ANKARA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

OPTİKSEL TELSİZ İÇİN İLETİŞİM GÜVENLİĞİ VE GİZLİLİK TEKNİKLERİNİN ANALİZİ VE DEĞERLENDİRİLMESİ

Muharrem AYYILDIZ

ELEKTRİK-ELEKTRONİK MÜHENDİSLİĞİ ANABİLİM DALI

ANKARA
2013

Her hakkı saklıdır

TEZ ONAYI

Muharrem AYYILDIZ tarafından hazırlanan "**Optiksel Telsiz için İletişim Güvenliği ve Gizlilik Tekniklerinin Analizi ve Değerlendirilmesi**" adlı tez çalışması 20.08.2013 tarihinde aşağıdaki jüri tarafından oy birliği ile Ankara Üniversitesi Fen Bilimleri Enstitüsü Elektrik-Elektronik Mühendisliği Anabilim Dalı'nda **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Danışman : Yrd. Doç. Dr. Ahmet AKBULUT

Jüri Üyeleri :

Başkan : Doç. Dr. H. Gül YAĞLIOĞLU
Ankara Üniversitesi, Fizik Mühendisliği ABD

Üye : Prof. Dr. H. Gökhan İLK
Ankara Üniversitesi, Elektrik-Elektronik Mühendisliği ABD

Üye : Yrd. Doç. Dr. Ahmet AKBULUT
Ankara Üniversitesi, Elektrik-Elektronik Mühendisliği ABD

Yukarıdaki sonucu onaylarım

Prof. Dr. İbrahim DEMİR
Enstitü Müdürü

ÖZET

Yüksek Lisans Tezi

OPTİKSEL TELSİZ İÇİN İLETİŞİM GÜVENLİĞİ VE GİZLİLİK TEKNİKLERİNİN ANALİZİ VE DEĞERLENDİRİLMESİ

Muharrem AYYILDIZ

Ankara Üniversitesi
Fen Bilimleri Enstitüsü
Elektrik-Elektronik Mühendisliği Anabilim Dalı

Danışman: Yrd. Doç. Dr. Ahmet AKBULUT

Tez çalışmasında, iletişim güvenliği ve gizlilik tekniklerinin optiksel telsiz için genel analizi ile değerlendirilmesi yapılmış ve s*teganografi* tekniğinin optiksel telsizde uygulanabilirliği araştırılmıştır. Bu kapsamda, bilgisayarlar arası optiksel telsiz bağlantısı için donanım gerçekleştirilmiştir. *Donanım* üzerinden steganografi tekniğiyle taşıyıcı resme eklenen bir dosyanın karşı tarafa iletilmesi ve karşı tarafta alınan resmin çözülerek, eklenen dosyanın tekrar elde edilmesi işlemleri için *yazılım* geliştirilmiştir. Ayrıca, veri gönderme performansı da değerlendirilmiştir. Son olarak, geleceğe yönelik öneriler sunulmuştur.

Ağustos 2013, 77 sayfa

Anahtar Kelimeler: Optiksel Telsiz, Güvenlik, Bilgi Gizliliği, Steganografi

ABSTRACT

Master Thesis

ANALYSIS AND EVALUATION OF COMMUNICATION SECURITY AND PRIVACY TECHNIGUES FOR OPTICAL WIRELESS

Muharrem AYYILDIZ

Ankara University
Graduate School of Natural and Applied Sciences
Electrical and Electronics Engineering Department

Supervisor: Asst. Prof. Dr. Ahmet AKBULUT

In this thesis, the communication security and privacy techniques of optical wireless have been analysed and the applicability of *steganopraphy* technique to optical wireless has been investigated. In this context, a *hardware* has been developed to conduct optical wireless connection between computers. In order to transfer a file which was added to a carrier image through the hardware by using steganopraphy technique and to obtain the same file by decrypting the transferred image, a *software* has been developed. Additionally, performance of data transfer has also been evaluated. Finally, various recommendations for further studies have been presented.

August 2013, 77 pages

Key Words: Optical Wireless, Secuity, Data Privacy, Steganography

TEŞEKKÜR

Tez çalışmam sırasında araştırma olanağı sağlayan, çalışmanın her safhasında yakın ilgi ve önerileri ile beni yönlendiren danışman hocam, Sayın Yrd. Doç. Dr. Ahmet AKBULUT'a (Ankara Üniversitesi Mühendislik Fakültesi Elektrik-Elektronik Mühendisliği), fahri tez danışmanlığı yaparak ilgi gösteren eski danışman hocam emekli öğretim üyesi Sayın Prof. Dr. Faruk ÖZEK'e (Ankara Üniversitesi Mühendislik Fakültesi Elektrik-Elektronik Mühendisliği), tez çalışmamda kullandığım donanım cihazını geliştirmemde yardımcı olan Gökhan USTA'ya ve aileme teşekkürlerimi sunarım.

Muharrem AYYILDIZ
Ankara, Ağustos 2013

İÇİNDEKİLER

ÖZET ..... **i**
ABSTRACT ..... **ii**
TEŞEKKÜR ..... **iii**
KISALTMALAR DİZİNİ ..... **vi**
ŞEKİLLER DİZİNİ ..... **vii**
ÇİZELGELER DİZİNİ ..... **ix**
1. GİRİŞ **1**
1.1 Tanımlar **1**
1.2 OTİS **2**
1.2.1 Uygulama örnekleri **5**
2. İLETİŞİM GÜVENLİĞİ VE GİZLİLİK TEKNİKLERİ **7**
2.1 Optisel Telsiz Teknolojisinde Güvenlik **8**
2.2 Steganografi **13**
2.2.1 Steganografi sistemi **16**
2.2.2 Görüntü steganografisi **18**
3. MATERYAL VE YÖNTEM **25**
3.1 Sistem Blok Diyagramı **25**
3.2 Sistem Veri İletim Tekniği **26**
3.2.1 Seri port veri iletimi **26**
3.3 Sistem Donanım Yapısı ve Bileşenleri **30**
3.4 Sistem Yazılım Uygulaması **34**
3.4.1 Yazılımın özellikleri **34**
3.4.2 Veri gizleme (saklama) işlemi **36**
3.4.3 Veri çözme işlemi **36**
4. BULGULAR **38**
4.1 Steganografi Yazılımının Performansı **38**
4.2 Optiksel Telsiz Veri İletim Değerlendirmesi **49**
5. TARTIŞMA VE SONUÇ **52**
KAYNAKLAR **55**
EKLER **58**

EK 1 Deney Düzeneği Görünümü 59
EK 2 Elektronik Devre Şeması 60
EK 3 Transistör Özellikleri 61
EK 4 Foton Diyotun Özellikleri 65
EK 5 Yazılım Veri Gizleme Adımları 68
EK 6 Yazılım Veri Çözme Adımları 72
EK 7 PSNR Hesaplama Kodu (MATLAB) 76
ÖZGEÇMİŞ 77

KISALTMALAR DİZİNİ

BMP	Bitmap
C#	C Sharp
DCT	Discrete Cosine Transform
DFT	Discrete Fourier Transform
EIA	Electronics Industries Association
GIF	Graphic Interchange Format
İİS	İnsan İşitme Sistemi
JPEG	Joint Photographic Experts Group
LED	Light Emitting Diode
LMDS	Yerel Çok Noktalı Dağıtım Sistemi
LOS	Line of Sight
LAN	Local Area Network
LSB	Least Significant Bit
MSB	Most Significant Bit
OSI	Open Systems Interconnection
OTIS	Optiksel Telsiz İletişim Sistemi
PSNR	Peak Signal to Noise Ratio
RF	Radyo Frekans
TTL	Transistor-Transistor Logic

ŞEKİLLER DİZİNİ

Şekil 1.1 Genel iletişim sistemi blok diyagramı 1
Şekil 1.2 OTİS çalışma prensibi 3
Şekil 1.3 Yeni kullanıcının son noktaya bağlantısı 5
Şekil 2.1 LOS ortamında optiksel telsiz teknolojisiyle LAN-LAN bağlantısı 9
Şekil 2.2 RF ve Optiksel telsiz güvenlik karşılaştırması 10
Şekil 2.3 Optiksel telsizlerde güvenlik ihtiyacı 12
Şekil 2.4 Optiksel telsiz sinyalinin korunması 12
Şekil 2.5 Steganografi sistemi (Şahin vd. 2005) 16
Şekil 2.6 Veri ekleme algoritması 17
Şekil 2.7 Veri çıkarma algoritması 17
Şekil 2.8 Sayısal resmin yapısı 18
Şekil 3.1 Bilgisayarlar arası seri port üzerinden OTİS iletişimi 25
Şekil 3.2 Sayısal sinyal değerleri 26
Şekil 3.3 Asenkron veri iletim formatı 28
Şekil 3.4 RS232 seri portun 9-pin D tipli konektör yapısı ve uç ayrıntıları 29
Şekil 3.5 Gönderici ünite 31
Şekil 3.6 Alıcı ünite 31
Şekil 3.7 Gaz moleküllerinin dalga boyuna değişimine bağlı geçirgenliği 33
Şekil 3.8 Yazılım modüler yapısı 35
Şekil 3.9 Veri gizleme işlemi 36
Şekil 3.10 Veri çözme işlemi 37
Şekil 4.1 Taşıyıcı resimler 39
Şekil 4.2 Beyaz renkli resim için LSB bit değişim miktarları 40
Şekil 4.3 Beyaz renkli resim için PSNR-Değişim miktarı grafiği 41
Şekil 4.4 Yeşil renkli resim için LSB bit değişimleri 42
Şekil 4.5 Yeşil renkli resim için PSNR-Değişim miktarı grafiği 43
Şekil 4.6 Az detaylı resim için LSB bit değişimleri 44
Şekil 4.7 Az detaylı resim için PSNR-Değişim miktarı grafiği 45
Şekil 4.8 Detaylı resim için LSB bit değişimleri 46
Şekil 4.9 Detaylı resim için PSNR-Resim değim miktarı grafiği 47

Şekil 4.10 Tez çalışmasında kullanılan taşıyıcı nesne ve taşınacak dosya 49

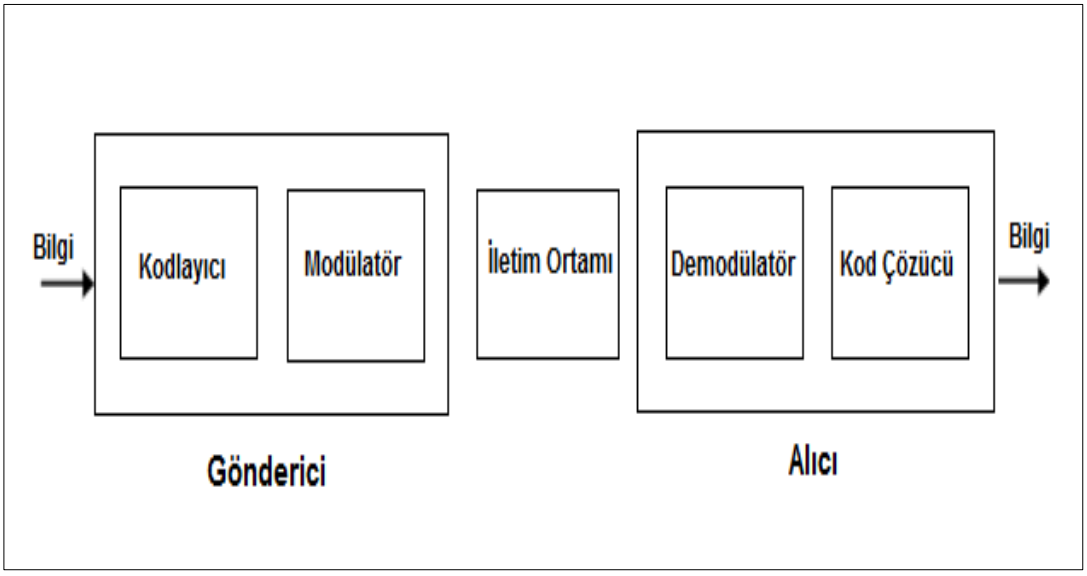
ÇİZELGELER DİZİNİ

Çizelge 2.1 Gri seviyeli resimlere LSB yöntemi uygulanması 20
Çizelge 2.2 8-bit renkli resimlere LSB yöntemi uygulanması 21
Çizelge 2.3 Orijinal 3 piksel değeri 21
Çizelge 2.4 A karakteri eklendikten sonraki piksel değerleri 22
Çizelge 3.1 Verici parametreleri 31
Çizelge 3.2 Alıcı parametreleri 32
Çizelge 4.1 Beyaz renkli resim için PSNR değerleri 40
Çizelge 4.2 Yeşil renkli resim için PSNR değerleri 42
Çizelge 4.3 Az detaylı bir resim için PSNR değerleri 44
Çizelge 4.4 Detaylı bir resim için PSNR değerleri 46
Çizelge 4.5 Büyük taşıyıcı resim ve büyük dosya taşınması 49
Çizelge 4.6 Orta boyutlu taşıyıcı resim ve orta boyutlu dosya taşınması 50
Çizelge 4.7 Küçük taşıyıcı resim ve küçük dosya taşınması 51

1. GİRİŞ

1.1 Tanımlar

İletişim, basitçe bir bilginin A noktasından bir B noktasına iletilmesidir. Günümüzde iletişim teknolojilerindeki gelişmeler sonucunda bilgi iletim işleminde mesafeler, cm mertebesinden binlerce km'ye kadar uzanabilmektedir. Bu nedenle kapsama alanına göre ağ yapıları gelişmiştir. Genel olarak bilgi iletilirken yapılması gereken, bilgiyi ortam koşullarından etkilenmeden en doğru bir şekilde iletmektir (Sarı 2008). İletişim teknolojilerinde haberleşme sistemleri şekil 1.1'de görüldüğü gibi üç ana bileşene sahiptir.



Şekil 1.1 Genel iletişim sistemi blok diyagramı

Gönderici: Gönderilecek olan bilginin kodlanması ve modüle edilmesi işlemleri yapılarak sinyalin iletim ortamına gönderilmesini sağlar.

İletim Ortamı: Sinyalleri iletmek için kullanılan ortamdır. Ortam kablolu ağlarda bakır veya fiber optik kablo olurken, kablosuz ağlarda RF (Radyo Frekansı) veya lazer ışın demetlerinin iletildiği atmosfer veya serbest uzay olabilmektedir.

Alıcı: İletim ortamında gönderilen sinyallerin alınarak demodüle edilmesi ve kod çözücüden geçirilerek bilginin elde edilmesini sağlamaktadır.

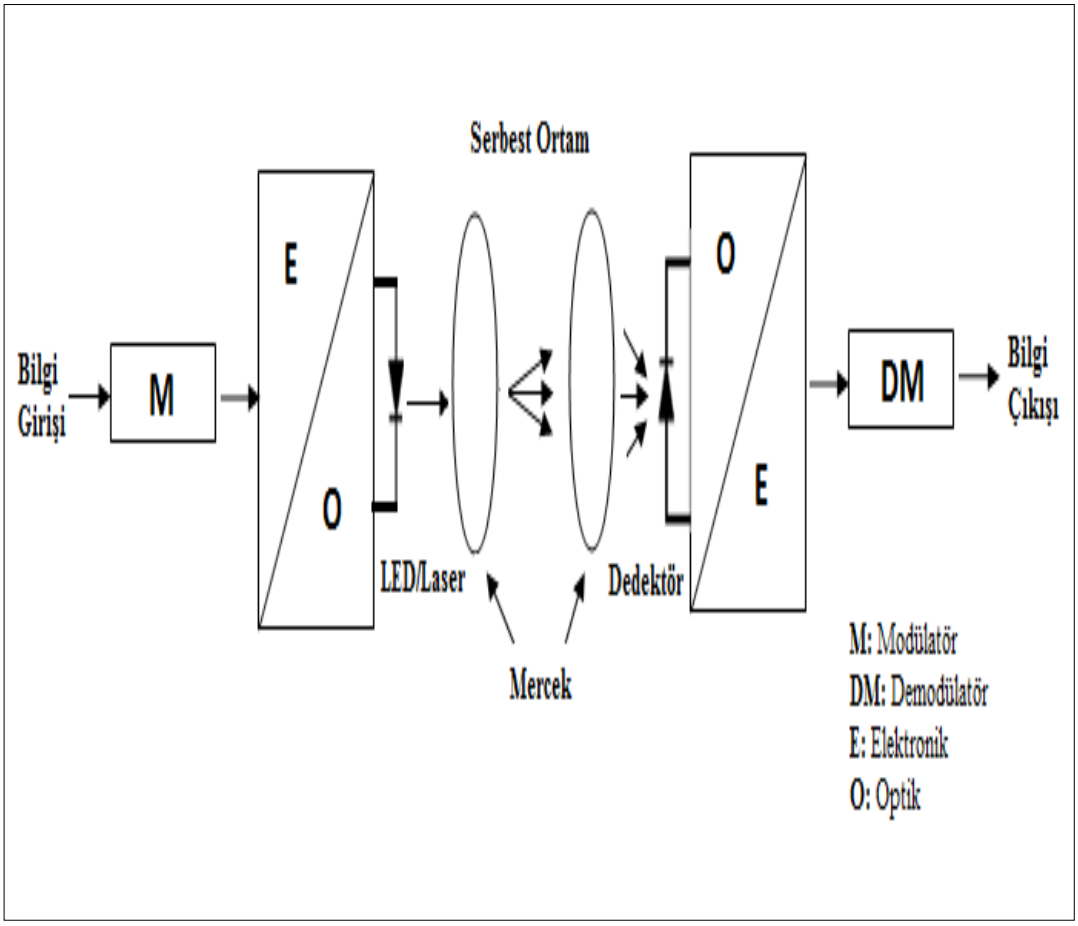
Bant genişliği (*band width*) iletişim ortamının haberleşme kapasitesini ifade etmektedir. Bant genişliğinin büyüklüğüne göre iletilecek sinyalin miktarı da değişim göstermektedir. Günümüzde internetin yaygınlaşması, kullanıcıların hareket halindeyken yüksek hızlarda bilgiye ulaşmak istemeleri, kısıtlı bir kaynak olan bant genişliğinin etkin kullanımını gerektirmiştir. Bu gereksinimi sağlamak için farklı teknolojiler kullanılmaktadır.

Bant genişliğini adresleme için kullanılan en iyi alternatif fiber optik teknolojisidir. Fiber, en güvenilir optik iletişim yapısına sahip olmasına rağmen, kablolama ve altyapı maliyetleri yönüyle oldukça pahalıdır. İkinci alternatif, RF teknolojisidir. RF günümüzde çok geniş bir kullanım alanı bulmuştur. RF tabanlı ağlar genelde spektrum lisansına sahiptir ve büyük yatırım gerektirmektedir. Bununla birlikte, RF tabanlı ağlar uzun mesafelerde ve noktadan çok noktaya çalışabilmektedir.

Üçüncü bir alternatif; kablo modem, DSL gibi bakır tabanlı teknolojilerdir. Bakır altyapısı fiber optik teknolojisine göre daha yaygındır. Temel sorun, bant genişliğinin ölçeklenmesi (scalability) olduğundan, bakır altyapısı da iyi bir alternatif olmamaktadır. Dördüncü ve en uygun alternatif ise FSO (Free Space Optics) teknolojisidir (Willebrand ve Ghuman 2002). FSO, optiksel telsiz iletişim sistemi (OTİS) olarak da adlandırılabilir. OTİS ölçeklenebilir bant genişliği, yüksek hız ve maliyet etkinliği sunmaktadır.

1.2 OTİS

İletişim teknolojilerindeki gelişmeler, kullanıcıların geniş bant ve kablosuz iletişime ihtiyaç duyması gibi nedenlerden dolayı; OTİS giderek büyük önem kazanmaktadır. OTİS'de bilgi taşıyıcı olarak, modüle edilmiş lazer demetleri kullanılmaktadır. Genel bir OTİS'in bileşenleri ve çalışma prensibi şekil 1.2'de gösterilmiştir.



Şekil 1.2 OTİS çalışma prensibi

Çalışma prensibi

OTİS'de iletilecek bilgi öncelikle bir kodlama işlemine tabi tutulmaktadır. Kodlanan bilgi daha sonra bu bilgiyi uzak mesafelere kadar taşıyacak olan periyodik bir sinyalin üzerine modülasyon teknikleriyle bindirilir (Sarı 2008). Elde edilen elektronik sinyal optik sinyale çevrilerek bir yarı iletken lazer diyod veya ışık yayıcı LED (Light Emitting Diode) diyod üzerinden iletim ortamı boyunca iletimi sağlanır. İletim ortamında ilerleyen bilgiyi içeren sinyal alıcı tarafından algılanır. Alıcı olarak genellikle foton dedektörler kullanılmaktadır. Algılanan optik sinyal elektronik sinyale çevrilir. Sinyal bindirme işleminin tersi bir işlemle (*demodülasyon*) bilgi ve iletişim sinyali ayrıştırılarak bilginin kodu çözülür (Sarı 2008). Sonuç olarak, bilgi alıcı tarafta elde edilmiş olur.

Avantajlar

- RF sistemleri, uluslararası organizasyonlar ve ülke kullanımlarında lisansa tabi olurken, optiksel telsizler lisans gerektirmeden kullanılabilmektedir.
- Yüksek bant genişliği sayesinde yüksek hızda veri iletimi sağlamaktadır. Böylece; ses, metin, görüntü gibi veriler geniş bant iletim ortamında yüksek sinyal kalitesinde iletilebilmektedir.
- Genellikle noktadan noktaya (*point to point*) ve lazer alıcı-verici arasında LOS (Line of Sight) denilen doğrudan görüş hattı özelliğiyle çalışır. Bu özelliğiyle, RF sistemlerinde olduğu gibi iletişim kanallarından kaynaklanan girişim (*enterferans*) olayından etkilenmez.
- OTİS'in kablolu sistemlere göre montajı kolaydır. Bu özelliğiyle, kurulumu fiber optik kablo maliyetlerine göre daha ucuzdur.
- Bilginin dar bir saçılma açısına sahip ışık demeti üzerinden gönderilmesinden dolayı dışarıdan hattın dinlenmesi ve bilgi sızması gibi durumlara karşı dayanıklılığı; RF iletişimine göre oldukça iyi bir yapıdadır. Böylece, iyi bir iletişim güvenliği ve bilgi gizliliği elde edilebilmektedir.

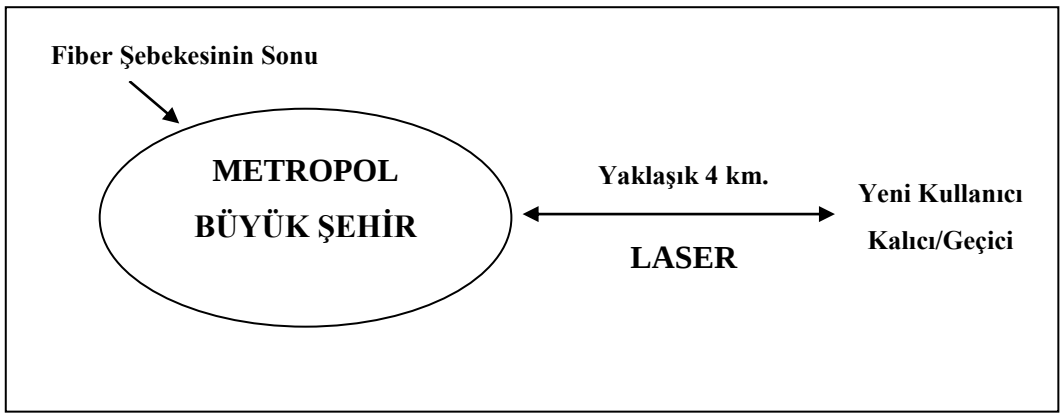
Dezavantajlar

- İletişim kanalı atmosfer olduğundan ortamın yapısal karakteristiklerinden ve iklimsel olaylardan kaynaklanabilecek bozucu etkilere maruz kalabilmektedir. Örneğin; puslu, karlı veya sisli havalarda optiksel telsiz sistemi olumsuz etkilenebilmektedir. Bu nedenle; iletişim uzaklığı kısa mesafeli olabilmektedir (2-5 km).
- Çevre ışığından olumsuz etkilenebilmektedir.
- Türbülans ve parıldama (*scintillation*) sonucu iletim etkilenmektedir.
- OTİS üzerinde sınırlayıcı bir diğer etken de LOS özelliğini sağlamak için ağaç, tepe, bina gibi nesnelerin iletişim ortamı üzerinde olmaması gerekliliğidir (Majumdar ve Ricklin 2008).

1.2.1 Uygulama örnekleri

OTİS; kurumsal ve sivil iletişim alanlarında; yüksek veri hızı sağlaması, çabuk kurulumu, taşınabilirliği ve güvenlik özelliklerinden dolayı oldukça yaygın bir kullanım alanına sahiptir. Günümüzde bu sistemlerin yoğun kullanım alanları şunlardır:

- **Last mile problem:** İlk ve en önemli uygulaması, fiber optik şebekenin son noktasında bağlantı sorununa sağladığı çözümüdür (Şekil 1.3).



Şekil 1.3 Yeni kullanıcının son noktaya bağlantısı

- **Kampüs ve üniversite alanları:** Özellikle LMDS (Yerel Çok Noktalı Dağıtım Sistemi) sistemlerine alternatif olarak kampüs alanlarında kullanılabilmektedir.
- **İş merkezleri grubu:** Eminönü-Maslak arasındaki veri omurgası kurulu olup, 13 km mesafe aralığında hizmet sunmaktadır (Anonim 2004).
- **Doğal afet bölgeleri:** Afet durumlarında noktadan noktaya çalışmasından dolayı acil iletişim sistemi olarak kullanım potansiyeli vardır.
- **Metro istasyonları - Tren:** RF sistemlerinin kapsama alanı dışında kalabileceği (metro istasyonu, tünel vs.) kapalı ortamlarda iletişimin sağlanmasında kullanılabilir.
- **Askeri stratejik alanlar:** Girişime maruz kalmaması, dar bir demet açısına sahip olmasından dolayı özellikle, gizlilik isteyen askeri terminaller arasında bilgi aktarımında kullanılabilmektedir. Ayrıca, mali, hukuki ve diğer hassas bilgilerin

kablosuz iletiminde de yüksek bir güvenlik sağlamak için ideal bir çözümdür (Majumdar ve Ricklin 2008).

- Hastane ve cezaevi blokları arası kablosuz iletişim sağlayabilir.
- Kısa kullanım süreli ve yüksek kapasiteli iletişimin gerektiği konferanslar, spor salonları gibi kapalı alanlardan yayın amacıyla kullanılabilir.
- Yer istasyonları ve uzay araçları arasındaki iletişimi sağlamak için de kullanılabilir (Majumdar ve Ricklin 2008).

Tez çalışmasının amacı, OTİS güvenliği için geliştirilen ve literatürde yer alan tekniklerin incelenmesi ve bilgi gizliliğini sağlamak amacıyla kullanılan *steganografi* tekniğinin iki bilgisayar arasında seri port OTİS üzerinden gerçekleştirilmesi ve sistemin performansının değerlendirilmesidir.

2. İLETİŞİM GÜVENLİĞİ VE GİZLİLİK TEKNİKLERİ

İletişim teknolojilerindeki gelişmeler bilgi çağı olarak nitelendirilen günümüzde giderek önem kazanmaktadır. Kullanıcıların ihtiyaç duyduğu bilgiye daha hızlı şekilde ulaşma istekleri, iletişim teknolojilerinin gelişimini sağlamıştır. Özellikle, internet teknolojisinin yaygınlaşması, paylaşılan bilginin artmasını da beraberinde getirmiştir. Bu durum, iletişim teknolojilerinde bilginin göndericiden alıcı tarafa güvenli bir şekilde iletimini gerektirmiştir.

Güvenlik, kablolu veya kablosuz her türlü ağ için oldukça önemli bir konudur. Klasik bir kablolu ağda iletişim, fiziksel kablolar üzerinden sağlanır ve güvenlik, genellikle fiziksel altyapıda dâhili olarak bulunur (Harmankaya vd. 2008). Kablosuz ağlar ise RF sinyalleri, mikro dalga veya serbest uzay optik ortamını kullanır ve bu nedenle aynı güvenlik önlemlerinin uygulanması mümkün olmamaktadır. Kablosuz ağ kullanıcılarının verilerini korumak için çeşitli güvenlik teknikleri kullanılmaktadır.

İletişim güvenliği kavramı; kullanıcılara giriş hakkı verilmesi (*authentication*), yetkilendirme (*authorization*), veri bütünlüğünün sağlanması (*data integrity*) ve gizlilik (*privacy*) alanlarında ele alınmaktadır (Karaboğa ve Ökdem 2006). Güvenliğin genel gereksinimleri şunlardır (Pehlivan vd. 2008):

- İletişim esnasında bilgilerin dinlenilmesini önlemek
- Bilginin ya da verinin değiştirilmesini önlemek
- Yapılan veri transferlerinin istenmeyen kişiler tarafından ele geçirilmesi, diğer bir ifade ile bilgi hırsızlığını önlemek

Bilgi güvenliği açısından iletişim ağına bağlanacak olan kullanıcıların yetkili bir şekilde giriş yapmalarının sağlanması gerekmektedir. İletim ortamından gönderilen bir verinin alıcı tarafından alındıktan sonra, gerçekten ilgili kaynak tarafından gönderilip gönderilmediğinin bilinmesi için veri doğrulama (*data authentication*) işleminin

yapılması önemlidir. Veri doğrulama için iletişimin gizli bir anahtar kodla yapılması gerekir. Bu kod, zamanla değişen yapıda olmalı ve ağ dışındaki elemanlar tarafından çözümlenemeyecek yapıda olmalıdır (Karaboğa ve Ökdem 2006).

Bir ağ tarafından yayınlanan verilerin, istenmeyen kişiler tarafından dinlenmesini önlemek amacıyla gizli bir anahtarla şifrelenmesi (*data encryption*) gerekmektedir. Karşılıklı haberleşen elemanlar tarafından bilinen bu anahtar, veri güvenliğinin sağlanmasında önemli rol oynamaktadır (Karaboğa ve Ökdem 2006).

İletişim esnasında alınan bir verinin istenilmeyen unsurlar tarafından değişikliğe uğradığının kontrolü gerekebilir. Bu işlem, veri bütünlüğü (*data integrity*) anlamına gelmektedir. İletişim hattı üzerinden farklı bilgilerin güvenli bir şekilde iletilmesi için kullanılan *kriptografi*, *steganografi* gibi teknikler ise bilgi gizliliği (*privacy*) sağlamaktadır (Karaboğa ve Ökdem 2006).

Bu bölümde ilk olarak, OTİS iletişim güvenliği ve gereksinimleri incelenmiştir. Son olarak, kriptografi ve steganografi teknikleri tanımlanmış ve steganografi sisteminin nasıl çalıştığı ve kullanılan tekniklerin neler olduğuna değinilmiştir.

2.1 Optisel Telsiz Teknolojisinde Güvenlik

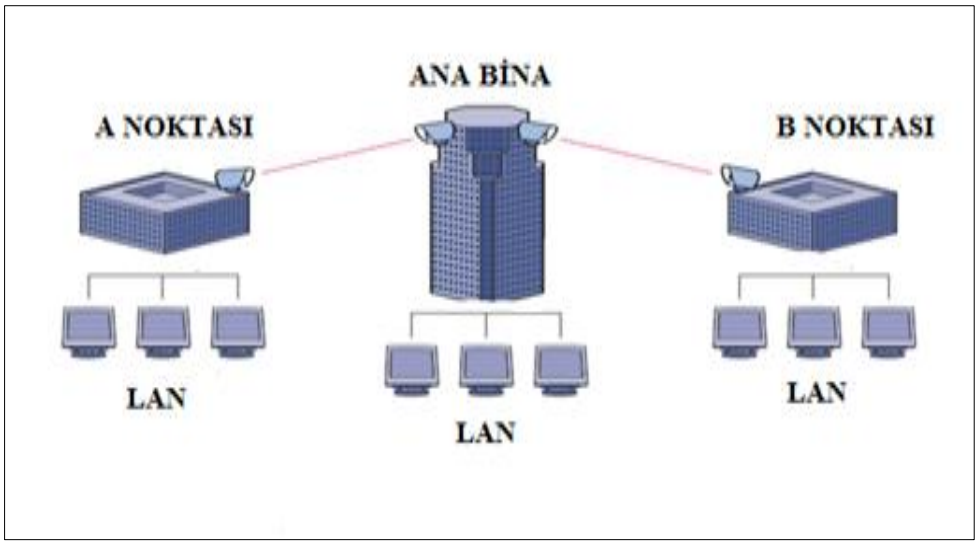
Optik iletişim, yüksek yoğunlukta trafik taşıyabilme kapasitesiyle günümüzün tercih edilen iletişim yöntemlerinden biri haline gelmiştir. Full duplex özelliğiyle gigabit ethernet hızlarına çıkabilmektedir. Diğer iletişim tekniklerinde olduğu gibi optik iletişimde de taşınan bu büyük miktardaki bilginin güvenliğinin sağlanması gerekmektedir (Toyran 2006).

RF sistemleri, OTİS'in etkilendiği atmosfer şartlarından etkilenmezler ve veri iletişiminde daha iyi bir doğruluk sağlayabilir. RF ağları geniş alanlara sinyal taşıyabilmelerine rağmen, dinleme (*intercept*) ve karıştırma (*jamming*) olarak

adlandırılan durumlara karşı dayanıksızdır. OTİS'de hassas olarak yönlendirilebilen lazerlerle; araya girme, karıştırma ve dinlenme riski olmadan noktadan noktaya (*point to point*) veri iletimi sağlanabildiği için, haberleşmedeki güvenlik boşlukları da ortadan kaldırılabilmektedir. İletişim sadece birbirini gören iki nokta arasında gerçekleşmekte; bu sayede hattın dış unsurlar tarafından dinlenmesi önlenmektedir.

OTİS, iyi bir güvenlik ortamı sağladığından dolayı geniş bir uygulama alanı bulmuştur. İlk kullanım alanlarından biri Amerikan donanmasında telsiz iletişimi ile gemiden gemiye veri iletimi sağlamasıdır (Anonymous 2002). İstenmeyen kişilere karşı ağı güvende tutmak önceliklidir. Günümüzde devlet kurumları, yüksek hızlı şebekelerde gizli bilgilerin korunması ve bütünlüğü sağlamak zorundadır. Fiber optik kablolama büyük maliyetler gerektirdiğinden bunun önüne geçmek için RF teknolojisi kullanan kablosuz çözümler geliştirilmiştir. Bu tür çözümler güvenlik riskleri ile karşı karşıyadır. Optik kablosuz çözümler ile yüksek hızlarda veri gönderebilmek hem daha ucuz hem de daha güvenli bir şekilde sağlanabilmektedir.

OTİS teknolojisi, şekil 2.1'de gösterildiği gibi birbirini gören binalar arasında LOS ortamında LAN-LAN (Local Area Network) bağlantısı sağlamak için yüksek hızlı optik kablosuz çözümler sunmaktadır (Majumdar ve Ricklin 2008).



Şekil 2.1 LOS ortamında optiksel telsiz teknolojisiyle LAN-LAN bağlantısı

Hava üzerinden kablosuz veri iletiminin güvenliği göz önüne alındığında, önemli elementlerden biri iletilen sinyalin (*path*) yoludur. RF teknolojisinde sinyal farklı yollardan alıcıya ulaşmaktadır. Bu nedenle daha çok saldırıya maruz kalmaktadır. OTİS iletim aracı olarak ayarlanmış lazer ışığı kullanır ve sinyal tüm yol boyunca çok dar tutulduğundan iletişim, güvenlik yönünden daha iyidir. Şekil 2.2'de gösterilen mavi hat RF teknolojisinin sinyal dağılımına aittir ve farklı yönlerden dağılarak alıcıya ulaşmaktadır. OTİS ise şekil 2.2 üzerinde kırmızı hat ile gösterilmiştir ve noktadan noktaya çalışmaktadır.

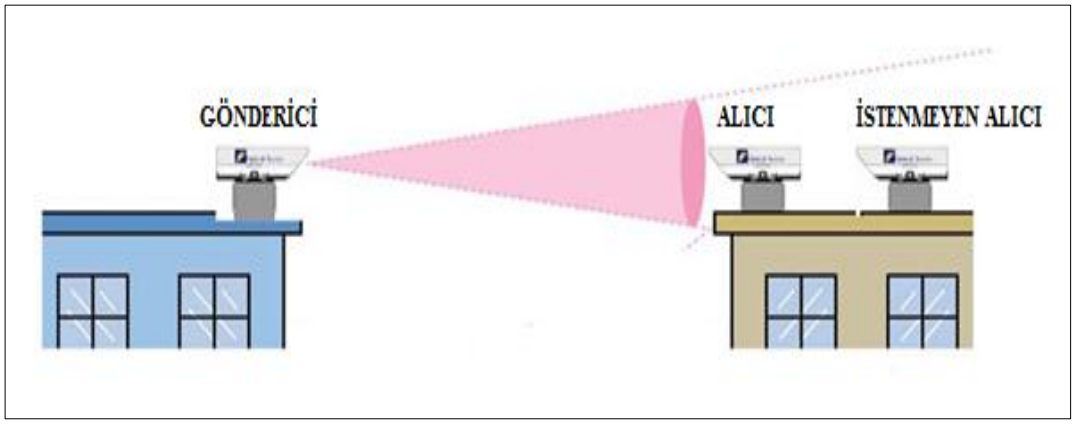


Şekil 2.2 RF ve Optiksel telsiz güvenlik karşılaştırması

OTİS, pek çok uygulamada dar bir ışın (*beam*) açısına sahip ve noktadan noktaya çalıştığından dolayı hattın dinlenmesi zordur. Bununla birlikte; bilgi gizliliğinin sağlanması ve bilginin istenmeyen alıcı tarafından alınmasını önlemek için OTİS'de güvenlik tekniklerine ihtiyaç duyulabilmektedir. OTİS'de kullanılabilecek yöntemler şunlardır:

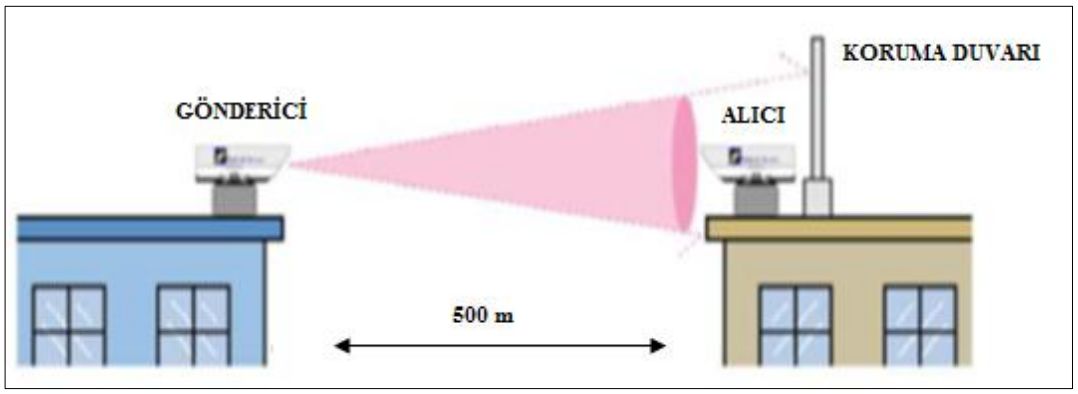
1. Kablolu ağlarda bir cihazı dinlemek (*intercept*) için "*wiretap*" terimi kullanılmaktadır. Optiksel telsiz teknolojisindeki ışık demeti üzerinden veri toplama için de "*beamtap*" terimi kullanabilir. OTİS'i tap etmek için fiziksel bir ekipmanın olması gerekmektedir (Anonymous 2002). OTİS, iletimi konik biçimli ışık hüzmesiyle sağlar. Bu konik şekil boyutları, bazı tasarımlarda çok dar bir ışın kullanırken bazılarında daha geniş bir ışın ile gönderim yapılmaktadır. Bunun sebebi, yüksek binaların deprem ve rüzgâr etkisiyle sallanıyor olmasıdır. Binalarda bir sallanma olması durumunda senkronizasyon kaybolabilir. Eş zamanlı olarak alıcı-verici bağlantıların her iki ucunda iletilen verinin *beamtap* edilmesi için, cihazın yaklaşık olarak optiksel telsiz birimlerine eşit uzaklıktaki noktaya yerleştirilmesi gerekmektedir. Birimlerden birine daha yakın *beamtapping* cihazı yerleştirilirse, konik biçimli saçılmalar daha küçük olacak ve ışının bozulma olasılığı daha büyük oranda artacağından iletişim kesilecektir. Pratikte, optiksel telsiz birimleri arasına *beamtapping* aygıtı yerleştirmek de zor bir işlemdir. Optiksel telsiz sistemleri genellikle binaların en yüksek yerine kurulur ve taşınabilir yapıdadır. Böyle bir ihtimale karşın; OTİS üzerinde güvenlik kameraları ile kolaylıkla herhangi bir şüpheli aktivite olduğunun tespit edilebilmesi daha uygun olacaktır.

2. Optiksel telsiz terminalleri başarılı bir işleyiş için kesintisiz bağlantı ve bütünlük sağlamaktadır. Işıma yolu üzerine istenmeyen alıcı yerleştirilerek sinyal dinlenme teşebbüsünde bulunulursa, bağlantı engellenecek ve iletişim sonlanacaktır. Optiksel telsiz sisteminde bir diğer güvenlik endişesi, alıcı arkasında geriye yansıyan ışınların bir tarafının bilgiyi alması istenmeyen ekipmanlardan, *beamtapping* edilebilmesi durumudur. Bu durum, muhtemelen tespit edilemez ve yıllarca da sürebilir. Bunu engellemek için optiksel telsiz cihazının arkasında duvar veya yansıtmayı önleyici bir nesne monte edilebilir. Optiksel telsiz cihazları, *beamtapping* gibi bir durumu engellemek için duvara yakın bir mesafeye monte edilir (Anonymous 2002). Şekil 2.3'te görüldüğü üzere gönderici tarafından gönderilen sinyal istenmeyen alıcı tarafından da alınabilecektir. Bu durumu önlemek için yetkilendirme işlemleri yapılabilmeli veya gönderilen bilginin güvenlik kodlama teknikleriyle kodlanarak istenilen alıcı tarafından alınması sağlanabilmelidir.



Şekil 2.3 Optiksel telsizlerde güvenlik ihtiyacı

Koruma amaçlı olarak; optiksel telsiz ışıma yarıçapının iki katı genişliğinde bir duvarın önüne alıcı kurulur (Kenneth 2012). Böylece, sinyal duvar tarafından emilecek ve bina ötesine yayılması engellenebilecektir (Şekil 2.4).



Şekil 2.4 Optiksel telsiz sinyalinin korunması

Geniş açılı lazer sistemlerinde istenmeyen alıcıların bilgiye ulaşabilmesini önlemek amacıyla RF teknolojisinde kullanılan kimlik asıllama işlemiyle sadece yetkili alıcıların bilgiye ulaşması sağlanabilmelidir.

3. Şifreleme ekipmanları da aynı zamanda her birimde şifreleme ve şifreyi çözme için ek olarak kullanılabilir. Örneğin, lazer sinyali elde edilse bile lazer iletiminde çıktı olarak ölçülemeyecek davranışta sayısal düzensiz kaotik (chaotic) ile iletimi

sağlayarak, şifreleme algoritmasını kırmak (*crack*) mümkün olmamaktadır. Bu durum, yüksek hızlı bağlantıları sağlayan optiksel telsiz teknolojisi için potansiyel bir şifreleme mekanizması olarak değerlendirilebilir (Anonymous 2002).

4. Güvenli bir optik iletişim yöntemi için kuantum kriptografi de kullanılabilmektedir. Kuantum kriptografi, iletişimin optik kanallar üzerinden fotonlar kullanılarak gerçekleştirildiği kriptografik bir gizli anahtar dağıtım yöntemidir. İletişim esnasında kullanılan optik hatta bir müdahale olup olmadığını da açığa çıkarabilmektedir. Kuantum kriptografide aynı polarizasyon tabanının kullanıldığı bir durum için gönderilen ve alınan bir bitin farklı çıkması, hattı dinleyen şüphelilerin varlığına işarettir. Bu özellik kullanılarak iletişim hattının güvenliğini doğrulamak, hatta şüpheli bir müdahale olup olmadığını açığa çıkarmak da mümkündür. Arada birinin olması durumunda göndericinin gönderdiği fotonları önce saldırgan alır ve yaptığı ölçümler neticesinde o da bir bit dizisi belirler. Fotonların kuantum doğasına göre saldırgan fotonları kopyalayamadığından (kopyalanamama ilkesi) onları yeniden oluşturur ve alıcıya bu yeni fotonları gönderir (Toyran 2006).

2.2 Steganografi

Steganografi ve kriptografi temelde birbirine yakın tekniklerdir. Her ikisi de haberleşme sırasında kaydedilmiş veriye bilgi ekleyerek çalışır (Elçi vd. 2008). Bunun yanında, kriptografi mesajın içeriğinin korunması ile ilgilenirken; steganografi tekniği mesaj varlığının gizlenmesiyle ilgilenmektedir (Şahin 2007).

Kriptografi, haberleşmenin güvenli olarak yapılmasını sağlar ve gizli bilginin istenmeyen üçüncü kişilerin anlayamayacağı şekle gelmesini sağlayarak koruma sağlar (Akbal vd. 2010). Kriptografi tekniğinin en büyük problemi, bilginin içeriği bilinmese bile ortada gizli bir haberleşme olduğunun anlaşılmasıdır (Çetin vd. 2008). Bu durum, kriptografi teknikleri ile değişime uğratılmış bilginin varlığından haberdar olan üçüncü kişilerin bir takım ataklar ve çözme teknikleri ile bilgiye ulaşabileceklerini

göstermektedir (Akbal vd. 2010). Kriptografi, bilgi güvenliğini sağlasa da gizliliği tam olarak sağlayamamaktadır.

Haberleşme esnasında üçüncü kişilerin bilgiden haberlerinin olmaması bilgi güvenliği açısından önemlidir. Şifreli haberleşme bilgilerinin izlenerek fark edilmesinin önüne geçmeye çalışmak için steganografi tekniği kullanılmaktadır (Çetin vd. 2008). Steganografik uygulamalarda bilgi, sadece gönderen ve alanının varlığını bildiği bir şekilde saklanmaktadır (Yalman ve Ertürk 2008). Böylece, üçüncü şahıslar mesajın varlığından haberdar olmamaktadır (Akbal vd. 2010).

Steganografi (*steganography*) iki parçadan oluşan Yunanca bir kelimedir. "*Steganos*" örtülü/gizli, "*grafi*" ise yazım/çizim anlamına gelmektedir (Amin vd. 2003). Örtülü yazma (*covered writing*) veya "*gizlenmiş yazı*" olarak dilimize çevrilebilir. Türkçe'de "*sırtörtme*" olarak da adlandırılmaktadır. Steganografi, en basit şekilde, bir nesne içerisine bir verinin gizlenmesi olarak tanımlanabilmektedir. Steganografi tekniğinin kullanımı, antik Yunan ve Herodot zamanına kadar uzanmaktadır (Akbal vd. 2010). Heredot, İran Savaşları sırasında, kafasını kazıtıp kafa derisinin üzerine, gizli bir mesaj dövmesinin yapılmasına izin veren bir haberciden bahsetmektedir. Mesaj yazıldıktan sonra haberci saçının uzamasını beklemekte, daha sonra mesajı bekleyen kişiye ulaşmakta, kafasını tekrar tıraş ettiğinde de mesaj ortaya çıkmaktadır (Şahin vd. 2005). Farklı bir uygulamada mum tablaları örtü kaynağı olarak kullanılmıştır. Mesaj, tahta üzerine yazılmakta ve bu yazı yeni bir mum tabakasıyla örtülmektedir. Böylece tablalar boş olarak gözükmektedir (Krenn 2004). 20. yüzyılda, görünmez mürekkep yaygın bir şekilde kullanılan bir diğer tekniktir. II. Dünya savaşında; meyve suyu, süt, sirke gizli mesajlaşma için kullanılmıştır. Bu teknik, sıvıların ısıtıldığında koyulaşması ve mesajın okunabilir olmasına dayanmaktadır. Daha sonraları, Almanlar mikro noktalar (*microdot*) olarak adlandırılan bir teknik geliştirmiştir. Mikrodot, bir belgenin daktilo yazısında kullanılan bir nokta kadar küçültülmesine dayanmaktadır. Mikrodotlar bir mektup veya zarf üzerine yazılan oldukça küçük bir yazı şeklindedir ve fark edilmeden gönderilebilmektedir (Krenn 2004).

Steganografi tekniğinde temel amaç, haberleşme esnasında gizli mesaj ya da bilginin varlığını saklamaktır. Yani iki nokta arasında gerçekleştirilen iletişimde gizli bir veri aktarıldığının anlaşılmasını önlemektedir. Steganografi, insanın görme ve işitme duyularınca algılanamayacak değişimler fark edilmeden resim ve ses dosyaları üzerinden veri saklanmasını desteklemektedir (Atıcı 2007).

Steganaliz kaplayıcı bir dosya içerisinde gizlenmiş olan veriyi tespit etmek amacıyla steganografiyle paralel olarak ortaya çıkmış bir bilimdir. Steganaliz, ulusal güvenliğin sağlanması ve meydana gelebilecek bir felaket durumunu önlemek amacıyla gizli (şifreli veya şifresiz) iletileri algılama için önem arz etmektedir. Steganaliz için benimsenen yaklaşımlar temel steganografi algoritmalarıyla bağlantılıdır (Meghanathan ve Nayak 2010).

Steganografi birçok alanda ve çeşitli amaçlar için kullanılmaktadır. Askeri ve istihbari alanda gizli haberleşmeyi sağlamak için kullanılabilir. Bir diğer uygulama alanı, sayısal verilerin korunması ve yasa dışı yollarla paylaşılmasını önlemek amacıyla sayısal damgalama veya filigran (*watermarking*) olarak adlandırılan bir teknik kullanılmaktadır (Çetin vd. 2008). Sahipliği sağlayan bu teknikle birlikte gizliliği sağlamak için steganografi de kullanılabilir. Ayrıca, sağlık sistemlerinde görüntüleri ve bunlar hakkındaki açıklamaları bu görüntü içine saklayıp göndermek için de kullanılmaktadır (Şahin 2007).

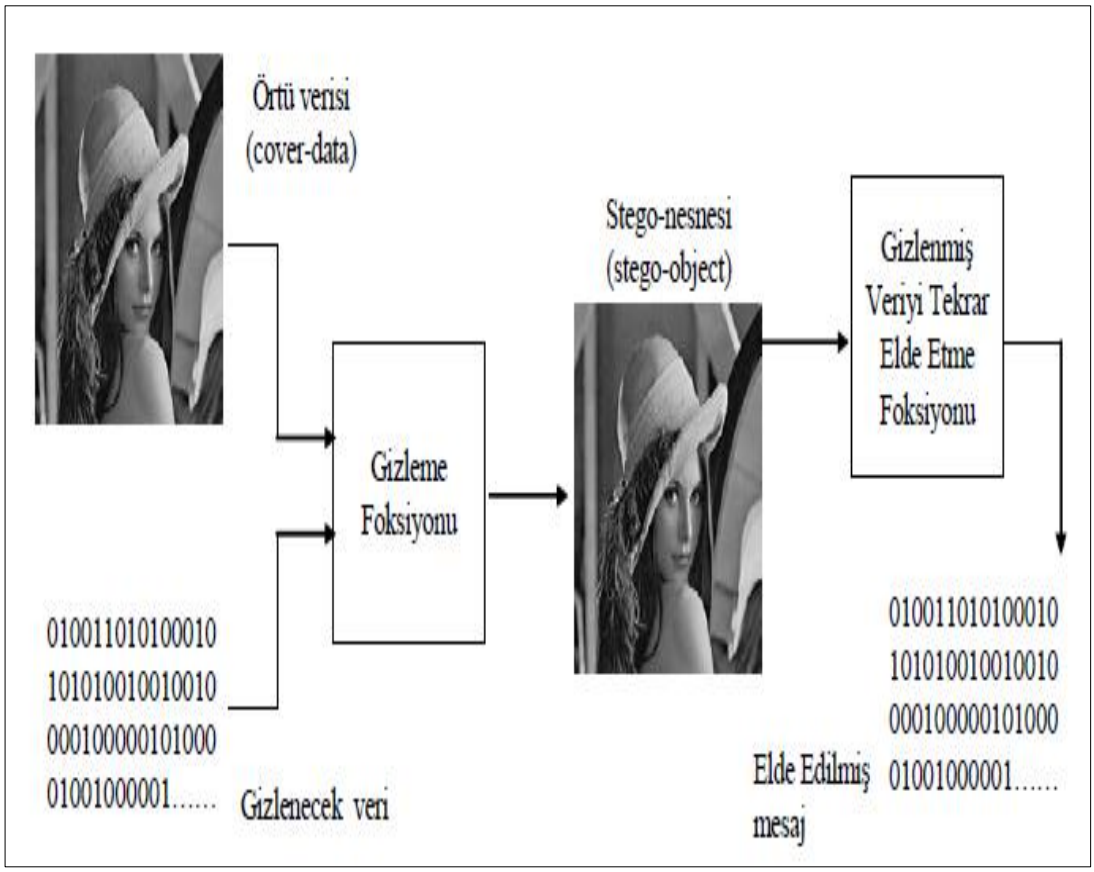
Günümüzde bilgi ve iletişim teknolojilerindeki gelişmeler, internetin dünya genelinde yaygınlaşması ve yüksek hızlarda veri iletimine ulaşılabilmesi dijital dosyaların çeşitliliğini de arttırmıştır. Steganografi kullanım ortamı açısından genel olarak üçe ayrılmaktadır:

- Metin (text) steganografi
- Görüntü (image) steganografi
- Ses (audio) steganografi.

Sayısal resimler paylaşımı en kolay ve internette hemen her sayfada karşılaşılabilecek dosyalardır. Steganografi uygulamalarında en yaygın kullanılan ortamlar resim dosyalarıdır. Bu nedenle, steganografi konusunda yapılan çalışmalar ve geliştirilen teknikler ağırlıklı olarak resim steganografi çerçevesinde yer almaktadır. Görüntü dosyalarının içerisine bir metin gizlenebileceği gibi bir resim dosyasının içine bir başka resmi de gizlemek mümkündür (Mesut vd. 2008).

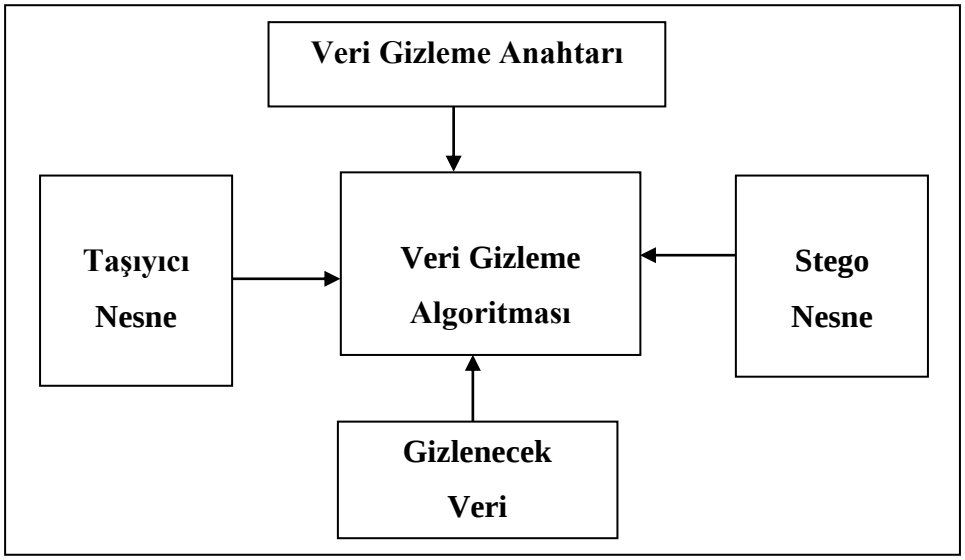
2.2.1 Steganografi sistemi

Steganografi sistemi üç temel bileşenden oluşmaktadır. İçine bilgi gizlenen nesneye taşıyıcı veri (*cover data*), saklanacak bilgiye "*gizli mesaj*" ve içerisinde gizli veri bulunduran taşıyıcıya da "*stego*" nesnesi denilmektedir. Genel bir steganografi sisteminin nasıl çalıştığı şekil 2.5'te gösterilmiştir.



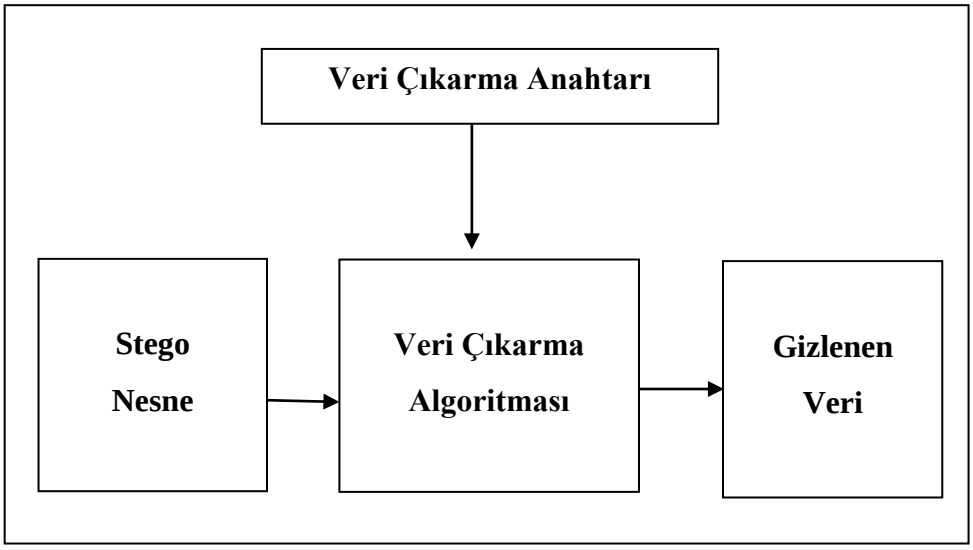
Şekil 2.5 Steganografi sistemi (Şahin vd. 2005)

Steganografi sisteminde gönderici tarafta gizli bilginin taşıyıcı veri içerisine gizlenmesi gerekmektedir. Şekil 2.6'da gösterildiği üzere, bu işlemi yapmak için veri ekleme algoritmaları kullanılmaktadır.



Şekil 2.6 Veri ekleme algoritması

Gönderici tarafında eklenen gizli verinin alıcı tarafında alınması ve anlamlandırılması için de veri çıkarma algoritmaları kullanılmaktadır (Şekil 2.7).



Şekil 2.7 Veri çıkarma algoritması

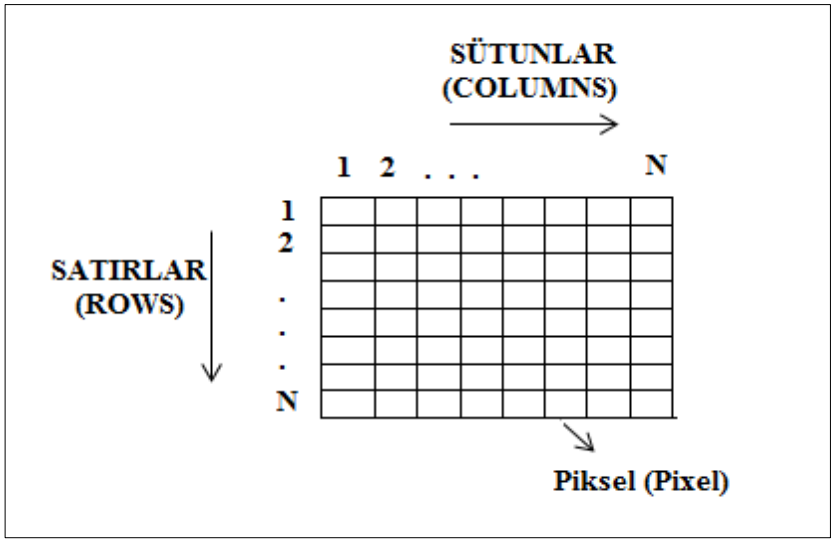
2.2.2 Görüntü steganografisi

Görüntü steganografi tekniğinde, bilgilerin görüntü dosyaları içerisinde saklanması için kullanılan yöntemler şunlardır (Johnson ve Jojodia 1998):

- LSB (Least Significant Bit) : En önemsiz bite ekleme
- Maskeleme ve filtreleme
- Algoritmalar ve dönüşümler

Görüntü steganografisi detaylarına girmeden önce genel olarak bir resim dosyasının özelliklerini belirtmek faydalı olacaktır.

Sayısal resmin yapısı: Resim dosyalarını oluşturan en küçük elemanlar piksel olarak adlandırılmaktadır. Piksel değerlerinin birleşmesiyle anlamlı bir görüntü oluşmaktadır. En basit durumda pikseller 0 veya 1 değerini alırlar. Bu piksellerden oluşan resimlere ikili (*binary*) resim denir (Şahin 2007). Sayısal (*dijital*) resim N satır ve M sütunlu bir dizi ile temsil edilmektedir (Şekil 2.8). Genellikle satır ve sütun indisleri (x;y) veya (c;r) ile gösterilir (Akar 2008).



Şekil 2.8 Sayısal resmin yapısı

Sayısal görüntü dosyaları renkli olarak genellikle 8 ya da 24 bit; gri-seviye (*grey level*) görüntüler ise 1-2-4-6 ya da 8 bit olabilmektedir (Yerlikaya 2006). Gri-seviye resimlerde her piksel, 0 (siyah) ile 255 (beyaz) arasında tam sayı değeri alabilen 1 byte ile temsil edilmektedir (Şahin 2007).

8 bitlik resimlerde de her bir piksel için 1 byte kullanılmaktadır. 8 bitlik görüntüler renk sınırlaması yüzünden çok iyi bir sonuç vermemektedir. Bu nedenle, saklanacak bilgi, saklama ortamını çok fazla değiştirmeyecek şekilde seçilmelidir. 8 bitlik görüntülerde 4 basit renk kullanılmaktadır. Bunlar; Beyaz (White-W), Kırmızı (Red-R), Mavi (Blue-B) ve Yeşildir (Green-G). Bu renklerin renk paletinde karşılık gelen girişleri ise sırasıyla 0 (00), 1 (01), 2 (10), 3 (11) şeklindedir (Johnson ve Jajodia 1998).

24 bit resimler bir piksel başına 3 byte kullanmaktadır. Her pikselin rengi; "kırmızı (*red*), yeşil (*green*), mavi (*blue*)" olmak üzere üç ana renkten elde edilmektedir. Buna pikselin RGB değeri denmektedir. Her byte değerinin son bitini değiştirmek suretiyle bir pikselde 3 bitlik veri saklanabilir. Yani 24 bit derinliğine sahip 1024x768 piksel boyutundaki bir resim, bilgi saklamak için kullanılabilir 2.359.296 bite (294.912 byte) sahiptir. Gizlenmek istenen mesaj, saklama işleminden önce sıkıştırılırsa çok daha fazla sayıda bilgi taşıyıcı resmin içine gizlenebilir (Johnson ve Jojodia 1998).

Renk değerleri ve resmin büyüklüğü resim dosyasının barındırdığı veri miktarını belirlemektedir (Erkin ve Örencik 2005). 24 bitlik piksellerden oluşan resimler en fazla veri saklayabilen resimlerdir. 24 bitlik görüntü kullanarak büyük miktarda veri saklamak mümkündür (Krenn 2004). Örneğin; 24 bitlik 1024x768 piksel büyüklüğünde bir resim dosyası 2 milyondan fazla piksel değerine sahiptir ve bu dosya 2 MB'ı aşan bir boyuta sahiptir (Johnson ve Jojodia 1998). Bu resim dosyasında her bir byte değerinin en az önemli bitleri veri saklama için kullanılsa toplam saklanabilecek veri boyutu: 1024x768x3/8 = 294912 byte olmaktadır (Atıcı 2007). Bu büyüklükteki veri içerisinde gizli mesaj saklamak için çeşitli yöntemler geliştirilmiştir. Bu yöntemlerden en basiti, renk değerlerinin en düşük anlamlı bitlerinin değiştirilmesi ilkesi ile çalışır (Erkin ve Örencik 2005).

En Önemsiz Bite Ekleme (LSB) ve BMP içerisine veri saklama: LSB, steganografide veri gizlemek için yaygın olarak kullanılan tekniktir. Bu yaklaşımın bazı dezavantajları olmasına rağmen, uygulama kolaylığı popüler bir yöntem olmasını sağlamıştır (Krenn 2004). 1 byte'lık (8 bit) verinin son biti en önemsiz bit olarak adlandırılmaktadır. Bu yöntemde; resmi oluşturan her pikselin her byte'nın en önemsiz biti yerine gizlenmesini istediğimiz verinin bitleri sırasıyla verinin başlangıcından itibaren birer birer yerleştirilmektedir (Şahin 2007). Bu işlemle, her sekiz bitin en fazla bir biti ve en önemsiz biti değişikliğe uğradığından gizlenen veri insan gözü tarafından algılanamayacaktır (Yerlikaya 2006). Sonuç olarak, resim orijinal halinden görsel olarak ayırt edilemez. Steganaliz yapıldığında, taşıyıcı verinin her byte değerinin son bitlerinin birleştirilmesiyle gizli mesajı oluşturmak kolaydır (Yerlikaya 2006).

Gizlenecek veri ardışık olarak saklanabileceği gibi bir anahtar yardımıyla rastgele olarak seçilen piksellere de saklanabilir (Atıcı 2007). Fakat yöntemin dikkatsizce uygulanması durumunda veri kayıpları ortaya çıkmaktadır. LSB yaklaşımını kullanmanın dezavantajı, büyük bir veri gizlemek için epeyce büyük bir resim seçilmesi gerekliliğidir. Bir diğer dezavantajı da kayıplı sıkıştırma algoritması kullanarak bir bilgiyi resim içerisine gizlerken sıkıştırma esnasında ortaya çıkmaktadır (Krenn 2004).

Gri seviyeli resimlere LSB yöntemi uygulanması: Örneğin, renk değeri 182 olan bir pikselin içine ikilik sayı sistemindeki 1 değeri saklandığında oluşan piksel ve renk değeri çizelge 2.1'de gösterilmektedir. Sadece LSB bitinde değişim olduğundan, son bitin 1 ya da 0 olması gözle görülebilir bir fark meydana getirmeyecektir (Şahin 2007).

Çizelge 2.1 Gri seviyeli resimlere LSB yöntemi uygulanması

Piksel Türü	Renk değeri	İkilik Sistemdeki Karşılığı
Orijinal Piksel	182	10110110
Bilgi saklanmış piksel	183	10110111

8-bit renkli resimlere LSB yöntemi uygulanması: 8 bitlik görüntülerin renk sınırlamasından dolayı LSB uygulamalarında örtü resmi oldukça dikkatli seçilmelidir ki taşıyıcı resim içerisinde mesaj bilgisi olduğu anlaşılmasın. Örnek olarak; verilen orijinal görüntü pikselleri "beyaz, beyaz, mavi, mavi" (00 00 10 10) ise 10 sayısının ikilik (*binary*) tabandaki karşılığı olan 1010 değeri bu piksellere gizlendiğinde, yapılan değişiklikler sonucunda görüntünün yeni piksel değerleri çizelge 2.2'deki gibi elde edilmektedir (Johnson ve Jojodia 1998).

Çizelge 2.2 8-bit renkli resimlere LSB yöntemi uygulanması

Piksel Türü	**Görüntü Pikselleri**
Orijinal Piksel	00 00 10 10 (beyaz, beyaz, mavi, mavi)
Saklanacak veri	10 10 (10 sayısı)
Bilgi saklanmış piksel	0**1** 00 1**1** 10 (kırmızı, beyaz, yeşil, mavi)

Bu değerler de renk paletinde sırasıyla kırmızı, beyaz, yeşil ve mavi değerlerine karşılık gelmektedir. Piksellerin renk değerleri oldukça değiştiğinden, gözle fark edilebilecektir ve bu durum 8 bitlik görüntü kullanmanın zayıflığını göstermektedir (Johnson ve Jajodia 1998).

24-bit renkli resimlere LSB yönteminin uygulanması: Örnek olarak; çizelge 2.3'teki 24 bitlik bir renkli görüntünün 3 pikseli dikkate alınabilir. Bu 3 piksel, hafızanın 9 byte değerini kullanır (Krenn 2004).

Çizelge 2.3 Orijinal 3 piksel değeri

(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)

Orijinal görüntü bitleri yukarıdaki gibi verilen 3 pikselin içine A harfini yerleştirelim. A harfinin ASCII karşılığı 065 olup ikili karşılığı (10000001) eklendiği zaman sonuç çizelge 2.4'teki gibi olmaktadır.

Çizelge 2.4 A karakteri eklendikten sonraki piksel değerleri

(00100111 11101000 11001000)
(00100110 11001000 11101000)
(11001000 00100111 11101001)

A karakterini başarılı şekilde saklamak için çizelge 2.4'te görüldüğü gibi altı çizili 3 bitin değişmesi yeterli olmaktadır. Sonuçta yapılan değişikliklerin, LSB bitleri üzerinde yapıldığından insan gözü tarafından algılanması oldukça düşüktür. Böylece, gizli mesaj etkin bir şekilde gizlenmektedir (Krenn 2004).

Maskeleme ve filtreleme: Maskeleme ve filtreleme yönteminde resmin, resim işleme teknikleri kullanılarak veri saklamaya en uygun alanları belirlenir ve saklama işlemi bu bölgelerde gerçekleştirilir (Atıcı 2007). Genellikle 24 bitlik veya gri seviyeli resimler için kullanılmaktadır. Bu yöntemler resmin en önemsiz alanlarının tespit edilerek buralarda saklama yapılmasını temel almaktadır. Genelde filigran uygulamalarına benzemektedir. Bu teknik, bir görüntü içerisinde görüntü parçalarının parlaklık değerlerini değiştirerek uygulanmaktadır (Johnson ve Jojodia 1998).

Maskeleme ile bir görüntünün görünen özellikleri değişmedikçe insan gözü bir anormallik algılamayacaktır. Maskeleme tekniğinde, bir görüntünün görünen çehresi maskelemede kullanıldığı için, görüntü işlemenin farklı çeşitleri, sıkıştırma ve kırpma ile ilgili olarak LSB modifikasyonlarına göre daha sağlamdır (Krenn 2004). Maskeleme teknikleri JPEG (Joint Photographic Experts Group) formatındaki resim dosyaları için daha uygundur (Şahin 2007).

Algoritmalar ve dönüşümler: Dönüştürme teknikleri, gizlenecek bilgiyi JPEG dosyalarını sıkıştırmak için kullanılan DCT (Discrete Cosine Transform) gibi dönüştürme alanı içerisinde katsayı değerlerinin değiştirilmesiyle saklar. Bu yöntem kaplayıcı görüntünün önemli bir alanı içerisinde mesajı sakladığından, steganaliz ataklarına karşı daha sağlamdır. Dönüştürme görüntü dışında meydana gelebilecek varyasyonları engellemek için tüm görüntüye uygulanabilmektedir (Amin vd. 2003). Dönüşüm teknikleri daha çok JPEG dosyalar üzerinde kullanılmaktadır. En yaygın olarak kullanılan dönüşümler ise DCT ve DFT'dir (Şahin 2007).

Resim dosyalarının sıkıştırılması: Resim dosyalarında kayıplı *(lossy)* ve kayıpsız *(lossless)* olmak üzere iki sıkıştırma yöntemi vardır. Her iki yöntemde dosya büyüklüğü azalmaktadır. Kayıpsız sıkıştırma, orijinal mesajın tam olarak tekrar yapılandırılmasını sağlamaktadır. Bu nedenle, orijinal bilginin bozulmamış olarak elde edilmesi gereken durumlarda tercih edilmektedir. GIF (Graphic Interchange Format) ve 8 bit BMP (Bitmap) formatları bu yapıdadır (Johnson ve Jojodia 1998). Kayıpsız sıkıştırmadan dolayı BMP formatlı resimlerde gizlenen bilgide veri kaybı olmamaktadır.

Kayıplı sıkıştırmada, dosya büyüklüğü büyük ölçüde azaltılmakta ancak resmin bütünlüğü korunamamaktadır. Bu tip sıkıştırma, JPEG formatlı resimler için kullanılmaktadır (Johnson ve Jojodia 1998). Sıkıştırma sonrasında gizlenen bilgide kayıplar meydana gelebilmektedir. Birçok steganografi yazılımı JPEG formatını desteklemez veya kullanımını tavsiye etmezken, 24 bit BMP resimlerin kullanılmasını tercih etmektedir. Diğer alternatifler ise gri tonlamalı ve 256 renk resimlerdir (Şahin 2007).

Resim dosyalarına benzer şekilde ses içerisine veri saklama yöntemleri de İİS'nin (İnsan İşitme Sistemi) zayıflıklarını kullanmaktadır. 2000'li yılların başından itibaren ses içerisine veri saklama çok popüler hale gelmiştir (Atıcı 2007). Bununla birlikte, İİS'in frekans aralığı yüzünden, ses sinyalleri içerisine bilgi gizleme oldukça uğraş gerektiren bir konudur. İİS; 1/1.000'den daha büyük frekans aralığını fark edebilmektedir (Şahin 2007). Ses içerisine veri saklama yöntemleri düşük bit kodlaması

(*low bit encoding*), faz kodlaması (*phase coding*), yayılmış spektrum (*spread spectrum*) ve yankı veri gizlemesi (*echo data hiding*) olarak sınıflandırılmaktadır (Bender vd. 1996).

Düşük bit kodlaması, resim steganografi tekniğinde kullanılan LSB yöntemine benzer şekilde ses örneğinin son bitlerinin saklanacak veriye göre değiştirilmesidir. Sesin analog ortamlara girmeksizin, tamamen sayısal ortamlarda transferi durumunda kullanılabilir. Faz kodlamasında ses dosyası bölümlere (*segment*) ayrılmakta ve bölümlere ait faz değeri, veriyi saklayacak şekilde yeniden oluşturulmaktadır. Bu yöntem, resim içine veri saklama yöntemlerinden dönüştürme tekniğine benzemektedir. Yayılmış spektrum yönteminde sese ait frekans spektrumu üzerinde veri gizlenmektedir. Bu yöntemde seste gürültüler oluşabilmektedir. Yankı veri saklaması yönteminde ise ses sinyali üzerine yankı eklenmekte ve yankının farklı gecikme değerleri kodlanarak veri saklanabilmektedir (Atıcı 2007).

Metin içerisine de veri saklanabilmektedir. Bu ortamda üç ayrı yöntem kullanılmaktadır. Birinci yöntemde, her sonlandırıcı karakterin sonuna bir veya iki boşluk bırakarak kodlama gerçekleştirilmektedir. İkinci yöntemde, satır sonlarına boşluk bırakılarak kodlama yapılmakta ve veri saklanmaktadır. Üçüncü yöntemde ise metnin sağa yaslanması durumunda oluşan boşlukların kodlanmasıyla veri saklama işlemi gerçekleştirilmektedir (Bender vd. 1996).

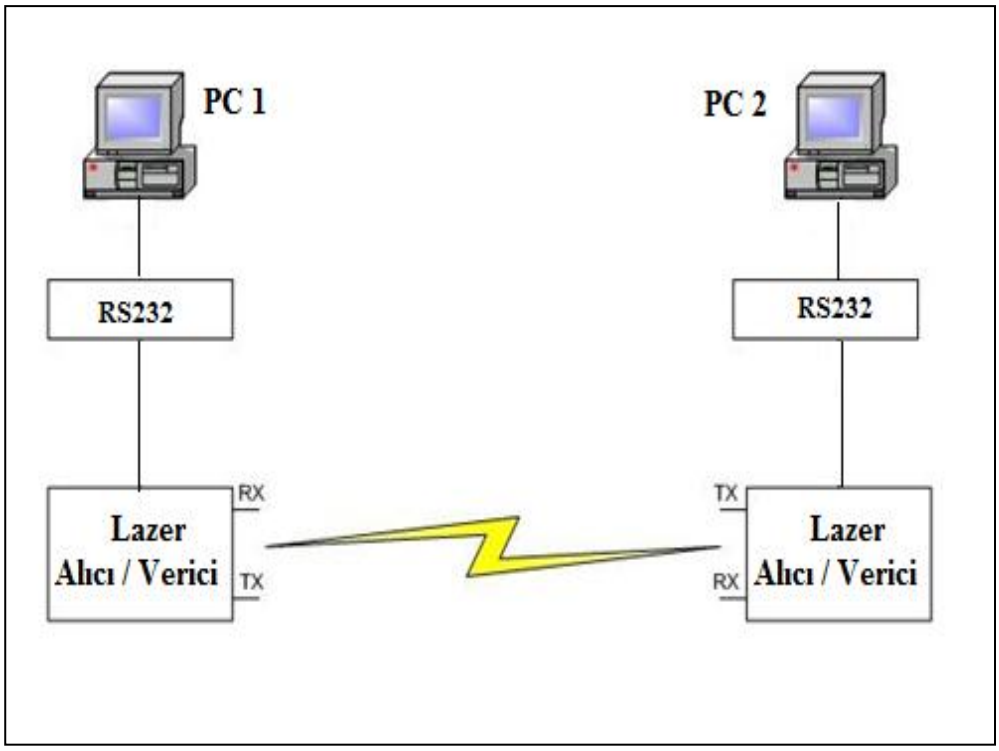
Steganografi uygulamalarında kullanılacak dosya türünde bir sınırlama olmamakta, dosyanın yapısal özellikleri uygun olduğu müddetçe her türlü sayısal dosya, veri saklamada taşıyıcı dosya olarak kullanılabilmektedir. Örneğin; MS Word dosyalarında metin rengiyle sayfa renginin aynı yapılmasıyla bir mesaj basitçe gizlenebilir ve bu durum steganografik amaçlı kullanılabilir. Steganografi uygulamalarında kullanılan taşıyıcı dosya türlerindeki çeşitlilik her geçen gün artmaktadır. Çok farklı sayısal dosya türleri içerisine veri saklama çalışmalarının gelecekte daha da artacağı değerlendirilmektedir (Atıcı 2007).

3. MATERYAL VE YÖNTEM

3.1 Sistem Blok Diyagramı

Tez çalışmasında kullanılan sistem blok diyagramı şekil 3.1'de gösterilmiştir. Bu diyagram; donanım ve yazılım kısımlarından oluşmaktadır. İki bilgisayar arasında optiksel telsiz iletişimin RS-232 standardıyla sağlanması ve steganografi yazılımının bu donanım üzerinde çalışması amaçlanmıştır.

Donanım kısmı; seri port üzerinden optiksel telsiz iletişimini sağlayacak şekilde tasarlanmıştır. Yazılım kısmı da steganografi sisteminde elde edilen verilerin seri port üzerinden gönderimini sağlamaktadır. Sistem çift yönlü (*full duplex*) veri iletişimini sağlayacak şekilde hem alıcı hem de verici kısımları olacak yapıda tasarlanmıştır. Tez çalışması kapsamında hazırlanan sistemin deney düzeneği görünümü EK 1'de sunulmuştur.

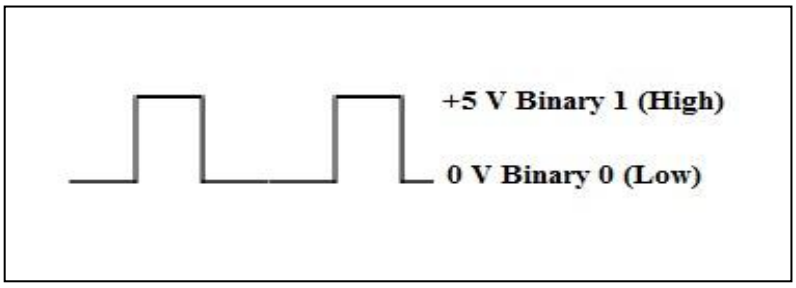


Şekil 3.1 Bilgisayarlar arası seri port üzerinden OTİS iletişimi

3.2 Sistem Veri İletim Tekniği

Veri iletimi, bir noktadan başka bir noktaya sayısal (*digital*) veya ikili (*binary*) bilgilerin iletilmesine, transfer edilmesine denir. Veri iletim sistemleri; bilgisayarlar, bilgisayar ile terminaller veya alıcılar (yazıcı, tarayıcı vs.) arasında veri iletimlerini gerçekleştirmektedir. Sayısal veya ikili hale dönüştürülebilen ses, görüntü gibi analog bilgilerin iletilmesi de veri iletimiyle gerçekleştirilmektedir. Sayısal tekniklerin, yüksek verimliliği yanında maliyetlerinin de düşük olması veri iletiminde kullanılmasının en önemli sebeplerinden olmuştur (Anonim 2008).

Sayısal sinyaller, her biri bir voltaj seviyesiyle tanımlanan ve birbirinden farklı iki durumdan oluşan ikili atım (*binary pulse*) olarak adlandırılmaktadır. Bu sinyaller, "0" veya düşük (*low*) ve "1" veya yüksek (*high*) şeklinde değişmektedir. İkili 0 seviyesi genellikle 0 V veya toprak (*ground*), ikili 1 seviyesi de genellikle +5 V olarak tanımlanmaktadır (Şekil 3.2). Kullanılan sisteme göre bunların dışında başka voltaj değerleri de kullanılabilmektedir (Anonim 2008).



Şekil 3.2 Sayısal sinyal değerleri

3.2.1 Seri port veri iletimi

Seri port veri iletiminde, gönderilmek istenen verinin bir defada sadece bir bitini transfer edilmektedir. Yani seri port haberleşmesi teker teker 1 ve 0 bilgilerinin iletilmesiyle gerçekleşmektedir (Anonim 2007). Seri portun özellikleri şunlardır (Karakaş vd. 2011):

Baud hızı (*Baud rate*) : Veri iletim hızıdır. Saniyede iletilen veri miktarını (*bit sayısı*) belirlemektedir. Standart veri hızları 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600 ve 115200 bit/s şeklindedir.

Başlangıç (*Start*) biti: Seri haberleşmede veriler senkron yada asenkron olarak iletilebilmektedir. Senkron iletimde belirli bir başlangıçtan sonra veriler sıralı olarak art arda gelmektedir. Uzun bir dosyanın iletiminde bu yol kullanılabilmektedir. Asenkron iletimde ise, bir veri gönderildikten sonra yeni bir veri belirli olmayan bir zamanda gelmektedir. Bu yeni verinin başlangıcı, başlangıç biti ile bildirilmektedir.

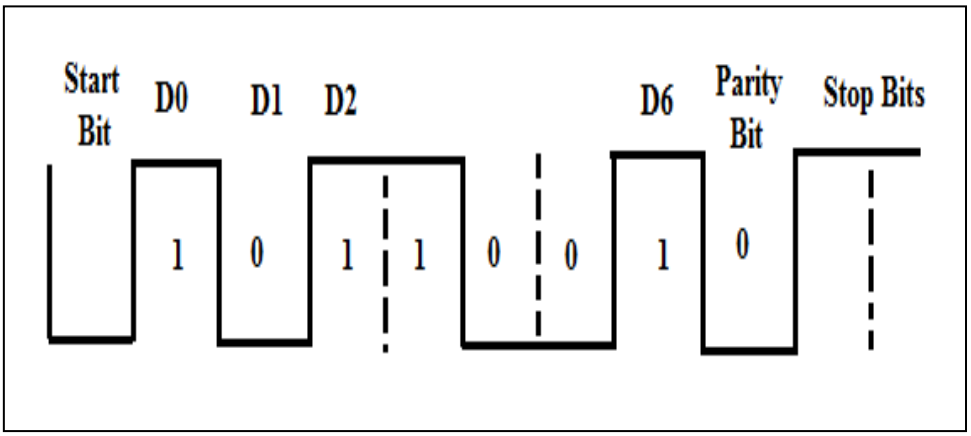
Bitiş (*Stop*) biti: Gönderilen verinin bittiğini ifade eden bittir. Bu biti alan alıcı yeni bir veri için başlangıç bitini gözlemeye başlar. Haberleşmenin tipine göre 1 veya 2 bit uzunluğuna sahip olabilmektedir.

Eşlik (*Parity*) Biti: Bir çeşit hata denetim bitidir. Başlangıç ve 8 bitlik bir veri iletildikten sonra bitiş biti gönderilmeden eşlik (*parity*) gönderilir. İletilen 8 bitlik veride 1'lerin sayısı çift ise "*even*", tek ise" *odd*" biti gönderilir. Alıcı bu biti kontrol ederek alınan verinin doğru olup olmadığını kontrol etmektedir. Bir eşlik, bir bit uzunluğunda olmaktadır (Karakaş vd. 2011).

RS232 standardıyla özdeşleşmiş olan seri portla iletimde, alıcı cihazın doğru haberleşme için karakter uzunluğu, başlangıç-bitiş bitlerini ve iletim hızını bilmesi gerekmektedir (Anonim 2008). RS232 standardında eğer bilgi 0 olarak algılandıysa bu bilgi +3V ile +25V arasında bir değer olabilir. Eğer, bilgi 1 olarak algılandıysa bu bilgi -3V ile -25V arasında gerilim değeri almıştır (Anonim 2007). Yani seri port 50 V maksimum voltaj değişim aralığına sahiptir. Bunun sonucu olarak da seri portta oluşan kayıp önemsenmemektedir. Seri iletişimde, cihaz ile bilgisayar arasındaki 3 telli kablo seri iletişim için yeterli olmaktadır (Çavuşoğlu ve Kırmızı 2007).

Veri akışının kontrolü için gerekli sinyallerden biri de saat (*clock*) sinyali veya zamanlama referansıdır. Hem gönderici hem de alıcı cihaz, bir bitin ne zaman

gönderileceğine ya da alınacağına karar verirken bir saat sinyali kullanmaktadır. Seri port ile senkron ve asenkron veri iletim formatlarının her biri saatleri farklı şekilde kullanır. Senkron gönderimde her cihaz, kendisi veya dışarıdan bir cihaz tarafından üretilen aynı saat sinyalini kullanır. Saatin frekansı sabit yâda düzensiz aralıklarda değişken de olabilir. Uzun mesafeli bağlantılarda senkron format uygun değildir. Asenkron iletişimde, bağlantıda saat hattı bulunmaz. Her uç, kendi sinyalini sunmaktadır. Bu iletişimde de, uçların saat frekansında anlaşmaları gerekir. Bu nedenle iletilen her byte değerinde saatleri eşitlemek üzere bir saat biti ve iletimin bittiğini bildirmek üzere bir bitiş biti bulunur (Şekil 3.3) (Çavuşoğlu ve Kırmızı 2007).

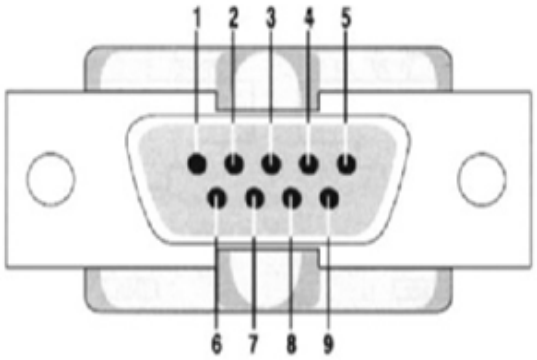


Şekil 3.3 Asenkron veri iletim formatı

Asenkron veri, senkron veri iletim formatına göre daha yaygın olarak kullanılmaktadır. Bilgisayarlardaki RS232 portları; modemler ve diğer cihazlarla iletişimde asenkron formatları kullanmaktadır. Asenkron transfer çeşitlerinden en yaygını 8-N-1'dir. Bu formatla gönderici cihaz her bir baytı 1 adet başlangıç bitini takiben 0 numaralı bitten başlayarak 8 veri biti ve 1 adet bitiş biti olarak yollamaktadır. 8-N-1 ifadesindeki N, iletimde eşlik biti kullanılmadığını anlatır. Diğer formatlarda hata kontrolünün basit bir formu olarak eşlik biti bulunur (Karakaş vd. 2011).

Seri veri iletiminde, bilgiler bitlere ayrılarak gönderildiği için paralel veri iletimine göre yavaştır. Sıradan bir seri portun veri iletim hızı yaklaşık olarak 9600 bps'dır. Seri veri iletim maliyetinin paralel veri iletimine göre az olması nedeniyle uzun mesafelerde

kullanılmaktadır (Anonim 2008). Seri portta bilgi transferi tek hat üzerinden yapıldığından dolayı çift yönlü (*full dublex*) çalışabilmektedir. Seri haberleşmede bilgi paketleri başlangıç ve bitiş bitleriyle işaretlenerek birbirinin ardı sıra gelen sinyallerle gönderilmektedir (Anonim 2007). Değişik üreticiler tarafından yapılmış veri haberleşme cihazları uyumluluğunu sağlamak amacıyla, EIA (Electronics Industries Association) tarafından 1960 yılında, RS232 olarak adlandırılan standart belirlenmiştir (Çavuşoğlu ve Kırmızı 2007). PC bilgisayarlarda seri port haberleşmesi RS232 standardında yapılmaktadır. Genelde 9 telli konektör yapısı seri portlar için kullanılmaktadır (Şekil 3.4) (Anonim 2007).



PİN NUMARASI	TANIM
1	DCD (Data Carrier Detect)
2	RxD (Receive Data)
3	TxD (Transmit Data)
4	DTR (DataTerminal Ready)
5	GND (Ground)
6	DSR (Data Set Ready)
7	RTS (Request To Send)
8	CTS (Clear To Send)
9	RI (Ring Indicator)

Şekil 3.4 RS232 seri portun 9-pin D tipli konektör yapısı ve uç ayrıntıları

Kabloların taşıdığı sinyaller şunlardır (Anonim 2007):

1. Taşıyıcı Tespit (*Carrier Detect*): Modemin çalışan bir telefon hattına takılıp takılmadığını tespit etmek için kullanılır.

2. Rx Bilgi Alma (*Receive Data*): Gönderilen bilgi sinyallerini almak için kullanılır.

3. Tx Bilgi Gönderme(*Transmit Data*): Bilgi sinyali göndermek için kullanılır.

4. Bilgi Terminali Hazır (Data Terminal Ready): Karşı tarafla anlaşmak ve hazır olunduğunu belirtmek için kullanılır.

5. GND (Ground): Topraklama için kullanılır.

6. Bilgi Gönderme Hazır (Data Set Ready): Karşı tarafın anlaşmak ve hazır olduğunu belirtmek için kullanır.

7. Gönderme İsteği (Request To Send): Karşı tarafa bilgi gönderilebilme uygunluğunu sormak için kullanılır.
8. Gönderme İsteği Tamam (Clear To Send): Karşı tarafın bilgi göndermenin uygun olduğunu belirtmek için kullanılır.
9. Zil İşaretçisi (Ring Indicator): Telefonla modem arandığında çağrı sinyali bu hat üzerinden gönderilir.

3.3 Sistem Donanım Yapısı ve Bileşenleri

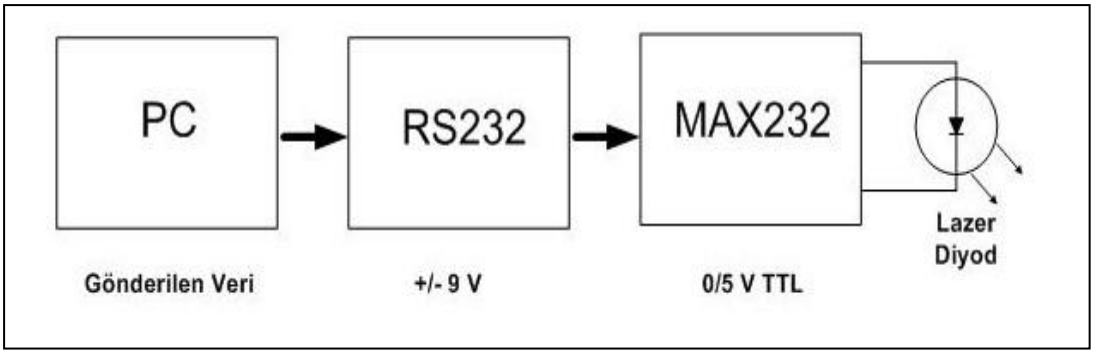
Tez çalışmasında kullanılan sistem donanım yapısının elektronik devre şeması EK 2'de sunulmuştur. Bu donanım yapısının temel bileşenleri şunlardır:

RS232: Seri asenkron olarak gönderilen verinin alınması veya iletilmesini gerçekleştiren cihazlar arasında bu tür haberleşmenin sağlanabilmesi için geliştirilen bir standarttır (Karakaş vd. 2011).

MAX 232: RS232 sinyallerinin elektriksel özelliği; 5 Volt "lojik 1" ve 0 Volt "lojik 0" değerine karşılık gelen standart TTL (Transistor-Transistor Logic) mantığına benzememektedir. RS232'de -12 Volt "lojik 1" , +12 Volt "lojik 0" değerine karşılık gelir. Bu özellik daha uzun mesafeli kablolarda, güçlendirme gerektirmeden iletişim sağlamaktadır. RS232 ile birlikte TTL devrelerin çalışabilmesini sağlayan yongalar kullanılmaktadır. Bunlardan en yaygın olanı MAXIM firmasının ürettiği MAX232 sürücüsüdür. MAX232 gerilim seviye dönüştürücüsüdür (Çavuşoğlu ve Kırmızı 2007). Bu yonga, +/- 12 V gerilimi lojik seviyeye indirgemek için kullanılmaktadır (Karakaş vd. 2011).

Gönderici Ünite (*Transmitter, Sender*): Bilgisayardan gelen veri RS232'nin 3 numaralı pininden MAX232'nin 8 numaralı bacağına gelir. Böylelikle +/- 9 V olan veri sinyali MAX232 tarafından 0/5 V TTL seviyesine çekilir. MAX232'nin 9 numaralı bacağından alınan TTL seviye PNP transistörün anahtarlama amaçlı kullanılmasını

sağlar. Transistör sayesinde on-off anahtarlama yapılarak veri alıcı kısmına iletilir (Şekil 3.5) (Karakaş vd. 2011). Transistörün özellikleri EK 3'te verilmiştir.



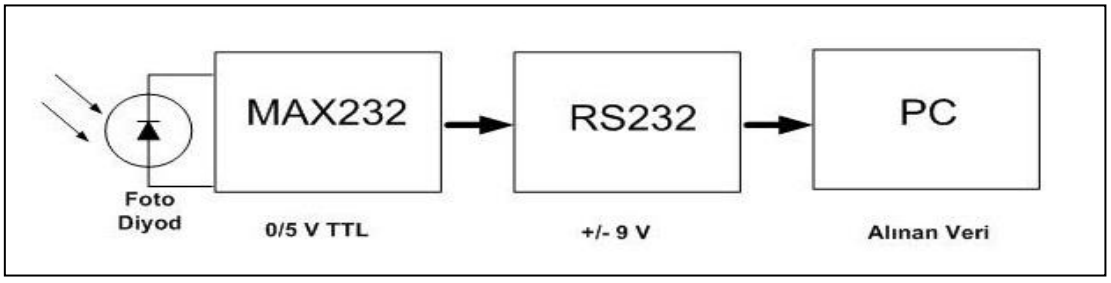
Şekil 3.5 Gönderici ünite

Gönderici Ünite içerisinde iletimi sağlayan lazer vericinin parametreleri çizelge 3.1'de verilmiştir.

Çizelge 3.1 Verici parametreleri

Çıkış Gücü	5 mW
Dalga Boyu	645 nm

Alıcı Ünite (*Receiver*): Lazer tarafından gönderilen veri foton diyot tarafından algılanır. MAX232'nin 10 numaralı bacağına gelen 0/5 V TTL seviye MAX232 sayesinde +/- 9V seviyelerine çekilir ve 7 numaralı bacağından RS232'nin 2 numaralı pinine verilerek bilgisayara aktarılır (Şekil 3.6) (Karakaş vd. 2011).



Şekil 3.6 Alıcı ünite

Alıcı kısmında BPW32 foton diyotu kullanılmıştır (Çizelge 3.2). Foton diyotun özellikleri EK 4'te sunulmuştur.

Çizelge 3.2 Alıcı parametreleri

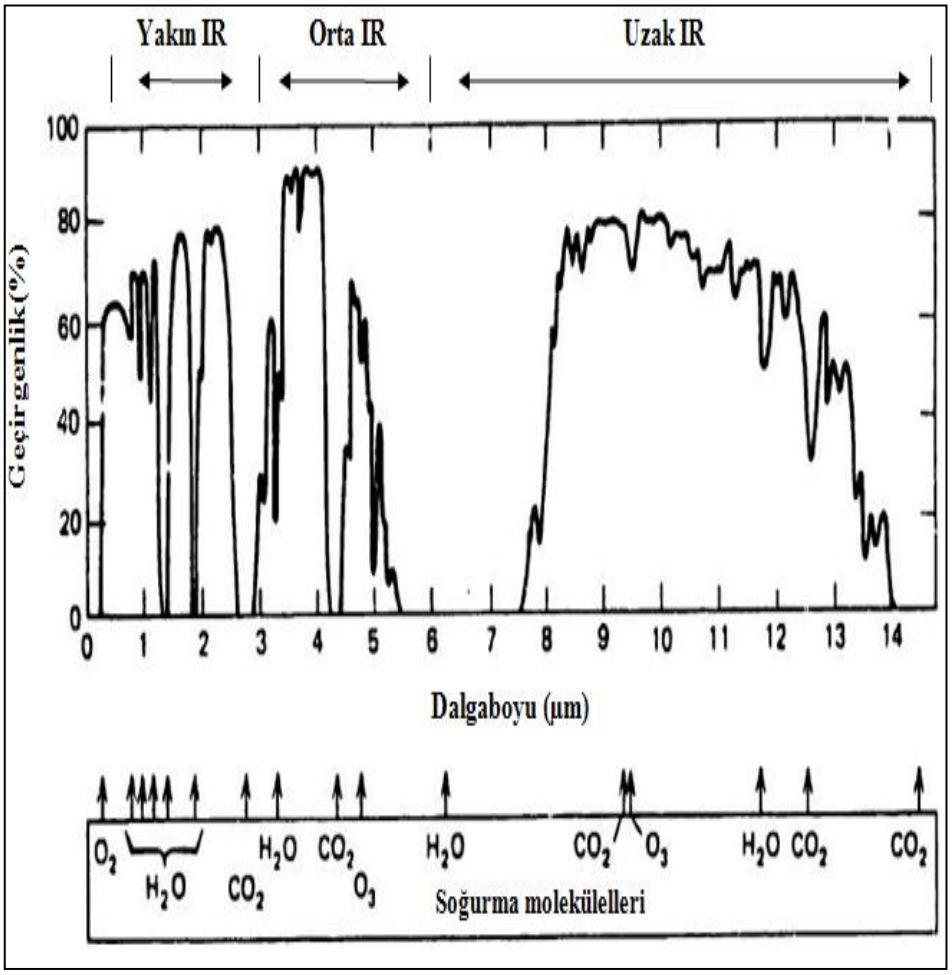
Parametre	**Değer**	**Birimi**
Dalga boyu	900	nm
İzgesel bant genişliği	430 to 1100	nm
Gürültü eşdeğer gücü	4×10^{-14}	W/√Hz
Yükselme süresi	100	ns
Düşüş süresi	100	ns

9600 baud rate hızında seri port üzerinden saniyede 9600 sembol iletilmektedir. 1 sembol 8 bitle ifade edilmektedir. Bu durumda, 1 bitin iletim süresi 13,02 µsn kadar olmaktadır. Foton diyotun yükselme zamanı (*rise time*) ve düşme zamanı (*fall time*) bu değerden küçük olduğundan sistemin iletiminde bir sorun yaşanmamaktadır. Devre maksimum veri iletim hızını desteklemektedir.

Parıldama (Scintillation) sistemin iletimini tamamen durdurmamakla beraber, ışının saçılmasına ve yolunu değiştirmesine neden olmaktadır. Genel olarak, parıldama 1 km ve daha üstü mesafelerde etkili olmaktadır (Popoola vd. 2009). Tez çalışması, bina içi ortamlarda denendiği ve alıcı-verici arasındaki mesafenin odaklamayı sağlamak amacıyla sabitlenmesinden dolayı parıldama olması durumu ihmal edilebilecek durumdadır.

Deneyler, sabit mesafe ve sabit koşullar altında laboratuvar ortamında yapıldı. Optik telsizin performansından çok steganografi tekniğinin performansı amaçlanmıştır. Deneyler bu koşullarda yapılmıştır. Daha uzun mesafelerde odaklama problemleri yaşandığından devre çalışmamaktadır.

Hava soğurması, atmosferde yayılan ışının atomlarla ve moleküllerle etkileşimden kaynaklanmaktadır. Atmosfer içindeki temel soğurma moleküllerinin IR ışımalar üzerindeki geçirgenlik miktarı dalga boyu değişimi şekil 3.7'de verilmiştir (Churnside ve Shaik 1989).



Şekil 3.7 Gaz moleküllerinin dalga boyuna değişimine bağlı geçirgenliği

Optiksel telsiz sistemleri genelde, dalga boyu λ =0.7 µm ile 1.55 µm arasında, optik band'ın özellikle *infrared* bölgesinde uygulanmaktadır. Şekil 3.7'de atmosferin hangi aralıkta ve hangi oranda geçirgen olduğu gösterilmektedir. Su molekülleri tarafından soğurmanın en az olduğu dalga boyları 0.8 µm ve 1.55 µm'dir. Dolayısıyla bu dalga boylarında iletişim tercih edilmektedir (Gökçe 2012). Verici kısmında kullanılan lazerin dalga boyu 0.65 µm olup, şekil 3.7 üzerinde bakıldığında %65'lik geçirgenliğe yakın bir geçirgenlik değeri sağlamaktadır.

3.4 Sistem Yazılım Uygulaması

3.4.1 Yazılımın özellikleri

Yazılım uygulaması Microsoft. NET Visual Studio Express Edition 2010 editöründe C# (C Sharp) programlama dili kullanılarak geliştirilmiştir. .NET Framework basit programlama seçenekleri ve geniş miktarda kullanılabilir araç (*tool*) barındırmaktadır (Maity 2010). Elde edilen stego nesneleri ve orijinal resim arasındaki PSNR (Peak Signal Noise Ratio) değerlerini hesaplamak için de MATLAB kullanılmıştır.

Steganografi tekniğinde veri gizlemek için kullanılan en popüler resim türü BMP uzantılı resimlerdir. BMP resim türü üzerinde steganografi algoritması geliştirmek basit olduğundan kullanımı kolaydır. Çünkü dosya boyutunu azaltmak için herhangi bir teknolojiye ihtiyaç duymamaktadır. Bu resimlerin yapısı, piksellerden ve her bir piksel de 3 ana renk olan kırmızı, yeşil ve maviden oluşmaktadır. Pikselin her bir rengi bir rengin yoğunluğunu (*density*) gösteren bir bitlik bilgi tutmaktadır. Bilgisayar biliminde her byte 8 bitten oluşur. Bu bitlerin ilki, MSB (Most Significant Bit) ve son biti LSB olarak bilinmektedir (Maity 2010).

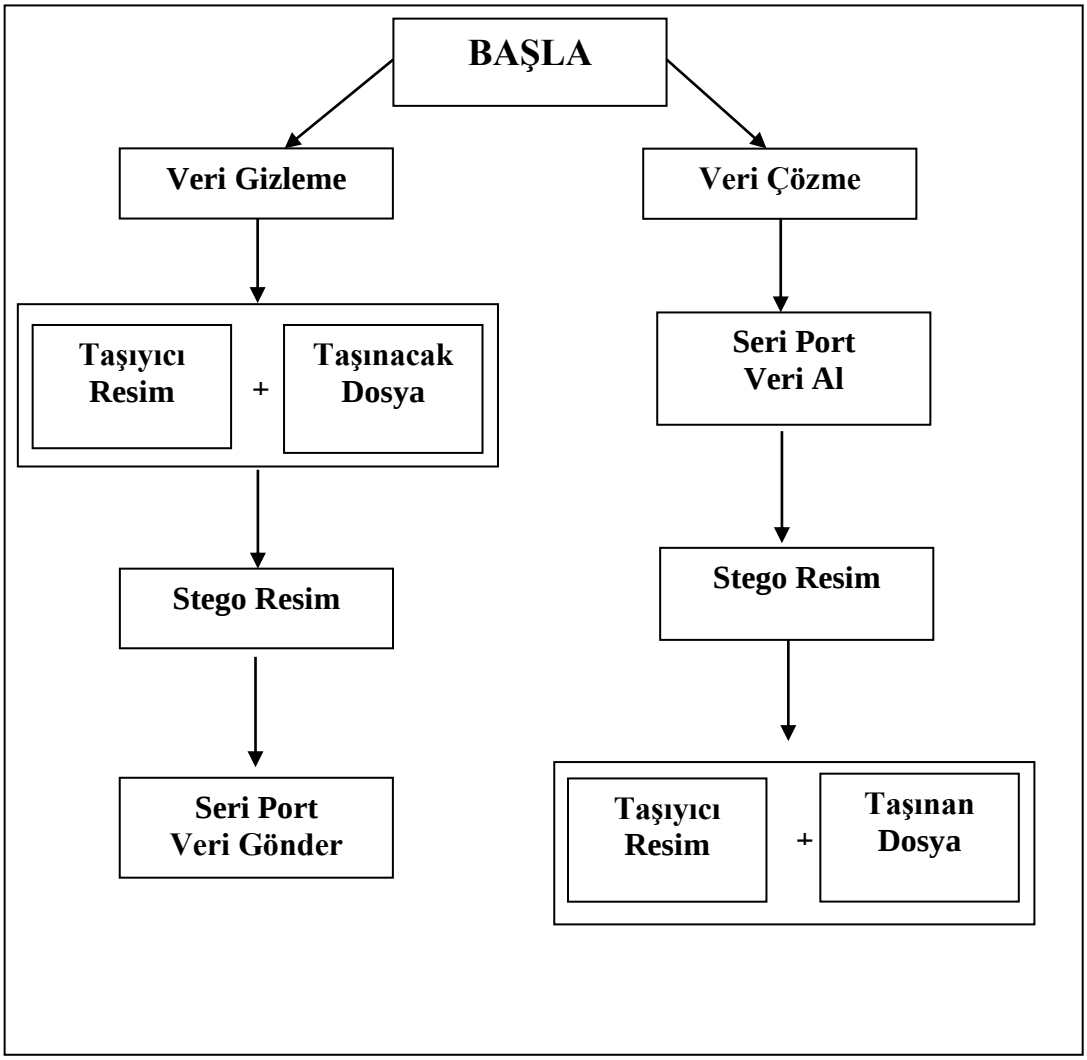
BMP tipindeki bir resim içerisine güvenli bir şekilde bilgi gizlemek için LSB metodu kullanılmaktadır. LSB katmanı en sonda (8. katman) bulunmaktadır ve resim üzerinde meydana gelebilecek değişimleri algılamak oldukça zor olmaktadır. Bilginin sadece son katmanını kullanırsak, pikselin son bitini değiştirmemiz yeterli olacaktır. Her bir piksel 3 bite sahip olduğundan bilgiyi hafızaya yazmak için 3*yükseklik*genişlik kadar bit gerektirmektedir. Veriyi yazmadan önce; veri (dosya) ismini, verinin isim boyutu ve veri boyutunu yazmalıyız. Bunu yapmak için 8 bitlik hafızanın herhangi bir ilk bitini kullanabiliriz (Maity 2010).

Taşıyıcı verinin her bir byte değerine taşınacak dosyayı saklamak için resmin 3 pikselinin her biri kullanılmaktadır. Yazılım uygulamasında da BMP uzantılı dosyalar üzerinde işlem yapılmıştır. Resim dosyalarında her bir üst katman bir alt katmana göre

daha önemlidir. Üst katmanda yapılan her bir işlem resim kalitesini azaltacaktır ve resim üzerinde değişiklik yapıldığını gösterecektir (Maity 2010).

Optiksel telsizlerle iki bilgisayar arasında iletişimi yazılımsal olarak sağlamak için .NET Framework içerisinde yer alan seri port (*serial port*) aracı kullanılmıştır. Bu tool üzerinde port, baud rate vs. gibi seçenekler ile geliştirme yapılabilmektedir.

Tez çalışmasında kullanılan yazılım; taşıyıcı dosya içerisinde taşınacak dosyayı eklemek ve çıkarmak için **veri gizleme (*encrypt*)** ve **veri çözme (*decrypt*)** işlemlerini kapsayan iki modülden meydana gelmektedir (Şekil 3.8).

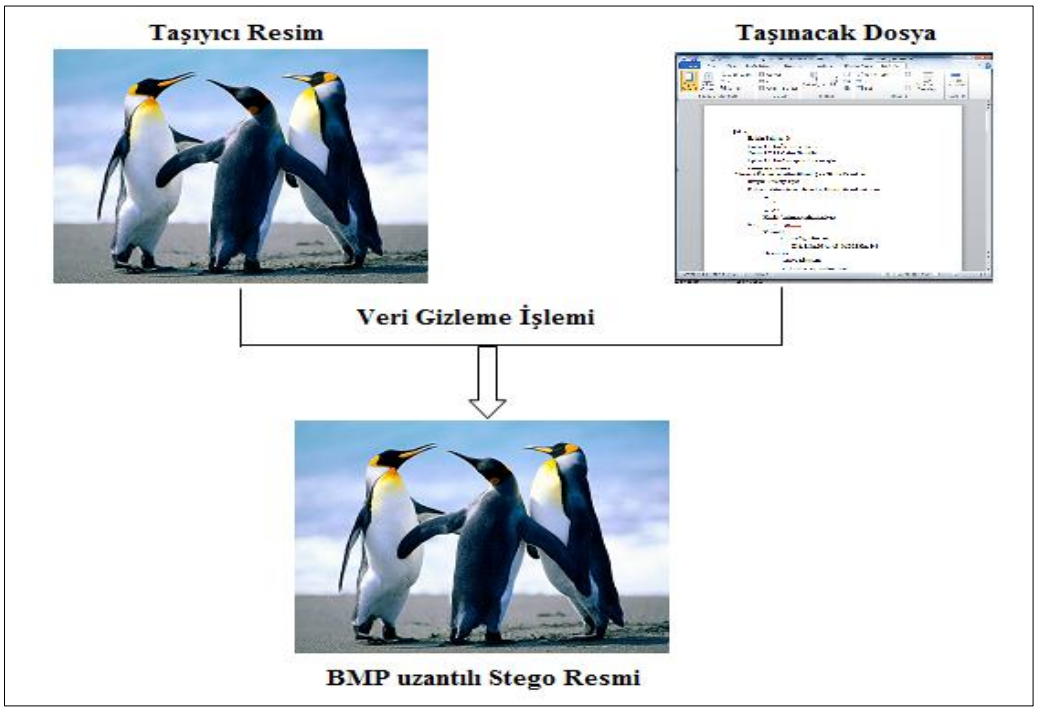


Şekil 3.8 Yazılım modüler yapısı

Veri gizleme modülü; taşınacak dosyanın veya bilginin taşıyıcı resim içerisine gizlenmesinde kullanılmaktadır. Gizlenen dosya stego resim dosyasıdır ve seri port üzerinden optiksel telsiz ortamı kullanılarak gönderimi yapılmaktadır. Veri çözme modülünde ise, seri port üzerinden alınan stego resim dosyasının çözülmesi sonucu taşıyıcı resim ve taşınan dosyanın elde edilmesi sağlanmaktadır.

3.4.2 Veri gizleme (saklama) işlemi

Veri gizleme işlemi şekil 3.9'da gösterilmektedir. Bu işlemde taşıyıcı resim üzerine gizlenen bilgi BMP uzantılı dosya olarak stego resmini oluşturmaktadır.

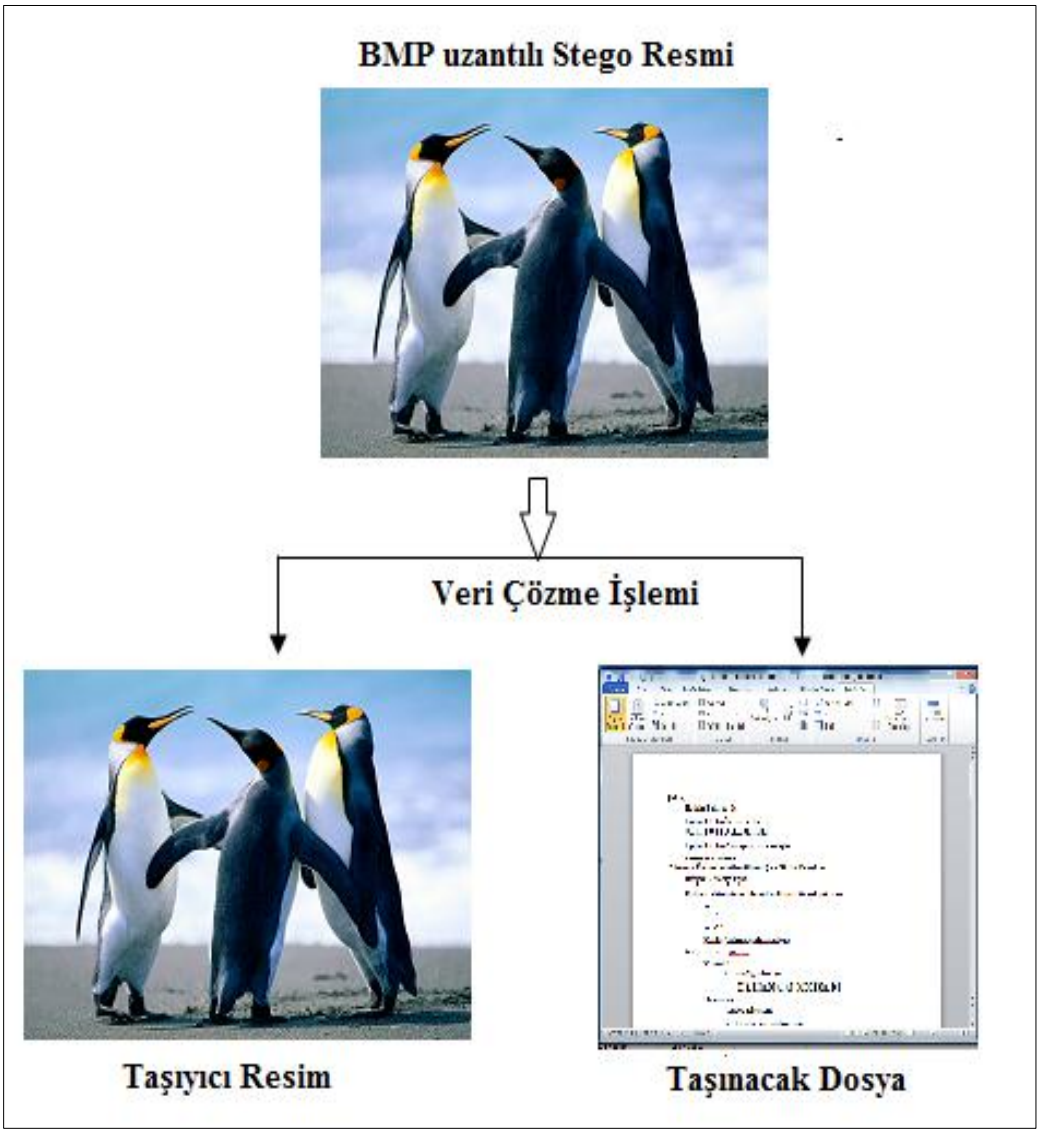


Şekil 3.9 Veri gizleme işlemi

3.4.3 Veri çözme işlemi

Veri çözme işlemi, şekil 3.10'da gösterilmektedir. Bu işlemde BMP uzantılı stego resim dosyası içerisinde LSB metodu ile gizlenen verinin çıkartılması işlemi yapılmaktadır.

Yazılım uygulamasında stego resmi elde etmek ve bu resmin seri port optiksel telsiz sistemi üzerinden iki bilgisayar arası iletimini sağlamak için yapılan veri gizleme ve çözme işleminin adımları EK 5 ve EK 6'da sunulmuştur.



Şekil 3.10 Veri çözme işlemi

4. BULGULAR

Tez çalışmasında, ilk olarak kullanılan seri port OTİS üzerinde LSB tekniğinin etkinliğini görmek, zayıflıklarını ortadan kaldırmak ve taşıyıcı resim üzerinde gönderilen gizli bir nesnenin algılanmasını güçleştirmek için alınması gereken önlemlere yer verilmiştir. Steganografi yazılımının performansı için LSB, LSB+1 ve LSB+2 durumlarında taşıyıcı resim üzerindeki maksimum bozulma miktarları değerlendirilmiştir.

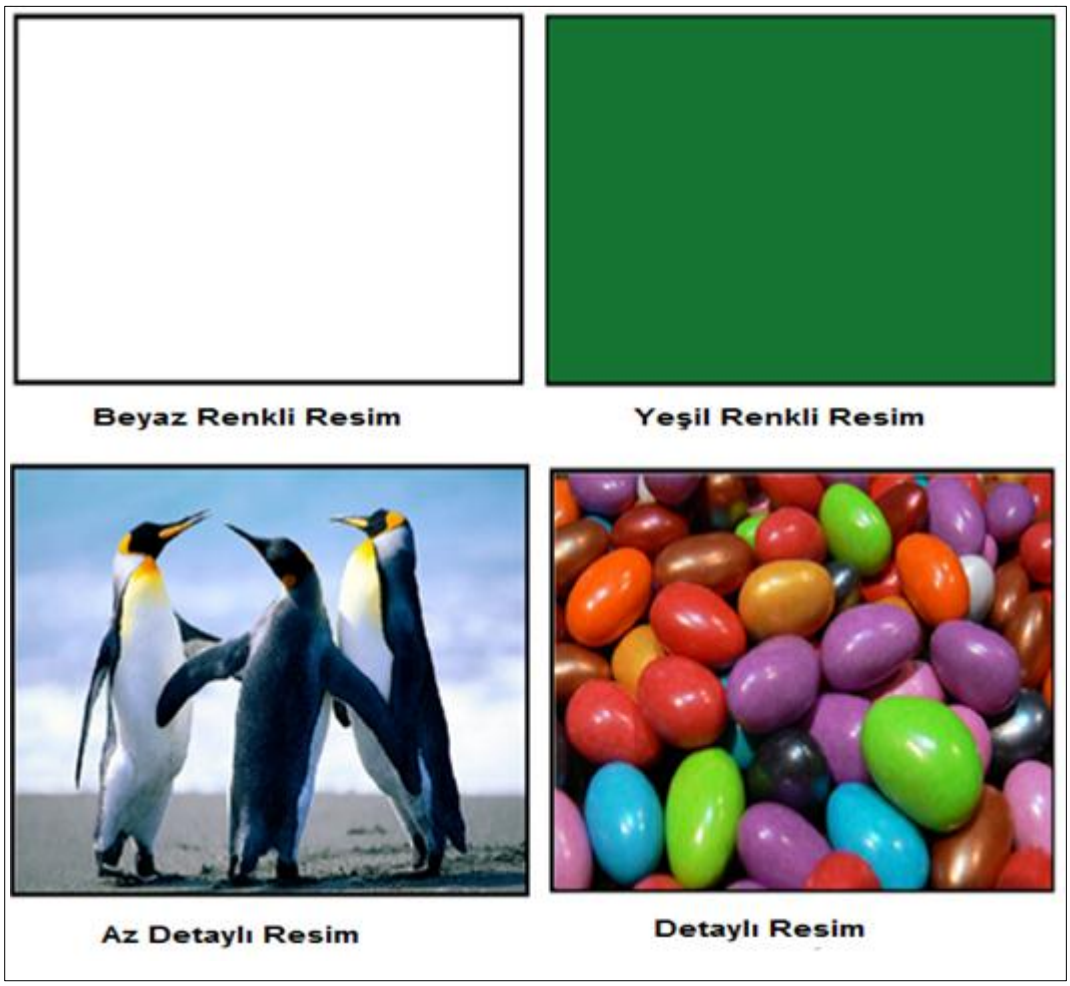
İkinci olarak da, farklı boyutlarda taşıyıcı resim dosyaları üzerinde sistemin taşıyabileceği gizli bilgi miktarının iletim süresi tespit edilmiştir. Taşıyıcı nesne olarak "bmp" uzantılı farklı boyutlarda resimler kullanılmıştır. Taşıyıcı resimler üzerine farklı boyutlarda "doc" uzantılı dosyalar eklenmiş ve stego nesnesi elde edilmiştir. Stego nesnesi seri port OTİS üzerinden farklı baud rate hızında iletilerek sistemin performansı gözlenmiştir.

4.1 Steganografi Yazılımının Performansı

LSB tekniğinde maksimum bozulmayı değerlendirmek amacıyla, tez çalışmasında taşıyıcı dosya olarak; 600 KB boyutundaki bir dosyanın sahip olduğu bit sayısına (600*1024*8 = 4.915.200 bit) eşit miktarda LSB bitine sahip resim dosyaları seçilmiştir. Sayısal resim dosyalarında her pikselde 3 LSB biti olduğundan 4.915.200 LSB bit miktarına sahip bir resim dosyasında 1.638.400 piksel bulunmaktadır. Bu değeri, 1024'e böldüğümüzde 1600 değerini elde ederiz. Bu nedenle; 1600*1024 boyutlarında bir resim dosyası, 600 KB boyutunun toplam bit sayısını karşılayacak LSB bitine sahip olacaktır. Taşıyıcı resim olarak 1600*1024 boyutlarında **beyaz, yeşil**, çok detaylı renklere sahip olmayan **az detaylı** ve çok detaylı renklere sahip **detaylı** olmak üzere 4 farklı resim seçilmiştir (Şekil 4.1).

Taşıyıcı resimlerin LSB bitlerinin 50 KB'lık kısmının (50*1024*8 bit) tersi alınarak stego resim elde edilmiştir. Bu işlem, 50 KB artırımla 600 KB boyutunu sağlayacak

maksimum LSB bitine kadar tekrarlanmıştır. Stego resimlerin elde edilmesi işlemlerinde, taşıyıcı resmin pikselleri üzerinde homojen dağılım sağlanmış ve bozulmanın sadece ilk kısımlarda olması önlenmiştir. Sırasıyla aynı boyuttaki beyaz renkli, yeşil renkli, az detaylı ve detaylı taşıyıcı resim üzerinde LSB, LSB+1, LSB+2 bitlerinin tersi alınarak stego resimleri elde edilmiş ve her bir resim üzerindeki maksimum bozulma değerlendirilmiştir.

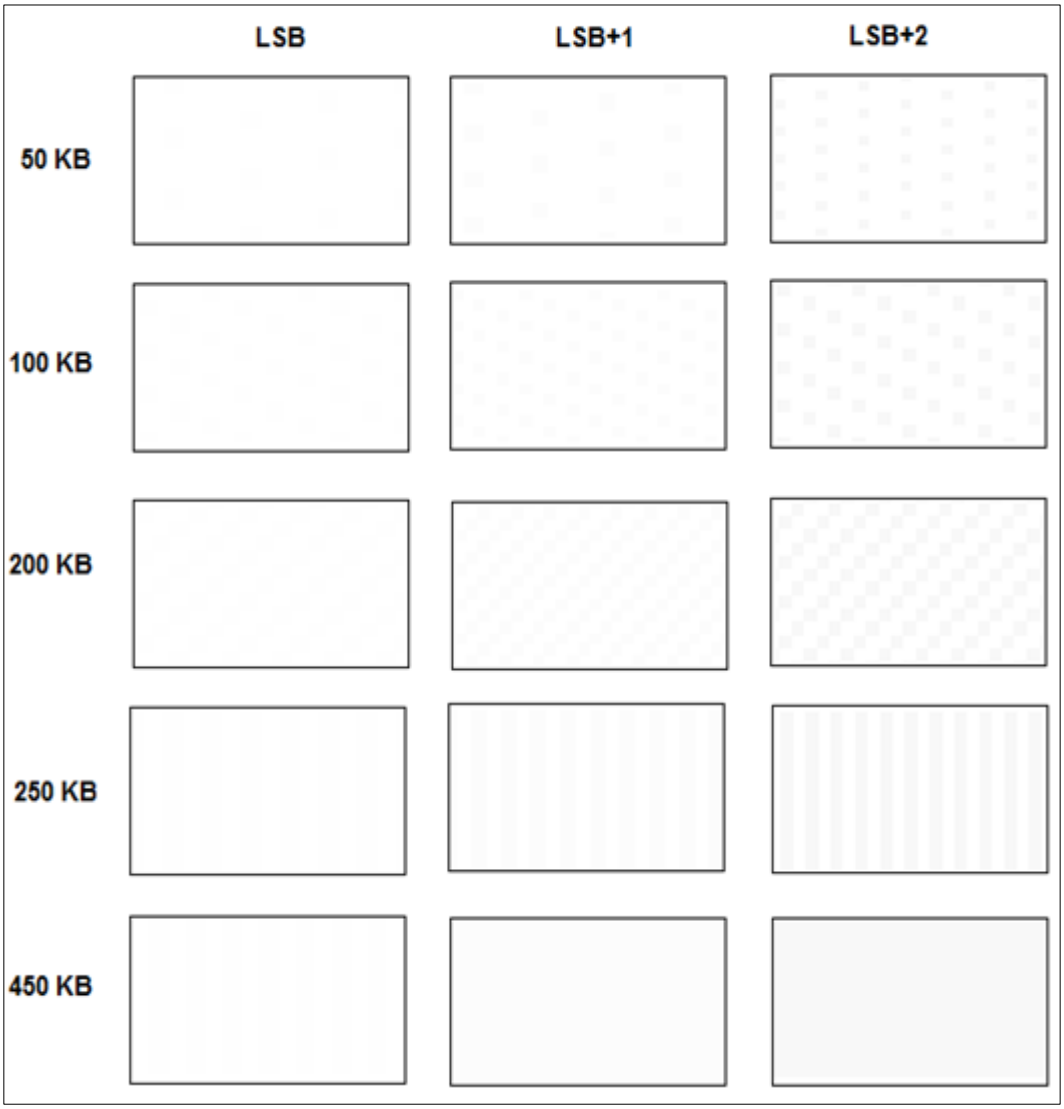


Şekil 4.1 Taşıyıcı resimler

Beyaz renkli resim için sonuçlar: Beyaz renkli resim (RGB: 255, 255, 255) için LSB, LSB+1 ve LSB+2 bitlerinin değişimi durumunda elde edilen PSNR değerleri çizelge 4.1'de verilmiştir. Şekil 4.2'de beyaz renkli resimden elde edilen stego resimlerdeki değişim miktarları gösterilmiştir.

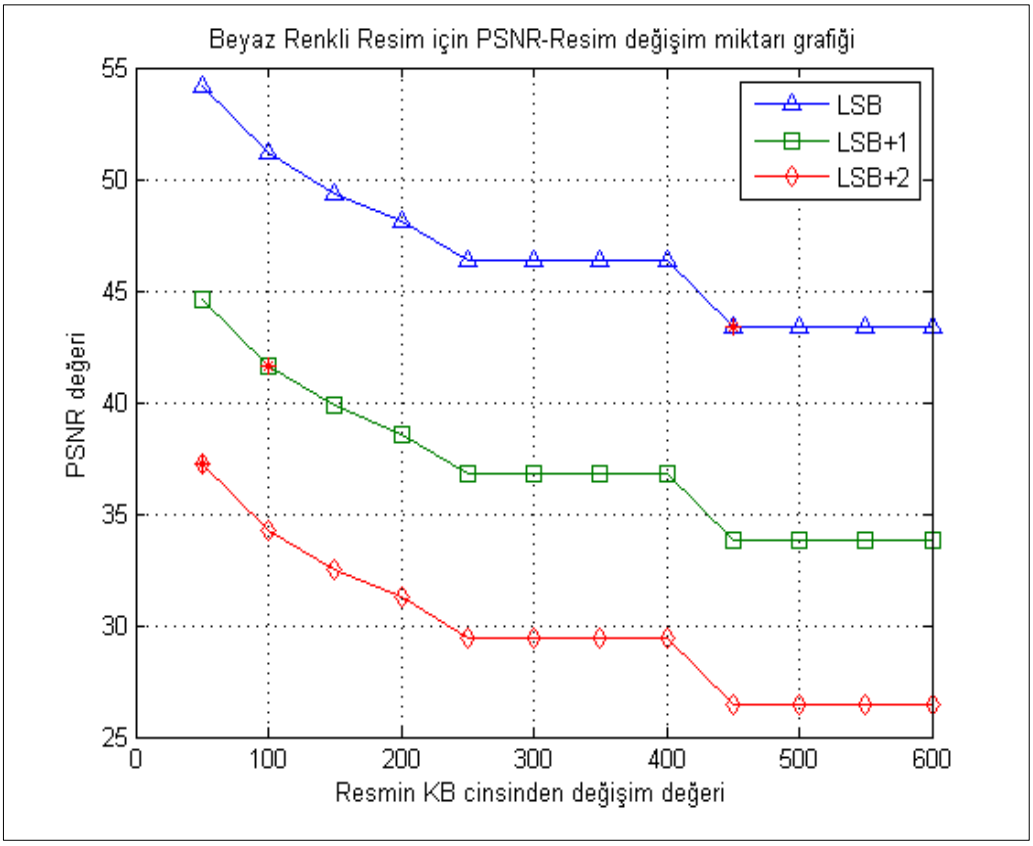
Çizelge 4.1 Beyaz renkli resim için PSNR değerleri

Değişim Miktarı(KB)	LSB	LSB+1	LSB+2
50	54.1514	44.6090	**37.2494**
100	51.1411	**41.5987**	34.2391
150	49.3802	39.8378	32.4782
200	48.1308	38.5884	31.2288
250-400	46.3699	36.8275	29.4679
450-600	**43.3596**	33.8172	26.4576



Şekil 4.2 Beyaz renkli resim için LSB bit değişim miktarları

Beyaz renkli resim için LSB bitinin değişime uğraması durumunda elde edilen stego resimlerde bir bozulma meydana gelmemektedir. LSB+1 bitlerinin değişimi durumunda stego resimde ilk bakışta bir bozulma olduğu algılanmamaktadır. Bozulma olup olmadığını daha detaylı görmek amacıyla stego resim % 800 oranında büyütüldüğünde; 100 KB'lık değişim miktarından sonra bozulma meydana geldiği rahatlıkla görülmektedir. Aynı şekilde LSB+2 bitleri için de elde edilen stego resim % 800 oranında büyütüldüğünde 50 KB'lık değişim miktarında bozulmanın insan gözü tarafından rahatlıkla algılanabileceği görülmektedir (Şekil 4.2). Beyaz renkli resimde kabul edilebilir eşik değerleri; LSB için 450-600 KB, LSB+1 için 100 KB ve LBS+2 için de 50 KB'lık değişim miktarı olarak alınabilir. Bu nedenle, beyaz renkli resimler detaylı incelendiğinde LSB tekniğinde iyi sonuçlar vermemektedir. Şekil 4.3'te beyaz renkli resim için PSNR-Değişim miktarı grafiği verilmiştir. Grafik üzerinde LSB, LSB+1 ve LSB+2 için kabul edilebilecek eşik değerleri kırmızı '*' işaretiyle gösterilmiştir.

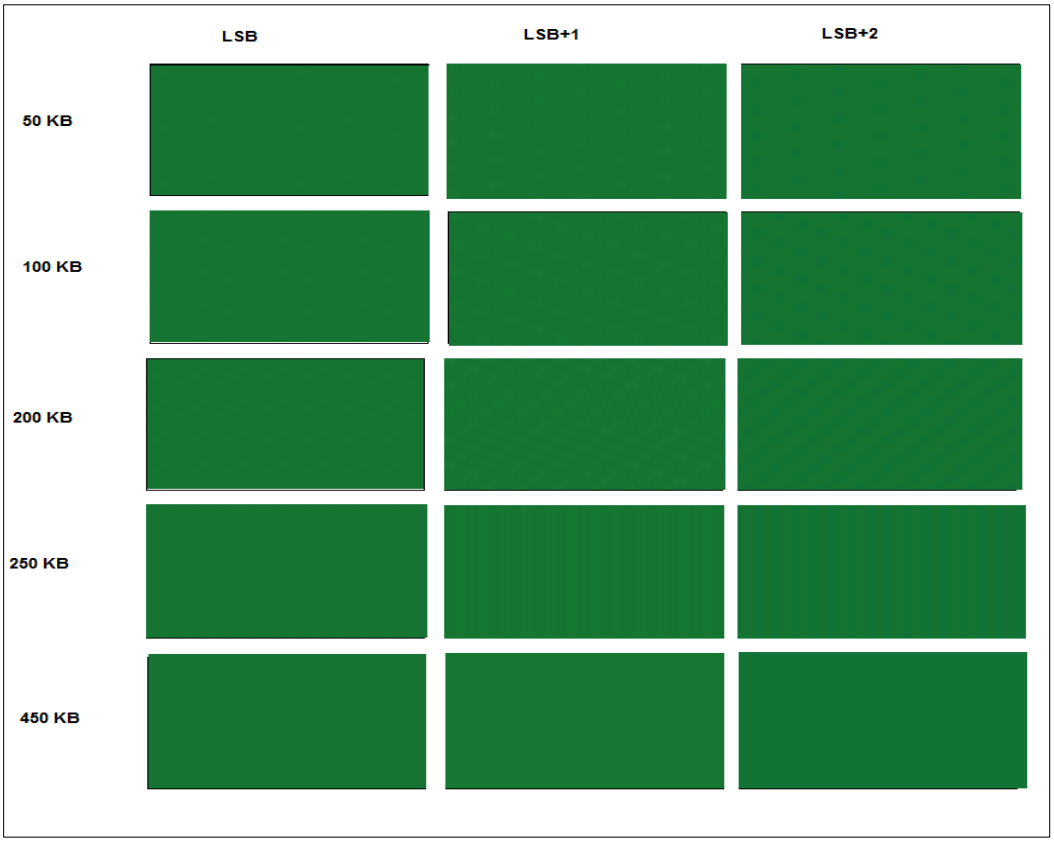


Şekil 4.3 Beyaz renkli resim için PSNR-Değişim miktarı grafiği

Yeşil renkli resim için sonuçlar: Yeşil renkli resim (RGB: 22, 116, 50) için LSB, LSB+1, LSB+2 bitlerinin değişimi durumunda elde edilen PSNR değerleri çizelge 4.2'de gösterilmiştir. Şekil 4.4'te ise yeşil renkli resimden elde edilen stego resimlerdeki değişim miktarları gösterilmiştir.

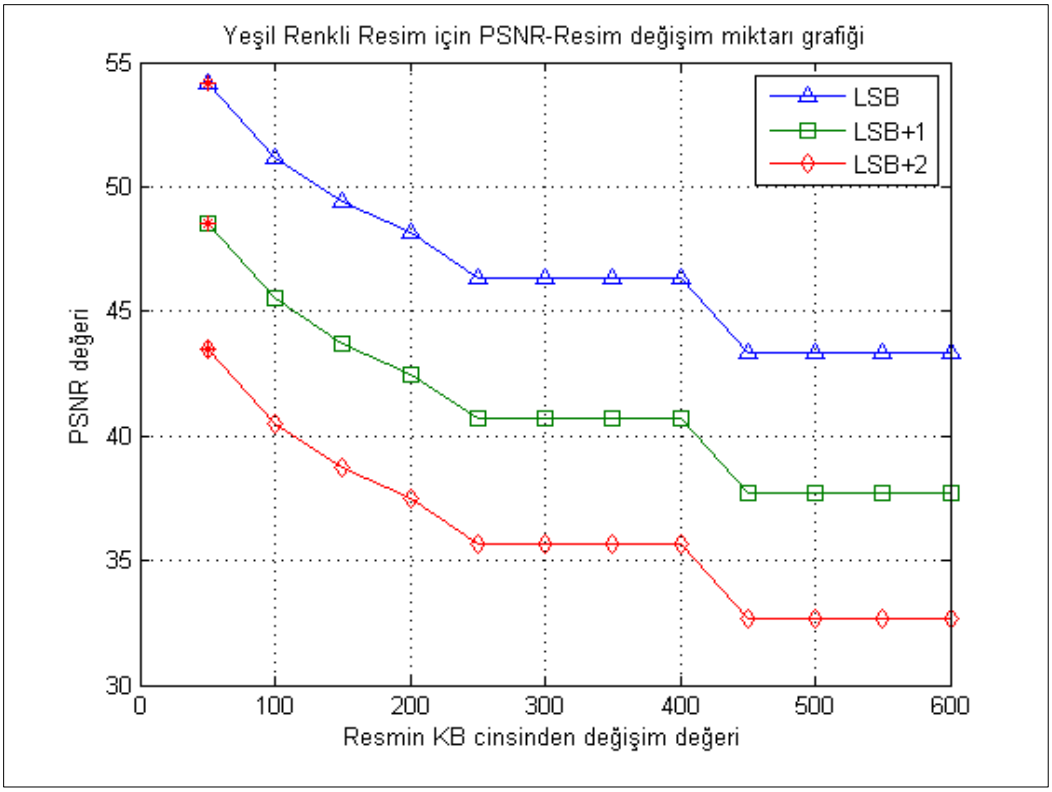
Çizelge 4.2 Yeşil renkli resim için PSNR değerleri

Değişim Miktarı (KB)	LSB	LSB+1	LSB+2
50	54.1514	**48.5087**	**43.4819**
100	**51.1411**	45.4984	40.4716
150	49.3802	43.7375	38.7107
200	48.1308	42.4881	37.4613
250-400	46.3699	40.7272	35.7004
450-600	43.3596	37.7169	32.6901



Şekil 4.4 Yeşil renkli resim için LSB bit değişimleri

Yeşil renkli resmin LSB bitinin değişimi göz önüne alındığında elde edilen stego resimlerin % 800 oranında büyütülüp incelenmesi durumunda; 100 KB'lık değişimde bozulmanın insan gözü tarafından rahatlıkla algılanabileceği görülmektedir. Aynı şekilde LSB+1 ve LSB+2 bitleri için de inceleme yapıldığında 50 KB'lık değişimde bozulma olduğu görülmektedir. Yeşil renkli resim için kabul edilebilir eşik değerleri; LSB, LSB+1 ve LBS+2 için 50KB'lık değişim miktarı olarak alınabilir. Bu nedenle, seçilen yeşil renkli resim detaylı incelendiğinde LSB tekniğinde iyi sonuçlar vermemektedir. Şekil 4.5'te yeşil renkli resim için PSNR-Değişim miktarı grafiği verilmiştir. Grafik üzerinde LSB, LSB+1 ve LSB+2 için kabul edilebilecek eşik değerleri kırmızı '*' işaretiyle gösterilmiştir.

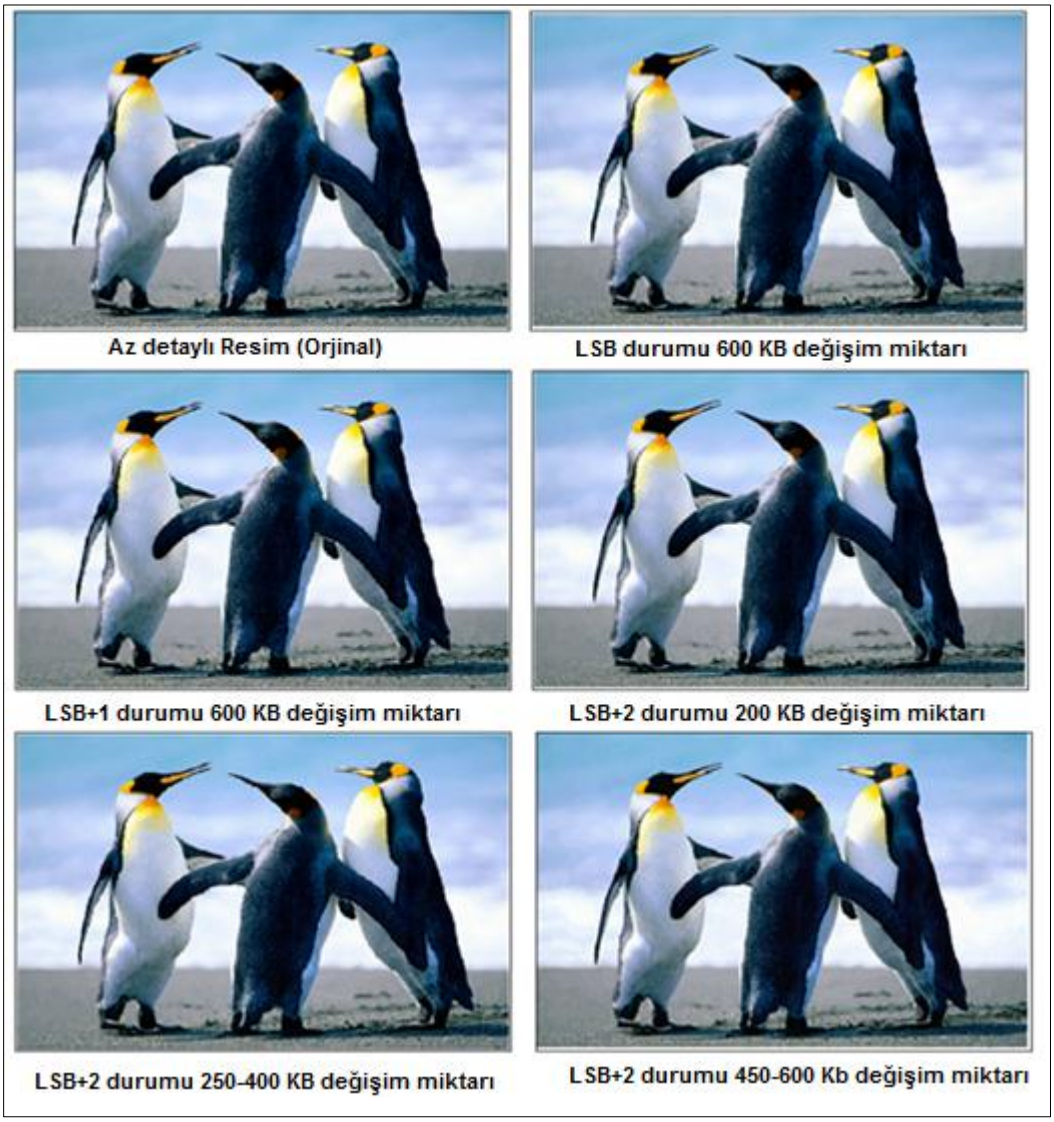


Şekil 4.5 Yeşil renkli resim için PSNR-Değişim miktarı grafiği

Az detaylı bir resim için sonuçlar: Az detaylı bir resim için LSB, LSB+1, LSB+2 bitlerinin değişimi durumunda elde edilen PSNR değerleri çizelge 4.3'te gösterilmiştir. Şekil 4.6'da az detaylı bir resim için elde edilen stego resimlerdeki değişim miktarı gösterilmiştir.

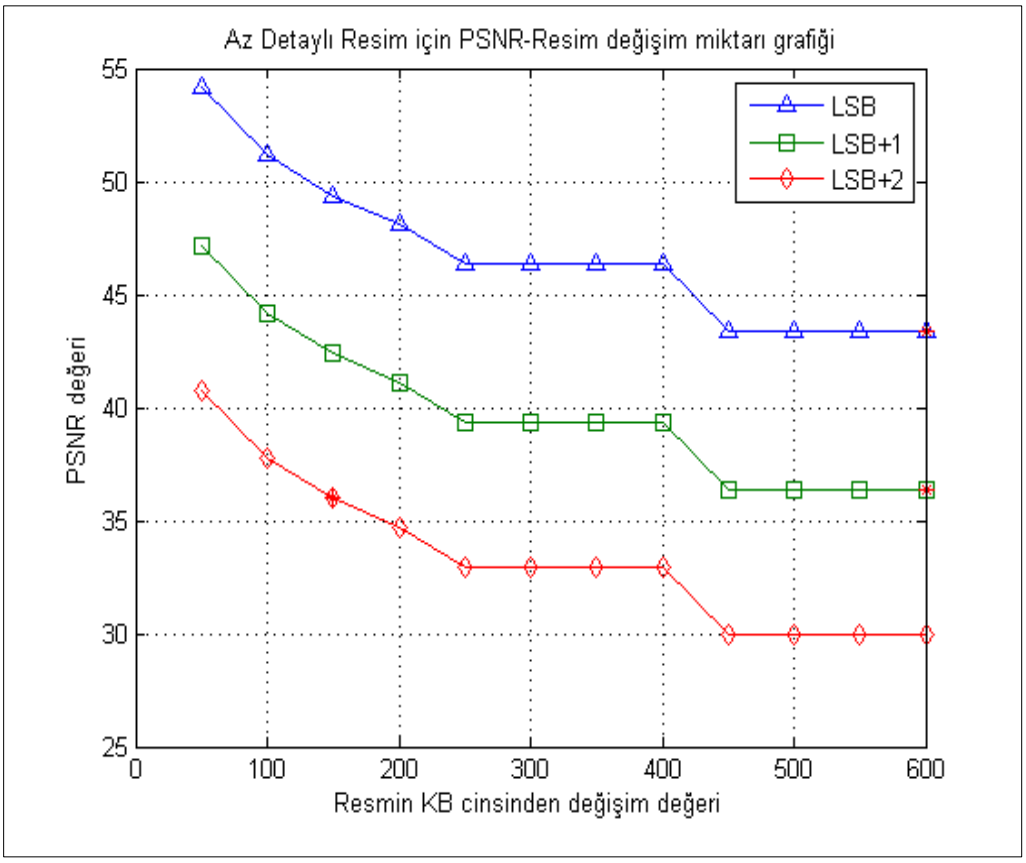
Çizelge 4.3 Az detaylı bir resim için PSNR değerleri

Değişim Miktarı (KB)	LSB	LSB+1	LSB+2
50	54.1514	47.1492	40.7427
100	51.1411	44.1322	37.7338
150	49.3802	42.3766	**35.9692**
200	48.1308	41.1225	34.7218
250-400	46.3699	39.3621	32.9589
450-600	**43.3596**	**36.3512**	29.9485



Şekil 4.6 Az detaylı resim için LSB bit değişimleri

Az detaylı bir resim için elde edilen stego resimler incelendiğinde LSB ve LSB+1 bitlerinde değişiklik yapıldığında 600 KB'a kadar iyi sonuçlar alındığı görülmektedir. LSB+2 bitleri için de 200 KB'lık değişimin üzerinde bozulmanın insan gözü tarafından rahatlıkla algılanabileceği görülmektedir. Bu nedenle, az detaylı resim için steganografi işleminde LSB ve LSB+1 bitleri değişikliğe uğradığında iyi sonuç vermektedir. LSB+2 bitlerinde değişiklik yapıldığında ise, resimde bozulmalar olduğu insan gözü tarafından rahatlıkla algılanmaktadır. Şekil 4.7'de az detaylı resim için PSNR-Değişim miktarı grafiği verilmiştir. Grafik üzerinde LSB, LSB+1 ve LSB+2 için kabul edilebilecek eşik değerleri kırmızı '*' işaretiyle gösterilmiştir.



Şekil 4.7 Az detaylı resim için PSNR-Değişim miktarı grafiği

Detaylı bir resim için sonuçlar: Detaylı bir resim için LSB, LSB+1 ve LSB+2 bitlerinin değişimi durumunda elde edilen PSNR değerleri çizelge 4.4'te gösterilmiştir. Şekil 4.8'de detaylı bir resim için elde edilen stego resimlerdeki değişim miktarları gösterilmiştir.

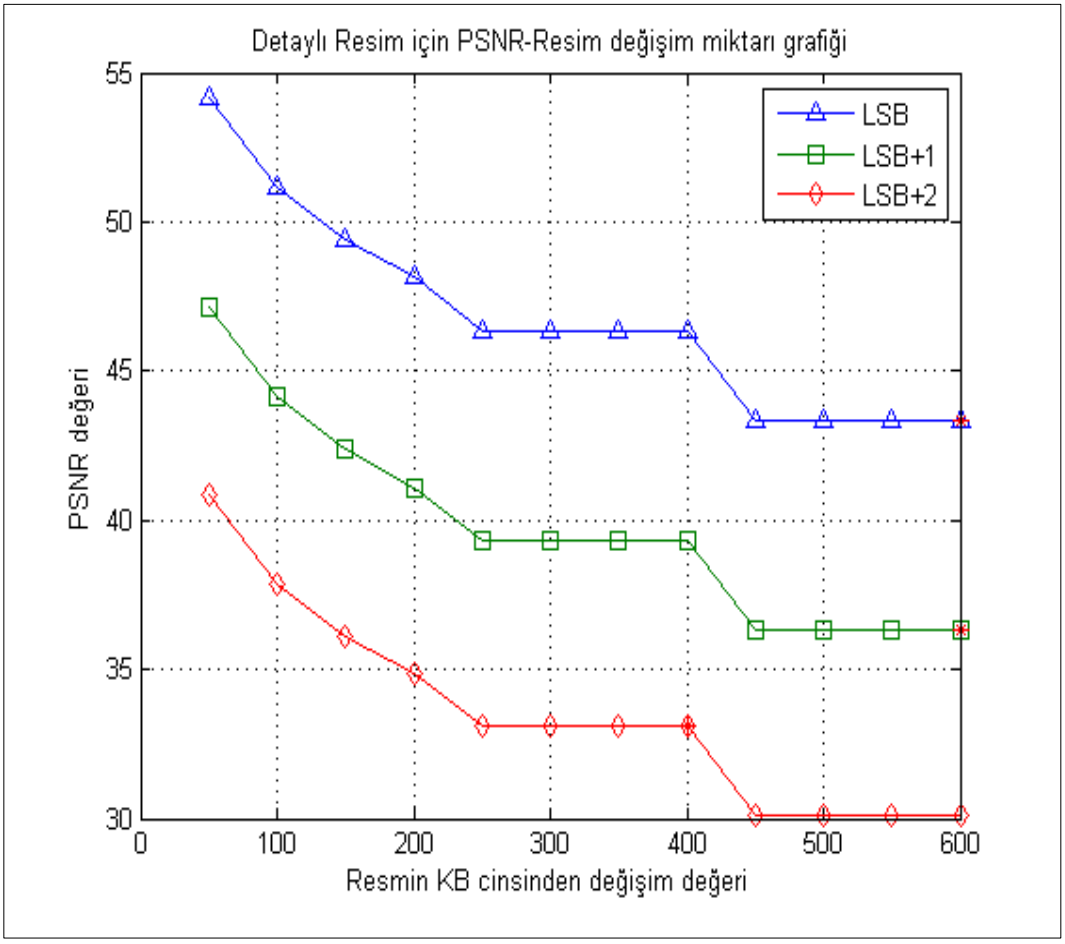
Çizelge 4.4 Detaylı bir resim için PSNR değerleri

Değişim Miktarı (KB)	LSB	LSB+1	LSB+2
50	54.1514	47.1333	40.8662
100	51.1411	44.1222	37.8574
150	49.3802	42.3627	36.0950
200	48.1308	41.1099	34.8438
250-400	46.3699	39.3482	**33.0842**
450-600	**43.3596**	**36.3380**	30.0731



Şekil 4.8 Detaylı resim için LSB bit değişimleri

Detaylı bir resim için elde edilen stego resimler incelendiğinde LSB ve LSB+1 bitlerinde değişiklik yapıldığında 600 KB değişim miktarına kadar iyi sonuçlar alındığı görülmektedir. LSB+2 bitlerinde değişiklik yapıldığında ise 400 KB'a kadar iyi sonuçlar alınmıştır. Şekil 4.9'da detaylı resim için PSNR-Değişim miktarı grafiği verilmiştir. Grafik üzerinde LSB, LSB+1 ve LSB+2 durumlarında kabul edilebilir eşik değerleri kırmızı '*' ile gösterilmiştir.



Şekil 4.9 Detaylı resim için PSNR-Resim değim miktarı grafiği

Tüm resim türleri kıyaslandığında LSB, LSB+1, LSB+2 için en iyi sonuçlar detaylı resimden elde edilmiştir. En kötü sonuçlar da yeşil renkli resim kullanılması durumunda ortaya çıkmıştır. Resim dosyalarında her bir üst katmandaki değişim bir alt katmana göre daha belirgin olmaktadır. LSB üstündeki her katmanda yapılan işlem, resim

kalitesini azaltmakta ve resim üzerinde değişiklik yapıldığını daha belirgin bir şekilde göstermektedir.

PSNR temelde orijinal resim ve elde edilen stego resmin pikselleri arasındaki farka dayanmaktadır. Taşıyıcı resimlerin PSNR değerlerine bakıldığında; LSB bitinin değişimi durumunda tüm resimlerin PSNR değerleri aynı çıkmaktadır. Bunun nedeni, sadece son bit olan LSB bitinde değişiklik yapıldığından (0 →1, 1→0) tüm resimlerdeki piksel farkları aynı olmaktadır. LSB+1 ve LSB+2 bitlerinde değişiklik yapıldığında ise, her resmin piksel değerleri homojen olmadığından pikseller arasındaki fark aynı olmamaktadır. Örneğin; beyaz renkli resim için RGB değerleri 255, 255, 255 iken, yeşil renkli resim için RGB değerleri 22, 116, 50'dir. Bu nedenle; piksellerdeki değişim farklı olacaktır. Bunun yanında, taşıyıcı resimler üzerindeki değişim miktarının düzgün olması (homojen dağılım) sağlandığından 250-400 KB ve 450-600 KB değişim miktarları için PSNR değerleri aynı çıkmaktadır. PSNR hesaplamasında EK 7'de yer alan MATLAB kodu kullanılmıştır.

LSB tekniği, steganografide kullanılan popüler bir teknik olmasına rağmen zayıflıklarını bulunmaktadır. Bu teknik, taşıyıcı resmin her pikselinin her byte değerinin son bitine taşınması istenen dosyanın bitlerinin sırasıyla birer birer yerleştirilmesine dayanmaktadır. Bu işlemle, her sekiz bitin en fazla bir biti ve en önemsiz biti değişikliğe uğradığından taşınan veri insan gözü tarafından algılanmayacaktır. Bununla birlikte, steganaliz yapıldığında, stego nesnenin her pikselinin her byte değerinin son biti sırasıyla alındığında taşınan veri kolaylıkla elde edilebilir. LSB tekniğinin bu zayıflıklarını ortadan kaldırmak amacıyla, steganografi yazılımında bazı önlemler alınmıştır. Taşıyıcı resmin LSB bitlerine veri yerleştirmede taşınacak verinin bit sırası değiştirilerek işlem yapılmıştır. Bu şekilde taşınan verinin bitleri sıralı bir şekilde kırmızı, yeşil ve mavi byte değerlerinin son bitine yerleştirilmemiştir. İkinci bir önlem olarak, her pikselin kırmızı, yeşil ve mavi byte değerlerinin son bitleri otomatik olarak değiştirilerek taşınan verinin bitleri eklenmiştir. Ayrıca, gizlenecek veriyi bir anahtar yardımıyla (*random generator*) rastgele seçilen piksellere saklama işlemi de yapılabilir. Bütün önlemler göz önüne alındığında LSB tekniği için stego resme istenmeyen kişi tarafından steganaliz yapıldığında taşınan veri kolaylıkla elde edilmeyecektir.

4.2 Optiksel Telsiz Veri İletim Değerlendirmesi

Tez çalışmasında; büyük (879 KB), orta (400 KB) ve küçük (120 KB) boyutta üç farklı taşıyıcı resim üzerinde; büyük (51,8 KB), orta (20,5 KB) ve küçük (5,5 KB) boyutlu taşınacak dosyalar seçilerek seri port OTİS üzerinde farklı baud rate hızlarında iki bilgisayar arası veri iletimi sağlanmıştır (Şekil 4.10).



Şekil 4.10 Tez çalışmasında kullanılan taşıyıcı nesne ve taşınacak dosya

Seri port OTİS üzerinden taşıyıcı nesne olarak büyük resim (bmp) ve taşınacak dosya (doc) olarak büyük dosya seçildiğinde; farklı baud rate hızında elde edilen sonuçlar çizelge 4.5'te verilmiştir.

Çizelge 4.5 Büyük taşıyıcı resim ve büyük dosya taşınması

Taşıyıcı Resim	Taşınacak Dosya	Baud Rate	İletim Süresi
Büyük Resim(879 KB)	Büyük Dosya (51,8 KB)	9600	19 dk.
Büyük Resim (879 KB)	Büyük Dosya (51,8 KB)	19200	9 dk.
Büyük Resim (879 KB)	Büyük Dosya (51,8 KB)	28800	6 dk.
Büyük Resim (879 KB)	Büyük Dosya (51,8 KB)	38400	5 dk.
Büyük Resim (879 KB)	Büyük Dosya (51,8 KB)	57600	3 dk.

Çizelge 4.5'te görüldüğü gibi büyük bir resim üzerine büyük bir dosya taşındığında gönderim süresinin seri port OTİS için oldukça uzun bir süre olduğu görülmektedir. Bunun sebebi, lazer iletişimi değil, veri iletim tekniği olarak seri port kullanılmasıdır. RS-232 haberleşmede her defasında bir bit gönderildiğinden iletim süresi uzun olmaktadır.

Taşıyıcı nesne olarak orta boyutlu resim (bmp) ve taşınacak dosya (doc) olarak orta boyutlu bir dosya seçildiğinde; farklı baud rate hızlarında elde edilen sonuçlar çizelge 4.6'da görülmektedir.

Çizelge 4.6 Orta boyutlu taşıyıcı resim ve orta boyutlu dosya taşınması

Taşıyıcı Resim	**Taşınacak Dosya**	**Baud Rate**	**İletim Süresi**
Orta Boyutlu Resim (400 KB)	Orta Boyutlu Dosya (20,5 KB)	9600	9 dk.
Orta Boyutlu Resim (400 KB)	Orta Boyutlu Dosya (20,5 KB)	19200	4 dk.
Orta Boyutlu Resim (400 KB)	Orta Boyutlu Dosya (20,5 KB)	28800	3 dk.
Orta Boyutlu Resim (400 KB)	Orta Boyutlu Dosya (20,5 KB)	38400	2 dk.

Orta boyutlu bir resim üzerinde dosya taşınması durumunda; baud rate değeri arttırıldığında veri gönderim süresinin daha optimal değerlere düştüğü görülmektedir.

Taşıyıcı nesne olarak küçük boyutta resim (bmp) ve taşınacak dosya (doc) olarak küçük boyutlu dosya seçildiğinde; farklı baud rate hızlarında elde edilen sonuçlar çizelge 4.7'de görülmektedir.

Çizelge 4.7 Küçük taşıyıcı resim ve küçük dosya taşınması

Taşıyıcı Resim	**Taşınacak Dosya**	**Baud Rate**	**İletim Süresi**
Küçük Resim (120 KB)	Küçük Boyutlu Dosya (5,55 KB)	9600	3 dk.
Küçük Resim (120 KB)	Küçük Boyutlu Dosya (5,55 KB)	19200	2 dk.
Küçük Resim (120 KB)	Küçük Boyutlu Dosya (5,55 KB)	28800	1 dk.
Küçük Resim (120 KB)	Küçük Boyutlu Dosya (5,55 KB)	38400	~ 1 dk.

Çizelge 4.7'de görüleceği üzere küçük boyutta bir resim üzerinde küçük bir dosya taşındığında veri gönderim süresi oldukça düşmektedir. Seri port veri iletim tekniği temelde veri iletim hızı olarak oldukça yavaştır. Tez çalışmasında iki bilgisayar arasında steganografi tekniği kullanılarak bilgi gönderimi sağlanmıştır. Bu çalışmada amaç, optiksel telsizin yüksek hızlı iletimi olmadığı için sadece seri port iletimi steganografi tekniğinin başarımı için ekonomik ve yeterli olduğundan USB veya Ethernet gibi teknolojiler kullanılmamıştır.

5. TARTIŞMA VE SONUÇ

Tez çalışmasında, OTİS üzerinde iletişim güvenliği ve gizlilik tekniklerinin incelenmesi yapılmıştır. Bu kapsamda kablosuz iletişim teknolojileri alanında özellikle; OTİS'le ilgili iletişim güvenliği hakkında literatürde yapılan çalışmalar araştırılmıştır. Günümüzde; şifreli haberleşme bilgilerinin izlenerek fark edilmesinin önüne geçmeye çalışmak için kullanılan steganografi tekniği oldukça popüler bir kullanım alanı bulmuştur. İletişim gizliliğinin OTİS üzerinde uygulanabilirliğini göstermek amacıyla da seri port üzerinden steganografi tekniğiyle veri göndermek için donanım ve yazılım kısımlarından oluşan seri port OTİS gerçekleştirilmiştir. İletişim sistemi üzerinden farklı boyutlarda ve iletim hızlarında veriler gönderilerek sistemin performansı değerlendirilmiştir. Ayrıca, LSB tekniğinin etkinliğini görmek, zayıflıklarını ortadan kaldırmak ve taşıyıcı resim üzerinde gönderilen bir nesnenin algılanmasını güçleştirmek için alınması gereken önlemlere yer verilmiştir.

OTİS; temelde noktadan noktaya, yüksek bant genişliği ve yüksek hızda kablosuz iletim ortamı sunmaktadır. Özellikle, noktadan noktaya çalışması ve genelde binaların kule kısımlarına yerleştirilmesi dolayısıyla oldukça iyi bir güvenlik sağlamaktadır. OTİS'in noktadan noktaya çalışması durumu göz önüne alındığında RF sistemlere göre daha iyi iletişim güvenliği sağlamaktadır. Bunun yanında, literatürde yapılan çalışmalarda optiksel telsiz iletişim güvenliğini sağlamak için bazı önlemler alındığı görülmektedir. OTİS'in istenmeyen bir terminal tarafından verilerinin alınmasını önlemek amacıyla istenen alıcının arkasına lazer sinyalinin ışıma yarıçapının iki katı genişliğinde yansımayı önleyici ve sinyal emici bir nesne konulabilir.

OTİS üzerinde daha iyi bir iletişim güvenliğini sağlamak için RF teknolojisindeki tekniklerin bazı özellikleri olan asıllama, yetkilendirme gibi işlemler kullanılarak sadece yetkili kişiler tarafından kullanımı sağlanabilir. Özellikle, geniş açılı OTİS'lerde yetkilendirme yapılmasıyla sadece yetkili olan kişilerin bağlanması ve bilgi paylaşımı yapmaları sağlanacaktır. Bunun yanında, şifreleme algoritmaları, kriptografi ve

steganografi yöntemleri de iletişim güvenliği ve gizliliğini sağlamak için OTİS üzerinde kullanılabilir.

İletişim gizliliğinin sağlanması için farklı teknikler kullanılmaktadır. Kriptografi bir verinin sadece gizlenmesini sağlarken, steganografi tekniği verinin içeriğinin de gizlenmesini sağlamaktadır. Böylece; steganografi kullanılarak gizli bir veri gönderildiği, gözle görünür olmayacağından istenmeyen alıcılar tarafından fark edilememektedir. Steganografi tekniğinde kullanılan farklı yaklaşımlar bulunmaktadır.

Tez çalışmasında LSB tekniği yardımıyla bir taşıyıcı resmin içerisindeki en önemsiz bitler kullanılarak gizli bilgi alıcı tarafa taşınmıştır. LSB, steganografide kullanılan popüler bir teknik olmasına rağmen bazı zayıflıkları bulunmaktadır. Her pikselin her byte değerinin son biti değişikliğe uğradığından insan gözü tarafından kolaylıkla değişim algılanmaz fakat, taşınacak dosyanın bitleri taşıyıcı resmin LSB bitleriyle sıralı bir şekilde değiştirilirse, steganaliz yapan istenemeyen bir kullanıcı kolaylıkla LSB bitlerini birleştirerek taşınan dosyayı elde edebilir. Bunu önlemek amacıyla, LSB bitlerine sıralı eklemek yerine farklı sıralarda ekleme işlemi yapılmıştır. Ayrıca LSB bitlerine yerleştirme işlemleri düzgün şekilde yapılarak taşıyıcı resim üzerindeki bozulmaların sadece ilk bölgede olması önlenmiştir.

LSB tekniğinin zayıflıklarını kaldırmak için alınabilecek bir diğer önlem *random generator* yardımıyla rastgele piksellere yerleştirme işlemi yapılmasıdır. LSB tekniği dışında farklı teknikler kullanılarak steganografi işlemleri yapılabilir. Bunun yanında taşıyıcı resmin LSB biti ve bir sonraki biti üzerinde de resim taşınabilir. MSB bitine gelindikçe taşıyıcı resim üzerinde bozulmaların daha fazla olduğu gözükecektir.

Tez çalışmasında iki bilgisayar arası optiksel telsiz iletişimi seri port üzerinden sağlanmıştır. Seri port veri iletiminde gönderilmek istenen verinin bir defada sadece bir bitini transfer ettiği için veri iletim hızı oldukça düşüktür. Farklı boyutlarda dosyalar üzerinde farklı baud rate hızlarında veri taşındığında veri iletim süresinin değiştiği gözlenmiştir. Tez çalışmasında amaç, optiksel telsizin yüksek hızlı iletimi olmadığı için

sadece seri port veri iletimi steganografi tekniğinin başarımı için ekonomik ve yeterli olduğundan USB veya Ethernet gibi teknolojiler kullanılmamıştır. Veri iletiminde daha iyi sonuçlar alabilmek için USB veya Ethernet teknolojisi kullanılabilir.

Steganografi sisteminde, bilgi taşıma işlemi incelendiğinde taşıyıcı resim üzerine bindirilen gizli bilginin boyutunun, taşıyıcı resmin LSB bitlerinin toplamından büyük olmaması gerektiği görülmektedir. Taşınan bilgi boyutu arttıkça taşıyıcı resmin görüntüsünde bozulmalar meydana geldiği görülmüştür.

KAYNAKLAR

Akar, F. 2008. BMP Resimler İçin Veri Gizleme Tabanlı Bilgi Güvenliği Uygulamaları. 2. Ağ ve Bilgi Güvenliği Ulusal Sempozyumu Bildirileri, 6s., Kuzey Kıbrıs Türk Cumhuriyeti.

Akbal, T., Yalman, Y. ve Özcerit, A.T. 2010. Gerçek Zamanlı Sayısal Ses İçerisinde Sıkıştırılmış ve Şifrelenmiş Veri Transferi. 3. Ağ ve Bilgi Güvenliği Ulusal Sempozyumu Bildirileri, 7s., Ankara.

Amin, M.M., Ibrahim, S., Salleh, M. and Katmin, M.R. 2003. Information Hiding Using Steganography. Univesity Technology of Malaysia, 42 p., Malaysia.

Anonim. 2007. Bilişim Teknolojileri Portlar. Mesleki Eğitim ve Öğretim Sisteminin Güçlendirilmesi Projesi, 49 s., Ankara.

Anonim. 2008. Motorlu Araçlar Teknolojisi Otomotiv Yönetim Sistemleri 1. Mesleki Eğitim ve Öğretim Sisteminin Güçlendirilmesi Projesi, 57 s., Ankara.

Anonymous. 2002. Free-Space Optics: A Viable, Secure Last-Mile Solution ?. SANS Institute InfoSec Reading Room. SANS Institute, 11 p., USA.

Anonymous. 2004. ITU Internet Reports The Portable Internet. 216 p. Geneva.

Atıcı, M.A. 2007. Steganografik Yaklaşımların İncelenmesi, Tasarımı ve Geliştirilmesi. Gazi Üniversitesi Fen Bilimleri Enstitüsü, 127 s., Ankara.

Bender, W., Gruhl, D., Morimoto, N. and Lu, A. 1996. Techniques for data hiding. IBM Systems Journal, 313-336 p., USA.

Churnside, J. H. and Shaik, K. 1989. Atmospheric propagation issues relevant to optical communications. Technical Memorandum ERL WPL-159, National Oceanic and Atmospheric Administration, Wave Propagation Laboratory, Boulder, Colorado.

Çavuşoğlu, İ. ve Kırmızı, F. 2007. Seri port ile Haberleşebilen Uzaktan Kumandalı Kameralı Araç. Yıldız Teknik Üniversitesi, 56 s., İstanbul.

Çetin, Ö., Özcerit, A.T. ve Boru, B. 2008. Yüksek Kapasiteli Bir Alındısız Video Sırtörtme Yöntemi. 2. Ağ ve Bilgi Güvenliği Ulusal Sempozyumu Bildirileri, 5s., Kuzey Kıbrıs Türk Cumhuriyeti.

Elçi, B., Örs, B. ve Dalmışlı, V. 2008. Bir Steganografi Sisteminin FPGA Üzerinde Gerçeklenmesi. 3. Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı, 73-77 s., Ankara.

Erkin, Z. ve Örencik, B. 2005. Steganografik Kütüphane. 1. Ağ ve Bilgi Güvenliği Ulusal Sempozyumu Bildirileri, 5s., İstanbul.

Gökçe, M.C. 2012. Optiksel Telsiz İçin Yüksek Dereceli Lorenz-Gauss Laser Demetlerinin Pırıldama Analizi ve Değerlendirilmesi. Ankara Üniversitesi Fen Bilimleri Enstitüsü, 91s., Ankara.

Harmankaya, A.O., Demiray, H.E., Ertürk, İ., Bayılmış, C. ve Bandırmalı, N. 2008. Kablosuz Ağlarda Güvenlik Protokollerinin Karşılaştırmalı İncelenmesi. 2. Ağ ve Bilgi Güvenliği Ulusal Sempozyumu, 7 s., Kuzey Kıbrıs Türk Cumhuriyeti.

Johnson, N.F. and Jojodia, S. 1998. Exploring Steganography: Seeing the Unseen. IEEE.

Karaboğa, D. ve Ökdem, S. 2006. Kablosuz Algılayıcı Ağlarında Güvenli İletişim Teknikleri. Ulusal Elektronik İmza Sempozyumu, 4 s., Ankara.

Karakaş, B., Soğancıoğlu, S. ve Yüksel, A. 2011. Optiksel Telsiz ile Bilgisayarlar arası Veri İletimi. Ankara Üniversitesi Mühendislik Fakültesi Elektronik Mühendisliği Bölümü Mühendislikte Projelendirme ELM-471, 45s., Ankara.

Kenneth, M. 2012. FSO. http://www.chipps.com/5/FSO.pptx. Erişim Tarihi: 22.06.2013.

Krenn, J.R. 2004. Steganography and Steganalysis. http://www.krenn.nl/univ/cry/steg/article.pdf, Erişim Tarihi:10.12.2012.

Maity, A. 2010. Steganography (A new technique to hide information within image file). Mumbai University, 55 p., Mumbai.

Majumdar, A.K. and Ricklin J.C. 2008 Free-Space Lazer Communications Principles and Advanced Springer, USA.

Meghanathan, N. and Nayak, L. Steganalysis Algorithms for Detecting The Hidden Information in Image, Audio and Video Cover Media. Inernational Journal of Network Security & Its Application (IJNSA), Vol2, No.1 43-55p., USA.

Mesut, A.Ş., Buluş, E., Sakallı, M.T. ve Buluş, H.N. 2008. RQP Steganalizinde Renk Çiftleri Arasındaki Yakınlık Derecesi Seçiminin Resmin İçindeki Gizli Bilginin Sezilmesine Etkisi. 2. Ağ ve Bilgi Güvenliği Ulusal Sempozyumu Bildirileri, 5s., Kuzey Kıbrıs Türk Cumhuriyeti.

Pehlivan, İ., Odabaş, C., Demircioğlu, S., Gezer, M. ve Coşkun, İ. 2008. Kablosuz Ağ Şifreleme Yöntemlerinin Karşılaştırılması. 2. Ağ ve Bilgi Güvenliği Ulusal Sempozyumu, 5 s., Kuzey Kıbrıs Türk Cumhuriyeti.

Popoola, W.O., Ghassemlooy, Z., Lee, C.G. and Boucouvalas, A.C. 2009. Scintillation effect on intensity modulated laser communication systems-a laboratory demonstration. Optics & Laser Technology. USA.

Sarı, H. 2008, FZM450 Elektro-Optik 2007-2008 Bahar Dönemi Ders Notları. Ankara Üniversitesi, Ankara.

Şahin, A. 2007. Görüntü Steganografide Kullanılan Yeni Metodlar ve Bu Metodların Güvenilirlikleri. Trakya Üniversitesi Fen Bilimleri Enstitüsü, Edirne.

Şahin, A., Buluş, E. ve Sakallı, M.T. 2005. 24-Bit Renkli Resimler Üzerinde En Önemsiz Bite Ekleme Yöntemini Kullanarak Bilgi Gizleme. Trakya Üniversitesi Araştırma Makalesi, 17-22 s., Edirne.

Toyran, M. 2006. Optik Ağlarda Kuantum Kriptografi Kullanarak Güvenli İletişim. ELECO 2006, 5 s., Bursa.

Yalman, Y. ve Ertürk, İ. 2008. Sayısal Ses İçerisinde Gizli Veri Transferinin Kablosuz Ortamda Gerçekleştirilmesi. Politeknik Dergisi, 319-327 s., Ankara.

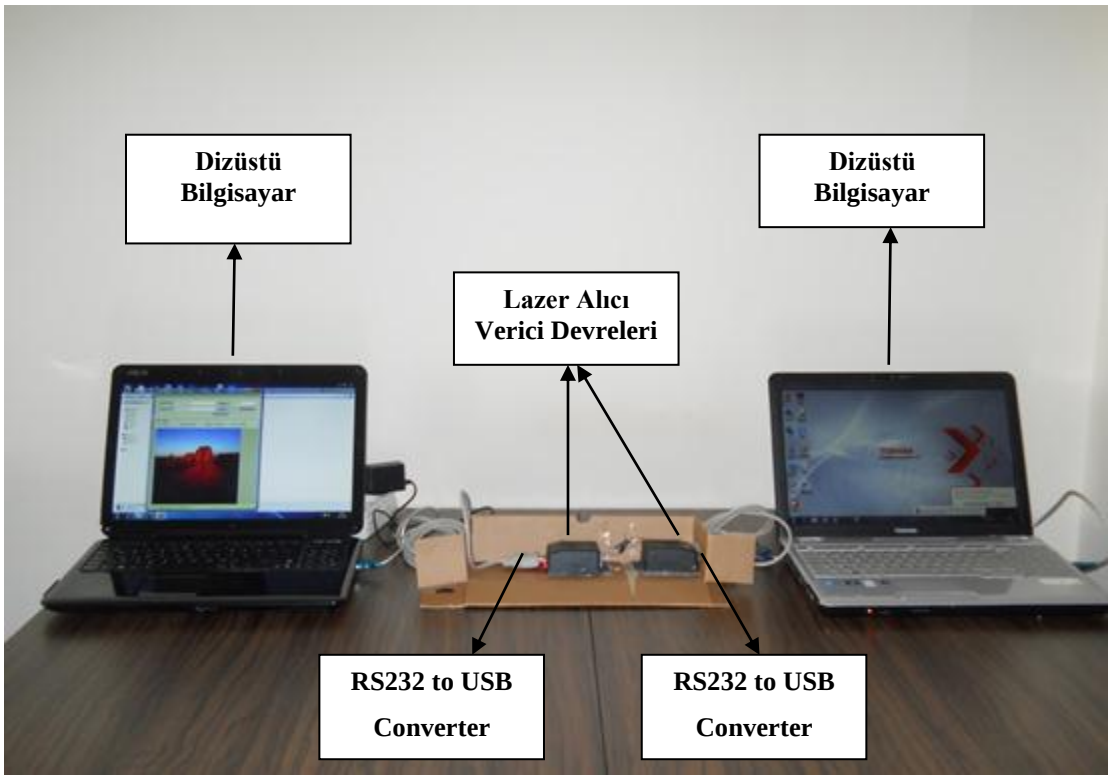
Yerlikaya, T. 2006. Yeni Şifreleme Algoritmalarının Analizi. Trakya Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Bölümü Doktora Tezi, 147s., Edirne.

Willebrand, H. and Ghuman, B.S. 2002. Freespace optics: Enabling optical connectivity in today's networks. SAMS, 259 p., Indiana.

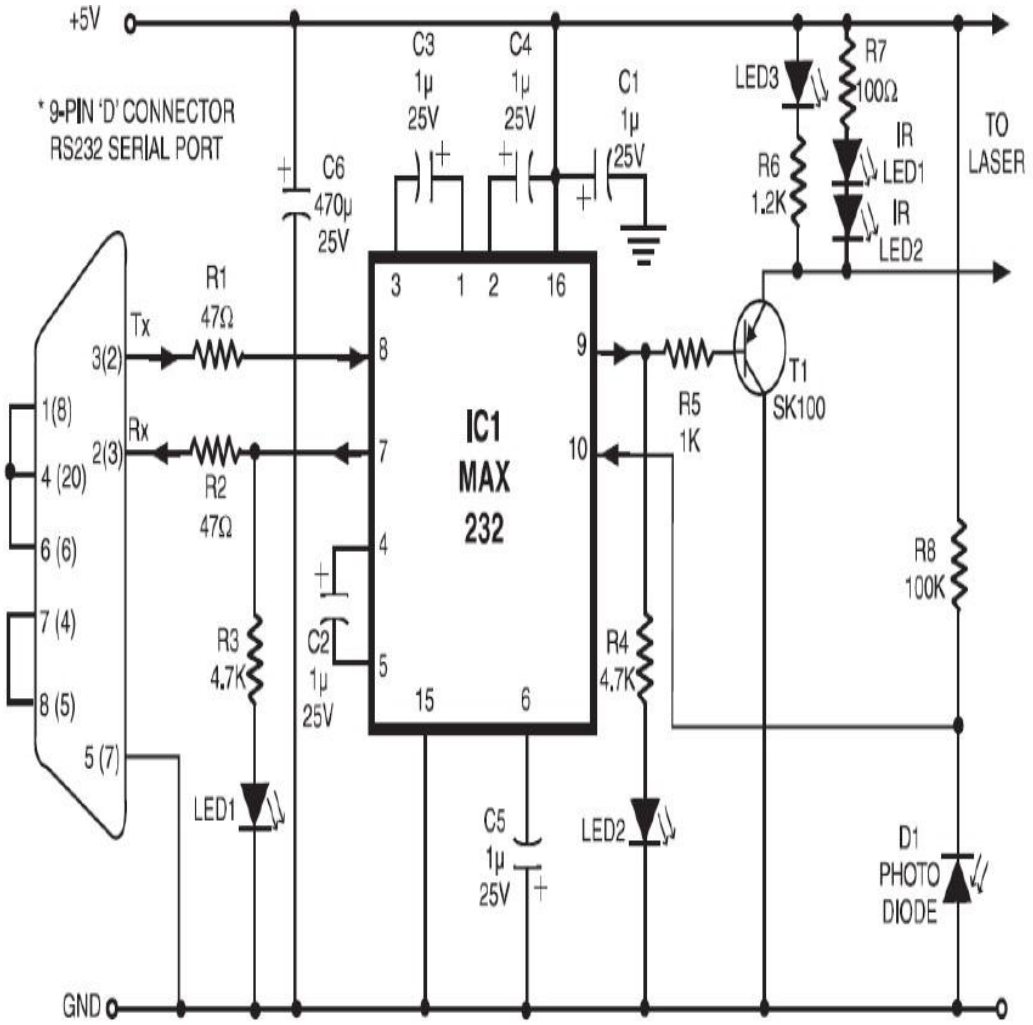
EKLER

EK 1 Deney Düzeneği Görünümü 59
EK 2 Elektronik Devre Şeması 60
EK 3 Transistör Özellikleri 61
EK 4 Foton Diyotun Özellikleri 65
EK 5 Yazılım Veri Gizleme Adımları 68
EK 6 Yazılım Veri Çözme Adımları 72
EK 7 PSNR Hesaplama Kodu (MATLAB) 76

EK 1 Deney Düzeneği Görünümü



EK 2 Elektronik Devre Şeması



- LED 1 veri alındığı zaman ışıma yapar.
- LED 2 veri gönderildiği zaman ışıma yapar.
- LED 3, IRLED 1 ve IRLED 2 lazer kullanılmadığı zaman veri iletiminde kullanılmaktadır (Karakaş vd. 2011).

EK 3 Transistör Özellikleri

MOSPEC

COMPLEMENTARY SILICON PLASTIC POWER TRANSISTORS

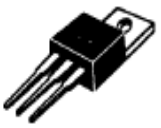
... designed for use in general purpose power amplifier and switching applications.

FEATURES:

* Collector-Emitter Sustaining Voltage -
  $V_{CEO(sus)}$ = 40V(Min)- TIP31,TIP32
  60V(Min)- TIP31A,TIP32A
  80V(Min)- TIP31B,TIP32B
  100V(Min)-TIP31C,TIP32C
* Collector-Emitter Saturation Voltage- $V_{CE(sat)}$=1.2V(Max)@I_C= 3.0 A
* Current Gain-Bandwidth Product f_T=3.0 MHz (Min)@ I_C=500 mA

NPN	PNP
TIP31	TIP32
TIP31A	TIP32A
TIP31B	TIP32B
TIP31C	TIP32C

3 AMPERE
COMPLEMENTARY SILICON
POWER TRANSISTORS
40 -100 VOLTS
40 WATTS



TO-220

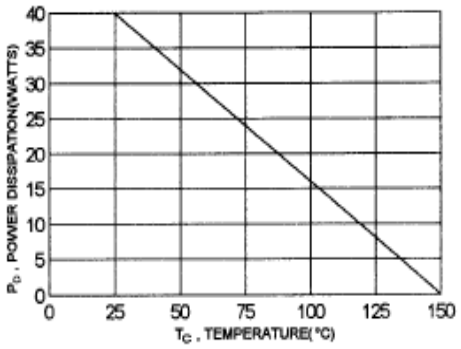
MAXIMUM RATINGS

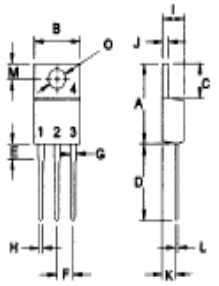
Characteristic	Symbol	TIP31 TIP32	TIP31A TIP32A	TIP31B TIP32B	TIP31C TIP32C	Unit
Collector-Emitter Voltage	V_{CEO}	40	60	80	100	V
Collector-Base Voltage	V_{CBO}	40	60	80	100	V
Emitter-Base Voltage	V_{EBO}	5.0				V
Collector Current - Continuous - Peak	I_C	3.0 5.0				A
Base Current	I_B	1.0				A
Total Power Dissipation@T_C = 25°C Derate above 25°C	P_D	40 0.32				W W/°C
Operating and Storage Junction Temperature Range	T_J,T_{STG}	-65 to +150				°C

THERMAL CHARACTERISTICS

Characteristic	Symbol	Max	Unit
Thermal Resistance Junction to Case	Rθjc	3.125	°C/W

FIGURE -1 POWER DERATING





PIN 1.BASE
2.COLLECTOR
3.EMITTER
4.COLLECTOR(CASE)

DIM	MILLIMETERS MIN	MAX
A	14.68	15.31
B	9.78	10.42
C	5.01	6.52
D	13.06	14.62
E	3.57	4.07
F	2.42	3.66
G	1.12	1.36
H	0.72	0.96
I	4.22	4.96
J	1.14	1.38
K	2.20	2.97
L	0.33	0.55
M	2.48	2.98
O	3.70	3.90

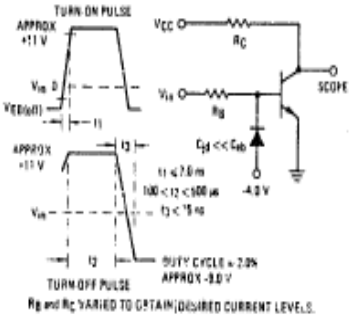
ELECTRICAL CHARACTERISTICS (T_C = 25°C unless otherwise noted)

Characteristic		Symbol	Min	Max	Unit
OFF CHARACTERISTICS					
Collector-Emitter Sustaining Voltage(1) (I_C= 30 mA, I_B= 0)	TIP31,TIP32 TIP31A,TIP32A TIP31B,TIP32B TIP31C,TIP32C	$V_{CEO(sus)}$	40 60 80 100		V
Collector Cutoff Current (V_{CE}= 30 V, I_B= 0) (V_{CE}= 60 V, I_B= 0)	TIP31,TIP32,TIP31A,TIP32A TiP31B,TiP32B,TIP31C,TIP32C	I_{CEO}		0.3 0.3	mA
Collector Cutoff Current (V_{CE}= 40 V, V_{EB}= 0) (V_{CE}= 60 V, V_{EB}= 0) (V_{CE}= 80 V, V_{EB}= 0) (V_{CE}= 100 V, V_{EB}= 0)	 TIP31,TIP32 TIP31A,TIP32A TIP31B,TIP32B TIP31C,TIP32C	I_{CES}		 0.2 0.2 0.2 0.2	mA
Emitter Cutoff Current (V_{EB}= 5.0 V, I_C= 0)		I_{EBO}		1.0	mA
ON CHARACTERISTICS (1)					
DC Current Gain (I_C =1.0 A, V_{CE} = 4.0 V) (I_C= 3.0 A, V_{CE} = 4.0 V)		hFE	 25 10	 50	
Collector-Emitter Saturation Voltage (I_C = 3.0 A, I_B =375 mA)		$V_{CE(sat)}$		1.2	V
Base-Emitter On Voltage (I_C =3.0 A, V_{CE}= 4.0 V)		$V_{BE(on)}$		1.8	V
DYNAMIC CHARACTERISTICS					
Current Gain - Bandwidth Product (2) (I_C = 500 mA , V_{CE} = 10 V , f_{TEST} = 1 MHz)		f_T	3.0		MHz
Small Signal Current Gain (I_C = 500 mA , V_{CE} = 10 V , f = 1 kHz)		h_{fe}	20		

(1) Pulse Test: Pulse width ≤ 300 μs , Duty Cycle ≤ 2.0 %

(2) $f_T = |h_{fe}| \cdot f_{TEST}$

FIGURE 2 – SWITCHING TIME EQUIVALENT CIRCUIT



R_B and R_C VARIED TO OBTAIN DESIRED CURRENT LEVELS.

FIG-3 TURN-ON TIME

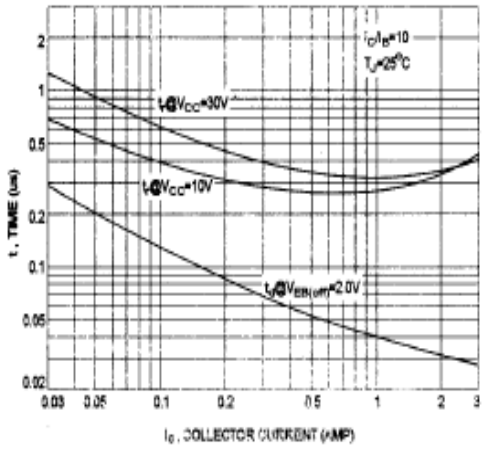


FIG-4 DC CURRENT GAIN

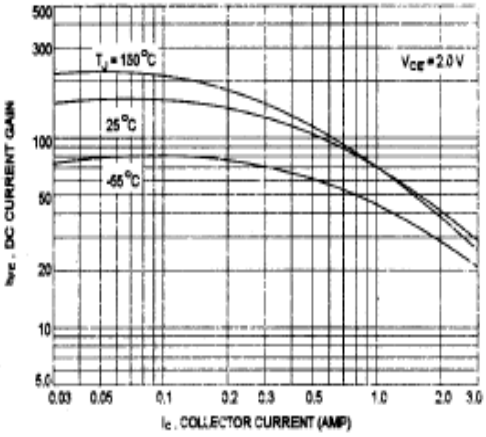


FIG-5 TURN-OFF TIME

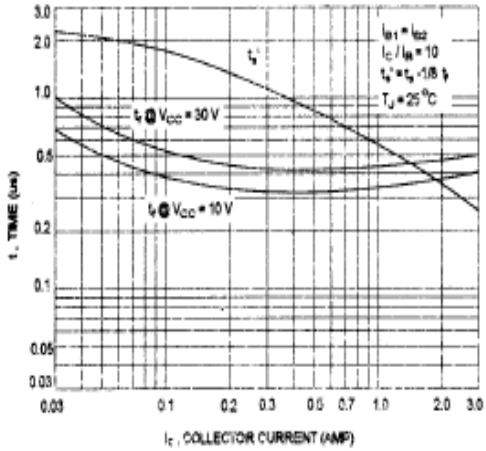
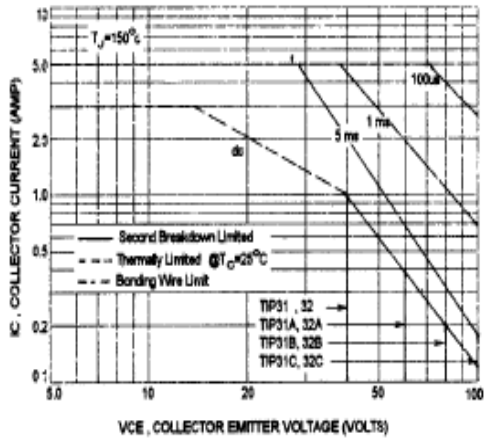


FIG-6 ACTIVE REGION SAFE OPERATING AREA



There are two limitation on the power handling ability of a transistor:average junction temperature and second breakdown safe operating area curves indicate I_C-V_{CE} limits of the transistor that must be observed for reliable operation i.e., the transistor must not be subjected to greater dissipation than curves indicate.

The data of FIG-6 curve is base on $T_{J(PK)}$=150 °C; T_C is variable depending on power level. second breakdown pulse limits are valid for duty cycles to 10% provided $T_{J(PK)} \leq$150°C.At high case temperatures,thermal limitation will reduce the power that can be handled to values less than the limitations imposed by second breakdown.

FIG-7 COLLECTOR SATURATION REGION

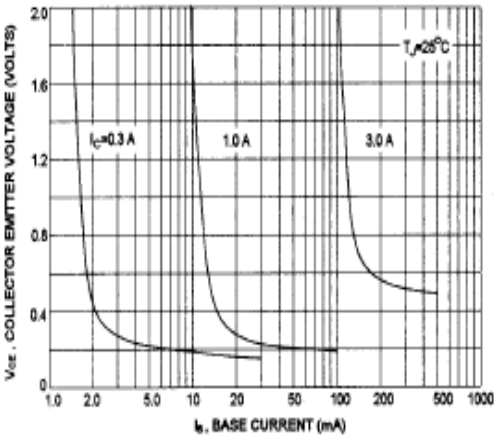


FIG-8 CAPACITANCES

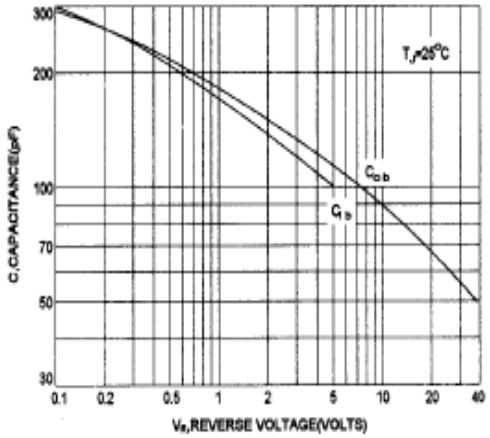


FIG-9 "ON" VOLTAGE

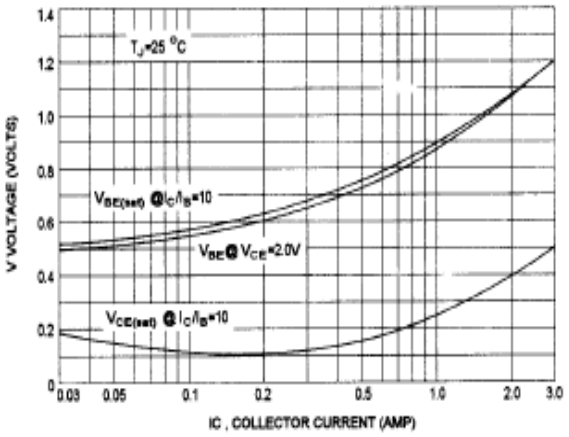
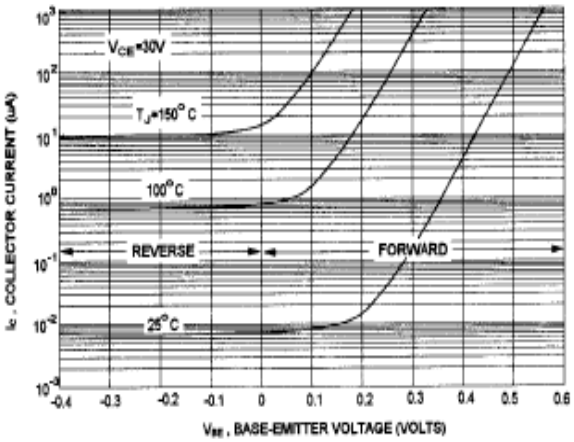


FIG-10 COLLECTOR CUT-OFF REGION



EK 4 Foton Diyotun Özellikleri

VISHAY.
www.vishay.com

BPW34, BPW34S

Vishay Semiconductors

Silicon PIN Photodiode



FEATURES

- Package type: leaded
- Package form: top view
- Dimensions (L x W x H in mm): 5.4 x 4.3 x 3.2
- Radiant sensitive area (in mm²): 7.5
- High photo sensitivity
- High radiant sensitivity
- Suitable for visible and near infrared radiation
- Fast response times
- Angle of half sensitivity: φ = ± 65°
- Compliant to RoHS Directive 2002/95/EC and in accordance to WEEE 2002/96/EC

Note

** Please see document "Vishay Material Category Policy": www.vishay.com/doc?99902

DESCRIPTION

BPW34 is a PIN photodiode with high speed and high radiant sensitivity in miniature, flat, top view, clear plastic package. It is sensitive to visible and near infrared radiation. BPW34S is packed in tubes, specifications like BPW34.

APPLICATIONS

- High speed photo detector

PRODUCT SUMMARY			
COMPONENT	I_{ra} (µA)	φ (deg)	$\lambda_{0.1}$ (nm)
BPW34	50	± 65	430 to 1100
BPW34S	50	± 65	430 to 1100

Note

- Test condition see table "Basic Characteristics"

ORDERING INFORMATION			
ORDERING CODE	PACKAGING	REMARKS	PACKAGE FORM
BPW34	Bulk	MOQ: 3000 pcs, 3000 pcs/bulk	Top view
BPW34S	Tube	MOQ: 1800 pcs, 45 pcs/tube	Top view

Note

- MOQ: minimum order quantity

ABSOLUTE MAXIMUM RATINGS (T_{amb} = 25 °C, unless otherwise specified)				
PARAMETER	TEST CONDITION	SYMBOL	VALUE	UNIT
Reverse voltage		V_R	60	V
Power dissipation	$T_{amb} \leq 25$ °C	P_V	215	mW
Junction temperature		T_j	100	°C
Operating temperature range		T_{amb}	- 40 to + 100	°C
Storage temperature range		T_{stg}	- 40 to + 100	°C
Soldering temperature	t ≤ 3 s	T_{sd}	260	°C
Thermal resistance junction/ambient	Connected with Cu wire, 0.14 mm²	R_{thJA}	350	K/W

BASIC CHARACTERISTICS (T_{amb} = 25 °C, unless otherwise specified)						
PARAMETER	**TEST CONDITION**	**SYMBOL**	**MIN.**	**TYP.**	**MAX.**	**UNIT**
Breakdown voltage	I_R = 100 µA, E = 0	$V_{(BR)}$	60			V
Reverse dark current	V_R = 10 V, E = 0	I_{ro}		2	30	nA
Diode capacitance	V_R = 0 V, f = 1 MHz, E = 0	C_D		70		pF
	V_R = 3 V, f = 1 MHz, E = 0	C_D		25	40	pF
Open circuit voltage	E_e = 1 mW/cm², λ = 950 nm	V_o		350		mV
Temperature coefficient of V_o	E_e = 1 mW/cm², λ = 950 nm	TK_{Vo}		- 2.6		mV/K
Short circuit current	E_A = 1 klx	I_k		70		µA
	E_e = 1 mW/cm², λ = 950 nm	I_k		47		µA
Temperature coefficient of I_k	E_e = 1 mW/cm², λ = 950 nm	TK_{Ik}		0.1		%/K
Reverse light current	E_A = 1 klx, V_R = 5 V	I_{ra}		75		µA
	E_e = 1 mW/cm², λ = 950 nm, V_R = 5 V	I_{ra}	40	50		µA
Angle of half sensitivity		φ		± 65		deg
Wavelength of peak sensitivity		λ_p		900		nm
Range of spectral bandwidth		$\lambda_{0.1}$		430 to 1100		nm
Noise equivalent power	V_R = 10 V, λ = 950 nm	NEP		4×10^{-14}		W/√Hz
Rise time	V_R = 10 V, R_L = 1 kΩ, λ = 820 nm	t_r		100		ns
Fall time	V_R = 10 V, R_L = 1 kΩ, λ = 820 nm	t_f		100		ns

BASIC CHARACTERISTICS (T_{amb} = 25 °C, unless otherwise specified)

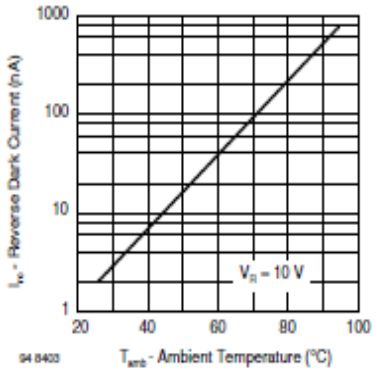


Fig. 1 - Reverse Dark Current vs. Ambient Temperature

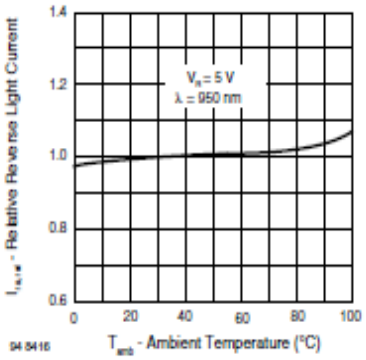


Fig. 2 - Relative Reverse Light Current vs. Ambient Temperature

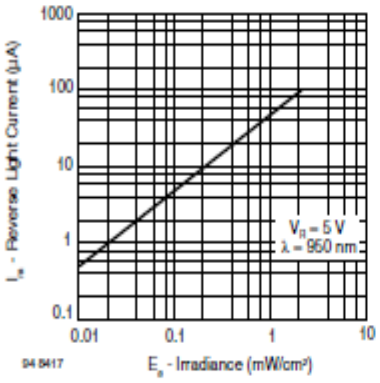


Fig. 3 - Reverse Light Current vs. Irradiance

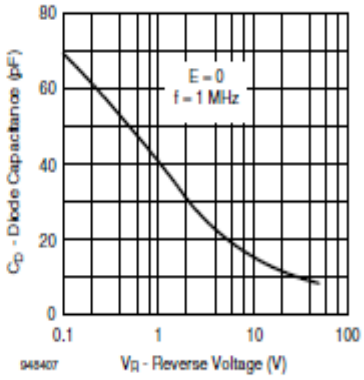


Fig. 6 - Diode Capacitance vs. Reverse Voltage

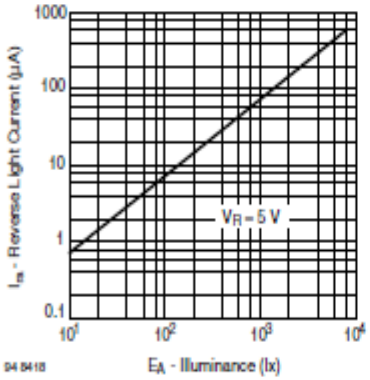


Fig. 4 - Reverse Light Current vs. Illuminance

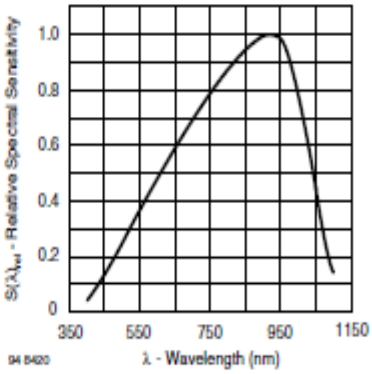


Fig. 7 - Relative Spectral Sensitivity vs. Wavelength

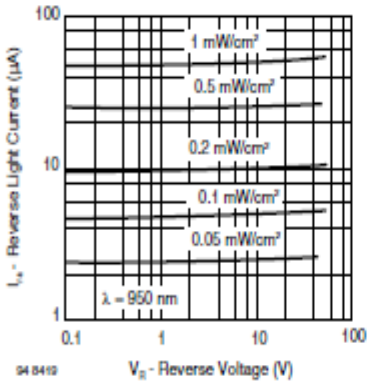


Fig. 5 - Reverse Light Current vs. Reverse Voltage

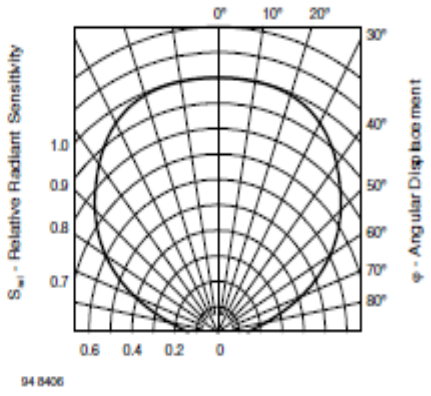
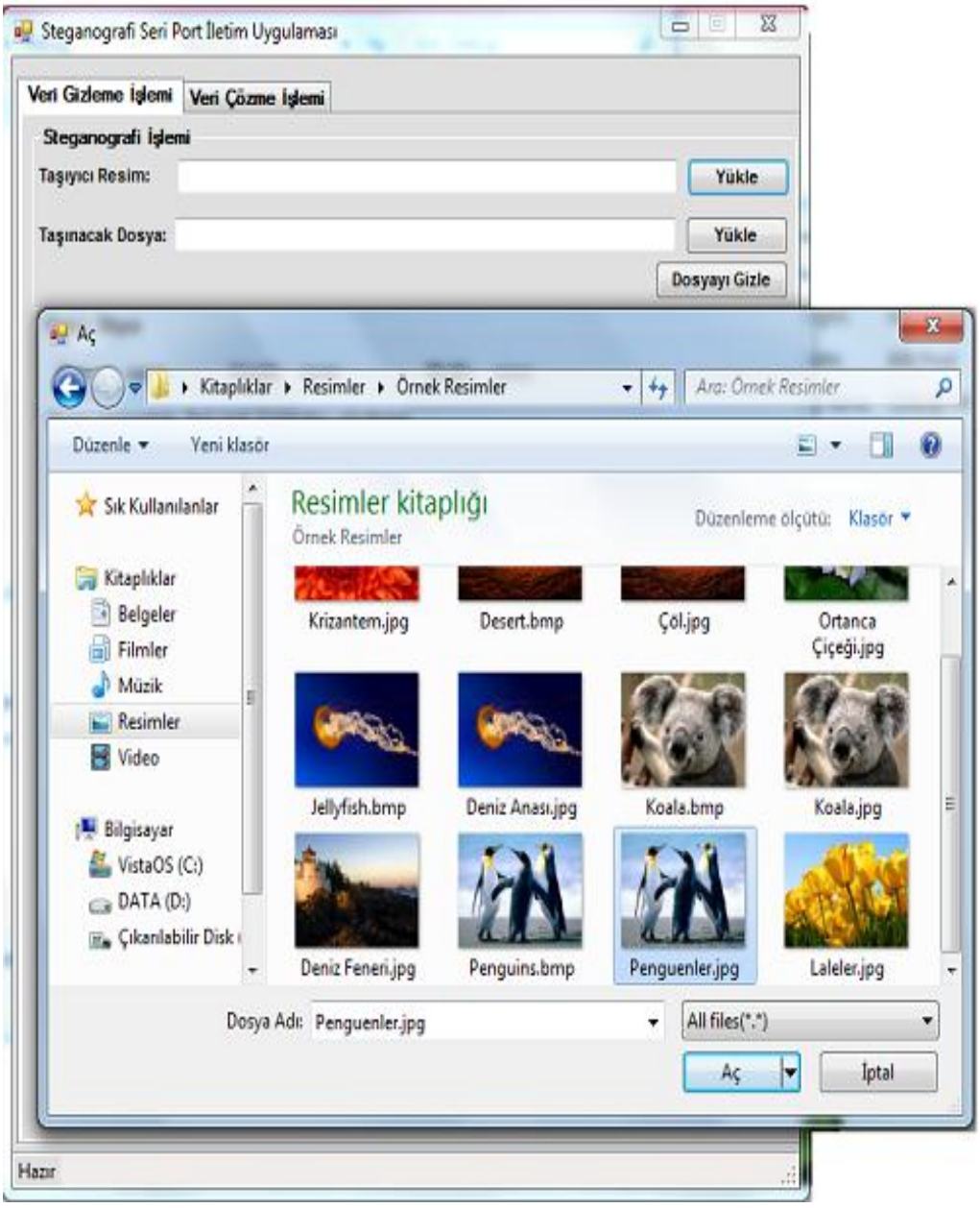


Fig. 8 - Relative Radiant Sensitivity vs. Angular Displacement

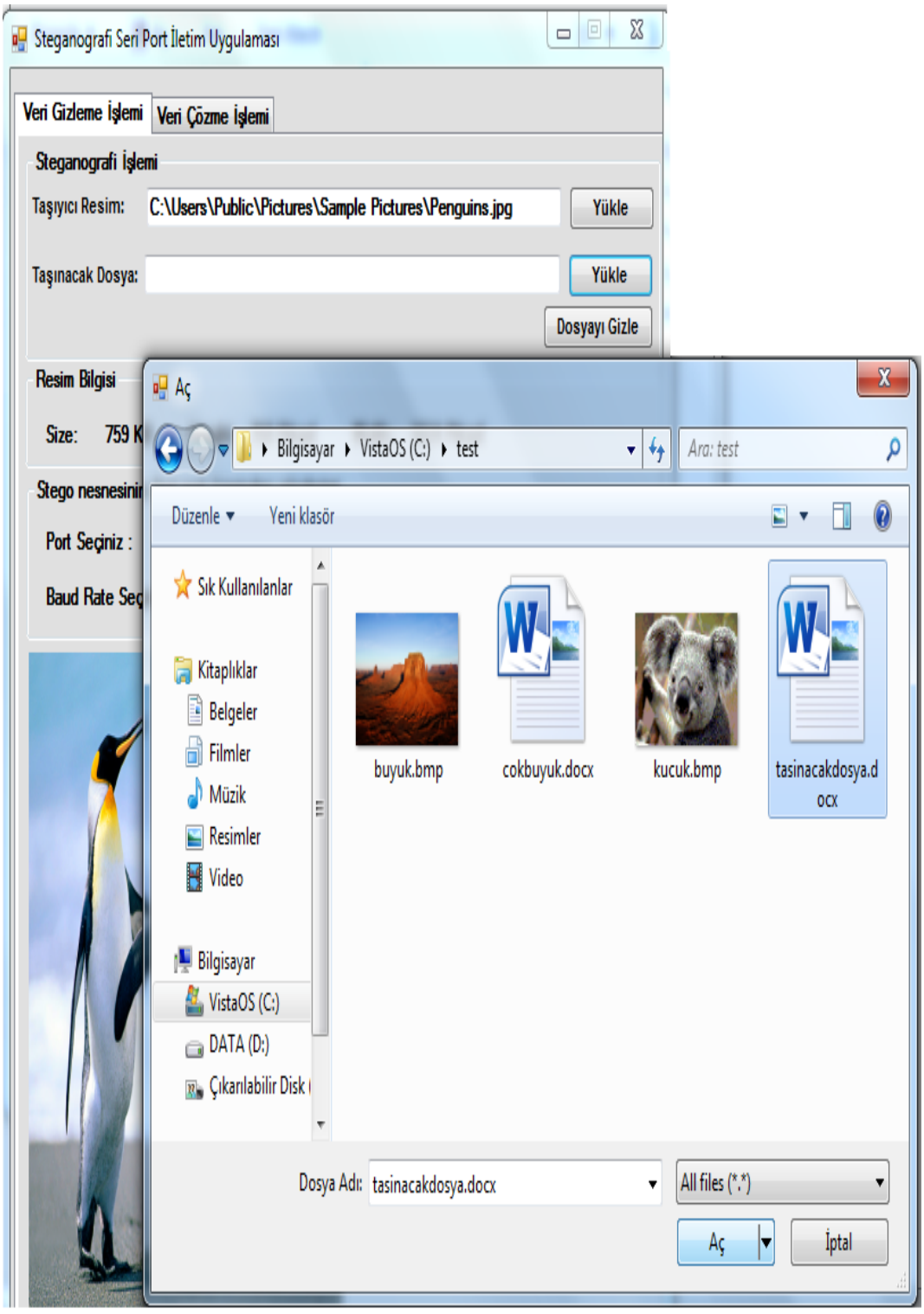
EK 5 Yazılım Veri Gizleme Adımları

1. Veri gizleme işleminde kullanılacak taşıyıcı resim seçilir. Bu resim taşınacak dosyanın boyutunun en az yarısından daha fazla büyüklükte seçilmelidir. Taşıyıcı resmi seçmek için uygulama ara yüzünde şekil 1'de görüldüğü gibi "Yükle" butonuna basılır. Açılan göz atma penceresinden taşıyıcı resim "Aç" denilerek seçilir.



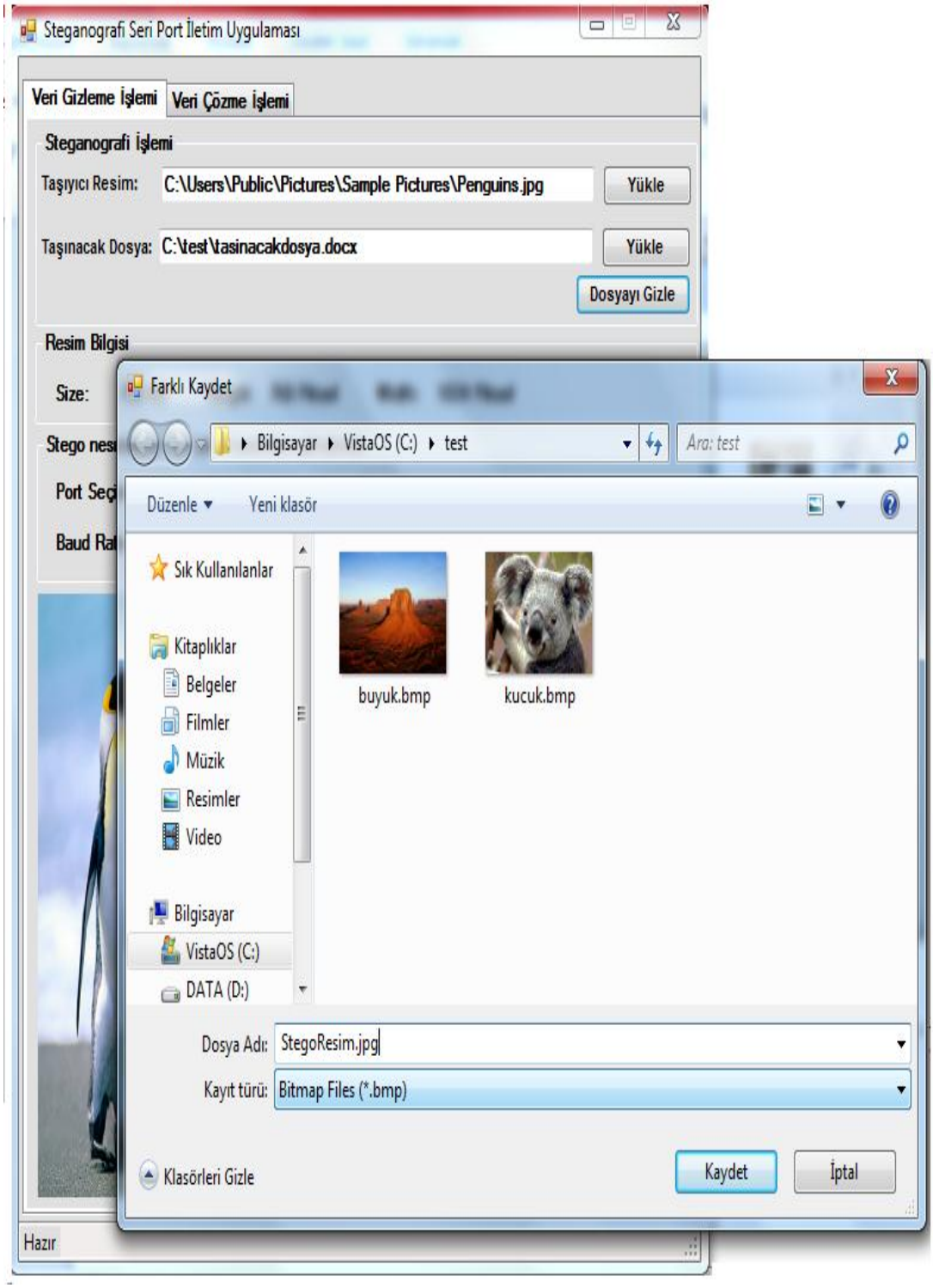
Şekil 1 Taşıyıcı resim seçimi

2. Taşınacak dosya da aynı şekilde “Yükle” butonuna basılarak açılan Open Dialog kutusundan seçilir (Şekil 2).



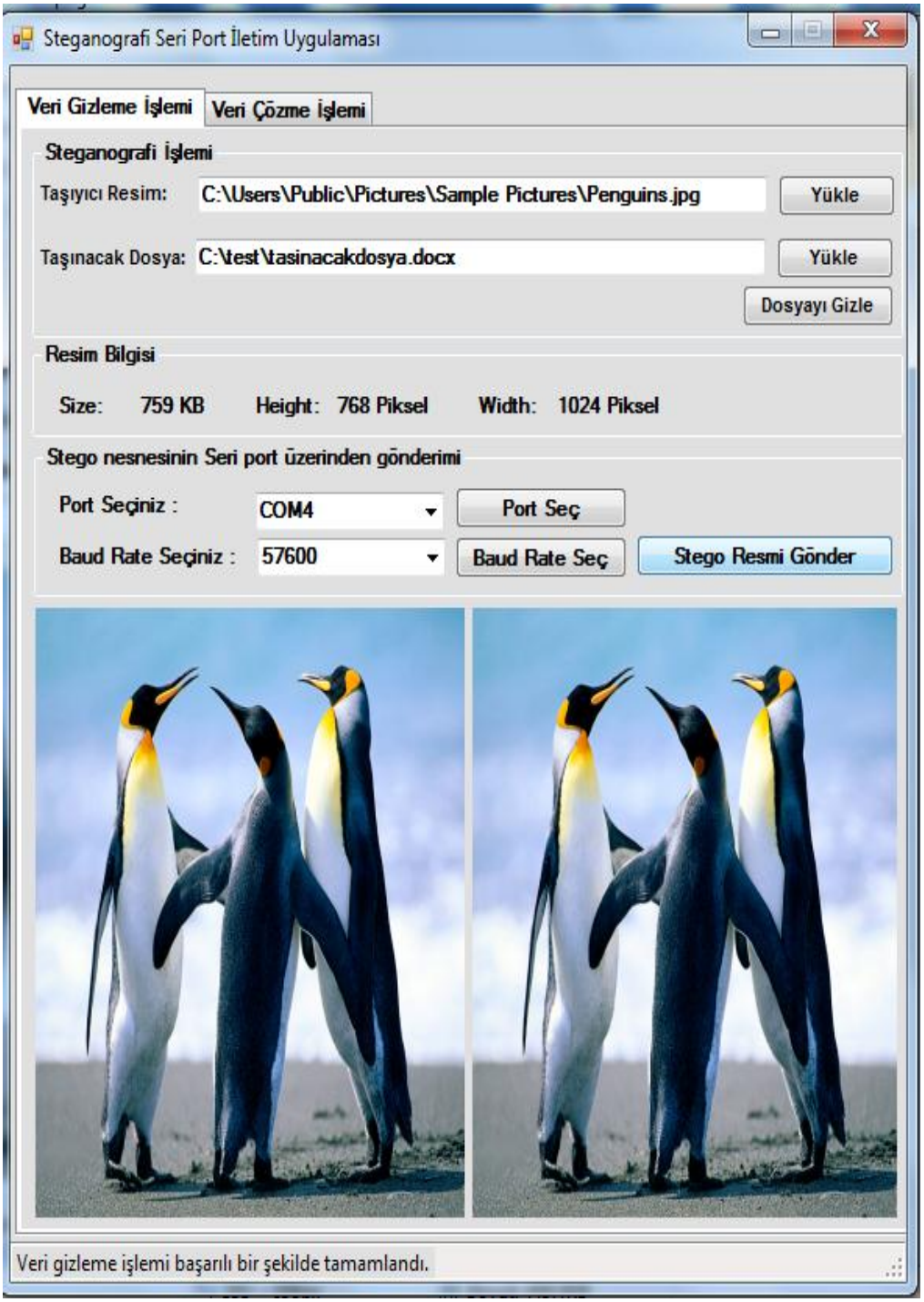
Şekil 2 Taşınacak dosya seçimi

3. Taşıyıcı resim ve taşınacak dosya seçildikten sonra “Dosyayı Gizle” butonuna basılır ve dosyanın kaydedileceği yer ve adı seçilir (Şekil 3).



Şekil 3 Stego resim kaydetme

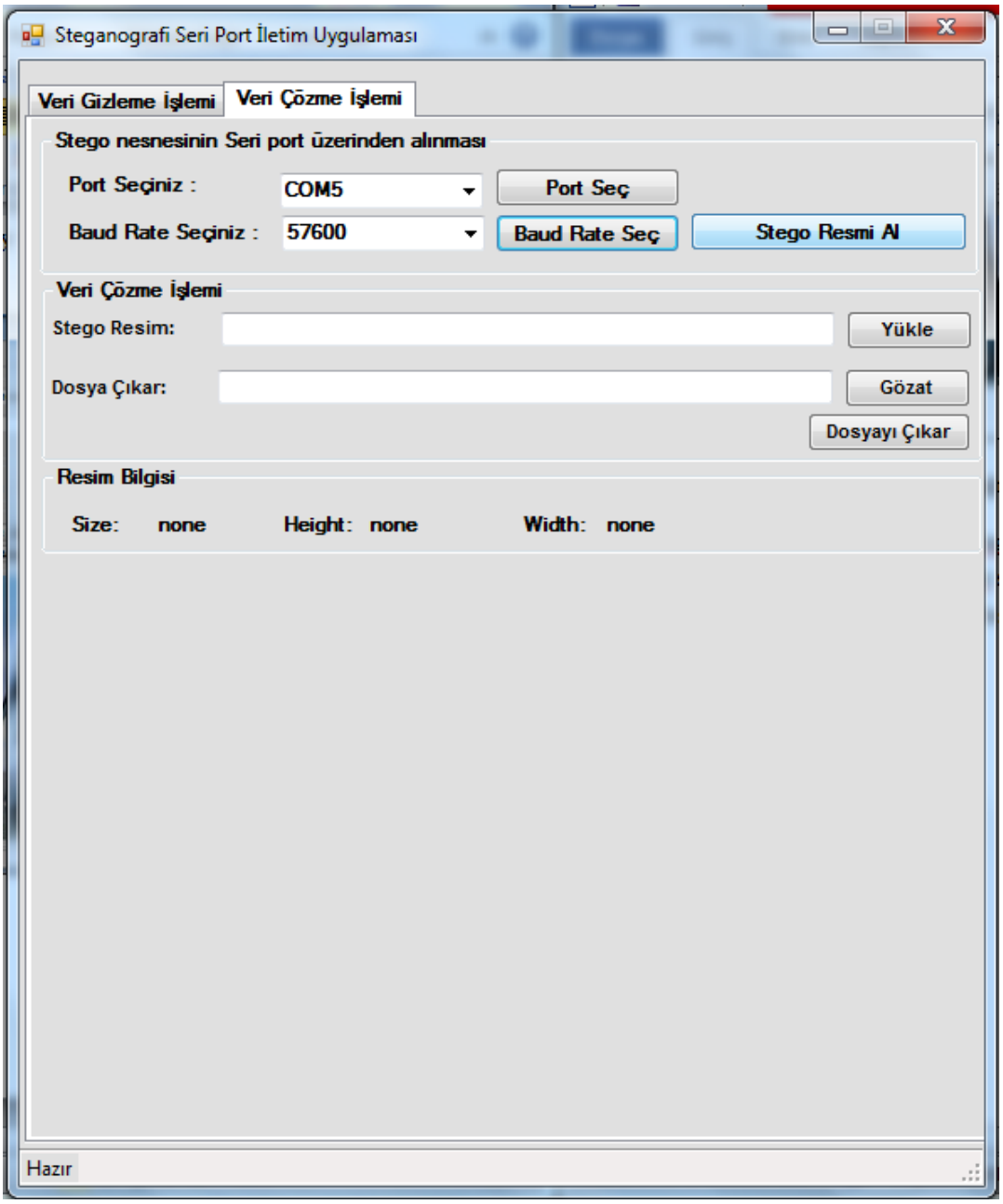
4. Veri gizleme işlemi tamamlandıktan sonra stego resmi seri port üzerinden göndermek için “Port” ve “Baud Rate” seçimi yapılır. “Stego Resmi Gönder” butonuna basılarak veri OTİS üzerinden gönderilir (Şekil 4).



Şekil 4 Stego resmin gönderilmesi

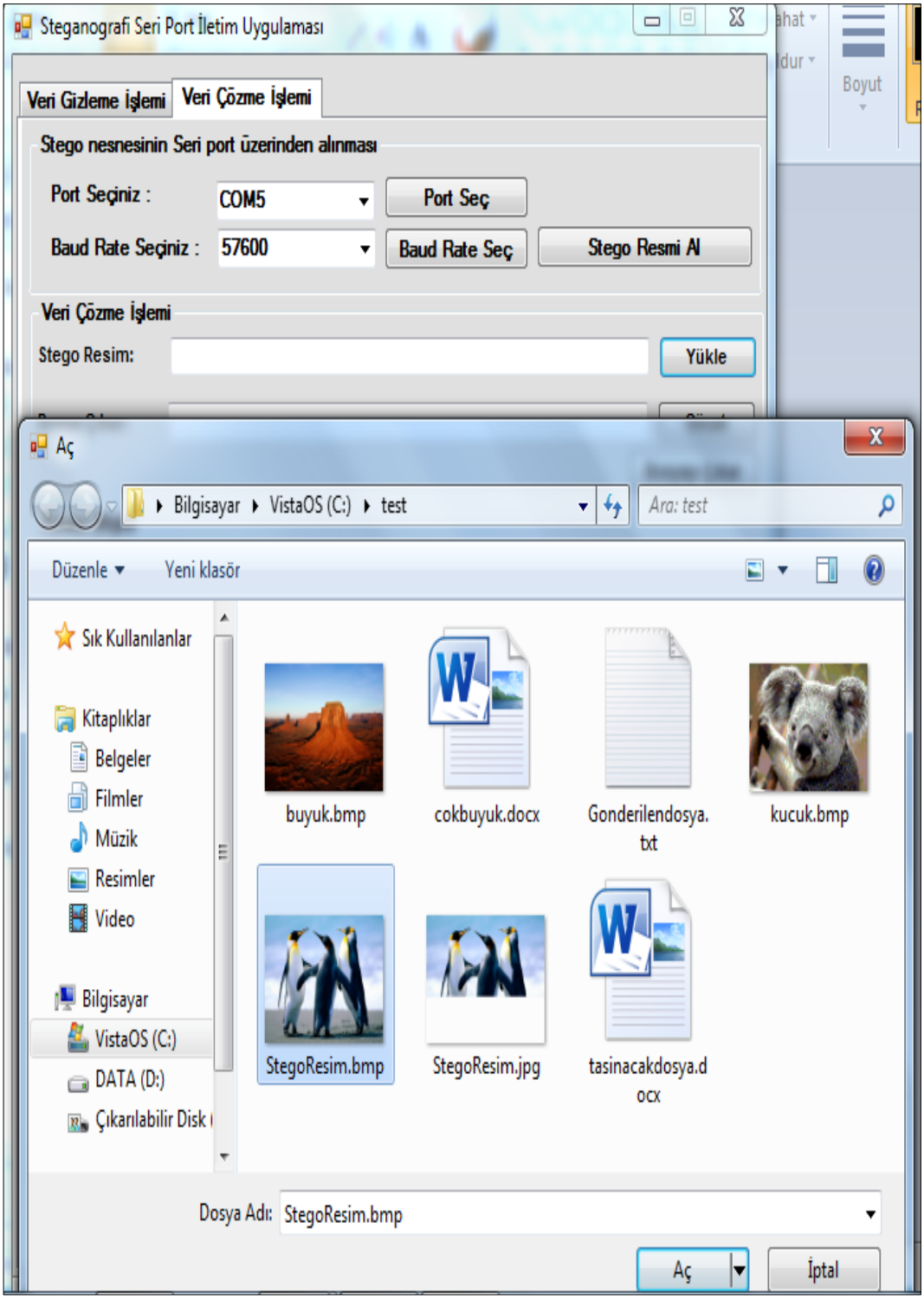
EK 6 Yazılım Veri Çözme Adımları

1. Verici tarafında gönderilen stego resmin seri port OTİS üzerinden alınması için seri port ve baudrate seçimi yapılarak "Stego Resmi Al" butonuna basılır. Alınan veri varsayılan olarak "C:/test" dizini içerisine iletilmektedir (Şekil 1).



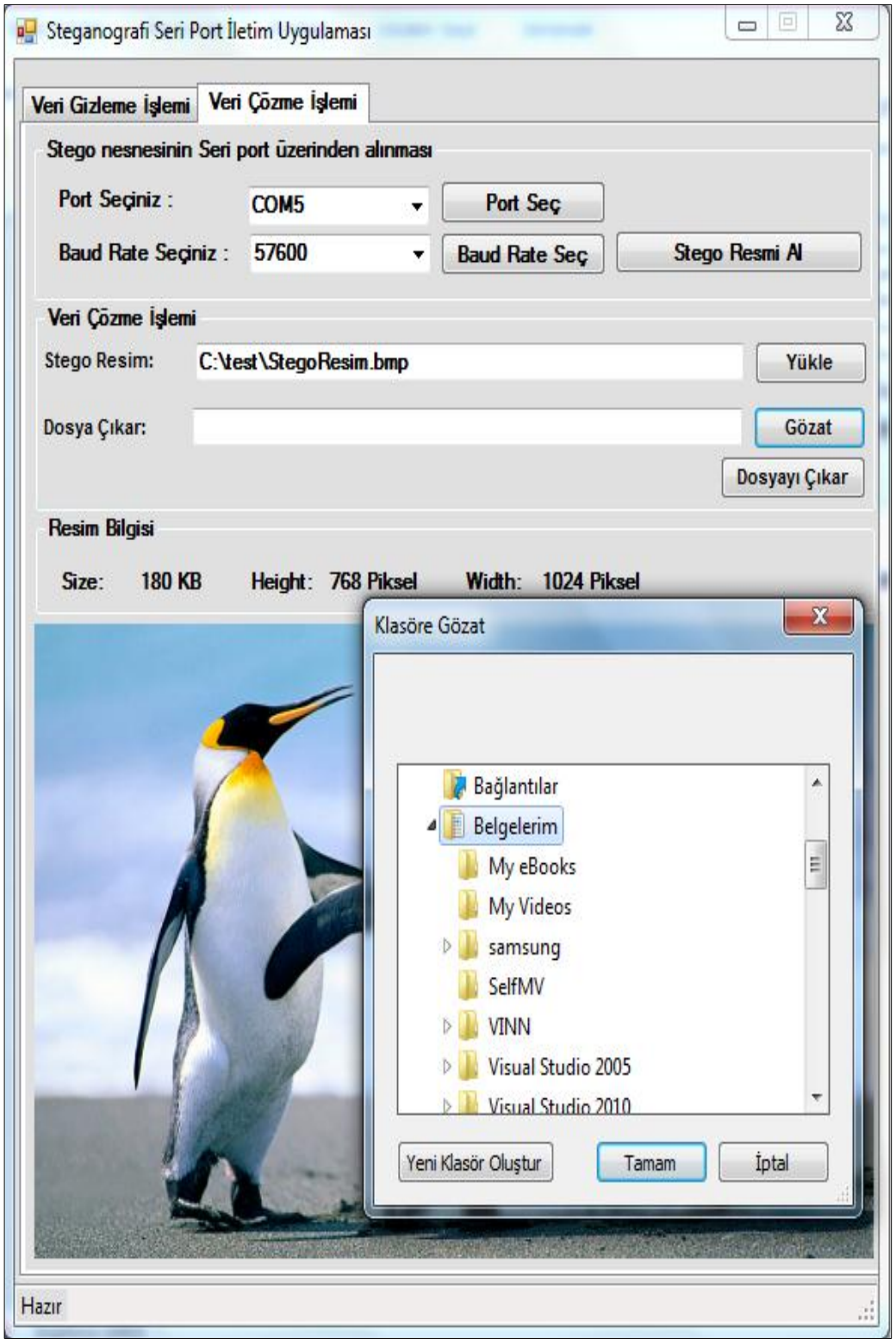
Şekil 1 Stego resmin alınması

2. Seri port üzerinden alınan stego resmi çözmek için “Yükle” butonuna basılır. Açılan kutudan stego resmin seçilmesi sağlanır (Şekil 2).



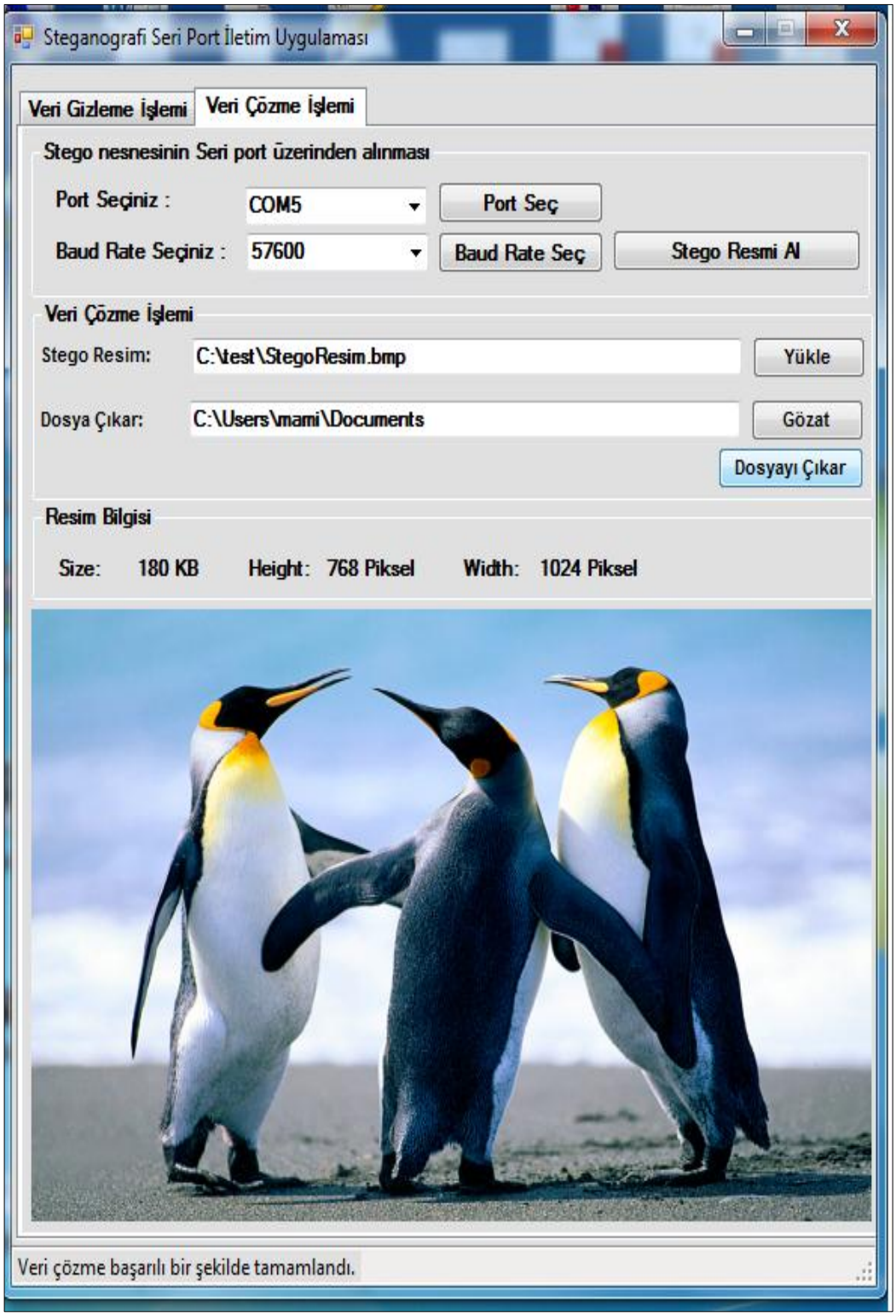
Şekil 2 Stego resmin seçilmesi

3. Stego resim içerisinde taşınan dosyanın çıkarılacağı yer seçilir (Şekil 3).



Şekil 3 Taşınan dosyanın kaydedilmesi

4. Taşınan dosyayı çıkarmak için “Dosyayı Çıkar” butonuna basılır (Şekil 4).



Şekil 4 Taşınan dosyanın stego resim içinden çıkartılması

EK 7 PSNR Hesaplama Kodu (MATLAB)

```
clc;
clear;

imgeOrig=double(imread(‘'));
imgeHide1=double(imread(‘'));
%%% imgenin boyutları alınmaktadır...
[X Y Z]=size(imgeOrig);
MAX=255;
Boyut=X*Y;
toplam=0;
disp('Islem devam ediyor. Lutfen bekleyiniz...');
for i=1:1:X*Y*Z
   toplam=toplam+((imgeOrig(i)-imgeHide1(i))^2);
end
MSE= toplam/Boyut;
PSNR1=10*log10((MAX^2)/MSE);
disp('PSNR 1..:');
disp(PSNR1);
```

ÖZGEÇMİŞ

Adı Soyadı: Muharrem AYYILDIZ

Doğum Yeri: Siirt

Doğum Tarihi: 29.10.1982

Medeni Hali: Evli

Yabancı Dili: İngilizce

Eğitim Durumu (Kurum ve Yıl)

Lise : Siirt Lisesi (1995-1999)

Lisans : Fırat Üniversitesi Mühendislik Fakültesi
Elektrik Elektronik Mühendisliği (1999-2003)
Anadolu Üniversitesi İşletme Fakültesi
İşletme Bölümü (2007-2012)

Yüksek Lisans: Ankara Üniversitesi Fen Bilimleri Enstitüsü
Elektrik-Elektronik Mühendisliği (Şubat 2009- Eylül 2013)