T.C. İSTANBUL TİCARET
ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

KAOTİK YÖNTEM İLE EN DÜŞÜK DEĞERLİKLİ BİT STEGANOGRAFİ MODELİ VE UYGULAMASI

İdris BAYAM

Danışman
Dr. Öğr. Üyesi, Mustafa Cem KASAPBAŞI

YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
İSTANBUL - 2018

KABUL VE ONAY SAYFASI

İdris BAYAM tarafından hazırlanan **"Kaotik Yöntem İle En Düşük Değerlikli Bit Steganografi Modeli Ve Uygulaması"** adlı tez çalışması 04/06/2018 tarihinde aşağıdaki jüri üyeleri önünde başarı ile savunularak, İstanbul Ticaret Üniversitesi Fen Bilimleri Enstitüsü **Bilgisayar Mühendisliği Anabilim Dalı**'nda **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Danışman	**Dr. Öğr. Üyesi Mustafa Cem KASAPBAŞI** İstanbul Ticaret Üniversitesi
Jüri Üyesi	**Prof. Dr. Rıfat YAZICI** İstanbul Ticaret Üniversitesi
Jüri Üyesi	**Dr. Öğr. Üyesi Muhammed Ali AYDIN** İstanbul Üniversitesi

Onay Tarihi : 27/../2018

Prof. Dr. Necip ŞİMŞEK
Enstitü Müdürü

AKADEMİK VE ETİK KURALLARA UYGUNLUK BEYANI

İstanbul Ticaret Üniversitesi, Fen Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında,

- tez içindeki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,
- görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu,
- başkalarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunduğumu,
- atıfta bulunduğum eserlerin tümünü kaynak olarak gösterdiğimi,
- kullanılan verilerde herhangi bir tahrifat yapmadığımı,
- ve bu tezin herhangi bir bölümünü bu üniversitede veya başka bir üniversitede başka bir tez çalışması olarak sunmadığımı

beyan ederim.

Tarih 04.06.2018

İmza

İdris BAYAM

İÇİNDEKİLER

ÖZET

Yüksek Lisans Tezi

KAOTİK YÖNTEM İLE EN DÜŞÜK DEĞERLİKLİ BİT STEGANOGRAFİ MODELİ VE UYGULAMASI

İdris BAYAM

İstanbul Ticaret Üniversitesi
Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı

Danışman: Dr. Öğr. Üyesi Mustafa Cem KASAPBAŞI

2018, 85 Sayfa

Bu çalışmada, kaotik yöntemler kullanılarak en düşük değerlikli bit steganografisine ait bir model ortaya konularak bir uygulamaya geliştilmiştir. Kaotik algoritmaların ilk değere hassas bağlılığı ilkesinden yola çıkılarak piksel seçimi gerçekleştirilmiş böylelikle güvenlik açısından hem rassallık ilkesi hem de gizli anahtar boyutlarında güçlü bir kazanım sağlanmıştır.

Gizli içerik, taşıyıcı resme gömülmeden önce sıkıştırılarak veri manipülasyonu en aza indirilmiştir. Böylelikle görünmezlik, yük kapasitesi, görüntü manipülasyonlara karşı saldırı ve istatistiksel saptanamamazlık güçlendirilmiştir.

MSE, PSNR, Histogram Analizi, Enerji, Kontrast, Homojenlik, Korelasyon, Entropi gibi istatistiksel ölçütler ve VSL kullanılarak modelin başarısı ölçülmüş ve modelin başarısı açıkça ortaya konulmuştur.

Anahtar Kelimeler: En az anlamlı bit, kaotik algoritmalar, korelasyon, PSNR, Steganografi.

ABSTRACT

M.Sc. Thesis

THE LOWEST BIT STEGONOGRAPY WITH CHAOTIC ALGORITHMS AND AN APLLICATION OF THE MODEL

İdris BAYAM

İstanbul Commerce University
Graduate School of Applied and Natural Sciences
Department of Computer Engineering

Supervisor: Ass. Prof. Mustafa Cem KASAPBAŞI

2018, 85 pages

In this study, a model of the least significant bit steganography was introduced by using chaotic methods and put into practice. Pixel selection was performed by sensitive dependency to initial values for chaotic algorithms, thus providing a strong gain in both randomness principle and secret key domains in terms of security accessed.

Hidden content is compressed before embedding in the carrier image for minimizing data manipulation. Thus, invisibility, load capacity, attack against image manipulations and statistical undetectability have been strengthened.

The success of the model was measured using statistical metrics such as MSE, PSNR, Histogram Analysis, Energy, Contrast, Homogeneity, Correlation, Entropy, VSL, and the success of the model was clearly demonstrated.

Keywords: Least significant bits, chaotic algorithms, correlation, PSNR, Steganography.

TEŞEKKÜR

Bu araştırma için beni yönlendiren, literatür araştırmalarımda ve karşılaştığım zorlukları bilgi ve tecrübesi ile aşmamda yardımcı olan değerli danışman hocam Dr. Öğr. Üyesi, Mustafa Cem KASAPBAŞI'na teşekkürlerimi sunarım.

Bu araştırmayı ortaya koyacak aşamaya gelmemi sağlayan ve her zaman daha iyisini başaramam için bilgi ve tecrübeleriyle yolumu aydınlatan İstanbul Ticaret üniversitesinin tüm değerli kadrosuna sonsuz şükranlarımı sunarım.

Tez çalışması sırasında elde edilen bildirinin 4. uluslararası ICAS konferansında yayınlanması için tezimi maddi olarak destekleyen İstanbul Ticaret Üniversitesi Yayın Araştırma ve Proje Koordinatörlüğü'ne teşekkür ederim.

Tezimin her aşamasında beni yalnız bırakmayan aileme sonsuz sevgi ve saygılarımı sunarım.

İdris BAYAM
İSTANBUL, 2018

ŞEKİLLER

Sayfa

ÇİZELGELER

Sayfa

SİMGELER VE KISALTMALAR

MSE	Mean Square Error (Ortalama Karesel Hata)
PSNR	Peak Signal to Noise Ratio (Tepe sinyali Gürültü Oranı)
LSB	Least Significant Bit (En az Değerlikli Bit)
dB	Desibel
Pixel	Resim Öğesi

1.GİRİŞ

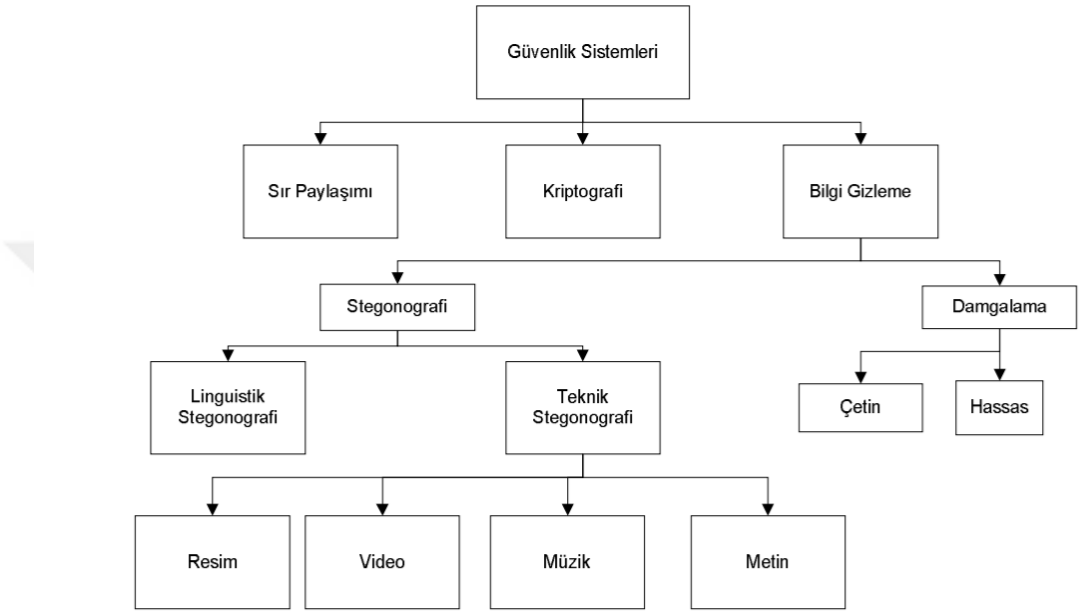
Gizli bilginin iletişimi, bilgi teknolojisinde artan seviyelerdeki karmaşıklıklarla zorluklar yaratmaya devam eden kritik bir faktördür. İletişim, aynı güvenli ağ üzerinde bulunan taraflar arasında gerçekleştiğinde, bu zorluklar yönetilebilir olarak düşünülebilir. Ancak, modern çağda beklenti kişinin bilgi gizliliğini tehlikeye atmadan dünyayı dolaşabilmesi ve aynı zamanda gizli bilgi alabilmesidir.

Dünyayı kapsayan genişlikte özel bir ağ hattına sahip olma olasılığının düşük olması nedeniyle, uzak kullanıcılar arasında gerçekleşen iletişim, çoğu zaman mevcut internete dayanır. World Wide Web (www) ve e-posta gibi genel kanallar, uzaktan iletişim için uygun olup, kullanılabilirlikleri temel avantajdır. Bununla birlikte, kabul edilebilir güvenliğin belirsizliği bu halka açık kanallarının en önemli dezavantajıdır. Bazı senaryolarda, iki taraf arasında özel bir tünel aracılığıyla güvenli iletişimi kolaylaştırmak için sanal özel ağlar (VPN'ler) uygulanabilir (Conklin ve ark. 2004: 266-7). Ancak, bu koşullarda bile bir VPN ağı kurmak için İnternet kullanılmaya devam edilir ve bir davetsiz misafir bir VPN tüneline girdiğinde, tüm ağa erişimi sağlanmış olur (Mavrakis 2003: 12).

Steganografi, dijital ortamda gizli bilgileri gizlemek için kullanılan ve böylelikle gizli iletişimin gerçekleştiğini gizleyen bir teknolojidir (Jamil 1999: 10). Gizli bilgileri daha az şüpheli dijital ortamlarda saklayarak, e-posta ve sosyal ağ siteleri gibi tanınmış kanallardan kaçınılır. Bu sayede bilginin aktarım sırasında sızma riskini azaltır (Artz 2001: 75).Bir saldırganın masum görünümlü bir resim dosyasına saldırmak için bir nedeni olmayacağından dolayı iletişimin güvenli sağlanmış olur.

2. LİTERATÜR ÖZETİ

Bilgisayar bilimlerinde güvenlik Cheddad ve ark. (2010) tarafından Şekil 2,1'deki gibi sınıflandırılmıştır. Bu sınıflandırmada veri güvenliği kriptografi, sır paylaşımı ve steganografi olmak üzere üç temel alana ayrılmıştır.



Şekil 2.1 Bilgisayar bilimlerinde, güvenlik sistemlerinin sınıflandırılması

Bölüm 1'de verilen amaçlardan biri, kriptografiye uygun bir alternatif olarak steganografinin görülebilir olup olmadığını ortaya koymaktır. Bu bölümde kriptografi ve steganografi tartışılmakta ve steganografi ile kriptografinin karşılaştırılması için çeşitli kıriterlere değinilmektedir. Aytıca tarihsel süreç içerisinde gelişimleri ele alınmaktadır.

Karşılaştırma için, öncelikle her bir teknoloji hakkında temel bilgiler verilecektir. Detaylı bir şekilde steganografi ortaya koyulduğu gibi karşılaştırma amaçlı kriptografinin de temel özelliklerine değinilmiştir. Hem steganografi hem de kriptografinin güçlü ve zayıf noktaları incelenmiş, iki teknoloji arasındaki farklılıklar ve benzerlikler üzerinde durulmuştur.

Dahası steganografi ve kriptografinin karşılaştırılması, her bir teknolojinin gerçekleştirmeyi amaçladığı, her birinin sunduğu güvenlik hizmetlerinin, her bir teknolojiyle ilgili problemlerin ve bunların uygulamalarının karşılaştırılması ile yapılmaktadır.

2.1 Karşılaştırma Ölçütleri

Her şeyden önce, steganografi ve kriptografi arasındaki ana fark, amaçlarında yatmaktadır. Kriptografi bir mesajın içeriğini saklamaya odaklanırken, steganografi mesajın varlığını gizlemeye odaklanır. Bu nedenle, hangisinin daha iyi olduğunu tespit etmek için bu iki teknoloji doğrudan karşılaştırılamaz. Bununla birlikte, karşılaştırma, güvenlik açısından her bir hizmetin sunduğu hizmetleri karşılaştırılarak genişletilebilir.

Güvenlik genel olarak üç temel boyutta tanımlanmıştır: gizlilik, bütünlük ve ulaşılabilirlik. Bu üç güvenlik boyutunun bir incelemesi olarak, ISO 7498-2 (1989) de beş güvenlik hizmetini tanımlamaktadır:

- Tanımlama ve kimlik doğrulama, bir kişinin kendini tanımlamasına ve sistemin bu kimliği doğrulamasına izin verir.
- Yetkilendirme, sistemin erişim hakkı verilen eylemlere izin veririp yasaklanan eylmeleri kısıtlamasıdır.
- Gizlilik, yetkisiz bir kişinin bilgi okumasını engeller.
- Bütünlük, yetkisiz kişilerin bilgileri değiştirmesini önler.
- İnkâr edilemezlik, bir kişinin yaptığı bir eylemi inkâr etmesini engeller.

Steganografi ve kriptografinin karşılaştırılması, iki teknolojinin, her birinin sunduğu güvenlik servislerinin hangileri olduğu, iki teknolojinin birbiriyle nasıl ilişkili olduğunu ve birbiriyle nasıl çeliştiğini göstererek yapılabilir.

Ayrıca karşılaştırma sadece her teknolojinin sunduğu güvenlik hizmetlerini içermemelidir aynı zamanda her bir teknolojiyle ilişkili problemleri de içermelidir. Beş güvenlik hizmetinin tümünü sunan ancak aynı anda çok fazla

sorun yaratan bir teknoloji, yalnızca bir veya iki güvenlik hizmeti sunan ancak ek bir sorunu olmayan bir teknolojiden daha iyi bir güvenlik çözümü değildir.
Son olarak, karşılaştırmanın bir parçası olarak, iki teknolojinin uygulanması karşılaştırılmıştır.

Bir sonraki bölümde kriptografinin temellerini oluşturan ana kavramlar kısaca ele alınacaktır. Buradaki odak noktası, kriptografi ve ilgili ortak sorun alanlarının sunduğu güvenlik hizmetleridir.

2.2 Kriptografi

Kriptografi alanı kâğıt-kalem yöntemlerinden başlayarak, özel olarak inşa edilmiş makinelerden ve bugün kullanılan matematiksel fonksiyonlara kadar zengin ve önemli bir tarihe sahiptir. . Kriptografinin kısa bir tarihçesi Çimen ve ark. (2008) tarafından şu şekilde verilmiştir.

1900'lü yılların başında Mısırlı bir yazar, yazdığı yazıtlarda standart olmayan hiyeroglif işaretler kullanmıştır.

MÖ 60-50 Julius Caesar devlet iletişiminde normal harflerin yerini değiştirerek resmi devlet yazışmalarında kriptografik yöntemi kullandı. Bu teknik metindeki her harfin alfabede kendisinden sonra gelen 3. harfle değiştirilmesine dayanıyordu.

725-790 Abu Abd al-Rahman al-Khalil ibn Ahmad ibn Amr ibn Tammam al Farahidi al-Zadi al Yahmadi, kriptografi hakkında bir kitap yazdı. Bizans imparatoru için Yunanca yazılmış şifreli bir metni çözmesi bu kitabı yazmasında ilham kaynağıdır olmuştur. Abu Abd al-Rahman, şifreli metni çözmek için ele geçirdiği mesajın başındaki açık metni tahmin etme yöntemini kullanmıştır.

1000 - 1200 yılları arasından, Gaznelilerden kalan bazı dokümanlarda şifreli metinlere rastlanmıştır. Bir tarihçinin bu dönemle ilgili yazdıklarına göre

yüksek rütbeli devlet görevlilerine yeni görev yerlerine giderken kişiye özel şifreleme bilgileri veriliyordu.

1586 Blaise de Vigenère (1523-1596) şifreleme ile ilgili bir kitap yazdı. Bu kitapta ilk kez, açık metin ve şifrelenmiş metin için otomatik anahtarlamadan bahsedilmiştir. Bugün, bu yöntem hala DES CBC ve CFB modlarında kullanılmaktadır.

1623 yılında, Sir Francis Bacon 5-bit bir ikili kodlama ve karakter tipi değişikliğine dayanan bir stenografi yöntemi buldu.

1790'da Thomas Jefferson, Strip Cipher'ı geliştirdi. Bu makineye dayanarak, M-138-A, II. Dünya Savaşı'nda ABD donanmasını kullanmıştır.

1917'de, Joseph Mauborgne ve Gilbert Vernam tek seferlik ped olarak adlandırılan ve mükemmel sayılabilecek bir şifreleme sistemi buldular.

1920'lerde ve 1930'larda FBI kaçakçıların iletişimini çözmek için bir araştırma bürosu kurdu. William Frederick Friedman, Riverbank Laboratuvarları'nı kurdu ve ABD için kriptoanaliz yaptı. İkinci Dünya Savaşı'nda Japon Mor Makine şifreleme sistemini çözdü. II. Dünya savaşında Almanlar, Arthur Scherbius tarafından icat edilen Enigma makinesini kullandılar. Bu makine Alan Turing ve ekibinin çalışmaları sonucunda çözüldü.

1970'lerde Horst Feistel (IBM), bugün hala kullanılmakta olan ve DES'in temelini oluşturan Lucifer algoritmasını buldu.

1976 yılında, DES (Data Encryption Standard) ABD tarafından FIPS 46 (Federal Bilgi İşlem Standardı) olarak ilan edildi.

1976 Whitfield Diffie ve Martin Hellman, Açık Anahtar sistemi hakkında bir makale yayınladı.

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

1985'te Neal Koblitz ve Victor S.Miller, ayrı çalışmalarında eliptik eğri kriptografik (ECC) sistemlerini tanımladılar.

1990 yılında Xuejia Lai ve James Massey, IDEA algoritmasını buldu.

1991 yılında Phil Zimmerman PGP sistemini geliştirdi ve yayınladı.

1995 yılında, SHA-1 (Güvenli Karma Algoritması) özet algoritması NIST tarafından standart olarak yayınlanmıştır. 1997 yılında, NIST (Ulusal Standartlar ve Teknoloji Enstitüsü), DES'in yerini alacak bir simetrik algoritma için bir yarışma açtı.

2001 yılında, NIST kazanan Belçikalı Joan Daemen ve Vincent Rijmen'in Rijndael algoritması, AES (Advanced Encryption Standard) olarak standartlaştırıldı.

2005 yılında, bir Çinli ekip tarafından SHA-1 algoritmasının kırıldığı açıklandı. Amerika, Microsoft ve Sun gibi birçok büyük şirket artık kullanmayacaklarını açıkladı.

2007'de, her programcı şimdi algoritmayı geliştirebilir ve bu algoritmayı programlayabilir. Bununla birlikte, geliştirilen algoritmalar her seferinde kırılarak doğrulanamadı. Bu gelişmeler Türkiye'de UEKAE tarafından takip edilmekte ve konuyla ilgili çalışmalar gerçekleştirilmektedir. (Ulutürk, 2010).

2.2.1 Kriptografinin tanımı

Gollman (1999:200) tarafından tanımlandığı gibi kriptografi, kodlanmış mesajların şifreleme ve deşifre etme yoluyla gizli yazışma bilimidir(Moerlan 2003). A ve B kişilerini dinleyen bir kişinin mevcut olması ve muhtemelen

iletişimi yakalayabilmesiyle, güvensiz bir kanal üzerinden haberleşmeleriyle ilgilenir.

Gollmann(1999:205) kriptografi teriminin genellikle şunları içeren kıriptografik mekanizmaların toplamına denk geldiğini belirtir:

- Şifreleme ve deşifreleme algoritmaları
- Bütünlük kontrolü fonksiyonları
- Dijital imza düzenleri

Şifreleme algoritmaları yetkili olmayan kişiye karşı veriyi karıştırarak anlaşılmaz hale getirip gizli mesajın özel tutulması üzerine odaklanır. Öte yandan, deşifreleme algoritmaları, şifrelenmiş mesajı tekrar deşifre ederek yetkili kişinin okuyabilmesi için açar.

Bütünlük fonksiyonun bir örneği de kriptografik hash fonksiyonudur(Whitman ve Mattord 2003:13). Bu, özgün olarak daha büyük dijital nesneleri tespit edebilen küçük bilgi parçalarını hesap eden matematiksel bir fonksiyondur. Farklı nesneler farklı hash değerleriyle sonuçlanır. Bu yüzden var olan nesneyle aynı hash değerine sahip olacak başka bir nesne yaratmak hesap bakımından mümkün değildir (Schneier 1963:94). Bu hash fonksiyonları bir mesajın gönderim sırasında değiştirilmediğini doğrulamak için kullanılır. Bütünlük kontrol fonksiyonlarının bir diğer örneği mesaj doğrulama kodlarıdır (MDK) (Gollmann 1999:206). Bir MDK iki girdiden işlenir: mesaj ve gizli kriptografik anahtar, ve ayrıca veriyle oynanmadığını belirten kontroller.

Dijital imza düzenleri, asimetrik şifreleme ile aynı prensipleri kullanarak bir mesajın iletişim kanalında dinleyen kişi tarafından değiştirilip değiştirtilmediğini tesbit etmeye yarayan mekanizmalardır.

Genel olarak şifreleme ve kriptografi terimleri birbirlerinin yerine kullanılırlar.

2.2.2 Kriptografinin geleneksel kullanımları

Esas olarak, kriptografinin şifreleme kısmı hassas bilgiyi yetkili olmayan kişilerden korumak amacıyla kullanılır. Bu kayıtlı veriler için şifrelemeyi ve güvenli iletişimi sağlamak için bilgiyi şifrelemeyi de içerir (Conklin ve ark. 2004:98). Eğer gizli dinleyen kişi mesajı yakalayabilirse de şifrelendikten sonra mesajın okunması imkânsız olmalıdır.

2.2.3 Şifreleme algoritmaları ve kriptografik anahtar

Auguste Kerckhoff 1883'te kriptografi mühendisliğinin ilk prensiplerini şekillendirdi. (Petitcolas, Anderson ve Kuhn 1999:1062). Kerckhoff prensibine göre şifreleme tekniği başkaları tarafından bilinebilir ama esas olan mesajı deşifre etmek için kullanılacak olan anahtar bilgisidir (Moerland 2003). Bu anahtar hem şifreleme evresinde hem de deşifre etme evresinde kullanılır ve anahtar olmaksızın şifrelenmiş mesaj deşifre edilemez, şifreleme algoritması bilinse bile. Modern şifreleme algoritmaları iki bölüme ayrılabilir. Simetrik ve asimetrik şifreleme. Her bir teknikteki anahtarların kullanışlılığına dayanır. Ayrıca gizli anahtar şifrelemesi diye bilinen simetrik şifreleme sistemleri göndericinin ve alıcının aynı anahtara sahip olmasını gerektirir. Bu anahtar hem mesajın şifrelenmesi ve deşifre edilmesi için gereklidir. Açık anahtar şifreleme diye de bilinen asimetrik şifreleme sistemi prensipleri alıcının ve göndericinin bir çift anahtara sahip olmasıdır. Anahtarlardan biri açıkken diğeri gizli tutulur.

Bu şifreleme algoritmalarının ikisi de güvensiz bir kanal üzerinden iletişim sırasındaki açıklara karşı koyabilecek güvenlik hizmetleri sunarlar.

2.2.4 Kriptografi tarafından sunulan hizmetler

Şifreleme algoritmalarının uygulanması yoluyla, gizlilik kriptografi tarafından sunulan en temel güvenlik hizmetidir. Hem simetrik hem de asimetrik şifreleme algoritmaları veri gizliliği sağlar. Ama ikisinde de bilginin gizliliğini güvenceye alan kullanılan teknik ve anahtarların uzunluğudur.

Bir mesaj gönderildiğinde hem göndericinin hem de alıcının iletişim sırasında bilginin değişikliğe uğramadığını bilmesi gerekmektedir. Bu değişiklik isteyerek ya da istemeyerek olmuş olabilir. Bu yüzden kriptografik hash fonksiyonları verinin bütünlüğünü güvenceye almak için kullanılır.

Hash fonksiyonları kriptografik anahtarlarla beraber kullanıldığında, MDK ler doğrulamayla beraber veri güvenliği de sağlarlar. Gönderici belirli bir mesaj için MDK çalıştırmak için ortak bir gizli anahtar kullanır. Alıcı MDK yi çalıştırdığında ve göndericiden aldığı MDK ile karşılaştırdığında, kullanıcı transfer sırasında mesajın değiştirilmediğine karar verir. İki MDK değerinin kıyaslanmasıyla, alıcı da mesajın beklediği kişiden geldiğine karar verir. Böylece göndericinin tanımlanması ve doğrulanması sağlanır.

Dijital imza düzenleri de veri kaynağını doğrulamayı sağlarlar (Schneier 1963). Ayrıca inkâr edememeyi de sağlar(Gollmann 1999:206). Asimetrik şifrelemeyle aynı prensiplere dayalı olarak, dijital imza da mesajı özel bir anahtarla şifreler. Şifrelenmiş mesaj imza olarak görev alır. Çünkü sadece belirli bir özel anahtar belirli bir sonucu doğurabilir.

Özetlemek gerekirse, kriptografi ISO 7498-2 tarafından belirlenen beş güvenlik hizmetlerinden aşağıdakileri sunar:

- Gizlilik
- Veri bütünlüğü
- Tanımlama ve Doğrulama
- İnkâr edememe

Ancak kriptografiye yönelik incelemeler burada bitmez. Çünkü kriptografiye bağlı sorunlar ayrıca kıyaslama önlemlerinin bir kısmını oluşturur.

2.2.5 Şifreleme sorunları

Farklı şifreleme algoritmalarından yola çıkarsak, simetrik şifrelemenin bariz sorunlarından biri eğer anahtar çalınırsa iletişimin açığa çıkabileceğidir. Bu

başka bir soruna da yol açar: anahtarların güvenli dağıtımı (Schneier 1963). Anahtar dağıtımı ya iki tarafın yüz yüze buluşmasıyla, ya güvenilir bir kurye yoluyla ya da var olan mevcut bir kriptografik kanalla yapılmasını içerir. İlk iki seçenek genellikle pratik ve güvenli değildir. Ancak üçüncü seçenek önceden bir anahtar değişiminin güvenliğine dayanır. Ayrıca anahtarları güvenli bir şekilde dağıtmak da yeterli değildir: anahtarlar güvenli bir şekilde depolanmalıdır, güvenli bir şekilde kullanılmalıdır ve en sonunda güvenli bir şekilde yok edilmelidir.

Açık anahtar şifrelemesi, simetrik şifrelemenin anahtar dağıtım sorununu çözer ama bu da kendine has sorunlar içerir. Açık anahtar şifrelemesinin dayandığı matematiksel fonksiyonlar henüz çözülemez olduklarını kanıtlamış değiller(Gisin ve ark. 2002:147). Şu anda, bir anahtarı diğer anahtarı açığa çıkarmak için kullanılan ve açık/özel anahtar arasındaki matematiksel ilişkiyi hızlıca hesaplayan algoritmalar yoktur ama olamayacak da denemez. Eğer bir bilim insanı böyle bir algoritma geliştirirse de şifreleme metodu savunmasız kalacaktır (Gisin ve ark. 2002:147).

Son olarak, kriptografi tarafından sunulan tüm güvenlik hizmetleri kriptoanalize karşı savunmasızıdır. Bazı şifreleme algoritmaları ve hash fonksiyonları çoktan kirptoanaliz tarafından kırılmıştır. (Wang ve Yu 2005:1; Gilbert ve Peyrin 2010:365; Bogdanov, Khovratovich ve Rechberger 2011:344).

Gollmann'a göre (1999:207) kriptografi nadiren bir güvenlik sorununa çözüm olabilir. Daha çok bir sorunu başka bir soruna dönüştürme mekanizması halini alır. Bir güvenlik sisteminde kirptografiyi uygulamak, sadece problemi güvenli iletişim sorunundan anahtar yönetim sorununa dönüştürür. Bu da genellikle sonuçta ortaya çıkan sorunun esas sorunu çözmekten daha kolay olması umudundan kaynaklanır.

Özetlemek gerekirse, kriptografinin karşılaştığı sorunlar:

- Anahtar dağıtım sorunu

- Asimetrik şifrelemenin matematiksel açıkları
- Devletler tarafından koyulan yasal sınırlar
- Kriptoanaliz

Buraya kadar kriptografi ile bilgiler verildi, güvenlik hizmetleri yaygın sorunlar tartışıldı. Esas soru peki stegonografi kriptografiye karşı uygun bir alternatif olabilir mi?

Bu soruyu cevaplamak için bir sonraki bölüm stegonografi üzerine odaklanacaktır. Temel kavramlar açıklanacak ve stegonografinin kullanımları vurgulanacaktır. En önemlisi de stegonografi tarafından sunulan güvenlik hizmetleri ve belirgin sorunlar kıyaslama için kullanılacaktır.

2.3. Steganografi

Stegonografi çok eski alan olsa da, modern formülasyonu Simmons (1983:57) tarafından mahkum problemi olarak ileri sürülmüştür. Daha resmi tanımı ise Birinci Uluslararası Veri Gizleme Çalışma grubunda yapılmıştır. Ancak, mahkûm problemi stegonografi uygulamaları için hala genel problem ifadesi olarak kullanılır.

Mahkûm problemi, iki mahkûmun bir kaçış planı oluşturmak için gizli bir şekilde iletişim kurmasıdır. Mahkumları bütün iletişimleri bir gardiyan tarafından iletilir ancak gardiyan herhangi açık bir iletişimden şüphe duyarsa ikisini de hücreye atacaktır (Chandramouli, Kharrazi ve Memon 2004:35). Bu yüzden mahkûmlar şüphe uyandırmadan iletişim kurmanın yollarını bulmalıdırlar. Mahkûmlar arasındaki iletişimi istediği gibi izleyebilen gardiyan, isterse aktif isterse pasif olabilir. Pasif bir gardiyan sadece iletişimi izler ve gizli bilgi içerip içermediğini anlamaya çalışır. Eğer gardiyan iletişimde gizli bilgi olduğundan şüphe ederse, pasif gardiyan bunu not alır ve dışardaki bir kişiye rapor eder ve mesaja da engel olmaz. Öte yandan, aktif gardiyan, şüpheli

iletişimdeki bilgide değişiklikler yaparak bilgiyi silmeye çalışır (Anderson ve Petitcolas 1998:474-81).

2.3.1 Stegonografinin tanımı

Steganografi, gizli bir mesajı örtülü bir mesaja bütünleştirmekle ilgilenen bir teknolojidir, öyle ki içindeki veri gizli kalır (Anderson ve Petitcolas 1998:475). Gizli mesaj açık yazı, şifreli yazı ya da veri akışı olarak temsil edilebilecek herhangi bir şey olabilir. (Johnson ve Jajodia 1998(a):273). Entegre etme işlemi bazen, stego anahtar denilen gizli bir anahtarla parametrize edilir ve bu anahtar bilgisine sahip olmaksızın yetkili olmayan kişinin gizli mesajı tespit etmesi ve çıkarması zordur. Örtülü nesne bilgiyi içine aldığı anda buna stego nesne denir.

Katzenbeisser ve Petitcolas'a göre (1999:25) güvenli bir steganografi sistemi esas örtülü nesnenin stego nesnesinden ne bir insan tarafından ne de istatistiki bir düzen arayan bir bilgisayar tarafından ayırt edilemez olması gibi tanımlanabilir.

Şimdiye kadar kriptografiyle steganografi arasındaki fark netleşmiş olması gerekir. Ancak, steganografiyle yakından alakalı olan ama farkın o kadar da net olmadığı teknolojiler de mevcuttur.

Steganografiyle yakından ilişkili olan ve aynı bilgi gizleme alanına giren iki teknoloji daha vardır: filigran ve parmak izi çıkarma (Anderson ve Petitcolas 1998:47481). Bu teknolojiler esas olarak fikri mülkiyetin korunması ile ilgilenir. Böylece, üç algoritma amaç, güç ve saklama kapasitesi bakımından ayrışır (Wang ve Wang 2004:10).

Filigranda bütün nesneler aynı şekilde "işaretlenir". Filigran kullanımında telif hakkı korunması amacıyla genellikle köken, sahiplik gibi bilgiler yer alır (Marvel, Boncelet ve Retter 1999:1075). Parmak izi çıkarma ise, öte yandan, farklı müşterilere dağıtılan farklı kopyalara özgün işaretler yerleştirir. Bu da fikri mülkiyet sahibine hangi müşterinin ürünü üçüncü şahıslara vererek lisans

anlaşmasını ihlal ettiğini anlama imkânı sunar (Anderson ve Petitcolas 1998:476).

Bu üç teknoloji arasındaki en temel fark filigran ve parmak izi çıkarmada iletişim nesnesi aynı zamanda telif korumasını taşıyan nesnedir (Wang ve Wang 2004:10). Öte yandan, steganografide gönderilecek şey entegre edilmiş veridir ve taşıyıcı nesne maske olarak hizmet verir.

Filigranda ve parmak izi çıkarmada bilginin dosyada gizlenmiş olması herkes tarafından bilinebilir ve hatta gözle de görülebilir. Ancak steganografide verinin algılanamaması önemlidir. Steganografik bir sisteme yapılan başarılı bir saldırıda karşı taraf dosyada bilgi gizlendiğini gözleyebilir (Artz 2001:75). Ancak filigrana ve parmak izi çıkarmaya karşı yapılan bir saldırıda ise esas olan gözlemlemek değil bu izleri silmektir.

2.3.2 Steganografinin geleneksel kullanımları

Genelde steganografi gizlice ve özgürce iletişim kurmak isteyen insanlar tarafından kullanılır. İletişimin gizliliği gözetlenen ortamlarda özellikle önemlidir. Steganografi ayrıca kriptografinin kullanımına izin olmayan ya da şüphe uyandıracak ortamlarda özel iletişimi korumak için kullanılabilir (Wang ve Wang 2004:10). Conklin ve ark. (2004:24) tarafından önerildiği gibi alternatif olarak steganografi diğer güvenlik mekanizmalarıyla beraber katmanlı bir güvenlik sağlayarak da kullanılabilir. Eğer davetsiz misafir bir katmanda başarılı olursa diğer katmanlarda da başarılı olmak zorunda kalacaktır.

Askeri ve istihbari ajanlar özellikle göze çarpmayan iletişim kurmak isterler. İçerik şifrelenmiş olsa bile, modern bir savaş alanında bir sinyalin tespiti gönderene karşı bir saldırıya dönüşebilir (Petitcolas, Anderson ve Kuhn 1999:1063). Steganografi bu sinyalleri gizli tutmak için kullanılabilir.

Staganografi ayrıca başkasına gönderilmesi gerekmeyen verileri depolamak için de kullanılabilir. Banka bilgileri gibi hassas bilgiler bilgisayarınızda örtülü bir nesne içerisinde tutulabilir.

2.3.3 Steganografi algoritmaları ve steganografik anahtar

Bütün steganografi sistemleri gizli bir anahtar kullanımını gerektirmez. Ama Kerckhoff prensibini steganografiye de uygulayarak teknoloji daha da güvenli hale getirilebilir. Bu prensibe göre, yetkisiz kişinin steganografik sistemin dizaynı ve uygulanması ile ilgili tam bilgiye sahip olduğu varsayılır. Böylece gizli anahtarları ya da açık anahtarları uygulamak steganografi uygulamaları için daha güvenlidir.

Ancak birçok mevcut steganografi uygulamalrı hala içlerinde anahtar bulundurmamayı tercih ediyorlar.

2.3.4 Steganografi trafından sunulan güvenlik hizmetleri

Steganografi bilgiyi başka bilgi içinde saklayarak hassas verinin güvenliğini sağlar. Tanımlama ve doğrulama sadece anahtar mevcutsa yapılabilir. Ama, bilginin saklanma tarzı ve kullanılan teknikler de kimlik olarak kullanılabilir. Bilgiyi entegre etme tekniği de böylece paylaşılan bir sır olur ve doğru şekilde entegre edilip çıkarıldığı zaman tanımlama ve doğrulama aracı olur.

Entegre edilen bilginin bütünlüğü kontrol edilemez çünkü bilgi kasti ya da kasti olamadan değişmiş olabilir ve yapılan değişiklikler de fark edilmeyecektir. Steganografide bilginin kökenini doğrulama işlevi olmadığı için, inkar edememe de sunulmaz çünkü biri sonradan bilgi entegre ettiğini inkar edebilir.

ISO 7498-2'de tanımlanan beş güvenlik hizmeti arasından stegonografi gizlilik sunar ve kısmen de tanımlama ve doğrulama sunar.

2.3.5 Steganografi sorunları

Bu alandaki en büyük endişe steganalizdeki ve karşı steganalizdeki araştırma ilerlemeleridir (Wang ve Wang 2004:10). Telif haklarını muhafaza etmek için filigran multimedya satıcıları tarafından başta çok ilgi gördü. Ancak son zamanlarda uzmanlar steganografinin yasadışı kullanımının dünya bilgi altyapısında ciddi bir tehdit oluşturabileceğini kabul ettiler(Kovacich ve Jones 2002:35). Örneğin steganografi teröristler tarafından devletin bilgisi olmadan iletişim kurabilirler. Bu tehdit yüzünden araştırmacılar aktif olarak var olan sistemlerdeki kusurları başarılı bir şekilde bulabiliyorlar. Bu kusurlar sadece gizli bilgiyi görmeye değil çıkarmaya ve yok etmeye de yarar. Steganaliz iki büyük tekniği içerir: görsel analiz ve istatistiki analiz. Görsel analiz gizli bilgiyi ya çıplak gözle (eğer ses ise dinleyerek) ya da bilgisayar yardımıyla açığa çıkarmaya çalışır. Öte yandan istatistiki analiz ise entegre yüzünden meydana gelen küçük değişiklikleri tespit etmek için kullanılır (Wang ve Wang 2004:10).

Hem kriptografi hem de stagonografi aslına bakılırsa bilgileri saklayarak masum insanlara zarar vermek için kötüye kullanılabilir. Standart şifreleme algoritmaları kriptoanalize karşı daha güçlü olduğu için devlet güçleri buna karşı daha güçlü düzenlemelere yöneldi. Steganografi, öte yandan, hala steganalize karşı zayıftır ve verinin yakalanıp okunma riski mevcuttur(Wang ve Wang 2004:12; Li ve ark. 2011:142).

Steganografiye karşı başka bir tehdit de, güvenli iletişim için e-mail servisinin bir güvenlik duvarı ile fotoğrafları engellemesidir.

2.4. Kriptografi Vs Steganografi

İkisi de bir mesajın farklı yönlerine odaklansa da amaçları mesajın güvenliğini sağlamaktır. İkisi arasındaki problemleri kıyaslarken sadece sorunların sayısını saymak elverişli değildir. Bunun yerine, sorunların etkisi ve bunların çözümünün olup olmadığı düşünülmelidir. Steganografiye karşı en büyük risk

steganalizdir. Eğer gizli anahtar kullanılıyorsa, anahtar dağıtımı da sorun olabilir.

Diğer taraftan kriptografik uygulamalar anahtar içermek zorundadır. Ancak anahtar dağıtımına ilişkin çözümler de (Bellare ve Rogaway 1994:232; Khalili, Katz ve Arbaugh 2003:342; Elboukhari, Azizi ve Azizi 2010:59) tarafından sunulmuştur.

2.5. Sonuç

Kıyaslamalardan sonra steganografinin kriptografiye alternatif olarak sunulabileceğini iddia etmek zordur. Kriptografi daha fazla güvenlik hizmeti sağlamaktadır ama daha fazla sorunu da beraberinde getirir. Ama bu steganografinin kirptografi yerine kullanılamayacağı anlamına gelmez. Bu sadece steganografinin şu anki envanterine daha fazla güvenlik hizmeti koyması gerektiğini belirtir. Tez boyunca steganografi aşağıdaki senaryolarda kullanılır.

- Öz-iletişim
- Kişiden kişiye iletişim
- Kişiden çok kişiye iletişim

3. STEGANOGRAFİNİN SINIFLANDIRILMASI

Steganografiyi sınflandırmak için iki yaklaşım vardır: (1) entegre etme sürecindeki farklı teknikleri tanımlayarak, ve (2) taşıyıcı dosya türlerine göre.

3.1 Steganografik Tekniklere Göre Sınıflandırma

Örtü nesnesine bilgi entegre etmenin üç yöntemi vardır(Weiss 2009:1):yerleştirme, değiştirme ve yaratma. Veri saklama teknikleri veriyi son kullanıcıyla alakası olmayan şekilde yerleştirilmesiyle uğraşır.

Değiştirme temelli teknikler ise kapaktaki veriyi gizli veriyle değiştirerek çalışırlar. Bu daha büyük boyutlu bir dosya oluşturmaz ama kapak maddesine ve steganografik algoritmaya bağlı olarak değiştirme kapak nesnesini özelliğini düşürebilir (Fridrich 2010:55).

Oluşturma tekniği is özel olarak bir kapak nesnesi yaratarak veriyi gizler. Oluşturulan kapak nesnesi genellikle gizli mesajın yapısına dayalıdır (Fridrich 2010:55). Yerleştirme ve değiştirme teknikleri stegoyu orijinal nesneyle kıyaslayarak keşfedebilirse de, oluşturma teknikleri buna karşı korunmalıdır çünkü oluşturma algoritmasının sonucu orijinal nesnenin kendisidir.

Kipper (2003:39) altı yeni kategori daha tanımlamıştır: ana olarak yer değiştirme, dönüşüm alanı, yayılma spektrumu, istatistiki metod, tahribat ve örtü üretme teknikleri.

Tabloda da gösterildiği gibi yer değiştirme en yaygın tekniktir. Yer değiştirme teknikleri kapak nesneye bilgi eklemediği için boyutu da artırmaz. Ama yer değiştirme tekniğinin dezavantajı değiştirilecek orijinal nesnenin veri miktarıdır ve dikkatle seçilmelidir. Eğer dikkatle seçilmezse, gizli bilgi arayan kişi için görünür olabilir. Birçok steganografik algoritma yer değiştirme tekniğini uygular.

3.2 Taşıyıcı Türlerine Göre Sınıflandırma

Dijital dosyalarda işlevsiz bitler nesnenin kullanımı ve işlenmesi için gerekenden çok daha fazla dosya kalitesi sağlayan bitler olarak tanımlanırlar (Currie ve Irvine 1996:194). Örneğin, insan gözü sadece10 milyon farklı renk algılayabilirken resim dosyaları 16 milyon farklı resmi gösterebilirler (Owens 2002:9). Böyece bir nesnenin işlevsiz bitleri tespit edilemeden değiştirilebilir(Anderson ve Petitcolas 1998:474). Steganografide yüksek seviyede işlevsiz bitlere sahip dosyalar tercih edilir çünkü bu bitler gizli bilgiyle değiştirilip algılanamayacak şekilde düzenlenebilir.

Resim ve ses dosyaları özellikle işlevsizlik görevi için gayet uygundur ancak bunu için başka dosya türleri de vardır.

- Yazı
- Resim
- Ses
- Protokol

Bu dosyaların her biri kendine has bilgi saklama tekniklerine uygundurlar.

3.2.1 Yazı steganografisi

Yazı içerisine bilgi saklamak tarihi olarak steganografinin en önemli metodudur. Yazı içine bilgi saklama metodlarından biri anlamsız şifredir. Burada her kelimenin N'inci harfi gizli mesajın bir harfini saklamak için kullanılır (Rabah 2004:245).

Bir diğer teknik de kitap şifresi olarak bilinir (Anderson ve Petitcolas 1998:474). Herkese açık kitap ya da gazete gibi kaynaklar örtü nesnesi olarak kullanılır. Taraflar arasında karakterleri gösteren bir kod paylaşılır. Örneğin

şifre grubu “54316” sayfa 54, 3. Satır ve 16ncı karakter anlamına gelebilir. Gizli mesajı bilmek için gizli kodu bilmek gerekir (Krenn 2004:3).

Ancak internetin çıkışıyla ve diğer dijital dosya türlerinin çıkmasıyla anlamsız şifreler ve kitap şifreleri önemini yitirmiştir (Moerland 2003).

Dijital dünyada, fontlara, font büyüklüğüne, satır aralıklarına, kalınlığa yapılacak ufak değişiklikler, steganografi için uygulanabilir. Mevcut bazı programlar White spacing ya da tabbing kullanırlar. Bu şekilde satırın sonundaki bir tab biri gösterebilirken tabın yokluğu ise sıfırı gösterebilir. (Moerland 2003).

Metin içinde bilgi saklamak için bir takım farklı teknikler tanımlanabilse de (Shirali-Shahreza 2008: 1912; Por, Ang ve Delina 2008: 735) metin dosyalarında çok az miktarda gereksiz veri olduğu için, dijital dosyaları kullanan metin steganografisi popülaritesi azalmıştır.

3.2.2 Resim steganografisi

Dijital görüntülerin temsil edildiği şekilde yaratılan büyük miktarda işlevsizlikten dolayı, resimler, steganografi için en uygun taşıyıcı tiptir. Resimlerdeki steganografi, aynı zamanda, sık sık web sitelerinde, e-posta ekleri, vb. Yerlerde sıkça görüldüğü için, en popüler biçimidir. Bu nedenle, dijital bir görüntü kullanıldığında, en az şekilde şüphe çekilir.

Görüntülerin popüler bilgi medyasının yanı sıra ideal taşıyıcılar olduğu düşünüldüğünde, bu tez sadece sonraki bölümlerde ve uygulamalarda görüntü steganografisine odaklanır.

3.2.3 Ses/vidyo steganografisi

Ses sıkıştırma, esas olarak, insan kulağının biyolojik özellikleri üzerinde yapılan araştırmalara dayanmaktadır, özellikle ses dosyasından çıkarılmadan ses

dosyasından çıkarılabilen veri miktarına bağlıdır (Bandyopadhyay ve diğerleri 2008: 109). Ses sıkıştırma algoritmaları, örneğin MPEG Model 1 Katman III (MP3), ses kalitesini kaybetmeden küçük dosya boyutlarını elde etmek için bu özellikleri kullanır (Atoum ve ark. 2011: 184). Bu özellikler, ses dosyalarındaki bilgileri işitilebilir olmaksızın gizleyerek ses steganografisi için de kullanılabilir. Sesin dijital gösterimi, belirli bir zamanda ses yoğunluğunu temsil etmeyi içerir. Bu ses yoğunluğu için 16 bitlik bir ses dosyası tipik olarak 216 seviyesine sahip olduğu için, 1 seviyedeki bir fark insan kulağı tarafından farkedilmeyecektir.

Ses steganografisine özgü bir teknik maskelemedir; soluk, ancak duyulabilir bir ses, daha yüksek sesli duyulabilir bir sesin varlığında duyulmaz hale gelir (Kipper 2003: 53). Yankı gizleme, bir ses dosyasına duyulmayan eko eklendiğinde oluşan başka bir tekniktir (Bender ve diğ. 1996: 332).

Steganografik potansiyeldeki görüntülere neredeyse eşit olmakla birlikte, anlamlı ses dosyalarının büyüklüğü onları görüntülerden daha az popüler hale getirmektedir (Artz 2001: 75).

Genel olarak, video dosyaları, görüntülerin ve seslerin bir koleksiyonu olarak görülebilir, bu nedenle görüntü ve ses steganografik tekniklerinin çoğu videoda da kullanılabilir (Papapanagiotou ve ark. 2005: 589). Video steganografinin avantajları, videoların büyük miktarda veriyi gizleyebilmeleridir. Görüntülerin ve sesin hareketli bir akışı olduğu gerçeği de faydalıdır, çünkü aksi takdirde dikkati dağıtan çarpıtmalar insanlar tarafından kolayca algılanmayacaktır. Video steganografinin bir dezavantajı, normal iletim kanalları üzerinden düzenli olarak iletilmeyen bir video klibin büyük boyutudur.

3.2.4 Protokol steganografisi

Protokol steganografisi terimi, ağ iletiminde yaratılan değişken veriler içerisine bilgi katma tekniğini ifade eder (Rabah 2004: 250).

Bir ağ paketi, paket başlıkları, kullanıcı verileri ve paket kutularından oluşur. OSI ağ modelini izleyen bir ağ üzerinden gönderilen tüm paketler aynı paket yapısına sahiptir. OSB ağ modelinin katmanlarında steganografinin kullanılabileceği gizli kanallar bulunmaktadır (Handel ve Sandford 1996: 23). Bilgi, mesajların işlevsiz kısımlarında gizlenebilir ve ağ üzerinden paketlerin iletilmesi için ağ kontrol protokolleri kullanılabilir.

Ahsan ve Kundur (2002), bir TCP / IP paketinin başlığında bilgilerin gizlenebileceği bir örnek sunmaktadır. İsteğe bağlı veya hiç kullanılmayan alanlar bilgileri gizlemek için idealdir. Her bir TCP paket segmenti, 6 bitin protokol tarafından kullanılmadığı, tek biçimli olarak biçimlendirilmiş 20 baytlık bir başlık ile başlar (Rabah 2004: 251). Tüm bu bitler gizli mesajı saklamak için kullanılabilir.

3.3 Sonuç

Bu bölüm, var olan farklı steganografi yöntemlerini göstermek için steganografiyi kategorilere ayırmıştır. Steganografi için uygun olan farklı taşıyıcı tiplerinden, dijital görüntüler şu anda mevcut olan en yaygın dosya türüdür (Fridrich 2010: xvii). Bu tezin kalan kısmı sadece görüntü steganografisine odaklanır. Bir sonraki bölümde farklı görüntü dosyası formatları ve üzerlerinde kullanılan sıkıştırma teknikleri ele alınmaktadır. Görüntü dosya formatları ve sıkıştırma üzerine bir tartışma, görüntü steganografisi için algoritmalar incelenmeden önce gereklidir.

4. DİJİTAL RESİM TÜRLERİ VE SIKIŞTIRMA

Steganography resim tekniğini anlayabilmek için resimlerin arka plandaki özellikleri ile ilgili çok sayıda sayısal verileri incelenmesi gerekmektedir. Bu bölümde resimlerin nasıl saklandığı, dijital resimlerin yapısı, renk kavramları ile ilgili geniş bir bakış açısı sunmaktadır.

Steganography tekniği resim özelliklerini bilgiyi saklayabilmek için bir mekanizma olarak kullanıldığı için bu tekniğin iyi anlaşılabilmesi için dijital resimlerin tanımlanması, resimlerin sıkıştırılması, farklı resim formatları ve özellikleri incelenecektir. Bu bölümde ele alınan kavramlar, Steganography tekniği ile ilgili olduğu için seçilmiştir ve bu nedenle, resim tanımları, resim sıkıştırma yöntemleri veya resim dosyası formatlarının kısa bir listesi değildir.

Bir sonraki bölümde renk gösterimi ve resim tanımı gibi dijital görüntüleme kavramları tartışılmaktadır. Bölüm 3, görüntü sıkıştırma teknikleri ile ilgili ayrıntıları ve bölüm 4 uzamsal etki alanı kategorilerinde tipik resim dosya biçimlerini inceler.

4.1. Dijital Resim Kavramlar

Bilgilerin görüntülere nasıl saklandığını tam olarak anlayabilmek için, dijital resim alanında düşünülmesi gereken birkaç kavram vardır. Renkler bölüm 2.1'de ele alınmış ve resim tanımına bölüm 2.2'de yer verilmiştir.

4.1.1 Renk gösterimi

Görünebilir ışık, elektromanyetik dalgalardan oluşur ve renkler, belirli bir dalga boyunda mevcut olan enerji miktarı ile tanımlanır. İnsan gözü, sayılamayacak kadar çok renk olmasına rağmen, sadece nispeten az sayıda olası rengi ayırt etme yeteneğine sahiptir.

Trichromatik renk teorisine göre, insan gözünün algılayabileceği her renk, üç temel renkten elde edilebilir: kırmızı, yeşil ve mavi. Bu teori, her sayısal olarak temsil edilen rengin kırmızı, yeşil ve mavi bileşenlerin doğrusal bir kombinasyonu olarak temsil edildiği ek renk modelinde kullanılmaktadır. Katkı renk modeli de RGB rengi olarak bilinir. R, G ve B ile gösterilen her bir renk miktarı ile model.

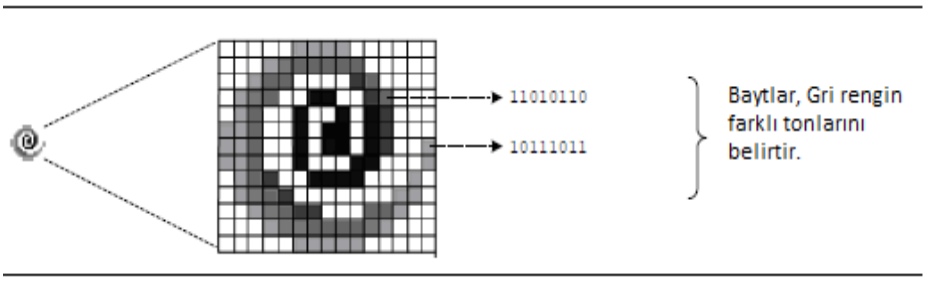
Bir başka popüler renk modeli, YUV renk modeli veya parlaklık / renklilik modelidir - RGB kanallarının ağırlıklı lineer kombinasyonu olarak tanımlanan parlaklık Y ile birlikte, U ve V renk bilgilerini taşır. Y, U ve V'nin 8-bit tam sayılarla temsil edileceği şekilde dönüştürüldüğünde, renk modeli YCrCb renk modeli olarak bilinir.

4.1.2 Resim tanımı

Bilgisayara göre, Resim, görüntünün farklı alanlarındaki farklı ışık yoğunluklarını oluşturan sayılar topluluğudur (Johnson ve Jajodia 1998(b):26). Noktalar piksel olarak ifade edilir ve pikseller, her bir pikselin bulunduğu ve renginin bulunduğu dikdörtgen bir harita oluşturur (Murray ve van Ryper 1996:124).

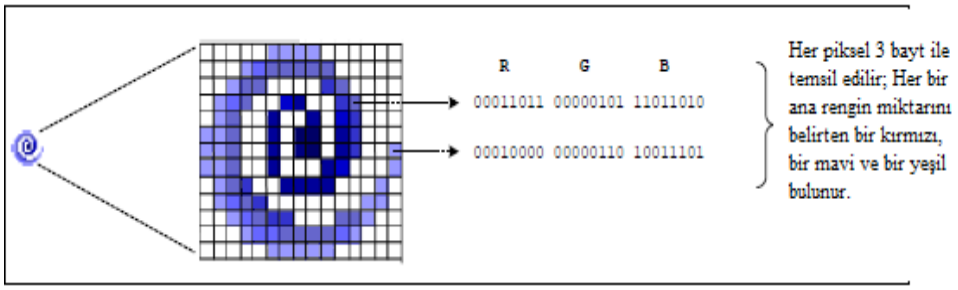
Bit derinliği olarak adlandırılan bir renk şemasındaki bit sayısı, her piksel için kullanılan bit sayısına karşılık gelir (Owens 2002: 8). Örneğin, bir görüntünün bit derinliği 8 ise, her pikselin rengini tanımlamak için 8 bit kullanılır ve toplam 256 farklı renk gösterilebilir.

Şekil 4.1. 256 farklı yoğunlukta griyi gösterebilen bit derinliği 8 olan gri tonlamalı bir görüntünün bir örneğini göstermektedir.



Şekil 4.1 8 bitlik gri tonlamalı bir görüntünün piksel ve bit gösterimi

Dijital renkli resimler genellikle bit derinliği 24 ile temsil edilir ve gerçek renk olarak da bilinen RGB renk modelini kullanır (Schneider ve Gersting 2004: 146). 24 bit görüntülerin pikselleri için tüm renk varyasyonları üç ana renkten türetilir: kırmızı, yeşil ve mavi ve her ana renk 8 bit ile gösterilir (Johnson ve Jajodia 1998 (b): 26).



Şekil 4.2 RGB renk modelinide 24 bitlik piksel ve bit gösterimi

Bir pikselde, 16 milyondan fazla kombinasyona sahip, 16 milyondan fazla renkle sonuçlanan 256 farklı kırmızı, yeşil ve mavi renk olabilir.

Karşılaştırma yapmak için, bir kalite ofset baskı makinesi yaklaşık 4000 renk basabilir, bir film fotoğrafı 6 milyon renkte bulunabilir ve insan gözü yaklaşık 10 milyon rengi tanıyabilir (Owens 2002: 9). Oluşan bu büyük atık miktarını Steganography algoritması avantaj olarak kullanabilmektedir.

Resim sıkıştırma teknikleri, bilginin dijital görüntülere nasıl yerleştirilebileceğini anlamada da çok önemlidir.

4.2 Resim Sıkıştırma

Resimlerin makul bir süre içinde görüntülenmesi ve görüntünün saklanması için makul miktarda alan kullanılması amacıyla, resmin dosya boyutunu küçültmek için teknikler kullanılmalıdır. Bu teknikler, resim verilerini analiz etmek ve yoğunlaştırmak için matematiksel formüllerden yararlanır ve daha küçük dosya boyutlarına neden olur. Bu sürece sıkıştırma denir (Schneider ve Gersting 2004: 147).

İki tip görüntü sıkıştırma yöntemi vardır: kayıplı ve kayıpsız (Moerland 2003: 4). Her iki yöntem de depolama alanından tasarruf sağlar, ancak uyguladıkları prosedürler farklılık gösterir. Aşağıdaki alt bölümler kayıplı ve kayıpsız arasındaki farkı anlatmaktadır. Kayıpsız sıkıştırma bölüm 3.1'de anlatılmıştır ve bölüm 3.2'de kayıplı sıkıştırma anlatılmıştır. Sıkıştırma ve steganografi arasındaki ilişki, bölüm 3.3'te anlatılmıştır. Farklı resim formatlarını anlatırken, sıkıştırma yöntemlerinin her birinin bir örneği daha sonra bölümde verilmektedir.

4.2.1 Kayıpsız sıkıştırma

Kayıpsız sıkıştırma, orijinal resimden herhangi bir bilgiyi kaldırırken, matematiksel formüllerde verileri temsil eder. Orijinal resimlerin bütünlüğü korunur ve sıkıştırılmış resim çıktısı orijinal resim girişiyle bit bazında aynıdır. (Schneider ve Gersting 2004: 149).

4.2.2 Kayıplı sıkıştırma

Kayıplı sıkıştırma, orijinal resimden fazla resim verisi atılarak daha küçük dosyalar oluşturur. İnsan gözünün ayırt edilmesi için çok küçük olan ayrıntıları ortadan kaldırır, tam bir kopya olmasa da, orijinal resmin yakın tahminleri ile sonuçlanır (Schneider ve Gersting 2004: 149).

4.2.3 Sıkıştırma ve steganografi

Sıkıştırma, steganografik algoritmaların tasarımında çok önemli bir rol oynar. Kayıplı sıkıştırma teknikleri, daha küçük resim dosyası boyutlarıyla sonuçlanır, ancak gömülü mesajın, gereksiz görüntü verilerinin kaldırılması nedeniyle kısmen kaybolabilme olasılığını artırır (Dunbar 2002: 5).

Kayıpsız sıkıştırma, orijinal dijital görüntüyü bozulmadan görüntü ayrıntılarını kaybetmeden korur. Ancak, görüntü küçük bir dosya boyutuna sıkıştırılmamıştır (Johnson ve Jajodia 1998 (b): 32).

Bu sıkıştırma türlerinin her ikisi için farklı steganografik algoritmalar geliştirilmiştir. Görüntü steganografi algoritmaları bir sonraki bölümde anlatılacaktır.

4.3.Resim Dosya Formatları

Resimlerin saklanma şekli çoğunlukla resmin dijital gösterimi ve sıkıştırma seviyesi arasında farklılık gösterir. Resim dosyası formatı genellikle görüntünün kullanım amacına bağlıdır, çünkü farklı resim dosyası formatları belirli bir amaç doğrultusunda geliştirilmiştir.

Çok çeşitli resim dosyası formatları olmasına rağmen, aşağıdaki bölümlerde açıklananlar, resim steganografisi ile ilgili olarak kabul edilir ve çoğu resim dosyası formatı, bu formatlardan birinin bir varyasyonu olarak görülebilir.

Resim formatları iki alana ayrılabilir: uzamsal alan ve dönüşüm alanı. Uzamsal alan formatındaki bir görüntü, yoğun bir dikdörtgen piksel ızgarası olarak temsil edilir (Fridrich 2010: 18).

Bununla birlikte, insan görsel sistemi bir resmi bir ızgara olarak algılamaz, aksine bir resmi dokuyla dolu parçaların bir koleksiyonu olarak algılar. Dönüşüm alanı formatındaki bir resim, daha yüksek bir sıkıştırma oranına izin vermek için sıkıştırma tekniklerine dayanan matematiksel formüller olarak temsil edilir (Fridrich 2010: 22).

4.3.1 Uzamsal alan formatları

Uzamsal alan formatları raster resim formatlarına ve palet tabanlı resim formatları olmak üzere ikiye ayrılabilir. Bir sonraki bölüm raster resim formatlarını anlatmaktadır ve palet tabanlı görüntüler bölüm 4.1.2'de daha ayrıntılı olarak ele alınacaktır. Her bölüm, resim dosya formatı görüntülerini örnekler verir ve varsa, her format için kullanılan sıkıştırma yöntemlerini anlatmaktadır.

4.3.1.1 Raster resimler

Raster resim formatında, bit derinliğine bağlı olarak bir pikseli saklamak için kullanılan bir veya daha fazla bayt içeren piksellerin sıralı bir satırında bir resim gösterilir (Fridrich 2010: 18).

Şekil 4.1 ve 4.2, raster resimlerin farklı bit derinliklerinde nasıl saklandığını gösteren örneklerdir. Microsoft Windows bitmap dosyası (BMP), bilgileri raster resim olarak saklayan bir resim dosyası biçimidir.

BMP formatı, kullanımdaki en basit resim dosyası formatlarından biridir. Resimler, 1 derinlik (2 renk), 4 (16 renk), 8 (256 renk), 16 (65 536 renk) veya 24 (16,7 milyon renk) ile saklanır.

BMP resim dosyası biçiminde sıkıştırma isteğe bağlıdır, ancak sıkıştırma gerektiğinde kayıpsız sıkıştırma kullanılabilir (Murray ve van Ryper 1996: 125).

BMP dosya formatları ile kullanılabilen kayıpsız bir teknik, uzunluk kodlamasını (RLE run length encoding) çalıştırmaktadır (Salomon 2004: 20). Bu sıkıştırma yöntemi, v1, v2,..., vn gibi özdeş değerlerin bir dizisini, v değerinin n kez çoğaltıldığını belirten bir değerler çifti (v, n) ile değiştirir (Schneider ve Gersting 2004: 147).

Çalışma uzunluğu kodlaması için iki yöntem vardır: Birinci yöntem, bitişik pikselleri bularak bir resmi sıkıştırır, örneğin, kırmızı, yeşil ve mavi bileşenlerin bit derinliği 24 için aynı olan piksellerdir. Bu pikseller, piksel çiftlerine sıkıştırılır. Örneğin, 24 bit renkli bir görüntüde aşağıdaki aynı piksel ızgarası:

RED	GREEN	BLUE
10100110	11000100	00001100
10100110	11000100	00001100
10100110	11000100	00001100

Tablo 4.1 24 Bit renkli bir görüntüde piksel ızgarası

Pikseller 10100110 11000100 00001100 değerine 3 kez sıkıştırılabilir. Belirli bir rengin sıklığı arttıkça, örneğin bir düz renk bloğu olan bir resimde, sıkıştırma oranı o kadar yüksektir.

Çalışma uzunluğu kodlaması için ikinci yöntem, her bir rengi ayrı ayrı sıkıştırmaktır. Belirli bir renk bileşeni için aynı değere sahip bitişik pikseller, diğer iki renk bileşeninin değerlerinden bağımsız olarak sıkıştırılabilir. Bu yaklaşım, aynı rengin geniş alanlarına değil, belirli bir rengin aynı yoğunluğunun tekrarına dayanmaz.

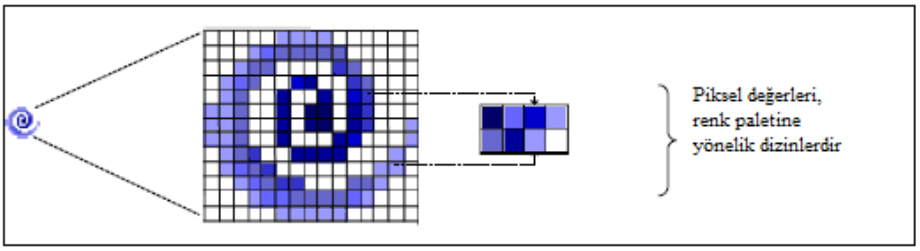
BMP resimleri çok büyük dosyalara (Fridrich 2010: 18) neden olabilir, ancak basitliği nedeniyle popüler bir resim dosyası formatı olarak kalır. BMP dosyaları resim steganografisi için de popülerdir, çünkü nispeten büyük mesajları saklama kapasitesi vardır (Fridrich 2010: 18). BMP dosyalarını kullanan resim steganografi algoritmaları, 5. bölümde ele alınmıştır.

4.3.1.2 Palet tabanlı görüntüler

Palet tabanlı görüntüler, İnternet'te yaygın olarak kullanılan bir başka popüler resim dosyası formatıdır. Bilgisayar tarafından oluşturulan grafikler, çizgi çizimleri ve çizgi filmler gibi resimler genellikle palet tabanlı resimler

kullanılarak saklanır. En yaygın olarak bilinen palet tabanlı resim dosyası formatı GIF'dir.

Bir GIF resminin format özellikleri, bir GIF resminin 8'den biraz daha fazla derinliğe sahip olamayacağını, dolayısıyla bir GIF'i renklendirmek için kullanılabilecek maksimum renk sayısının 256 olduğunu belirtmektedir.



Şekil 4. 3 Resim paletiyle 8 bitlik GIF görüntüsünün pikselleri ve dizinleri

Palet tabanlı resim formatı kayıpsız bir formattır. Bununla birlikte, bir raster resmini palet tabanlı bir resime dönüştürürken, bir ayrıntı kaybı oluşabilir. 24 bit RGB tarama resmini palet tabanlı resime dönüştürmek için, renk paletini oluşturup orijinal renkleri yeni oluşturulan palete eşlemek gerekir (Fridrich 2010: 19). Orijinal resmi 256'dan fazla farklı renk içeriyorsa, orijinal resimdeki renklerin sayısının azaltılması gerekir. Renk nicelleştirme, orijinal renklerin sayısını, mümkün olan en az görsel bozulma ile palete sığacak şekilde daha az farklı renklere indirgemek için kullanılan bir işlemdir.

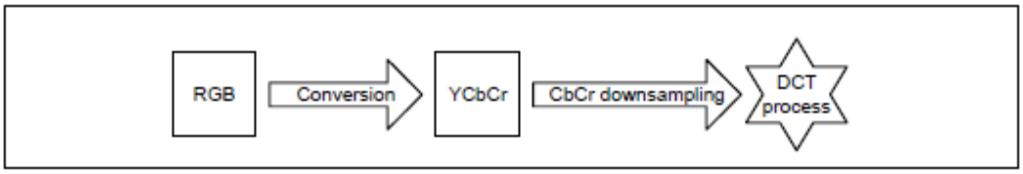
Palet elde edildikten sonra, orijinal renkler renk paletine dithering denen bir süreçle eşleştirilir. Renk paletinde olmayan orijinal renkler için, en az görsel bozulma ile sonuçlanan bir yaklaşım bulundu. Dithering de kayıp bir süreçtir.

4.3.2 Dönüşüm domain formatları

Dönüştürme alanı teknikleri, sıkıştırılması kolay resimleri ele alır. Bu tür teknikler normal olarak kayıplıdır ve bu nedenle, orijinal resmin bir detay kaybıyla bir yakınlaştırılmasını oluşturur.

Kayıplı sıkıştırma tekniğini kullanan bir resim formatı örneği, Joint Photographic Experts Group (JPEG) dosya formatıdır. JPEG dosya formatı, görüntülerin küçük boyutu nedeniyle İnternet'teki en popüler resim dosyası formatıdır. Özellikle gerçek dünyadaki sahnelerin veya nesnelerin foto grafik resimlerinin sıkıştırılmasında iyidir ve genellikle dijital kameralar ve tarama cihazları için yazılım tarafından kullanılmaktadır.

JPEG sıkıştırma, resmi kolayca sıkıştırılabilir bir forma dönüştürmek için ayrık kosinüs dönüşümünden (DCT) yararlanır. Bir JPEG görüntüsünü sıkıştırmak için, RGB renk gösterimi ilk önce bir YCrCb temsiline dönüştürülür. İnsan gözü, bir pikselin parlaklığındaki değişikliklere, renkteki küçük değişikliklerden daha hassastır. Dosyanın boyutunu azaltmak için chrominance bileşenini örnekleyerek kayıplı sıkıştırma şeması tarafından kullanılabilir. Kayıp sıkıştırmanın bu bileşeni Şekil 4.4'te gösterilmiştir.



Şekil 4.4 RGB dönüşüm ve UV örneği

Bir sonraki adım, resmin gerçek dönüşümüdür. JPEG resimleri için DCT kullanılır, ancak benzer dönüşümler örneğin ayrık fourier dönüşümü (DFT) ve ayrık dalgacık dönüşümü (DWT) olabilir. DCT, uzamsal alandan bir sinyali bir

frekans temsiline dönüştürür - dönüşüm alanı. Pikseller ilk önce 8 × 8 piksel bloklara ayrılır. Her bir piksel bloğu daha sonra DCT matematiksel formül kullanılarak 64 DCT katsayılarına dönüştürülür.

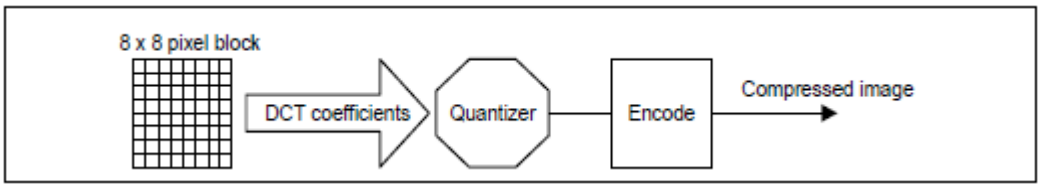
Sıkıştırma, bir resmi saklamak için gereken verileri azaltmak için iki tekniğe dayanmaktadır:

1. Görüntünün DCT katsayılarının niteliklendirilmesi, bir miktarın olası değerlerinin sayısını azaltmak, böylece görseli temsil etmek için gereken bit sayısını azaltır.

2. Nicelleştirilmiş verileri mümkün olduğu kadar kompakt bir şekilde temsil etmek için kuantize edilmiş katsayıların entropi kodlaması. Niceleme sırasında DCT katsayıları ilk olarak bir tamsayı değerine bölünür. Bölümde kullanılan tamsayılar kuantizasyon adımları olarak adlandırılır ve değerleri JPEG standardıyla önerilmektedir. Niceleme adımları daha yüksek frekanslar için daha büyüktür, bu yüzden yüksek frekansların çok küçük olmasını sağlar. Daha büyük kuantizasyon adımları daha yüksek sıkıştırma ile daha küçük dosya boyutları üretir, ancak daha fazla görsel bozulma ortaya çıkarır.

Daha büyük kuantizasyon adımları daha yüksek sıkıştırma ile daha küçük dosya boyutları üretir, ancak daha fazla görsel bozulma sağlar.

Bölümden sonra sonuçlar tamsayı değerlerine yuvarlanır. Algoritmanın kayıp kısmı yüksek frekanslar için, bu çoğunlukla sıfır olacaktır, bu da sıkıştırılması daha kolay olan büyük sıfır sıraları ile sonuçlanır. Katsayılar daha sonra entropi kodlaması kullanılarak kodlanır, örneğin Huffman kodlaması, renk frekanslarını sayısal değerlere dönüştürmek ve daha da küçültmek için kodlama yapmaktadır. DCT süreci Şekil 4.5'te tasvir edilmiştir.



Şekil 4.5 Ayrık kosinüs dönüşümü (DCT) süreci

4.4.Sonuç

Bu bölüm, kabul edilen resim dosyalarının formatını ve sıkıştırmasını ele almıştır. Resim steganografisinde bir çalışmanın devamı için önemli. Uzamsal alanda ve dönüşüm alanındaki görüntü formatları tartışıldı. Her alandaki ilgili sıkıştırma yöntemleri de tartışıldı. Bir sonraki bölüm, mekansal ve dönüşüm alanındaki resim steganografisini inceler.

5. RESİM STEGANOGRAFİSİ

Bu bölüm, resim steganografisine odaklanmakta ve tezin geri kalanı için gerekli temel bilgileri vermektedir. Nihai amaç, görüntü steganografisinin güvenli iletişim gereksinimlerine uygun olup olmadığını belirlemektir. Bu amaca ulaşmak için farklı uygulamalar için uygun algoritmalar belirlenmeli ve bu algoritmaların teknik detayları ele alınmalıdır.

Bölüm 4'te ele alındığı gibi, uzamsal alanın ve transform domainin JPEG görüntülerinin raster ve palet tabanlı görüntüleri, en popüler görüntü dosyası formatlarıdır. Bu nedenle bu bölüm sadece uzamsal ve trasnform domainlerindeki resimleri için özellikle geliştirilmiş steganografi algoritmalarını inceler. Bilgi teorisine, istatistiksel fiziğe veya sinyal işlemeye dayanan steganografi algoritmaları bu bölümün dışında tutulmuştur.

Bununla birlikte, bu bölüm önce resim steganografi algoritmaları için değerlendirme kriterlerini ele almaktadır. Bir resim steganografi algoritmasının belirli bir uygulama için uygun olup olmadığını görmek için, algoritmalar bir takım kıriterlere göre değerlendirilir.

Mekansal steganografi algoritmaları bölüm 3'te tartışılmakta ve transform domaini algoritmaları bölüm 4'te ele alınmıştır. Veri çıkarma işlemi genellikle gömme işleminin tersi olduğu için, her steganografi algoritması için sadece veri gömme işlemi ele alınmıştır.

Son olarak bölüm 5, bölüm 3 ve 4'te ele alınan görüntü steganografi algoritmalarının bölüm 2'de tartışılan değerlendirme kıriterlerine nasıl uyduğunun bir özetini vermektedir.

5.1. Değerlendirme Kriterleri

Wang ve Wang (2004: 78) bir resim steganografi algoritmasının üç önemli gerekliliği olarak saldırılarılara karşı görünmezlik, yük kapasitesi ve sağlamlık kriterlerini tespit etmişlerdir. Fridrich (2010: 13) bir başka önemli gereklilik olarak istatistiksel olarak saptanamazlığı bu kriterlere ekledi.

Değerlendirme kriterleri aşağıda açıklanmıştır:

Görünmezlik - Gömülü bilgilerin görünmezliği ilk ve en önemli gerekliliktir, çünkü resim steganografisinin gücü insan gözü tarafından fark edilmeme yeteneğinde yatmaktadır. Resimde değişimler fark edildiği an algoritma tehlikeye girer.

Yük kapasitesi - Yük kapasitesi, görüntünün bozulmasına yol açmadan dijital bir görüntüye gömülebilen bilgi miktarıdır. Gizli iletişim için resim steganografisi kullanıldığı için, algoritmalar yeterince büyük gizli mesajları saklamaya uygun olmalıdır.

Görüntü manipülasyonu saldırılarına karşı dayanıklılık - Yetkili taraflar arasında bir stego resim ile sağlanan iletişimi sırasında, görüntü gizli bilgileri silinerek aktif bir gözlemci tarafından değişikliklere uğratılabilir. Bu nedenle, steganografik algoritmaların, görüntüde kasıtsız olarak yapılan değişikliklerin yanı sıra kötü niyetli yazılımlara karşı da güçlü olması önemlidir.

İstatistiksel saptanamazlık – Birçok steganografik algoritma bilgi gömerken geriye istatisktisel yöntemlerle kolayca tespit edilebilecek izler bırakır. Bir algoritmanın istatistiksel olarak tespit edilememesi için, bir gözlemcinin gizli bilgilerin varlığını istatistiksel olarak kanıtlaması imkânsız olmalıdır.

Resim steganografi algoritmalarının yukarıdaki kıriterlere uyma derecesi, sonraki bölümde ele alınmaktadır.

5.2. Spatial Domain Steganografisi

Uzamsal domain steganografisi, bilgileri gizlemek için uzamsal biçimindeki görüntü formatlarını kullanır. Uzamsal domain teknikleri, bilgi gömmek için bit ekleme ve gürültü manipülasyonuna dayanan bit tabanlı yöntemleri kapsar (Johnson ve Jajodia 1998(a):273). Veri yerleştirme işlemi, görüntü pikseli değerlerinin verilerinin doğrudan gizli bilgilerle değiştirilmesişyle yapılır (Li ve ark. 2011:146). Uzamsal domain steganografi algoritmaları, dijital görüntülerin uzamsal alanda depolanma biçiminde yaratılan fazla miktardaki veriden yararlanır. (Kipper 2003:41).

Raster görüntülere uygulanabilen görüntü steganografi algoritmaları, bölüm 3.1'de tartışılmıştır ve bölüm 3.2, palet tabanlı görüntüler için görüntü steganografi algoritmalarını ele alınmıştır.

5.2.1 Raster resimler

Raster görüntüler için geliştirilen en iyi bilinen algoritma, en az anlamlı bit (LSB) algoritmasıdır (Fridrich 2010:59). Bir baytın son bitinin değerindeki değişiklikler, baytın temsil ettiği bilgiler üzerinde en az etkiye sahipt olduğundan en az anlamlı bit olarak kabul edilir. Bölüm 3.1.1, LSB ile veri gömmenin ve güçlü noktalarının kısa bir özetini verilmiştir. Daha sonra algoritmanın zayıf yönleri bölüm 3.1.2'de analiz edililip ve bölüm 3.1.3, LSB ile veri gömülmesine dayanan fakat daha fazla güvenlik sağlayan bir algoritma ele alınmıştır.

5.2.1.1 LSB gömülmesine genel bakış

En az anlamlı bite (LSB) veri saklama, bir baytın en az anlamlı bitini değiştirirken oluşan küçük farklardan yararlanır ve bir taşıyıcı görüntüye bilgi saklamak için yaygın ve basit bir yaklaşımdır (Johnson ve Jajodia 1998(b):28). Bir resmin içindeki baytların bir kısmının veya bazılarının en az anlamlı bit'i (diğer bir deyişle 8'inci bit) değiştirilerek gizli iletinin bir parçasına dönüştürülür. Popüler bir yaklaşım, göndericinin ve alıcının paylaştığı bir stego anahtardan üretilen bir yalancı rasgele yol boyunca gizli mesajı bitlere gizlemektir. Bu yola seçim kanalı denir (Fridrich 2010:54,60).

24 bitlik bir görüntü kullanıldığında, kırmızı, yeşil ve mavi renk bileşenlerinin her biri bir byte ile temsil edildiğinden her bir bileşenin bir kısmı kullanılabilir. Böylece yük kapasitesi, görüntüdeki piksel sayısının üç katı kadar yüksekseltilebilir (Moerland 2003). Uzamsal domain steganografisinde, bir algoritmanın gömme kapasitesi piksel başına bit olarak tanımlanır (bpp) (Li ve ark. 2011:146). LSB 24 bit renkli bir görüntüye için kullanıldığından 3 bpp'lik bir gömme oranı vardır.

Her bir renk kanalı 256 olası yoğunluk değerine sahip olduğundan, bir pikselin LSB'sinin değiştirilmesi, renklerin tonundaki küçük değişikliklerle sonuçlanır. Bu değişiklikler insan gözüyle algılanamaz (Fridrich 2010:60), bu durum da LSB gömülmesinin farkedilememezlik ilkesine uygundur. İyi seçilmiş bir görüntü ile en anlamsız iki bitin seçilmesi durumunda dahi farkedilememezlik ilkesi sağlanabilir (Johnson ve Jajodia 1998(b):28).

LSB ile veri yerleştirme iki geniş kategoriye ayrılabilir: veri saklamak için kullanılan her bir baytın LSB'lerinin sayısına bağlı olarak sabit büyüklükte veri yerleştirme yöntemleri ve değişken büyüklükte veri ekleme yöntemleri olarak iki kategoride ele alınabilir (Potdar, Han ve Chang 2005:717). Sabit boyutlu ekleme yöntemleri, taşıyıcı görüntünün her baytında sırrı saklamak için sabit

sayıda LSB kullanır (Lou ve Liu 2002:449). Değişken büyüklükte yerleştirme yöntemleri, her pikselin gömülme uygunluğuna göre bilgileri gömmek için kapak görüntüsünün her baytından değişken sayıda LSB kullanır (Lou ve Liu 2002:449). Tek rengin hakim olduğu büyük alanlarındaki pikseller ya da keskin şekillere sahip sınırlarda bulunan piksellerden kaçınılmalıdır, çünkü bu piksellerdeki değişiklikler görüntünün görsel olarak bozulmasına neden olabilir. Bununla birlikte, yüksek kontrastlı ve yüksek parlaklık alanlarındaki pikseller, fark edilebilir bir fark olmaksızın gizli mesajdan daha fazla biti barındırabilir (Lou ve Liu 2002:449). Görüntünün uygun olmayan alanlarda gömülmesini önlemek için tasarlanan algoritmalara adaptif steganografi algoritmaları denir (Fridrich 2010:54).

5.2.1.2 LSB gömülmesinin zayıf yönleri

LSB gömülmesi, uygulama kolaylığı nedeniyle popüler bir görüntü steganografi algoritmasıdır. Bununla birlikte, algoritmanın zayıf yönü, bir saldırganın kullanılan tekniğin farkında olması durumunda gömülü bilgiyi kolayca tespit edilebilmesidir (Wang ve Wang 2004:10).

LSB ile veri yerleştirme, görüntü kırpma, yeniden boyutlandırma, renk alanı dönüşümü veya yeniden örnekleme gibi görüntü işleme saldırılarına da duyarlıdır (Venkatraman, Abraham ve Paprzycki 2004:347). LSB algoritması, kayıplı sıkıştırmayla sıkıştırılmış görüntüler için uygun değildir. En az anlamlı bit çoğu zaman kayıplı sıkıştırma algoritmaları tarafından gereksiz olarak görülmekte ve bu nedenle sıkıştırma sırasında atılmaktadır. LSB gömülmesi bu nedenle görüntü işleme saldırılarına karşı güçlü değildir. Katıştırılmış bilgilerin algılanması kolay olduğu için LSB gömülmesi istatistiksel saldırılara karşı da dirençli değildir. Histogram saldırısı olarak adlandırılan oldukça basit bir istatistiksel saldırı, bir stego görüntüsünün histogramını inceleyerek gömülü bilgilerin varlığını tespit etmek için kullanılabilir (Fridrich 2010:63). LSB

gömülmesi sırasında kapak görüntüsünün LSB'lerini değiştirme işlemi, steganografinin kullanıldığını tanımlamak için kullanılabilecek görüntü histogramında karakteristik artefaktlara yol açar (Xi, Ping ve Zhang 2010:203).

5.2.1.3 LSB gömülmesine yönelik iyileştirmeler

LSB gömme için LSB değerlerini değiştirmek, algılanması kolay olan doğal olmayan bir histogram ile sonuçlanır(F ridrich, Soukal ve Goljan 2005:596). LSB gömülmesinin istatistiki saptamaya karşı savunmassını geliştiren, ± 1 gömülmesi adı verilen bir algoritma deişikliği yapılabilmektedir (Li ve ark. 2011:147). Bir LSB'nin değişmesi gerektiğinde, bitin karşıt bit değerine çevrilmesi yerine, baytta depolanan değer bir arttırılır ya da azaltılır (Fridrich 2010:119). Bu, LSB'yi modifiye etme etkisine sahiptir, fakat diğer bitleri de değiştirebilir. Örneğin, orijinal bayt 127 değerini (011111112) bir arttırılırsa 128 (100000002) olarak değişir. ± 1 gömme algoritması, stego görüntüsünün histogramı üzerinde açık bir imza bırakmadığı için LSB gömülmesinden daha zor algılanır(Fridrich, Soukal ve Goljan 2005:596).

5.2.2 Palet tabanlı görüntüler

Palet tabanlı görüntülerde, bir görüntü bir paletteki renklere işaretçi olarak saklanır. LSB yerleştirme, orijinal LSB algoritmasına birkaç ayarlamayla birlikte palet tabanlı bir görüntüde bilgi gizlemek için kullanılabilir. Bölüm 3.2.1, palet tabanlı görüntülerde LSB gömülmesine genel bir bakış ve palet tabanlı görüntüleri daha verimli bir şekilde yerleştirmek için LSB'ye yapılması gereken ayarlamaları göstermektedir. Bölüm 3.2.2, palet tabanlı görüntülerde LSB'nin zayıflıklarını tartışmaktadır. Palet tabanlı görüntüler için gelişmiş bir steganografi algoritması olan optimal parite yerleştirme, bölüm 3.2.3'te ele alınmıştır.

5.2.2.1 Palet tabanlı Görüntülere LSB gömme

Palet tabanlı bir görüntülerde pikselinin renkleri yerine indeksler saklandığından LSB'lerinde değişiklikler görsel bozulmaya neden olabilir. Bir pikselin en az anlamlı biti değiştirilirse, renk paletindeki indeks değiştiği için piksel tamamen farklı bir renk gösterebilir (Johnson ve Jajodia 1998(c):113). Bitişik palet girişleri benzer ise, çok az veya hiç fark edilmeyen bir değişiklik olabilir, ancak bitişik palet girişleri çok farklı olursa, değişiklik belirgin ve gizli bilgi görünür olacaktır. Bitişik palet girişlerinin renk değerleri arasındaki değişiklikler kademeli olarak değişebilir, ancak bir bit kayması nadiren oluşabilir (Johnson ve Jajodia 1998(a):273).

Yoğun renk değişikliklerinden kaçınmak için basit bir çözüm olarak palet için ön işleme yapılabilir (Fridrich 2010:69). Paleti önceden işlemek için bir yaklaşım paleti renk olarak sıralamaktır böylelikle ardışık renkler arasındaki farklar minimize edilmiş olur (Wang ve Wang 2004:79).

Başka bir yaklaşım, veriyi yerleştirmeden önce paletteki renk sayısını azaltmaktır. Farklı renklerin sayısı azaldığında, renkler tekrar orijinal renklere yakın olan renk paletine eklenir, ancak bu sefer farklı bir indekslerle ekleme yapılır (Katzenbeisser ve Petitcolas 1999:53). Örneğin, orijinal palet maksimum 256 renkten oluşuyorsa, renkler ilk önce renk nicemlemesi ile 128'e düşürülür. 128 rengin her biri için, orijinal rengin aynısı olan, ancak farklı bir indeksle yeni bir renk eklenir. Palet daha sonra sıralanırsa, bir dizinin LSB'si, orijinal rengin bir kopyasına işaret eder. Palet 128 renge düşerse, gömme oranı 1 bpp'dir. Ancak, orijinal renkler 64 veya 32'ye düşürülürse, piksel başına iki veya üç bitlik bir gömme oranı elde edilebilir (Fridrich 2010:69).

5.2.2.2 Palet tabanlı görüntülerde LSB gömülmesinin zayıflıkları

LSB'nin palet tabanlı görüntülerde gömülmesinin ana zayıflığı, palet tabanlı görüntünün kendisinin doğası ve indekslerin değiştirilmesi gerektiğinde görsel bozulma olasılığığının ortaya çıkmasıdır. Paleti ön işlemek, gömülü bilginin görünmezliğini artırır, ancak aynı zamanda, paletle kurcalama işlemi geriye net bir imza bıraktığından dolayı gömülü bilginin tespit edilebilirliğini de arttırır. Renk değerlerine göre sıralanan bir paletin doğal olarak oluşması muhtemel değildir (Fridrich 2010: 70) aynı zamanda iki, dört veya sekiz özdeş renk içeren bir palet de şüphelidir.

Optimal parite yerleştirme algoritması, palette değişiklik olmadan palet tabanlı görüntülerin içeriklerini gizlemek için Fridrich ve Du (1999: 47-60) tarafından geliştirilmiştir.

5.2.2.3 Optimal parite gömme

Optimal parite gömme, renk paletindeki her rengi o renklerin kırmızı, yeşil ve mavi değerlerine göre bir eşlik biti (0 veya 1) atar (Fridrich ve Du 1999:50). Parite biti P, aşağıdaki gibi formül 4.1 ile hesaplanır:

$$P = (R + G + B) \bmod 2 \qquad (4.1)$$

Burada P eşlik biti, R, G, B renk kanallarını temsil eder.

Gizli bir mesajı yerleştirirken, mesajın her bir biti için bir piksel seçilir ve pikselin parite biti ve mesaj biti arasında bir karşılaştırma yapılır. Aynı değilse, algoritma paletteki en yakın rengi zıt parite ile belirler. Bu renk bulunduğunda, pikselin indeksi en yakın renge işaret edecek şekilde değiştirilir.

Bilgiler, piksellerin LSB değerlerinde değil, piksellerin parite bitlerinde gizlenir. Görüntüdeki görsel bozulma, pikseldeki paletlerde benzer renklere işaret edecek şekilde değiştirildiği için minimumda tutulur.

5.3. Dönüşüm Domain Steganografisi

Dönüşüm domainindeki steganografi, görüntü dönüşümlerinin manipülasyonunu içerir(Johnson ve Jajodia 1998(a):273). Bu teknik ile gizli mesaj resmin daha anlamlı alanlarına saklanır böylece saldırılara karşı daha dayanıklı hale gelir ve saklanan veri kayıplı ve kayıpsız sıkıştırmalarda korunabilir(Provos ve Honeyman 2001)). Döşümün domain steganografisinin bir örneği olarak aşağıdaki alt bölümler JPEG steganografisini kullanır. Bölüm 4.1, JPEG steganografisine genel bir bakış sunmakta, ardından algoritmanın zayıf yönleri bölüm 4.2 de tartışılmaktadır. JPEG görüntü için daha gelişmiş steganografi algoritmaları, Outguess ve F5, daha sonra bölüm 4.3 ve 4.4'te kısaca ele alınmaktadır.

5.3.1 JPEG steganografi

JPEG sıkıştırma algoritması, genel olarak kayıplı ve kayıpsız aşamalara ayrılmıştır. Huffman kodlaması (Fridrich 2010: 23) daha fazla kayıpsız veri sıkıştırmak için kullanılırken bir önceki bölümde ele alınan DCT ve kuantizasyon fazı kayıplı veri sıkıştırma aşamasının bir parçasını oluşturur. Steganografi, genellikle gereksiz verilerdeki bilgileri gizlediğinden ve kayıplı sıkıştırma sırasında gereksiz veriler çıkarıldığı için, DCT ve kuantizasyon fazları sırasında steganografi yapılamaz. Steganografi, ancak, kayıp ve kayıpsız aşamalar arasında gerçekleşebilir. JPEG steganografisi için, Huffman kodlamasını uygulamadan önce mesajı sıfır olmayan tüm DCT katsayılarının en az anlamlı bitlerine yerleştirmek için LSB gömme kullanılır (Kipper 2003:50). Veriyi piksellere, başka bir deyişle uzamsal alana yerleştirmek yerine dönüşüm

domaininde bilgiler DCT katsayılarına gömülerek gizli veriyi görünmez kılar (Fridrich 2010:67). Dönüşüm alanı steganografi algoritmaları için gömme oranı sıfır olmayan katsayılar başına bit olarak ölçülür (bpnc) (Li ve ark. 2011:150). Bu nedenle JPEG steganografi için gömme oranı 1 bpnc'dir (Fridrich 2010:67).

5.3.2 JPEG steganografisinin zayıf yönleri

Doğal bir görüntünün DCT katsayılarının histogramı, tüm JPEG görüntüleri için sıfır civarında yoğunlaşmış belirli bir simetrik dağılım gösterir (Fridrich 2010:29). Bu dağılımın karakteristiklerine dair bilgi sayesinde gizlenmiş bilgi bulunmayan bir görüntünün dağılımı ile bir stego görüntüsünün histogramını karşılaştırarak bir bilginin gizlenip gizlenmediği tespit edilebilir. JPEG steganografisi bitlerin yerini değiştirdiğinden histogram normdan sapar ve gömülü bilgilerin varlığı istatistiksel olarak tespit edilebilir (Westfeld 2001:291).

JPEG steganografisinin istatistiksel olarak tespitini zorlaştırmak için, Outguess ve F5 algoritmaları, istatistiksel saldırılara karşı daha yüksek bir direnç seviyesi sunmak üzere geliştirilmiştir.

5.3.3 Outguess

Outguess algoritması ilk olarak Provos (2001: 323) tarafından tanıtılmış ve istatistiksel restorasyon gerçekleştiren steganografik algoritmaların bir örneği olarak görülmektedir. LSB gömülmesi, sıfır ve bir katsayılar hariç, DCT katsayılarının LSB'lerine mesaj bitlerini gömmek için kullanılır (Li ve ark. 2011:150). Histogramda görünür değişikliklerden kaçınmak için sıfır ve birler atlanır (Fridrich 2010:108). Gömmme işleminden sonra , taşıyıcı görüntünün histogramı stego görüntünün katsayılarının histogramına uyarlamak için kullanılmayan DCT katsayılarında düzeltmeler yapılır (Provos 2001:323). Gömmeden önce, algoritma yerleştirilebilecek gizli mesajın maksimum

uzunluğunu için düzeltme aşamasında yeterli kullanılmayan katsayıların olup olmadığını tespit eder (Fridrich 2010:108).

5.3.4 F5

F5 algoritması Westfeld (2001: 289) tarafından geliştirilmiş ve aynı zamanda bir stego görüntüsünün histogramının korunmasına odaklanmıştır. Gömme sırasında, LSB, mesaj bitine uymayan katsayıların LSB'lerini değiştirmek yerine, F5 algoritması, katsayıların mutlak değerini birer azaltmaktadır (Li ve ark. 2011:150). Bir birine eşit olan katsayılar, görsel bozulmadan sakınmak için kullanılmamaktadır (Fridrich 2010: 120). Katsayıların LSB'lerinin üzerine tekrar yazılmadığından, taşıyıcı görüntüsündeki değişiklikler artık stego görüntüsünün histogramında görünmez (Westfeld 2001: 300).

Yük kapasitesini arttırmak ve F5 algoritmasının istatistiksel olarak saptanamazlığını daha da artırmak için, taşıyıcı görüntüsünde yapılan değişikliklerin sayısını azaltmak adına matris gömme işlemi yapılır (Westfeld 2001:297).

5.4. Görüntü Steganografi Algoritmalarının Değerlendirilmesi

Bölüm 2, görüntü steganografi algoritmaları için dört değerlendirme kriterini tartışmıştır: görünmezlik, yük kapasitesi, görüntü manipülasyonu ataklarına karşı sağlamlık ve istatistiksel görünmezlik. Bölüm 3 ve 4'teki farklı görüntü steganografi algoritmalarının tartışmaları sırasında, algoritmaların kriterlere uyma düzeyi ele alınmıştır Bu bölüm yedi görüntü steganografi algoritmasının değerlendirmesinin bir özetini sunmaktadır: LSB gömme, ± 1 gömme, LSB palet tabanlı görüntülere gömme, optimum eşlik gömme, JPEG steganografi, Outguess ve F5.

Aşağıdaki yer alan 5.1 ile 5.4 bölümleri, algoritmaları görünmezlik, yük kapasitesi, görüntü manipülasyon ataklarına karşı sağlamlık ve istatistiksel olarak saptanamazlığa göre değerlendirmektedir. Bölüm 5.5, farklı görüntü steganografi algoritmalarının karşılaştırmasının bir özetini vermektedir.

5.4.1 Görünmezlik

Palet tabanlı görüntülerde LSB gömülmesi haricinde, yukarıdaki görüntü steganografi algoritmalarının hepsinde görünmezlik düzeyi yüksektir. LSB ile palet tabanlı görüntülerde gömme işleminin görünmezliği sadece palet sıralama veya renk çoğaltma yoluyla ön işlem yapılırsa yüksek olur. Paleti ön işleme tabi tutmadan palet tabanlı görüntülerin LSB değerlerinde değişiklikler yapılşması görsel bozulmalara yol açabilir.

5.4.2 Yük kapasitesi

Görüntü steganografi algoritmalarının yük kapasitesi karşılaştırıldığında, uzamsal domain steganografisi ile dönüşüm domain steganografisi arasında bir ayrım yapılmıştır. uzamsal alan steganografi algoritmalarının gömme oranı bpp (piksel başına bit) olarak ölçülürken, dönüşüm alanı steganografisinin gömme oranı bpnc (sıfır olmayan katsayı başına bit) olarak ölçülür. Bu yüzden farklı alanlardan gelen algoritmaların yük kapasitesi doğrudan karşılaştırılamaz. Uzamsal alanda, LSB gömme, palet tabanlı görüntülere LSB gömme ve ± 1 gömme, her biri 3 bpp'ye kadar bir gömme oranına sahiptir. Taşıyıcı görüntü olarak gürültülü görüntüler kullanılıyorsa bu algoritmalar, herhangi bir bozulma olmadan görsellere daha fazla bilgiyi gömebilir.

Bununla birlikte iletiden, LSB yerine her pikselin parite biti içine bir bit gömülü olduğundan optimal eşlik gömme 1 bpp'ye karşılık gelir. Ancak, Outguess'in yük kapasitesinin belirlenmesi daha zordur çünkü gömme sadece sıfır olmayan

katsayıların bir alt kümesi üzerinde gerçekleştirilebilirken, görüntüdeki histogramı düzeltmek için yeterli kullanılmayan katsayıların kalmasını gerekiyor. Gömme oranı, mesaj uzunluğu ile görüntünün sıfır olmayan katsayılarının sayısı arasında bir oran olarak görülebilir ve bir görüntüden diğerine değişebilir.

5.4.3 Görüntü manipülasyonu saldırılarına karşı dayanıklılık

Görüntü manipülasyonu saldırılarına karşı algoritmaların sağlamlığını belirlerken, uzamsal domaindeki görüntüler ile dönüşüm domainindekiler arasında bir ayrım yapılabilir. uzamsal domain formatları ve bu nedenle uzamsal domain steganografi algoritmaları görüntü manipülasyonu saldırılarına karşı güçlü değildir, çünkü görüntüdeki değişiklikler mesajın bitlerinde doğrudan değişikliklerle sonuçlanır. Diğer yandan, dönüşüm domaini steganografi algoritmalarında, görüntü verileri dönüşüm domaini alanında depolandığından ve doğrudan erişilemediğinden, görüntü işleme saldırılarına karşı daha dayanıklıdır.

5.4.4 İstatistiksel saptanamazlık

Bir görüntü steganografi algoritmasının istatistiksel olarak saptanamaması seviyesi, normal bir görüntü ile bir stego görüntüsü arasındaki fark edilebilir fark miktarına göre belirlenir. Gömme genellikle, doğal olarak meydana gelmeyecek bir stego görüntüsünün histogramında değişikliklere yol açar ve bir gözlemci tarafından tespit edildiğinde gizli bilgilerin varlığını işaret etmiş olur. Palet tabanlı görüntülerde LSB gömülmesi durumunda, paletin ön işlemesi yoluyla istatistiksel olarak saptanamazlığı arttırılır. LSB gömülmesinin, LSB'nin palet tabanlı görüntülere gömülmesinin ve JPEG steganografisinin istatistiksel olarak saptanamaması düşüktür bu nedenle gelişmiş algoritmalar ortaya çıkmıştır: LSB gömülmesinde ± 1 gömülme, palet tabanlı görüntülerde yer alan LSB gömülmesinde optimal parite gömülmesi geliştirilmiş ve hem Outguess

hem de F5, JPEG steganografisinde iyileştirme sağlayan yöntemler olarak geliştirilmiştir. Geliştirilmiş dört algoritma, görüntü histogramında bırakılan imzanın gömülme yoluyla en aza indirilmesi amacıyla geliştirilmiştir ve böylece bu algoritmaların istatistiksel olarak saptanamaması yükseltilmiştir.

5.4.5 Görüntü steganografi algoritmalarnın karşılaştırmalı özeti

Tablo 5.1, görüntü steganografi algoritmalarının bir karşılaştırmasını göstermektedir. Her algoritma için, algoritmanın değerlendirme kriterlerine uygun olduğu seviye, yüksek veya düşük olarak belirtilmiştir. Yük kapasitesi gömme oranını verir. Tablo 5,1'den görüldüğü gibi, yük kapasitesi ve istatistik görünmezlik arasında bir ödünleşim söz konusudur. Daha gelişmiş algoritmalar genellikle istatistiksel saldırılara karşı daha fazla direnç sağlar, ancak gömme kapasitesinde bir kayıp olur. Geride bir imza bırakmadan, bir görüntüye mesaj gömmek sadece küçük mesajlarla başarılı bir şekilde yapılabilir.

5.5. Sonuç

Bu bölüm, tüm olası görüntü steganografi algoritmalarının tam bir listesini sunmamıştır, bunun yerine, güvenli iletişimde görüntü steganografisi üzerine uygun görülen ve iyi bilinen algoritmaların bir listesi verilmiştir. Bu bölümün odak noktası farklı görüntü steganografi algoritmaları ve bunların nasıl uygulandığıydı. Görüntü steganografi algoritmalarının işlevselliğinin bilinmesiyle güvenli iletişim uygulamaları için algoritmaların uygunluğu konusunda bilinçli kararlar verilebilir. Bu bölümde yapılan görüntü steganografi algoritmalarının değerlendirilmesi de karar verme sürecine yardımcı olmak için kullanılabilir.

Tablo 5.1 Görüntü steganografi algoritmalarının karşılaştırılması

	LSB gömme	**± 1 gömme**	**Palet tabanlı resimlerde LSB gömme**	**Optimal parite gömme**	**PEG steganografi**	**Outguess**	**F5**
Görünmezlik	Yüksek	Yüksek	Yüksek*	Yüksek	Yüksek	Yüksek	Yüksek
Yük kapasitesi	3 bpp ye kadar	3 bpp ye kadar	3 bpp ye kadar*	1 bpp	1 bpnc	Resime göre değişir	1 bpnc
Görüntü manipülasyonu saldırılarına karşı dayanıklılık	Düşük	Düşük	Düşük	Düşük	Yüksek	Yüksek	Yüksek
İstatistiksel saptanamazlık	Düşük	Yüksek	Düşük*	Yüksek	Düşük	Yüksek	Yüksek

* palet ön işlemeye tabi tutulduysa

Bu tezin ilk yarısı, bu bölüm de dahil olmak üzere, görüntü steganografisini ayrıntılı olarak incelemeye odaklanmış ve teknolojinin durumu hakkında bilgi vermek için mevcut literatür gözden geçirilmiştir.

6.GZİP

Gzip dosya sıkıştırma ve sıkıştırılmış dosyayı açmak için kullanılan bir dosya formatı ve yazlım uygulamasıdır. Program Jean-loup Gailly ve Mark Adler tarafından erken Unix sistemlerinde kullanılan ve GNU tarafından ücretsiz bir yazılım olarak ("g", "GNU" dan geliyor) kullanılması amaçlanan bir sıkıştırma programı olarak yaratıldı. Versiyon 0.1, ilk olarak 31 Ekim 1992 tarihinde yayımlandı ve bunu Şubat 1993'te sürüm 1.0 takip etti.

6.1 Dosya Formatı

Gzip, LZ77 ve Huffman kodlamasının bir kombinasyonu olan DEFLATE algoritmasına dayanır. DEFLATE, zaman içinde, sıkıştırma ve diğer popüler arşivleyicilerin kullanılabilirliğini sınırlayan LZW ve diğer patent-korumalı veri sıkıştırma algoritmalarının yerini almayı amaçlamıştır.

"gzip" genellikle gzip dosya formatını ifade etmek için de kullanılır ve aşağıdaki özelliklere sahiptir:

- Sihirli bir sayı (1f 8b),sıkıştırma kimlik numarası, dosya bayrakları, zaman damgası, sıkıştırma bayrakları ve işletim sistemi kimliğini içeren 10 baytlık bir başlık bilgisine sahiptir.
- Orijinal dosya adı gibi dosya bayrakları ile belirtilen isteğe bağlı ekstra başlıklar.
- DEFLATE ile sıkıştırmış veriyi içeren gövde kısmı.
- CRC-32 sağlama bitlerini ve orijinal sıkıştırılmamış verinin uzunluğunu içeren 8 baytlık bir altbilgi.

Her ne kadar dosya formatı, çoklu dosyaların birleştirilmesine izin verse de (sıkıştırılmış dosyalar, tek bir dosyaymış gibi sıkıştırılmıştır) , gzip normalde sadece tekli dosyaları sıkıştırmak için kullanılır. Sıkıştırılmış arşivler, genellikle

dosya koleksiyonlarının tek bir tar arşivine birleştirilmesi ve ardından bu arşivin gzip ile sıkıştırılmasıyla oluşturulur. Nihai .tar.gz veya .tgz dosyasına genel olarak tarball denir.

Gzip kendisi gibi DEFLATE kullanan ZIP arşiv formatı ile karıştırılmamalıdır. ZIP formatı harici bir arşivleyici olmadan dosya yığınlarını tutabilir, ancak aynı veri miktarı için tarballardan daha az sıkıştırma yapar çünkü dosyaları tek tek sıkıştırır ve dosyalar arasında artık alanlardan yararlanamaz (katı sıkıştırma).

6.2 Uygulamalar

Programın çeşitli uygulamaları yazılmıştır. En yaygın olarak bilinen GNU Projesi'nin Lempel-Ziv kodlaması (LZ77) kullanılarak yapılan uygulamadır. OpenBSD'nin gzip sürümü, aslında OpenBSD 3.4'te gzip formatının eklenmesini sağlayan sıkıştırma programıdır. Bu özel versiyondaki 'g' gratis (bedava) için kullanılır. FreeBSD, DragonFlyBSD ve NetBSD, GNU sürümü yerine kullanılan BSD lisanslı uygulamalardır; aslında GNU uygulama seçenekleri ile uyumlu olması amaçlanan zlib bir komut satırı arabirimidir.

6.3 Kullanım Alanları

6.3.1 Web tabanlı sistemlerde veri trafiğinin sıkıştırılarak yönetilmesi

Web sitesini kodlarken bir çok farklı dosya kullanırız mesela resimler, videolar, yazılar, javascript, html veya php kodları gibi dosyalara hiç bir işlem yapmadan sunucumuza yüklersek dosya boyutu haliyle çok olur bu da web sitemizin yavaş yüklenmesine neden olur. GZip, web sitenize giriş yapan ziyaretçilerinize, web sitenizin dosyalarını sıkıştırarak iletmesinde kullanılır. Örneğin internet sitenize giren bir ziyaretçi, normalde indireceği boyut 80KB olmasına karşılık, bunu GZip ile 12-13KB olmasıdır. Bu sayede hem hızlı girişler yapılır, hem de CPU sorunu yaşamanızı engeller.

Arama motorları sitenin açılma hızına önem verirler. Bizim bu kullandığımız dosyaların bi şekilde boyutunu azaltmamız(sıkıştırmamız) lazım ki sitemiz görüntüsünden ve çalışmasından hiçbir ödün vermeden hızlansın.

6.3.2 Dosya sıkıştırma/açma işlemlerinde

Gzip hem uygulama olarak bağımsız bir şekilde hem de programların içinde kütüphane şeklinde dahil edilerek kullanılabilir. Uygulamamızda gzip bir kütüphane olarak eklenmiş ve sıkıştırma amaçlı kullanılmıştır.

7. UYGULAMADA KULLANILAN KAOS TABANLI ALGORİTMALAR

Kaos teorisi, başlangıç koşullarına oldukça hassas bağımlı olan ve dinamik sistemlerin davranışına odaklanan bir matematik dalıdır. 'Kaos', kaotik karmaşık sistemlerin görünürdeki rasgeleliği içinde, altta yatan paternler, sürekli geri besleme döngüleri, tekrarlama, öz benzerlik, fraktallar, öz-örgütlenme ve başlangıç koşullarına hassas bağımlılığı ifade eden disiplinler arası bir teoridir.

Kaotik sistemler, doğrusal olmayan dinamik sistemlerin basit bir alt türüdür. Çok az etkileşimli parça içerebilirler ve bunlar çok basit kurallar izleyebilir, ancak bu sistemlerin hepsi başlangıç koşullarına çok hassas bir bağımlılığa sahiptir. Belirleyici basitliklerine rağmen, bu sistemler zaman içinde tamamen tahmin edilemez ve çılgınca ıraksak (aka kaotik) davranışlar üretebilirler. Bu yüzden kaos teorisinin babası olarak kabul edilen Edward Lorenz, kaos'u "şimdiki geleceği belirler, ancak şimdiki yaklaşık, gelecekteki yaklaşığı belirlemez" şeklinde tanımlamıştır.

7.1 Başlıca Kaotık Haritalama Yöntemleri

Bu çalışmada kullanılan başlıca kaotik haritalama yöntemleri:

- Lojistik Harita
- Tent (Çadır) Harita
- Quadratic (Kuadratik) Harita
- Bernoulli Harita
- Sine Harita
- Chebyshev Harita

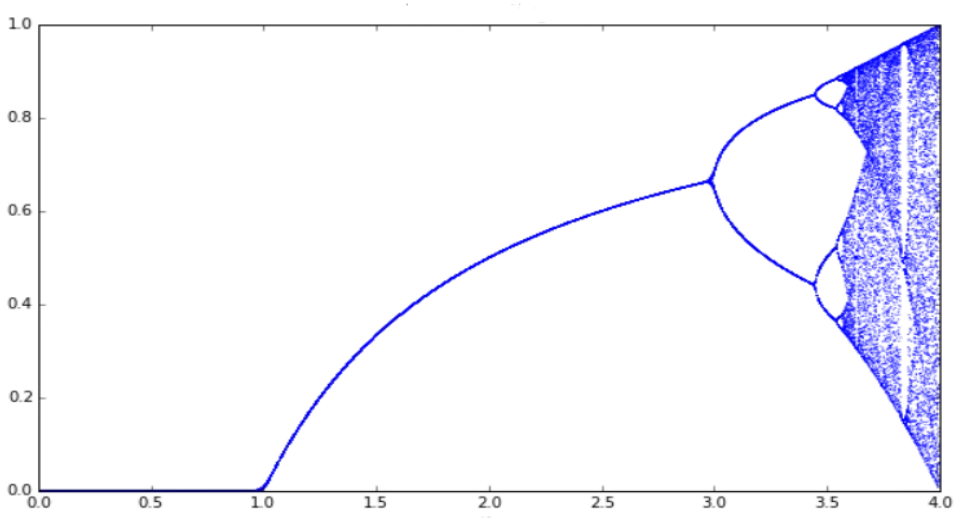
Ayrıca kaotik olmayan, ardışıl bitler üzerinden sıralı işlme yapan Sequential Harita örnekleri kullanılmıştır.

7.1.1 Lojistik harita

Bu model, bir nüfusun, taşıma kapasitesine ulaşması esnasında gittikçe azalmadan, önce yavaşça daha sonra hızla büyüdüğünü gösteren ortak s eğrisi lojistik fonksiyonuna dayanmaktadır. Lojistik fonksiyon, zamanı sürekli olarak değerlendiren diferansiyel bir denklem kullanır. Lojistik harita, ayrık zaman adımlarına bakmak için doğrusal olmayan bir fark denklemi kullanır. Buna lojistik harita denilmesinin nedeni nüfus değerini herhangi bir zaman adımında bir sonraki zaman adımındaki değerine eşlemesidir. Lojistik haritanın denklemi formül 7.1 de verildiği gibidir.

$$X_{n+1} = \mu X_n(1 - X_n) \qquad (7.1)$$

X, herhangi bir t anındaki nüfusu temsil eder ve μ, büyüme oranını temsil eder. Başka bir deyişle, herhangi bir zamanda nüfus seviyesi, büyüme oranı parametresinin ve önceki zaman adımı nüfus düzeyinin bir işlevidir. Büyüme oranı çok düşük ayarlanırsa, nüfus ölecek ve soyu tükenecektir. Bu denklemde belirli büyüme oranı parametrelerinde sistem kaotik davranmaya başlar.



Şekil 7.1 Biforkasyon (çatallanma)diyagramı

7.1.2 Tent (çadır) harita

Parçalı olarak tanımlanabilen çadır haritanın parametrik yapısı aşağıdaki gibi formül 7.2 ile tanımlanabilir.

$$T_r(x) = \begin{cases} 2rx, & 0 \le x \le \frac{1}{2} \\ 2r(1-x), & \frac{1}{2} < x \le 1 \end{cases} \tag{7.2}$$

$0 < r \le 2$ için bu harita aralıkların her birinde sürekli, doğrusaldır $(-1, 1/2)$ ve$[1/2, 1]$ (eğim r ve −r'ye göre) grafiğinde (0,0) ve (1,0) noktaları vardır. Bu harita, çadır haritaları olarak bilinir ve genellikle doğrusal olmayan ayrık dinamik sistemler için kaotik harita literatürünün ilk örneklerinden biri olarak tanıtılır. Dinamiklerinin sergilediği çeşitli özellikler kaotik sistemlerin tanımlanmasında yaygın olarak kullanılmaktadır. Kaos teorisi, karmaşık hareketleri ve hassas sistemlerin dinamiklerini tanımlar. Kaotik sistemler matematiksel olarak belirleyicidir fakat tahmin edilmesi neredeyse imkânsızdır. Kaos, uzun vadeli sistemlerde kısa vadeli sistemlere göre daha belirgindir. Kaotik sistemlerde davranış, periyodiktir, başka bir deyişle, hiçbir değişken, değerlerin düzenli tekrarına giren sistemin durumunu tarif etmez. Kaotik bir sistem, düzgün ve düzenli görünen bir şekilde evrim geçirebilir; Bununla birlikte, kaos, başlangıç koşulları doğru bir şekilde biliniyorsa, herhangi bir sistemin doğru ve uzun vadeli tahminlerini yapmanın mümkün olup olmadığına bakmaktadır.

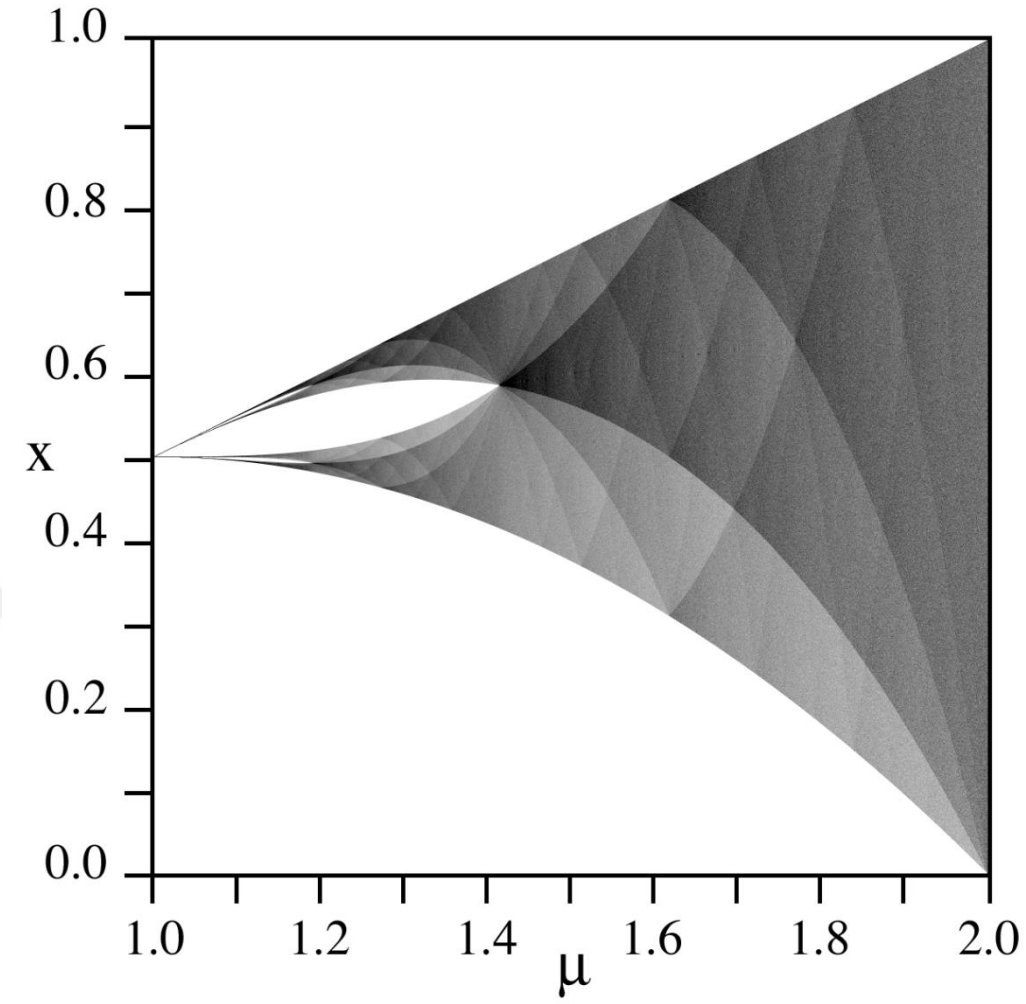
Deterministik kaos, çadır haritası T_r gibi deterministik harita ile aşağıdaki şekilde tanımlanabilir:

0 ile 1 arasındaki herhangi bir noktadan başlayarak, haritanın izi hala emici bir set olan çadır haritasının [0, 1] aralığında yer alacaktır. Ayrıca, [0, 1] içindeki

her bir nokta, herhangi bir 'tipik' çözüm tarafından keyfi olarak yakın ve sonsuz bir şekilde ziyaret edilecektir, dolayısıyla bu nokta aynı zamanda bir çekicidir.

Biz $0 < r \leq 2$ durumunda gözlemlerimizi sınırlandırabiliriz. Belirli parametre değerleri için, haritalama, germe ve katlama dönüşümlerine uğrar, başlangıç koşullarına ve periyodikliğe duyarlılık gösterir.

Çadır haritası, dinamik sistemlerin matematiğinde çalışılmaktadır. Basit şekli nedeniyle, çadır haritası iterasyonlar altında çok iyi şekilde anlaşılmıştır. Ancak basit şekline rağmen, birkaç ilginç özelliği vardır.Aşağıda çadır haritanın [1,2] aralığında sergilediği kaotik davranışının haritası verilmiştir.



Şekil 7.2 Tent haritasına ait çatallanma diyagramı

Bir bifürkasyon, çözümün doğasındaki temel bir değişikliktir. Dinamik sistemler çalışırken, genellikle sistemin ne zaman bifürkasyon geçirdiğini bilmek isteriz. Bir bifürkasyon diyagramı, değişen parametrenin değerini, bizim durumumuzda r, bir eksende ve diğer eksende sisteme olan çözümü gösteren bir tür çizimdir.

Genellikle sistem davranışlarının parametreler üzerinde nasıl olduğunu bilmek isteriz. Çadır haritası T_r denkleminde tek bir parametre olan r değerine sahibiz ve r <1/2 için kararlı bir denge olduğunu zaten biliyoruz. Ayrıca r> 1/2 için iki adet sabit olmayan denge durumu mevcuttur, bazı kararsız periyodik çözümler

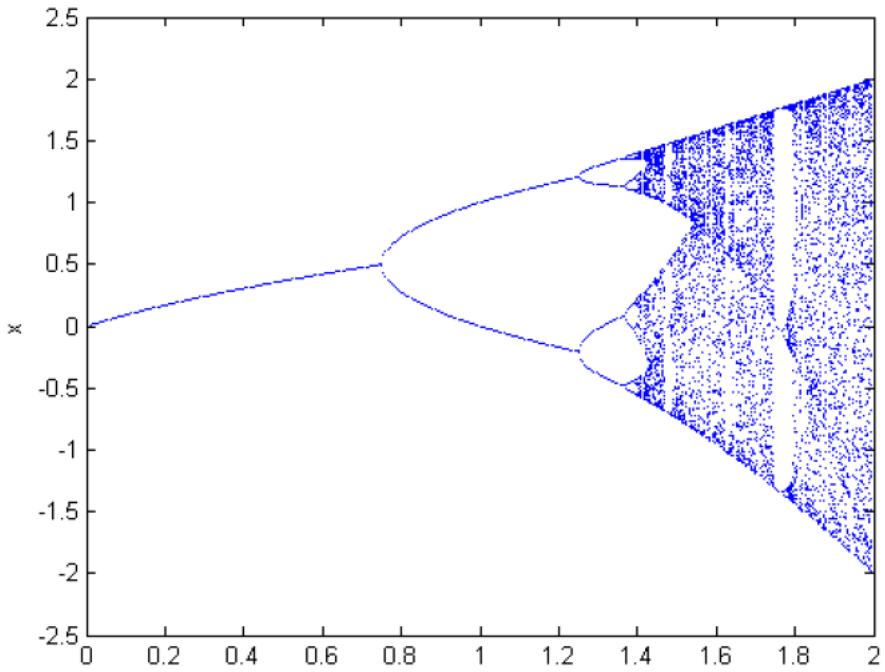
ve daha önce de gördüğümüz gibi kaotik çözümler olduğunu biliyoruz. Böylece tüm bunların, bir bifürkasyon diyagramı ile r parametresine nasıl bağlı olduğuna dair bir genel bakış elde edebiliriz.

7.1.3 Quadratic(kuadratik) harita

Kuadratik harita kaos davranışı sergileyen basit bir ayrık sistemdir ve aşağıdaki gibi formül 7.3 ile tanımlanmış.

$$X_{n+1} = r - X_n^2 \tag{7.3}$$

Burada $0 < r \leq 2$ kontrol parametresi olarak adlandırılır ve $X_n \in (-2,2)$ sistemin durum değişkeni olarak tanımlanır. Kuadratik harita, durağan bir sistemden kaotik bir duruma kadar zengin dinamik davranışlar gösterebilir. $r \in (0.0.74)$ olduğunda, harita sabit durumda hareket eder ve $r \in [0,74,1.5)$ ise, harita periyodik davranışa sahiptir. $r \in [1.5,2]$ olduğunda, kuadratik harita çok karmaşık bir davranışı sergileyebilir, bu da haritanın çıkışının, başlangıç koşullarına aperiyodik, yakınsak olmayan ve çok hassas olduğu anlamına gelir. Bu nedenle, kontrol parametresinin değeri sistemin dinamik davranışını belirler.

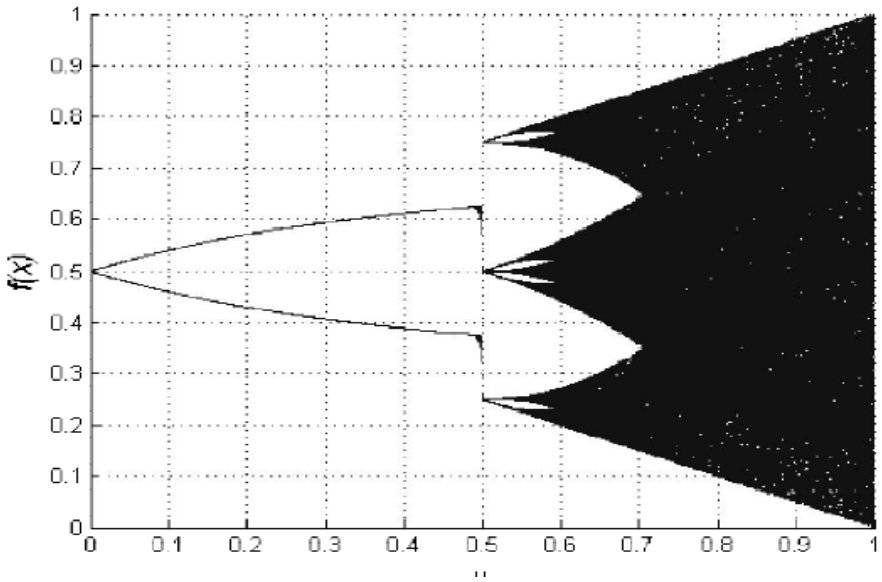


Şekil 7.3 Kuadratik haritanın çatallanma diyagramı

7.1.4 Bernoulli harita

Basit deterministik sistemler, çok karmaşık ve rastgele davranışlar sergileyebilen kaotik süreçler üretebilir. Bunun yanında kaotik fonksiyonlarla kaotik dizileri oluşturmak için en basit şekilde tek boyutlu haritalar kullanılabilir. Aynı zamanda bernoulli haritasının basit bir sayısal iplementasyonu mevcuttur. Bu fonksiyon aşağıdaki 7.4 formülüyle ifade edilebilir.

$$X_{i+1} = \begin{cases} 2\mu x_{i+} \frac{(1-\mu)}{2}, \ ve 0 \leq x < 0.5 \\ (2\mu x_i - 1) + \frac{(1-\mu)}{2}, \ ve 0.5 \leq x < 1 \end{cases} \quad (7.4)$$



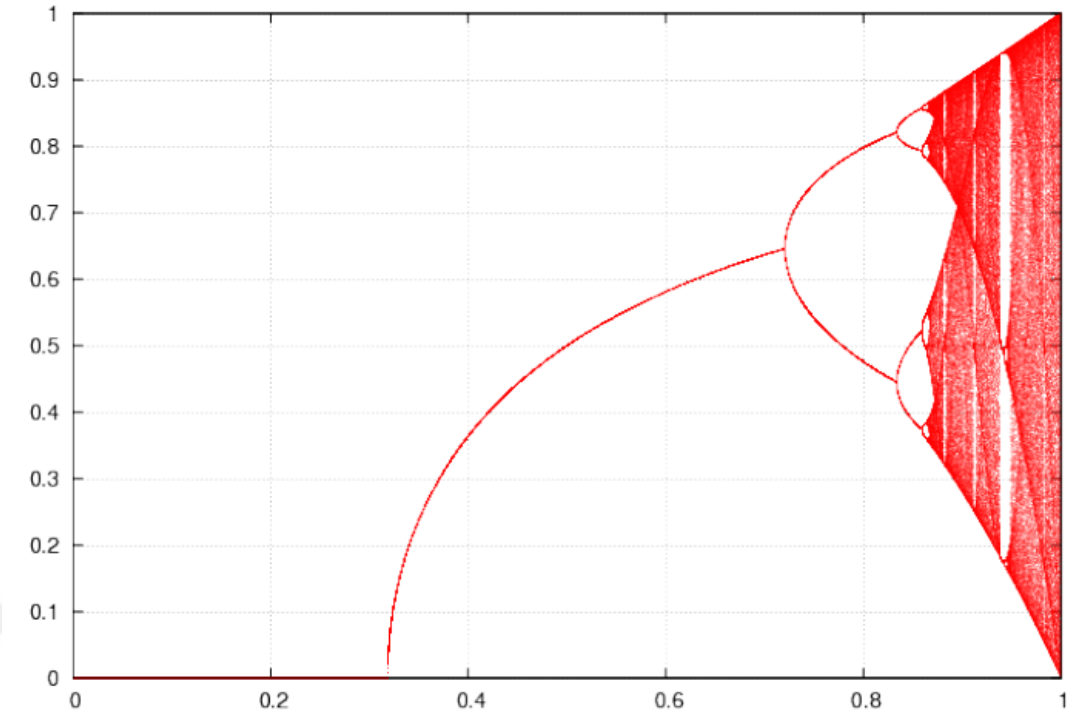
Şekil 7.4 Bernoulli haritasının çatallanma diyagramı

7.1.5 Sinüs harita

Sinüs haritası formül 7.5 teki gibi tanımlanır. Haritanın unimodal olması için X ∈ [0,1] aralığını kullanacağız

$$X_{n+1} = \mu \sin(\pi X_n) \qquad (7.5)$$

Sinüs haritası tek modelli ve maximum yakınında ikinci dereceden davranışa sahip olduğu için, lojistik haritaya benzer davranışlar gösterir. 0 sabit noktası $\mu < \frac{1}{\mu}$ için kararlı durumdadır.



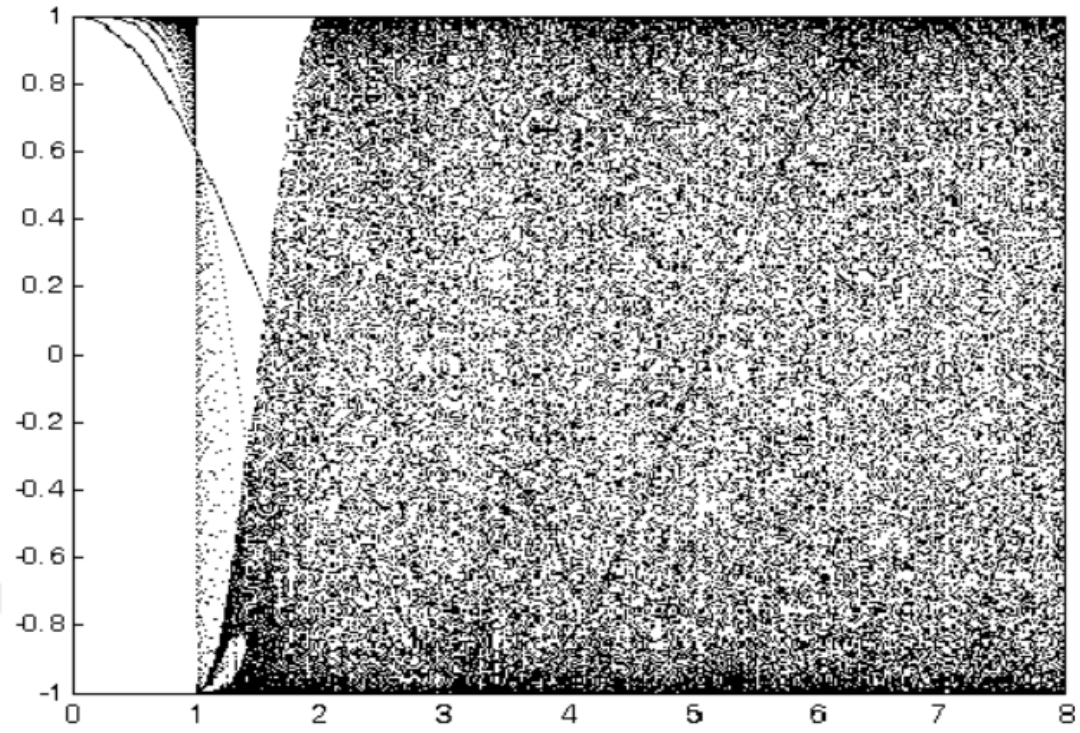
Şekil 7.5 10000 iterasyon için çatallanma diyagramı

7.1.6 Chebyshev harita

Chebyshev haritası formül 7.6 daki gibi verilebilir.

$$X_{n+1} = \cos(\mathrm{k} * \cos^{-1}(X_n)) \tag{7.6}$$

Burda $-1 \leq \mathrm{X} \leq 1$ ve k kontrol parametreleridir.



Şekil 7.6 Chebyshev haritasına ait örnek bir çatallanma diyagramı.

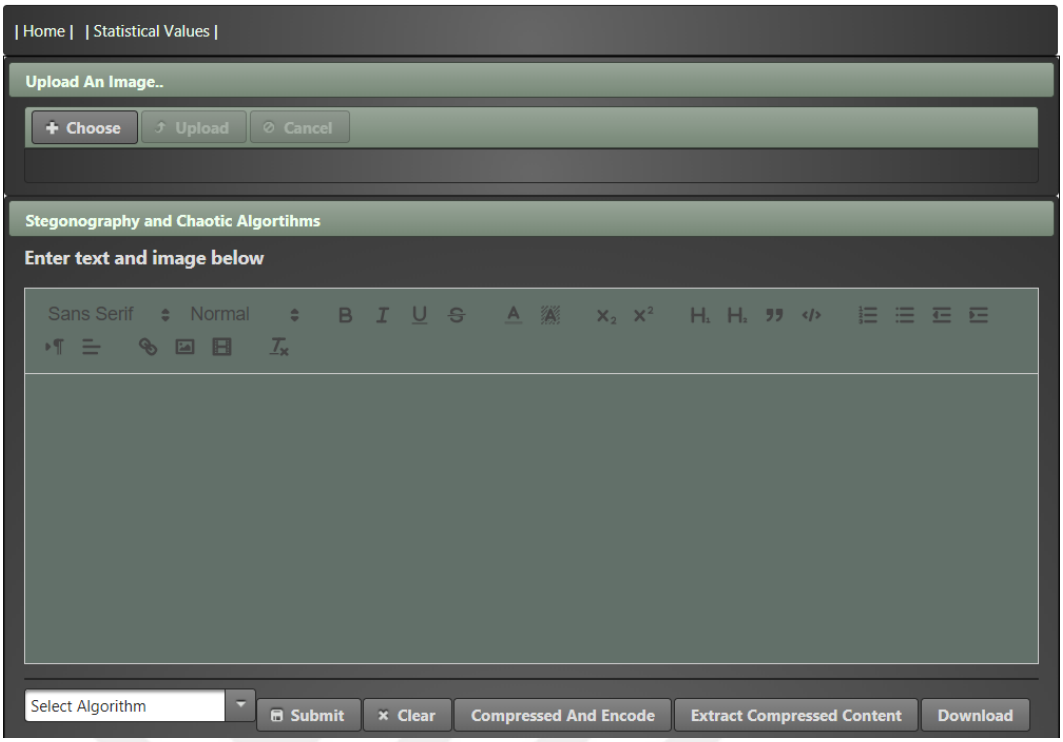
8. UYGULAMA

Uygulama Eclips IDE ve MySQL Administrator kullanılarak aşağıdaki teknolojiler yarımıyla geliştirildi.

- Spring Boot 1.5
- PrimeFaces 6.1
- JoinFaces 2.4
- Maven 3.5
- JSF
- JPA
- Hibernate
- MySQL
- Afterdark Tema

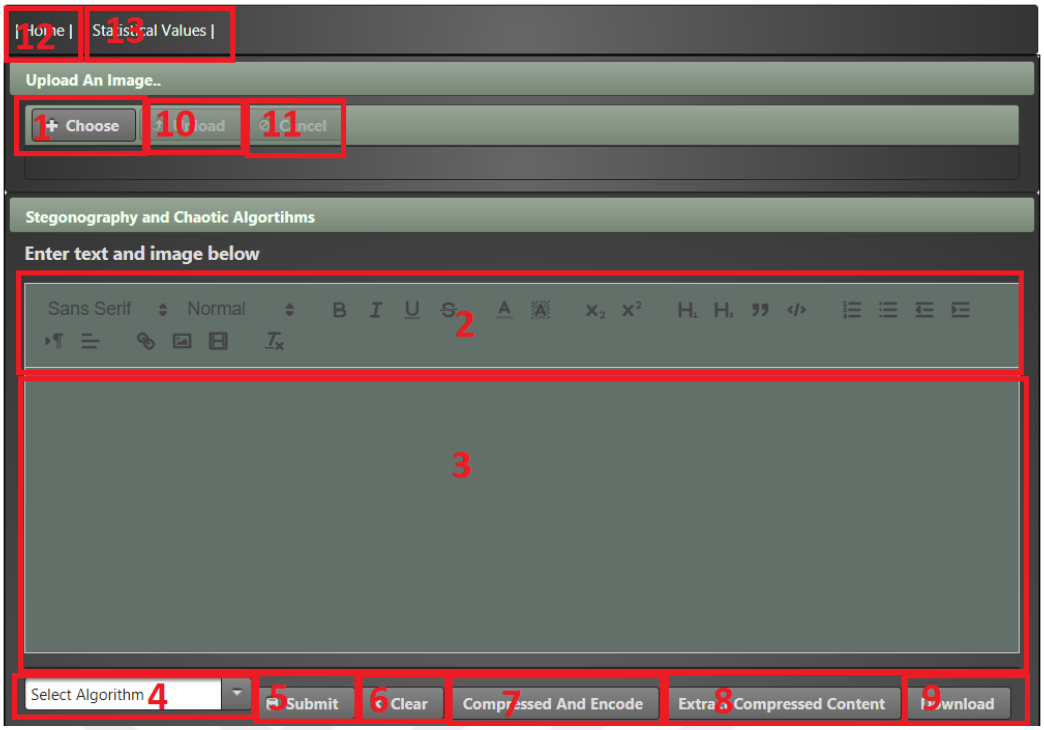
8.1 UYGULAMA ARAYÜZÜ

Uygulamayaarayüzünün ilk sayfası şekil 8.1 de verildiği gibidir.



Şekil 8.1 uygulama arayüzü home sekmesi.

Uygulama arayüzünü anlatabilmek için ilgili yerler numaralandırılarak aşağıdaki gibi verilmiştir.



Şekil 8.2 Numaralnadırılmış uygulama arayüzü

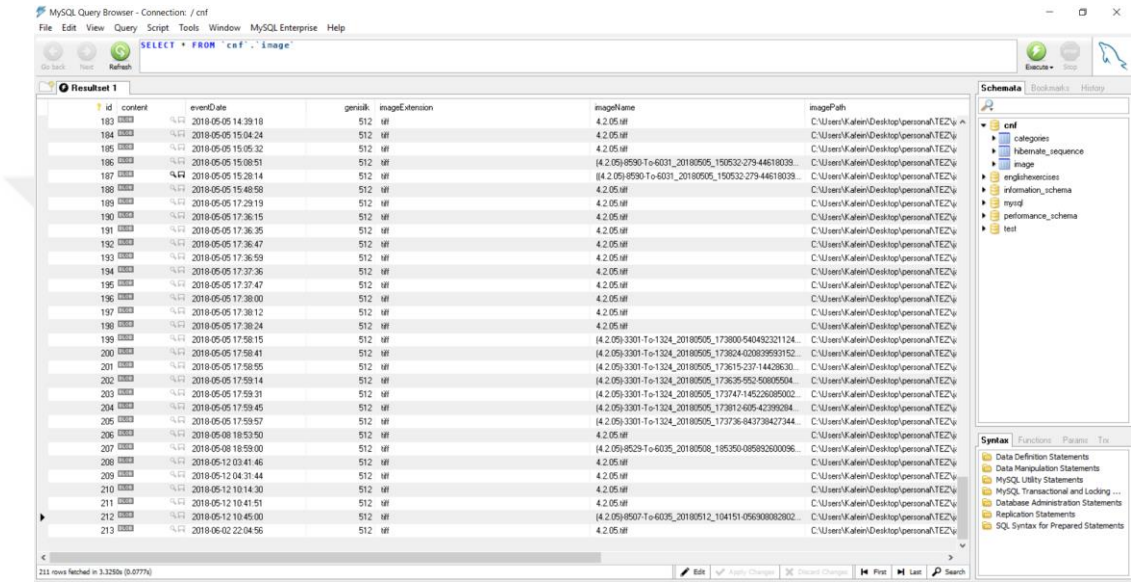
8.1.1 Chose butonu (1)

Bu buton yardımıyla taşıyıcı olarak kullanılacak resim seçilir. Ayrıca istenilirse resim fare yardımıyla seçilip komponentin üstüne bırakılarak da aynı işlem gerçekleştirilebilir. Uygulamanın örnek bir resim seçilmiş hali şekil 8.3 te verilmiştir.

Şekil 8.3 Uygulamada örnek bir resim seçilmiş ekran görüntüsü

8.1.2 Upload butonu (10)

Bu buton yardımıyla seçilmiş olan resim sisteme yüklenir. Sisteme Yüklenen resimler aynı zamanda veri tabanında şekil 8.4'teki gibi tutolmaktadır.



Şekil 8.4 Sisteme yüklenen resimlere ait veri tabanı görüntüsü

Ekleme işleminin başarılı bir şekilde tamamlandığına dair kullanıcıyı billgilndirmek amaçlı şekil 8.5 teki gibi ekrana bir mesaj verilir.

Şekil 8.5 taşıyıcı resmin başarılı yüklenmesine ait bilgilendirme mesajı.

8.1.3 Cancel butonu (11)

Yüklenmek üzere seçilmiş resmin sisteme yüklenmesini iptal etmek için kullanılır. Aynı zamanda şekil 8.3 teki "X" butonuna basmakla da bu işlem gerçekleştirilebilir.

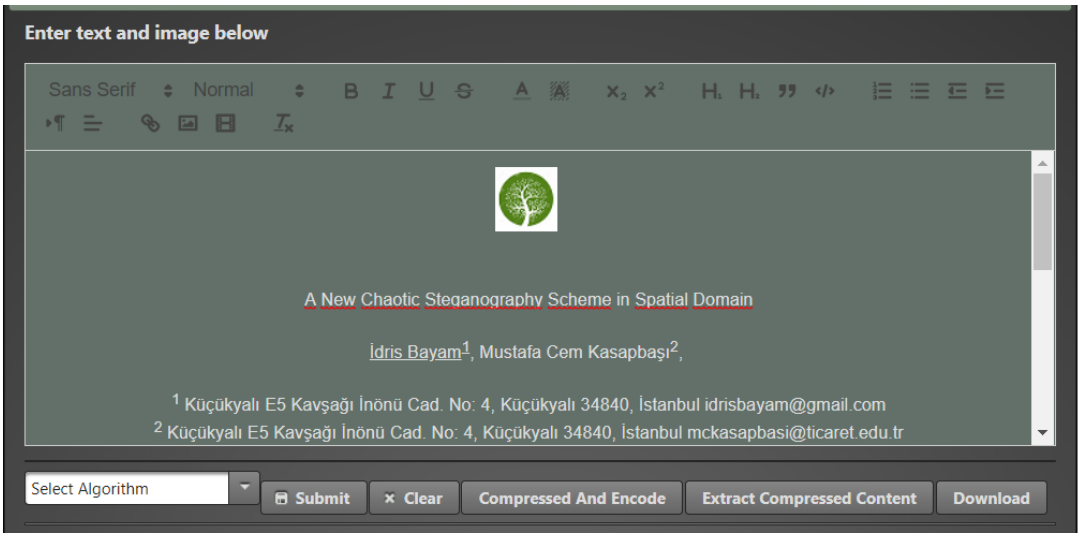
8.1.4 Text editörüm menüsü (2)

Editör, zengin metin düzenleme yeteneklerine sahip bir giriş bileşenidir. Bu alan yardımıyla girişi yapılan metnin still ve font ayarları, sol/sağ hizalama gibi temel işlevlerinin yanı sıra video link ve resim içeriklerinin seçilerek biçimlendirilmesi sağlanır.

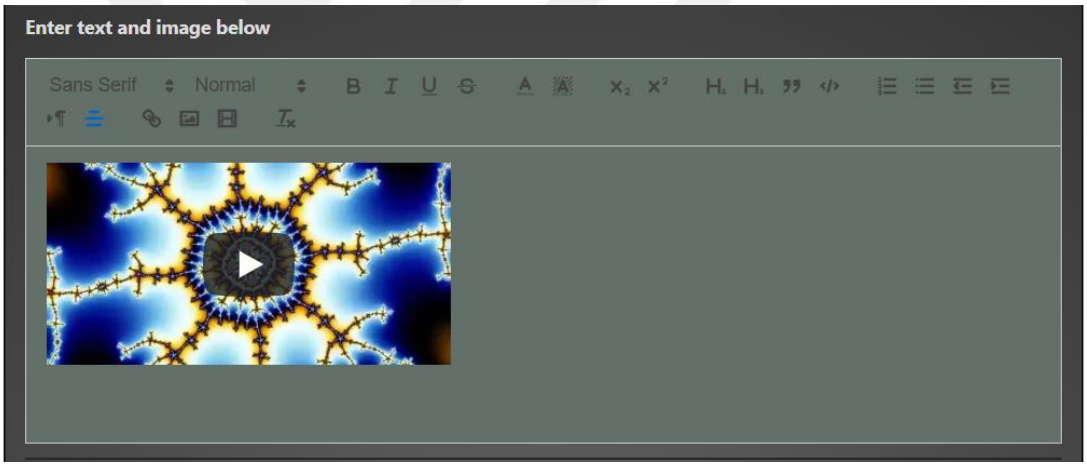
Bu alanda yazılanlar taşıyıcı resmin içine gömülecek gizli mesajımızı oluşturur.

8.1.5 Text editör mesaj alanı (3)

Gizli mesajın yazıldığı alandır. Şekil 8.6 ve 8.7 de görüldüğü gibi zengin metin içerikler gizli mesaj olarak eklenebilir.



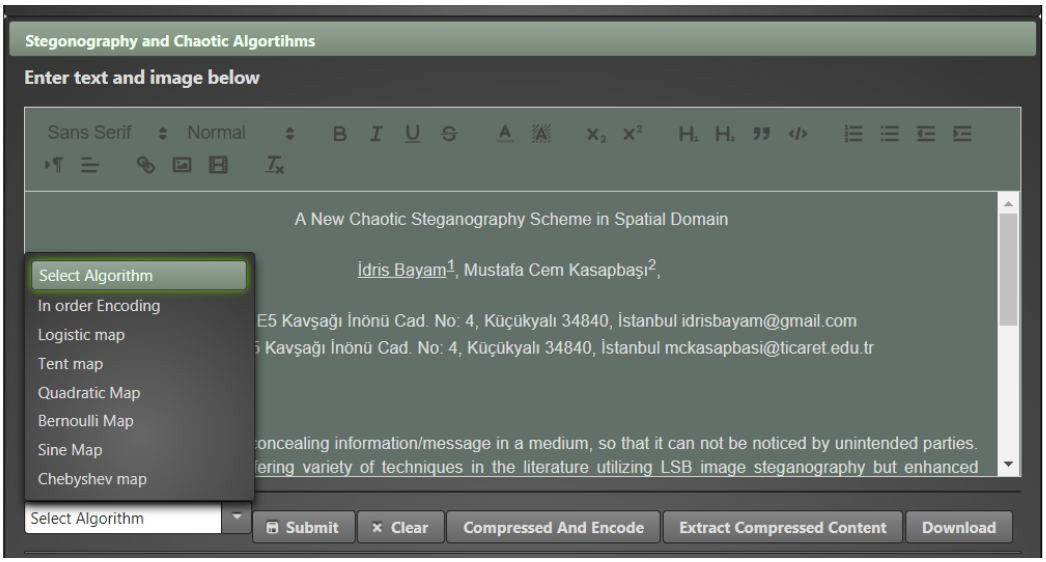
Şekil 8.6 Formatlı zengin metin ve resim içeren mesaj



Şekil 8.7 Gömülü video içeren içerik

8.1.6 Gömme işleminde kullanılacak algoritma seçimi (4)

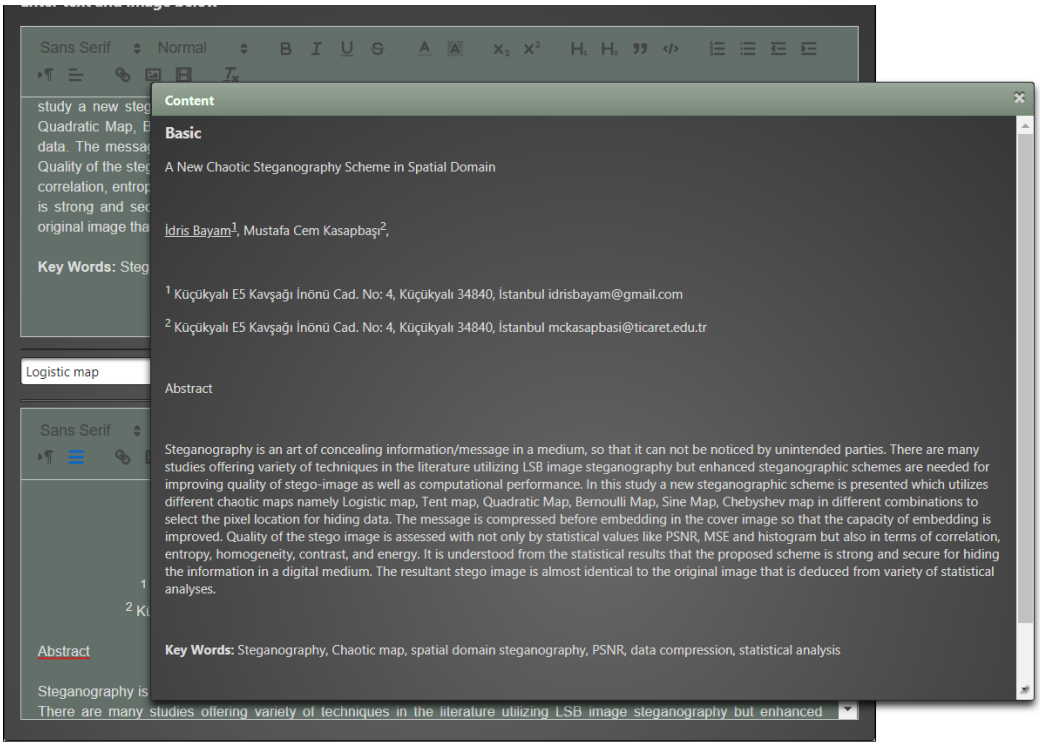
Gömme işlemi sırasında pixel seçimi için kullanılacak algoritma girişi için kullanılır. Şekil 8.8'den görüllldüğü gibi menüden ilgili algoritma seçilerek giriş algoritması belirlenmiş olur.



Şekil 8.8 Pixel Seçim algoritmaları

8.1.7 Submit butonu (5)

Submit butonu , gömülmüş veri çıkartılırken tam ekran haline getirmek için kullanılır. Şekild 8.9 da görüldüğü üzere yeniden boyutlandırılabilin bir pop up alanı açılarak kullanıcının daha rahat bir şekilde sonuç metninin görmesi sağlandı.



Şekil 8.9 Submit butonu ile sonuç metninin gösterilmesi.

8.1.8 Clear butonu (6)

Bu buton yardımıyla text editör mesaj alanına yazılmış içerik temizlenir. Böylece bir sonraki mesaj için kullanıcı arayüzünün hazır hale getirilmiş olur.

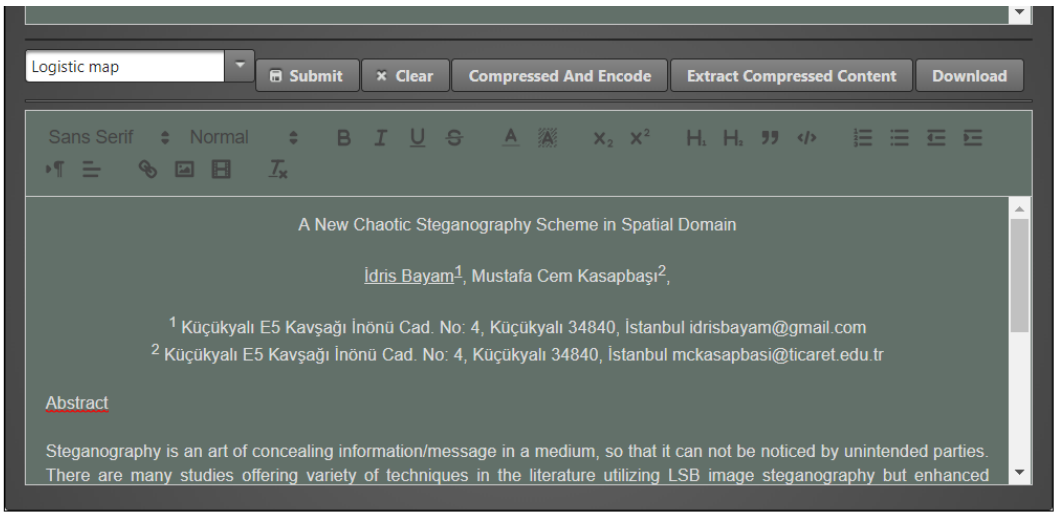
8.1.9 Compressed and encode butonu (7)

Bu botun yardımıyla text editör mesaj alanındaki içerik önce ziplenerek sıkıştırılır. Daha sonra seçilmiş olan kaotik algoritmaya göre en az anlamlı bit yöntemi uygulanarak taşıyıcı resme saklanır. Şekil 8.10 da görüldüğü üzere “compressed message is encoded” uyarısıyla birlikte işlem bitiminde kullanıcı bilgilendirilir.

Şekil 8.10 Mesajın sıkıştırılıp taşıyıcı resme gömülme işlemi

8.1.10 Extract compressed content butonu(8)

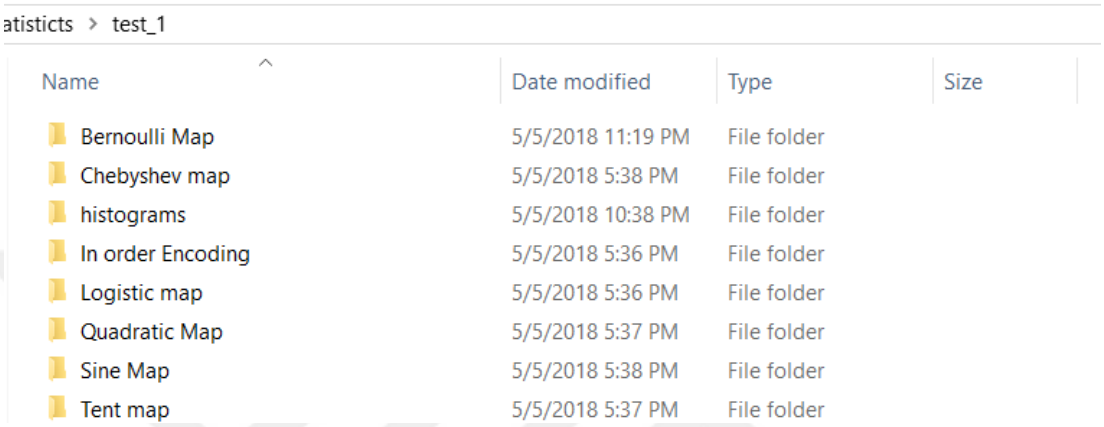
Resmin içine zipli şekilde gömülmüş veriyi çıkartarak önce zipten çıkartıp daha sonra ikinci text editörü mesaj alanına yazar. Şekil 8.11 de görüldüğü üzere ilgili içerik gömmede kullanılan kaotik algoritmanın seçilmesiyle birlikte elde ediliyor. Burda resim içine gömme işlemi yapılırken kullanılan başlangıç değerleri ve katsayılar aynı oduğu için gömme işleminin yapıldığı pikseller tespit edilebilir.



Şekil 8. 11 Taşıyıcı resimden elde edilmiş içerik

8.1.11 Download butonu(9)

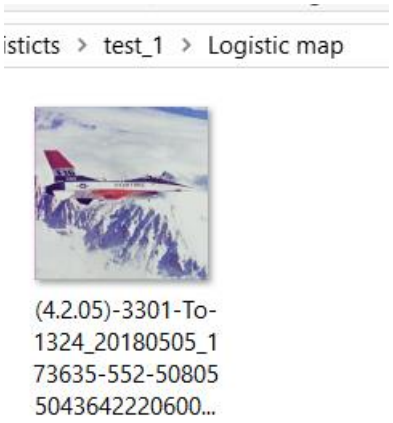
Download butonu kullanılarak içine veri saklanmış taşıyıcı resim indirilebilir. İndirilen taşıyıcı resimler şekil 8.12 deki gibi bir dosya hiyarerşisi oluşturularak alt dosyalara ayrılır. Taşıyıcı dosya kaydedilirken, dosya adları seçilen ve kodlaması yapılan algoritmaya göre belirlenir ve ilgili klasörün altına atılır.



Şekil 8.0.12 Sistemden indirilen dosyalara ait klasör hiyerarşisi

İndirilen resimin adlandırılması yapılan işleme ait ipuçları içerekecek şekilde yapıldı. Örnek bir adlandırmayı şekil 8.13 te görebilirsiniz. (4.2.05)-3301-To-1324_20180505_173635-552-5080550436422206001.tiff

Taşıyıcının adlandırılmasına yakından baktığımızda tablo 8.1 deki gibi kısımların olduğu görülecektir.



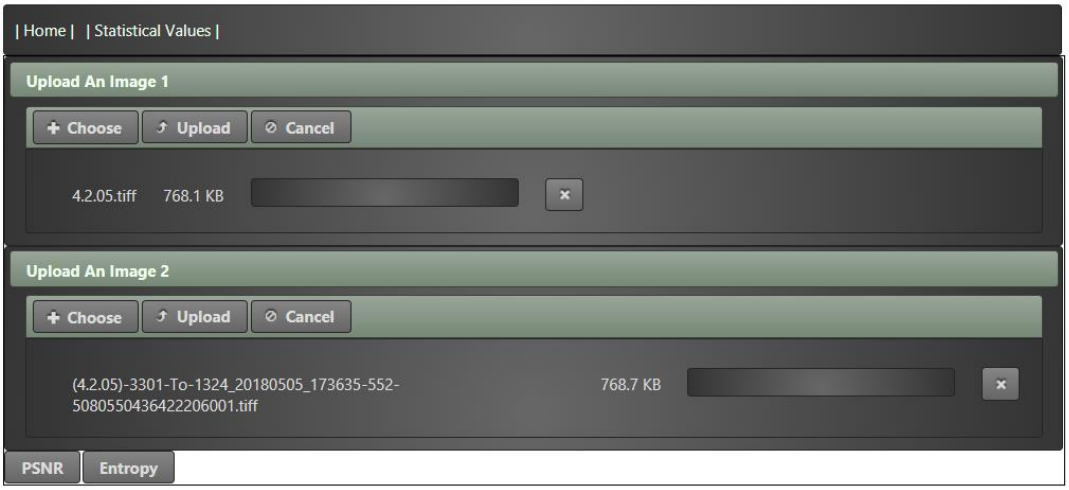
Şekil 8.13 Taşıyıcı resmin adlandırılması işlemi

AÇIKLAMA	DEĞER
Orijinal resmin adı	(4.2.05)
Orijinal mesajınuzunluğu	3301
Mesajın sıkıştırılmış uzunluğu	1324
İşlem tarihi	20180505
İşlem zamanı(milisaniye)	173635-552
Random sayı	5080550436422206001
Resim uzantısı	Tiff

Tablo 8.1 Taşıyıcı resmin isimlendirlmesi

8.1.12 Statistical value menüsü

Elde edilen taşıyıcı resimlerin orijinal resimlerle karşılaştırılması için şekil 8.14 teki gibi bir arayüz kullanılmıştır. Bu arayüzden 2 adet resim seçilerek entropy, MSE ve PSNR değerleri elde edilebilir. Diğer istatiksel karşılaştırmalar için R programlama ve Adobe Photoshop kullanılmıştır.



Şekil 8.14 Statistical Values menüsü ve değerlerin elde edilmesi

9. İSTATİSTİKSEL METRİKLER

9.1 Mean Squared Error (MSE)

İstatistikte, bir kestiricinin (gözlemlenmemiş bir miktarı tahmin etmek için bir prosedürün) ortalama kareli hatası (MSE) veya ortalama kareli sapma (MSD), hataların veya sapmaların karelerinin ortalamasını ölçer – ki bu tahmin ediciler arasındaki farktır ve tahmin edilmektedir.

MSE, karesel hata kaybının veya kuadratik kayıpların beklenen değerine karşılık gelen bir risk fonksiyonudur. Fark, rassallık nedeniyle veya tahmincinin daha doğru bir tahminde bulunabilecek bilgileri hesaba katmadığından kaynaklanır. MSE, bir kestiricinin kalitesinin bir ölçüsüdür – her zaman negatif değildir ve sıfıra daha yakın değerler daha iyidir.

MSE, hatanın ikinci anıdır (orijin etrafında) ve dolayısıyla hem kestiricinin varyansını hem de önyargılarını içerir. Bir tarafsız tahmincide MSE, tahmincinin varyansıdır. Varyans gibi, MSE de tahmin edilen miktarın karesi ile aynı ölçüm birimlerine sahiptir. Standart sapmaya analog olarak, MSE'nin karekökünü alarak, tahmin edilen miktarla aynı birimlere sahip olan kök-ortalama karesel hata veya kök-ortalama-karekök sapmasını (RMSE veya RMSD) verir; Tarafsız bir tahmincide RMSE, standart sapma olarak bilinen varyansın karekökü'dür.

$I_1(i,j)$ ve $I_2(i,j)$ gibi iki görüntü arasındaki ortalama karesel hata (MSE), bizim durumumuzdaki kapak resmi ve stego görüntüsü, formül 9.1 olarak verilmiştir.

$$MSE = \frac{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}[I_1(i,j)-I_2(i,j)]^2}{MxN} \quad (9.1)$$

Burada M ve N, kapak görüntüsünün satır ve sütunlarının sayısıdır.

9.2 Peak Signal to Noise Ratio (PSNR)

PSNR, gömme işleminden kaynaklanan stego görüntüsündeki bozulmanın bir ölçüsüdür ve logaritmik desibel (dB) cinsinden ifade edilir. PSNR değerini ölçmek için formül 9.2 kullanılır.

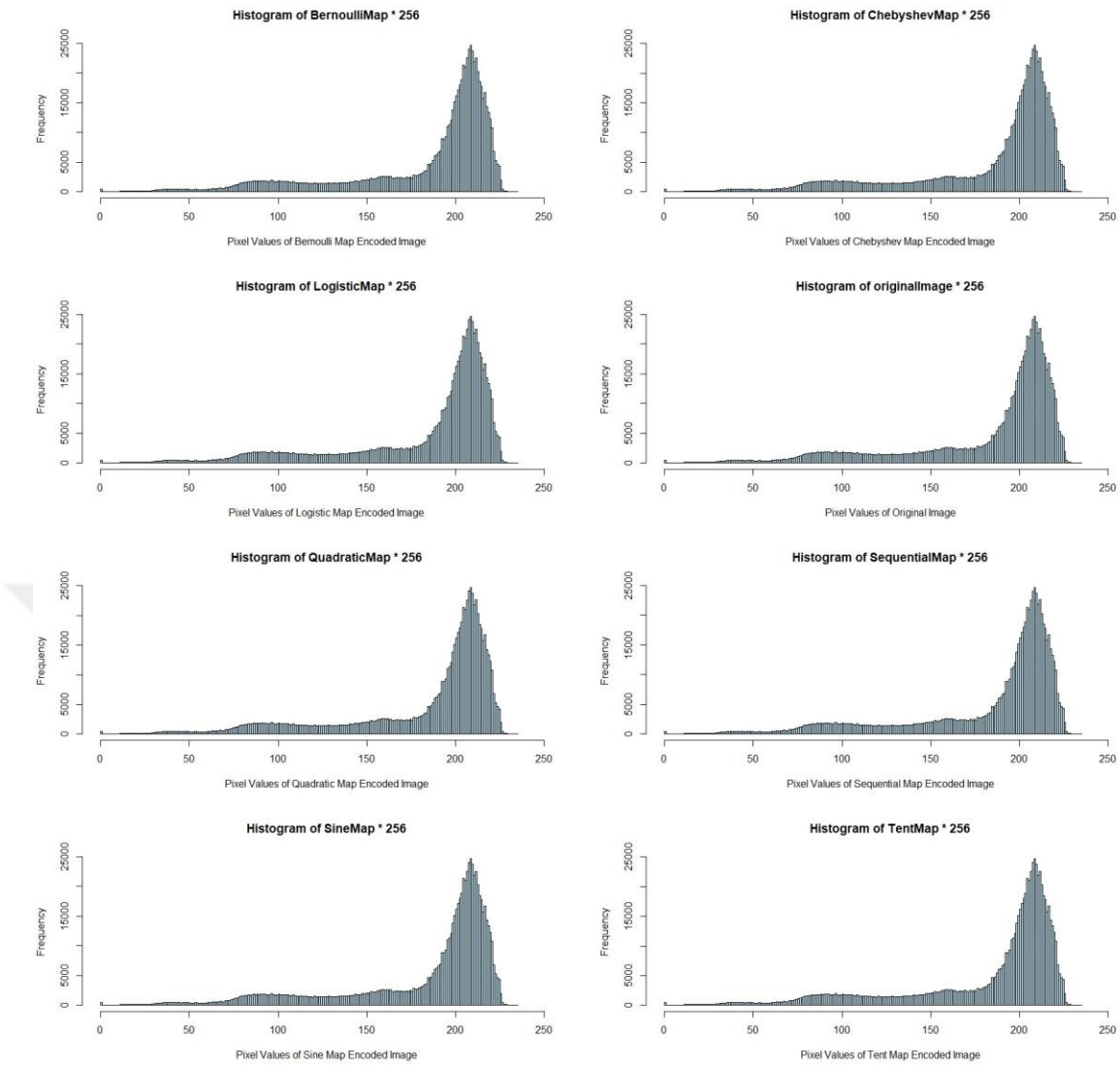
$$PSNR = 10 \log_{10} \frac{MAX^2}{MSE} \tag{9.2}$$

Burada MAX değeri, bir piksel 8 bit kullanılarak temsil edildiğinde (her bir kanal 8 bit olarak alınır), görüntünün maksimum olası piksel değeridir ki bu da 255 değerine karşılık gelir.

9.3 Histogram Analizi

Bir görüntü histogramı, bir görüntüdeki piksel yoğunluğu dağılımının grafiksel bir gösterimidir. Diğer bir ifadeyle tekrarlı sayılardan oluşan elimizdeki verileri, uygulanan işlemlerden sonra önce tabloya, tablodan yararlanarak grafiğe aktarılması yani veri gruplarının grafiğinin dikdörtgen sütunlar halinde gösterilmesine histogram denir. Resimler için histogram görüntünün renk yoğunluklarına göre piksel sayısındaki değişimi verir.

Saklanma tekniğinin başarılı kabul edilebilmesi için hem stego görüntünün hem de kapak görüntüsünün oldukça benzer histogramlara sahip olması gerekmektedir. Şekil 9.0.1 de görüleceği üzere orjinal resim ve taşyıcı resimlerin histogram grafikleri bir birine oldukça yakındır.



Şekil 9.1 Histogram gfrafiklerinin karşılaştırışması

9.4 Enerji

Enerji özelliği görüntüdeki homojenliğin bir ölçüsüdür. Tekdüzelik veya açısal ikinci moment olarak da bilinir. Sabit görüntüler için enerji 1'dir. Karşıtlık özelliği görüntüde bulunan yerel değişimlerin miktarını gösterir. Bir piksel ve komşusu arasındaki yoğunluk zıtlığıdır.

Her bir matris elemanının kare toplamı, görüntülerin gri tonlamalı dağılım homojenliğini ve doku sertliğini yansıtır. Tüm birlikte oluş matrisinin aynı değerleri, küçük enerji profilleri ile sonuçlanır. Birlikte meydana gelen matris değerleri arasındaki eşit olmayan değerler durumunda yüksek enerji beklenebilir. Enerji hesaplama denklemi formül 9.3 ile verilmiştir.

$$\mathrm{En}_{\mathrm{d,0}} = \sum_{\mathrm{i=1}} \sum_{\mathrm{j=1}} \mathrm{p}_{\mathrm{d,0}}(\mathrm{i,j})^2 \tag{9.3}$$

Burda $\mathrm{P}_{\mathrm{d,0}}(\mathrm{i,j})$; (i,j) konumundaki renk değerinin (normalize histogram) yoğunluğunun olasılığını ifade eder.

9.5 Kontrast

Resimlerin netliğini ve dokuların derinliğini yansıtır. Daha derin doku olukları yüksek kontrast ve daha iyi görsel netlik ile ilişkiliydi; Aksine, düşük kontrast, sığ oluklara ve bulanık resimlere yol açar. Sabit görüntülerde kontrast 0'dır. Gri tonlamada yüksek farklılığa sahip daha yüksek piksel sayısı daha yüksek kontrast değerleri ile ilişkilendirilir.

$$Constrast_{\mathrm{d,0}} = \sum_{\mathrm{i=1}} \sum_{j=1} (i-j)^2 \, \mathrm{p}_{\mathrm{d,0}}(i,j) \tag{9.4}$$

9.6 Homojenlik

Homojenlik özelliği GLCM'deki elemanların dağılımının diyagonal GLCM'deki elemanların dağılımına yakınlığının bir ölçüsüdür. Doku özellikleri analizi, resimlerde homojenliğin değerlendirilmesi için en önemli yaklaşımlardan biridir. Homojenlik formül 9.5 ile ifade idilir.

$$Homogeneity_{\mathrm{d,0}} = \sum_{\mathrm{i=1}} \sum_{j=1} \frac{p_{d,0}(i,j)}{1+|i-j|} \tag{9.5}$$

9.7 Korelasyon

Korelasyon görüntü dokusunun tutarlılığını yansıtır ve formül 9.6 ile ifade edilebilir.

Korelasyon özelliği görüntüdeki gri seviyesi lineer bağımlılıklarının bir ölçüsüdür. Bir piksel ve komşusunun birbiriyle nasıl ilişkili olduğunu gösterir. Korelasyon özelliği birbirleriyle tamamen pozitif ilişkili görüntülerde 1 ve tamamen negatif ilişkili görüntülerde ise -1'dir

$$Correalation_{d,0} = \sum_{i=1}\sum_{j=1} \frac{(i-u_x)(j-u_y)p_{d,0}(i,j)}{Q_x Q_y} \tag{9.6}$$

Formülde Q_X ve Q_y olasılık yoğunluk fonksiyonunu, $P_{d,0}(i,j)$ satırların ve sütunlarının ortalaması ve standart sapmasıdır.

9.8 Entropi

Entropi, görüntü dokusunun tekdüzeliği ve karmaşıklığını yansıtır ve formül 9.7 ile ifade edilir.

Entropi görüntüde bulunan gri seviyelerinin uzaysal düzensizliğinin düzeyini gösterir.

$$Entropy_{d,0} = -\sum_{i=1}\sum_{j=1} p_{d,0}(i,j)\log(p_{d,0}(i,j)) \tag{9.7}$$

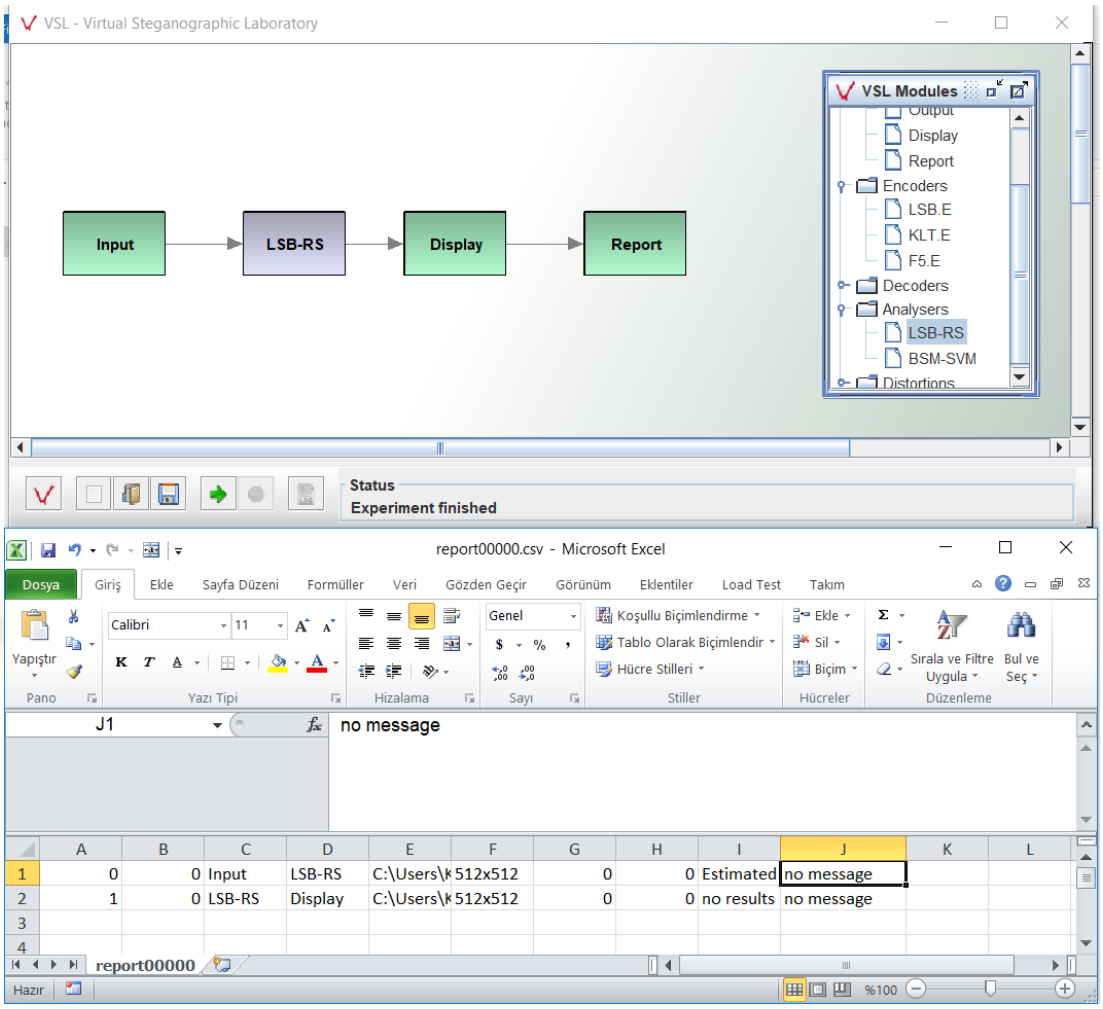
10. SONUÇ VE ÖNERİLER

Örnek değerler tablo 10.0.1 de verilmiştir. Bu değerlere bakıldığında PSNR değerinin 3.3K lık bir veri için 65 db üstünde olması sistemin başarlı sonuç ürettiğinin bir göstergesidir. Literatürde 40 db üstü sonuçlar başarılı kabul edilmektedir. Ayrıca korelasyon değerinin 1'e oldukça yakın olması taşıyıcı resim ve orijinal resim arasında yüksek bir ilşki olduğunu yani değişimin az olduğunu göstermektedir. Aynı ilişki entropi ve MSE değerleri incelendiğinde de görülmektedir.

3.3K byte	Bernoulli	Chebyshev	Logistic	Quadratic	Sine	Tent
Orjinal resmin entropisi	0.1565853749505	0.1565853749505	0.1565853749505	0.0202522277832	0.1565853749505	0.1565853749505
Taşıyıcı resmin entropisi	0.1565857788824	0.1565867290263	0.1565850577751	0.1565855630971	0.1565852400236	0.1565865214799
Entropi farkı	-0.00000040393196	-0.00000135407587	-0.00000135407587	-0.00000018814662	0.00000013492685	-0.00000114652948
Korelasyon	0.99999826637121	0.99999826406839	0.99999824765612	0.99999825685202	0.99999824634734	0.99999826669674
MSE	0.02014160156250	0.02016830444336	0.02035903930664	0.02025222778320	0.02037429809570	0.02013778686523
PSNR	65.08986360285750	65.08410972414460	65.04323080015980	65.06607557478410	65.03997704850430	65.09068620818610

Tablo 10.1: Kaotik yöntemlere ait istatistiksel metrikler.

LSB steganografi tespit etmek için en popüler algoritma Forczmanski ve Wegrzyn tarafından Digital Resimler için Sanal Steganografi Laboratuvarı (VSL) adıyla geliştirilmiştir. Steganografi ve stegoanaliz için oldukça popüler araçlar sağlar. VSL'ye dahil olan LSB-RS algoritmasının, LSB steganografisini tespit etmek için en güçlü algoritma olduğu bilinmektedir. Bununla birlikte, bu çalışmada gösterilen yazılımla üretilen stego-görüntülere uygulandığında, VSL'nin, içlerinde steganografinin varlığını tespit edemediği görülmüştür. Bununla birlikte, bu çalışmada gösterilen yazılımla üretilen stego-görüntülere uygulandığında, VSL'nin, içlerinde steganografinin varlığını tespit edemediği bulunmuştur. Şekil 10.1, VSL'nin stego-görüntüleri analiz etmek için kullanılma şeklini göstermektedir.



Şekil 10.1 VSL ile stegoanaliz

Elde edilen sistemde verinin gömüleceği piksellerin tespitinde kaotik algoritmalar kullanıldığı için anahtar değerler bilinmeden üçüncü parti kişilerce gömülen verinin elde edilmesi neredeyse imkânsızdır.

Sistem daha kaotik hale getirilmek için seçilen kanal yine kullanılan kaotik harita yardımıyla belirlenebilir. Böylece hem pixel seçimi hem de RGB kanal seçimi olmak üzere çift katmanlı bir kaotik rassallık sağlanmış olur.

Piksel seçiminde Entropi değeri yüksek alanlardan ve keskin kenarların olduğu adalardan kaçınılarak stegoanaliz bakımında sistem daha da güçlendirilebilir.

Veri sıkıştırılırken bir AES şifreleme tekniğiyle şifrelenirse güvenlik için ekstra bir katman daha eklenmiş olur.

KAYNAKLAR

Ahsan, K. ve Kundur, D. 2002. Practical data hiding in TCP/IP. Proceedings of ACM Workshop on Multimedia Security.

Anderson, R.J. ve Petitcolas, F.A.P. 1998. On the limits of steganography. IEEE Journal on Selected Areas in Communication, 16(4):474-481.

Atoum, M.S. et al. 2011. A steganography method based on hiding secret data in MPEG/Audio layer III. International Journal of Computer Science and Network Security, 11(5):184-188.

Artz, D. 2001. Digital steganography: Hiding data within data. IEEE Internet Computing Journal, 5(3):75-80.

Bandyopadhyay, S.K. et al. 2008. A tutorial review on steganography. Proceedings of the International Conference on Contemporary Computing, 105-114.

Bellare, M. ve Rogaway, P. 1994. Entity authentication and key distribution. Lecture Notes in Computer Science, 773:232-249.

Bender, W. et al. 1996. Techniques for data hiding. IBM Systems Journal, 35(3):313-336.

Bogdanov, A., Khovratovich, D. ve Rechberger, C. 2011. Biclique cryptanalysis of the full AES, Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, 344-371.

Chandramouli, R., Kharrazi, M. ve Memon, N. 2004. Image steganography and steganalysis: Concepts and practice. Lecture Notes in Computer Science, 2939:204-211.

Cheddad, A., Condell, J., Curran, K. ve Mc Kevitt, P., 2010, Digital image steganography: Survey and analysis of current methods, Signal Processing, 90 (3), 727-752.

Conklin, A. et al. 2004. Principles of computer security. McGraw-Hill Technology Education.

Currie, D.L. ve Irvine, C.E. 1996. Surmounting the effects of lossy compression on steganography. Proceedings of the National Information System Security Conference, 194-201.

Çimen, C., Akleylek, S. ve Akyıldız, E., 2008, Şifrelerin matematiği: kriptografi, ODTÜ, p. 17-22.

Dunbar, B. 2002. A detailed look at steganographic techniques and the use in an opensystems environment. SANS Institute, Information Security Reading Room, 1-11.

Elboukhari, M., Azizi, M. ve Azizi, A. 2010. Quantum key distribution protocols: A survey. International Journal of Universal Computer Sciences, 1(2):59-67.

Fridrich, J. 1998(a). Image watermarking for tamper detection. Proceedings of the International Conference on Image Processing, 2:404-408.

Fridrich, J. 1998(b). Methods for detecting changes in digital images. Proceedings of the IEEE International Workshop on Intelligent Signal Processing and Communication Systems.

Fridrich, J. 1999. Methods for tamper detection in digital images. Proceedings of AMC Multimedia and Security Workshop, 26-30.

Fridrich, J. 2010. Steganography in digital media: Principles, algorithms and applications. Cambridge University Press.

Fridrich, J. ve Du, R. 1999. Secure steganographic methods for palette images. Lecture Notes in Computer Science, 1768:47-60.

Fridrich, J. ve Goljan, M. 1999. Protection of digital images using self-embedding. Proceedings of the Symposium on Content Security and Data Hiding in Digital Media.

Fridrich, J., Goljan, M. ve Du, R. 2001. Steganalysis based on JPEG compatibility. Special Issue on Theoretical and Practical Issues in Digital Watermarking and Data Hiding, SPIE Multimedia Systems and Applications, 275-280.

Fridrich, J., Soukal, D. ve Goljan, M. 2005. Maximum likelihood estimation of length of secret message embedded using PMK steganography in spatial domain. Proceedings of IST/SPIE Electronic Imaging: Security, Steganography and Watermarking of Multimedia Contents, 5681:595-606.

Gilbert, H. ve Peyrin, T. 2010. Super-Sbox cryptanalysis: Improved attacks for AES-like permutations, Proceedings of the International Workshop on Fast Software Encryption, 365- 383.

Gisin, N. et al. 2002. Quantum cryptography. Reviews of Modern Physics, 74:145-196.

Gollmann, D. 1999. Computer security. John Wiley ve Sons Publishers.

Handel, T. ve Sandford, M. 1996. Hiding data in the OSI network model. Lecture Notes in Computer Science, 1174:23-38.

Jamil, T. 1999. Steganography: The art of hiding information in plain sight. IEEE Potentials, 18(1):10-12.

Johnson, N.F., Duric, Z. ve Jajodia, S. 2001. Information hiding: Steganography and watermarking - attacks and countermeasures. Kluwer Academic Publishers.

Johnson, N.F. ve Jajodia, S. 1998(a). Steganalysis of images created using current steganography software. Lecture Notes in Computer Science, 1525:273-289.

Johnson, N.F. ve Jajodia, S. 1998(b). Exploring steganography: Seeing the unseen. IEEE Computer Journal, 31(2):26-35.

Johnson, N.F. ve Jajodia, S. 1998(c). Steganalysis: The investigation of hidden information. Proceedings of the IEEE Information Technology Conference, 113-116.

Katzenbeisser, S. ve Petitcolas, F.A.P. 1999. Information hiding techniques for steganography and digital watermarking. Artech House Books.

Khalili, A., Katz, J. ve Arbaugh, W.A. 2003. Toward secure key distribution in truly ad-hoc networks. Proceedings of the Applications and the Internet Workshops, 342-346.

Kipper, G. 2003. Investigator's guide to steganography. Auerbach Publishers.

Kovacich, G. ve Jones, A. 2002. What infosec professionals should know about information warfare tactics by terrorists. Computers ve Security, 21(1):35-41 ve 21(2):113-119.

Krenn, R. 2004. Steganography and steganalysis. http://www.krenn.nl/univ/cry/steg/ article.pdf, last accessed on 2012-04-12.

Li, B. et al. 2011. A survey on image steganography and steganalysis. Journal of Information Hiding and Multimedia Signal Processing, 2(2):142-172.

Lou, D. ve Liu, J. 2002. Steganographic method for secure communication. Computer and Security, 21(5):449-460.

Marvel, L.M., Boncelet, C.G. ve Retter, C.T. 1999. Spread spectrum image steganography. IEEE Transactions on Image Processing, 8(8):1075-1083.

Mavrakis, N. 2003. Vulnerabilities of ISPs: an overall look. IEEE Potentials, October/ November:9-15.

Moerland, T. 2003. Steganography and steganalysis. Leiden Institute of Advanced Computing Science http://www.liacs.nl/home/tmoerl/privtech.pdf, last accessed on 2006-05- 01.

Murray, J.D. ve Van Ryper, W. 1996. Encyclopedia of graphics file formats. O'Reilly Publishers.

Owens, M. 2002. A discussion of covert channels and steganography. SANS Institute, Information Security Reading Room.

Papapanagiotou, K. et al. 2005. Alternatives for multimedia messaging system steganography. Lecture Notes in Computer Science, 3802:589-596.

Petitcolas, F.A.P., Anderson, R.J. ve Kuhn, M.G. 1999. Information hiding – A survey. Proceedings of the IEEE Special Issue on Protection of Multimedia Content, 87(7):1062- 1078.

Por, L.Y., Ang, T.F. ve Delina, B. 2008. WhiteSteg: A new scheme in information hiding using text steganography. WSEAS Journal of Transactions on Computers, 7(6):735-745.

Potdar, V.M., Han, S. ve Chang, E. 2005. Fingerprinted secret sharing steganography for robustness against image cropping attacks. Proceedings of the IEEE International Conference on Industrial Informatics, 717-724.

Provos, N. 2001. Defending against statistical steganalysis. Proceedings of the USENIX Security Symposium, 323-335.

Provos, N. ve Honeyman, P. 2001. Detecting steganographic content on the internet. Proceedings of the Internet Society Symposium on Network and Distributed System Security.

Rabah, K. 2004. Steganography – The art of hiding data. Information Technology Journal, 3(3):245-269.

Salomon, D. 2004. Data compression: The complete reference. Springer-Verlag Publishers.

Schneider, G.M. ve Gersting, J.L. 2004. Invitation to computer science. Course Technology.

Schneier, B. 1963. Secrets ve Lies: Digital Security in a Networked World. Wiley Computer Publishing.

Shirali-Shahreza, M. 2006. Stealth steganography in SMS. Proceedings of IFIP International Conference on Wireless and Optical Communications Networks.

Shirali-Shahreza, M. 2008. Text steganography by changing words spelling. Proceedings of the International Conference on Advanced Communication Technology, 3:1912-1913.

Shirali-Shahreza, M. ve Shirali-Shahreza, S. 2006. Collage steganography. Proceedings of the IEEE/ACIS International Conference on Computer and Information Science, 316-321.

Simmons, G.J. 1983. The prisoners' problem and the subliminal channel. Advances in Cryptology: Proceedings of CRYPTO, 51-67.

Ulutürk, A., 2010, Gelişmiş şifreleme standardı, Gazi Üniversitesi, Ankara, 4-7.

Venkatraman, S., Abraham, A. ve Paprzycki, M. 2004. Significance of steganography on data security. Proceedings of the International Conference on Information Technology: Coding and Computing, 2:347.

Wang, H. ve Wang, S. 2004. Cyber warfare: Steganography vs. steganalysis. Communications of the ACM, 47(10):76-82.

Wang, X. ve Yu, H. 2005. How to break MD5 and other hask functions, Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, 1-18.

Westfeld, A. 2001. F5 – A steganographic algorithm: High capacity despite better steganalysis. Lecture Notes in Computer Science, 2317:289-302.

Weiss, M. 2009. Principles of Steganography. http://www.math.ucsd.edu/~crypto/Projects/ MaxWeiss/steganography.pdf, last accessed on 2012-04-12.

Whitman, M.E. ve Mattord, H.M. 2003. Principles of information security, Thomson Course Technology Publishers.

Xi, L., Ping, X. ve Zhang, T. 2010. Improved LSB matching steganography resisting histogram attacks. Proceedings of the IEEE International Conference on Computer Science and Information Technology, 203-206.

ÖZGEÇMİŞ

Adı Soyadı : idris BAYAM

Doğum Yeri ve Yılı : ERUH, 20/08/1985

Medeni Hali : Bekar

Yabancı Dili : İngilizce

E-posta : idris.bayam@iticu.edu.tr

Eğitim Durumu

Lise : Siirt Atatürk Anadolu Lisesi, 2005

Lisans :Karadeniz Teknik Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü

Yüksek Lisans :İstanbul Ticaret Üniversitesi, Fen Bilimleri Enstitüsü 2012-

Yayınları

Bayam, İ., Kasapbaşı, M.C, 2018. A New Chaotic Steganography Scheme in Spatial Domain. 4th International Conference on Advances in Statistics, May 11-13, 2018, St. petersburg, Russia