

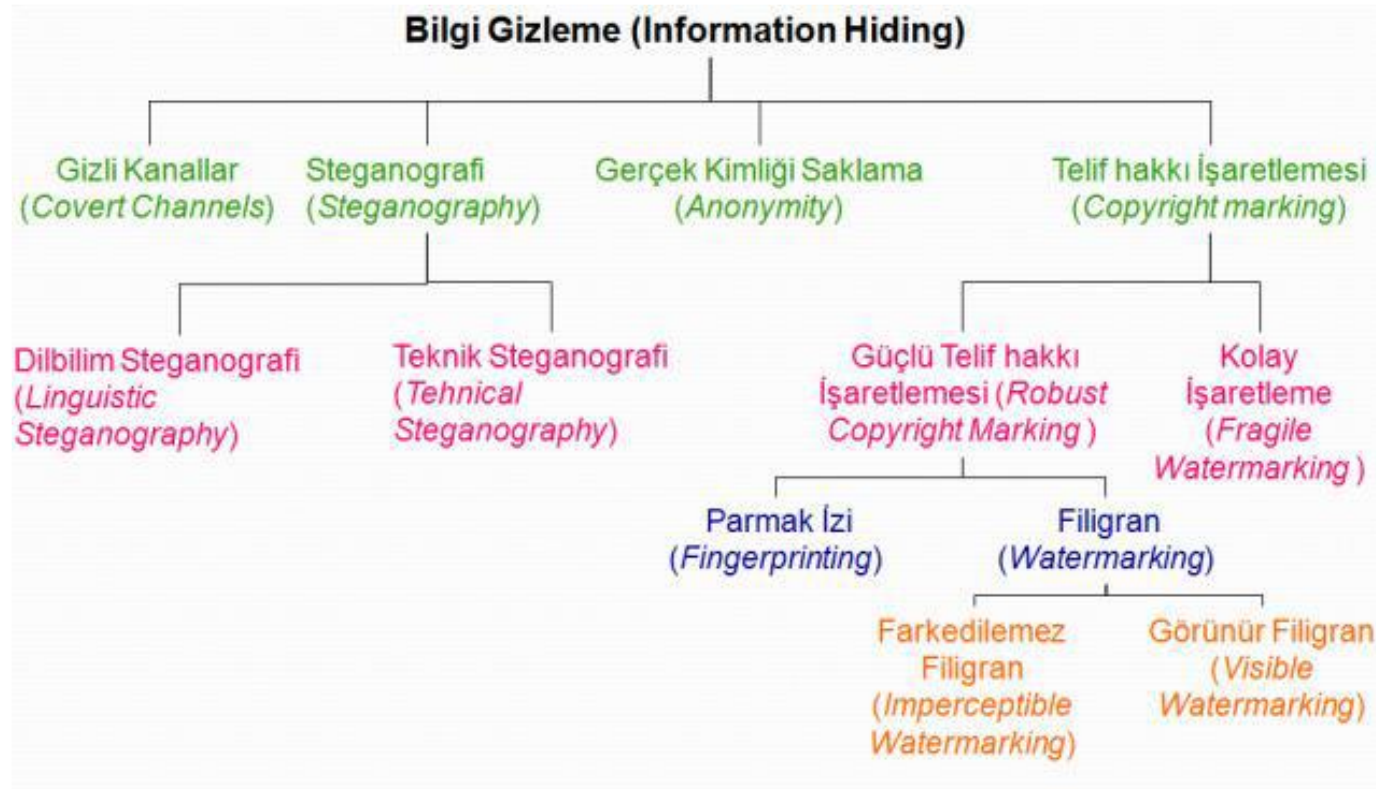
Steganografi

İÇİNDEKİLER

- Bilgi Gizleme Nedir?
- Steganografi Nedir?
 - Steganografi ve Kriptografi' nin Farkları
 - Steganografi' nin Doğuşu
 - Nasıl Çalışır?
- Steganografik Bir Algoritmanın Temel Özellikleri
- Steganografi'de Kullanılan Yöntemler
- Kullanım Alanları

Bilgi Gizleme

- Bilgi gizleme, bir mesajın ya da bilginin, herhangi bir masum görünümlü ortam içerisine saklanarak bir diğer kişiye ulaştırılmasıdır



Steganografi Nedir?

- Steganografi
 - Yunanca “gizli yazı”
 - İletişimin varlığını saklayan yöntem
 - ”Veri içerisinde veri saklama”
- Amaç, içinde gizli mesaj veya bilgiler bulunan bir veriyi, alıcıdan başka kimsenin fark edemeyeceği bir biçimde saklayarak göndermek

Steganografi Nedir?

- Dilbilim Steganografi
 - Taşıyıcı verinin metin (text) olduğu
- Teknik Steganografi
 - Görünmez mürekkep, gizli yerler, microdot'lar ve bilgisayar tabanlı yöntemler(ses, görüntü, resim dosyalarını kullanarak veri gizleme)

Steganografi ve Kriptografi

- Steganografi
 - Verinin nasıl taşınacağı saklanmak zorundadır
 - Verinin varlığı saklanması gerekir
- 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
- Çinli'lerin meyve sepetleri
- II. Dünya Savaşı
 - Mendiller
 - Mikrofilm ve MikroDotlar

Steganografi'nin Doğuşu

Kafa derisine kazınan mesaj

- M.Ö.400 lü yıllarda
- İran'da bulunan yunanlı casus, Pers istilasını Yunan İmparatorluğu'na haber vermek için bir kölenin kafa derisine mesajı kazıtmıştır.
- Ardından casus, kölenin saçının yazıyı göstermeyecek büyüklüğe kadar uzamasını beklemiş ve bu köleyi mesajı iletmek amacıyla İmparatorluğa göndermiş. Kölenin burada tek bilmesi gereken bilgi “kafamı kazıyın” şeklindeydi.



Steganografi'nin Doğuşu

Çinli'lerin Meyve Sepetleri

- Gizli Bir İletişim Aracı
- Meyve sepetindeki her meyvenin birbirlerine göre konumu farklı anlamlar ifade etmekteydi.

Steganografinin Doğuşu

İkinci Dünya Savaşı

- Alman casusların kimyevi bir madde kullanarak beyaz bir mendile mesaj yazdıkları ortaya çıkartılmıştır

Mesaj:

- “After The Theater, All Clients Keep A Tab Down At Wesley’s Nook”

Saklanan mesaj:

- “*ATTACK AT DAWN*”

Steganografinin Doğuşu

- İkinci Dünya Savaşı
Mesaj

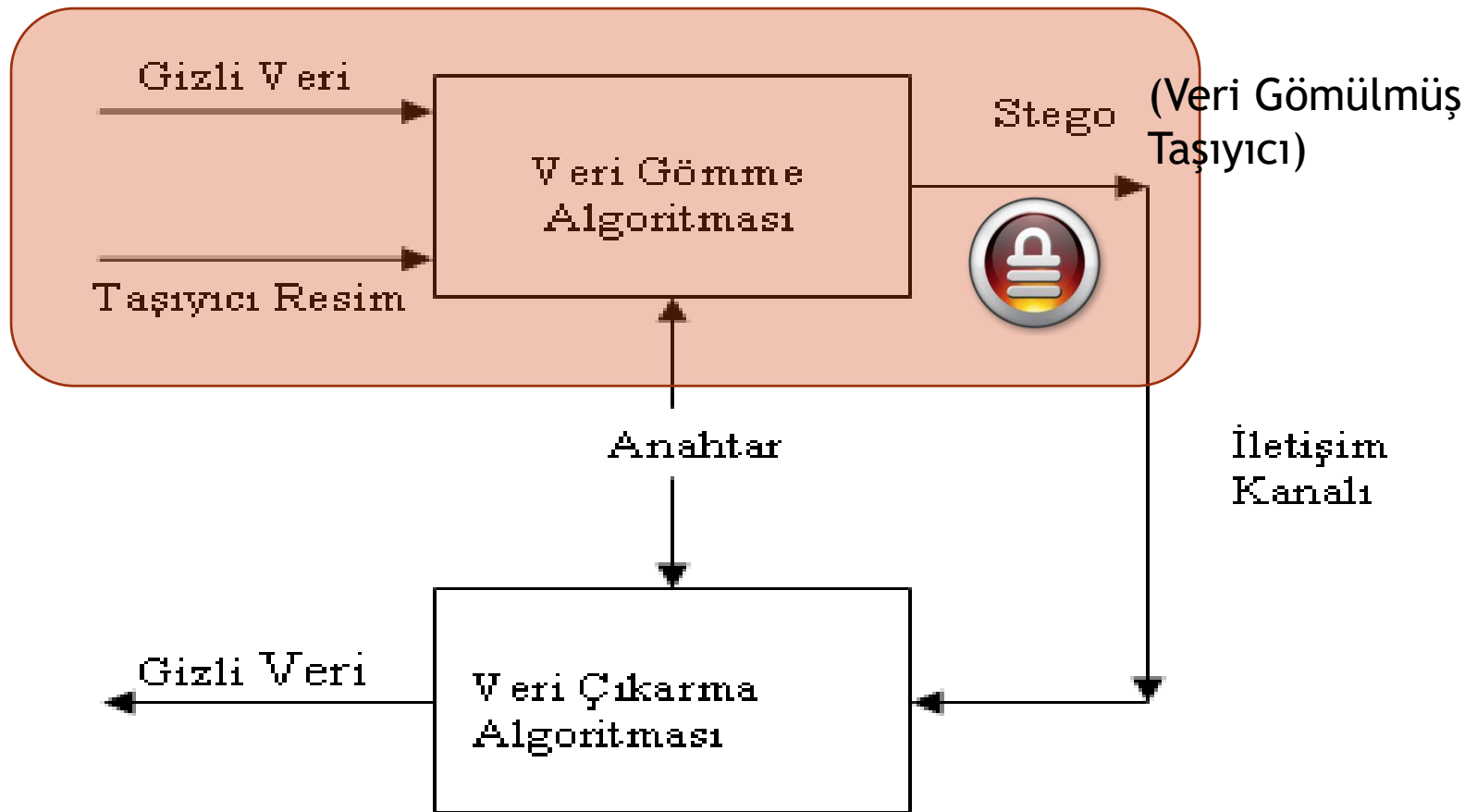
“Apparently neutrals protest is thoroughly discounted and ignored. Isman hard hit. Blockade issue affects pretext for embargo on by-products, ejecting suets and vegetable oils.”

Saklanan mesaj:

“Pershing sails from NY June 1.”

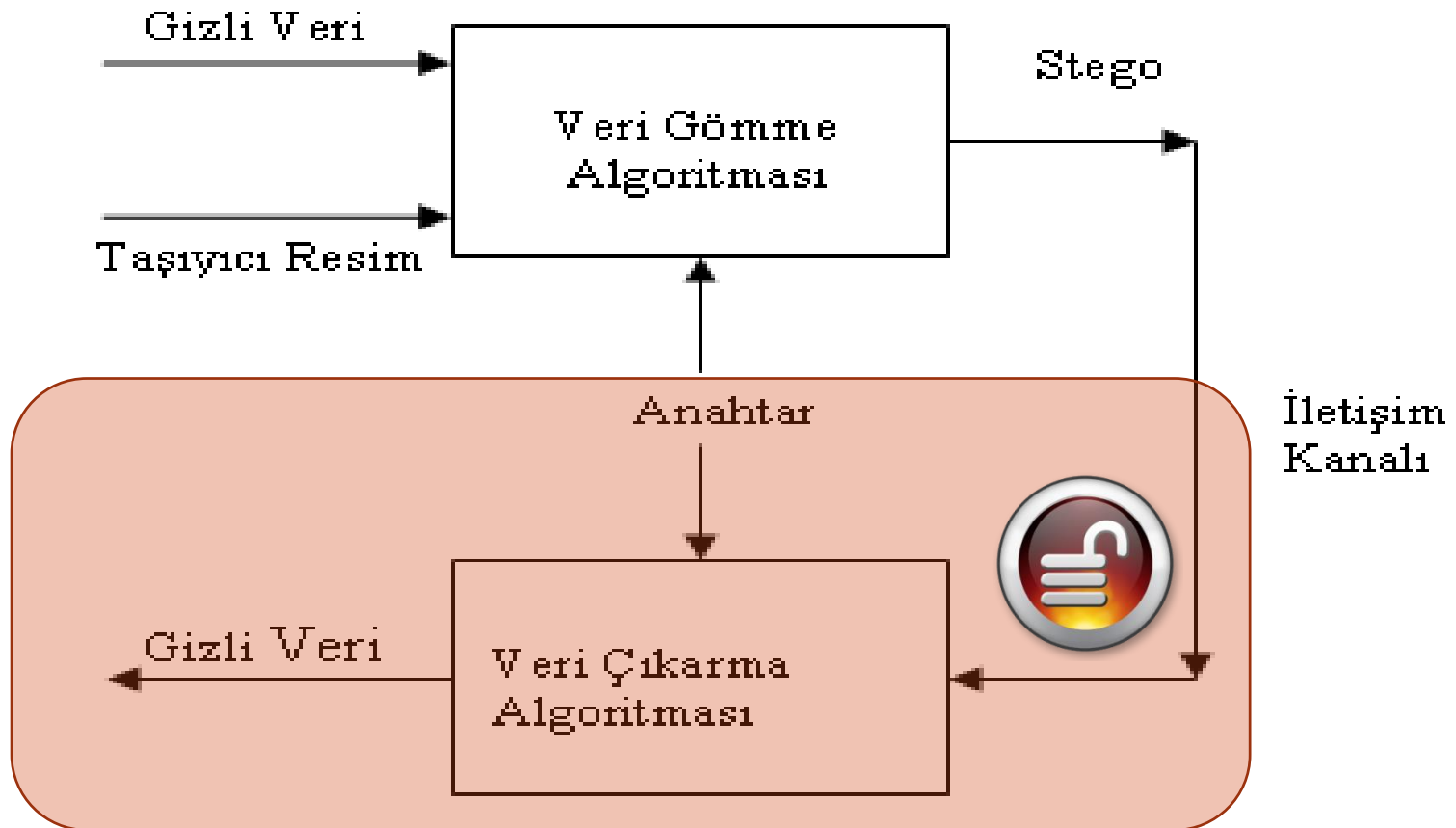
Nasıl Çalışır?

Veri gizleme adımı



Nasıl Çalışır?

Veri çözme adımı



Steganografik Bir Algoritmanın Temel Özellikleri

- Değişimin Fark Edilememesi
- Saklanabilecek Veri Miktarı
- Dayanıklılık

Steganografik Bir Algoritmanın Temel Özellikleri

- Değişimin fark edilememesi
 - Stego(taşıyıcı veri) üzerinde yapılan değişiklikler insan duyuları tarafından algılanabilecek konumda olmamalı
- Çünkü, algılanması durumunda gizli iletişim ortaya çıkar ve üçüncü kişinin, taşıyıcının içerisindeki gizli veri üzerinde çeşitli işlemler yapabilir

Steganografik Bir Algoritmanın Temel Özellikleri

- Saklanabilecek Veri Miktarı
 - Örtü veri içerisinde gizlenebilecek veri miktarı da önemli bir etkindir 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.

Steganografik Bir Algoritmanın Temel Özellikleri

- Dayanıklılık
 - Gizlenen verinin yapılan saldırılar sonucunda bile, gizliliğini korumaya devam etmesi
 - 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.

- Bilgi Gizleme Nedir?
- Steganografi Nedir?
 - Steganografi ve Kriptografi' nin Farkları
 - Steganografi' nin Doğuşu
 - Nasıl Çalışır?
- Steganografik Bir Algoritmanın Temel Özellikleri
- Steganografi'de Kullanılan Yöntemler
- Kullanım Alanları

Kullanılan Yöntemler

- Yer Değiştirmeye dayalı yöntemler
- İşaret İşlemeye dayalı yöntemler
- Spektrum Yayılmasına Dayanan Yöntemler
- İstatistiksel yöntemler

Kullanılan Yöntemler

- Yer Değiştirmeye Dayalı Yöntemler
 - Temel olarak resim dosyasında piksel renklerini temsil eden değerler üzerinde çalışılmaktadır
 - Pikselin rengi bir byte ile ifade edilmektedir
 - Bu byte'ların en düşük bitlerinin değişmesi resim görüntüsünde gözle fark edilmesi zor bir fark yaratmaktadır

Kullanılan Yöntemler

- Yer Değiştirmeye Dayalı Yöntemler
 - Bu yöntemde resim dosyalarını oluşturan renk birimlerinin en küçük anlamlı biti artırıp azaltılarak bu bit üzerinde veri saklanır.



255,0,0



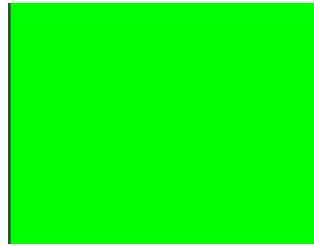
0,255,0



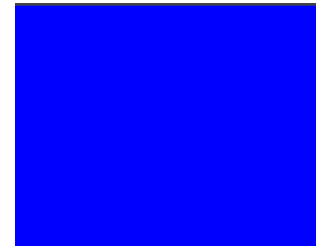
0,0,255



254,0,0



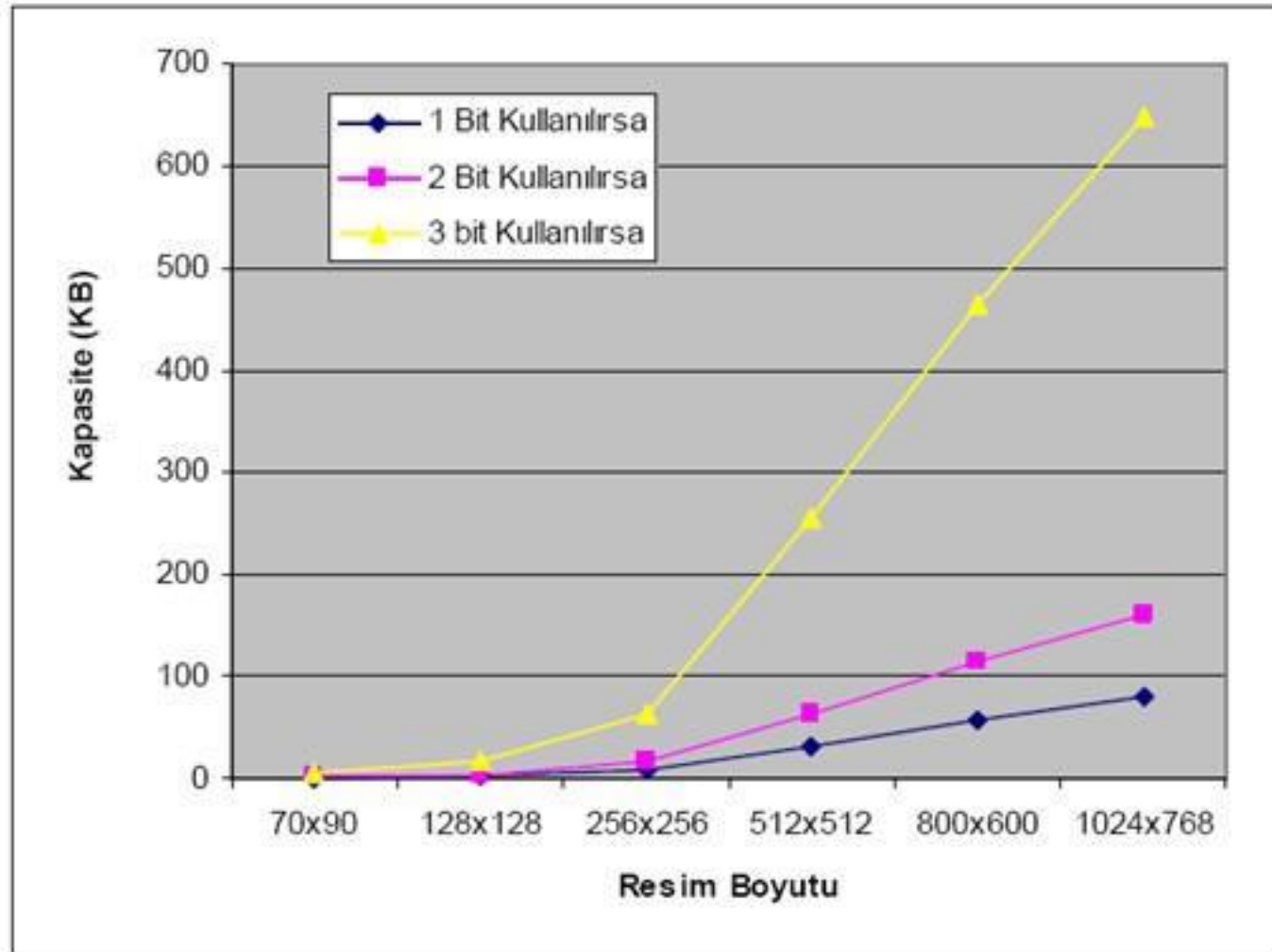
0,254,0



0,0,254

Kullanılan Yöntemler

- Yer Değiştirmeye Dayalı Yöntemler



Kullanılan 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.

Kullanılan Yöntemler

- Avantajları:
 - Gerçeklemeleri oldukça basit
 - Yüksek veri saklama miktarı
- Dezavantajları:
 - En hafif resim işleme yöntemlerine karşı oldukça zayıf olmaları
 - Taşıyıcı resmin parlaklığının bile değiştirilmesi gizli verinin tamamen yok olmasına neden olacaktır

Kullanılan Yöntemler

- Spektrum Yayılmasına Dayanan Yöntemler
 - Spektrum yayılmasına dayanan yöntemlerde, gönderilmek istenen mesaj ihtiyaç duyduğu frekans bandından çok daha fazlasına dağıtılmaktadır. Üçüncü bir kişi araya girip bir yada birden fazla frekans bandında bozulmalara neden olsa bile, alıcı geri kalan frekans bantlarındaki bilgiler ile asıl mesajı elde edebilmektedir.

Kullanılan Yöntemler

- İstatistiksel Yöntemler
- Çalışmalar, 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.

Kullanılan Yöntemler

- İstatistiksel 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.

Kullanım Alanları

- Örgüt içi haberleşmelerde
- Ülke güvenliğinde
- Savaş anında



Kullanım Alanları

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

Kullanım Alanlar

Metin Steganografi

- Taşıyıcı ortamın text olduğu Steganografi alanı
- Uygulanması zor bir veri gizleme şekli
- Saklanacak veri miktarı az
- Bunun nedeni taşıyıcı text'in içindeki gereksiz alanların ve boşlukların miktarının az olması
- 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.

- Açık Alan Yöntemleri (Open Space Methods)
- Yazımsal Yöntemler
- 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

Yazımsal 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 “0” olarak belirlenir ve kodlama işlemi bu şekilde yapılır.
- “bread, butter, and milk”
- “bread, butter and milk”

Kullanım Alanlar

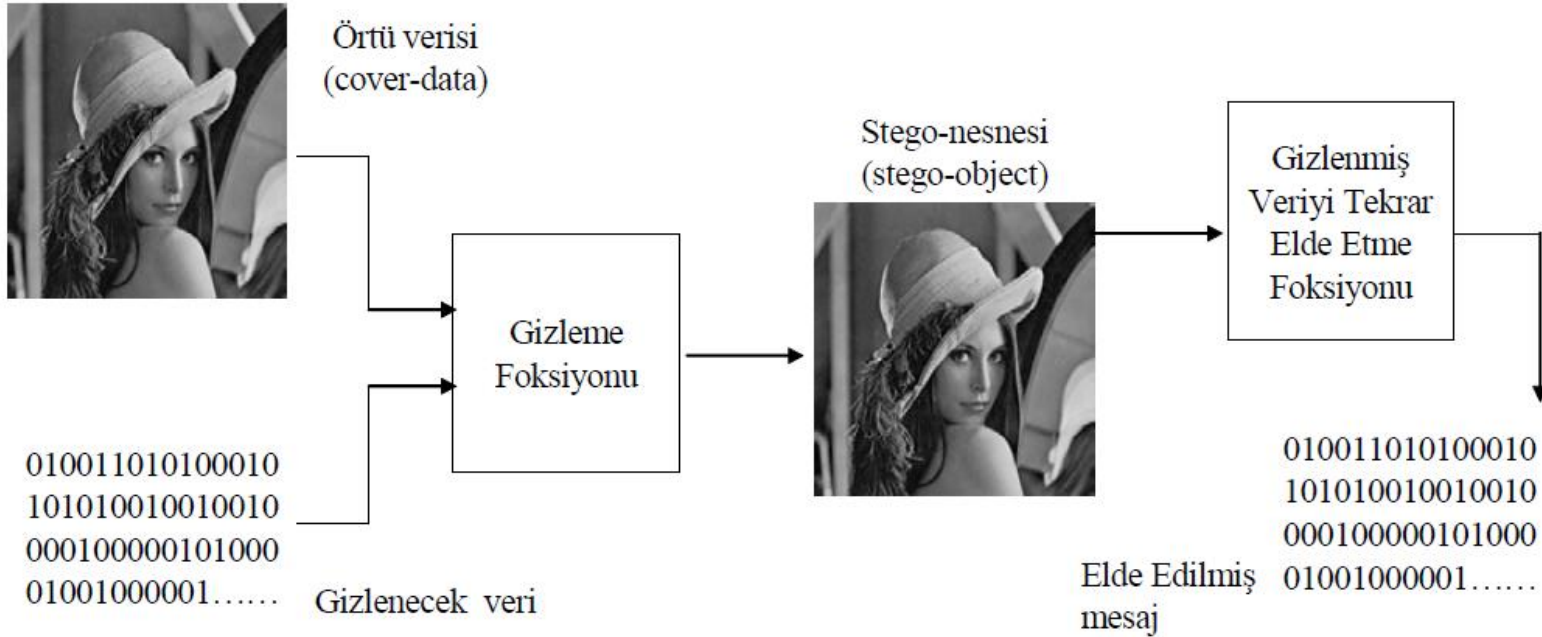
Metin Steganografi

Anlamsal Yöntemler

- Bu yöntemde eş anlamlı 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 Steganografi



Şekil 1. Steganografik sistem

Kullanım Alanları

Görüntü Steganografi

Bilgilerin görüntü dosyaları içerisine saklanması için çeşitli yöntemleri vardır. Bunlardan en bilinen 2 tanesi:

1. En önemsiz bite ekleme
2. Maskeleye ve filtreleme

Kullanım Alanları

Görüntü Steganografi

En önemsiz bite ekleme(LSB Insertion)

- En önemsiz bite ekleme yöntemi yaygın olarak kullanılan ve uygulaması basit bir yöntemdir.
- Renkli dijital görüntüler 24 bit ya da 8 bit olabilir.

Kullanım Alanları

Görüntü Steganografi

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 Steganografi

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 Steganografi

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 Steganografi

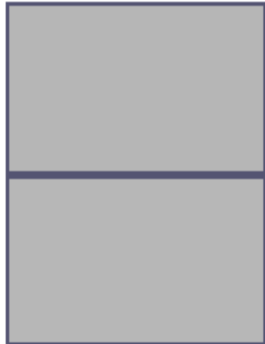
Gri-Seviye görüntüler:

- 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 Steganografi

Gri-Seviye görüntüler:

	Renk değeri	İkilik Sistemdeki Karşılığı	Rengi
Orijinal piksel	182	10110110	
Bilgi saklanmış piksel	183	1011011 1	

Kullanım Alanları

Görüntü Steganografi

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 Steganografi

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

Ses Steganografi

- Yaygın dağıtımı ve içerdiği bilginin özelliklerinin benzerliği dolayısıyla ses dosyaları da resim dosyaları gibi steganografi uygulamalarında kullanılmaktadır.
- Mevcut Yöntemler:
 - Düşük Bit Kodlaması (Low bit encoding)
 - Faz Kodlaması (Phase coding)
 - Yayılmış Spektrum (Spread spectrum)
 - Yankı Veri Saklaması (Echo data hiding)

Kullanım Alanları

Ses Steganografi

Düşük Bit Kodlaması

- Görüntü steganografi de bahsettiğimiz LSB insertion yöntemiyle aynı şekilde gerçekleştirilir
- Ses dosyasındaki verinin her byte ının 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 Steganografi

Faz Kodlaması

- Gizli veriyi gömme işleminde ses dosyası küçük segmentlere bölünür ve her segmente ait faz, gizlenecek veriye ait faz referansı ile değiştirilir;
 - 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 Steganografi

Yayılmış Spektrum

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

Kullanım Alanları

Ses Steganografi

Yankı Veri Saklaması

- 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.
- Yankı ile veri saklama yöntemi herhangi bir gürültüye neden olmamakta veya kayıplı bir kodlama kullanmamaktadır.

Teşekkürler..

Semih CANPOLAT