T.C.
İSTANBUL AYDIN ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

WEB GÜVENLİK DAHİLİNDE STEGANOGRAFİ KULLANIMI VE KULLANICI GİRİŞ SİSTEMİNDE UYGULANMASI

YÜKSEK LİSANS TEZİ

Toghrul VALIBAYLI

Bilgisayar Mühendisliği Ana Bilim Dalı

Bilgisayar Mühendisliği Programı

MART 2020

T.C.
İSTANBUL AYDIN ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

WEB GÜVENLİK DAHİLİNDE STEGANOGRAFİ KULLANIMI VE KULLANICI GİRİŞ SİSTEMİNDE UYGULANMASI

YÜKSEK LİSANS TEZİ

Toghrul VALIBAYLI

(Y1613.010028)

Bilgisayar Mühendisliği Ana Bilim Dalı

Bilgisayar Mühendisliği Programı

Tez Danışmanı: Dr. Öğr. Üyesi AHMET GÜRHANLI

MART 2020

T.C.
İSTANBUL AYDIN ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ MÜDÜRLÜĞÜ

YÜKSEK LİSANS TEZ ONAY FORMU

Bilgisayar Mühendisliği Anabilim Dalı Bilgisayar Mühendisliği Tezli Yüksek Lisans Programı Y1613.010028 numaralı öğrencisi TOGHRUL VALIBAYLI'nin "**WEB GÜVENLİK DAHİLİNDE STEGANOGRAFİ KULLANIMI VE KULLANICI GİRİŞ SİSTEMİNDE UYGULANMASI**" adlı tez çalışması Enstitümüz Yönetim Kurulunun 24.02.2020 tarihli ve 2020/03 sayılı kararıyla oluşturulan jüri tarafından oybirliği/oyçokluğu ile Tezli Yüksek Lisans tezi 12.03.2020 tarihinde kabul edilmiştir.

	Unvan	Adı Soyadı	Üniversite	İmza
		ASIL ÜYELER		
Danışman	Dr. Öğr. Üyesi	Ahmet GÜRHANLI	İstanbul Aydın Üniversitesi	
1. Üye	Prof. Dr.	Ali GÜNEŞ	İstanbul Aydın Üniversitesi	
2. Üye	Doç. Dr.	Zeynep ORMAN	İstanbul Üniversitesi-Cerrahpaşa	
		YEDEK ÜYELER		
1. Üye	Dr. Öğr. Üyesi	Adem ÖZYAVAŞ	İstanbul Aydın Üniversitesi	
2. Üye	Dr. Öğr. Üyesi	Ali HAMİTOĞLU	İstanbul Sabahattin Zaim Üniversitesi	

ONAY

Prof. Dr. Ragıp Kutay KARACA
Enstitü Müdürü

YEMİN METNİ

Yüksek lisans tezi olarak sunduğum "Web Güvenlik Dahilinde Steganografi Kullanımı ve Kullanıcı Giriş Sisteminde Uygulanması" adlı çalışmanın, tezin proje safhasından sonuçlanmasına kadarki bütün süreçlerde bilimsel ahlak ve geleneklere aykırı düşünecek bir yardıma başvurulmaksızın yazıldığını ve yararlandığım eserlerin Bibliyografya'da gösterilenlerden oluştuğunu, bunlara atıf yapılarak yararlanılmış olduğunu belirtir ve onurumla beyan ederim. (12/03/2020)

Toghrul VALIBAYLI

Tez çalışmalarımda her zaman yanımda olan, yardım eden arkadaşlarıma teşekkür ederim. Her zaman yanımda olan babama ve anneme Beni her zaman motive eden ve destekleyen sevgilime, desteklerinden dolayı teşekkür ederim.

ÖNSÖZ

Günümüzde internet hayatımızın ayrılmaz bir parçası haline gelmiştir. Çok büyük bir bilgi denizinin içinde bulunmuş durumdayız. Nerdeyse her gün kullandığımız bilgisayar ve telefonlarımızda bilgi almak, alış-veriş yapmak, dinlenmek ve s. gibi bir çok işlem yapıyoruz. Bu işlemlerin en temel noktalarından bir tanesi güvenliktir. Gerçek hayatta nasıl güvenliğimize dikkat ediyorsak artık sanal hayatta da güvenliğimize dikkat etmemiz gerekiyor.

Site sahibi ve geliştiriciler olarak kullanıcı güvenliği hep önceliğimiz olmuştur, dışarıdan gelen saldırılara karşı sistemimizi korumak, kullanıcı bilgilerini güvende tutmak için farklı teknolojiler kullanıyoruz. Bu tezde kullanıcı giriş sisteminin güvenliğini artırmak ve korumak için steganografi kulanımı gösterilmiştir. Ayrıca steganografi algoritmalarından sistem için en kullanışlı algoritma seçilmiştir.

Tez yazım süresi boyunca baştan sona kadar büyük bir sabırla bana gösterdikleri destek ve yardımlarından dolayı saygıdeğer hocam ve tez danışmanım olan Dr. Öğr. Üyesi Ahmet GÜRHANLI'ya teşekkür ederim. Sayın Gürhanlı'nın bilgi, tecrübe ve yönlendirmeleri çalışmanın yürütülmesinde son derece faydalı olmuştur.

Mart 2020 **Toghrul VALIBAYLI**

İÇİNDEKİLER

Sayfa

ŞEKİL LİSTESİ

Sayfa

WEB UYGULAMALARINDA GÜVENLİĞİN STENOGRAFİ KULLANILARAK GÜÇLENDİRİLMESİ

ÖZET

Steganografinin önemli amacı, gizli bilgiyi, yetkisi olmayan kişilerin görmesi durumunda, bilginin gizlendiği alan dahilinde bilginin saklandığına dair şüpheleri ortadan kaldırmaktır. Yani steganografinin hedefi, yetkisiz kişilerin saklı bilginin gizlendiğini öğrenmelerine engel olmaktır. Bir steganografi uygulaması, taşıyıcı ortamla ilgili şüpheler oluşturuyorsa, bu durumda yöntem başarılı şekilde sonlandırılamaz. Gizli mesajları ulaştıran kılıflar, dijital ortamda sık-sık kullanılan görüntüler, resimler, sesler veya metinler şeklinde olabilir (Agarwal, 2013:91). Gizlenen bilgi sade bir yazı, şifreli yazı ya da dijital ortamda gönderile bilen çeşitli dosyalar olabilir. Yapacağımız uygulamada giriş paneli üzerinden kimlik doğrulaması yaparken, yalnız kullanıcı ismi ve şifre değil, public resimler kullanarak sunucuya gönderilen verilerin seçilen resmin içine gömülmesi ve kullanıcı adı ve şifre ile yanaşı resmin ve resmin içindeki verinin doğrulanması 2 katı doğrulama yapacaktır. Steganografi kullanım amacının dış müdahelede sadece şifre ve resime müdahele etseler bile resmin içindeki veri doğru olmadığında ve zarar gördüğünde kimlik doğrulaması olmayacaktır. Gönderilen verinin gizli olması sonucunda nereye müdahele edeceği bilinmediği sürece sistem dışı müdahelelerden her hangi bir verim elde edemeyecekler.

Anahtar Kelimeler: *Stenografi, Web Güvenlik, Kriptografi, Web giriş, Şifre Gizleme.*

STRENGTHENING SECURITY BY USING STENOGRAPHY IN WEB APPLICATIONS

ABSTRACT

The main purpose of steganography is to eliminate doubts that information is stored within the area where information is hidden, if unauthorized people see it. So the goal of steganography is to prevent unauthorized people from learning that hidden information is hidden. If a steganography application raises doubts about the carrier environment, then the method cannot be successfully terminated. Cases that transmit secret messages can be in the form of frequently used images, pictures, sounds or text in digital media (Agarwal, 2013:91). The hidden information can be plain text, encrypted text or various files that can be sent digitally. While authenticating through the input panel in the application we will do, it will be double verification of embedding data sent to the server using public pictures, not the user name and password, and verifying the data with the user name and password. Even if the purpose of steganography usage is only to interfere with the password and the picture in external intervention, there will be no authentication when the data in the picture is not correct and damaged. As long as it is not known where to intervene as a result of the confidential data sent, they will not be able to obtain any efficiency from non-system interventions.

Keywords: *Stenography, Web Security, Cryptography, Web Login, Password Hiding.*

1. GİRİŞ

Yetkisiz erişime karşı bilgiyi koruma görevi her zaman önemli bir konu olmuştur. Eski dönemlerden bu yönde bugün de hala sürdürülen iki ana yön bulunmaktadır: kriptografi ve steganografi. Kriptografinin amacı, mesajların içeriğini şifreleyerek gizlemektir. Buna karşılık, steganografi bir mesajın varlığını gizler (Kumar vd., 2014:31).

"Steganografi" kelimesi Yunanca bir kelimedir ve kelime "gizli yazı" anlamına gelir. II. Dünya Savaşı sırasında, ABD hükümeti gizli bilgi aktarma yöntemleriyle mücadeleye büyük önem verdi. Posta ile ilgili bazı kısıtlamalar getirildi. Son yıllarda bilgisayar teknolojisinin gelişimi, bilgisayar steganografisinin gelişimine yeni bir ivme kazandırdı (Garg, 2011:129). Bu yönde yeni uygulama alanları geliştirildi. Mesajlar artık bir kural olarak analog nitelikteki dijital verilere gömülüdür. Bunlar konuşma, ses kayıtları, resimler ve videolardır.

Steganografinin önemli amacı, gizli bilgiyi, yetkisi olmayan kişilerin görmesi durumunda, bilginin gizlendiği alan dahilinde bilginin saklandığına dair şüpheleri ortadan kaldırmaktır. Yani steganografinin hedefi, yetkisiz kişilerin saklı bilginin gizlendiğini öğrenmelerine engel olmaktır. Bir steganografi uygulaması, taşıyıcı ortamla ilgili şüpheler oluşturuyorsa, bu durumda yöntem başarılı şekilde sonlandırılamaz. Gizli mesajları ulaştıran kılıflar, dijital ortamda sık-sık kullanılan görüntüler, resimler, sesler veya metinler şeklinde olabilir (Agarwal, 2013:91). Gizlenen bilgi sade bir yazı, şifreli yazı ya da dijital ortamda gönderile bilen çeşitli dosyalar olabilir.

Steganografinin farklı bir şekli, filigran yaratma olduğu belirtilmektedir ve ticari ortamda geliştirilerek kullanılmaktadır. Filigran oluşturmada taşıyıcı alan dikkat çekmeyecek şekilde değiştirilerek küçük hacimli bir bilgi saklanılır. Filigran oluşturma esasen, telif hakkı bulunan web sayfaları veya ses dosyaları şeklinde dijital alanların korunmasında kullanılmaktadır. Filigran oluşturma ve steganografi arasındaki tek fark, Filigran oluşturmada kılıf, haberleşme yönündeyse steganografide, saklanan mesaj haberleşme yönündedir (Agarwal, 2013:93).

İnternet yaygınlaştıkça ve yeni alanlar keşfedildikçe insanların web sitelerine ilgisi artmıştır. Bu ilgi, 2000'li yıllardan sonra daha çok arttığından web sitelerinin sayısı da sürekli olarak artmıştır. Bunun yanı sıra, web sitelerinde bulunan kullanıcı bilgilerini çalmak veya sitenin kapanması için sürekli saldırılar düzenleyen insanlar ve gruplar da çoğalmaya başlamıştır. Günümüzde de internet insanların vazgeçilmezi olduğu için ve gündelik hayatlarında kullandıkları için güvenlik konusu da dikkate alınmaya başlandı. Çeşitli şifreleme algoritmaları ve başka uygulamalar kullanılarak güvenliğin sağlanması yanı sıra, veri aktarımında da güvenlik protokollerinin uygulanması zorunlu hale gelmiştir. Bu tezde uygulanacak Steganografi yöntemi ile kimlik doğrulama ve olası veri çalma olaylarına karşı steganografinin yöntemlerinden bahsedilecektir. Bu araştırmada, bilgi saklama yöntemi olan steganografi kavramı, çalışma şekli, metotları ve modern dönemde kullanım alanları incelenmiştir. Çalışmanın amacı Web uygulamalarında güvenliğin Stenografi kullanılarak güçlendirilmesi yöntemlerinin belirlenmesidir. Bu yönde bir mesajı korumak ve şifrelemek için etkin ve güvenli bir uygulama tasarlamak amaçlanmaktadır.

Yapacağımız uygulamada giriş paneli üzerinden kimlik doğrulaması yaparken, yalnız kullanıcı ismi ve şifre değil, public resimler kullanarak sunucuya gönderilen verilerin seçilen resmin içine gömülmesi ve kullanıcı adı ve şifre ile yanaşı resmin ve resmin içindeki verinin doğrulanması 2 katı doğrulama yapacaktır. Steganografi kullanım amacının dış müdahelede sadece şifre ve resime müdahele etseler bile resmin içindeki veri doğru olmadığında ve zarar gördüğünde kimlik doğrulaması olmayacaktır. Gönderilen verinin gizli olması sonucunda nereye müdahele edeceği bilinmediği sürece sistem dışı müdahelelerden her hangi bir verim elde edemeyecekler.

Araştırmada ilk olarak Kriptografi ve Steganografi kavramları incelenecektir. Bu kavramların tarihi süreçte gelişimleri ile ilgili bilgiler verilecektir. Klasik ve yeni şifreleme çeşitleri incelenecektir. Daha sonra steganografinin kullanım alanları araştırılacaktır. Görüntü, metin, ses steganografi kavramları incelenecektir. Sonuncu bölümde geliştirilen uygulama ile ilgili bilgiler sunulacaktır.

2. LİTERATÜR TARAMASI

Prashanti ve Sandyarani (2015), LSB tabanlı görüntü steganografisinin son başarıları üzerine araştırma yapmışlardır. Bu ankette yazarlar, yüksek sağlamlık, yüksek yerleştirme kapasitesi ve gizli bilgilerin tespit edilememesi gibi steganografik sonuçları geliştiren gelişmeleri tartışmaktadır. Bu anketle birlikte iki yeni teknik de önerilmektedir. Birinci teknik, veri veya gizli mesajları kapak görüntüsüne gömmek için kullanılır ve ikinci teknikte gizli bir gri ölçekli görüntü başka bir gri ölçekli görüntüye gömülür. Bu teknikler sözde rasgele sayılar üreten dört durum tablosu kullanır. Bu, gizli bilgilerin gömülmesi için kullanılır. Bu iki yöntemin güvenliği daha yüksektir çünkü gizli bilgiler, tablo tarafından oluşturulan sözde rasgele sayılar yardımıyla görüntünün LSB'lerinin rasgele seçilen konumlarında gizlenir.

Savita Goel ve diğ. (2015) tarafında farklı mesajlar kullanarak LSB yöntemi kullanılarak gizli mesajların kapak görüntüsüne yerleştirilmesi için yeni bir yöntem önerilmiştir. Yazarlar, Pik Sinyal Gürültü Oranı (PSNR), Ortalama Kare Hatası (MSE), histogramlar ve CPU zamanı, Yapı Benzerliği (SSIM) endeksi ve Özellik Benzerliği gibi görüntü kalitesi parametrelerinin sayısını kullanarak stego görüntünün kalitesini kapak görüntüsüne göre karşılaştırırlar. Çalışma ve deneysel sonuçları, önerilen yöntemlerinin temel LSB yöntemlerine kıyasla hızlı ve yüksek verimli olduğunu göstermektedir.

Della Baby ve ark. (2015) "Steganografi kullanarak yeni DWT tabanlı Görüntü Koruma yöntemi" önermişlerdir. Çalışmalarında, DWT steganografik tekniği kullanılarak birden fazla RGB görüntüsünün tek RGB görüntüsüne gömüldüğü yeni steganografi tekniği incelenir. Kapak resmi 3 renge ayrılmıştır, yani Kırmızı, Yeşil ve Mavi renk alanı. Bu üç renk alanı gizli bilgileri gizlemek için kullanılır. Bu sistem kullanılarak elde edilen deneysel sonuçlar iyi bir sağlamlığa sahiptir. PSNR ve SSIM indeksinin değeri yazarlar tarafından stego ve orijinal kapak imajlarının kalitesini karşılaştırmak için kullanılmıştır. Önerilen yöntem iyi düzeyde PSNR ve SSIM indeks değerlerine sahiptir. Yazarlar deneysel sonuçlarının mevcut yaklaşımlardan daha iyi olduğunu ve veri sıkıştırması nedeniyle gömme kapasitesinin arttığını bulmuşlardır.

Dolayısıyla yaklaşımlarının genel güvenliği yüksektir ve stego imgesindeki algılanabilir değişiklikler daha azdır.

Bingwen Feng, Wei Lu ve Wei Sun, "Dokudaki Bozulmayı En Aza İndirmeye Dayalı Güvenli İkili Görüntü Steganografisi" (2015) makalesinde ikili görüntü steganografisinin son teknoloji yaklaşımını önermişlerdir. Bu teknik doku üzerindeki bozulmayı en aza indirmek için önerilmektedir. Bu steganografi yönteminde, ilk olarak, dönme, tamamlayıcı ve yansıtma değişmez doku desenleri ikili görüntüden çıkarılır. Ayrıca bir ölçüm önerdiler ve bu önerilen ölçüme dayanarak bu yaklaşım pratik olarak uygulanmaktadır. Pratik sonuçlar, önerilen steganografik yaklaşımın yüksek stego görüntü kalitesi ve yüksek gömme kapasitesi ile yüksek istatistiksel güvenliğe sahip olduğunu göstermektedir.

Nusrati ve diğ. (2015), bir kapak görüntüsünde gizli bilgileri gizlemek için sezgisel genetik algoritmaya dayalı steganografik yöntem üzerinde çalışmışlardır. Bu yöntem, "gizleme tekniklerini gömmeden önce" odaklanarak gizli bilgileri gömmek için kapak görüntüsünde uygun konumları en uygun şekilde bulur. Görüntü histogramında minimum değişikliklere yol açan bitlerde en az değişiklik yapmaya çalışır. LSB'leri ve gizli mesajı blok kümesine gizlemek için, bu genetik algoritmada segmentasyon yapılır. Bu algoritma katıştırma için uygun yerleri bulduktan sonra, gizli bloklar katıştırılır ve mesaj çıkarma işlemi sırasında kullanılan anahtar dosyasını oluşturur. Deneysel sonuçlar, bu genetik tabanlı yöntemin, yüksek stego görüntü kalitesine sahip temel LSB algoritmasından daha verimli olduğunu göstermektedir.

Kazem Qazanfari ve Reza Safabakhsh (2014) LSB ++ yaklaşımının geliştirilmiş bir versiyonunu önerdiler. Bu gelişmiş LSB ++ ile hassas pikseller arasında ayrım yaparlar ve ekstra bitlerin gömülmesine karşı koruma sağlarlar, bu da eşzamanlılık matrislerinde daha az bozulmaya neden olur. Ayrıca JPEG biçimindeki görüntülerin DCT katsayılarını korumak için bu yöntemi genişletirler. Bu geliştirilmiş yöntem, birlikte yaşlanma matrislerinde eski LSB ++ tekniğinden daha az iz bırakmaktadır. Bu yöntem histogram tabanlı saldırılara karşı da güvenlidir, çünkü bu yöntem histogramda herhangi bir değişiklik yapmaz ve bu nedenle hem kapak görüntüsünün hem de stego görüntüsünün histogramları aynı olacaktır. Ekstra bit gömülmesinin ortadan kaldırılması nedeniyle stego görüntülerinin kalitesi de yüksektir.

Huffman Kodlamasına dayanarak, Amitava Nag ve ark. (2014) LSB ikamesinin yeni bir steganografik tekniğini sunar. Teknikleri temel olarak yüksek güvenlik, daha büyük yerleştirme kapasitesi ve kabul edilebilir stego görüntü kalitesi düzeyine odaklanmaktadır. Öncelikle Huffman ağacı, her 8 bitlik gizli görüntüyü kodlamak için üretilir. Kodlamadan sonra, kodlanan bitleri dört parçaya bölerler ve 0 ila 3 ondalık değere sahiptirler. Bir iletinin kapak görüntüsüne gömülmesinin konumu, bu ondalık değerlerle belirlenir. Deneysel sonuçlar, Huffman tablosu kapak görüntüsünün boyutunu azalttığı için saldırganın gizli bilgileri çıkarmasının çok zor olduğunu göstermektedir. Amaçlanan teknikler sadece kabul edilebilir PSNR değerlerine sahiptir ve 30 dB ila 31 dB arasındadır.

Akhtar ve arkadaşları (2014) geleneksel LSB görüntü steganografi tekniğinin geliştirilmiş versiyonunu sunmakta ve uygulamaktadır. Çalışmaları bit ters çevirme yöntemini kullanarak stego görüntünün kalitesini arttırır. Bit ters çevirme tekniklerine iki yaklaşım önerir ve uygularlar. Bu her iki teknik de, taşıyıcı görüntünün piksellerinin LSB'lerinin yalnızca ve yalnızca belirli piksel bitleri modeliyle ortaya çıktıklarında ters çevrildiği bit ters çevirme tekniklerini çözer. Bu, piksellerde daha az değişikliğe yol açan geleneksel LSB yöntemiyle karşılaştırılır. Gizli mesajın doğru bir şekilde alınması için, ters çevrilmiş bitlerin stego görüntüsü içinde bir yere gömülmesi gerekir. Deneysel sonuçlar, stego görüntüsünün PSNR değerinin iyileştiğini göstermektedir; dolayısıyla stego görüntü kalitesi iyileştirilir.

Deshmuk ve arkadaşları (2014) ayrıca LSB ikamesine dayanan kenar uyarlamalı steganografiyi sunmaktadır. Uyarlayıcı şema ve taşıyıcı görüntünün iki bitişik pikseli arasındaki fark kullanılarak gizli bilgileri taşıyıcı görüntünün keskin (kenarlar) bölgelerine gömerler. Teknikleri diğer LSB ve Pixel fark tabanlı tekniklerden daha iyi performans gösterir ve stego görüntüsünün kalitesini korur.

Dagar ve Dagar (2014), internet üzerinden veri aktarımının güvenlik seviyesini artırmak için renkli RGB görüntüler için steganografi tekniğini sunmaktadır. 24 bit RGB görüntü, gizli verileri kırmızı, yeşil ve mavi piksellere gömmek için kapak görüntüsü olarak kullanılır. X-Box eşleme kullanılır ve birkaç kutuda 16 farklı değer bulunur. Burada "X", 0 ila 9 arasında bir tamsayı sayısını temsil eder. X Kutularına kaydedilen bu değerler, taşıyıcı görüntünün LSB'leriyle eşleştirilir. Saldırganın gizli bilgileri çıkarması çok zordur, çünkü haritalamayı kullanırlar. Böylece bu eşleme gizli

bilgilere yüksek düzeyde güvenlik sağlar. PSNR değeri de hesaplanır ve yüksek PSNR değerine sahiptir, bu da daha yüksek stego görüntü kalitesine yol açar.

Modi ve arkadaşları (2013), kapak görüntüsünün LSB'lerinin gizli bilgilerini gömmek için yeni bir steganografi tekniği önermişlerdir. Yöntemlerinde, kenar bölgeleri, gizli bilgileri gömmek için kapak görüntüsünün diğer düz bölgelerine göre çok iyi alanlar olduğu için gizli mesajı saklamak için en az iki önemli kenar biti kullanılır. Bu yöntemde kenar bölgesi, gizli bilgi miktarı temelinde algılanır, bu da uyarlanabilir kenar algılaması yaptığı anlamına gelir. Deneysel sonuçlar analizi, yöntemlerinin geleneksel LSB görüntü steganografik yöntemlerden daha iyi performans gösterdiğini ve görsel saldırılara karşı daha fazla güvenliğe sahip olduğunu göstermektedir.

Samidha ve Agrawal (2013) "Mekânsal Alanda Rastgele Görüntü Steganografisi" araştırma makalelerinde çeşitli görüntü steganografik yöntemleri incelemiş ve rastgele bit seçimi ile LSB tabanlı steganografi yöntemini önermişlerdir. Tekniklerinde, gizli bilgilerin kapak görüntüsünün içine gömülmesi için rastgele en az önemli bit seçilir. Ayrıca kapak görüntüsünün rastgele piksellerine dayanan bazı teknikler önerdiler ve gizli bilgiler rastgele seçilen rastgele piksellerin bitlerine gömüldü. Bu amaçla yoğunluk değerleri, piksellerin konumu vb. parametreler kullanılır.

Sachdeva ve Kumar (2012) gizli bilgileri gömmek için vektör nicemleme tablosunu kullanırlar. Modifiye edilmiş QT'ye dayanan JMQT olarak adlandırılan yeni steganografi yöntemini sunarlar (Nicemleme Tablosu). Ayrıca önerilen yaklaşımlarını JPEGJSteg steganografi yöntemiyle karşılaştırırlar. Gömme kapasitesi ve stego görüntü boyutu performans analizi parametreleri olarak kullanılır ve deney sonuçları da JPEGJSteg yöntemiyle karşılaştırılır. Deneysel sonuçlar, gizli kapasitenin ve stego boyutunun arttığını göstermektedir. Bu nedenle JMQT sistemi iyi kapasiteye sahipken, JPEG-JSteg daha iyi stego boyutuna sahiptir.

İnsan görsel sisteminin (HVS) temelleri üzerine Qing ve arkadaşları (2010), hassas bilgilerin bir görüntünün RGB bileşenlerinin tüm düzlemlerine gömüldüğü yeni bir teknik önermiştir. Bu teknikte, bilgi gizleme algoritmasının uyarlanabilir doğası ile çoklu plan bit kullanılır. Önerilen bu yöntem, geleneksel LSB yönteminden daha yüksek yerleştirme kapasitesine ve düşük hesaplama karmaşıklığına sahiptir. Önerilen sistem aynı zamanda iyi kalitede stego imajına sahiptir.

Che-Wei Lee ve Wen-Hsiang Tsai (2010) gizli bilgileri gizlemek için PNG görüntülerini kullanan yeni bir steganografi yöntemi önerdiler. Shamir'in gizli paylaşım yöntemi, bazı polinomların payları hesaplamak için veri taşıyıcısı olarak katsayıları yardımıyla belirli veri dizisinden kısmi paylaşımlar üretmek için kullanılır. Bu kısmi paylaşımlar daha sonra Alfa kanalına (Şeffaf bölgeler) gömülür ve beyaz gürültüye sahip stego görüntüsü oluşturur. Beyaz gürültüyü azaltmak için küçük asal sayı kullanılabilir. Önerilen yöntem, gelişmiş güvenlik düzeyi ve stego görüntü kalitesi ile verileri gizlemek için etkin veri kapasitesine sahiptir.

Yang ve arkadaşları (2009), görüntü steganografisi için yeni bir uyarlanabilir LSB tabanlı yöntem sundu. Daha iyi stego görüntü kalitesi için piksel ayarlama tekniğini kullanır. Bu uyarlanabilir LSB ikamesi, yüksek gizli kapasiteye neden olur. LSB tabanlı görüntü steganografi yöntemi önerilmektedir. Verileri gizlemek için ortak bit kalıbı kullanılır. Mesaja ve desen bitlerine göre piksellerin LSB'leri değiştirilir. Bu yöntem düşük gizli kapasiteye sahiptir.

3. KRİPTOGRAFİ

3.1 Şifreleme Çeşitleri

İnsan uygarlığının ortaya çıkmasıyla birlikte, bilginin doğru kişilere aktarılması ihtiyacı doğdu ve gizlilik kavramı ortaya çıktı. İlk başta insanlar mesaj yayınlamak için sadece ses ve jestleri kullandılar. Yazının gelişiyle birlikte, yayın mesajlarının gizliliği ve özgünlüğü konusu özellikle önem kazanmıştır. Bunun bir sonucu olarak, yazma işleminden sonra, kriptografi sanatının, "gizlice yazma" yöntemi - kaydedilen mesajları bir kişiden diğerine gizlice iletmek için tasarlanmış bir dizi yöntem ortaya çıktı. İnsanlık, metnin yazılmasından kısa bir süre sonra veya en başından itibaren görünmez olan çok sayıda gizli yazma teknolojisini, özellikle de sempatik mürekkepleri ortaya çıkardı, değerli bilgileri büyük boyutlu bir metinde "tamamen" yabancı bir anlamla "çözerek", tuhaf belirsiz karakterler kullanarak mesajlar hazırladı.

Şifreleme, bilgiyi şifreleme yöntemlerini inceleyen ve geliştiren pratik bir konu olarak ortaya çıktı, yani mesaj aktarılırken - iletim gerçeğini gizlemez, ancak mesaj metnini deneyimsiz insanlar tarafından okunmak için erişilmez hale getirir. Bunun uğruna, mesajın metni, tek bir kişinin muhatapların kendisi hariç, içeriğini tanımayacak şekilde yazılmalıdır. 20. yüzyılın ortalarında ilk bilgisayarların ortaya çıkması durumu büyük ölçüde değiştirdi ... Pratik şifreleme, gelişiminde büyük bir sıçrama yaptı ve kriptografi gibi bir terim orijinal anlamından, kriptografiden, gizli yazımdan önemli ölçüde uzaklaşdı. Bu günlerde, bu konu, çeşitli gizli parametreler kullanan algoritmalar da dahil olmak üzere gizli algoritmalar kullanılarak verilerin dönüştürülmesine dayalı olarak tamamen heterojen bir doğanın bilgisini koruma yöntemlerini birleştirmektedir.

Kriptografi, gizli yazma ve mesaj gizleme tekniklerinin bilim veya çalışmasıdır (Merriam, 2009). Kriptografi, örgün eğitimi olmayanlardan anlamını gizleyen biçimsel dilbilim kadar geniştir. Ayrıca, dijital ağlar arasında yapılan işlemleri güvence altına almak için kullanılan modern şifreleme algoritmaları kadar spesifiktir. Kriptografi, bir kişinin bir mesajı veya anlamını bir ortamda gizlemeye çalıştığı herhangi bir yöntemi oluşturur (Brodney, Asher, 2009:199).

Şifreleme, verilerin veya bilgileri çözülemeyen bir koda dönüştürerek gizlediği şifreleme öğelerinin belirli bir öğesidir. Şifreleme, veri dönüşümünü gerçekleştirmek için genellikle belirtilen bir parametreyi veya anahtarı kullanır. Bazı şifreleme algoritmaları, anahtarın kodlanacak mesajla aynı uzunlukta olmasını gerektirir, ancak diğer şifreleme algoritmaları mesaja göre çok daha küçük anahtarlarda çalışabilir. Şifre çözme genellikle tersi olarak şifreleme ile birlikte sınıflandırılır (Kahn, 1996:118). Şifrelenmiş verilerin şifresi çözülürken orijinal veriler elde edilir.

Şifreleme günlük modern yaşamda kullanılır. Şifreleme, en çok internet gibi güvenli olmayan iletişim kanalları üzerinden yapılan işlemler arasında kullanılır. Şifreleme, otomatik vezne makineleri (ATM'ler), cep telefonları ve daha pek çok cihaz arasında aktarılan verileri korumak için de kullanılır. Şifreleme, bir mesajın kimliğinin doğrulanmasına izin veren dijital imzalar oluşturmak için kullanılabilir. Doğru bir şekilde uygulandığında, dijital imza alıcıya mesajın talep edilen gönderen tarafından gönderildiğine inanması için bir mesaj nedeni verir (Knuth, 1981:688). Dijital imzalar, hassas e-posta ve diğer dijital iletişim türlerini gönderirken çok kullanışlıdır. Bu, geleneksel el yazısı imzalara nispeten eşdeğerdir, çünkü daha karmaşık bir imza, daha karmaşık bir sahtecilik yöntemi taşır.

Şifreleme, şifreleme ve şifre çözme gerçekleştirmek için kullanılan bir algoritma, işlem veya yöntemdir. Bir şifre, mesajları şifrelemek ve şifresini çözmek için izlenebilecek bir dizi iyi tanımlanmış adım içerir. Bir şifrenin çalışması genellikle büyük ölçüde bir şifreleme anahtarının kullanımına bağlıdır. Anahtar, belirli çıkışları üretmek için şifreye eklenen herhangi bir yardımcı bilgi olabilir (Diffie, 1976:40).

Düz metin ve şifreli metin genellikle birbirinin zıttıdır. Düz metin şifrelenmeden önceki bilgilerdir. Şifreleme, bir şifreleme şifresinin çıktı bilgisidir. Birçok şifreleme sistemi, şifreli metin çıktısının başka bir şifreleme katmanına düz metin girişi olduğu birçok şifreleme katmanı taşır. Şifre çözme işlemi şifreleme metnini alır ve orijinal düz metne geri dönüştürür. (Merkle, 1982:104)

Güvenli kalma çabalarında, Hükümetler şifreleme ve bunların kırılması için personel istihdam etmiştir. Kriptanaliz, gizli yazıları veya iletişimi, anahtarın bilinmediği kodlar ve şifreler olarak çevirmek veya yorumlamak için kullanılan prosedürler, süreçler ve yöntemlerdir. Amaç aynı olmasına rağmen, kriptanalizin yöntem ve

teknikleri zaman içinde büyük ölçüde değişti (Jones, 2009:23). Bu değişiklikler, kriptografinin artan karmaşıklığına uyum sağlama girişiminden kaynaklanmaktadır.

Manuel ve bilgisayar şifreleme yöntemleri arasında büyük bir boşluk vardır. Manuel şifreler çok çeşitlidir ve nlar tarafından şifrelenen mesajlar oldukça özlü ve kısadır. Bu nedenle, bilgisayar korsanlığı insanlar tarafından makinelerden çok daha verimli bir şekilde yapılır. Bilgisayar şifreleri daha stereotipik, matematiksel olarak çok karmaşıktır ve oldukça uzun mesajlar şifrelemeye yöneliktir. Tabii ki, bunları manuel olarak çözmek denemeye bile değmez. Bununla birlikte, bu alanda, kriptanalistler, savaşın sadece donanım ve yazılım tarafından yürütülmesine rağmen, kriptografik bir saldırının komutanları olarak lider bir rol oynamaktadır. Bu fenomenin hafife alınması, İkinci Dünya Savaşı sırasında Enigma şifreleme makinesinin şifrelerinin çöküşüne yol açtı. Şifreleme türü ve mesaj dili neredeyse her zaman bilinmektedir.

Kriptografinin alfabetik ve istatistiksel özellikleri onları önerebilir. Bununla birlikte, genellikle şifrenin dili ve türü hakkında bilgi gizli kaynaklardan öğrenilir. Böyle bir durum bir kasayı kırmaya benzer: "kraker" önceden kırılacak kasanın tasarımını bilmiyorsa, bu pek olası görünmüyorsa, hala görünüşü ve kurumsal logosu ile hızlı bir şekilde belirler. Bu bağlamda, bilinmeyen sadece çözülmesi gereken bir anahtardır. Zorluk, tüm hastalıkların aynı ilaçla aynı şekilde iyileştirilememesi ve bunlardan herhangi biri için spesifik araçların olması ve spesifik tipte şifrelerin sadece kendi yöntemleriyle kırılması gerçeğinde yatmaktadır.

3.1.1 Klasik şifreleme çeşitleri

Açık ağ bağlantılı sistemlerde, iletişimde çeşitli düzeylerde saldırıları kolaylaştırarak bilgi rakipler tarafından alınır ve kötüye kullanılır (Stallings, 2004:3). Veri şifreleme, saldırılara karşı koymanın en etkili yolu olmaya çalışmaktadır (Charles, 2004:642). Kullanımda, i) Gizli anahtarlar kullanılarak simetrik anahtar şifrelemesi ve ii) Genel ve özel anahtarlar kullanılarak asimetrik anahtar şifrelemesi olarak adlandırılan iki şifreleme sınıfı vardır. Ortak anahtar algoritmaları yavaşken, Simetrik anahtar algoritmaları genellikle 1000 kat daha hızlı çalışır (Jose vd., 2005:178). Simetrik Anahtar şifrelemesi, güvensiz bir kanal üzerinden geleneksel iletişim sorununu çözmek için yaygın olarak kullanılmaktadır - ve - hala kullanılmaktadır (Dragos, 2006:25). İnternet gibi açık ağlarda, veri güvenliğini sağlamak için veri şifreleme yaygın olarak kullanılmaktadır. Her veri türünün kendine özgü özellikleri vardır. Bu

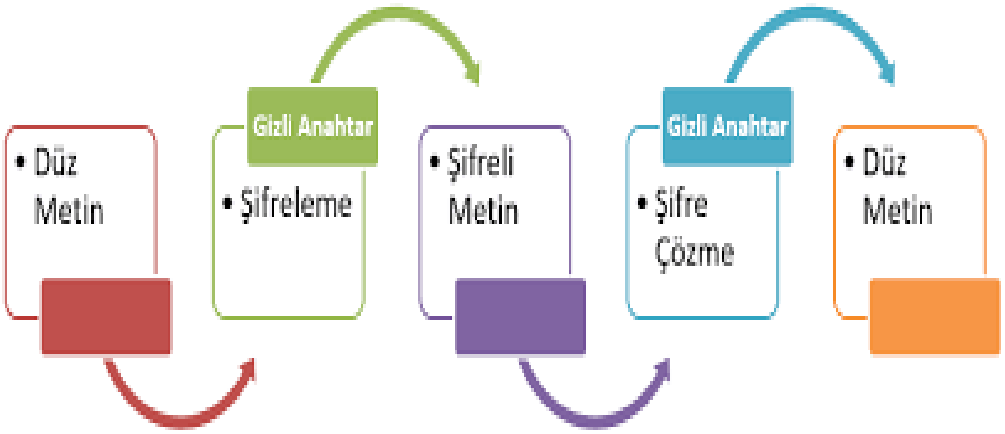
nedenle, gizli verileri yetkisiz kullanıma karşı korumak için farklı şifreleme teknikleri kullanılmalıdır. Metin verileri için birçok şifreleme algoritması bulunurken, metin verilerine uygulanabilen algoritma görüntü verilerine uygulanamayabilir. Kalsik şifreleme yöntemleri aşağıdakı şekilde belirtilebilir:

A. Yapı Taşları

i. Tüm klasik şifreleme tekniklerinin iki yapı taşı ikame ve aktarımdır.
ii. Değiştirme, düz metnin bir öğesinin bir şifre metni öğesiyle değiştirilmesi anlamına gelir.
iii. Aktarma, düz metnin öğelerinin görünüm sırasını yeniden düzenlemek anlamına gelir.
iv. Aktarma, permütasyon olarak da adlandırılır.

B. Simetrik Şifre Modeli: Simetrik şifreleme şemasının beş bileşeni vardır:

1. Düz Metin: Bu, algoritmaya girdi olarak beslenen orijinal anlaşılabilir mesaj veya verilerdir.
2. Şifreleme Algoritması: Şifreleme algoritması, düz metin üzerinde çeşitli ikameler ve dönüşümler gerçekleştirir.
3. Gizli Anahtar: Gizli anahtar aynı zamanda şifreleme algoritmasına da girilir. Anahtar, düz metinden ve algoritmadan bağımsız bir değerdir. Algoritma, o anda kullanılan belirli anahtara bağlı olarak farklı bir çıktı üretir.
4. Şifre metni: Bu çıktı olarak üretilen şifreli mesajdır. Düz metin ve gizli anahtara bağlıdır.
5. Şifre Çözme Algoritması: Bu aslında tersine çalışan şifreleme algoritmasıdır. Şifreleme metnini ve gizli anahtarı alır ve orijinal düz metni üretir.



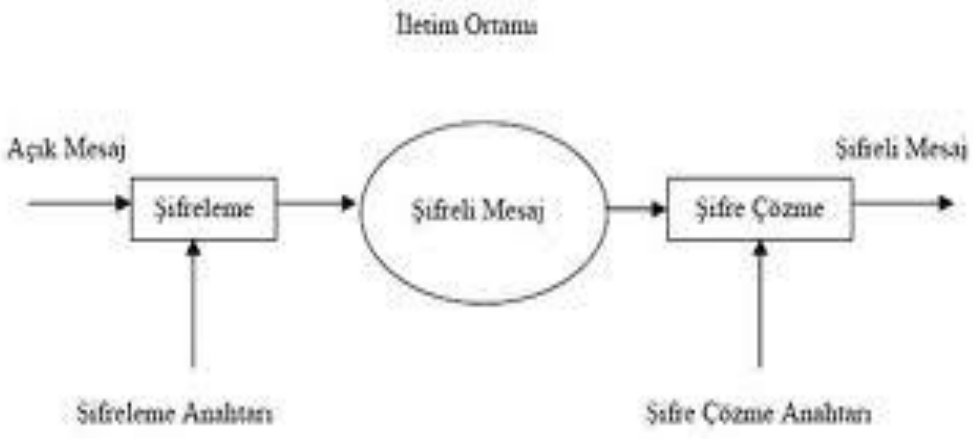
Şekil 3.1: Simetrik Şifre Modeli

Kaynak: https://dergipark.org.tr/tr/download/article-file/839739, 10.02.2020

C. Kriptografi Kriptografik sistemler üç bağımsız boyutta karakterize edilir:

1. Düz metni şifreli metne dönüştürmek için kullanılan işlemlerin türü: Tüm şifreleme algoritmaları iki genel ilkeye dayanır: düz metindeki her öğenin (bit, harf, bit veya harf grubu) başka bir öğeye eşlendiği ikame ve düz metindeki öğelerin yeniden düzenlendiği transpozisyon. Temel gereklilik, hiçbir bilginin kaybolmamasıdır.
2. Kullanılan anahtar sayısı: Hem gönderen hem de alıcı aynı anahtarı kullanıyorsa, sistem simetrik, tek anahtar, gizli anahtar veya geleneksel şifreleme olarak adlandırılır. Gönderen ve alıcı farklı anahtarlar kullanıyorsa, sistem asimetrik, iki anahtar veya ortak anahtar şifrelemesine dönüştürülür.
3. Düz metnin işlenme şekli: Bir blok şifresi, girişi bir kerede bir eleman bloğunu işleyerek her giriş bloğu için bir çıkış bloğu üretir. Bir akış şifresi, giriş elemanlarını sürekli olarak işler ve ilerledikçe bir kerede bir eleman üretir.

D. Kriptanaliz: Cyptanaltic saldırıları algoritmanın doğasına ve ayrıca düz metnin genel özellikleri hakkında biraz bilgiye dayanır.



Şekil 3.2: Kriptografi

Kaynak: http://www.bakimliyiz.com/egitim-ve-ogretim/120048-kriptografi-nedir-kriptoloji-nedir-kriptanaliz-nedir.html, 10.02.2020

E. Kaba kuvvet saldırısı: Saldırgan, düz metne anlaşılır bir çeviri elde edilene kadar bir şifre parçasındaki olası tüm anahtarları dener. Ortalama olarak, başarı elde etmek için tüm olası anahtarların yarısı denenmelidir.

İkame Teknikleri: İkame tekniği, düz metin harflerinin diğer harflerle veya rakamlarla veya sembollerle değiştirildiği tekniktir.

Sezar Şifresi: Bu, bir ikame şifresinin bilinen en eski örneğidir. Bir iletinin her karakterinin yerine, alfabe içinde üç konumlu bir karakter gelir. ben. Düz metin: hazır mısın ii. Şifre metni: DUH BRX UHDGB Alfabenin her harfini alfabedeki konumuna karşılık gelen bir tamsayı ile temsil edersek, düz metnin her 'p' karakterini şifre metninin 'C' karakteriyle değiştirmek için formül olabilir olarak ifade edilen

$C = E(3, p) = (p + 3) \bmod 26$

Bu şifrenin herhangi bir dereceye kadar kaymaya izin veren daha genel bir versiyonu,

$C = E(k, p) = (p + k) \bmod 26$

Şifre çözme formülü:

$p = D(k, C) = (C - k) \bmod 26$

Bu formüllerde 'k' gizli anahtar olacaktır. 'E' ve 'D' sembolleri şifreleme ve şifre çözmeyi temsil eder.

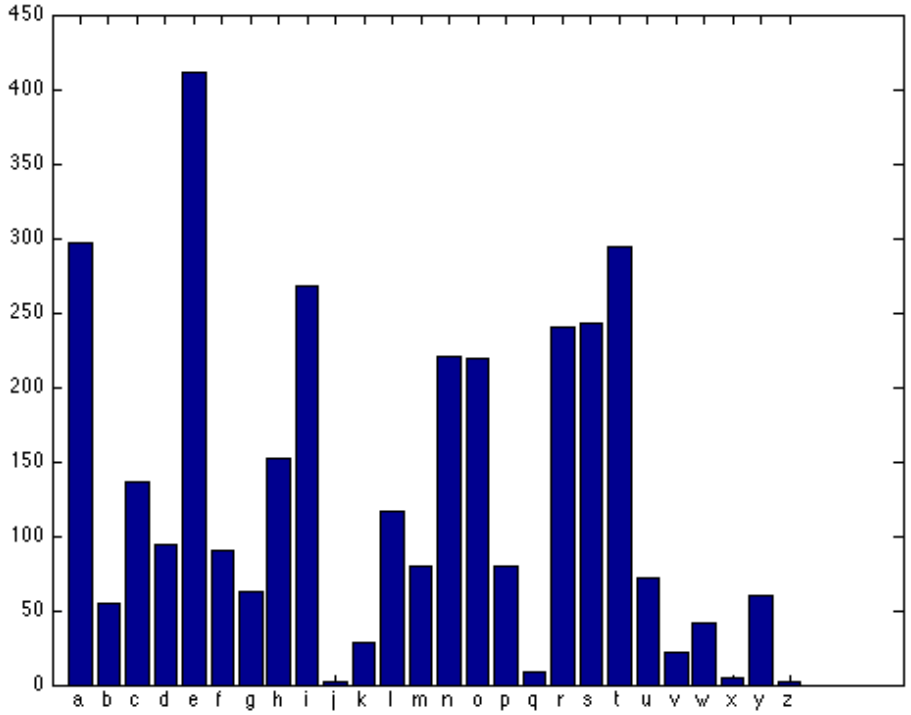
Mono-alfabetik Şifreler: Mono-alfabetik bir şifrede, ikame karakterlerimiz, alfabenin 26 harfinin rastgele bir permütasyonudur:

Düz metin harfler: a b c d e f .....

Oyuncu değişikliği harfleri: t h i j a b ....

Şimdi anahtar, ikame mektuplarının dizisidir. Başka bir deyişle, bu durumda anahtar, kullanılan alfabenin gerçek rastgele permütasyonudur. Bu, 4 × 10 ^ 26'dan büyük bir sayıdır. Tüm Korkunç İstatistiksel Saldırı: Düz metnin doğasını biliyorsanız, anahtar alanın boyutundan bağımsız olarak herhangi bir ikame şifresi, istatistiksel bir saldırı ile kolayca kırılabilir.

Düz metin düz İngilizce olduğunda, basit bir istatistiksel saldırı biçimi, tek karakterler, karakter çiftleri, karakter üçlüleri vb. İçin frekans dağılımını ölçmeyi ve benzer istatistiklere sahip olanları İngilizce için karşılaştırmayı içerir. Şekil, İngilizce bir metin örneğindeki harflerin göreli sıklığını gösterir. Açıkçası, bu dağılımı bir parça metin içindeki karakterler için bir histogramla karşılaştırarak, şifre metin karakterlerinin gerçek kimliklerini oluşturabilirsiniz.



Şekil 3.3: Kaba Kuvvet Saldırı Histogramı

Düz Metin Yapısını Maskelemek için Çoklu Karakter Şifreleme: Bir seferde bir karakter değiştirme, açık metin yapısının çok fazla kısmını şifre metninde bırakır. Çok karakterli oyuncu değişikliği gerçekleştiren en iyi bilinen yaklaşım Playfair Şifresi olarak bilinir. PlayFair Şifresinde Eşli İkame Değişiklikleri için Matris Oluşturma: Playfair şifresinde ilk olarak bir şifreleme anahtarı seçilir. Daha sonra, sol üst köşedeki ilk hücreden başlayarak soldan sağa doğru 5 × 5 matrisin hücrelerine anahtarın harfleri girilir. Kalan harfler alfabetik sırada olacak şekilde, matrisin geri kalan hücreleri elde edilir. I ve J harflerine aynı hücre atanır. Aşağıdaki örnekte, anahtar "smythework" dür.

M	O	N	A	R
C	H	Y	B	D
E	F	G	I	K
L	P	Q	S	T
U	V	W	X	Z

Şekil 3.4: Playfair Şifreleme Örneği

Playfair Şifresindeki Karakter Çiftleri İçin Değiştirme Kuralları: 5 × 5 matrisinin aynı satırına düşen iki düz metin harfinin yerini, satırdaki her birinin sağındaki harfler alır. "Doğruluk" özelliği, her satırda dairesel olarak yorumlanacaktır, yani her satırdaki ilk giriş son girişin sağındadır. Bu nedenle, düz metindeki "bf" harfleri, şifre metninde "CA" ile değiştirilir.

a. Aynı sütunda yer alan iki düz metin harfinin yerini, sütundaki hemen altındaki harfler alır. "Altlık" özelliği, bir sütundaki en üstteki girişin en alttaki girişin altında olması anlamında, dairesel olarak düşünülmelidir. Bu nedenle, düz metnin "ol" çifti şifre metninde "CV" ile değiştirilir.
b. Aksi takdirde, bir çiftteki her düz metin harfi için, aynı satırdaki ancak diğer harfin sütunundaki harfle değiştirin. Düz metnin "gf" çiftini düşünün. Dördüncü sırada ve ilk sütunda 'g' var; ve üçüncü satırda 'f' ve? fth sütununda. Bu yüzden, 'g' yerine 'g' ile aynı satırdaki, ancak 'f' içeren sütundaki harfle değiştiriyoruz. Bu bize 'G' yerine 'P' verdi. Ve 'f' yerine 'f' ile aynı satırdaki,

ancak 'g' içeren sütundaki harfle değiştiriyoruz. Bu bize 'f' yerine 'A' verir. Bu nedenle, 'gf' yerine 'PA' gelir.

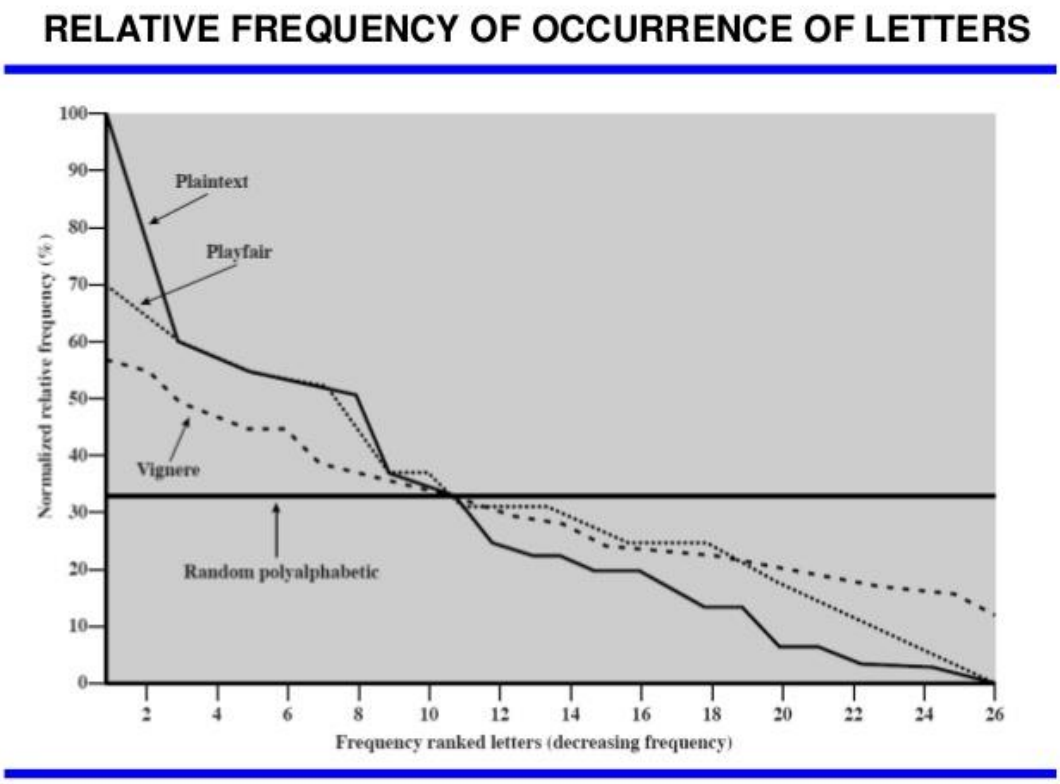
D. Bir Anahtardaki Yinelenen Harflerle Çalışma ve Düz Metindeki Tekrarlama Harfleri

Bir kopyadaki tüm kopyaları bırakmanız gerekir. İkame kuralları uygulanmadan önce, düz metindeki yinelenen harfler arasına seçilmiş bir "? Ller" harfi (diyelim 'x' dır) eklemeniz gerekir. Yani "hurray" gibi düz metinli bir kelime "hurxray" olur.

E. Play Fair:

i. Playfair'in onlarca yıl çözülmez olduğu düşünülüyordu. ii. Birinci Dünya Savaşı'nda İngiliz Ordusu tarafından şifreleme sistemi olarak kullanıldı. Ayrıca 2.Dünya Savaşı'nda ABD Ordusu ve diğer Müttefik güçler tarafından da kullanıldı. iii. Ancak, ortaya çıktığı gibi, Playfair'in kırılması son derece kolaydı. iv. Beklendiği gibi, şifre tek tek harflerle ve diyagramlarla ve trigramlarla ilişkili göreli frekansları değiştirir, ancak yeterince değil. v. Şekilde tek harfli göreli frekanslar, farklı şifreler için azalan sırada (ve 'e' harfinin göreli frekansına normalize edilmiştir) gösterilmektedir. İyi tahminler için dağıtımda hâlâ önemli miktarda bilgi bulunmaktadır.

vi. Playfair şifresinin kriptanalizine, bir şema ve tersinin benzer bir şekilde şifreleyeceği gerçeği de yardımcı olur. Yani, AB XY'ye şifrelerse, BA YX'e şifreleyecektir. Dolayısıyla, ters şemalarla başlayan ve biten kelimeleri arayarak, daha sonra benzer düz metin sözcüklerle karşılaştırmayı deneyebiliriz. Ters şemalarla başlayan ve biten kelimelere örnek: alıcı, ayrıldı, tamirci, redder, yalandan çıkarılmış, vb. Bu şekil William Stallings'in 2. Bölümünden alınmıştır (Stallings, 2002:80).



Şekil 3.5: Harflerin Göreli Sıklığı

Kaynak: https://www.slideshare.net/ayyakathir/cryptography-and-network-security-52030354 10.02.2020

F. Çok Harfli Şifre: Tepe Şifresi: Tepe şifresi çok harfli ikame için çok farklı (daha matematiksel) bir yaklaşım benimser: i. Alfabenin her harfine bir tamsayı atarsınız. Tartışma amacıyla, düz metnin 'a' - 'z' harflerine 0 ile 25 arasında bir tam sayı atadığınızı varsayalım. ii. K olarak adlandırılan şifreleme anahtarı, 3 × 3 tamsayı matrisinden oluşur:

$$K = \begin{matrix} K_{11} & K_{12} & K_{13} \\ K_{21} & K_{22} & K_{23} \\ K_{31} & K_{32} & K_{33} \end{matrix}$$

Şimdi düz metinden p1, p2 ve p3 sayıları ile temsil edilen harfler, bir kerede üç harfi, sayısal gösterimlerinde c1, c2 ve c3 üç harfli metne dönüştürebiliriz.

$$C_1 = (K_{11}p_1 + K_{12}p_2 + K_{13}p_3) \ mod\ 26$$

$$C_2 = (K_{21}p_1 + K_{22}p_2 + K_{23}p_3) \ mod\ 26$$

$$C_3 = (K_{31}p_1 + K_{32}p_2 + K_{33}p_3) \ mod\ 26$$

Yukarıdaki doğrusal denklemler seti, aşağıdaki vektör matris formunda daha kompakt olarak yazılabilir:

$$\vec{C} = [K]\vec{P} \ \ mod\ 26$$

Açıkçası, şifre çözme K matrisinin tersini gerektirecektir.

$$\vec{P} = [K^{-1}]\vec{C} \ \ mod\ 26$$

Bu işe yarıyor çünkü:

$$\vec{P} = [K^{-1}][K]\vec{P} \ \ Mod\ 26 = \vec{P}$$

Yalnızca şifre metin saldırılarına karşı son derece güvenlidir. Bunun nedeni, anahtar boşluğunun, büyük bir tamsayı kümesinden matris elemanları seçilerek son derece büyük hale getirilebilmesidir (Anahtar alanı, tekniği daha büyük boyutlu matrislere genelleştirerek daha da büyük hale getirilebilir). Ancak, düz metin şifreleme metin çiftleri bilindiğinde sıfır güvenliği vardır. Anahtar matris, bilinen çiftlerden kolayca hesaplanabilir.

G. One Time Pad: Anahtar, tek bir mesajı şifrelemek ve şifresini çözmek için kullanılmalı ve sonra atılmalıdır. Her yeni mesaj, yeni mesajla aynı uzunlukta yeni bir anahtar gerektirir. One Time Pad olarak bilinen böyle bir şema kırılmaz. Bir Zaman Pedi tam güvenlik sunar, ancak pratikte iki temel zorluk vardır:

1. Rastgele tuşların büyük miktarlarda yapma pratik sorunu var.
2. Daha da ürkütücü olan anahtar dağıtım ve koruma sorunudur. Gönderilecek her mesaj için, hem gönderen hem de alıcı tarafından eşit uzunlukta bir anahtar gereklidir.

Transpozisyon Teknikleri: Düz metin harfleri üzerinde bir çeşit permütasyon gerçekleştirerek çok farklı bir haritalama elde edilir. Bu teknik, bir transpozisyon şifresi olarak adlandırılır.

Ray Çiti: Bu tür en basit şifre, düz metnin bir köşegen dizisi olarak yazıldığı ve daha sonra bir sıra dizisi olarak okunduğu raylı çit tekniğidir. Örneğin, "toga partisinden sonra buluşalım" mesajını derinlik 2 bir raylı çitle şifrelemek için aşağıdakileri yazıyoruz:

m e m a t r h t g p r y

e t e f e t e o a a t

Şifrelenmiş mesaj-*MEMATRHTGPRYETEFETEOAA*T

Bu tür şeyler kriptanalize etmek için önemsiz olurdu. Daha karmaşık bir şema, mesajı dikdörtgene, satır satır yazmak ve mesajı sütun, sütunlar halinde okumak, ancak sütunların sırasına izin vermektir. Ardından sütunların sırası algoritmanın anahtarı olur. Örneğin,

Anahtar: 4 3 1 2 5 6 7

Plaintext: a t t a c k p o s t p o n e d u n t i l t w o a m x y z

Şifreli metin: TTNAAPTMTSUOAODWCOIXKNLYPETZ

Orijinal düz metinle aynı harf frekanslarına sahip olduğundan, saf bir transpozisyon şifresi kolayca tanınır. Yeni gösterilen sütunsal transpozisyon tipi için, kriptanaliz oldukça basittir ve şifreleme metnini bir matriste yerleştirmeyi ve sütun pozisyonları ile oynamayı içerir. Diyagram ve trigram frekans tabloları faydalı olabilir. Transpozisyon şifresi, transpozisyonun birden fazla aşaması gerçekleştirilerek önemli ölçüde daha güvenli hale getirilebilir. Sonuç, kolayca yeniden yapılandırılamayan daha karmaşık bir permütasyon. Dolayısıyla, yukarıdaki mesaj aynı algoritma kullanılarak yeniden şifrelenirse,

Key: 4 3 1 2 5 6 7

Input: t t n a a p t m t s u o a o d w c o i x k n l y p e t z

Output: NSCYAUOPTTWLTMDNAOIEPAXTTOKZ

Bu çift aktarımın sonucunu görselleştirmek için, orijinal düz metin mesajındaki harfleri, konumlarını belirten sayılarla belirtin. Böylece, mesajdaki 28 harfle, orijinal harf sırası aşağıdaki şekilde olur:

01 02 03 04 05 06 07 08 09 10 11 12 13 14

15 16 17 18 19 20 21 22 23 24 25 26 27 28

İlk aktarımdan sonra:

03 10 17 24 04 11 18 25 02 09 16 23 01 08

15 22 05 12 19 26 06 13 20 27 07 14 21 28

ki bu biraz düzenli bir yapıya sahiptir. Ama ikinci aktarımdan sonar:

17 09 05 27 24 16 12 07 10 02 22 20 03 25

15 13 04 23 19 14 11 01 26 21 18 08 06 28

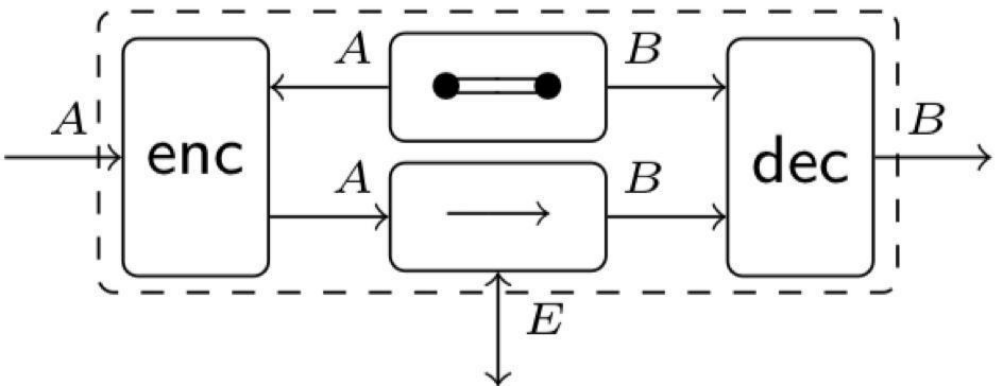
Bu çok daha az yapılandırılmış bir permütasyon ve kriptanalize edilmesi çok daha zordur.

3.2 Gizli Bilgi

Kayıtlı gizli kayıtlar ve bilgi yönetimi, gizli tutulması gereken ve yetkilendirilmedikçe açıklanmaması gereken kayıt ve bilgileri ifade eder. Gizli kayıtlar ve bilgi yönetimi özel kişisel bilgileri içerir ancak bunlarla sınırlı değildir. Kavram olarak gizlilik, kayıtları ve bilgileri koruma görevi için geçerlidir ve sadece kişisel kayıtlar ve bilgiler için değil, çeşitli kayıt ve bilgiler için de uygulanabilir. Kayıtlı gizli kayıtların ve bilgilerin açıklanması, belirli bir amaç için belirli kişiler veya gruplarla sınırlandırılmalıdır.

Yapıcı kriptografinin temel fikri (Maurer,2010:1) hem kurulum varsayımlarını hem de protokollerin garantilerini açıkça kaynak olarak belirtmek ve bir protokolü bu tür: kaynakların dönüşümü olarak değerlendirmektir. Burada, kaynak, çerçevelerdeki ideal işlevlere benzer şekilde, birkaç tarafın eriştiği paylaşılan bir işlevdir (Backes vd., 20047:1685). Gerçek kaynaklar, protokollerin (ağ gibi) yürütülmesi için gerekli işlevsellikler olarak kabul edilir ve ideal kaynaklar, tarafların ulaşmak istediği garantili işlevleri tanımlar.

Bir tarafın bir kaynağa erişme şekli, kaynak tarafından bu tarafa sağlanan arabirim tarafından tanımlanır; kaynak taraf başına bir arayüz sağlar. Dönüştürücü sistemleri, örneğin bir şifreleme şeması kullandığında, bir tarafın yerel olarak gerçekleştirdiği eylemleri resmileştirir. Dönüştürücünün iki arabirimi vardır: İç arabirim, kaynağın arabirimine eklenir ve dış arabirim, kaynağın özgün arabirimi yerine taraf tarafından kullanılır. Özellikle, kaynağın ve dönüştürücünün bileşimi, yine her bir taraf için bir arayüze sahip bir kaynaktır; bu, Şekil'de simetrik şifreleme durumunda tasvir edilmiştir.



Şekil 3.6: Kanala Uygulanan Şifreleme Protokolü (enc, dec) - → ve Tuşu • == •

Şifrenin her türlü saldırıya dayanma kabiliyetine şifrenin gücü denir. Bir şifreye yapılan saldırı, bu şifreyi açma girişimi olarak anlaşılır. Şifreleme gücü kavramı kriptografinin merkezinde yer alır. Her ne kadar nitel olarak anlamak oldukça kolay olsa da, her bir şifre için kesin kanıtlanabilir güç tahminleri elde etmek çözülmemiş bir sorundur.

Bunun nedeni, böyle bir sorunu çözmek için hala hiçbir matematiksel sonucun bulunmamasıdır. Bu nedenle, belirli bir şifrenin gücü sadece onu açmak için yapılan çeşitli girişimlerle değerlendirilir ve şifreye saldıran kriptanalistlerin niteliklerine bağlıdır. Bu prosedüre bazen dayanıklılık testi denir. Bir şifrenin gücünü kontrol etmek için önemli bir hazırlık adımı, bir düşmanın şifreye saldırabileceği iddia edilen çeşitli olasılıkları düşünmektir. Rakipte bu tür yeteneklerin ortaya çıkması genellikle kriptografiye bağlı değildir, bu bir dış ipucudur ve şifrenin gücünü önemli ölçüde etkiler. Bu nedenle, şifre gücü değerlendirmeleri her zaman, bu tahminlerin elde edildiği düşmanın hedefleri ve yetenekleri hakkındaki varsayımları içerir. Her şeyden önce, yukarıda belirtildiği gibi, genellikle düşmanın kodun kendisini bildiğine ve ön çalışması için fırsata sahip olduğuna inanılmaktadır. Bunun nedeni, böyle bir sorunu çözmek için hala hiçbir matematiksel sonucun bulunmamasıdır. Bu nedenle, belirli bir şifrenin gücü sadece onu açmak için yapılan çeşitli girişimlerle değerlendirilir ve şifreye saldıran kriptanalistlerin niteliklerine bağlıdır. Bu prosedüre bazen dayanıklılık testi denir.

Bir şifrenin gücünü kontrol etmek için önemli bir hazırlık adımı, bir düşmanın şifreye saldırabileceği iddia edilen çeşitli olasılıkları düşünmektir. Rakipte bu tür yeteneklerin ortaya çıkması genellikle kriptografiye bağlı değildir, bu bir dış ipucudur ve şifrenin

gücünü önemli ölçüde etkiler. Bu nedenle, şifre gücü değerlendirmeleri her zaman, bu tahminlerin elde edildiği düşmanın hedefleri ve yetenekleri hakkındaki varsayımları içerir. Her şeyden önce, yukarıda belirtildiği gibi, genellikle düşmanın kodun kendisini bildiğine ve ön çalışması için fırsata sahip olduğuna inanılmaktadır.

4. STEGANOGRAFİ

4.1 Steganografi Kavramı

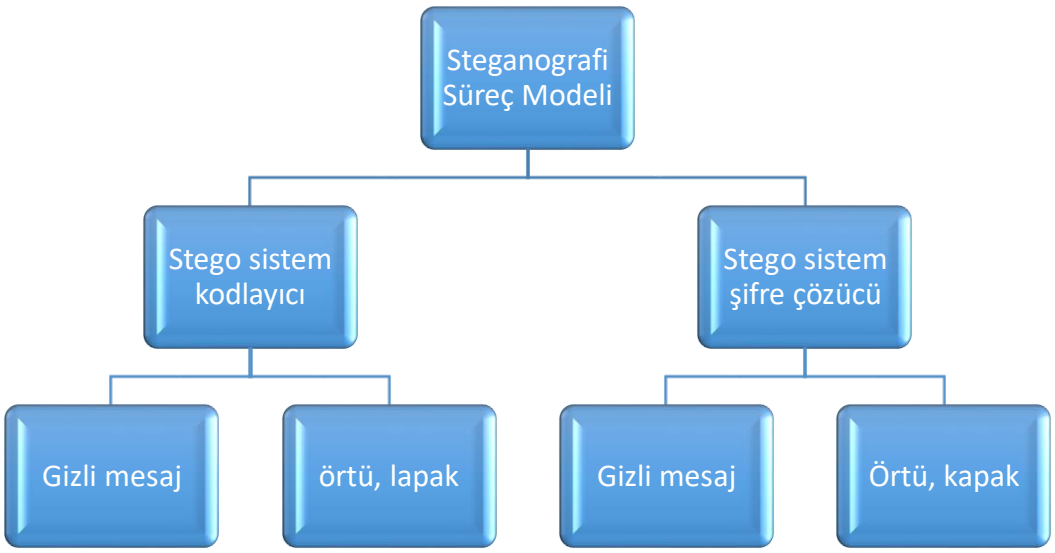
Steganografi, gizli bilgiyi başka bir ortamın içine gizleme sanatı ve bilimidir. Dijital steganografinin temel amacı, iletim sırasında herhangi bir davetsiz misafir tarafından fark edilmeden internet üzerinden gizli veri göndermektir (Katzenbeisse ve Petitcolas, 2000:77). İnternetin yaygın kullanımıyla birlikte, veri iletişimi için gizlilik daha savunmasız hale gelmiştir. İnternet üzerinden güvenli bilgi aktarımı talebi saatin ihtiyacı haline gelmiştir. Güvenlik konusundaki güvensizlik, internet istemcilerini ve şirketlerini, geleneksel şifreleme yöntemlerinin yanı sıra gelişmiş steganografi teknikleri biçiminde alternatifler aramaya itmiştir. Resimler, metin, ses ve video dosyaları, ağ üzerinden aktarılan en yaygın dosyalardır. Dijital dosyalarda fazlalık, bir kapak ortamındaki verileri gizleme fırsatı verir. Görüntüler steganografik amaçlar için en yaygın kullanılan kapak türleridir. En az anlamlı bit (LSB) steganografisi görüntü steganografisinde en sık kullanılan mekanizmadır. LSB görüntü steganografisi, görsel kaliteyi etkilemeden LSB'lerin değiştirilme esnekliğini kullanarak makul veri gizleme kapasitesi ve optimum algılanamayan seviye sağlar (Bender vd., 2000:3).

İnternet ve iletişim teknolojisinin gelişimi veri aktarımına yardımcı olmuştur. Açık iletişimin nedeni, bilginin güvenliği ve yasaklanmış verilerin varlığı açısından tehlikelerdir. Steganografi, verileri bu taşıyıcılar aracılığıyla herhangi bir dijital dosya, örneğin bir görüntü, metin, video, ses, vb. Olabilen bir taşıyıcı üzerine gizleme ve aktarma tekniğidir. Dijital görüntüler bilginin gizlenmesinde daha çok kullanılır, çünkü internette yaygın olarak kullanılırlar ve çok sayıda yedek bit içerirler (Desai ve Patel, 2016:295).

Steganografi gizli mesajı başka bir ortamın örtüsünün içine gizler. Steganografi kelimesi “steganos” ve “grafia” kelimelerinden oluşan bir kavramdır. “Steganos” kapak, “grafia” yazı anlamına gelir (Robert, 2004:12). Başka bir deyişle steganografi, kapalı yazı sanatı ve bilimi olarak tanımlanabilir. Görüntü steganografisinde görüntüler, görüntünün görsel kalitesini etkilemeden gizli bilgileri gizlemek için kullanılır. Steganografi, bir tür bilgiyi diğer bilgilerin kapağında saklayan tekniğin

adıdır (Cheddad vd., 2010:727). Bu nedenle, mesajın içeriğini korumak yeterli değildir, gizli mesajların varlığını gizlemek de bilgi koruması için önemlidir. Başka bir ortamın kapağında gizli bilgilerin varlığını gizlemek için kullanılan tekniklere steganografik teknikler denir.

Genel steganografi işlem modelinde, steganografi tekniklerinin uygulandığı enkodere gizli mesaj ve kapak beslenir. Kodlamadan sonra normal kapak şeklindeki stego nesnesi iletişim kanalından alıcıya gönderilir. İletişim sırasında gizli mesajın varlığı kapak altına gizlenir. Alıcı uçta, stego sistem kod çözücü, stego nesnesinden gizli mesajı ortaya çıkarmak için steganografi tekniğinin kod çözme yöntemini kullanır.



Şekil 4.1: Steganografi Süreç Modeli

Steganografi, bazı taraflarda şifreleme yerine diğer taraflara daha az şüphe verdiği için tercih edilmektedir (Petitcolas vd., 1999:1062). Bu tekniklerin her ikisi de bilgi güvenliği teknikleri olarak kabul edilir. Daha önce de belirtildiği gibi, her iki yöntem için bilgilerin güvenliğini sağlamada farklılıklar vardır. steganografi bilgileri görünmeyecek şekilde kapak ortamında saklayarak, güvence altına alır. ifreleme yöntemi, bilgi sinyalini işleyerek veya şifreli bir sinyale dönüştürerek verileri güvenceye alırken, sadece bit akışı dizisini saçarak veya bit akışını okunamayan veri formuna sahip olacak şekilde yeniden düzenleyerek saklar.

Hem stenograı, hem kriptografının paylaştığı unsurlardan biri, her ikisini de güvenceye alan bir anahtar olması gerçeğidir. Her iki yöntemde de anahtarın bulunmaması durumunda, kullanılan yöntem tipi gibi başka unsurlar bilinse bile

mesajın çıkarılması veya yeniden yapılandırılması yetersizliğine neden olacaktır. Her iki tekniğe sahip olmanın ilginç yanı, bu tekniklerin her ikisini de aynı anda iki seviyeli bir bilgi güvenliği yöntemi olarak bilgi sinyaline uygulamanızdır. Her iki tekniğin uygulanmasının kombinasyonu, sisteme daha yüksek düzeyde güvenlik ve ek karmaşıklık ile sonuç verecektir. Başka bir deyişle, bilgi sinyali üçüncü tarafça alındıysa, yapılması çok zor ve karmaşık olacak bilgileri elde etmek için hem steganografi hem de şifreleme analizi ile uğraşmaları gerekir.

Steganografi bir mesajın varlığını gizlerken, kriptografi karışıklığın içerdiği bir mesajı gizler. Steganografi bilimi, günümüzde mahremiyet kaybından dolayı önemli bir ihtiyaçtır. Steganografi, insanların başkalarının müdahalesi olmadan iletişim kurmasını sağlar. Steganografi teknikleri, başkalarının kapak ortamında gizlenmiş gizli verileri deşifre etmeye çalışmasını engellemedeki etkinliği nedeniyle hız artmaktadır.

Dijital bilgisayar dosyalarındaki bilgileri gizlemek gittikçe yaygınlaşmaktadır. Ücretsiz gizli yazma yazılımı indirmek ve kullanımı kolay hale gelmiştir (Kang, 2011:2). Son yıllarda steganografi tekniklerini araştırmak ve geliştirmek ve bunları ticari olarak uygulamak için uluslararası ilgi artmaktadır (Pevný, 2008:120). Steganografi, fikri mülkiyet haklarının korunmasında ve kişisel mahremiyetin korunmasında önemli faydalara sahip olmasına rağmen, her şeyin olumsuz ve olumlu etkileri vardır. Gizli yazma belki de kişisel, iş dünyası ve güvenlik perspektif bilgilerinin olumsuz etkilerini ortaya çıkarır. Gizli güdülere sahip olan bazı kişiler, yasaların uygulanmasından kaçınmak için yasadışı faaliyetler planlamak için bu tekniği yanlış kullanırlar.

Örneğin, bazı kişiler ticari mesajlar veya teknik mesajlar çalabilir ve bunları büyük miktarlarda para karşısında steganografi teknikleri kullanarak rakiplerine ulaştırır (Geetha ve Kamaraj, 2010:162). 2007'de bir ticari saldırı olayı vardı, bir rakip şirkete gizli bilgileri sızdırdı, resimleri ve müzik dosyalarındaki bilgileri gizlemek için gizli bir yazma aracı kullandı. Bu davada failin tutuklanmasına rağmen, gizli yazının uygulanabileceği geniş alan hakkında bir fikir vermektedir (Badr ve ark., 2014:12). Gizli yazma tekniklerinin bilgi güvenliği için potansiyel bir tehdit oluşturduğuna dair endişeler vardır. Gizli yazma, dijital ürünlerde neredeyse algılanamayan ek bilgilerin gizliliğini sağladığından, gizli bilgilerin ve kötü amaçlı yazılımların yayılması olasılığı çok büyüktür. Mevcut endişeler arasında, bu sırlara erişimi olan devlet sırlarının

korunması ve ifşa edilmesine karşı hassas hassas verileri gözetlemek için internet korsanlarının ve gizli iletişimin kullanılması da bulunmaktadır. Endişeler ayrıca, bilgisayar korsanları tarafından hile ve mali veya kimlik bilgilerinin çalınması gibi cezai faaliyetler için gizli iletişimin kullanılmasıyla da ilgilidir (Pevný, 2008:122).

4.2 Tarihsel Süreç

Bir yazı sisteminin geliştirilmesi stenografinin gerçek başlangıcıdır. Eski zamanlarda Sümerler çivi yazısı denilen sembolik bir yazı biçimi yarattılar. Yumuşak kildeki resimleri işaretlemek için derme çatma bir kalem kullanarak yazıları kaydettiler. Bu yazı sistemi Mezopotamya'da MÖ 100'e kadar kullanılmıştır. Son haliyle, telaffuza yardımcı olacak fonogramlar içeriyordu (Moerland, 2002:85).

Uzun zamandan beri gizli iletişim var. Steganografi kelimesi başlangıçta "Kapalı Yazı" anlamına gelen Yunanca kelimelerden elde edilmiştir. Uzun yıllar boyunca farklı şekillerde kullanılmıştır. Suudi Arabistan'da Kral Abdul-Aziz bilim ve yenilik kentinde, 12 yıl önce yazıldığı kabul edilen gizli yazı hakkında bazı eski Arapça orijinal kopyalarını İngilizceye dönüştürmek için bir proje başlatıldı. Bu kompozisyonların bazıları Türkiye ve Almanya'da bulundu (Cheddad ve diğerleri, 2010:727).

Steganografinin ilk kullanımı, gizli bilgileri yazmak için ahşap tabletlerin kullanıldığı ve daha sonra yazıyı balmumu ile kaplayarak gizlediği zaman Yunanlılara kadar uzanır. Korsanlar vücut kısımlarında gizli bilgileri dövme fikrini kullandılar ve ayrıca tıraş başlarını kullandılar, böylece saçlar büyüdüğünde gizli mesajların varlığını gizleyecekti. Almanlar, İkinci Dünya Savaşı sırasında güvensiz iletişim kanallarından hassas bilgiler göndermek için benzersiz bir teknik kullandı. Yüksek kaliteli görüntüler oluşturmak için mikro noktaları kullanmanın benzersiz bir yolunu kullandılar ve bu mikro noktalar kullanılarak bilgi gizlendi, o sırada davetsiz misafirlerin bu bilgilerin şifresini çözmesi neredeyse imkansızdı. Günümüzde steganografi kullanımı artmakta ve çeşitli alanlarda ve uygulamalarda güvenliğin sağlanması için kullanılmaktadır. Steganografinin en önemli kullanımlarından biri, telif hakkı verilerinin kullanımını korumak için telif hakkı uygulamasındadır (Moerland, 2002:87).

17. yüzyılda Schott, her müzik notasının belirli bir harfi temsil ettiği müzik skorlarındaki bilgileri gizleme yöntemi gerçekleştirmiştir Ayrıca resimlerin arkasında gizli mesajların gizlendiği de biliniyordu. Başka bir yol da mesajların gizlenmesine

örnek olarak görünmez mürekkep kullanmaktı. Bazı görünmez mürekkepler için, sadece belirli bir çalışma frekansı bandındaki belirli bir ışıkla gözlemlenebilir veya tespit edilebilir. Mikro yazma, mesajın ancak yazı boyutunun bazı optik büyütme araçları ile büyütülmesi ile gözlemlenebildiği steganografi yöntemlerinden biri olarak düşünülebilir (Petitcolas vd., 1999:1062). Tarihte steganografi yöntemlerini kullanmanın birçok örneği var ve muhtemelen bugüne kadar hala kullanılıyor.

4.3 Stenografı Yöntemleri

Steganografi, bir bağlantının varlığını gizleyen bir iletişim organizasyonu yöntemidir. Düşmanın iletilen mesajın şifrelenmiş metin olup olmadığını doğru bir şekilde belirleyebildiği şifrelemenin aksine, steganografi yöntemleri gizli mesajların zararsız mesajlara gömülmesine izin verir. Birkaç çeşit görüntü steganografisi vardır. Ortak stratejiler aşağıdakilerdir (Al- Ethawi, 2002:77):

4.3.1 LSB

LSB, gizli verileri görüntü piksellerinde olduğu gibi kapak veri baytlarının en az önemli bitlerine ileten bir steganografi yöntemidir. Steganografide kullanılan en ünlü, temel ve basit gömme yöntemidir. Yöntemin algılanamazlığı ve sağlamlığının parametrelerini geliştirmek için LSB yöntemine birçok iyileştirme yaklaşımı uygulanmıştır. Dijital steganografiyle ilgilenen herhangi bir araştırmacı için, LSB'yi diğer birçok steganografi yöntemine gömmenin en eski ve temel konsepti olarak inceleyerek başlayın. Temel LSB yönteminde, pikseller sıralı bir biçimde gömmek için kullanılır (Johnson ve Jajodia, 1998:331). LSB gizlenmesi, daha sonra açıklanacak olan rastgele bir şekilde de yapılabilir (Smitha, 2016:47).

Verilerin LSB yöntemine nasıl gömüleceğini anlamak için LSB, herhangi bir ikili değerin sağ tarafından son bit olarak bulunur (Smitha, 2016:49). Örneğin, (11110101) bayt ikili değerine sahipsek, ilk LSB (1) ve ilk iki LSB biti (01) 'dir, ayrıca son üç LSB bitinin (101) eşit olduğunu bilmek istiyorsak. Örnekte, LSM gömme için, veri gömme için bayt veya pikselin ikili değerinde yalnızca son biti, son iki biti veya son üç biti kullanmak mümkün olduğunu belirtmemiz gerekir. Bu nedenle, 1 bayt piksel boyutumuz varsa, minimum LSB kapasitesi piksel başına 1 bittir (bpp) (Smitha, 2016:50).

LSB'ye uygulanan iyileştirme yöntemlerinden biri, LSB gömme için kapak ortam parçalarının (pikseller) rasgele seçimi için psödondom kodlaması kullanmaktır.

Rastgele gömme sözde rasgele sayı üreteci (PRNG) kullanılarak yapılabilir (Smitha, 2016:57). LSB steganografisinde kullanılan özel yalancı benzersiz kod aslında yöntemin anahtarıdır. Yalancı kod anahtarı olmadan mesaj alıcı tarafından çıkarılamaz (Petitcolas et., 1999:1062). Rasgeleleştirme yöntemi, kapak ortamındaki rasgele gürültü ile aynı özelliklere sahiptir. Bu nedenle, gömülü veriler üçüncü taraflarca gürültü olarak kabul edilebilir ve bu, sözde kodlama kullanmanın amacıdır (Petitcolas et., 1999:1065)

4.3.2 DCT

Ayrık Kosinüs Dönüşümünde, her renk bileşeni için JPEG görüntü biçimi, görüntünün birbirini izleyen 8 x 8 piksel bloklarını her biri 64 DCT katsayısına dönüştürmek için ayrı bir kosinüs dönüşümü kullanır. 8 x 8 görüntü pikseli f (x, y) bloğunun DCT katsayıları F (u, v) tarafından verilir (Denslin ve Brabin, 2017:77).

$$F(u,v) = \frac{1}{4}C(u)C(v)\sum_{x=0}^{7}\sum_{y=0}^{7} f(x,y)cos\frac{(2x+1)u\pi}{16}cos\frac{(2x+1)u\pi}{16}$$

Burada, $C(u) = \begin{cases} 1 \\ \sqrt{2} \quad if\ u \leq 0 \\ 1, \quad \text{İ}f\ u \geq 0 \end{cases}$

DCT tekniğini kullanarak metin mesajını gömme algoritması aşağıdaki gibidir (Stuti et., 2013:14): -

- Kapak resmini okuyun.
- Gizli mesajı okuyun ve ikili dosyaya dönüştürün.
- Kapak resmi 8 × 8 piksel bloğuna bölünür.
- Soldan sağa, yukarıdan aşağıya doğru çalışarak, her piksel bloğunda 128 çıkartın.
- Her bloğa DCT uygulanır.
- Her blok niceleme tablosu ile sıkıştırılır.
- Her DC katsayısının LSB'sini hesaplayın ve gizli mesajın her bir bitiyle değiştirin.
- stego resmi yazın.

DCT tekniği kullanarak kısa mesaj almak için algoritma: (Raja, Chowdary, 2013:89)

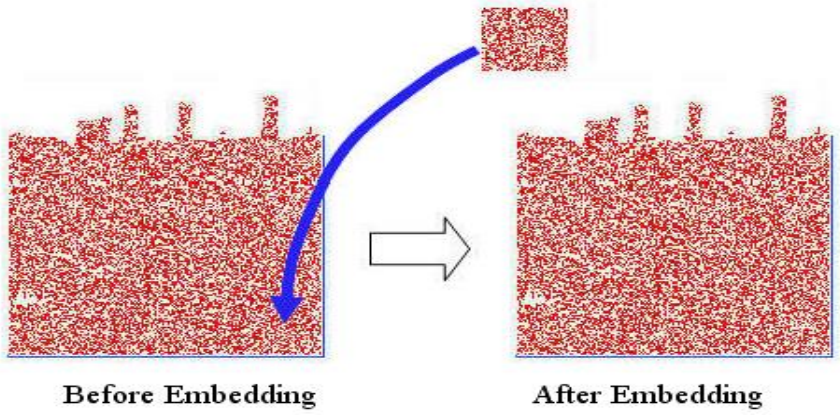
1. stego görüntüsünü okuyun.

2. Stego görüntüsü 8 × 8 piksel bloğuna bölünür.
3. Soldan sağa, yukarıdan aşağıya doğru çalışarak, her piksel bloğunda 128 çıkartın.
4. Her bloğa DCT uygulanır.
5. Her blok nicemleme tablosuyla sıkıştırılır.
6. Her bir DC katsayısının LSB'sini hesaplayın. 7. Her 8 biti alın ve bir karaktere dönüştürün. DCT blok F, 64 DCT katsayısından oluşur.

Üst taraf katsayıları F (0,0), DC katsayı olarak adlandırılan orijinal görüntü bloğunun daha düşük frekansı ile ilişkilidir. Tüm yönlerde F (0,0) 'dan uzaklaştıkça DCT katsayıları daha yüksek frekanslarla ilişkilidir, burada F (7,7) en yüksek frekansa karşılık gelir.

4.3.3 BPCS

BPCS başka bir ikame tipi yöntemidir, ancak belirli bitleri değiştirmek yerine, BPCS bir görüntünün karmaşık alanlarını tarar ve bunları mesaj verileriyle değiştirir. Fikir, bir insanın karmaşık bir yama ile başka bir karmaşık yama arasında ayrım yapamayacağıdır (Xianhua et., 2016:55).



Şekil 4.2: Rasgele Veri Yamaları

Kaynak: http://datahide.org/BPCSe/principle-e.html, 10.02.2020

Kesinlikle, bu görüntülere yan yana bakıp karşılaştırarak farklılıkları görebilirsiniz. Ancak, birine daha büyük bir görüntünün küçük bir parçası olarak bakarsanız ve daha sonra diğeriyle değiştirilirseniz, muhtemelen bir fark fark etmeyeceksiniz. Bu görüntüler büyüktür, 512 x 512, ancak BPCS algoritması 8 x 8 yama kullanır, bu da algılanabilir algılamayı daha az olası hale getirir. BPCS bir görüntüyü bit düzlemlerine ayırır ve her düzlemde değer sıfır veya birdir. Sonra BPCS 8x8 yamayı tarar ve

“karmaşıklığı” belirler. Ne kadar değişiklik var? Örneğin, saf siyah veya saf beyaz yama sıfır karmaşıklığa sahiptir, yani değişiklik yok. Değişen siyah ve beyaz bir dama tahtası deseni maksimum karmaşıklığa sahiptir - satır, ardından sütun ile tarandığında 112 değişiklik vardır. Basit bir karmaşıklık ölçüsü, görüntü örneğindeki değişiklik sayısını maksimuma bölmek ve 0'dan 1'e bir değer elde etmektir (Johnson, 1998:26).

Deneysel olarak iyi bir eşik değeri 0.3 olarak belirlenmiştir. (0,5'ten az OLMALIDIR) Yani, en az 34 değişiklik varsa (34/112 = 0.305), görüntü örneği karmaşıktır ve verilerimizi orada gizleyebiliriz. Eşik karşılanmazsa, BPCS sonraki 8x8 matrisine devam eder ve bu yamayı değiştirmeden bırakır. aha sonra, 64 bit mesaj verileri ile değiştirilir. Şimdi sorun şudur: İleti verileri karmaşık değilse ne olur? Çıkarma sırasında, program bu bit düzlemini atlayacaktır. Çözüm, verileri özel veya bir dama tahtası deseniyle "birleştirmek" tir. Konjugat karmaşıklığı daima bir eksi konjugat olmayan verilerin karmaşıklığıdır. Bu yüzden eşik 0,5'ten az OLMALIDIR, aksi takdirde konjugasyon çözümü işe yaramaz, eşik 0,7 ise ve mesaj verilerinin karmaşıklığı 0,6 ise, eşiği karşılamak için eşlenemezsiniz.

5. STEGANOGRAFİNİN KULLANIM ALANLARI

5.1 Metin Steganografi

Steganografi, gizli bilgileri taşıyan kapak ortamının tipine göre çeşitli tiplerde sınıflandırılabilir. Bu ortamlar genellikle görüntü, video, ses, metin ve protokolü içerir (Robert, 2004:15). Artıklığı fazla olan bilgi ortamlarının, steganografi ortamı olarak kullanım için daha uygun olduğu düşünülmektedir. Artıklık, ortama göre değişir ve ses veya video dosyasının piksellerini veya örneklerini temsil eden bitler olabilir. Gereksiz bitler, dosyayı steganografi amacıyla kullanmak için dosyayı kapsamlı bir şekilde etkilemeden değiştirilebilir. Görüntü, ses ve video gibi dosya formatları yüksek derecede fazlalıklara sahiptir, bu nedenle steganografi işlemi için kullanılırlar.

Metindeki steganografi sadece bazı metin özelliklerini değiştirmeye odaklanır. Bu, metin özniteliklerini veya metin biçimlendirmesini değiştirerek yapılabilir. Aşağıdaki liste, steganografi metnini uygulamanın bazı yollarını tartışmaktadır (Agarwal, 2013:41). Verileri normal metinde gizlemek birçok şekilde yapılır. Bunun bir yolu, belge satırlarının sonuna sekmeler ve boşluklar eklemektir. Başka bir yöntem, içeriğin on kez basılıp kopyalanmasına rağmen gizli mesajın hala kurtarılabileceği eğitim bölümlerinde etkili bir şekilde kullanılmıştır (Por ve Delina, 2008:47)

Bir metne gizli mesaj koymanın bir başka yolu, açık bir şekilde erişilebilir bir kapak kaynağı, bir kitap veya gazete kullanmak veya örneğin bir sayfa numarası, bir satır numarası ve bir karakter numarası kombinasyonu içeren bir kod kullanmaktır. Bu şekilde kapak kaynağının içine kaydedilen hiçbir veri gizli bir mesaj istemez. Başlıca kullanılan steganografik yaklaşımlardan biri, arka plan rengi ve yazı tipi rengini ayarlamaktır. Bu teknik Microsoft word belgesi için hazırlanmıştır. Önceden tanımlanmış tonları seçilir ve boşluk, sekmeler veya satır başı karakterleri gibi görünmeyen karakterlerin metin stilini ve arka plan tonları ayarlanır. Kırmızı, yeşil ve mavi değerler 8 bittir, 0 ile 255 arasında kapsamı etkinleştirildiği anlamına gelir. Bu yaklaşımın gerekli bitleri gizlemek için ek verilere ihtiyacı yoktur (Shirali-Shahreza, 2008:1912).

Metnin içindeki bir metni gizleme prosedürü, metin biçimini değiştirerek veya harfler gibi metin öğelerindeki belirli özellikleri değiştirerek gerçekleştirilebilir. Kodlama yöntemlerini tasarlamanın amacı, gürültü içeriyor olsalar bile kırılamayan değişiklikleri başlatmaktır (Brassil vd., 1995:1495). Bu önlemler güvenilir bir şekilde çözülemez ve içlerindeki görsel değişiklikler minimum düzeydedir. Bilgisayar dosya biçimindeki dosya biçimi veya belge, belgenin içeriğini ve TeX, @off, PostScript2 vb. Standart açıklama dillerini kullanan sayfa düzenini veya biçimini açıklar. Aşağıdaki üç kodlama tekniği form yerine farklı bir yaklaşımı tanımlar:

- Satır Kayması Kodlaması: Bu yöntem, belgeyi benzersiz şekilde kodlamak için dikey metin satırları konumlarını dönüştürerek belgeyi kodlamak için kullanılır. Gömülü kod daha sonra bitmap veya format dosyasından çıkarılabilir. Bazı özel durumlarda bu kod çözme sistemi, buluşa ait görüntüye gerek kalmadan elde edilebilir, çünkü orijinal olanın bir paragraf içindeki bitişik çizgiler arasında sabit satır aralığına sahip olduğu kabul edilir (Brassil vd., 1995:1496).
- Sözcük Kaydırma Kodlaması: Bu yordam, belgeyi benzersiz bir şekilde kodlamak için yatay bir konumda metin satırlarını dönüştürerek belgeyi kodlamak için kullanılır. Bu gömme yordamı, bit eşlemine veya sayfa görüntüsünün dosya biçimine uygulanabilir. Kod çözme bit haritasından veya dosya biçiminden uygulanabilir. Bu yaklaşım, komşu değişkenler arasında boşluk içeren belgelere uygulanabilir. Metin belgelerindeki değişken alan, metni denetlerken beyaz boşluk ayırmak için sıklıkla kullanılır (Chapman, 2001:156).
- Özellik Kodlama: Bu kodlama prosedürü bit eşleme görüntüsüne veya belgenin biçim dosyasına yerleştirilebilir. Görüntüler daha sonra seçilen metnin özelliklerine bağlı olarak test edilir ve bu özellikler önce terime bağlı olarak değiştirilir. Kod çözme işleminin gerçek görüntüye veya ek bir görüntüye, bir özellikteki piksellerdeki değişikliğin ölçülmesi gerekir. Metin özelliklerinin birçok olası seçimi olduğundan; burada, b, d, h, vb. harflerin üst kısmı olan dikey uç çizgilerini yukarı doğru değiştirmeyi seçiyoruz. Bunlar bitiş çizgisi özelliğini değiştirmez. Chapman ve ark. Tarafından tanımlanan steganografi metninin başka formları da vardır. Açıklanmayan mesajı gizlemek için doğal yazı dilini kullanmanın yolu olarak. Bu değişken aralıktan ötürü,

kod çözme işleminin başlangıçtaki görüntüye veya daha özel olarak kodlanmamış belgedeki kelimeler arasındaki boşluğa ihtiyacı vardır (Singh vd., 2009:26).

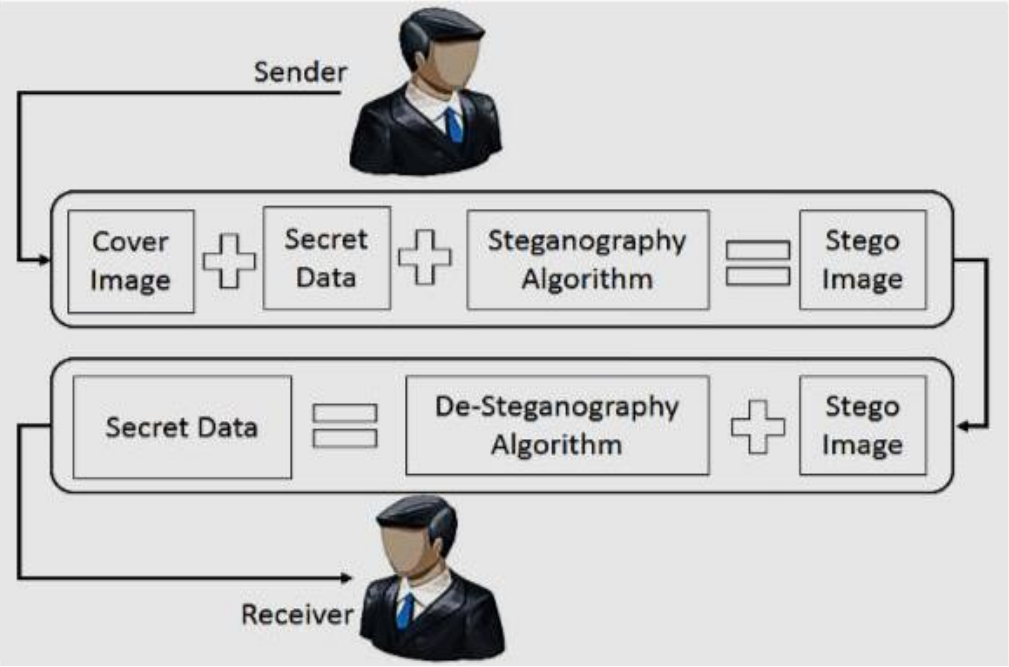
5.2 Görüntü Steganografi

Video steganografisinde, gizli mesajları gizlemek için ek bilgiler içeren bir video dosyası yerleştirilecektir. Bir stego video sinyali, gizli mesaj bilgilerinin ve kapak video dosyasının bir kombinasyonudur. Ara sinyal, kodlamayı almak için içerik bilgileriyle birleştirilir. Ekteki bilgiler, tüketicinin elektronik cihazlarından alınan ve kopyalamayı devre dışı bırakmak için kullanılan çift kontrol bilgisi olarak dahil edilmiştir (Sadek vd., 2015:70).

Geçiş sinyali ayrıca, gizli verileri kodlanmış içerikten ayıklamak için eşdeğer bir anahtar gerektiren kodlamayı ve kod çözmeyi gizlemek için sözde rastgele anahtar bilgileri de taşır. Birkaç uygulamada, düzenleme sinyaline yardımcı veriler içeren düzenleme bilgisi yerleştirilir. Bu kodlama, ölçeklendirme yeniden örnekleme ve diğer bozunma türlerine karşı güçlü bir şekilde karşıdır; amaç, ek bilgilerin bozulmuş olabilecek maddelerden tanınabilmesidir (Rhoads, 2000:193). Video steganografinin en çok bilinen yaklaşımlarından bazıları aşağıda listelenmiş ve tartışılmıştır.

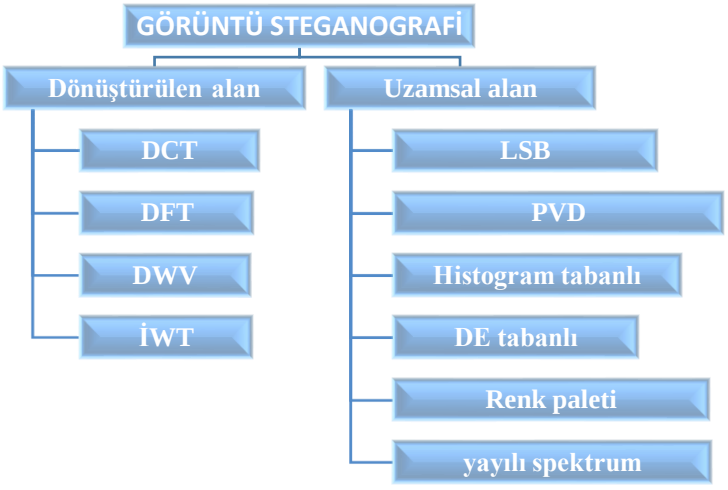
En Az Önemli Bit Yerleştirme, hemen hemen tüm steganografi türleri için en temel ve bilinen yaklaşımdır. LSB video steganografisinde dijital video dosyası ayrı kareler olarak alınır ve her video anahattının resmini değiştirir. Görüntülerin LSB'leri gizli verileri depolamak için kullanılır. Teknik, gizli mesajın kapasitesini yükseltir ancak veri bütünlüğü gibi güvenlik gereksinimlerini tehlikeye atabilir (Ramalingam, 2011:502).

Bu tip steganografi, cihazdaki çalışma süresi çıktı videosundaki verilerin gizlenmesini içerir. Teknik, görüntüde bloklara dağıtıldıktan sonra, mesajda ortaya çıkan ne olursa olsun, herhangi bir noktada gösterilen her kareyi dikkate alır. Bu noktada blokların piksel tonları benzerse, bu piksellerin sayısının renk özelliklerini bir dereceye kadar değiştirir. Her kareyi bir sıra numarası ile etiketleyerek eksik bilgi kısımlarını tanımlamak kolaydır. Önce görüntülenen kare kaydedilmeli ve daha sonra video dosyasından bilgileri çıkarmak için ilgili programı kullanmalıdır (Jenifer vd., 2014:319).



Şekil 5.1: Görüntü Steganografi İşlem Bloğu Şeması

Görüntüler steganografi için kapak dosyaları olarak kullanılan en uygun ortamdır. Veriler, İnsan Görselleştirme Sisteminin (HVS) zayıflığından yararlanarak görüntüye gömülür. Görüntü steganografisinin genel süreci Şekil 'te gösterilmektedir. Gönderen tarafında, gizli veriler herhangi bir steganografi tekniği kullanılarak görüntüde gizlenir. Gizli bilgilere sahip olan görüntüye artık stego görüntüsü denir. Stego görüntüsü iletişim kanalı üzerinden hedefe gönderilir. Alıcı tarafta, steganografi tekniği ile tanımlanan kod çözme yöntemine bağlı olarak gizli verilerin çıkarılması yapılır. Farklı görüntü formatları vardır ve her dosya formatı için bazı görüntü steganografik teknikleri vardır.



Şekil 5.2: Görüntü Steganografi Alanları

Görüntü steganografisi için iki ana etki alanı vardır, yani dönüştürme etki alanını ve görüntü etki alanını. Dönüştürme alanı görüntü steganografisi frekans alanı içinde saklanan veriler için kullanılır. Görüntüler önce dönüştürülür ve daha sonra veri gizleme işlemi gerçekleştirilir. Oysa görüntü alanında uzamsal alan adı olarak da bilinen veriler doğrudan piksellerin yoğunluğuna yerleştirilir.

Uzamsal alan teknikleri olarak da bilinen görüntü alanı, bilgileri görüntü piksellerinin yoğunluğuna veya renklerine gömer. Görüntü alanı tekniğinde, görüntü piksellerine bitsel olarak gizli bilgilerin eklenmesi yapılır. Kayıpsız görüntü formatları, görüntü alanı steganografisinde bilgileri gizlemek için en uygun olarak kabul edilir; oysa gömme teknikleri kullanılan görüntü formatlarındaki sapma ile birlikte değişir (Morkel vd., 2005:10). Bu görüntü alanında steganografi modifikasyonu, frekans alanına herhangi bir dönüşüm yapılmadan doğrudan piksel değerlerinde yapılır. Bu etki alanı, verilerin tam kapak değişikliği yapılmadan gömüldüğü veri yerleştirme açısından basittir. Tüm mekansal alan steganografik teknikleri kayıpsız ortam tiplerine uygulanabilir. Kayıpsız sıkıştırma, orijinal verilerin sıkıştırılmış verilerden mükemmel bir şekilde yeniden oluşturulmasını sağlayan bir veri sıkıştırma algoritmaları sınıfıdır.

Uzaysal alan tabanlı steganografide çeşitli tipler vardır; ancak temel olarak, hepsi verileri gizlemek için görüntü piksellerindeki bitleri değiştirmeye dayanır. Günümüzde kullanılan en dikkat çekici steganografi tekniği, verileri en az anlamlı piksel bitlerinde değiştiren ve gömen en az anlamlı bit steganografisidir (LSB). LSB steganografisi için kilit nokta, verileri gizlemek için piksellerde yapılan değişikliklerin insan gözü tarafından görülememesi ve değişikliklerin gözle görülür görüntü bozulmasına yol açmamasıdır. Görüntülerdeki verilerin güvenliğini sağlamak için çeşitli steganografi teknikleri kullanılmaktadır (Khodaei, Faez, 2012:677). LSB, verileri gizlemek için en yaygın kullanılan tekniktir.

PVD, stego görüntünün kaliteli olmasını sağlamanın yanı sıra yüksek veri gömme kapasitesine sahiptir. PVD, pikseller arasındaki değer farkının dikkate alınmasına dayanır. Görüntünün pürüzsüz ve kenar alanlarını ayırt eder. Kenarlarda piksel değerleri arasındaki fark daha büyüktür, bu nedenle görüntü kalitesini etkilemeden daha fazla veri biti gömülür. Düzgün alanlarda piksel farklılıkları daha azdır, bu nedenle değişime daha duyarlı oldukları için bu alanlarda daha az veri biti gizlenir (Wang, 2008:150).

Bu yöntemde veriler, histogram kaydırma yoluyla piksel konumlarının üretildiği histogram kullanılarak gömülür. Görüntülerdeki değişiklikleri bulmak için çoğunlukla histogram analizine dayanan stegnalysis teknikleri kullanılır. Bu yöntem, piksel bitlerinde değişiklik yaparken histogramdaki değişiklikleri korur, böylece görüntünün stegnalizi yapılırsa hiçbir değişiklik veya minimum değişiklik fark edilemez (Vleeschouwer, 2001:345).

Liu ve diğ. (2011:263) basit konum haritası ve bilinear enterpolasyonu ile DE yöntemi önerdiler. Bu, uygun konumların bulunmasına ve stego görüntü kalitesinin iyileştirilmesine neden olur. Steganografide kullanılan fark genişletme yöntemleri, sınırlı veri yükü ve veri gizliliği için sınırlı konumlar ile sınırlıdır. Bu tür tekniklerin sınırlandırılması, verilerin kodlanması sırasında yanlış piksel üretimidir. Palet tabanlı görüntüler için steganografi yöntemi ilk olarak Fridrich tarafından önerilmiştir (Fridrich ve Du. Rui, 1999:41). Bu görüntüler Grafik değişim formatını (GIF) içerir. Renk paletine dayanarak tek bit gömülüdür. Yalancı sayı seçimi, veri gömme için pikselleri seçmek için rastgele taramanın kullanıldığı ve renk eşleştirmenin verileri gizlemeye yardımcı olduğu anahtar olarak kabul edilir. Bu alanda farklı teknikler önerilmiştir. Bu tip steganografi, iyi stego görüntü kalitesine sahiptir ve daha az bozulma üretir.

Dönüşüm alanı teknikleri bir görüntünün frekans bileşenlerini kullanır. Görüntü önce frekans alanına dönüştürülür ve sonra mesaj gömülür (Sharma, 2015:22). Dönüştürme alanı görüntü steganografi teknikleri, görüntünün dik dönüşümünün değiştirilmesine dayanır. Dönüşümün iki bileşeni vardır; büyüklük ve faz. Büyüklük frekans içeriğinden oluşur, faz ise uzamsal alana dönüşüm için kullanılır. Bu teknikler, görüntü dosya formatlarından daha sağlam ve bağımsız olan belirli görüntü alanlarına bilgi bitleri yerleştirir. Uzamsal alanda, Ayrık Fourier Dönüşümü (DFT), Ayrık Kosinüs Dönüşümü (DCT), Ayrık Dalgacık Dönüşümü (DWT) ve Tamsayı Dalgacık Dönüşümü (IWT) içeren görüntü steganografisini içeren az sayıda ana görüntü steganografi tekniği vardır.

5.3 Ses (Audio) Steganografi

Ses steganografi, ses dosyalarının içindeki gizli mesajı gizlemek için kullanılan bir tekniktir. Bu, çok çeşitli ses sinyallerini dinleme yeteneğine sahip insan işitsel sisteminden (HAS) sorumludur. HAS'ın ana kısa gelişi, gizli mesajları kodlamak için

maruz bırakılan sesi tanınmadan ayırt etmeye çalıştığında ortaya çıkar (Jayaram, 2011:87). Ses için steganografide en çok kullanılan yöntemler LSB kodlamasına ve Spread Spectrum'a dayanmaktadır.

En az anlamlı bit steganografi, değişiklikler seslerde bariz değişiklikler yapmayacağı için sesdeki bilgileri gizlemek için LSB'leri kullanır (Singh, 2010:88). Eşlik kodlama tekniği, bir sinyali farklı örnek alanlarına ayırır ve her parçayı, bir örnek alanının eşlik bitindeki gizli mesajdan kodlar. Faz kodlaması, ses steganografisi için gürültüye neden olan stratejilerin eksikliğini giderir. Faz kodlaması, sesin evrelerinin kargaşa gibi göründüğü kadar insan kulağına duyulma biçimini kullanmaz. Bu prosedür mesaj bitlerini bilgisayarlı bir sinyalin faz aralığında faz kaymaları olarak kodlar ve gürültü oranını tespit etmek için sinyaller açısından belirsiz bir kodlama gerçekleştirir (Cvejic, 2002:336). Temel yayılma spektrumu (SS) tekniği, gizli verileri mümkün olduğunca ses sinyali frekans spektrumu üzerine yaymaya çalışır (Gopalan, 2003:74).

Bilgiyi gizleme süreci bilgisayar tabanlı ses steganografi sistemidir, gizli mesajlar dijital sese gömülüdür (Katzenbeisser, 2000:77). Burada bir mesaj, bir ses dosyasının ikili dizisindeki basit bir değişiklik modunda gizlenir. Mevcut sistem mesajları AU, Wav, Mp3 vb. Birçok dosya şeklinde gizleyebilir (Hariri vd., 2011:191). Bu işlemi kullanarak mesajın gizlenmesi, mesajı dijital görüntü gibi başka bir ortam kullanarak gizlemekten nispeten daha zordur. Bu yöntemdeki bilgileri gizlemek amacıyla kullanılan çeşitli teknikler ve yöntemler vardır, bu yöntemler basitten en zoruna kadar değişir, bu da bilgiyi ses dosyasında bir gürültü modelinde gizler, ancak aynı zamanda sofistike yöntemler de vardır. Bu yöntemler, basitlik ve karmaşıklık boyutundan sadece ses dosyasındaki metni gürültü biçiminde gizlemekle kalmaz, aynı zamanda bilgi teknolojilerini gizlemek için gelişmiş sinyal işleme üzerinde daha doğru çalışma konusunda sofistike yöntemler de vardır. Aşağıda, ses steganografisi nedeniyle yaygın olarak seçilen yolların bir listesi bulunmaktadır (Jayaram, 2011:86):

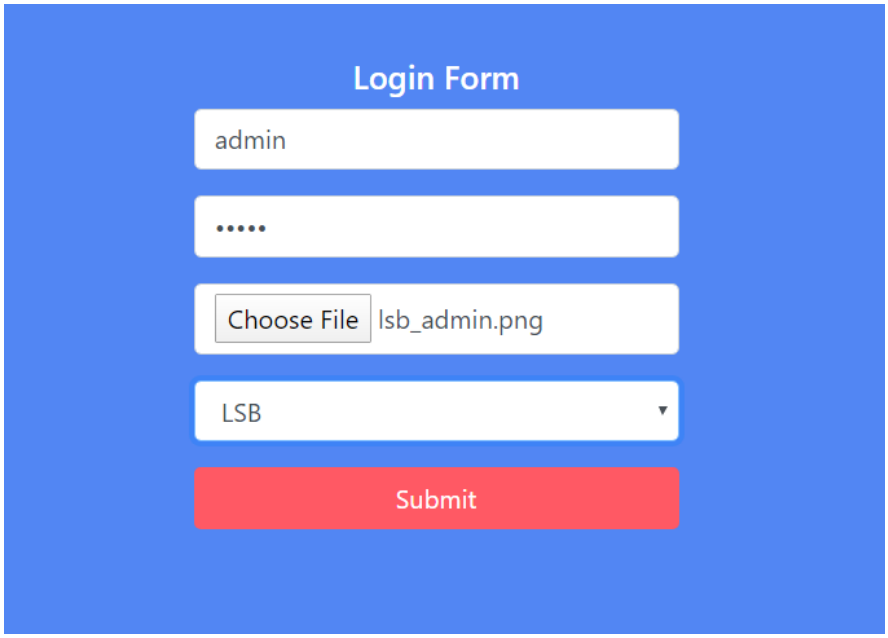
- Düşük bit kodlaması: Bu prosedür, fotoğraflarda genellikle uygulanan LSB ile aynıdır. Bu yaklaşım genellikle insan kulağı tarafından not edilir, bu nedenle kullanımı risklidir.
- Spektrum spektrumu: Bu yöntem bilgi sinyaline rastgele bir ses eklemek için çalışır ve bu ses spektrumun her tarafına yayılır.
- Yankı verileri gizleme: Bu yöntem ses dosyalarındaki yankıları kullanır ve bu yankıya ekstra ses ekler.

- Diferansiyel faz varyasyonu: Bu yöntemde, dosya gömülü mesaj kullanılarak bloklara dağıtılır.

6. UYGULAMA

6.1 Deney Kurulumu ve Yöntem

Standart uygulamalarda kullanıcı girişi zamanı kullanıcı ismi ve şifre kullanılarak veritabanında bilgiler kontrol edilip daha sonra sisteme giriş izni veriliyor. Bu sistemi daha güvenli hale getirmek için Django/Python üzerinden bir giriş sistemi hazırladık. Steganografi kullanılarak yapılan bu kullanıcı girişi panelinde sisteme giriş için kullanıcı ismi, şifrenin yanı sıra daha önceden kaydı yapılan kullanıcı için steganografi algoritmaları kullanılarak şifrelenen resim de yüklenmesi gerek. Resim uygulamanın kullanım tarzına göre daha önceden şifrelenmiş halde kullanıcıya mail ve ya dosya transfer yoluyla gönderile bilir. Ya da kayıt esnasında yine bu steganografi algoritmaları kullanılarak şifrelenip direk kullanıcının bilgisayarına indirile bilir. Elimizde bulanan kullanıcı ismi , şifre ve resimle birlikte sisteme giriş sağlanması mümkün. Sistem bir web uygulama ve giriş panelinden oluşuyor (Şekil 6.1). Kodlar Ek 1-de verilmiştir.



Şekil 6.1: Kullanıcı Giriş Paneli

Uygulamada 3 algoritmayı karşılaştırarak en hızlı ve psnr değeri en yüksek olan algoritmayı seçiyoruz. Bu çalışmada LSB, DCT ve BPCS algoritmalarını

kullanıyoruz. Resimlerin içinde şifreleri saklamadan önce onları Kriptografi algoritmalarından sha256 ile şifreliyoruz. Kullandığımız gizli anahtar, kullanıcının kayıt zamanı belirtdiği şifrenin sha256 vasıtasıyla şifrelenmiş halının ilk 30 karakteridir. Gizli anahtarı oluşturdukdan sonra aynı resmi 3 algoritmayı da ayrı ayrı kullanarak saklıyoruz. Sonuçta elimizde 3 steganografi kullanılarak içerisine gizli anahtar saklanmış 3 resim oluyor (Şekil 6.2).

Orjinal **LSB** **DCT** **BPCS**

Şekil 6.2: Şifrelenmiş Resimler

Uygulamaya giriş yapmak için kullanıcı ismi, şifre ve resmi gerekli bölümlere girip, algoritmamızı seçiyoruz ve giriş butonuna basıyourz (Şekil 6.2).

Arka kısma giden sorguda öncelikle seçilmiş algoritma belirleniyor, daha sonra aynı algoritma kullanılarak kullanıcı tarafından yüklenmiş resmin şifresi çözülüyor ve gizli anahtar daha önceden belirlenmiş değişkene atanıyor. Eğer resim şifrelenmemişse ve ya elde edilen gizli anahtar boşsa hata sayfasına yönlendiriliyor ve şifre yanlıştır hatası kullanıcıya gösteriliyor (Şekil 6.3).

Şekil 6.3: Hata Ekranı

Resimdeki gizli anahtar alındıktan sonra şifre yeniden sha256 algoritması ile özeti çıkarılıyor ve ilk 30 karakteri alınıp daha önceden değişkene atadığımız gizli anahtarla karşılaştırılıyor. Bu kısımda başarıyla tamamlanırsa veritabanından kullanıcın bilgileri sorgulanıyor, kullanıcı varsa veritabanındakı şifre ile kullanıcının girdiği şifrenin hash

edilmiş versiyonu karşılaştırılıyor. Tüm bu adımlar başarı ile bitdikden sonra sisteme giriş izni veriliyor. Kullanıcı bulunmadıkda ve ya şifreler aynı olmadıkda yine hata ekranına yönlendiriliyor.

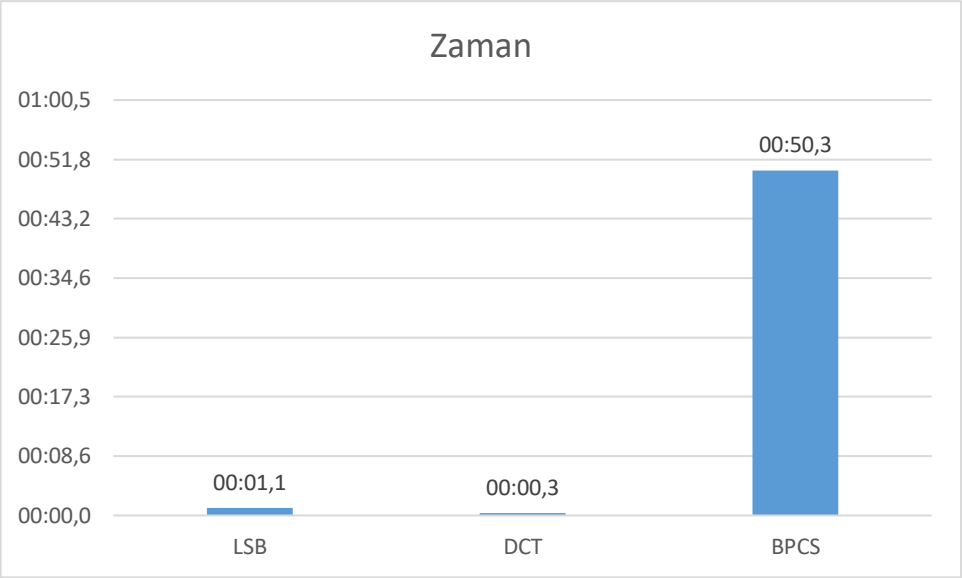
Burada steganografi kullanılmasının amacı brute force atakların karşısının alınmasıdır. Ayrıca vertibana daha az sorgu gitmesi ve veritabanı hekleme riskini azaltmaya hesaplanmıştır.

Uygulamada kullanılan her 3 algoritma için hız ve psnr değerleri ölçülmüştür. Hız testleri zamanı python data kütüphanesi, psnr değeri içinse numpy kütüphanesi kullanılarak orjinal ve encode olunmuş resim arasındakı fark ölçümlenmiştir (Şekil 6.4). Her algoritma için birden fazla kez denenmiş ortalama zaman ve psnr değeri alınmıştır. Buradakı farklılıklar sunucu ve internet hızına bağlı olarak değişe bilir.

Şekil 6.4: LSB Zaman ve Psnr Değer Ölçümü

6.2 Bulgular ve Değerlendirme

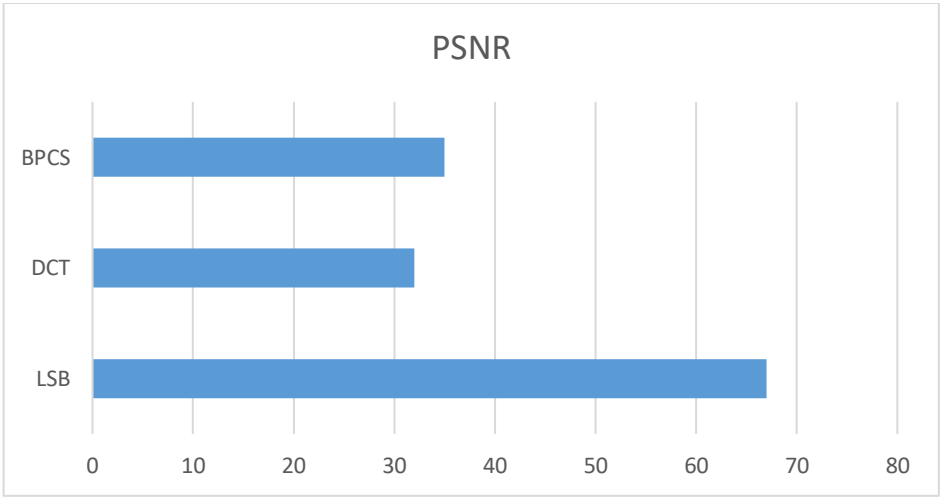
Sonuç olarak yapılan uygulamada algoritmalar hız ve psnr değerine göre değerlendirildi. Zaman giriş butonuna basıldığıdan tüm proseduran bitimine kadar olan zamanı kapsıyor. Hız kıyaslamasında DCT 1 saniyenin altında gösterici ile en başarılı algoritma oluyor. LSB 1 saniyeden fazla , BPCS 50 saniyeden fazla sürede prosedürü tamamlıyor (Şekil 6.5).



Şekil 6.5: Steganografi Algoritmalarının Zaman Kıyaslaması

Algoritma hızının yanı sıra resmin orijinallığını korumasıda gerek ki, daha önceden şifrelendiği fazla belli olmasın. Resmin değeri Tepe sinyal-gürültü - PSNR oranı ile ölçülüyor. Yüksek PSNR değeri, yüksek kalite demektir (Mehra, 2016:172).

Kullandığımız algoritmalar sırasında en iyi değerler LSB algoritmasında bulundu. Ortalama olarak 70-e yakın bir değere sahib bu resimlerde gözle görülür de bir deformasyon bulunmuyor. DCT ve BPCS algoritmalarının değerleri yakın olsa da DCT resmi daha fazla deformasyona uğratıyor ve resmin çıplak gözle bile modifiye edildiği belli oluyor. BPCS algoritmasında deformasyon değerleri falza olmasa da, hız konusunda diğerlerinden çok geri kalıyor (Şekil 6.6).



Şekil 6.6: Steganografi Algoritmalarının PSNR Değerleri Kıyaslaması

7. SONUÇ

Web Uygulamalarda hız günümüzde en önemli konulardan biridir. İnternet hızının her geçen gün artdığı dünyaya, uygulamalar ayak uydurmaya çalışıyor.

Uygulamada ölçtüğümüz değerlere göre DCT en hız algoritma ünvanını alıyor fakat köçü çıkan PSNR değerleri algoritmanın güvenliğini risk altına aldığı için kullanışlı sayılmıyor. BPCS algoritmasının PSNR değerleri DCT-den iyi olsa da hız konusunda onların çok gerisinde kalıyor, ölüşmüş 50 defalık bir zaman farkı bu algoritmayı da kullanışlı yapmıyor. Son olarak LSB algoritması az farkla DCT-den zayıf olsa da, PSNR değeri çok yüksek olduğu için riski azaltıyor. Yaptığımız değerlendirmeler sonucu Web Uygulama giriş sisteminde LSB algoritmasını kullanmak hız bakımından çok kullanışlı ve gizli anahtarın bulunma riskini azaltıyor (Grafik 1, Grafik 2).

KAYNAKLAR

Agarwal M. (2013). Text Steganographic Approaches: A Comparison. *International Journal of Network Security & Its Applications (IJNSA),* Vol.5, No.1. pp.91-106.

Akhtar N., S. Khan and P. Johri, (2014) "An Improved Inverted LSB Image Steganography", *IEEE International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT),* Feb. 2014, pp. 749-755.

Al- Ethawi, G. and A. Salman, (2002) "Text hiding in image border" , Dean of the Military College of Engineering, *MSc thesis.*

Baby, D., J. Thomas, G. Augustine, E. George, and N.R. Michael, (2015) " A Novel DWT based Image Securing method using Steganography", *International Conference on Information and Communication Technologies (ICICT), Procedia Computer Science,* April 2015, pp. 612-618.

Backes, M., Pfitzmann, B. and Waidner, M. (2007) The reactive simulatability (RSIM) framework for asynchronous systems. Information and Computation 205(12), 1685–1720

Badr, S. M., Ismaial, G. and Khalil, A. H. (2014). A Review on Steganalysis Techniques: From Image Format Point of View. International Journal of Computer Applications, 102(4), 11-19.

Bender, W, W. Butera, D. Gruhl, R. Hwang, F. J. Paiz and S. Pogreb, (2000) "Techniques for data hiding", *IBM Systems Journal,* Volume 39, pp. 547 – 568, Issue 3-4.

Brassil, Jack T., Steven Low, Nicholas, F. Maxemchuk, and Lawrence, O. Gorman (1995) "Electronic marking and identification techniques to discourage document copying." *Selected Areas in Communications, IEEE Journal* on 13, no. 8: 1495-1504.

Brodney, A. and Asher, J. (2009) *Tales of the Encrypted [home page on the Internet]*. Team 28005

Chapman, Mark, George I. Davida, and Marc Rennhard. (2001) A practical and effective approach to large-scale automated linguistic steganography." In Information Security, pp. 156-165. *Springer Berlin Heidelberg*.

Charles P. (2004) *Pfleeger, Shari Lawrence Pfleeger. "Security in computing"* Pearson Education 642-666.

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

Cvejic & T. Seppanen. (2002) Increasing the capacity of LSB-based audio steganography. *IEEE Workshop on Multimedia Signal Processing* (pp. 336-338).

Dagar, E. and S. Dagar, (2014) LSB based Image Steganography using X-Box Mapping", *IEEE International Conference on Advances in Computing, Communications and Informatics (ICACCI),* Sept. 2014, pp. 351-355.

Denslin, D.R. and Brabin, Dr. V. Sadasivam, (2017) *QET Based Steganography Technique for JPEG Images.*

Desai, M. B. and Patel, S. V. (2016). Performance analysis of image steganalysis against message size,message type and classification methods. International Conference on Advances in Electronics, Communication and Computer Technology (ICAECCT), 295-302.

Deshmukh P.U. and T.M. Pattewar, (2014) "A Novel Approach for Edge Adaptive Steganography on LSB Insertion Technique" *IEEE International Conference on Information Communication and Embedded Systems (ICICES),* Feb. 2014, pp. 1-5.

Diffie, W. and Hellman, M. (1976) *New Directions in Cryptography.* Stanford University.

Dragos Trinica, (2006) "Sequential and Parallel Cascaded Convolution Encryption with Local Propagation: Toward future Directions in Cryptography", *Proceedings of The third International Conference on information Technology-New Generations. (ITNG'06), 0- 7695-2497- 4 / IEEE Computer Society.*

Feng, B. W. Lu, and W. Sun, (2015) "Secure Binary Image Steganography Based on Minimizing the Distortion on the Texture", *IEEE transactions on Information Forensics and Security,* Feb. 2015.

Fridrich & Du. Rui. (1999) Secure steganographic methods for palette images. *International Workshop on Information Hiding.* Springer, Berlin, Heidelberg.

Garg, M. (2011). A Novel Text Steganography Technique Based on Html Documents. *International Journal of Advanced Science and Technology.* Vol. 35, pp.129-138.

Geetha, S. and Kamaraj, N. (2010). Optimized image steganalysis through feature selection using MBEGA. *International Journal of Computer Networks & Communications (IJCNC),* 2(4), 161-175.

Gopalan. (2003), Audio steganography using bit modification. *ICME'03. Proceedings of International Conference on Multimedia and Expo.*

Hariri, Mehdi, Ronak Karimi, and Masoud Nosrati. (2011) "An introduction to steganography methods." *World Applied Programming* 1, no. 3 : 191-195

Jayaram, H.R. Ranganatha & H.S. Anupama. (2011).Information hiding using audio steganography–a survey. *The International Journal of Multimedia & Its Applications (IJMA)* Vol, 3, 86-96

Jenifer, K.S., G. Yogaraj. & K. Rajalakshmi. (2014) LSB approach for video Steganography to embed images. International Journal of Computer Science and Information Technologies, 5(1), 319-322.

Johnson, N. F. and S. Jajodia, (1998)"Exploring Steganography: Seeing the Unseen," *IEEE, Computer,* vol. 31, no. 2, pp. 313 - 336.

Jones, A Z. (2009) What Is a Quantum Computer?.About.com-Physics http://physics. about.com/od/quantumphysics/f/quantumcomp.htm. 10.02.2020

Jose, J. Amador and Robert W. Green, (2005) "Symmetric-key Block Ciphers for Image and Text Cryptography" , *International Journal of imaging System Technology,* Vol. 15 - pp. 178-188.

Kahn, D. (1996) The Codebreakers: The Story of Secret Writing. *Scribner*; 1996. 11-81 p.

Kang, L.C. (2011). *steganalysis of binaryimages*. Department of Computing Faculty of Science, Macquarie University Australia, 1-160.

Katzenbeisser S. and F. Petitcolas. (2000) *Information hiding techniques for steganography and digital watermarking*. Artech house.

Khodaei & K. Faez (2012) New adaptive steganographic method using leastsignificant-bit substitution and pixel-value differencing. *IET Image processing,* 6(6), 677-686.

Knuth D E. (1981) *The Art of Computer Programming: Semi-numerical Algorithms. Addison-Wesley.*

Kumar K. A., Pabboju S. and Desai N. M. (2014). Advance Text Steganography Algorithms: An Overview. *International Journal of Research and Applications,* 1(1): pp.31-35.

Liu, Yu-Chi, Hsien-Chu Wu, & Yu. Shyr-Shen. (2011)Adaptive DE-based reversible steganographic technique using bilinear interpolation and simplified location map. *Multimedia Tools and Applications* 52.2-3 : 263-276.

Maurer, U. (2010) Constructive cryptography—A primer. In: Sion, R., Curtmola, R., Dietrich, S., Kiayias, A., Miret, J.M., Sako, K., Seb´e, F. (eds.) FCDS 2010. *LNCS,* vol. 6054, p. 1. Springer-Verlag

Merkle R C. (1982) *Secrecy, Authentication, and Public Key Systems.* UMI Research Press.

Modi M. R., S. Islam and P. Gupta, (2013) "Edge Based Steganography on Colored Images", *9th International Conference on Intelligent Computing (ICIC),* July 2013, pp. 593- 600

Moerland T. (2002). Steganography and steganalysis, *Leiden Institute of Advanced Computing Science,* www.liacs.nl/home/tmoerl/privtech.pdf

Morkel T., J.H. Eloff & M.S. Olivier. (2005) *An overview of image steganography. In ISSA* (pp. 1-11).

Nag A. , J.P. Singh, S. Biswas, D. Sarkar, and P.P. Sarkar, (2004) "A Huffman Code Based Image Steganography Technique", *1st International Conference on Applied Algorithm (ICAA),* Jan. 2014, pp. 257 265.

Nusrati M., A. Hanani and R. Karimi, (2015) "Steganography in Image Segments Using Genetic Algorithm", *5th IEEE International Conference on Advanced Computing & Communication Technologies (ACCT),* Feb 2015, pp. 102 107

Petitcolas, F. A., P. R. J. Anderson and M. G. Kuhn, (1999) "Information Hiding - A Survey," *Proceedings of the IEEE*, vol. 87, no. 7, pp. 1062 - 1078.

Pevný, T. (2008). *Kernel methods in steganalysis.* State University of New York at Binghamton,Thomas J. Watson School of Engineering and Applied Science, Department of Computer Science., 1-128.

Por L. Y. and B. Delina. (2008) Information hiding: A new approach in text steganography. Proceedings. WSEAS International Conference oMathematics and Computers in Science and Engineering (No. 7). *World Scientific and Engineering Academy and Society.*

Prashanti G. and K. Sandhyarani, (2015) "A New Approach for Data Hiding with LSB Steganography", *Emerging ICT for Bridging the Future - Proceedings of the 49th Annual Convention of the ComputerSociety of India CSI,* Springer 2015, pp. 423-430.

Qazanfari K. and R. Safabakhsh, (2014) "A new Steganography Method which Preserves Histogram: Generalization of LSB++", *Elsevier International Journal of Information Sciences,* Sept. 2014, pp. 90-101.

Qing X. , X. Jianquan and X. Yunhua., (2010) "A High Capacity Information Hiding Algorithm in Color Image", *Proceedings of 2nd IEEE International Conference on E-Business and Information System Security,* May 2010, pp. 1-4.

Raja K.B., C.R.Chowdary, Venugopal K.R. and L.M.Patnaik, (2013) *"A Secure Image Steganography using LSB, DCT and Compression Techniques on Raw Images".*

Ramalingam, M. (2011) Stego machine–video steganography using modified LSB algorithm. *World Academy of Science, Engineering and Technology*, 74, 502- 505. 2011.

Rhoads, B. Geoffrey. (2000) Video steganography. *U.S. Patent* 6,026,193, issued February 15, .

Robert K. (2004) *Steganography and steganalysis,* http://www.krenn.nl/univ/cry/ steg/ article.pdf, January .

Sachdeva S. and A. Kumar, (2012) "Colour Image Steganography Based on Modified Quantization Table", *Proceedings of IEEE 2nd International Conference on Advanced Computing & Communication Technologies,* Jan. 2012, pp. 309-313.

Sadek M., A.S. Khalifa & M.G. Mostafa. (2015) Video steganography: a comprehensive review. *Multimedia tools and applications,* 74(17), 7063-7094.

Samidha D. and D. Agrawal, (2013) "Random Image Steganography in Spatial Domain" *IEEE International Conference on Emerging Trends in VLSI, Embedded System, Nano Electronics and Telecommunication System (ICEVENT),* Jan. 2013, pp. 1-3.

Sharma & U. Kumar. (2015) Review of Transform Domain Techniques for Image Steganography. *International Journal of Science and Research,* 2(2), 1.

Shirali-Shahreza M. (2008). Text steganography by changing words spelling. *IEEE, 10th International Conference on Advanced Communication Technology. (Vol. 3, pp. 1912-1913).*

Singh, Hitesh, Pradeep Kumar Singh, and Kriti Saroha. (2009) "A survey on text based steganography." *In Proceedings of the 3rd National Conference,* pp. 26-27.

Singh, R.K. Aggrawal. (2010) Enhancement of LSB based Steganography for Hiding Image in Audio, *International Journal on Computer Science and Engineering,* Vol. 02, No. 05,

Smitha G. L. and E. Baburaj, (2016) A Survey on Image Steganography Based on Least Significant Bit Matched Revisited (LSBMR) Algorithm, *in International Conference on Emerging Technological Trends (ICETT).*

Stallings William (2002) , *"Cryptography and Network Security",* Fourth Edition, Prentice-Hall -pp.80-81.

Stallings William, (2004) *"Network Security Essentials* (Applications and Standards)" Pearson Education, pp.2-80

Stuti Goel, Arun Rana & Manpreet Kaur, (2013) "A Review of Comparison Techniques of Image Steganography", *Global Journal of Computer Science and Technology,* Volume XIII Issue IV Version I, , pp. 8-14.

Vleeschouwer, J. Delaigle & B. Macq, (2001) Circular Interpretation on Histogra for Reversible Watermarking, in Proceedings of *the 4th IEEE International Workshop on Multimedia Signal Processing,* Cannes, pp. 345-350.

Wang, N.-I. Wu, C.-S. Tsai, and M.-S. Hwang, (2008) "A high-quality steganographic method with pixel value differencing and modulus function," Journal of Systems and Software, vol. 81, pp. 150-158.

Xianhua Song, Shen Wang and Xiamu Niu, (2016) “An Integer DCT and Affine Transformation Based Image Steganography Method”, *Eighth International Conference on Intelligent Information Hiding*

Yang H. , X. Sun and G. Sun, (2009) “A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution”, *Journal of Radio Engineering*, Vol. 18, No. 4, pp. 509-516.

EKLER

Ek 1

```
class LoginView(View):
    template_name = 'login.html'

    def get(self, request):
        return render(request, self.template_name)

    def post(self, request):
        start_time = datetime.now()
        username = request.POST.get('username', None)
        password = request.POST.get('password', None)
        myfile = request.FILES['myfile']
        fs = FileSystemStorage()
        filename = fs.save(myfile.name, myfile)
        uploaded_file_url = fs.url(filename)

        algo = request.POST.get('algo', None)
        if not algo:
            return HttpResponse('You did not select algorithm!')

        hash_algo = 'pbkdf2_sha256'
        salt = 'stego'
        custom_password = make_password(password, salt=salt, hasher=hash_algo)
        custom_password = custom_password.split('$')[3][:30]

        decoded_password = None
        psnr_value = 0
        if algo and int(algo) == 1:
            # encode_lcb(custom_password, username)
            decoded_password, psnr_value = decode_lcb(uploaded_file_url)
        elif algo and int(algo) == 2:
            # encode_dct(custom_password, username)
            decoded_password, psnr_value = decode_dct(uploaded_file_url)
        elif algo and int(algo) == 3:
            # encode_bpcs_new(custom_password, username)
            decoded_password, psnr_value = decode_bpcs_new(uploaded_file_url)

        if decoded_password and decoded_password == custom_password:
            try:
                user = User.objects.get(username=username)
            except ObjectDoesNotExist:
                user = None
            if user and user.check_password(password):
                end_time = datetime.now()
                messages.success(request, f'You successfully logged in! Time taken {end_time - start_time}. '
                                          f'PSNR value {psnr_value}')
                return render(request, 'success.html')
            messages.error(request, 'Username is wrong!')
            return render(request, 'error.html')
        messages.error(request, 'Password is wrong!')
        return render(request, 'error.html')
```

ÖZGEÇMİŞ

Ad -Soyad: Toghrul Valibayli

Doğum Tarihi ve Yeri: 1994, Azerbaycan

E-Posta: togrul.velibeyli@gmail.com

ÖĞRENİM DURUMU:

- **Lisans:** 2015, Azerbaycan Devlet Kültür ve Güzel Sanatlar Üniversitesi, Müzecilik
- **Yüksek Lisans:** 2020, İstanbul Aydın Üniversitesi, Bilgisayar Mühendisliği

ÇALIŞMA DURUMU:

- **2019 - Günümüz:** Yazılım Uzmanı, "Bank Respublika" OJSC, Azerbaycan
- **2019- 2019:** Yazılım Uzmanı, Spechy, İstanbul
- **2018 – 2019:** Yazılım Uzmanı, ES SA İnternet Hizmetleri, İstanbul

YABANCI DİLLER:

- **İngilizce**
- **Rusça**
- **Türkçe**
- **Azerbaycan dili (Ana dil)**