T.C.
İSTANBUL TEKNİK ÜNİVERSİTESİ
Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı

BİLGİSAYAR AĞLARINDA GÜVENLİK
Prof. Dr. Bülent ÖRENCİK

Steganografi
Dönem Raporu

Yük. Müh. Zekeriya Erkin
504042510

İçerik

Giriş 3
Steganografide Temel Yöntemler 5
Yer Değiştirmeye Dayalı Yöntemler 6
İşaret İşlemeye Dayanan Yöntemler 9
Spektrum Yayılmasına Dayanan Yöntemler 11
İstatistiksel Yöntemler 14
Diğer Yöntemler 14
Sonuç 15
Kaynaklar 16

Steganografi

Giriş

Steganografi Yunanca “gizli yazı” anlamına gelmektedir. Taşınmak istenen mesajın bir başka masum görünüşlü ortamda saklanarak, üçüncü şahısların iletilen mesajın varlığından haberdar olması engellenir. Bu özellik kriptografi ile steganografi arasındaki en temel farkı oluşturmaktadır.

Kriptografide, üçüncü kişiler gizli bir iletişimin varlığını bilirler. Ancak, alıcı ve vericinin en temel varsayımı, üçüncü kişinin takip edebildiği gizli iletişimin içeriğini “makul” bir sürede çözememesidir. Oysa steganografide gizli iletişimin varlığı saklanmaktadır.

Steganografi eski çağlarda da gizli iletişim için oldukça yoğun kullanılmıştır. Yunan tarihçi Herodotus, eserinde İran’da bulunan casusun, Pers istilasını Yunanistan’a nasıl ilettiğini kaydetmektedir. Yazıya göre, casus kölesinin saçını kazıtmış; istila uyarısını da kafa derisine kazıtmıştır. Daha sonra yapılacak olan, kölenin saçının yazıyı kapatacak kadar uzamasını beklemek ve bu köleyi Yunanistan’a göndermektir. Kölenin bilmesi gereken tek bilgi “kafamı kazıyın” olacaktır. Yine aynı kaynakta avcı kılığındaki bir ulağın, avladığı hayvanın karnına parşömen saklayarak Yunanistan’a girmesi anlatılmaktadır. Steganografinin kullanımı yalnızca Yunanistan ile sınırlı değildir. Çinliler de kendi kaynaklarında meyve sepetini nasıl gizli iletişim için kullandıklarını anlatmaktadırlar. Meyve sepetindeki her meyvenin birbirine göre pozisyonu farklı bir anlam ifade edecektir.

Antik dönemdeki bu basit uygulamalar steganografinin gizli iletişimdeki kullanımının insanlık kadar eski olduğunu bizlere göstermektedir. Ancak, çarpıcı kullanımı ikinci dünya savaşında kendini göstermektedir. İkinci dünya savaşı esnasında Alman casusların kimyevi bir madde ile beyaz bir mendile yazdıkları ortaya çıkartılmıştır. Casus, gizli mesaj içeren bu mendili daha önce belirlenen noktalarda çöpe atmakta; alıcı ise yine kimyevi maddeler kullanarak bu yazıyı okumaktadır. Yine ikinci dünya savaşı döneminde Almanlar “mikrofilm” teknolojisi kullanarak “mikro noktalar” (microdot) kullanmıştırlar. Bu yöntemde A4 büyüklüğündeki herhangi bir belge veya çizim bir dizi işlem sonrasında daktilo yazısında kullanılan bir nokta kadar küçültülmektedirler. Bu yöntem kullanılarak masum içerikli bir sayfa düz metindeki i ve j harflerinin noktalarına oldukça büyük miktarda veri saklamak mümkün olmuştur.

Aşağıda, ikinci dünya savaşında kullanılan bir steganografi örneği verilmiştir.

"Apparently neutrals protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretex for embargo on by-products, ejecting suets and vegetable oils."

Yukarıda verilen paragrafta her kelimenin ilk harfleri yan yana getirildiğinde

"Pershing sails from NY June 1."

mesajı ortaya çıkmaktadır.

Steganografinin bu tür uygulamaları genellikle kimyasal bazı işlemler gerektiren sınırlı yöntemlerdir. Oysa günümüz teknolojisi, bilgisayarların bize sağlamış olduğu işlem gücü ve sayısal ortamda saklanan veriler ile steganografi uygulamaları için oldukça uygun bir ortam sağlamaktadır. Gizli veri, yine masum içeriğe sahip olan bir dizi dosyanın içinde saklanabilmektedir. Bunlardan en ilgi çekicileri, vermiş oldukları olanaklardan dolayı, resim, ses ve görüntü dosyalarıdır. Benzer bir şekilde düz metin dosyaları, sabit disklerdeki kullanılmayan alanlar, IP paketlerinin ileride kullanmak üzere ayrılmış bölümleri gizli verinin saklanması için kullanılabilmektedir.

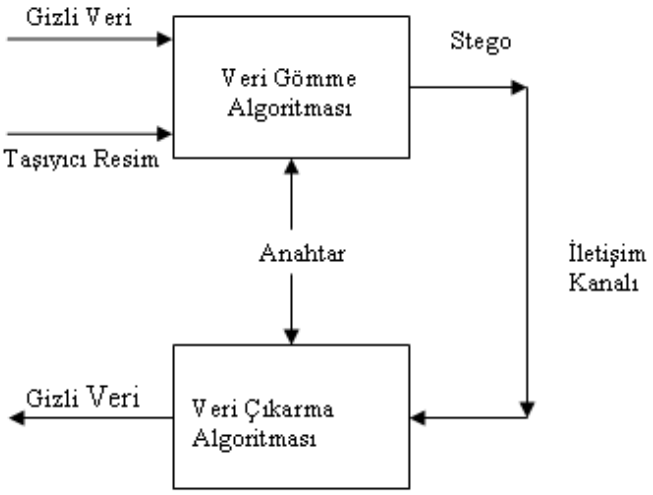
Steganografi iletişimin gizliliğini sağlamaktadır. Bilgi teknolojilerinin 70'li yıllardaki başlayan hızlı gelişimine rağmen steganografinin adının anılması 90'lı yılların sonuna denk gelmektedir. Bunda iki önemli unsurun etkisi vardır: Bunlardan ilki Amerikan hükümetinin uzun yıllardır uyguladığı güçlü kriptografik algoritma ihracının sınırlandıran yasa ve 11 Eylül saldırıları.

Amerikan hükümeti ve hükümetin ulusal güvenlik ajansının işletim sistemlerinde kullananlar dâhil tüm kriptografik uygulamalara ve bunlarda kullanılan anahtar uzunluğuna getirmiş olduğu sınırlandırmanın amacı ortadır. Bu sınırlandırmanın kişisel gizliliğe zarar verdiği gerekçesiyle aralarında PGP programının yazarı olan Phil Zimmerman dâhil birçok bilim adamı iletişimin gizliliğine dayanan steganografik yöntemlere vurguda bulunmuştur. Oysa 11 Eylül saldırılarını planlayanların kanıtlanamasa bile steganografik yöntemlerle iletişime geçtikleri kuşkusu Amerikan hükümetini harekete geçirmiştir. Günümüzde birçok hükümet kuruluşu ve akademik dünya steganografi konusunda çalışmaktadır. Steganografi kadar gizli iletişimin varlığını tespit etmekte kullanılan steganaliz de güncel bir konudur.

Bu raporda temel olarak resim dosyaları üzerinde çalışan steganografik algoritmalar incelenmiştir.

Steganografide Temel Yöntemler

Steganografi, gizli verinin masum içeriğe sahip ve taşıyıcı olarak adlandırılan bir başka veri içersinde saklanması olarak tanımlanabilir. Bu saklama işlemi için kullanılan algoritma gizli değildir ancak güvenlik algoritma için kullanılan anahtar ile sağlanmaktadır. İçersinde gizli veri bulunduran taşıyıcıya "stego" adı verilmektedir. Stego herhangi bir yolla alıcıya ulaştırılır. Alıcı veri saklama algoritmasının tersi olan bir işlemle gizli veriyi, anahtarı da kullanarak ortaya çıkarır (Şekil 1).



Şekil 1: Steganografi Sistemi

Steganografik bir algoritma incelenirken 3 temel unsur göz önüne alınmaktadır:

- Değişimin fark edilememesi
- Saklanabilecek veri miktarı
- Dayanıklılık

Resim üzerinde gerçekleştirilen değişiklikler insan gözü tarafından algılanmamalıdır. Aksi durum, birinci ilkenin ihlali ve gizli iletişimin ortaya çıkmasıyla sonuçlanacaktır. Öte yandan iletişim her ne kadar gizli de olsa üçüncü bir kişinin içerisinde gizli veri olan dosya üzerinde bazı işlemler yapma olasılığı vardır. Steganografik yöntemin bazı sınırlar içerisinde de olsa bu tür saldırılara karşı belli bir dayanıklılık sergilemesi gerekir. Steganografik algoritmalarda sağlanmak istenen, yüksek miktarda gizli verinin saklanabilmesidir. Maalesef, var olan algoritmaların tüm bu koşulları tam olarak sağlayamadığı bir gerçektir. Daha da kötüsü, bu koşullar arasında ciddi ikilemler vardır.

Taşıyıcı içerisine yüksek miktarda veri gömebilmek istenilen bir özelliktir. Ancak, veri miktarı arttıkça resim üzerindeki değişim insan gözüyle algılanabilecek sınırlara ulaşabilmektedir. Bu da kapasite ve değişim arasında bir ikilem yaratmaktadır. Yine benzer şekilde gömülen gizli verinin yapılan saldırılar sonucunda bile alıcı tarafında başarıyla çıkartılabilmesi için düşünülen dayanıklılığı arttırıcı önlemler ve/veya yöntemler yapılması gereken işlem miktarını arttırmakta ve yine dosya üzerinde yapılan değişimi belli edebilecek seviyeye ulaşabilmektedir.

Tüm bu koşullar ve ikilemler dâhilinde her türlü saldırıya göğüs gerebilecek bir algoritma henüz yayınlanmamıştır. Ancak, çeşitli düzeydeki ihtiyaçlar doğrultusunda önerilen algoritmalar başarılı olarak kullanılabilir.

Yer Değiştirmeye Dayalı Yöntemler

Bu grupta yer alan yöntemler temel olarak resim dosyasında renkleri temsil eden değerler üzerinde çalışmaktadır. Sayısal ortamda birçok resim dosya türü bulunur. Bu dosyalar temelde resimleri sıkıştırıp sıkıştırmadıklarına göre iki gruba ayrılabilirler. Ayrıca, her resim dosyası türü renk değerlerini farklı şekilde saklı tutabilirler. En yaygın türler parlaklık bilgisinin ön planda tutulduğu YCbCr ve HSV(HSB), renklerin ön planda tutulduğu RGB'dir. Yine bu türlerin her bir renk bileşenini nasıl tuttuğu ayırt edici olabilir. Örneğin üç renk değerinin de bir sekizlide tutulduğu RGB resim dosyaları ile her bir renk değerini ayrı ayrı üç adet sekizlide saklayan RGB resim dosyaları çeşitli yönden farklıdır. En önemli fark, temsil edilebilecek renk sayısıdır. Belirtilen ikinci temsil yönteminde çok daha fazla renk değerini barındıran resim dosyalarını saklamak mümkündür. Ancak, resim dosyasının bu bilgileri saklamak için çok daha fazla yere ihtiyaç duyacağı da açıktır.

Şekil 2 Y bileşeni

Şekil 3 Cb bileşeni

Şekil 4 Cr bileşeni

Şekil 5 H bileşeni (HSV)

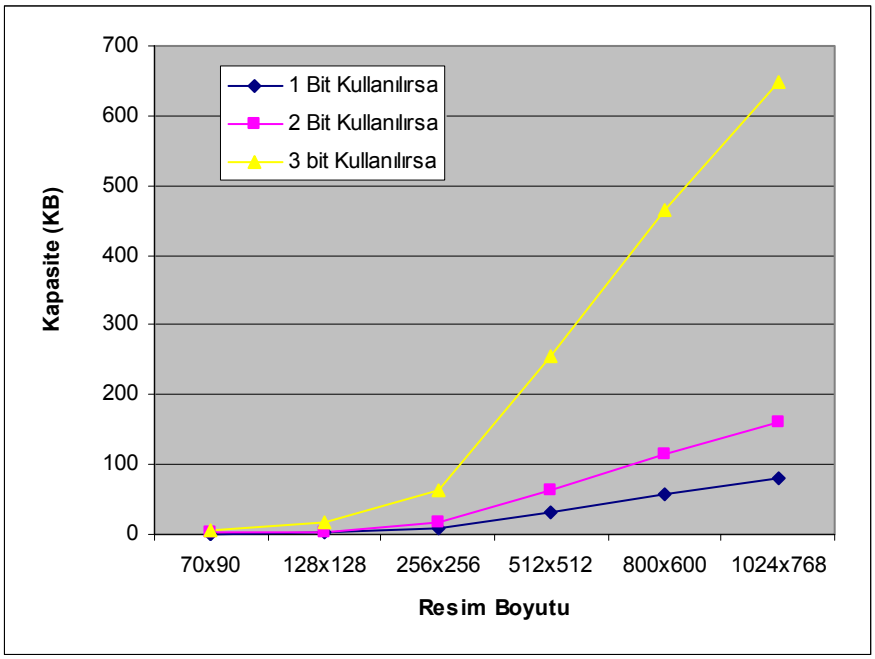
Şekil 6 S bileşeni (HSV)

Şekil 7 V bileşeni (HSV)

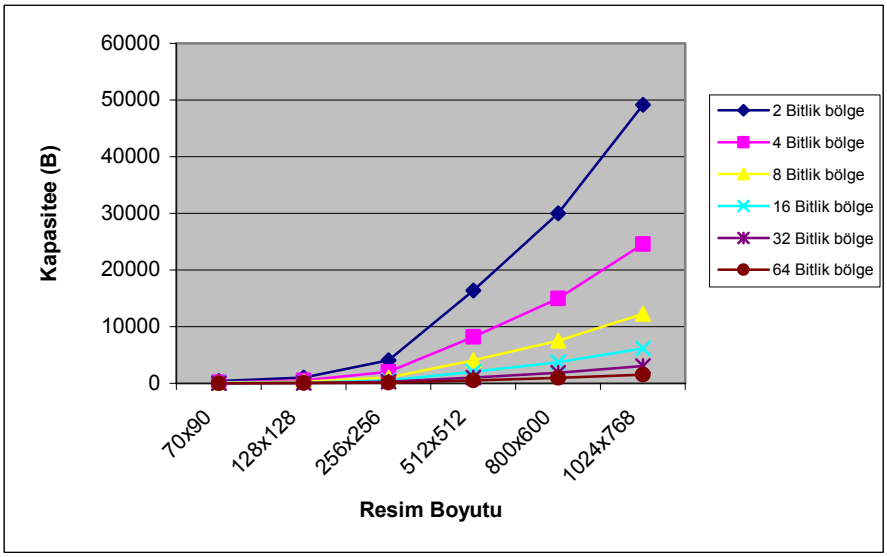
Yer değiştirmeye dayalı steganografik yöntemlerde çalışma ilkesi oldukça basittir. Renk değerinin tek bir sekizlide tutulduğunu varsayalım. Bu durumda 256 adet farklı renk değerini resim dosyasında temsil edebiliriz. Adı geçen yöntemde renk değerinin en düşük anlamlı biti ile gizli verinin bitleri değiştirilir. Sonuçta ortaya çıkacak resim dosyasındaki renk değerleri ya olduğu gibi kalır ya bir artar ya da bir azalır. Ancak, her üç durumda da söz konusu olan, bu durumun insan gözü tarafından algılanamamasıdır.

Yer değiştirmeye dayalı yöntemlerde, yer değişimi için kullanılacak bitlerin sayısı bir bitten daha fazla olabilir. Ancak, karar vermede, kullanılan resmin özelliği belirleyicidir. Resim dosyasında düz alanlar fazlaysa yapılan yer değiştirme işlemi çıplak gözle bile fark edilebilir. Öte yandan, steganografide unutulmaması gereken en önemli ilke, taşıyıcı dosyanın bir kere kullanılması ve sonra yok edilmesidir.

Yer değiştirmeye dayanan yöntemler temelde aynı ilke ile çalışmakla beraber birden fazla şekilde gerçeklenebilirler. Her bir renk değerinin değiştirildiği gerçeklemelerle beraber renk değerlerinin gruplanarak, eşlik değer olarak gizli veri bitinin kullanıldığı ve bu grubun eşlik bitine uyum sağlaması için gruptaki tek bir renk değerinin değiştirildiği yöntemler örnek olarak sayılabilir. Aralarında ki tek fark saklanacak veri miktarıdır.



Şekil 8: Yer değiştirme algoritmalarına dayanan yöntemlerin bilgi gömebilme miktarı



Şekil 9: Eşlik biti hesabına dayanan yöntemlerin kapasite miktarı

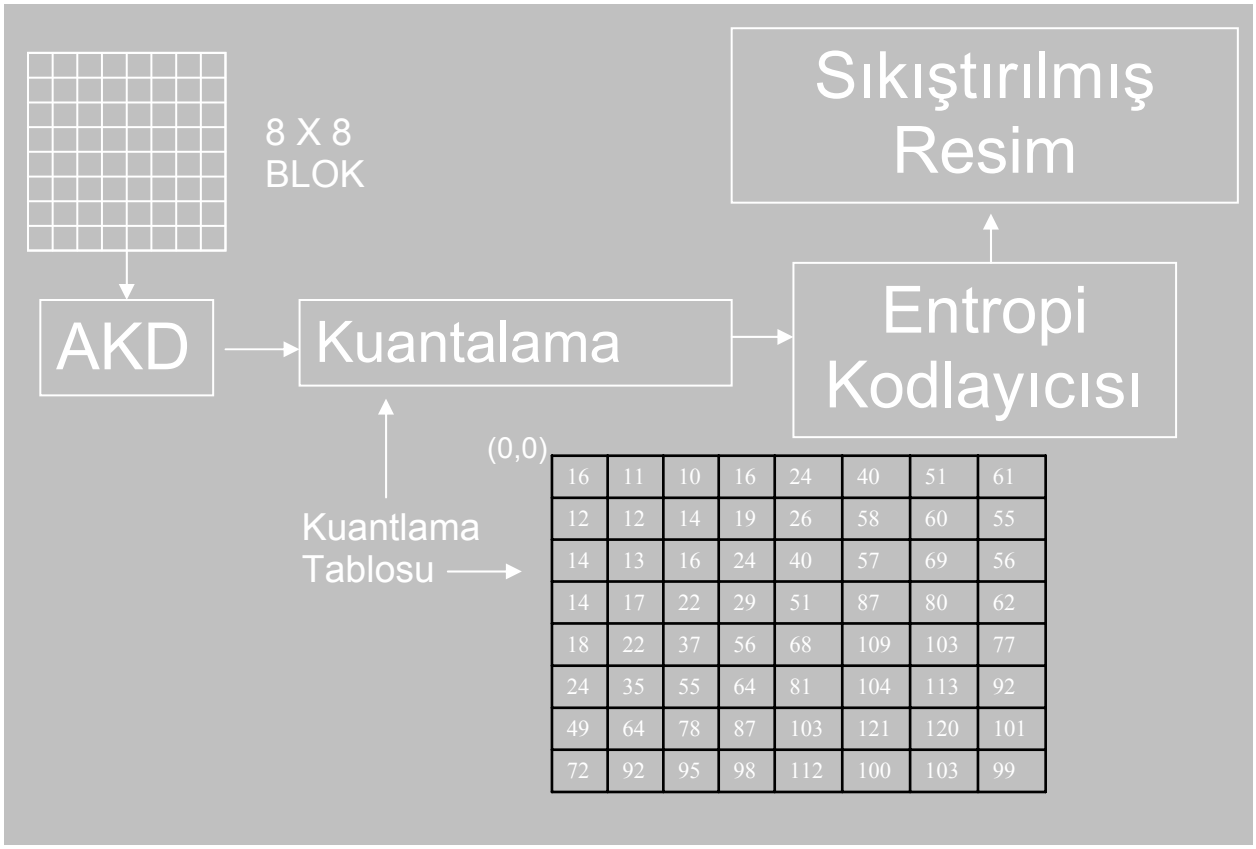
Yer değiştirme yöntemine dayanan gerçeklemeler oldukça kolay bir şekilde programlanabilir. Sunmuş oldukları yüksek veri saklama miktarı ile gizli iletişim için oldukça ilgi çekicidirler. Ancak, bu yöntemlerin karşılarında iki önemli engel vardır: bunlardan ilki resim dosyaların Internet trafiğinde yaratmış oldukları yükü azaltmak için sıkıştırılmaları ve yine bu yöntemlerin sıkıştırma başta olmak üzere en hafif resim işleme yöntemlerine karşı oldukça zayıf olmaları. Gizli veri bitlerinin taşıyıcı resme gürültü olarak eklendiğini hatırlayacak olursak, parlaklığın bile değiştirilmesi bu bilgilerin tamamen yok olmasına neden olacağı açıktır.

İşaret İşlemeye Dayanan Yöntemler

Günümüz bilgi dünyasında Internet en önemli bilgi kaynağı olarak algılanmaktadır. Bu inanılmaz büyüklükteki veritabanının ihtiyaçlara en uygun şekilde cevap verebilmesi için en önemli koşullardan biri sunucu ve istemci arasındaki iletişimin mümkün olduğu kadar kısa bir sürede, son kullanıcıyı memnun ederek sonlanmasıdır. Bu nedenle Internet trafiğinin düzenlenmesi konusunda oldukça fazla çalışma yapılmaktadır. Ancak, bilgiyi paylaşanlar en başta yaptıkları iyileştirici uygulama, Internet'e sunulan grafik dosyaların sıkıştırılmasıdır. Kaliteden biraz ödün vererek grafik dosyalarının büyüklüğü ile ciddi miktarda oynamak mümkündür. Internet kullanıcıları var olan resim sıkıştırma algoritmaları ile yüksek oranda verim alabilmektedir. Bu sıkıştırma algoritmaları içinde JPEG, GİF, PNG önemli yer tutar.

Tüm sıkıştırma algoritmaları insan gözünün filtreleme özelliğini kullanır. İnsan gözü belli bir frekanstan sonrasında ki renk değişimlerini algılayamaz. Dolaysıyla, asıl resimdeki renk değerleri frekans düzlemine taşınabilir. Frekans düzleminde kullandığımız dönüşüme göre çeşitli katsayılar karşımıza çıkacaktır. Bu katsayılar kullanılarak ters işlem sonrası tekrar asıl resmi elde etmek mümkündür. Ancak, asıl resmi elde etmek için sonsuz sayıda frekans bileşeninden yararlanmak gereksizdir. Belirli bir kaybı göze alarak yüksek frekans katsayılarından vazgeçilebilir. Vazgeçilen frekans sayısı tekrar elde edilen resmin kalitesini ortaya koyacaktır. Yapılan uygulamalarda resim kalitesinden küçük miktarlarda kalite kayıplarına karşın resim boyutunda 1:100 oranında küçültme mümkün olmuştur.

Sıkıştırma algoritmaları içerinde yaygın olarak kullanılan JPEG sıkıştırma algoritması da benzer bir ilkeyle çalışmaktadır.

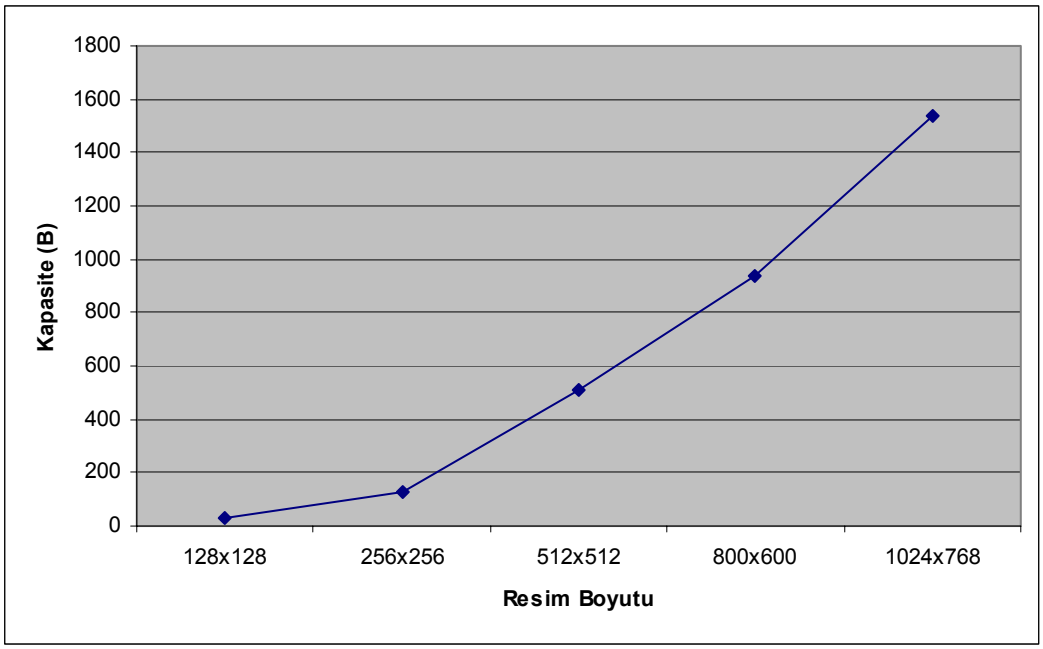


Yukarıda verilen şekilde de özetlendiği gibi JPEG sıkıştırması ilk önce resmi 8x8 renk değerinden oluşan parçalara ayırırı. Her biri üzerinde frekans düzlemine geçmek üzere ayrık kosinüs dönüşümü uygular. Bu dönüşümün tercih edilmesinin sebebi katsayıların karmaşık değil reel sayılar olmasıdır. Elde edilen sayılar seçilen kalite oranına göre seçilen bir tablo kullanılarak kuantalanır. Kuantalam tablosu kaliteye göre yüksek frekans katsayılarından kaç tanesinin yok edileceğini belirler. Kuantalama işlemi sonucunda ayrık kosinüs dönüşümü sonrası elde edilen 64 adet frekans katsayılarından bir kısmı sıfır değerini alacaktır. Bu katsayıların Huffman kodlaması ile sıkıştırılması ciddi oranda yer kazanımı sağlar.

Resim tekrar elde edilmek istenildiğinde sıkıştırma işleminin tersi uygulanacaktır. İlk önce Huffman kodu çözülür ve içerisinde sıfır katsayılarının da olduğu 64 adet katsayıdan oluşan blok elde edilir. Bu blok yine aynı kuantalama tablosu ile çarpılır. Birçok katsayı asıl değerine yakın değerlere ulaşacaktır ancak sıfır ile çarpılanlar sıfır kalacaktır. İşte bu, ters kosinüs dönüşümü sonrası elde edilen 8x8 renk değerlerindeki kayıbı belirleyecektir.

Sıkıştırma işleminde kullanılan yöntem, steganografik bir algoritma oluştururken bize yol göstermektedir. Her şeyden önce 8x8 renk bloklarının dikkate alınması gerekir. Öte yandan sıkıştırma işlemi kayıplı olacaktır. Bu işlemlere dayanıklı bir algoritma ayrık kosinüs dönüşümünü dikkate almalıdır. Önerilen birçok yöntemde, algoritmalar ayrık kosünüs dönüşümünü kendileri yapmaktadırlar. Daha sonra yok edilecek frekans katsayılarını dikkate alarak her bir blokta 1 bit saklarlar. Burada önemli olan, düşük frekans değişimlerinin resmi bozacağının kesin olmasıdır. Öte yandan, yüksek frekans katsayıları da muhtemelen yok edileceklerdir. Dolaysıyla resmi değiştirmeyecek kadar yüksek, yok edilmeyecek kadar düşük frekans katsayılarının bulunması gerekir.

Ayrık kosinüs dönüşümü kullanarak gizli iletişimi sağlayan yöntemlerde ortak sorun katsayıların belirlenmesidir. Ancak, katsayılar resimden resime fark göstereceklerdir. Resimde bozulma olup olmayacağı maalesef ancak işlem sonrası anlaşılabilir. Ayrıca, her 64 adetlik bloklara 1 bit gömülebilmesi, saklanabilecek veri miktarını önemli oranda düşürmektedir.

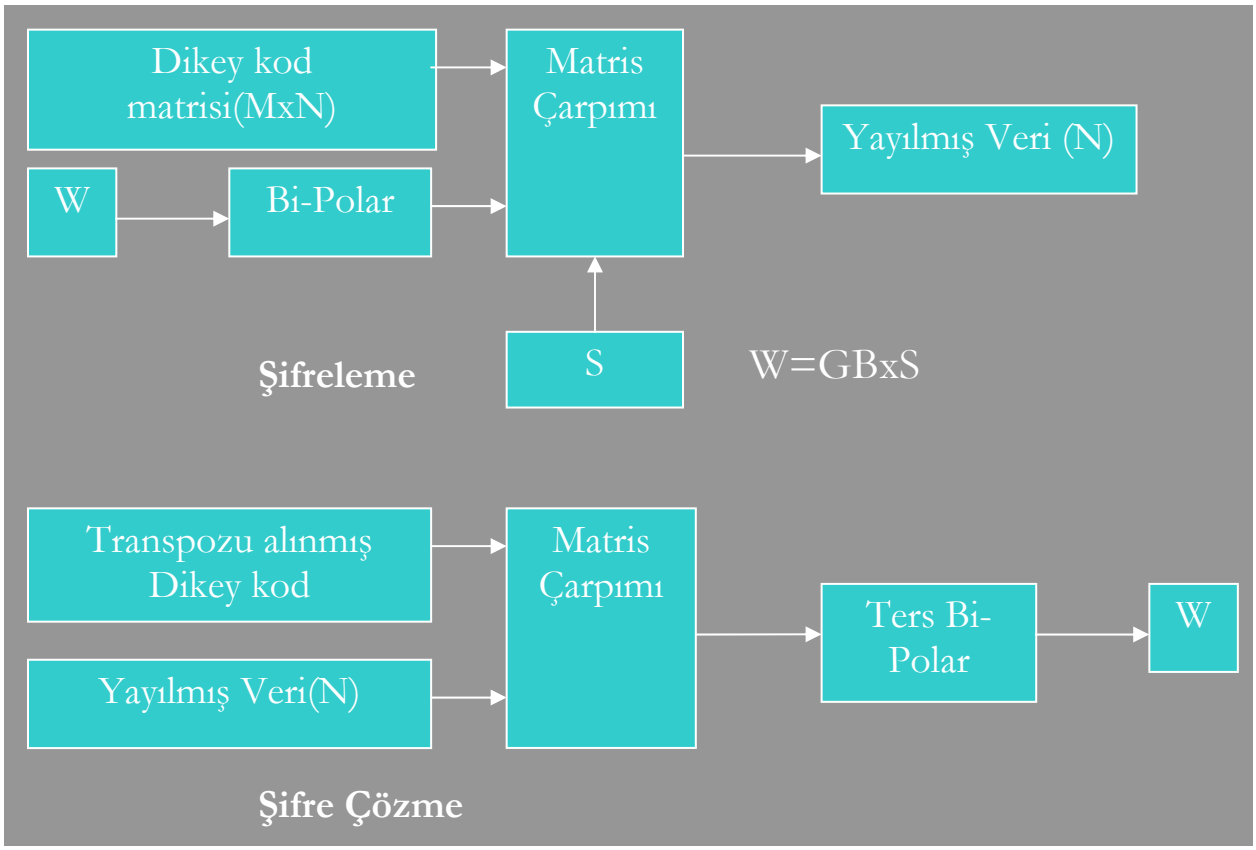


Şekil 10: Frekans düzleminde katsayı değiştirmeye dayanan yöntemlerin kapasite miktarı

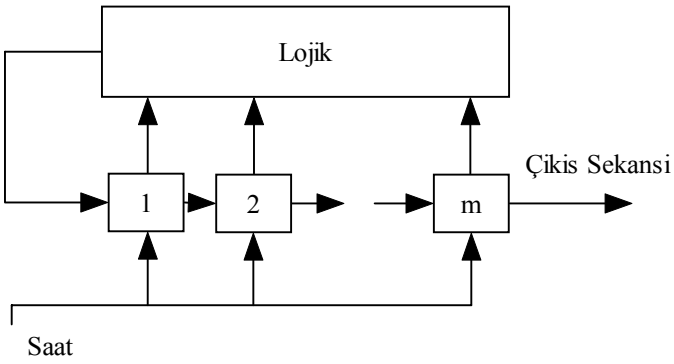
Spektrum Yayılmasına Dayanan Yöntemler

Son yıllarda yapılan çalışmalarda en dikkat çekici olanları spektrum yayılmasına dayanan yöntemlerdir. Spektrum yayılması aslında askeri iletişimde çok eskiden beri kullanılan bir yöntemdir. Bu yöntemde gönderilmek istenen mesaj ihtiyaç duyduğu frekans bandından çok daha fazlasına dağıtılır. Üçüncü bir kişi araya girip bir ya da birden fazla frekans bandında bozulmalara neden olsa bile, alıcı geri kalan frekans bantlarındaki bilgiler ile asıl mesajı elde edebilmektedir.

Aynı yöntem steganografi için de uygulanabilir. Gizli mesaj birden fazla bantta yayılarak resme gürültü olarak eklenebilir.



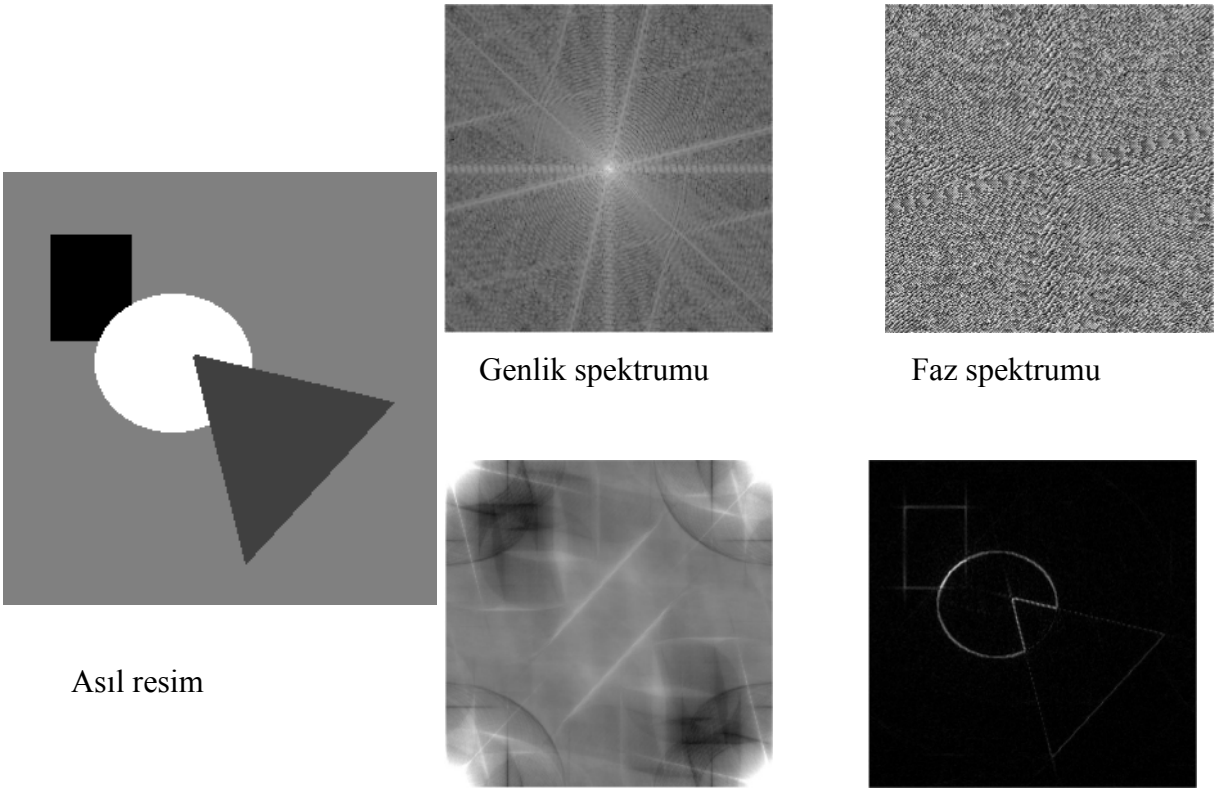
Yukarıdaki şekilde de görüldüğü gibi spektrum yayılmasına dayanan yöntemlerde en önemli kısım dikey kodlardır. Dikey kodlar birbirleri ile korelâsyonu yüksek olan ve “0” “1” dizileridir. Bu özel katarlar genelde m-sekansı adı verilen yapılar olarak üretilirler. Bu katarların üretilmesinde lineer geri beslemeli ötelemeli saklayıcılar kullanılmaktadır.



Şekil 11 Lineer geri beslemeli ötelemeli saklayıcı

Spektrumu yayılan bilgilerin resmin renk değerlerine nasıl gömüleceği uygulamadan uygulamaya değişmektedir. Bunlardan ilkinde resmin Fourier dönüşümünü alıp genlik kısmına gürültü olarak eklenir. Önerilen ikinci bir yöntem ise bu bilgilerin resme doğrudan gürültü olarak eklenmesidir. Bu yöntemde en büyük sorun karşı tarafta değiştirilmemiş taşıyıcının tahmininin yapılması gerekmektedir. Bunun için görüntü işleme teknikleri kullanılmaktadır.

Fourier dönüşümü kullanılarak verinin resme gömülmesinde dikkat edilmesi gereken nokta genlik bilgileri değiştirilirken faz bilgisinin aynen korunmasıdır. Dönüşümdeki faz bilgilerinin kısmen de olsa değişmesi durumunda ters Fourier işlemi sonucunda elde edilecek resim, taşıyıcı resim olmayacaktır. Faz ve genlik bilgilerinin önemini ortaya koyan aşağıdaki şekiller ilgi çekici olacaktır.



Genlik spektrumu

Faz spektrumu

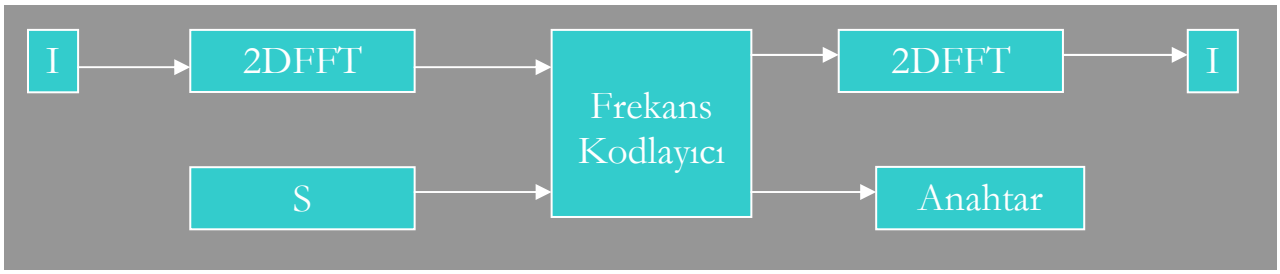
Asıl resim

Elde edilen resim(faz bilgisi yok)

Elde edilen resim (genlik bilgisi yok)

Resimlerde de görüldüğü gibi genlik bilgilerinden hareketle asıl resim elde edilememektedir. Oysa yalnızca faz bilgisi dahi resim hakkında önemli miktarda bilgi vermektedir.

Yayılan gizli veri aşağıdaki diyagramda belirtilen yöntemle resme eklenmektedir.



Bu yöntem ile gömülen bilgi karşı tarafta kolayca elde edilmektedir. Ancak, yolda gerçekleşecek birçok müdahaleye diğer belirtilen yöntemlere göre çok daha fazla dayanıklıdır. Resmin sıkıştırılması, bir bölümünün tamamen bozulması ve parlaklık değerleri ile oynanması durumunda bile alıcı gizli mesajı başarılı bir şekilde alabilmektedir.

Spektrum yayılmasına dayanan yöntemlerde kapasite kullanımı kullanılan dikey koda bağlıdır. Bu durumda örnek diyagramdan da görülebileceği gibi gizli verinin miktarının önemi yok gibi görünmektedir. Ancak, verinin sağlıklı çıkarılması için dikey kod uzunluğunun gizli veriden çok büyük olması gerekmektedir. Bu durum gönderilebilecek veri miktarını sınırlamakla beraber yapılan çalışmalarda bu oranın ne olması gerektiği konusunda bir bilgi yoktur.

İstatistiksel Yöntemler

Önerilen çalışmalardan bazıları resmin bazı istatistiksel bilgilerinin değiştirilmesi ile alıcıya gizli bir mesaj verilebileceğini belirtmektedirler. Burada bir hipotez fonksiyonu belirlenir ve bu hipotez fonksiyonuna parametre olarak resim veya resmin bir kısmı gönderilir. Bu fonksiyonun geri döndürdüğü değer fonksiyonda incelenen istatistiksel özelliğin değişip değişmediğini belirtmektedir.

Bu yöntemler çeşitli resim işlemlerine dayanıklı olduklarını iddia etmektedirler. Yine bu yöntemlerde karşılaşılan sorun ise uygun bir hipotez fonksiyonunun bulunmasıdır. Ancak, en büyük sorun gönderilebilecek gizli bilgi miktarıdır. Önerilen yöntemlerde resim dosyası başına 1 adet gizli veri biti gönderilebilmektedir.

Diğer Yöntemler

Üzerinde çalışılan bir diğer yöntem ise taşıyıcı resmin, gizli veriden hareketle oluşturulma çabasıdır. Böyle bir yöntemde taşıyıcı resim hiçbir şekilde değiştirilmediği için üçüncü bir kişinin fark etmezi mümkün değildir. Ancak yine bu yöntemde en büyük sorun bu yolla üretilen resimlerin insan gözünü bile aldatamamasıdır.

Düz metin steganografisi bir diğer çalışma alanıdır. Dilin yapısına uygun olarak cümle elemanlarına 0 veya 1 değerleri atanır ve gizli veri bitlerine göre seçilen kelimeler ile cümleler oluşturulur. Ancak, burada en büyük sorun sürekli bir akış sağlanmasıdır. Üretilen cümlelerin anlamlı ve birbirleriyle ilgili olması ciddi bir sorundur.

Resim dosyaları üzerinde gerçekleştirilen steganografik uygulamaların benzerleri ses ve görüntü dosyaları üzerinde de gerçekleştirilmektedir. Ancak, burada en büyük sorun bu tür dosyaların ciddi miktarda sıkıştırılmış olması veya görüntü dosyalarında olduğu gibi çerçevelerin fark tablolarını yansıtmasıdır.

Sonuç

Günümüz itibariyle iletişimin bile gizli olmasının gerektiği durumlarda steganografi başarıyla uygulanmaktadır. Ancak, henüz yeni olan bu çalışmalarda üçüncü şahısların her türlü müdahalelerine dayanıklı bir yöntem geliştirilmemiştir. Var olan yöntemler sorunun bir veya iki yönüyle ilgilenmektedirler. Dolaysıyla bu alanda yapılacak birçok çalışma vardır. Öte yandan, steganografi çalışmalarında en önemli kıstaslardan veri mümkün olduğu kadar çok gizli veriyi karşı tarafa iletmekle beraber bu verinin sağlam bir şekilde alınabilmesidir. Üçüncü şahıs saldırılarına karşı önerilen yöntemler zaten sınırlı olan kapasite kullanımı azaltırken belirtilen koşulları sağlamak için artıklıklar kullanmak bu oranı çok daha aşağıya çekmektedir. Dolaysıyla, steganografi kullanımında istenilen güvenlik seviyesine ve gönderilecek veri miktarına uygun yöntemler uygun parametrelerle dikkatle seçilmelidir.

Kaynaklar

Schneier, B., 1996. Applied Cryptography-Protocols, Algorithms and Source Codes in C, *2. Baskı*, John Wiley and Sons, New York.

Zilnerr, J., Federrath, H., Klimat, H., Pfitzmann, A., Piotraschke, R., Wesfeld, A., Wicke, G. and Wolf, G., 1998. Modeling the Security of Steganographic Systems, *Proc. 2nd Workshop on Information Hiding*, Nisan, LNCS 1525, Springer-Verlag, Portland.

Chandramouli, R., Memon, N., 2001. Analysis of LSB Based Image Steganography Techniques, *Proceedings of the International Conference on Image Processing*, Thessalonica, Ekim, Yunanistan, 1019-1022.

Katsenbeisser, S. and Petitcolas, F., 2000. Information hiding Techniques for Steganography and Digital Watermarking, Artech House, Boston.

Ogihara, T., Nakamura, D. and Yokoya, N., 1996. Data Embedding into Pictorial Images with Less Distortion Using Discrete Cosine Transform, Proc. 13th IARP Int. Conference on Pattern Recognition, **1** , 675-679.

Zhao, J. and Koch, E., 1995. Embedding Robust Labels into Images for Copyright Protection, Proceedings of the International Conference on Intellectual Property Rights for Information, Knowledge and New Techniques, Münih, 242-251.

Pickholtz, R. L., Schilling, D. L. and Milstein, L. B., 1982 .Theory of Spread-Spectrum Communications-A Tutorial,. *IEEE Transactions on Communications*, **30(5)**, 855–884.

Marvel, L. and Retter, C., 1999. Spread Spectrum Image Steganography, *IEEE Transactions on Image Processing*, **8(8)**, 1075-1083.

Pitas, I., 1999. A Method for Signature Casting on Digital Images , *IEEE International Conference on Image Processing*, (3), 215-218.

Sandford, M. T., Bradley, J. N. and Ettinger, J. M., 1996. Data Embedding Method, *Proceeding of the SPIE 2615, Integration Issues in Large Commercial Media Delivery Systems*, 226-259.