

Milattan önce 5.inci yüzyılda Pers Kralı Daryus'un elinde tutsak olan eski Yunanlı komutan Histiaeus, Anadolu'da Milet şehrindeki damadı Aristagoras'a gizli bir mesaj göndermek istedi. Histiaeus kolesinin basını tras ettirip mesajı dogme yaptırdı. Saçları dogmeyi ortecek kadar uzadığında kole Milet şehrine gönderildi. İste Herodot, bilgi saklama sanatı steganografinin eski zamanlardaki ilk uygulamalarından birisini böyle haber veriyor. Sanat geliserek çağlar boyunca insanların gizli bilgileri birbirlerine göndermelerini sağladı. Eski Romalılar mektup satırları arasına gizli mesajlarını meyva özleri, süt gibi tabii kaynaklardan elde ettikleri görünmez murekkeplerle yazdılar. Bugün bile çocuklar casusculuk oyunlarında, ancak isitildiğinde görülen murekkeplerle gizli mesajlar yazıyorlar. İkinci Dünya savaşında Almanya'da mikro-nokta (microdot) teknolojisini geliştirildi. Gizli mesaj, plan ve harita gibi dokümanlar fotografik metodlarla nokta boyutlarına küçültülüp mektuplarda noktali harf ve noktalama işaretlerinin üzerine yapıştırılarak saklandı. Steganografinin yaygın kullanılması karşısında mütefikler de gazete kupurları, orgu tarifleri, çocukların çizdikleri resimler gibi mikro-noktaların kolaylıkla gizlenebileceği malzemelerin posta ile gönderilmesini yasakladı. Sovyet Rusya'da yurtdışından gelen ve yurtdışına gönderilen bütün mektuplar teker teker acilip incelendi.

Tabii teknolojinin hızlı gelişimi bu tedbirleri bosa çıkardı. Artık herkes (!) steganografinin avantajlarından kolaylıkla yararlanabiliyor. New York ve Washington'da yapılan saldırılardan sonra da teroristlerin eBay, Usenet ve Amazon gibi popüler web sitelerinde hatta porno sitelerinde bilgi saklı resimler kullanarak haberleştikleri iddia edilmisti. Resimlerde saklı bilgileri tesbit etmek için yapılan çalışmalarda, özel analiz programları kullanılarak iki milyonun üzerinde görüntü dosyası incelendi. Beyaz Saray savaşın başlamasından sonra televizyon kanallarını, gizli mesajlar taşıyabilecek teroristlerin video görüntülerini yayınlamamaları konusunda uyardı.

Uzmanlar internetten en az 28 steganografi yazılımının freeware veya shareware olarak yüklenebileceğini belirtiyorlar. Steganografi yazılımlarının kullanımının çok kolay olması ve bilginin saklanmadan önce şifrelenemesi ulusal güvenlik birimlerinde endişelere sebep olmaktadır. İnternet üzerindeki yoğun e-mail trafiği içinde şifrelenmiş mesajlar ateş böcekleri gibi dikkat çekiyor, gizli mesajlar saklayan yazı, ses ve görüntü dosyaları ise kalabalığa karışabilirler!

Steganografik Yazılım

Bilgisayarla steganografi iki temel prensipten yararlanmaktadır. Birincisi sayısallaştırılmış görüntü veya ses kaydedilmiş dosyaların içeriklerinin, görüntü veya ses kaydına zarar vermeden bir dereceye kadar değiştirilebilmesidir. Diğer prensip ise, insanların görüntü, renk ve ses kalitesindeki ufak değişiklikleri fark edememesidir.

Yazı dosyalarında kullanılan bilgi saklama teknikleri: satır aralıklarının, kelime aralıklarının ve harf özelliklerinin değiştirilmesidir. Satır aralıklarını milimetrenin ondan bir kadar farklılaştırmak, basit ölçümler yaparak en kolay yakalanabilen yöntemdir. Kelime aralıklarındaki farkları yakalayabilmek için, metnin aynı font ve puntoda yeniden yazılması ve karşılaştırılması gereklidir. Kuyruklu harflerin (b, p, h gibi) uzunluklarını değiştirmek metin üzerinde yoğun bilgi saklamakta kullanılan, farkedilmesi güç bir tekniktir.

Bilgi saklamak için, gereğinden fazla detay taşıyan 16-bit ses, 8-bit veya daha da detaylı 24-bit görüntü dosyalarından kolaylıkla faydalanılmaktadır. Görüntü dosyalarında piksel renklerinin en az değerli (least significant) bit'lerinin değiştirilmesi görüntü üzerinde gözle farkedilebilir bir değişiklik yapmamaktadır.

S-Tools Windows95/98/NT için yazılmış en iyi ve en çok kullanılan programlardan birisidir. Bu programı kullanarak .gif, .bmp ve hatta .wav dosyaları için bilgi saklayabilirsiniz. İlave olarak S-Tools saklanacak bilgileri şifrelemek özelliğine de sahiptir. Simetrik anahtarlı şifreleme algoritmalarından DES (modası geçti), veya günümüzde tercih edilen 3-DES veya IDEA algoritmaları kullanılabilir.

Steganografi uygulanmış dosyalar tek başlarına tamamen masum görünmekte, ancak orijinali ile karşılaştırıldığında farkedilebilmektedir. Başarılı bir uygulama için herkesin iyi tanıdığı resimlerin kullanılmaması, daha çok yarım tonların belirgin olduğu görüntülerin tercih edilmesi tavsiye edilebilir.

Başarılı bir başka steganografi ürünü de Steganos Security Suite. Bu paketin içinde şifrelenmiş sanal sürücü, İnternet iz silici, şifreleyici gibi güvenlik araçları bulunuyor. Saklamak istediğiniz bilgiler AES ve Blowfish şifreleme algoritmaları kullanılarak şifrelenip .bmp ve .wav dosyalarına yerleştirilebilmektedir. Soru yaparken ziyaret ettiğiniz siteler ile ilgili bilgiler bilgisayarınızda saklanmakta ve merak eden kişilerin İnternetteki faaliyetlerinizi izlemesine imkan vermektedir. Steganos Suite içinde yer alan İnternet iz silici ile bu bilgileri de bilgisayarınızdan silebilirsiniz. Yine Suite içinde yer alan Shredder programı silinen alanları bozarak bu bilgilere erişimi imkansız hale getirmektedir. Şekil-1'deki resim için Steganos Security Suite ile bir yazı dosyası saklanarak Şekil-2'deki resim oluşturulmuştur.

Scramdisk, steganografik özelliklere sahip diğer bir şifreleme programı. Bu programı kullanarak .wav dosyalarını şifrelenmiş sanal sürücü haline getirip saklamak istediğiniz bilgileri bu dosyalara kaydedebilirsiniz. Şifrelenmiş partiyon orijinal dosyanın %25'i ile %50'i arasında yer kaplayabilmektedir.

Sayısal Watermarking (Filigran)

Lazer yazıcılar, hatta fotokopi makinaları yaygınlaşmadan önce, kirtasiyecilerden sayı ile aldığımız ithal dosya kâğıtlarında işiga tutulduğunda seçilen gizli damga baskılarını hatırlayabilirsiniz. Kâğıt banknotlar üzerinde yer alan filigranlar da ancak işiga tutulduğunda görülebilir. Modern Steganografi uygulamalarından bahsederken anlatılması gereken sayısal watermarking de görüntü ve ses dosyalarında kopyalanmayı önlemek amacıyla damgalar bırakıyor. Özel programlar kullanılarak okunabilen bu damgalardan dosyanın üretildiği tarih, copyright sahibi, üreticiye nasıl ulaşılacağı gibi bilgiler elde edilebiliyor. Eğer bir tasarımcı iseniz, hergün pek çok yeni ürünün kopyalandığı, çalıştığı İnternet ortamında, ürünlerinizi korumak için bu teknolojiye yararlanabilirsiniz.

İnternet üzerinde watermarking ürünleri pazarlayan pek çok firma var. Digimarc, milyonun üzerinde satış yaptığını iddia eden onca firmalardan. Photoshop veya CorelDraw ile birlikte plug-in olarak kullanılabilen PictureMarc veya kendi başına kullanılabilen ReadMarc'ın website'lerinden ücretsiz olarak indirebilirsiniz. Digimarc, İnternette yayınlayacağınız görüntüye watermark yerleştirmek için Creator ID isimli ürününü bir yıl için bedava kullanıma sunuyor. Firmanın şirketlere yönelik bir başka ürünü de İnternette watermark koyduğunuz ürünlerinizin peşine düşen ve izinsiz kullanımları yakaladığında raporlayan MarcSpider.

Artık sanatçı ve şirketlerin İnternette yayınladıkları görüntü ürünlerini watermarking uygulayarak koruyabileceklerini düşünüyorsanız, yanılıyorsunuz. Watermarking ile korunmuş görüntüler parlaklık ve kontrast ayarlarının değiştirilmesi, özel filtrelerin kullanılması, kâğıda baskı veya tarama gibi bir çok yöntemle karşı koyabiliyor. Ancak StirMark ve UnZign gibi,

watermarking teknolojisinin internette uygulanmasından hemen sonra ortaya çıkan bazı programlar kullanılarak damga bertaraf edilebiliyor. Aslında, kullanıcıların watermarking algoritmalarının etkinliğini değerlendirmeleri için hazırlanan bu programlar maalesef aynı zamanda resim kalitesine pek zarar vermeden watermarking izlerini de yok edebiliyor.

Sonuç olarak, tedbirler ve karşı-tedbirler, hepsi benzer düşünce, gayret ve teknoloji ürünü. Gecici savunma, karşı-tedbirlerin herkesin eline kolaylıkla geçmeyeceği varsayımına dayanıyor.

GIF Görüntülerinde Renk Modeli

GIF görüntülerinde kullanılan renkler, 0 ile 255 arası değer alabilen uçlu kümelerle ifade edilmektedir. İlk sayısal değer kırmızı, ikincisi yeşil ve sonuncusu da mavi tonlarına karşı gelmektedir. Sayısal değer büyüdükçe renk daha koyulasmaktadır. Üç temel renkten faydalanılarak arzulanan renk oluşturulmaktadır. RGB (Kırmızı-Yeşil-Mavi) renk modelinde $256 \times 256 \times 256 = 16,777,216$ değişik renk ifade edilebilmektedir.

R (Kırmızı)

G (Yeşil)

B (Mavi)

Kırmızı

255

0

0

Yeşil

0

255

0

Mavi

0

0

255

Sarı

255

255

0

Beyaz

255

255

255

Siyah

0

0

0

GIF görüntüsünde kullanılacak renklerin listesine palet adı verilmektedir. Günümüzde İnternette erişilebilen GIF görüntülerinde genellikle 8-bit paletler kullanılmaktadır. 8-bit sayılarla ancak 255 farklı değer oluşturulabildiğinden, her GIF görüntüsünde = 16,777,216 renkten ancak 255 değişik renk seçilebilmektedir.

GIF görüntüsü piksel adı verilen hücrelerden oluşan bir tablodur. Her hücrede yer alan sayı görüntü paletindeki bir rengi göstermektedir.

Steganografik Kodlama Örneği

Steganografi programı GIF görüntüsünün renk paletininin bir kopyasını oluşturur. Yeni palette renkler, renk modelindeki sıralarına göre yeniden düzenlenir. Piksellerde yer alan sayıların (ikilik sistemde) en az değerli basamakları saklanacak mesajdan bir basamaklık bilgi ile değiştirilir.

Palette oluşturulan yeni sayının gösterdiği renk bulunur. Piksele rengin orijinal paletteki numarası yazılır. Artık piksel, mesajdan alınan bilgiye göre eski rengini veya palette yer alan yakın bir rengi göstermektedir.

Renk Paleti
Sıra Numarası
Renk Kodu

28
67,365,897

29
69,321,456

30
67,500,788

31
66,552,639

…..
…..

1,589 numaralı piksel
28

Programın oluşturduğu sıralı palet

Sıra Numarası
Renk Kodu

14 (0000 1110)
66,552,639

15 (0000 1111)
67,365,897

16 (0001 0000)
67,500,788

17 (0001 0001)
69,321,456

…..
…..

Mesajdan alinan sayi
0

67,365,897 numarali rengin yeni palette karsiligi 15 (0000 1111)’dir. Son basamak degistirildiginde (0000 1110) yeni palette gosterilen renk 66,552,639. Bu rengin orijinal paletteki sira numarasi 31’dir.

Islemden sonra

1,589 numarali piksel
31

Cozumlemek icin once sirali paletteki rengin sira numarasina ulasilir. Sira numarasinin son basamagindaki sayi saklanan mesajdan alinmistir

Erdal CAKMAK

bilgicenneti.com