Sayısal Ses İçerisinde Gizli Veri Transferinin Kablosuz Ortamda Gerçekleştirilmesi

Yıldıray YALMAN, İsmail ERTÜRK

ÖZET

Günümüzde veri gizleme (steganografi) tekniklerinin önemi özellikle kablosuz iletişim sistemleri içerisinde giderek artmaktadır. Çoklu ortam ve bilgi güvenliği uygulamaları gibi güncel gereksinimler ile birlikte veri gizleme üzerine yapılan çalışmalar da yoğun bir talep ve ilgi görmektedir. Bu makalede sunulan çalışmanın temel hedefi; sayısal ses içerisinde yeni bir steganografi yaklaşımı ile gizli dosya ya da veri transferinin kablosuz iletişim ortamında gerçekleştirilmesidir. Bu amaçla kablosuz ortamda iletilen sayısal ses paketleri içerisine veri/dosya gömme algoritmaları ve uygulaması geliştirilmiştir. Gerçekleştirilen uygulama, klasik gerçek zamanlı ses haberleşmesini de oldukça iyi bir şekilde yapabilmektedir. Çalışmalarda donanım araçları olarak kablosuz haberleşme yeteneği bulunan değişik özelliklere sahip bilgisayarlar ve kablosuz erişim noktası, yazılım aracı olarak ise Borland Delphi 7.0 programlama dili kullanılmıştır. Ayrıca, çeşitli uygulama örneklerinden elde edilen sonuçlar sunularak, gerçekleştirilen steganografi sistemine ait donanım tabanlı başarım değerlendirmeleri yapılmaktadır.

Anahtar Kelimeler: Veri Gizleme, Steganografi, Sayısal Ses, Kablosuz İletişim

A Hidden Data Transfer System Implementation Within Digital Voice For Wireless Communications

ABSTRACT

Techniques for information hiding (steganography) have nowadays become increasingly more sophisticated and widespread. Researches on secret information embedding have received considerable attention for a decade due to both its ever increasing potential applications in multimedia data transfer and information security. The main objective of this research work presented is to design and implement a new hidden data transfer mechanism within digital voice for real-time wireless communications using the LSB steganography approach. Furthermore, the application programme developed aims at enabling a high quality conventional wireless real-time voice communication. In this research study, computers with different configurations and a wireless access point are utilized. These computers are equiped with wireless communication tools and software components. The softwares introduced in this paper are developed with Borland Delphi 7.0 programming language. Examples of the application results of the proposed steganography system implementation are also presented, followed by a basic hardware-based performance evaluation.

Keywords: Data Hiding, Steganography, Digital Voice, Wireless Data Transfer

1. GİRİŞ

Bu makalede sunulan çalışmada, yeni bir steganografi yaklaşımı ile gerçek zamanlı sayısal ses çerçeveleri (paketleri) içerisine yerleştirilen gizli gömü verileri, kablosuz iletişim yöntemiyle transfer edilerek, geliştirilen kod çözücü algoritma ile elde edilmekte ve kullanıcıya bilgi verilmektedir. Çalışmanın, ataklara (steganaliz) karşı dayanıklılığı, gizli verilerin ne şekilde gömüldüğünün de gizli tutulması ile orantılı olarak artmaktadır. Diğer bir ifadeyle, istenmeyen kullanıcıların steganaliz işlemini yapamaması amacıyla gerçekleştirilen bu uygulamada, gizli veri transferi yapılıyor olduğunun kolayca sezinlenememesi, önerilen yönteme oldukça büyük bir önem ve ayrıcalık kazandırmaktadır. Ayrıca, gizli verinin gömülme algoritması hakkında üçüncü şahısların bilgilerinin olmaması da bu yaklaşımın avantajları arasındadır.

Temeli antik çağlara kadar dayanan gizli haberleşme, teknoloji değişip geliştikçe şekil ve yöntem açısından da faklılıklar göstermiştir. Bununla birlikte önemini devamlı korumaktadır. Gizliliğin öneminin had safhaya ulaştığı kritik uygulamalarda; gizli bilgilerin, üçüncü kişilerin eline geçmeden ilgili hedefe ulaştırılması amaçlanır. Yaygın anlamda sayısal veri gizleme ile ilgili önemli çalışmalardan ilki, bir müzik şirketinin, müzik kayıtlarına sahiplik bilgisini içeren kod yerleştirmek için 1954 yılında aldığı patenttir (1).

1990'ların başında imge damgalama kavramı geliştirilerek, faks gibi ikili imgelerin korunmasında kullanımı literatüre kazandırılmıştır (2). Gerçekleştirilen bir başka gizli veri gömme tekniğine; daha sonra

Makale 07.05.2008 tarihinde gelmiş,02.11.2008 tarihinde yayınlanmak üzere kabul edilmiştir.

Y. YALMAN, İ. ERTÜRK, Kocaeli Üniversitesi, Teknik Eğitim Fakültesi, Elektronik ve Bilgisayar Eğitimi Bölümü, Umuttepe, 41380 Kocaeli

e-posta : yildiray.yalman1@kocaeli.edu.tr, erturk@kou.edu.tr

Digital Object Identifier 10.2339/2008.11.4. 319-327

"watermark" olarak birleştirilecek olan "water mark" ismi verilmiştir (3).

Steganografi (= Stego + Grafi) iki parçadan oluşan Yunanca bir kelimedir. "Steganos" örtülü/gizli, "Grafi" ise yazım/çizim anlamına gelmektedir. Steganografik uygulamaların yapılabilmesi için mutlaka taşıyıcı bir sayısal verinin (ses, resim, video, vb.) kullanımı gerekmektedir. Bu uygulamalara, Adlı ve Nakao'nun ".midi" uzantılı dosyalar için geliştirdikleri üç farklı steganografi algoritması örnek olarak verilebilir (4). Xu ve arkadaşları da sıkıştırılmış video görüntülerine farklı bir steganografi uygulama algoritması önermişlerdir (5). Yukarıdaki uygulamalarda da esas alındığı gibi, steganografide üçüncü kişilerin steganaliz yapamaması için, gizli verilerin ne şekilde gömüldüğünün saklı tutulması, bu verilerin güvenliği açısından büyük önem arz etmektedir. Ancak bu çalışmaların en büyük dezavantajı gizli veriyi ihtiva eden taşıyıcı verilerin kaydedilmesi ve ilerleyen zamanlarda ataklara maruz kalma ihtimalleridir.

Makale yedi ana bölümden oluşmaktadır. 2. bölümde klasik steganografi uygulamaları ve gerçekleştirilen çalışmanın önemi üzerinde durulmaktadır. 3. ve 4. bölümlerde ise çalışmanın önemli bileşenlerinden sırasıyla kablosuz sayısal veri haberleşmesi ve analog ses sinyallerinin sayısal veri formuna dönüştürülmesi açıklanmaktadır. Önerilen steganografi uygulamasının kullanıcı arayüzleri ve geliştirilen algoritmaları 5. bölümde detaylandırılırken, uygulama örnekleri ve sonuçları 6. bölümde sunulmaktadır. Çalışmada elde edilen bulgular 7. bölümde değerlendirilmektedir.

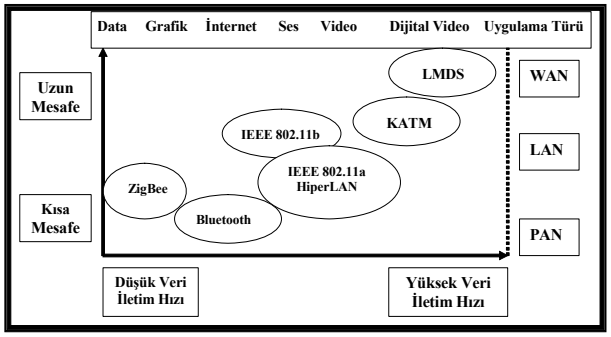
2. KLASİK STEGANOGRAFİ UYGULAMALARI VE GERÇEKLEŞTİRİLEN ÇALIŞMANIN ÖNEMİ

Kriptoloji, haberleşen iki veya daha fazla tarafın bilgi alışverişini emniyetli olarak yapmasını sağlayan ve gizli bilgiyi istenmeyen kişilerin anlayamayacağı hale getirerek korumayı esas alan, temeli matematiksel yöntemlere dayanan tekniklerin ve uygulamaların bütünüdür. Modern steganografi ise teknik olarak, bir veriyi (mesaj) bir nesnenin içine gizli biçimde yerleştirmeyi esas alan bilim dalıdır. Öyle ki, sadece belirlenen alıcı, kendisine iletilmek istenen mesajı nesneden seçebilmekte ve diğer gözlemcilerin o nesnenin içindeki mesajın varlığından haberleri olmamaktadır. Kriptoloji ile birlikte de anılan steganografi, bu önemli özelliğiyle kriptolojiyi bir adım ileri taşımaktadır. Kriptoloji, güvenilirliği sağlasa da bir bakıma mesajın gizliliğini (sezilememesini) sağlayamamaktadır. Kriptografik uygulamalarda bilgi sadece gönderici ve alıcının anlayabileceği şekilde şifrelenirken, steganografik uygulamalarda bilgi sadece gönderici ve alıcının varlığını bildiği şekilde saklanmakta, gerekli görüldüğünde şifrelenip ilave koruma sağlanabilmektedir (6 ve 7). Bu bilgiler ışığında, özellikle internet üzerinden yapılan haberleşmelerde zararsız görülen dosyaların (metin, resim, ses, video vb.) içerisine gizli bilgilerin gömülebileceği ya da yerel bir ağda kablolu/kablosuz şekilde gerçekleştirilen haberleşme ve dosya alışverişlerinde steganografinin kullanılabileceği gerçeği, bu makaleye konu olan çalışmanın temel motivasyonunu oluşturmaktadır. Literatürdeki benzer çalışmalarda, genel olarak taşıyıcı verinin ve gömülecek verinin boyutu bilinmekte ve bu temelde veri gömme ve steganaliz uygulamaları önerilmektedir (8─10). Ancak taşıyıcı verinin bilgisayar ortamında sabit halde bulunuyor olması, gizli veriye sahip olduğu sürece ataklara maruz kalma riskini de taşıdığı anlamına gelmektedir. Sunulan çalışma ile benzer özelliklere sahip olan (6)'da ise sadece gerçek zamanlı metin transferi yapılabilmektedir.

Sunulan çalışmanın farklılığı iki ana unsuru içermektedir; Gerçek zamanlı olarak elde edilen sayısal ses verileri, bir steganografik veri gömme algoritması içerisinden geçirilerek hedef noktaya (alıcıya) kablosuz ortamda gönderilmekte ve ancak bu durumdan haberdar olan bir alıcı yazılım yardımı ile gizli gömü verileri ayrıştırılarak tekrar elde edilmektedir. Diğer bir ifadeyle, iletişim öncesinde taşıyıcı veri ve gönderilecek olan gizli gömü verisinin içeriği bilinmemektedir. Kullanıcılar uygulama çalışırken istedikleri şekilde konuşmakta ve sayısallaştırılarak gerçek zamanlı olarak gönderilen kendi ses verilerine istedikleri herhangi bir dosya ya da veriyi gömerek gizli bir şekilde gönderebilmektedir. Bu yöntem diğer eşleniklerinden farklı olarak, gizli gönderilecek gömü verilerinin boyutunu sınırlandırmamaktadır. Kablosuz ses iletişimi gerçekleştirildiği sürece istenilen boyuttaki gizli veriler alıcıya ulaştırılmaktadır. Bununla birlikte, gizli bilgiyi içeren örtülü veri kaydedilmeyerek ilerleyen zamanlarda muhtemel ataklara karşı, sistemin dayanıklılığı (robustness) arttırılmış olmaktadır. Geliştirilen uygulama saniyede 44100 örneğin alındığı durumlarda her bir örneğe 1 bit gömdüğünden, veri gömme kapasitesi yaklaşık 44 Kbps olup; aynı amaca dönük diğer uygulamalarda ise bu kapasite 0,83 bps (11), 4 bps (12), 16 bps (13), 22 bps (14), 20─30 bps (15), 25 bps (16), 38 bps (17), 43 bps (18), 50 bps (19), 128 bps (20) (16 KHz örnekleme frekansında), 5 Kbps (21) ve 48 Kbps (22) şeklindedir.

3. KABLOSUZ SAYISAL VERİ HABERLEŞMESİ

Kablosuz ağlar, haberleşme amacıyla çoğunlukla radyo frekans (RF) teknolojilerini kullanan gezgin veya sabit terminallerden oluşmaktadır. Bunlar kablo kullanan eşleniklerinden farklı olarak kurulum kolaylığı, ölçeklenebilirlik, hareketlilik, üretkenlik, ileriye yönelik maliyet kazancı ve mevcut ağ yapısını kolayca genişletme gibi birçok avantajlar sunmaktadır. Bunlara karşın, kablosuz iletim ortamının doğasından kaynaklanan yüksek bit hata oranı ve sınırlı bant genişliği gibi önemli dezavantajlara da sahiptirler (23). Farklı uygulamalar ve ihtiyaçları karşılamak üzere günümüzde birçok kablosuz ağ teknolojisi geliştirilmektedir. Şekil 1, mevcut ve geliştirilmekte olan kablosuz ağ standartlarının, destekledikleri uygulama türü, veri iletim hızı, kapsama alanının büyüklüğü ve coğrafik yapılarına göre yapılan sınıflandırmalarını özetlemektedir (24).

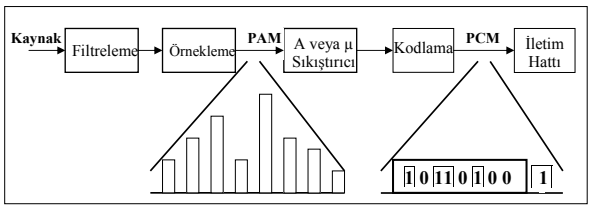


Şekil 1. Kablosuz ağ uygulamaları

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 (25). Bu makalede sunulan çalışmada sayısal ses haberleşme altyapısı olarak, hem geniş bir uygulama alanına sahip hem de diğer yöntemlere kıyasla dezavantajları oldukça az olan IEEE 802.11 kablosuz iletişim sistemi esas alınarak steganografi uygulama araçları geliştirilmiştir.

4. ANALOG SES SİNYALLERİNİN SAYISAL VERİ FORMUNA DÖNÜŞTÜRÜLMESİ

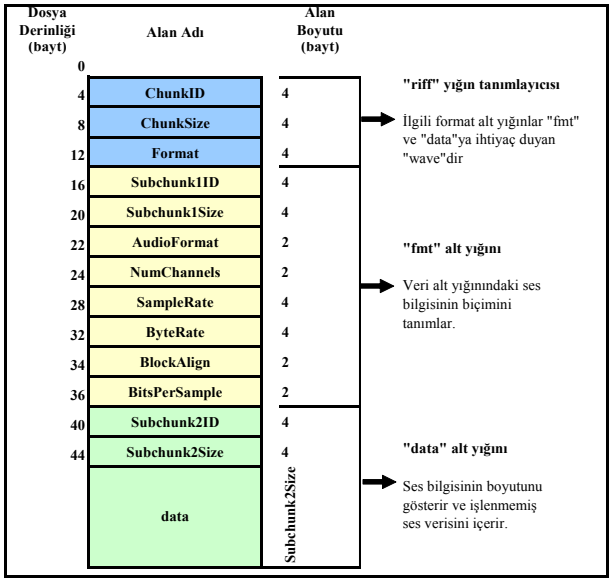
Darbe Kod Modülasyonu (Pulse Code Modulation: PCM), analog işaretlerin belirlenmiş bir sayısal forma dönüştürülmesinde kullanılır. Bu teknikte analog işaretten sayısal bilgiye ve sayısal bilgiden analog işarete dönüşüm sırasında oluşan örnekleme kayıpları oldukça küçüktür. Bu nedenle, örnekleme kayıplarından oldukça fazla etkilenen işaretlerin (konuşma işaretleri gibi) sayısal formda iletilmesi amacıyla, PCM günümüzde sıklıkla tercih edilir. Şekil 2'de PCM'nin yapısı görülmektedir.



Şekil 2. PCM yapısı

Analog ses sinyallerinin sayısallaştırılması sürecinde önemli kayıplar meydana gelmektedir. Bu kayıpların en aza indirgenmesi için analog ses sinyalinden birim zamanda alınan örnek sayısının arttırılması çoğunlukla benimsenen bir yaklaşımdır. Bu makalede sunulan çalışmada, örnekleme sayısına bağlı olarak hem ses iletişim kalitesi hem de yeni steganografik yaklaşım ile veri/dosya gömme kapasitesi açılarından toplam sistem başarımında önemli farklılıklar ortaya çıkmaktadır. Sayısal ortamda incelendiğinde, örneklenerek elde edilen ses verileri temel olarak ".wav" dosya tipindedir. Bu tip bir dosyanın atası ise Microsoft'un ".riff" (Resource Interface File Format) uzantılı dosya yapısıdır. Şekil 3'de "wave" ses dosyasının yapısı görülmektedir.

Sayısal ses verilerinin ele alındığı uygulama programlarında Şekil 3'de sunulan dosya yapısına uygun nesneler kullanılmaktadır. Bu makalede sunulan çalışmalar sonucunda geliştirilen yazılımlar, sayısallaştırılmış ham ses verileri (45. bayttan itibaren başlayan) üzerinde, takip eden bölümlerde de anlatıldığı gibi bir takım steganografik işlemler yapmaktadır.



Şekil 3. "wave" dosya yapısı

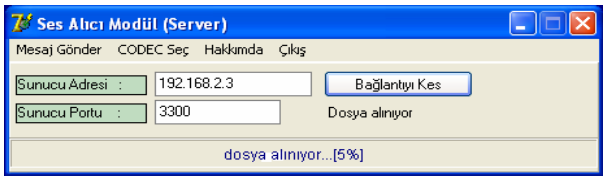
İzleyen bölümde bu sayısal ses verilerine gizli "veri/dosya" gömme uygulamasına dair kullanıcı arayüzleri, uygulama programının çalışma prensibi ve akış şemaları ile kısa bir başarım değerlendirmesi verilmektedir.

5. GELİŞTİRİLEN STEGANOGRAFİ UYGULAMASI: ALGORİTMA VE KULLANICI ARAYÜZLERİ

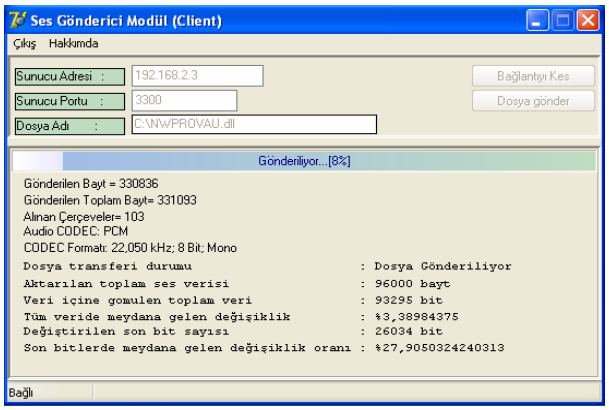
Geliştirilen steganografi uygulaması Borland Delphi 7.0'da gerçekleştirilmiş olup, temel olarak Network Multi Medya (NMM) bileşeninden faydalanılmaktadır. Uygulama, Ses Gönderici Modülü (SGM) ve Ses Alıcı Modülü (SAM) olmak üzere, gizli veriyi/dosyayı vericide sayısal ses örtü paketlerine geliştirilen algoritma ile gömen ve alıcıda bunları ayrıştırarak elde eden iki ana kısımdan oluşmakta ve ilgili modüller TCP/IP iletişim protokolünü kullanmaktadır. Şekiller 4 ve 5'de, geliştirilen steganografi uygulamasının SAM ve SGM kullanıcı arayüzleri verilmektedir (26).

Geliştirilen uygulamada kullanılan bilgisayarın ses kartından birim zamanda (1 saniye) kullanıcının belirlediği değerde (8000, 11025, 16000, 22050, 32000 veya 44100) sayısal örnek bilgisi SGM tarafından alınmaktadır. Daha sonra bu örneklerin en küçük değerlikli bitleri (LSB) gömülmek istenen gizli verinin/dosyanın bitleri ile değiştirilerek kablosuz ortamdan gönderil-

mektedir. Ters bir yaklaşımla, bu sayısal ses paketlerini algılayarak gizli gömü verisini/dosyasını tespit eden ve SAM'da çalışan algoritma da geliştirilmiştir. İnsanların duyu sistemi, görme sisteminden daha hassastır (27). Her bir ses örneğinde, gizli veri/dosya gömme işleminin sebep olduğu bozulmanın, kulak tarafından algınamayacak minumum düzeyde tutulması amacıyla, sayısal ses paketlerinin en küçük değerlikli bitlerine (LSB) veri/dosya gömülmüştür.



Şekil 4. Ses Alıcı Modül (SAM) arayüzü



Şekil 5. Ses Gönderici Modül (SGM) arayüzü

SAM ve SGM uygulamaları, bağlantının kurulması ile birlikte kablosuz sayısal ses iletişimine başlamaktadırlar. SGM, ses iletişimi sırasında elde edilen, aktarılan toplam ses verisi büyüklüğü, gizli gömülü veri/dosya büyüklüğü, değişikliğe uğrayan ses verisi LSB bit oranı gibi istatistiksel bilgileri de kullanıcıya sunmaktadır. SGM'de ses kartından alınan veriler 3200 baytlık paketler haline getirilerek, bu paketler üzerinde işlemler yapılmaktadır.

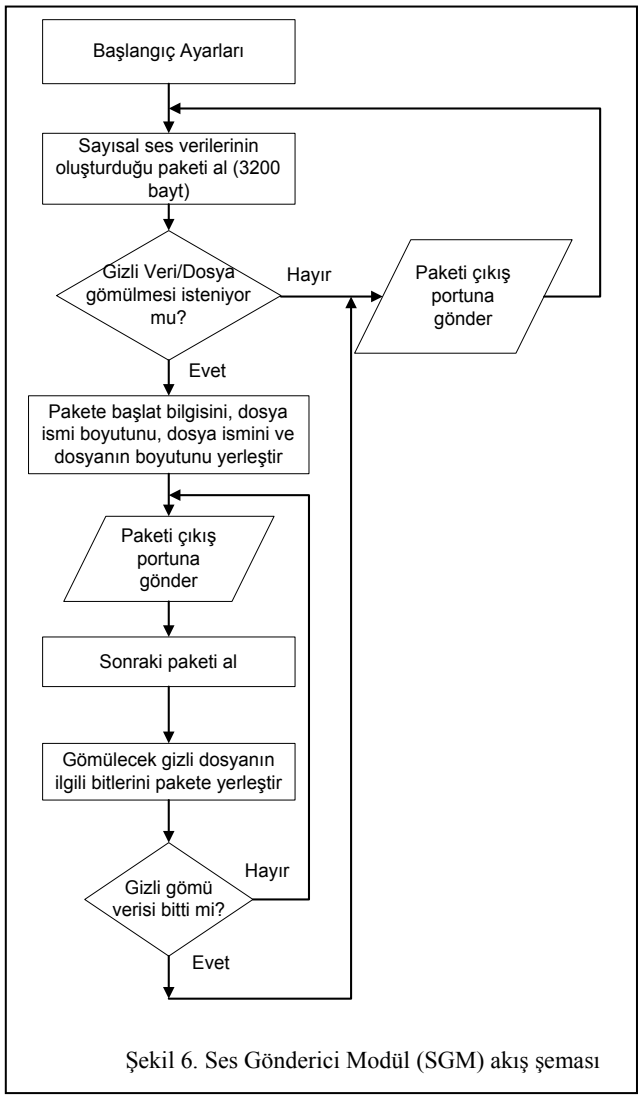
Tablo 1. Gizli gömü (veri/dosya) bilgilerinin ses çerçevesi içerisindeki yerleri

Çerçevedeki Sıra	**Gömülen Gizli Veri**
20 — 35. bayt	Başlat bitleri (örüntüsü) **"0000111100001111"** olarak belirlenmiştir.
40 — 54. bayt	Dosya ismi uzunluk bilgisi.
60 — 99. bayt	Gönderilecek verinin/dosyanın uzunluğu.
100 — n. bayt	Dosyanın ismi (dosya ismine göre bitiş baytı (n) değişmektedir).

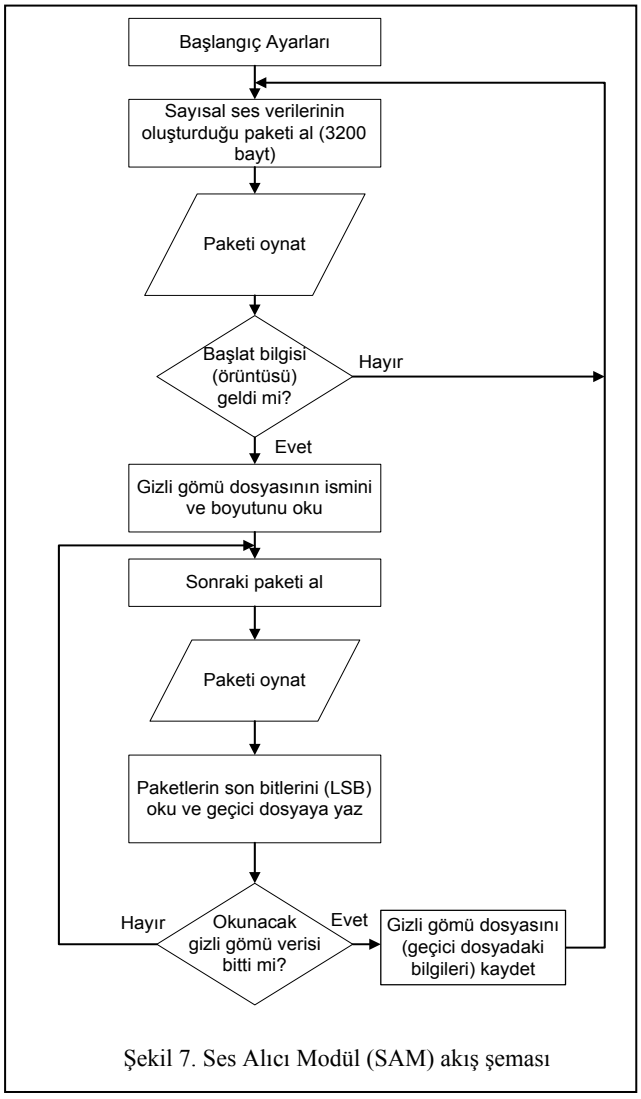
Bir gizli veri/dosya gönderme isteğinin ardından, iletilecek ilk ses paketine Tablo 1'de belirtildiği gibi önceden tesbit edilen "başlat dizisi", "dosya isminin uzunluğu", "dosya boyutu" ve "dosya ismi" bilgileri, daha sonra gelen sayısal ses paketlerine ise gömü verisinin/dosyasının "bit"leri sırasıyla yerleştirilir. Tablo 2'de "başlat bitleri"nin bir sayısal ses çerçevesi içerisine yerleştirilmesi görülmektedir. Şekil 6 ve 7'de geliştirilen steganografi modüllerinin (SGM ve SAM) akış şemaları verilmektedir.

Tablo 2. Ses çerçevesine başlat bilgisinin (örüntüsünün) yerleştirilmesi

Çerçevedeki Sıra	**Örnek Bir Orijinal Ses Verisi**	**Ses Verilerinin Son Durumu**
20. bayt	1 1 0 0 1 0 1 **1**	1 1 0 0 1 0 1 **0**
21. bayt	0 0 1 0 0 1 1 **0**	0 0 1 0 0 1 1 **0**
22. bayt	0 1 0 0 1 1 1 **0**	0 1 0 0 1 1 1 **0**
23. bayt	0 0 1 1 1 0 0 **1**	0 0 1 1 1 0 0 **0**
24. bayt	1 1 1 0 0 1 1 **0**	1 1 1 0 0 1 1 **1**
25. bayt	1 1 0 0 1 1 0 **1**	1 1 0 0 1 1 0 **1**
26. bayt	0 0 0 1 1 0 0 **0**	0 0 0 1 1 0 0 **1**
27. bayt	0 1 0 1 1 0 1 **0**	0 1 0 1 1 0 1 **1**
28. bayt	1 0 0 1 0 0 1 **0**	1 0 0 1 0 0 1 **0**
29. bayt	0 1 0 0 1 1 1 **0**	0 1 0 0 1 1 1 **0**
30. bayt	0 0 1 1 1 0 0 **1**	0 0 1 1 1 0 0 **0**
31. bayt	1 1 1 0 0 1 1 **0**	1 1 1 0 0 1 1 **0**
32. bayt	1 1 0 0 1 1 0 **1**	1 1 0 0 1 1 0 **1**
33. bayt	0 1 0 1 1 0 0 **0**	0 1 0 1 1 0 0 **1**
34. bayt	1 0 0 1 1 0 1 **0**	1 0 0 1 1 0 1 **1**
35. bayt	1 0 1 1 1 0 1 **1**	1 0 1 1 1 0 1 **1**



Şekil 6. Ses Gönderici Modül (SGM) akış şeması



Şekil 7. Ses Alıcı Modül (SAM) akış şeması

SAM, sayısal ses verilerinden oluşan 3200 baytlık ilk ses paketini aldıktan sonra başlat bilgisinin (örüntüsünün) çerçeve içerisinde olması şartını aramaksızın ses verilerini ilgili uygulama programında oynatmaktadır. Bu işlemin ardından başlat bilgisinin gelip gelmediği sürekli kontrol edilmektedir (20—35. baytların son bitleri incelenilerek). Başlat bilgisi alınması durumunda gizli gömü dosya bilgileri bu paketten elde edilerek, müteakip ses paketlerinden bu bilgiler ışığında gizli gömü dosyasının alınması işlemi gerçekleştirilmektedir. Gizli gömü dosyasının alım işlemi tamamlandığında kullanıcının dosyayı kaydetmesi sağlanmaktadır.

6. GELİŞTİRİLEN STEGANOGRAFİ SİSTEMİNİN UYGULAMA ÖRNEKLERİ

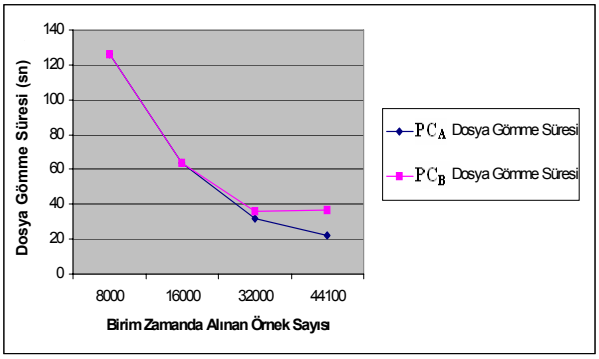
Çalışmanın kullanımı öngörülen uygulamalar, değişik kullanıcıların erişimine açık, iletişim ortamını paylaşan ve çoğunlukla hareketli düğümlerden oluşmaktadır. Geliştirilen steganografi uygulaması, internet üzerinden gerçek IP numaraları yardımıyla çalıştırılabildiği gibi, bir eşe-eş ağda da kolaylıkla kullanılabilmektedir. Eşe-eş ağlar, gerçeklemesi hızlı ve kolay, geçici bağlantılar sağlamak üzere kurulan yapıdadır. Aynı iletişim protokolünü kullanan en az iki kablosuz terminalin bir araya gelmesi ile oluşur. Böylece, herhangi bir erişim noktası olmaksızın tüm kablosuz kullanıcılar birbirleri ile iletişim kurarlar (28). Ancak, geliştirilen steganografi sistemi ve uygulamalarının yerel ağda daha yüksek veri iletim hızlarında ve daha geniş kapsama alanında çalışabilmesi amaçlarıyla bir erişim noktası (Access Point) kullanılmış ve 54 Mbps veri iletim hızında iletişim gerçekleştirilmiştir. Aslında band genişliğinin belirli bir bölümünden, kullanılan tekniğin ve çoklu erişim yönteminin getirdiği kısıtlamalar dolayısıyla veri iletişiminde etkin olarak faydalanılamamaktadır. Bu sebeple, 54 Mbps band genişliğinin sadece 32 Mbps'lik kısmı etkin veri iletişimi için kullanılabilmektedir (29). Hızla gelişen teknolojiler ve yeni yöntemler ile birlikte veri iletim hızlarında da istenilen düzeye gelinmesi mümkün olacak ve birden fazla uygulamanın aktif olduğu ağ ortamlarında çalışılsa bile, steganografi sistemini kullanan veri yükü yüksek çoklu ortam uygulamaları (örneğin ses ve videonun birlikte kullanıldığı), herhangi bir erişim noktasına ve veri sı-

kıştırmaya ihtiyaç duymadan hedeflenen başarımlara ulaşabilecektir.

Kablosuz haberleşme uygulamalarında çeşitli nedenlerle veri kayıpları oluşmaktadır. Bu kayıplar/hatalar ve olumsuz sonuçları değişik yöntemlerle telafi edilir. Geliştirilen steganografi sisteminin bazı uygulama örneklerinde, RF (Radyo Frekansı) etkisi sebebi ile gürültü yoğun ortamlarda kablosuz olarak yapılan iletişimde, istenmeyen ses paketi kayıpları meydana gelmiş olup, TCP protokolünün kullanımı sayesinde, gömü verisini/dosyasını taşıyan LSB'nin bozulmadan alıcıya (SAM) ulaşması sağlanmıştır. Gömü verisi taşımayan paketlerin kaybı söz konusu olduğunda, bu paketlerin tekrar üretilmemesi sağlanarak, band genişliği ve işlem yükü tasarrufuna gidilmiştir. Ancak uçtan-uca kablosuz iletişimde, paket gecikmesine bağlı olarak ses gecikmelerinin (jitter) meydana geldiği görülmüştür. Bunun temelinde, geliştirilen sistemin gizli gömü veri/dosya kayıplarına karşı bağışık yapıda olmasını sağlayan donanım/yazılım bileşenlerinden yararlanılmış olması yatmaktadır. Uygulama örneklerinde, Tablo 3'de belirtilen değişik özelliklere sahip iki bilgisayar kullanılmıştır. Tablo 4'de ise gömü verisi/dosyası olarak kullanılan örnek dosyaya ait özellikler verilmektedir. İlerleyen paragraflarda, bu bilgisayarlar ve değişik örnek sayıları için yapılan uygulamalar sonucunda gizli veri gömme/alma süreleri açısından değerlendirmeler sunulmaktadır.

Dosya gömme ve gizli gömü dosyasını kablosuz olarak iletilen sayısal ses verilerinden ayrıştırarak kullanıcıya sunma işlemlerinde "gecikme" (işlem yüküne, iletişim hızına ve donanım özelliklerine bağlı), başarım değerlendirmesi açısından çok büyük önem kazanmaktadır. Dosya gömme ve gizli gömü dosyasını ayırt etme işlemleri yapılırken sayısal ses iletişiminin insan kulağının algılayabileceği bir düzeyde bozulmaya uğramaması da başarım parametreleri içerisinde yer almaktadır. Bu nedenlerle, gerçekleştirilen uygulama örneklerinde, bir bütün olarak steganografi işlemlerinin ne kadar zaman aldığının ve tüm donanım özelliklerinin toplam başarıma etkilerinin anlaşılması amacıyla farklı özelliklerde bilgisayarlar kullanılmıştır. Bilgisayarların donanım özelliklerinin birbirinden farklı olması, işlem yapabilme kapasitesinin bu araştırma sonucunda geliştirilen yazılımların başarımına etkisini değerlendirirken ayırt edici olmaktadır.

Şekil 8'de, PC_A'nın ve PC_B'nin ayrı ayrı, "sndrec32.exe" gizli gömü dosyasını örtü verisine (gerçek zamanlı transfer edilen taşıyıcı sayısal ses paketleri) gömme süreleri karşılaştırılmaktadır. Birim zamanda (1 saniyede) ses kartından alınan örnek sayısının artması, birim zamanda daha fazla işlem yapılmasını da gerektirmektedir. Çünkü, birim zamanda tampon belleğe (buffer) alınan sayısal ses verisinin artması işlem görmeyi bekleyen veri miktarının artması anlamına gelmektedir. Dolayısıyla PC_A, daha iyi donanımsal özelliklere sahip olduğundan yüksek örnekleme oranlarında PC_B'ye göre daha iyi başarım göstermektedir.



Şekil 8. "sndrec32.exe" dosyası SGM gömme süreleri

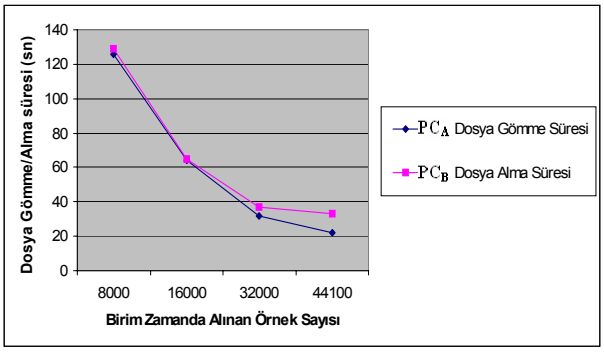
Tablo 3. Örnek uygulamalarda kullanılan bilgisayarların donanım özellikleri

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

Tablo 4. Gizli gömü dosyası ve özellikleri

Gizli Gömü Dosyası Adı	Dosya Uzantısı	Dosya Boyutu (KB)
sndrec32	exe	122

Şekil 9'da "sndrec32.exe" gömü dosyasını, kaynak düğüm PC_A'nın örtü verileri (gerçek zamanlı transfer edilen taşıyıcı sayısal ses paketleri) içerisine gömme (SGM) süresi, hedef düğüm PC_B'nin ise bu gizli dosyayı örtülü veriden (taşıyıcı sayısal ses ve gizli dosyanın bitlerinden oluşan paketler) süzerek alma (SAM) süreleri karşılaştırılmaktadır.

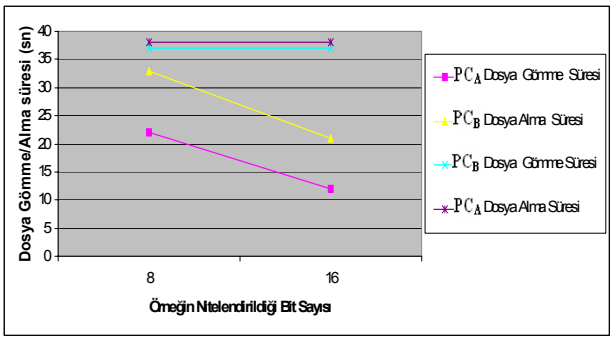


Şekil 9."sndrec32.exe" dosyası SGM gömme ve SAM alma süreleri

Grafiklerden anlaşılacağı gibi, sayısal ses örnekleme değerine paralel olarak PC_A daha kısa sürede gizli dosyayı gömme işlemini tamamlamaktadır. Ancak birim zamandaki örnek sayısı 16000'i aştığında gömme/alma süreleri arasındaki fark artmaya başlamaktadır. Bu sonuç PC_B'nin birim zamanda işlem yapabilme kapasitesinin daha az olmasından kaynaklanmaktadır. Çünkü ses iletişimi uygulamalarında birim zamanda alınan örnek sayısı arttıkça kapasite kullanımı ve işlem yükü artmaktadır (30).

Geliştirilen steganografi sistemi yazılımında, daha önce de belirtildiği gibi, 3200 bayt boyutundaki sayısal ses paketleri üzerinde işlemler yapılmaktadır. Her bir örneğin 16 bit ile nitelendirilmesi durumunda, 8 bit ile nitelendirmenin yapıldığı uygulama örneklerine kıyasla, 3200 bayt boyutundaki bir dizinin 2 kat daha hızlı sürede dolacağı sonucu ortaya çıkmaktadır. Bu durum, daha yüksek işlem yapabilme kapasitesinin gerekliliğine işaret etmektedir. Ancak, bununla birlikte gizli dosyaların daha kısa sürede gömülmesi sonucu da ortaya çıkmaktadır. Çünkü birim zamanda alınan sayısal ses veri miktarı nispi olarak iki katına çıkmakta ve aynı zaman dilimi içerisinde alınan her bir örneğe (16 bit) iki bit veri gömülebilmektedir. Diğer bir ifadeyle, 16 bitlik veri bloğu, sekizer bitlik iki kısma ayrılarak, yeni oluşan ilk sekizli ve ikinci sekizli bloğun son bitlerine (LSB) gizli veriler gömülmektedir. Tablo 5'de her bir örneğin 16 bit ile nitelendirildiği durumda gizli veri/dosya gömme işlemi sunulmaktadır. Görüleceği üzere her bir ses örneği daha fazla veri gömülmesine olanak sağlamaktadır; ancak, ilk sekiz bit bilginin LSB'sinin değerliği nispeten yüksektir. Bu durum, her ne kadar örtü verileri (gerçek zamanlı transfer edilen taşıyıcı sayısal ses paketleri) üzerindeki bozucu etkinin yüksek olacağı anlamına gelse de, bu bozulmalar, birim zamanda oynatılan (seslendirilen) örnek sayısının fazlalığı nedeniyle insan kulağı tarafından algılanamayacak düzeydedir.

Şekil 10'da görüleceği üzere işlem hızı yüksek olan PC_A'nın veri gömme başarımı oldukça iyidir. Zira birim zamanda alınan 44100 örnekten her birisinin 16 bit ile nitelendirilmesine ve buna bağlı olarak işlenmesi gereken veri açısından yükün artmasına rağmen, SGM tamamını işleyebilmekte ve veri gömme işlemini 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 uygulamayla hemen hemen aynı sürelerde gizli veriyi gömebilmektedir.



Şekil 10. 8 bit ve 16 bit örnekleme durumlarında gömü dosyasına ait (sndrec32.exe) SGM gömme ve SAM alma süreleri

7. SONUÇLAR VE DEĞERLENDİRMELER

Bu makalede, gerçek zamanlı elde edilen sayısal ses paketleri içerisine gömülen verilerin/dosyaların kablosuz ortamda iletilerek alıcı tarafından elde edilmesi için geliştirilen steganografi yaklaşımı ve yazılımı sunularak, farklı donanım özelliklerine sahip bilgisayarların, değişik uygulama örneklerinde başarıma etkisi incelenmektedir. Yapılan uygulama örneklerinde elde edilen temel bulgular şunlardır:

- Bilgisayar donanım özellikleri iyileştikçe, özellikle yüksek örnekleme durumlarında, veriyi/dosyayı gömme ve gizli gömü verisini/dosyasını elde etme sürelerinde azalma görülmektedir.
- Gömü dosyasını elde etme işlemini gerçekleştiren

Tablo 5. Her bir ses örneğinin 16 bit ile nitelendirildiği durumda gizli verinin gömülme işlemi

16 bit'lik Bir Örnek	Ses Dizisi İçerisindeki Yerleşimi	Gizli Gömü Verisi	Veri Gömüldükten Sonraki Durum	16 bit'lik Örneğin Son Durumu
1000100111010010	1000100**1**	01	1000100**0**	1000100**0** 1101001**1**
	1101001**0**		1101001**1**	

(hedef) bilgisayarın, dosya gömme işlemini yapan (kaynak) bilgisayardan daha hızlı olması, gömme ve alma sürelerinin birbirine paralel olmasına sebep olmaktadır. Aksi takdirde SGM veri gömme ve SAM alma süreleri önemli farklılıklar göstermektedir.

- Birim zamanda alınan sayısal ses örnekleme değerinin yüksek olması durumunda gizli gömü dosyalarının uçtan-uca (kaynak-hedef) gönderim hızı artmaktadır.
- Küçük boyutlu dosyaların gönderiminin söz konusu olduğu durumlarda bilgisayarların donanım özelliklerinin faklılığı iletişimde anlamlı bir değişikliğe sebep olmamaktadır.
- Geliştirilen uygulamada, gizli verilerin ses verileri içerisine şifrelenmeden yerleştirilmesinin, gömme algoritmasının üçüncü kişiler tarafından bilinmesi durumunda yapılacak ataklarda bir dezavantaj olacağı değerlendirilmektedir. Ayrıca gizli veri iletimi başlamadığı halde bir ses paketi içerisinde başlat bitlerinin rastgele oluşması ihtimali de (2^{-16}) geliştirilen yazılım için bir dezavantaj oluşturmaktadır. Fakat tasarlanan yöntemin esnek yapısı sayesinde, bu olasılık kullanılacak daha uzun başlat örüntüsüyle oldukça azaltılabilmektedir.
- Birim zamanda alınan sayısal ses örnekleme sayısı 32000'e kadar olduğunda SGM/SAM gömme/alma sürelerinde donanım özelliklerinin etkisi fazla hissedilmemektedir.
- İletişim hızının yüksek olması ve bozucu (RF) etkilerden uzak ortamlar, gizli verinin gönderim süresini düşürmektedir.
- Her bir örneğin 16 bit ile nitelendirilmesi durumunda kapasitesi ve hızı yüksek olan bilgisayarlar için dosya gönderim süreleri önemli ölçüde düşmekte ve sayısal ses paketlerindeki steganografiye bağlı değişiklikler (gürültü) anlamlı olumsuzluk teşkil etmemektedir.

8. KAYNAKLAR

1. 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.
2. 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.
3. Van Schyndel, R. G., Tirkel, A.Z., Osborne, C. F., "Towards a Robust Digital Watermark", Proceedings of ACCV'95, pp. II504–II508, 1995.
4. Adlı, A., Nakao, Z., "Three Steganography Algorithms for MIDI Files", IEEE Proceedings of the Fourth International Conference on Machine Learning and Cybernetics, 2005.
5. Xu, C., Ping, X., Zhang, T.,"Steganography in Compressed Video Stream", Proceedings of the First International Conference on Innovative Computing, IEEE, 2006.
6. Yalman, Y., Ertürk, İ., "Sayısal Ses İçerisinde Gizli Metin Transferinin Kablosuz Ortamda Gerçekleştirilmesi", Ulusal Teknik Eğitim, Mühendislik ve Eğitim Bilimleri Genç Araştırmacılar Sempozyumu, UMES'07, Kocaeli, 41-45, 20-22 Haziran 2007.
7. Akleylek, S., Nuriyev, U., "Steganografi ve Steganografinin Yeni Bir Uygulaması", IEEE 13. Sinyal İşleme ve İletişim Uygulamaları Kurultayı (SİU'05), 16-18 Mayıs 2005, Kayseri, Türkiye, 2005.
8. Doerr, G., Dugelay, J., "Security Pitfalls of Frame-by-Frame Approaches to Video Watermarking", IEEE Transactions on Signal Processing, Vol. 52, No. 10, pp. 2955-2964, October, 2004.
9. Barni, M., Bartolini, F., Checcacci, N., "Watermarking of MPEG-4 Video Objects", IEEE Transactions on Multimedya, Vol. 7, No. 1, pp. 23-32, February, 2005.
10. Lyu, S., Farid, H., "Steganalysis Using Higher-Order Image Statistics", IEEE Transactions on Information Forensics and Security, Vol. 1, No. 1, pp. 111-119, March, 2006.
11. Arnold, M., "Audio Watermarking: Features, Applications and Algorithms", Proc. IEEE Int. Conf. Multimedia and Exposition (ICME), 2000, pp. 1013-1016.
12. Ko, B. S., Nishimura, R., Suzuki, Y., "Time-Spread Echo Method for Digital Audio Watermarking Using PN Sequences", Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing, Vol. II, pp. 2001-2004, 2002.
13. Daniel, G., Anthony, L., Walter, B., "Echo Hiding", Lecture Notes in Computer Science, Information Hiding, Vol. 1174, pp. 295-315, 1996.
14. Li, X.,Yu, H.H.,"Transparent and Robust Audio Data Hiding in Cepstrum Domain" Proc. IEEE Int. Conf. Multimedya and Exposition (ICME'00), pp.397-400, 2000.
15. Kuo, S.S., Johnston, J.D., Turin, W., Quackenbush, S.R. "Covert Audio Watermarking Using Perceptually Tuned Signal Independent Multi Phase Modulation", Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing, Vol. II, pp. 1753-1756, 2002.
16. Shin, S., Kim, J., Choil, J., "A Robust Audio Watermarking Algorithm Using Pitch Scaling", Proc. IEEE 14th Int. Conf. Digital Signal Processing, pp. 701-704, 2002.
17. Li., X.,Yu, H.H., "Transparent and Robust Audio Data Hiding in Subband Domain", Proc. IEEE Int. Conf. Information Technology: Coding and Computing, pp. 74-79, 2000.
18. Lie, W., Chang, L., "Robust and High-Quality Time-Domain Audio Watermarking Based on Low-Frequency Amplitude Modification", IEEE Transactions on Multimedia, Vol. 8, no. 1, February 2006.
19. Ikeada, M., Takeda, K., Itakura, F., "Audio Data Hiding by Use of Band-limited Random Sequences", Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing, Vol. 4, pp. 2315-2318, 1999.
20. Ciloğlu, T., Karaaslan, S.U., "An Improved All-pass Watermarking Scheme for Speech and Audio", Proc.

IEEE Int. Conf. Multimedia and Exposition (ICME), pp. 1017-1020, 2000.

21. Tilki, J.F., Beex, A.A., "Encoding a Hidden Auxilary Channel onto a Digital Audio Signal Using Psychoacoustic Masking",Proc. IEEE Southeactcon'97, pp.331-333, 1997.
22. Wang, Y., "A New Watermarking Method of Digital Audio Content for Copyright Protection", Proc. 4th Int. Conf. Signal Processing, Vol. II, pp. 1420-1423, 1998.
23. Çeken, C., "Kablosuz ATM Kullanarak Servis Kalitesi Desteği Sağlanmış Gerçek Zamanlı Veri Transferi", Doktora Tezi, Kocaeli Üniversitesi F.B.E., 2004.
24. Bayılmış, C., Ertürk, İ., Çeken, C., "Kablosuz Bilgisayar Ağlarının Karşılaştırılmalı İncelemesi", Gazi Üniversitesi Politeknik Dergisi, Cilt 7, Sayı 3, pp. 201–210, 2004.
25. Levillain, P., "Wireless LAN for Enterprises", Alcatel Telecommunications Review, Vol. 4, pp. 287–291, 2002.
26. Yalman, Y., "Sayısal Ses İçerisinde Gizli Veri Transferinin Kablosuz Ortamda Gerçekleştirilmesi", Yüksek Lisans Tezi, Kocaeli Üniversitesi F.B.E., 2007.
27. Erçelebi, E., Subaşı, A., "Robust Multi Bit and High Quality Audio Watermarking Using Pseudo-random Sequences", Elsevier Computer and Electrical Engineering, pp. 525-536, 2005.
28. Bayılmış, C., Ertürk, İ., 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, Vol. 2, pp. 1–12, 2004.
29. Çölkesen, R., Örencik, B., "Bilgisayar Haberleşmesi ve Ağ Teknolojileri", Papatya Yayınları, Sayfa 239, 2003.
30. Kratzer, C., Dittman, J., Vogel, T., Hillert, R., "Design and Evaluation of Steganography for Voice-over-IP", IEEE ISCAS'06, pp. 2397-2400, 2006.