

STEGANOGRAFİ
NEDİR NASIL ÇALIŞIR ve ARAÇLARI

- İstanbul Şehir Üniversitesi -

Bilgi Güvenliği Mühendisliği Yüksek Lisans Programı Bilgisayar Adli Analizi Dersi

NOT: Eğitmenlerimizden Huzeyfe Önal'ın İstanbul Şehir Üniversitesi 2016 bahar döneminde Yüksek Lisans Programı Adli Bilişim Dersi öğrencileri tarafından hazırlanmıştır.

Hazırlayan: Selim ÖZCAN

Tarih: 29.05.2016

[STEGANOGRAFİ NEDİR NASIL ÇALIŞIR ve ARAÇLARİ]

ÖZET

Steganografi'nin tanımı, tarihi, ilk kullanım yöntemleri ve günümüzdeki kullanım yöntemleri ile faydalanıldığı alanlar incelenmiştir.

You can search and search, but when you've found nothing you can only conclude: Maybe I didn't look hard enough, but maybe there is nothing to find. (Clair, 2001)
(İstediğin kadar ara, birşey bulamadığında şöyle düşüneceksin: Ya ben yeteri kadar bakmadım ya da bulacak birşey yoktu.)

1. GİRİŞ

Steganografi, İngilizce "Steganography" adında ve Yunanca "Steganos" ve "Graphein" kelimelerinden oluşmaktadır. "Steganos", gizlenmiş, örtülü ve korunmuş anlamlarına ve "Graphein" ise yazı anlamına göre çevrilebilir. Sonuç olarak, steganografi "Gizli-Gizlenmiş Yazı" manasında Türkçe "Veri Gizleme" olarak düşünülebilir.

Güvenli haberleşme, iletişim, bilgi iletimi gibi konularda "Güvenlik, gizlilik, mahremiyet, veri bütünlüğü, erişilebilirlik" gibi bilgi güvenliği kavramlarını sağlamak adına yaygın olarak bilinen iki yol mevcuttur. İlki kriptografi ve diğeri steganografi yani veri gizleme yöntemleridir. Her ikisinde de amaç bilginin sadece gönderen ve alan taraflar dışında başka üçüncü kişilerin öğrenememesinin sağlanmasıdır. Buna göre iki dalda da değişik metotlar, araçlar ve kavramlar kullanılmıştır ve geliştirilmektedir. Kriptografi iki taraf arasındaki iletişimi özel, mahrem (privacy) olarak ele alırken, Steganografi iletişimin gizliliğine (secrecy) yönelir.

Kriptografinin yolu ve yöntemi, bilgiyi matematiksel hesaplamalar sonucunda üretilen değerler ile okuyan ve inceleyen kişinin anlayamayacağı şekilde dönüştürme işlemidir. Üçüncü kişiler ele geçirdikleri mesajı ilk hali ile anlamlandıramazlar çünkü mesaj karıştırılmıştır. Mesajın çözümlenmesi gerekir ve çözümleme işlemi ayrı bir zaman ve çaba harcanmasını zorunlu kılar. Kriptografinin ana düşüncesi, gönderilen mesaja üçüncü kişilerin ulaşması durumunda çözmelerini olabildiğince zorlaştırmak mümkünse orijinal mesajı anlamalarını engellemektir.

Diğer dal olan Steganografi de ise amaç mesajı dönüştürerek önlem almak değil, mesajın varlığını tamamen gizleyerek göndermektir. Birçok yöntemler ve kullanılan araçlar mevcuttur. Mesaj bir taşıyıcıya dikkat çekmeyecek şekilde gizlenerek gönderilir. Kriptografi de mesaj her ne kadar şifrelense de görünür haldedir ve tarafların ilgisini, dikkatini çeker, analiz edilebilir ve şifrelemenin çözülmesini teşvik eder. Üçüncü kişiler taşıyıcıya ulaştıklarında mesaja dair bir iz fark edemeyeceklerinden ellerinde mesajın olup olmadığını anlayamazlar ve mesajı

öğrenmeleri engellenmiş olur. Yukarıda bahsedilen şekilde, Markus Kuhn steganografinin tanımını aşağıdaki şekilde yapmaktadır:

> *"Steganography is the art and science of communicating in a way which hides the existence of the communication. In contrast to cryptography, where the "enemy" is allowed to detect, intercept and modify messages without being able to violate certain security premises guaranteed by a cryptosystem, the goal of steganography is to hide messages inside other "harmless" messages in a way that does not allow any "enemy" to even detect that there is a second secret message present."* (Kuhn, 1995)

2. STEGANOGRAFİ TARİHİ

Tarih boyunca steganografi tekniklerinin birçok alanda kullanıldığı düşünülmektedir, ulaşılan yazılı kaynaklara göre bilinmektedir. Savaş öncesi hazırlıklarda, savaşlarda, politik ve diplomatik görüşmelerde, istihbari faaliyetlerde (espionage), hapislerden kaçışlarda, isyanlarda ve hazırlıklarında steganografi teknikleri kullanılabilir, kullanılmıştır.

MÖ 5. Yüzyılda Eski Yunan tarihlerinde anlatılanlar steganografiye ilk örnekler olarak sayılabilir. Yazılı olarak sayılabilecek ilk kaynak Eski Yunan tarihçisi ve yazar Heredot (Herodotus, MÖ 484 - MÖ 425), Herodot Tarihi (Histories) adlı eserinde steganografinin kullanıldığı iki olaydan bahseder. O yıllarda Eski Yunan ve Pers imparatorluğu savaş halindedir ve Pers imparatorluğu bazı Yunan şehir devletlerini kontrolü altına almıştır. İlk olay olarak, Pers imparatorluğu Milet (Miletus) şehrini kontrol etmektedir ve yöneticilerinden Histiaeus (Histiaeus, tarih yok), bugünkü İran topraklarında bulunan Susa kentine gönderilmiştir. Yerine Aristagoras'ı (Aristagoras, tarih yok) Milet yönetimine bırakmıştır. Histiaeus Milet'e geri dönmek niyetindedir, bu amaçla Susa'dan steganografi ile gizli bir mesaj göndererek Aristagoras'dan isyan başlatmasını istemiştir. Mesajı sadık bir kölesinin saçlarını kazıtarak kafasına yazmıştır, saçları yeniden uzadığında köleyi Aristagoras'a göndererek mesajı dikkat çekmeden ulaştırmıştır.

Eski Yunan'da kullanılan bir başka yöntem ise, odundan yapılan balmumu tabletlerine yazı yazılırdı. Yazının üstü bir kez daha balmumu ile kaplandığında yazı gizlenir ve o şekilde gönderilirdi. Herodot'un kitabında bu şekilde gizli mesaj gönderilerek Pers İmparatorluğu'nun Eski Yunan'ı işgal edeceği haberinin ulaştırıldığı anlatılır.

Bir başka sayılabilecek yöntem olarak basit ve çok eskilerden İkinci Dünya Savaşı zamanlarına kadar kullanılan görünmez mürekkep (invisible ink) ile yazıların yazılmasıdır. Fransızlar Almanlara karşı direnirken kullanmışlardır. Her iki tarafta yeni görünmez mürekkep formülleri bulmak ve düşmanın tekniğini çözmek için birbirleri ile yarışmışlardır. 18. Yüzyıldaki Amerikan Devrimi zamanlarında haberleşmek için taraflar görünmez mürekkeplerden faydalanmışlardır. Görünmez mürekkep olarak bir çok sıvı kullanılabilmektedir. Limon suyu,

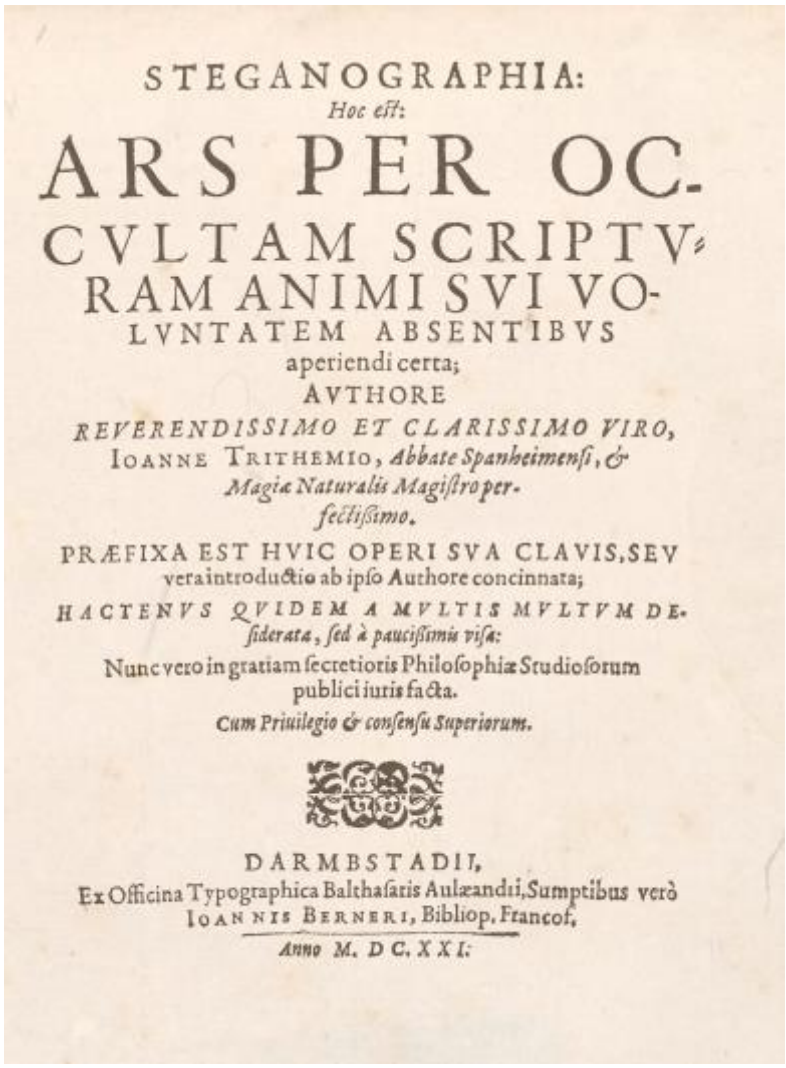
soğan suyu, süt, idrar, meyve suları ve sirke kullanılarak yazılan gizli yazılar ısıtıldıklarında koyulaşırlar ve gizli yazı ortaya çıkar. Resim 1 örnek bir görünmez mürekkep ile yazılmış gizli mesajın ısıtılarak ortaya çıkarılmasını göstermektedir. Günümüzde kullanılan görünmez mürekkepler, ultraviyole ışığı altında ortaya çıkmaktadır ve sahteciliğe karşı önlem olarak kullanılmaktadır.



Resim 1 Görünmez mürekkebin ısıtılması ile gizli mesajın açığa çıkartılması

15. ve 16. Yüzyıllarda Johannes Trithemius (1462 - 1516) Stegonagrafi (Stegonagraphia - 1499) adında bir kitap yazmıştır. İlk Steganografi teriminden bahsedilen kaynaklardandır. Gizli mesajların nasıl taşıyıcı metinlere gizlenebileceğine dair yöntemlerden bahsetmektedir. Resim 2 kitabın Latince kapağını (Steganographia, tarih yok) göstermektedir. Kitapta Aşağıda steganografi alanında tarih boyunca yazılan yazılar-incelemeler listelenmiştir (Petitcolas, tarih yok):

- *Hypnerotomachia poliphili, Anonymous, 1499*
- *Steganographia, Trithemius (1462-1516), 1499*
- *Steganographica, Gaspari Schotti, 1665*
- *Cryptology in the 15th and 16th century, T Leary, Cryptologia v. XX no. 3 (July 96) pp 223–242*
- *The Pigeon Post into Paris 1870-1871, J.D. Hayhurst O.B.E.*
- *Cryptographie militaire, Auguste Kerckhoffs, 1883*
- *A mathematical theory of communication systems, Claude E. Shannon Les Filigranes, Charles-Moïse Briquet, Geneva, 1907*
- *Solved: the Ciphers in Book III of Trithemius' Steganographia, J Reeds, Cryptologia v XXII no 4, October 1998, pp 291–318.*

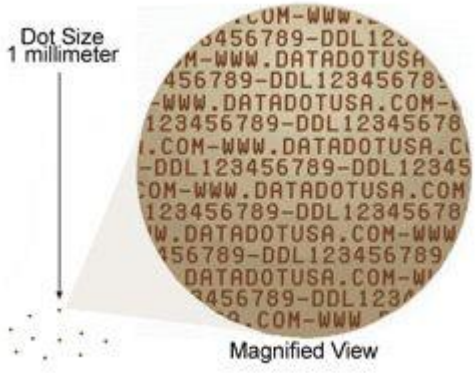


STEGANOGRAPHIA:
Hoc eſt:
ARS PER OC.
CVLTAM SCRIPTV-
RAM ANIMI SVI VO-
LVNTATEM ABSENTIBVS
aperiendi certa;
AVTHORE
REVERENDISSIMO ET CLARISSIMO VIRO,
IOANNE TRITHEMIO, Abbate Spanheimenſi, &
Magiæ Naturalis Magiſtro per-
fectiſſimo.
PRÆFIXA EST HVIC OPERI SVA CLAVIS, SEV
vera introductio ab ipſo Authore concinnata;
HACTENVS QVIDEM A MVLTIS MVLTVM DE-
ſiderata, ſed à paucißimis viſa:
Nunc vero in gratiam ſecretioris Philoſophiæ Studioſorum
publici iuris facta.
Cum Priuilegio & conſenſu Superiorum.

DARMBSTADII,
Ex Officina Typographica Balthaſaris Aulæandri, Sumptibus verò
IOANNIS BERNERI, Bibliop. Francof.
Anno M. DC. XXI.

Resim 2 Steganographia kitabının Latince kapağı

İkinci Dünya Savaşı zamanlarında birçok yeni teknik kullanılmıştır. Fotoğrafçılığın gelişmesi ile birlikte Almanlar "mikro noktalama" (microdots) tekniğini kullanmışlardır. Mikro noktalama tekniğinde yazılan mesaj fotoğraf teknikleri ile 200 kat ve üstünde küçültülüp bir nokta boyutuna getirilir ve dergi, gazete ya da herhangi bir taşıyıcı üzerine yerleştirilip gönderilir. Şifrelenmesi gerekmez, başarılı olmasının nedeni gönderilen mesajların gözle fark edilemeyecek kadar çok küçük olmasından dolayı kimsenin dikkatini çekmemesi. Resim 3'de (Mikro Noktalama, tarih yok) örnek bir mikro noktalama tekniği görülebilir. 1 nokta yaklaşık 1 milimetre boyutuna kadar küçültülebilmektedir ve içerisine büyük boyutlarda mesaj sığdırılabilmektedir. Sadece metin değil, aynı zamanda resim, harita, grafik gibi mesajlarda mikro noktalama ile gizlenerek gönderilmiştir. Mikro noktalama tekniğini FBI yöneticisi J. Edgar Hoover "the enemy's masterpiece of espionage" tanımlamıştır, yani "düşmanın casusluk için kullandığı en harika yöntemi" demek istemiştir.



Resim 3 Mikro Noktalama

İkinci Dünya Savaşı'nda kullanılan bir başka teknik ise Boş Şifreleme (Null Cipher)'dir. Bu yöntemin amacı hiçbir anlamı olmayan bir mesaja ki hava durumu, alışveriş listesi, günlük notları gibi herhangi bir konudan bahsedilebilir, gizli mesajın gizlenmesidir. Gizlenecek mesaj harf harf olarak sıralı tekrar eden bir şekilde taşıyıcı mesaja gizlenir. İkinci Dünya Savaşı zamanlarında birçok casus bu yöntem ile birçok bilgi iletilmiştir. Aşağıda bu tekniğe dair İngilizce dilinde örnekler verilmiştir.

Örnek 1:

"Fishing freshwater bends and saltwater coasts rewards anyone feeling stressed. Resourceful anglers usually find masterful leapers fun and admit swordfish rank overwhelming anyday."

Çözüm 1: Her bir kelimenin üçüncü harfi alınarak gizli mesaj çıkarılır.

"Send Lawyers, Guns, and Money."

Örnek 2: Bu örnek Amerika'da bulunan bir Nazi casusu tarafından gönderilmiştir. (Stego Örnek, tarih yok)

"Apparently neutral's protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by products, ejecting suets and vegetable oils."

Çözüm 2: Her bir kelimenin ikinci harfi alınarak gizli mesaj çıkarılır.

"Pershing sails from NY June 1"

İlk cümleden "Füzenin Newyork'tan Haziran 1'de denize açılacağını" anlamak oldukça zordur.

Örnek 3:

"***S**usan s**A**ys Ga**l**l **L**ies. M**A**tt le**T**s **S**usan f**E**el jo**V**ial. **E**lated (or) a**N**gry?"* (Null Cipher, tarih yok)

Çözüm 3: Her kelimenin harflerinden sıralı olarak (1, 2, 3,1,2,3...) alınırsa gizli mesaj çıkarılır.

Steganografi tarihinde bir başka gizli haberleşmenin kullanıldığı örnek ise Vietnam Savaşı zamanlarında Amerikan esirlerinin fotoğrafları çekilmiştir. Bu fotoğraflarda esirler çeşitli el hareketleri yaparak kendi ülkelerine gizli mesajlar ile haberleşme sağlamışlardır. Başka bir olayda, basın toplantısına çıkarılan esirlerin toplantı da gözlerini kapatıp açarak Mors alfabesinde "T-O-R-T-U-R-E" mesajını göndermeleri ve kendilerine işkence yapıldığını iletmeleridir.

2001 yılında Ron Howard'ın Akıl Oyunları (A Beautiful Mind) filminde, John Nash gazete ve dergilerde gizli mesajlar aramaktadır.

3. UYGULAMA ALANLARI

Dijital dünyanın gelişmesi ile birlikte steganografi de dijital dünyaya giriş yapmıştır. İnternetin gelişmesi ile birlikte yoğun bir bilgi akışı gerçekleşmektedir. Verilerin gizlilik içinde bir yerden başka bir yere taşınması fikri normal hayatta olduğu gibi bilgisayar aleminde de oldukça popüler bir hale gelmiştir. Öyle ki; New York ve Washington'a yapılan saldırılardan sonra da teröristlerin bazı popüler web sitelerinde bilgi saklı resimler kullanarak haberleştikleri iddia edilmiştir. Yazı, resim, ses, video dosyaları dünya üzerinde internet ile birlikte hem sıkıştırılmış olarak hem de sıkıştırılmamış olarak gönderilip alınmaktadır. Sıkıştırılan bilgiler de veri kaybı olan ve veri kaybı olmayan yöntemler bulunmaktadır. En çok kullanılan dosya uzantıları .bmp, .doc, .gif, .jpeg, .mp3, .txt, .png ve .wav resim, ses ve yazı dosya tipleridir.

Günümüzde birden fazla veri gizleme metodu bulunmaktadır. Bu yöntemler arasında en iyi en kötü ayrımı yapamayız, herbirinin diğerlerine göre kısıtlamaları ya da üstünlükleri bulunmaktadır. Steganografi bu dosya biçimlerinde (format) bulunan gereksiz (redundant) ve gürültülü (noisy) veri alanlarının silinip yerine gizli mesajın yerleştirilmesi ile yapılmaktadır.

Steganografinin bilgisayar dünyasında kullanımı başlıca 2 temel prensibe dayanır. İlki veri içine veri gömmek ve ikincisi ise görüntü veya ses dosyaları içine veri gizlemektir. Bunda yararlanılan başlıca prensiplerden bir tanesi; görüntü veya ses dosyalarının içeriklerinin, görüntüye ya da sese zarar vermeksizin bir dereceye kadar değiştirilebilmesidir. Yaygınca kullanılan diğer prensip ise insan duyularının görüntü, ses ya da renkte ufak değişiklikleri fark edememesidir.

Fabien A.P. Petitcolas (Petitcolas, Information Hiding: Techniques for Steganography and Digital Watermarking, 2000) bahsettiği gibi mükemmel bir sistemde normal bir taşıyıcı ile gizli mesajın gömüldüğü stego dosyasının istatistiksel desenlerinin ne insan gözü ile ne de bilgisayar analizi ile ayırt edilememesi gerekir.

Steganografik bir algoritma incelenirken 3 temel özelliğe dikkat edilmelidir:

- Değişimin fark edilememesi

Değişimin fark edilememesi ilkesi gereğince örtü veri (cover data) üzerinde yapılan değişiklikler insan duyuları tarafından algılanabilecek konumda olmamalıdır. Algılanması durumunda gizli iletişim ortaya çıkar ve üçüncü kişinin, içerisinde gizli veri olan dosya üzerinde çeşitli işlemler yapma olasılığı vardır.

- Saklanabilecek veri miktarı

Örtü veri içerisinde gizlenebilecek veri miktarı da önemli bir etkendir fakat veri miktarı artışı örtü veri üzerindeki değişimi insan gözüyle algılanabilecek konuma getirebilir. Bu da ilk iki ilke, değişim ve kapasite arasında bir ikilem yaratmaktadır.

- Dayanıklılık

Yine benzer biçimde gizlenen verinin yapılan saldırılar sonucunda bile, alıcı tarafından başarıyla ortaya çıkartılabilmesi için düşünülen dayanıklılığı arttırıcı önlemler, yapılması gereken işlem düzeyini arttırmakta ve dosya üzerinde yapılan değişim algılanabilecek seviyeye gelebilmektedir.

4. STEGANOGRAFİ TEKNİKLERİ

a. Gizli Mesajın Yazıya Gizlenmesi (Metin Steganografi - Text Steganography)

Steganografi örnekleri ilk olarak kağıt üzerinde yazılı metinlere gizlenerek yapıldığı düşünüldüğünde sayısal metinler üzerinde de bu işlem elbette ki gerçekleştirilebilir. Yazıya gizlemede en basit yöntem olarak her kelimenin ilk harfine gizlemektir. Yazının kullanılması bu aşamadan sonra farklı yöntemler ile daha çok gelişmiştir. Yazıya gizlenecek mesajın boyutu çok azdır ve kolaylıkla gizli mesaj ortaya çıkarılabilmektedir. Bunun nedeni taşıyıcı yazının içindeki gereksiz alanların ve boşlukların miktarının az olmasıdır. Örneğin:

After **T**he **T**heater, **A**ll **C**lients **K**eep **A** **T**ab **D**own **A**t **W**esley's **N**ook.

A T T A C K A T D A W N

(Mesaj kelimelerin ilk harfleri şeklinde kodlanmış)

b. Akrostiş(İlkleme):

Akrostiş bir şiirde dizelerin ilk harflerinin yukarıdan aşağıya doğru sıralandığında anlamlı bir sözcük meydana getirmesi olarak tanımlanabilir. Örneğin Edgar Alan Poe tarafından "An Acrostic" başlığıyla yazılmış bir şiir:

***E**lizabeth it is in vain you say*
*'**L**ove not' — thou sayest it in so sweet a way:*
***I**n vain those words from thee or L. E. L.*
***Z**antippe's talents had enforced so well:*
***A**h! if that language from thy heart arise,*
***B**reathe it less gently forth — and veil thine eyes.*
***E**ndymion, recollect, when Luna tried*
***T**o cure his love — was cured of all beside —*
***H**is folly — pride — and passion — for he died.*

Şiirde yeralan dizelerin ilk harfleri birleştirildiğinde "ELIZABETH" mesajının olduğu rahatlıkla görülebilir. Bu tip şiirler, aslında verilmek istenen mesajın gizlenmesinden çok, okuyan kişi tarafından fark edilmesi amacını gütmektedir. Ancak bu temelden hareketle metin içerisine daha komplike şekilde mesaj gizlendiğinde bu durum gizli yazı biliminin ilkelerine daha uygun hale gelebilecektir. Örneğin, bir paragraftaki her kelimenin ikinci harflerinin birleştirilmesi sonucu gizli mesajın elde edilmesi ya da şifrelenmiş bir metnin bir başka metne "akrostiş" uygulaması şeklinde yerleştirilmesi gibi.

c. Açık Alan (Open spaces) Yöntemleri

Bu yöntemler, anormal gözükmeyen iki kelime arasında extra boşluklar, satır sonu boşlukları ile çalışmaktadır. Bununla birlikte Açık Alan Yöntemlerinin ASCII kodları ile kullanılması daha uygundur.Açık alan yöntemleri de kendi içerisinde 5 farklı uygulama tipine sahiptir.

- Cümle içi boşluk bırakma (Word shifting)

Metinlerin sağa hizalanması da metin dosyalarında veri saklanmasında kullanılabilir. Kelimeler arasındaki boşluklar hesaplanıp kontrol edilerek, masum metin dosyalarına veri gizlenebilir. Kelimeler arasındaki tek boşluk "0"ı, çift boşluk "1"i temsil eder. Bu işlem işe yarar, ancak çok küçük bir veriyi saklamak için çok büyük veriye ihtiyaç duyar. Bununla birlikte bir çok kelime işleme programı da çift boşlukları otomatik olarak temizler.
Ancak bu yöntem, normal bir boşluk ile gizlenmiş bir boşluk arasındaki farkı anlamak imkansız olduğu için çözme işlemini zorlaştırır. Bu amaçla, Manchester kodlamasını temel olan başka bir teknik kullanılır. "01" "1" olarak, "10" "0" olarak yorumlanır. Bununla birlikte "00" ve "11" ise null boşluk bitlerini gösterir.

- Satır kaydırma Kodlaması (Line shifting method)

Bu yöntemde text satırları dikey olarak kaydırılarak gömülecek mesajın kodlanması sağlanır. Gömülmüş kelime yine text dosyası yada bitmap dosya olarak açılabilir. Örneğin, her satır 1/300 oranında aşağı ya da yukarı kaydırılması ile kodlama yapılabilir.

- Satır sonu boşluk bırakma

Satır sonu boşluğu yöntemi, her satırın sonundaki boşluktan faydalanır. Veri, tüm satır sonlarında daha önceden belirlenen sayıda boşluklar bırakarak gizlenir. Örneğin, iki boşluk bir bit, dört boşluk iki bit, sekiz boşluk dört bit vb. gizler. Bu yöntem, iç boşluk metodundan daha iyi çalışır çünkü satır sonundaki boşluk sayısı arttırılarak daha fazla veri gizlenebilir.

- Gelecek kodlaması

Bu yöntemde, "b, d, T" gibi harflerin yatay/düşey uzunlukları gibi bazı metin özelliklerini değiştirerek, biçimlendirilmiş metin içine gizli mesajları saklamayla ilgilenir. Bu yöntem, her biçimlenmiş metnin, gizli mesaj saklamak için kullanılabilecek çok sayıda özelliği olmasından dolayı, uzak ara durdurulması en zor yöntemdir.

- Yazımsal Yöntemler(Syntactic Methods)

Bu yöntem, dökümanı kodlamak için noktalama işaretlerini kullanır. Örneğin aşağıdaki iki cümle de ilk bakışta aynıymış gibi gözükmektedir, fakat dikkatlice bakıldığında ilk cümlenin fazladan bir ',' işareti içerdiği görülür. Bu yapıların biri "1", diğeride "0" olarak belirlenir ve kodlama işlemi bu şekilde yapılır.

"ekmek, yağ **,** ve süt"

"ekmek, yağ ve süt"

- Anlamsal Yöntemler (Semantic methods)

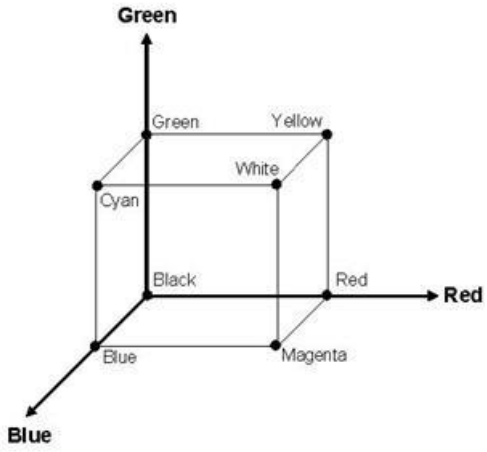
Bu yöntemde eşanlamlı kelimelere birincil ve ikincil değerler atanmaktadır. Sonra bu değerler "1" ve "0" olarak binary'e dönüştürülür. Örneğin "big" kelimesi birincil, "large" kelimesi de ikincil olarak işaretlenmiş olsun. Birincil "1", ikincil de "0" olarak binary'e çevrilir.

Bir diğer yaklaşım da şablon kullanılmasıdır. Bu şablonda daha önceden belirlenmiş yerler vardır ve gizlenmek istenen bilgi bu belirli yerlere yerleştirilerek gizleme işlemi yapılır. Alıcıda da şablon bilgisi olduğundan kelimeleri seçerek gizli bilgiyi elde edebilir.

d. Gizli Mesajın Resim Dosyasına Gizlenmesi(Görüntü Steganografi-Image Steganography)

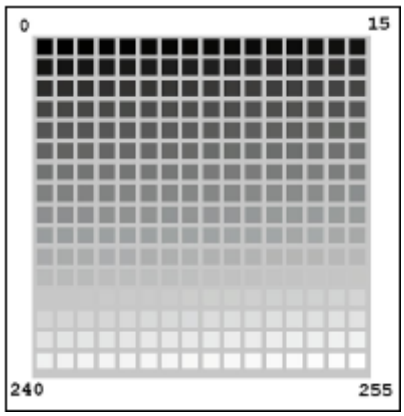
Bilgisayar ortamın resim her noktadaki ışık şiddetini temsil eden bir dizi sayıdır. Dijital resimler 24 bit veya 8 bit dosyalar olarak saklanırlar. Bir 24 bitlik resim bilgi saklamak için en fazla alnı sağlar ancak oldukça büyük olabilir (JPEG resimler hariç). Bütün renk değişimleri üç temel rengin birleştirilmesiyle elde edilir.

Basit dijital resim dosyasını ele alırsak, her temel renk 1 bayt ile gösterilir ve 24 bitlik bir resimde her piksel için renk değerini taşıyan 3 byte kullanılır. Resim 4, 24 bitlik bir resmin her bir pixel parçasının renk uzayında yerleşebileceği alanları göstermektedir.



Resim 4 24 Bit RGB (Red, Green, Blue) Renk Uzayı

Steganography uzmanları 256 gri tonlamalı resimlerin kullanımını önermektedir. Gri tonlamalı resimlerin tercih edilme sebebi koyuluğun her değer için çok küçük farklarla artmasıdır. Bu tip resimlerde palet içermektedir (Resim 5) ve palet değerlerindeki küçük değişimler gözün fark edemeyeceği kadar azdır. Bazı gri tonlamalı resimler 4 bitliktir ve 16 farklı gri ton içermektedirler. Bu yapıdaki resimlerde değişimler daha belirgin olmaktadır.

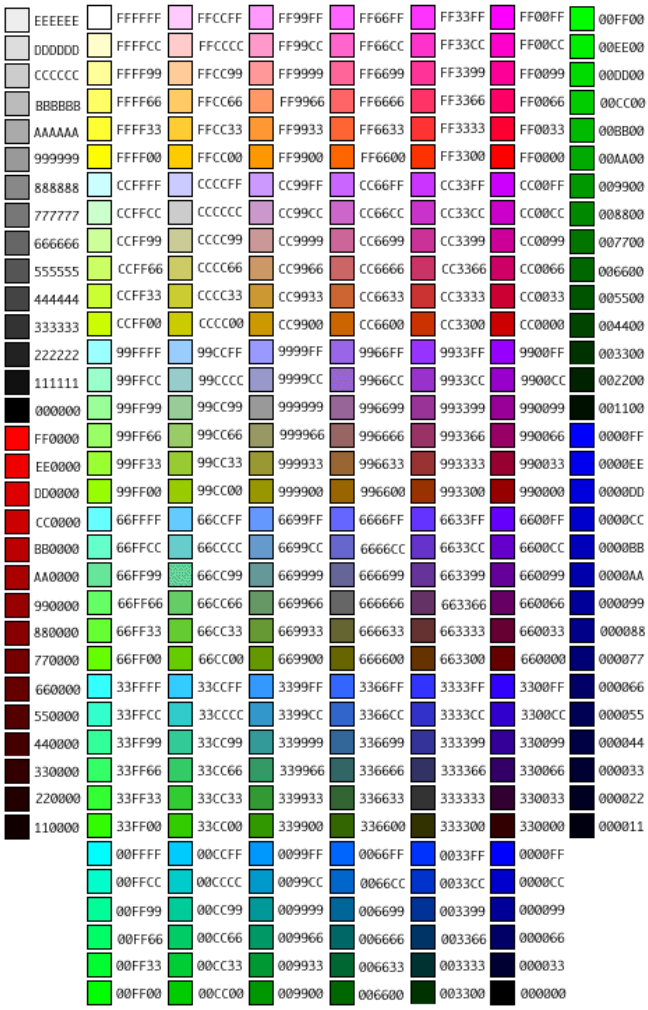


Resim 5 8-bit, 256 farklı gri tonlamalı resimlerin Renk Paleti (Johnson & Jajodia, 1998)

Fotoğraflardaki her pikselde, her bir 8 bit kırmızı, yeşil ve mavi rengi gösterecek şekilde 24 bitlik bir harita kullanılır. Sadece maviyi düşünecek olursak, 2^8 tane farklı mavi renk vardır diyebiliriz. 24 bitlik resimler 16,777,216 (2^{24}) eşsiz renk seçeneği sunar. (Johnson & Jajodia, 1998)

Resim dosyalarının tipik özelliklerini çok iyi kavramamız gerekir. Bunlar;

- Bütün resimler dosya başlığı (header) ve piksellerden oluşur.
- Her piksel sadece bir renk içeren/gösteren küçük bir bloktur.
- Her pikseldeki renk temel 3 rengin karışımından elde edilir.(Red,Green,Blue)
- Her pikselde bu 3 rengin verileri tutulur. Her temel renk 1 pikselde 1 byte (0...255) yer kaplar, yani 1 piksel 3 byte (R, G, B) veri taşır. (Resim 6)



Resim 6 24-bitlik RGB Resimlerinin Başlıca Renk Paleti

Yöntemlerin en kolayı gizlenecek olan veriyi resim dosyasının "açıklama" alanında gizlemektir. Bu ideal bir yöntem değil çünkü "açıklama" alanının bir sınırı var (255 byte kadar). Ayrıca bu yöntemde değişik resim dosyaları için değişik algoritmalar kurmanız gerekecektir.

Bir başka yöntem ise resim dosyasında renkler için ayrılan ama kullanılmayan alanların veri gizleme için kullanılmasıdır. Bu yöntem de bazı veri çözme araçları ile kolayca bulunabilir, fark edilebilir.

Birçok farklı yöntem kullanılarak resimlerde bilgi gizlenebilir. Kullanılan yöntemleri, gömme işlemi sırasında kullandıkları veriyi dikkate alarak iki başlık altında toplayabiliriz.

- Spatial / Image Domain tekniği
- Frequency / Transform Domain Tekniği

Spatial Domain veya Image Domain olarak adlandırılan teknik, gömme işleminde resim dosyasındaki veriyi doğrudan kullanılır. Gömme işlemin de bilgiyi gizlediği veri kümesi piksel değerlerini temsil eden kısımdır. Bu tekniğe örnek olarak ileride değinilecek olan ve yaygın olarak kulanılan Least Significant Bit Insertion yöntemini gösterebiliriz.

Freqency Domain veya Transform Domain olarak bilinen teknik ise kapak verideki değişimler üzerinde gömme işlemini uygular. Transform domain tekniğine örnek olarak ise JPEG formatlı resim dosyalarına veri gömme işleminde kullanılan algoritmaları verebiliriz. Bu algoritmalar JPEG sıkıştırma sırasında kullanılan DCT katsayıları üzerinde veri gömme işlemini uygular.

- Least Significant Bit Insertion(En Az Öneme Sahip Bite Ekleme) Yöntemi
- JPEG Algoritması (DCT)
- BPCS Steganography Yöntemi
- Maskeleme ve Filtreleme (Masking and Filtering)

e. En az öneme sahip bite ekleme (Least Significant Bit) Yöntemi

"LSB (Least Significant Bit) Insertion" yöntemi, örtü verisine ait segmentlerde her byte'ın en az anlamlı biti yerine gizlenecek verinin bitleri sırasıyla verinin başlangıcından itibaren birer birer yerleştirilir. Burada her sekiz bitin en fazla bir biti değişikliğe uğratıldığından ve eğer değişiklik olmuşsa da değişiklik yapılan bitin byte'ın en az anlamlı biti olmasından dolayı, ortaya çıkan stego verisindeki (= örtü verisi + gömülü veri) modifikasyonlar insan tarafından algılanamaz boyuttadır. Steganaliz yapıldığında, stego verinin her byte'ının son bitlerinin birleştirilmesiyle gizli mesajı oluşturmak kolaydır; dolayısıyla pratikte diğer yöntemlere göre daha az güvenilirdir ve daha az kullanılır.

Sondaki bitin 1 veya sıfır olması sayının değerini çok fazla değiştirmeyecektir. Sondaki bit değerimiz 1 yerine 0 olsaydı bu, renk üzerinde gözle görülecek büyük bir değişikliğe neden olmayacaktı. İşte bu sondaki bitimiz LSB olarak adlandırılır. Bu bitler yerine bizim gireceğimiz datanın verileri girilirse eğer datamız gizlenmiş olabilir. Orijinal resimle içerisine data sakladığımız resim arasında gözle görülür bir fark yoktur.

Örnek:

Beyaz Renk RGB formatında **FF-FF-FF** hexadecimal değeri ile ifade edilir. Yani Red: FF (hex), Green: FF (hex), Blue: FF (hex), FF binary sistemde **11111111** in karşılığıdır. 1 pikselde beyaz rengi ifade etmek için (11111111- 11111111- 11111111) verisi kullanılır. (1111111**1**- 1111111**1**- 1111111**1**) verisinin en anlamsız bitlerini (least significant bit) gizlenecek olan veri için kullanma yöntemi üzerine kuruludur. Bu küçük renk değişikliğini insan gözü algılayamaz. Aynı değiştirme işlemini kırmızı ve yeşil renklerinin bitleri için de yapıldığında, ASCII tablosunda bir harfe denk gelen sayılar elde edilebilir.

Her piksele 3 bit. İlk bakışta çok çok az gibi görünse de 800x600 ebatında bir resimde
800 x 600 = 480.000 adet piksel bulunur.

480.000 x 3 bit = 1.440.000 bit (gizlenecek olan veri için kalan yer) 1.440.000 bit = 175,7 KiloByte olduğunu düşünürsek gizlenecek veri için kalan yer oldukça fazladır. [5]

Örnek olarak 'A' harfini 24 bit BMP resim dosyasına gömmek için 8 bayt gereklidir. Gereken sekiz bit için üç piksel seçebiliriz. Bu işlemi aşağıdaki gibi gösterebiliriz.

Bilginin gömüleceği üç pikselin içerdiği değerler:

(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)

Gizlenecek bilgi olan 'A' harfinin ikili sistemdeki değeri:

(1 0 0 0 0 0 1 1)

Piksel değerlerinin veri gömüldükten sonraki durumu:

(00100111 1110100***0*** 11001000)
(0010011***0*** 11001000 1110100***0***)
(11001000 00100111 11101001)

Bilginin gömülmesinden sonra bitlerin eklendiği sekiz bayttan sadece üçünde değişiklik meydana geldiği görülmektedir. Genel olarak son bitlere ekleme yapıldığında verideki değişme oranı %50 olmaktadır. Bu prensibe dayanılarak sadece son bitlere ekleme yapmak yerine son iki bite ekleme yapmak da mümkündür. Böylece bir resimde saklanabilecek veri miktarı iki kat artmaktadır ve 24 bit BMP formatlı resimlerde bu fark hala gözün fark edemeyeceği düzeyde kalmaktadır.

Örnekte fark edebilceğiniz gibi gömme işleminde altı çizili bayt kullanılmamıştır. Verinin gömülmesinde ilk bayttan son bayta doğru bir sıra izleme zorunluluğu olmadığını buradan anlayabiliriz. Verinin gömülmesi işleminde baytların hangi sırayla kullanılacağı genellikle stego-key vasıtasıyla düzenlenmekte ve tamamen karışık sırayla veri gömülmesi yapılabilmektedir.

LSB insertion yöntemi 24 bit BMP, 8 bit BMP, GIF ve gri tonlamalı resimlerde uygulanabilir. Her formatın farklı avantaj ve dezavantajları olmakla birlikte daha önce de belirtildiği gibi en uygun format 256 renk gri tonlamalı resimlerdir.

Kullanabileceğimiz formatları tek tek değerlendirmek gerekirse 24 bit BMP formatındaki resimler LSB yöntemi için en uygun yapıdaki ve en geniş alanı sağlayan resimlerdir. Kullandığı geniş renk spectrumu (16 milyon renk) sayesinde gömme işleminin yaratacağı değişimler fark edilmemektedir. Ancak bu formattaki resimler çok büyük alan kaplamaktadır ve dağıtımı diğerlerine göre daha zor olmaktadır.

f. JPEG Algoritması (DCT)

JPEG formatlı resimler yüksek kalitedeki resimleri kaliteden çok az kayıpla ve hacmini önemli ölçüde düşürerek taşıyabilmektedirler. İnsanın görüş sistemi bu tip bir dönüştürmeyi mümkün kılmaktadır. Genel yapı olarak incelemek gerekirse JPEG sıkıştırma işleminde öncelikle piksellerin RGB bilgileri luminance-chrominance bilgilerine dünüştürülür. İnsan gözü luminance bilgisine daha duyarlı olduğu için chrominance bilgisi komşu pikseller için aynı değer kullanılmak üzere yarı yarıya azaltılır. Elde edilen yeni piksel değerlerine 8x8 bloklar halinde Discrete Cosine Transform işlemi uygulanır ve DCT katsayıları elde edilir. Bu katsayılardan yüksek freaknsaları ifade edenler bir quantization tablosundaki değerler ile bölünür. Elde edilen yeni katsayılara sıkıştırma işlemi uygulanır ve header eklenerek dosya oluşturulur.

Bilginin saklanması işleminde kullanılan değerler bölünmüş DCT katsayılarıdır. Çünkü bölünmüş katsayıların elde edilmesine kadar yapılan işlemler kayıplı işlemlerdir ve verinin bu değerlerde gizlenmesi mümkün değildir. Her blok bir bit taşıyacak şekilde gömme işlemi gerçekleştirilir. Kullanılan değerlerin katsayılar olması dolayısıyla dosyada olabilecek bozulmalara karşı oldukça dayanıklıdır.

JPEG dosyalarına yapılacak gizleme işlemlerinde gizlenebilecek bilgi miktarı düşük tutulmak zorundadır. Büyük miktarda veri gizlenmesi dosyada görülebilir değişmeler meydana getirecektir.

g. BPCS Steganografi Yöntemi

Bit-Plane Complexity Segmentation Based Steganography Yöntemi oldukça yeni bir yöntemdir. Yapısal olarak bakıldığında Spatial Domain tekniğine dahil edilebilir. Diğer tekniklerle karşılaştırıldığında en belirgin fark sağladığı kapasitedir. Diğer teknikler en fazla orjinal verinin %15'i kadar bir gömme alanı sağlarken BPCS orjinak verinin %50'si miktarında bilginin gizlenmesini sağlayabilmektedir. (BPCS-Steganography, tarih yok) BPCS 24 bit BMP formatı için geliştirilmiş bir yöntemdir. Daha sonra yapılan çalışmalar ile 8 bit BMP ve GIF formatlarına da uygulanması sağlanmıştır.

Gizleme işleminde öncelikle dosyanın analizini yapılmakta ve veri gizlemede kullanılabilecek bitler tespit edilmektedir. Bitlerin belirlenmesinde resmin şekil bilgisini ne kadar taşıdıklarına dair bir inceleme yapılmaktadır. Resim öncelikle her piksele ait bitler gruplanarak tek renkli resimler haline getirilir. Genel prensip olarak n bitlik bir resimden her pikselin birinci bitleri ile bir resim, ikinci bitleri ile başka bir resim elde edilir.

P=(P1,P2,...,Pn)

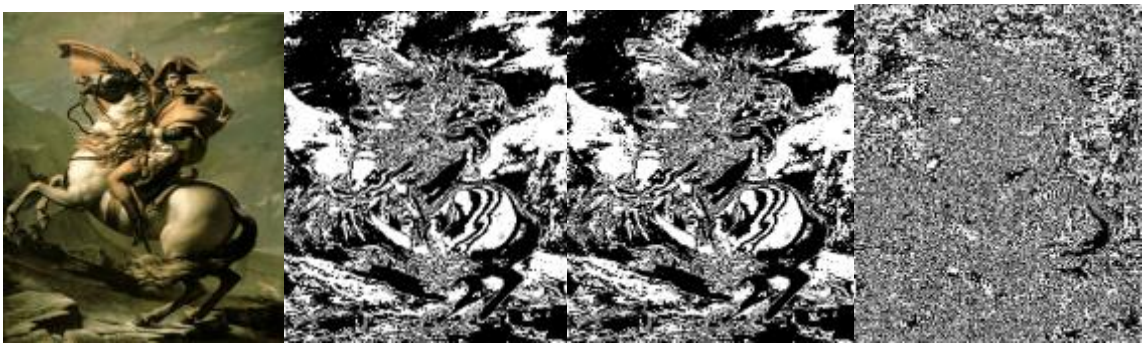
Bu prensibi 24 bit BMP için uygularsak:

P=(PR1,PR2,..,PR8,PG1,PG2,..,PG8,PB1,PB2,..,PB8) biçiminde

PR1, PG1, PB1 most significant bit pozisyonları,

PRn, PGn, PBn least significant bit pozisyonları,

her renk için 8 ayrı resim elde ederiz. Sekizinci bitler LSB olmak üzere elde edilen resimler incelendiğinde bit değerliği azaldıkça resimlerin şekil bilgisinden çok gürültü benzeri veri içerdiği görülür. Resim 7 Gömme işleminde bu alanlar kullanılarak geniş bir kapasite sağlanmış olur. Resim 7'de, A resmi orijinal resimdir. B resmi PR3, (PR3-PG3-PB3) sadece 3. bitler ile. C resmi, PR4, (PR4-PG4-PB4) sadece 4. bitler ile. D resmi, PR5, (PR5-PG5-PB5) sadece 5. bitler ile sonuçlandırılmıştır.



Resim 7 a.orijinal resim. b.PR3 c.PR4 d.PR5

h. Maskeleme ve Filtreleme (Masking and Filtering)

Maskeleme ve filtreleme görünür watermarking uygulamalarında kullanılan bir tekniktir. Uygulama alanı gri tonlamalı resimler ve 24 bit BMP ve gri tonlamalı resim formatları ile sınırlıdır. Resimde görülebilir işaretleme yapmak için kullanılır. Piksellerin parlaklık değerinin arttırılması ile yapılır.

Şekil 8'de bir uygulama görülmektedir. Yapılan işlem ile belirli piksellerin parlaklık değerini %15 arttırılmış ve ("Invisible Man" ©1997, Neil F. Johnson) metni resme eklenmiştir.



Resim 8 Maskeleme ve filtreleme uygulaması

i. Gizli Mesajın Ses Dosyasında Gizlenmesi (Ses Steganografi - Audio Steaganography)

Yaygın dağıtımı ve içerdiği bilginin özelliklerinin benzerliği dolayısıyla ses dosyaları da resim dosyaları gibi steganography uygulamalarında kullanılmaktadır. Ses Steganografi, insan işitme sistemi (Human auditory system-HAS) aralığı yüzünden, ses sinyalleri içerisine bilgi gizleme oldukça uğraş gerektiren bir konudur. HAS 1/1.000'den daha büyük frekans aralığını farkedebilir. Aynı zamanda HAS nereden geldiği belli olmayan gürültülere de oldukça duyarlıdır. Ses steganografide kullanılan birçok yöntem mevcuttur. Bunlardan bazıları:

- Düşük Bit Kodlama (Low bit encoding)

Resim steganografide bahsettiğimiz LSB insertion yöntemiyle aynı şekilde gerçekleştirilir. Ses dosyasındaki verinin her baytının son bitine gizlenecek bilginin bir biti yazılır. Sonuçta oluşan değişiklik ses dosyasında gürültüye neden olmaktadır. Ayrıca dayanıksız bir yapısı vardır. Tekrar örnekleme veya kanalda oluşabilecek gürültü ile mesaj zarar görebilir veya yok edilebilir.

- Faz-Aşama Kodlama (Phase Coding)

Phase coding yöntemi de resim dosyalarında uygulanan JPEG algoritması benzeri bir yapı taşımaktadır. Gömme işleminde ses dosyası küçük segmentlere bölünür ve her segmente ait faz gizlenecek veriye ait faz referansı ile değiştirilir. Phase coding prosedürü aşağıdaki gibidir.

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

- Yayılı İzge (Spread Spectrum)

Gizleme işlemini ses sinyalinin kullandığı frekans spectrumu üzerinde yapmaktadır. Güçlü bir yapısı olmamakla birlikte seste gürültü meydana getirmektedir.

- Yankı Veri Gizlemesi (Echo data hiding)

Bilginin gizlenmesi taşıyıcı ses sinyali üzerine bir yankı eklenmesi ile sağlanmaktadır. Bilgi yankının gecikme miktarı, zayıflama oranı veya büyüklüğü gibi değerler kullanılarak gizlenir. İki farklı gecikme değeri kullanılarak insan kulağının algılamayacağı düzeyde 0 veya 1'in kodlanması mümkündür. Her bitin kodlanması için sinyal segmentlere bölünür. Echo data hiding yöntemi herhangi bir gürültüye neden olmamakta veya kayıplı bir kodlama kullanmamaktadır.

j. Gizli Mesajın TCP/IP Paketlerinde Gizlenmesi

TCP başlıklarında yer alan, aktif olarak kullanılmayan ya da rezerve olarak tutulan kısımlara istenilen gömü verisinin yerleştirilmesi etkili bir yöntem olarak karşımıza çıkmaktadır.

k. Gizli Mesajın HTML Sayfalarında Gizlenmesi (HTML Steganography)

En basit olarak, HTML ile yazılan web sayfalarının kaynak kodları arasına web tarayıcılar tarafından gösterilmeyen yorum satırları eklenerek gizli mesaj gizlenebilir. Ancak bu metod gizli mesajın açık olması güvenlik problemi teşkil etmektedir. İlgili mesajın gözden kaçırılmasını sağlayacak farklı alternatiflerin düşünülmesi bu noktada büyük önem arz etmektedir. HTML kodları içerisinde sıklıkla kullanılan "src, width, height, alt, title, border, bgcolor, href" gibi anahtar ifadelerin ardı sıra gelme kombinasyonlarının anlamlandırılması ile ikili bilgilerin gizlenmesi yaklaşımı da etkili olup, ilk bakışta gizli mesajın tespit edilmesi ihtimalini ortadan kaldırmaktadır. (Garg, 2011)

Resim 9'da HTML taglarının yerleri kodlanır ve bilgi gizleme işlemi gerçekleştirilir. Bu yapılarda biri '1' diğer '0' olarak kodlanır.

```
<span class="bigText" style="color:#0088ff">
        Text with a CSS class and special color
</span>

<span style="color:#0088ff" class="bigText">
        Do you see the difference?
</span>
```

Resim 9 HTML kodlarına CSS ile gizlenmiş gizli yazı

Kurallar şu şekilde tanımlanabilir Resim 10:

```
if( class-attribute before style-attribute ){
    the tag encodes a "1"-bit
}
else{
    the tag encodes a "0"-bit
}
```

Resim 10 HTML kodlarına gizlemenin kuralları

5. STEGANOGRAFİ ARAÇLARI

İnternet aracılığı ile açık kaynak kodlu, direkt çalıştırılıp uygulanabilen, serbest kullanım lisanslı ya da ücret karşılığı lisanslı olmak üzere bir çok veri gizleme aracına ulaşılabilir. Her aracın kullandığı algoritmalar, desteklediği dosya uzantıları farklıdır. Bu çalışmada, internette var olan bütün veri gizleme araçlarını incelemek, nasıl kullanıldıklarını anlatmak tercih edilmemiş, yerine en çok kullanılan, açık kaynak lisansa sahip iki tane araç tanıtılmıştır. Kullanıcının nasıl bir veri gizleme ihtiyacına göre ve hangi kapak dosya kullanacağına uygun olarak en uygun yazılımı kendisinin internet ortamında bulup kullanması tavsiye edilmektedir.

Günümüzde birçok steganografik yöntem bulunmaktadır. Bir steganografik yöntem değerlendirilirken dayanıklılık - kapasite ve taşıyıcıdaki değişim – kapasite arasında ikilemler söz konusudur. Kapasite arttıkça dayanıklılık azalacaktır. Yine aynı şekilde kapasite miktarı arttıkça taşıyıcı ortamdaki değişimler artacaktır.

LSB Steganografi Örnek Algoritması: (Goel, Rana, & Kaur, 2013)

- *Algorithm to embed text message:-*

Step 1: Read the cover image and text message which is to be hidden in the cover image.
Step 2: Convert text message in binary.
Step 3: Calculate LSB of each pixels of cover image.
Step 4: Replace LSB of cover image with each bit of secret message one by one.
Step 5: Write stego image
Step 6: Calculate the Mean square Error (MSE), Peak signal to noise ratio (PSNR) of the stego image.

- *Algorithm to retrieve text message:-*

Step 1: Read the stego image.
Step 2: Calculate LSB of each pixels of stego image.
Step 3: Retrieve bits and convert each 8 bit into character.

DCT Steganografi Örnek Algoritması: (Goel, Rana, & Kaur, 2013)

- *Algorithm to embed text message:-*

Step 1: Read cover image.
Step 2: Read secret message and convert it in binary.
Step 3: The cover image is broken into 8×8 block of pixels.
Step 4: Working from left to right, top to bottom subtract 128 in each block of pixels.
Step 5: DCT is applied to each block.
Step 6: Each block is compressed through quantization table.
Step 7: Calculate LSB of each DC coefficient and replace with each bit of secret message.
Step 8: Write stego image.
Step 9: Calculate the Mean square Error (MSE), Peak signal to noise ratio (PSNR) of the stego image.

- *Algorithm to retrieve text message:-*

Step 1: Read stego image.
Step 2: Stego image is broken into 8×8 block of pixels.
Step 3: Working from left to right, top to bottom subtract 128 in each block of pixels.
Step 4: DCT is applied to each block.
Step 5: Each block is compressed through quantization table.
Step 6: Calculate LSB of each DC coefficient.
Step 7: Retrieve and convert each 8 bit into character.

a. Steghide Kullanımı

Steghide, bir çok çeşit resim ve ses dosyasının içine veri saklamamıza yarayan bir steganografi programıdır. Bir gizleme işlemine tabi tuttuğunuz zaman bir parola da belirleyebilirsiniz. Bu sayede data direk extract edilemez.

Özellikleri:

* Saklanmış data sıkıştırma
* Saklanmış data şifreleme
* Saklanmış veri bütünlüğünü sağlamak için doğrulama kodu yerleştirme
* JPEG , BMP , WAV ve Au dosya uzantılarını desteklemek.

Bağımlılıkları:

libmhash , libmcrypt , libjpeg ve zlib kütüphanelerine bağımlıdır.

Kurulumu:

Linux ' de dağıtımınızın deposundan kolaylıkla kurabilirsiniz , eğer ki dağıtımınızın deposunda bulunmuyorsa internet[1] adresinden uygun paketi indirebilirsiniz.

Kullanımı**:**

Veriyi saklamak için: Resim 11 örnek kullanımı temsil etmektedir.

$ steghide --embed -ef (saklanacak_veri) -cf (icine_gomulecek_dosya) -p (sifre) -sf (olusturulacak_dosya_adi) -e (sifreleme_metodu) -z (sıkıştırma-derecesi) -v (verbose - ayrıntılar)

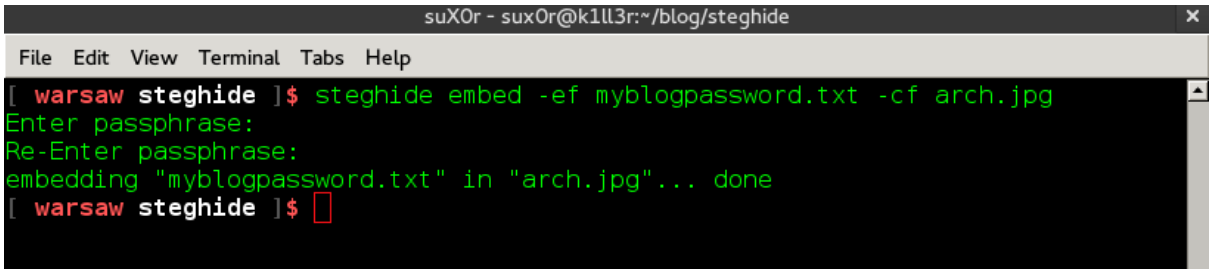
Veriyi kontrol etmek için:

$ steghide --info (kontroledilecekdosya) -p (sifre)

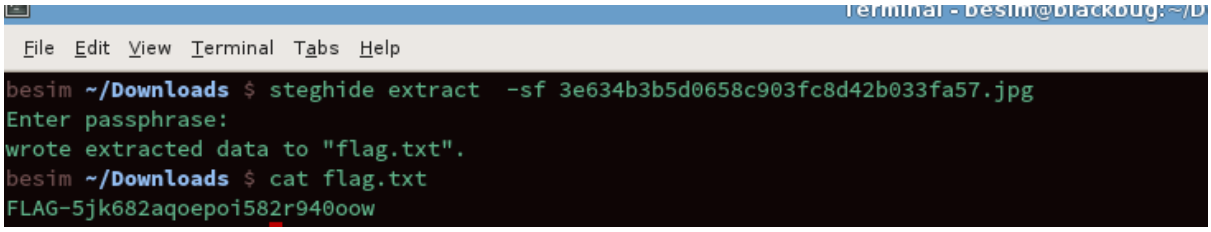
Veriyi açmak için: Resim 12 örnek kullanımı temsil etmektedir.

$ steghide --extract -sf (sifrelenmis_dosya) -p (sifre) -xf (olusturulacak_dosya_adi) -v (verbose - ayrıntılar)

[1] http://steghide.sourceforge.net/download.php (19.11.2015)



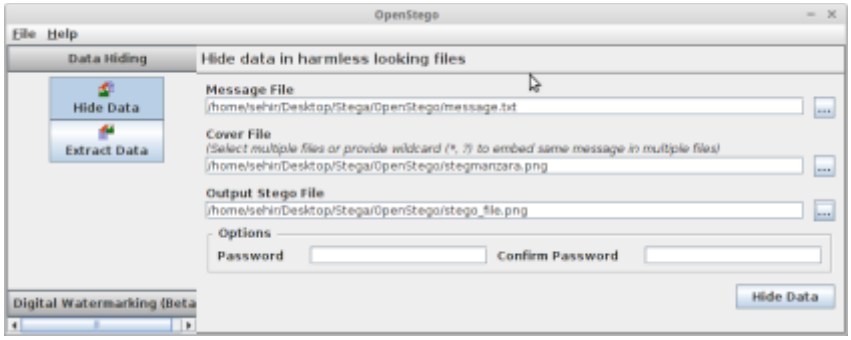
Resim 11 Örnek Steghide Veri Gizleme Kullanımı



Resim 12 Örnek Steghide Gizli Veri Çıkartma Kullanımı (Altınok)

b. OpenStego

OpenStego tamamen Java ile yazılmıştır ve Java destekli bütün ortamlarda çalışabilmektedir. Şifrelemeyi destekler, DES şifreleme algoritmasını ve MD5 özetleme algoritmasını kullanır. Herkesin kendi eklentilerini geliştirip programda kullanabileceği bir yapısı vardır. Farklı veri gizleme algoritmaları, damgalama yöntemleri geliştirilerek kullanılabilir. Yüklü olarak gelen iki tane eklentisi vardır: Veri gizlemek için Randomized LSB yöntemi ve damgalama için Dugad algoritması vardır. İnternet[2] adresinden indirilebilir. Resim 13 OpenStego programının Linux ortamında çalıştırılan arayüzünü göstermektedir.



Resim 13 OpenStego Programı Arayüzü

c. Diğer Araçlar

i. Invisible Secrets 4

1. Format:BMP, JPG, PNG
2. Şifreleme:AES-Rijndael, Twofish, RC4, Cast128, GOST, Diamond 2, Sapphere II, Blowfish
3. Algoritma: LSB

ii. Puffer 4.04

1. Format: BMP, JPG, PNG, GIF
2. Şifreleme: AES

[2] https://github.com/syvaidya/openstego/releases (19.11.2015)

3. Algoritma: Least Significant 3 bits

iii. Xiao Steganography2.6.1

1. Format: BMP
2. Şifreleme: RC2, RC4, DES, Triple DES, 3Des 112 Hashing MD2, MD4, MD5, SHA
3. Algoritma: LSB Substitution

iv. S-Tools

1. Format: BMP, GIF, WAV
2. Şifreleme IDEA, DES, Triple DES, MDC
3. Algoritma: LSB

6. DAMGALAMA(Watermarking)

Steganografi'nin iki kullanım araçlarından bir diğeri de damgalama (watermarking) tekniğidir. Digital ortamda resim, ses, video ve döküman gibi tüm dosyalar kolayca kopyalanabilmekte, kullanılabilmekte ve dağıtılabilmektedir. Bu kopyalama işlemi digital ortamın yapısı gereği orjinal dosyanın aynı kalitede bir kopyasını oluşturmaktadır. Bu yüzden bir yazar ya da fotoğrafçı yazdığı yazının ya da çektiği resmin böyle bir digital ortamda bir çok insan aynı kopyaya sahip olabilirken telif hakkı için nasıl bir hak iddia edebilecek. Bunu için dosyaya ekstra bir bilgi eklemek ve sadece bu bilgiyi içeren dosyayı dağıtmak yeterli bir çözümdür. Watermark olarak bilinen bu gömülen bilgi dosya hakkında sahiplik, telif hakkı veya lisans bilgisi sağlar. Yani bir dosyanın (metin, ses, resim, video) telif hakkını sağlayabilmek için o dosyaya bir bilgi gömme işlemine watermarking bu bilgiye de watermark diyoruz.

Digital watermarklar ikiye ayrılır. Bunlar;

- Görünür watermark (visible watermark)
- Görünmez watermark (invisible watermark)

Gönenen damgalamalar insan gözünün rahatlıkla görebileceği izlerdir. Örneğin paralar da bulunan ışığa tutunca görünen resimler (Türk Lirasındaki Atatürk resmi gibi), bir başka örnek ise televizyon kanallarında o görüntünün hangi kanal yada ajans tarafından çekildiğini gösteren ekranın köşesinde bulunan bir logo. Bu görünen damgalamaya yapılacak bir saldırı için ancak o kısımın kesilerek çıkarılmasıyla sağlanır.

Görünmeyen damgalamada bir örnek ise; pasaportlarda bulunan kişiye ait seri numarası fotoğrafın içerisine de gömülmesidir. Herhangi biri elde ettiği bir pasaporta kendi resmini yapıştırdığı zaman özel tarayıcılar ile fotoğrafın tarandığında seri numarasının tutmadığı ya da olmadığı gözükecektir.

Görünmeyen watermarklar görünen watermarklara göre bazı avantajları vardır. Watermak yerleri belli değildir ya da watermak olup olmadığı farkedilmeyebilir. Watermarkı tüm resim içine dağıtmak genel bir uygulamadır Resim 14. Bu resmi kesme saldırılarına (cropping attacks)

karşı biraz olsun koruma sağlar. Fakat dosya içerisine gömülecek olan bilgi ne kadar az ise saldırılara karşı o kadar güçlü ve güvenli olur. Bu dosya içerisindeki tekrarlılığın (redundancy) azalması için gereklidir.



Resim 14 Resmin tamamı damgalanmaktadır

a. SALDIRILAR

Damgalama üzerine yapılan saldırılar sadece damgayı kaldırmak üzerine değillerdir. Damganın okunabililirliğini silmekte (disable) yeterli olabilir. Bunların başında resmi bir kaç derece döndürmek, parlaklığını azaltmak, resmi bulanıklaştırmak, resmi bir miktar kesmek vb. resim işleme teknikleri gelir. Internet üzerinden watermark uygulama ve kaldırma araçları ücretsiz olarak ulaşılabilir.

7. STEGANALİZ (STEGANALYSIS)

Steganaliz steganografik (steganagraphic) sistemlerin gizliliğini kırma sanatı ve bilimi olarak tanımlanabilinir. Bu bilimle uğraşanlara ise steganalist (steganalyst) denir. Elektronik ortamda bilgiyi saklama ortam özelliklerinin değişmesini gerektirir. Bu değişiklikler gömülü mesajın varlığını ortaya çıkaran bir imza ya da bir parmak izi (fingerprint) bırakırlar. Bu da steganographynin amacını bozar. Saldırılar steganalistin elinde var olan bilgilere bağlı olarak farklı formlarda olabilir (Tablo 1). Steganalizde saldırı tipleri iki ana başlık altında incelenir. Bunlar;

- Tarama (Detection) - Pasif Saldırı
- Yok Etme/Bozma (Distortion) - Aktif Saldırı

Stego-only attack	Sadece stego-object elimizde
chosen stego attack	The stego-tool (algoritması) biliniyor ve stego-object elimizde
known cover attack	Stego-object ve cover object'in orijinal bir kopyası elimizde
Known stego attack	Stego-tool (algoritması) biliniyor ve stego-object and orijinal kapak (cover) elimizde.
known message attack	Gizli mesaj ve stego-object elimizde
choosen message attack	Bir mesaj seçilir ve bilinen algoritma ile stego-object oluşturulur.

Tablo 1

a. Gizli Mesajın Taranması

Alışılmamış modeller gizli bilginin varlığının ihtimalini teşhir ederler. Eklenen boşluklar ve kullanıcıya görünmeyen karakterler dosyanın bir kelime işlemci tarafından açılmasıyla kolayca görülebilinir. Metin eğer ekranda yazılırsa normal gözükebilir fakat dosya bir kelime işlemci ile açılırsa boşluklar, tablar ve diğer karakterler metinin biçimini bozar.

Bazı resimlerde içine az miktarda bir bilgi gömülerek büyük bozulmalar olabilir. Görünen bir gürültü (noise) gizli bilginin varlığını ele verir. Aynı durum audioalar için de geçerlidir. Yankılar ve gölge sinyaller duyulabilir gürültü ihtimalini aza indirgerler. Fakat bunlar da birkaç işlem ile fark edilebilinir.

Stego-image ler cover imageleri ile görsel olarak karşılaştırıldıklarında gizlenmiş olan bilginin varlığı hakkında bir ipucu vermezler. Bunu belirlemek için detaylı bir analiz yapmak gerekir. En basit yöntem stego-image ile cover-image arasındaki artan dosya boyutu. Fakat günümüzdeki birçok steganografik araçlar bu farkı ortadan kaldırmaktadır. Bir başka imza ise cover imagelerin renk paletlerinde yapılan hiledir. Bu parmakizi tek renklerin sayısındaki büyük artış ya da azalış olarak kendini gösterir. Bir diğer parmak izi ise paletteki renklerin rastgele den çok artan bir şekilde artmasıdır. Gray scale bir resimde siyah gölgelerin sayısının orantısız olması ise bir başka güçlü gizli bir mesajın varlığının göstergesidir.

Bazı disk analiz programları hard-diskin kullanılmayan partition larında veya clusterlarında saklanan bilgiyi filtreden geçirip rapor edebilirler.

Filtreler aynı zamanda paket headerlarında gizli ya da geçersiz bilgi içeren TCP/IP paketlerini yakalamak içinde uygulanabilinirler. Filtreler paketlerin firewall domain'nin içinden üretilip üretilmediğini ve SYN ile ACK bitlerinin geçerliliğini tespit etmek için ayarlanabilinir. Yani kullanılmayan ve reserve edilen boşluklardaki bilginin yakalanması için firewall ayarları düzenlenebilinir.

Steganography de aynı kapak iki defa kullanılmamalı bu karşılaştırma için bir saldırı imkanı doğurur. Aynı zamanda herkesçe bilinen genel dosyalar da kullanılmamalı, mesela windows açılış sesi ya da windows en genel duvar kağıtları vs.

b. Steganografiği Bozma

Bir stego-image keşfedildiği zaman gizli mesajı yok etmek veya işlevsiz bırakacak birçok adım vardır. Gizlenmiş bilginin varlığı biliniyorsa her zaman tarama yapmak gerekli değildir. Bu durumda yapılacak en iyi şey gizli mesajı bozarak onun kullanışsız hale gelmesini sağlamaktır. Bilgiyi saklamanın her yolunda gömülecek olan gizli bilginin boyutu ile bu bilginin varlığını koruması ya da manipulasyonlara karşı güçlü olması arasında bir vazgeçim vardır.

Daha önce bahsettiğimiz gibi metin üzerinde boşluklar eklenerek ve görünmeyen karakterler ile gizlenen mesajın bozulması yine bir kelime işlemci tarafından gerçekleştirilebilinir. Extra boşluklar ve karakterler metin dokümanlardan kolayca çıkartılıp atılabilinirler.

Resim dosyalarından gizli bilginin yok edilmesi image processing teknikleri ile kolayca yapılır. Bunlar resmi 1 kaç derece döndürmek, resmi bir yerinden kesmek, resmin parlaklığını azaltmak, resmi bulandırmak, resmi eğriltmek vs. ya da resmi bir formattan başka bir formata dönüşmek gibi (mesela bmp den jpeg'e).

Eğer bir object üzerinde gizli bilgi olduğu taranamıyorsa tekrar o object içine bilgi bilinen steganographic metodlarla gömülerek önceki gizli bilginin yok olmasını sağlayabiliriz. Ses ve video dosyaları da resimler gibi aynı saldırı tiplerine maruz kalabilirler. Sinyallerin manipülasyonu gömülü mesajı yok etmek ya da tekrar üzerine yazmak için yeterli olabilen gürültü seviyesindeki (LSB) gömülü sinyalleri değiştirecektir. Yankıları ya da güç farkedilen sinyalleri iptal etmek için filtreler kullanılabilinirler. Fakat bu umulduğu kadar başarılı olmayabilir.

TCP/IP paket başlıkları (header) kolayla denetlenebilinir. Firewall filtreleri kaynak ve hedefin IP adreslerinin, SYN ve ACK bitlerinin geçerliliğini test etmek için ayarlanırlar. IP adresleri kaplı bilgiyi geçirmek için değiştirilirse veya spoof edilirse, DNS 'teki geri bakım (reverse lookup) bu adresi tanımlayabilir. Eğer IP adresi hatalıysa paket iptal edilebilinir. Bilgi saklamak için bu tekniği kullanmak yönlendirme sürecinde TCP/IP başlıklarında üzerine yazılabileceğinden dolayı risklidir. Reserve edilen bitlerin üzerine tekrar bir bilgi yazılabilinir.

8. SONUÇ

Steganografi aslında şifrelemenin alternatifi değil onun tamamlayıcısıdır. Steganografi son yıllarda yeni bir şifreleme metodu olarak karşımıza çıkmaktadır. Bu yaklaşım kısaca bir nesnenin içerisine bir verinin gizlenmesi olarak tarif edilebilir. Bugünün steganografi teknikleri güvenliği daha da arttırmak için şifrelenmiş verileri gizlemek için genelde ses, sayısal resim veya video dosyalarını kullanmaktadır. Şifrelenmiş veriler kendi başlarına hacker'ların dikkatini çekerken görüntü ya da ses dosyalarının içine gizlenmiş olduklarında hiç kimse fark etmeyeceğinden kırılmaya da çalışılmayacaktır.

Steganography köklü bir tarihi ve yeni teknolojilere ayak uydurabilecek yapıda olması nedeniyle dinamik bir araçtır. Steganographic gizlilikteki başarı uygun bir mekanizma seçerek elde edilir. Hernasılsa zararsız görünen bir stego-medium gerçekte gömülü bir bilginin varlığını yayar. Kapaklı iletişim alanında ve steganography deki gelişmeler devam etmektedir. İmage manipülasyonunda hayatta kalmayı başaran çok daha güçlü metodların yapımındaki araştırmalar ve saldırı teknikleri büyümeye devam ediyor.

9. Kaynakça

Altınok, B. (tarih yok). *Steghide.* 11 19, 2015 tarihinde http://besimaltinok.com/steghide-ctf/ adresinden alındı

Aristagoras. (tarih yok). 11 12, 2015 tarihinde https://en.wikipedia.org/wiki/Aristagoras adresinden alındı

BPCS-Steganography. (tarih yok). 11 18, 2015 tarihinde https://en.wikipedia.org/wiki/BPCS-Steganography adresinden alındı

Clair, B. (2001, 10 08). *Steganography*. StrangeHorizons: http://www.strangehorizons.com/2001/20011008/steganography.shtml adresinden alındı

Curran, K., & Bailey, K. (Sonbahar 2003). An Evaluation of Image Based Steganography Methods. *International Journal of Digital Evidence, 2*(2).

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

Goel, S., Rana, A., & Kaur, M. (2013, Mayıs-Haziran). A Review of Comparison Techniques of Image Steganography. *IOSR Journal of Electrical and Electronics Engineering(IOSR-JEEE), 6*(1), 41-48.

Histiaeus. (tarih yok). 11 12, 2015 tarihinde https://en.wikipedia.org/wiki/Histiaeus adresinden alındı

Johnson, N. F., & Jajodia, S. (1998, Şubat). Exploring Steganography: Seeing the Unseen. *IEEE Computer*, 26-34. 11 17, 2015 tarihinde http://www.jjtc.com/pub/r2026.pdf adresinden alındı

Kuhn, M. (1995). *Steganography Mailing List.* 11 16, 2015 tarihinde http://www.jjtc.com/Steganography/steglist.htm adresinden alındı

Kumar, A., & Pooja, K. (Kasım 2010). Steganography- A Data Hiding Technique. *International Journal of Computer Applications (0975 – 8887), 9*(7).

Mikro Noktalama. (tarih yok). 11 12, 2015 tarihinde http://carinsurance.arrivealive.co.za/wp-content/uploads/2009/07/datadot.jpg adresinden alındı

Null Cipher. (tarih yok). 11 13, 2015 tarihinde https://en.wikipedia.org/wiki/Null_cipher adresinden alındı

Petitcolas, F. A. (tarih yok). 11 13, 2015 tarihinde http://www.petitcolas.net/steganography/history.html adresinden alındı

Petitcolas, F. A. (2000). *Information Hiding: Techniques for Steganography and Digital Watermarking.*

Steganographia. (tarih yok). 11 13, 2015 tarihinde http://www.esotericarchives.com/tritheim/steganographia_title_page300.jpg adresinden alındı

Stego Örnek. (tarih yok). 11 13, 2015 tarihinde http://www.jjtc.com/stegdoc/sec202.html adresinden alındı

10. EKLER

a. Terimlerin Tanımlamaları

- Açık Yazı (Plaintext): Gizlenecek gömülecek mesaj.
- Taşıyıcı Dosya - Örtü Verisi (Cover File - Carrier File - Vessel Data - Dummy Data - Covertext): İçine bilgi gizlenen ortam. Resim, ses, yazı olabilir.
- Stego (Stego File - Stego Object - Stego Text): Gizleme sonrası oluşan ortam. Gömülmüş olan bir mesajı içeren cover'ın modifiye edilmiş bir versiyonu.
- Stego-anahtar (Stego-key, Ciphertext) bilginin saklanması işlemini kontrol etmek için ve gömülü bilginin elde edilmesini zorlaştırmak için kullanılmaktadır.

BGA Bilgi Güvenliği A.Ş. Hakkında

BGA Bilgi Güvenliği A.Ş. 2008 yılından bu yana siber güvenlik alanında faaliyet göstermektedir. Ülkemizdeki bilgi güvenliği sektörüne profesyonel anlamda destek olmak amacı ile kurulan BGA Bilgi Güvenliği, stratejik siber güvenlik danışmanlığı ve güvenlik eğitimleri konularında kurumlara hizmet vermektedir.

Uluslararası geçerliliğe sahip sertifikalı 50 kişilik teknik ekibi ile, faaliyetlerini Ankara ve İstanbul ve USA'da sürdüren BGA Bilgi Güvenliği'nin ilgi alanlarını "*Sızma Testleri, Güvenlik Denetimi, SOME, SOC Danışmanlığı, Açık Kaynak Siber Güvenlik Çözümleri, Büyük Veri Güvenlik Analizi ve Yeni Nesil Güvenlik Çözümleri*" oluşturmaktadır.

Gerçekleştirdiği başarılı danışmanlık projeleri ve eğitimlerle sektörde saygın bir yer edinen BGA Bilgi Güvenliği, kurulduğu günden bugüne alanında lider finans, enerji, telekom ve kamu kuruluşlarına 1.000'den fazla eğitim ve danışmanlık projeleri gerçekleştirmiştir.

BGA Bilgi Güvenliği, kurulduğu 2008 yılından beri ülkemizde bilgi güvenliği konusundaki bilgi ve paylaşımların artması amacı ile güvenlik e-posta listeleri oluşturulması, seminerler, güvenlik etkinlikleri düzenlenmesi, üniversite öğrencilerine kariyer ve bilgi sağlamak için siber güvenlik kampları düzenlenmesi ve sosyal sorumluluk projeleri gibi birçok konuda gönüllü faaliyetlerde bulunmuştur.

BGA Bilgi Güvenliği AKADEMİSİ Hakkında

BGA Bilgi Güvenliği A.Ş.'nin eğitim ve sosyal sorumluluk markası olarak çalışan Bilgi Güvenliği AKADEMİSİ, siber güvenlik konusunda ticari, gönüllü eğitimlerin düzenlenmesi ve siber güvenlik farkındalığını arttırıcı gönüllü faaliyetleri yürütülmesinden sorumludur. Bilgi Güvenliği AKADEMİSİ markasıyla bugüne kadar "Siber Güvenlik Kampları", "Siber Güvenlik Staj Okulu", "Siber Güvenlik Ar-Ge Destek Bursu" , "Ethical Hacking yarışmaları" ve "Siber Güvenlik Kütüphanesi" gibi birçok gönüllü faaliyetin destekleyici olmuştur.