Steganaliz

Metin Bilgin[1,2]

[1] Tophane Teknik ve Endüstri Meslek Lisesi, Bursa

[2] Yıldız Teknik Üniversitesi, İstanbul

f0111301@std.yildiz.edu.tr

Özet: Steganografi, içinde gizli mesaj veya bilgiler bulunan bir veriyi, alıcıdan başka kimsenin fark edemeyeceği bir bicimde gönderme sanatıdır. Latincede 'steganos' kelimesi 'görünmeyen', steganografi de 'gizlenmiş yazı' anlamına gelmektedir. Kısaca steganografi 'veri gizleme sanatı' olarak tanımlanabilir. Steganaliz ise bir örtü verisi içinde gizli veri olup olmadığını anlamaya yarayan saldırı yöntemleridir. Bu çalışmada steganaliz ve kullanılan yöntemler hakkında bilgiler verilecektir.

Anahtar Kelimeler: Steganografi, Steganaliz, Bilgi Gizleme.

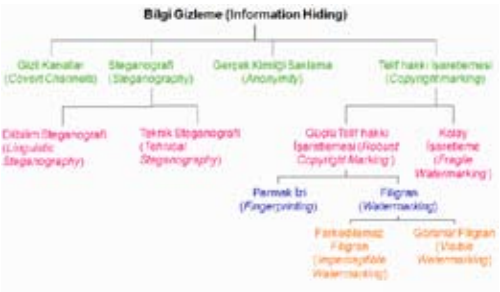
Steganalysis

Abstract: Steganography is a forwarding art that you forward a data includes confidential meseage or information to receiver by making no one noticed. Steganos's meaning is 'invisible', also Steganography's meaning is 'concealed word' in Latin. In brief, steganography can depicted like a 'data concealing art' . On the other hand, steganalysis the group of the attack methods to understand information whether it is hidden on cover object or not. The methods used in this study and will receive information about steganalysis.

Keywords: Steganography, Steganalysis, Information Hiding.

1. Giriş

Bilgi gizleme, bir mesajın ya da bilginin, herhangi bir masum görünüşlü ortam içerisine saklanarak bir diğer kişiye ulaştırılmasıdır [1].



Şekil 1. Bilgi Gizleme

Steganografi, içinde gizli mesaj veya bilgiler bulunan bir veriyi, alıcıdan başka kimsenin fark edemeyeceği bir bicimde gönderme sanatıdır. Latincede 'steganos' kelimesi 'görünmeyen', steganografi de 'gizlenmiş yazı' anlamına gelmektedir. Kısaca steganografi 'veri gizleme sanatı' olarak tanımlanabilir. Amaç, iletilmek istenen bilgiyi ve bu bilginin varlığını başkalarının fark etmesini engelleyecek kadar iyi saklamaktır. Steganografi'de kendisine bilgi gönderilen kişi bile ancak anahtar bilgisini bilmesi durumunda gizli veriyi elde edebilir [2].

After The Theater, All Clients Keep A Tab Down At Wesley's Nook.

A T T A C K A T D A W N [5]
(Mesaj kelimelerin ilk harfleri şeklinde kodlanmış)

Steganaliz, bir taşıyıcı verisi içerisinde, saklanmış bir bilgi olup olmadığını bulmayı, eğer var ise bu bilgiyi elde etmeyi amaçlayan ve steganografik sistemlere karşı yapılan saldırılara

denmektedir. Kısaca, Steganografik metotlarca gizlenen verileri ortaya çıkartma bilimine steganaliz denir.

Klasik anlamda steganografi, hükümlü problemi ile özdeşleşmiştir. Alice arkadaşı Bob'a açık bir mesajın içerisine saklanmış gizli bir mesaj göndermek istemektedir. Gardiyan Wendy ise Alice ve Bob arasında iletişimi dinlemekte, gizli veri iletimine engel olmaya, gizli veri iletim kanallarını kapatmaya ve eğer varsa olası gizli verileri bozmaya çalışmaktadır. Klasik anlamdaki steganaliz probleminde ise Wendy gizli haberleşmeyi bozmak ve engellemek yerine sadece varlığını tespit etmekle yetinmekte, eğer mümkünse iletilen gizli verileri deşifre etmeye çalışmaktadır.

Steganografik yöntemler kullanılarak saklanan verileri açığa çıkartmak için ortaya konmuş genel bir steganaliz yöntemi bulunmamaktadır. Ancak çoğu steganaliz uygulamasının temeli matematiksel - istatistiksel analizlere dayanır.

Steganaliz yöntemleri amaçlarına göre iki gruba ayrılırlar:

- Pasif steganaliz: Gizli verinin sadece varlığını tespit eden yöntemler ,
- Aktif steganaliz: Gizli mesajın bir kısmını veya benzerini elde etmeyi sağlayan yöntemlerdir.
- Steganaliz metotları, gizli veri içeren örtücü verinin toplandığı bölge üzerinde çalışırlar. Steganaliz metotlarının çalıştığı boyuta göre söz konusu metotlar üç kategoriye ayrıştırılabilir.
- Uzaysal dağılımlı veri üzerinde çalışan metotlar (Resim)
- Zamana dağılmış veri üzerinde çalışan metotlar (Ses)
- Hem uzaysal hem de zamana yayılmış veri üzerinde çalışan metotlar (Video)
- Steganografi yöntemleri, steganaliz yöntemlerine karşı koyabilmek için iki iletişim kavramından fazlasıyla yararlanır.

Baraj gürültüsü: Gizli veriyi içeren taşıyıcı sinyalde, gizli veri eklenmesi haricinde oluşan, kayıt, iletim, kodlama vb. nedenlerden kaynaklanan bozulma. Eğer gizli veri gömme işlemi sırasında oluşan bozulma sinyali baraj gürültüsünün altında kalıyorsa, dahası tüm istatistiksel özellikleri baraj gürültüsü ile aynı, çok yakın veya benzer tutulabiliyorsa gizli verinin varlığının tespit edilmesi (Pasif steganaliz) ve gizli verinin içeriğinin açığa çıkartılması (Aktif steganaliz) çok zorlaşmaktadır.

Kriptolu gizli veriler: Gizli veriler gömülmeden önce şifrelenirler. Gizli verinin şifrelenmesi aktif steganaliz yöntemlerine karşı kesin çözüm sağlar; daha açık bir anlatımla gizli veri gömülü olduğu sinyalden bir şekilde sökülebilse bile içeriğinin elde edilmesi için zorlu kriptoanaliz sürecinin başarıyla sonuçlandırılması gerekir.

2. Steganaliz Saldırı Çeşitleri

Steganografi sonucunda oluşturulmuş olan stego nesnesi orijinal haliyle kıyaslandığında görsel olarak herhangi bir değişim olmadığı görülür. Görsel olarak herhangi bir değişiklik olmadığı için steganografiyi belirlemek için daha detaylı analiz yöntemlerine ihtiyaç duyulmaktadır. Bazı steganografi araçları üzerinde yapılan incelemelerde Johnson ve Jajodia birkaç elektronik iz keşfetmişlerdir [3][4].

Bunlardan en belirgin olanı resmin boyutunda olan değişimdir. Belirlenen imzaların çoğu taşıyıcı resmin renk paletinde değişime neden olduğudur. Bu izler ya renk paletinde azalma ya da renk paletinde artmaya neden olmaktadır.

Stego resimlere yapılan saldırılar üç sınıf altında toplanabilir.

1. Gizli mesajın varlığının tespit edilmesi,
2. Gizli mesajın elde edilmesi,
3. Gizlenmiş olan mesajın yok edilmesi.

Bir resim içerisinde eğer gizli bilgi olduğu tes-

pit edilmiş ise bu mesajı yok etmek ya da bozmak için birkaç tane yol vardır.

Bunlardan bir tanesi resim bir resim aracı ile açılıp ve en basit olarak tekrardan JPEG formatında saklanmasıdır. Bu işlem özellikle LSB yöntemi ile saklanmış bilginin bozulması için işe yarayan bir yöntemdir. Ancak dönüşüm yöntemleri kullanılarak yaratılan stego resimler için daha farklı bir yöntem kullanılması gerekmektedir.

Tek bir dönüşüm bu araçlar ile oluşturulan resimlerdeki bilgilerin yok edilmesi için yeterli olmasa da birkaç kere farklı formatlarda resim dönüşümlerinin yapılması bu bilgilerin kaybolmasını sağlamaktadır [5].

Ayrıca kesme, bazı bölümlerini çıkartma, bulanıklaştırma, pikseller arasındaki kontrastı azaltma/arttırma, gürültü ekleme ya da çıkarma, tekrar örnekleme, bit yoğunluğunda değişiklik yapma (gri-seviye 8-bit, 24-bit vb.), gibi resim değiştirme işlemleri uygulanması durumunda eldeki resimde bulunan gizli bilginin yok edilmesi sağlanabilmektedir.

Resim içerisinden saklanmış olan bilginin çıkartılması işlemi incelenmesi gereken çok farklı bir konudur. Resim içerisinde bilgi olduğu tespit edilmesine rağmen bu bilginin çıkartılması mümkün olmayabilir. Kullanılan algoritma bilinmiyorsa, şifreleme kullanılıp kullanılmadığı bilinmiyorsa işlem oldukça zor hale gelmektedir.

Steganografi sistemlerine saldırı yaparak bilginin varlığını ortaya çıkartmaya çalışan kişiye steganalist denmektedir. Genelde steganalistin kullanılan steganografi sistemini bildiği varsayılır. Eğer steganalist kullanılan sistemi bilmiyorsa, bu onun işini zorlaştıracaktır. Steganalistin bir steganografik sisteme saldırabilmesi için sahip olması gereken bazı veriler vardır. Bu sahip olduğu verilere göre saldırı modellerinden birini seçebilir. Steganalizde kullanılan bu modeller kriptanalizde kullanılan saldırılar kullanılarak açıklanabilir. Kriptanalizde kullanılan saldırılar, sadece şifreli metin, bilinen açık metin, seçilen açık metin ve seçilen şifreli metindir. Steganalizde ise sadece stego, bilinen taşıyıcı, bilinen mesaj, seçilen stego, seçilen mesaj ve bilinen stego saldırılardır [6].

1. Sadece stego saldırısı: Analiz için sadece stego-nesnesi (Stego-object) bilinmektedir. Kriptanalizdeki sadece şifreli metin atağına benzemektedir. En zor durumdur. Elde sadece içerisinde bilgi olduğu şüphelenilen dosya bulunmaktadır.

2. Bilinen taşıyıcı saldırısı: Elde resmin hem mesaj gizlenmeden önceki hali hem de mesaj gizlendikten sonraki hali bulunmaktadır.

3. Bilinen mesaj saldırısı: Analist gizlenmiş olan mesajı biliyorsa stego medyayı analiz etmek için kullanabilir. Bu atakta oldukça zordur. Sadece stego atağıyla benzer olarak düşünülebilir.

4. Seçilen stego saldırısı: Kullanılan steganografi algoritması ve stego medyasının bilindiği durumdaki ataktır.

5. Seçilen mesaj saldırısı: Bu atakta steganalist elde bulunan stego resmini analiz edebilmek için seçilen mesajlardan çeşitli steganografi algoritmaları kullanarak stego medyalar elde eder. Amaç belirli steganografi araçlarını ya da algoritmalarını işaret eden stego resimdeki örüntüyü/modeli belirlemektir [7].

Saldırı Tipi	Saldırı Yapan kişinin elinde bulunması gerekenler			
Saldırı	Stego-Resmi	Taşıyıcı	Gizli Mesaj	Algoritma
Sadece stego saldırısı	✓			
Bilinen taşıyıcı saldırısı		✓		
Bilinen mesaj saldırısı			✓	
Seçilmiş stego saldırısı	✓			✓
Seçilmiş mesaj saldırısı			✓	✓

Şekil 2. Steganaliz saldırı çeşitleri [7]

3. Steganalizde Kullanılan Yaklaşımlar

İyi bir steganaliz yöntemi geliştirmek zordur. Çünkü belli bir steganografi yöntemi için başarılı olan bir analiz başka bir yönteme uygulandığı takdirde işe yaramayabilir. Steganalizde amaç daha çok tek bir yöntem yerine bütün yöntemlere uygulanabilir, geniş çaplı bir sistem geliştirmektir. Günümüzde kullanılan yöntemler göz önüne alındığında steganalizde iki yaklaşım olduğu söylenebilir [8].

- İncelenen resim hakkında çok az ya da hiçbir istatistiksel varsayım olmadan yapılan analiz; burada istatistikler çok geniş bir veritabanı üzerinden elde edilir.
- İncelenen resim için bir parametrik model önerilir ve kullanılacak olan istatistikler bu model üzerinden hesaplanarak steganaliz çalışmalarında kullanılır.

Steganaliz problemlerini çözmek için geliştirilen yaklaşımları sınıflandırırsak;

- Öğrenmeye dayalı steganaliz,
- Kör tanımlamaya dayalı steganaliz,
- Parametrik istatistiksel steganaliz,
- Hibrit teknikler olarak sıralanabilir.

4. Yapılan Çalışmalar

Steganaliz konusunda birçok çalışma yapılmıştır. Bunlardan bazıları hakkında bilgiler verilecektir.

Westfeld ve Pfitzmann (2000). resimlere mesajın saklanması sonucu değişen değer çiftlerinin istatistiksel analizine dayanan bir steganaliz metodu geliştirdiler. Bu yöntem ardışık saklama gibi durumlarda daha güvenilir sonuçlar vermiştir [9].

Fridrich ve ark. (2000), 24 bitlik renkli resimlerde LSB yöntemiyle gerçekleştirilen veri saklamayı tespit etmek için, bir birine yakın renk değeri çiftlerinin istatistiksel analizine dayanan bir çalışmada tekil renk oranının toplam piksel sayısının %30 undan az olduğu resimlerde güvenilir sonuçlar verebilen bir yöntem sunmuşlardır.

Bu yöntemin sıkıştırılmamış yüksek çözünürlüğe sahip, yani günümüzdeki sayısal fotoğraf makinelerinin çektiği resimlerde başarılı olamayacağı ve ayrıca gri seviyeli resimlere bu yöntemin uygulanamayacağını bildirmişlerdir [10].

Provos ve Honeyman (2001), JPEG resimlerinin steganalizi üzerine kapsamlı bir çalışma yaptılar ve geliştirdikleri yazılımla internet üzerinde binlerce şüpheli resmi tespit edebilmişlerdir [11].

Farid (2001), taşıyıcı ve stego resimlerden oluşan bir veritabanı üzerinde yaptığı analizlerden ve özellik çıkarımlardan sonra steganografi algoritmasının bilinmesine ihtiyaç duymaksızın steganaliz tahmininde bulunan evrensel tespit çalışmasını sunmuştur [12].

Fridrich (2006), veri saklama sonucu oluşan değişim ile değişim sayısı arasındaki ters orantıyı analiz ettiği çalışmasında, herhangi bir tespit edilebilirlik profilinde, (tespit edilebilirlik profili gömme etkisinin dağılımını ifade etmektedir) sadece en küçük gömme etkisine sahip piksellerin kullanılmasının asla optimum olmadığını belirlemiştir [13]

5. Kullanılan Teknikler

Resimler için steganaliz yaklaşımlarından bazıları şunlardır [14]:

- Görsel tespit (Görsel ataklar) ,
- $\chi 2$ Testi ,
- Histogram analizleri ,
- Yüksek seviyeli istatistiksel analizler (RS analizi, İkili istatistik yöntemi) ,
- Algoritmaya ve türe özel tespitler (JPEG Steganaliz) ,
- Evrensel tespit sistemleri ,
- RQP Yöntemi.

Görsel tespit, veri gömme sonucu oluşan resmin gözle orijinalinden farkının anlaşılması veya orijinali yoksa resmin üzerindeki normal bir resimde olması beklenmeyen bozuklukların fark edilmesiyle gerçekleşir. Ancak bu durumda da kendinden gürültülü resimlerle stego resimleri ayırt edebilmek mümkün olmayacaktır. Görsel atakların güvenilirliğinin tartışılır olduğu açıktır.

Histogram analizleri resme veri gömme sonucu değişen piksel değeri çiftlerinin istatistiksel analizlerini esas almaktadır.

Yüksek dereceli istatistiksel analizler ise histogram analizinden fazla olarak değişimin gerçekleştiği piksellerin konumlarına yönelik istatistiksel analizleri de içermektedir.

Algoritmaya veya türe özel tespitler de algoritması bilinen steganografi uygulamalarıyla oluşturulan stego resimlerdeki mesajı ortaya çıkarmaya yönelik yöntemlerle JPEG gibi resim türlerine özel steganaliz çalışmalarını içermektedir.

Evrensel tespit sistemleri ise resme ait bazı özelliklerin çıkarımıyla orijinal resimlerle stego resimler arasındaki ayırımı yapmaya yönelik yöntemleri içermektedir.

RQP Yöntemi Fridrich ve arkadaşları tarafından geliştirmiştir [10]. Bu metot LSB gizlemesi tarafından yaratılan yakın renk çiftlerini analiz etmeye yöneliktir. Öncelikle seçilen resim için yakın renk çiftlerinin tüm renk çiftlerine oranı hesaplanır. Daha sonra bu resim içerisine bir test mesajı gizlenerek oran yeniden hesaplanır. Bu iki oran arasındaki fark büyük ise resminin içinde gizlenmiş bilgi yok demektir. Bu iki oranın birbirine yakın olması resmin içinde gizlenmiş bilgi olduğunu göstermektedir.

6. Sonuçlar

Günümüzde teknolojinin gelişmesi beraberinde dijital ortamlarda bulunan verilerin güvenliğinin sağlamasını da beraberinde getirmektedir. Şifreleme ve steganografi teknikleri bu güvenliğin sağlanmasında kullanılan çözüm tekniklerini içermektedir. Bu tekniklerin sağlamlığı da analiz teknikleriyle test edilmektedir.

Ülkemizde steganografi ve steganaliz konusunda cesitli calısmalar yapılıyor olsa da, genel olarak ve ozellikle ses icerisine veri saklamaya yonelik calısmaların henuz yeterli olmadığı değerlendirilmektedir. ses icerisine veri saklama uygulamalarında henuz yeterli ilerleme sağlanamamıstır. Veri transferi teknikleri hızlandıkca resim dosyalarına gore daha buyuk boyutlu olan ses dosyalarının da sayısal iletisimde cok yoğun bir sekilde kullanılacağı dusunulmektedir.

JPEG ve GIF formatındaki resim dosyaları özelliklerinden dolayı taşıyıcıdaki değişime daha duyarlıdır. Taşıyıcıdaki değişim açısından BMP dosyalar daha iyi sonuçlar vermektedir.

Kapasite açısından bakıldığında ise BMP ve GIF formatındaki resimlerin daha fazla bilgiyi saklayabilmelerinden dolayı tercih edildiği görülmüştür. JPEG formatındaki resimler dosya yapılarından dolayı her 8x8 piksellik bloklara 1 byte saklayabilmektedirler. Bu yüzden saklama kapasitelerinin düşük olduğu söylenebilir.

Dayanıklılık ise çeşitli steganalitik saldırılara karşı ne kadar başarılı olduğu ile değerlendirilmektedir.

Her steganografik yöntem için ayrı steganaliz yöntemleri geliştirilmiştir. Bir yöntem için çok iyi sonuçlar veren bir steganaliz yöntemi bir diğeri için doğru sonuç vermeyebilir. Genelde JPEG formatındaki resimler steganalitik saldırılara karşı daha başarılıdırlar.

Bir resmin içinde gizli bilgi olduğunun anlaşılmasından sonra yapılacak işlem bu verinin elde edilmesidir. Fakat bunun için bilgi gizlemede kullanılan steganografik yöntemin bilinmesi gerekmektedir. Resmin içindeki bilginin elde edilmesi uğraş gerektiren ve zaman alan bir süreçtir. İnternet üzerinden hergün milyonlarca resim ya da video dosyası gönderildiği

düşünülürse gizli bilgilerin sezilmesi bile oldukça zordur.

Steganografinin kötü amaçlar için kullanılması durumunda insanlık açısından kötü sonuçlar ortaya çıkabilmektedir. Steganografik yöntemlerin çeşitliliği ve her steganaliz yönteminin gizli verileri yakalayamaması dolayısıyla kötü amaçlı kişiler bu yöntemleri tercih etmeye başlamışlardır. Bu nedenle steganografi ve steganaliz yöntemleri gelişmeye ve ilerlemeye oldukça açık bir konudur.

7. Kaynaklar

[1] http://andacmesut.trakya.edu.tr/bgt/ (Erişim Tarihi:2012)

[2] Dereli, Ç. , Dilbilimsel Steganografi Yöntemleri üzerine bir Araştırma, Yüksek Lisans Tezi, Ege Üniversitesi, İzmir, 2010.

[3] Cox J., Miller L., Bloom J., Fridrich J., Kalker T., 2008, Digital Watermarking and Steganography, Morgan Kaufmann.

[4] Johnson F., Jajodia S., 1998, Steganalysis of Images Created Using Current Steganography Software, Information Hiding, LNCS 1525, pp. 273-289.

[5] Katzenbeisser, S., Petitcolas, F.A.P., 2000, Information Hiding Techniques for Steganography, Artech House, INC.

[6] Stallings W., 2006, Cryptography and Network Security Principles and Practices, Pearson Prentice Hall.

[7] Aktaş, Firdes , Steganaliz yöntemleri kullanılarak resim içerisindeki saklı bilgilerin tespit edilmesi, Yüksek Lisans Tezi, Hacettepe Üniversitesi, Ankara, 2011.

[8] Chandramouli R., Subbalakshmi K.P., 2004, Current Trends in Steganalysis: A Critical Survey, Control, Automation, Robotics and Vision Conference,USA, Vol.2, 964-967.

[9] Westfeld, A., Pfitzmann, A., "Attacks on Steganographic Systems", Proceedings of the Third International Workshop Information Hiding, Dresden, Germany, 61-76 (2000).

[10] Fridrich, J., Du R., Meng, L., "Steganalysis of LSB Encoding in Color Images",Multimedia and Expo, 2000. ICME 2000. 2000 IEEE International Conferece, New York City, USA, 3: 1279-1282 (2000).

[11] Proves, N., Honeyman, P., "Detecting Steganographic content on the internet", Tech. Rep. CITI 01-1a, University of Michigan, 1-14 (2001).

[12] Farid, H. "Detecting Steganographic Messages in Digital images." Technical Report TR2001-412, Dartmouth College, 1-9 (2001).

[13] Fridrich, J., "Minimizing the embedding impact in steganography", Proceeding of the 8th Workshop on Multimedia and Security, Geneva-Switzerland, 2-10, (2006).

[14] Hassan, D.M., Steganaliz yaklaşımların karşılaştırılması, Y. Lisans Tezi, G.Ü.,Ankara, 2008.