİ GELİŞTİRİLEN VERİ GÖMME ALGORİTMALARI

YÜKSEK LİSANS TEZİ

İbrahim COŞKUN

Enstitü Anabilim Dalı	**:**	**ELEKTRONİK VE BİLGİSAYAR EĞİTİMİ**
Tez Danışmanı	**:**	**Yard. Doç. Dr. Özdemir ÇETİN**

Eylül 2010

Bu çalışma SAÜ Bilimsel Araştırma Projeleri Komisyonu tarafından desteklenmiştir. (Proje no: 2010-50-01-024)

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

SAYISAL GÖRÜNTÜLERDE İNSAN GÖRME SİSTEMİ MERKEZLİ GELİŞTİRİLEN VERİ GÖMME ALGORİTMALARI

YÜKSEK LİSANS TEZİ

İbrahim COŞKUN

Enstitü Anabilim Dalı : ELEKTRONİK VE BİLGİSAYAR EĞİTİMİ

Bu tez 16 / 09 /2010 tarihinde aşağıdaki jüri tarafından Oybirliği ile kabul edilmiştir.

Prof. Dr. Etem KÖKLÜKAYA	Yrd. Doç. Dr. Özdemir ÇETİN	Yrd. Doç. Dr Cüneyt BAYILMIŞ
Jüri Başkanı	Üye	Üye

TEŞEKKÜR

Bu çalışmanın hazırlanması esnasında bana yol gösteren, bu alanda çalışmam için beni teşvik eden, yardımlarını ve desteğini benden esirgemeyen değerli danışman hocam Yrd. Doç. Dr. Özdemir ÇETİN' e teşekkür ederim.

Çalışmalarım sırasında çalışabilmem için gerekli ortamı sağlayan, manevi desteğini benden esirgemeyen ve her zaman yanımda olan sevgili aileme teşekkür ederim.

İÇİNDEKİLER

SİMGELER VE KISALTMALAR LİSTESİ

LSB	:En Az Ağırlıklı Bit (LSB, Least Significant Bit)
RGB	:Kırmızı Yeşil Mavi (RGB, Red Green Blue)
ASCII	:American Standard Code for Information Interchange
EBCDIC	:Extended Binary Coded Decimal Interchange Code
BMP	:Bit Map
ANSI	:American National Standarts Institute
JPEG	:Joint Photographic Experts Group
PDF	:Probability Density Function
PNG	:(Portable Network Graphics Format), Taşınabilir ağ grafikleri, biçimler
İGS	:İnsan Görme Sistemi
DB	:Dalgaboyu Yöntemi
YCbCr	:(Luma blue-difference, red-difference),
HSV	:(Hue, Saturation, Value), Renk tonu, Doyum, Değer
HSL	:(Hue, Saturation, Lightness), Renk tonu, Doyum, Açıklık
CIE	:Commission Internationale de l'Eclairage – Ulusal Aydınlatma Komisyonu
SED	:Spektral Enerji Dağılımı

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

ÖZET

Anahtar kelimeler: Sırörtme, Steganografi, Veri Gizleme, Sayısal Görüntü, Dalgaboyu, İnsan Görme Sistemi

Bilgisayar ortamında bilginin gizli bir şekilde gönderilme işlemi herhangi bir sayısal ortama; sese, videoya, görüntüye ya da yazıya, bu bilginin görünmez bir şekilde saklanarak bilginin masum görünümlü bir taşıyıcı aracılığıyla yollanarak gerçekleştirilir. Sırörtme (Steganography) adı verilen bu yöntemde, gönderilecek gizli taşıyıcı dosyada fark edilebilir bir değişikliğe sebep olmayan bir yöntem kullanılarak eklenir. Böylece gönderilen sayısal ortam içinde herhangi bir bilginin bulunduğuna dair hiç bir ize rastlanmaz.

Bu tez çalışması ile, sırörtme uygulamalarında çözüm bekleyen algılanabilirliğe bağlı güvenli haberleşme sorununun iyileştirilmesi amaçlanmıştır. Veri gömme işleminde birinci ve en önemli gereksinim algılanamazlıktır. Resim, video gibi görsel içerikli taşıyıcı dosyalarda algılanabilirlik ölçüsü İGS'ne (İnsan Görme Sistemi) bağlıdır. Bu durumda geliştirilmesi gereken yeni yöntemin İGS özelliklerine, sınırlarına hassas olması gerekmektedir. Tez çalışmasında gizli verinin resim dosyasının veri gömmeye uygun pikselleri içerisine yerleştirilmesinde daha önceki yapılmış benzer çalışmalarda eksik yanları kalan ışık dalgaboyu yöntemi tamamlanarak kullanılmıştır. Görüntü dosyalarında İGS'nin duyarlı olduğu en önemli nokta, renk geçişleridir. Burada ana fikir; taşıyıcı görüntü içerisindeki görülebilir ışığın sınırlarına yakın olan dalgaboyu değerlerine sahip piksellerin bulunarak veri gömmek için kullanılmasını sağlamaktır. Bu sayede sırörtme uygulamalarında çözüm bekleyen algılanabilirliğe bağlı güvenli haberleşme sorununun iyileştirilmesi amaçlanmıştır.

EMBEDDING OF THE DATA IN DIGITAL IMAGING HUMAN VISUAL SYSTEM DEVELOPMENT ORIENTED ALGORITHMS

SUMMARY

Key Words: Steganography, Data Hiding, Digital Image, Wavelenght, Human Visual System.

Confidential information is sent to a computer environment to process any digital media, audio, video, image or article, this information is hiding in an invisible way innocent-looking information is sent via a carrier. In this method which is called Steganography, the carrier sent a secret file. This file is added by using a method not cause a noticeable change in. Thus, any information submitted in the digital media not found any evidence ever been found.

With this thesis, the problem of secure communication due to perceptibility steganography pending applications intended to improve. Data embedding process, the first and most important requirement is imperceptibility. In audio content carrier files such as images, videos, dimensions of perceptibility depends on Human Visual System (HVS). In this case, new method which should be developed must be sensitive of HVS's features. In this thesis the secret data into the image file data to bury the pixels in accordance with similar studies have been made to locate the missing aspects of the earlier completion of the light wavelength method was used. In the image files the most important point is that the HVS is sensitive to color transitions. Here the main idea; carrier close to the borders of the wavelength of light can be seen in the image pixel values is to be used to embed data discovered. In this way, the problem of secure communication due to perceptibility steganography pending applications intended to improve.

BÖLÜM 1. GİRİŞ

Her geçen gün gelişen teknoloji, hayatımıza birçok kolaylık getirmiştir. Özellikle bilgisayar alanında yaşanan gelişmeler, bilgi paylaşımının daha hızlı, ucuz ve kolay olmasını sağlamıştır. Dünya üzerindeki bilgisayarların birbirlerine bağlanmasını ve karşılıklı bilgi alışverişinde bulunabilmesine olanak sağlayan Internet ağı da teknolojinin getirdiği diğer bir ürün olarak karşımıza çıkmaktadır. Son birkaç yıl içinde büyüyen talep karşısında Internet altyapısına yapılan yatırımların artması ve bunun sonucu olarak hızlanan veri iletişimi sayesinde, dünyanın herhangi bir yerindeki bir bilgiye erişmek artık sorun olmaktan çıkmıştır.

Bu gelişmelere paralel olarak, bilgisayar yazılımlarında da birçok yeniliği beraberinde getiren ilerlemeler görülmüştür. Bilgisayar ortamına aktarılan ses, video, görüntü ve metin verileri, geliştirilen yazılımlarla daha kolay işlenebilmektedir. Hem maliyet hem de zaman açısından kazandırdığı avantajların büyük olması nedeniyle, günümüzdeki birçok çalışma artık bilgisayar ortamında gerçekleştirilmektedir.

Bilgisayar ve iletişim teknolojilerindeki gelişime paralel olarak bilgisayar sistemlerinin güvenliği ve özellikle bilgi güvenliği oldukça önemli bir konu olarak karşımıza çıkmaktadır. Özellikle son 10 yılda internetin yaygınlaşmasıyla veri alışverişi ve paylaşımı da artmıştır. Metin, resim, ses, video gibi birçok veriyi içeren dosyalar, etkin bir şekilde dünyanın birçok yerindeki insanlar tarafından paylaşılabilir hale gelmiştir. Fakat hayatı kolaylaştıran bu iletişim ağı çok ciddi güvenlik açıklarını da beraberinde getirmiştir. Birbiriyle haberleşen iki kişi arasındaki iletişim bir üçüncü kişi tarafından erişilebilir ve değiştirilebilir hale gelmiştir.

Temeli antik çağlara kadar dayanan gizli haberleşme, teknoloji değişip geliştikçe şekil ve yöntem açısından da önemli değişiklikler geçirmiş olmasına rağmen önemini

devamlı korumaktadır. Gizliliğin öneminin arttığı uygulamalarda; gizli bilgilerin, üçüncü kişilerin eline geçmeden ilgili hedefe ulaştırılması amaçlanmaktadır.

Bilgisayar ortamında bilginin gizli bir şekilde gönderilmesi için önerilen yöntemlerden biri, herhangi bir sayısal ortama; sese, videoya, görüntüye ya da yazıya, bu bilginin görünmez bir şekilde saklanarak bilginin masum görünümlü bir taşıyıcı aracılığıyla yollanmasıdır. Sırörtme (Steganography) adı verilen bu yöntemde, gönderilecek gizli taşıyıcı dosyada fark edilebilir bir değişikliğe sebep olmayan bir yöntem kullanılarak eklenir [1]. Böylece gönderilen sayısal ortam içinde herhangi bir bilginin bulunduğuna dair hiç bir ize rastlanmaz. Kriptolojiden farklı olarak bilgi, üzerinde herhangi bir deşifre işlemine gerek duyulmadan anlaşılır bir şekilde geri elde edilir. Kriptoloji de ise, bilginin kendisi bir algoritma ile şifrelenir. Şifrelenmiş bilgi, herhangi bir taşıyıcı olmaksızın iletilir. İletim boyunca bilgi şifrelidir. Haberleşmenin sonunda alıcı, deşifre algoritmasını kullanarak şifrelenmiş bilgiyi çözer. Böylece yetkisiz kişiler iletimin herhangi bir yerinde şifrelenmiş bilgiyi elde etse bile çözmek için deşifre algoritmasını bilmediği için asıl bilgiye ulaşamaz [2].

Sırörtme kelimesi Yunanca “steganos: gizli, saklı” ve “grafi: çizim yada yazım” kelimelerinden gelmektedir. Sırörtme, Antik yunan ve Heredot zamanına kadar uzanan oldukça eski bir veri gizleme yöntemidir. Heredot, İran Savaşları sırasında, kafasını kazıtıp kafa derisinin üzerine, gizli bir mesajın dövmesinin yapılmasına izin veren bir ulaktan bahsetmektedir. Mesaj yazıldıktan sonra ulak saçının uzamasını beklemekte, daha sonra ulak mesajı bekleyen kişiye ulaşmakta, kafasını tekrar tıraş etmekte, böylelikle mesaj ortaya çıkmaktadır. Bu yöntem bilinen ilk sırörtme uygulamasıdır. Daha sonraki zamanlarda sırörtme, harflere müzik notalarının atanması, I. ve II. Dünya Savaşlarında kullanılan mors kodları, II. Dünya savaşı esnasında başarıyla uygulanan görünmez mürekkeplerin kullanımı gibi uygulamalarla karşımıza çıkmaktadır [3].

Yukarıda da ifade edildiği gibi sırörtmenin en temel amacı iletişimin gizliliğini sağlamaktır. Sırörtmede sayısal bir verinin başka bir sayısal veri içerisine, fark

edilebilir değişikliklere sebep olmadan saklanması gerçekleştirilmektedir. Örneğin bir metin dosyası, bir resim dosyasına saklanmakta ve sonuçta oluşan resim dosyası hem fiziksel olarak hem de görsel olarak orijinalinden farklı olmamaktadır. Böylece iki uç arasındaki iletişimi gözetleyenler, arada sadece transfer edilen bir resim görmekte, ama aslında bu resim yoluyla gizli bir mesajlaşma gerçekleştiğinin farkında olmamaktadırlar.

Veri saklama yöntemlerinin temel mantığı, sayısal veri dosyası formatlarındaki gereksiz veya çok önemli olmayan kısımların kullanılmasına veya insan duyularının zayıf kaldığı ya da sınırlarının kullanılmasına dayanmaktadır.

İnsan görme sistemi (İGS) sırörtme yöntemlerinden olan LSB yöntemi kullanılarak elde edilen taşıyıcı resimdeki küçük değişimleri fark edememekte veya farkına varamamaktadır. Örneğin bir Bitmap dosyasındaki piksel değerlerinin bir arttırılması veya azaltılması sonucu oluşan renk değişimini göz fark edemez. Bu durumda resim dosyasının bazı piksel değerleri, saklanacak verinin bitlerini barındırmak amacıyla değiştirilebilir ve bu değişiklikler insan gözü tarafından fark edilemez. Saklama işlemi sonucunda görsel açıdan ve boyut olarak orijinal dosya ile aynı bir resim dosyası oluşturulur.

Bu çalışmada, yapılmış önceki çalışmalardan farklı olarak veri gizleme yöntemi olarak dalga boyu yöntemi kullanılmıştır. Elektromanyetik tayfta görülebilir alanın dalga boyu değerleri her bir renk için farklıdır ve alt sınırı 350 nm ile mor, üst sınırı da 780 nm ile kırmızı temsil eder. Dalga boyu yönteminde İGS'nin zaafından faydalanılarak veri gizleme şeklinde gerçekleştirilir. İçerisine veri gömülmek istenen sayısal görüntüde sınır dalga boyu değerlerine (350 nm morötesi için – 780 nm kızılötesi için) yakın renklere sahip pikseller belirlenir. Bu sınırlara yakın dalga boyu değerlerine sahip renkler kullanılarak veri gizleme işlemi gerçekleştirilir. Burada faydalanılan durum insan gözünün mor ötesi ve kızıl ötesi ışık dalgalarını algılayamamasıdır. Böylelikle mor ötesi ve kızıl ötesi ışınlarına yakın renklerin İGS tarafından algılanması daha zor olacaktır. [4]

Bu tez çalışması beş bölümden oluşmaktadır. Birinci bölümde bu çalışmanın gereği açıklanmıştır. İkinci bölümde sayısal görüntü hakkında temel bilgiler verilmiştir. Ayrıca insan gözünün yapısı, ışık bilgisi, renk teorisi ve renk uzayı hakkında bilgiler sunulmuştur. Üçüncü bölümde veri gizleme/gömme teknikleri incelenmiştir. Tez çalışmasının ana kısmını oluşturan dördüncü bölümde ise sayısal görüntülerde İGS merkezli geliştirilen veri gömme algoritmaları dalga boyu yöntemi ve yazılan kullanıcı arayüz programı hakkında bilgiler bulunmaktadır. Beşinci bölümde sonuçlar ve öneriler başlığı altında yapılan deneysel çalışmalardan elde edilen sonuçlar değerlendirilmiş ve devam niteliğini taşıyabilecek yeni çalışmalara öneriler sunulmuştur.

BÖLÜM 2. SAYISAL GÖRÜNTÜ ESASLARI VE GÖRÜNTÜ İŞLEME

2.1. Giriş

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

Sayısal görüntü işleme matematiksel ve olasılık hesaplarının üzerine kurulu olmasına rağmen, sayısal görüntü işlemede hangi tekniklerin kullanılacağı noktasında insanın görsel algılaması büyük ve önemli bir rol oynamaktadır [5].

Görsel algılama, göz ve ışık ile yapılan kavrayış eyleminden kaynaklanan ve canlıların sahip olduğu en etkili algılama metotlarından biridir. Optik bir yapıdan oluşan göz organına sahip canlılar, nesnelerin uzaydaki *x, y, z* referanslarını iki boyutlu bir düzlem üzerinde ifade ederek bu bilgiyi bellek veri tabanlarında saklarlar. Canlıların görebildikleri ışık belirli dalga boyları, enerji seviyeleri ve ışık ısısı değerleri arasındadır. Ancak bu dar gösterge çizelgesi bile, özellikle insanın çevresini çok detaylı bir şekilde tanımlamasına ve renklenmesine yetmektedir.

Renkler, yansımanın bir sonucu olarak beyin tarafından yaratılmış kavramlardır. Bir başka değişle renkler, nesnelerin yüzey gerilimlerinin ışığın baskısına verdiği tepkiyi beynin sınıflandırması sonucu oluşturulmuş sanal kavramlardır. Nesnenin yüzeyine çarpan ışık bir baskı oluşturur. Bu baskının bir bölümünü nesnenin yüzeyi rezonansa geçerek sönümler. Böylece yansıyan ışığın dalga boyu, derinliği, şiddeti, enerjisi gibi parametreleri değişime uğrar. İnsan beyni kendi içinde bu parametreleri alt ve üst değerler olarak ölçeklendirilmiştir. Her bir ölçek beyinde bir renk çağrışımı şekline dönüşür. Bu durum, canlının bir bakışta nesnenin nitelikleri ile ilgili bilgi edinmesi için tasarlanmış çok gelişmiş bir algılama meydana getirmiştir. Nesnelerin yüzey

gerilimleri, onların sert veya yumuşak olmaları, pütürlü veya parlak olmaları, organik veya inorganik olmaları gibi canlı için çok önemli bilgileri, nesnenin yanına gitmeden veya dokunmadan uzaktan edinmesini sağlar. Gözün arka bölümündeki ışığa duyarlı hücreler, ışığın şiddeti, rengi gibi parametrelerini elektrik sinyallerine çevirerek beyne iletirler. Sesin havasız ortamda iletilememesine rağmen ışığın evrenin her köşesinde var olması görsel algılamanın, evrenin büyük patlamadan bu yana saçtığı enerjiyi ve termodinamik yasalarını kullanan çok temel ve önemli bir kavrayış olduğunu göstermektedir [6].

Günümüzde gelişen teknolojilerin başında Görüntü İşleme teknikleri gelmektedir. Görüntü İşleme, insan gözü ile yapılan işlemlerin; görüntüleme cihazları ve akıllı yazılımlar kullanan makinelere yaptırılmasını amaçlayan bir çalışma alanıdır. Görüntü işleme tekniklerini anlayabilmek için görme olayının nasıl gerçekleştiği hakkında bilgi sahibi olmak önemlidir.

2.2. Görme Olayı

Elektromanyetik dalgalar geçtikleri ortamın atom yapısına bağlı olarak hızları yavaşlar, emilir veya yansır. Elektromanyetik tayfta 350 nm ile 780 nm arasında kalan dalga boyuna sahip alan "görülebilen ışık" olarak adlandırılır. İşte göz bu “görülebilen ışığı” algılayarak görme işlemini gerçekleştirir. Görme olayının daha iyi anlaşılabilmesi için, İGS yapısından ve mekanik görme olayının nasıl gerçekleştiğinden bahsetmek gereklidir. Görüntü işleme teknikleri yine İGS’ye bağlı olarak geliştirilmektedir.

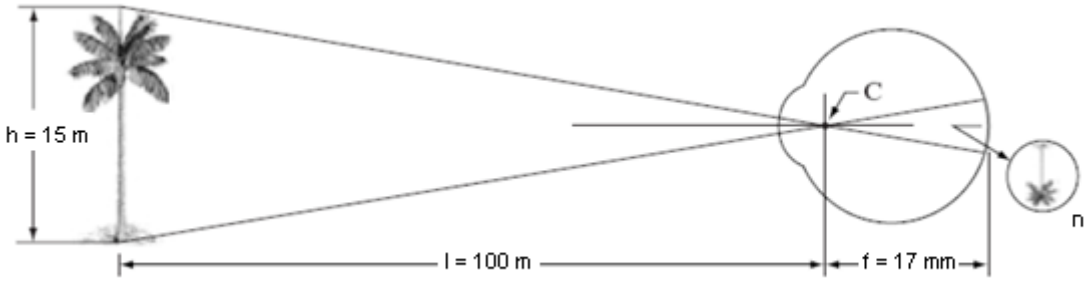
2.2.1. Görme olayının oluşması

Görme olayı için gerekli en önemli şart, ortamda bir ışık kaynağının olmasıdır. Nesnelerden yansıyarak korneadan göze giren ışık görmeye neden olur. Korneanın kavisli bir yapıya sahip olmasından dolayı ışık korneadan kırılarak geçer. Gözün bir nesneye ya da noktaya odaklanması mercek yardımı ile olur. 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 kırpma yapar. Bu bilgilerden faydalanılarak ağ tabakası üzerine düşen nesnenin görüntü boyu matematiksel olarak şu şekilde hesaplanabilir.

$$\frac{h}{l} = \frac{n}{f} \tag{2.1}$$

Burada h gerçek nesnenin yüksekliği, l nesne ile göz arasındaki mesafe, f mercek merkezinin ağ tabakaya mesafesi (17 mm), n gözde oluşan görüntünün boyunu belirtir.



Şekil 2.1. İnsan gözünde bir görüntünün oluşması.

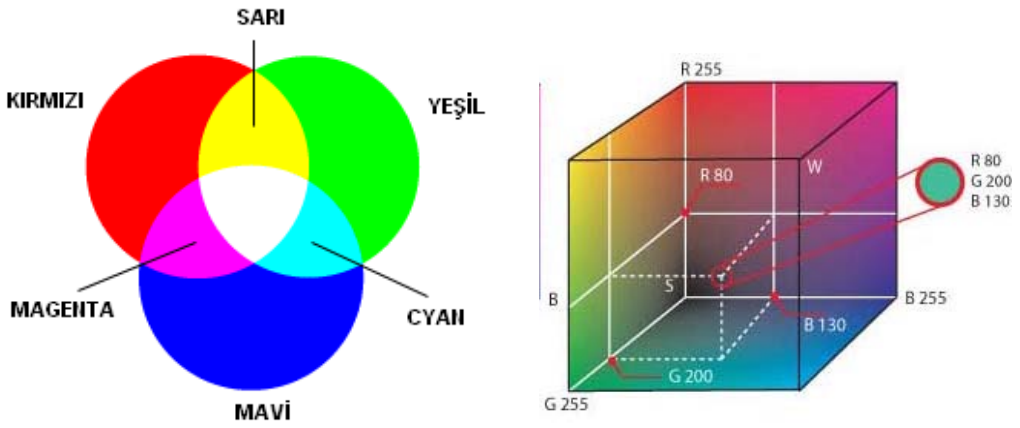
2.3 RGB Renk Uzayı

RGB renk uzayı, İngilizcedeki 'Red' 'Green' 'Blue' (yani 'Kırmızı' ‘Yeşil' 'Mavi') kelimelerinin baş harflerinden ismini alan bir renk uzayıdır. En sık kullanılan renk uzaylarındandır.

Işığı temel alarak, doğadaki tüm renklerin kodları bu üç temel renge referansla belirtilir. Her renk %100 oranında karıştırıldığında beyaz ve %0 oranında karıştırıldığındaysa siyah elde edilir.

Bu uzayda, ana renkler olan kırmızı, mavi ve yeşil belirtilmediği için, bu ana renklerin tanımı değiştikçe, tüm renkler değişir.

Internette kullanılan renk sistemi RGB renk sistemidir. Bunun sebebi, 1953'te ilk fotoğraf makinesi Polaroid'te ve ondan sonra da televizyonlarda standart kabul edilmiş olmasıdır. Günümüzde de tüplü ekranlarda, tarayıcılarda, televizyon ve manuel fotoğraf makinelerinde standart olarak kullanılır [7].



(a) Diyagonel model (b) Küp Modeli

Şekil 2.2. RGB renk modelleri

2.4. CIE 1931 Renk Uzayı

Elektromanyetik spektrum, görünür ışığı ve elektromanyetik enerjinin diğer formlarını içerir (X-ışınları, mor ötesi ışınlar, kızılötesi ışınlar, vb.). Işık, "dalgaboyu" ile tanımlanır ve kullanılan en uygun birimi nanometredir (1 nm = 10^{-9} m'dir). İnsan gözü elektromanyetik spektrum içerisinde görünü alan olarak adlandırılan 350 - 780 nm aralığında algılama yapabilir. "Işık kaynağı", "cisim" ve "gözlemci", rengin algılanmasını etkileyen üç temel öğedir. Renk ölçümü, bu üç öğenin birbiriyle etkileşimi ile ilgilidir ve rengi sayısal olarak ifade edebilmek için her bir öğenin sayısal olarak ifade edilebilmesi ve tanımlanması gereklidir. Yapısındaki değişkenliklerden dolayı, renk ölçümünde doğal ışık kaynağı olan güneş kullanılamaz, "yapay ışık kaynakları" kullanılır. Yapay ışık, genellikle "akkor ışıma" (Örnek: tungsten filamanlı lamba) veya "gaz deşarjı" (Örnek: fluoresans lamba) yoluyla elde edilebilir. Işık kaynakları, Spektral Enerji Dağılımı (SED) değerleri ile karakterize edilir ve bir ışık kaynağının SED değeri, ışık kaynağının her bir dalga

boyundaki radyatif ışımasının gücüdür (W.cm-2.nm-1). Bir ışık kaynağının önüne çeşitli renkte filtreler (jelatin veya sıvı filtreler) konmak suretiyle SED değerlerinde değişiklikler yapılabilir. Böylece, farklı SED değerlerine sahip yeni bir sistem oluşturulabilir. Günümüzde yaygın kullanım alanı bulan renk spesifikasyonu, CIE (Commission Internationale de l'Eclairage - Uluslararası Aydınlatma Komisyonu) tarafından belirlenen bir sisteme dayanmaktadır. 1931'de oluşturulmuş bu sisteme temel yapı ve prensiplerde değişiklik yapılmaksızın bugüne kadar yeni eklemeler yapılmıştır. CIE, 1931 yılında, o zaman mevcut olan ve spektral karakterleri (SED değerleri) bilinen temel ışık kaynaklarından bir seri standart illüminantın (SED değerleri bilinen filtrelenmiş veya filtrelenmemiş ışık kaynaklarının) renk ölçümünde kullanımını önermiştir. Bunlar, CIE İllüninant A, CIE İllüminant B, CIE İllüminant C ve CIE İllüminant D65'dir. Işık kaynakları, SED değerleri ile "tanımlanır" ve Planck radyasyon kaynağının renk sıcaklığı kavramı ile de "isimlendirilir" (Örnek: 6500 K renk sıcaklığındaki bir ışık kaynağı, vb.).

Bir ışık hüzmesi, pigment partikülleri ile kaplı bir yüzey üzerine düşürüldüğünde bu yüzey tarafından yansıtılır (geldiği ortama geri gönderilir), kırınıma uğratılır, pigment partikülleri tarafından emilir veya saçınıma uğratılır. Üzerine bir ışık huzmesi düşürülen herhangi bir yüzeyden gelen yansıma, aynı ışık hüzmesinin BaSO4 ile kaplı beyaz plakadan gelen yansıma ile karşılaştırılarak "% Reflektans" olarak ifade edilir. BaSO4 beyazının reflektans değeri, "100 birim" olarak kabul edilmektedir. Bu şekilde cisme ait özellikler tanımlanmaktadır.

Renk ölçümüne ait son öğe olan standart gözlemci kavramı, CIE tarafından 1931 yılında gerçek denekler ile yapılan çalışmalar sonucunda tanımlanmıştır. 700 nm dalgaboyunda "kırmızı", 546.1 nm dalgaboyunda "yeşil" ve 435.8 nm dalgaboyunda "mavi" primer birincil referans uyarıcılar kullanılmış, bir görsel kolorimetre yardımıyla deneklerin monokromatik test lambasının rengini bu üç birincil kaynağın şiddetlerini değiştirmek suretiyle "eşleştirilmeleri" istenmiştir. Bu deneysel çalışmanın sonucunda, insan gözünün farklı dalgaboylarındaki ışığa karşı davranışını ifade eden üç adet hassasiyet eğrisi elde edilmiş ve deneklerin 2°'lik gözlem açısı ile çalışmış olmalarından dolayı da bu eğriler, "2° Standart Gözlemci" veya "CIE 1931 Gözlemcisi" olarak tanımlanmıştır [8].

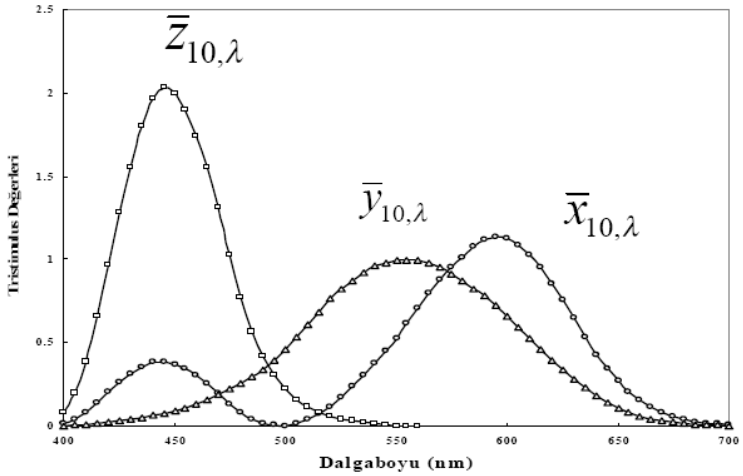
x : “kırmızı hassasiyeti” eğrisi,

y : “yeşil hassasiyeti” eğrisi ve

z : “mavi hassasiyeti” eğrisi olarak adlandırılabilir.

“λ” indisi, bu eğrilerin dalgaboyuna bağımlı olarak değiştiğini göstermektedir.

Şekil 2.2’de 10° Standart Gözlemci için renk eşleme fonksiyonları eğrisi görülmektedir [8].



Şekil 2.3. 10° Standart Gözlemci için “renk eşleme” fonksiyonları

2.4.1. Tristimulus değerleri

Rengin sayısal olarak ifade edilmesinde, ışık kaynağına ait SED değerlerinin, cisme ait % reflektans değerlerinin ve Standart Gözlemci’ye ait (2° veya 10°) renk eşleme fonksiyonlarının (renk hassasiyet değerlerinin) her bir dalgaboyuna ait büyüklüklerinin çarpımlarının toplamı, bize o rengin “sayısal değerleri”ni verecektir. Bu değerler, o rengin “tristimulus” değerleri olarak adlandırılırlar ve X, Y ve Z ile ifade edilirler. Yukarıdaki tanımı aşağıdaki denklemler ile ifade edebiliriz:

$$X = \int_0^\infty I(\lambda)\,\overline{x}(\lambda)\,d\lambda \tag{2.2}$$

$$Y = \int_0^\infty I(\lambda)\,\overline{y}(\lambda)\,d\lambda \tag{2.3}$$

$$Z = \int_0^{\infty} I(\lambda)\,\bar{z}(\lambda)\,d\lambda \tag{2.4}$$

Burada X, Y ve Z rengin tristimulus değerleri olmaktadır.

Sonuç olarak, X-Y-Z değerleri renk tayfındaki görülebilir alana ait değerler değildir. Bununla birlikte renkserlik (chromaticity) şeması genellikle doğrusal bir değere sahip değildir. Çünkü iki parlaklık değeri arasındaki birim vektörün değeri, insan gözü ile daima görünebilir bir renk değerine sahip olmayabilir. Bu sistemde renk Yxy olarak tanımlanır ve adlandırılır. Üçüncü koordinat olan z, tanımlanabilir fakat gerekli değildir [8].

2.4.2. Renk eşleştirme fonksiyonları

İnsan gözü kırmızı, yeşil, mavi olarak bilinen kısa, orta ve uzun dalga boylarına duyarlı hücrelere sahiptir. Bu renk hissinin tanımlanabilmesi için üç parametrenin yeterli olması anlamına gelmektedir. XYZ renk uzayı doğrudan insan gözünün ölçümünü esas aldığı için diğer renk modlarından farklıdır ve diğer renk modellerine de temel oluşturur. Herhangi bir renk, o renge ait tristimulus değerlerinden kromatasite koordinatları olan x, y, z değerleri tanımlanmak isterse aşağıdaki bağlantılar kullanılır.

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

$$y = \frac{Y}{X + Y + Z} \tag{2.6}$$

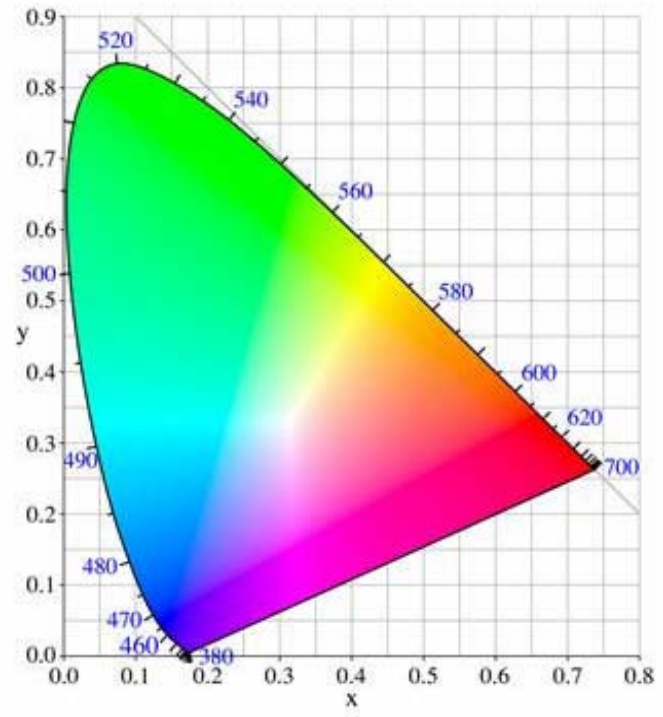
$$z = \frac{Z}{X + Y + Z} \tag{2.7}$$

x. y ve z değerleri 0 ile 1 arasındadır.

x = y = z = (1/3) noktası teorik olarak beyazdır. Bu noktadan uzaklaşıldıkça renklerin doymuşluğu artar. CIE tarafından 1931 yılında standart aydınlatıcı (A, B, C, D_{50}, D_{65}, E, F) ve standart gözlemci (2^0, 10^0) tanımları üzerine kurulan CIE XYZ renk uzayının iki boyutlu gösterimi bu esasa dayanır.

Şekil 2.2' deki at nalına benzeyen bu şekle "gamut" denir. Renk biliminde gamut renkli görüntü işleme cihazlarının sahip olduğu renk yelpazesi olarak tanımlanır [9].

1931 ve 1964 yıllarında gerçek denekler kullanılarak, 2° ve 10° gözlem açıları ile bir görsel kolorimetre yardımıyla renk eşleme işlemi yapan gözlemcilere ait hassasiyet fonksiyonları tanımlanmıştır.



Şekil 2.4. XYZ renk modeli

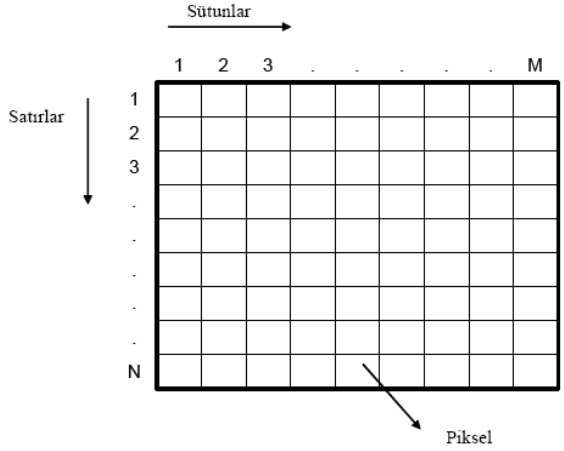
2.5. Sayısal Görüntü ve Temel Terminolojisi

Bilgisayarların ve sayısal cihazların yaygınlaşması ve sayısal haberleşmenin analog haberleşmeden daha kolay uygulanabilir olması tüm bilgi türlerinde olduğu gibi analog 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 [4].

2.5.1. Sayısal resmin yapısı

Sayısal resim N satır ve M sütunluk bir dizi ile temsil edilir. Genellikle satır ve sütun indeksleri y, x veya r, c olarak gösterilir. Bu dizinin her bir elemanı piksel olarak isimlendirilir. En basit durumda pikseller 0 veya 1 değerini alırlar. Bu piksellerden oluşan resimlere ikili (binary) resim denir.



Şekil 2.5. Sayısal resmin yapısı

‘1’ ve ‘0’ değerleri sırasıyla aydınlık ve karanlık bölgeleri veya nesne ve zemini (nesnenin önünde veya üzerinde bulunduğu çevre zemini) temsil ederler [10]. Sayısal görüntü dosyaları renkli olarak genellikle 8 yada 24 bit; gri-seviye görüntüler ise 1-2-4-6 ya da 8 bit olabilirler.

Gri-seviye resimlerde her piksel, 0 (siyah) ile 255 (beyaz) arasında tam sayı değer alan 1 bayt ile temsil edilmektedir. 0–255 arasındaki değerler gri ve tonları renklerdir. Bundan dolayı bir resme ait tam sayı gri ton seviye (gray level) olarak isimlendirilmektedir [11].

8 bitlik renkli görüntülerde piksel başına 1 bayt kullanılır. 8 bitlik görüntüler renk sınırlaması yüzünden çok iyi bir sonuç vermemektedir. Saklanacak bilgi, saklama ortamını çok fazla değiştirmeyecek şekilde dikkatlice seçilmelidir. Orijinal görüntüde son bite ekleme işlemi yapıldığında, renk girişi göstergeleri değişmektedir. 8 bitlik görüntülerde 4 basit renk (WRBG) kullanılmaktadır. Bunlar; beyaz (White-W), kırmızı (Red-R), mavi (Blue-B) ve yeşildir (Green-G).

Bu renklerin renk paletinde karşılık gelen girişleri ise sırasıyla 0 (00), 1 (01), 2 (10), 3 (11) şeklindedir [1].

24 bit resimler ise bir piksel başına 3 bayt kullanmaktadır. Her pikselin rengi; Kırmızı (red), Yeşil (green), Mavi (blue) olmak üzere üç ana renkten elde edilmektedir. Buna pikselin RGB değeri denmektedir [12].

2.5.2. Çözünürlük ve depolama kapasitesi

Resim çözünürlüğü resmin taşıdığı detayı tanımlar. Yüksek çözünürlük resimde daha fazla detay anlamına gelir. Resim çözünürlüğü değişik şekillerde ölçülebilir:

- Resim çözünürlüğü ekranda taradığı satır sayısına göre
- Yatay ve dikey piksel sayısına göre
- Yatay ve dikey piksel sayıları çarpılarak ifade edilebilir.

Örneğin bir resim için 640x480 çözünürlüğe sahiptir ifadesi kullanıldığında; bu resim alanının dikey olarak 480 piksel, yatay olarak 640 piksel kullanılarak oluşturulduğu (640x480 = 307200 piksel içerdiği) anlaşılır. O halde bir sayısal görüntü için çözünürlük ne kadar yüksek ise gerçek görüntüye o kadar yakın görüntüdür denilebilir.

Kapasite açısından da BMP ve GIF formatındaki dosyalar daha iyi sonuçlar vermektedir. JPEG formatındaki dosyalarda 8x8 piksellik bloklara sadece 1 bayt saklanabilmektedir. Bu yüzden saklanabilecek veri miktarı oldukça azdır [13].

BÖLÜM 3. VERİ GİZLEME / GÖMME TEKNİKLERİ

3.1. Giriş

Bu bölümde; veri gizleme / gömme teknikleri hakkında temel bilgilerin verilmesi ile yapılan tez çalışmasının daha iyi anlaşılabilmesi amaçlanmaktadır.

Bilişim teknolojilerinin hayatımıza daha fazla girmesi ve yaygınlaşmasıyla birlikte yapılan iş ve işlemler elektronik ortamlara kaymakta, bu ortamlarda bulunan, saklanan, işlenen ve transfer edilen bilgilerin ise korunması veya güvenliğinin sağlanması çok büyük önem arz etmektedir. Sayısal olarak veri iletişimi gerçekleştirilen bir ortamda, göndericiden alıcıya giden veriye yönelik izinsiz erişim, zarar verme, yok etme, değişiklik yapma ve yeniden üretme gibi birçok tehdit mevcuttur. Bu tehditlerin alınan önlemlere rağmen her gecen gün arttığı rapor edilmektedir [14, 15]. Bu tehditlerin ortaya çıkmasına karşılık olarak bu tehditlerden korunmak için de çeşitli teknikler geliştirilmiştir. Şifreleme teknikleri bunların başında gelen çözüm yolları arasındadır.

Veri şifrelemeyi konu edinen bilim dalı kriptoloji; gizli ve güvenlikli haberleşme ile ilgilenen matematik biliminin bir dalıdır. Krptografi kelimesi gizli yazı manasına gelen, gizli (crypto-) ve yazı (-graphy) kelimelerinden türemiştir. Kriptoloji hakkında daha detaylı bilgi için [4], [16] kaynakları faydalı olabilir. Veri şifreleme maksadıyla geliştirilen çeşitli algoritma ve teknikler bulunmaktadır. Alıcıdaki mesajın, orijinali ile aynı olmasını sağlamak, doğruluğunu ispatlamak yine bu algoritma tasarımları ile mümkündür. Haberleşme ağlarında bir merkezden diğer bir merkeze gönderilen ve alındığı veya gönderildiği yerde saklanan bilgilerin korunması, yetkilendirilmemiş kişilerin bu bilgilere ulaşmasının önlenmesi, günümüz bilgi teknolojilerinde şifrelemeye (encryption – decryption ve cipher-decipher) ayrılan zaman ve önemi sürekli olarak artırmaktadır. Internet ve Intranet uygulamalarında; elektronik mektup,

banka işlemleri, kişisel işlem ve bilgilerin saklanması, dijital imza ve kimlik üretimi, veritabanı dosyalarının korunumu, video kriptolojisi, elektronik oyun ve program şifrelemesi, faks ve telefon şifrelemesi gibi uygulamaları sıkça kullanılmaktadır.

Başlangıçta sadece askeri veya uluslararası/diplomatik mesajların korunarak güvenli bir şekilde alıcıya aktarılması ihtiyacı ile ortaya çıkan şifreleme teknikleri günümüzde bu alanlardaki özelliğini hala korumakta olup ticari uygulamalardaki gereksinim de küçümsenmeyecek boyutlara ulaşmıştır [17].

Sayısal görüntü dosyalarını doğrudan şifrelemek için geleneksel saklı yazı sistemleri (RSA ve DES gibi) kullanabilmesine rağmen bu sistemler iki nedenden dolayı uygun değildir. Bunlardan birincisi görüntü dosyalarının boyutları metin dosyalarından daha büyüktür ve şifrelemek için daha fazla süreye ihtiyaç duyarlar. İkincisi ise şifrelenen metin dosyası çözüldükten sonra metin dosyası için ilki ile eşdeğerde olması zorunludur. Görüntü dosyalarında ise insan gözünün algılamasına göre ufak bozulmalar genellikle kabul edilebilmektedir [18]. Bu nedenlerden dolayı sayısal görüntü dosyalarının içerisine veri gizlemek için sırörtme yöntemleri tercih edilmiş ve geliştirilmiştir.

Sırörtmenin şifrelemeden en önemli farkı; sırörtmede saklı mesajın varlığının gizlenmesidir. Yani saklı verinin örtü verisi içine gömüldüğü bilgisi sadece mesajın alıcısı tarafından bilinir ve örtü verisine sahip olan bir başkası saklı verinin varlığını fark edemez. Şifrelemede ise gönderilen verinin gizli olduğu herkes tarafından bilinir. İçeriği gizli anahtar olmadan anlaşılamaz ve gizli verinin anlaşılabilmesi için çok büyük çabanın ve zamanın harcanması gerekir [19]. Şifrelemede güçlü algoritmaların kullanılması nedeniyle deneme (brute-force) saldırılarına karşı dirençli olup gizli verinin elde edilmesi çok güç olmaktadır. Analiz için güçlü bilgisayarlara ihtiyaç duyulmaktadır. Sırörtmede ise mesajın herhangi bir nesnede saklandığı anlaşıldığında eğer gizli veri şifrelenmemiş ise elde etmek nispeten daha kolaydır.

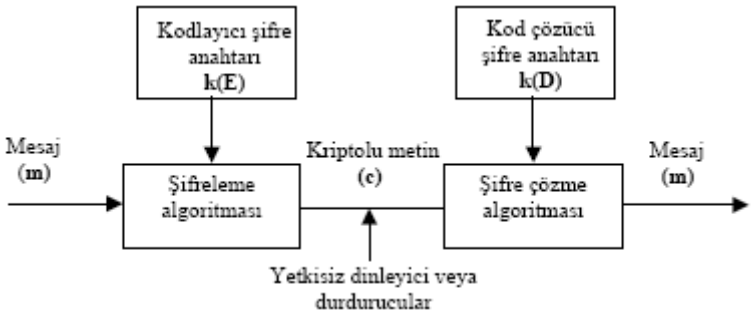
Sırörtme sistemlerinde gizli bilgi şifrelendiğinde yetkisiz kişiler tarafından mesajın varlığı tespit edilse bile gizli anahtar olmadan mesaj hala gizliliğini koruyacaktır.

Ancak haberleşmenin gizliliğinin fark edilmesi nedeniyle sırörtme esas amacına ulaşamamış olacaktır.

Ayrıca şifrelemede kullanılan algoritmaların birçoğu herkes tarafından bilinmektedir. Ancak sırörtme yöntemleri hâlihazırda geliştirilmeye açıktır ve çalışmalar devam etmektedir.

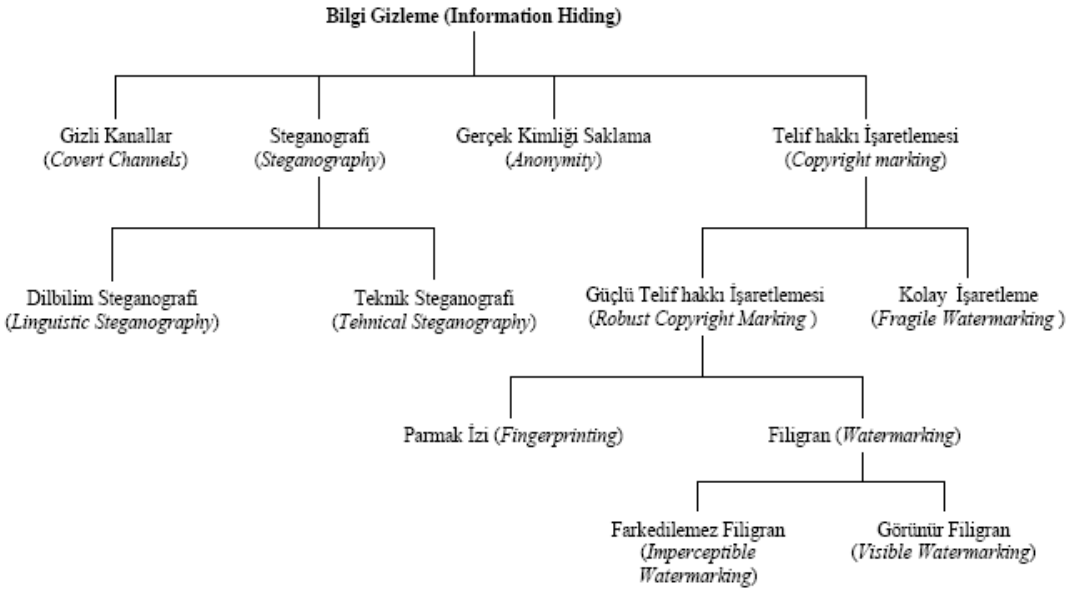
3.2. Veri Gizleme Terminolojisi

Şekil 3.1 genel olarak bir şifreleme sisteminin diyagram olarak açıklamasını göstermektedir.



Şekil 3.1 Genel olarak şifreleme ve çözme blok diyagramı [20].

İletişimin güvenli bir şekilde gerçekleştirilebilmesi için çeşitli yöntemler geliştirilmiştir. Veri gizlemenin sınıflandırılması Şekil 3.2'de gösterilmektedir [21]. Bu sınıflandırma, veri gizleme konusunda yapılan ilk çalıştayda üzerinde çalışılarak kabul edilmiştir [22].



Şekil 3.2. Veri gizleme yöntemlerinin sınıflandırılması

3.2.1. Kriptografi

Kriptografinin amacı mesajları anlaşılmaz hale getirerek gizli anahtara sahip olmayan yetkisiz kişilerin mesajı yeniden elde ederek orijinal haline getirmesini önlemektir.

Bir kriptografik sistem, bilgi güvenliğini sağlamak için bir araya getirilmiş birçok küçük yöntemler bütünlüğü olarak görülebilir. Bu yöntemler yapıları itibarı ile üç ana grupta incelenebilirler:

1- Anahtarsız şifreleme; anahtar kullanmayan kriptografik algoritmalar, veya diğer adlarıyla Veri Bütünlüğü ve Özet Fonksiyonları, veri bütünlüğünü garanti etmek için kullanılan MD5, SHA-1, RIPEMD-160 gibi kriptografi algoritmalarının kullanıldığı yöntemlere verilen isimdir.

2- Gizli anahtarlı şifreleme; hem şifreleme hem de deşifreleme işlemi için aynı anahtarı kullanan kripto sistemlere verilen isimdir. Simetrik şifreleme olarak da isimlendirilmektedir. DES, 3DES, Blowfish, IDEA, SAFER gibi algoritmalar gizli anahtarlı şifreleme algoritmalarına örnek olarak verilebilir.

3- Açık anahtarlı şifreleme; şifreleme ve deşifreleme işlemleri için farklı anahtarların kullanıldığı bir şifreleme sistemidir. Sistemin bu özelliğinden dolayı asimetrik şifreleme olarak da adlandırılır. Haberleşen taraflardan her birinde birer çift anahtar bulunur. Bu anahtar çiftlerini oluşturan anahtarlardan biri gizli anahtar diğeri açık (gizli olmayan) anahtardır.

Kriptografinin kökeni muhtemelen insanlığın var oluşunun başlangıçlarına, insanların iletişim kurmayı öğrenmeye başlamalarına kadar uzanmaktadır [23, 24]. Kısacası insanlık ne zaman var olmuşsa kriptolojide o zaman var olmuştur. İlk başlarda insanlar sadece gizlilik ihtiyacını gerçekleştirmek için bu bilime ihtiyaç duydular. Sonraları ise devir değiştikçe ve teknoloji ilerledikçe kriptolojinin ilgi alanları da değişti, gelişti. Özellikle web teknolojisinin gelişmesiyle kriptolojiye olan ihtiyaç daha da arttı.

Kriptolojinin tarihi gelişimi şu şekildedir:

MÖ.1900 dolaylarında bir Mısırlı katip yazdığı kitabelerde standart dışı hiyeroglif işaretleri kullandı.

MÖ.60-50 Julius Caesar (MÖ 100-44) normal alfabedeki harflerin yerini değiştirerek oluşturduğu şifreleme yöntemini devlet haberleşmesinde kullandı. Bu yöntem açık metindeki her harfin alfabede kendisinden 3 harf sonraki harfle değiştirilmesine dayanıyordu.

725-790 Abu Abd al-Rahman al-Khalil ibn Ahmad ibn Amr ibn Tammam al Farahidi al-Zadi al Yahmadi, kriptografi hakkında bir kitap yazdı (Bu kitap kayıp durumdadır). Kitabı yazmasına ilham kaynağı olan, Bizans imparatoru için Yunanca yazılmış bir şifreli metni çözmesidir. Abu Abd al-Rahman, bu metni çözmek için ele geçirdiği şifreli mesajın başındaki açık metni tahmin etme yöntemini kullanmıştır.

1000-1200 Gaznelilerden günümüze kalan bazı dokümanlarda şifreli metinlere rastlanmıştır. Bir tarihçinin dönemle ilgili yazdıklarına göre yüksek makamlardaki

devlet görevlilerine yeni görev yerlerine giderken şahsa özel şifreleme bilgileri (belki şifreleme anahtarları) veriliyordu.

1586 Blaise de Vigenère (1523-1596) şifreleme hakkında bir kitap yazdı. İlk kez bu kitapta açık metin ve şifreli metin için otomatik anahtarlama yönteminden bahsedildi. Günümüzde bu yöntem hala DES (Data Encryption Standart – Simetrik Şifreleme Algoritması), kiplerinde kullanılmaktadır. 1623'de Sir Francis Bacon, 5-bit ikili kodlamayla karakter tipi değişikliğine dayanan sırörtme kullandı.

1790'da Thomas Jefferson, Strip Cipher makinesini geliştirdi. Bu makineyi temel alan M-138-A, ABD donanmasında 2. Dünya savaşında da kullandı.

1917'de Joseph Mauborgne ve Gilbert Vernam mükemmel şifreleme sistemi olan "one-time pad"'i buldular.

William Frederick Friedman, Riverbank Laboratuarlarında ABD için kriptoanaliz yaptı. 2. Dünya savaşında Japonlar'ın Purple Machine şifreleme sistemini çözdü.

2. Dünya savaşında Almanlar Arthur Scherbius tarafından icat edilmiş olan Enigma makinesini kullandılar. Bu makine Alan Turing ve ekibi tarafından çözüldü.

1970'lerde Horst Feistel (IBM) DES'in temelini oluşturan Lucifer algoritmasını geliştirdi.

1976'da DES (Data Encryption Standard), ABD tarafından FIPS 46(Federal Information Processing Standard) standardı olarak açıklandı.

1976 Whitfield Diffie ve Martin Hellman Açık Anahtar sistemini anlattıkları makaleyi yayınladılar.

1978'de Ronald L. Rivest, Adi Shamir ve Leonard M. Adleman: RSA algoritmasını buldular.

1985'de Neal Koblitz ve Victor S.Miller ayrı yaptıkları çalışmalarda eliptik eğri kriptografik (ECC) sistemlerini tarif ettiler.

1995'de SHA-1 (Secure Hash Algorithm) özet algortiması NIST tarafından standart olarak yayınlandı.

1997'de ABD'nin NIST (National Institute of Standards and Technology) kurumu DES'in yerini alacak bir simetrik algoritma için yarışma açtı.

2001'de NIST'in yarışmasını kazanan Belçikalı Joan Daemen ve Vincent Rijmen'e ait Rijndael algoritması, AES (Advanced Encryption Standard) adıyla standart haline getirildi.

3.2.2. Sırörtme

Petitcolas (1999) tanımıyla sırörtme bilgi gizleme yöntemlerinin en önemli alt dalıdır [25]. Bu yaklaşım, bir nesnenin içerisine bir verinin gizlenmesi olarak tanımlanabilir. Sırörtme konusu bir sonraki üst başlıkta ayrıntılı olarak anlatılacaktır.

3.2.3. Sayısal damgalama (digital watermarking)

Veri gizleme tekniklerin ticari kullanımı yavaş yavaş sayısal damgalamanın (watermarking) gelişmesini sağlamaktadır. Burada söz konusu olan gizli bilginin insan duyularından gizlenmesidir. 1990'ların başında imge filigrasyonu (damgalama) kavramı gelişmiş; Tanaka ve arkadaşları (1989, 1990) faks gibi ikili imgelerin korunması kavramını ortaya atmışlardır [26]. 1993 yılında Tirkel ve arkadaşları gerçekleştirdikleri uygulamaya; daha sonra "watermark" olarak birleştirilecek "water mark" ismini vermişlerdir [27]. Bilim çevreleri bu yıllarda konu üzerine daha fazla eğilmeye başlamış ve sayısal damgalama ile ilgili projeler başlatmış bulunmaktadır. Geliştirilen projeler; platformdan bağımsız, genel çözümler olarak ortaya konulmaktadır. Bunların yanında geliştirilen ürünlerin standartlaştırılmasını sağlamak amacıyla; standardizasyon kurumları da konu üzerinde yoğun araştırmalara girişmişlerdir. Bu konu ile ilgili ilk çalışmaları başlatan kurul DAVIC (The Digital

Audio Visual Council) başarıya ulaşamamıştır. Avrupa Birliği komisyonu da bu konu üzerinde bir çok uluslararası projenin oluşturulmasına destek sağlayarak konu ile ilgili şirket ve kişilerin bir araya gelmesini sağlamaktadır.

Dünya çapında telif haklarının korunması ve düzenlenmesi ile ilgili çalışmalar yapan ve hükümetler üstü bir kuruluş olan WIPO (World Intellectual Property Organization) sayısal damgalamanın yasal alanlarıyla ilgili çalışmalarını sürdürmektedir [28]. Günümüzde DICOM gibi imgelerden hasta ismi, tarih, şikayet ve hastalık detayları gibi bir çok bilgi elde edilebilmekte ve hasta mahremiyeti sağlanabilmektedir. Bugün sayısal damgalama endüstriden, standardizasyon kuruluşlarından ve kanuni birçok kuruluştan ilgi görmesine rağmen konu ile ilgili en geniş çalışmalar üniversitelere ve araştırma enstitülerine bağlı imge ve işaret işleme grupları tarafından gerçekleştirilmektedir [29].

3.2.4. Sayısal imzalama (Digital signature)

Sayısal imzalama, bir doküman sahibinin kendi özel anahtarı (private key) ile dokümanı imzalaması yani şifrelemesidir. Bu özel anahtardan üretilen açık anahtar (public key), dokümanın gönderileceği alıcı tarafında bulunur ve dokümanı açmakta kullanılır. Sayısal imzalama, özel ve açık anahtarın kullanıldığı damgalama olarak tanımlanabilir. Bir özel anahtar ile imzalanan doküman, sahibi hakkında bilgi de birlikte taşımış olur. Bazı otoritelerin, sayısal damgalama ile sayısal imzalamanın eş anlamlı olduğuna dair görüşlerine karşın bunları birbirinden ayrı tutan görüşler de vardır [30].

Uygulamada sayısal dokümanların imzalanması için çeşitli yazılımlar mevcuttur. Her kişi için oluşturulan açık ve özel imzalar, kendisine elektronik kartlarda verilir. Bu konuda, birçok yerde yasal düzenlemelerin ve teknik altyapının henüz sağlanmamış olmasından dolayı kullanımı yaygın değildir. Sayısal imza kullanılarak, gönderilecek dokümanın bütünlüğü sağlanır, göndericinin özel imzası kullanılarak şifrelendiğinden gönderici tarafından inkar edilemez ve göndericinin imzası taklit edilemeyeceğinden belirtilen göndericiden geldiği kesindir. Alıcı kendisine ait açık anahtarı kullanarak bu dokümanı açar, ancak göndericinin özel anahtarı olmadan üzerinde değişiklik yapamaz [31].

3.3. Sırörtme

3.3.1. Sırörtme kavramı ve terminolojisi

Sırörtme eski bir bilgi gizleme sanatıdır [25]. Sırörtme kelimesi kökleri “στεγαυος” ve “γραΦειν”’den gelen Yunan alfabesinden türetilmiştir. Tam olarak anlamı “kaplanmış yazı” (covered writing) demektir [32].

Sırörtme hakkında literatürde çeşitli tanımlar yapılmaktadır. Bir tanıma göre sırörtme gizli mesajın varlığının tespit edilemediği bir iletişim bilimidir [33]. Başka bir tanıma göre ise görünüşte zararsız bir mesajın içerisine veri saklama sanatıdır [34]. Bu bilim dalı askeri literatürde ise kısaca TRANSEC (Transmission Security – İletişim Güvenliği) olarak adlandırılmaktadır [35, 36].

Sırörtme bir nesnenin içerisine bir verinin gizlenmesi olarak tarif edilebilir. Metin, ses, sayısal resim, video dosyaları üzerine veri saklanabilir. Bu veriler metin dosyası olabileceği gibi, herhangi bir görüntü içerisine başka bir görüntüyü gizlemekte olasıdır. Yine aynı şekilde bir ses dosyasının içine bir metin dosyası da saklanabilmektedir [37, 38].

Özellikle 11 Eylül sonrası teröristlerce de gizli mesajlaşma için kullanıldığı düşünülen herhangi bir obje içerisine özelliklerini bozmadan başka bir verinin gizlenmesi mantığına dayanan veri gizleme tekniği artan bir ilgi konusu olmuştur.

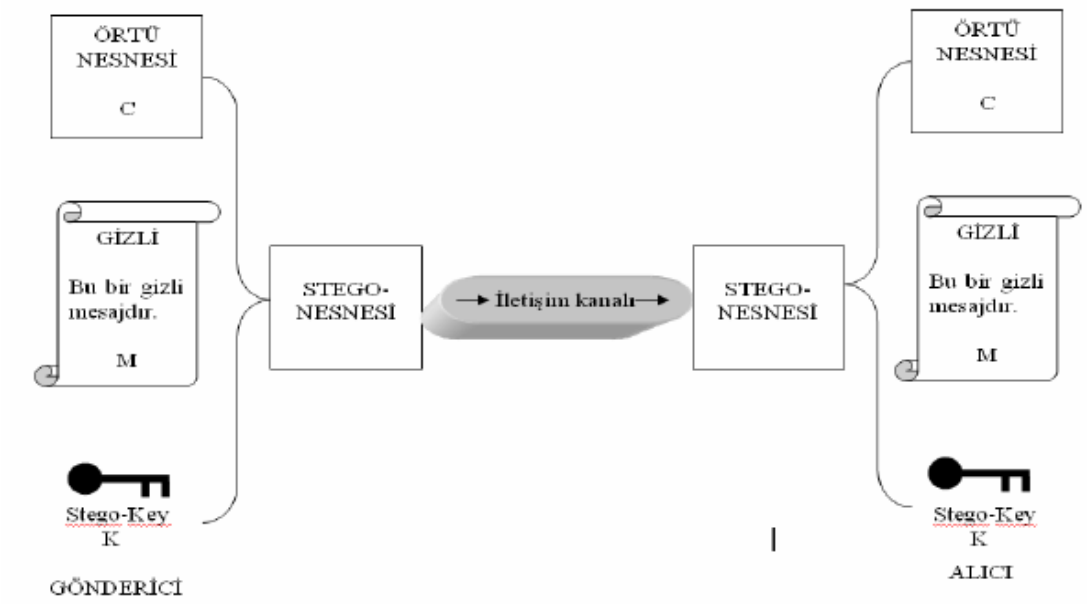
Bilimsel ortamda sırörtme çalışmaları 1983 yılında Simmons tarafından “Prisoner Problem” in [39] tanımlanması ile başlamaktadır. Bu problemde Alice ve Bob hapishanededir ve hapishaneden kaçmak için planlar yapmaktadırlar. Fakat bu planların gardiyan Willie’ye fark ettirilmeden yapılması gerekmektedir. Eğer Willie bunu fark ederse kaçma planları suya düşecektir. Bu nedenle de çeşitli gizli haberleşme yöntemleri geliştirilmesi gerekmektedir.

Bu yaklaşımda içine bilgi gizlenen ortama örtü dosyası (cover-image) veya örtü nesnesi (cover-object), oluşan ortama da gömü dosyası (stego-image) veya gömü

nesnesi (stego-object) denmektedir. Örtü anahtarı (stego-key) ise gizleme işlemi sırasında kullanılan güvenlik anahtarıdır. Bunu formülüze edecek olursak;

Örtü dosyası + Gizli veri + Gizli Anahtar = Gömü dosyası (3.1)

Ayrıca Şekil 3.3'de genel sırörtme modeli özetlenmektedir.



Şekil 3.3. Genel steganografi teknikleri

Sayısal görüntü sırörtmesinde kullanılan örtü nesneleri bmp, png, jpeg, gif gibi değişik formatlardaki renkli veya gri seviyeli imgeler olabilmektedir. Görüntü içerisinde veri saklama işlemi ya imge uzayında piksel değerlerinin değiştirilmesi ile ya da dönüşüm uzayı içerisinde belirli alanlara gizli verinin saklanması ile yapılmaktadır.

Sayısal görüntülerde sırörtme uygulamaları;

- En önemsiz bit yöntemi,
- Maskeleme ve filtreleme yöntemi,
- Algoritma ve dönüşüm yöntemleri

olmak üzere üç kategoride incelenebilir.

Sırörtme uygulamalarında ilk olarak kullanılan ve en basit yöntem olan en düşük değerlikli bit (LSB – Least Significant Bit) gömme yöntemidir [40, 41, 42]. Burada önerilen işlem genellikle sayısal resimler içerisinde en düşük değerlikli bitin gürültü tarafından maskelenerek değiştirilmesidir. Aslında renkli resim durumunda, mesaj gizleme için daha fazla oda bulunur; çünkü, her bir piksel kırmızı, yeşil ve maviden oluşan üçlü bir karışımdır. Yine iki veya daha fazla "en düşük değerlikli bit" yer değiştirilerek her bir pikselin kapasitesi artırılır. Ancak aynı zamanda istatistiksel olarak çözünebilirlik riski doğal olarak artacaktır. Sonuç olarak her bir özel stenografik tekniğin güvenli çalışması önemlidir ve neden güvenli olduğu tartışılır [17].

Maskeleme ve filtreleme yöntemleri İGS'nin sınırlarını kullanarak bakmayla anlaşılmayacak bölgeleri bulur ve gizleme işlemini gerçekleştirir. Bu teknik genellikle 24 bit ve gri seviyeli imgeler ile sınırlıdır. Gizlenecek veri sadece görüntünün gürültü taşıyabilen kısımlarına değil imgeyle bütünleşmiş olacak şekilde gömülür. Genellikle ticari amaçlar için kullanılmaktadır. Örneğin; televizyon kanallarının logoları, imgeler içindeki sayısal imzalar ve imgeler içindeki görünmeyen veya görünen yazılar bu tip uygulamalardandır.

Dönüşüm ve algoritma tekniklerinde ise gizlenecek veri/mesaj, taşıyıcı imge veya imgeler başka bir uzaya dönüştürüldükten sonra görüntünün belirli alanlarına gömülmektedir. Dönüşüm tekniklerinde sıklıkla kullanılan yöntemlerin başında Ayrık Kosinüs Dönüşümü (Discrete Cosinus Transform-DCT), Ayrık Frourer Dönüşümü (Discrete Fourier Transform-DFT) ve Ayrık Dalgacık Dönüşümü (Discrete Wavelet Transform-DWT) gelmektedir.

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 göndermiştir. Histiaeus kölelerinden birinin saçlarını kazıtır ve mesajını dövme şeklinde kölenin kafa

derisine işletir. Kölenin saçları yeterince büyüyünce onu Miletus'a oğlunun yanına gönderir. Bu tarihçi Herodotus'un bizlere aktardığı gizli yazma sanatı sırörtmenin ilk kullanıldığı yerlerden biridir. Bu gizleme sanatı, çağlar boyunca insanların ilgisiyle giderek gelişerek bilgi iletiminde bir bilim dalı haline gelmiştir. Eski Romalılar satırların arasına gözle görünmeyen mürekkepler kullanarak farklı gizleme teknikleri geliştirdiler. Bu mürekkepler doğal maddelerden, meyve özünden (limon gibi), idrar ve de sütten oluşmaktaydı. 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 geliştirdiler. Bu teknikte alfabede kullanılan noktalama işaretleri içerisine fotografik olarak ebatları küçültülmüş olan bir takım gizli mesajlar gömülür. Böylece Almanlar teknik çizimleri de içeren geniş miktarda basılı bilgi göndermeyi başarmışlardır. Savaş sırasında stenografinin 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 bilgi taşıması muhtemel dokümanların gönderilmesi yasaklanmıştır. Yine aynı dönemde SSCB tarafından da tüm uluslararası postalar casusluk aktivitelerine karşı sürekli olarak taranmaktaydı. Bilgisayar teknolojisinin hızlı ilerlemesi ile birlikte bu sınırlamaların tümü geçerliliğini kaybetmiştir. Günümüzde sırörtme telif hakkı korumasında olduğu gibi gizli veri transferinde de önemli bir araç olarak kullanılmaktadır.

3.3.3. Resim dosyaları için sırörtme teknikleri

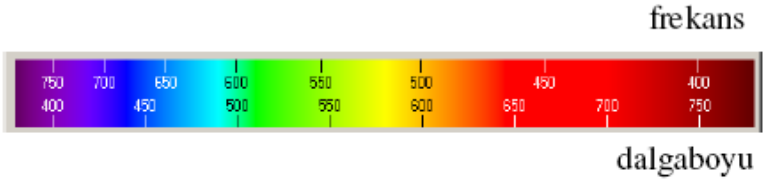
Resim içerisine veri gizleme yöntemleri iki kategoride sınıflandırılabilir. Bunlardan biri ‘uzay düzleminde’ veri gizleme, diğeri ise ‘frekans – düzleminde’ veri gizlemedir. Uzay-düzleminde veri gizleme işlemi sırasında, gizli veri resim pikselleri içerisine doğrudan yerleştirilir [43, 44, 45]. Frekans-düzleminde ise, öncelikle örtü dosyası, frekans-düzlemine dönüştürülür daha sonra gizlenecek veri taşıyıcı resmin dönüşüm katsayılarına yerleştirilir [46].

BÖLÜM 4. SAYISAL GÖRÜNTÜLERDE İNSAN GÖRME SİSTEMİ MERKEZLİ GELİŞTİRİLEN VERİ GÖMME ALGORİTMASI VE UYGULAMA YAZILIMI

4.1. Giriş

Tez çalışmasının ana kısmını oluşturan bu bölümde önceki çalışmalardan farklı olarak sayısal görüntü içindeki veri gömmeye uygun pikseller İGS'ne duyarlı yeni bir yaklaşımla belirlenmiştir. Yapılan çalışmada sadece veri gömme üzerinde durulmuştur. Gizli haberleşme süresince taşıyıcı görüntünün dışarıdan gelebilecek saldırılara maruz kalmaması için gizli veri algılanabilirliğinin en düşük seviyelerde tutulması çalışmanın asıl amacıdır. Bu sebepten dolayı sayısal görüntülerde İGS'nin fark edemediği görülebilir ışık dalga boyu değerleri kullanılmıştır.

Elektromanyetik tayfta görülebilir alanın dalgaboyu değerleri Şekil 4.1'de görüldüğü gibi her bir renk için farklıdır ve alt sınırı 350 nm ile mor, üst sınırı da 780 nm ile kırmızı temsil eder.



Şekil 4.1. Görülebilir ışık dalgaboyu tayfı

4.2. ASCII Kodu

1968 yılında ANSI (American National Standards Institute) tarafından geliştirilen ASCII (American Standard Code for Information Interchange); bilgisayar ağ ve sistemlerinde bilginin gösterilmesi/temsil edilmesi amacıyla kullanılan bir kod standardıdır. 7 bit olarak 0–127 arasında 128 değişik karakteri kapsamaktadır. Her bir karakter Tablo 4.1'de görüldüğü gibi 7 bitlik bir kod ile ifade edilir. Örneğin "a" harfi; 7 bit ASCII kodunda $(110\ 0001)_{ascii}$ olarak ifade edilmektedir. Benzer şekilde "8" rakamı $(011\ 1000)_{ascii}$, "+" işareti $(010\ 1011)_{ascii}$ kodları ile ifade edilmektedir.

Standart sembollerin dışında birtakım sembol ve şekillerinde ilave edilmesi ile 0–255 arasında genişletilmiş ASCII kodu oluşturulmuştur. 7 bit ASCII 0–127 arasında toplam 128 farklı karakteri içerirken, genişletilmiş 8 bit ASCII kodu 0–255 arasında 256 farklı karakteri bünyesinde barındırmaktadır.

Diğer bir ifadeyle 128–255 arasında toplam 128 yeni sembol ya da karakterin 7-bit ASCII ailesine katılmasıdır. Bunun dışında 1990'ların başında UNICODE olarak adlandırılan 16-bit kod geliştirilmiştir. ASCII alfanumerik karakterleri 0-127 arasında sayılar tarafından temsil ederek 7-bit ikili koda dönüştürmektedir. ASCII bilgisayarların farklı türdeki metin dosyalarının kolay transferine izin vermektedir. 7-bit ASCII kodu ve karakter karşılıları Tablo 4.1.'de görülmektedir.

Tablo 4.1. ASCII kodlarının 7-bit olarak karakter karşılıkları. (Standard No. X3.4 - 1968 of the ANSI,American National Standards Institute).

		$b_6b_5b_4$ (column)							
$b_3b_2b_1b_0$	Row (hex)	000 0	001 1	010 2	011 3	100 4	101 5	110 6	111 7
0000	0	NUL	DLE	SP	0	@	P	`	p
0001	1	SOH	DC1	!	1	A	Q	a	q
0010	2	STX	DC2	"	2	B	R	b	r
0011	3	ETX	DC3	#	3	C	S	c	s
0100	4	EOT	DC4	$	4	D	T	d	t
0101	5	ENQ	NAK	%	5	E	U	e	u
0110	6	ACK	SYN	&	6	F	V	f	v
0111	7	BEL	ETB	'	7	G	W	g	w
1000	8	BS	CAN	(	8	H	X	h	x
1001	9	HT	EM	)	9	I	Y	I	y
1010	A	LF	SUB	*	:	J	Z	j	z
1011	B	VT	ESC	+	;	K	[	k	{
1100	C	FF	FS	,	<	L	/	l	|
1101	D	CR	GS	-	=	M	]	m	}
1110	E	SO	RS	.	>	N	^	n	~
1111	F	SI	US	/	?	O	_	o	DEL

4.2.1. Kontrol kodları (control codes)

Tablo 4.2.'de ise ASCII kodlarının kontrol fonksiyonlarını oluşturan kodlar ve bunların anlamları ayrı bir grup olarak verilmiştir.

Tablo 4.2 ASCII kontrol kodlarının karşılıkları.

NUL	Null	DLE	Data link escape
SOH	Start of heading	DC1	Device control 1
STX	Start of text	DC2	Device control 2
ETX	End of text	DC3	Device control 3
EOT	End of transmission	DC4	Device control 4
ENQ	Enquiry	NAK	Negative acknowledge
ACK	Acknowledge	SYN	Synchronize
BEL	Bell	ETC	End transmitted block
BS	Backspace	CAN	Cancel
HT	Horizontal tab	EM	End of medium
LF	Line feed	SUB	Substitute
VT	Vertical tab	ESC	Escape
FF	Form feed	FS	File separator
CR	Carriage return	GS	Group separator
SO	Shift out	RS	Record separator
SI	Shift in	US	Unit separator
SP	Space	DEL	Delete or rubout

4.2.2. Genişletilmiş ASCII kodları

7−bit tüm karakterler için yeterli olmadığından ASCII kodu 8−bit yapılarak toplam 256 farklı kod dizilimi ve karşılığında Tablo 4.3'te görülen karakterler elde edilmiştir. ASCII alfanumerik karakterleri (harf, rakam, bir kaç sembol ve kontrol karakterleri) 0-127 arasında sayılar tarafından temsil ederek 7–bit ikili koda dönüştürmektedir. ASCII bilgisayarların farklı türdeki metin dosyalarının kolay transferine izin vermektedir.

Başlangıçta telem işlemler için tasarlanan ASCII, bilgisayar uygulamalarında oldukça geniş yer bulmuştur. 7-bit ikili sayı dizileri 128 fa rklı koddan birisi olarak sunulmaktadır. Böylece onluk (decimal) karşılıkları bir dizi halinde "72, 69, 76, 76, 79" kullanıldığında ASCII kod karşılığı olarak "h, e, l, l, o" kelimesini oluşturmaktadır. 1981 yılında kişisel bilgisayarların gelişmesiyle birlikte IBM (International Business Machines Company) firması tarafından mevcut karakter sayısı 256'ya çıkarılarak 8-bit (1 bayt) genişletilmiş ASCII kodu türetilmiştir. ABD

ve İngiltere dışında diğer ülke dillerindeki karşılanmayan karakterler sebebiyle biri diğeriyle uyumsuz, US-ASCII dışında birtakım farklı ulusal genişletilmiş kodlar türemiştir. Muhtemel bir kargaşaya son vermek üzere standardizasyona gitmek amacıyla 16-bit (2 Bayt) 65,536 karakter kümesinden oluşan UNICODE tasarlanmıştır. İçerisinde harf, rakam, özel karakterler ve diğer dilbilimsel sembol ve karakterleri içermekte olup günümüzün en önemli dillerinde kullanılmaktadır. İngilizce için Latin Alfabesi'ni, Rusça için Kiril Alfabesini, Yunanca, İbrani'ce ve Arap alfabelerini Avrupa, Afrika, Hint Yarımadası, Asya (Japonya, Kore, Çin) dillerine ait harf ve sembolleri kapsar.

Tablo 4.3. ASCII kodlarının 8-bit olarak karakter karşılıkları.

Extended ASCII Codes

128	Ç	144	É	161	í	177	▒	193	┴	209	╤	225	ß	241	±
129	ü	145	æ	162	ó	178	▓	194	┬	210	╥	226	Γ	242	≥
130	é	146	Æ	163	ú	179	│	195	├	211	╙	227	π	243	≤
131	â	147	ô	164	ñ	180	┤	196	─	212	╘	228	Σ	244	⌠
132	ä	148	ö	165	Ñ	181	╡	197	┼	213	╒	229	σ	245	⌡
133	à	149	ò	166	ª	182	╢	198	╞	214	╓	230	µ	246	÷
134	å	150	û	167	º	183	╖	199	╟	215	╫	231	τ	247	≈
135	ç	151	ù	168	¿	184	╕	200	╚	216	╪	232	Φ	248	°
136	ê	152	ÿ	169	⌐	185	╣	201	╔	217	┘	233	Θ	249	∙
137	ë	153	Ö	170	¬	186	║	202	╩	218	┌	234	Ω	250	·
138	è	154	Ü	171	½	187	╗	203	╦	219	█	235	δ	251	√
139	ï	156	£	172	¼	188	╝	204	╠	220	▄	236	∞	252	ⁿ
140	î	157	¥	173	¡	189	╜	205	═	221	▌	237	φ	253	²
141	ì	158	₧	174	«	190	╛	206	╬	222	▐	238	ε	254	■
142	Ä	159	ƒ	175	»	191	┐	207	╧	223	▀	239	∩	255	
143	Å	160	á	176	░	192	└	208	╨	224	α	240	≡		

4.2.3. EBCDIC kodları

ASCII kodu, kullanılan tek uluslararası format değildir IBM tarafından 1960'ların başında geliştirilip benimsenen EBCDIC (Extended Binary Coded Decimal Interchange Code) günümüz ana bilgisayarlarında halen kullanılmaktadır. En az 6 değişik forma sahip olup en yaygın olan türü Tablo 4.4'de verilmiştir.

Tablo 4.4. EBCDIC (Extended Binary Coded Decimal Interchange Code) kodlarının 8-bit olarak karakter karşılıkları

Dec	Hx	Oct	Char		Dec	Hx	Oct	Char	Dec	Hx	Oct	Char	Dec	Hx	Oct	Char
0	0	000	nul	(Null)	65	41	101		130	82	202	b	195	c3	303	C
1	1	001	soh	(Start of Heading)	66	42	102		131	83	203	c	196	c4	304	D
2	2	002	stx	(Start of Text)	67	43	103		132	84	204	d	197	c5	305	E
3	3	003	etx	(End of Text)	68	44	104		133	85	205	e	198	c6	306	F
4	4	004	pf	(Punch Off)	69	45	105		134	86	206	f	199	c7	307	G
5	5	005	ht	(Horizontal Tab)	70	46	106		135	87	207	g	200	c8	310	H
6	6	006	lc	(Lower Case)	71	47	107		136	88	210	h	201	c9	311	I
7	7	007	del	(Delete)	72	48	110		137	89	211	i	202	ca	312	
8	8	010	ge		73	49	111		138	8a	212		203	cb	313	
9	9	011	rlf		74	4a	112	¢	139	8b	213		204	cc	314	
10	a	012	smm	(Start of Manual Message)	75	4b	113	.	140	8c	214		205	cd	315	
11	b	013	vt	(Vertical Tab)	76	4c	114	>	141	8d	215		206	ce	316	
12	c	014	ff	(Form Feed)	77	4d	115	(	142	8e	216		207	cf	317	
13	d	015	cr	(Carriage Return)	78	4e	116	+	143	8f	217		208	d0	320	}
14	e	016	so	(Shift Out)	79	4f	117	|	144	90	220		209	d1	321	J
15	f	017	si	(Shift in)	80	50	120	&	145	91	221	j	210	d2	322	K
16	10	020	dle	(Data Link Escape)	81	51	121		146	92	222	k	211	d3	323	L
17	11	021	dc1	(Device Control 1)	82	52	122		147	93	223	l	212	d4	324	M
18	12	022	dc2	dc2 (Device Control 2)	83	53	123		148	94	224	m	213	d5	325	N
19	13	023	tm	(Tape Mark)	84	54	124		149	95	225	n	214	d6	326	O
20	14	024	res	(Restore)	85	55	125		150	96	226	o	215	d7	327	P
21	15	025	nl	(New Line)	86	56	126		151	97	227	p	216	d8	330	Q
22	16	026	bs	(Backspace)	87	57	127		152	98	230	q	217	d9	331	R
23	17	027	il	(Idle)	88	58	130		153	99	231	r	218	da	332	
24	18	030	can	(Cancel)	89	59	131		154	9a	232		219	db	333	
25	19	031	em	(End of Medium)	90	5a	132	!	155	9b	233		220	dc	334	
26	1a	032	cc	(Cursor Control)	91	5b	133	$	156	9c	234		221	dd	335	
27	1b	033	cu1	(Customer Use 1)	92	5c	134	*	157	9d	235		222	de	336	
28	1c	034	ifs	(Interchange File Separator)	93	5d	135	)	158	9e	236		223	df	337	
29	1d	035	igs	(Interchange Group Separator)	94	5e	136	;	159	9f	237		224	e0	340	\
30	1e	036	irs	(Interchange Record	95	5f	137		160	a0	240		225	e1	341	
31	1f	037	ius	(Interchange Unit Separator)	96	60	140	-	161	a1	241	~	226	e2	342	S
32	20	040	ds	(Digit Select)	97	61	141	/	162	a2	242	s	227	e3	343	T
33	21	041	sos	(Start of Significance)	98	62	142		163	a3	243	t	228	e4	344	U
34	22	042	fs	(Field Separator)	99	63	143		164	a4	244	u	229	e5	345	V
35	23	043			100	64	144		165	a5	245	v	230	e6	346	W
36	24	044	byp	(Bypass)	101	65	145		166	a6	246	w	231	e7	347	X
37	25	045	lf	(Line Feed)	102	66	146		167	a7	247	x	232	e8	350	Y
38	26	046	etb	(End of Transmission Block)	103	67	147		168	a8	250	y	233	e9	351	Z
39	27	047	esc	(Escape)	104	68	150		169	a9	251	z	234	ea	352	
40	28	050			105	69	151		170	aa	252		235	eb	353	
41	29	051			106	6a	152	|	171	ab	253		236	ec	354	
42	2a	052	sm	(Set Mode)	107	6b	153	,	172	ac	254		237	ed	355	
43	2b	053	cu2	(Customer Use 2)	108	6c	154	%	173	ad	255		238	ee	356	
44	2c	054			109	6d	155		174	ae	256		239	ef	357	
45	2d	055	enq	(Enquiry)	110	6e	156	<	175	af	257		240	f0	360	0
46	2e	056	ack	(Acknowledge)	111	6f	157	?	176	b0	260		241	f1	361	1
47	2f	057	bel	(Bell)	112	70	160		177	b1	261		242	f2	362	2
48	30	060			113	71	161		178	b2	262		243	f3	363	3
49	31	061			114	72	162		179	b3	263		244	f4	364	4
50	32	062	syn	(Synchronous Idle)	115	73	163		180	b4	264		245	f5	365	5
51	33	063			116	74	164		181	b5	265		246	f6	366	6
52	34	064	pn	(Punch On)	117	75	165		182	b6	266		247	f7	367	7
53	35	065	rs	(Reader Stop)	118	76	166		183	b7	267		248	f8	370	8
54	36	066	uc	(Upper Case)	119	77	167		184	b8	270		249	f9	371	9
55	37	067	eot	(End of Transmission)	120	78	170		185	b9	271		250	fa	372	|
56	38	070			121	79	171	`	186	ba	272		251	fb	373	
57	39	071			122	7a	172	:	187	bb	273		252	fc	374	
58	3a	072			123	7b	173	#	188	bc	274		253	fd	375	
59	3b	073	cu3	(Customer Use 3)	124	7c	174	@	189	bd	275		254	fe	376	
60	3c	074	dc4	(Device Control 4)	125	7d	175	'	190	be	276		255	ff	377	eo
61	3d	075	nak	(Negative Acknowledge)	126	7e	176	=	191	bf	277					
62	3e	076			127	7f	177	"	192	c0	300	{				
63	3f	077	sub	(Substitute)	128	80	200		193	c1	301	A				
64	40	100	Sp	(Space)	129	81	201	a	194	c2	302	B				

4.3. Bilinen RGB Değerlerinden Dalgaboyu Hesaplama

Her piksele ait RGB değerlerinden dalgaboyu değerinin hesaplanması üç aşamalı bir süreçtir.

1- Pikselin sahip olduğu RGB değerlerinin CIE – XYZ formuna dönüştürülmesi için ilk olarak bir lineer matris dönüşümü yapılır. X, Y, Z değerleri bizim tristimulus değerlerimizdir. Tristimulus değeri her bir rengi oluşturan üç birincil rengin (R –

kırmızı, G – yeşil, B – mavi) miktarıdır. Aşağıda sahip bilinen RGB değerlerinden X, Y, Z tristumulus değerlerini hesaplayan formüller verilmiştir. Ayrıca Uluslararası Aydınlanma Komisyonu CIE–1931 için çeşitli RGB mekanların kolorimetrik özelliklerine göre RGB renk uzayından CIE 1931 XYZ değerlerine dönüşümde kullanılacak matris çarpan katsayılarını Tablo 4.5'de görüldüğü gibi belirlemiştir.

$$\begin{vmatrix} X \\ Y \\ Z \end{vmatrix} = \begin{vmatrix} Xr & Xg & Xb \\ Yr & Yg & Yb \\ Zr & Zg & Zb \end{vmatrix} * \begin{vmatrix} R \\ G \\ B \end{vmatrix} \quad (4.1)$$

Buradan RGB değerlerini eşitliğin diğer tarafına çekebilmek için matrisin tersi alınır.

$$\begin{vmatrix} R \\ G \\ B \end{vmatrix} = \begin{vmatrix} Xr & Xg & Xb \\ Yr & Yg & Yb \\ Zr & Zg & Zb \end{vmatrix}^{(-1)} * \begin{vmatrix} X \\ Y \\ Z \end{vmatrix} \quad (4.2)$$

Tablo 4.5'de farklı RGB mekanları için verilen katsayılardan sRGB olanı seçip denklemde yerine yerleştirilir. sRGB uzayının seçilmesinin sebebi web uygulamalarında daha çok bu standardın kullanılmasıdır.

$$\begin{vmatrix} X \\ Y \\ Z \end{vmatrix} = \begin{vmatrix} 0.4124 & 0.3576 & 0.1805 \\ 0.2126 & 0.7152 & 0.0722 \\ 0.0193 & 0.1192 & 0.9505 \end{vmatrix} * \begin{vmatrix} R \\ G \\ B \end{vmatrix} \quad (4.3)$$

Lineer dönüşüm de yapıldığı zaman;

$$\begin{aligned} X &= 0.4124*R + 0.3576*G + 0.1805*B \\ Y &= 0.2126*R + 0.7152*G + 0.0722*B \\ Z &= 0.0193*R + 0.1192*G + 0.9505*B \end{aligned} \quad (4.4)$$

eşitlikleri elde edilir.

2- Yukarıda formüller yardımıyla bulunan X, Y ve Z değerlerinden x, y ve z kromatisite koordinat değerleri aşağıdaki formül yardımıyla bulunur.

$$x = \frac{X}{X + Y + Z}$$

$$y = \frac{Y}{X + Y + Z} \tag{4.5}$$

$$z = \frac{Z}{X + Y + Z} = 1 - x - y$$

Tablo 4.5. Farklı RGB mekanları için verilen katsayı değerleri [47]

RGB space	Primaries / Phosphors R	G	B	White Illuminant	XYZ to RGB matrix			RGB to XYZ matrix			Power Functions Exponents, i.e. gamma (γ) encoding gamma "detailed"		γ for each element of the imaging chain	
Adobe (1998)	Adobe RGB (1998)			D65	XYZ to RGB (Adobe)			RGB (Adobe) to XYZ			N.A.		"simple" encoding:	0,45 (2,20)
x :	0,6400	0,2100	0,1500	0,3127	2,0414	-0,5649	-0,3447	0,5767	0,1856	0,1882			LUT:	1
y :	0,3300	0,7100	0,0600	0,3290	-0,9693	1,8760	0,0416	0,2974	0,6273	0,0753			CRT:	0,40 (2,50)
z :	0,0300	0,0800	0,7900	0,3583	0,0134	-0,1184	1,0154	0,0270	0,0707	0,9911			overall:	1,14
Apple	Trinitron			D65	XYZ to RGB (Apple)			RGB (Apple) to XYZ			N.A.		"simple" encoding:	0,56 (1,80)
x :	0,6250	0,2800	0,1550	0,3127	2,9516	-1,2894	-0,4738	0,4497	0,3162	0,1845			LUT:	0,69 (1,45)
y :	0,3400	0,5950	0,0700	0,3290	-1,0851	1,9909	0,0372	0,2447	0,6720	0,0833			CRT:	0,40 (2,50)
z :	0,0350	0,1250	0,7750	0,3583	0,0855	-0,2695	1,0913	0,0252	0,1412	0,9225			overall:	0,96
CIE	CIE RGB			E	XYZ to RGB (CIE)			RGB (CIE) to XYZ			N.A.		"simple" encoding:	0,45 (2,20)
x :	0,7350	0,2740	0,1670	0,3333	2,3707	-0,9001	-0,4706	0,4887	0,3107	0,2006			LUT:	1
y :	0,2650	0,7170	0,0090	0,3333	-0,5139	1,4253	0,0886	0,1762	0,8130	0,0108			CRT:	0,40 (2,50)
z :	0,0000	0,0090	0,8240	0,3333	0,0053	-0,0147	1,0094	0,0000	0,0102	0,9898			overall:	1,14
ColorMatch	P22-EBU			D50	XYZ to RGB (P22-EBU)			RGB (P22-EBU) to XYZ			N.A.		"simple" encoding:	0,56 (1,80)
x :	0,6300	0,2950	0,1500	0,3457	2,6423	-1,2234	-0,3930	0,5093	0,3209	0,1340			LUT and CRT:	0,56 (1,80) (combined)
y :	0,3400	0,6050	0,0750	0,3585	-1,1120	2,0590	0,0160	0,2749	0,6581	0,0670			overall:	1,00
z :	0,0300	0,1000	0,7750	0,2958	0,0822	-0,2807	1,4560	0,0243	0,1088	0,6922				
HDTV (HD-CIF)	HDTV (ITU-R BT.709-5)			D65	XYZ to RGB (R709)			RGB (R709) to XYZ			offset:	0,099	"simple" encoding:	0,51 (1,95)
x :	0,6400	0,3000	0,1500	0,3127	3,2405	-1,5371	-0,4985	0,4125	0,3576	0,1804	γ :	0,45	LUT:	1
y :	0,3300	0,6000	0,0600	0,3290	-0,9693	1,8760	0,0416	0,2127	0,7152	0,0722	transition:	0,018	CRT:	0,40 (2,50)
z :	0,0300	0,1000	0,7900	0,3583	0,0556	-0,2040	1,0572	0,0193	0,1192	0,9503	slope:	4,5	overall:	1,28
NTSC (1953)	NTSC (1953)			C	XYZ to RGB (NTSC)			RGB (NTSC) to XYZ			offset:	0,099	"simple" encoding:	0,51 (1,95)
x :	0,6700	0,2100	0,1400	0,3101	1,9100	-0,5325	-0,2882	0,6069	0,1735	0,2003	γ :	0,45	LUT:	1
y :	0,3300	0,7100	0,0800	0,3161	-0,9847	1,9992	-0,0283	0,2989	0,5866	0,1145	transition:	0,018	CRT:	0,40 (2,50)
z :	0,0000	0,0800	0,7800	0,3738	0,0583	-0,1184	0,8976	0,0000	0,0661	1,1162	slope:	4,5	overall:	1,28
PAL / SECAM	EBU 3213 / ITU			D65	XYZ to RGB (EBU)			RGB (EBU) to XYZ			offset:	0,099	"simple" encoding:	0,51 (1,95)
x :	0,6400	0,2900	0,1500	0,3127	3,0629	-1,3932	-0,4758	0,4306	0,3415	0,1783	γ :	0,45	LUT:	1
y :	0,3300	0,6000	0,0600	0,3290	-0,9693	1,8760	0,0416	0,2220	0,7066	0,0713	transition:	0,018	CRT:	0,40 (2,50)
z :	0,0300	0,1100	0,7900	0,3583	0,0679	-0,2289	1,0694	0,0202	0,1296	0,9391	slope:	4,5	overall:	1,28
SGI	Trinitron			D65	XYZ to RGB (SGI)			RGB (SGI) to XYZ			N.A.		"simple" encoding:	0,68 (1,47)
x :	0,6250	0,2800	0,1550	0,3127	2,9516	-1,2894	-0,4738	0,4497	0,3162	0,1845			LUT:	0,59 (1,70)
y :	0,3400	0,5950	0,0700	0,3290	-1,0851	1,9909	0,0372	0,2447	0,6720	0,0833			CRT:	0,35 (2,86)
z :	0,0350	0,1250	0,7750	0,3583	0,0855	-0,2695	1,0913	0,0252	0,1412	0,9225			overall:	1,14
SMPTE-240M	SMPTE-C			D65	XYZ to RGB (240M)			RGB (240M) to XYZ			offset:	0,112	"simple" encoding:	0,52 (1,92)
x :	0,6300	0,3100	0,1550	0,3127	3,5054	-1,7395	-0,5440	0,3936	0,3652	0,1916	γ :	0,45	LUT:	1
y :	0,3400	0,5950	0,0700	0,3290	-1,0691	1,9778	0,0352	0,2124	0,7010	0,0865	transition:	0,023	CRT:	0,40 (2,50)
z :	0,0300	0,0950	0,7750	0,3583	0,0563	-0,1970	1,0502	0,0187	0,1119	0,9582	slope:	4,0	overall:	1,30
SMPTE-C	SMPTE-C			D65	XYZ to RGB (SMPTE-C)			RGB (SMPTE-C) to XYZ			offset:	0,099	"simple" encoding:	0,51 (1,95)
x :	0,6300	0,3100	0,1550	0,3127	3,5054	-1,7395	-0,5440	0,3936	0,3652	0,1916	γ :	0,45	LUT:	1
y :	0,3400	0,5950	0,0700	0,3290	-1,0691	1,9778	0,0352	0,2124	0,7010	0,0865	transition:	0,018	CRT:	0,40 (2,50)
z :	0,0300	0,0950	0,7750	0,3583	0,0563	-0,1970	1,0502	0,0187	0,1119	0,9582	slope:	4,5	overall:	1,28
sRGB	HDTV (ITU-R BT.709-5)			D65	XYZ to RGB (R709)			RGB (R709) to XYZ			offset:	0,055	"simple" encoding:	0,45 (2,20)
x :	0,6400	0,3000	0,1500	0,3127	3,2405	-1,5371	-0,4985	0,4125	0,3576	0,1804	γ :	0,42	LUT:	1
y :	0,3300	0,6000	0,0600	0,3290	-0,9693	1,8760	0,0416	0,2127	0,7152	0,0722	transition:	0,003	CRT:	0,40 (2,50)
z :	0,0300	0,1000	0,7900	0,3583	0,0556	-0,2040	1,0572	0,0193	0,1192	0,9503	slope:	12,92	overall:	1,14
Wide Gamut	700 / 525 / 450 nm			D50	XYZ to RGB (Wide)			RGB (Wide) to XYZ			N.A.		"simple" encoding:	0,45 (2,20)
x :	0,7347	0,1152	0,1566	0,3457	1,4625	-0,1845	-0,2734	0,7164	0,1010	0,1468			LUT:	1
y :	0,2653	0,8264	0,0177	0,3585	-0,5228	1,4479	0,0681	0,2587	0,7247	0,0166			CRT:	0,40 (2,50)
z :	0,0000	0,0584	0,8257	0,2958	0,0346	-0,0958	1,2875	0,0000	0,0512	0,7740			overall:	1,14

3- Son adımda ise 5 nm aralıklarla her bir dalgaboyuna ait x, y ve z değerlerinin karşılıkları aşağıdaki yazılım ile hesaplanır [48].

```
NM_TO_XYZ converts a light wavelength to CIE xyz chromaticities.
!       x = X / ( X + Y + Z ), y = Y / ( X + Y + Z ), z = Z / ( X + Y + Z )
Input, real W, the wavelength of the pure light signal, in nanometers.
Input wavelengths outside this range will result in X = Y = Z = 0.
Output, real X, Y, Z
```

```
implicit none
integer, parameter :: ndat = 81
real, save, dimension ( ndat ) :: ldat = (/ &
    380.0, 385.0, 390.0, 395.0, 400.0, &
    405.0, 410.0, 415.0, 420.0, 425.0, &
    430.0, 435.0, 440.0, 445.0, 450.0, &
    455.0, 460.0, 465.0, 470.0, 475.0, &
    480.0, 485.0, 490.0, 495.0, 500.0, &
    505.0, 510.0, 515.0, 520.0, 525.0, &
    530.0, 535.0, 540.0, 545.0, 550.0, &
    555.0, 560.0, 565.0, 570.0, 575.0, &
    580.0, 585.0, 590.0, 595.0, 600.0, &
    605.0, 610.0, 615.0, 620.0, 625.0, &
    630.0, 635.0, 640.0, 645.0, 650.0, &
    655.0, 660.0, 665.0, 670.0, 675.0, &
    680.0, 685.0, 690.0, 695.0, 700.0, &
    705.0, 710.0, 715.0, 720.0, 725.0, &
    730.0, 735.0, 740.0, 745.0, 750.0, &
    755.0, 760.0, 765.0, 770.0, 775.0, &
    780.0E+00 /)
  real w
  real x
  real, save, dimension ( ndat ) :: xdat = (/ &
    0.1741, 0.1740, 0.1738, 0.1736, 0.1733, &
    0.1730, 0.1726, 0.1721, 0.1714, 0.1703, &
    0.1689, 0.1669, 0.1644, 0.1611, 0.1566, &
    0.1510, 0.1440, 0.1355, 0.1241, 0.1096, &
    0.0913, 0.0687, 0.0454, 0.0235, 0.0082, &
    0.0039, 0.0139, 0.0389, 0.0743, 0.1142, &
    0.1547, 0.1929, 0.2296, 0.2658, 0.3016, &
    0.3373, 0.3731, 0.4087, 0.4441, 0.4788, &
    0.5125, 0.5448, 0.5752, 0.6029, 0.6270, &
    0.6482, 0.6658, 0.6801, 0.6915, 0.7006, &
    0.7079, 0.7140, 0.7190, 0.7230, 0.7260, &
    0.7283, 0.7300, 0.7311, 0.7320, 0.7327, &
    0.7334, 0.7340, 0.7344, 0.7346, 0.7347, &
    0.7347, 0.7347, 0.7347, 0.7347, 0.7347, &
    0.7347, 0.7347, 0.7347, 0.7347, 0.7347, &
    0.7347, 0.7347, 0.7347, 0.7347, 0.7347, &
    0.7347 /)
  real y
  real, save, dimension ( ndat ) :: ydat = (/ &
    0.0050, 0.0050, 0.0049, 0.0049, 0.0048, &
    0.0048, 0.0048, 0.0048, 0.0051, 0.0058, &
    0.0069, 0.0086, 0.0109, 0.0138, 0.0177, &
```

```
    0.0227, 0.0297, 0.0399, 0.0578, 0.0868, &
    0.1327, 0.2007, 0.2950, 0.4127, 0.5384, &
    0.6548, 0.7502, 0.8120, 0.8338, 0.8262, &
    0.8059, 0.7816, 0.7543, 0.7243, 0.6923, &
    0.6589, 0.6245, 0.5896, 0.5547, 0.5202, &
    0.4866, 0.4544, 0.4242, 0.3965, 0.3725, &
    0.3514, 0.3340, 0.3197, 0.3083, 0.2993, &
    0.2920, 0.2859, 0.2809, 0.2770, 0.2740, &
    0.2717, 0.2700, 0.2689, 0.2680, 0.2673, &
    0.2666, 0.2660, 0.2656, 0.2654, 0.2653, &
    0.2653, 0.2653, 0.2653, 0.2653, 0.2653, &
    0.2653, 0.2653, 0.2653, 0.2653, 0.2653, &
    0.2653, 0.2653, 0.2653, 0.2653, 0.2653, &
    0.2653 /)
  real z
  real, save, dimension ( ndat ) :: zdat = (/ &
    0.8209, 0.8210, 0.8213, 0.8215, 0.8219, &
    0.8222, 0.8226, 0.8231, 0.8235, 0.8239, &
    0.8242, 0.8245, 0.8247, 0.8251, 0.8257, &
    0.8263, 0.8263, 0.8246, 0.8181, 0.8036, &
    0.7760, 0.7306, 0.6596, 0.5638, 0.4534, &
    0.3413, 0.2359, 0.1491, 0.0919, 0.0596, &
    0.0394, 0.0255, 0.0161, 0.0099, 0.0061, &
    0.0038, 0.0024, 0.0017, 0.0012, 0.0010, &
    0.0009, 0.0008, 0.0006, 0.0006, 0.0005, &
    0.0004, 0.0002, 0.0002, 0.0002, 0.0001, &
    0.0001, 0.0001, 0.0001, 0.0000, 0.0000, &
    0.0000, 0.0000, 0.0000, 0.0000, 0.0000, &
    0.0000, 0.0000, 0.0000, 0.0000, 0.0000, &
    0.0000, 0.0000, 0.0000, 0.0000, 0.0000, &
    0.0000, 0.0000, 0.0000, 0.0000, 0.0000, &
    0.0000, 0.0000, 0.0000, 0.0000, 0.0000, &
    0.0000 /)
  if ( w >= 380.0E+00 .and. w <= 780.0E+00 ) then
    call interp ( ndat, w, ldat, x, xdat )
    call interp ( ndat, w, ldat, y, ydat )
    call interp ( ndat, w, ldat, z, zdat )
  else
    x = 0.0E+00
    y = 0.0E+00
    z = 0.0E+00
  end if
  return
end
```

4.4. Geliştirilen Veri Gömme Uygulamasının Genel Çalışma Prensibi

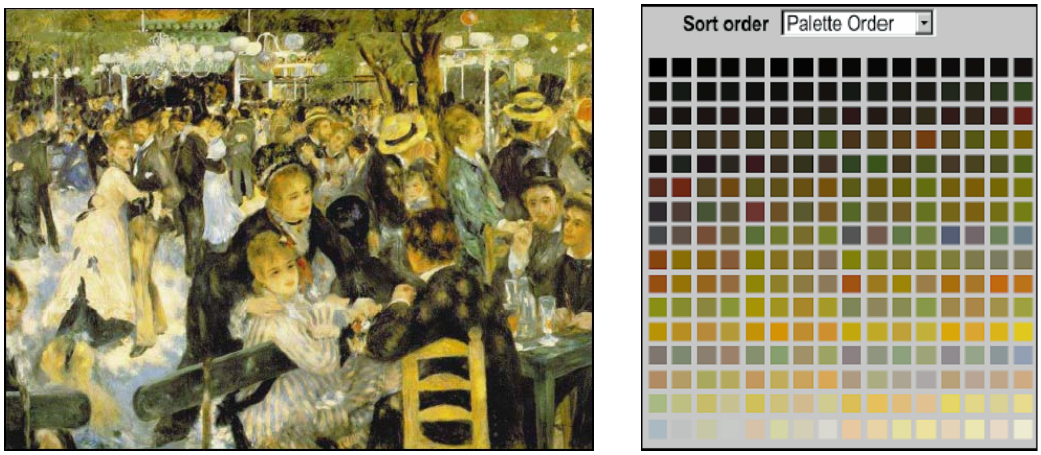
Bu çalışmada İGS'nin zaafından faydalanarak yeni bir veri gömme yöntemi geliştirilmiştir. Taşıyıcı görüntü içerisinde veri gömme yapılabilecek bölgelerin belirlenmesinde daha önceki yapılmış çalışmalardan farklı bir yol izlenmiştir. Algılanabilirliği daha da düşürerek neredeyse imkansız hale getirmek için piksel seçiminde ışık dalgaboyu yaklaşımı kullanılmıştır.

4.4.1. Veri gömme işlemi

Gizli bilgiyi bir resme gömme işleminde iki dosya söz konusudur. Örtü resim (cover image) olarak adlandırılan ilk dosya, gizli bilgiyi saklayacak resim dosyasıdır. İkinci dosya ise gizlenecek bilgi (gömü verisi) olan mesajdır. Mesaj açık metin (plain text), şifreli metin (chipher text), başka resimler veya bit dizisi içinde saklanabilecek başka bir veri olabilir. Gömme işlemi sonucunda örtü resim ve gömülü mesajın oluşturduğu dosyaya sırlı resim (stego image) adı verilmektedir.

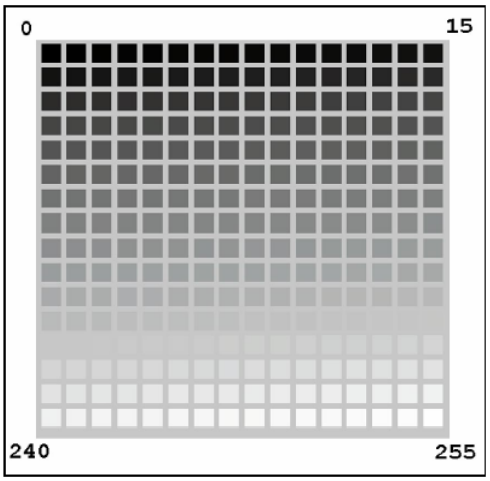
Birçok stenografi yazılımı JPEG formatının kullanımını tavsiye etmezken, 24–bit BMP resimlerin kullanılmasını tercih etmektedir. Diğer alternatifler ise gri tonlamalı ve 256 renk resimlerdir. Söz edilen 256 renk resimlerin en yaygın kullanılanı GIF formatıdır.

GIF formatlı resim dosyaları ve 8–bit BMP resimlerde her piksel 1–bayt ile gösterilir. Bu tip resimler görüntüde kullanılan renkleri içeren 256 renkli bir palet taşırlar. Her piksel bu palette bir renge karşılık gelen 1 bayt'lık değeri taşımaktadır (Şekil 4.2).



Şekil 4.2. 256 renk resim ve kullandığı palet

Birçok stenografi uzmanı da 256 gri tonlamalı resimlerin kullanımını önermektedir [38]. Gri tonlamalı resimlerin tercih edilme sebebi, koyuluğun her değer için çok küçük farklarla artmasıdır. Bu tip resimler de palet içermektedir (Şekil 4.3) ve palet değerlerindeki küçük değişimler gözün fark edemeyeceği kadar azdır. Bazı gri tonlamalı resimler 4–bitliktir ve 16 farklı gri ton içermektedir. Bu yapıdaki resimlerde değişimler daha belirgin olmaktadır.



Şekil 4.3. 256 gri tonlamalı resme ait palet

4.4.2. Gizli verinin geri elde edilmesi

Gömülü verinin geri elde edilme işlemi sırlı görüntünün program tarafından okunması ile başlanır. İlk işlem olarak 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 sırlı resmin piksellerinden gizlenmiş veriler alınır. Bu işlem gömü dosyası boyutuna ulaşılıncaya kadar devam eder. Gömü dosyasının boyutuna ulaşıldığı zaman geri elde edilen gizli veri kaydedilir ve veri geri elde etme işlemi sonlandırılır.

4.5. Geliştirilen Veri Gömme Yöntemi

Tez çalışmasında öncelikle veri gömülebilecek uygun piksellerin belirlenmesi gerçekleştirilir. Piksel seçiminde algılanabilirliği en aza indirgemek için dalgaboyu yöntemi geliştirilmiştir. Dalgaboyu yöntemi hakkında [4, 49]' lerde bugüne kadar yapılmış çalışmalara ulaşılabilir. Bu çalışmayla dalgaboyu yöntemini bir adım daha ileri götürerek veri gizleme yöntemleri için yeni bir algoritma sunulmuştur.

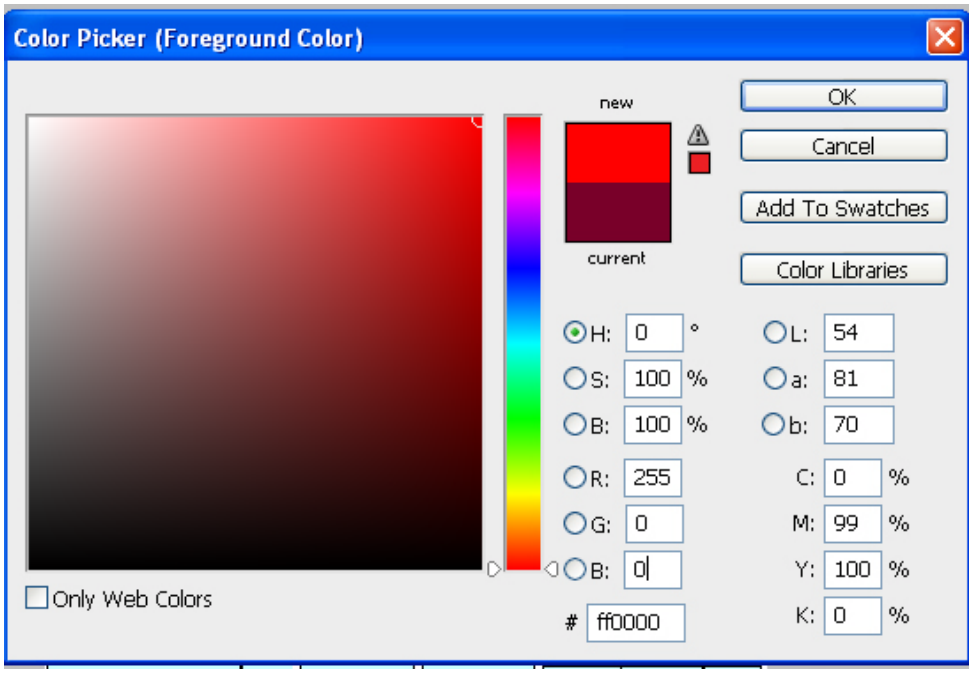
4.5.1. Dalgaboyu yöntemi

Daha önce de söylenildiği gibi dalgaboyu yöntemi ile ilgili yapılan araştırmalar [4,49] diğer yöntemlere göre daha azdır. Dalgaboyu yönteminde İGS'nin zaafından faydalanılarak veri gömme işlemi gerçekleştirilir. Elektromanyetik tayfta İGS'nin algıladıgı renk dalgaboyu aralığı, yani görülebilir ışık alanı bilgisinden faydalanarak veri gizlenecek piksellerin belirlenmesi bu yöntemin temelini oluşturmaktadır.

İçerisine veri gömülmek istenen sayısal görüntünün piksellerinde görülebilir ışık aralığının sınır dalgaboyu değerlerine (350nm−780nm) yakın renklere sahip pikseller belirlenir. Başka bir ifadeyle, 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. Bu yöntemde, her pikselin ait olduğu renk dalgaboyu değeri bulunur. Her bir pikselin sahip olduğu RGB değerinden dalgaboyunu hesaplama işlemini Bölüm 4.3'de ayrıntılı bir şekilde anlatılmıştır. Ayrıca internette kolayca bulunabilen renk kodlarının listelerinden de faydalanmak mümkündür. Bu örnek tablolardan biri de Tablo 4.6'da verilmiştir.

Tablo 4.6 Mor ve kırmızı renklerin yaklaşık dalgaboyu değerleri

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



Şekil 4.4. R = 255 G = 0 ve B = 0 değerlerine sahip olan rengin seçilmesi.

Örneğin, yukarıda görüldüğü gibi RGB değerleri; R = 255, G = 0, B = 0 olan bir pikselin dalgaboyu değeri hesaplamasını inceleyelim. Öncelikle Formül 4.4'de, verilen ifadeleri yerlerine koyarak X, Y ve Z değerleri bulunur.

```
X = 0.4124*255 + 0.3576*0 + 0.1805*0
Y = 0.2126*255 + 0.7152*0 + 0.0722*0
Z = 0.0193*255 + 0.1192*0 + 0.9505*0
```

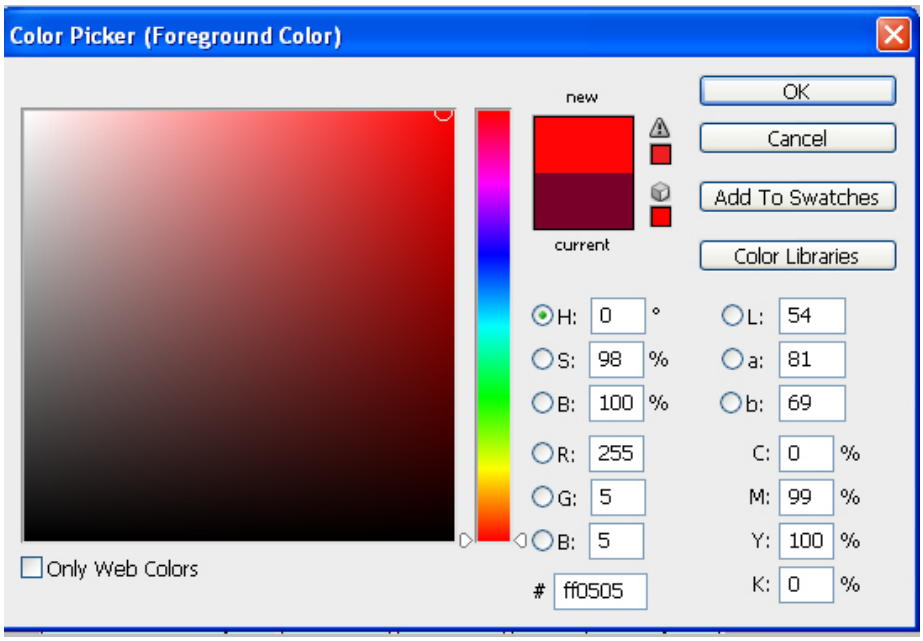
X = 105,162 Y = 54,213 Z = 4,9215 olarak elde edilir. Daha sonrasında ise x, y ve z değerleri hesaplanır.

x = X / X + Y + Z x = 105,162 / 164,2965 x = 0,6400

y = Y / X + Y + Z y = 54,213 / 164,2965 y = 0,3300

z = 1 – x – y z = 1 – 0,6400 – 0,3300 z = 0,0300

Bu x, y ve z değerlerine sahip olan dalgaboyu değeri Tablo 4.5'den bakıldığı zaman 780 nm çıkmaktadır.



Şekil 4.5. R = 255 G = 5 ve B = 5 değerlerine sahip olan rengin seçilmesi

Şimdi de Şekil 4.5' deki gibi R = 255 G = 5 ve B = 5 olan değerlerinin dalgaboyu hesaplamasını inceleyelim.

```
X = 0.4124*255 + 0.3576*5 + 0.1805*5
Y = 0.2126*255 + 0.7152*5 + 0.0722*5
Z = 0.0193*255 + 0.1192*5 + 0.9505*5
```

X = 107,8525 Y = 58,15 Z = 10,27 olarak elde edilir.

x = X / X + Y + Z x = 107,8525 / 176,2725 x = 0,6118

y = Y / X + Y + Z y = 58,15 / 176,2725 y = 0,3298

z = 1 – x – y z = 1 – 0,6118 – 0,3298 z = 0,0584

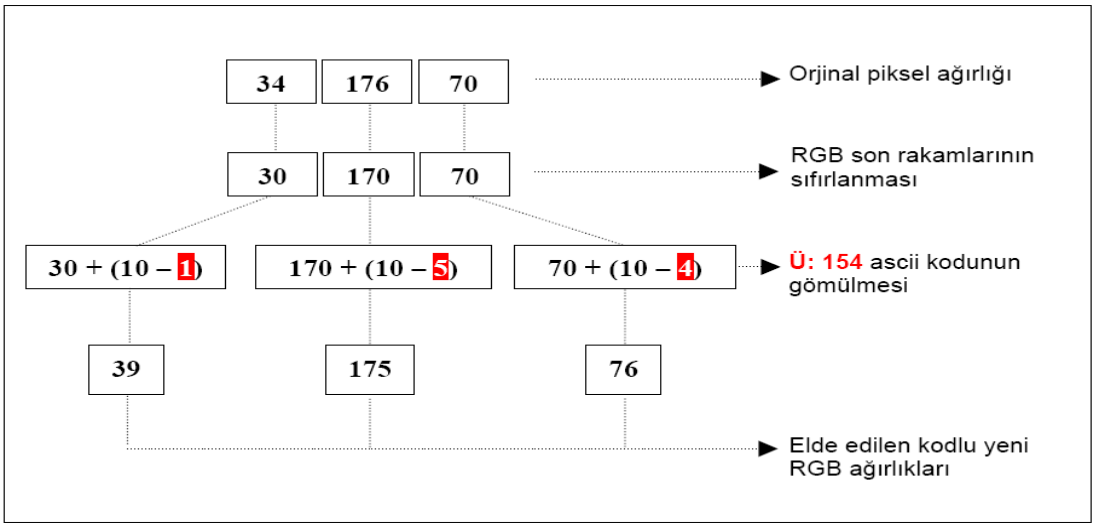
4.6. Sayısal Görüntüler İçin Veri Kodlama Yöntemleri

4.6.1. LSB kodlama

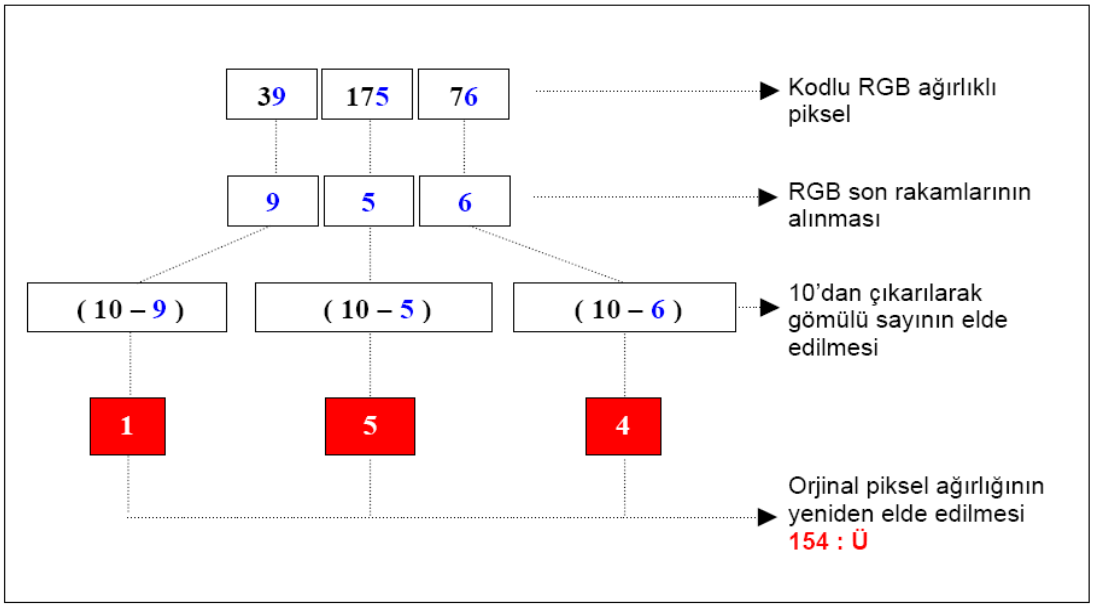
8–bitlik bir resmin her pikseli ‘1’ ve ‘0’ bitlerinden oluşmaktadır ve bu bitlerin 2^8 yani 256 renk meydana getirdiği bilinmektedir. İkili sayı sistemine göre 10110111 sayısını ele alalım. Bu sayının onlu sistemdeki karşılığı hesaplandığında 183 sayısı elde edilir. Sondaki bitin ‘1’ veya ‘0’ olması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

4.6.2. RGB kodlama

İlk olarak Akar (2005)’ın önerdiği bu sistemde örneğin, RGB ağırlıkları (38, 176, 70) olan bir pikselin içerisine “Ü” harfinin ASCII karşılığı olan “(10011010)ascii = 154” verisinin gömülmesi işlemi ve gömülü bilginin yeniden elde edilmesi işlem süreci sırasıyla Şekil 4.6 ve Şekil 4.7’de görülmektedir [17].



Şekil 4.6. Bir piksel içerisine bir ASCII kodunun gömülmesi işlem süreci [17].



Şekil 4.7. Bir piksel içerisinden gömülü bir ASCII kodun çıkarılması işlemi [17].

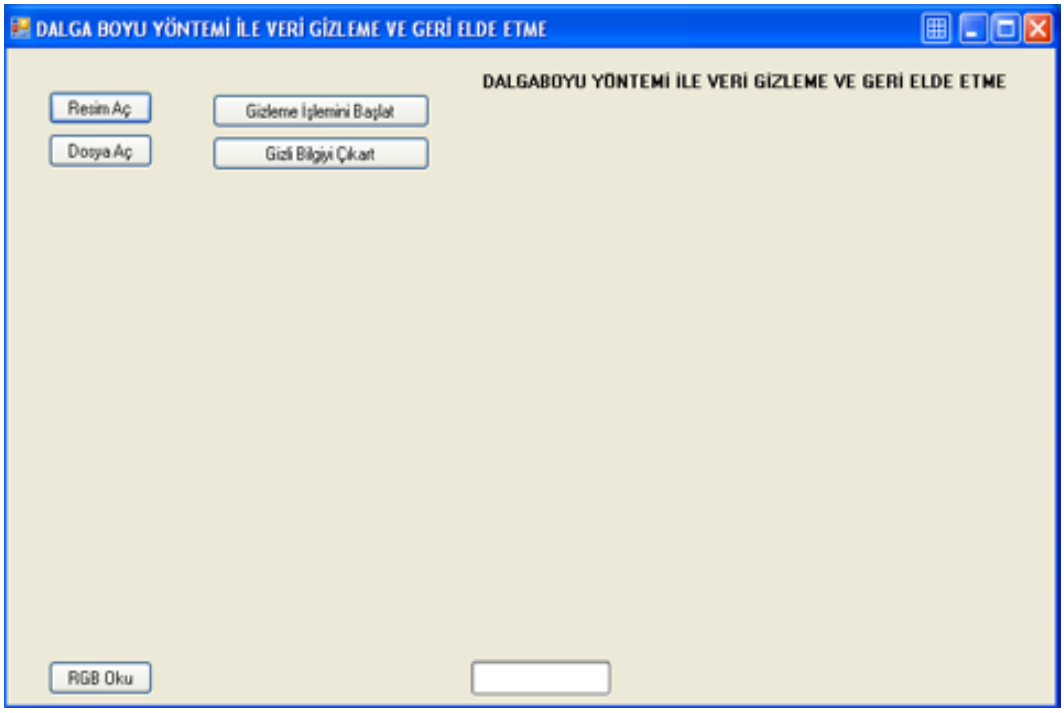
310 × 220 = 68200 pikselden oluşan RGB: 34,176,70 ile RGB:39,175,76 ağırlıklarına sahip iki farklı renk Şekil 4.8 (a)'da görülmektedir. Birbirine oldukça yakın olan bu iki renkten Şekil 4.8 (b)'de yer alan gömme işlemine başlanmadan önce orijinal rengi temsil etmektedir. Sağdaki ise gömme işleminden sonra elde edilen yeni rengi göstermektedir. İki renk arasında çok az da olsa bir fark olduğu söylenebilir. Ancak unutulmamalıdır ki yukarıda yer alan her iki resim 68200 pikselden oluşmaktadır. Halbuki "Ü" (154) ASCII kodunun gömüldüğü piksel sayısı sadece 1'dir. Yalnızca bir piksele ait rengi göstermek oldukça zordur. Asıl renk ayrımı bir resim içerisine tüm ASCII kodlarının gömülmesi işleminden sonra ortaya çıkan iki resmin kıyaslanması ile görülebilir.

Şekil 4.8. Gömme işlemi sonunda yer değiştiren iki pikselin renk dağılımı.

Bu işlemde öncelikli olarak amaçlanan, resim üzerinde çok büyük bozulmaya yol açmadan en büyük miktarda bilginin resim içerisine gömülmesidir. Hedefe göre her bir piksele bir adet ASCII kodu gömülebilmekte ve sonuç olarak 1 Bayt bilgi saklanmaktadır. Dolayısıyla (310 × 220) piksel yani (10,94 × 7,76) cm gibi çok küçük bir alana sahip bulunan resim üzerine 310 × 220 = 68200 Byte bilgi gömülebilmektedir. Dolayısıyla (1024 Bayt = 1 KBayt) yaklaşık 66,6 Kbayt'lık bir bilginin gömülebileceği anlamına gelir. Bu kadar küçük bir alanda elde edilen maksimum performans açıkça görülmektedir.

4.7. Uygulama Yazılımının Tanıtılması

Tasarlanan uygulama yazılımı Visual Studio 2005 programlama paketinden Visual C# yazılımı kullanılarak geliştirilmiştir. Uygulama yazılımı proje dosyaları ile birlikte 322 Kbayt büyüklüğündedir. Veri gömme işlemi için Dalgaboyu tabanlı algoritma kullanılmaktadır. Veri Gömme ve Gizli Verinin Geri Elde Edilmesi yazılımları aynı arayüz üzerinden yapılmaktadır. Şekil 4.12'de Veri Gömme ve Gizli Verinin Geri Elde Edilmesi yazılımının ana penceresi görülmektedir.



Şekil 4.9. Veri Gömme ve Gizli Verinin Geri Elde Edilmesi uygulama yazılımı ana penceresi

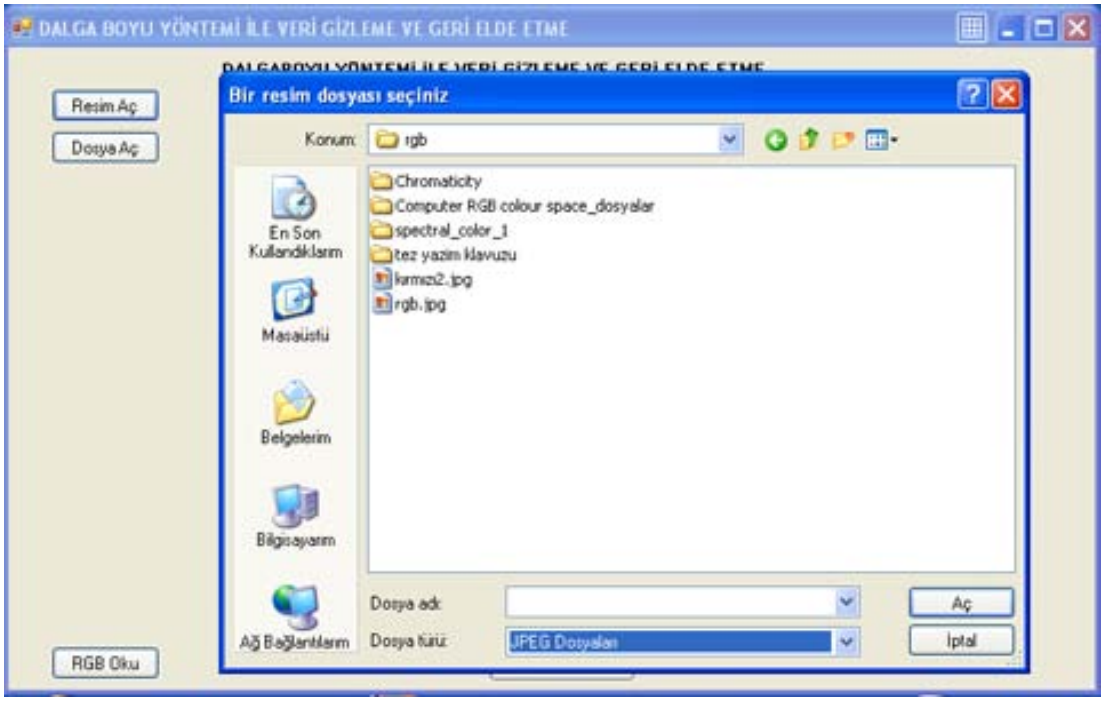
4.7.1. Verinin gömülmesi

Tez çalışması süresinde veri gizleme nesnesi olarak resim dosyaları (bmp, jpg, jpeg uzantılı) kullanılırken, gizlenmek istenen veri olarak da metin dosyaları (txt ve rtf uzantılı) kullanılmıştır. Gizlenmek istenen nesne türlerinin çeşitliliğinin ve sayısının artırılması uygulama yazılımına yapılacak birkaç küçük ekleme ile mümkündür.

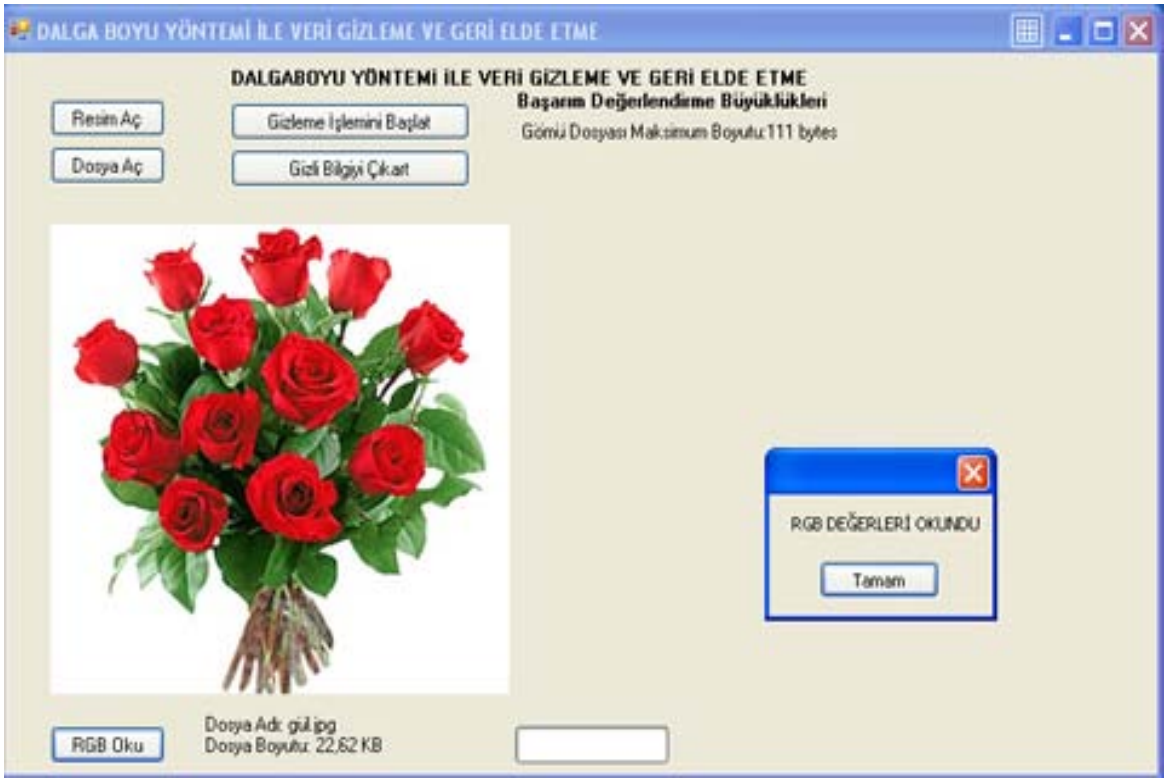
4.7.2. Dalgaboyu yöntemi ile veri gömme uygulaması

Dalgaboyu yönteminde veri gömme işlemi için İGS'nin fark edemeyeceği dalgaboyu değerlerine sahip renkler kullanılmıştır. Bu sebepten dolayı veri gizleme için seçilecek resim dosyasının bahsedilen renklerden oluşturulmuş olması gizlenebilecek bilgi kapasitesini olumlu olarak etkileyecektir.

Uygulama yazılımı çalıştırıldığında ilk adım olarak örtü dosyası (cover image) seçilir. 'Resim Aç' butonuna tıklandığı zaman ekrana gelen iletişim penceresinden istenen bir resim dosyası seçilir (Şekil 4.13). Örtü dosyası seçildikten sonra seçtiğimiz resim dosyasının ön izlemesi program üzerinde gösterilir. Ön izleme resminin altında 'Dosya Adı' ve 'Dosya Boyutu' bilgileri gösterilir. Yine ön izleme resminin altında bulunan 'RGB Oku' butonu ile resim dosyasındaki her bir piksel değerinin ayrı ayrı dalgaboyu (DB) bulunur. DB hesaplanırken program, daha önceki konu başlıklarında anlatılan ve verilen formüller doğrultusunda hesaplamalarını yaparak uygun pikselleri seçer. Uygun pikselleri belirleme işleminden sonra programın sağ üst köşesinde bulunan 'Başarım Değerlendirme Büyüklükleri' bölümü altında 'Gömü Dosyası Maksimum Boyutu' gösterilir (Şekil 4.14).



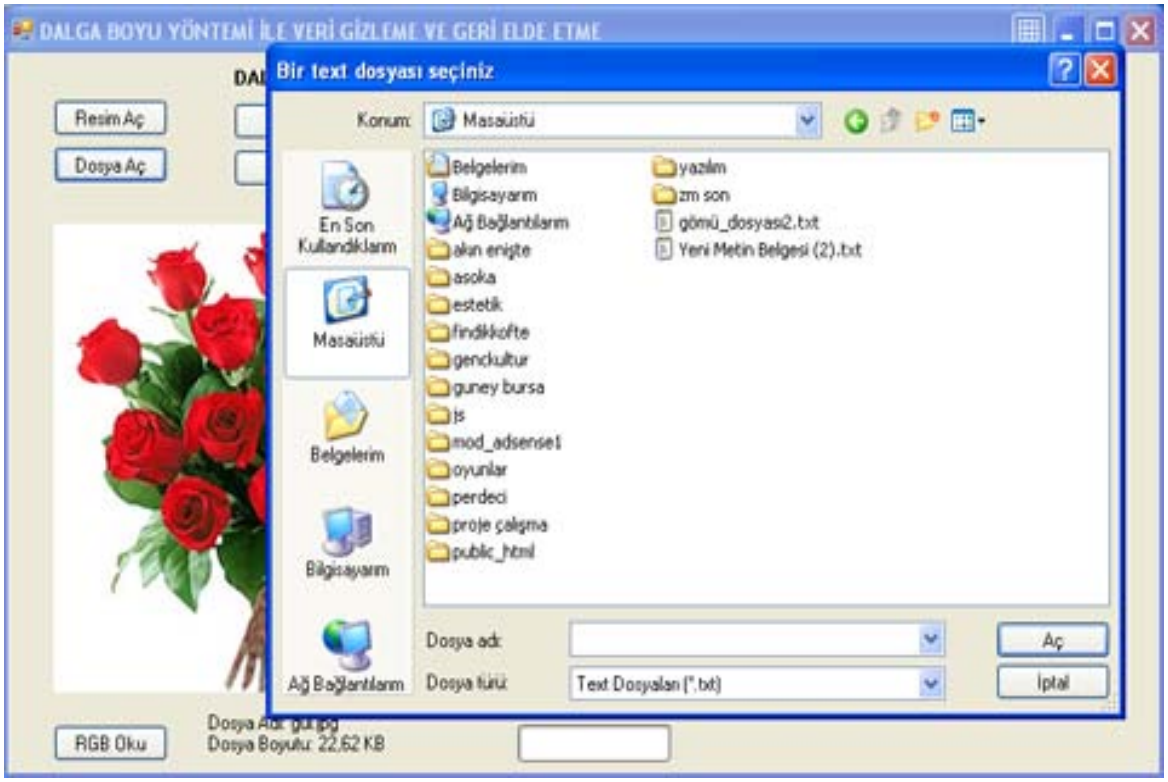
Şekil 4.10. Resim dosyası seçme iletişim penceresi.



Şekil 4.11. Gizleme işlemi için kullanılacak resim dosyası ön izleme görüntüsü ve gömü dosyası maksimum boyutu.

Bir sonraki adım da ise gizli haberleşme için gerekli olan gömü dosyası (gizli veri) seçilir. Uygulama yazılımında ‘Dosya Aç’ butonuna tıklanarak Şekil 4.15’de görülen iletişim penceresi açılır. Gömü dosyası seçilirken ‘Gömü Dosyası Maksimum Boyutu’ bilgisi göz önünde tutulmalıdır. Daha büyük boyutta bir gömü dosyası seçildiğinde uygulama yazılımı hata verecektir.

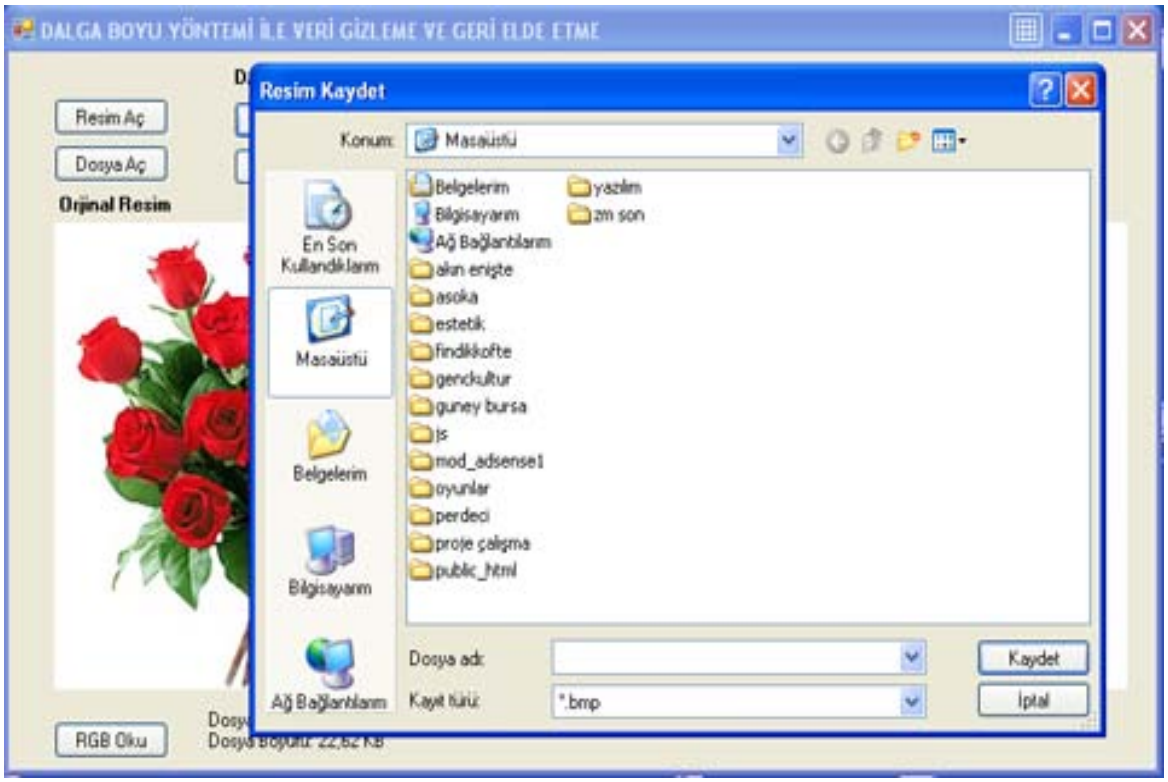
Gömü dosyası seçildikten sonra, seçilen gömü dosyasının boyut bilgisi ‘Dosya Boyutu’ bölümünde gösterilmektedir. Gömme işlemini başlatmak için ‘Gizleme İşlemini Başlat’ butonuna basılır. Gömü dosyasının boyutuna göre gizleme işleminin süresi değişebilir. Veri gizleme işleminde RGB kodlama yöntemi kullanılmıştır. RGB tekniğinin kullanılmasının sebebi, resim sırörtme için gizli veri kapasitesini önemli ölçüde artırmasıdır. Resim dosyası içerisindeki uygun piksellere gizleme işlemi yapılırken piksellerin yeni değerlerinin DB yöntemine göre belirlenen aralıkların dışarısına çıkmamasına dikkat edilir. Böyle bir piksel olduğu takdirde piksele veri gömülmeden değeri eşik değerlerinin dışında olacak şekilde değiştirilir. Böylelikle daha sonra gizli veriyi geri elde etme işleminde o piksellere bakılmamış olur. Gömme işlemi sürerken Şekil 4.16’daki gibi bir ekran görülür.



Şekil 4.12. Gömü dosyasının seçilmesi.

Şekil 4.13. Gizleme işlemi başlatıldıktan sonra görülen bekleme mesajı.

Gömme işlemi bittiğinde elde edilen sırlı resmin (stego – image) nereye kaydedileceğini soran Şekil 4.17'deki gibi bir iletişim kutusu açılır.



Şekil 4.14. Sırlı resmin kaydedilmesi.

İstenilen bir isim verilerek sırlı resim bilgisayarda istenilen bir yere kaydedilir. Kaydetme işleminde sırlı resmin uzantısını '.bmp' veya '.jpg' olarak girip kaydedilir. Gömme işlemi tamamlandıktan sonra şifreli resim ön izlemesinin altında bulunan bölümde sırlı resmin 'Dosya Adı' ve 'Dosya Boyutu' bilgileri verilir (Şekil 4.18). Gömme işleminin sona ermesiyle 'Orijinal Resim' ve 'Şifreli Resim' karşılaştırma yapabilmek için ön izlemeleri yan yana gösterilir.

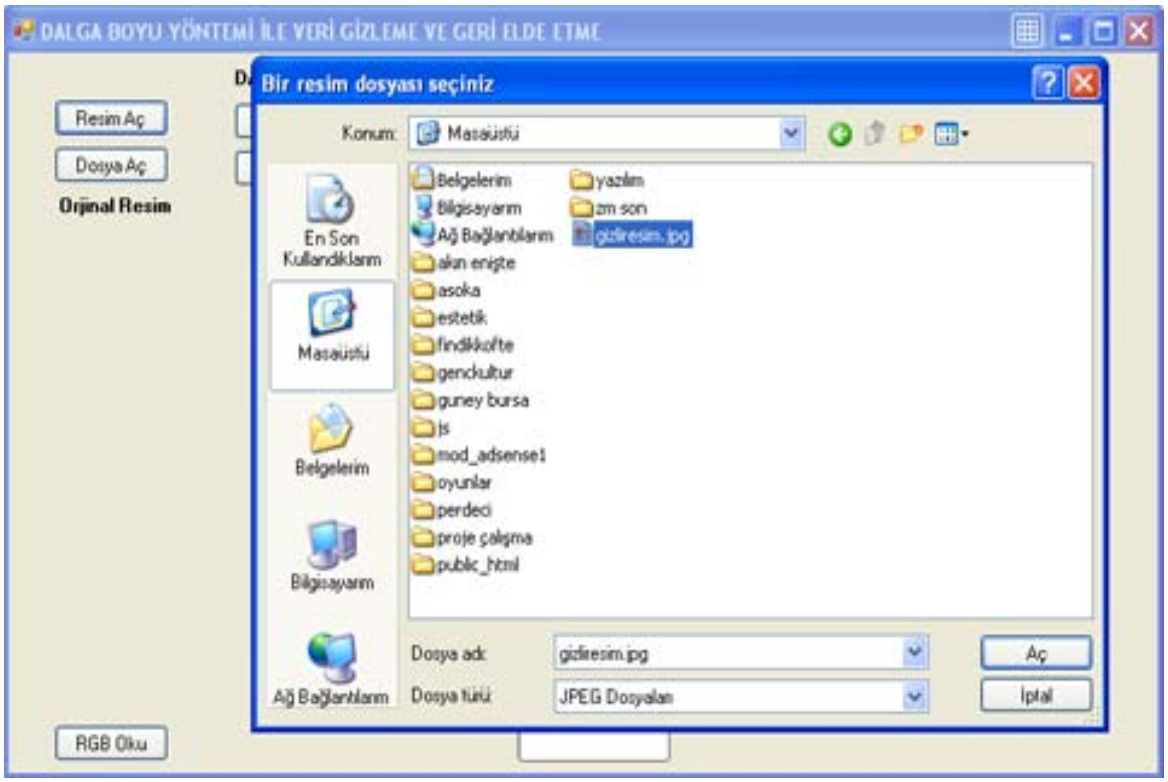
Şekil 4.15. Sırlı resmin ön izleme görüntüsü ve istatistiki bilgiler.

4.7.3. Gizli verinin geri elde edilmesi

Bir önceki bölümde anlatılan veri gömme yazılımı kullanılarak elde edilen sırlı resimden gizli veriyi geri elde etme işlemi için aynı yazılım kullanılır.

Uygulama yazılımı çalıştırıldığında sırlı resim dosyasını açmak için daha önce veri gizleme işleminde yapıldığı gibi, sol üst tarafta bulunan ‘Resim Aç’ butonuna basılarak açılan iletişim penceresinden sırlı resim dosyası seçilir (Şekil 4.19). Sırlı resmin seçilmesi ile aktif hale gelen ‘Gizli Bilgiyi Çıkart’ butonuna tıklandığında gizli verinin geri elde edilmesi işlemi başlayacaktır.

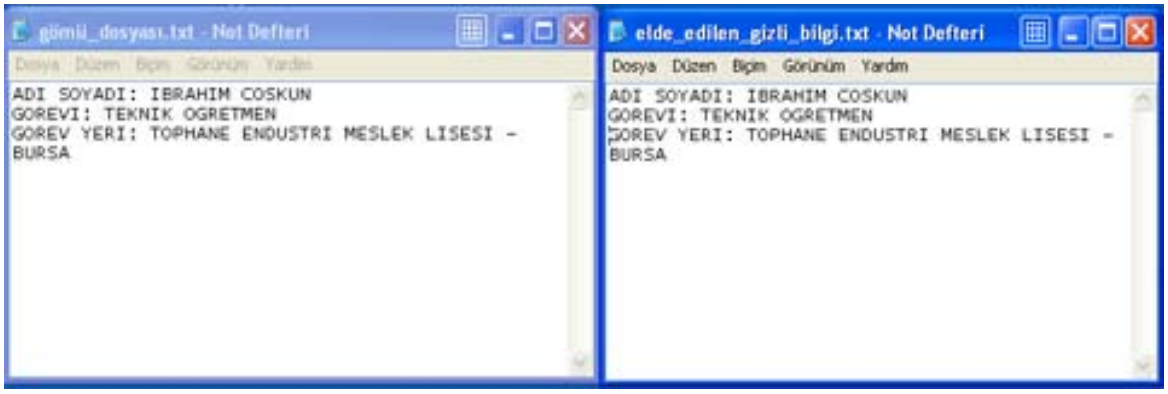
Gizli verinin çıkarılması işlemi bittiğinde ekrana elde edilen gizli verinin bilgisayarda nereye kaydedileceğini soran bir iletişim penceresi gelir (Şekil 4.20). Bu pencerede elde edilen gizli veriyi ‘txt’ veya ‘rtf’ uzantılı olarak istenilen bir isim verilerek bilgisayarda istenilen bir yere kaydedilir.



Şekil 4.16. Sırlı resmin seçilmesi.

Şekil 4.17. Geri elde edilen gizli verinin kaydedilmesi.

Şekil 4.21'de orijinal gizli veri ile elde edilen gizli veri görülmektedir. Şekilde sağ tarafta görülen geri elde edilen bilgi, sol tarafta görülen ise saklanan bilgidir.



Şekil 4.18. Orijinal gizli veri ve elde edilen gizli veri.

BÖLÜM 5. SONUÇ VE ÖNERİLER

Bu tezin amacı internet gibi güvenli olmayan ortamlarda güvenli haberleşme sağlayabilmek için haberleşme bilgilerinin korunmasını amaçlayan yeni bir veri gömme yaklaşımını ortaya koymak ve gerçekleştirmektir.

Veri gömme işleminde birinci ve en önemli gereksinim algılanamazlıktır. Resim, video gibi görsel içerikli taşıyıcı dosyalarda algılanabilirlik ölçüsü İGS'ne bağlıdır. Bu durumda geliştirilmesi gereken yeni yöntemin İGS özelliklerine, sınırlarına hassas olması gerekmektedir. Tez çalışmasında gizli verinin resim dosyasının veri gömmeye uygun pikselleri içerisine yerleştirilmesinde daha önceki yapılmış benzer çalışmalarda eksik yanları kalan ışık dalgaboyu yöntemi tamamlanarak kullanılmıştır. Görüntü dosyalarında İGS'nin duyarlı olduğu en önemli nokta, renk geçişleridir. Burada ana fikir; taşıyıcı görüntü içerisindeki görülebilir ışığın sınırlarına yakın olan dalgaboyu değerlerine sahip piksellerin bulunarak veri gömmek için kullanılmasını sağlamaktır. Veri gizlemek için kullanılacak olan piksellerin dalgaboyu değerleri kızılötesi (780nm) veya morötesi (350nm) dalgaboyu değerlerine ne kadar yakın olursa, algılama işlemi de o kadar imkânsız olacaktır. Bu tez çalışması ile, sırörtme uygulamalarında çözüm bekleyen algılanabilirliğe bağlı güvenli haberleşme sorununun iyileştirilmesi amaçlanmıştır.

DB yöntemi kullanılan yazılımda resim dosyalarına veri gizleme için RGB kodlama tekniği kullanılmıştır. RGB tekniğinin kullanılmasının sebebi, resim sırörtme için gizli veri kapasitesini önemli ölçüde artırmasıdır.

Tez çalışması kullanıcı arayüzü Visual Studio 2005 programlama paketinden Visual C# ortamında tasarlanmıştır. Daha önceki yapılan görüntü işleme çalışmalarının hemen hemen hepsinde Matlab yazılımı kullanılırken, bu çalışmada Visual C# tercih edilerek diğer çalışmalarla karşılaştırılma imkanı bulunmuştur. Ayrıca, Visual C#

yazılımının toolbox desteği, sayısal görüntü işleme, sayısal sinyal işleme gibi konularda sağladığı alt yapı ve kod desteği tez çalışmasının gerçekleştirilmesini sağlamıştır. Ayrıca Visual C# programı ile yazılan yazılım kolayca derlenerek elde edilen ‘exe’ dosyası aracılığı ile istenilen bilgisayarda herhangi bir program platformuna bağlı kalmadan kullanılabilmesi en büyük avantajıdır.

DB tabanlı sırötme yöntemi kullanılarak yapılacak veri gizleme işleminde kapasiteyi artırmak için, gömü dosyası olarak daha çok kızılötesi ve mor ötesi renklere sahip olan resim dosyaları tercih edilmelidir.

Bu çalışma ile güvenli bilgi haberleşmesinde daha önceki yapılan çalışmalarda [4, 49] tavsiye edilen bir yöntem geliştirilerek gerçeklenmiştir. Ancak gerçekleştirilen yöntem ile ilgili tüm bilgilerin bu çalışma ile duyurulması sonucunda yapılan çalışmaya karşı bir saldırı yönteminin geliştirilmesi kolaylaşmıştır. Tez çalışması ile gerçekleştirilen yöntem bir akademik çalışmanın amacıdır.

KAYNAKLAR

[1] JOHNSON, N. F., JAJODIA, S., "Exploring Steganography: Seeing the Unseen", February 1998

[2] BARNİ, M., BARTOLONI, F., "Data hiding for fighting piracy", *EEE* Signal Processing Magazine, vol. 21, no. 2, pp. 28-39, March 2004.

[3] KATZENBEISSER, S., PETITCOLAS, F. A. P., "Information Hiding Techniques for Steganography and Digital Watermarking", Artech House, INC. 685 Canton Street Norwood, MA 02062, 2000.

[4] ÇETİN, Ö., "A Data Embedding Algorithm Design for Video Applications Using a New Steganography Approach (Thesis or Dissertation style)," Ph.D. dissertation, Dept. Elect. Eng., Sakarya Uni., Sakarya, Turkey, 2008.

[5] GONZALES, R.C., WOODS, R.E., Digital Image Processing SE, Prentice-Hall, International Inc., Upper Saddle River, New Jersey 2002.

[6] ÇAMOĞLU, D., (2005) Algılama, Örüntü ve Görsel Tanımlama, http://www.yapay-zeka.org/modules/icontent/index.php?page=30 (Erişim Tarihi: Nisan 2010)

[7] http://tr.wikipedia.org/wiki/RGB_renk_uzay%C4%B1 (Erişim Tarihi: Nisan 2010)

[8] ÖNER, E., "Tekstil Endüstrisinde Renk Ölçümü", Marmara Üniversitesi, Yayın No: 672, İstanbul, 2001.

[9] YILMAZ, İ., "Renk Sistemleri, Renk Uzayları ve Dönüşümler" Selçuk Üniversitesi Jeodezi ve Fotogrametri Mühendisliği Öğretiminde 30. Yıl Sempozyumu, Konya, 16-18 Ekim 2002

[10] SAĞIROĞLU, Ş., TUNÇKANAT, M., "Güvenli İnternet Haberleşmesi İçin Bir Yazılım: Türksteg", Erciyes Üniversitesi 2002.

[11] POTDAR, Vidyasagar M., CHANG, E., "Grey Level Modification

Steganography for Secret Communication", Porceedings of IEEE Conference on Industrial Informatics, pp.223-228, Berlin June 2004.

[12] T. Morkel, J.H.P. Eloff, M.S. Olivier, "An Overview of Image Steganography", Information and Computer Security Architecture (ICSA) Research Group Depertment of Computer Science, universty of Pretoria, Sourth Africa.

[13] HASSAN, M. D., "Comparison For Steganalysis Approaches", M. Sc. Thesis, Gazi Üniversitesi 2008.

[14] CANBEK, G., SAĞIROĞLU, Ş., "Bilgi ve Bilgisayar Güvenliği Casus Yazılımlar ve Korunma Yöntemleri", Grafiker, Ankara, 1-50 (2006).

[15] SAĞIROĞLU, Ş., ALKAN M., "Her Yönüyle Elektronik İmza (e- İmza)", Grafiker, Ankara,3,5,33 (2005).

[16] ŞAHİN, A., Görüntü Steganografide Kullanılan Yeni Metotlar ve Bu Metotların Güvenilirlikler, Trakya University 2007.

[17] AKAR, F., "Veri Gizleme ve Şifreleme Tabanlı Bilgi Güvenliği Uygulaması" Elektronik ve Bilgisayar Eğitimi Anabilim Dalı, Marmara Üniversitesi, İstanbul, 2005.

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

[19] AMIN M. M., M. SALLEH, S. Ibrahim, KATMIN M.R., SHAMSUDDIN M.Z.I., "Information Hiding Using Steganography", 4 th. National Conferance on Telecommunication Technology Proceedings, Shah Alam, Malaysia, 0- 7803-7773-7/03, 2003 IEEE.

[20] PIPER, Fred, "Cryptography: A Very Short Introduction ", 2002.

[21] FRANZ, E., JERICHOW A., MOLLER, S., PFITZMANN A., STIERAND, I., Stierand, Computer Based Steganography: How it works and why therefore any restrictions on cryptography are nonsense, at best, Proc. Information Hiding Workshop, pp. 7−21, 1996.

[22] ANDERSON, R.J., ed., Information Hiding: First International Workshop, vol 1174 of Lecture Notes in Computer Science, Isaac Newton Institute, Cambridge, England, Springer-Verlag, Berlin, Germany, ISBN 3-540-1996-8, May 1996.

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

[24] KAHN, D., The Codebreakers: The stroy of secret writing, MacMillan publishing, 1996.

[25] 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, July 1999.

[26] TANAKA, K., NAKAMURA, Y., MATSUI, K., Embedding secret information into dithered multilevel image, in Proc. IEEE Military Commun. Conf. Pp. 216-220, 1990

[27] HARTUNG, F., KUTTER, M., "Multimedya Watermarking Techniques", Proceedings of the IEEE, Vol.87, No.7, pp 1079–1107, 1999.

[28] DELAIGLE, J. K., Protection of Intellectual Property of Images by Perceptual Watermarking, Doktora Tezi, Universitè Catholique de Louvain, (2000).

[29] YALMAN, Y., "Sayısal Ses İçerinde Gizli Veri Transferinin Kablosuz Ortamda Gerçekleştirilmesi", Elektronik ve Bilgisayar Eğitimi Anabilim Dalı, Kocaeli Üniversitesi,

[30] MOHANTY, S. P., Digital Watermarking: A Tutorial Review, Technical Report, Department of Electrical Engineering, Indian Instute of Science, Bangalore, India, 1999.

[31] TOPLASAN, M., 2004. Sayısal İmza ve Şifreleme. Lisans Tezi, Mustafa Kemal Üniversitesi, 68, Hatay.

[32] MURRAY, A.H., BURCHFILED R.W., (eds.), "The Oxford English Dictionary: Being a Corrected Re-issue", Oxford, England: Clarendon Pres, 1933.

[33] CUMMINS, J., DISKIN, P., LAU, S., PARLETT, R., " Steganography and Digital Watermarking", 2004.

[34] CALDWELL, J., "Steganography", CROSSTALK The Journal of Defense Software Engineering, 25-27, 2003.

[35] JAMIL, T., "Steganography: the art of hiding information in plain sight," Potentials, IEEE , 18(1):10-12, 1999.

[36] RABAH, K., “Steganography-The Art of Hiding Data.”, Information Technology Journal, 3 (3):245-269 (2004).

[37] MEMON N., WONG, P., “Protecting digital media content”, Communications of the ACM, vol 41, no. 7 , pp. 34–43, July 1998.
.

[38] WANG H., WANG S., “Cyber Warfare: Steganography vs. Steganalysis”, Communications of the ACM, vol. 47, no. 10, October 2004.

[39] SIMMONS G., “The Prisoners' Problem and the Subliminal Channel", CRYPTO83 Advances in Cryptology, pp. 51-67, Aug 22 -24, 1984.

[40] SELLARS, D., An Introduction to Steganography, Students Papers, 1999. http://www.cs.uct.ac.za/cources/CS400/NIS04/papers99/dsellars/index.htm (Erişim Tarihi: Nisan 2010)

[41] BENDER, W., GRUHL, D., MORIMOTO, M., LU, A., 1996. Techniques for data hiding. IBM Syst. J. 35 (3-4), 313-336

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

[43] VENKATRAMAN, S., ABRAHAM, A., PAPYRZYCKI, M., Significance of Steganography on Data Security, Proceedings of the Internatıonal Conference on Selected Areas in Communications Vol. 16, No:4 1998.

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

[45] JOHNSON, N., F., JAJODIA, S., Steganalysis of Images Created Using Current Steganography Software, Proc. Information Hiding Workshop, Portland, Oregon, USA, April 1998.

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

[47] PASCALE, D., A Review of RGB Color Space, BabelColor Compnay, 06.10.2003.

[48] http://orion.math.iastate.edu/burkardt/f_src/colors/colors.f90 (Erişim Tarihi: Nisan 2010)

[49] ÇETİN, Ö., ÖZCERİT, A.T., "İGS Tabanlı Yeni Bir Video – Sırörtme Yöntemi", 3. Uluslar arası Bilgi Güvenliği & Kriptoloji Konferansı 25-27 Aralık 2008, Ankara, TÜRKİYE

ÖZGEÇMİŞ

İbrahim COŞKUN, 28.12.1980 de Bursa' da doğdu. İlk, orta ve lise eğitimini Bursa'da tamamladı. 1998 yılında Tophane Anadolu Meslek Lisesi, Elektronik Bölümünden mezun oldu. 1998 yılında başladığı Sakarya Üniversitesi Teknik Eğitim Fakültesi Elektronik Öğretmenliği'ni 2003 yılında bitirdi. 2003 yılında Bursa Gemlik Endüstri Meslek Lisesi'nde elektronik öğretmeni olarak göreve başladı. 2006 – 2007 eğitim – öğretim döneminde Bursa Osmangazi Hayri Terzioğlu Endüstri Meslek Lisesi'nde müdür yardımcısı olarak görev yaptı. 2007 – 2008 döneminde İstanbul Şişli Endüstri Meslek Lisesi' nde çalıştı. 2008 – 2009 tarihinden beri Tophane Endüstri Meslek Lisesi'nde görev yapmaya devam ediyor. Evli ve 1 kız çocuk babasıdır.