

Steganografi

STEGANOGRAFI NEDİR?

- Steganografi-”Veri içerisinde veri saklama”
 - Yunanca “gizli yazı”
 - İletişimin varlığını saklayan yöntem
- Kriptografi
 - Gizli mesajın anlaşılamaz hale getirilmesi
 - Mesajın varlığı bilinir ancak, içeriği anlaşılamaz
- Kriptografi mesajın içeriğini anlaşılmaz hale getirirken, steganografi mesajı görülemeyecek şekilde *saklar*.

Steganografinin Doğuşu

- Kafa derisine kazınan mesaj
- Av ve avcı
- Çinli'lerin meyve sepetleri
- II. Dünya Savaşı
 - Mikrofilmler
 - Mendiller

Steganografinin Doğuşu

- Kafatası derisine kazınan mesaj



Steganografinin Doğuşu

- Av ve Avcı



Steganografinin Doğuşu


- İkinci Dünya Savaşı
Mesaj

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

Saklanan mesaj:

“Pershing sails from NY June 1.”

Güvenlik -Gündem



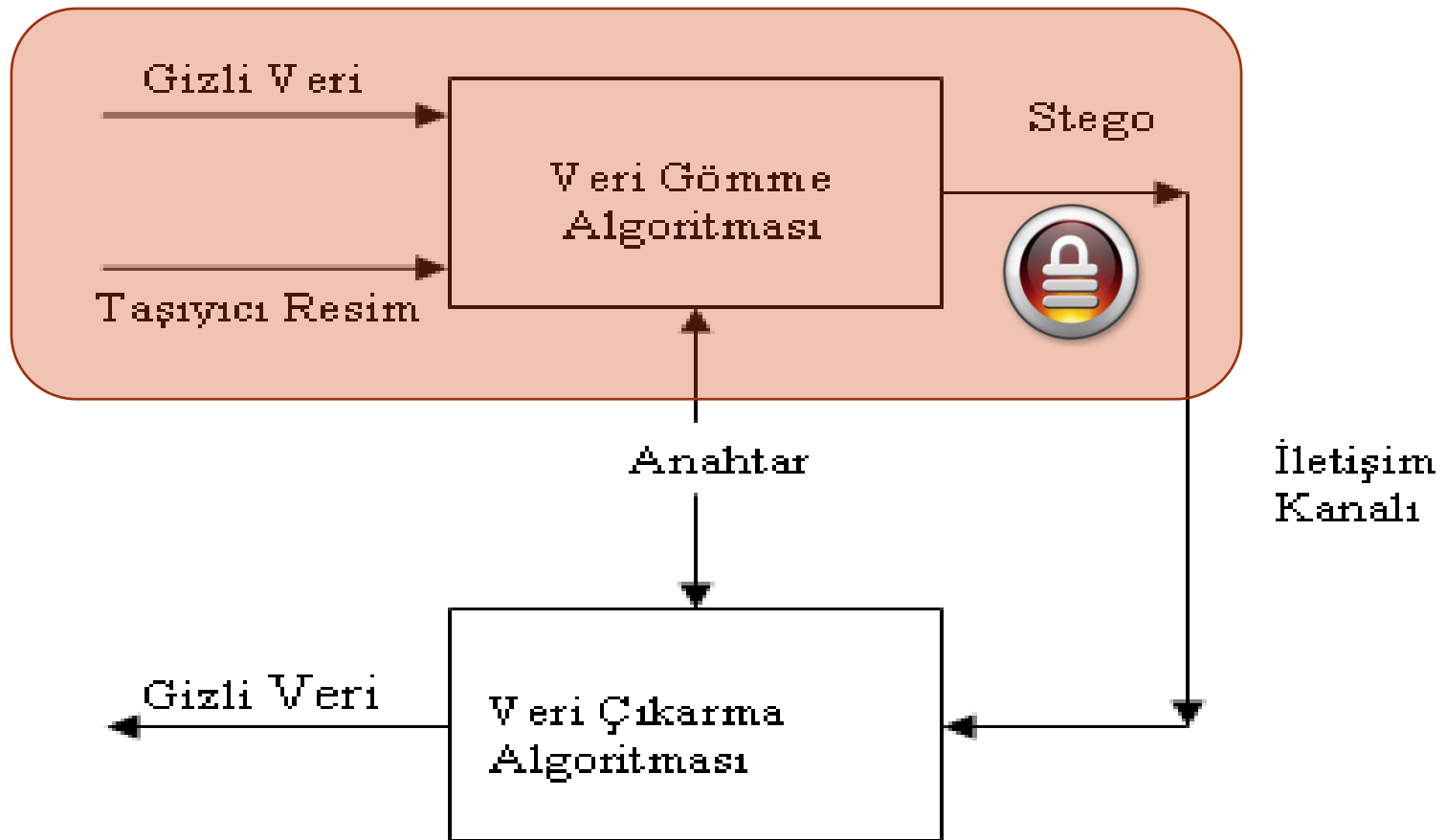
The image shows a large black padlock in the center, symbolizing security. The background is filled with various mathematical formulas, including:

$$y^2 f(x) + e_1(x)y_1 + e_2(x)y_2 + e_3(x)y_3$$
$$(x+1) = \left(\frac{x(x-2)}{2}\right)1 + (x(x-1))0 + \left(\frac{x(x-1)}{2}\right)$$
$$= \left(\frac{(x-1)(x-2)}{2}\right)1 + (x(x-1))0 + \left(\frac{x(x-1)}{2}\right)$$
$$f_p(x, y)$$
$$(y+6x+7)^4 - (y+7x+8)^4 + 8x^2(y+9x+6)^4(y+10x+8)^2$$
$$1)(x+6)^4(x+9)^4 x(x+8)^2(x+2)^4$$
$$-9b + \sqrt{3}\sqrt{4a^3 + 27b^2} y^3 + 6x)^2(y+10x+8)^2 x+1$$
$$\frac{2^{1/3} 3^{2/3}}{x(x+6)^2} \frac{(y+8x)^2}{(y+9x+6)^4}$$
$$\frac{(1-i\sqrt{3})(-9b + \sqrt{3}\sqrt{4a^3 + 27b^2})^{1/3}}{2^{4/9} 3^{5/2} x+9} \frac{(y+8x+9)^2}{(y+8x)^2(y+7x+4)^4(y+9x+6)^4}$$

- Örgüt içi haberleşmelerde
- Ülke güvenliğinde
- Savaş anında

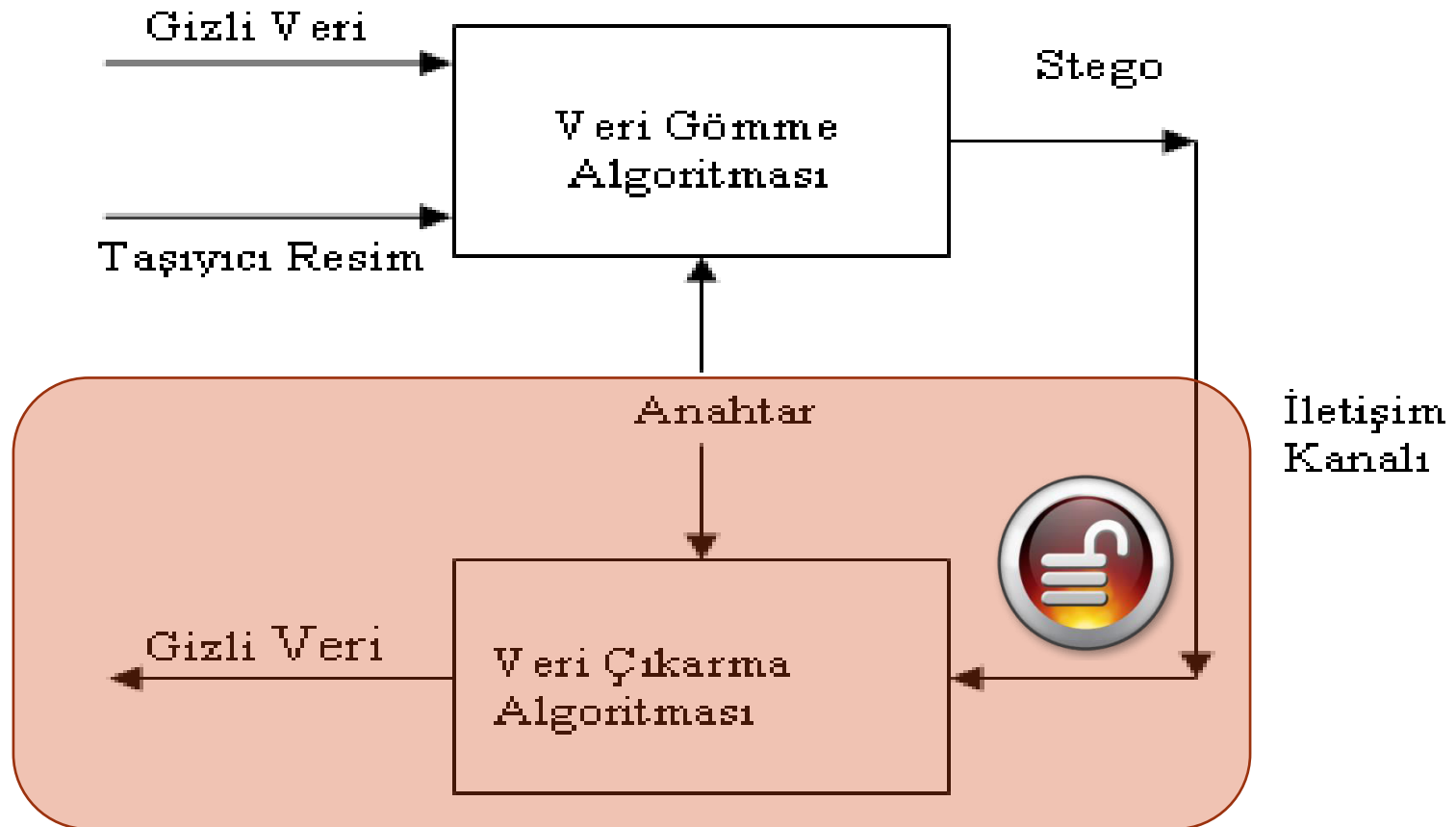
Temel Yöntemler

Veri gizleme adımı



Temel Yöntemler

Veri çözme adımı



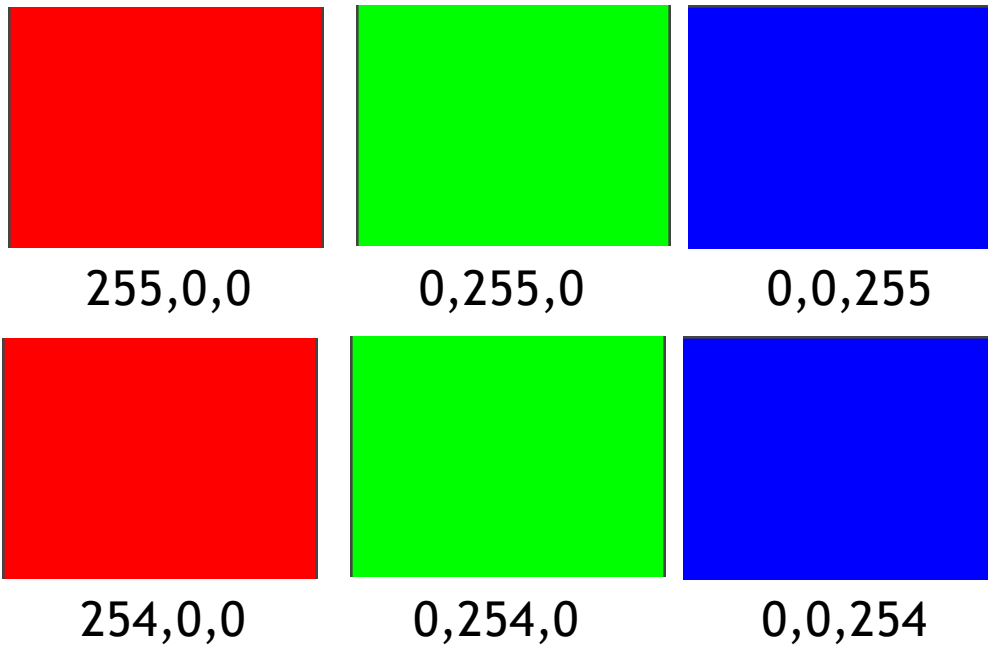
Temel Yöntemler

- Değiştirmeye dayalı yöntemler
- İşaret İşlemeye dayalı yöntemler
- İstatistiksel yöntemler
- Diğer yöntemler

Temel Yöntemler

Değiştirmeye Dayalı Yöntemler

Bu yöntemde resim dosyalarını oluşturan renk birimlerinin en küçük anlamlı biti artırıp azaltılarak bu bit üzerinde veri saklanır.



Temel Yöntemler

İşaret İşlemeye Dayalı Yöntemler

Buradaki teknik sıkıştırılmış resim dosyalarındaki yöntemi baz alır. Resim sıkıştırma teknikleri insan gözünün algılayabileceği renk değişimi dışında kalan frekanstaki renkleri sıfırlar. Daha sonra bir sıkıştırma algoritması ile bu bilgiler kaldırarak boyutun kısılmasını sağlar.

Buradan elde edilen boş alana büyük miktarda veri yazmak mümkün hale gelir.

Temel Yöntemler

İşaret İşlemeye Dayalı Yöntemler

- 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.

Temel Yöntemler

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.

Temel Yöntemler

İstatiksel Yöntemler

- 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.

Temel Yöntemler

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 etmesi mümkün değildir.

Kullanım Alanları

- Metin Steganografi (Text Steganography)
- Görüntü Steganografi (Image Steganography)
- Ses Steganografi (Audio Steganography)

Kullanım Alanlar

Metin Steganografi

- Metin Steganografi taşıyıcı ortamın text olduğu Steganografi alanıdır.
- Metin steganografi genelde uygulanması zor bir veri gizleme şeklidir.
- Metin Steganografi'de saklanacak veri miktarı azdır.
- Bunun nedeni taşıyıcı text'in içindeki gereksiz alanların ve boşlukların miktarının az olmasıdır.
- Metin tabanlı gizleme yöntemlerinin hepsi, gizli mesajı geri çözebilmek için ya orijinal metne, yada orijinal metnin biçimlendirme bilgisine ihtiyaç duyar.

Kullanım Alanlar

Metin Steganografi

Metin Steganografi veri saklanacak yerlerin özelliklerine göre aşağıdaki yöntemleri kullanır.

1. Açık Alan Yöntemleri (Open Space Methods)
2. Yazımsal Yöntemler
3. Anlamsal Yöntemler

Kullanım Alanlar

Metin Steganografi

Açık Alan Yöntemi

- Bu yöntemler, anormal gözükmeyen iki kelime arasında extra boşluklar, satır sonu boşlukları ile çalışmaktadır.
- Bununla birlikte Açık Alan Yöntemleri'nin ASCII kodları ile kullanılması daha uygundur.

Kullanım Alanlar

Metin Steganografi

Açık Alan Yöntemi

Açık alan yöntemleri de kendi içerisinde 5 farklı uygulama tipine sahiptir.

- Cümle içi boşluk bırakma
- Satır kaydırma
- Satır sonu boşluk bırakma
- Sağ hizalama
- Gelecek kodlaması

Kullanım Alanlar

Metin Steganografi

Yazılımsal Yöntemler

- Bu yöntem, dökümanı kodlamak için noktalama işaretlerini kullanır.
- Örneğin aşağıdaki iki cümle de ilk bakışta aynıymış gibi gözükmemektedir, fakat dikkatlice bakıldığında ilk cümlenin fazladan bir ‘,’ işareti içerdiği görülür.
- Bu yapıların biri “1”, diğeri de “0” olarak belirlenir ve kodlama işlemi bu şekilde yapılır.
 - “bread, butter, and milk”
 - “bread, butter and milk”

Kullanım Alanlar

Metin Steganografi

Anlamsal Yöntemler

- Bu yöntem W. Bender tarafından ortaya atılmıştır.
- 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.

Kullanım Alanları

Görüntü Steganografı

Bilgilerin görüntü dosyaları içerisine saklanması için çeşitli yöntemleri vardır. Bunlar:

1. En önemsiz bite ekleme
2. Maskeleye ve filtreleme
3. Algoritmalar ve dönüşümler

Kullanım Alanları

Görüntü Steganografı

En önemsiz bite ekleme(LSB Insertion)

- En önemsiz bite ekleme yöntemi yaygın olarak kullanılan ve uygulaması basit bir yöntemdir.
- Fakat yöntemin dikkatsizce uygulanması durumunda veri kayıpları ortaya çıkmaktadır.
- 0-255 arası 1 byte ile temsil edilen gri-seviye (gray-scale) görüntüler vardır.
- Renkli dijital görüntüler 24 bit yada 8 bit olabilir.

Kullanım Alanları

Görüntü Steganografı

24 bit görüntüler:

- 24 bitlik bir görüntü bir pixel başına 3 byte kullanmaktadır.
- Her pixel için renk üç ana renkten elde edilir.
 - Kırmızı (red), Yeşil (green), Mavi (blue)
- Her byte'ta son biti değiştirmek suretiyle her pixel'de 3 bitlik bilgi saklayabiliriz.
- Yani 24 bitlik 1024x768 resim, bilgi saklamak için kullanılabilir 2.359.296 bit (294.912 byte)'e sahiptir.
- Eğer gizlemek istediğimiz mesajı resmin içine gömmeden önce sıkıştırırsak çok daha fazla sayıda bilgiyi gizleyebiliriz.

Kullanım Alanları

Görüntü Steganografı

24 bit görüntüler:

Örneğin “101101101” bilgisini 3 pixel’e gizleyelim. Orjinal görüntü bitleri şu şekilde olsun:

10010101 00001101 11001001 (149,13,201)

10010110 00001111 11001010 (150,15,202)

10011111 00010000 11001011 (159,16,234)

İçine bilgiyi gizlediğimizde oluşan pixeller ise şöyledir:

10010101 0000110**0** 11001001 (149,12,201)

1001011**1** 0000111**0** 1100101**1** (151,14,203)

10011111 00010000 11001011 (159,16,234)

Kullanım Alanları

Görüntü Steganografı

8 bit görüntüler:

- Orijinal görüntü pixellerimiz aşağıdaki gibi verilmiş olsun.
 - Beyaz, beyaz, mavi, mavi (00 00 10 10)
- 10 sayısının binary karşılığı olan 1010 değerini bu pixellere gizlemek istersek, yapılan değişiklikler sonucunda elde edilen pixel değerlerimiz şöyle olur:
 - 01 00 11 10
- Bu değerlerde renk paletinde sırasıyla aşağıdaki renk değerlerine karşılık gelmektedir.
 - kırmızı, beyaz, yeşil, mavi
- Pixellerin renk değerleri oldukça değiştiğinden, gözle fark edilebilecektir ve bu kabul edilemez bir durumdur.
- Veri-gizleme uzmanları bu nedenle 8 bitlik renkli görüntüler yerine gri-seviye görüntülerin kullanılmasını daha uygun bulmaktadırlar.

Kullanım Alanları

Görüntü Steganografı

Gri-Seviye görüntüler:

- Bununla 0 (siyah) ile 255 (beyaz) arasında tam sayılar elde edilebilir. Bu sayılar arasındaki değerler gri'dir ve bundan dolayı bir resime ait tam sayı "gri ton seviye" (gray level) olarak isimlendirilir.
- İkili sayı sistemine göre 10110111 sayısını ele alalım. Bu sayı onluk düzende 183 sayısının karşılığıdır.
- Sondaki bit'in 1 veya 0 olması bu değeri çok fazla değiştirmeyecektir.
- Sondaki bit değerimiz eğer 0 olsaydı bu değer 182 olacak ve renk üzerinde gözle görülecek büyük bir değişikliğe neden olmayacaktır.

Kullanım Alanları

Görüntü Steganografı

Maskeleme ve Filtreleme

- Maskeleme ve filtreleme teknikleri genellikle 24 bit ve gri-seviye görüntüler üzerinde işaretleme (marking) ve filigran yapılarak uygulanmaktadır.
- İşaretleme yada filigran tekniklerinin görüntülere sıkça uygulanması nedeniyle, görüntünün değişmesi korkusu olmadan uygulanabilmektedir.
- Teknik olarak filigran bir steganografik biçim değildir.

Kullanım Alanları

Görüntü Steganografı

Maskleme ve Filtreleme

- Maskleme işlemi, sıkıştırma, kırpma ve bazı görüntü işlemleri açısından son bite ekleme yönteminden daha güçlüdür.
- Maskleme teknikleri belirlenmiş alanlara bilgileri gömer.
- Maskleme tekniklerinin JPEG görüntülerde kullanılması daha uygundur.



Kullanım Alanları

Görüntü Steganografı

Algoritmalar ve Dönüşümler

- Son bite ekleme yöntemi bilgi gizlemek için oldukça kolay ve hızlı bir yöntemdir, fakat görüntüye uygulanan işlemler yada kayıplı sıkıştırmalar sonucunda bilgi zarar görebilmektedir.
- Yüksek kalitedeki resimlerin sıkıştırılarak örneğin jpeg formatı kullanılarak internet üzerinden gönderilmesi daha uygundur. Bunun için gizlenen bilginin kaybolmaması ve görüntünün sıkıştırılmasını sağlayan bazı yöntemler ve steganografik araçlar ortaya çıkarılmıştır.

Kullanım Alanları

Görüntü Steganografı

Algoritmalar ve Dönüşümler

Algoritmalarda olması gereken özellikler:

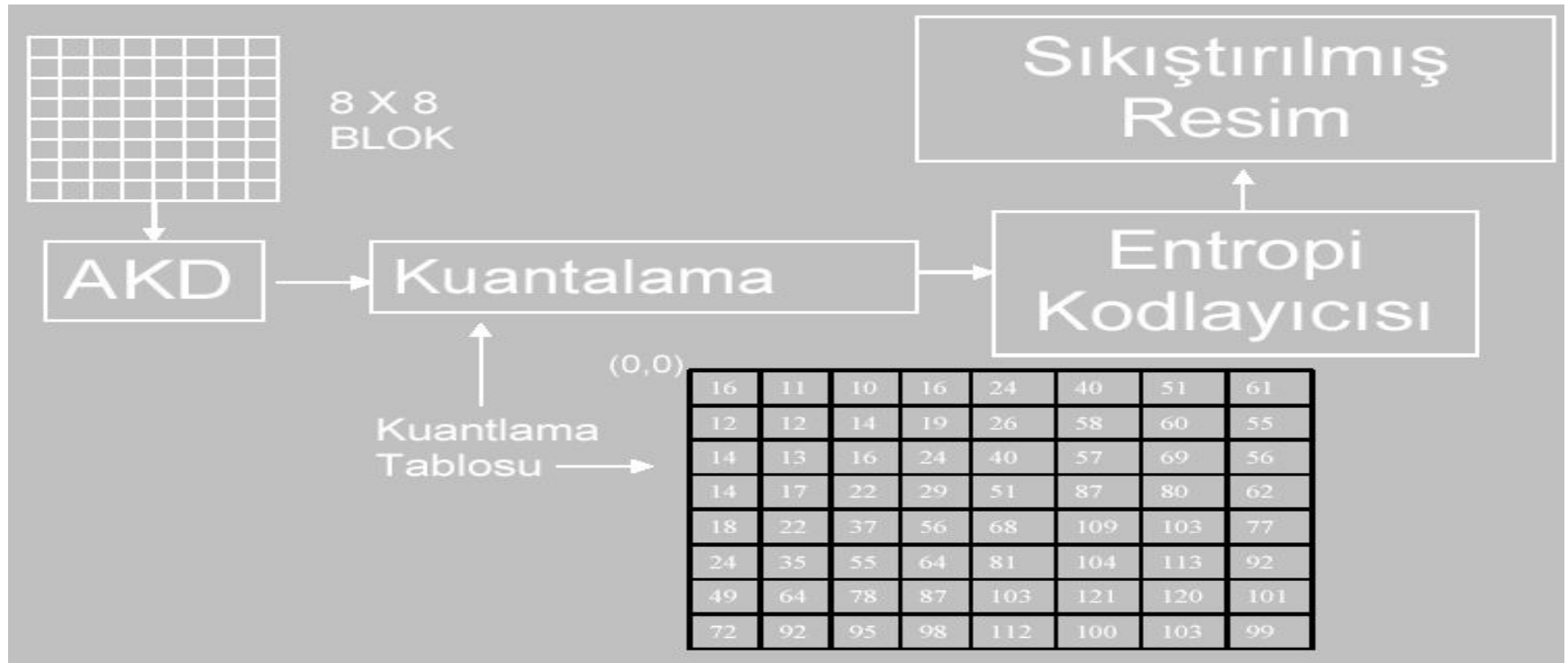
- Değişimin fark edilememesi
- Saklanabilecek veri miktarı
- •Dayanıklılık

Kullanım Alanları

Görüntü Steganografi

Algoritmalar ve Dönüşümler

- Jpeg Algoritması (Dct)



Kullanım Alanları

Görüntü Steganografi

Algoritmalar ve Dönüşümler

Jpeg Algoritması (Dct)

- JPEG sıkıştırma işleminde öncelikle piksellerin RGB bilgileri luminance-chrominance bilgilerine dönüştürülür.
- 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 frekansları ifade edenler bir quantization tablosundaki değerler ile bölünür.
- Elde edilen yeni katsayılara sıkıştırma işlemi(Huffman Kodlaması) uygulanır ve header eklenerek dosya oluşturulur.

Kullanım Alanları

Görüntü Steganografi

Algoritmalar ve Dönüşümler

Jpeg Algoritması (Dct)

- 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.

Kullanım Alanları

Görüntü Steganografi

Algoritmalar ve Dönüşümler

Bpcs Yöntemi

- En belirgin fark kapasitedir

Diğer teknikler en fazla orjinal verinin %15'i kadar bir gömme alanı sağlarken BPCS orjinak verinin %50'si miktarında bilginin gizlenmesini sağlayabilmektedir.

- 24 bit, 8 bit BMP ve GIF formatlarına uygulanabilir.
- Gizleme işleminde öncelikle dosyanın analizini yapılmakta ve veri gizlemede kullanılabilecek bitler tespit edilmektedir.
- Genel prensip olarak n bitlik bir resimden her pikselin birinci bitleri ile bir resim, ikinci bitleri ile başka bir resim elde edilir.

Kullanım Alanları

Görüntü Steganografı

Algoritmalar ve Dönüşümler

Bpcs Örnekleri

- 24 bit BMP de her renk için 8 ayrı resim elde ederiz.

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

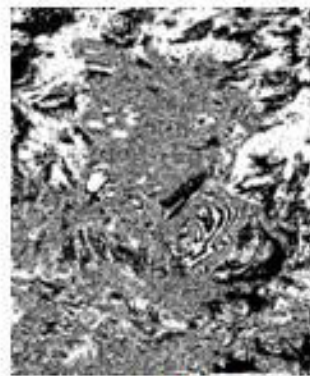
- Elde edilen resimler incelendiğinde bit değeri azaldıkça resimlerin şekil bilgisinden çok gürültü benzeri veri içerdiği görülür.
- Gömme işleminde bu alanlar kullanılarak geniş bir kapasite sağlanmış olur.



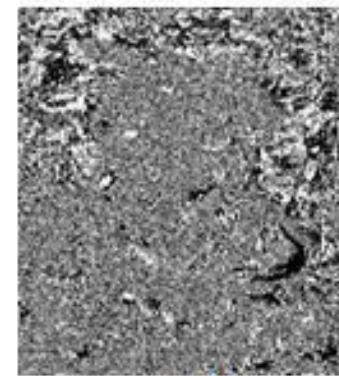
Orjinal resim



PR3



PR4



PR5

Kullanım Alanları

Ses Steganografi

- Yaygın dağıtımı ve içerdiği bilginin özelliklerinin benzerliği dolayısıyla ses dosyaları da resim dosyaları gibi steganografi uygulamalarında kullanılmaktadır.
- Mevcut Yöntemler:
 - Low bit encoding
 - Phase coding
 - Spread spectrum
 - Echo data hiding

Kullanım Alanları

Ses Steganografı

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.

Kullanım Alanları

Ses Steganografı

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.

Kullanım Alanları

Ses Steganografı

Spread Spectrum

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

Kullanım Alanları

Ses Steganografı

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.