Steganografi

Metin Bilgin[1]

[1] Tophane Teknik ve Endüstri Meslek Lisesi, BURSA

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. 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.

Anahtar Kelimeler: Steganografi, Kriptografi, Bilgi Gizleme

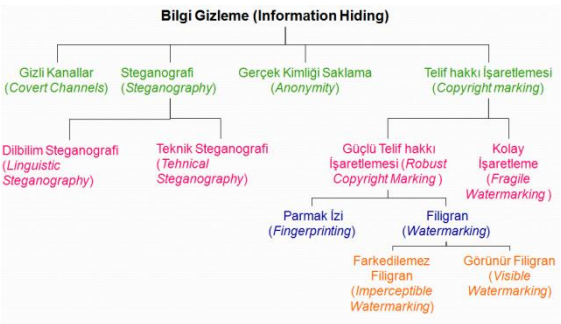
Steganography

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’ . The aim is to hide the data which is wanted to bereceived and this data' s existance, averting to detected from anyone else. In Steganography, the person who sent the data get the confidential data if only he knows the key information.

Keywords: Steganography, Cryptography, Information Hiding

1. Giriş

Bilgi gizleme, bir mesajın ya da bilginin, herhangi bir masum görünüşlü ortam içerisine saklanarak bir diğer kişiye ulaştırılmasıdır [4].



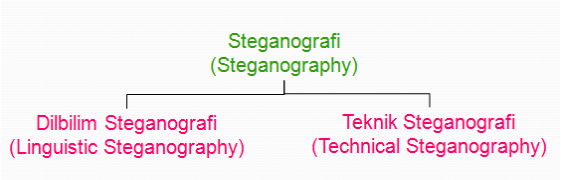
Şekil 1 Bilgi Gizleme

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 [1].

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)

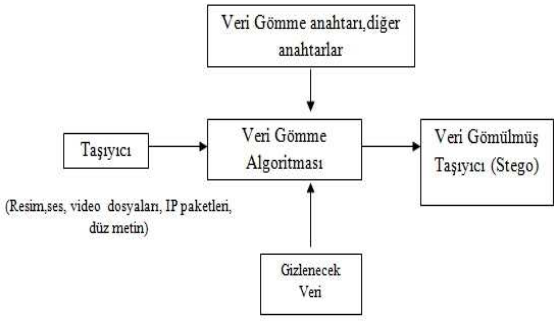
Steganografi kendi içinde iki kısma ayrılır [4].



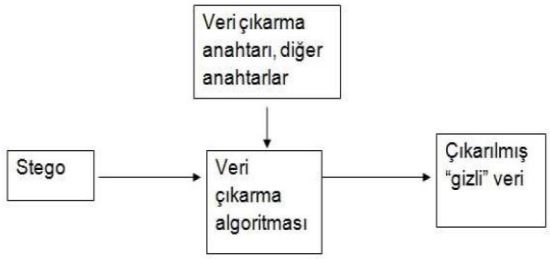
Şekil 2 Steganografi Kısımları

Kriptografiden farklı olarak steganografide bilginin şifrelenmesi önemli değildir. Kriptografi, sağlamlığını şifreleme algoritmasından alan ve iletilmek istenen verinin varlığının bilinmesinden çekinmeyen bir bilimdir. Dolayısıyla, kriptografide verinin hangi kanalla taşınacağı önemsenen bir durum değildir, fakat ne kadar sağlam olursa olsun hiçbir algoritma çözülemez değildir. Bundan farklı olarak steganografide, verinin nasıl taşınacağı saklanmak zorundadır [1].

Steganografide önemsenen nokta, verinin varlığının gizlenmesidir. Verinin varlığı ne kadar iyi gizlenebilirse, taşınacak veri o kadar güvendedir. Sıradan bir resim veya müzik dosyası kimsede kuşku uyandırmazken, içinde çok gizli bilgiler taşıyor olabilir. Alıcı dâhil hiç kimse anahtar bilgi olmadan, verinin nerde saklandığını bilmeden, bundan kuşkulanmaz. Bu yüzden steganografide, alıcının elinde, verinin hangi kanalla taşınacağı ve mesajın nasıl çözülebileceği bilgileri olmadan verinin karşı tarafa iletilmesi hiçbir önem taşımaz. Şekil 3 ve Şekil 4'de veri gömme ve çıkarma prosedürleri görülmektedir [1].



Şekil 3 Steganografi'de veri gömme prosedürü



Şekil 4 Steganografi'de gizli veriyi çıkarma prosedürü

Günümüzde yaygın olarak kullanıldığı bilinmekle birlikte, steganografinin tarihteki ilk ortaya çıkışı M.Ö. 400lu yıllarda olmuştur. Herodot tarafından anlatılan ve steganografinin tarihteki ilk bilinen örneği, M.Ö.440 yılında Demaratus'un Yunanistan'a yaklaşan bir saldırı tehlikesini, tahta bir tabletin üzerine kazıdıktan sonra üzerini balmumu ile kaplamasıdır. Üzeri balmumu ile örtülü tablet hiçbir şekilde dikkat çekmezken, ısıtılarak mumun eritilmesi sonrasında, tabletteki saldırı uyarısı ortaya çıkmıştır. Bu ilk örnek olmakla birlikte Eski Yunan'da balmumuyla kaplanan tahta tabletlerin kullanımına birçok örnek vardır [1].

Bir başka eski örnek de bir kölenin saçlarının kesilerek verilmek istenen bilgini dövme şeklinde yapılışı ve kölenin sacları uzadıktan sonra mesajın ulaştırılması gereken yere gönderilmesidir. Köle mesajın gideceği yere ulaştıktan sonra sacları tekrar kesilmiş ve böylece mesaj güvenli olarak karşı tarafa ulaştırılmıştır.

Bilinen ilk örnekleri bunlar olan steganografi, ikinci dünya savaşında da sıkça kullanılmıştır. Amerika'da yaşayan bir Japon ajanının, oyuncak bebek siparişi gibi görünen mesajlarla diğer ajanlarla ve hükümetiyle gizli bir şekilde mesajlaşması, Fransızların görünmez mürekkep kullanarak gönderilen postaların üzerine bir takım notlar saklaması, mektup pullarının arka yüzeylerine yazılan bir takım notlar da steganografinin 20nci yüzyıldaki yaygın kullanımına örnek olarak gösterilebilir. Bir diğer örnekse ikinci dünya savaşı sırasında Alman bir casus tarafından gönderilen bir telgraftır;

“Apparently neutral’s protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-product, ejecting suets and vegetable oils.”

Bu yazıda her kelimenin ikinci harfleri alınıp yan yana koyulduğu zaman Alman casusun göndermek istediği gizli mesaj elde edilmektedir;

“Pershing sails from NY June 1” [1]

2. Steganografi Neden Önemlidir?

“Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."

United Nations Universal Declaration of Human Rights

Birleşmiş Milletlerin uluslar arası insan hakları deklarasyonuna göre, her insan, düşünme ve açıklama özgürlüğüne sahiptir. Elbette ki bu özgürlükler, başkalarının menfaatlerine zarar vermeye başladığı anda önlenmek istenecektir. Bununla beraber kişilere, topluluklara veya devletlere zarar verebilecek her turlu bilgi de ciddi sonuçlar doğurmadan engellenmelidir. Teknolojinin getirdikleriyle birlikte, kişisel iletişimler dâhil her turlu konuşma veya bilgi alışverişi takip edilmektedir. Bilgiyi saklamayı amaçlayan kriptografi biliminin kullanımı sonucu ortaya çıkan veriler ve cümleler, doğal dil davranışlarına veya doğal verilere benzemediği için daha fazla dikkat çekecektir. Bu yüzden artık bilgiyi saklamaktansa bilginin varlığını saklamak daha etkili ve gerekli hale gelmiştir. İşte bu noktada steganografi, taşıyıcı medyanın içindeki bilgiyi değil de bilginin varlığını sakladığı için çok büyük önem kazanmıştır [1].

3. Steganografik Teknikler

Steganografik bir algoritma incelenirken 3 temel özelliğe dikkat edilmelidir:

• Değişimin fark edilememesi
• Saklanabilecek veri miktarı
• Dayanıklılık

Değişimin fark edilememesi ilkesi (birinci ilke) 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. Steganografik yöntemin kısıtlamalar olsa da bu tip saldırılara karşı belli bir dayanıklılık göstermesi gereklidir.

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. Yine benzer bicimde 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. Çeşitli düzeydeki ihtiyaçlar paralelinde önerilen algoritmalar başarılı olabilse de, göz önüne alınan tüm koşullar ve ikilemler karşısında olabilecek saldırılara dayanabilecek bir algoritmanın henüz bulunamadığı bilinmektedir.

Steganografide kullanılan yöntemleri

• Değiştirmeye dayalı yöntemler
• İşaret İşlemeye dayalı yöntemler
• İstatistiksel yöntemler
• Diğer yöntemler

Olarak dört ana grup altında inceleyebiliriz [1].

4. Steganografi Çalışmaları

Bender ve arkadaşlarının (1996) kaleme aldığı makalede, resim, ses ve metin gibi dosya türleri içerisine veri saklama teknikleri detaylı bir şekilde açıklanmıştır. Ses içerisine, düşük bit kodlaması (Low Bit Encoding), faz kodlaması (phase coding), yayılmış spektrum (spread spectrum) ve yankı veri saklaması (echo data hiding) yöntemleriyle veri saklanması ve metin içerisine boşluk kullanımı, konumsa dilinin yapısı ve eşanlamlı kelimelerden faydalanarak veri saklama yöntemleri bu çalışmada ayrıntılı bir şekilde irdelenmiştir [2].

2000'li yıllardan sonra, LSB (Least Significant Bit) yöntemiyle, BPCS (Bit Plane Complexity Segmentation) yöntemiyle, dönüştürme tekniğiyle ve permutasyon tekniğiyle resim içerisine veri saklama çalışmaları gerçekleştirilmiştir [2].

Lee ve Chen (2000), LSB yöntemiyle ve anahtar kullanılarak, gri seviyeli resimlerde, piksel değerini oluşturan bitlerin ilk dördünün modifikasyonu ile %50 ye yaklaşan kapasiteyle veri saklamışlardır [2].

Niimi ve ark. (2002), BPCS yöntemini temel alarak palet tabanlı resimler içerisine veri saklayan ve paletteki renk vektörlerinin sırasına bağlı olmayan bir metot geliştirmişlerdir [2].

Noda ve ark. (2002), kayıplı sıkıştırma gerçekleştiren resimler üzerinde BPCS yöntemiyle veri saklayan diğer bir çalışma yapmışlardır. Bu çalışmada, sıkıştırma işlemi esnasında, wavelet katsayılarının niceleme (quantization) işlemiyle bit düzlemine döndürülmüş hali üzerinde BPCS yöntemiyle veri saklama gerçekleştirilmiş ve %9 ile %15 arasında değişen kapasitelerde veri saklanabilmiştir [2].

Sağıroğlu ve Tunckanat (2003), gri seviyeli Bitmap resimleri içerisine, görsel olarak fark edilmeksizin, en önemsiz 4. bit seviyesine kadar, LSB modifikasyonu yöntemiyle veri saklanabileceğini gösteren Türkçe bir yazılım geliştirmişlerdir [2].

Tseng ve Chang (2004), JPEG resimleri içerisine, yine sıkıştırma işlemi esnasında daha fazla saklama kapasitesi ile veri saklayabilen bir yöntem geliştirmişlerdir [2].

Brisbane ve ark. (2005), palet tabanlı renkli resimler içerisine, yüksek veri saklama kapasitesiyle, şeffaflığa zarar vermeksizin veri saklayabilen bir yöntem geliştirmişlerdir [2].

Akleylek ve Nuriyev (2005), geliştirdikleri acık anahtar ve gizli anahtar çiftiyle çalışan bir şifreleme sistemiyle, resim dosyalarının en az önemli bitlerini değiştirerek veri saklayan bir yöntem önermişlerdir. AS knapsack ismini verdikleri şifreleme sistemi sayesinde göndericinin alıcıya yolladığı veriyi inkar edememesi ve alıcının göndericinin ilettiği gerçek veriyi görebilmesi sağlanmıştır. Saklama sonrası oluşan resim dosyalarının fiziksel boyutunun, orijinal resim dosyasından farklı olduğu belirtilmiştir [2].

Shahreza (2006), mobil telefonlarda SMS (Short Message Service) altyapısıyla kullanılan siyah-beyaz resimler içerisine metin saklayarak, SMS yoluyla gizli mesajlaşmayı sağlayan bir çalışma sunmuştur. Siyah-beyaz resimlerin, yapılacak modifikasyonlara karsı, renkli resimlere oranla çok daha dayanıksız olması ve saklama boyutunun küçüklüğü gibi dezavantajlarına rağmen, SMS'lerdeki siyah beyaz resimler içerisine veri saklama yöntemi, İngiltere'de yakın zamanda hayata geçirilen Gizli-Metin SMS fonksiyonuna göre, 40 saniye içinde, alınıp görüntülenen mesajın imha edilmesinin gerekmemesi ve kullanılacak mobil telefonlarda WAP uyumluluğunun aranmaması gibi nedenlerle, daha avantajlı bir yöntem olarak değerlendirilmiştir [2].

Chou ve ark. (2001), transformasyon tekniklerini kullanarak, o donemde mevcut olan ses içine veri saklama sistemlerinden daha fazla oranda veri saklanabileceğini tespit etmişlerdir [2].

Cvejic ve Seppanen (2002), LSB modifikasyonu ile ses içerisine veri saklama kapasitesini %33 oranında arttıran bir yöntem geliştirmişlerdir. Gopalan (2003), ses dosyası içerisine, en az önemli bit modifikasyonu ile veri saklanması üzerine çalışma yapmış ve kokpit sesi gibi ses dosyaları içerisine daha fazla bit seviyesinde veri saklanabildiğini göstermiştir [2].

Adli ve Nakao (2005), internette sıkça kullanılan küçük boyutlu midi ses dosyaları içerisine, LSB yöntemi, tekrarlanan komut kodları algoritması ve sistem harici kodları algoritmasını kullanarak veri saklayan bir çalışmayı sunmuşlardır. Resim ve ses dışındaki dosya türleri de veri saklama çalışmalarında kullanılmaya başlanmıştır [2].

Sui ve Luo (2004), yardımlı metin (hypertext) içerisine, boşluklar ekleme yerine biçimleme (markup) etiketlerinin pozisyonlarını değiştirerek veri saklayan bir çalışma sunmuşlardır. Bu çalışmanın sonucunda, uyguladıkları yöntemin su an için, her ne kadar ses ve resim içerisine veri saklama yöntemlerine göre henüz zayıf olsa da, ilerideki bilgi güvenliği sistemleri acısından potansiyel değerinin tahmin edilemez olduğunu rapor etmişlerdir [2].

5. Sonuç ve Öneriler

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. Taşıyıcıdaki değişim, dayanıklılık ve kapasite özelliklerinden hangisi bizim için daha önemliyse bu duruma göre daha uygun olan yöntem veri gizleme işlemi için kullanılmalıdır.

Steganografik yöntemler şifreleme yöntemleri ile birlikte kullanılarak daha güvenli bir sistem oluşturulabilir. Saklanacak verinin miktarı arttırılmak istenirse de gizlenecek verinin gizleme işleminden önce sıkıştırılmasıyla bu sağlanabilmektedir.

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 her gün 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 [3].

Kaynaklar

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

[2] Atıcı, M.A. , Steganografik Yaklaşımların İncelenmesi, Tasarımı ve Geliştirilmesi, Yüksek Lisans Tezi, Gazi Üniversitesi, Ankara, 2007.

[3] Şahin, A., Görüntü Steganografide Kullanılan Yeni Metodlar ve Bu Metodların Güvenilirlikleri, Doktora Tezi, Trakya Üniversitesi, Edirne, 2007.

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

[5] web.itu.edu.tr/~orencik /Steganografi.ppt (Erişim Tarihi:2012)