ANKARA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

STEGANOGRAFİ İLE BİLGİ GÜVENLİĞİ

Batmunkh GANBAT

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

ANKARA
2017

TEZ ONAYI

Batmunkh GANBAT tarafından hazırlanan **"Steganografi ile Bilgi Güvenliği"** adlı tez çalışması 25/05/2017 tarihinde aşağıdaki jüri tarafından oy birliği ile Ankara Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı'nda **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Danışman : Doç. Dr. Semra GÜNDÜÇ
Ankara Üniversitesi Bilgisayar Mühendisliği Anabilim Dalı

Jüri Üyeleri :

Başkan: Yrd. Doc. Dr. İhsan Tolga MEDENİ
Ankara Yildirim Beyazit Universitesi Yönetim Bilişim Sistemleri Bölümü

Üye : Yrd. Doç. Dr. Mehmet Serdar GÜZEL
Ankara Üniversitesi Bilgisayar Mühendisliği Anabilim Dalı

Üye : Doç. Dr. Semra GÜNDÜÇ
Ankara Üniversitesi Bilgisayar Mühendisliği Anabilim Dalı

Yukarıdaki sonucu onaylarım.

Prof. Dr. Atila YETİŞEMİYEN
Enstitü Müdürü

ETİK

Ankara Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına uygun olarak hazırladığım bu tez içindeki bütün bilgilerin doğru ve tam olduğunu, bilgilerin üretilmesi aşamasında bilimsel etiğe uygun davrandığımı, yararlandığım bütün kaynakları atıf yaparak belirttiğimi beyan ederim.

25.05.2017

Batmunkh GANBAT

ÖZET

Yüksek Lisans Tezi

STEGANOGRAFİ İLE BİLGİ GÜVENLİĞİ

Batmunkh GANBAT

Ankara Üniversitesi
Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı

Danışman : Doç. Dr. Semra GÜNDÜÇ

Çağımızda internet kullanımın yaygınlaşmasıyla artmakta olan veri alışverişi ve paylaşımlarını çeşitli yöntemleriyle daha güvenilir hale getirilmeye çalışılmaktadır. İnsanlar ve kurumlar arası bilgi güvenliğini sağlamak amacıyla steganografi hakkında çok sayıda literatür bulunmaktadır. Bu çalışmada bu literatürleri derleyerek günlük bilgi güvenliği için Metin, Görüntü ve Ses steganografi yöntemleri incelenecek ve resim dosyası içerisine resim, düz metin saklamak için bir yazılım geliştirilmiştir. Haberleşme güvenliğinin sağlamasının yanında bilgi güvenliğinin de sağlanması için AES şifreleme seçenekleri geliştirilen yazılım içerisinde sunulmuştur. Geliştiren yazılımda bir anahtar yardımıyla, belirlenen JPEG ve BMP dosyaları içerisine LSB modifikasyonu yöntemiyle rastgele saklama gerçekleştirmektedir. Bu tez çalışmasında geliştirilen yazılım ile hem iletişim hem de veri gizliliği sağlanabilmiştir.

Mayıs 2017, 49 sayfa

Anahtar Kelimeler: Steganografi, Bilgi Güvenliği, Güvenli Veri İletişimi, Görüntü Steganografi, Ses Steganografi, Metin Steganografi, LSB , JPEG steganografi

ABSTRACT

Master Thesis

INFORMATION SECURITY BY STEGANOGRAPHY

Batmunkh GANBAT

Ankara University
Graduate School of Natural and Applied Sciences
Department of Computer Engineering

Supervisor: Assoc.Prof.Dr. Semra GÜNDÜÇ

In this age of widely increased usage of Internet, data exchange and sharing have been challenged by different methods to bring it into more reliable form. Many literatures about steganography, which are for the purpose of ensuring the information security between individuals and institutions, can be found. In this study, by compiling those literatures, Text, Image and Audio steganography methods will be examined and a software have been developed to store stego image and flat Text into cover image for daily information security. In order to provide communication safety beside information security, different options of encryption as AES have been presented in the developed software. In the developed software, random storage performs with LSB modification method inside JPEG and BMP files which are stated with the aid of a key. With the software developed in this thesis study, both communication and data security are achieved.

May 2017, 49 pages

Key Words : Steganography, Information Security, Secure Data Communication, Image Steganography, Audio Steganography, Text Steganography**,** LSB, JPEG Steganography

TEŞEKKÜR

Bu çalışmanın hazırlanması esnasında bana yol gösteren , bu alanda çalışmam için beni teşvik eden, yardımlarını ve desteğini benden esirgemeyen değerli danışman hocam Doç. Dr. Semra GÜNDÜÇ'e (Ankara Üniversitesi Bilgisayar Mühendisliği Anabilim Dalı) teşekkür ederim.

Bilgi Güvenliği konusunda kendilerinden çok şeyler öğrendiğim Gazi Üniversitesi Fen Bilimleri Enstitüsü Müdürü Sayın Prof. Dr. Şeref SAĞIROĞLU'a,

Çalışmalarım sırasında değerli katkılarıyla bana yardım eden arkadaşlarım Abubakr RAKHIMOV , Taner YILDIZ ve Gantulga BAASANJARGAL'a,

Son olarak manevi desteğini benden esirgemeyen tüm hocalar ve arkadaşlarıma teşekkür ederim.

Batmunkh GANBAT
Ankara , Mayıs 2017

İÇİNDEKİLER

KISALTMALAR DİZİNİ

3DES	Triple Data Encryption Standard -Üçlü Veri Şifreleme Standardı
AES	Advanced Encryption Standard - Gelişmiş Şifreleme Standardı
AIIF	Audio Interchange File Format - Ses Değişim Dosya Format
BMP	Windows Bitmap - Nokta esaslı
CBC	Cipher Block Chaining - Şifreli Blok Zinciri
DCT	Discrete Cosine Transform - Ayrık Kosinüs Dönüşümü
DES	Data Encryption Standard - Veri Şifreleme Standardı
DFT	Discrete Fourier Transform - Ayrık Fourier Dönüşümü
DOS	Disc Operating System - Disk İşletim Sistemi
GIF	Graphics Interchange Format - Grafik Değiştirme Biçimi
HAS	Human Auditory System - İnsan İşitme Sistemi
HTML	HyperMetin Markup Language - Üstün Metin İşaretleme Dili
IDEA	International Data Encryption Algorithm – Uluslararası Veri Şifreleme Algoritması
IP	Internet Protocol - internet protokolü
JPEG	Joint Photographic Experts Group - Birleşik Fotoğrafik Uzmanlar Grubu
LSB	Least Significant Bit - En az Önemli Bit
MD5	Message-Digest Algorithm 5 - Mesaj Alma Algoritması 5
MPEG	Moving Picture Experts Group - Hareketli Resim Uzmanları Grubu
MSE	Mean Squared Error - Ortalama Kare Hata
PAE	Peak Absolute Error - Zirve Mutlak Hata
PCBC	Propagating Cipher Block Chaining - Şifreli Blok Zincirliğini Yaymak
PNM	Portable Any Map - Taşınabilir Harita
PNG	Portable Network Graphics - Taşınabilir Ağ Grafikleri
PoVs	Pairs of Values - Değer Eşleri
PSNR	Peak SNR (Signal-to-Noise Ratio) - Tepe SNR (Sinyal-Gürültüyü Oranı)
RQP	Raw Quick Pairs - İşlenmemiş Hızlı Çiftler
RMSE	Root MSE (Mean Squared Error) - Kök MSE (Ortalama Kareli Hata)
WAV	Windows Audio-Visual - Ses Dosyası Biçimidir

ŞEKİLLER DİZİNİ

ÇİZELGELER DİZİNİ

1. GİRİŞ

Bilgi güvenliği, ”bilginin dış tehditlerden korunması, bilginin her türlü ortamda doğru teknolojinin doğru amaçla ve doğru şekilde kullanılmasıyla, istenmeyen kişiler tarafından elde edilmesini önleme olarak” tanımlanır (Koçak 2015).

Bilgi, insanlığın yaşamını, davranışını, iletişimini, düşüncesini, tüketmesini belirleyen faktörlerin başında her zaman yerini koruyan ve en değerli varlıktır (Kaygusuz 2003, Koçak 2015).

Tarih boyunca kişiler, kurumlar ve ülkeler varlıklarını korunmak için çeşitli şifrelemeler kullanmışlardır. Çünkü bilgi, elde edilmesi ve aynı zamanda elde tutulması zor olan bir varlıktır (Kaygusuz 2003).

Bilgi güvenliği, bilgiyi yetkisiz erişimlerden koruyarak gizliliğini sağlamayı, bilginin bozulmadan bütünlüğünü ve doğruluğunu temin etmeyi ve istenilen zamanda erişilebilirliğini garanti etmektedir.

Son yıllarda internet kullanımının yaygınlaşmasıyla veri alışverişi, veri paylaşımı ve insanlar arasındaki iletişim artmıştır. Buna bağlı olarak bilgi güvenliği sorunları karşımıza çıkmaktadır.

Günümüzde bilgi güvenliği, fiziksel ve çevresel güvenlik, haberleşme güvenliği, bilgisayar güvenliği, ağ güvenliği, uygulama güvenliği, veri tabanı güvenliği ve web güvenliği gibi güvenlik önlemleri ile sağlanmaktadır.

Bilgi güvenliği önlemleri arasında en yaygın önlemlerden biri haberleşme güvenliğidir.

Haberleşme, karşılıklı olarak bilgi alışverişinde güvenli bir haberleşme ortamını oluşturmak için yapılan faaliyetlerin ortak adıdır. Haberleşme anında fiziksel olarak bilgilerin güvenliğinin sağlanması, güvenlik açısından yeterli değildir. İletişim sırasında

bilginin hedefe ulaşmadan önce başka kişiler tarafından ele geçirilmesi ve içeriğinin öğrenilmesi riski her zaman mevcuttur. Haberleşme güvenliğinin sağlanmasında kullanılan yöntemler tarih boyunca değişmemiş fakat bu güvenliği sağlamak için kullanılan teknikler ve yöntemler sürekli olarak gelişmiştir.

Haberleşme güvenliğinin sağlanmasında iki temel yöntem kullanılmaktadır. Bu yöntemler kriptografi ve steganografı yöntemleridir.

Kriptografi yönteminde mesajın varlığı bilinir ancak içeriği anlaşılamaz. Steganografi yönteminde ise mesaj görülemeyecek şekilde saklanır.

Bilgi Güvenliği için mevcut yöntemler kendi içinde yetersiz değil ancak uygulanabilirlik açısından eksiktir. Bu tez çalışmasındaki amacımız haberleşme güvenliğinin sağlamasında kullanılan yöntemlerin uygulanabilirliği konusundaki eksikliği gidermek ve mevcut durumu daha iyi hale getirmektir. Bu iyileştirmeyi sağlamak için de kriptografi ve steganografi yöntemleri bir araya getirilerek bir yazılım geliştirilmiştir. Geliştirilen bu yazılımda bir görüntü steganografi yöntemi olan LSB modifikasyonu kullanılarak resim dosyası içerisine resim veya düz metin saklanıp iletilecek mesajın görüntülenmesi engellenmiş ve bir kriptografi yöntemi olan AES şifreleme seçeneği ile de mesajın varlığının bilinmesine rağmen içeriğinin anlaşılamaması sağlanmıştır. Bu sayede hem iletişim hem de veri gizliliği sağlanabilmiştir.

2. KRİPTOGRAFİ

Kriptografi; kimlik doğrulama, veri kaynağı doğrulama, veri bütünlüğü ve gizlilik konuları gibi bilgi güvenliği ile alakalı matematiksel teknik çalışmalardan oluşmaktadır. Kriptografi, Yunanca dilinde gizli/saklı anlamına gelen "kryptos" ve yazı anlamına gelen "graphein" kelimelerinden türetilmiştir. Kriptoloji ise "şifre bilimi" demektir ve bilgi güvenliğini sağlamaktadır. Burada şifrelenecek mesaj "düz metin", dönüşüm sonrasında elde edilen mesaj "şifreli metin", dönüştürme sürecinde kodlama işlemi "şifreleme", tersi işlem de "şifre çözme" olarak isimlendirilir (Kaygusuz 2003, Koçak 2015).

"Açık metin"(clear metin), şifrelenmemiş bir bilgi olarak tanımlanır . Bir insanın okuyabileceği bir yazı ya da bir bilgisayarın anlayabileceği çalıştırılabilir (.exe, .com) bir program ya da bir veri dosyası(.txt) olabilir. Bir kripto(şifreleme) algoritması kullanılarak, herkesin okuyup anlayamayacağı bir şekilde kodlanmış bilgi de "şifreli metin"(criphered metin) adıyla ifade edilir (Kaygusuz 2003, Koçak 2015).

Şifreleme ve şifre çözme işlemlerinde aynı gizli anahtar kullanılmalıdır . Kriptografi işleminde en çok kullanılan yöntem Advanced Encryption Standard (AES) metodudur. AES methodu; ayını zamanda standart Rijndael algoritması adıyla da bilinen, güvenlik ve hız bakımından yüksek verimliliğe sahip bir simetrik anahtar blok şifreleme yöntemidir(Koçak 2015).

2.1 Şifreleme Çeşitleri

AES (Advanced Encryption Standard)

AES metodu 128 bit veri bloklarını 128, 192, 256 bit anahtar seçeneklerini kullanarak şifreleyen algoritma türlerinden biridir. 10 döngüde şifreleme işlemi 128 bit anahtar için yapılırken 12 ve 14 döngüde şifreleme işlemleri ise sırasıyla 192 ve 256 bit anahtarlar için gerçekleştirilmektedir. AES metodunun her bir döngüsü dört katmandan meydana

gelmektedir. İlk etapta 128 bit veri 4x4 byte matrisi olarak ayarlanır. Bundan sonraki işlemler ise her döngüde sırasıyla byte'ların yer değiştirmesi, satırların ötelenmesi, ve sütunların karıştırılmasıdır.

DES (Veri Şifreleme Standardı, Data Encryption Standard)

DES, veri şifrelemek (encryption) ve şifrelenmiş verileri açmak (decryption) için geliştirilmiş bir standarttır. Esas olarak kullanılan algoritma DEA(Data Encryption Algorithm, Veri Şifreleme Algoritması)'dir. Bu algoritmanın standartlaştırılmış halinin ismi DES olarak bilinmektedir (Sharma vd. 2015).

DES yapısı gereği bir blok şifreleme örneğidir. Başka bir deyişle basitçe şifrelenecek olan açık metni parçalara ayırarak (blok) her parçayı birbirinden bağımsız olarak şifreler ve şifrelenmiş metni açmak için de aynı işlemi bloklar üzerinde uygular. Bu blokların uzunluğu ise 64 bitten oluşmaktadır.

RC-4 şifreleme

RC4 algoritması şifrelenecek veriyi akan bir bit dizisi olarak algılayan bir algoritma türüdür. RC4 algoritmasında, veri belirlenen bir anahtar ile şifrelenir.

RC4 algoritmasının başlıca özellikleri şunlardır:

• Genellikle hız gerektiren uygulamalarda kullanılır.
• Şifreleme hızı yüksektir ve MB/sn seviyesindedir.
• Güvenliği rastgele bir anahtar kullanımı ile sağlanır.
• Tekrarlama periyodu 10100′den daha fazladır.
• Anahtar uzunluğu değişkendir.

MD5 şifreleme

MD5 (Message-Digest algorithm 5) algoritması 1991 yılında Ron Rivest tarafından bir tek yönlü şifreleme algoritması olarak geliştirilmiştir. Veri bütünlüğünü test etmek için kullanılır. Bu algoritma girdinin büyüklüğünden bağımsız olarak 128-bit'lik bir çıktı üretir ve girdideki en ufak bir bit değişikliği bile çıktının tamamen değişmesine neden olmaktadır. MD5 en çok, bir verinin (dosyanın) doğru transfer edilip edilmediği veya değiştirilip değiştirilmediğinin kontrol edilmesinde kullanılır.

SHA-1 Şifreleme

• SHA (Secure Hash Algorithm – Güvenli Özetleme Algoritması), Amerika'nın ulusal güvenlik kurumu olan NSA tarafından oluşturulmuştur.

• SHA-1, uzunluğu en fazla 264 bit olan mesajları girdi olarak kullanır ve 160 bitlik mesaj özeti üretir. Bu işlem sırasında, öncelikle mesajı 512 bitlik bloklara ayırır ve gerekirse son bloğun uzunluğunu 512 bite tamamlar. SHA-1 çalışma prensibi olarak R. Rivest tarafından oluşturulan MD5 özet fonksiyonuna benzemektedir. 160 bitlik mesaj özeti üreten SHA-1, çakışmalara karşı aynı zamanda 80 bitlik güvenlik sağlamaktadır Premkumar vd.2014).

2.2 Klasik Şifreleme Teknikleri

Steganography(Metni Gizleme)

Şifrelenmemiş düz bir metnin, çeşitli dönüşümler kullanılarak başka kişiler tarafından anlaşılamaz bir metin haline getirilmesi işlemidir. Verilebilecek en basit örnek, bir metnin bütün harflerinin diğer metnin içindeki sözcüklerin ilk harflerine gizlenmesidir. Örneğin; "**S**ezen **A**ksu **v**e **a**şk **ş**arkıları **b**enim **i**çin **t**üm **t**esellilerden **i**yidir."

Yukarıda verilen örnek cümledeki her kelimenin baş harfleri sırasıyla birleştirilerek oluşturulacak metin, bize aslında örnek cümle içerisinde gizlenmiş mesajı vermektedir.

Fakat her durum için böyle bir mesajı oluşturmak zor ve zaman alıcı olmaktadır. Üstelik bu şifreleme yöntemi ile oluşturulan şifrelerin de kırılması oldukça kolaydır.

Caesar Cipher(Sezar Şifrelemesi)

Bilinen en eski yerine koyma şifreleme yöntemidir. Ünlü Roma İmparatoru Julius Caesar tarafından oluşturulmuştur. Sezar şifrelemesinin mantığı, her harfin kendisinden sonra gelen üçüncü harfle değiştirilmesi kuralına dayanmaktadır.

Örneğin;

düz metin: "Bilgisayarların şifreleri kırıldı"

şifrelenmiş metin: "DLOİUÖÇBÇTOÇTKÖ ÜLHTĞOĞTL NKTKOGK"

Sezar şifreleme yönteminin 3 temel eksiği bulunmaktadır. Bunlardan birincisi, şifrelenmiş metinden hangi dilin kullanıldığının rahatlıkla anlaşılabilir olmasıdır. İkincisi, Türkçe için düşündüğümüz zaman sadece 28 ayrı şifreleme geliştirilebilir olmasıdır. Sonuncusu ise şifreleme ve deşifreleme algoritmalarının biliniyor ve kolaylıkla uygulanabiliyor olmasıdır. Sezar şifrelemesi ile şifrelenmiş bir metin "Brute Force" bir saldırısı ile kırılabilir. Brute Force, kelime anlamı olarak kaba kuvvet demektir. En zayıf ama en kesin saldırı yöntemidir. Sezar şifrelemesi gibi algoritmaların çözümünde olası bütün kombinasyonların denenmesi gereklidir.

Tek Kullanımlık Karakter Dizisi (One-time Pad)

Bu şifreleme yöntemi basit ve kolaydır. Rastgele üretilen bir karakter (harf veya rakam) dizisi kullanılarak şifreleme yapılır. Açık mesaj içinde yer alan her karakter, üretilen

dizide karşısına denk gelen karakterle işleme sokularak (Örneğin modüler toplama işlemi) şifreli mesaj oluşturulur. Mesajın çözülebilmesi için rastgele seçilen dizinin bilinmesi gereklidir. Bu yöntem Vernam şifreleme yöntemi olarak bilinir.

Açık Mesaj : BULUSMAYERIGAZZE

Rastgele Dizi : DEFRYPLCNMLJKHFGH

Şifreli Mesaj : RLDYDOY....

Bu şifreleme yönteminin güvenliği, Rastgele üretilen diziye bağlı olduğu için, bir kurala bağlı kalarak dizi üretilirse ve bu kural saldırgan kişi tarafından bilinirse sistem kolayca kırılabilir.

ROT13 Şifreleme Tekniği

ROT13 (Rotate13) yer değiştirme yöntemi kullanılarak oluşturulan bir Caesar(Sezar) şifreleme türüdür. İngiliz alfabesindeki bir harfin 13 harf sonraki harf ile eşleşmesi mantığına dayanır.

Base64 Şifreleme Tekniği

Kodlama sırasında 3 baytlık veriler 6 bitlik dörtlü gruplara bölünürler. Her bir 6 bitlik grup 0 ile 63 arasında bir sayı oluşturur (26=64). Aşağıdaki eşleşmeye göre her sayı bir ASCII yazdırma karakterine dönüştürülür (Şekil 2.1).

Sayı	Karakter	Sayı	Karakter	Sayı	Karakter	Sayı	Karakter
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/

Şekil 2.1 Karakterlerin ASCII kod karşılıkları

Bir Base64 kodlamasının uzunluğu 4’ ün katları şeklindedir ve uzunluğu 4’ ün katı olmayan hiç bir metin geçerli bir Base64 metin değildir. Base64 kodlaması bitmiş bir verinin uzunluğu 4’ün katı değilse, gerektiği kadar ‘=‘ karakteri çıktının sonuna eklenir, örneğin uzunluğu 10 olan bir çıktının sonuna ‘==‘ eklenmelidir. Bu sayede veri uzunluğu 4’ün katına tamamlanır.

ASCII:ASCII’de 33 tane basılmayan kontrol karakteri ve 95 tane basılan karakter vardır. Kontrol karakterleri metnin akışını kontrol eden ve ekranda çıkmayan karakterlerdir. Basılan karakterler ise ekranda görünen ve okuduğumuz metni oluşturan karakterlerdir.

Açık anahtarlı şifreleme

Açık anahtarlı şifreleme, şifre ve deşifre işlemleri için farklı anahtarların kullanıldığı bir şifreleme yöntemidir. Yöntemin bu özelliğinden dolayı asimetrik şifreleme olarak da bilinmektedir. Haberleşen taraflardan her birinde birer çift anahtar bulunur. Bu anahtar çiftlerinden biri gizli anahtar diğeri açık (gizli olmayan) anahtardır.

Gizli anahtarın tek bir sahibi vardır. Gizli anahtara sahip olan taraf, gizli anahtar yardımıyla, kendi açık anahtarıyla şifrelenmiş bilgilerin şifresini çözebilir, kendisine ait sayısal imzaları oluşturabilir ya da kendi kimliğini ispat edebilir.

Açık anahtar, yalnızca gizli anahtarın sahibi tarafından oluşturulabilir ve herkes tarafından ulaşılabilir. Açık anahtarla, bilgiler sadece gizli anahtarın sahibi tarafından çözülebilecek şekilde şifrelenebilir ya da gizli anahtar sahibinin sayısal imzasının ve kimliğinin doğruluğu kontrol edilebilir.

3. STEGANOGRAFİ

3.1 Steganografi

Bilgi gizleme metotlarının en temel alt dalı olan Steganografi resim, ses veya video görüntüleri içerisine veri saklamak için kullanılan bir bilgi güvenliği yaklaşımıdır. Genel olarak literatürde veri saklama yöntem ise steganografi terimini işaret etmektedir (Şahin 2007). Steganografi eskiden beri kullanılan bilgi gizleme sanatıdır . Yunan alfabesinden türetilmiş ve kökleri "στεγαυος" ve "γραΦειν"'den gelmektedir. Tam anlamı "kaplanmış yazı" (covered writing) demektir.

Steganografi birçok alanda , çeşitli amaçlar için kullanılmaktadır. Örnegin:

− Askeri: Askeri'i alanında iletişimin şifrelemesine alternatif olarak kullanılabilmektedir.Çünkü şifrelenmiş bilgiyi düşman tarafından fark edilebilir. Buna karşılık steganografik yöntemle yapılırsa daha başarılı olacaktır.

− Damgalama and Parmak izi : Damgalama ve Parmak izi saklandığında fark edilmemesi ve güvenli olması gerekir. Bu sebepten dolayı steganografi yönteminden faydalanılmaktadır.

− Sağlık alanı: Birtakım sağlık sistemi görüntüleri ve görüntüler ile ilgili ifadeler bir yere gönderildiği zaman birbirinden ayırt edilebilir ve bu da olumsuz sonuçlara sebep olabilir. Görüntünün içine kendisi hakkındaki bilgiler gizlenirse daha güvenli olacaktır.

Steganografide temel amaç iletişimin gizliliğinin sağlanmasıdır. Yani iki kişi arasındaki paylaşılan özel bilgileri, şahıs veya kurumun önemli bilgileri üçüncü kişi tarafından ele geçmesiyle ortaya çıkan sorunları kaldırmasıdır. Bilgi güvenliğinde diğer bir önemli bilim dalı kriptografidir. Kriptografi ,kimlik doğrulama, veri kaynağı doğrulama, veri bütünlüğü, gizlilik konuları gibi bilgi güvenliği ile ilgili matematiksel teknik çalışmaların bütünüdür. Kriptografinin asıl amaç verinin gizliliğinin sağlanmasıdır. Bu

bağlamda yüksek seviyede güvenli bir iletişim için kriptografi ve steganografi bilimleri birlikte kullanılarak önce verinin daha sonra ise iletişimin gizliliğinin gerçekleştirilmesi yönüyle yüksek seviyede bir bilgi güvenliğinin oluşturulmasına katkılar sağlamaktadır.

3.2 Steganografinin Tarihsel Süreci

Steganografi, son derece eski bir veri gizleme metodudur ve bu metot, Antik Yunan ve Heredot dönemine kadar uzanır. Steganografinin tarihsel gelişim süreci (Çizelge 3.1).

Çizelge 3.1Steganografinin tarihsel gelişim süreci

MÖ 440 Antık Çağlar	- Antik Yunan'da ulakların saçlarının kazınıp, saç derisine mesajın yazılması, ulağın saçları uzayıp varacağı yere gitmesi ve saçların tekrar kazınması (Krenn,2004). - Antik Yunan'da balmumu kaplı tabletlerin kullanımı (Bender,Gruhl,Morimoto ve Lu, 1996). - Antik Çin'de meyve sepetinin kullanımı.Meyve sepetindeki her meyvenin birbirine göre pozisyonu farklı bir anlam ifade etmektedir (Petircolas,Anderson ve Kuhn,1999).
1650	- Gaspar Schott'un müzik notları ile bilgileri kodlaması (Bender,Gruhl,Morimoto ve Lu, 1996).
1918'e kadar	- Görünmez mürekkeplerin kullanımı. İlk olarak I Dünya Savaşında kullanılmıştır. - I. ve II. Dünya savaşları sırasında Semagram'ların kullanımı (Petircolas,Anderson ve Kuhn,1999).
1870-1945	- I. ve II. Dünya savaşları sırasında Microdot'ların kullanımı (Johnson ve Jajodia,1998)
Dijital Çağ	- Dijital çağda,sayısal (dijital) nesneler üzerinde steganografi uygulamaları yapılmaktadır ve gelişen teknoloji nedeniyle, verilerimizi korumak amacıyla son yıllarda sıklıkla kullanılmaya başlanmıştır. Gizli veri, yine masum içeriğe sahip olan bir dizi dosyanın içinde saklanabilmektedir.

Yunan tarihçi Heredot, eserinde (Heredotus, M.Ö. 430), İran'daki ajanın, Pers baskınını Yunanistan'a nasıl ilettiğini kaydetmektedir. Yazıya göre, ajan kölesinin saçını kazıtmış; baskın uyarısını da kafa derisine kazıtmıştır. Daha sonra yapılacak olan, kölenin saçının yazıyı kapatacak kadar uzamasını beklemek ve bu köleyi Yunanistan'a yollamaktır. Köle, sadece "kafamı kazıyın" bilgisini bilmek zorundadır. Benzer şekilde aynı dönemde avcı kılığındaki bir habercinin, avladığı hayvanın karın bölgesine parşömen gizleyerek Yunanistan'a girmesi anlatılmaktadır (Şahin 2007).

Antik çağda steganografinin kullanımı yalnızca Yunanistan ile sınırlı değildir. Çinliler de kendi kaynaklarında meyve sepetini nasıl gizli iletişim için kullandıklarını anlatmaktadırlar. Meyve sepetindeki her meyvenin birbirine göre pozisyonu farklı bir anlam ifade edecektir.

Antik dönemdeki bu basit uygulamalar steganografinin gizli iletişimdeki kullanımının insanlık kadar eski olduğunu bizlere göstermektedir (Şahin 2007).

Steganografi hakkında yazılan ilk kitap Johannes Trithemus (1462–1516) tarafından yazılmış olan Steganographiæ isimli kitaptır. Gaspar Schott 1608–1666 seneleri arasında yaşamıştır ve yazmış olduğu Schola Steganographica (Schott,1665) adlı kitabında müzik notaları kullanılarak nasıl bilgi saklandığından bahsedilmiştir. Bu veri gizleme metodu kendisinden sonra gelen veri gizleme metotlarına da referans olmuştur.

İlerleyen senelerde steganografi yöntemi, metin belgelerindeki harf frekanslarını kullanma, görünmez mürekkep, I. ve II. Dünya Savaşlarında kullanılan mors kodları gibi pek çok uygulamalar ile karşımıza gelmektedir (Katzenbeisser ve Petitcolas 2000).

En etkili kullanımı ikinci dünya savaşında olmuştur. Alman casuslar, İkinci dünya savaşı sırasında kimyasal bir madde aracılığıyla beyaz renkli bir beze bilgi saklamışlardır ancak saklanan bu bilgiler gün yüzüne çıkarılmıştır. Mesaj saklı olan bez Casus tarafından, önceden belirlenmiş olan yerlerde çöpe atılmış ve daha sonra alıcı

tarafından alınan bu beze benzer şekilde kimyasal işlemler uygulanarak saklanmış mesaj ortaya çıkarılmıştır. (Şahin 2007).

İkinci dünya savaşında steganografinin kullanıldığı başka bir durum ise bu dönemde Almanların "mikrofilm" teknolojisi sayesinde "mikro noktalar" (microdot) yöntemiyle tanışmış olmalarıdır. Bu yöntemde bir takım işlemler neticesinde A4 büyüklüğündeki herhangi bir belge veya çizim, daktilo yazısında bulunan bir nokta kadar ufaltılabilmektedir. Herhangi bir metin sayfasındaki noktalı harflerin noktalarına önemli oranda bilgi saklamak bu yöntemin kullanılmasıyla olası duruma gelmiştir (Şahin 2007).

Aşağıda, ikinci dünya savaşında kullanılan bir steganografi örneği verilmiştir (Şahin 2007).

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

Yukarıdaki paragrafta her kelimenin ikinci harfleri birleştirildiğinde "Pershing sails from NY June 1." mesajı verildiği anlaşılmaktadır.

Steganografi, çağımızda sayısal nesneler için uygulanmaktadır ve teknolojinin gelişmesi sayesinde, son yıllarda bilgilerimizi korumak için oldukça sık kullanılan bir yöntem olarak tercih edilmektedir.

Masum bir içeriğe sahipmiş gibi görünen pek çok dosyanın içerisine veri gizlenebilmektedir. Bu dosyalardan en çok resim, video ve ses dosyaları bu amaç için kullanılmaktadır. Ayrıca veri saklamak için; düz metin dosyaları, sabit disklerdeki kullanılmayan alanlar, IP (Internet Protocol) paketlerinin ileride kullanmak içibn ayrılmış kısımları ve bunlara ek olarak html dosyaları, exe dosyaları vb. gibi dosyalar da kullanılabilmektedir.

3.3 Steganografinin Alt Alanları

Dilbilim Steganografi (Linguistic Steganography) ve Teknik Steganografi (Technical Steganography) olarak Steganografi yöntemini ikiye ayırmak mümkündü (Şahin 2007).

Dilbilim Steganografi'de taşıyıcı olarak kullanılan veri Metin'tir. Bu bölümde değişiklik yapmak için bazı yöntemler vardır. Örneğin; grafik kullanılarak yapılabilir, metin'in yapısı değiştirilerek yapılabilir ya da amacı sadece veriyi saklamak olan yeni bir metin yaratılabilir.

Dilbilim Steganografi'de aşağıdaki yöntemler kullanılır:

- Açık kodlar: Saklanan mesaj, açık ve net bir şekilde okunabilir. Maskeleme, boş şifreler ve grid (ızgara) yöntemiyle bu işlem yapılabilmektedir.
- Şemagramlar: Saklanacak mesaj için açık metinde küçük ve gizli bir parça seçilir. Bu işlem için farklı yazı tipleri, eski daktilo yazıları, resimler içinde boşluklar kullanma gibi yöntemler uygulanır.

Teknik Steganografi, birçok konuyu içine almaktadır. Bunları bazı başlıklar altında toplayabiliriz;

- Görünmez mürekkep: Geleneksel haline gelmiş olan görünmez mürekkeple yazma yöntemidir.
- Gizli yerler: Kimsenin göremeyeceği gizli yerlerdir (bavul, kasa vb.).
- Microdot'lar: Veriyi noktalar biçiminde saklama biçimdir.
- Bilgisayar tabanlı yöntemler: Bilgi saklamak için metin, ses, görüntü, resim dosyaları kullanılır.

4. STEGANOGRAFİNİN KULLANIM ALANLARI

Kullanım alanları bakımından Sayısal Steganografi aşağıda verildiği gibi 4 e ayrılır.

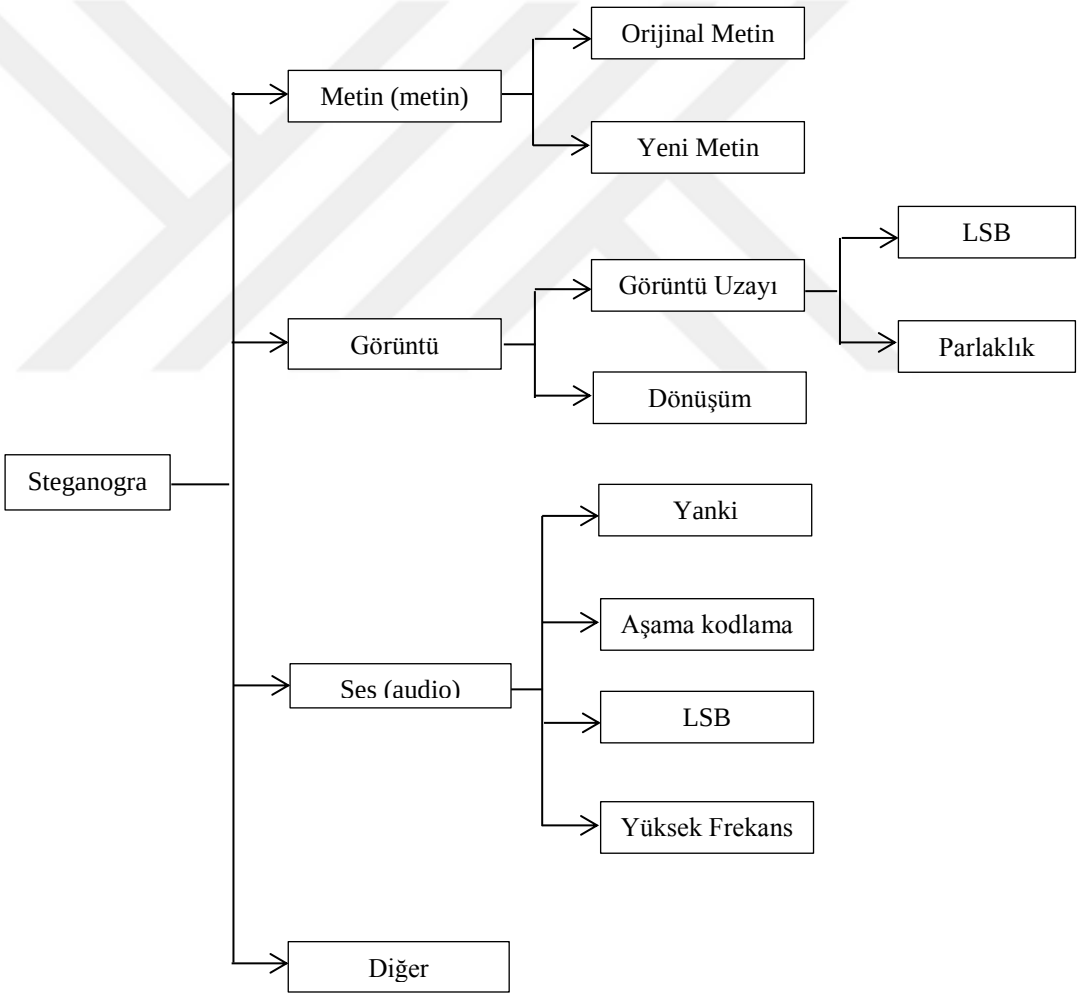
− Metin steganografi

− Ses steganografi

− Görüntü steganografi

− Video steganografi

Steganografi metodunun sınıflandırılması şekil 4.1'de verilmektedir.



Şekil 4.1 Sayısal Steganografi yönteminin sınıflandırılması

4.1 Metin Steganography

Metin steganography'nın uygulanabilmesi için birçok yöntemler vardır.

− Open Space Methods

 Line shift coding

 Word Shift Coding

 Future Coding

− Syntactic Methods

− Semantic Methods

4.1.1 Open space methods

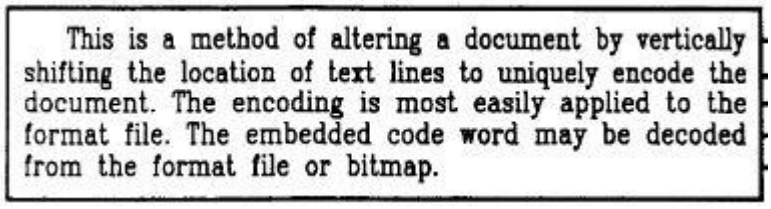
- Open Space Methods genelikle ASCII kodları ile kullanılmaktadır.

– kelimeler arasına boşluk koyarak ve satır sonu boşluk ekleyerek çalışmaktadır.

Kullanılan kodlama yöntemleri şunlardır :

- **Line shift coding**

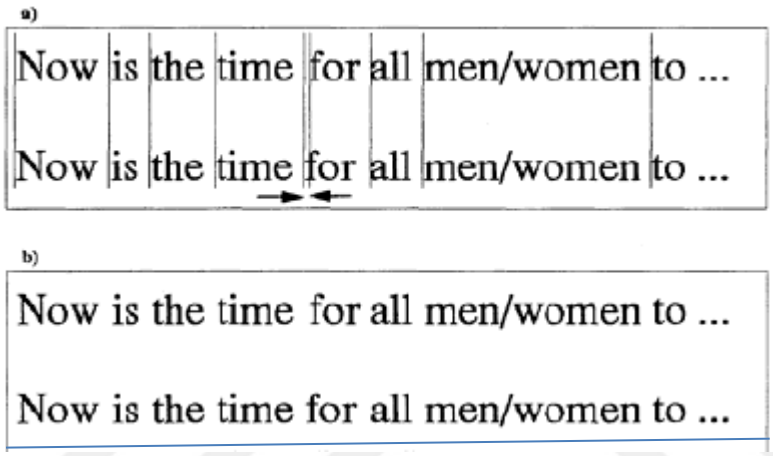
Line shift coding yönteminde ise metin biraz kaydırılarak gizlenecek mesajın kodlanması sağlanmaktadır. Saklanmış sözcük metin dosyası ya da BMP dosyası biçiminde açılacak şekilde elde edilir. Şekil 4.1'de ikinci satır 1/300 inch yukarıya kaydırılmıştır. Ve bu metin özüyle aynıdır. Bu işlem için kodlama "0" ya da "1" ile yapılır (Şahin 2007, Koluguri vd. 2014)


This is a method of altering a document by vertically shifting the location of text lines to uniquely encode the document. The encoding is most easily applied to the format file. The embedded code word may be decoded from the format file or bitmap.

Şekil 4.2 Satır kaydırma kodlaması örneği

- **Word shift coding**

Word Shift Coding metodunda dokümanın kodlanması için metnin satırları ile belli olmayacak biçimde oynanır. Gizlenmiş metin, metin ve BMP dosyası şeklinde açılarak elde edilebilir. Doküman için, Word shift coding metodu kullanıldığı zaman birbirine yakın kelimeler arasında belli olmayacak biçimde aralıklar fark edilmektedir. Bu aralıklar yüzünden dokümana gizlenmiş veriyi elde etmek için ilk kullanılan belge gerekecektir (Şahin 2007, Koluguri vd. 2014).



Şekil 4.3.a.Birinci satırda "for" sözcüğünden önce bir aralık kullanılmıştır, ikinci satırda ise "for" ile "all" arasında birden fazla aralık bulunur, b. Dikey şeritler yokken her iki satırdaki metnin görünüşü

- **Future coding**

Future Coding metodu, kelimelerin yerleriyle ve bazı harflerin boylarıyla oynanarak, ASCII kodlarında değişiklik yapılarak metin belgelerine ve bitmap dosyalara uygulanabilir.

4.1.2 Yazımsal yöntemler(syntactic methods)

Yazımsal yöntemlerde, dokümanı kodlamak için noktalama işaretleri kullanılır. Örneğin: aşağıdaki cümleler ilkin aynı gibi gözükür, ama dikkatlice okunduğunda birinci cümlenin fazladan bir ‘,’ işareti kapsadığı fark edilmektedir. Kodlama işleminin yapılması için bu yapıların biri “1”, diğeri de “0” olacak şekilde belirlenir (Şahin 2007, Koluguri vd. 2014).

“elma, armut, ve çilek”
“elma, armut ve çilek”

4.1.3 Anlamsal yöntemler(semantic methods)

Anlamsal yöntemleri W.Bender ortaya çıkarmıştır. Bu yöntemde eş anlamlı sözcüklere primary ve secondary değerler verilir, sonra bunlar “1” ve “0” şeklinde binary’e çevrilir. Mesela “small” sözcüğü birincil, “narrow” kelimesi de ikincil değer olacak biçimde işaretlensin. Primary değer “1”, secondary değer de “0” yapılarak binary’e dönüştürülmektedir (Şahin 2007, Koluguri vd.2014).

4.2 Görüntü Steganografi

İstediğimiz herhangi bilgiyi bir görüntü içinde gizlemede iki dosya söz konusudur. İlk dosya olan bilgiyi saklayacak resim dosyasına, orjinal resim ya da cover image adı verilir. İkinci dosya ise saklanacak bilgidir. Stego bu saklanacak bilgiye denir. Bilgi; açık metin (plain metin), şifreli metin (chipher metin), başka resimler ve bit dizisi içinde gizlenebilecek başka bir veri olabilmektedir. Gömme işleminde orjinal resim ve gizlenmiş bilginin oluşturduğu dosyaya “stego image” denir (Şahin 2007, Goel vd. 2013, Choudhury vd. 2015). Görüntü dosyaları üzerinde bilgi ve verileri gizlemek için farklı farklı steganografik yöntemler geliştirilmiştir.

Bunlar 3 başlık altında incelenebilmektedir.

1. Least Signification Byte yöntemi
2. Masking and Filtering yöntemi
3. Algorithms and Transformation yöntemi

4.3 Ses (Audio) Steganografi

Ses sinyalleri içene veri saklama işlemi, İnsan işitme sistemi (Human auditory system-HAS) frekans aralığı (20-20.000Hz) sisteminin kompleks olması nedeniyle, bayağı zahmetli bir iştir (Atıcı, 2007, Şahin 2007). Aynı zamanda İnsan İşitme sistemi, kaynağı belirsiz olan gürültülere de hassasiyet gösterir.

Ses sinyalleri ile ilgili çalışma yapılırken ses dosyalarına ait olan özelliklerin hangileri ve nasıl olduğunu araştırmış ve bilmiş olmamız gerekmektedir.

Ses dosyaların iki ana özellikleri vardır:

- Basit nitelendirme metodu: En çok kullanılan yöntemdir. Birtakım bozulmuş sinyaller WAV ve AIIF dosya formatlarında meydana gelebilir.
- Geçici seçme oranı: 8 kHz, 9.6 kHz, 10 kHz, 12 kHz, 16 kHz, 22.05 kHz ve 44.1 kHz frekanslar ses için en fazla kullanılan değerlerdir. Bu değerler frekans aralığının kullanılabilecek en üst seviyelerdir. (Atıcı, 2007, Şahin 2007) Bir diğer sayısal gösterim ise ISO MPEG-Audio formatıdır. Bu yöntemde sinyal istatistiği değiştirilir. Böylece ses korunur fakat sinyal değiştirilmiş olur.

Ses dosyalarında veri gizleme yöntemleri:

- Düşük bit kodlaması (Low-bit encoding)
- Aşama kodlaması (Phase coding)
- Taft yayılması (Spread spectrum)
- Yankı veri gizlemesi (Echo data hiding)

4.3.1 Düşük bit kodlaması

Düşük bit kodlaması yöntemi görüntü steganografide kullanılan LSB eklemeyle aynı kullanılır. Ses dosyasındaki verinin her bitinin son bitine gizlenecek bilginin bir biti yazılır (Atıcı 2007, Şahin 2007). Oluşan değişiklik ses dosyasında gürültüye neden olmaktadır. Bunun yapısı dayanıksızdır. Tekrar örnekleme veya kanalda oluşabilecek gürültü ile mesaj zarar görüp yok edilebilme dezavantajları vardır.

4.3.2 Aşama kodlaması

Aşama kodlaması yöntemi JPEG algoritması benzeri yapılıdır. Gömme işleminde ses dosyası küçük segmentlere bölünür ve her segmente ait aşama (faz) gizlenecek veriye ait aşama referansı ile değiştirilir (Atıcı ve Sağıroğlu 2016). Aşama kodlaması prosedürü aşağıdadır:

-Ses verisi N adet kısa segmente bölünür.
-Her segmente DFT uygulanarak aşama ve büyüklük (magnitude) matrisleri yaratılır.
-Komşu segmentler arasındaki aşama farklılıkları hesaplanır.
-Her segment için yeni bir aşama değeri bilgi gizlenerek oluşturulur.
-Yeni aşama matrisleri ile büyüklük matrisleri birleştirilerek yeni segmentler elde edilir.
-Yeni segmentler birleştirilerek kodlanmış çıkış elde edilir.

4.3.3 Taft yayılması

Gizleme işlemini ses sinyalinin kullandığı frekans taftı üzerinde yapmaktadır. Güçlü bir yapısı değil ve seste gürültü oluşturmaktadır.

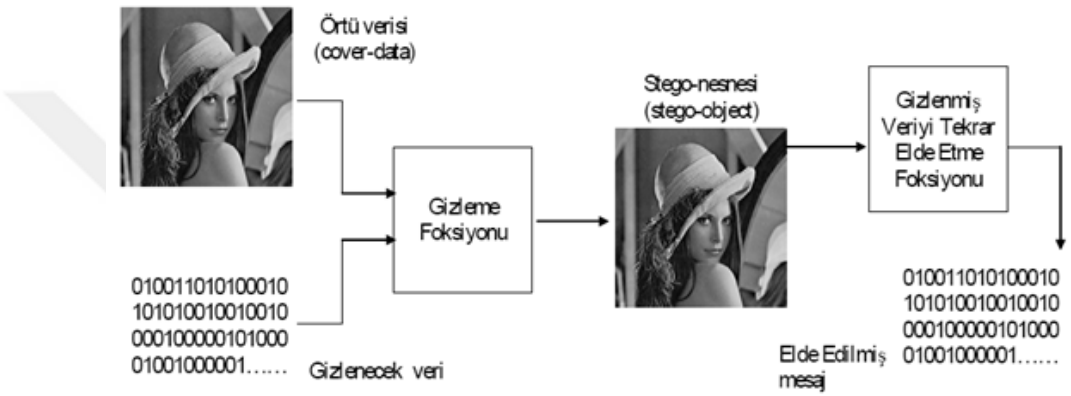
4.3.4 Yankı veri gizlemesi

Bilginin gizlenmesi taşıyıcı ses sinyali üzerine bir bilgi yankının gecikme miktarı, zayıflama oranı veya büyüklüğü gibi değerler kullanılarak sağlanmaktadır. İki farklı

gecikme değeri kullanılarak insan kulağının duyamayacağı frekansta 0 veya 1'in kodlanabilmesi olanaklıdır. Tüm bitlerin kodlanabilmesi için sinyal parçalara ayrılır. Eko(yankı) bilgi saklanması yöntemi rasgele bir gürültüye ve herhangi bir kodlama kaybına neden olmamaktadır.

5. GÖRÜNTÜ (IMAGE) STEGANOGRAFİ

Sayısal resimler dağıtımı, internetten kolay erişebileceğimiz dosyalardır. Steganografi uygulamalarında çok fazla tercih edilen sayısal ortamların resim dosyası olmasının nedenleri arasında küçük boyutlara sahip olmalarının yanında çok sayıda veri içermesi yer almaktadır. Bu sebeple steganografidaki çalışmalar ve gelişmeler görüntü üzerinde yoğunlaşmıştır.



Şekil 5.1 Steganografik Sistem

Veri saklamada en çok tercih edilen yöntemler aşağıda verilmiştir:

a. Least Signification Byte Yöntemi
b. Masking ve Filtering Yöntemi
c. Algorithms ve Transformation Yöntemi

a. Least Signification Byte yöntemi: Bu yöntem en çok tercih edilen veri saklama yöntemidir. Taşıyıcı ortamın diğerlerine göre daha az önemli bitlerini insan gözünün gözlemleyemeyeceği şekilde saklı bilgiyi gizlemeyi amaç edinir (Coşkun vd. 2013).
b. Masking ve Filtering Yöntemi: Bu yöntem daha çok 24 bit resimler için tercih edilmekte ve resmin diğerlerine göre daha az önemli bölgeleri belirlenerek bu kısımlarda gizleme işlemi yapılmaktadır (Şahin 2007). Bu yöntemler genelde filigran uygulamalarında kullanılır ve JPEG türündeki resim dosyalarına daha uygundur.

c. Algorithms ve Transformation Yöntemi : JPEG dosyalar üzerinde DCT ve DFT dönüşümlerin yapıldığı yöntemdir.

5.1 Veri Gömme Yöntemleri

Veri gömme işlemi esnasında kullanılan veriye dikkat edilerek 2 alt başlık altında incelenebilir. Bunlardan ilki Uzaysal / Görüntü Alan Tekniği (Spatial / Image Domain Technique), ikincisi ise Frekans / Dönüşüm Alan Tekniği (Frequency / Transform Domain Technique)'dir.

1. Uzaysal Alan/Görüntü Alan Tekniği: Görüntü dosyasındaki veriyi, gizleme metodu direkt kullanır. Gizleme işlemi sırasında bilginin saklandığı veri kümesi, piksel değerlerini ifade eder (Şahin, 2007, Choudhury, Das, Tuithung, 2015). Örnek olarak En Önemsiz Bite Ekleme (Least Significant Bit Insertion - LSB) verilebilir.
2. Frekans Alan/Dönüşüm Alan Teknik: Gizleme metodu, orijinal verideki değişimler üzerinde uygulanır. Bu teknik için, JPEG türündeki görüntü dosyalarına veri gömme işleminde tercih edilen algoritmalar örnek verilebilir. Değinilen algoritmalar JPEG formatındaki resim dosyalarını sıkıştırma esnasında tercih edilen DCT katsayıları üzerinde veri saklamaktadır.

5.2 Görüntü Dosyalarında Steganografik Yöntemler

Görüntü Dosyalarında veriyi saklamak için tercih edilen yöntemler 3'e ayrılır ve bunlar aşağıda belirtilmiştir:

a. Değiştirmeye Dayalı Yöntemler
b. İşaret Işlemeye Dayalı Yöntemler
c. Spektrum Yayılmasına Dayalı Yöntemler

a. Değiştirmeye Dayalı Yöntemler: LSB Yöntemi veya Amplitude (Genlik) Modülasyonu kullanılarak veri saklama bu yönteme örnek verilebilir (Khan, Rai,

2014). Bu yöntemde veriyi saklamak için, ya renk değerlerinin düşük anlamlı bitleriyle saklı verinin bitleri değiştirilerek renk değerleri ile oynanabilir ya da renk bilgilerinin palet üzerinde tutulduğu resim dosyaları kullanılarak palet değiştirilebilir. İnsan gözü bu renk değişimini fark edemez ve saklı bilgi, "gürültü (noise)" şeklinde resme ilave edilmektedir (Goel vd. 2013). Bu teknik önemli ölçüde bilgi gizleme olanağı sağlar, ancak resimde gerçekleştirilecek değişimlere duyarlıdır. Paket değiştirme yöntemde resim hatta resmin türü değiştirildiğinden tüm yapılar bozulabilmektedir.

b. İşaret Işlemeye Dayalı Yöntemler: Bu yöntem de DCT, DFT gibi çeşitli dönüşümler kullanılır. İşaret işlemeye dayalı yöntemler resim üzerinde yapılan değişikliklere karşı dayanıklıdır ancak resimde bozulmaya neden olabilirler. Resimde herhangi bir bozulma meydana gelip gelmediği sadece işlem bitiminde gözlenebilmektedir ve 64 adetlik bloklara sadece 1 bit saklanabilmesi, gizlenecek veri miktarında önemli ölçüde azalmaya neden olmaktadır.
c. Spektrum Yayılmasına Dayalı Yöntemler: Bu yöntem askeri iletişimde fazla kullanılmak ve son yıllarda oldukça yayın kullanılmaktadır. Spektrum yayılmasına dayalı yönteminde iletilecek veri gerekli olan frekans bandından daha fazlasına gönderilir ve bu sayede saklı verinin yayıldığı bant sayısı artırılarak resme gürültü şekilinde ilave edilir. Üçüncü kişi olaya dahil olup bir veya daha fazla frekans bandının bozulmasına sebep olsa da alıcı diğer frekans bantlarındaki bilgiler sayesinde gerçekte verilmek istenen mesaja eksiksiz ulaşabilmektedir.

Bahsedilen metotlar uygulanarak veri saklayan steganografik algoritmalardan en çok Patchwork Algoritması, Amplitude (Bolluk) Modülasyonu kullanılarak bilgi gizleme, Superposition Algoritması, SSIS Yöntemi, Frekans Domaini İçine Veri Saklanması ve Son Bite Ekleme (LSB-Least Significant Bit Insertion) yöntemi kullanılmaktadır.

5.2.1 Patchwork algoritması

Hala sık bir şekilde kullanılmakta olan bu algoritmanın öncüsü Render'dir. Bu bilgi Gauss dağılımını ifade eden istatistikesl yönteme dayanır ve bunun amacı istatistiğe

sahip örtü verisinin içine gizlemekdir. Bu algoritma filigran (Damgalamaing) uygulamalarında daha çok kullanılmaktadır (Şahin, 2007).

Patchwork algoritması genelikle 256 bit gray-scale için tercih edilir. Resim içerisinde rasgele herhangi iki nokta seçilir (A_i ve B_a) , A_i noktasının parlaklığı, ise B_b noktasının parlaklığıdır.

Image şifreleme aşamalar şunlardır:

Step 1: (a_i , b_i) ikilisini seçmek için rasgele (pseudo random) numara üreteci aracılığıyla belirli bir anahtarın kullanılmasını gerekir.

Step 2: *a* parçasının parlaklığı δ^1 kadar arttırılır.

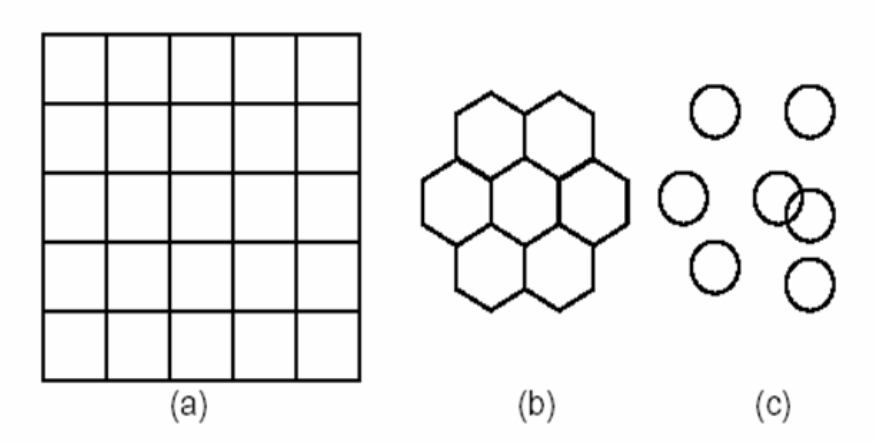
Step 3: b_i parçasının parlaklığı ise aynı δ kadar azaltılır.

Step 4: Son adımda ilk üç adım *n* için tekrarlanır (n'in değeri 10.000 civarındadır)

(δ değeri, 256'lık gri-seviye renk aralığı içerisinde 1 ile 5 arasında bir değerdir)

Burda üç adet tek boyutlu patch şekli vardır.

1. Eğer keskin kenar içeren küçük patch'lar alırsak , yamanın enerjisi görüntü analizinin yüksek frekanslı kısmı içerisinde yoğunlaşacaktır. Fark edilmesi oldukça zordur fakat filtreleme sonucunda kolaylıkla elde edilebilir.
2. Yumuşatılmış kenarlar içeren yamalar kullanılmasıdır. Bu durumda bilgiler düşük-frekans analizi içinde kalacaktır.
3. ilk iki patch'ını birleştirilmesidir. Bu şekilde yamanın enerjisi dağıtılmaktadır.



Şekil 5.2 Yama çeşitleri

a. doğrusal bir kafes biçimi kullanılmıştır. Pek tercih edilen bir yöntem değildir
b. a'nın yerine tercih edilebilir olarak gösterilmiştir. Alternatif çözüm
c. a'nın yerine tercih edilebilir olarak gösterilmiştir. Rasgele olarak dağılmakta ve seçilebilmektedir.

5.2.2 Superposition algoritması

Filigran uygulamalarda Superposition algoritmasını daha çok kullanılmaktadır

NxM çözünürlüğe sahip bir görüntü şu şekilde ifade edilmektedir.

$$I = \{x_{nm}, n \in \{0,.....,N-1\}, m \in \{0,.....,M-1\}\} \quad (5.1)$$

Buradaki $X_{nm} \in \{0,1,....., L-1\}$, (n,m) pikselinin koyuluk seviyesini belirlemektedir. Gizlenecek bitler, 1 ya da 0 değeri alabilen aynı büyüklükteki binary çiftler olarak gösterilebilir.

$$S=\{s_{mn}, n \in \{0,...., N-1\}, m \in \{0,...., M-1\}, s_{nm} \in \{0,1\}\} \quad (5.2)$$

Bu aşamadan sonra I , S kullanılarak iki eş büyüklükte alt kümeye bölünebilir.

$$A=\{x_{nm} \in I,\ s_{nm}=1\}$$

$$B=\{x_{nm} \in I,\ s_{nm}=0\}$$

$$|A|=|B|=\frac{|I|}{2}=\frac{N \times M}{2}=P$$

$$I=A \cup B \tag{5.3}$$

Filigran (işaret), görüntü üzerinde şu şekilde gibi ilave edilir. $C=\{x_{nm} \otimes k,\ x_{nm} \in A\}$ .Buradaki $\otimes$ işlemi superposition kuralı (Einstein, 1905) olarak bilinmektedir. İşaretlenmiş görüntü şu şekilde verilmektedir.

$$I_s = C \cup B \tag{5.4}$$

5.2.3 SSIS (spread spectrum image steganography) Yöntemi

SSIS yöntemi, sayısal görüntünün içindeki bilgi bitlerinin işaretleme kalitesini, saklama ve geri getirme işlemlerinin gözlemleyen biri tarafından fark edilemeyecek şekilde yapılması yeteneği sağlar. Saklanmış bitleri elde etmek için orijinal görüntüye ihtiyacı duymamaktadır.

SSIS yöntemi tayf (spectrum) yayılım iletişimi, hata kontrol kodlaması, görüntü işleme gibi tekniklerle birleştirilebilmektedir. Bu düşünce tarzıyla saklanacak bilgi bir gürültü (noise) içine konularak görüntü içerisine yerleştirilir. SSIS mükemmel değildir. Çünkü gürültünün düşük güçte ve kod-çözme işlemi oldukça karışıktır.

Step 1 : Mesajin yapısına göre key1 ile şifrelenir.

Step 2: Düşük oranlı hata kontrol kodu (error control code-ecc) ile kodlanarak, m kodlanmış mesajı üretilir.

Step 3: Gönderici; aynı zamanda n sıralamasına sahip bir yayılım üretmek için key2'yi gönderir.

Step 4: Bu iki değer (m ve n) bir modülasyon işlemine tabi tutulur ve s gömülü sinyali oluşturulur.

Step 5: Elde edilen gömülü sinyal bir key3 ile birleştirme (interleaving) işlemine girer.

Step 6: Örtü verimiz (cover data) olan f ile işleme girerler.

Step 7: Sinyal orijinal örtü verimizin (f) içine yerleştirilerek stegoimage elde edilir.

Step 8: Alıcıya gönderilir.

5.2.4 Son Bite Ekleme (least significant bit insertion-LSB) Yöntemi

Son bite ekleme yöntemi (Least Significant Bit Insertion Methods) (Şahin 2007) yaygın bir şekilde kullanılır ve uygulaması basittir. Fakat yöntemin dikkat edilmeden kullanılması bazı veri kayıplarına sebep olabilir. Son bite ekleme yöntemi (Least Significant Bit Insertion Methods)'nde her bitin diğer bitlere göre daha önemsiz biti olan son bit değiştirilerek o bitin yerine gizlenmek istenilen verinin bitleri yerleştirilir. Bu sırada her sekiz bitin bir bitinin değiştirilmesinden ve eğer değişiklik yapılmışsa değişiklik yapılan bitin en az anlamlı biti olmasından dolayı ortaya çıkan steganogramdaki (örtü verisi pozitif gömülü veri) değişimler insanların algılayamayacağı boyutta olmabilmektedir. Resimlerin sahip oldukları özelliklere göre son bite ekleme yönteminin çalışma şekilleri aşağıda verilmiştir.

Gri seviye resimler üzerinde LSB yönteminin uygulanması

Gray level resimlerde, 0 = siyah ile 255 =beyaz arasında tam sayı değer alabilen bütün pikseller 1 byte ile gösterilir. 0-255 arasındaki değerler gri'dir ve bu sebepten dolayı bir resme ait tam sayı gray level olarak isimlendirilir.

Çizelge 5.1 LSB yönteminde renk karşılığı

	Renk değeri	İkilik Sistemdeki Karşılığı	Rengi
Orijinal piksel	120	01111000	
Bilgi saklanmış piksel	121	0111100**1**	

Örneğin, color value = 120 olan bir piksel(pixel)in içerisine binary value'ye 1 değeri gizlendiğinde değişen piksel ve renk değeri tablo'da görülmektedir. Tablo'daki gösterilen iki renk arasındaki renklerden de gözle fark edilemeyecek kadar az bir değişim gözükmektedir. Binary number daki 1 ya da 0 olması gözle görülebilir bir fark bulunmamaktadır.

8-bit color image ve LSB yönteminin uygulanması

8 bitlik image'lerde piksel(pixel) başına 1 byte kullanılmakta ve bu image'lerden color sınırlamasında iyi bir value elde edilememektedir. Gizlenecek veri, gizleme ortamını çok fazla değiştirmeyecek biçimde tercih edilmelidir. Orijinal görüntüde LSB işlemi yapıldığında renk girişi göstergeleri değişirler. 8 bitlik görüntülerde 4 basit renk (White,Red,Blue,Green) kullanılmaktadır. Bunlar ise: sırasıyla White-0 (00), Red-1 (01), -Blue- 2 (11), Green-3 (10) dir.

Örnek olarak verilen orijinal görüntü pikselleri "Beyaz, beyaz, mavi, mavi" (00 00 11 11) ise 10 sayısının ikilik (binary) tabandaki karşılığı olan 1111 değeri bu piksellere saklandığında, yapılan değişiklikler neticesinde görüntünün yeni piksel değerleri aşağıdaki verilmiştir.

01 00 10 11

Elde edilen bu değerler renk paletinde kırmızı, beyaz, yeşil ve mavi değerlerine karşılık gelmektedir. Piksellerin renk değerleri değiştiği için fark edilmesi daha kolay olduğundan veri gizleme uzmanları 8 bitlik renkli görüntüler yerine gri-seviye görüntülerin tercih edilmesinin daha doğru olduğunu belirtmektedirler .

24-bit color image ve LSB yönteminin uygulanması

24 bit resimler için bir piksel başına 3 byte kullanılır. Her pikselin rengi "Kırmızı (red), Yeşil (green), Mavi (blue)" olarak üç temel renkten meydana gelir. Bu pikselin RGB değeri olarak adlandırılır.

Her byte'ta son biti değiştirmek şartıyla bir piksel'de 3 bitlik veri gizlenebilir. Başka bir ifadeyle 24 bit derinliğine sahip 1024x768 piksel boyutundaki bir resim, veri gizlemek amacıyla kullanılabilir 2.359.296 bit (294.912 byte)'e sahiptir. Saklanması gereken mesaj, gizleme işleminden önce sıkıştırılırsa eskisine oranla çok daha fazla sayıda bilgi resmin içine saklanabilir.

10010101 00001101 11001001 (149,13,201)
10010110 00001111 11001010 (150,15,202)
10011111 00010000 11001011 (159,16,234)

Orijinal görüntü bitleri yukarıdaki gibi verilen 3 pikselin içerisine "*101101101*" bilgisi saklandığında meydana gelen yeni piksel değerleri aşağıda verilmiştir.

10010101 0000110**0** 11001001 (149,12,201)
1001011**1** 0000111**0** 1100101**1** (151,14,203)
10011111 00010000 11001011 (159,16,234)

Yukarıda verilen örnekte yalnızca 4 bitte değişim yapılarak veri saklanmıştır. Uygulanan bu metotta mümkün olan en az değişiklik yapılarak sonuca ulaşmak ve saklanacak verinin 9 bitten az olması durumunda ise yok sayılacak bitlerin belirlenmesi son derece önemlidir.

6. LSB YÖNTEMİ KULLANILARAK GELİŞTİREN SBG PROGRAMI VE DEĞERLENDİRİLMESİ

6.1 Resim İçine Veri Gizleme Uygulaması

Bu çalışmada Steganografi yöntemlerden olan resim içine veri saklama yöntemi kullanarak SBG (Steganografi ile Bilgi Güvenliği) yazılım geliştirilmiştir. JPEG ve BMP formattakı dosya içerisine LSB ve AES yöntemleri kullanılarak düz metin(.txt), Microsoft Word (.docx) dosya gibi verileri gizleyen SBG isimli Visual Studio 2013 kullanılarak C# yazılım dilinde geliştirilmiştir. Bu bölümde yer alan alt başlıklarda, JPEG, BMP, txt ve Microsoft Word dosya yapısı, LSB yöntemi geliştirilen uygulamanın modülleri ,saklama işlemi ve detayları, veri saklama analizleri ve histogram analizleri sunulmuştur.

6.2 JPEG Dosyası

256'dan fazla renk ile uğraştığımız zaman, GIF formatını kullanmanız mümkün değildir. BMP olarak sakladığımızda çok fazla disk alanı kaplamaktadır ve Gigabytelık HD'ler kullanmanız gerekebilir. Onun yerine JPEG daha iyi bir alternatif olabilir. Fakat JPEG az renk içeren uygulamalarda hem kaliteyi düşürmektedir ve hem de dosya boyutunda önemli bir değişiklik sağlamamaktadır (Anonim 2001).

Standart JPEG formatında, resmin kalitesinden bir miktar ödün vererek sıkıştırma uygulanır. Böylece dosya boyu bir hayli düşer. Özellikle 24 bit true color uygulamalarda resim kalitesinin düştüğünü anlamak mümkün değildir. Bu tip uygulamalarda JPG tercih edilmektedir.

JPEG'den ne kadar sıkıştırma istendiği (0-100 arası bir faktör) seçilir ama genellikle 5-95 arası kullanılmaktadır. 95'den fazlası detay kaybına yol açmaktadır ve 5'ten küçüğü de dosyayı fazla küçültmemektedir.

24 bit'den 8 bit'e çevrimli JPG formatı vardır. JPG de, GIF gibi, Web listeleyiciler tarafından görüntülenebilen standart bir formattır. JPG, ISO standardı ile tanımlanmış bir formattır ve birçok değişik kodlama sistemleri içermektedir.

6.3 BMP Dosyası

BMP , resim formatın en temelidir. BMP'nin birbirinden farklı bir kaç türü var. Özellikle bir X-Windows kullanıcısı ile MS-Windows ya da OS/2 kullanıcısı için farklar mevcuttur.

X-Windows üzerindeki BMP formatı, sadece 2 rengi desteklemektedir. MS-Windows ya da OS/2 üzerindeki BMP formatının X-Windows'daki karşılığı XPM'tir (pixmap)'dir. MS- Windows üzerinde BMP 16 ya da daha çok renk kaydedebileceğiniz, herhangi bir sıkıştırma yapmayan oldukça hızlı bir formattır. Bu formatta resmin içindeki renk sayısı değil, resmin büyüklüğü önemlidir (Anonim 2001).

16 renk, 800x600 çözünürlüğünde bir BMP dosyası, 800x600x1/2=240000 byte yer kaplayacaktır (16 renk icin 4 bit gerekli =1/2byte). Resmin içinde 1, 2 ya da 12 renk olması hiç önemli değil. 256 renk olarak kaydedilen bir dosya ise, 800x600x1=480000 byte yer tutacaktır (256 için 8 bit=1 byte gerekli. 2^8=256).

6.4 TXT Dosyası

TXT, birçok işletim sistemi içerisinde kullanılabilen metin dosyası uzantısıdır. Metin yani Yazı sözcüğünün kısaltılmasından oluşturulmaktadır. TXT dosyaları birçok farklı metin editörü tarafından kullanılabilmektedir. TXT Dosyası içerisinde insanların okuyabileceği karakterleri ve kelimeleri içeren, bilgisayarlar tarafından okunabilen dosya formatıdır. Metin dosya formatının keskin bir standardı yoktur. İçerisinde birçok yaygın format kullanılabilir. Bir Metin dosyası içerisinde ASCII veya ANSII gibi kodlama türleri kullanılabilir (https://webhocam.com 2011).

6.5 Microsoft Word Dosyası

Microsoft Word kelime işleme yazılımı tarafından oluşturulan dosyadır; metin, görüntüler, biçimlendirme, stiller, çizili nesneler ve diğer belge elemanlarını içerir; yazarlık, iş, akademik ve kişisel belgeler için kullanılmaktadır. En popüler kelime işleme belgesi formatlarından biridir. Belge verilerini tek bir binary dosyasında depolayan .DOC dosyalarının aksine, DOCX dosyaları Open XML formatı kullanarak oluşturulur, bu format da belgeleri sıkıştırılmış bir zip paketinde ayrı dosyalar ve klasörler olarak depolar. Bir DOCX dosyasının içinde XML dosyaları ve üç klasör bulunur (docProps, Word ve _rels). Bu klasörler, belge özelliklerini, içeriğini ve dosyalar arasındaki ilişkileri tutar. Bu yapı, belgenin içeriğinin daha fazla erişilebilir olması için tasarlanmıştır. Örneğin, belge metni düz metin dosyaları kullanılarak kaydedilir ve belge görüntüleri DOCX dosyasının içinde bireysel görüntü dosyaları olarak depolanır. DOCX dosyaları Windows için Word 2007 veya daha üst versiyonları ve Mac OS X için Word 2008 veya daha üst versiyonları tarafından açılabilir (Anonim , 2001).

6.6 SBG Uygulaması İçin LSB Yöntemi

Bu uygulamada veriyi gizlemek için, veriye ait bit değerleri taşıyıcı JPEG ve BMP dosyasının veri bölümündeki piksellerin en son bitlerine dağıtılmaktadır. Taşıyıcı resim dosyasının belirlenen resim örneklerinin en az önemsiz bitlerinde (LSB), saklanacak olan bit değerini gizlenecek olan bit değerine eşitlemek anlamına gelmektedir. Örneğin veri kısmı aşağıdaki 8 byte değeriyle başlayan bir JPEG dosyası olduğunu varsayalım:

11010100 – 10010011 – 00101101 – 01011100 – 11101001 -01110001 - 11001011- 00111001 ve bir byte uzunluğundaki 10110110 verisi saklanacaktır. Saklama işleminde sonra, resim dosyasının veri kısımındaki ilk 8 byte lık uzunluğun yeni değeri.

11010101 – 10010010 – 00101101 – 01011101 – 11101000 - 01110001 – 11001011 - 00111000 şeklinde olacaktır. Altı çizili sayılar saklama sonucu değişen bit değerlerini

göstermektedir. Bu yeni haldeki byte değerlerinin son bitlerini yan yana sıraladığımızda gizlediğimiz veriyi elde ettiğimizi göreceğiz.

6.7 Programın Modülleri

SBG uygulama Visual Studio 2013 ortamında C# programlama diliyle kodlamıştır. Uygulamada JPEG ve BMP dosyası taşıyıcı dosya olarak alınmakta ve içine .txt , Microsoft Word, JPEG, BMP gibi bir çok dosya gizlenmektedir. Ancak gizlenecek olan dosyaların toplam boyutu taşıyıcı dosyanın boyutundan az olması gerekmektedir. Gizlenecek olan veri, JPEG ve BMP dosyasının veri kısmında gizlenecektir.

Çizelge 6.1 SBG uygulamasında, JPEG,BMP dosyasına saklanabilen dosya türleri

SBG Uygulamasının Desteklediği Dosya Türleri	
Joint Photographic Experts Group	JPEG
Windows Bitmap	BMP
Portable Document Format	.pdf
Microsoft Word	.docx
Microsoft Excel	.xlsx
TXT	.txt
WinRAR	.rar
Microsoft PowerPoint	.pptx
Graphics Interchange Format	.gif

Uygulamada JPEG, BMP dosyasının veri kısmının byte değerlerinin en önemsiz bitlerine(son bitlerine) veri gizlenmektedir.

SBG uygulamasının çalıştırıldığı bilgisayarın teknik özellikleri:

- Windows 10, 64 bit
- Intel® Turbo Boost Technology 2.0 destekli 3. nesil Intel® Core™ i7-3630QM İşlemci
- Sabit disk 1,500 (750 + 750) GB
- 8,192 (4,096 + 4,096) MB, DDR3 RAM (1.600 MHz)
- CUDA™ Teknolojisini ve NVIDIA® Optimus™ Teknolojisini destekleyen NVIDIA® GeForce® GTX 670M

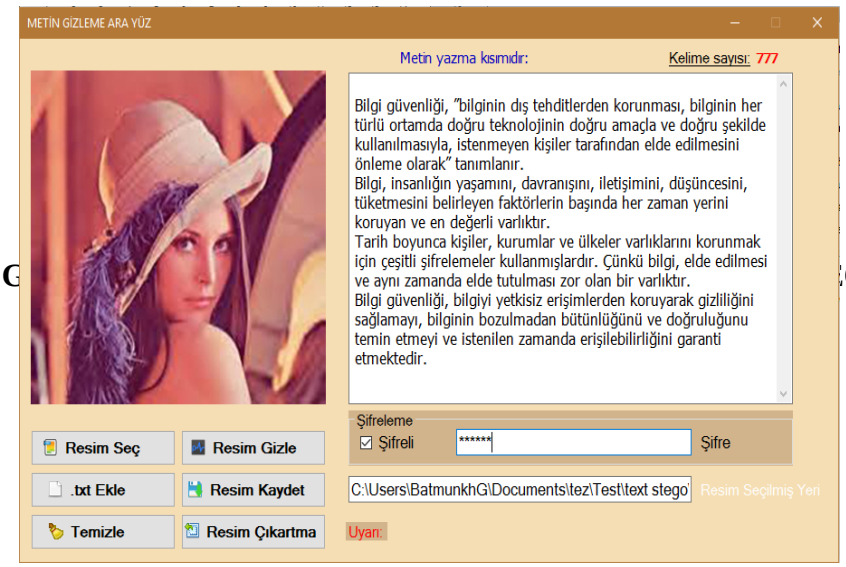
Programda 2 tane seçenği göstermektedir (Şekil 6.1).Bunlar :

- Metin Gizleme
- Dosya Gizleme

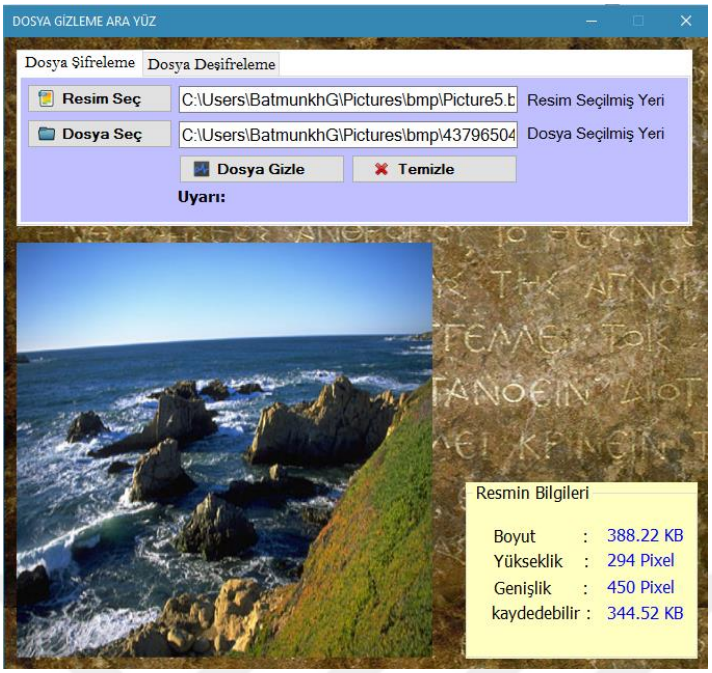
Şekil 6.1 Programın ana ekranı

Metin Gizleme : JPEG, BMP dosya içine düz metin (.txt) manuel olarak ya da hazır (.txt) dosayı gizleyebilmektedir.Şekil 6.2'de 100 kb boyutundaki bir metin resmin içine düz metin gizlenmektedir.

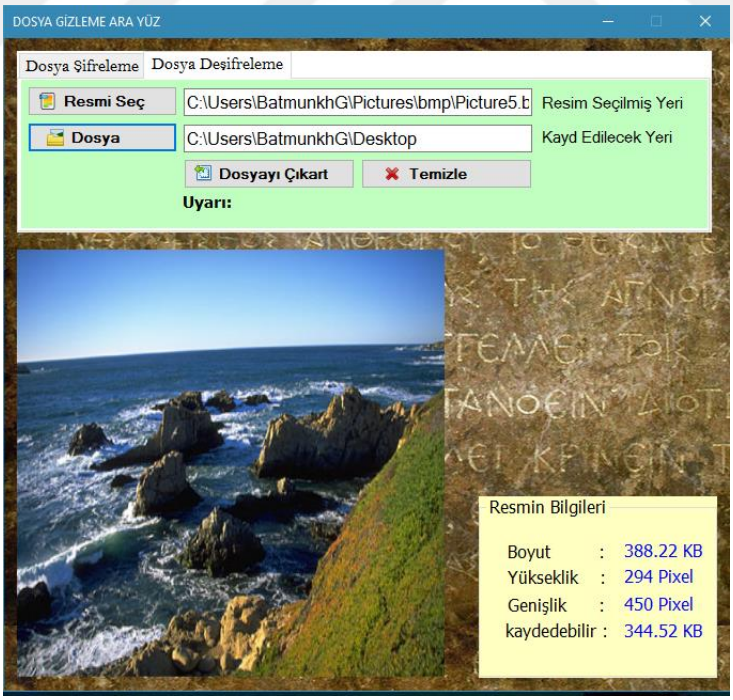
Dosya G ...G ve BMP gibi



Şekil 6.2 Metin gizleme ve şifreleme ekranı



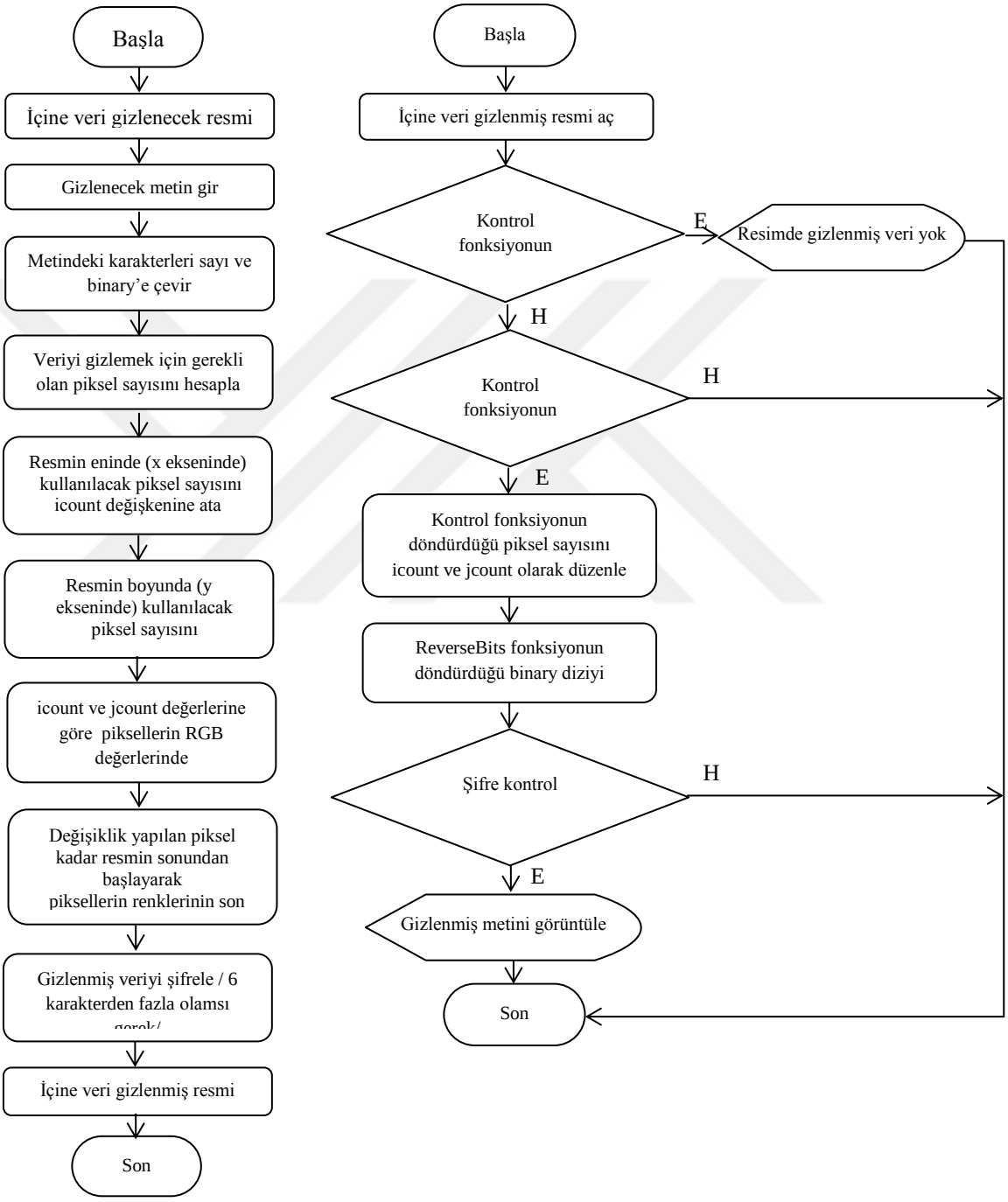
Şekil 6.3 Dosya şifreleme ekranı



Şekil 6.4 Dosya deşifreleme

Metin Gizleme:

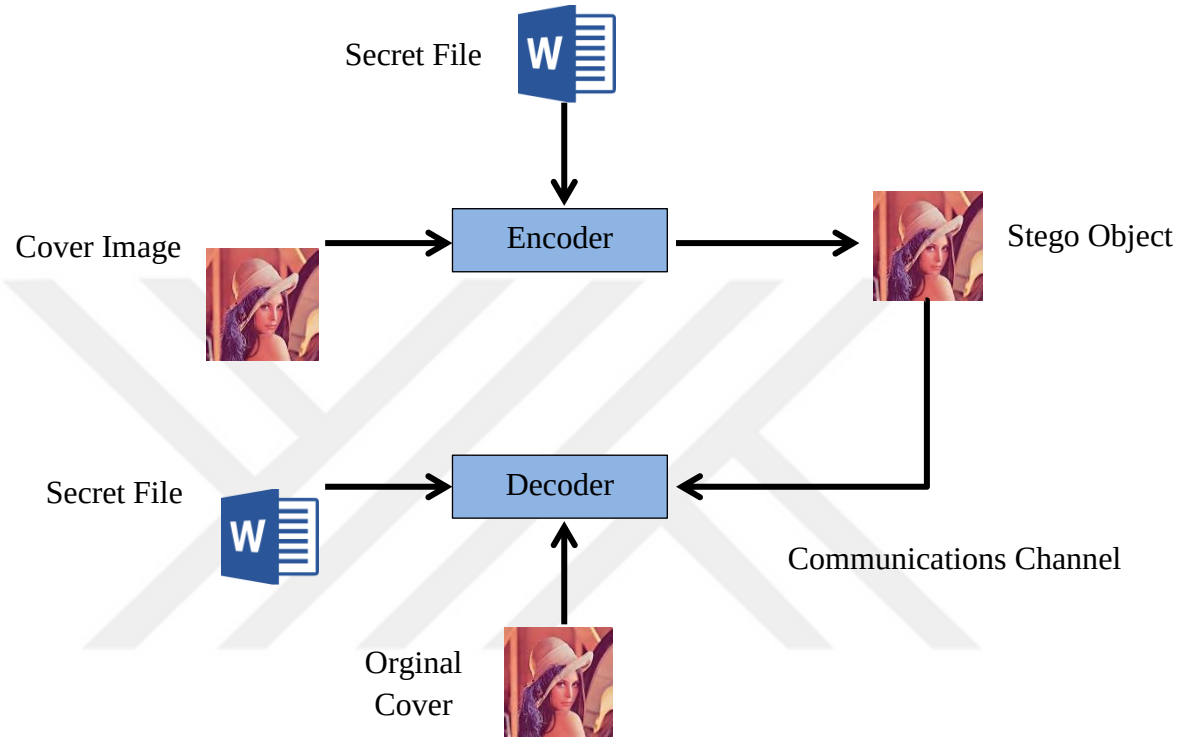
Şekil 6.5'de geliştiren programın veri gizleme ve gizlenmiş veriyi elde etme işlemlerinin akış şemaları gösterilmektedir.



Şekil 6.5,a. Programın Veri Gizleme işlemin akış şeması, b. Programın Gizlenmiş Veriyi Elde Etme işleminin temel akış şeması

Dosya Gizleme

Şekil 6.6'du geliştiren programın dosya şifreleme seçeneğin gizleme ve veriyi elde etme işlemi



Şekil 6.6 Dosya gizleme şeması

Metin mesajını gömmek için kullanılan algoritma

Adim1: Cover Image ve Cover Image içindeki metin mesajını oku.

Adim2: Metin masajını binary formata çevir.

Adim3: Cover Image'in her bir pikselinin LSB'sini hesapla.

Adim4: Secret Message'in her bir biti ile Cover Image'in her bir pikselinin LSB'sini birebir yer değiştir.

Adim5: Stego Image'i yaz.

Metin mesajini kurtarmak için kullanılan algoritma

Adim1: Stego Image'i oku.

Adim2: Stego Image'in her bir pikselinin LSB'sini hesapla.

Adim3: Bitleri kurtar ve her 8 biti karaktere çevir.

Şekil 6.7'de geliştiren programın kullandığı fonksiyonlar gösterilmektedir.

Kontrol () fonksiyonu:

Adım 1: Resmin son satırındaki piksellerin renklerinin son bitlerini kontrol et.

Adım 2: Eğer ilk iki pikselin renklerinin binary olarak son bitleri 1 ise şifrelenmiş toplam piksel sayısını bul ve değer olarak döndür.

ReverseBits () fonksiyonu:

Adım 1: Kontrol fonksiyonunun döndürdüğü toplam piksel sayısını kullanarak icount ve jcount değerlerini hesapla.

Adım 2: Sıra ile her pikseldeki renklerin son bitlerine bak ve str adlı stringe ekle.

Adım 3: str uzunluğu kadar dinamik bir dizi oluştur ve str'deki bitleri 8'erli gruplar olarak al.

Adım 4: Bit gruplarını byte'a çevir ve fonksiyon değeri olarak diziyi döndür.

Şekil 6.7 SBG uygulamasında kullanılan fonksiyonlar

6.8 Taşıyıcıdaki Değişim

Bir Steganografi algoritması analiz edilirken orijinal resimdeki değişim oranı oldukça önemlidir. Resimdeki bu değişim ya da başka bir deyişle resimdeki bozulma oranını hesaplanması için farklı ölçme teknikleri mevcuttur. Steganografi algoritması analiz eden MSE, RMSE ve PSNR teknikler arasındaki en çok bilinenleridir. Bazı durumlarda MSE kullanımından ziyade, hatanın büyüklüğünün, orijinal piksel değerinin en büyüğü(peak-tepe) ile olan alakasıyla ilgilenilir. Böyle durumlarda PSNR yöntemine başvurulur. PSNR, orijinal görüntü ile gizli veri içeren görüntü arasındaki benzerlik

kalitesini hesaplar. PSNR değerinin hesaplanmasında gizleme sonucu oluşan hataların kareleri toplamının ortalaması yani MSE (Mean Squared Error) değeri kullanılmakta (Atıcı ve Sağıroğlu 2016).

I_1 ve I_2 sırasıyla örtü orijinal resim ve stego resimlerini, M ve N resim boyutlarını göstermektedir.

$$MSE = \frac{\sum_{MN}[I_1(m,n)-I_2(m,n)]^2}{M*N} \quad (6.1)$$

R – resmin mümkün olan en yüksek piksel değeridir.

$$\text{PSNR(dB)} = 10*\log_{10}\left(\frac{R}{MSE}\right) \quad (6.2)$$

6.9 Kapasite Açısından Değerlendirilmesi

Uygulamada kullandığımız least significant bit (LSB) yönteminde uygulamanın kapasitesi resmin boyut ile ilgilidir. BMP ve GIF formatındaki dosyalar, diğer formattaki dosyalardan kapasite açısına göre çok daha iyi sonuç vermektedir. JPEG formatındaki dosyalar ise 8x8 piksellik bloklara yalnızca 1 byte gizlenebilmektedir. Bundan dolayı gizlenebilecek veri miktarı son derece azdır.

Metin gizleme seçeneğindeki JPEG dosyasına gizlenmiş resim için yapılan analiz

Farklı boyutlardaki orijinal resim dosyalarının (JPEG, BMP) içerisine metinler şifreli ve şifresiz olarak gizlenmiştir. Gizlenen bu metinlerin karakter sayısı ve dosya boyutu, orijinal resim ile metin gizlenmiş resim arasındaki gürültü oranı değeri (PSNR) , orijinal resmin yüzde olarak ne kadar büyüdüğü ve son olarak saklanan metin dosyasının orijinal resmin yüzde kaçını kapsadığı JPEG dosyası için çizelge 6.2 - 6.3'de ; BMP dosyası için ise çizelge 6.4 - 6.5'te gösterilmiştir.

Çizelge 6.2 JPEG dosyasına gizlenmiş şifresiz metin için yapılan analiz

Orijinal resim boyutu/KB	Saklanan Kapasite		PSNR	orijinal resim yüzde kaç büyüdü?	saklanan metin orijinal resmin yüzde kaçıdır?
	karakter	.txt boyut/ KB			
-	-	-	-	-	-
30	5490	5.36	54.2 dB	40.06 %	17.45 %
40	8664	8.46	54.09 dB	71.39 %	21.41 %
50	12150	11.8	54.12 dB	90.94 %	23.74 %
60	16537	16.1	54.17 dB	119.38 %	27.38 %
70	23437	22.8	54.19 dB	161.42 %	32.57 %
-	-	-	-	-	-
100	45937	44.8	54.19 dB	261.53 %	45.11 %
ortalama			55.85 dB	106.81 %	25.70 %

Şifresiz metin

Çizelge 6.3 JPEG dosyasına gizlenmiş şifreli metin için yapılan analiz

Orijinal resim boyutu/KB	kapasitesi		PSNR	orijinal resim yüzde kaç büyüdü?	saklanan metin orijinal resmin yüzde kaçıdır?
	karakter	.txt boyut/ KB			
-	-	-	-	-	-
30	4354	4.25	59.26 dB	40.06 %	13.84 %
40	7432	7.25	59.26 dB	71.39 %	18.35 %
50	10161	12.7	59.26 dB	90.94 %	25.55 %
60	14178	13.8	59.26 dB	119.38 %	23.46 %
70	20985	20.4	59.26 dB	161.42 %	29.14 %
-	-	-	-	-	-
100	30024	29.3	59.26 dB	261.53 %	29.50 %
ortalama			58.76 dB	106.81 %	21.49 %

Şifreli metin

Metin gizleme seçeneğindeki BMP dosyasına gizlenmiş resim için yapılan analiz.

Çizelge 6.4 BMP dosyasına gizlenmiş şifresiz metin için yapılan analiz.

Orijinal resim boyutu/KB	kapasitesi		PSNR	orijinal resim yüzde kaç büyüdü?	saklanan metin orijinal resmin yüzde kaçıdır?
	karakter	.txt boyut/ KB			
-	-	-	-	-	-
30	5673	5.54	36.80 dB	98.32 %	18.59 %
40	7884	7.69	36.80 dB	98.30 %	18.57 %
50	9600	9.37	36.79 dB	100 %	18.74 %
60	11484	11.2	36.79 dB	97.67 %	18.60 %
70	13537	13.2	36.79 dB	100 %	18.72 %
-	-	-	-	-	-
100	18984	18.5	36.79 dB	98.38 %	18.63 %
ortalama			36.79 dB	98.13 %	18.48 %

Şifresiz metin

Çizelge 6.5 BMP dosyasına gizlenmiş şifreli metin için yapılan analiz.

Orijinal resim boyutu/KB	kapasitesi		PSNR	orijinal resim yüzde kaç büyüdü?	saklanan metin orijinal resmin yüzde kaçıdır?
	karakter	.txt boyut/ KB			
-	-	-	-	-	-
30	4565	4.45	36.73 dB	98.32 %	14.93 %
40	5974	5.83	36.77 dB	98.30 %	14.08 %
50	7952	7.76	36.77 dB	100 %	15.52 %
60	9684	9.45	36.76 dB	97.67 %	15.69 %
70	11580	11.3	36.77 dB	100 %	16.02 %
-	-	-	-	-	-
100	15484	15.1	36.76 dB	98.38 %	15.20 %
ortalama			36.74 dB	97.29 %	14.75 %

Şifreli metin

Dosya gizleme seçeneğindeki JPEG dosyada gizlenmiş resim için üzerine yapılan analiz.

Farklı boyutlardaki orijinal resim dosyalarının (JPEG, BMP) içerisine kendi boyutunu geçmeyen herhangi bir dosya gizlenebilmektedir. Gizlenen bu dosyaların boyutları, orijinal resim ile dosya gizlenmiş resim arasındaki gürültü oranı değeri (PSNR), orijinal resmin yüzde olarak ne kadar büyüdüğü ve son olarak saklanan dosyanın orijinal resmin yüzde kaçını kapsadığı JPEG dosyası için çizelge 6.6 ve BMP dosyası için ise çizelge 6.7'de gösterilmiştir.

Çizelge 6.6 JPEG dosyasına gizlenmiş herhangi bir dosya için yapılan analiz

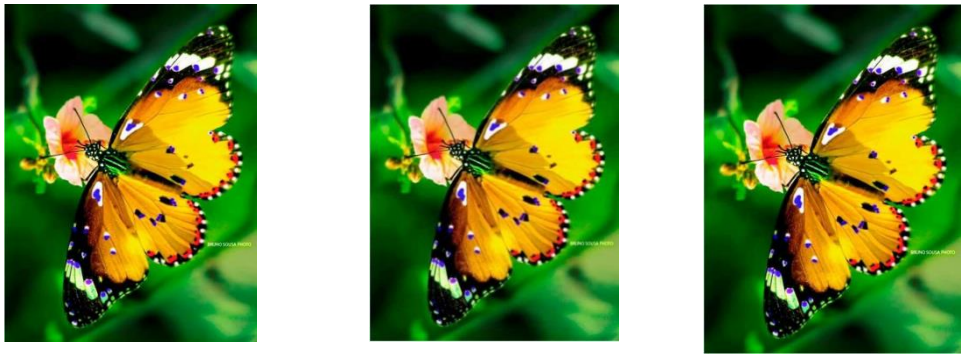
Orijinal resim boyutu/KB	Kapasitesi/ KB	PSNR	Yeni resim yüzde kaç büydü?	Saklanan resim orijinal resmin yüzde kaçıdır
-	-	-	-	-
30	37.8	38.47 dB	47.55 %	123.12%
40	59.6	45.88 dB	76.96 %	150.27 %
50	84.36	48.42 dB	94.76 %	169.73 %
60	114.83	50.99 dB	119.38 %	195.28 %
70	162.1	52.82 dB	152.85 %	231.57 %
-	-	-	-	-
100	207.82	55.32 dB	226.28 %	319.40 %
ortalama		47.49 dB	99.85 %	182.21 %

Dosya gizleme seçeneğindeki BMP dosyada gizlenmiş resim için üzerine yapılan analiz.

Çizelge 6.7 BMP dosyasına gizlenmiş herhangi bir dosya için yapılan analiz.

Orijinal resim boyutu/KB	Kapasitesi/ KB	PSNR	Yeni resim yüzde kaç büyüdü?	Saklanan resim orijinal resmin yüzde kaçıdır
-	-	-	-	-
30	37.8	37.45 dB	50 %	126.84 %
40	59.36	22.96 dB	54.34 %	143.38 %
50	84.36	37.07 dB	20.4 %	168.72 %
60	114.83	37 dB	11.79 %	190.74 %
70	162.1	36.94 dB	5.53 %	229.92 %
-	-	-	-	-
100	317.17	36.72 dB	-9.264 %	319.40 %
ortalama		32.55 dB	23.52 %	191 %

Uygulamada butterfly.JPEG isimli 480x648 piksel ve 39kb boyutunda renkli bir resim kullanılmaktadır. Şekil 6.8'de orijinal resmin içine 5kb büyüklüğündeki şifrelenmiş metin ve 5kb büyüklüğünde şifresiz metin dosyanın gizlenmesiyle elde edilen resimleri karşılaştırmaktadır.



a b c

Şekil 6.8.a. Orijinal resim (480x648 piksel), b. 5 KB şifreli gizlenmiş resim, c, 5 KB şifresiz gizlenmiş resim

SBG uygulamasının benzer uygulamalarla karşılaştırılması

Çizelge 6.8 SBG uygulamasının benzer uygulamalarla karşılaştırılması

Uygulama	Taşıyıcı dosya türü	Saklanan dosya türü	Dosya setine saklama	Şifreleme	Saklama kapasitesi	Klasör saklama özelliği	Dil
OpenPuff	bmp, jpeg, pcx,png	hepsi	var	var	256mb	var	İtalyanca
snow	ascii txt	metin	yok	var	<TB	yok	İngilizce
QuickCrypto	N/A	hepsi	N/A	var	N/A	yok	İngilizce
securengine	html, bmp, gif,png	hepsi	yok	var	<TB	var	İngilizce
stegoMagic 1.0	txt, bmp, wav	hepsi	yok	var	TB/8	yok	İngilizce
gifshuffle	gif	metin	yok	var	< TB	yok	İngilizce
TürkSteg	bmp	metin	yok	var	< TB	yok	Türkçe
Vergigizle.com	bmp	metin	yok	var	< TB	yok	Türkçe
stegHide	Jpg,bmp,wav	hepsi	yok	var	< TB	yok	İngilizce
deogol	html	metin	yok	yok	< TB	yok	İngilizce
Jphs	jpeg	hepsi	yok	var	< TB	yok	İngilizce
SBG	jpeg,bmp,pdf,docx xlsx,txt, rar,pptx, gif	hepsi	var	var	taşıyıcı dosyaların toplam boyutuyla sınırsız	var	Türkçe

7. TARTIŞMA VE SONUÇ

Bilgi Güvenliği için mevcut yöntemler kendi içinde yetersiz değil ancak uygulanabilirlik açısından eksiktir. Bu tez çalışmasındaki amacımız haberleşme güvenliğinin sağlamasında kullanılan yöntemlerin uygulanabilirliği konusundaki eksikliği gidermek ve mevcut durumu daha iyi hale getirmektir. Bu iyileştirmeyi sağlamak için de kriptografi ve steganografi yöntemleri bir araya getirilerek bir yazılım geliştirilmiştir. Bu sayede hem iletişim hem de veri gizliliği sağlanabilmiştir.

Uygulamamız bize iki seçenek sunmaktadır. Birinci seçenek Görüntü dosyasının içerisine metin gizleme işlemi, ikinci seçenek ise Görüntü dosyası içerisine çizelge 6.1'de gösterilen dosyaları gizleme işlemidir.

İlk seçenekte JPEG ve BMP görüntü dosyalarının içerisine şifreli ve şifresiz metin gizleme işlemi yapılmıştır ve yapılan analizler neticesinde; JPEG görüntü dosyası için çizelge 6.2 - 6.3'de, BMP görüntü dosyası için de çizelge 6.4 - 6.5'te gösterildiği gibi "orijinal resim yüzde kaç büyüdü" kısmındaki değerlerin değişmediği, bunun dışındaki bütün değerlerin (PSNR değeri, saklanan metin kapasitesi vs.) görüntü dosyasının boyutu yükseldikçe arttığı gözlemlenmiştir.

İkinci seçenekte ise JPEG ve BMP görüntü dosyalarının çizelge 6.1'de gösterilen dosyaları gizleme işlemi yapılmıştır ve yapılan analizler sonucunda; JPEG görüntü dosyası için çizelge 6.6'da, BMP görüntü dosyası için de çizelge 6.7'de gösterilen "PSNR değeri", "saklanan metin kapasitesi" gibi değerlerin, görüntü dosyasının boyutunun büyüdüğü sürece arttığı belirlenmiştir.

Sonuç olarak yukarıda bahsedilen her iki seçenek için hesaplanan PSNR değerlerinin yüksek olması, yapılan işlemlerin kalitesinin de yüksek olduğu (resim üzerinde yapılan işlemin, değişimin algılanabilirlik düzeyine etkisinin az olması) anlamına gelmektedir.

Steganografi ile Bilgi güvenliği konusunda literatürde pek çok çalışma ve uygulama bulunmaktadır. Ancak bu çalışmaların büyük çoğunluğu, steganografi yöntemini daha basit ve tekdüze ele almıştır. Steganografi üzerinde yapmış olduğumuz çalışma, bu konularda yapılan diğer çalışmaların hepsinin bir sentezi şeklindedir. Daha net bir ifadeyle geliştirdiğimiz uygulamamız yapılan diğer uygulamalara göre çok daha geniş bir uygulama alanına hitap etmektedir. Görüntü dosyası içerisine metin veya dosya gizleme işlemleri, yaptığımız uygulamada tek platformda sunulduğu için diğer rakip uygulamalara göre her zaman bir adım ileride olacaktır. Ayrıca veri gizleme ve iletim kalitesi konusunda da minimum hatayla başarı elde edilmiştir.

Teknolojinin gelişmesi ile dünyada hızlı yayınlayan steganografi ile bilgi güvenliği, askeriye, sağlık, gibi veri alışverişi yapılan pek çok alanında kullanılmaktadır. Teknolojinin rekabet üstünlüğü oluşturduğu bu devirde bilgi güvenliği ile uğraşan firmalar bu konularda yaptıkları çalışmaların kullanılabilirliği ve güvenirliği ile ilgili her zaman akıllıca çözümler üretmelidirler.

KAYNAKLAR

Anonim .2001 Web Sitesi: https://webhocam.com/default.html, Erişim Tarihi:25.02.2017

Atıcı, M.A. 2007. Steganografik Yaklaşımların İncelenmesi, Tasarımı Ve Geliştirilmesi. Yüksek lisans Tezi, Gazi Üniversitesi, Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı, 109,Ankara.

Atıcı, M.A. ve Sağıroğlu, S. 2016. Steganografi tabanlı yeni bir klasör kilitleme yaklaşımı ve yazılımı geliştirilmesi. Gazi Üniversitesi Mühendislik Mimarlik Fakülte Dergisi, 31(1), 129-144.

Choudhury, B., Das, R. and Tuithung, T. 2015. A Novel Method for Distributed ImageSteganography. Department of Computer Science and Engineering and Information Technology, 42, 423-435.

Coşkun, I., Akar, F. and Çetin Ö. 2013. A new digital image steganography algorithm based on visible wavelength. Turkish Journal of Electrical Engineering & Computer Sciences, 21 ,548-564.

Goel, S., Rana, A. and Kaur, M. 2013. A Review of Comparison Techniques of Image Steganography. Double Blind Peer Reviewed International Research Journal.

Juneja, B. and Sandhu, P. S. 2013. A New Approach for Information Security using an Improved Steganography Technique. J Inf Process Syst, 9(3), 405-424.

Kaygusuz, F. 2003. Bilişim Güvenliği, Pro-G Bilişim Güvenliği ve Araştırma Ltd, 64, Ankara.

Khan, M.S. and Rai, S.S. 2014. Encryption Based Steganography- Modern Approach for Information Security. International Journal of Computer Science and Information Technologies, 5(3), 2914-2917.

Koluguri, A., Gouse, and S. Reddy, B. 2014. Metin Steganography Methods and its Tools. International Journal of Advanced Scientific and Technical Research, 4(2), 888-902.

Koçak, C. 2015. Kriptografi ve stenografi yöntemlerini birlikte kullanarak yüksek güvenlikli veri gizleme. Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 31(2), 115-123.

Koech, V.K. 2016. Using Image Steganography Technique to Obscure Information from Unauthorized Users. A Project Report Submitted in Partial Fulfillment of the Requirements for the Award of Masters of Science in Computer Science of the University of Nairobi, 69, Nairobi.

Premkumar, S, Krishnakumar, V. and Vijayakumar, R. 2014. Steganography Usıng Target Pıxels Combıned Wıth Psnr And Vısual Cryptography For Secure Applıcatıon.

Sharma, H, Sharma, K.K. and Chauhan, S. 2015. Steganography Techniques Using Cryptography-A Review Paper. International Journal of Recent Research Aspects.3,106-108

Şahin, A. 2007. Görüntü Steganografide Kullanılan Yeni Metodlar Ve Bu Metodların Güvenilirlikleri. Doktora Tezi, Trakya Üniversitesi, Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı, 184, Edirne.

ÖZGEÇMİŞ

Adı Soyadı : Batmunkh GANBAT

Doğum Yeri : Moğolistan

Doğum Tarihi : 25/06/1990

Medeni Hali : Bekar

Yabancı Dili : Türkçe, İngilizce

Eğitim Durumu (Kurum ve Yıl)

Lise : Gegee (2008)

Lisans : Moğolistan Devlet Eğitim Üniversitesi Çizim Sanat Fakültesi Bilgisayar Grafik Tasarım (2012)

Yüksek Lisans : Ankara Üniversitesi Fen Bilimleri Enstitü Bilgisayar Mühendisliği Anabilim Dalı (Eylül 2013-Mayıs 2017)