İKİLİ GÖRÜNTÜ KULLANARAK İMZA STEGANOGRAFİ MODELLERİNİN GELİŞTİRİLMESİ

Muntadher Khamees AL-KARAWI

YÜKSEK LİSANS TEZİ
ELEKTRONİK BİLGİSAYAR EĞİTİMİ

GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ

OCAK 2012
ANKARA

Muntadher Khamees AL-KARAWI tarafından hazırlanan İKİLİ GÖRÜNTÜ KULLANARAK İMZA STEGANOGRAFİ MODELLERİNİN GELİŞTİRİLMESİ adlı bu tezin Yüksek Lisans tezi olarak uygun olduğunu onaylarım.

Doç. Dr. O. Ayhan ERDEM
Tez Yöneticisi

Bu çalışma, jürimiz tarafından oy birliği ile Elektronik Bilgisayar Eğitimi Anabilim Dalında Yüksek lisans tezi olarak kabul edilmiştir.

Başkan : Prof. Dr. M. Ali AKCAYOL

Üye : Doç. Dr. O. Ayhan ERDEM

Üye : Doç. Dr. Sabri KOÇER

Tarih : 18 /01/2012

Bu tez, Gazi Üniversitesi Bilişim Enstitüsü tez yazım kurallarına uygundur.

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada orijinal olmayan her türlü kaynağa eksiksiz atıf yapıldığını bildiririm.

Muntadher Khamees AL-KARAWI

İKİLİ GÖRÜNTÜ KULLANARAK İMZA STEGANOGRAFİ MODELLERİNİN GELİŞTİRİLMESİ
(Yüksek Lisans Tezi)

Muntadher Khamees AL-KARAWI

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

Ocak 2012

ÖZET

Steganografi, mesaj iletilmek istenen alıcıdan başka hiç kimsenin mesajın varlığından haberi olmayacağı şekilde gizli mesajlar yazma sanatı ve bilimine verilen addır. Bilgi güvenliği alanında sınıflandırılır. Son zamanlarda bilgisayar ve ağ teknolojileri, steganografide iletişim kanallarını kullanmak için kolay bir yöntem sağlamıştır. Ayrıca, günümüzde elle atılan imzalarla birlikte elektronik imzalar da günlük hayatın önemli bir parçası haline gelmiştir. Steganografi bu imzaların izinsiz kullanımını önlemek ve kulanıcıların güvenli bir şekilde iletişim kurmasına fırsat tanır. Bu tezde ikili görüntülere dayalı bir imza steganografi modeli sunulmaktadır. Piksellerin sınırlı sayıda değer almasından dolayı, görünür hatalar olmadan verileri ikili görüntü içerisine saklamak bu yöntemin zorluklarındandır. Bu yöntemle, stego imza görüntüsü elde etmek üzere düşük düzeyli özellikleri (siyah bir pikseli beyaza dönüştürme ya da beyaz bir pikseli siyaha dönüştürme gibi) değiştirmeye dayalı bir şekilde kapak görüntüsü içerisine gizli imza verisini saklanmaktadır. Ardından, orijinal görüntü kullanılmadan gizlenmiş imza çıkarılabilir. Yapılan çalışmaya ait modelin başarısı bir bilgisayar yazılımı ile de edilmiştir.

Bilim Kodu : 702.1.014
Anahtar Kelime : elektronik imza, ikili görüntü steganografi, sınır bit manipülasyon tekniği, bilgi güvenliği
Sayfa Adedi : 33
Tez Yöneticisi : Doç. Dr. O. Ayhan ERDEM

DEVELOPMENT SIGNATURE STEGANOGRAPHY MODEL USING BINARY IMAGE
(M.Sc. Thesis)

Muntadher Khamees AL-KARAWI

GAZİ UNIVERSITY
INFORMATICS INSTITUTE

JANUARY 2012

ABSTRACT

Steganography as the art and science of writing hidden messages in such a way that no one apart from the intended recipient knows of the existence of the message. Being classified under information security. Current days, computers and networks technologies provide an easy method to use communication channels for steganography. Moreover, lately, manual and electronic signatures became one of the important topics in the daily life. To prevent unauthorized use of these signatures and allows any pair of users to communicate securely. Therefore, this thesis presents a signature steganography model based on binary images. However, hiding the data in binary images without visible defects increases the difficulty of this method, because the pixel take on only a limited number of values. This method hides secret signature data inside cover image depending on changing low level features technique (such as flipping a black pixel to white or vice versa) in order to obtain the stego signature image. Then, the hidden signature can be extracted without using the original image. The performance of the proposed model has been successfully tested using computer programs.

Science Code : 702.1.014
Key Words : electronic signature, binary image steganography, boundary bits
manipulation technique, information security.
Page Number : 33
Adviser : Assoc. Prof. Dr. O. Ayhan ERDEM

TEŞEKKÜR

Çalışmalarım boyunca değerli yardım ve katkılarıyla beni yönlendiren danışmanım Sayın Doç. Dr. O. Ayhan ERDEM'e, manevi destekleriyle beni hiçbir zaman yalnız bırakmayan aileme ve değerli eşim Hacer MAJED'e teşekkürlerimi ve sevgilerimi iletmekten mutluluk duyarım.

İÇİNDEKİLER

Sayfa

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

1. GİRİŞ

Son yıllarda bilgisayar sistemlerinin güvenliği ve özellikle de bilgi güvenliği oldukça önemli bir konu olarak karşımıza çıkmaktadır. Özellikle son 10 yılda internetin yaygınlaşmasıyla veri alışverişi ve paylaşımı da artmıştır. Metin, resim, ses vb. birçok veriyi içeren dosyalar, etkin bir şekilde dünyadaki kullanıcılar 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 [1].

Bunu engellemek amacıyla çeşitli koruma mekanizmaları geliştirilmiş ve yeni teknolojiler ve yeni uygulamalar ortaya çıkmıştır. Bu teknolojilerden biri de şifrelemedir . Şifrelemede gönderilecek ve korunması istenen sayısal veri şifreleme algoritmalarıyla bir anahtar yardımıyla anlaşılmaz bir hale dönüştürülür ve bu şekilde gönderilir. Ancak şifrelerin de zaman içinde kırılabilmesi şifrelemenin güvenli iletişim için tek başına yeterli olmadığını göstermektedir. Bu nedenle şifreleme ve bilgi gizleme yöntemleri, özellikle de steganografi, birlikte kullanılarak güvenli bir iletişimin yapılması sağlanabilmektedir. Bilgi gizleme iletişim güvenliği için oldukça önemli bir konudur. Bilgi gizlemede amaç iletişimin bir üçüncü kişinin fark edemeyeceği şekilde yapılmasıdır. Şifrelemede üçüncü kişi gizli bir bilginin gönderildiğinden haberdardır, fakat bilgi gizleme yöntemleriyle iki kişi arasındaki iletişimin gizli bir şekilde yapılması mümkün olmaktadır. Üçüncü şahıslar arada gizli bir iletişim olduğunu fark edememektedir [1].

Bilgi saklama çok eski yıllardan beri kullanılmaktadır. Günümüzde teknolojinin gelişmesiyle birlikte birçok yeni teknik geliştirilmiştir ve hala geliştirilmeye devam edilmektedir [2].

Bilgi gizlemenin çok önemli bir alt disiplini olan steganografi, dijital (sayısal) ortamdaki verilerin (metin, ses ve görüntü dosyaları) korunması için son yıllarda

saklakla kullanılmaktadır. Steganaliz ise gizli yapılan iletişimin ele geçirilmesi için yapılan saldırıları içermektedir [1].

Bir steganografik sistemin güvenilirliği çeşitli açılardan değerlendirilmektedir. Bunlar bilgi gizlemenin kapak verisini ne kadar değiştirdiği, bilgi saklama kapasitesinin ne kadar olduğu ve dayanıklılığının ne kadar olduğudur. Dayanıklılık ölçütü steganalitik yöntemlere karşı ne kadar başarılı olduğu ile ölçülmektedir. Teknolojinin gelişmesiyle birlikte birçok steganografik yöntem ortaya çıkmıştır, bu gelişmeyle birlikte birçok steganalitik yöntemin de geliştirilmesi gerekmiştir. Her steganografik yöntem farklı bir yöntem izlediği için bunları sezmede kullanılacak steganalitik yöntemler de çeşitlidir. Bir steganografik yöntem için geliştirilen steganaliz yöntemi bir diğeri için çalışmamaktadır. Her steganografik yöntemin kendine özgü bir steganaliz yöntemi bulunmaktadır [1].

Günlük yaşamda giderek daha fazla sayıda dijital ikili görüntü kullanılmaktadır. Elektronik imza pedleri tarafından yakalanılan el yazısı imzalar dijital olarak saklanmaktadır. Bu dijital imzaların kullanım yerlerinden birisi de Amerika Birleşik Devletlerindeki pek çok mağaza tarafından kredi kartı ödeme kayıtlarında olarak kullanılmaktadır. United Parcel Service adlı kurye şirketi gibi büyük kargo şirketleri de bu sistem kullanmaktadır. Microsoft Word gibi kelime işlemci yazılımlar, bir belgenin tanımlanan konumlarına dahil edilmek üzere kullanıcının kendi imzasını ikili görüntü dosya içerisinde saklamasına izin vermektedir. Bu şekilde imzalanan belgeler doğrudan bir faks makinesine gönderilebilir ya da ağ üzerinden dağıtılabilir [3].

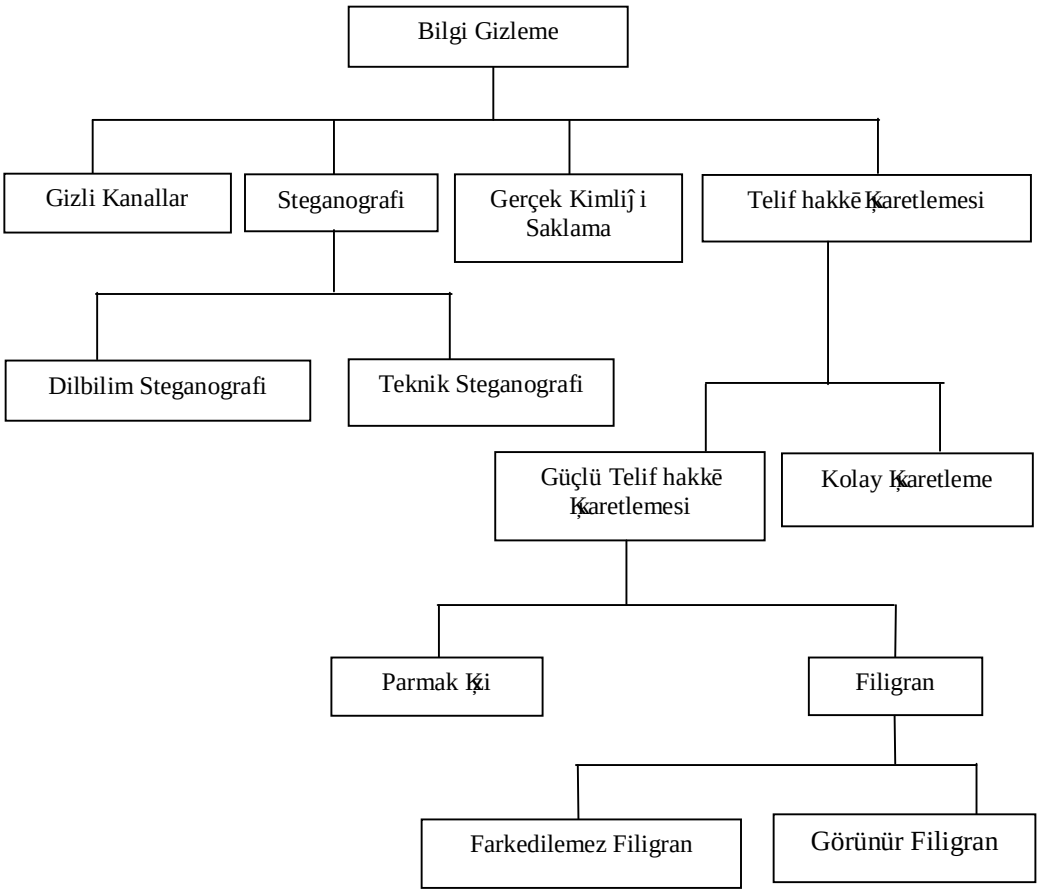
Bir imzanın, izin verilmemiş bir ödeme belgesi üzerine kopyalanması gibi izinsiz kullanımı büyük bir kaygı kaynağı haline gelmektedir. Ek olarak, sosyal güvenlik kayıtları, sigorta bilgileri, mali belgeler gibi bir dizi önemli belge de sayısal hale getirilmiş ve saklanmaktadır.

Bu çalışmada, ikili görüntüler kullanılarak sıradır bit değiştirme tekniğine dayalı imza steganografi sisteminin tasarımı ve uygulaması gerçekleştirilmiştir.

Bu tez beş bölümden oluşturulmuştur. Birinci bölüm giriş bölümüdür, ikinci bölüm imza saklama sistemlerinde imzanın kaynak araştırmasını ele almaktadır. Üçüncü bölüm önerilen sistemi tanımlamaktadır. Dördüncü bölüm imza içinde imza saklama modellerinin geliştirilmesini ele almaktadır. Beşinci bölüm ise sonuçları ve gelecekte çalışılması önerilen konuları içermektedir.

2. BİLGİ SAKLAMA VE BU KONUDA YAPILAN ÇALIŞMALAR

Bu bölüm, bilgi saklama, dijital görüntü temelleri ve ikili görüntülerde veri saklama gibi konularla ilgili çalışmaları kapsamaktadır.



Şekil 2.1. Bilgi gizleme yöntemlerinin sınıflandırılması

2.1. Bilgi Saklama

Bilgi saklama, görüntü, ses ya da metin gibi çeşitli ortam formlarına veri gömmek üzere kullanılan süreçler sınıfını temsil etmektedir. Gömülü veri gözlemleyici insan açısından görünmez olmalıdır [4].

Gömme süreci daha sonra gizli mesajdan gelen verilerle yer değiştirecektir. Bilgi saklama teknikleri ve yöntemlerine ait daha detaylı bilgiler aşağıda verilmiştir

2.1.1. Bilgi saklama teknikleri

Bilgi saklama tekniklerinin şekil 2.1.'de gösterildiği gibi sınıflandırılabileceğini bildirmektedir [5].

Gizli Kanallar, bilgi gizlemenin ilk alt disiplini olan gizli kanallar Lampson [1], tarafından tanımlanmıştır. Gizli kanallar iki kişi arasında gizli bilgilerin el değiştirmesi için iletişimi sağlayan kanallardır. Gizli kanal kurulması iki kişinin karşılıklı anlaşmasını gerektirmektedir. Gizli kanalların amaçları, iletişimimizdeki veriyi saklamaya çalışmak ve iletişimin amacını gizlemektir. Böylece; gerçek veri iletimi zararsız ve uygunmuş gibi gözükecek ve veriyi karıştırmak için ayrı bir şifreleme yapılmasına gerek kalmayacaktır [1].

Gerçek Kimliği Saklama, diğer bir alt alan olan gerçek kimliği saklama, veri gönderimi sırasında gerçek kimliği saklayarak, bilginin bilinmeyen ya da anlaşılamayan bir ortamdan gidiyormuş izlenimi verilerek gönderilmesidir. Bu şekilde bilgi zarar görmeden gönderilebilir. Fakat ağlar üzerinde bilinmeyen kullanıcıların varlığı ağ yöneticilerinin daha fazla dikkatini çekmekte ve bu da güvenliği tehlikeye sokmaktadır. Bu yüzden sadece çok gerektiği durumlarda kullanılmasıuygundur [1].

Telif Hakkı İşaretlemesi , telif hakkı işaretlemesinde ise orijinal dosyanın korunması amacıyla dosyanın içine bazı bilgiler gizlenmektedir. Bunlar; dosyaların üretildiği tarih, telif hakkı sahibi, üreticiye nasıl ulaşılabileceği gibi bilgileri içermektedir. Bu yöntemler steganografi ile beraber kullanılmaktadır. Telif hakkı işaretlemesi, sayısal görüntülerde sayısal filigran olarak kullanılmaktadır. Filigran, bir çeşit gizli damga baskısıdır. (Örneğin kâğıt banknotlar üzerindekiler gibi). Bunlar ancak ışığa tutularak bakıldıklarında görülebilmektedirler. Modern steganografi uygulamalarında kullanılan filigranlar ise görüntü ve ses dosyalarında kopyalamayı önlemek amacıyla

damgalar bırakmaktadırlar. Bu damgalar özel programlar tarafından okunabilmekte ve dosyaların üretildiği tarih, telif hakkı sahibi, üreticiye nasıl ulaşılabileceği gibi bilgileri içermektedir [1].

Steganografi bilgi gizleme yöntemlerinin en önemli alt dalıdır . Bu yaklaşım, bir nesnenin içerisine bir verinin gizlenmesi olarak tanımlanabilir. Dilbilim ve teknik steganografi olarak ikiye ayrılmaktadır. Bu yaklaşımla ses, sayısal resim, video görüntüleri üzerine veri saklanabilir.
Görüntü dosyaları içerisine saklanacak veriler metin dosyası olabileceği gibi, herhangi bir görüntü içerisine gizlenmiş başka bir görüntü dosyası da olabilir [1].

2.1.2. Bilgi saklama yöntemleri

Bilgi saklama, gömülü mesajların varlığını algılanamayacak bir şekilde gizli mesajlar gönderme yöntemlerini kapsamaktadır. Bu gibi mesajların taşıyıcıları dijital olarak temsil edilen kod ya da iletim şeklinde olabilir.

Taşıyıcılar (kapaklar) iki şekle ayrılabilir. Kapak, dijital telefon bağlantısı gibi kesintisiz bir veri akımı olabilir ya da tek bir bit eşlem görüntüsü gibi bir dosya olabilir. Birincisi akım kapağı olarak adlandırılırken ikincisi rasgele erişimli kapak olarak adlandırılmaktadır. Bunlar dışında bilgi saklamak üzere pek çok farklı yöntemler de kullanılmaktadır [6].

Metin içerisinde saklama

Metin steganografi bilgi gizlenecek ortamın metin (text) olduğu steganografi koludur. Metin steganografinin uygulanabilmesi için çeşitli yöntemler vardır. Bunlar şu şekilde sınıflandırılabilir [1].

- Açık Alan Yöntemleri (Open Space Methods)
  - Satır Kaydırma Kodlaması
  - Kelime Kaydırma Kodlaması

- Gelecek Kodlamasē

ī Yazēmsal Yöntemler (Syntactic Methods)

ī Anlamsal Yöntemler (Semantic Methods)

Açēk alan yöntemleri, bu yöntemler, anormal gözükmeyen iki kelime arasēnda fazladan boĸluklar ve satēr sonu boĸluklarē esasēna göre çalēĸmaktadēr. Bununla birlikte açēk alan yöntemlerinin ASCII kodlarēile kullanēlmasē daha uygundur [1].

Yazēmsal yöntemler, Bu yöntem, dokumanē kodlamak için noktalama iĸaretlerini kullanēr. Örneĵin aĸaĵēdaki iki cümle ilk bakēĸta aynēymēĸ gibi gözükmektedir, fakat dikkatlice bakēldēĵēnda ilk cümlenin fazladan bir ó,ô iĸareti içerdiĵi görülmektedir. Bu yapēlarēn biri ñ1ò, diĵeri de ñ0ò olarak belirlenmekte ve kodlama iĸlemi bu ĸekilde gerçekleĸtirilmektedir [1].

ñbread, butter, and milkò
ñbread, butter and milkò

<u>Disk boĸluĵunda veri saklama</u>

Bir gözlemci açēsēndan kolayca belirgin olmayan kullanēlmamēĸ boĸluĵu bulmaya dayalē diĵer bilgi saklama yöntemleri hakkēnda bir fikir vermiĸtir. ĸletim sistemlerinin dosyalarē saklama ĸekli, tipik olarak dosyalara tahsis edilmiĸ görünen kullanēlmayan boĸluklarla sonuçlanmaktadēr. Örneĵin Windows 95 iĸletim sistemi altēnda, bir dosyaya tahsis edilen minimum alan 32 kilobayttēr. Eĵer bir dosya 1 kilobayt büyüklükteyse, bu durumda ek 31 kilobayt alan israf edilmektedir [7] .

Dosya sistemlerinde veri saklamanēn diĵer bir yöntemi gizli bölümler oluĸturmaktēr. Bu bölümler eĵer sistem normal olarak baĸlatēlmēĸsa görünmemektedir. Bu kavramlar daha yeni bir steganografik dosya sisteminin önerilmesi yapēlmēĸtēr [8].

Aş paketlerinde veri saklama

Aş protokollerinde var olan özelliklerden faydalanılarak bilgi saklamak için yararlanılabileceş ini göstermiştir. Şnternet üzerinden sayılmayacak kadar çok sayıda veri paketi gönderilmektedir. Örneş in TCP/IP paket başlıklarında veri saklamak gibi, bunlardan herhangi birisi, mükemmel gizli bir iletişim yolu saş layabilir [7].

Yazılım ve devrelerde veri saklama

Ayrıca verilerin taşıyıcının fiziksel düzenlemesine dayalı olarak da saklanabilmektedir. Düzenlemenin kendisini oluşturan kişi açısından benzersiz bir gömülü imza olabilir. Bu bir program içerisinde kodun yerleştirilmesi ya da bir devre kartı üzerine elektronik devrenin yerleşimi şeklinde olabilir [7].

Görüntüler içerisinde veri saklama

Görüntüler içerisinde veri saklamanın pek çok farklı yöntemi vardır. Bu yöntemler fazladan bilgi saklamak üzere dosya başlıklarındaki kullanılmayan yer içerisinde bilgi saklamayı içermektedir [7].

Gömme teknikleri, bilginin algılanamaz düzeylerde (gürültü) yerleştirilmesinden, sıkıştırma algoritmalarının düzenlenmesine (görüntünün tipine baş lı olarak) lüminans (aydınlık şiddeti), kontrast ya da renk gibi taşıyıcı özelliklerin deş iştirilmesine kadar farklılık göstermektedir. Bunlarla birlikte, üçüncü bölümde bahsedileceş i gibi verilerin görüntüler içerisinde saklanmasına dayanan teknikler de bu tezde geliştirilmiştir.

Ses içerisinde veri saklama

Seste veri saklama teknikleri iki sınıfa ayrılmaktadır. Bunlar, ses steganografisi ve ses telif hakkı koruma şeklindedir. Ses steganografisi iletişim sürecinde fazladan

bilginin varlığından yararlanan tekniklere karşıdık gelmektedir. Dijital ses doğal olarak, bir gürültü bileşeni şeklinde fazlalıklar içermektedir [9].

Ses verisi açısından, stego veri ğtipik ses verisiğ gibi görünmelidir [10]. Ses steganografisinin genel yöntemleri şunlardır: düşük bit, kodlama, faz kodlama, spektrum yayma ve eko gizlemedir.

Ses de telif hakkı koruma ya içeriğe dayalı olabilir ya da fligran oluşturma yoluyla gerçekleştirilebilir. Fligran oluşturma en az miktarda veri gömen, ancak en fazla güvenilir bir uygulamadır [11].

Seste fligranın korunması şunlar kullanılarak sağlanmaktadır: Fazladan yaydığım ve psiko akustik frekans maskelemedir. Dijital fligran oluşturma, potansiyel olarak dijital çoklu ortam verilerinin telif haklarını ve bütünlüğünü sağlamak üzere kullanılabilecek bir teknolojidir [12].

2.2. Dijital Görüntü Temelleri

Fotoğraf görüntüleri yakalamak, saklamak, değiştirmek ve görmek üzere dijital ekipman kullanırken, bu görüntüler ilk olarak sayısallaştırma ya da tarama olarak adlandırılan bir süreç içerisinde bir dizi numaraya dönüştürülmelidir. bilgisayar rakamları saklamada ve değiştirme de çok iyidir; dolayısıyla görüntünüz bir kere sayısallaştırıldığında fotoğraflarınızı inanılmaz çeşitlilikteki şekillerde arşivlemek, incelemek, değiştirmek, görüntülemek, iletmek ya da yazdırmak için bilgisayarlar kullanılabilir [13].

2.2.1. Piksel ve bit eşlemler

Dijital görüntüler piksellerden oluşmaktadır. Her bir piksel görüntüdeki tek bir noktadaki rengi (ya da siyah beyaz fotoğraflardaki grilik düzeyini) temsil etmektedir; dolayısıyla bir piksel belirli bir renkteki küçük bir noktadır. Bir görüntünün rengini çok fazla sayıda noktada ölçerek, orijinalin bir kopyasının tekrar oluşturulabileceği

görüntünün dijital bir örneğini oluşturabiliriz. Pikseller geleneksel fotoğrafik görüntüdeki tahıl parçacıklarına gibidir . Bu pikseller düzenli bir satır ve sütun yapısı içerisinde düzenlenmiştir ve bilgiyi bir parça farklı saklamaktadır. Dijital bir görüntü bazen bir bit eşlem olarak adlandırılan dikdörtgensel bir pikseller dizisidir [13].

2.2.2. Dijital görüntü tipleri

Fotoğraf olarak, dijital görüntülerin iki önemli tipi bulunmaktadır: Renkli ve siyah ı beyaz. Renkli görüntüler renkli piksellerden oluşurken, siyah beyaz görüntüler grinin farklı tonlarındaki piksellerden oluşmaktadır [13].

Siyah ı beyaz görüntüler

Siyah beyaz bir görüntü her biri, belirli bir konumda görüntünün belirli bir gri düzeyine karşılık gelen tek bir rakam ile tutulmaktadır. Bu gri düzeyleri, normal olarak 256 farklı griden oluşan siyahtan beyaza kadar tüm aralıklarda olabilmektedir. Gözün yaklaşık 200 gri düzeyini zorlukla ayırt edebilmesinden dolayı, basamaksız bir tonlama oluşturmak için bu aralık yeterli olmaktadır [13].

Renkli görüntüler

Renkli bir görüntü, belirli bir konumda görüntünün kırmızı, yeşil ve mavi düzeylerine karşılık gelen üç rakamı tutan piksellerden oluşmaktadır. Bunlar (Bazen RGB-Red Green Blue olarak bahsedilen) kırmızı, yeşil ve mavi renklerdir. Kırmızı, yeşil ve mavi renkler belirli oranda birbirine eklenerek bütün renkler oluşturulabilir. Her bir ana renk için 256 düzey olduğunu varsayılarak, her bir renkli piksel üç bayt (24 bit) ile bellekte saklanabilir. Bu kabaca 16.7 milyon farklı olası renge karşılık gelmektedir. Aynı büyüklükteki görüntüler için siyah beyaz sürümde renkli bir sürümden üç kat daha az bellek kullanılacaktır [13].

İkili görüntüler

Bir ikili dijital görüntü için sadece iki olasılığı vardır. Genelde herhangi iki renk kullanılabilir olsa da, ikili bir görüntü için kullanılan iki renk siyah ve beyazdır. Nesne için kullanılan renk arka plan rengi, resmin geri kalanının ise görüntü ön plan rengidir. Belge tarama işleminde bu genellikle iki ton olarak adlandırılır [13].

İndeksli renkli görüntüler

Bazı renkli görüntüler tipik olarak 256 farklı renkten oluşan renk paleti kullanılarak oluşturulmaktadır. Her bir pikseldeki verinin paletteki hangi renk için kullanıldığını gösteren bir palet dizininden oluşmasından dolayı, bu görüntüler indeksli renkli görüntüler olarak adlandırılmaktadır.

Fotoğrafik görüntüleri temsil etmek üzere indeksli renk kullanmada pek çok sorunlar vardır. İlk olarak, eğer görüntü palette bulunandan daha farklı renkler içeriyorsa, eksik renkleri temsil etmek üzere titrekleştirme (dithering) gibi teknikler uygulanmalıdır ve bu durum görüntüyü bozar. İkincisi, iki adet birbirinden farklı paletler kullanan indeksli renkli görüntüyü birleştirmek ve hatta tek bir indeksli renkli görüntünün bir kısmına rötuş yapmak olabilir.Anacak bu durum renklerin sayısının sınırlı olmasından dolayı sorunlar yaratır [13].

2.3. İkili Görüntülerde Veri Saklama

İkili görüntülerde, 1 var olan 1 piksellik alan 1 bit ile, olmayan bir piksellik alan ise 0 ile ifade edilir.

Eşik alma, kenar algılama, doldurma ve bölge analizi gibi parçalama işlemleriyle elde edilir [3].

İkili görüntü işlemleri , düzgün olmayan parçalanmayı düzeltmek veya iyileştirmek, bileşenlerin bağlantı analizi ve geometrik özellikler kullanılarak nesne seçmek gibi durumlar için kullanılmaktadır [3].

2.3.1. İkili görüntülerde veri saklama konusundaki çalışmalar

Görüntü içinde veri saklama hakkındaki çoğu önceki çalışmalar, piksellerin geniş bir yelpazedeki değerlerden birini alabileceği renkli ya da gri ölçekli görüntüler içindir. Bu görüntüler için, piksel değerlerinin küçük bir miktar değiştirilmesi genellikle normal görme koşulları altında fark edilmemektedir.

İnsan görme sisteminin bu özelliği algısal medya verilerinde fligran oluşturmada kilit bir rol oynamaktadır [14]. Pikselin yalnızca sınırlı sayıda değer alabileceği ikili görüntülerde, görünür değişikliklere neden olmaksızın veri saklamak daha zordur.

Özellikle sınır üzerinde bulunmayan beyaz ya da siyah piksellerin tersine çevrilmesinin ikili görüntülerde görünebilir özellikler oluşturmasi olasıdır.

Özel tipte ikili görüntülerde veri saklamak için literatürde pek çok yöntem önerilmiştir. Matsui ve Tanaka, titreklestirme yapılarını düzenleyerek titreklestirilmiş görüntülere ve çalışma uzunluklarını kullanarak da faks görüntüsüne bilgi gömmüştür [15].

Maxemchuk ve Low, kapsamlı elektronik yayınlarda metinsel görüntülere bilgi gömmek üzere satırlar arası boşluğu ve karakterler arası boşluğu değiştirmiştir [16]. Bu yaklaşımlar diğer ikili görüntülere kolaylıkla aktarılamamaktadır ve saklanan veri miktarı sınırlıdır. Koch ve Zhao, ikili görüntüye bilgiyi görünmez bir şekilde saklamayı hedefleyen bir veri saklama algoritması önermiştir [17].

Bu artırıcı gömme işlemleri için, büyük miktarlarda veri gizleme ve orijinal ikili görüntü olmaksızın algılama yapılması özellikle de çok zordur. Özet olarak, daha

önceden önerilen yaklaşımlar ya kolaylıkla diğer ikili görüntülere uygulanamaz ya da yalnızca küçük miktarda veri gömülebilmektedir.

3. ÖNERİLEN MODEL

Veri saklamak için ikili görüntüleri oluşturulmasının iki temel yolu vardır. Bu yaklaşımların ilki, siyah bir pikseli beyaza ya da beyaz bir pikseli siyaha çevirmek gibi düşük düzey özellikleri değiştirmektir. Yaklaşımların ikincisi ise, çizgilerin kalınlığını, kıvrımlarını, boşluklarını ve görece konumlarını değiştirmek gibi yüksek düzey özellikleri değiştirmektedir [3]. Bu tezde stego imza görüntüsünü elde etmek üzere düşük düzey özellikleri değiştirmeye odaklanılmıştır.

3.1. Tasarım Hedefleri

Önerilen modellerin tasarım hedefleri şunlardır:

(i) Gizli imzayı kapak imza görüntüsü içerisine saklayabilme özelliği.

(ii) Kişisan algısının stego imzayı orijinal imza görüntüsünden ayıramamasını nedeniyle mükemmel gizlilik ve mükemmel tanınmazlık oluşturması,

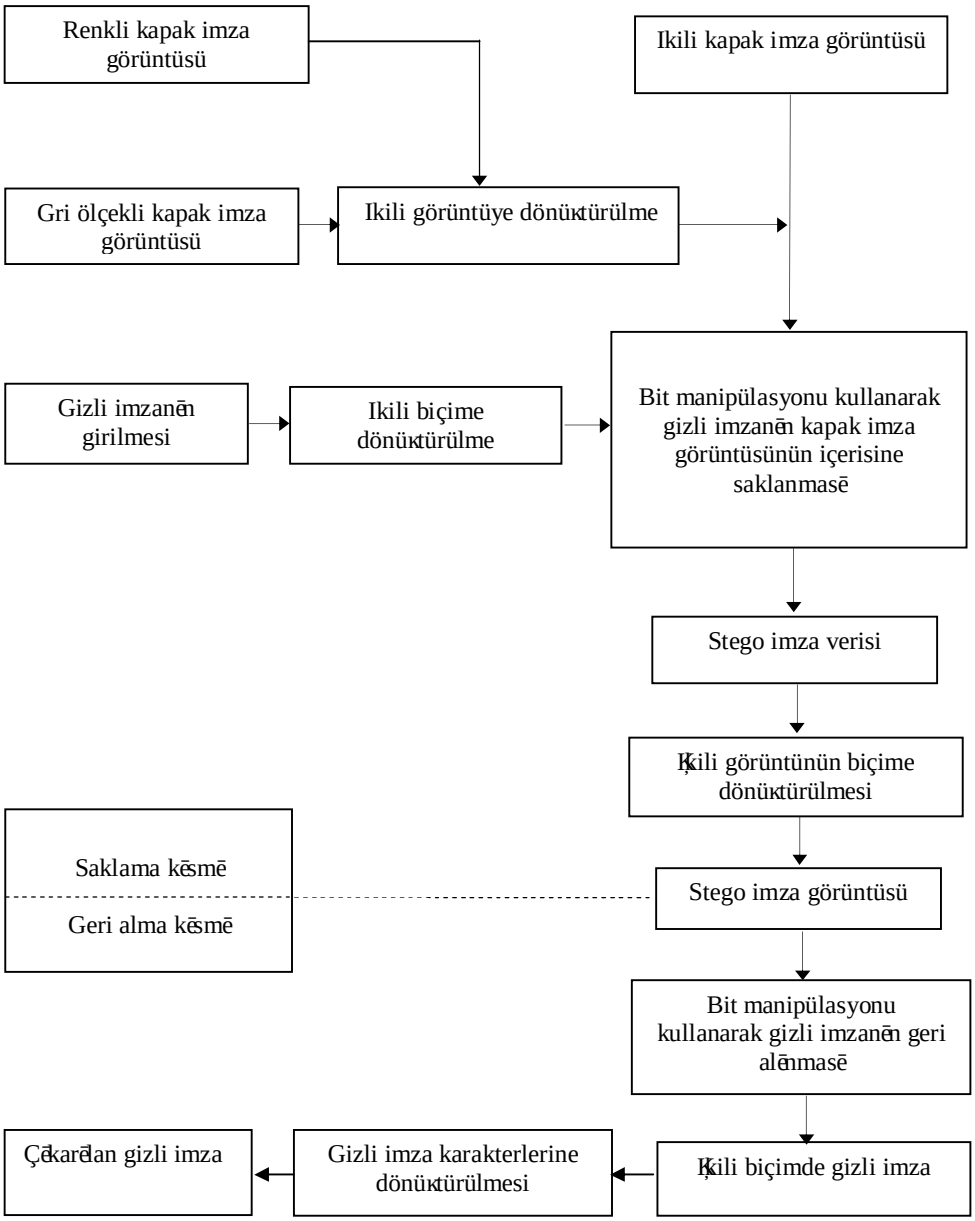
(iii) Saklama bant genişliğinin yeterince yüksek olması.

3.2. Başlatma

İmza görüntüsü örnekleri bir Windows donatısı olan. Paint yazılımı kullanılarak elde edilmiştir. Bu örnekler ACDSee yazılımı kullanılarak gösterilmiştir. Önerilen modeller araçlığıyla görüntü işleme, Visual Basic programlama dili kullanılarak uygulanmıştır. Visual Basic yazılımı kullanılmasının avantajlarından birisi görüntünün gövdesinin (görüntü verilerinin) Pascal, C, ya da Fortran lisanlarında olduğu gibi özel program kullanılmaksızın doğrudan alınabilmesidir.

İmza görüntüleri bmp dosya biçimleri olarak saklanmaktadır. Bmp (Bit eşlem) dosya şekli yalnızca Windows platformundaki bit eşlem grafikleri için kullanılmaktadır. Görüntü verisini üstten aşağıya ve kırmızı, yeşil, mavi sıralamasıyla saklayan dosya biçiminin aksine, bmp biçimi görüntü verilerini aşağıdan yukarı ve pikseller mavi, yeşil, kırmızı sıralamasında saklamaktadır. bmp dosyası genellikle çok büyüktür ve bmp biçimindeki bir dosyayı kaydederken, dosya

isminin sonuna ñ.bmpò dosya uzantēsē eklenmelidir. bmp dosya biçimi iki bölüme ayrēlmēktadēr, bunlardan birincisi ñGörüntü Adēò dosya adē, dosyanēn büyüklüğü ve bmp veya (jpg vs) dosya tipi gibi görüntü bilgilerini saklayan baölēk kēsmēdēr. Ikinci bölüm ise, görüntü bilgisinin saklandēğē dosyanēn gövdesi olarak adlandērēlmaktadēr [17].



şekil 3.1. Ikili görüntü kullanarak imza steganografi modeli

3.3 . İkili Görüntü Kullanarak İmza Steganografi Modeli

Bu tezde önerilen ve gerçekleştirilen model ,saklama ve geri alma olmak üzere iki kısıma ayrılmaktadır.

İkili görüntü kullanarak imza steganografi modeli şekil 3.1.'de gösterilmektedir.

3.3.1. Saklama (gömme) kısmı

İkili olmayan kapak imza görüntüsünün ikili görüntüye dönüştürülmesi

Bu modelin saklama tarafındaki ilk işlemdir. Bu süreçte, ikili olmayan bir görüntü (renkli ya da gri ölçekli bir görüntü) ikili görüntüye dönüştürülmektedir. Her bir 8 biti 1 bitlik değere dönüştürmek üzere, 128 eşik değeri alınmıştır. Eğer 8 bitlik değer eşik değerinden daha fazla ise 1 ikilik değeri elde edilmektedir. Eğer 8 bitlik değer eşik değerinden daha az ise 0 ikilik değeri elde edilmektedir. Bu teknik ikili kapak imza görüntüsü olması durumunda göz önünde bulundurulmuştur. Bu gibi bir durumda, 0'dan eşik değerden düşük olması ve 1-255 eşik değerinden daha büyük olmasından nedeniyle yapılacak hiç bir şey yoktur. Dolayısıyla, bu adımda kapak imza ikili olmayabilir ya da ikili olabilir ancak sonuç daima ikili görüntüyle ilgili olmalıdır. Akağıdaki bu konu ile ilgili algoritma verilmiştir.

İkili olmayan kapak imza görüntüsünün ikili görüntüye dönüştürülmesinin Algoritması

GİRİŞ : İKİLİ OLMAYAN KAPAK GÖRÜNTÜSÜNÜN DOSYASI
ÇIKTI : İKİLİ KAPAK GÖRÜNTÜSÜNÜN DOSYASI

```
WHILE NOT END OF INPUT FILE
1- FROM INPUT FILE RED CHAR
2- IF CHAR VALUE < 128
{
3- OUTPUT FILE = (0)
 }
```

```
ELSE
  {
4- OUTPUT FILE = (1)
  }
} END WHILE
```

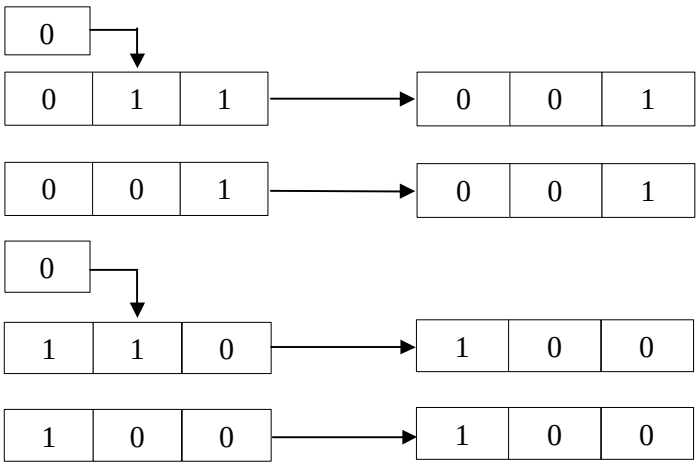
Gizli imzanın girilmesi ve ikili biçime dönüştürülmesi

Bu gizleme tarafındaki ikinci süreçtir. Gizli imza bir dizi karakter ve ondalık sayıdır. Bu noktada gizli imza kapak imza büyüklüğünden daha fazla olmayan bir büyüklükle modele girilmektedir. Gizli imza her bir karakterin sekiz bitten oluştuğu göz önünde bulundurularak ikili formdaki dosyaya dönüştürülebilir. Daha sonra bu karakterin ASCII değeri göz önünde bulundurulur. Bundan sonra, bu ASCII değeri ondalık noktasından sonraki küsuratları ihmal edilerek ikiye bölünür. Eğer küsuratı ihmal etmeden önceki sonuç ihmal ettikten sonraki sonuca eşitse, bu durumda ikili değer sıfırdır, diğer halde ikili değer birdir. Aşağıda bu konu ile ilgili algoritma verilmiştir.

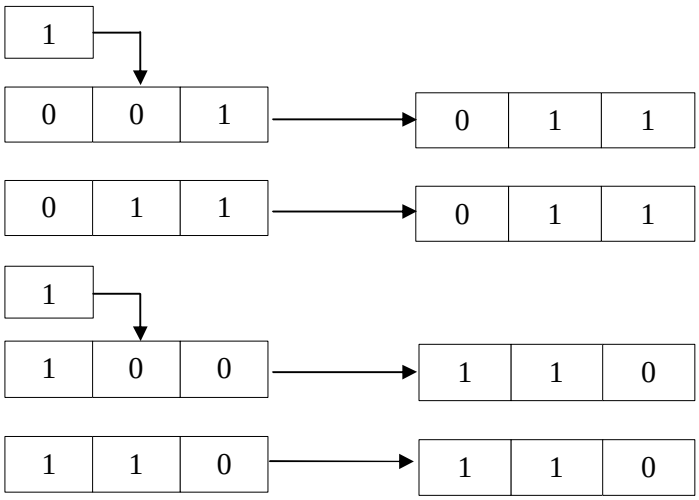
Gizli imzanın girilmesi ve ikili biçime dönüştürülmesinin algoritması

```
GİRİŞ : GİZLİ İMZA
ÇIKTI : İKİLİ BİÇİM DOSYASI
        WHILE NOT END OF SECRET MESSAGE
        {
        1- READ A CHAR
           FOR ( 1→8 ) DO
        {
        2- ASCII VALUE OF CHARACTER
        3- DIVIDE ASCII  VALUE BY 2
        4- TAKE THE INTEGER VALUE OF DIVIDE ASCII  VALUE BY 2
        5- IF (THE VALUE OF STEP 3 = THE VALUE OF STEP 4)
              BINARY = 0
           ELSE
              BINARY  = 1
```

6- PUT ASCII VALUE = RESULT OF STEP 4
7- OUTPUT FILE = BINARY
} END (END FOR)
} END (END WHILE)



(a) 0õ gizlemek için



(b) 1õi gizlemek için

ķekil 3.2. 3-bitlik manipülasyon kullanarak saklama (gömme) teknikleri (a) 0õ gizlemek için (b) 1õi gizlemek için

Bit işlemleri kullanarak gizli imzanın kapak imza görüntüsünün içerisine saklanması

Bu, modelin saklama tarafındaki üçüncü sürecidir. Bu tekniğin fikri bit işlemidir. Saklayan kapak imza dosyasından gizli imzanın her bir bitiyle birlikte bir pencerede üç bitlik bir blok alınır. Bu saklama süreci, bütün olasılıklarının yani (2^3=8) göz önünde bulundurulduğu durum şekil 3.2'de gösterilmiştir.

Gizli imza bitleri ve kapak imza bloğu arasında karşılaştırma yaparak, şekil 3.2.'deki fikre dayalı olarak stego imza dosyasına yeni bloklar eklenmektedir. Gizli imza bitlerinin tamamlanmasından sonra, kapak imzasının bloklarının değiştirilmeden kalmaktadır. Aşağıdaki bu konu ile ilgili algoritma verilmiştir.

Bit işlemleri kullanılarak gizli imzanın kapak imza görüntüsünün içerisine saklanması algoritması

GİRİŞ : İKİLİK KAPAK GÖRÜNTÜSÜNÜN DOSYASI , İKİLİK GİZLİ İMZA DOSYASI

ÇIKTI : STEGO İMZA VERİSİNİN DOSYASI

```
WHILE NOT END OF (INPUT FILE (100))
{  WHILE NOT END OF (INPUT FILE (200))
{
1- READ  3 BIT FROM INPUT FILE  (100)
   2- WHILE (BLOCK = 000   OR   010   OR  101   OR   111)
      { FROM INPUT FILE (100) READ ANOTHER 3 BIT  }
   1-  READ BIT FROM INPUT FILE (200)
   2-  IF  BIT = 0 AND BLOCK = 011
            BLOCK = 001
       IF BIT = 0 AND BLOCK = 110
            BLOK = 100
       IF BIT = 1 AND BLOK = 001
            BLOCK = 011
       IF  BIT = 1  AND  BLOCK = 100
            BLOCK = 110
   } END WHILE
```

```
3- READ BLOCK FROM INPUT FILE (100)
4- OUTPUT FILE  = BLOCK
        } END WHILE
```

Gizli stego imza verisinin görüntü biçimine dönüştürülmesi

Bu, modelin saklama tarafındaki son sürecidir. Bu teknik görüntü bakılacak kısmına (karakterlere dönüştürdükten sonraki stego görüntü verileriyle) birleştirme tekniği idir. Aşağıdaki bu konu ile ilgili algoritma verilmiştir.

Gizli stego imza verisinin görüntü biçime dönüştürülmesinin algoritması

```
GİRİŞ : STEGO İMZA VERİSİNİN DOSYASI
ÇIKTI : STEGO İMZA GÖRÜNTÜSÜ
      1-ADD HEADER BYTES TO BEGINNING OF OUTPUT FILE
       WHILE NOT END OF INPUT FILE
        {
       2-READ A DATA  FROM INPUT FILE.
       3-CONVERT A DATA INTO A CHAR
       4- OUTPUT FILE = CHAR
     }
       END WHILE
```

3.3.2. Geri alma kısmı

Bit işlemi kullanılarak gizli imzanın geri alınması

Bu işlem bu modelin geri alma tarafındaki ilk sürecidir. Bu tekniğin esası her bir bloktaki sıfır ve birlerin sayısına bağlıdır. Bir pencere (üç bitlik bir blok) stego kapak imza dosyasından alınmaktadır. Eğer bloktaki ardışık sıfırların sayısı çiftse, sonuç dosyasına (gizli imza veri dosyasına) sıfır konulur. Eğer bloktaki kesintisiz birlerin sayısı çiftse, bu durumda sonuç dosyasına bir konulur. Geri alma süreci şekil 3.3.'de gösterilmektedir.

Stego kapak imza bloğu			Stego kapak imza bloğu			Çıkış (gizli imza biti)
1	1	1	0	0	1	0
0	1	0	1	1	0	1
1	0	1	1	0	0	0
0	0	0	0	1	1	1

(a) İşlemal edilen bloklar (b) Önemli olan blolklar

Şekil 3.3. 3-bitlik manipülasyon kullanarak geri alma teknikleri fikri , (a) İşlemal edilen bloklar, (b) Önemli olan blolklar

Şekil 3.3.'te tanımlanan sürece stego kapak imza dosyasının son bloğuna kadar devam edilecektir. Aşağıdaki bu konu ile ilgili algoritma verilmiştir.

Bit manipülasyonu kullanılarak gizli imzanın geri alınması algoritması

```
GİRİŞ : STEGO İMZA GÖRÜNTÜSÜ
ÇIKTI : GİZLİ İMZA VERİSİ
WHILE NOT END OF INPUT FILE
{
 1- FROM INPUT FILE  READ 3 BIT
   2- WHILE ( BLOCK = 010  OR  000  OR 111  OR  101 )
          { FROM INPUT FILE  READ  ANOTHER 3 BIT }
   3- WHILE ( BLOCK  = 100  OR  001  OR  110  OR  011 )
   4-IF  NUMBER OF  ZEROS IN 3 BIT IS EVEN
      OUTPUT FILE = 0
   5-IF  NUM OF  ONES IN BLOCK IS EVEN
       OUTPUT FILE = 1
  }  END WHILE
```

İkili gizli imzanın gizli imza karakterlerine dönüştürülmesi

Bu, modelin geri alma tarafındaki ikinci sürecidir. Bu işlemde, ikili gizli imzanın her sekiz biti bir karaktere dönüştürülür. Bu karakterler orijinal gizli imzadır. Aşağıda bununla ilgili algoritma verilmiştir.

İkili gizli imzanın gizli imza karakterlerine dönüştürülmesinin algoritması

GIRIŞ : İKİLİ GİZLİ İMZA DOSYASI
ÇIKTI: ORİJİNAL GİZLİ İMZA
WHILE NOT OF INPUT FILE
{
1- FROM INPUT FILE READ (8) BITS
VALUE = FIRST BIT × 128 + SECOND BIT
× 64 + THIRD BIT × 32 + FOURTH BIT
× 16 + FIFTH BIT × 8 + SIXTH BIT
× 4 + SEVENTH BIT × 2 + EIGHTH BIT
2- ASCII OF VALUE
3- CHAR OF SIGNATURE = VALUE IN STEP2
4- OUTPUT FILE = CHAR OF SIGNATURE
} END WHILE

4. İKİLİ GÖRÜNTÜ KULLANARAK İMZA STEGANOGRAFI MODELİNİN GELİŞTİRİLMESİ

Gömülü bilginin olabilirliğinin testinde ele alınan yaklaşım olarak, aşağıdaki adımları içeren bir test metodolojisi tanımlanmıştır [7].

(i) Mevcut görüntüler kullanılması ya da test için görüntüler oluşturulması.
(ii) Görüntülere mesajlar gömülmesi.
(iii) Sonuçta ortaya çıkan stego görüntünün gömülü mesajları içerdiğinin doğrulanması.
(iv) Sonuçta ortaya çıkan stego görüntünün orijinal görüntülerle karşılaştırılması.
(v) Farklı mesajlar ve/veya farklı görüntüler kullanırken örüntüler (pattern) aranması.

4.1. Test Örnekleri

Kapak imza görüntülerinin dijital sunumu ikili görüntüler için 1-bit, gri ölçekli görüntüler için 8-bit ve renkli görüntüler için 24-bit çözünürlükteki (bmp) biçimidir. Kapak imza görüntülerinin test örneği Çizelge 4.1'de verilmektedir ve Gizli İmza Test Örneği Çizelge 4.2'de gösterilmektedir:

Çizelge 4.1. Kapak imza görüntülerinin test örnekleri

Örnek Adı	Piksel	Büyüklüğü	Özellikler
kapak 1	340×148	50.1	gri ölçekli
kapak 2	368×185	199	Renkli
kapak 3	400×195	9.96	İkili
kapak 4	246×132	95.4	Renkli
kapak 5	247×204	6.43	İkili

Çizelge 4.2. Gizli imza test örnekleri

Örnek Adı	**İmza**
Gizli imza 1	Gazi#
Gizli imza 2	Sara!2
Gizli imza 3	G60u?4
Gizli imza 4	4538
Gizli imza 5	c81bxin!3

4.2. Sistemin Testi

Nesnenin aslına uygunluk kriteri aşağıdaki eşitlik 4.1'deki gibi ifade edilebilir [18]. Eğer orijinal kapak görüntü h(x,y) öğelerinden oluşan (NxN)'lik bir diziden oluşuyorsa ve stego kapak görüntü g(x,y) öğelerinden oluşan (NxN)'lik bir diziden oluşuyorsa, ve burada: x,y=0, 1, 2, … N-1 ise, bu durumda görüntü dizisinin ortalama kare hatası (e^2) :

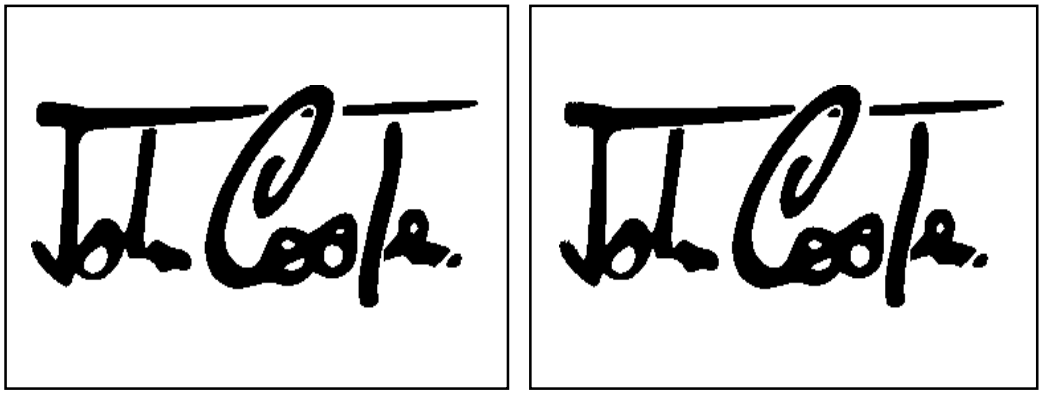
$$\mathbf{e^2} = \left(\frac{1}{N^2}\right) * \sum_{x=0}^{N-1}\sum_{y=0}^{N-1} [\, g(x,y) - h(x,y) \,]^2$$

$$\mathbf{e_{rms}} = \sqrt{e^2}$$

Stego kapak görüntülerinin ortalama karesi alınmış Sinyal-Gürültü Oranı (SNRms) eşitlik 4.3'deki gibi tanımlanır:

$$\mathbf{SNR_{ms}} = \sum_{x=0}^{N-1}\sum_{y=0}^{N-1} \frac{[g(x,y)]^2}{\sum_{x=0}^{N-1}\sum_{y=1}^{N-1} [g(x,y) - h(x,y)]^2}$$

Orijinal imza görüntüsü olarak, 8- bitlik gri ölçekli görüntü kullanılarak önerilen modelle gizli imzasız gömülmüş ve geri alınmış stego imza görüntüsü arasındaki karşılaştırma, Şekil 4.1'de gösterilmektedir. Şekil 4.1'de, Çizelge 4.1'de tanımlanan kapak imza görüntüsü örneği (kapak1) ve gömülü gizli imza (Çizelge 4.2'de tanımlanan Gizli imza1'dir)



(a) Orijinal görüntü (kapak1) (b) Stego imza görüntüsü

(c) gizli imza (Gizli imza 1)

Şekil 4.1. 8-bitlik tek renk görüntü kullanarak, (a) Orijinal imza görüntüsü (b) Stego imza görüntüsü (c) gizli imza

Esas imza görüntüsü ve 24- bitlik renkli görüntü kullanılarak önerilen modelle gizli imzasız gömülmüş ve geri alınmış stego imza görüntüsü arasındaki karşılaştırma, Şekil 4.2'de gösterilmektedir. Şekil 4.2'de, Çizelge 4.1'de tanımlanan kapak imza görüntüsü örneği (kapak2) ve gömülü gizli imza (Çizelge 4.2'de tanımlanan Gizli imza4'dir).

(a) Orijinal görüntü (kapak2)

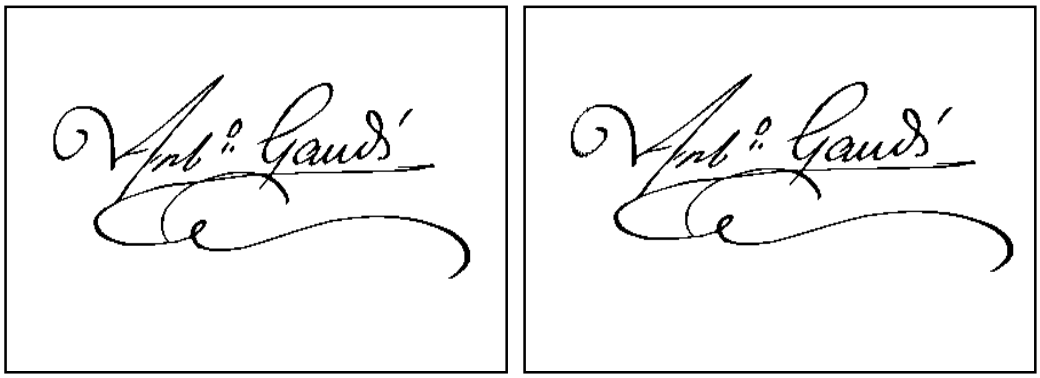
(b) Stego İmza görüntüsü

4538

(c) gizli imza (Gizli imza4)

Şekil 4.2. 24- Bitlik renkli görüntü kullanarak, (a) Orijinal imza görüntüsü (b) Stego imza görüntüsü (c) Gizli imza

Orijinal imza görüntüsü ve 1- bitlik ikili görüntü kullanılarak önerilen modelle gizli imzasın gömülmüş ve geri alınmış stego imza görüntüsü arasındaki karşılaştırma, şekil 4.3'de gösterilmektedir. Şekil 4.3'de, Çizelge 4.1'de tanımlanan kapak imza görüntüsü örneği (kapak3) ve gömülü gizli imza (Çizelge 4.2'de tanımlanan Gizli imza2'dir).



(a) Orijinal görüntü (kapak3) (b) Stego imza görüntüsü

Sara!2

(c) gizli imza (Gizli imza2)

şekil 4.3. 1-bitlik ikili görüntü kullanarak, (a) Orijinal imza görüntüsü (b) Stego imza görüntüsü (c) Gizli imza

Önerilen modelin hesaplanan sonuçları Çizelge 4.3.'te gösterilmektedir.

Çizelge 4.3. Önerilen modelin hesaplanan sonuçları

erms	SNR	Gömme için gereken zaman (s)	Geri alma için gereken zaman (s)
0.0035	47.105	0.65	0.57

4.3. Diğer Testler

Her bir steganografi ve fligran aracıyla, gizlenen bilginin algılanıp algılanmayacağını ve geri kazanılıp kazanılmayacağını belirlemek üzere bir dizi test yapılmıştır [4].

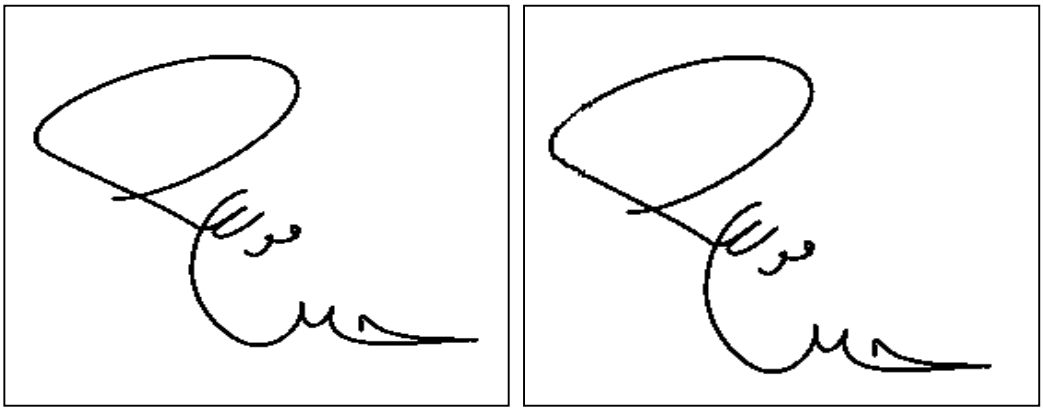
Aşağıdaki test bu çalışmanın olabilirliğini ölçmek üzere yapılmıştır.

Önerilen modeli ,Çizelge 4.1'de tanımlanan, 1 bitlik test örneği ve Çizelge 4.2'de tanımlanan farklı gizli imzalarla kullanarak, stego örtü imza 1 bitten 8 bite ya da 24 bit görüntüye dönüştürüldü. Bu modelde gömülü gizli imza normal gözle algılanamamış ve geri alınabilmiştir.

5. SONUÇLAR

Önerilen model, ikili görüntü kullanarak imza içinde imza saklanmasının bakış açısıyla kullanılabileceği ini göstermiştir.

İkili görüntüde çok fazla seçeneğe izin verilmediği için (pikseller 0 ya da 1 değerliklidir), ikili görüntüler saklama tekniklerinin uygulanmasında tek renkli ya da renkli görüntülere nazaran daha zordur. Şekil 5.1.'da gösterildiği gibi saklama bant genişliği önerilen modelde sınırlıdır.



(a) Orijinal görüntü (kapak5) (b) Stego İmza görüntü

c81bxin!3

(c) gizli imza (Gizli imza 5)

Şekil 5.1. Saklama bant genişliğinin etkisi (a) Orijinal kapak imza (b) Stego imza görüntüsü (c) Gizli imza

Önerilen modelde saklama tekniği fikri 3-bitlik bloğa dayalıdır. Olasılık sayısını azaltmak üzere 3 bitlik seçenek kullanılmıştır. Olasılıklar şekil 3.2 ve 3.3'te gösterilmektedir. Şekil 3.2 ve 3.3'ün fikri: Sınırdaki siyah pikselin bir grup siyah

piksele eklenmesi ve bir grup siyah pikselden sēnērdaki siyah pikselin silinmesi insan görsel sisteminde hiç bir etkiye sahip deĵildir.

Önerilen modelin uygulanmasē kapak imza görüntüsünün tipi, gizli imzanēn büyüklüĵü, blok (pencere) büyüklüĵü ve deĵiken gömülme konumlarē gibi önemli faktörlerin göz önünde bulundurulmasēgerektiĵini göstermiktir

KAYNAKLAR

1. ķahin, A. , ñGörüntü Steganografide Kullanēlan Yeni Metodlar ve Bu Metodlarēn Güvenilirlikleri " ***Trakya Üniversitesi , Fen Bilimleri Enstitüsü*** , p1,2, 2007 Edirne.

2. Katzenbeisser, S., Petitcolas F., ñInformation Hiding Techniques for Steganography and Digital Watermarkingò, Artech House, INC. 685 Canton Street Norwood, MA 02062, 2000.

3. Min, W. , Bede, L ., "Data Hiding in Binary Image for Authentication And Annotation", ***Proc. IEEE***, Transaction on Multimedia, Vol. 6 August (2004)

4. Stefan, K. , Fabien, A. Petitcolas, B. , "Information Hiding Techniques for Steganography and Digital Watermarking ", ***Book from Artech House Inc***, (2000).

5. Fabien , A. Petitcolas, R., Anderson , J. , Kuhn ,M. *," Information Hiding–a survey"*, ***proc. IEEE***, vol.87, pp.1062ï 1078, (July 1999)

6. Tuomas, A. ,"Invisible Communication", Seminar on Network Security in Proceeding of the HUT (EPSOO' 95), also available from Telecommunications Software and Multimedia Laboratory, ***Helsinki University of Technology***, Finland, November (1995)

7. Johnson F. Neil, Z., Sushil J., "Information Hiding: Steganography and Watermarkingï Attacks and Countermeasures", ***Book from Kluwer Academic Publishers ,(*** 2001).

8. Anderson,R. , Needham, R., Shamir, A., "The Steganographic File System" , ***Information Hiding: Second International Workshop Proceedings***, Vol.1525 of lecture Notes in Computer Science, spring, PP. 73-82, (1998)

9. Laurunce, B. , Ahmed, H . Tewfik, T. , Khalid, N ., " Digital Watermarks for Audio Signal " , ***Department of Electrical Engineering, University of Minnesota***, , (1996)

10. Joachim J.,Egger,E. Bauml, R., Girod,E., "A Communication Approach to Image Steganography ", ***security and Watermarking of Multimedia Contents IV***, Proceedings of SPIE, Vol. 4675, (2002).

11. Internet : Computer Science Division University of California, " Digital Music Distribution and Audio Watermarking ", http://www.cs.brekely.edu (2000)

12. Joachim J., Bauml, R., Bernd, G., "Digital Watermarking Facing Attacks by Amplitude Scaling and Additive White Noise", ***4th Intl .ITG Conference on Source and Channel Coding*** , Berlin , 28,(2002)

13. Internet: ***Jonthan Sachs***, "Digital Image Basics", http://www.dl-c.com/basics.pdf (1999).

14. Podilchuk,C., Zeng, W., "Image Adaptive Watermarking Using Visual Models", ***IEEE Journal Selected Areas of Communications (JSAC),*** vol.16, no.4, May,(1998)

15. Matsui,K., Tanaka,K., "Video-Steganography: How to Secretly Embed a Signature in a Picture", ***Proc. of IMA Intellectual Property Project***, vol.1, no.1, (1994)

16. Internet: *Maxemchuk, S. Low*: "Marking Text Documents", http://citereer.ist.psu.edu/maxemchuk97marking.html, (1997).

17. Koch, E. , Zhao,J. "Embedding Robust Labels Into Images for Copyright Protection", ***Proceedings of the International Congress on Intellectual Property Rights for Specialized Information, Knowledge & NewTechnologies***, (1995)

18. Gonzalez R., Wintz P., " Digital Image Processing ", Book from ***Addison–Wesely Publishing Company***, 1987

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, Adı : AL-KARAWI, Muntadher Khamees
Uyruğu : Irak
Doğum Tarihi ve Yeri : 03.09.1979, Baquba
Medeni Hali : Evli
Telefon : 05546495048
Faks :
e-mail : montadery@yahoo.com

Eğitim

Derece	**Eğitim Birimi**	**Mezuniyet tarihi**
Yüksek Lisans	Gazi Üniversitesi / Bilişim Enstitüsü	2012
Lisans	Al-Mustansiriyah Üniversitesi/ Bilgisayar Bölümü	2003
Lise	Jlaolaa Lisesi / Irak	1999

İş Deneyimi

Yıl	**Yer**	**Görev**
2003-2011	Diyala Üniversitesi	Araştırma Görevlisi

Yabancı Dil

İngilizce
Türkçe

Hobiler

Satranç, Bilgisayar teknolojileri, Futbol