KOCAELİ ÜNİVERSİTESİ * FEN BİLİMLERİ ENSTİTÜSÜ

SAYISAL SES İÇERİSİNDE GİZLİ VERİ TRANSFERİNİN KABLOSUZ ORTAMDA GERÇEKLEŞTİRİLMESİ

YÜKSEK LİSANS TEZİ

Yıldıray YALMAN

Ana Bilim Dalı: Elektronik ve Bilgisayar Eğitimi

Danışman: Doç. Dr. İsmail ERTÜRK

KOCAELİ, 2007

KOCAELİ ÜNİVERSİTESİ * FEN BİLİMLERİ ENSTİTÜSÜ

SAYISAL SES İÇERİSİNDE GİZLİ VERİ TRANSFERİNİN KABLOSUZ ORTAMDA GERÇEKLEŞTİRİLMESİ

YÜKSEK LİSANS TEZİ

Yıldıray YALMAN

Tezin Enstitüye Verildiği Tarih: 28.03.2007

Tezin Savunulduğu Tarih: 09.05.2007

Tez Danışmanı	Üye	Üye
Doç.Dr.İsmail ERTÜRK	Yrd.Doç.Dr.Celal ÇEKEN	Yrd.Doç.Dr.A.Turan ÖZCERİT
(.....)	(.....)	(.....)

KOCAELİ, 2007

ÖNSÖZ VE TEŞEKKÜR

Kablosuz haberleşmede veri gizliliğinin ön plana çıktığı günümüzde, veri gizleme teknikleri bilgi güvenliği konusunda sunduğu yaklaşımlarla önemini giderek arttırmaktadır. “Stenografi” (Steganography) yöntemleri yazılımlarla desteklenmekte ve veri gizliliği için güçlü yazılımlar oluşturulmaktadır. Bu noktadan hareketle, gerçek zamanlı ses haberleşmesinde, gömülü gizli veri/dosya gönderilmesi yönünde tez çalışmaları yapılmış olup, geliştirilen yazılımlar sunulmaktadır.

Yüksek lisans eğitimim süresince değerli birikimlerini bana aktaran, tezimin başlangıcından bitimine kadar her aşamasında sorunlarımı dinleyen ve çalışmalarıma yön veren ve değerli zamanını sorunlarımın çözümüne ayıran tez danışmanım sayın Doç.Dr. İsmail ERTÜRK’e, tez ile ilgili araştırmaların yapılmasından, uygulamaların ve tezin yazılmasına kadar yardımlarını ve birikimlerini benimle paylaşan değerli arkadaşlarım Cemil ASLAN ve Tuncay AKBAL’a teşekkürlerimi sunarım.

Bugünlere gelmemi sağlayan anneme, babama ve huzurlu bir çalışma ortamı sağlayarak her türlü desteği bana gösteren değerli eşime teşekkür ederim.

İÇİNDEKİLER

ŞEKİLLER DİZİNİ

TABLOLAR DİZİNİ

SİMGELER

C : Mesaj iletim süresi (s)
D : Mesajın varma sınır değeri (s)
d : Mesajın yük büyüklüğü (bayt)
R : En kötü durum gecikme süresi (s)
T : Mesajın üretim aralık zamanı (s)
t : Mesajın kuyruğa atılmasından veri yolu erişimini kazanmasına kadar geçen süre (s)
k_{m_i} : i. ses çerçevesine eklenecek modüle gizli anahtar işareti
k : Gizli anahtar işareti
w_j : j. gömülecek veri (damga) bilgisi
L : Gömülen verinin uzunluğu
f() : Doğrusal olmayan veri gömme fonksiyonu
s_i : Orijinal i. ses çerçevesi
$s_{i_{WM}}$: Veri gömülü olan i. ses çerçevesi
g() : Doğrusal olmayan gömülü veriyi çözme algoritması
$\hat{w}_j$: Öngörü ile çözülen j. gömülecek veri biti
a : Kuantalama aralığı
Q : Kuanta seviyesi sayısı
n : İşaretin kodlandığı bit sayısı
x(t) : Mesaj işareti
$x_q(t)$: Kuantalanmış örnek işareti
A_{max} : Maksimum genlik
A_{min} : Minumum genlik
f_N : Örnekleme frekansı

Kısaltmalar

ACK	: Acknowledgement (Alındı Bilgisi)
AP	: Access Point (Erişim Noktası)
ARPANet	: Advanced Research Project Agency Network
ASCII	: American Standard Code for Information Interchange
BSS	: Basic Service Set (Temel Servis Seti)
CAN	: Controller Area Network
CCK	: Complementary Code Keying
CRC	: Cyclic Redundancy Check
CSMA/CD	: Carrier Sense Multiple Access with Collision Detection
CTS	: Clear to Send (Göndermeye Açık)
DAVIC	: The Digital Audio Visual Council
DCF	: Distrubuted Coordination Function
DIFS	: Distrubuted Coordination Function Inter Frame Space
DQPSK	: Differantial Quadrature Phase Shift Keying
DS	: Digital Signal (Sayısal Sinyal)
DSSS	: Direct Sequence Spread Spectrum
DVD	: Digital Versatile Disc
EBCDIC	: Extended Binary Coded Decimal Interchange Code
EIFS	: Extended Inter Frame Space
FHSS	: Frequency Hopping Spread Spectrum
HiperLAN	: High Performance Radio Local Area Network
IAPP	: Inter Access Point Protocol
IBM	: International Business Machines Company
IFS	: Inter Frame Space (Çerçeveler arası boşluk)
ISO	: International Standards Organization
ISM	: Industries, Scientific, Medical
ITU	: International Telecommunications Union
KLAN	: Kablosuz Yerel Alan Ağları
LAN	: Local Area Network (Yerel Alan Ağı)
LSB	: Least Significant Bit (En Az Değerlikli Bit)
MAC	: Medium Access Protocol (Ortam Erişim Kontrolü)
MPDU	: MAC Protocol Data Unit
MPEG	: Moving Picture Experts Group
OFDM	: Orthagonal Frequency Division Multiplexing
PAM	: Pulse Amplitude Modulation (Darbe Genlik Modülasyonu)
PCF	: Point Coordination Function
PCM	: Pulse Code Modulation (Darbe Kod Modülasyonu)
PLCP	: Physical Layer Convergence Procedure
PMD	: Physical Medium Dependent
RF	: Radyo Frekansı
RGB	: Red Green Blue (Kırmızı Yeşil Mavi)
RIFF	: Resource Interface File Format
RTS	: Request to Sent (Gönderme İstemi)

SDMI	: The Secure Digital Music Initiative
SIFS	: Short Inter Frame Space
TCP/IP	: Transfer Control Protocol / Internet Protocol
U-NII	: Unlicensed National Information Infrastructure
WIPO	: World Intellectual Property Organization
WECA	: Wireless Ethernet Company Alliance
WLAN	: Wireless Local Area Network
SSGM	: Sayısal Ses İçerisinde Gizli Metin
SSGD	: Sayısal Ses İçerisinde Gizli Dosya
Gömü Verisi (Dosyası)	: Gönderilmek istenen gizli veri/dosya
Örtü Verisi (Dosyası)	: Gömü verisinin/dosyasının gömüleceği taşıyıcı veri/dosya
Örtülü Veri (Dosya)	: İçerisinde gömü verisi/dosyası bulunan örtü verisi/dosyası

SAYISAL SES İÇERİSİNDE GİZLİ VERİ TRANSFERİNİN KABLOSUZ ORTAMDA GERÇEKLEŞTİRİLMESİ

Yıldıray YALMAN

Anahtar Kelimeler: Sayısal Ses, Veri Gizleme, Stenografi

Özet: Günümüzde veri gizleme (stenografi) teknikleri özellikle kablosuz iletişim sistemleri içerisinde giderek artan bir öneme sahip olmaktadır. Çoklu ortam ve bilgi güvenliği uygulamaları gibi güncel gereksinimler ile veri gizleme üzerine yapılan çalışmalar da yoğun bir talep ve ilgi görmektedir.

Bu tezde sunulan projenin temel amacı; sayısal ses içerisinde gizli veri transferinin kablosuz ortamda gerçekleştirilmesidir. Bu nedenle iki uygulama geliştirilmiştir. Birinci uygulama kablosuz ortamda transfer edilen sayısal ses içerisine metin gömme, ikincisi ise kablosuz ortamda transfer edilen sayısal ses içerisine veri/dosya gömme uygulamasıdır. Buna ek olarak her iki uygulamada gerçek zamanlı ses haberleşmesi yapmaktadır.

Tez çalışmalarında donanım aracı olarak kablosuz haberleşme yapabilen iki adet değişik özelliklere sahip bilgisayar ve bir adet Erişim Noktası (Access Point), yazılım aracı olarak ise Borland Delphi 7.0 programlama dili kullanılmaktadır.

Örnek çalışmaların sonucunda, elde edilen sonuçlar sunularak başarım değerlendirmeleri yapılmaktadır.

DESIGN AND IMPLEMENTATION OF HIDDEN DATA TRANSFER WITHIN DIGITAL VOICE FOR WIRELESS COMMUNICATIONS

Yıldıray YALMAN

Keywords: Digital Voice, Data Hiding, Steganography

Abstract: Techniques for information hiding (Steganography) have nowadays become increasingly more sophisticated and widespread. Researches on information embedding, have received considerable attention for a decade due to its potential applications in multimedia and information security.

The main objective of this research presented is to design and implement hidden data transfer within digital voice for wireless communications. For this reason, two application programmes have been developed. The first application is used for text embedding or data hiding within digital voice, while the other is used for file embedding within digital voice. Furthermore, both applications enable a conventional wireless realtime voice communication.

In this research, studies two different computers and an access point are utilized. These computers are equiped with wireless communication tools and software components. The softwares are developed with Borland Delphi 7.0 programming language.

Examples of application results of the softwares developed are presented and their performances are evaluated.

1.GİRİŞ

Temeli antik çağlara kadar dayanan gizli haberleşme, teknoloji değişip geliştikçe şekil ve yöntem açısından da faklılıklar göstermektedir. Bununla birlikte önemini devamlı korumaktadır. Gizliliğin öneminin had safhaya ulaştığı uygulamalarda; gizli bilgilerin, üçüncü kişilerin eline geçmeden ilgili hedefe gönderilmesi amaçlanır.

Veri gizleme aynı zamanda "stenografi" (steganography) adını almaktadır ve kriptografi ile yakından ilişkilidir. Kriptografinin amacı, mesajları anlaşılmaz hale getirerek gizli anahtara sahip olmayan yetkisiz kişilerin mesajı yeniden elde ederek orijinal haline getirmesini önlemektir. Bazen şifreli mesajları değiştirmek yerine, haberleşmenin maskelenmesi yoluyla güvenlik ve gizliliğin elde edilmesi durumu arzu edilebilir. Bu problem stenografiyi ön plana çıkarmaktadır. Tarihte ilk stenografik teknikler özel mürekkep veya kimyasal maddeler kullanarak görünmeyen yazılar elde etmeyi içermektedir. O dönemde metin içinde gizli mesajlar oldukça yaygındır. Kelime veya cümlelerin ilk harflerini referans alarak, bazı masum görünümlü kelimelerle gizli bir mesaj iletilmekteydi. Günümüzde veriyi gizleme amacıyla, değişik taşıyıcıları belirli oranda kullanmak doğal görünümü değiştirmemektedir. Dijital resimler, videolar ve ses işaretleri bu amaç için idealdir.

Günümüzdeki yaygın şekliyle sayısal veri gizleme ile ilgili en önemli çalışma ilk olarak 1954 yılında; Emil Hembrooke'un sahip olduğu Muzak şirketinin, müzik kayıtlarına sahiplik bilgisini içeren kod yerleştirmek için almış olduğu patenttir (Cox ve diğ., 2000, 2002).

80'li yıllarda İngiltere Başbakanı Margaret Thatcher'in kabinesinde kabine içi bilgileri sızdıran bakanın kim olduğunun tespit edilmesi amacı ile kelime işlem programı her bakan için ayrı ayrı tanımlayıcı bilgi ekleyecek şekilde programlanmış ve sorumlu bakanın kim olduğu ortaya çıkarılmıştır (Anderson ve diğ., 1998).

En basit ve en yaygın stenografi tekniği "En düşük değerlikli bit"e (Least Significant Bit embedding; LSB) gömme tekniğidir. Burada önerilen işlem genellikle dijital resimler veya ses dosyaları içerisindeki belirli bit bloklarının en düşük değerlikli bitini, gürültü (orijinal dosya açısından gürültü şeklinde beliren bu durum aslında gizli veriyi ifade eder) tarafından maskelenerek değiştirilmesidir. Aslında renkli resim kullanımında, mesaj gizleme için daha fazla oda/piksel mevcuttur; çünkü, her bir piksel kırmızı, yeşil ve maviden oluşan üçlü bir birleşimdir. Yine iki veya daha fazla "en düşük değerlikli bit" yer değiştirilerek her bir pikselin veri gizleme kapasitesi artırılır; ancak, aynı zamanda istatistiksel olarak çözünebilirlik riski de arttırılmış olur. Böylece her bir özel stenografik tekniğin güvenli çalışması önemlidir ve neden güvenli olduğu tartışılır. Hatta basit en düşük değerlikli bit, belirli durumlar altında kodlanarak saptanabilir değişiklikler ortaya koymaktadır. Resim veya ses gürültüsüne bağlı değişiklikler ile karmaşık şüpheler oluşturularak, resmin veya elde bulunan sayısal ses bilgisinin herhangi bir istatistiksel model ile kolayca anlaşılamaması başarılı bir şekilde sağlanır.

Bu tez çalışmasında, iki bilgisayar arasında kablosuz ve gerçek zamanlı olarak ses iletişimi yapılırken, sayısal ses verilerine kullanıcının istediği bilgilerin (metin ya da dosya) gömülerek gönderilmesi sağlanmaktadır. Bu işlemin sonucunda ses verilerini alan bilgisayarda örtülü veri içerisinden gömü verisinin (dosyasının) ayırt edilmesi uygulaması da yapılmaktadır.

1.1. Literatürde Yapılan Çalışmaların Özetleri

Muzak şirketinin, 1954 yılında müzik kayıtları içerisine sahiplik bilgisini içeren kod yerleştirmek için almış olduğu patentle birlikte, telif haklarının korunmasına yönelik ses bilgileri içerisine veri gömme tekniği üzerine çalışmalar yoğunlaşmıştır. Bu durumun sadece kayıtlı ses verilerine değil, gerçek zamanlı ses verilerine de uygulanabileceği tartışılmaktadır. Örneğin hava trafik kontrolünde daha güvenli iletişim için ses bilgileri içerisine veri gömülmesinden bahsedilmekte ve bu da Data in Voice (DiV) olarak adlandırılmaktadır (Sajatovic ve diğ., 2003).

1990'ların başında imge damgalama kavramı gelişmiş; Tanaka ve arkadaşları faks gibi ikili imgelerin korunması kavramını ortaya atmışlardır (Tanaka ve diğ., 1989, 1990). 1993 yılında Tirkel ve arkadaşları gerçekleştirdikleri veri gömme tekniğine, daha sonra "watermark" olarak birleştirilecek olan "water mark" ismini vermişlerdir (Hartung ve diğ., 1999).

Özellikle müzik dosyaları için telif haklarının korunması amacıyla "Audio Watermarking" adı verilen çalışmalar genel olarak gömülü verilerin sezilemezliği üzerine yoğunlaşmıştır (Kim ve diğ., 2004).

Dünya çapında telif haklarının korunması ve düzenlenmesi ile ilgili çalışmalar yapan ve hükümetler üstü bir kuruluş olan WIPO (World Intellectual Property Organization) sayısal veri gömme sistemlerinin yasal alanlarıyla ilgili çalışmalarını sürdürmektedir (Delaigle, 2000).

Stenografinin uygulandığı taşıyıcı verilerin, süzülerek içerisindeki gizli verinin elde edilmesi işlemi steganaliz olarak adlandırılır. Cheng ve arkadaşları elektronik metin resimleri için ilgili resim içerisinde veri gömülü olup olmadığını sezen bir steganaliz tekniği ileri sürmüşlerdir (Cheng ve diğ., 2005).

Stenografi uygulamalarının yapılabilmesi için mutlaka taşıyıcı veri kullanılması gerekmektedir. Bunlar ses, resim, video vb. olabilir. Bunlardan birine örnek olarak, Adlı ve Nakao ".midi" uzantılı dosyalar için 3 farklı stenografi algoritması geliştirmişlerdir (Adlı, Nakao, 2005). Xu ve arkadaşları da sıkıştırılmış video görüntülerine stenografi uygulama algoritması önermişlerdir (Xu ve diğ., 2006).

1.2. Tez Çalışmasının Amacı ve Motivasyonu

II. Dünya Savaşı sırasında Almanlar bir mikro-noktalama aleti geliştirmişlerdir. Bu alet aracılığıyla gizli bir mesaj, resimleme tekniğinden faydalanılarak, örneğin "i" harfindeki veya başka bir noktalama işaretindeki noktanın boyutuna indirgenip bir kağıda işlenebilmiştir. Mesajı alan kişi tarafından ise tüm bu noktalar

birleştirildiğinde gizli mesaj ortaya çıkarılmaktadır. Bu aletler, teknik çizimleri de kapsayan büyük miktarda yazılı veri aktarımını gerçekleştirebilecek potansiyele sahiptir ve bütün bunları da bilgileri çok etkili bir şekilde saklı tutarak yapabilmektedir. Neticede bu sanat günümüzde; insanlığa, bilgilerin gizlice iletilmesi konusunda çağlar boyu yardımı dokunmuş bir bilime dönüşmüştür. Modern stenografi teknik olarak, bir veriyi (mesaj) bir nesnenin içine gizli biçimde yerleştirmeyi esas almaktadır. Öyle ki, sadece belirlenen alıcı, kendisine iletilmek istenen mesajı nesneden seçebilmekte ve diğer gözlemcilerin o nesnenin içindeki mesajın varlığından haberleri olmamaktadır. Kriptografinin bir kolu olarak görülen stenografi, bu önemli özelliğiyle Kriptografiyi bir adım ileri taşımaktadır. Kriptografi güvenilirliği sağlasa da bir bakıma mesajın gizliliğini sağlayamamaktadır. Kriptografik uygulamalarda bilgi sadece gönderen ve alanın anlayabileceği şekilde şifrelenirken, stenografik uygulamalarda bilgi sadece gönderen ve alanın varlığını bildiği şekilde saklanmakta, bazen de şifrelenip ekstra koruma sağlanmaktadır.

11 Eylül'de yaşanan trajik olaylarda teröristlerin ileri teknolojileri kullandığı saptandıktan sonra, stenografi oldukça popüler hale gelmiştir. Çünkü teröristlerin ECHELON tipi sistemleri devre dışı bırakarak aralarında gizlice haberleşmek için bu teknolojiden yararlandıkları söylentisi tüm dünyada yayılmıştır. Ve bu konu üzerinde 2000'li yılların başından itibaren yoğun çalışmalar yapılmaktadır.

Yukarıdaki bilgiler ve gelişmeler de göz önünde bulundurulduğunda, özellikle internet üzerinden yapılan haberleşmelerde zararsız görülen dosyaların (metin, resim, ses, video vb.) içerisine gizli bilgilerin gömülebileceği ya da yerel bir ağda kablolu veya kablosuz şekilde gerçekleştirilen haberleşme ve dosya alışverişlerinde stenografinin kullanılabileceği gerçeği bu tez çalışmasının temel motivasyonunu oluşturmaktadır.

Literatürde sunulan çalışmalarda, genel olarak boyutu belli kayıtlı dosyalar üzerinde veri gömme uygulamaları yapılmaktadır. Bu tezde sunulan çalışmada ise gerçek zamanlı olarak elde edilen sayısal ses verileri, bir veri gömme algoritması içerisinden geçirilerek hedef noktaya kablosuz ortamda gönderilmekte ve bu durumdan haberdar olan bir alıcı yazılım yardımı ile gömü verileri ayrıştırılarak tekrar elde edilmektedir.

1.3. Tez Organizasyonu

Yapılan çalışmaların sunulduğu bu tez 7 ana bölümden oluşmaktadır.

Bölüm 1 Giriş: Bu bölümde tez çalışmasına konu olan problemin tanımı, çalışmanın amacı, literatürdeki ilgili problemle ilgili yapılan çalışmaların özetleri ve tez çalışmasının amacı ve motivasyonu hakkında bilgi sunulmaktadır.

Bölüm 2 Kablosuz Yerel Alan Ağları: Kablosuz ağların avantajları ve kullanım alanlarından bahsedilmekte ve tez çalışmasının bir parçası olan IEEE 802.11 kablosuz yerel alan ağlarının protokol mimarisi, standartları, çerçeve biçimleri ve ortam erişim mekanizmasına ayrıntılı olarak değinilmektedir.

Bölüm 3 Veri Gizleme ve Gömme Teknikleri: Kriptoloji (Cryptology), Damgalama (Watermarking) ve Stenografi (Steganography) terimlerinin tanımlamaları yapılmaktadır. Stenografik teknikler hakkında bilgi verilmektedir. Ayrıca stenografide sıkça rastlanan bir yöntem olan steganaliz anlatılmaktadır.

Bölüm 4 Metinlerin ve Analog Ses Sinyallerinin Sayısal Veriye Çevrilmesi: Metin kodlama standartları ASCII ve EBCDIC anlatılmakta ve tablolar halinde karakterlerin sayısal karşılıkları verilmektedir. Aynı zamanda ilgili alt bölümde analog ses bilgisinin örneklenerek sayısal ses verisi haline getirilmesi süreci anlatılmakta ve bilgisayarda PCM ses verisi formatının detayları incelenmektedir.

Bölüm 5 Sayısal Ses İçerisinde Gizli Veri Transferinin Kablosuz Ortamda Gerçekleştirilmesi: Geliştirilen uygulamaların kullanıcı arayüzleri, çalışma prensipleri anlatılmakta ve akış diyagramları verilmektedir. Ayrıca programların nasıl kullanılacağı hakkında bilgi sunulmaktadır.

Bölüm 6 Geliştirilen Yazılımların Uygulama Örnekleri: Geliştirilen yazılımların uygulama başarımları ve çalışmalar sırasında karşılaşılan problemler hakkında tespitler vurgulanmaktadır. Buna ek olarak farklı boyut ve tipteki dosyaların

gönderilme ve alınma sürelerine ilişkin sonuçlar tablolar ve grafikler yardımıyla karşılaştırılmaktadır.

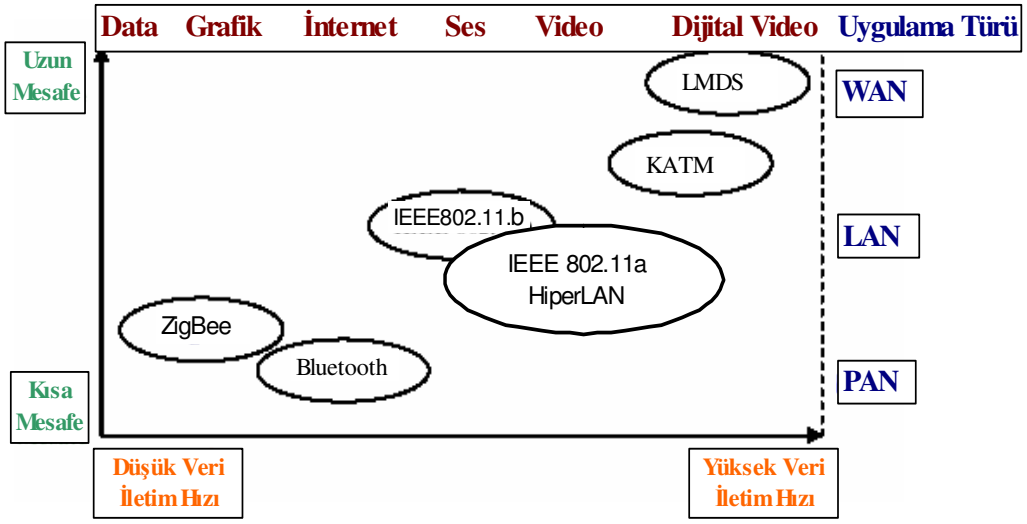
Bölüm 7 Tartışma ve Değerlendirmeler: Karşılaşılan problemlerin aşılabilmesi için çözüm önerileri sunulmakta, ilgili çalışmaların maliyet-etkin hale getirilebilmesi için yapılabilecekler hakkında önerilerde bulunulmakta ve bundan sonra yapılabilecek çalışmalar önerilmektedir.

2. KABLOSUZ YEREL ALAN AĞLARI

2.1. Giriş

Kablosuz ağlar, haberleşmek için radyo frekans (RF) teknolojilerini kullanan terminallerin oluşturduğu sistemlerdir. Bunlar kablo kullanan eşleniklerinden farklı olarak kurulum kolaylığı, ölçeklenebilirlik, hareketlilik, üretkenlik, ileriye yönelik maliyet kazancı ve mevcut ağ yapısını genişletme gibi bir çok avantajlar sunmaktadır. Bunlara karşın, kablosuz iletim ortamının doğasından kaynaklanan yüksek bit hata oranı ve sınırlı bant genişliği gibi önemli dezavantajlara da sahiptir (Bayılmış, 2003, Çeken, 2004).

Farklı uygulamalar ve ihtiyaçları karşılamak üzere bir çok kablosuz ağ teknolojisi geliştirilmiş ve geliştirilmektedir. Şekil 2.1'de günümüzde mevcut ve geliştirilmekte olan kablosuz ağ standartlarının, destekledikleri uygulama türlerine, veri iletim hızlarına, kapsama alanlarının büyüklüğüne ve coğrafik ağ yapılarına göre yapılan sınıflandırmaları özetlemektedir (Bayılmış ve diğ., 2004a).



Şekil 2.1: Kablosuz ağlar ve uygulamadaki yerleri

IEEE 802.11 Kablosuz Yerel Alan Ağları (KLAN), kablolama sınırlamaları olmaksızın Ethernet ve Token Ring gibi geleneksel LAN teknolojilerinin tüm özelliklerini ve yararlarını sağlar. Bu nedenle mevcut yerel alan ağlarının kablosuz ortam üzerinden haberleşen şekli olan kablosuz yerel alan ağları hava üzerinden Ethernet (Ethernet on air) olarak da adlandırılır (Levillain, 2002).

Bu bölümde tez çalışmasının bir parçası olan ve yaygın olarak kullanılan IEEE 802.11 Kablosuz Yerel Alan Ağları (Wireless Local Area Network) incelenmektedir. Tez çalışmasının amaçlarından birisi de kablosuz olarak ses iletişiminin gerçekleştirilmesidir. Bu amaçla bu bölümde Kablosuz ağlar ile ilgili temel bilgiler verilmektedir.

2.2. Kablosuz Yerel Alan Ağlarının Avantajları

Kablosuz ağların avantajları aşağıdaki şekilde sıralanabilir:

- Hareketlilik: Kablosuz ağlar, ağ kullanıcılarına kapsama alanı içerisinde kalmak şartı ile hangi noktada olurlarsa olsunlar, hareket halinde dahi gerçek zamanlı bilgi iletişimi imkanı sağlar.
- Kurulum hızı ve basitliği: Kablosuz ağ sistemlerinin kurulumu hızlı ve kolaydır. İletişim hava üzerinden radyo dalgaları ile sağlandığından klasik LAN'lardaki gibi duvar ve tavanlardan kablo çekme zorunluluğu yoktur.
- Kurulum esnekliği: Kablosuz ağ teknolojisi kablolu LAN'ların erişemeyeceği (fiziki olarak) yerlere (noktalara) ulaşımı sağlar.
- İleriye yönelik maliyet kazancı: Kablosuz ağların ilk kurulum maliyetleri nispeten kablolu bir ağdan daha fazla olmakla birlikte hayat evresi sarfiyatı çok azdır. Uzun vadeli kazançları, çok yer değiştirme gerektiren dinamik ortamlarda ortaya çıkar.
- Genişletilebilirlik: Kablosuz iletişim ortamı sayesinde dinamik bir yapıya sahip kablosuz ağlar ile kurulan sistemler kolaylıkla tekrar düzenlenebilir ve alan genişletilebilir. Aynı zamanda kurulu kablolu yapıların da genişlemesini sağlarlar. En az iki düğümün bir araya gelmesiyle oluşabileceği gibi erişim

noktası kullanarak haberleşen düğüm sayısı yüzler hatta binleri bulabilir (Gast 2002, Nicopolitidis ve diğ., 2003).

2.3. Kablosuz Yerel Alan Ağlarının Kullanım Alanları

Kablosuz yerel alan ağları, kablolu ağların kullanıldığı tüm yerlerde kullanılabilmektedir. Aşağıda KLAN'ların kullanım alanlarına birkaç örnek verilmektedir.

- Endüstri: Gerçek zamanlı kontrol, dağıtık kontrol sistemleri, otomasyon sistemleri, veri tabanı bağlantısı, kent bilgi sistemleri bağlantısı.
- Ofis ortamı: Video konferans, bilgisayar çevre birimlerinin haberleşmesi.
- Hastane: Uzaktan görüntüleme, medikal görüntüler, hasta takibi.
- Eğitim merkezleri: Bilgi erişim, uzaktan eğitim.
- Taşıtlar: Araç tanıma sistemleri, araç içi kontrol uygulamaları.

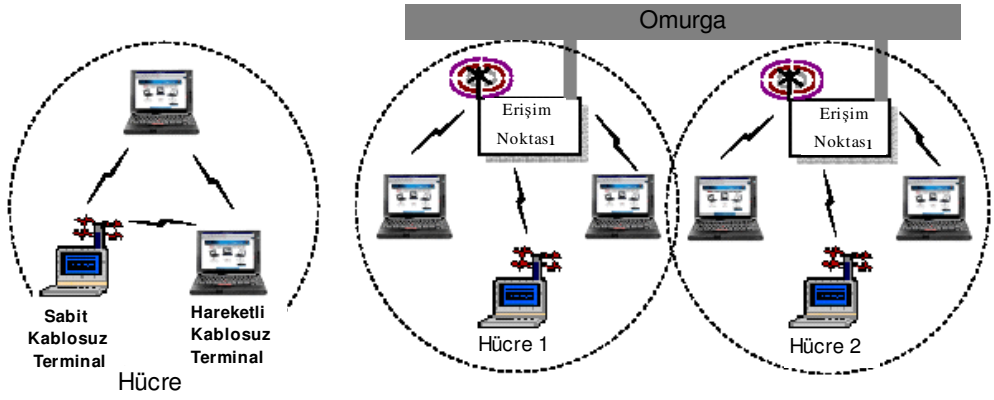
2.4. Kablosuz LAN Ağ Topolojisi

IEEE 802.11 KLAN, hücresel mimariye dayalı ağ topolojilerini destekler. İletişim ortamı hücre olarak adlandırılan küçük alanlara bölünür. Her bir hücre Temel Servis Seti (Basic Service Set, BSS) olarak adlandırılır. Kablosuz ağlar, eşe-eş ya da birebir ağ topolojisi (Ad-Hoc veya independent BSS) ve erişim noktalı ağ topolojisi (Infrastructure BSS) olmak üzere iki tür ağ topolojisini desteklemektedir.

Eşe-eş ağ, gerçekleştirilmesi hızlı ve kolay olan, geçici bağlantılar sağlamak üzere kurulan bir ağ yapısıdır. Aynı protokolü kullanan en az iki kablosuz terminalin bir araya gelmesi ile oluşur. Herhangi bir erişim noktası olmaksızın tüm kullanıcılar birbirleri ile iletişim kurarlar (Bayılmış ve diğ., 2003, 2004b, Nicopolitidis, 2003).

Erişim noktalı ağlar, yalnızca kablosuz terminallerin kendi aralarında haberleşmesine imkan veren eşe-eş ağların genişletilmesini, kurulu kablolu yerel alan ağları ile bütünleşmesini ve kablolu yerel alan ağları üzerinden sunuculara ulaşılabilmesini

sağlar. Bu yapıda hücre içerisinde iletişim koordinasyonu sağlayan erişim noktaları (Access Point, AP) kullanılır. AP'ler kablolu ve kablosuz yerel alan ağları arasında köprü görevi gördüğü gibi kablosuz yerel alan ağlarının bant genişliklerini arttırarak daha çok sayıdaki kablosuz terminalin daha uzun mesafeli haberleşmelerini de sağlar (Çeken ve diğ., 2004).



a) Eşe-eş ağ topolojisi (Ad-Hoc) b) Erişim noktalı ağ topolojisi (Infrastructure)

Şekil 2.2: KLAN topolojileri: a) Eşe-eş b) Erişim noktalı ağ

2.5. TCP/IP

TCP/IP, ilk defa ABD'de ARPANet (Advanced Research Projects Agency Network) adı altında, askeri bir proje olarak geliştirildi. Önceleri askeri amaçlı düşünülen proje, üniversiteler tarafından da kullanılmaya başlandı. Ardından ABD'nin dört bir yanında birbirinden bağımsız geliştirilen ağlar, tek bir omurga altında NSFNet olarak adlandırıldı ve ulusal boyutu aşarak dünyaya yayıldı. İnternet'in ve ağ sistemlerinin oluşup yaygınlaşması da bu döneme denk gelmektedir.

Ağ işletim sistemlerine ek olarak ağı yönetmek, denetlemek, bağlantı uyumluluğu sağlamak açısından protokol olarak adlandırılan kurallar kümesi kullanılır. TCP/IP (Transport Control Protocol/Internet Protocol) tüm dünyada en yaygın olarak kullanılan protokol kümesidir. Eğer farklı ağ işletim sistemlerine veya protokolüne sahip LAN'lar birbirine bağlamak istenirse, büyük olasılıkla TCP/IP kullanılır. Çünkü, hemen her işletim sistemi TCP/IP'ye uyumlu yazılımlara sahiptir.

TCP/IP protokolünde tüm bilgisayarlar 32 bitlik "özgün" bir IP numarasına sahip olacak şekilde adreslenirler (bunun anlamı: internete aynı anda bağlı olabilecek bilgisayar sayısının en fazla 2^{32} = 4.294.967.296 olabileceğidir). Bunu bir örnekle ele alırsak, internet üzerinde 3.559.735.317 sayısı ile adreslenmiş bir bilgisayar düşünelim. Bu sayının onaltılık sayı sistemindeki karşılığının D42D4015 olduğunu kolaylıkla hesaplayabiliriz. Bu şekilde bir gösterimin hemen hiç kimseye bir şey ifade etmeyeceği oldukça açık bir şekilde görülmektedir. Bunun yerine 32 bitlik adres, 8 bitlik adresler halinde 4'e ayrılıp (D4 2D 40 14 şeklinde), daha alışıldık bir sayı sistemiyle çalışabilmek için onluk sayı sistemine çevrilir.($(D4)_{16} = (212)_{10}$, $(2D)_{16} = (45)_{10}$, $(40)_{16} = (64)_{10}$ ve $(15)_{16}=(21)_{10}$). Bu gösterim son olarak aralara konan bir nokta ile birleştirilir ve sonuçta IP numarası olarak tanımlanan notasyona ulaşılır. Yani internet üzerinde 3.559.735.317 sayısı ile adreslenmiş bilgisayar 212.45.64.21 IP nolu bilgisayardır.

TCP/IP'de, iletilen veriler katmanlara göre paketlenerek gönderilir ve alıcıda bu paketler teker teker açılıp orijinal veriye ulaşılır. Bu yöntem, iletilen veri, iletim şekli ve iletişim yolunu birbirinden ayırarak birlikte çalışmayı kolaylaştırır.

Tez çalışmaları çerçevesinde geliştirilen uygulamalarda iki adet kullanıcı arayüzü mevcuttur. Bunlardan biri Ses Gönderici Modül, diğeri ise Ses Alıcı Modüldür. Kablosuz ağ üzerinde iki bilgisayardan her biri bu modüllerden birine sahiptir ve bu modüller yardımı ile kablosuz ses haberleşmesini gerçekleştirmektedir. Modüllerin ses haberleşmesini yapmaları IP numaraları kullanılarak gerçekleştirilmiş olup, IP numaralarında yaşanacak herhangi bir sorun ses haberleşmesinin gerçekleşmemesine sebep olmaktadır.

2.6. IEEE 802.11 Standardı

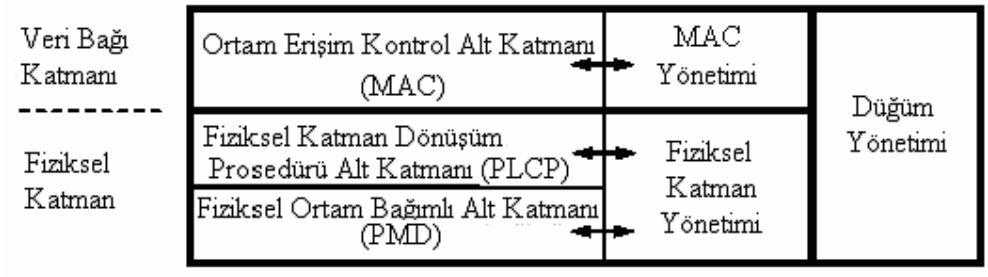
IEEE 802.11 KLAN standardı Amerikan Elektrik ve Elektronik Mühendisleri Enstitüsü (IEEE: The Institute of Electrical and Electronic Engineers) tarafından 1997 yılında geliştirilmiştir. IEEE, KLAN standartlarını IEEE 802.11x şeklinde tanımlamış ve bu alanda yeni standartlar geliştirmek üzere bir grup oluşturmuştur.

Kablolu yerel alan ağlarındaki Ethernet bağlantılarını kablosuz ortam üzerinden sağlayan IEEE 802.11 standardı, kablosuz yerel alan ağı standartları ailesinin temelini oluşturmaktadır. Zamanla farklı ihtiyaçlar ve farklı veri iletişim hızlarını karşılamak için bir çok alt standart geliştirilmiştir.

IEEE 802.11 standardı 2.4 GHz lisanssız ISM (Industries, Scientific, Medical) bandında FHSS, DSSS ve infrared fiziksel bağlantı seçenekleri ile 2 Mbit/s'e ve 5 GHz bandında ise 54 Mbit/s'e kadar veri iletim hızlarına ulaşabilmektedir (ANSI/IEEE Std 802.11, 1999, Bing, 2000).

2.6.1. IEEE 802.11 Protokol mimarisi

IEEE 802.11 standardı protokol mimarisi OSI referans modelinin Fiziksel ve Veri Bağı katmanlarını kapsar. Şekil 2.3'de IEEE 802.11 standardı temel referans modeli görülmektedir (Bing, 2000).



Şekil 2.3: IEEE 802.11 temel referans modeli

Fiziksel katman, kablosuz iletişim ortamı (medya) ile Ortam Erişim Kontrol (MAC) alt katmanını birbirine bağlayan arayüzdür. Fiziksel Katman Dönüşüm Prosedürü (Physical Layer Convergence Procedure, PLCP) ve Fiziksel Ortam Bağımlı (Physical Medium Dependent, PMD) olmak üzere iki alt katmandan meydana gelmektedir.

PMD alt katmanı, kablosuz ortam karakteristiklerini (DSSS, FHSS veya DFIR) ve kablosuz ortam yoluyla veri iletimi için gerekli metotları (modülasyon, kodlama vb.) tanımlar. PLCP katmanı ise, MAC katmanından gelen paketleri PMD alt katmanı için düzenler. Aynı zamanda MAC katmanı için taşıyıcı sezme ve kanal tahsis

(carrier sensing and channel assessment) işlemini gerçekleştirir (ANSI/IEEE Std. 802.11, 1999, Bing, 2000).

MAC katmanı, kablosuz ortamın kullanıcılar arasında etkin olarak paylaştırılmasını yani kullanıcıların ortama erişim mekanizmasını tanımlar. Bunun yanı sıra veri paketlerinin parçalanması (fragmentation), hata iyileştirme, hareketlilik yönetimi, güç tasarrufu ve şifreleme gibi işlemleri de gerçekleştirir. MAC tüm fiziksel katman türleri (DSSS, FHSS, DFIR) için ortak olmakla birlikte veri iletim hızları farklılık gösterir.

Fiziksel katman yönetimi, farklı bağlantı şartlarının uyarlanması fonksiyonlarını, MAC yönetimi ise senkronizasyon, güç yönetimi, birliktelik (association) ve tekrar birliktelik fonksiyonlarını içerir. Düğüm yönetimi, fiziksel ve MAC yönetim katmanlarının etkileşiminden sorumludur (Bing, 2000).

2.6.2. Çerçeve formatları

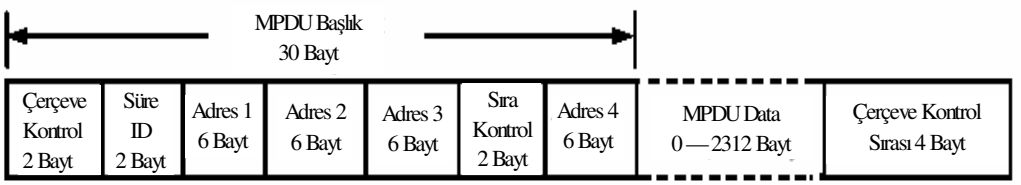
KLAN, MAC katmanında farklı amaçlar için kullanılan üç temel çerçeve biçimi (MAC Protocol Data Unit, MPDU) vardır (ANSI/IEEE Std 802.11, 1999). Bunlar:

- Veri çerçeveleri,
- Kontrol Çerçeveleri (RTS, CTS, ACK) ve
- Yönetim çerçeveleri (işaretleşme).

MAC veri çerçeve biçimi: Veri ve yönetim çerçeveleri için kullanılır. Şekil 2.4'de genel MAC çerçeve biçimi görülmektedir. MPDU başlık kısmındaki bölümler ve işlevleri şunlardır:

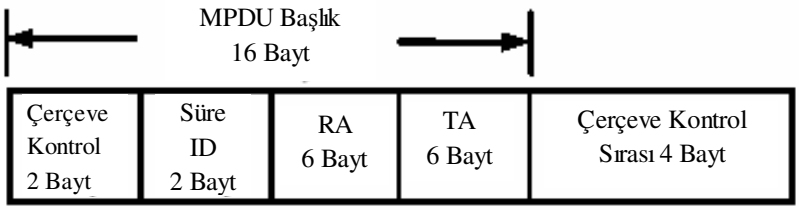
Çerçeve Kontrol: Dağıtık sisteme gönderilen/alınan paketlerin kontrolü, güç yönetimi, paket ayırma, şifreleme, kimlik belirleme (authentication).
Süre ID: Tahsis edilen vektörün süresi, güç koruma modunda çalışan düğümün tanımlanması.
Adres 1-4: BSS ID, hedef, kaynak, verici/alıcı için adresler.

Sıra Kontrol: Paket ve paket parçacıkları için sıra numarası.



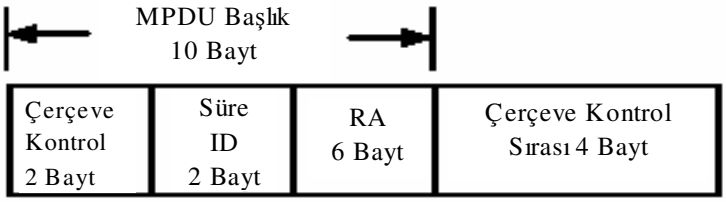
Şekil 2.4: MAC (MPDU) genel çerçeve biçimi

RTS (Request to Send) kontrol çerçeve biçimi: Süre alanında bir sonraki veri/yönetim çerçevesinin iletimi için gerekli zaman tanımlanmaktadır (Şekil 2.5). RA, bir sonraki veri/yönetim çerçevesini alacak düğümün adresini içerirken, TA ise RTS çerçevesini gönderen düğümün adresini içermektedir.



Şekil 2.5: RTS çerçeve biçimi

CTS (Clear to Send) kontrol çerçeve biçimi: CTS, RTS çerçevesine yanıt olarak gönderilir (Şekil 2.6). RA, alanına alınan RTS çerçevesindeki TA alanı adres bilgisi yüklenir. Süre alanına ise RTS çerçevesindeki süre alanındaki değerden CTS göndermek için gerekli zaman ve SIFS (Short Inter Frame Space) değerlerinin çıkarılması sonucu kalan değer yüklenir.

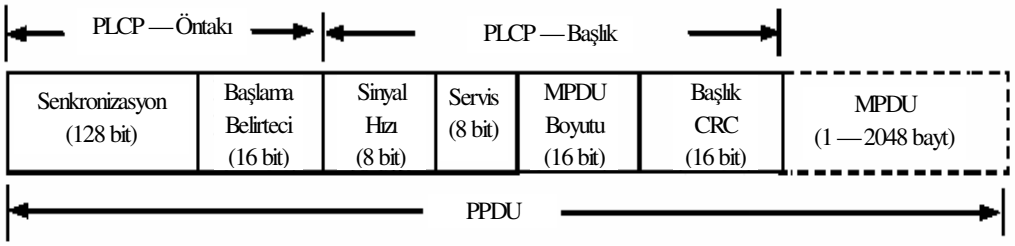


Şekil 2.6: CTS çerçeve biçimi

ACK kontrol çerçeve biçimi: ACK çerçeve CTS çerçevesi ile aynı biçimdedir. RA alanına hedef düğüm adresi, süre alanına da alınan çerçevenin süre alanındaki

değerden ACK çerçeve göndermek için gerekli zaman ve onun çerçeve iletim boşluğu (SIFS) süresi çıkartılarak kalan değerler yüklenir.

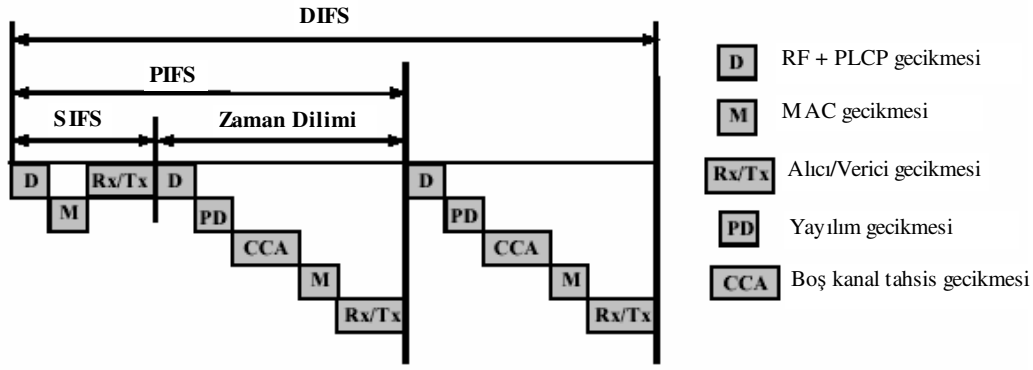
MAC katmanında oluşturulan çerçeveler iletilmek üzere fiziksel katmana gönderilir. Kullanılan fiziksel katmana (DSSS, FHSS, kızılötesi vb.) göre MAC çerçevesine bazı ilaveler yapılır. Şekil 2.7'de görülen IEEE 802.11b DSSS Fiziksel Katman Dönüşüm Prosedürü (PLCP) çerçeve biçimi; PLCP öntakısı (Preamble), PLCP başlık (header) ve MAC çerçevesinden oluşmaktadır. Öntakı alanı senkronizasyon, kanal tahsisi ve çerçeve zamanlaması için gerekli başlangıç bilgisini içerir. Başlık alanı ise kullanılan modülasyon tekniğini (DBPSK, DQPSK vb), veri iletim hızı bilgisini, gönderilen MAC çerçevesinin boyutu ve başlık alanındaki hata kontrolü (CRC) için gerekli bilgileri içerir.



Şekil 2.7: IEEE 802.11b DSSS PLCP çerçeve biçimi

2.6.3. Çerçeveler arası boşluk (Inter Frame Space, IFS)

Çerçeveler arasındaki zaman aralıkları, çerçeveler arası boşluk olarak adlandırılır ve kablosuz veri iletim hızlarından bağımsızdır. IFS her bir fiziksel katman için sabittir. IEEE 802.11 standardında MAC protokolünün ortama erişimi belirlemesinde çerçeveler arasındaki boşluk çok önemlidir. Çünkü çerçeveler arası boşluklar, ortama erişimi belirleyen Backoff algoritmasının çalışma süresini etkilemektedir (ANSI/IEEE Std 802.11, 1999, Bing, 2000). IEEE 802.11 ortama erişim için farklı öncelikler sağlamak için dört farklı çerçeveler arası boşluk tanımlar (Şekil 2.8).



Şekil 2.8: Çerçeveler arası boşluk tanımlamaları

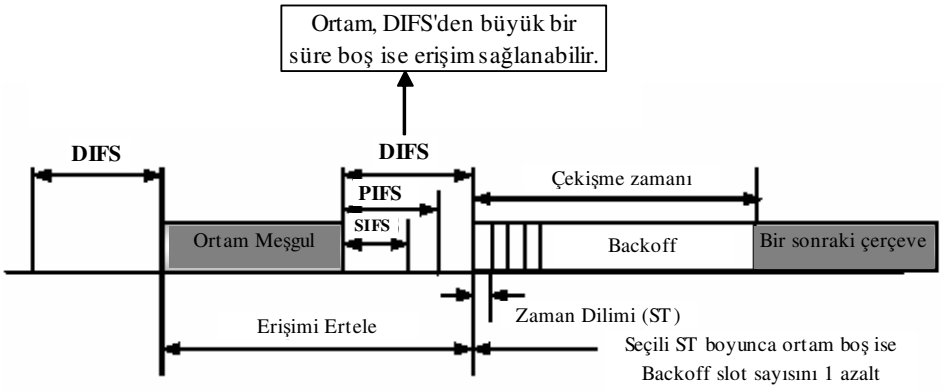
- Zaman dilimi (Slot time): Backoff algoritmasında, her zaman diliminde ortamın meşgul olup olmadığı kontrol edilir.
- En kısa çerçeveler arası boşluk (Short IFS, SIFS): Acil yanıt gönderiminde (ACK, RTS, CTS çerçevelerinin) kullanılır. SIFS, kullanılan fiziksel katmana bağlı olarak sabit bir değerdir. Ortam erişimini kazanmış bir düğüm, SIFS aralıklara yüksek öncelikli olarak iletimini gerçekleştirir.
- Nokta eşgüdüm fonksiyon çerçeveler arası boşluk (Point Coordination Function IFS, PIFS): PCF erişim mekanizmasında ortam erişimini kazanmak için kullanılır. PIFS, SIFS ve Zaman Dilimi sürelerinin toplamına eşittir.
- Dağıtık eşgüdüm fonksiyon çerçeveler arası boşluk (Distributed Coordination Function IFS, DIFS): Ardışık veri paketleri arasındaki minimum gecikmedir. Ortamın boş olduğundan kesinlikle emin olmak için düğümler DIFS süresi boyunca erişimlerini ertelerler. DIFS, PIFS ve Zaman Dilimi sürelerinin toplamına eşittir.
- Genişletilmiş IFS (Extended IFS, EIFS): En uzun çerçeveler arası boşluktur. Hatalı paket alan düğüm tarafından kullanılır.

Örneğin DSSS kullanılan bir sistemde SIFS = 10 µs, Zaman Dilimi ise 20 µs'dir. FHSS kullanılan bir sistemde ise SIFS = 28 µs, Zaman Dilimi ise 50 µs'dir (ANSI/IEEE Std 802.11, 1999).

2.6.4. Ortam erişim mekanizması (MAC)

Ortam erişim mekanizmaları, sınırlı bant genişliğine sahip kablosuz iletim ortamını kullanıcılar arasında etkin olarak paylaştırmayı sağlayan kurallar bütünüdür. IEEE 802.11 MAC katmanında çekişme esaslı dağıtık eşgüdüm fonksiyonu (Distributed Coordination Function, DCF) ve çekişmeden bağımsız nokta eşgüdüm fonksiyonu (Point Coordination Function, PCF) olmak üzere iki farklı erişim mekanizması kullanılabilir (Aad, 2003, ANSI/IEEE Std 802.11, 1999, Bing, 2000).

Şekil 2.9'da IEEE 802.11 ortam erişim mekanizmasının genel çalışma prensibi görülmektedir. PIFS yalnızca PCF erişim yöntemi ile çalışan düğümlerde kullanılır. PCF erişim noktası kullanılan sistemlerde geçerlidir. Bu yöntemde çekişmeden bağımsız olarak ortam boş olduğu sürece düğüm PIFS aralıkları ile çerçeve iletimini gerçekleştirir. DIFS ise DCF erişim mekanizmasını kullanan düğümlerde çerçeve iletimi arasındaki minimum süredir (Aad, 2003, ANSI/IEEE Std 802.11, 1999, Bing, 2000).



Şekil 2.9: IEEE 802.11 ortam erişim mekanizmasının genel çalışması

2.6.5. Hata sezme

802.11 standardında bir paketin doğru olarak iletilip iletilmediği, ACK alındı paketlerinin gönderimi ile belirlenir. Bir paket doğru olarak alındığında vericiye bir ACK gönderilir. ACK SIFS'den sonra gönderilir. SIFS, DIFS'den küçük olduğundan herhangi yeni bir paketin gönderim zamanından önce alındı bilgisi gönderilmiş olur. ACK gelmez ise kaynak düğüm, paketin bozulduğunu (hata oluştuğunu) varsayar ve

tekrar gönderir. Tekrar gönderme işleminin daha üst katman yerine MAC katmanı tarafından gerçekleştirilmesi, kaybedilen çerçevelerin daha hızlı şekilde yeniden transferine (elde edilmesine) olanak sağlar (Bing, 2000).

ACK her ne kadar güvenli paket iletimi için kullanılsa da yayın (broadcast) modunda veya çoklu gönderim durumunda çok sayıda ACK gönderimi, çarpışma meydana getireceğinden pratik bir yöntem değildir.

2.6.6. IEEE 802.11 alt standartları

IEEE 802.11x ailesinin temelini IEEE 802.11 standardı oluşturmaktadır. Bu standart 2,4 GHz Lisanssız ISM bandında FHSS, DSSS ve kızıl ötesi uygulama seçenekleri ile 2 Mbit/s'e kadar veri ilerim hızlarını destekleyebilmektedir. Gelişen teknoloji ile birlikte farklı ihtiyaçları karşılamak üzere farklı iletim hızları ve farklı fiziksel katman seçenekleri ile IEEE 802.11 standardını esas alan alt standartlar geliştirilmiştir. IEEE tarafından geliştirilen bu standartlar ANSI ve ISO tarafından da kabul edilmiştir. Bu alt standartların en yaygınları IEEE 802.11a, IEEE 802.11b ve IEEE 802.11g'dir.

2.6.6.1. IEEE 802.11a standardı

IEEE 802.11 ailesi içerisinde yeni nesil kablosuz LAN standardıdır denilebilir. 2,4 GHz'deki band genişliğini kullanan değişik uygulamalara, 5 GHz'lik frekans bandını tanımlayarak alternatif oluşturmaktadır. 5, 15-5, 25 GHz, 5, 25-5, 35 GHz ve 5, 725-5, 825 GHz frekansları arasında 300 MHz'lik bir frekans bandında çalışır. IEEE 802.11.a standardı, 5 GHz lisanssız U-NII (Unlicensed National Information Infrastructure) bandda OFDM modülasyonu kullanarak veri iletim hızını kanal (üst üste binmeyen 8 kanal kullanır) başına 54 Mbit/s'e kadar çıkarmıştır. 6 Mbit/s, 9 Mbit/s, 12 Mbit/s, 24 Mbit/s, 36 Mbit/s, 48 Mbit/s ve 54 Mbit/s veri iletim hızlarını destekleyen bu standart çoklu ortam uygulamaları ve veri aktarımının yoğun olduğu uygulamalar için daha uygun olacaktır (Bayılmış ve diğ., 2003, Gast, 2005).

DSSS yerine OFDM tekniğinin kullanılması daha iyi başarım ve daha geniş kapsama alanı sunmakla birlikte daha fazla güç harcaması gerektirir. IEEE 802.11a HiperLAN2 standardına rakip olarak geliştirilmiştir.

2.6.6.2. IEEE 802.11b standardı

Uygulamada en yaygın kabul gören standarttır. 802.11b standardı 2,4 GHz ISM bandında çalışır ve modülasyon tekniği olarak yalnızca DSSS kullanır. 1 Mbit/s, 2 Mbit/s, 5,5 Mbit/s ve 11 Mbit/s veri iletim hızlarını destekler. Kablosuz yerel alan ağlarının 2,4 Ghz ISM bandını mikrodalga fırın ve Bluetooth gibi ürünler ile paylaşması, olası parazitlerden dolayı veri kayıplarına ve veri iletim hızlarının düşmesine neden olabilmektedir.

Farklı firmaların 802.11b ürünleri arasındaki birlikte çalışabilirliğin bugün WiFi Alliance olarak bilinen WECA (Wireless Ethernet Company Alliance) tarafından onaylanması ile IEEE 802.11b bir endüstri standardı haline gelmiştir. Bu kurumun amacı WiFi ürünlerinin işlerliğini sertifikalandırmak ve IEEE 802.11b'yi global bir standart yapmaktır (Levillain, 2002).

2.6.6.3. IEEE 802.11g standardı

Bu standardın kullanımındaki amaç, mevcut IEEE 802.11b standardı üzerinden veri iletim hız artırımını sağlamaktır. 802.11b'de olduğu gibi 2,4 GHz bandı kullanılmakla birlikte 54 Mbit/s'lik veri iletim hızı sağlar. OFDM ve CCK (Complementary Code Keying) modülasyon tekniklerinin her ikisini de destekler. Günümüzde 802.11b'nin yerini almak üzeredir.

Anılan 802.11 standartları ile bu standartlar ailesi üzerinde yapılan çalışmalar Tablo 2.1'de gösterilmektedir.

Tablo 2.1: IEEE 802.11 standart ailesi

Standart	Özellikleri
IEEE 802.11	Orijinal WLAN standardı.1—2 Mbit/s veri iletim hızlarını destekler.
IEEE 802.11a	5 GHz U-NII bandında çalışsan yüksek hızlı KLAN standardı. Kanal başına 54 Mbit/s veri iletim hızını desteklemektedir.
IEEE 802.11b	2,4 GHz ISM bandında 11 Mbit/s veri iletim hızını destekler.
IEEE 802.11e	IEEE KLAN yapıları için servis kalitesini arttırmak ve yönetmek.
IEEE 802.11f	AP'ler arasında haberleşme protokolüdür (Inter Access Point Protocol, IAPP)
IEEE 802.11g	802.11b standardı üzerinde kurulan bu Standard 2,4 GHz'de 54 Mbit/s veri iletim hızına ulaşabilmektedir.
IEEE 802.11h	IEEE 802.11a için dinamik kanal seçimi ve iletim gücü kontrolü sağlar.
IEEE 802.11i	IEEE 802.11X ile kombine güvenlik özellikleri sunmaktadır.
IEEE 802.11n	2007'nin ortalarında standartlaşma çalışmalarının tamamlanması beklenmektedir. Kablosuz yerel alan ağları içerisinde en yüksek veri iletim hızını (540 Mbit/s) ve çalışma mesafesini (kapalı ortam 50 m) desteklemesi planlanmaktadır. 802.11n, diğer 802.11 standartlarına MIMO (Multiple Input Multiple Output) eklenilerek geliştirilmektedir.
IEEE 802.11X	IEEE ağları için güvenlik çerçeve standardı.
WISPR (Wireless ISP Roaming)	Kablosuz Ethernet Uyumluluğu Topluluğu tarafından geliştirilen, kablosuz kamusal ağlar arasında dolaşım için tavsiyeler bütünüdür

2.7. Sonuç

Kablosuz iletişim ortamının sınırlamalarına rağmen, kablosuz yerel alan ağlarının kullanımı; kurulum kolaylığı ve basitliği, esnekliği, ileriye yönelik maliyet kazancı,

hareketlilik ve mevcut yerel alan ağ yapısını genişletme gibi avantajlarından dolayı gün geçtikçe artmaktadır.

Günümüzde mevcut ve geliştirilmekte olan bir çok kablosuz iletişim teknolojisi olmasına rağmen, kablosuz Ethernet olarak adlandırılan IEEE 802.11 standardının en büyük avantajı, oldukça yaygın bir kullanım oranına sahip (%95 civarında) standart kablolu Ethernet yapısı ile sağladığı kolay entegrasyondur.

IEEE 802.11 standart ailesi farklı ihtiyaçlara cevap veren ve farklı veri iletim hızlarına sahip olan alt standartlardan oluşmaktadır. İlgili tüm bu standartlar, CSMA/CA ortam erişim yöntemine dayalı olarak çalıştırılmakta ve geliştirilmektedir.

Veri iletim hızı uygun olmayan teknolojilerle gerçekleştirilecek bir ses haberleşmesinde veri gönderimindeki gecikmeler gerçek zamanlı ses haberleşmesine imkan vermeyecek, dolayısı ile uygulamanın hayata geçirilmesini önleyecektir. Burada sunulan tez çalışmalarında bu durum göz önünde bulundurularak, gerçek zamanlı ses haberleşmesinde ideal bir çözüm olan IEEE 802.11g standardını destekleyen donanımsal aygıtlar kullanılmakta ve uygulamalar bu temelden hareketle geliştirilerek çalıştırılmaktadır.

3. VERİ GİZLEME / GÖMME TEKNİKLERİ

3.1. Giriş

Temeli antik çağlara kadar dayanan gizli haberleşme, teknoloji değişip geliştikçe şekil ve yöntem açısından da faklılıklar göstermektedir. Bununla birlikte önemini devamlı korumaktadır. Gizliliğin öneminin had safhaya ulaştığı uygulamalarda; gizli bilgilerin, üçüncü kişilerin eline geçmeden ilgili hedefe gönderilmesi amaçlanmaktadır.

Veri gizleme ve gömme denildiğinde günümüzde araştırmacıların karşısına üç temel kavram çıkmaktadır. Bunlar Kriptoloji (Cryptography), Damgalama (Watermarking) ve Stenografi (Steganography)'dir. Aşağıda takip eden alt bölümlerde bu kavramlar hakkında bilgiler sunulmaktadır.

3.2. Kriptoloji (Cryptography)

"Cryptography" kelimesi gizli yazı anlamına gelen, "secret(crypto-)" ve "writing (-graphy)" kelimelerinden türetilmiştir. Özel/kişisel nitelikli, gizli içeriğe sahip bilgi veya mesajların anlamlı olarak, kaynak veya alıcıdan başka üçüncü kişilerin eline geçmesini önlemek amacıyla kullanılan tüm teknikleri içeren bir bilim dalıdır. Bu maksatla, gelişmiş algoritma teknikleri kullanılmaktadır. Alıcıda elde edilen mesajın, orijinali (kaynaktaki) ile aynı olmasını sağlamak, doğruluğunu ispatlamak yine bu algoritma tasarıları ile sağlanmaktadır.

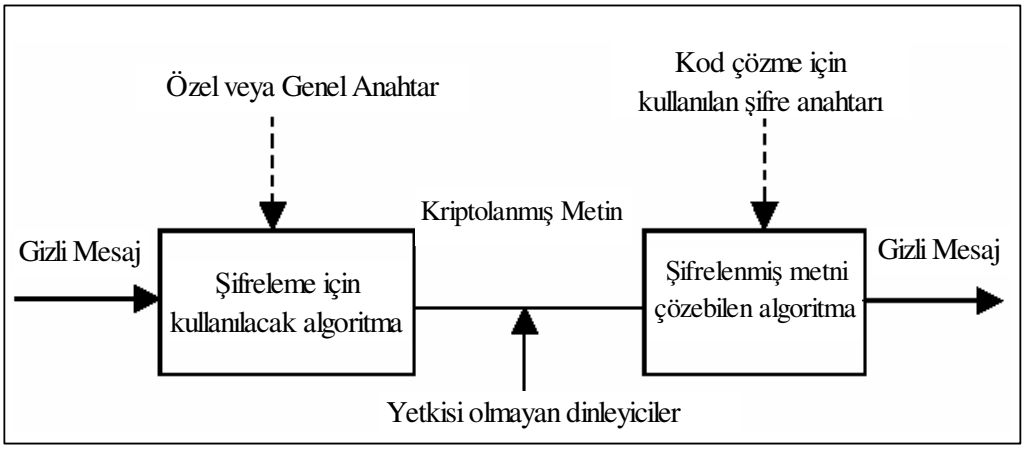
Haberleşme ağlarında bir merkezden diğer bir merkeze gönderilen ve alındığı veya gönderildiği yerde saklanan bilgilerin korunması, yetkilendirilmemiş kişilerin bu bilgilere ulaşmasının önlenmesi, günümüz bilgi teknolojilerinde şifrelemeye (encryption-decryption & encipher-decipher) ayrılan zaman ve önemi sürekli olarak

artırmaktadır. İnternet & İntranet uygulamalarında; e-mail, banka işlemleri, kişisel işlem ve bilgilerin saklanması, dijital imza ve kimliklerin üretimi, veri tabanı dosyalarının korunumu, video kriptolojisi, elektronik oyun ve program şifrelemesi, faks ve telefon şifrelemesi vb. uygulamaları sıkça kullanılır durumdadır.

Ticari güvenlik, askeri ve devlet güvenliği alanlarında bütün kurumların ortak hedefi, sahip oldukları önemli veya gizli bilgilerin güvenli ortamlarda saklanması ve sadece yetkisi olan kişilerin, yetkileri oranında bu bilgilere ulaşabilmelerini sağlamaktır. Bu son derece önemli bir konu olup, bunu sağlamak ise tüm şifreleme/şifre çözme tekniklerini içeren bilim dalı olan kriptolojinin görevidir.

Başlangıçta sadece askeri veya uluslararası/diplomatik mesajların korunarak güvenli bir şekilde alıcıya aktarılması ihtiyacını karşılamak amacıyla ortaya çıkan şifreleme teknikleri günümüzde bu alanlardaki özelliğini hala korumakla birlikte, özellikle ticari uygulamalardaki gereksinim de küçümsenmeyecek boyutlara ulaşmıştır.

Şekil 3.1'de genel bir şifreleme sisteminin blok diyagramı görülmektedir. Sistemin amacı gizli bilginin görünümünü değiştirerek saklamak olduğundan, yetkisiz birisi tarafından bu bilgiler (veriler) anlaşılamamaktadır.



Şekil 3.1: Genel şifreleme ve şifre çözme blok diyagramı

Bütün veri gizleme teknikleri, veri gömme algoritması ve bir algılayıcı fonksiyondan meydana gelir. Gömme algoritması gömü verisini (gizli mesajı) bir örtü verisine

(veya taşıyıcıya) gömmek için kullanılır. Ve örtülü veri elde edilir. Gömme süreci bir "anahtar" mekanizmasıyla korunmaktadır. Bu yüzden yalnızca yetkili kişiler gizli anahtar ile gömü verisine ulaşabilmektedirler.

Algılayıcı fonksiyon örtülü veriye uygulanarak gömü verisi yeniden elde edilebilir. Halen dijital resimlerde veri gizleme ile sınırlı olarak konu genişletilmektedir. Her bir veri gizleme tekniği, planlanan uygulama tarafından dikte edilen belirli özelliklere sahip olmalıdır (örneğin, "taşıyıcı ve gizli mesaj arasında bir ilişki var mı?", "kaç alıcı söz konusudur?", gibi).

Sayısal ses içerisine veri gömme/şifreleme ve şifre çözme işlemleri üç temel adımla özetlenebilir:

1) Taşıyıcı işaretin "*i.*" ses çerçevesine gömülecek "k_{m_i}" gizli anahtar işaretinin belirlenmesi:

Ses çerçevesine gömülecek anahtar işareti tipik olarak; "*k*" gizli anahtar bilgisi ve "ω_j" gizli veri bilgisinin bir fonksiyonu olarak üretilir (Hartung ve diğ., 1999).

$$k_{m_i} = f(\omega_j, k) \quad j=1, 2, \ldots\ldots, L \tag{3.1}$$

(3.1) ifadesinde, *L* eklenecek gömü verisinin uzunluğunu belirtmekte olup, "ω_j" ise "*i.*" çerçeveye eklenecek gömü verisinin "*j.*" bitini göstermektedir. "*f*" fonksiyonu sadece "*k*" ve ω_j'nin değil, gömü verisinin eklendiği orijinal ses çerçevesi s_i'nin de bir fonksiyonu olarak tanımlanabilir (Malvar ve diğ., 2003).

Netice olarak hedeflenen sistemde "*f*" üç değişkenli doğrusal olmayan bir fonksiyondur.

$$k_{m_i} = f(\omega_j, k, s_i) \tag{3.2}$$

2) k_{m_i} modüle edilmiş gizli anahtar işaretinin taşıyıcı "s_i" işaretine gömülmesiyle örtülü veri "$s_{i_{WM}}$" işaretinin elde edilmesi:

$s_{i_{WM}}$ 'nin elde edilmesi s_i ve k_{m_i} 'ye bağlı " $f_1(s_i, k_{m_i})$ " fonksiyonunun belirlenmesi olarak tanımlanabilir.

$$s_{i_{WM}} = f_1(s_i, k_{m_i}) \tag{3.3}$$

3) Gizli anahtar ve orijinal taşıyıcı işaret yardımıyla gömü verisinin elde edilmesi, bir başka deyişle veri çözme:

$\hat{w}_j$ öngörü ile çözülen *j.* gizli veri biti olmak üzere, (3.4) eşitliğinde *g( )* doğrusal olmayan fonksiyonu veri çözme(algılama) işlemini modellemektedir.

$$\hat{w}_j = g(s_i, s_{i_{WM}}, k) \tag{3.4}$$

Alıcıda orijinal ses işaretinin bilinmemesi durumunda *g()* fonksiyonu (3.5) eşitliğinde görüldüğü gibi iki değişkenli bir fonksiyon olarak tanımlanır.

$$\hat{w}_j = g(s_{i_{WM}}, k) \tag{3.5}$$

3.3. Damgalama (Watermarking)

Stenografik tekniklerin ticari kullanımı yavaş yavaş dijital "filigran"ın (watermarking) gelişmesini sağlamaktadır. Burada söz konusu olan gizli bilginin insan duyularından gizlenmesidir. 1990'ların başında imge filigrasyonu (damgalama) kavramı gelişmiş; Tanaka ve arkadaşları faks gibi ikili imgelerin korunması kavramını ortaya atmışlardır (Tanaka ve diğ., 1989, 1990). 1993 yılında Tirkel ve arkadaşları gerçekleştirdikleri uygulamaya; daha sonra "watermark" olarak birleştirilecek "water mark" ismini vermişlerdir (Hartung ve diğ., 1997). Bilim çevreleri bu yıllarda konu üzerine daha fazla eğilmeye başlamış ve "sayısal damgalama" (digital watermarking) ile ilgili ilk seminer 1996 yılında gerçekleşmiştir. Bilgisayar teknolojisinde ortaya çıkan hızlı gelişmeler ve internet

teknolojisi ile birlikte; telif hakları sorunu da hızlı bir şekilde yayılmış ve 1990'ların ortalarından itibaren bir çok ticari şirket telif haklarının korunması ve sayısal veri filigrasyonu ile ilgili projeler başlatmış bulunmaktadır. Geliştirilen projeler; platformdan bağımsız, genel çözümler olarak ortaya konulmaktadır. Bunların yanında geliştirilen ürünlerin standartlaştırılmasını sağlamak amacıyla; standardizasyon kurumları da konu üzerinde yoğun araştırmalara girişmişlerdir. Bu konu ile ilgili ilk çalışmaları başlatan kuruluş DAVIC (The Digital Audio Visual Council) olmasına rağmen başarıya ulaşamamıştır. Bununla birlikte; gelecek nesil optik disk teknolojileri üzerinde çalışan DVD (Digital Versatile Disk), TVAnytime, sayısal müzik kayıtlarının oynatılması, kaydı ve dağıtımı ile ilgili şirketleri, organizasyonları, internet servis sağlayıcılarını güvenlik teknolojileri ile ilgili kişi ve kurumları bir araya getiren SDMI (The Secure Digital Music Initiative), görsel ve işitsel ortamlar ile ilgili kodlama ve sıkıştırma standartlarını belirleyen MPEG (Moving Picture Experts Group) gibi kurumlar sayısal filigrasyon standartları üzerinde yoğun bir şekilde çalışmalarına devam etmektedirler. Avrupa Birliği komisyonu da bu konu üzerinde bir çok uluslararası projenin oluşturulmasına destek sağlayarak konu ile ilgili şirket ve kişilerin bir araya gelmesini sağlamaktadır.

Dünya çapında telif haklarının korunması ve düzenlenmesi ile ilgili çalışmalar yapan ve hükümetler üstü bir kuruluş olan WIPO (World Intellectual Property Organization) sayısal filigrasyonun yasal alanlarıyla ilgili çalışmalarını sürdürmektedir (Delaigle, 2000). Günümüzde DICOM gibi imge formatları; hastalara ait resimlerden, hasta ismi, tarih, şikayet ve hastalıkları gibi bir çok bilgiyi çıkarabilmekte ve medikal güvenliği sağlayabilmektedir. Bugün sayısal damgalama endüstriden, standardizasyon kuruluşlarından ve kanuni birçok kuruluştan ilgi görmesine rağmen konu ile ilgili en geniş çalışmalar üniversitelere ve araştırma enstitülerine bağlı imge ve işaret işleme grupları tarafından gerçekleştirilmektedir.

3.4. Stenografi – Gizli Haberleşme

11 Eylül 2001'de yaşanan trajik olaylarda teröristlerin ileri teknolojiler kullandığı saptandıktan sonra, stenografi oldukça popüler olmaya başlamıştır. Çünkü

teröristlerin ECHELON tipi sistemleri devre dışı bırakarak aralarında gizlice haberleşmek için bu teknolojiden yararlandıkları söylentisi tüm dünyada yayılmıştır. Bugün, hala bunu doğrulamak için tatmin edici bir kanıt bulunabilmiş değildir. Yalnızca 2000'li yıllarda adı duyulmaya başlanan stenografi (steganography) bu kadar "yeni bir uygulama mıdır?" ve "özünde nedir?" gibi soruların cevapları aşağıda verilmektedir.

Stenografi (=Stego) iki parçadan oluşan Yunanca bir kelimedir. "Steganos" örtülü/gizli, "grafi"de yazım/çizim anlamına gelmektedir. Örtülü yazma sanatı olarak çevrilen "stego" aslında antik Yunan ve Herodot zamanına kadar uzanan derin bir geçmişe sahiptir. Herodot bu konuda birkaç olay anlatmaktadır. Örneğin, M.Ö. 5. yüzyılda, Yunan tiran Histiaeus'un, Susa Kralı Darius'un krallığında göz hapsine alındığı sırada, bir Anadolu şehri olan Milet'te yaşayan damadı Aristagoras'a gizli bir mesaj göndermek istemesiyle ilgilidir. Histiaeus, kölelerden birinin saçını kazıtır ve mesajı dövme şeklinde kölenin kafa derisine işler. Kölenin saçı yeteri kadar uzadığında, köle, Milet'e gönderilir. Köle yanında hiçbir şey götürmediği için Kral Darius bundan şüphelenmez. Köle oraya vardığında durumu anlatır ve saçları tekrar kazıtılan kölenin kafa derisinden Histiaeus'un mesajını içeren dövmesi ortaya çıkar.

Diğer örnek uygulamalar ise; odunların üzerine asitle yazılan mesajları balmumuyla kamufle etmek (Demaratus'un Spartalılar'ı uyardığı hikaye) ve mesajları tavşanların midesine kazımak gibi yöntemlerin kullanıldığı olaylardır. Eski Romalılar birbirleri arasında, meyve suyu veya süt gibi sıvılardan oluşturulan görünmez mürekkepler kullanarak yazışırlardı. Bu yazışma, gelişme göstererek günümüze kadar gelebilmiştir. Rönesans döneminde Johannes Trithemius'un kriptoloji ile ilgili kitapları üçleme olarak basılmıştır. Trithemius'un stego metodu birbirini izleyen sütunlardaki kelimelerin ilk harflerini birleştirmeye dayalıdır; ve bir nevi akrostiş uygulamasıdır. "Steganographia" isimli yazısıyla terim geçerlilik kazanmış ve yaygın olarak o dönemde kullanılmaya başlanmıştır.

II. Dünya Savaşı sırasında Almanlar bir mikro-noktalama aleti geliştirir. Bu alet aracılığıyla gizli bir mesaj, resimleme tekniğinden faydalanılarak örneğin "i" harfindeki veya başka bir noktalama işaretindeki noktanın boyutuna indirgenip bir

kağıda işlenebilmektedir. Mesajı alan kişi tarafından ise tüm bu noktalar birleştirildiğinde gizli mesaj ortaya çıkmaktadır. Bu aletler, teknik çizimleri de kapsayan büyük miktarda yazılı veri aktarımını gerçekleştirebilecek potansiyele sahiptir ve bütün bunları da bilgileri çok etkili bir şekilde saklı tutarak yapmaktadır.

Bir takım gizli mesajların yetkilendirme prensibinden hareketle yalnızca ilgililer tarafından okunması, diğer kişiler tarafından ise ya "gizlenmiş veriden" haberdar dahi olmaması ya da haberi olsa dahi gömülü bilgiyi elde edememesi arzu edilir. Bu maksatla veri gizleme (data hiding) teknikleri bünyesinde "stenografi" bilim dalı kullanılmaktadır (Akar, 2005). Neticede bu sanat bugün; insanlığa, bilgilerin gizlice iletilmesi konusunda çağlar boyu yardımı dokunmuş bir bilime dönüşmüştür. Modern stenografi teknik olarak, bir veriyi (mesaj) bir nesnenin içine gizli biçimde yerleştirmeyi esas alır. Öyle ki, sadece belirlenen alıcı kendine iletilmek istenen mesajı nesneden alır ve diğer gözlemcilerin o nesnenin içindeki mesajın varlığından haberleri olmaz. Kriptografinin bir kolu olarak görülen stenografi bu özelliğiyle onu bir adım ileri taşır. Kriptografi güvenilirliği sağlasa da bir bakıma mesajın gizliliğini sağlamaz. Kriptografik uygulamalarda bilgi sadece gönderen ve alanın anlayabileceği şekilde şifrelenirken, stenografik uygulamalarda bilgi sadece gönderen ve alanın varlığını bildiği şekilde saklanır, bazen de şifrelenip çift kat koruma sağlanır. Veriler genelde metin ve resim; taşıyıcı nesneler ise metin, ses, resim ve video görüntüleri olabilir.

Bilgisayar stenografisi iki temel prensip üzerine kurulmuştur. Bunlardan ilki sayısal hale getirilmiş resim veya ses dosyalarının, diğer türlerden farklı olarak, sahip oldukları fonksiyonlarını yitirmeden değiştirilebilmeleri ilkesidir. İkincisi ise, insanın, renk veya ses kalitesinde meydana gelen küçük değişiklikleri ayırt edememesine dayanmaktadır. Bunun mantığı da lüzumsuz bilgiler taşıyan nesnelerin içindeki bilgileri, başka bilgi parçacıklarıyla yer değiştirmektir.

3.4.1. Gizli bilginin araştırılması (Steganalysis)

Stenografinin amacı gizli bir mesajın veya bir gömü verisinin, şüphelerden sakınarak transferinin gerçekleştirilmesidir. Eğer kuşkular artarsa, gizli mesajın ortaya çıkarılması kaçınılmaz olur. Bu mesajların keşfedilerek faydasız hale getirilmesi sanatı literatürde stego-analiz (steganalysis) sanatı olarak bilinmektedir. Ve bu sanatın gelişmesi amacıyla çeşitli algoritmalar geliştirilmekte ve gizli bilgiler elde edilmeye çalışılmaktadır.

Sunulan tez çalışmalarında stenografinin uygulandığı ses paketleri içerisindeki gömü verisi/dosyası geliştirilen kod çözücü algoritma ile elde edilmekte ve kullanıcıya bilgi verilmektedir. Stenografide üçüncü kişilerin steganaliz işlemini yapamaması için, verinin ne şekilde gömüldüğünün gizli tutulması, gömü verilerinin güvenliği açısından önem arz etmektedir.

3.4.2. Stenografik metotlar

Mesajların örtü verisi içerisine ne şekilde yerleştirildiği çok büyük önem arz eder. Gömü verisinin/dosyasının hangi bitlere yerleştirildiği, hangi veri bloklarının içerisine konumlandığı, şifreleme yapılıp yapılmadığı gibi parametreler steganalizin ilgi alanına girer.

İnternet, haberleşmenin artan geniş bandında bilginin kitlelere dağıtılma vasıtası olarak kullanılmaktadır. Böyle bilgiler, kitle haberleşmesini sağlamak üzere metin, resim ve ses dosyalarını kapsamaktadır. Bu uygulamalarda gizli bilginin taşınması bir çok farklı teknikle ve mükemmel taşıyıcılarla mümkün olabilir. Diğer taşıyıcılar gizli bilgi için depolama cihazları ve TCP/IP paketleri içerirler. İlk yaklaşım metin içerisinde bilginin gizlenmesi olacaktır. Bilgisayarlar bilgi gizlemede daha fazla kapasite imkanı sağlamaktadır.

Sunulan tez çalışmalarında, ses verilerini TCP/IP paketleri şeklinde ağ üzerindeki diğer bilgisayara gönderildiğinden, uygulama yerel alan ağında çalışabildiği gibi,

internet üzerinden de çalışabilmektedir. Bu durum ilgili uygulamanın kullanım alanının genişlemesi anlamına da gelmektedir.

Bir belgenin yerleşim planı bilgiyi açığa çıkarır. Belgeler, kelimeler ve çizgilerin pozisyonlarının modülasyonu ile işaretlenerek tanımlanabilir. Boşlukların eklenmesi ve görünmeyen karakterler gizli bilginin geçişine bir metot oluşturur. Görülecek ilginç bir yol bir HTML dosyasına ekstra kesme çizgileri ve boşluklar eklemektir. Web listeleyici bu ekstra çizgi ve boşlukları göz ardı eder, ancak web sayfasının kaynağı açığa çıkarılarak ekstra karakterler gösterilir. Bilginin metin içerisinde gizlenmesi için bir çok metot vardır. Bu metotlar en küçük değerlikli bit (Least Significant Bit, LSB) veya gürültü ekleme, resmin işlenmesi ve sıkıştırma algoritmaları ve parlaklık gibi resim özelliklerinin değiştirilmesi metotlarıdır. Diğer algoritmaların zaafından ve resim işleme veya onun bileşenlerinde bilgi gizleme katsayılarından yararlanarak resim içinde bilgi gizlemenin metotlarını daha güçlü yapmaktadır. Bu metotlar mesajları resmin belirgin alanlarına gizlerler ve sıkıştırma, kesme ve bazı resim işleme saldırılarına karşı LSB yaklaşımından daha güçlü kılarlar (Akar, 2005).

Bu tez çalışmalarının da temelini teşkil eden sayısal ses verilerine stenografi uygulaması, teorik ve pratik olarak mümkündür. Çünkü ses içerisine küçük yankılar veya göze çarpmayan sinyaller eklenebilir ve bunlar daha yüksek genlikte ses tarafından maskelenebilir (Franz ve diğ., 1996, Gruhl ve diğ., 1996).

3.5. RGB Resimler İçin LSB Veri Gömme Tekniği

En basit ve en yaygın stenografi tekniği “En Düşük Değerlikli Bit” (Least Significant Bit, LSB) gömme tekniğidir. Burada önerilen işlem genellikle dijital resimler içerisinde en düşük değerlikli bitin gürültü tarafından maskelenerek değiştirilmesidir. Aslında renkli resim durumunda, mesaj gizleme için daha fazla oda mevcuttur; çünkü, her bir piksel kırmızı, yeşil ve maviden (RGB: Red, Gren, Blue) oluşan üçlü bir birleşimdir. Yine iki veya daha fazla “en düşük değerlikli bit” yer değiştirilerek her pikselin kapasitesi arttırılır; ancak, aynı zamanda istatistiksel olarak

çözünebilirlik riski hali hazırda artacaktır. Sonuç olarak her bir özel stenografik tekniğin güvenli çalışması önemlidir ve neden güvenli olduğu tartışılır. Hatta basit en düşük değerlikli bit, belirli durumlar altında kodlanarak saptanabilir değişiklikler ortaya koymaktadır. Kimi çalışmalarda taşıyıcı bitlerinde küçük kesirli değişimler önerilmiştir (Aura, 1995). Örneğin taşıyıcıda bulunan her yüzüncü bitin gri seviye ile değiştirilmesi söz konusudur. Resim gürültüsüne bağlı olarak bu değişiklikler ile uygun karmaşık şüpheler yaratılarak, resmin herhangi bir istatistiksel model ile kolayca anlaşılamaması başarılı şekilde sağlanmış olur.

Önce güvenli bir şekilde herhangi bir mesaj gizleme tekniği istenir, bu durumda taşıyıcı resimleri ve onların istatistiksel özellikleri dikkatli bir şekilde incelenmelidir. Gürültü bileşeni resim ile birlikte tek biçimli olmamalıdır; ancak, resim içinde piksel konumlarına bağlı olabilir. Örneğin pikseller parlak beyaz renge uygun olarak 255'de doymuş olabilir. Sıfırdan farklı değişimlere rağmen gürültünün bütün modeli Gaussian olabilir (bu özellikle Gama düzeltmesi işlemine tabi tutulmuş taranmış resimler içindir).

Bir tarayıcı ile taranmış ve parlaklığı Gama korelasyonu kullanılarak ayarlanan orijinal resimden elde edilen kodlu resim, bir siyah ve beyaz resimde siyah piksellerle ilgili olarak çift gri seviyeler ve beyaz pikseller ile ilgili olarak tek değerlikli gri seviyeleri gösterir. Birisi açık bir biçimde piksellerin geniş bir parçasında 255 maksimum gri seviyesi ile doymuş olduğu düşünülebilir. Piksellerin yalnızca küçük bir bölümü değiştirilerek, resim içerisinde güvenli bir şekilde oynanabilir, aşırı yamalar bazı şüpheleri de beraberinde getirecektir. Bu problemden taşıyıcı resmin dikkatli bir şekilde seçimi ile veya aşırı/az akış ile elbette sakınılabilir. Bu bölgelerde de zamanından önce stenografik plan tarafından eğitilerek aşırı/az akışa uğramış bölgelerden sakınılabilir ve resim içerisine uyarlanabilir.

Eğer taranmış resimler biliniyorsa yatay yönde daha geniş gürültü bağıntılarıyla ve daha küçük bağıntılar dikey yönde sergilenebilir böylece her bir piksel için dağıtım olasılığı sırasında, ne aşırı akışa ne de az akışa izin verilmez. Belirli standart sapmalar ile gerçekleştirilen işlemlerden sonra bu deliller hesaba alınarak mesaj

gizleme planları, ilgili taşıyıcı değişikliğe uğratılarak istatistiksel delilleri ile tutarlı hale getirilir. Burada dikkat edilmesi gereken nokta; birisi büyük bir çaba ile daha fazla memnuniyet verici gürültü modeli ve hazır mesajları ortaya çıkarabilir; ancak, bunun maliyeti, vakit alan ve pahalı araştırmalar ile gerçekleşebilir (Akar, 2005).

3.6. Sonuç

Tarih boyunca gizlenmesi gereken bilgilerin olduğu her yerde, bu bilgilerin iletilmesi için değişik yöntemler geliştirilmiş ve başarılı olunduğu sürece bu yöntemler uygulanmıştır. Bu tarihsel gelişim sürecinde stenografi doğmuş ve yoğun olarak gizli bilgi iletiminde kullanılan bir sanat haline gelmiştir. Günümüzde bu sanat, insanlığa, bilgilerin gizlice iletilmesi konusunda çağlar boyu yardımı dokunmuş bir bilime dönüşmüştür. Modern stenografi teknik olarak, bir veriyi (mesaj) bir nesnenin içine gizli biçimde yerleştirmeyi esas alır. Öyle ki, sadece belirlenen alıcı kendine iletilmek istenen mesajı nesneden alır ve diğer gözlemcilerin o nesnenin içindeki mesajın varlığından haberleri olmaz.

Kriptografinin bir kolu olarak görülen stenografi bu özelliğiyle onu bir adım ileri taşır. Kriptografi güvenilirliği sağlasa da bir bakıma mesajın gizliliğini sağlamaz. Kriptografik uygulamalarda bilgi sadece gönderen ve alanın anlayabileceği şekilde şifrelenirken, stenografik uygulamalarda bilgi sadece gönderen ve alanın varlığını bildiği şekilde saklanır, bazen de şifrelenip çift kat koruma sağlanır. Gizli veriler genelde metin ve resim; taşıyıcı nesneler ise metin, ses, resim ve video görüntüleri olabilir.

Yapılan tez çalışmalarında, stenografi uygulaması gerçekleştirmek üzere, gizli bilgileri belli bir düzene göre sayısal ses içerisine gömen ses gönderici yazılımlar ve bu gizli bilgileri gelen sayısal ses verilerinden ayrıştıran ses alıcı yazılımlar geliştirilmiş olup, bu yazılımların detayları ilerleyen bölümlerde sunulmaktadır.

4. METİNLERİN VE ANALOG SES SİNYALLERİNİN SAYISAL VERİYE ÇEVRİLMESİ

4.1. Giriş

Bilgisayar teknolojilerine dair tüm uygulamalar temel olarak ikili sayı sisteminde çalışırlar ve bilgiler bu sistem temelinde depolanılar. Kullanıcıların yazdığı metinlerin ikili sayı sistemindeki karşılıklarını belirlemek için bir takım kodlama standartları mevcuttur. Bu kod standartlarına göre metinler sayısal bilgilere dönüştürülmektedir. Bununla birlikte bu bilgiler değişik ortamlarda iletilmek istendiğinde bir takım yöntemlerle analog sinyallere çevrilerek gönderilirler. Bu bölümde tez çalışmalarında faydalanılan kodlama standartları ve analog sinyal çevrimleri anlatılmaktadır.

4.2. Metin Kodlama Standartları

Tez çalışmalarında geliştirilen yazılımlardan sayısal ses verileri içerisine metin gömme uygulamasını gerçekleştiren yazılım metin kodlama standartlarından ASCII kullanılarak kodlama yapan metinleri ikili sisteme çevirmekte ve elde ettiği verileri sayısal ses paketlerine gömerek iletmektedir. Geliştirilen standartlar sadece ASCII kodlama sisteminden ibaret değildir. Aşağıda bu kod standartları hakkında bilgiler verilmektedir.

4.2.1. ASCII kodu

1968 yılında ANSI (American National Standards Institute) tarafından ortaya atılan ASCII, bilgisayar ağ ve sistemlerinde bilginin gösterilmesi/temsil edilmesi amacıyla kullanılan bir kod standardıdır. 7 bit olarak 0—127 arasında 128 değişik karakteri

kapsamaktadır. Her bir karakter aşağıdaki tabloda gösterildiği gibi 7 bitlik bir kod ile ifade edilir. Örneğin "a" harfi; 7 bit ASCII kodunda $(1100\ 001)_{ascii}$ olarak ifade edilmektedir. Benzer şekilde "8" rakamı 011 1000, "+" işareti 010 1011 ASCII kodları ile ifade edilmektedir. Standart sembollerin dışında bir takım sembol ve şekillerin de ilave edilmesi ile 0—255 arasında genişletilmiş ASCII kodu oluşturulmuştur. 7 bit ASCII, 0—127 arasında toplam 128 farklı karakteri içerirken, genişletilmiş 8 bit ASCII, 0—255 arasında 256 farklı karakteri bünyesinde barındırmaktadır. Tablo 4.1 ASCII kodlarını göstermektedir.

Tablo 4.1: ASCII kod tablosu
(Standard No.X3-1968 of the ANSI, American National Standards Institute)

	0	1	2	3	4	5	6	7
0	NUL	DLE	space	0	@	P	`	p
1	SOH	DC1 XON	!	1	A	Q	a	q
2	STX	DC2	"	2	B	R	b	r
3	ETX	DC3 XOFF	#	3	C	S	c	s
4	EOT	DC4	$	4	D	T	d	t
5	ENQ	NAK	%	5	E	U	e	u
6	ACK	SYN	&	6	F	V	f	v
7	BEL	ETB	'	7	G	W	g	w
8	BS	CAN	(	8	H	X	h	x
9	HT	EM	)	9	I	Y	i	y
A	LF	SUB	*	:	J	Z	j	z
B	VT	ESC	+	;	K	[	k	{
C	FF	FS	,	<	L	\	l	|
D	CR	GS	-	=	M	]	m	}
E	SO	RS	.	>	N	^	n	~
F	SI	US	/	?	O	_	o	del

8 bit ASCII'nin anlamı 128—255 arasında toplam 128 yeni sembol ya da karakterin 7 bit ASCII ailesine katılmasıdır. Bunun dışında 1990'ların başında UNICODE olarak adlandırılan 16-bit kod geliştirilmiştir. ASCII alfanumerik karakterleri 0—127 arasında sayılar tarafından temsil ederek 7 bit ikili koda dönüştürmektir. ASCII bilgisayarların farklı türdeki metin dosyalarının kolay transferine izin vermektedir.

4.2.2. Kontrol kodları

Tablo 4.2'de ASCII kodlarının kontrol fonksiyonlarını oluşturan kodlar ve bu kodların anlamları verilmiştir.

Tablo 4.2: ASCII kontrol kodlarının karşılıkları

NUL	Null	DLE	Data line escape
SOH	Start of heading	DC1	Device control 1
STX	Start of text	DC2	Device control 2
ETX	End of text	DC3	Device control 3
EOT	End of transmission	DC4	Device control 4
ENQ	Enquiry	NAK	Negative acknowledge
ACK	Acknowledge	SYN	Synchronous idle
BEL	Bell	ETB	End transmission block
BS	Backspace	CAN	Cancel
HT	Horizontal tab	EM	End of medium
LF	Line feed	SUB	Substitute
VT	Vertical tab	ESC	Escape
FF	Form feed	FS	File separator
CR	Carriage return	GS	Group separator
SO	Shift out	RS	Record separator
SI	Shift in	US	Unit separator

4.2.3. Genişletilmiş ASCII kodları

7-bit ASCII kodunun bazı karakterler için yetersiz kalmasıyla birlikte 7 bit, 8 bite çıkarılarak toplam 256 farklı kod ve Tablo 4.3'de görülen karakterler elde edilmiştir.

ASCII, alfanumerik karakterleri (harf, rakam, sembol ve kontrol karakterleri) 0—127 arasında sayılar tarafından temsil ederek 7 bitten oluşan ikili kodlara dönüştürmektedir. ASCII bilgisayarların farklı türdeki metin dosyalarının kolay transferine izin vermektedir.

Tablo 4.3: ASCII kodlarının 8-bit olarak karakter karşılığı

Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char
128	80	Ç	160	A0	á	192	C0	└	224	E0	α
129	81	ü	161	A1	í	193	C1	┴	225	E1	ß
130	82	é	162	A2	ó	194	C2	┬	226	E2	Γ
131	83	â	163	A3	ú	195	C3	├	227	E3	π
132	84	ä	164	A4	ñ	196	C4	─	228	E4	Σ
133	85	à	165	A5	Ñ	197	C5	┼	229	E5	σ
134	86	å	166	A6	ª	198	C6	╞	230	E6	µ
135	87	ç	167	A7	º	199	C7	╟	231	E7	τ
136	88	ê	168	A8	¿	200	C8	╚	232	E8	Φ
137	89	ë	169	A9	⌐	201	C9	╔	233	E9	Θ
138	8A	è	170	AA	¬	202	CA	╩	234	EA	Ω
139	8B	ï	171	AB	½	203	CB	╦	235	EB	δ
140	8C	î	172	AC	¼	204	CC	╠	236	EC	∞
141	8D	ì	173	AD	¡	205	CD	═	237	ED	ø
142	8E	Ä	174	AE	«	206	CE	╬	238	EE	ε
143	8F	Å	175	AF	»	207	CF	╧	239	EF	∩
144	90	É	176	B0	░	208	D0	╨	240	F0	≡
145	91	æ	177	B1	▒	209	D1	╤	241	F1	±
146	92	Æ	178	B2	▓	210	D2	╥	242	F2	≥
147	93	ô	179	B3	│	211	D3	╙	243	F3	≤
148	94	ö	180	B4	┤	212	D4	╘	244	F4	⌠
149	95	ò	181	B5	╡	213	D5	╒	245	F5	⌡
150	96	û	182	B6	╢	214	D6	╓	246	F6	÷
151	97	ù	183	B7	╖	215	D7	╫	247	F7	≈
152	98	ÿ	184	B8	╕	216	D8	╪	248	F8	°
153	99	Ö	185	B9	╣	217	D9	┘	249	F9	∙
154	9A	Ü	186	BA	║	218	DA	┌	250	FA	·
155	9B	¢	187	BB	╗	219	DB	█	251	FB	√
156	9C	£	188	BC	╝	220	DC	▄	252	FC	ⁿ
157	9D	¥	189	BD	╜	221	DD	▌	253	FD	²
158	9E	₧	190	BE	╛	222	DE	▐	254	FE	■
159	9F	ƒ	191	BF	┐	223	DF	▀	255	FF	

Başlangıçta haberleşme işlemleri için tasarlanmakla birlikte bilgisayar uygulamalarında geniş yer bulmuştur. 7-bit ikili sayı 128 farklı koddan birisi olarak sunulmaktadır. Böylece, örneğin onluk (decimal) karşılıkları bir dizi halinde “72, 69, 76, 76, 79” kullanıldığında, ASCII kod karşılığı olarak “h, e, l, l, o” kelimesini oluşturmaktadır. ABD ve İngiltere dışında diğer ülke dillerindeki karşılanmayan karakterler sebebiyle biri diğeriyle uyumsuz US-ASCII dışında birtakım farklı ulusal

genişletilmiş kodlar türemiştir. Bu duruma bir son vererek bir standardizasyona gitmek üzere 16-bit (2 Bayt) 65,536 karakter kümesinden oluşan UNICODE geliştirilmiştir. İçerisinde harf, rakam, özel karakterler ve diğer dilbilimsel sembol ve karakterleri içermekte olup günümüzün en önemli dillerinde kullanılmaktadır. İngilizce için Latin Alfabesi'ni, Rusça için Kril Alfabesini, Yunanca, İbranice ve Arapça alfabelerini; Avrupa, Afrika, Hint Yarımadası, Asya (Japonya, Kore, Çin) dillerine ait harf ve sembolleri kapsar.

Yapılan tez çalışmalarında geliştirilen uygulamalardan ilki sayısal ses verileri içerisine metin gömme uygulamasıdır. Bu uygulamada, ses iletişimi yapılırken Ses Gönderici Modülünde bulunan metin kutusuna yazılan tüm metinler ASCII kod karşılıkları bulunduktan sonra ikili sisteme çevrilmekte ve elde edilen veriler ses çerçeveleri içerisine gömülerek gönderilmektedir. Ve bu işlemler zamanlayıcı yardımı ile her saniye tekrar edilmektedir. Aynı şekilde Ses Alıcı Modülde ise gelen ses paketleri içerisinden alının ikili sistemdeki bilgiler onluk sisteme ardından da ASCII kod karşılıklarına göre metin haline getirilmekte ve kullanıcıya sunulmaktadır.

4.2.4. EBCDIC kodları

ASCII kodu kullanılan tek metin kodlama formatı değildir. IBM tarafından 1960'ların başında geliştirilip benimsenen EBCDIC (Extended Binary Coded Decimal Interchange Code) günümüz bilgisayarlarında az da olsa kullanılmaktadır (Tablo 4.4).

Tablo 4.4: EBCDIC kodlarının karakter karşılıkları

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0					(SP)	&	–	ø	Ø	°	µ	¢	ä	å	É	0
	000	016	032	048	064	080	096	112	128	144	160	176	192	208	224	240
1					(RSP)	`	/	\	a	j	ü	£	A	J	÷	1
	001	017	033	049	065	081	097	113	129	145	161	177	193	209	225	241
2					â	ê	Â	Ê	b	k	s	¥	B	K	S	2
	002	018	034	050	066	082	098	114	130	146	162	178	194	210	226	242
3					{	ë	#	Ë	c	l	t	·	C	L	T	3
	003	019	035	051	067	083	099	115	131	147	163	179	195	211	227	243
4					à	è	À	È	d	m	u	©	D	M	U	4
	004	020	036	052	068	084	100	116	132	148	164	180	196	212	228	244
5					á	í	Á	Í	e	n	v	[	E	N	V	5
	005	021	037	053	069	085	101	117	133	149	165	181	197	213	229	245
6					ã	î	Ã	Î	f	o	w	¶	F	O	W	6
	006	022	038	054	070	086	102	118	134	150	166	182	198	214	230	246
7					}	ï	$	Ï	g	p	x	¼	G	P	X	7
	007	023	039	055	071	087	103	119	135	151	167	183	199	215	231	247
8					ç	ì	Ç	Ì	h	q	y	½	H	Q	Y	8
	008	024	040	056	072	088	104	120	136	152	168	184	200	216	232	248
9					ñ	ß	Ñ	é	i	r	z	¾	I	R	Z	9
	009	025	041	057	073	089	105	121	137	153	169	185	201	217	233	249
A					§	¤	ö	:	«	ª	¡	¬	(SH̄Y)	1	2	3
	010	026	042	058	074	090	106	122	138	154	170	186	202	218	234	250
B					.	Å	,	Ä	»	º	¿	|	ô	û	Ô	Û
	011	027	043	059	075	091	107	123	139	155	171	187	203	219	235	251
C					<	*	%	Ö	š	æ	Š	¯	¦	~	@	Ü
	012	028	044	060	076	092	108	124	140	156	172	188	204	220	236	252
D					(	)	_	'	ý	¸	Ý	¨	ò	ù	Ò	Ù
	013	029	045	061	077	093	109	125	141	157	173	189	205	221	237	253
E					+	;	>	=	ž	Æ	Ž	´	ó	ú	Ó	Ú
	014	030	046	062	078	094	110	126	142	158	174	190	206	222	238	254
F					!	^	?	"	±	]	®	×	õ	ÿ	Õ	(EO)
	015	031	047	063	079	095	111	127	143	159	175	191	207	223	239	255

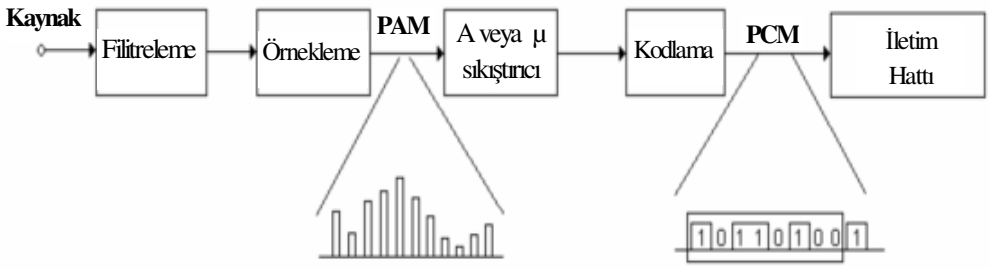
4.3. Analog Ses Sinyallerinin Sayısal Veriye Çevrilmesi

Darbe Kod Modülasyonu (Pulse Code Modulation: PCM), analog işaretlerin belirlenmiş sayısal forma dönüştürülmesini sağlayan bir tekniktir. Bu teknikte analog işaretten sayısal bilgiye ve sayısal bilgiden analog işarete dönüşüm sırasında oluşan örnekleme kayıpları oldukça küçüktür. Bu nedenle PCM günümüzde örnekleme

kayıplarından oldukça etkilenen (konuşma gibi) işaretlerin sayısal formda iletilmesini sağlayan önemli bir tekniktir.

4.3.1. Darbe kod modülasyonu

Sayısal işaretlerin, gürültüden etkilenmemesi ve tüm devre teknolojisinin gelişmesi ile sayısal verinin işlenmesinin (iletilme, sıkıştırma) nispeten daha ucuz olması artık bilgi iletimi, saklanması ve işlenmesi sırasında sayısal formatın analog formata göre tercih edilmesini doğurmuştur. Ancak analog formdaki kaynak bilgisinin sayısal forma dönüştürülmesi sırasında meydana gelen örnekleme ve kodlama hatalarından dolayı alıcıda elde edilen bilgideki bozulma bir problem olarak ortaya çıkmaktadır. Özellikle kaynak verisinin konuşma işaretleri olması, alıcıdaki bozulmayı daha da belirgin hale getirmekte ve sayısal formun konuşma bilgisi için kullanılmasını engellemektedir. PCM yukarıda açıklanan probleme bir çözüm önerisi olarak 1970'li yıllarda ortaya çıkmış ve günümüzde bu amaç için en çok kullanılan sayısallaştırma tekniği olmuştur. PCM'de önce analog işaret örneklenir, sonra kuantalanır ve son olarak da kodlanır. Şekil 4.1'de PCM yapısının şeması görülmektedir.



Şekil 4.1: PCM yapısının şeması

4.3.2. Örnekleme

Örnekleme devresi, analog giriş sinyalini belirlenen frekansta periyodik olarak örnekleyerek çıkışa PAM sinyali olarak aktaran devredir. Burada Nyquist teoremi dikkate alındığında, işaret bantgenişliğinin iki katı frekansında örnekleme yapılmalıdır. Yani ses işareti 4 KHz kabul edildiğinde, saniyede 8000 (2x4000=8000) örnek alınmalıdır. İşaretin örneklenmesi örnekle-tut devreleri yardımı ile yapılmaktadır. Teorik olarak, Nyquist frekansının kullanılması örtüşmeye yol

açmadığı halde, pratikte örnekleme frekansı minimum Nyquist sınırından biraz yüksek tutulur. Örneğin PCM kanallarından iletilecek sesin örnekleme frekansı, ITU-T tarafından f_N=8 KHz olarak belirlenmiştir.

4.3.3. A veya μ kuantalayıcı

A veya μ tipi kuantalama yaklaşımı özellikle ses haberleşmesi uygulamalarında ses işaretlerinin sayısal işaretlere dönüştürülmesi için kullanılmaktadır. Bu tip bir kuantalama işlemine sıkıştırıcı-genleştirmeli kuantalama da denilir. Kuantalama işleminde düzgün dağılımlı olmayan giriş işareti, bir sıkıştırıcıdan geçirilerek daha sık rastlanan düşük genlikli değerlerin arası açılırken, daha düşük olasılıklı yüksek genlikli değerlerin arası sıkıştırılmakta ve bu sayede giriş düzgün dağılımlı hale getirilmektedir. Böylece düzgün dağılımlı hale getirilmiş işaret, doğrusal bir kuantalayıcı ile nicemlenmektedir. Alıcıda PCM kod çözümü yapılırken, kuantalanan işaret seviyelerinin sıkıştırıcının tam tersi bir işlev yerine getiren bir genleştiriciden geçirilmesi sonucu işaret değerleri normal seviyelerine geri getirilmektedir.

4.3.4. PCM kodlayıcı

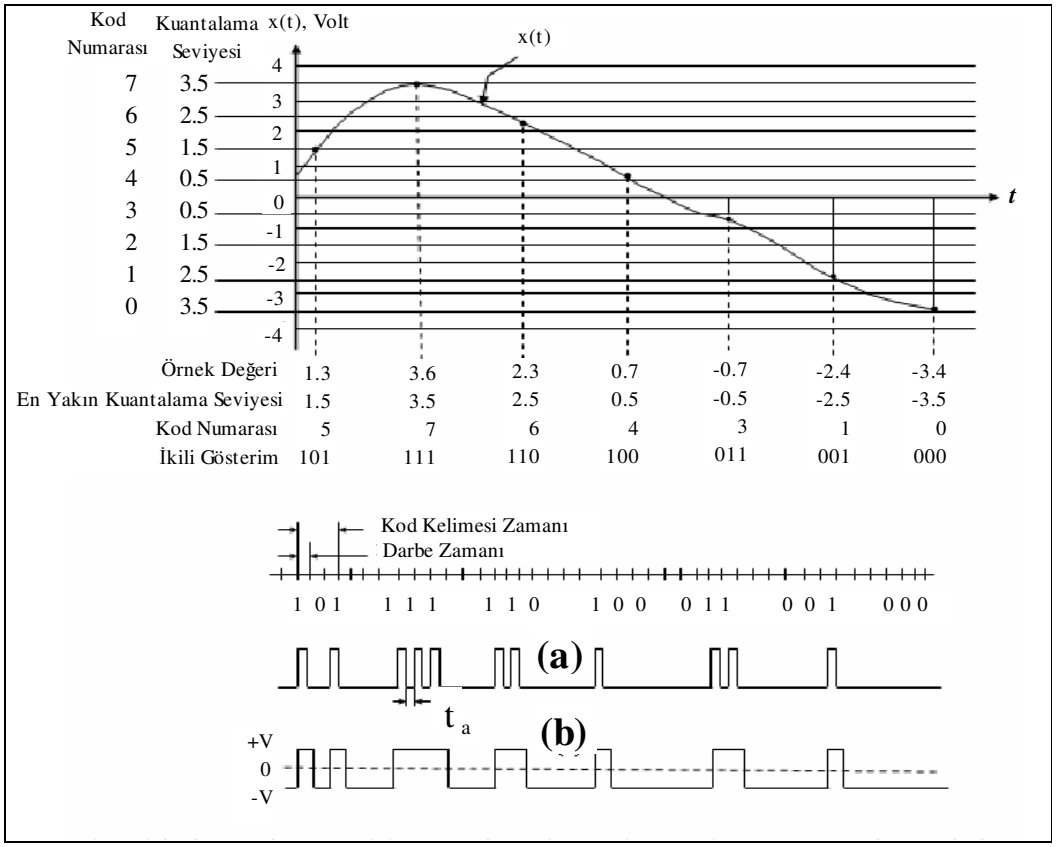
PCM Kodlayıcıda, kuantalanmış örnek değerleri sayısal kod sözcükleri şekline çevrilmektedir. Haberleşmede kuantalanmış örnek değerleri, 8 bitlik ikili kodlar olarak ifade edilmektedir. PCM kullanılan bir haberleşme sisteminde, örneklenen işaret 256 seviyeli olarak kuantalanmakta ve 8 bit ile temsil edilmektedir. Bundan dolayı PCM'li sayısal veri transferi için 8x8000 = 64000 bps yani, 64 Kbps taşıma kapasitesine sahip bir veri iletim kanalına ihtiyaç vardır. Elde edilen bu işarete DS-0 (Digital Signal-0) denir.

Örnekleme sonucu elde edilen genlik değerleri hala analogdur ve minimum genlik ile maksimum genlik arasında herhangi bir değeri alabilirler. Bu örnekleri alıcıya değişmeden iletmek için sonsuz sayıda bit kullanmak gerekir. Oysa, kullanılacak genlik değerlerinin sayısı sınırlı olursa, kullanılacak bit sayısı da sınırlı olur. Daha sonra kuantalanmış işaret belli bir sayı sistemine göre kodlanır. Kuantalanmış işarete,

bir kod kelimesi karşı düşürülür. İkili sayı sisteminde, 1 olan yerlerde örneğin $+V$ genliğinde bir darbe, 0 olan yerlerde ise boşluk göndererek bu kodu iletmek mümkün olur (Şekil 4.2(a)). Daha farklı bir iletim şekli olarak, 1 olan yerlerde $+V$ genliğinde bir darbe, 0 olan yerlerde $-V$ genliğinde bir darbe de iletilebilir (Şekil 4.2(b)). Bu darbelerin genişlikleri kanala uygun şekilde seçilerek, iki darbe arasında güven aralığı (t_g) bırakılabilir. Kuantalama işleminde kullanılan kuanta seviyesi sayısı arttıkça işaret daha iyi temsil edilir. Buna karşılık bir örneği iletmek için gereken bit sayısı artar. İşaret n bit ile kodlanıyorsa, kuanta seviyesi sayısı $Q=2^n$ olmalıdır. Kuantalanmak istenen işaretin maksimum genliği A_{max}, minimum genliği A_{min} ise ve işaretin bu aralıkta değişen genlik değerleri Q adet eşit kuanta seviyesine bölünmek isteniyorsa, kuantalama aralığı veya adımı şöyledir;

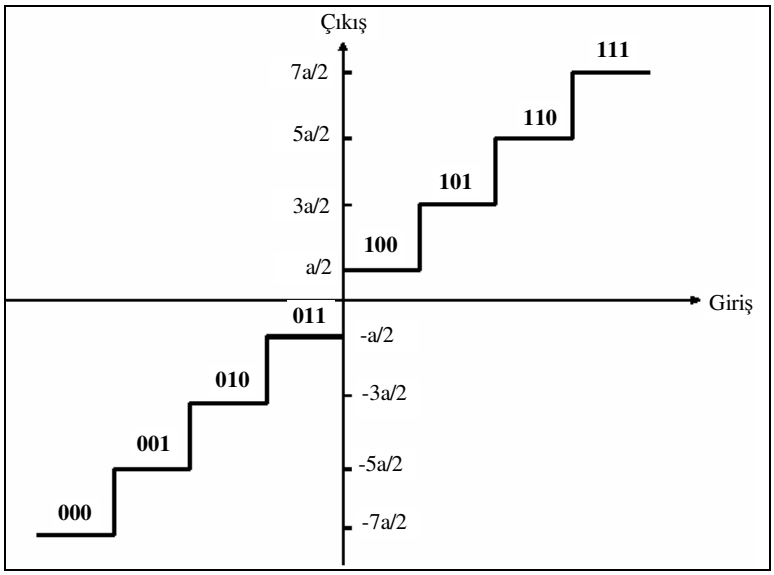
$$a = \frac{A_{max} - A_{min}}{2^n} \tag{4.1}$$

Şekil 4.2'de Q = 8, n = 3 ve a = 1 için örnek bir işleyiş görülmektedir.

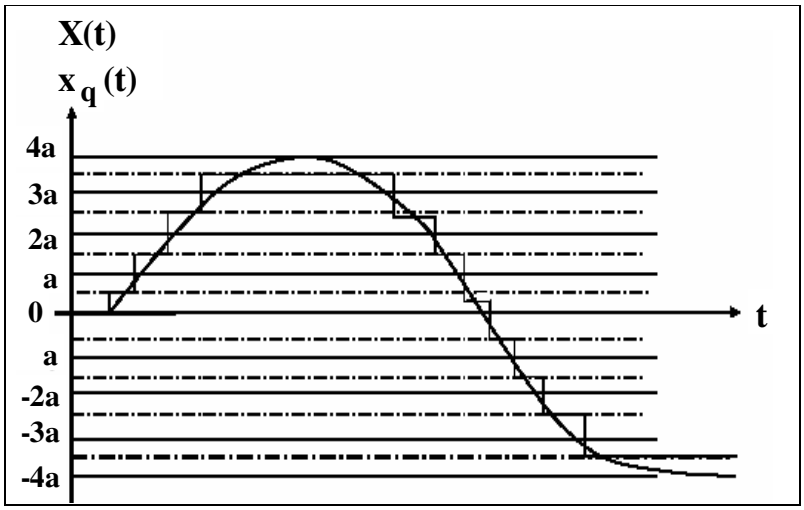


Şekil 4.2: Analog bir işaretin örneklenmesi ve karşılığı olan PCM işaretinin gösterimi

Kuantalama aralıklarının eşit seçildiği kuantalayıcılara düzgün kuantalayıcı adı verilir. Şekil 4.3'de düzgün bir kuantalayıcının giriş-çıkış eğrisi ve karşı düşen kod kelimeleri görülmektedir. Tersinir (reversible) bir işlem olmayan kuantalama sonucunda bir bilgi kaybı olmaktadır. Kuantalanmış örnek işaret X(t), mesaj işareti $x_q(t)$'nin yaklaşık bir değeri olduğundan bir bozulma söz konusudur (Şekil 4.4).



Şekil 4.3: Düzgün kuantalama eğrisi



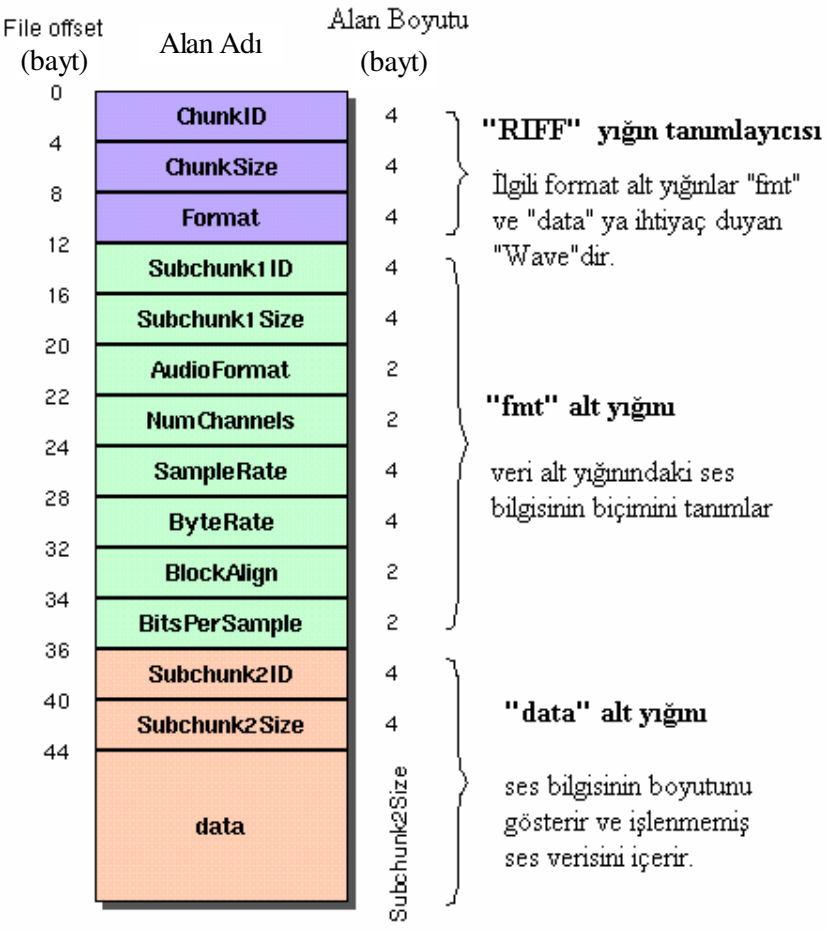
Şekil 4.4: Analog işaret ile kuantalanmış işaret arasındaki hata

Kuantalama hatası etkisi bir toplamsal gürültünün etkisine eşdeğerdir. Bu nedenle bu bozulma kuantalama gürültüsü olarak da adlandırılır. Bu bilgilerden hareketle, tez çalışmalarında hedeflenen amaca ulaşmak için yapılan uygulamalar, zaten

kuantalama hatası sebebi ile bozulmaya uğrayan ses verilerini değiştirerek bozulmayı daha da arttıracak bir etki oluşturmaktadır. Bu sebeple bozucu etkinin çok az olması için veri gömme işlemlerinde, sayısal ses bilgilerinin en düşük değerlikli bitleri kullanılmaktadır. Yukarıdaki anlatılanlar göz önünde bulundurulduğunda gerçek zamanlı olarak sayısal ses verilerine ulaşılıp, bu verilerin son bitlerinin değiştirilerek alıcıya gönderilmesi işleminde bozulma oranı ile birlikte, verilerin aktarım hızı ve yapılan örnekleme sayısı çok büyük önem kazanmaktadır.

4.3.5. PCM ses verisi formatı

Ses kartından alınan analog sesler, bilgisayar ortamında PCM yöntemi ile sayısallaştırılmaktadır. Standart olarak alınan ses bilgileri ".wav" dosya tipindedir. Bu tip bir dosya yapısının ilkel versiyonu ise Microsoft'un ".riff" (Resource Interface File Format) uzantılı dosya yapısıdır. "Wave" ses dosyasının yapısı Şekil 4.5'de sunulmaktadır.



Şekil 4.5: Kurallara uygun wave dosya formatı

Yukarıda görüldüğü üzere ilgili ses dosyasının yapısı temel olarak 3 bölümden oluşmaktadır. Bunlar "RIFF" yığın tanımlayıcısı, "fmt" alt yığını ve "data" alt yığınıdır. Tablo 4.5'de RIFF yığın tanımlayıcı bilgileri görülmektedir.

Tablo 4.5: RIFF yığın tanımlayıcısı

Boyut (Bayt)	Ad	Açıklama
4	ChunkID	ASCII biçimindeki "RIFF" yazısını içerir.
4	ChunkSize	Yığın boyutunu içerir.
4	Format	ASCII biçiminde "WAVE" bilgisini içerir.

İnsanların soldan sağa veya sağdan sola doğru okunan farklı alfabelere sahip olmaları gibi işlemciler de baytları saklarken en büyük değerlikli (MSB) baytın solda veya sağda olmasına göre sınıflandırılır.

“fmt” alt yığını ses verisinin formatını tanımlamaktadır. “fmt” alt yığını bilgileri Tablo 4.6’da görülmektedir.

Tablo 4.6: “fmt” alt yığını

Boyut (Bayt)	Ad	Açıklama
4	Subchunk1ID	“fmt” yazısını içerir.
4	Subchunk1Size	PCM için 16’dır.
2	Audioformat	PCM için 1’dir. Sıkıştırma tiplerinin bazıları için 1’den faklı değerler mevcuttur.
2	NumChannels	Mono için 1, Stereo için 2’dir.
4	SampleRate	8000, 44100 gibi örnek oranlarıdır.
4	ByteRate	= SampleRate x NumChannels x BitsPerSample/8
2	BlockAlign	= NumChannels x BitsPerSample/8
2	BitsPerSample	8 bit için 8, 16 bit için 16.

“data” alt yığını verinin boyutunu ve güncel ses bilgisini içermektedir. “data” alt yığını bilgileri Tablo 4.7’de görülmektedir.

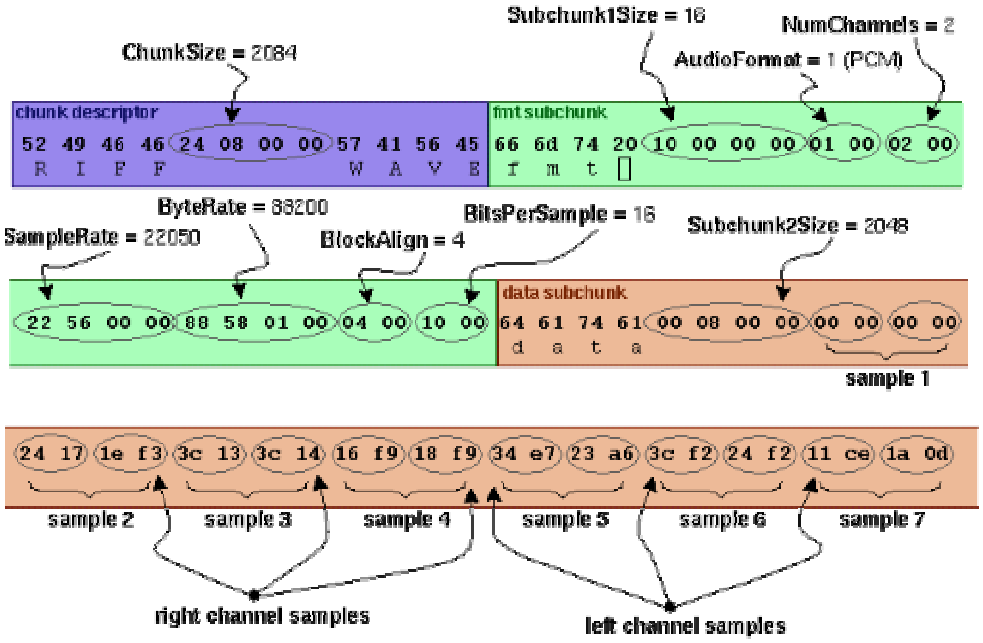
Tablo 4.7: “data” alt yığını

Boyut (bayt)	Ad	Açıklama
4	SubChunk2ID	“data” yazısını içerir.
4	SubChunk2Size	= NumSamples x NumChannels x BitsPerSample/8 (Bu bilgi, data bölümünde bulunan veri boyutu bilgisidir.)
n	Data	Güncel ses bilgisi (44.bayttan itibaren).

Yapılan tez çalışmalarında, Şekil 4.5’de görülen “data” alt yığınındaki veriler üzerinde değişiklikler yapılarak stenografi uygulaması gerçekleştirilmektedir. RIFF yığın tanımlayıcısı ve fmt alt yığını üzerinde yapılacak herhangi bir değişiklik orijinal ses verisinin yapısını bozacağından ses haberleşmesinin gerçekleşmesine engel teşkil etmektedir. Aşağıda onaltılık (hexadecimal) sayı sisteminde verilmiş 72 bayt boyutunda Wave dosya bilgisi verilmektedir:

52 49 46 46 24 08 00 00 57 41 56 45 66 6d 74 20 10 00 00 00 01 00 02 00
22 56 00 00 88 58 01 00 04 00 10 00 64 61 74 61 00 08 00 00 00 00 00 00
24 17 1e f3 3c 13 3c 14 16 f9 18 f9 34 e7 23 a6 3c f2 24 f2 11 ce 1a 0d

Şekil 4.6'da bu bilgilerin bir ses dosyasında yerleşimi verilmektedir.



Şekil 4.6: Örnek bir ses dosyası

4.4. Sonuç

Görüldüğü gibi insan sesi analog veriler içermektedir. Bilgisayarlar bu verileri ancak sayısallaştırarak depolayabilmekte veya çalabilmektedir. Analog ses verilerinin sayısallaştırılması süreci tez çalışmaları açısından önem arz etmektedir. Anlaşılacağı üzere bu sayısallaştırma sürecinde birim zamanda alınan örnek sayısı ile seste meydana gelecek olan bozulma arasında ters orantı söz konusudur. Bu nedenle birim zamanda ne kadar fazla örnek alınırsa gerçek sese o kadar yakınlaşılmış olmaktadır.

Veriler bilgisayarlarda ikili sistemdeki sayılar şeklinde (0 veya 1) ifade edilmektedir. Bu zorunluluk karakterlerin de sayısal karşılıklarının oluşturulması için kodlama sistemlerinin geliştirilmesine sebep olmuştur. Bunlardan en çok kullanılanı ASCII kodlama sistemidir. Yapılan tez çalışmalarında geliştirilen uygulamalardan birincisi sayısal ses verileri içerisine metin gömme uygulamasıdır. Bu uygulamada kablosuz

ses iletişimi yapılır iken Ses Gönderici Modülde bulunan metin kutusuna yazılan tüm metinler ASCII kod karşılıkları bulunduktan sonra ikilik sisteme çevrilmekte ve elde edilen veriler ses çerçeveleri içerisine gömülerek gönderilmektedir.

5. SAYISAL SES İÇERİSİNDE GİZLİ VERİ/DOSYA TRANSFERİNİN KABLOSUZ ORTAMDA GERÇEKLEŞTİRİLMESİ

5.1. Giriş

Bu bölümde, geliştirilen iki adet stenografi uygulaması hakkında bilgiler verilerek, alt bölümlerde bu uygulamaların çalışma prensipleri ve algoritmaları detaylı şekilde anlatılmaktadır.

Tez çalışmaları, gerçek zamanlı kablosuz sayısal ses haberleşmesinin üzerine, iki temel uygulama yapılarak sunulmaktadır. Gerçek zamanlı kablosuz ses haberleşmesi yapılır iken, birincisi gönderilecek sayısal ses bilgilerine metin gömme, diğeri ise sayısal ses haberleşmesi yapılır iken, gönderilecek sayısal ses bilgilerine kullanıcının istediği herhangi bir veri kümesini/dosyayı (özellikle ses dosyalarını) gömme uygulamasıdır.

Yapılan çalışmalarda kablosuz haberleşme özelliğine sahip olan 2 adet diz üstü bilgisayar (P4 3.2 GHz, 384 MB RAM ve Celeron 1.7 GHz, 224 MB RAM) ve bir adet erişim noktası (U.S. Robotics 54 MBit/s) kullanılmaktadır.

İlgili uygulamalar Borland Delphi 7.0'da geliştirilmektedir ve temel olarak Network Multi Medya (NMM) bileşeninden (component) faydalanılmaktadır. Görüntü özelliklerinin Windows XP'ye uyumlu olması açısından dosya gönderme uygulamasında "Jedi" bileşeni kullanılmaktadır. İlgili uygulamalarda "main.pas" dosyalarının dışında bir çok "pas" uzantılı dosya kullanılmaktadır. Bu dosyaların önemlileri şunlardır.

- NMMP2PVoiceServer.pas (Gelen verinin hangi aşamada olduğunu tespit etmektedir).

- NMMVoiceClient.pas, (Giden verinin hangi aşamada olduğunu tespit etmektedir).
- NMMAudioPlayThread.pas (Gömülü verileri ayırt etme işlemi yapmaktadır).
- NMMAudioRecordThread.pas (Verileri gömme işlemi yapmaktadır).

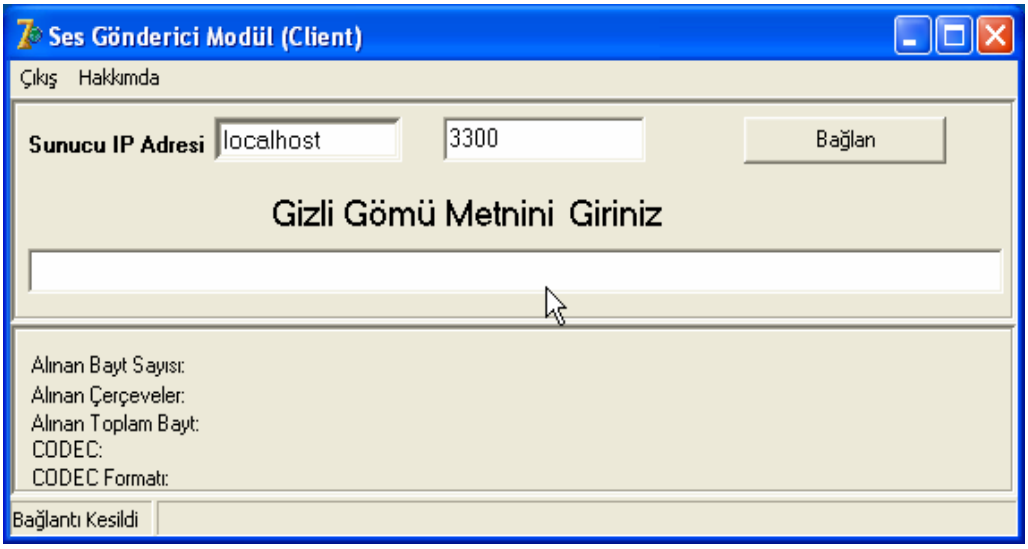
Bu dosyalar temel olarak yanlarında belirtilen işlevlere sahip olup, kaynak kodları Ek-A ve Ek-B'de verilmektedir. İzleyen alt bölümlerde tez çalışması olarak gerçekleştirilen uygulamalar detaylı bir şekilde anlatılmaktadır.

5.2. Sayısal Ses İçerisinde Gizli Metinlerin (SSGM) Kablosuz Transferi İçin Geliştirilen Yazılım

Geliştirilen bu yazılımda ses kartından birim zamanda (1 saniye) 8000 örnek bilgisi alınmakta ve ilgili örneklerin (her bir örnek 1 bayt) en küçük değerlikli bitine, gömü verisi olan metnin ilgili biti yerleştirilerek gönderilmektedir (Ses Gönderici Modül). Aynı şekilde bu gizli metinleri sezerek kullanıcıyı bilgilendiren algoritma da geliştirilmiş olup, detayları takip eden bölümlerde anlatılmaktadır (Ses Alıcı Modül). Uygulamada örtü verisi olan ses verileri değiştirilirken, sesin orijinal şeklinde bozulmanın algılanamayacak seviyede olmasına özen gösterilmektedir. Şekil 5.1'den Şekil 5.7'ye kadar, gerçekleştirilen uygulamanın ekran görüntüleri verilmektedir.

5.2.1. SSGM kablosuz transferi için geliştirilen yazılımın kullanıcı arayüzleri

Uygulamanın başlatılması için ilk olarak erişim noktası (Access Point, AP) ile birbirine bağlanmış olan iki adet bilgisayardan birinde Ses Gönderici (Client) Modül diğerinde ise Ses Alıcı (Server) Modül çalıştırılarak ses haberleşmesinde temel adım atılmış olmaktadır. Ses gönderici modül çalıştırıldığında Şekil 5.1'deki ekran görüntüsü elde edilmektedir.



Şekil 5.1: Ses Gönderici Modülün başlangıç görünümü (Metin için)

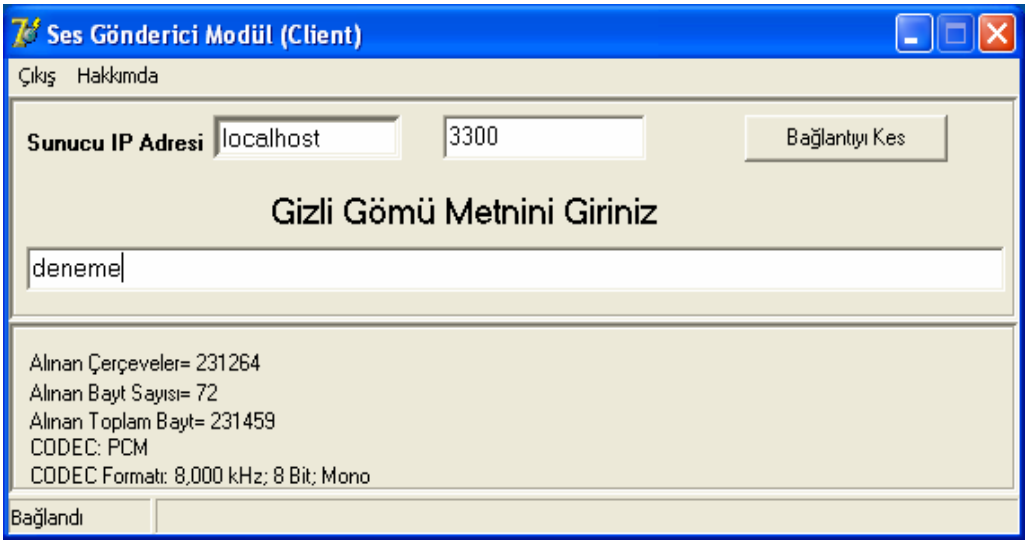
Bu modül ilk açıldığı anda IP adresi "localhost", port ise "3300" olarak belirlenmiş şekilde ekrana gelmektedir. Kullanıcı, "Server IP Adresi" olarak belirtilmiş olan kısma, ses bilgilerini alacak olan bilgisayarın IP adresini yazmalı ve ardından "Bağlan" butonuna basmalıdır.

Ses Alıcı Modül çalıştırıldığında ise kullanıcı Şekil 5.2'deki görüntüyü elde etmektedir.

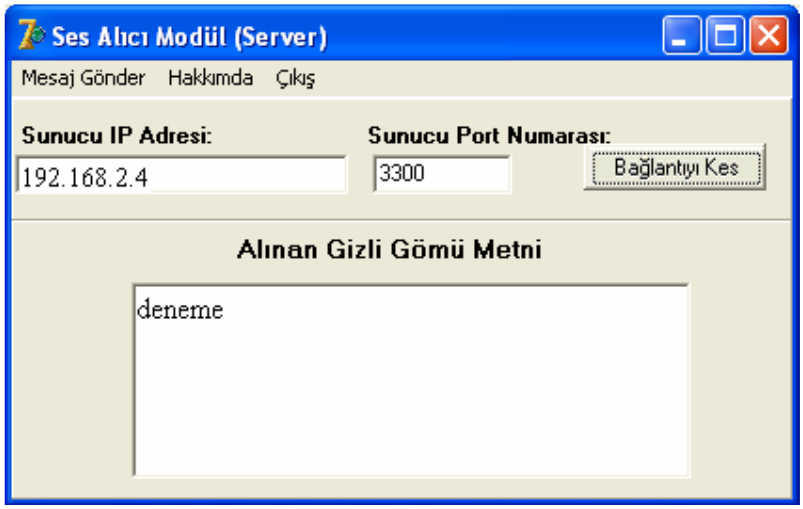
Şekil 5.2: Ses Alıcı Modülün başlangıç görünümü(Metin için)

Bu modülde ise ilk ekran görünümünde Server IP kısmı boş, Server Port kısmı ise "3300" olarak ekrana gelmektedir. Kullanıcı bu noktalara herhangi bir şekilde müdahale edememektedir. Kullanıcı "Dinle" butonuna bastığında; modülün,

kullanılan bilgisayarın IP numarasını alıp ilgili kutucuğa otomatik olarak yazması sağlanır. Şekil 5.3 a ve Şekil 5.3 b'de bu işlem yapılarak, ses iletişiminin başlatıldığı bir uygulama görüntüsü verilmektedir.



(a)



(b)

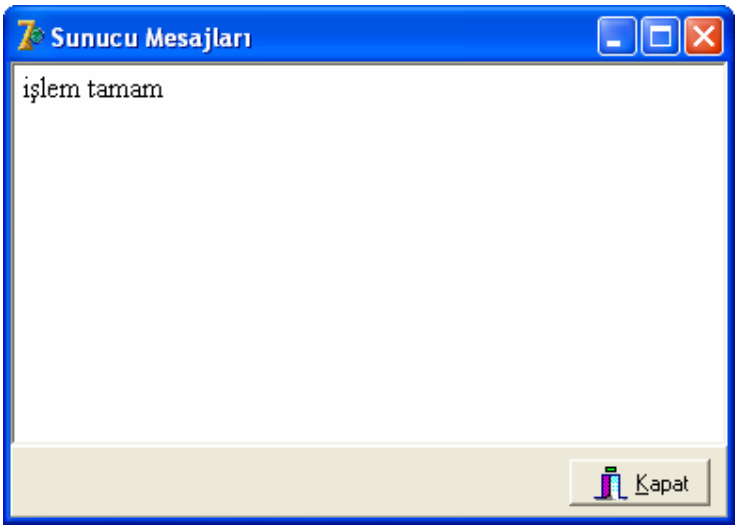
Şekil 5.3: Ses Gönderici Modülün ve Ses Alıcı Modülün iletişim başladığındaki görünümü (Metin için)

Ses Alıcı Modül adından da anlaşılacağı üzere ses bilgilerini alan bir uygulama parçasıdır. Ses Gönderici Modüle herhangi şekilde ses gönderememektedir. Bu nedenle, Ses Gönderici Modüle bilgi verilmek istendiğinde kullanmak üzere bu modülde menüler içerisinde "Mesaj Gönder" seçeneğine yer verilmektedir. Bu seçenek yardımı ile Ses Alıcı Modül kullanıcısı, Ses Gönderici Modülün

kullanıcısına yazılı mesaj gönderebilmektedir. Mesaj gönder menüsüne tıklandığında Şekil 5.4'deki görüntü elde edilmektedir.

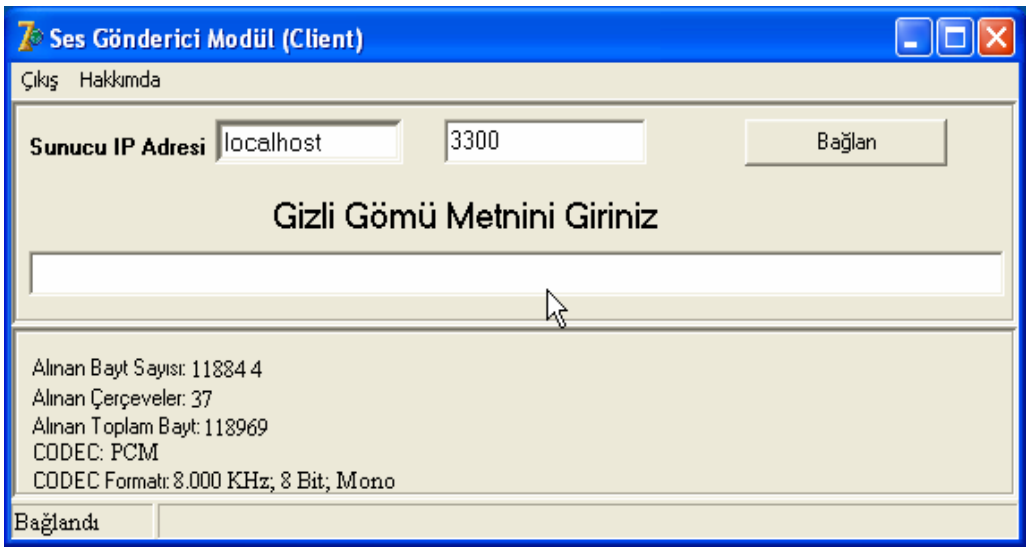
Şekil 5.4: Mesaj gönderme penceresinin görünümü

Kullanıcı ekrana gelen pencereye göndermek istediği mesajı yazarak "Gönder" butonuna bastığında, Ses Gönderici Modülde aşağıdaki pencerenin görünmesi sağlanmış olur.



Şekil 5.5: Mesaj alma penceresinin görünümü

Görüldüğü üzere bu işlem ile karşılıklı haberleşme sağlanmış olmaktadır. Ses Gönderici Modül sunucu IP adresini ilgili kutucuğa yazıp bağlantının başlatılmasını sağlayacak olan butona bastıktan sonra hem ses haberleşmesi başlamış olur, hem de gizli metin bilgilerini gönderebilme özelliği aktif edilmiş olunur. Kullanıcıya istatistiki bilgilerin verilmesi açısından da Ses Alıcı Modülün aldığı çerçeveler (her biri 3200 bayt), alınan çerçeve sayıları (çerçevex3200) ve CODEC formatı bilgisi verilmektedir. Şekil 5.6'da çalışma esnasında elde edilen bir görüntü örneği verilmektedir.



Şekil 5.6: Ses Gönderici Modülün bağlantı sonrası görünümü (Metin için)

Modülde görülen "Hakkımda" menüsünde ise program uyarlaması ve yazar hakkında bilgi verilmektedir.

Şekil 5.7: Hakkımda penceresinin görünümü

5.2.2. SSGM kablosuz transferi için geliştirilen yazılımın ses gönderici modülünün çalışma prensibi ve akış diyagramı

Bu alt bölümde ilgili uygulamanın metin gömmeyi gerçekleştiren Ses Gönderici Modülünün akış şeması ve algoritması hakkında bilgi verilmektedir.

İlk olarak Bölüm 5.2.1'de da açıklaması yapılan başlangıç ayarları (program çalıştırılarak sunucu IP adresinin yazılması ve bağlan butonuna tıklanması) yapılır.

Ve ses iletişimi başlatılır (burada diğer modülün de çalışır vaziyette olduğu varsayılmaktadır).

Ses iletişimi yapılırken bu modülde bulunan metin kutusu, üzerinde yapılacak değişimlere duyarlıdır. Üzerinde herhangi bir değişiklik yapılmadığı sürece, yani herhangi bir metin yazılmadığı sürece, ses iletişimi normal şekilde devam etmektedir. Metin kutusuna herhangi bir metnin girilmesi durumunda, o andan itibaren gönderilecek ilk 3200 baytlık pakete başlat bilgisi (uygulamada başlat bilgisi 0011111100 olarak belirlenmektedir), yazılmış olan metnin boyutu ve metnin kendisi gömülür. Başlat bilgisi paketin 11—20. baytlık bölümlerinin son bitlerine yazılır. Örnek bir başlat bilgisi gömme uygulaması Tablo 5.1'de gösterilmektedir.

Tablo 5.1: Ses çerçevesine başlat bilgisinin gömülmesi

Çerçevedeki Sıra	**Orijinal Ses Verisi (Rastgele Belirlenmiştir)**	**Son Durum**
11. bayt	1 1 0 0 1 0 1 **1**	1 1 0 0 1 0 1 **0**
12. bayt	0 0 1 0 0 1 1 **0**	0 0 1 0 0 1 1 **0**
13. bayt	0 1 0 0 1 1 1 **0**	0 1 0 0 1 1 1 **1**
14. bayt	0 0 1 1 1 0 0 **1**	0 0 1 1 1 0 0 **1**
15. bayt	1 1 1 0 0 1 1 **0**	1 1 1 0 0 1 0 **1**
16. bayt	1 1 0 0 1 1 0 **1**	1 1 0 0 1 1 0 **1**
17. bayt	0 0 0 1 1 0 0 **0**	0 0 0 1 1 0 0 **1**
18. bayt	0 0 0 1 1 0 1 **0**	0 0 0 1 1 0 1 **1**
19. bayt	1 0 0 1 0 0 1 **0**	1 0 0 1 0 0 1 **0**
20. bayt	0 0 1 1 1 0 1 **1**	0 0 1 1 1 0 1 **0**

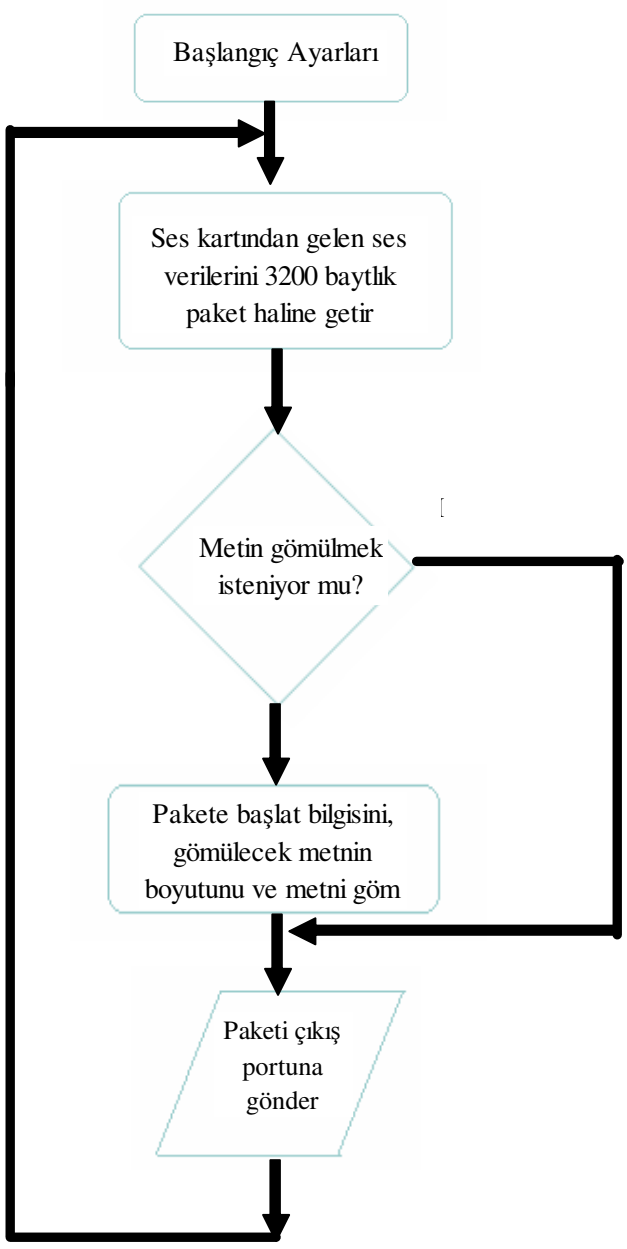
Aynı şekilde 21—30. baytlar arasındaki 8'li ses verilerinin son bitlerine de gönderilecek metnin boyutu gömülmektedir. Bu sayede Ses Alıcı Modül, paket içerisinde nereye kadar gizli verinin gömülü olduğunu öğrenmektedir. Sonrasında ise yazılmış olan metnin her bir karakteri ASCII kod tablosunda belirtildiği şekli ile ondalık sayıya ardından ikili sayı sistemindeki ifadelere çevrilmektedir (örneğin "a" harfinin kod tablosundaki karşılığı 97'dir. Bu rakam ikilik sisteme çevrildiğinde ise 110 0001 ifadesi elde edilir). Metnin ikili sistemdeki karşılığı 31.bayttan itibaren gönderilecek pakete gömülmektedir. Gömülecek verilerin bitimi ile birlikte paket

çıkış portu olan 3300 portuna gönderilmektedir. Bu işlemler kullanıcının her yazdığı karakter sonrasında tekrar tekrar gerçekleştirilmektedir.

Tablo 5.2: Metin ile ilgili bilgilerin ses çerçevesi içerisindeki yerleri

Çerçevedeki Sıra	**Gömülen Veri**
11 - 20. bayt	Başlat bitleri (0011111100 olarak rastgele belirlenmektedir).
21 – 30. bayt	Gömülecek metnin boyut bilgisi.
31 – n. bayt	Gömülecek metin (Metnin boyutuna göre bitiş baytı (n) değişmektedir).

Yukarıdaki açıklamalar göz önünde bulundurulduğunda, ilgili 3200 baytlık ses verilerinin içerisine başlat bilgisi ve metnin boyutu gömüldükten sonra kalan 3170 baytlık kesimin son bitlerine yaklaşık 396 karakter (3170/8=396,25) bilgisinin gömülebileceği ortaya çıkmaktadır (her bir karakter 8 bitten oluşmaktadır ve veri gömme kapasitesi 3170 bitten ibarettir). 1 saniyede gönderilebilecek olan bu veri kapasitesi oldukça iyi bir başarım olarak değerlendirilmektedir. Gerçekleştirilen Ses Gönderici Modül akış şeması Şekil 5.8'de görülmektedir.



Şekil 5.8: Ses Gönderici Modülün akış diyagramı (Metin için)

5.2.3. SSGM kablosuz transferi için geliştirilen yazılımın ses alıcı modülünün çalışma prensibi ve akış diyagramı

Bu alt bölümde ilgili uygulamanın, gömülü metinleri ayırt eden Ses Alıcı Modülünün akış şeması ve algoritması hakkında bilgi verilmektedir.

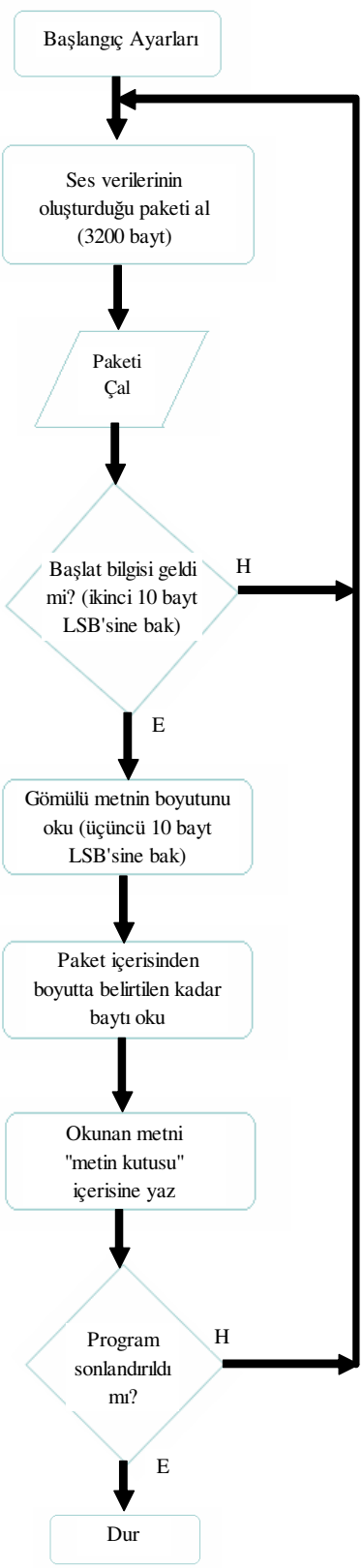
İlk olarak Bölüm 5.2.1'de açıklanan başlangıç ayarları (program çalıştırılarak dinle butonuna basılır) yapılmaktadır. Ve ses iletişimi başlatılmaktadır (burada diğer modülünde çalışır vaziyette olduğu varsayılmaktadır).

NMM bileşeni yardımı ile ilgili IP adresinden gelen 3200 baytlık ses bilgisi elde edilmektedir. Ve ardından gelen tüm paketler kesintiye uğramaksızın bilgisayarda kullanıcının duyacağı ses bilgileri şeklinde çaldırılmaktadır.

Gelen ses paketleri içerisinde sürekli olarak ikinci 10 baytlık (11—20.bayt) ses bilgilerinin son bitleri kontrol edilmekte ve beklenen başlat (start) bilgisi ile aynı olup olmadığı (başlat bilgisi: 0011111100) karşılaştırılmaktadır. Eğer başlat bilgisi gelmemişse sonraki paket beklenmekte ve tekrar gelen pakete bakılmaktadır.

Başlat bilgisinin gelmesi durumunda, bu bilgiyi taşıyan paketin üçüncü 10 baytlık (21—30.bayt) bölümünün son bitlerine bakılarak gömülmüş olan verinin boyutu elde edilmektedir. Bu boyut bilgisi algoritma için ilgili paket içerisindeki gizli veriyi okuma işleminin sonlanacağı noktayı belirtmektedir.

İlgili boyut bilgisi de okunduktan sonra paket içerisinden 31. bayttan itibaren bitler okunmakta ve ASCII kod tablosundaki yerlerine göre metnin detayları belirlenmektedir. Belirlenmiş olan metin, modülün kullanıcı arayüzünde bulunan metin kutusuna yazılmaktadır. İlgili işlemler program sonlandırılıncaya kadar devam etmektedir. Şekil 5.9'da bu modülün akış şeması verilmektedir.



Şekil 5.9: Ses Alıcı Modülün akış diyagramı (Metin için)

5.3. Sayısal Ses İçerisinde Gizli Gömü Verilerinin/Dosyalarının (SSGD) Kablosuz Transferi İçin Geliştirilen Yazılım

Yapılan çalışmalarda, diğer uygulamada olduğu gibi kablosuz haberleşme özelliğine sahip olan 2 adet diz üstü bilgisayar (P4 3.2 GHz, 384 MB RAM ve Celeron 1.7 GHz, 224 MB RAM) ve bir adet erişim noktası (U.S. Robotics 54 MBit/s) kullanılmaktadır.

İlgili uygulama Borland Delphi 7.0'da geliştirilmiş olup, temel olarak Network Multi Medya (NMM) bileşeninden (component) faydanlanılmaktadır. Ses kartından birim zamanda (1 saniye) kullanıcının istediği kadar (8000, 11025, 16000, 22050, 32000 veya 44100) örnek bilgisi alınmakta ve ilgili örneklerin en küçük değerlikli bitine, gömülmek istenen dosyanın ilgili bitleri yerleştirilerek gönderilmektedir (Ses Gönderici Modül). Aynı şekilde bu verileri sezerek gömülmüş olan veriyi tespit eden algoritma da geliştirilmiş olup detayları izleyen alt bölümlerde anlatılmaktadır (Ses Alıcı Modül).

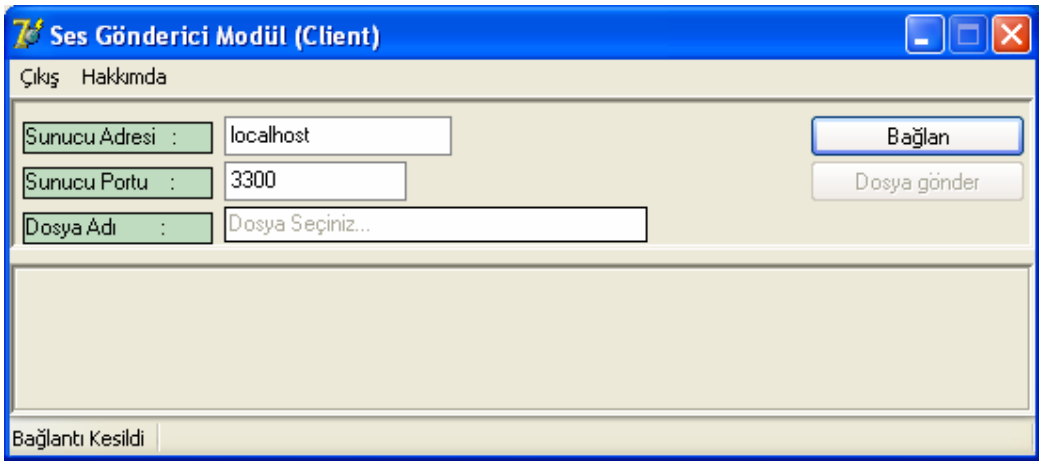
Geliştirilen uygulamada ses verileri değiştirilirken, meydana gelecek olan bozulmanın algılanamayacak seviyede olmasına özen gösterilmektedir. Bölüm 5.3.1—5.3.3'de gerçekleştirilen uygulamanın kullanıcı arayüzleri, çalışma prensipleri ve akış şemaları verilmektedir.

5.3.1. SSGD kablosuz transferi için geliştirilen yazılımın kullanıcı arayüzleri

Uygulamanın başlatılması için ilk olarak erişim noktası (Access Point, AP) ile birbirine bağlanmış olan iki adet bilgisayardan birinde Ses Gönderici(Client) modül diğerinde ise Ses Alıcı (Server) modül çalıştırılarak kablosuz sayısal ses haberleşmesinde temel adım atılmış olmaktadır.

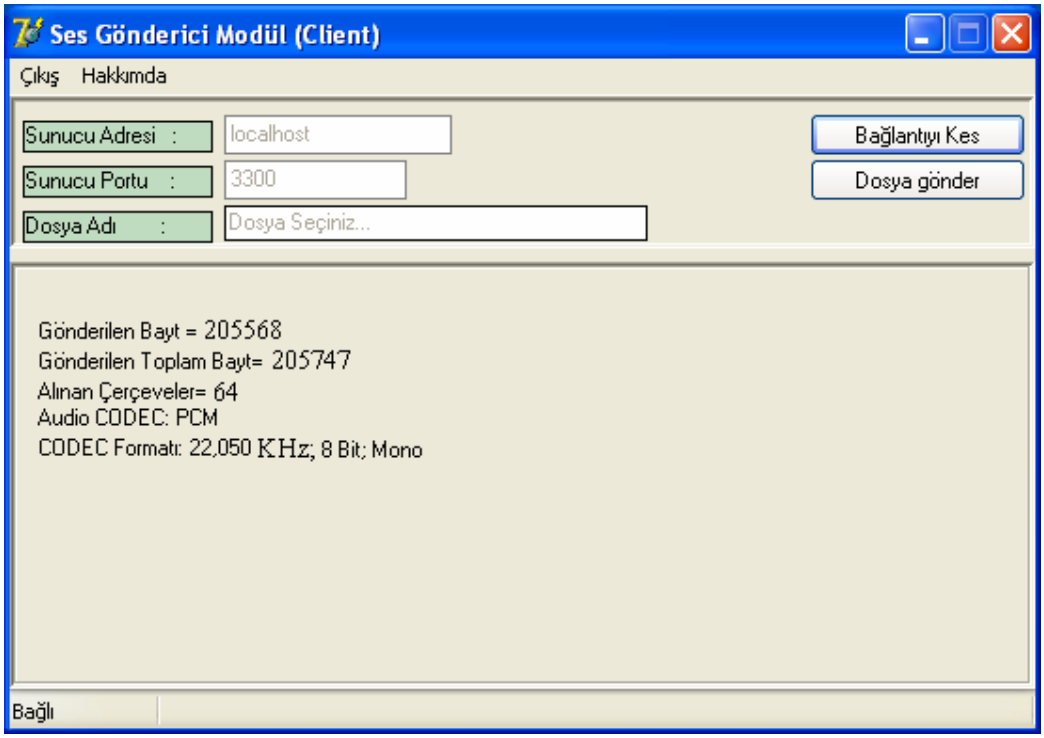
Ses Gönderici Modül ilk açıldığı anda IP adresi "localhost", port ise "3300" olarak belirlenmiş şekilde ekrana gelmektedir. Kullanıcı "Server IP Adresi" olarak

belirtilmiş olan kısma, ses bilgilerini alacak olan bilgisayarın IP adresini yazmalıdır. Ses Gönderici Modül çalıştığında Şekil 5.10'daki ekran çıktısı elde edilmektedir.



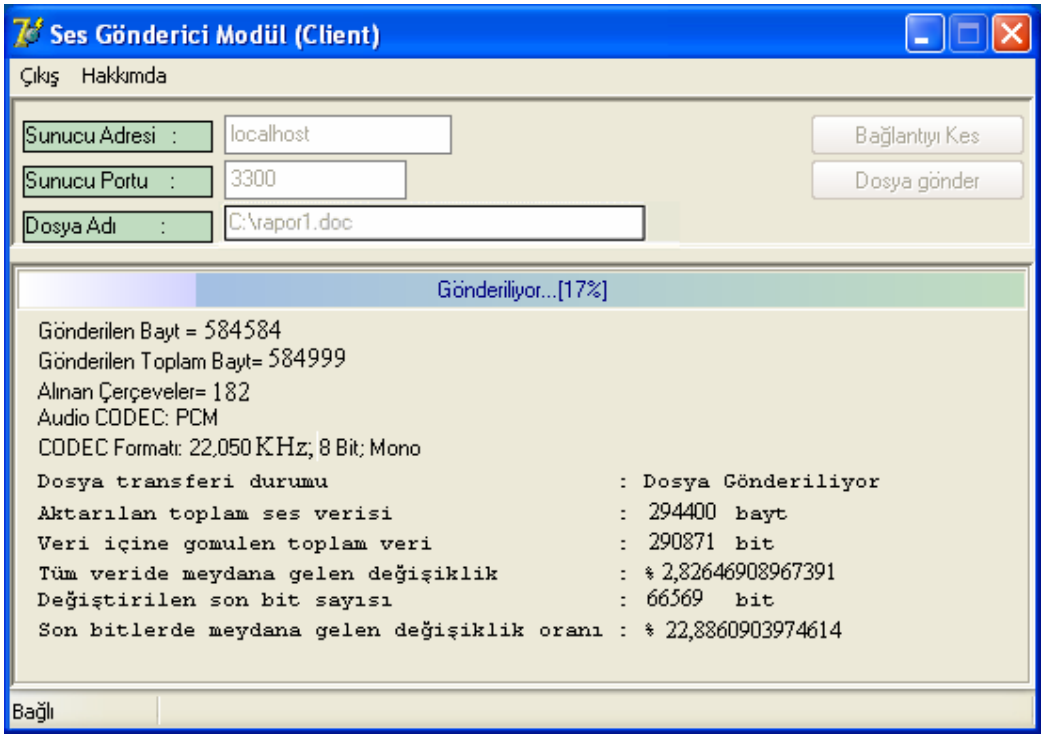
Şekil 5.10: Ses Gönderici Modülün başlangıç görünümü (Dosya için)

Kullanıcı, sunucu adresini yazıp bağlan butonuna bastığında ses iletişimini başlatmış olmaktadır. Ve ilgili istatistiki bilgilerde görünmeye başlamaktadır. Şekil 5.11'de bu durumu gösteren bir ekran çıktısı verilmektedir.



Şekil 5.11: Ses Gönderici Modülün çalışma görünümü (Dosya için)

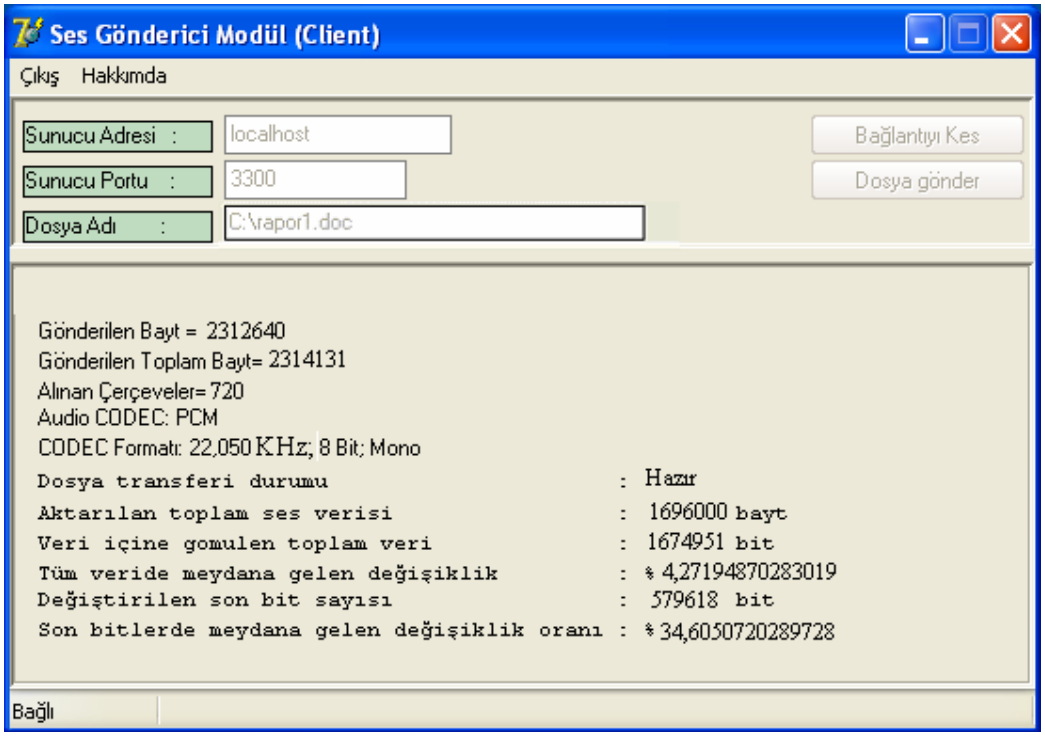
Kullanıcı, herhangi bir anda dosya gönder yazan butona tıklayarak istediği bir dosyayı gönderebilmektedir. Dosya gönderimi yapılmaya başlandığı andan itibaren, dosya gönderim oranını belirten bir durum belirteci de ekranda görünmektedir. Bununla birlikte dosya gönderimi boyunca, taşıyıcı ses verilerindeki yüzdelik değişimi ve diğer istatistiki bilgiler de ekrana gelmektedir. Şekil 5.12'de bu durumu gösteren bir ekran çıktısı verilmektedir.



Şekil 5.12: Ses Gönderici Modülün veri aktarımı yapıldığı andaki görünümü (Dosya için)

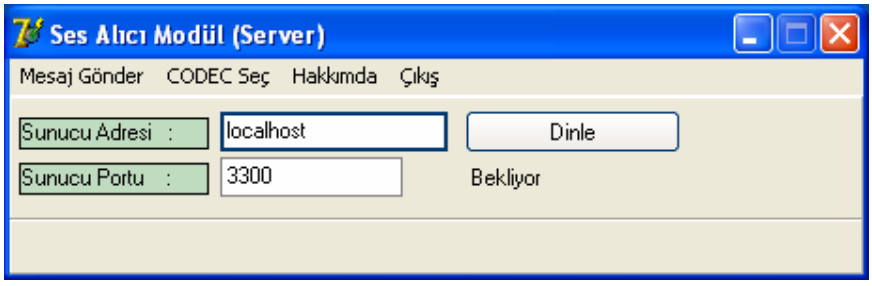
Yukarıdaki şekilde görülen istatistikler dosya gönderimi boyunca değişmektedir. İlgili dosyanın gönderimi sırasında değişimlerin hangi oranda olduğu, yani net sonuçlar dosya gönderimi tamamlandıktan sonra belli olmaktadır.

Şekil 5.13'de bir dosya gönderimi işlemi tamamlandıktan sonra elde edilen son görüntü ve istatistikler verilmektedir. Ekran görünümünden de anlaşılacağı üzere ilgili dosya gönderilirken, taşıyıcı ses verilerinin % 34,6 oranındaki kısmı son bitlerinin değişimi anlamında farklılaşmış görünmektedir. Ancak bu ses verileri matrissel anlamda (tüm veride meydana gelen değişiklik) düşünüldüğünde, taşıyıcı ses verilerinin bit düzeyinde % 4,27'si değişmiş olarak yansımaktadır.



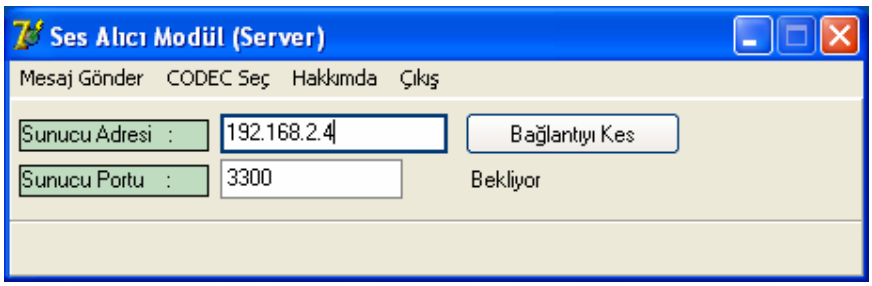
Şekil 5.13: Ses Gönderici Modülün veri aktarımı yapıldıktan sonraki görünümü (Dosya için)

Ses Alıcı modül açıldığında ise kullanıcı ilk olarak Şekil 5.14'deki görüntüyü elde etmektedir.



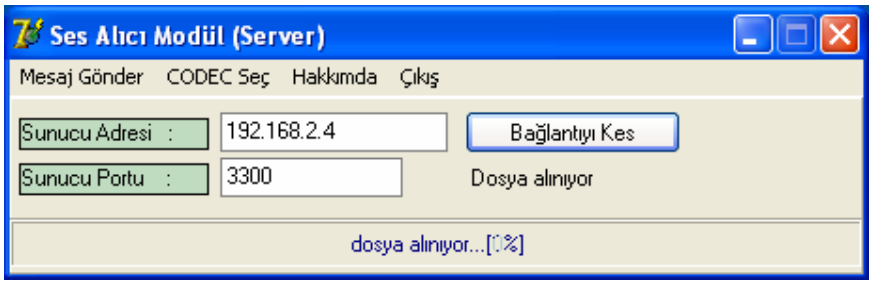
Şekil 5.14: Ses Alıcı Modülün çalıştırıldığı andaki görünümü (Dosya için)

Bu modülde ilk ekran görünümünde Sunucu Adresi kısmı "localhost", Sunucu Portu kısmı ise "3300" olarak belirlenmiş olarak ekrana gelmektedir. Kullanıcı "Dinle" butonuna bastığında; modülün, IP numarasını sistemden alarak ilgili kutucuğa otomatik olarak yazmasını sağlamaktadır. Şekil 5.15'de bu işlemin yapılarak, ses iletişiminin başlatıldığı bir ekran çıktısı verilmektedir.



Şekil 5.15: Ses Alıcı Modülün iletişim başladığındaki görünümü (Dosya için)

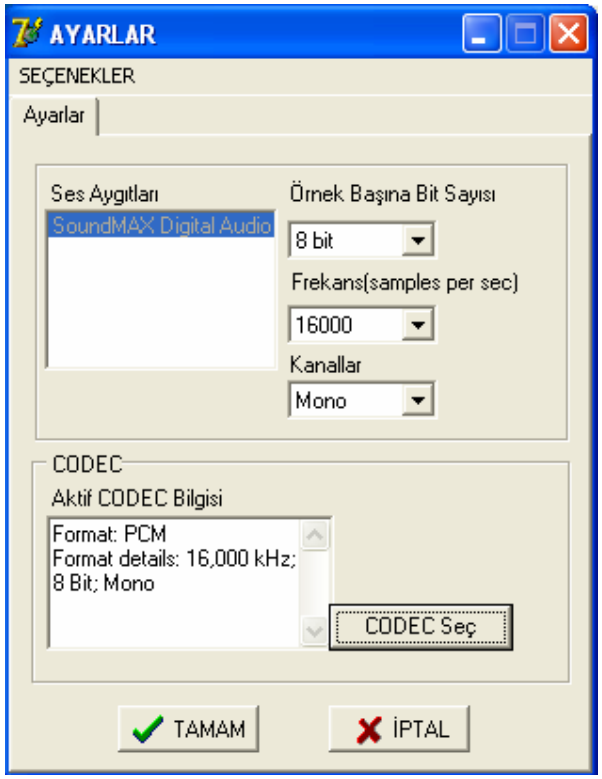
Eğer Ses Gönderici Modül kullanıcısı iletişim esnasında herhangi bir dosyayı göndermeye başlarsa, Ses Alıcı Modül bundan kullanıcısını haberdar etmekte ve durum hakkında bilgi vermektedir. Şekil 5.16'da bu durum ile ilgili bir ekran çıktısı verilmektedir.



Şekil 5.16: Ses Alıcı Modülün veri aktarımı anındaki görünümü (Dosya için)

Dosya aktarımı tamamlandıktan sonra kullanıcıya gelen dosyanın adı da görünerek kayıt yapması sağlanmakta ve aktarım tamamlanmaktadır.

Bu modülde de metin gömme işleminin yapıldığı modülde olduğu gibi alıcı düğümden kaynak düğüme yazılı mesaj gönderme özelliği söz konusudur ve temel olarak aynı işlevi gerçekleştirmektedir. Ancak menülerde "Codec Seç" seçeneği mevcuttur. Bu menü yardımı ile CODEC seçimi yapılarak, analog ses bilgilerinin örnekleme sayısı ve her bir örneğin kaç bit ile gösterileceği (8 veya 16 bit) seçilebilmektedir. İlgili değerler seçilerek "Tamam" butonuna basıldıktan sonra iletişim başlatılır (Şekil 5.17).



Şekil 5.17: CODEC seçimi yapılmasını sağlayan menü

5.3.2. SSGD kablosuz transferi için geliştirilen yazılımın ses gönderici modülünün çalışma prensibi ve akış diyagramı

Uygulamanın bu bölümünde kaynak tarafından kablosuz ses iletimi yapılırken herhangi bir anda istenilen bir dosya gönderimi gerçekleştirilebilmektedir. İlerleme çubuğu yardımı ile de dosya gönderimindeki son durum hakkında oransal olarak bilgi verilmektedir. İlgili dosyanın, ses bilgilerinin içerisine yerleştirilmesi işlemi "en düşük değerlikli bit" kullanılarak yapılmaktadır. Yani taşıyıcı ses verilerinin son bitleri, gömülecek dosyanın bitleri ile değiştirilmektedir. Birim zamanda gömülecek olan verinin diğer modül tarafından alınma süresi birim zamanda (1 saniye) ses kartından alınan ses bilgisi sayısına bağlı olarak değişmektedir.

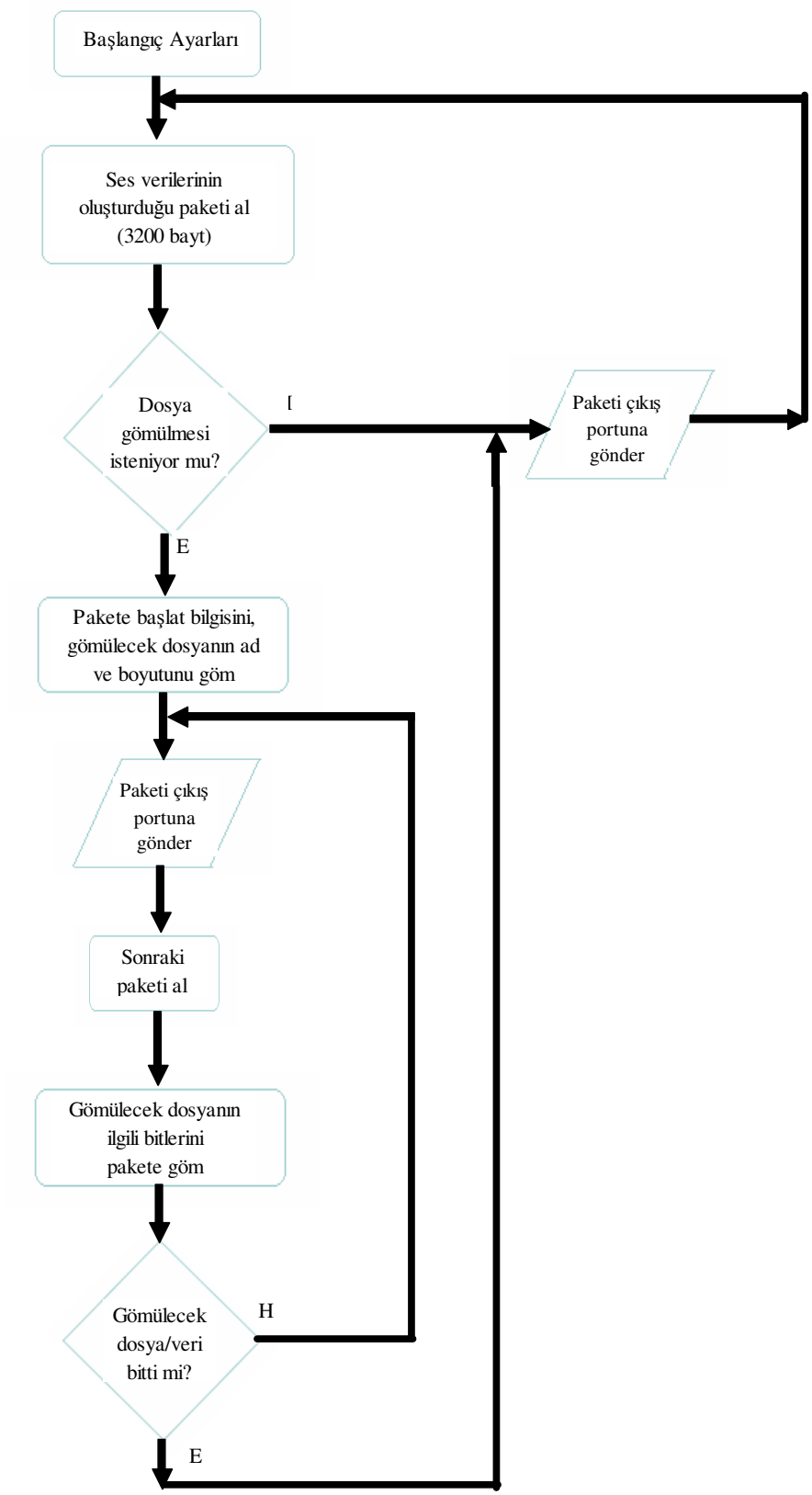
Sistemden alınan ses bilgileri Ses Gönderici Modülde 3200 bayt boyuta sahip bir ara belleğe (buffer) alınmaktadır. İlgili bellek dolduktan sonra işlemler gerçekleştirilmektedir. Eğer gömülecek herhangi bir dosya ya da veri yok ise ara bellekteki ilgili ses verisi bloğu porttan gönderilmektedir.

Eğer kullanıcı dosya gönderilmesi yönünde eylemde bulunmuş ise, dosya gönderilmek istenmesinin hemen ardından giden ilk veri bloğuna; "başlat" anahtarı (uygulamada başlat anahtarı 16 bitten oluşan 0000111100001111 olarak belirlenmektedir), dosya adının boyutu, dosya adı ve dosyanın boyutu bilgisi gömülerek gönderilmektedir (Tablo 5.3). Ve ardından gelen 3200 baytlık veri bloklarına dosyanın son bit değerine kadar gömme işlemi yapılmaktadır. İlgili veri bloğundaki her bayt bilginin son biti değiştirilerek gömme işlemi gerçekleştirilmektedir.

Tablo 5.3: Dosya ile ilgili bilgilerin ses çerçevesi içerisindeki yerleri

Çerçevedeki Sıra	**Gömülen Veri**
20 — 35.bayt	Başlat biti (Burada 0000111100001111 olarak belirlenmiştir).
40 — 54.bayt	Dosya isminin uzunluğu bilgisi.
60 — 99.bayt	Gönderilecek dosyanın uzunluğu.
100 — n bayt	Dosyanın adı (Dosya ismine göre bitiş baytı(n) değişmektedir).

Dosyaya ilişkin bilgiler bir pakete gömülerek gönderildikten sonraki ilk pakete dosyanın bitleri gömülmeye başlanmaktadır. Ses bilgileri daha önceden de belirtildiği gibi 3200 bayt boyutunda bir ara bellekte bulunmaktadır. Gömülerek gönderilecek olan dosya (bu dosya hangi tipte olursa olsun gönderilebilir; ancak, bu tez çalışmasında esas amaç ses dosyalarının gönderilmesidir, yani ses içerisinde ses bilgilerinin gönderilmesi hedeflenmektedir) paketlerin 21—3180. baytlarının son bitlerine gömülmektedir. Diğer bir ifadeyle 3160 bayt ses verisinin son bitleri 3160 bit veri gömme alanı sağlamaktadır. Bu da paket başına 395 bayt veri gömme kapasitesi anlamına gelmektedir. Gömü Verisi (Dosyası), 395 baytlık parçalar halinde her pakete gömülmekte ve böylece dosya gönderme işlemi gerçekleştirilmiş olmaktadır (Şekil 5.18).



Şekil 5.18: Ses Gönderici Modülün akış diyagramı (Dosya için)

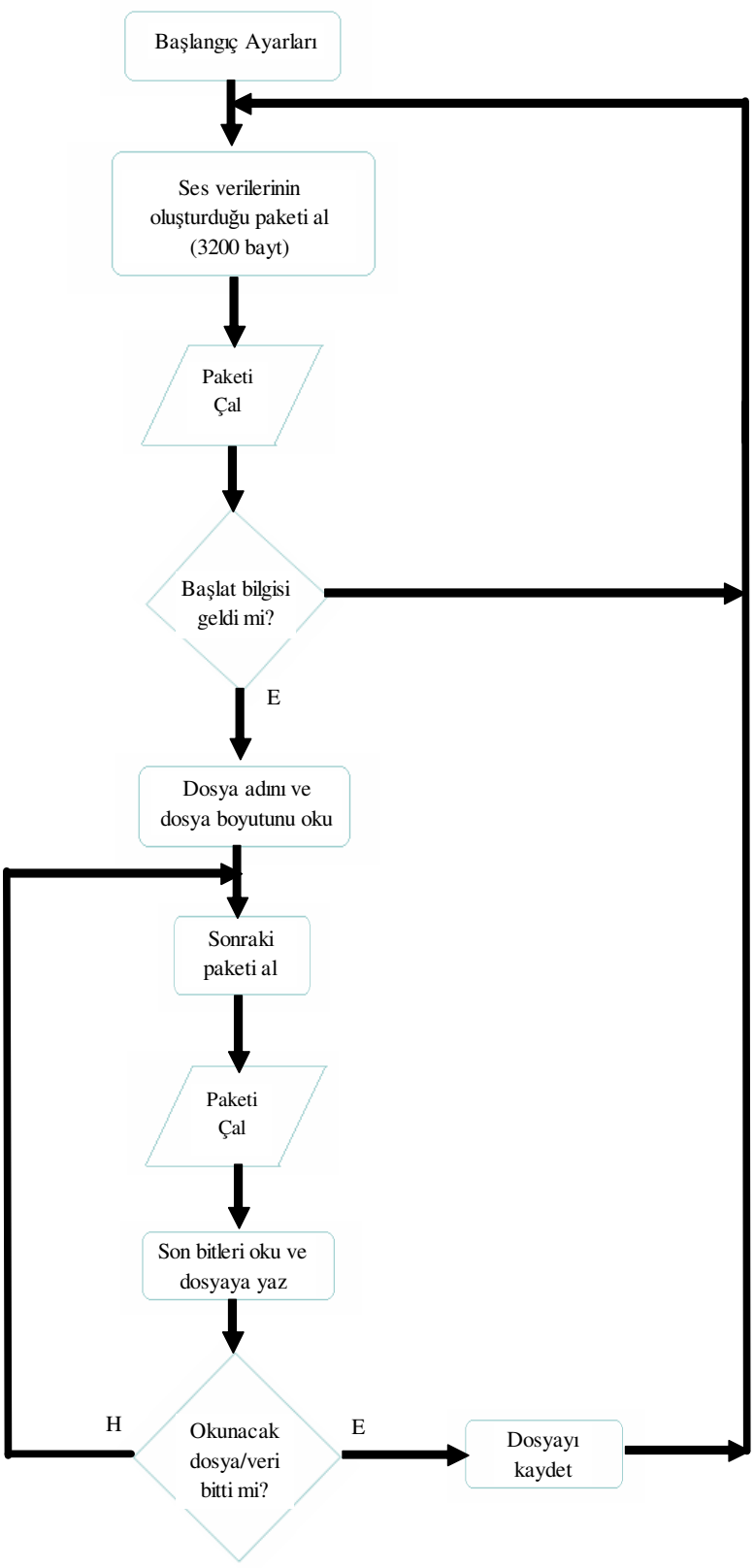
5.3.3. SSGD kablosuz transferi için geliştirilen yazılımın ses alıcı modülünün çalışma prensibi ve akış diyagramı

Uygulamanın, kablosuz olarak gönderilen ses bilgilerini alarak çalan ve eğer ses bilgileri içerisinde gömü verisi (dosyası) varsa bunu sezen ve kullanıcıya bildiren parçası bu bölümde açıklanmaktadır. İlgili bu yazılımdaki CODEC seç menusu yardımı ile kaynaktan birim zamanda (1 saniye) ses kartından kaç örnek alınacağı (8000, 11025, 16000, 22050, 32000 veya 44100) ve her bir örneğin kaç bit ile nitelendirileceği belirlenebilmektedir. Bu bilgiler oturumun açılması esnasında başlangıç ayarları yapılırken Ses Gönderici Modüle otomatik olarak gönderilmekte ve iletişim başlatılmaktadır.

Sayısal ses verilerinden oluşan 3200 baytlık paket alındıktan sonra ilgili yazılım başlat bilgisinin gelip gelmediğini kontrol etmektedir (20—35. baytların son bitlerine bakarak). Başlat bilgisi gelse de gelmese de ses hoparlörlerde çalınmaktadır. Başlat bilgisinin gelmesi durumunda dosyaya ait bilgiler bu paketten okunarak, gelecek olan diğer paketlerden bu bilgiler ışığında, dosyanın okunması işlemi gerçekleştirilmektedir (Şekil 5.19).

Dosya alımı bittikten sonra dosyanın hangi ad ile nereye kaydedileceği kullanıcıya sorulmakta ve aktarım işlemi sonlanmaktadır. Ancak ses iletişimi, kullanıcılar ses iletişimini kesmediği sürece devam etmektedir.

Ses alıcı yazılımında, ilgili bu yazılımı kullanan operatörün Ses Gönderici ile yazılı olarak haberleşmesini sağlayan “Mesaj Gönder” menusu mevcuttur. Bu sayede Ses Alıcı Modülü kullanan operatör istediği bir anda Ses Gönderici Modülünü kullanan operatöre yazılı mesaj gönderebilmektedir.



Şekil 5.19: Ses Alıcı Modülün akış diyagramı (Dosya için)

5.4. Sonuç

Bilgisayarlar tüm işlemleri ikili sayı sisteminden oluşan veri blokları üzerinde yapmaktadır. Bu temel bilgiden hareketle; bu tez çalışması için geliştirilen yazılımlarda, genel olarak daha önce kaydedilmiş metin, resim ve ses dosyalarına uygulanan stenografi tekniğinin, gerçek zamanlı olarak yapılan kablosuz ses haberleşmesine de uygulanabileceği gösterilmektedir.

Geliştirilen uygulamalar, "metin stenografisi" ve "veri/dosya stenografisi" olmak üzere iki ayrı bölümde sunulmuştur. Metin stenografisinde kablosuz ses haberleşmesi yapılırken kullanıcının yazacağı metinler sayısal ses bilgileri içerisine gömülmektedir ve alıcı yazılım tarafından gömülü veriler ayırt edilmektedir. Dosya stenografisinde ise kablosuz ses haberleşmesi yapılırken kullanıcının göndermek istediği herhangi bir dosya sayısal ses bilgileri içerisine gömülmekte ve alıcı yazılım tarafından ilgili dosya ayırt edilerek alınmaktadır.

Görülmektedir ki, eğer analog ses bilgileri yeterli bellek ve yeterli hıza sahip aygıtlarda işlenip, sayısallaştırılarak kısa zamanda stenografi algoritmalarından geçirilirse, gerçek zamanlı ses haberleşmesinde stenografi uygulaması çok kullanışlı bir gizli veri gönderme şekli olarak ortaya çıkabilmektedir.

Elde edilen sonuçlardan anlaşılmaktadır ki, donanımsal şartlar sağlandığında (özellikle bellek kapasitesi ve hız) gerçek zamanlı görüntü haberleşmesinde de stenografi uygulanabilecek ve çok büyük boyutlardaki gömü verilerinin (gerçek zamanlı ses ve video gibi) gömülerek iletilmesi sağlanabilecektir.

6. GELİŞTİRİLEN YAZILIMLARIN UYGULAMA ÖRNEKLERİ

6.1. Giriş

Bu bölümde, geliştirilen yazılımların başarımlarının, çalıştırıldıkları donanımların hız ve kapasitelerinin büyüklüğüne ve diğer parametrelere ne kadar bağımlı olduğunu tespit etmek amacı ile iki farklı özelliğe sahip bilgisayarda değişik uygulamalar çalıştırılmış olup elde edilen sonuçlar tablolar ve grafikler halinde verilmektedir. Bununla birlikte uygulamaların değişik ortamlardaki (düşük veri iletim hızı, RF etkisinin yoğun olduğu mekanlar) başarımları da incelenmektedir.

6.2. Sayısal Ses İçerisine Metin Gömme ve Kablosuz İletimi

Ses içerisine metin gömme yazılımı için uygulama örnekleri yapıldığında ve bu uygulamalar sonucunda ses haberleşmesini yapabilecek kapasitede olan bilgisayarlar kullanıldığı sürece sorun ortaya çıkmadığı tespit edilmektedir. Bu noktada hızlı veya yavaş bir bilgisayarın alıcı/kaynak durumunda olmasının başarıma kayda değer bir etkisi gözlemlenmemiştir. Bu durum metin gömme algoritmasının oldukça basit ve bilgisayarlar için zaman kaybettirecek boyutta olmamasından kaynaklanmaktadır.

6.3. Sayısal Ses İçerisine Veri/Dosya Gömme ve Kablosuz İletimi

Kablosuz haberleşme uygulamalarında çeşitli nedenlerle veri kayıpları olmakta ve bu kayıplar geliştirilen bir takım yöntemlerle telafi edilmeye çalışılmaktadır. Geliştirilen uygulamaların ortam değişimi söz konusu olduğunda (örneğin veri iletim hızı düştüğünde ve bozucu etkilerin söz konusu olduğu ortamlarda) başarım değerlendirmesi yapmak amacı ile çeşitli örnek uygulamalar yapılmış olup bu uygulamaların sonuçları verilmektedir.

RF (Radyo Frekansı) etkisi sebebi ile bazı ortamlarda kablosuz olarak yapılan iletişimde istenmeyen ses bozuklukları meydana geldiği görülmektedir. Ancak uygulama çalışır iken gizli şekilde gönderilen verilerde herhangi bir bozulma meydana gelmediği tespit edilmektedir. Bunun temelinde uygulamaların geliştirildiği platform olan Borland Delphi 7.0'ın içerisindeki veri kayıplarının en aza indirgenmesini sağlayan bileşenlerden yararlanılmış olması yatmaktadır.

Ses içerisinde gömü verisi(dosyası) gönderimi (dosyalar hakkındaki bilgiler Tablo 6.1'de verilmektedir) yapılmasını sağlayan modüller ile çeşitli örnek uygulamalar yapılmış olup, elde edilen sonuçlar Tablo 6.3'de gösterilmektedir. Stenografi örnek uygulamaları, boyutu ve tipi farklı 3 adet dosya için gerçekleştirilmiştir. Kullanılan bilgisayarların teknik özellikleri ise Tablo 6.2'de verilmektedir.

Tablo 6.1: Ses içerisine gömülerek gönderilen gömü dosyaları

No	Gömü Dosyası Adı	Dosya Uzantısı	Dosya Boyutu (KB)
1	demo	.mp3	38
2	sndrec32	.exe	122
3	svega	.wav	1771

İlgili dosyalar sıradan bilgisayar kullanıcılarının ulaşabileceği dosyalardır. "demo.mp3" 5 saniyelik bir ses dosyası olup, müzik dinlemek için kullanılan Winamp programı kurulduğunda elde edilebilmektedir. "sndrec32.exe" dosyası Microsoft Windows'un ses kayıt programıdır. "svega.wav" dosyası ise bilimsel çevrelerde stenografi uygulamalarında kullanılan 20 saniyelik bir referans ses dosyasıdır.

Tablo 6.2: Kullanılan bilgisayarların donanım özellikleri

Bilgisayar Adı	İşlemci Tipi	Hız (GHz)	Bellek Boyutu
PC_A	Intel(R)Pentium(R)4 CPU	3,2	384 MB RAM
PC_B	Intel(R)Celeron Mobile CPU	1,6	224 MB RAM

Özellikle gerçek zamanlı kablosuz haberleşme uygulamalarında kullanılan donanımların birim zamanda işlem yapabilme kapasitelerinin yüksekliği,

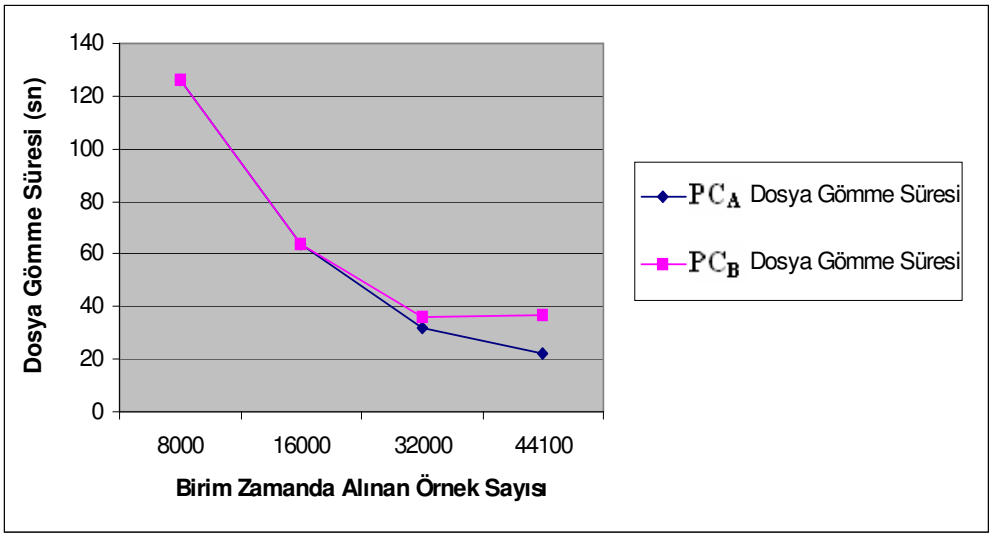
uygulamaların sağlıklı şekilde gerçekleştirilmesi açısından hayati önem taşımaktadır. Tez çalışmasına konu olan uygulamaların geliştirilmesi aşamalarında bu ilke dikkate alınmış olup, kullanılan bilgisayarlar birbirinden farklı teknik özelliklere sahiptir. Bu sayede yapılan denemelerde elde edilen sonuçlar üzerine yoğunlaşıldığında bilgisayarların hız ve kapasitelerinin haberleşmenin başarımına ne kadar etki ettiği de ortaya çıkarılmaktadır. Tablo 6.3'de, kullanılan bilgisayarlar ile yapılan örnek uygulamalar için elde edilen sonuçlar görülmektedir.

Tablo 6.3: Farklı gömü dosyaları için elde edilen dosya gömme ve dosya alma sürelerine ilişkin sonuçlar

Gömü Dosyasının Adı	**Gömü Dosyası Boyutu (KB)**	**Veri İletim Hızı (Mbps)**	**Örnek Sayısı* (1sn'de)**	**Dosya Gömme Süresi (sn)**		**Gömülü Dosyayı Alma Süresi (sn)**	
				PC_A	**PC_B**	**PC_A**	**PC_B**
Demo.mp3	38	36	22050	15	15	18	18
Demo.mp3	38	36	44100	8	12	15	12
Demo.mp3	38	54	8000	40	42	43	41
Demo.mp3	38	54	16000	20	21	22	21
Demo.mp3	38	54	32000	11	12	13	12
Demo.mp3	38	54	44100	7	12	13	10
sndrec32.exe	122	36	22050	47	47	50	50
sndrec32.exe	122	36	44100	22	46	49	34
sndrec32.exe	122	54	8000	126	126	129	129
sndrec32.exe	122	54	16000	64	64	65	65
sndrec32.exe	122	54	32000	32	36	38	37
sndrec32.exe	122	54	44100	22	37	38	33
svega.wav	1771	36	22050	670	667	674	674
svega.wav	1771	36	44100	335	486	490	520
svega.wav	1771	54	44100	335	520	522	470

*Alınan her bir örnek 8 bit ile nitelendirilmektedir.

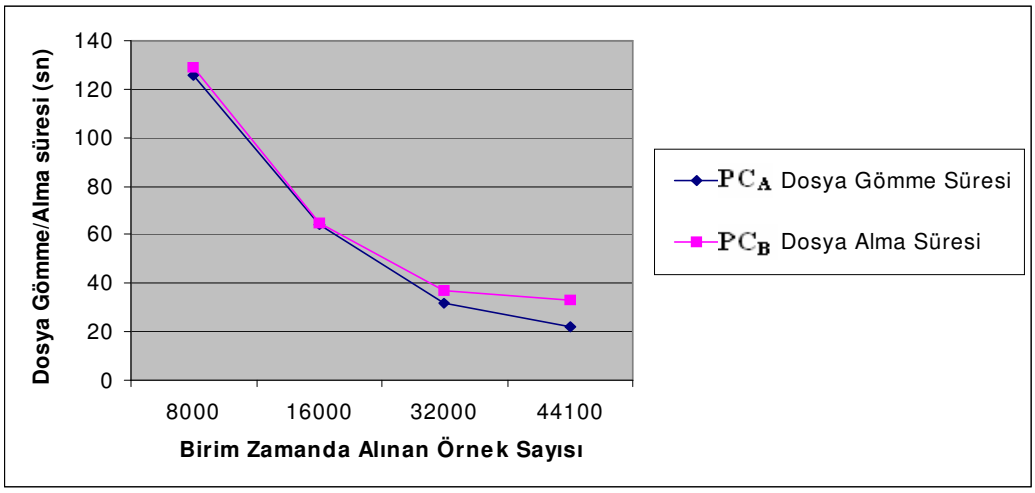
Şekil 6.1'de, örnek uygulamaların daha iyi değerlendirilebilmesi için değişik örnekleme sayılarına göre elde edilmiş gizli dosya gömme sonuçlarına ait grafik verilmektedir. PC_A'nın ve PC_B'nin sırasıyla birim zamanda 8000, 16000, 32000 ve 44100 örnek alındığı durumlarda, 54 Mbps iletim hızında, 122 KB boyutundaki "sndrec32.exe" gömü dosyasını örtü verisine (sayısal ses verilerine) gömme süreleri karşılaştırılmaktadır.



Şekil 6.1: PC_A ve PC_B'nin "sndrec32.exe" dosyasını sayısal ses verilerine gömme sürelerinin karşılaştırılması

Bir saniyede ses kartından alınan örnek sayısının artması birim zamanda daha fazla işlem yapılmasını gerektirmektedir. Çünkü birim zamanda tampon belleğe alınan sayısal ses verisinin artması işlem görmeyi bekleyen veri miktarının artması anlamına gelir. Bu nedenledir ki; PC_A, PC_B'ye göre daha iyi donanımsal özelliklere sahip olduğundan yüksek örnekleme oranlarında daha iyi başarım göstermektedir.

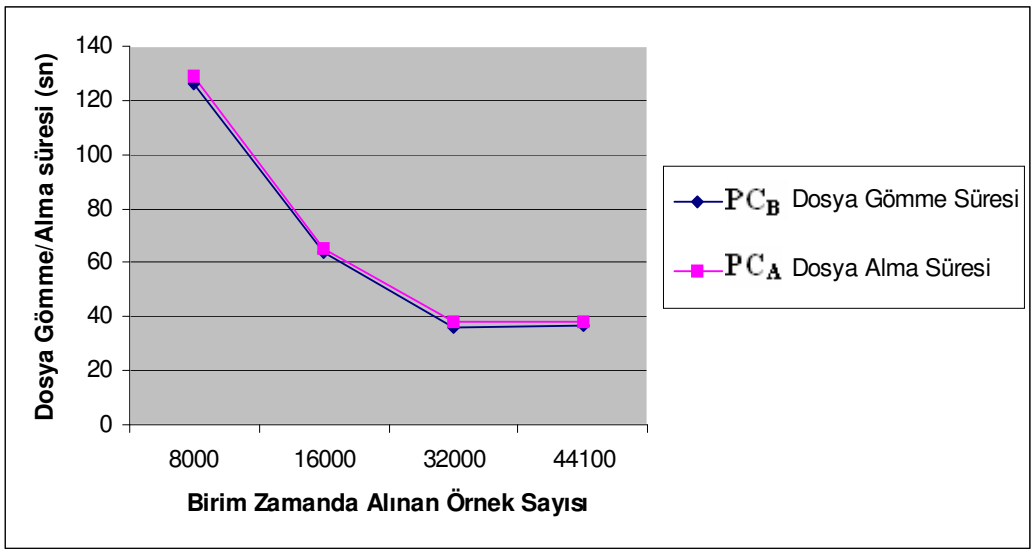
Şekil 6.2'de "sndrec32.exe" gömü dosyasını, PC_A'nın örtü verileri (taşıyıcı sayısal ses verileri) içerisine gömme süresi, PC_B'nin ise bu dosyayı örtülü veriden (taşıyıcı verileri ve gizli dosyalardan oluşan sayısal ses verilerinden) süzerek alma süreleri karşılaştırılmaktadır.



Şekil 6.2: PC_A'nın "sndrec32.exe" dosyasını gömme süreleriyle PC_B'nin dosyayı alma sürelerinin karşılaştırılması

Görüleceği üzere PC_A örnek sayısının artması ile birlikte daha kısa sürede ilgili gömü dosyasını gömmektedir. Ancak örnek sayısı 16000'i aştığında gömme/alma süreleri arasındaki fark artmaya başlamaktadır. Bu da PC_B'nin birim zamanda işlem yapabilme kapasitesinin daha az olmasından kaynaklanmaktadır. Çünkü 3300 portundan gelen ses paketlerinin sayısı artmakta dolayısı ile incelenmesi ve işleme alınması gereken veri boyutu büyümektedir.

Şekil 6.3'de ise "sndrec32.exe" gömü dosyasını, PC_B'nin örtü verisine gömme süresi, PC_A'nın ise bu dosyayı örtülü veriden süzerek alma süresi karşılaştırılmaktadır. Burada ise PC_B kendi kapasitesi ölçüsünde örnek sayısına göre işlem yapmakta ve ilgili dosyayı gömmektedir. Ancak PC_A daha iyi donanım özelliklerine sahip olduğundan, bu işlem sürelerine çok yakın bir sürede gömülmüş olan dosyayı elde etmektedir. Dikkat edilmesi gereken noktalardan bir diğeri ise; örnek sayısı 32000 ve üzerinde olduğunda PC_B, PC_A'ya göre daha uzun sürede gömme işlemini gerçekleştirmektedir.



Şekil 6.3: PC_B'nin "sndrec32.exe" dosyasını gömme süreleriyle PC_A'nın dosyayı alma sürelerinin karşılaştırılması

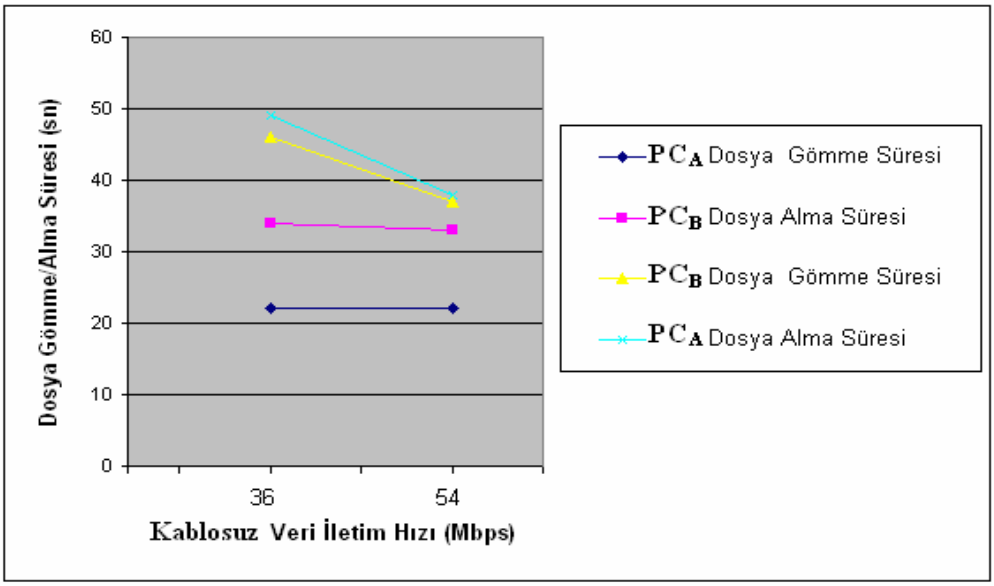
Tablo 6.4'de çalışmalarda kullanılan bilgisayarların farklı kablosuz iletim hızlarında "sndrec32.exe" gömü dosyasını sayısal ses bilgileri içerisine gömme ve süzerek elde etme süreleri verilmektedir. Burada dikkat edilmesi gereken nokta ise; iletim hızının artmasının verileri elde etme sürelerinin azalmasına sebep olduğudur. İletişimin hızlo

olması, toplamda (medya gecikmesini azalttığından) da dosya alma süresinin düşmesine yardımcı olmaktadır.

Tablo 6.4: "sndrec32.exe" gömü dosyasının farklı kablosuz iletim hızlarındaki gömülme/alınma süreleri

Gömü Dosyasının Adı	Gömülen Dosya Boyutu (KB)	Örnek Sayısı (1sn'de)	Veri İletim Hızı (Mbps)	PC_A Dosya Gömme Süresi (sn)	PC_B Dosya Alma Süresi (sn)	PC_B Dosya Gömme Süresi (sn)	PC_A Dosya Alma Süresi (sn)
sndrec32.exe	122	44100	36	22	34	46	49
sndrec32.exe	122	44100	54	22	33	37	38

Şekil 6.4'den veri iletim hızının artmasının dosyanın karşı tarafta alınma süresini azalttığı kolaylıkla görülmektedir. Ancak yine görülmektedir ki, PC_A daha hızlı veri gömmekte ve alıcı pozisyonunda iken de daha hızlı şekilde veriyi almaktadır. PC_B ise 36 Mbps veri iletim hızında % 54,54 gecikme ile gömü dosyasını almakta, 54 Mbps veri iletim hızında ise % 50 gecikme ile almaktadır.



Şekil 6.4: Farklı kablosuz iletim hızlarında "sndrec32.exe" gömü dosyasının gömülme/alınma sürelerinin karşılaştırılması

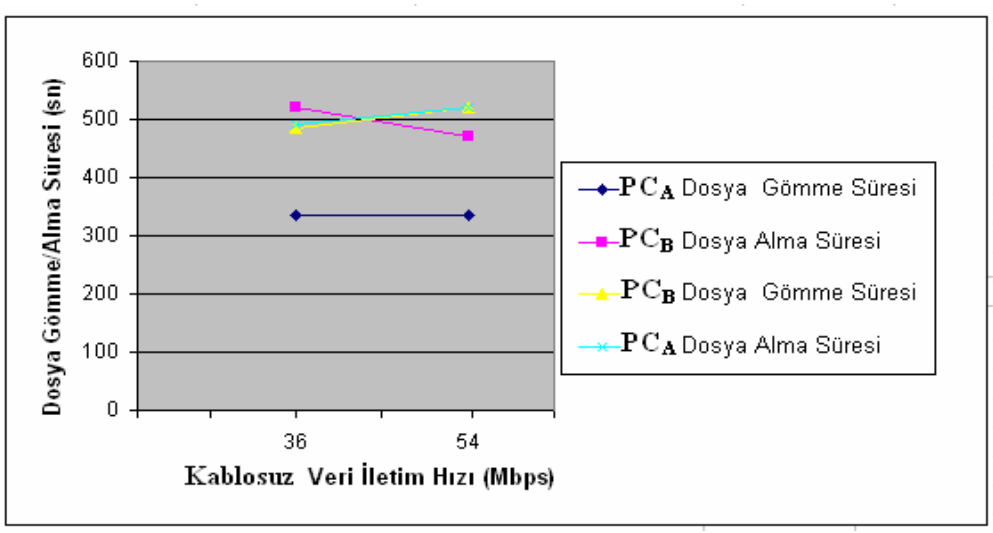
Dosya boyutunun ve kablosuz veri iletim hızlarının değişmesi durumunda geliştirilen uygulamaların başarımlarının nasıl etkileneceğini incelemek maksadı ile 1,73 MB boyutundaki "svega.wav" dosyası da benzer şekilde işleme tabi tutularak elde edilen

sonuçlar Tablo 6.5 ve Şekil 6.5'de sunulmuştur. Şekil 6.5 incelendiğinde, büyük boyutlu gömü dosyası (1,73 MB) için elde edilen sonuçların, Şekil 6.4'te sunulan ve daha küçük boyutlu (122 KB) bir gömü dosyası için elde edilen sonuçlara nispi olarak benzediği ortaya çıkmaktadır.

Tablo 6.5: "Svega.wav" dosyasının farklı kablosuz iletim hızlarında gömülme/alınma süreleri

Gömü Dosyasının Adı	Gömülen Dosya Boyutu (KB)	Örnek Sayısı (1sn'de)	Veri İletim Hızı (Mbps)	PC_A Dosya Gömme Süresi (sn)	PC_B Dosya Alma Süresi (sn)	PC_B Dosya Gömme Süresi (sn)	PC_A Dosya Alma Süresi (sn)
svega.wav	1771	44100	36	335	520	486	490
svega.wav	1771	44100	54	335	470	520	522

Burada da PC_A veri gömme ve alma süreleri açısından oldukça iyi başarım göstermektedir. Ancak PC_B gömülen dosyanın boyutunun büyümesi ile birlikte 36 Mbps veri iletim hızında % 55 (335 saniye de gönderilen dosyayı 520 saniyede alması sebebiyle) gecikme ile (122 KB'lık dosyada da yaklaşık % 55'dir) dosyayı almakta, 54 Mbps veri hızında ise % 40,2 (122 KB'lık gömü dosyasında % 50 idi) gecikme ile dosyayı almaktadır. Bu durum, nispi başarımların gömü dosyasının boyutu ile doğrudan ilişkili olmadığını gösterir.



Şekil 6.5: Farklı kablosuz iletim hızlarında "svega.wav" dosyasının gömülme/alınma sürelerinin karşılaştırılması

Buraya kadar sunulan örnek uygulamalarda birim zamanda alınan tüm örnekler 8 bit ile nitelendirilerek işlenmekte ve bu doğrultuda elde edilen sonuçlar verilmektedir. Buna ek olarak "sndrec32.exe" ve "demo.mp3" dosyaları için örnek başına bit sayısının 8 bit ve 16 bit olduğu durumlarda elde edilen sonuçlar Tablo 6.6, Şekil 6.6 ve Şekil 6.7'de karşılaştırılarak sunulmaktadır.

Tablo 6.6: Her bir örneğin 8 bit ve 16 bit ile gösterildiği durumlarda dosyaların gömülme/alınma süreleri

Gömü Dosyasının Adı	**Gömü Dosyasın Boyutu (KB)**	**Örnek Sayısı (1sn'de)**	**Örnek Başına Bit Sayısı**	**PC_A Dosya Gömme Süresi (sn)**	**PC_B Dosya Alma Süresi (sn)**	**PC_B Dosya Gömme Süresi (sn)**	**PC_A Dosya Alma Süresi (sn)**
sndrec32.exe	122	44100	8	22	33	37	38
sndrec32.exe	122	44100	16	12	21	37	38
Demo.mp3	38	44100	8	7	10	12	13
Demo.mp3	38	44100	16	5	8	12	13

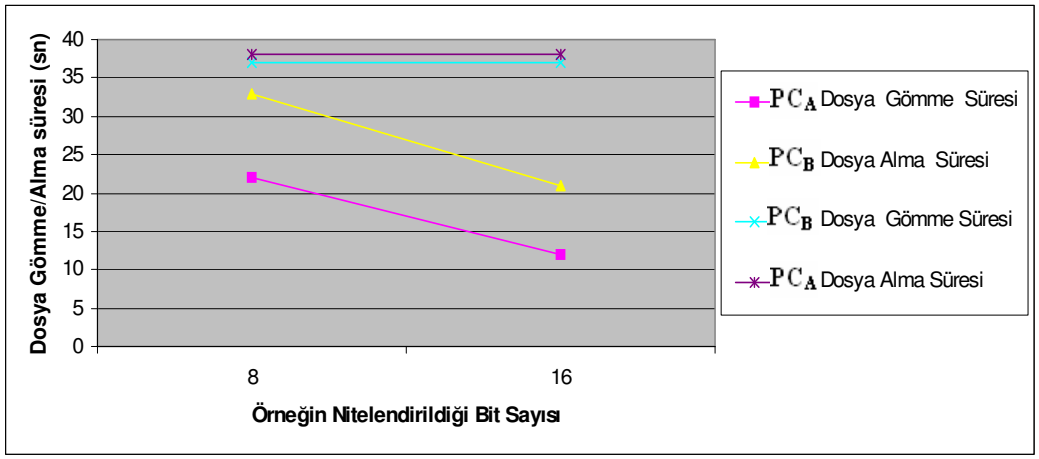
Geliştirilmiş olan yazılımlarda daha önceden de belirtildiği gibi 3200 bayt boyutundaki veri blokları üzerinde çalışmalar yapılmaktadır. Her bir örneğin 16 bit ile nitelendirilmesi durumunda, 8 bit ile nitelendirmenin yapıldığı uygulamalara göre 3200 bayt boyutundaki dizinin 2 kat daha çabuk sürede dolacağı sonucu çıkmaktadır. Bu da daha yüksek işlem yapabilme kapasitesi gerektiği anlamına gelmektedir. Ancak bununla birlikte verilerin daha kısa sürede gömülmesi sonucu da doğmaktadır. Çünkü birim zamanda alınan veri miktarı nispi olarak iki katına çıkmakta ve o zaman dilimi içerisinde alınan her bir örneğe (16 bit) iki bit veri gömülmektedir. Yani 16 bitlik veri sekizer bit olarak ikiye ayrılarak, ilk sekiz ve ikinci sekiz bitin son bitlerine veriler gömülmektedir.

Tablo 6.7'de her örneğin 16 bit ile gösterildiği durumda veri gömme şekli sunulmaktadır.

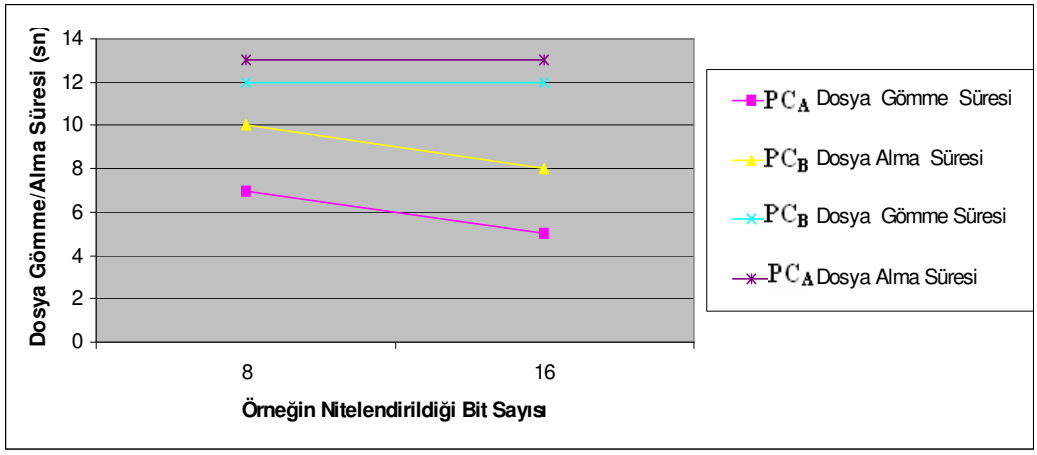
Tablo 6.7: Her bir örneğin 16 bit ile gösterildiği durumlarda verinin gömülme şekli

16 Bitlik bir örnek	Dizi içerisindeki yerleşimi	Gömülecek veri	Veri gömüldükten sonraki durum	Örneğin son durumu
1000100111010010	1000100**1**	01	1000100**0**	1000100 **0**1101001**1**
	1101001**0**		1101001**1**	

Görüleceği üzere her bir örnek daha fazla veri gömülmesini sağlamakta; ancak, ilk sekiz bit bilginin sonundaki bit, değerliği yüksek olan bir bittir. Bu durum bozucu etkinin yüksek olacağı anlamına da gelmektedir. Yapılan örnek uygulamalarda bu durumun çok büyük bir sorun oluşturmadığı görülmektedir.



Şekil 6.6: Örneklerin 8 bit veya 16 bit ile gösterildiği durumlarda "sndrec32.exe" dosyasının PC_A ve PC_B'de gömülme/alınma sürelerinin karşılaştırılması



Şekil 6.7: Örneklerin 8 bit veya 16 bit ile gösterildiği durumlarda "demo.mp3" dosyasının PC_A ve PC_B'de gömülme/alınma sürelerinin karşılaştırılması

Şekil 6.6 ve Şekil 6.7'de görüleceği üzere hızlı olan PC_A'nın her iki örnekte de veri gömme başarımı oldukça iyi oranda artmaktadır. Zira, birim zamanda alınan 44100 örneğin her biri 16 bit ile nitelendirilmesine, dolayısı ile işlenmesi gereken veri açısından yükün artmasına rağmen, tamamını işleyebilmekte ve dolayısı ile işlemi daha kısa sürede tamamlamaktadır. Daha yavaş hızla çalışan ve daha küçük bellek alanına sahip PC_B ise veri gömme başarımı açısından aynı başarıyı gösterememektedir. Veri gömme başarımı zaten daha düşük olan bu bilgisayar birim zamanda alınan verinin iki katına çıkması durumunda başarımını arttıramamakta, örneklerin 8 bit ile nitelendirildiği uygulamadakiyle hemen hemen aynı sürelerde veriyi gömebilmektedir.

6.4. Sonuç

Yapılan uygulama örneklerinde özetle şu önemli bulgulara ulaşılmıştır:

- Tablo 6.3 incelendiğinde; bilgisayar donanım özellikleri (işlemci türü, işlemci hızı ve bellek kapasitesi) iyileştikçe, özellikle yüksek oranlı örnek sayılarında veriyi gömerek gönderme ve gömülmüş veriyi elde etme sürelerinde azalma görülmektedir.
- Gömülü dosyayı elde etme işlemini yapan bilgisayarın, dosya gömme işlemini yapan bilgisayardan daha hızlı olması gömme ve alma sürelerinin birbirine paralel olmasına sebep olmaktadır. Aksi takdirde gömme/alma süreleri önemli farklılıklar arz etmektedir.
- Birim zamanda alınan örnek sayısının yüksek olması durumunda gömü dosyalarının gönderim hızı artmaktadır.
- Küçük boyutlu dosyaların gönderimi söz konusu olduğu durumlarda bilgisayarların donanım özelliklerinin faklılığı gönderme süresinde önemli bir değişikliğe sebep olmamaktadır.
- Birim zamanda alınan örnek sayısının 32000'e kadar olduğu durumlarda dosya gömme/alma sürelerinde donanım özelliklerinin etkisi fazla hissedilmemektedir.
- Veri iletim hızının yüksek olması ve bozucu etkilerden (RF) uzak ortamlar gizli verinin gönderim süresini düşürmektedir.

- Her bir örneğin 16 bit ile gösterilmesi durumunda kapasitesi ve hızı yüksek olan bilgisayarlar için gizli veri gönderim süreleri düşmektedir.

Veri gizleme üzerine yapılan ve bu tezde sunulan çalışmalar, çokluortam (multimedya) ve bilgi güvenliği uygulamaları gibi güncel gereksinimler ile daha yaygın bir öneme sahip olmaktadır. Bu araştırmanın amacı bilgi veya verinin korunması için en bilindik veri gizleme yaklaşımı olan LSB tekniğini gerçek zamanlı kablosuz ses haberleşmesinde gerçekleştirmektir. Böylece yetkisiz/istenmeyen alıcılar gizli bilginin ana obje/sayısal ses bilgileri üzerinde olduğundan habersiz bulunmaktadırlar. Gerçekleştirilen uygulamalardan sayısal ses içerisine metin gömmede; seste minumum bozulma, maksimum metin saklama kapasitesi, sayısal ses içerisine dosya gömmede; seste minumum bozulma, maksimum veri saklama kapasitesi amaçlanmaktadır.

Yapılan tez çalışmalarında örtü verisi (gömme/gizleme objesi) olarak sayısal ses bilgileri seçilmiş olup; gömü verisi (gizli mesajlar/dosyalar), içeriği ve boyutu bilinmeyen ve gerçek zamanlı olarak elde edilen bu sayısal ses bilgilerine gömülmektedir. Ses bilgileri 3200 baytlık işlenmiş paketler halinde gönderilmektedir. Ses Alıcı Modüllerde ise aynı paket alınarak, gömü verisi/dosyası elde edilmekte ve kullanıcılar dosya aktarımı konusunda bilgilendirilmektedir.

7. TARTIŞMA VE DEĞERLENDİRMELER

SSGM ve SSGD algoritmaları ve ara yüzlerinin geliştirildiği ve gerçekleştirildiği bu tez çalışmaları kapsamında elde edilen sonuçlar ışığında, konuya ilgi duyan araştırmacılara ve bilim camiasına aşağıdaki öneri/tartışma ve değerlendirmelerin sunulması uygun görülmektedir.

1. Uygulamalar yapılırken RF etkisinin söz konusu olduğu ortamlarda seste bozulmalar meydana geldiği gözlemlenmiştir. Bu bozulmaların en aza indirgenmesini sağlamak için çeşitli algoritmalar geliştirilebilir.
2. Ses haberleşmesinin yapıldığı esnada veri/dosya gömülmeye başlandığı andan itibaren insan kulağının oldukça zor algıladığı periyodik bir bozulma meydana gelmektedir. Bu durum hem paketlerdeki sayısal ses bilgilerinin değiştirilmesinden hem de paketlerin veriyi/dosyayı ayırt eden algoritmaya sokulması ile meydana gelen zaman kaybından kaynaklanmaktadır. Daha hızlı çalışabilecek algoritmaların geliştirilmesinin bu durumu olumlu yönde etkileyeceği anlaşılmaktadır.
3. Sayısal ses bilgileri içerisine veriler/dosyalar gömülür iken son bitler kullanılmıştır. Birim zamanda gömülen veri/dosya boyutunun arttırılması amacıyla her ses örneği 16 bit ile nitelendirilip gömülecek bit sayısı 2 ya da 3'e çıkarılabilir.
4. Gömü Dosyasının gönderilme süresi, ilgili dosyanın boyutu ile doğru orantılı olarak arttığından gömülecek bit sayısının azaltılması maksadı ile öncelikle sıkıştırma algoritması uygulanabilir.
5. Bilindiği üzere stenografide gizli bilgiler yalnızca kaynak ve alıcı algoritmanın bildiği şekilde gömülmektedir. Ancak bu gömme şeklinin üçüncü kişilerce bilinme ihtimali de dikkate alındığında gömülecek verilere şifreleme gerekli olmaktadır.
6. Gerçekleştirilen örnek uygulamalarda aynı anda sadece bir tek dosya gömülerek gönderilmesi söz konusudur. Bu durum yapılacak olan bir algoritma ile geliştirilerek aynı anda birden fazla dosyanın gönderimi gerçekleştirilebilir.

7. Çalışmalar bilgisayara bağımlı olduğu için tam anlamıyla istenen hızda sonuçlara veya başarıma ulaşmak mümkün olmamaktadır. İlgili uygulamalar eğer bilgisayardan bağımsız platformda gerçekleştirilirse daha fazla verim elde edilecektir.
8. Bugün gerek bilgisayar ağlarında ve gerekse internet ortamında çok sayıda ses verisi mevcut olup, bunlardan hangisinin veri gizlediğini tahmin etmek oldukça zordur. Bu da stenografinin kriptolojiye avantajı olarak görülebilir. Kullanılan tekniklerde kod çözme esnasında orijinal ses verisine ihtiyaç duyulmaması da bir diğer önemli özelliği oluşturmaktadır.
9. Günümüzde telif haklarının (copyright) korunması uygulamalarından olan sanal dijital filigran (Digital Watermarking) teknolojilerinde sıkça stenografi uygulamalarını görmek mümkündür. Bir kişiye ait olan orijinal bir çalışma (resim, ses vb.) başkaları tarafından izin alınmadan sahiplenilmesi yine bu tekniklerle önlenmektedir. Orijinal obje üzerine yerleştirilen gizli tanıtıcı veriler, nesnenin sahibine işaret etmektedir. Bu bakımdan da gerçekleştirilen çalışmaların oldukça faydalı ve uygulanabilir alanları olduğu görülmektedir.
10. Bilgisayar donanım özellikleri (işlemci türü, işlemci hızı, RAM bellek) iyileştikçe yapılan stenografi uygulamasının daha sorunsuz çalıştığı tespit edilmiştir. Gelecekteki donanım konfigürasyonlarının çok daha gelişmiş olacağı göz önüne alındığında gömme ve gömülü veriyi/dosyayı ede etme süreleri daha da kısalacak ve böylece akıcı (streaming) görüntü/video uygulamalarının da veri gizleme amaçlı kullanımında alternatif olacağı düşünülmektedir.

KAYNAKLAR

Aad, I., Castelluccia, C., "Priorities in WLANs", ***Computer Networks***, Vol. 41, 505–526, (2003).

Adlı, A., Nakao, Z., "Three Steganaography Algorithms for MIDI Files", ***IEEE Proceedings of the Fourth International Conference on Machine Learning and Cybernetics,*** (2005).

Akar, F., "Veri Gizleme ve Şifreleme Tabanlı Bilgi Güvenliği Uygulaması", Doktora Tezi, ***Marmara Üniversitesi Fen Bilimleri Enstitüsü***, (2005).

Anderson, R., J., Petitcolas, F. A. P., "On the Limits of Steganography", ***IEEE Journal of Selected Areas in Communications***, Vol. 16, No.4, pp 474–481, (1998).

ANSI/IEEE Std 802.11, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications", ***IEEE Standards 802.11***, 70–90, 1999.

Aura Tuomas, **Invisible Communication**, *EET* 1995.

Bayılmış, C., "Kablosuz Bilgisayar Ağlarının Performans Analizi", Yüksek Lisans Tezi, ***Sakarya Üniversitesi Fen Bilimleri Enstitüsü***, (2003).

Bayılmış, C., Ertürk, I., Çeken, C., "Kablosuz Bilgisayar Ağlarının Karşılaştırılmalı İncelemesi", ***Gazi Üniversitesi Politeknik Dergisi,*** Cilt 7, Sayı 3, 201–210, (2004a).

Bayılmış, C., Ertürk, I., Çeken, C., "A Comparative Performance Evaluation Study of IEEE 802.3 Wired and IEEE 802.11 Wireless LANs for Multimedia Data Traffic", ***Journal of Naval Science and Engineering,*** 2, 1–12, (2004b).

Bing, B., "High–Speed Wireless ATM and LANs", ***Artech House Mobile Communications Library,*** 1–102, (2000).

Cheng, J., Kot, A.C., Liuand, J., Cao, H., "Steganalysis of Data Hiding in Binary Text Images", ***Proceedings of the IEEE,*** pp 4405–4408, (2005).

Cox, I. J., Miller, M. L., Bloom, J. A., "Watermarking Applications and Their Properties", ***Int. Conf. on Information Technology, Las Vegas, USA,*** (2000).

Cox, I. J., Miller, M.L., "The First 50 Years of Electronic Watermarking", ***Journal of Applied Signal Processing***, Vol. 16, No.4, pp 126–132, (2002).

Çeken, C., "Kablosuz ATM Kullanarak Servis Kalitesi Desteği Sağlanmış Gerçek Zamanlı Veri Transferi", Doktora Tezi, ***Kocaeli Üniversitesi Fen Bilimleri Enstitüsü,*** (2004).

Çeken, C., Ertürk, I., Bayılmış, C., "Wireless Networks for Real–Time Multimedia Communications", ***Broadband Wireless and WiMAX, Comprehensive Report by International Engineering Consortium (IEC),*** (2004).

Delaigle, J. K., Protection of Intellectual Property of Images by Perceptual Watermarking, Doktora Tezi, ***Universitè Catholique de Louvain***, (2000).

Franz, E., Jerichow, A., Moller, S., Pfitzmann, A., Stierand, I., "Computer Based Steganography:How It Works And Why Therefore Any Restrictions on Cryptography Are Nonsense, At Best", **Proc.Information Hiding Workshop**, pp. 7–21, (1996).

Gast, M., "802.11 Wireless Networks: The Definitive Guide", Second Edition, ***Q'Reilly***, (2005).

Gruhl, D., Bender, W., Lu., A., "Echo Hiding", **Proc. Information Hiding Workshop**, pp. 295–315, (1996).

Hartung, F., Kutter, M., "Multimedya Watermarking Techniques", ***Proceedings of the IEEE,*** Vol.87, No.7, pp 1079–1107, (1999).

Levillain, P., "Wireless LAN for Enterprises", ***Alcatel Telecommunications Review***, Vol. 4, 287–291, (2002).

Matsui, K., Tanaka, K., Nakamura, Y. , "Digital Signature on Facsmile Document by Recursive MH Coding", ***International Symposium on Cryptography and Information Security (CIS89)***, (1989).

Nicopolitidis, P., Obaidat, M., S., Papadimitriou, G., I., Pomportsis, A., S., "Wireless Networks", ***Wiley,*** 239–269, (2003).

Tanaka, K., Nakamura, Y., Matsui, K., "Embedding a Secret Information into a Dithered Multi-level Image", ***Proceedings of IEEE Military Communcations Conference***, pp 216–220, (1990).

"WAVE PCM soundfile format", Stanford Üniversitesi, http://ccrma.stanford.edu/CCRMA/Courses/422/projects/WaveFormat/, **(Ziyaret Tarihi: 16 Aralık 2006).**

Xu, C., Ping, X., Zhang, T., "Steganography in Compressed Video Stream", ***Proceedings of the First International Conference on Innovative Computing, IEEE,*** (2006).

EK-A. Sayısal Ses İçerisinde Gizli Metinlerin Kablosuz Transferi İçin Geliştirilen Yazılımın Program Kodları CD içerisinde sunulmuştur (EK-A.doc)

EK-B. Sayısal Ses İçerisinde Gizli Verilerin/Dosyaların Kablosuz Transferi İçin Geliştirilen Yazılımın Program Kodları CD İçerisinde Sunulmuştur (EK-B.doc).

EK-C. Geliştirilen Uygulama Yazılımlarının Çalıştırılabilir Dosyaları CD İçerisinde Sunulmuştur (VoiceClient.exe, VoiceServer.exe).

EK-D. Tez pdf Dosyası CD İçerisinde Sunulmuştur (Tez.pdf).

ÖZGEÇMİŞ

1981 yılında Kocaeli ilinde doğdu. İlköğrenimini çeşitli illerde okuduktan sonra, lise eğitimini Kocaeli Teknik Lisesi Bilgisayar Bölümünde tamamladı. 1999 yılında girdiği Kocaeli Üniversitesi Teknik Eğitim Fakültesi Elektronik ve Bilgisayar Eğitimi Bölümü Bilgisayar Öğretmenliği Programından 2004 yılında sınıf birinciliği ve bölüm üçüncülüğü derecesi ile mezun oldu. Aynı yıl ilgili bölümün yüksek lisans programına kayıt oldu. 2004-2005 yıllarında Hereke Nuh Çimento Anadolu Teknik Lisesi, Teknik Lise ve Endüstri Meslek Lisesinde Bilgisayar Öğretmeni olarak görev yaptı. 2006 yılından itibaren Ümraniye Anadolu Ticaret Meslek ve Ticaret Meslek Lisesi Bilgisayar Bölümünde Bilgisayar Öğretmeni olarak görev yapmaktadır.