BURSA TEKNİK ÜNİVERSİTESİ ❖ FEN BİLİMLERİ ENSTİTÜSÜ

SES STEGANOGRAFİ YÖNTEMLERİNİN KARŞILAŞTIRMALI ANALİZİ

YÜKSEK LİSANS TEZİ

Funda ASLANTAŞ BEYİN

Elektrik Elektronik Mühendisliği Anabilim Dalı

TEMMUZ 2021

BURSA TEKNİK ÜNİVERSİTESİ ❖ FEN BİLİMLERİ ENSTİTÜSÜ

SES STEGANOGRAFİ YÖNTEMLERİNİN KARŞILAŞTIRMALI ANALİZİ

YÜKSEK LİSANS TEZİ

Funda ASLANTAŞ BEYİN
(181278034007)

Elektrik Elektronik Mühendisliği Anabilim Dalı

Tez Danışmanı: Doç.Dr. Cemal HANİLÇİ

TEMMUZ 2021

BTÜ, Fen Bilimleri Enstitüsü'nün 181278034007 numaralı Yüksek Lisans Öğrencisi Funda ASLANTAŞ BEYİN, ilgili yönetmeliklerin belirlediği gerekli tüm şartları yerine getirdikten sonra hazırladığı "SES STEGANOGRAFİ YÖNTEMLERİNİN KARŞILAŞTIRMALI ANALİZİ" başlıklı tezini aşağıda imzaları olan jüri önünde başarı ile sunmuştur.

Tez Danışmanı :	**Doç. Dr. Cemal HANİLÇİ** Bursa Teknik Üniversitesi	.....
Jüri Üyeleri :	**Doç. Dr. Ersen YILMAZ** Bursa Uludağ Üniversitesi	.....
	Dr. Öğr. Üyesi Mustafa ÖZDEN Bursa Teknik Üniversitesi	.....

Teslim Tarihi : /08/2021
Savunma Tarihi : 27/07/2021

20.04.2016 tarihli Resmi Gazete'de yayımlanan Lisansüstü Eğitim ve Öğretim Yönetmeliğinin 9/2 ve 22/2 maddeleri gereğince; Bu Lisansüstü teze, Bursa Teknik Üniversitesi'nin abonesi olduğu intihal yazılım programı kullanılarak Fen Bilimleri Enstitüsü'nün belirlemiş olduğu ölçütlere uygun rapor alınmıştır.

İNTİHAL BEYANI

Bu tezde görsel, işitsel ve yazılı biçimde sunulan tüm bilgi ve sonuçların akademik ve etik kurallara uyularak tarafımdan elde edildiğini, tez içinde yer alan ancak bu çalışmaya özgü olmayan tüm sonuç ve bilgileri tezde kaynak göstererek belgelediğimi, aksinin ortaya çıkması durumunda her türlü yasal sonucu kabul ettiğimi beyan ederim.

Öğrencinin Adı Soyadı: Funda ASLANTAŞ BEYİN

İmzası :



Aileme ve eşime,

ÖNSÖZ

Bu tez çalışmasının planlanmasında, araştırılmasında ve yürütülmesinde bilgi ve tecrübelerini esirgemeyen, ilgi ve sabrı ile tüm süreçte destek olan değerli hocam Doç. Dr. Cemal HANİLÇİ'ye teşekkür ederim.

Hayatımın her anında yanımda olan, motive eden, sevgilerini ve ilgilerini eksik etmeyen aileme ve bu süreçte yaşadığım zorluklarda bana güç veren eşime teşekkürü borç bilirim.

TEMMUZ 2021

Funda ASLANTAŞ BEYİN
Öğretim Görevlisi

İÇİNDEKİLER

Sayfa

ÖNSÖZ…..... v
İÇİNDEKİLER vi
KISALTMALAR viii
SEMBOLLER ix
ÇİZELGE LİSTESİ..... x
ŞEKİL LİSTESİ..... xi
ÖZET……..... xii
SUMMARY xiv
1. GİRİŞ……...1
1.1 Tezin Amacı 2
1.2 Literatür Araştırması 2
2. STEGANOGRAFİYE AİT TEORİK TEMELLER..... 10
2.1 Sinyal Kavramı..... 10
2.1.1 Analog sinyal 10
2.1.2 Dijital sinyal..... 10
2.1.3 Örnekleme frekansı 10
2.2 SNR Değeri 11
2.3 Konvolüsyon 11
2.4 Fourier Dönüşümü..... 12
2.5 Steganografi 12
2.6 Ses Steganografi..... 14
2.7 Ses Steganografi Yöntemleri..... 14
3. MATERYAL VE YÖNTEM..... 16
3.1 LSB (En Az Önemli Bit) Yöntemi..... 16
3.2 Yankı Veri Gizleme Yöntemi 18
3.3 Dalgacık Kodlaması Yöntemi 20
3.4 Tayf Yayılımı Yöntemi 21
3.5 Kepstrum Yöntemi 23
4. DENEYSEL SONUÇLAR VE TARTIŞMA..... 24
4.1 LSB Yönteminin Uygulanması 24
4.3 Dalgacık Kodlaması Tekniğinin Uygulanması 30
4.4 Tayf Yayılımı Tekniğinin Uygulanması 33
4.5 Kepstrum Tekniğinin Uygulanması 36
5. SONUÇ VE ÖNERİLER..... 39
KAYNAKLAR 43
ÖZGEÇMİŞ..... 45

KISALTMALAR

BER **:** Bit Error Rate

DFT **:** Discrete Fourier Transform

HAS **:** Human Auditory System

Hz **:** Hertz

IDFT : Inverse Fourier Transform

KHz **:** KiloHertz

Kbps **:** Kilobit per Second

LSB **:** Least Significant Bit

LWT **:** Lift Wavelet Transform

MSB **:** Most Significant Bit

PRS : Pseudo Random Sequence

SNR **:** Signal Noise Ratio

VoIP **:** Voice Over Internet Protocol

SEMBOLLER

fs **:** Örnekleme frekansı
E1 **:** 1 numaralı örnek erkek sesi
E2 **:** 2 numaralı örnek erkek sesi
E3 **:** 3 numaralı örnek erkek sesi
E4 **:** 4 numaralı örnek erkek sesi
E5 **:** 5 numaralı örnek erkek sesi
E6 **:** 6 numaralı örnek erkek sesi
E7 **:** 7 numaralı örnek erkek sesi
E8 **:** 8 numaralı örnek erkek sesi
E9 **:** 9 numaralı örnek erkek sesi
E10 **:** 10 numaralı örnek erkek sesi
K1 **:** 1 numaralı örnek kadın sesi
K2 **:** 2 numaralı örnek kadın sesi
K3 **:** 3 numaralı örnek kadın sesi
K4 **:** 4 numaralı örnek kadın sesi
K5 **:** 5 numaralı örnek kadın sesi
K6 **:** 6 numaralı örnek kadın sesi
K7 **:** 7 numaralı örnek kadın sesi
K8 **:** 8 numaralı örnek kadın sesi
K9 **:** 9 numaralı örnek kadın sesi
K10 **:** 10 numaralı örnek kadın sesi
α **:** Gömülen yankı genliği
δ **:** Delta/ Birim dürtü

ÇİZELGE LİSTESİ

Sayfa

Çizelge 4.1 : LSB tekniğine ait tüm mesaj uzunluklarındaki SNR değerleri. **26**
Çizelge 4.2 : Yankı Veri Gizlemetekniğine ait tüm mesaj uzunluklarındaki SNR değerleri **29**
Çizelge 4.3 : Dalgacık kodlaması tekniğine ait tüm mesaj uzunluklarındaki SNR değerleri.. ..... **32**
Çizelge 4.4 : Tayf Yayılımıtekniğine ait tüm mesaj uzunluklarındaki SNR değerleri **35**
Çizelge 4.5 : Kepstrum tekniğine ait tüm mesaj uzunluklarındaki SNR değerleri.... **38**

ŞEKİL LİSTESİ

Sayfa

Şekil 2.1 : Steganografi çeşitlerinin şematik gösterimi **13**
Şekil 2.2 : Steganografinin temel unsurları **13**
Şekil 2.3 : Çalışmada kullanılan ses steganografi teknikleri **15**
Şekil 2.4 : Stego sesten gizli mesaj elde etme işleminin şematik gösterimi **15**
Şekil 3.1 : LSB yönteminin örnek gösterimi **17**
Şekil 3.2 : Eşit zaman aralıklarına bölünen örnek bir sinyal **18**
Şekil 3.3 : Yankı çekirdekleri ve karıştırıcılar ile stego sinyal üretimi **19**
Şekil 3.4 : 3 Seviyeli dalgacık dönüşümünün temel yapı diyagramı **20**
Şekil 3.5 : Tayf yayılımı tekniğinde gizli mesaj yerleştirme prosedürü **22**
Şekil 4.1 : Orijinal ses dosyası ile LSB stego ses dosyasının karşılaştırılması **25**
Şekil 4.2 : Orijinal ses dosyası ile Yankı veri gizleme stego ses dosyasının karşılaştırılması **28**
Şekil 4.3 : Orijinal ses dosyası ile Dalgacık kodlaması stego ses dosyasının karşılaştırılması **30**
Şekil 4.4 : Orijinal ses dosyası ile Tayf Yayılımı stego ses dosyasının karşılaştırılması **34**
Şekil 4.5 : Orijinal ses dosyası ile Kepstrum stego ses dosyasının karşılaştırılması. **36**
Şekil 5.1 : 32–448-bit arası mesaj uzunluklarında SNR değerleri için yöntemlerin karşılaştırılması. **39**
Şekil 5.2 : 5 Steganografik tekniğe ait Spektrogram görüntüleri. **40**

SES STEGANOGRAFİ YÖNTEMLERİNİN KARŞILAŞTIRILMALI ANALİZİ

ÖZET

Bilgi güvenliği, hem bireyler hem de şirketler için tüm zamanların en önemli konularından biri olmuştur. Verilerin doğru alıcıya iletilmesi, kişisel verilerin korunması, kişisel yaşamın gizliliği ve ulusal güvenlik için çok önemlidir. Bu amaçla, kötü niyetli kişilerden bilgi gizlemek için yıllar içinde farklı yöntemler geliştirilmiştir. Steganografi büyük ilgi gören en önemli bilgi gizleme yöntemlerinden biridir. Bu çalışmada beş farklı konuşma steganografi tekniği kullanılmış ve deneysel verilerle tekniklerin kalite karşılaştırmaları yapılmıştır. Farklı gömme algoritmaları kullanılarak aynı çerçeve boyutuna sahip 10 kadın ve 10 erkek konuşmacıdan alınan toplam 20 adet konuşma sinyaline uzunluğu 32 ile 448-bit arasında değişen 14 farklı mesaj yerleştirilmiştir. Buna göre, kullanılan her ses dosyası için on dört farklı SNR değeri elde edilmiştir. Stego ve cover audio dosyaları arasında hesaplanan sinyal-gürültü oranları (SNR), gömülü mesaj uzunluğu, örneklerin genlik değerlerinin toplamı ve kullanılan çerçeve boyutu faktörlerinin kaliteyi belirleyen ana faktörler olduğunu göstermektedir. Ayrıca oluşturulan stego ses dosyalarının dinlenmesinde insan işitme sisteminin ayırt edebileceği kapak sesi ile stego sesi arasında bir fark olmadığı görülmüştür. Çalışmaya kapak ve stego sesi grafikleri eklenmiş ve aralarında hemen hiç fark olmadığı görülmüştür. Ayrıca kapak ses sinyali ve stego sinyallerin spektrogramları karşılaştırımış ve mesaj gizlemenin daha çok yüksek frekans bölgesini etkilediği gösterilmiştir.

Anahtar kelimeler: Ses Steganografi Teknikleri, Stego Ses, İnsan İşitsel Sistemi, Veri Gizleme, Gizli Mesaj.

COMPARATIVE ANALYSIS OF AUDIO STEGANOGRAPYH METHODS

SUMMARY

Information security has been one of the most important issues of all time for both individual and companies. Delivering data to the correct recipient is crucial for personal data protection, privacy of personal life and national security. To this end, different methods have been developed over the years to hide information from malicious individuals. Steganography is one of the most important information hiding method received great attention. In this study, five different audio steganography techniques are utilized and comparisons of these techniques are performed with experimental data. Using different embedding algorithms, 14 different messages ranging in length from 32 to 448 bits were placed in 20 audio files of 10 females and 10 males with the same frame size. Accordingly, fourteen different SNR values were obtained for each audio file used. Signal-to-noise ratios (SNR) computed between stego and cover audio files show that embedded message length, sum of amplitude values of the samples and frame size are the main factors that determine the quality. In addition, it was observed that there is no perceptual differences between the cover and stego audio recordings. Hence, the human auditory system is unable to determine whether an audio recording is authentic or conveys a hidden message. The spectrographic comparison of the cover and stego audio recordings show that hiding the secret message to an original audio signal highly affects the high-frequency region than the low-frequency components.

Keywords: Audio Steganography Techniques, Stego Audio, Human Auditory System, Data Hiding, Secret Message.

1. GİRİŞ

Bilgi güvenliği hayatın her alanında çok önemli bir yer kaplamaktadır. Özellikle ülkelerin milli güvenliği konusunda çeşitli gizlilik derecelerine sahip her türlü verinin, iletilmek istenen kişi ve kişilere aktarımının sağlıklı bir şekilde yapılması gereklilikten çok mecburiyettir. Teknolojinin ilerlemesi ve internet kullanımının yaygınlaşması ile birlikte artan siber saldırılar bu alandaki çalışmaların baş motivasyonlarından biridir. Sahte yazılımlarla gizli bilgilere doğrudan erişim sağlanabilmektedir. İletilen verinin korunması ile ilgili olarak farklı çalışmalar mevcuttur. Kişilerin sosyal/özel hayatlarında kullandıkları mesajlaşma platformlarında özel hayatın gizliliğinin korunması ve bilgi güvenliğinin sağlanması kapsamında kullanılan uçtan uca şifreleme yöntemi de bu çalışmalara örnektir. Kriptoloji bilimi de mesajı vericiden alıcıya ulaştırırken içeriğini üçüncü şahıslardan korumak için kullanılmaktadır. İletilmek istenen mesaj, sadece alıcı ve vericinin anlayacağı şekilde şifrelenmektedir. Bunu sağlamak amacıyla farklı algoritmalar geliştirilmiştir. Fakat kriptolojide şifrenin çözülebilmesi riski nedeni ile tek başına kullanıldığında saldırılara karşı yetersiz kalabilmektedir.

Bu çalışmaya konu olan steganografi de bir mesaj gizleme tekniğidir. Ses sinyalinin kılıf/taşıyıcı olarak kullanılması sinyalin kalitesini artıran bir bakış açısı sunmaktadır. Oldukça fazla sayıda bite sahip olması nedeniyle, yerleştirilen mesaj bitleri sinyal içerisinde yüksek bozulmalara neden olmaz. Kılıf/taşıyıcı dosyada kullanılan bit sayısı arttıkça medya içerisine gizlenen mesajın insan işitsel sistemi (Human Auditory System - HAS) tarafından fark edilebilirliği ve sinyaldeki bozulma oranı azalır. Böylece sinyal gürültü oranı (signal-to-noise ratio - SNR) değeri artar.

Ses steganografide mesaj, ses dosyasının içine gömülür. Yine kılıf/taşıyıcı dosyada olduğu gibi gizlenecek mesaj da resim, video, ses gibi farklı dosya tipine sahip olabilir. Gönderilen dosyadaki bozulma oranı, gömme kapasitesi ve dosya boyutunda meydana gelebilecek değişiklik gibi farklı parametreler mesaj tipinin belirlenmesinde önemli rol oynamaktadır.

1.1 Tezin Amacı

Ses steganografiye ait az sayıda çalışma yapılmış olması bu çalışmanın ortaya çıkmasının ana sebeplerinden biridir. Diğer steganografi yöntemlerine kıyasla daha az tercih edilmesinin sebebi olarak insan işitsel sisteminin hassaslığı öne çıkmıştır. Ses steganografi işlemini gerçekleştirebilmek için farklı teknikler mevcuttur. Temelde, kullanılan tüm tekniklerin amacı bir ses dosyasının içerisine bir metin mesajı gizlemektir. Tek bir yöntem yerine birden çok yöntem kullanılması, gizlenecek mesaj boyutunun stego seste meydana gelecek bozulma miktarına doğrudan etki etmesinden kaynaklanmaktadır. Bu çalışmada amaç; LSB kodlaması, dalgacık kodlaması, tayf yayılımı, yankı veri gizlemesi ve kepstrum yöntemlerini kullanarak aynı kılıf/taşıyıcı ses dosyasına aynı mesajın gizlenmesi sonucu oluşan stego seslerin SNR sonuçlarını karşılaştırmak ve kullanılması en uygun yöntemi önermektir. Çalışmada farklı uzunluklardaki ses dosyalarının kullanılmasının sebebi, dosya boyutlarının steganografi yöntemlerine etkisini ortaya koymaktır. Kadın ve erkek toplam 20 ses dosyası kullanılarak cinsiyetin kalite üzerine etkisinin olup olmadığı gözlenmeye çalışılmıştır.

1.2 Literatür Araştırması

Dutta ve arkadaşları [1] çalışmalarında steganografiye ait 4 farklı tekniği genel olarak ele almış, avantaj ve dezavantajlarından bahsetmişlerdir. Bu teknikler faz kodlaması (phase coding), eşlik kodlaması (parity coding), yankı veri gizlemesi (echo hiding) ve tayf yayılımı (spread spectrum) yöntemleridir. Faz kodlaması ve eşlik kodlaması için dezavantajlarını ortaya koymuş, LSB metodunun ses steganografi için daha uygun olduğunu belirtmişlerdir. Bu çalışmada LSB metodunun öne çıkarılmasının sebebi olarak tek seferde daha büyük miktarlarda verinin kodlanmasına izin vermesi ve steganografi işlemi tamamlandıktan sonra dosya boyutunda bir değişiklik olmaması gösterilmiştir.

Ingemar ve arkadaşları [2] çalışmalarında steganografi ile ilgili bir öneri ortaya koymuşlardır. Bu öneri mesajın iletilmesi için kullanılan kılıf/taşıyıcı multimedya dosyasının tipi ile mesajın dosya tipinin aynı olmasıdır. Bu çalışmada yapılan steganografi işlemi bir resim dosyası içerisine yine bir resim dosyası gizlemektir. Fakat önerilen yöntem gönderilecek mesajın boyutunu kısıtlamakta ve küçülmesine

yol açmaktadır. Önerilen yöntemin diğer (ses ve video gibi) dosya/veri tipleri içinde uygun olduğu belirtilmiştir.

Bandyopadhyay ve arkadaşları [3] internetin kullanımının yaygınlaşması ile bilgiye ulaşmanın kolaylığından dolayı steganografiye duyulan ihtiyacın arttığını belirtmişlerdir. Bu çalışmada literatürde yer alan steganografi tekniklerinin bir derlemesi yapılmış olup resim, video, ses ve metin steganografi hakkında temel bilgiler verilmiştir. Steganografinin tarihçesi ile ilgili bilgiler de bu çalışmada yer almaktadır. Kriptoloji ile işbirliği yapılması halinde yapılan steganografinin daha sağlam olacağı belirtilmiştir.

Kumar ve arkadaşları [4] bilgi güvenliğini sağlamak amacıyla steganografide kullanılan farklı iki yöntemi karşılaştırmak için yaptıkları çalışmada LSB yöntemi ve faz kodlaması tekniğini ele almışlardır. Genel hatları ile bu tekniklerin nasıl uygulanacakları hakkında bilgileri veren akış şemaları ve şablonlar sunulmuştur. Yapılan steganografi işlemine ait sonuçlara ilgili çalışmada yer verilmiştir.

Mishra ve arkadaşları [5] bilgi güvenliği ve veri gizliliğinin steganografi stratejileri uygulanarak sağlanabileceğini mevcut steganografik stratejilerin büyük kısmının, gizemli bilgileri gizlemek için bilgisayarlı görüntü ve ses belgelerini yayılmış bir ortam olarak kullanmışlardır. Kaynak dosyalarının karşılaştırmalarını yaparak ses dosyalarının, mesaj gizlemek için daha geniş alanlara sahip olduğu belirtilerek ses steganografi yöntemlerinden LSB, eşlik kodlaması ve yankı veri gizlemesi yöntemleri ele alınmıştır.

Sridevi ve arkadaşları [6] çalışmalarında gelişmiş ses steganografisinden bahsetmişlerdir. Gelişmiş ses steganografisi, ses steganografisi ve kriptografisine dayanan, kaynak ve hedef arasında veri aktarımı sağlamak için önerilen bir sistemdir. Şifreleme algoritmasını ilk güvenlik düzeyinde kullanan bu sistem çok karmaşık bir yapıya sahiptir. İkinci güvenlik seviyesinde, mesajı sese kodlamak için LSB algoritması kullanılmaktadır. Yani mesajı kodlamak için bit seviyesinde işlem yapılmaktadır. Çalışmada asıl amaç bilgisayar korsanlarından verileri gizlemek ve hedefe daha güvenli bir şekilde gönderilen veriler için iyi ve etkili bir yöntem sağlamaktır. Bu yöntemde ses kalitesi, kullanıcının seçtiği sesin boyutuna ve mesajın uzunluğuna bağlıdır. Bir bütün olarak bitteki sapmalara rağmen sesteki değişiklik tespit edilememiştir. Önerilen bu sistem ile veri boyutunda herhangi bir değişiklik

olmamaktadır. Güvenlik sistemini sağlam kılmak için şifreleme ve şifre çözme teknikleri kullanılmıştır.

Petrovic ve arkadaşları [7] veri gizleme tekniklerine genel bir bakış sunan bir çalışma yapmışlardır. Çalışmada kısa vadeli özilinti modülasyonundan bahsedilmiştir. Süreci optimize etmek için öncelikle doğal özilinti hesaplanmış ve gerekli değişkenler belirlenmiştir. Gömülü kanal kapasitesini ya da güvenliğini artırmak için örtüşen aralıklarla çoklu gecikmelerde otomatik korelasyon modülasyon yapmanın mümkün olduğunu savunmuşlardır.

Wakiyama ve arkadaşları [8] çalışmalarında LSB kodlaması ile bir ses steganografisi işlemi yapmışlardır. Buradaki yaklaşım, kılıf/taşıyıcı ses verisindeki alt bitin verisini gizli veri biti ile değiştirmek olmuştur. Ses verisi olarak 8-bit mono ses kullanılmıştır. Gizlenilen veri yazılı bir metin dosyasıdır. Bu çalışmada iki çeşit yeni düşük bit kodlama tekniği önerilmiştir. Yeni bir program tasarlanmış ve programın doğruluğunu test etmek için deneyler yapmışlardır. Önerdikleri yöntemde çevre ses verilerinin ortalama genlik verilerini eşik olarak kullanan bir yöntemdir. 2 biti gömmek için 8 bitlik örneğin kalan 6 bitinin genliklerinin ortalamasını hesaplamışlardır. Gömülecek bitin genlik seviyesi bu ortalama değerden büyükse gömme verileri için iki basamak kullanılmıştır.

Djebbar ve arkadaşları [9] dijital ses steganografi teknikleri ile ilgili literatür ortaya koymuşlardır. Güvenli iletişimi sağlamak için steganografik tekniklerin potansiyelleri ve sınırları araştırılmıştır. İncelenen teknikler için bir karşılaştırma ve değerlendirme sunulmuştur. Bu karşılaştırma sinyal/gürültü oranı (SNR) kullanılarak yapılmıştır.

Asad ve arkadaşları [10] çalışmalarında geleneksel LSB metodunun steganalize karşı daha hassas steganografi işleminin daha güvenli olması için geleneksel LSB yönteminde bir takım değişiklikler yapmışlardır. Kullandıkları teknik, kılıf/taşıyıcı sinyale ait dört bit için gizli mesaj bitini gömmektedir. Maksimum gömme oranı taşıyıcı mesaj biti başına gizli mesaj bitidir. Minimum gömme oranı taşıyıcı mesajın 8 biti için bir gizli mesaj bitidir. Gizli iletinin tamamen gömülü olduğundan emin olmak için taşıyıcı örneklerinin gizli ileti bit sayısının sekiz katı olması gerekir. Önerilen metodoloji temelinde oluşturulan stego mesaj, taşıyıcı (orijinal) mesajdan ayırt edilemez.

Bilgin [11] çalışmasında ağırlıklı olarak steganografinin amacından ve öneminden bahsetmiştir. Steganografi hakkında genel bilgilere yer verirken, gizlenen mesajın boyutunun artması ile birlikte dayanıklılığın azalacağı belirtilmiştir. Mesaj kapasitesindeki artışın, kılıf/taşıyıcı dosyada da dayanıklılık ve kapasite ile ilgili değişimler meydana getirdiği belirtilmiş olup, yapılacak işlem için önem sırasına göre steganografik teknik seçmenin daha uygun olduğu ifade edilmiştir. Yine bu çalışmada steganografi ile kriptoloji yani şifreleme yöntemlerinin birlikte kullanılmasının veri gizleme açısından daha sağlıklı olacağından bahsedilmiştir.

Cao ve Zhang [12] "Researches on Echo Kernels of Audio Digital Watermarking Technology Based on Echo Hiding" adlı makalelerinde yankı veri gizlemesi tekniğinin temelleri olan ve literatürde "Echo Kernels" olarak geçen matematiksel ifadeleri açıklamış ve yankı veri gizlemesi için yeni bir eko kerneli önermişlerdir. Önerilen yöntemin, tek bir yankı yerine birden çok küçük yankı getirdiğini söylemişlerdir. Geleneksel yankı veri gizleme yöntemi ile karşılaştırıldığında, ortak sinyal işleme işlemlerine karşı daha sağlam ve kurcalamaya karşı dayanıklı olduğunu savunmuşlardır.

Tekeli ve Aşlıyan [13] 2017 yılında yayınladıkları makalede yankı veri gizlemesi yöntemine ait yankı çekirdeği fonksiyonlarını matematiksel olarak açıklamış ve bu modellerin hangilerinin kullanımının daha avantajlı ve pratik olduğunu belirtmişlerdir. MATLAB ortamında kodlanan tek, bipolar, geri-ileri, bipolar geri-ileri ve zaman aralığı gibi birçok yankı çekirdeği mp3 sıkıştırma, algılanamazlık ve kapasiteye karşı sağlamlık açısından karşılaştırmışlardır. Sonuç olarak, bipolar ileri geri yankı çekirdeğinin sıkıştırmaya karşı daha sağlam olduğunu ve daha yüksek bir SNR verdiği gösterilmiştir.

Cvejic ve Seppänen [14] geleneksel olarak, temel LSB işitsel steganografi yöntemine örnek başına üç vuruşluk algısal bir sınır uygulandığını söyleyerek standart LSB algoritmasında örnek başına dört bit gömülebilen, böylece veri gizleme kanalının kapasitesini% 33 artırabilen yeni bir değişiklik sunmuşlardır. Bu çalışmada önerilen algoritma, LSB tekniği için minimum hata değiştirme yöntemini ve SNR değerini azaltmak için değiştirilmiş hata difüzyon yöntemini kullanılmıştır.

Kekre ve arkadaşları [15] çalışmalarında genel olarak steganografinin ne için kullanıldığından bahsetmiş ve steganografi için bazı yöntemler sunmuşlardır. Bu

yöntemlerden bir tanesi LSB metodunu kullanarak kılıf/taşıyıcı sesin güvenliğini artırmak için şifreleme yönteminin steganografi ile birlikte yapılmasıdır. İkinci yöntemde ise lsb'lerde XOR işlemini gerçekleştirir ve XOR işleminin sonucu ile gömülecek mesaj bitine bağlı olarak lsb'nin değiştirilip değiştirilemeyeceğine karar verilir. Bu işlemin yararlarından birkaçı uygulamanın basit ve ucuz olmasıdır. LSB metodunda XOR işleminin detayları makalede ayrıntılı bir şekilde açıklanmıştır.

Kaur ve Behal [16] çalışmalarında ses steganografisi ve ses steganografi tekniklerini açıklayarak ses steganografisindeki güvenlik seviyesini artırmayı amaçlamışlardır. Steganografinin güvenlik seviyesini saldırılara karşı daha güvenli hale getirmek için bir yöntem önermişlerdir. Önerdikleri yöntem iki seviyeli güvenlik işleminden oluşmaktadır. Bu yöntemde mesaj olarak resim veya ses dosyası seçilmiş olup seçilen mesaj binary(ikili) forma dönüştürülür. Dönüştürülen mesaj, bir resim dosyasının içerisine gömülür. Daha sonra asıl olarak alıcıya gönderilecek olan ses, kılıf/taşıyıcı dosya seçimi yapılır ve önceden resim steganografisi yapılmış stego resim, mesaj olarak seçilen ses dosyasına gömülerek güvenlik artırılmaktadır.

Djebbar ve arkadaşları [17] çalışmalarında çok yönlü steganografik yöntemler önermişlerdir. Mevcut dijital ses steganografi teknikleri incelenmiş ve performans, sağlamlık, güvenlik ve gizleme kapasitesi parametrelerine dayanarak değerlendirilmiştir. Steganografik yöntemlerin avantaj ve dezavantajlarına yer verilmiştir. Ses dosyasının sıklıkla kullanılmasının ve popülaritesinin, dosyadan ilgisiz kişiler için şüphe yaratmayacağını savunmuşlardır.

Bender ve arkadaşları [18] çalışmalarında veri gizleme sürecini ele almak için hem mevcut hem de yeni teknikleri araştırmışlardır. Araştırılan teknikleri, telif hakkı koruması, karıştırma/kurcalama koruması ve genişletme/artırma verilerinin eklenmesi parametrelerine göre karşılaştırmışlardır. Metin, resim ve ses için steganografi yapılmış ve tüm yöntemlerin başarılı sonuçlara ulaşılsada farklı kısıtlamalara sahip olduğu belirtilmiştir.

Tian ve arkadaşları [19] çalışmalarında internet protokolü üzerinden LSB metodunu temel alan bir iletişim modeli sunmaktadır. Önerilen model VoIP için hayati öneme sahip gizli mesajların ve gerçek zamanlı performansın güvenliğini sağlamayı amaçlamaktadır. Bu amaçla gömme işleminden önce bir gizli mesaj şifrelemesi kullanılmıştır. Bu şifreleme yönteminin gizli mesajlar için kısa süreli koruma

sağlamakla birlikte VoIP için düşük gecikme süresi arasında iyi bir denge kurduğu belirtilmiştir.

Kadhom ve Azize [20] çalışmalarında gizli mesajları güvenli bir şekilde iletmek için, dijital seste, şifreleme ve gizleme işlemini kılıf/taşıyıcı dosyada herhangi bir bozulma olmadan yapmayı önermişlerdir. Önerilen yöntem büyük bir yük kapasitesine ve yüksek SNR değerine sahiptir. Mesajı şifrelemek için knapsack (sırt çantası) algoritması kullanmışlardır. İşlem, mesajı çözmek için anahtarın belirlenmesi, mesajın şifrelenmesi ve şifrelenmiş mesajın binary (ikili) forma dönüştürülmüş ses sinyali örneklerine gömülmesi adımlarından oluşmaktadır. Burada ses sinyalinin örnekleri yaklaşık ve ayrıntılı katsayılar olarak adlandırılan iki vektöre ayrıştırılır. Bu işlem için Lift Wavelet Transform (LWT) kullanmışlardır. Gizleme işleminde LSB yöntemini seçmiş ve yaklaşık katsayıları kullanmışlardır. Gizleme işlemi yapıldıktan sonra stego çerçeve ve orjinal çerçeve aynı olmuş, herhangi bir bozulma meydana gelmemiştir.

Bhavana ve arkadaşları [21] çalışmalarında MATLAB yazılımı kullanılarak bir ses ve resim dosyasına mesajın nasıl gizleneceğini açıklamışlardır. Genel olarak kriptoloji ve steganografinin tanım ve tekniklerinden bahsetmişlerdir. Çalışmada steganalizin kısa bir tanımı yapılmış, örüntü tanıma ve özellik çıkarımının steganaliz için öneminden bahsedilmiştir. Bir resim ve bir ses dosyası için steganografi işlemi yapılmıştır.

Tian ve arkadaşları [22] bu çalışmada VoIP için gerçek zamanlı performanstan ödün vermeden, gizli mesajlar için daha iyi güvenlik sağlamayı amaçlayan yeni bir gerçek zamanlı steganografi modeli sunmuşlardır. Bu modele LSB metodunu kullanarak ulaşmışlardır. Yaptıkları deneyler ile önerilen tekniğin VoIP'nin gerçek zamanlı gereksinimlerini yeterli bir şekilde yerine getirirken, gizli mesajları iletmek için yüksek güvenlik ve şeffaflık sağladığını göstermişlerdir.

Shah ve arkadaşları [23] çalışmalarında orijinal kapak ses sinyalinin dalgacık paket katsayılarını, önerdikleri Adaptive Wavelet Packet Based Audio Steganography isimli teknik ile değiştirerek ses steganografi yapmışlardır. Bu teknik ile steganografi uygulanırken meydana gelen gürültünün oldukça düşük olduğu ve bu sebeple yüksek SNR değeri elde edildiği gösterilmiştir.

Gupta ve Sharma [24] da yine güvenlik kaygıları ile Discrete Wavelet Transform (DWT) kavramını ve LSB tekniğini kullanarak yeni bir yöntem önermişlerdir. Kapak ses dosyasını ikili (binary) forma çevirdikten sonra ses dosyasının içine bir resim mesajı gömmüşlerdir. Mesaj gömüldükten sonra sinyale Discrete Wavelet Transformunu uygulamışlardır.

Bilal ve arkadaşları [25] steganografiye ait son teknikleri ele almışlar ve bunların avantaj ve dezavantajlarını içeren bir karşılaştırma sunmuşlardır. Yine bahsettikleri steganografi yöntemlerinin performans değerlendirmelerini de paylaşmışlardır.

Kartheeswaran ve arkadaşları [26] mesaja şifreleme tekniği uygulayan Multi-Agent Based steganografiyi önermiş ve daha güvenli bir steganografi sonucu elde edileceğini ileri sürmüşlerdir. Bu işlem ile steganografinin uygulanabilirliğini arttırmayı hedeflemişlerdir.

Lindawati ve Siburian [27] Android akıllı telefon kullanarak LSB tekniği ile steganografi yapmışlardır. Steganografiyi bir akıllı telefon ile yapacak programı tasarlayarak steganografinin uygulama kolaylığını öne çıkarmışlardır.

Rajput ve arkadaşları [28] LSB tekniğini uygularken kapak ses sinyalinin en değerli bit (most siginificant bit - MSB) değerini de hesaba katmışlardır. Mesaj sinyalinin örneklerini sırayla ikişer ikişer, kapak ses sinyalinin MSB'sine bağlı olarak (0 veya 1 olması durumuna göre) tek seferde gömerek steganografide güvenliği arttırdıklarını savunmuşlardır.

Teotia ve Srivastava [29] çalışmalarında ses ve video steganografideki hataları azaltan hibrit bir algoritma sunmuşlardır. Huffman kodlaması olan sıkıştırma tekniğini kullanarak veriyi sıkıştırmışlardır. Bu işlemin hem veri saklama alanını artırdığını hem de alıcı tarafındaki kullanıcının sıkıştırma işlemini fark edememesinden dolayı güvenlik seviyesini artırdığını öne sürmüşlerdir.

Anwar ve arkadaşları [30] çalışmalarında Lifting Wavelet Transform (LWT) ve Dynamic Key tekniği kullanarak steganografi yapmışlardır. Advanced Encryption Standard (AES) ile şifreledikleri gizli mesajı LWT tekniği ile kapak ses dosyasına gömmüşlerdir. Bu yöntemin Android cihazlarda iyi çalışacağını tahmin etmektedirler.

Sobin C.C. ve Manikandan [31] çalışmalarında steganografi işleminde güvenli bir şifreleme şemasının kullanılmasının gerekliliğinden bahsetmişlerdir. Şifrelenmiş

gizli mesaj seçilmiş olan bit düzlemine gömüldükten sonra genetik algoritmanın stego ses üzerindeki bozulmaları azalttığını ileri sürmüşlerdir.

2. STEGANOGRAFİYE AİT TEORİK TEMELLER

Çalışmanın bu bölümünde steganografinin tarihini de içine alan kapsamlı bir tanımı yapılmış, ağırlıklı olarak bu çalışmanın konusu olan ses steganografisi ve ses steganografi teknikleri ve alakalı teorik temellere yer verilmiştir.

2.1 Sinyal Kavramı

Sinyal, bir cihazdan veya ağdan diğerine veri taşımak için kullanılan bir elektrik veya elektromanyetik akımdır. Başka bir deyişle sinyal, tek değerli bir zaman fonksiyonudur. Sinyaller kendi içlerinde farklı kıstaslara göre sınıflandırılabilirken, temelde analog ve sayısal sinyaller olarak ikiye ayrılmaktadır.

2.1.1 Analog sinyal

Sürekli genliğe sahip bir sürekli zaman sinyaline genellikle analog sinyal denir. Konuşma sinyali, analog sinyale bir örnektir. Bu sinyallerin işlenmeden önce dijital sinyale dönüştürülmesi gerekir.

2.1.2 Dijital sinyal

Sonlu sayıda basamakla temsil edilen ayrık değerli genliklere sahip ayrık bir zaman sinyali dijital sinyaldir. Analog sinyaller, örnekleme adı verilen bir işlemle dijital sinyallere dönüştürülür. Burada sinyal analog sinyalden dijital sinyale dönüştürülürken önemli olan faktör örnekleme frekansıdır.

2.1.3 Örnekleme frekansı

Örnekleme frekansı (veya örnekleme oranı) analog sinyalin örneklenirken sinyalden bir saniyede kaç adet örnek alınacağını belirten bir parametre olup Nyquist kriterine göre seçilmesi büyük önem arz etmektedir. Bu değer sinyalin bir saniyede kaç adet örneğe sahip olacağını belirler. Sembolü fs'dir. Bu tez çalışmasında örnekleme frekansı 8 kHz olan konuşma sinyalleri kullanılmıştır. Örnek sayısının fazla olması sinyal üzerinde çalışılabilir alanı artırdığından steganografi açısından gömülebilecek veri boyutunu da etkilemektedir.

2.2 SNR Değeri

Literatürde geçen ismiyle "Signal to Noise Ratio" sinyal-gürültü oranını ifade eder. Bir sinyalin gücünü belirlemek için sinyal-gürültü oranının hesaplanması gerekir. Bu oran ne kadar yüksek olursa, gerçek bir sinyali tespit etmek veya ham sinyalden faydalı bilgileri çıkarmak o kadar kolay olur. Elektronikte sinyal ve gürültü, desibel cinsinden ölçülür. Bazı çalışmalarda sinyal kalitesini hesaplamak için bit hata oranını veren BER ölçütünün kullanıldığı görülmüştür. Bu çalışmada karşılaştırmalar ve değerlendirmeler SNR'ye göre yapılmıştır. Denklem 2.1, sinyal-gürültü oranını desibel cinsinden hesaplayan matematiksel ifadeyi göstermektedir [14]. Denklemdeki $x[n]$ değerleri orjinal sinyal örneklerini temsil ederken, $y[n]$ değerleri stego ses sinyaline ait sinyal örneklerini temsil etmektedir. Buradaki n değeri, kullanılan sinyalde bulunan mevcut örnek sayısıdır.

$$SNR = 10.log\frac{\sum_n x^2(n)}{\sum_n [x(n)-y(n)]^2} \tag{2.1}$$

2.3 Konvolüsyon

Konvolüsyon en temel haliyle, iki fonksiyondan birinin diğeri tarafından nasıl değiştirildiğini ifade eden üçüncü bir fonksiyon üreten, iki fonksiyon üzerinde uygulanan matematiksel bir işlemdir. Bu çalışmada konvolüsyon yankı veri gizlemesi tekniğinde yankı çekirdeği adı verilen yapıların ve stego seslerin oluşturulması için kullanılır. f ve g gibi iki fonksiyonlarının [0,t] sonlu aralığında konvolüsyonu denklem 2.2 yardımı ile,

$$[f * g](t) = \int_0^t f(\tau).g(t-\tau)d\tau \tag{2.2}$$

şeklinde hesaplanır. Genellikle konvolüsyon sonsuz aralıkta $[-\infty,+\infty]$ alınır [32].

Yankı veri gizleme yöntemi uygulanırken gizli mesaj sinyali, ses sinyalinin içerisine yankı olarak ekleneceği için öncelikle bir yankı oluşturulmak istenir. Bu da orijinal ses sinyali ve verilen gecikme miktarı kadar bir ötelemenin konvolüsyonu ile elde edilir.

2.4 Fourier Dönüşümü

Fourier dönüşümü, sinyal hakkında bilgi sahibi olmak için sinyal işlemede sıklıkla kullanılan bir dönüşüm türüdür. Sinyali, katsayıları sinyale özel sinüs ve kosinüler toplamı şeklinde ifade ederek işlenebilecek forma dönüştürür. Fourier dönüşümü hem sürekli hem de ayrık sinyaller için kullanılabilir. Sinyallerin genellikle zaman domeninde gösterilir ancak frekans domeni sinyal ile ilgili daha geniş ölçekte bilgi elde etme imkanı sunmaktadır. Bundan dolayı fourier dönüşümü kullanılarak sinyal zaman domeninden frekans domenine aktarılır. Bir $\boldsymbol{x}[\boldsymbol{n}]$ ayrık sinyaline Ayrık Zamanlı Fourier Dönüşümü (DFT) uygulanır. DFT'nin formülü denklem 2.3'te verilmiştir [33].

$$X\left(e^{jw}\right) = F\left\{x[n]\right\} = \sum_{n=-\infty}^{\infty} x(n)e^{-jwn} \tag{2.3}$$

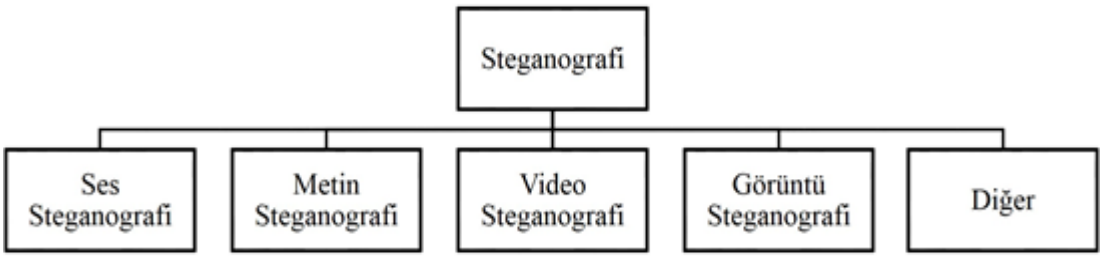
Bu şekilde sinyalin değişik frekanslarda karmaşık üstel bileşenleri elde edilir. Sinyalin frekans domenindeki analizleri tamamlandığına Ters Fourier Dönüşümü (IDFT) ile tekrar zaman domenine geçiş yapılır. IDFT'nin formülü denklem 2.4'te verilmiştir [33].

$$f(t) = \frac{1}{N}\sum_{n=0}^{N-1} X(k)e^{j2\pi kn/N} \tag{2.4}$$

2.5 Steganografi

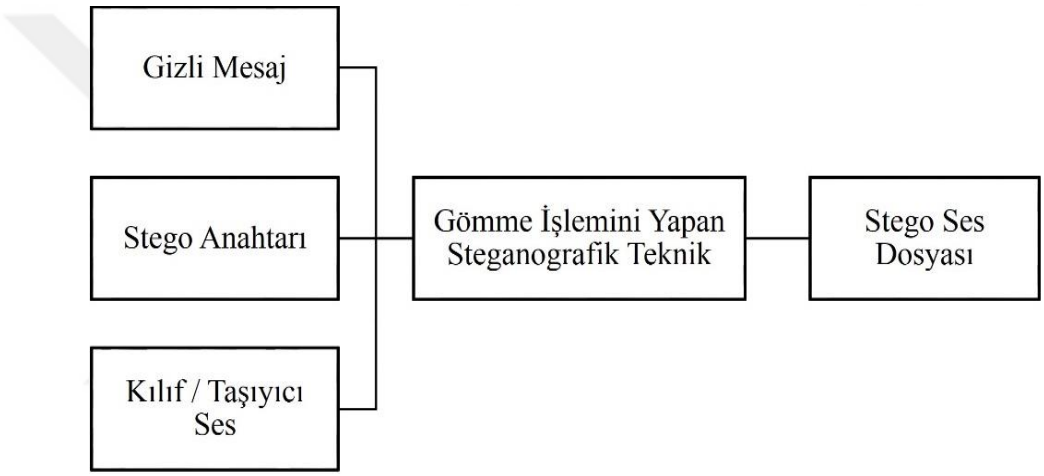
Steganografi, literatürde veri gizleme sanatı ya da bilimi olarak geçmektedir. Yunanca, gizli veya örtülü anlamına gelen "stegos" ve yazma anlamına gelen "graphia" kelimelerinin birleştirilmesi ile oluşmuştur. Antik Yunan kayıtlarında, balmumu kullanılarak yapılan steganografiden bahsedilmektedir. Tahta üzerine yazılan mesaj üzerine eritilen balmumu tabletleri ile tahta üzerine hiç yazı yazılmamış görüntüsü verilmiş ve böylece gizli mesaj üçüncü kişilerce hiç şüphe uyandırmadan alıcıya iletilebilmiştir [33].

Steganografinin amacı gizli bir mesajı başka bir medya dosyasını kılıf/taşıyıcı olarak kullanarak alıcıya iletmektir. Şekil 2.1'de gösterildiği gibi genel olarak tüm dijital ortamlar, sinyaller veya dosyalar steganografi işlemi için kılıf/taşıyıcı olarak kullanılabilir.



Şekil 2.1: Steganografi çeşitlerinin şematik gösterimi.

Steganografi işleminin temel unsurları Şekil 2.2'de gösterilmiştir. Kılıf/taşıyıcı olarak adlandırılan orijinal dosya, gizlenecek mesaj, alıcının mesaja ulaşması için gerekli olan stego anahtarı ve gizleme işlemi bittikten sonra oluşan stego dosyadır.



Şekil 2.2: Steganografinin temel unsurları.

Kılıf/taşıyıcı medyanın içine gömülen mesaj, alıcı ve verici haricindeki kişiler tarafından fark edilmezken, yalnızca stego anahtarı bilen kişiler gizli mesaja ulaşabilmektedir. Oluşan stego dosyanın içindeki mesajın fark edilmemesinin sebebi, insan duyu sisteminin bit veya piksel bazında yapılan değişiklikleri algılayamamasıdır.

2.6 Ses Steganografi

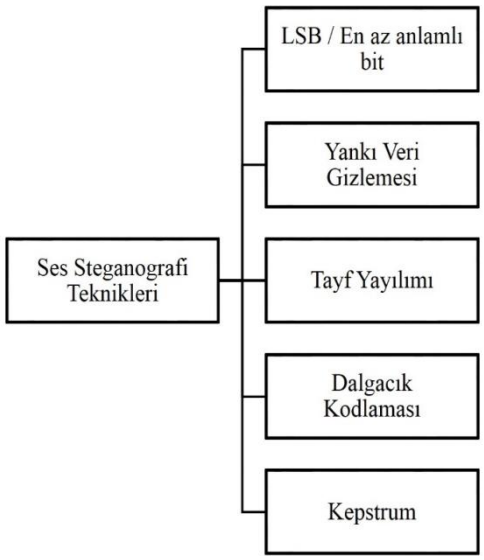
Ses steganografi, saf bir ses dosyasına gizli bilgileri gizlemeye veya güvenli ve sağlam bir şekilde sinyal vermeye odaklanmıştır [35]. Steganografi işleminde gizli bilgilerin varlığı iletişim sırasında gizlenmektedir.

Ses steganografinin temel modeli kılıf/taşıyıcı ses dosyası, mesaj ve şifredir. Burada mesaj, göndericinin gizli kalmasını istediği verilerdir. Bu çalışmada mesaj olarak düz metin mesajı kullanılmıştır. Şifre, literatürde genellikle stego-key olarak geçmektedir. Kılıf taşıyıcı dosya ile mesajı birbirinden ayırmak için kullanılmaktadır. Ses dosyalarının steganografi işlemi için kullanılmasının ana sebeplerinden biri kılıf/taşıyıcı sesin kalitesini bozmadan değiştirilebilecek bit sayısının fazla olmasıdır.

2.7 Ses Steganografi Yöntemleri

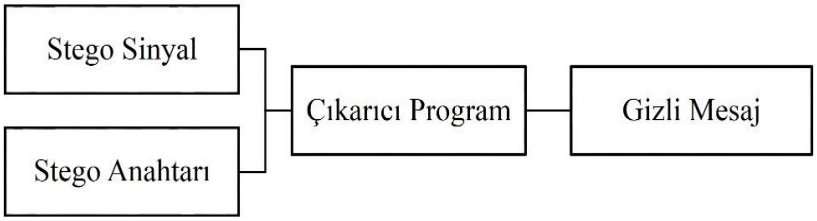
Ses steganografi için birden fazla yöntem vardır. Sayısal sinyalin farklı parametrelerine hitap eden yöntemler ihtiyaca göre uygulanmaktadır. Bu yöntemler uygulanarak yapılan steganografi işleminde kalite unsurları belirleyici olarak öne çıkmaktadır. Yöntemlerin birbirlerine göre avantaj veya dezavantajları bulunmaktadır. Bir yöntemin diğerine göre üstünlüğü öne çıkarılırken çoğunlukla elde edilen sinyal kalitesine yer verilir. Bu tez çalışmasında elde edilen ve SNR değerlerine göre karşılaştırılmaları yapılan veriler beş farklı steganografik yönteme aittir. Literatürde geçen İngilizce ve Türkçe karşılıkları ile; Least significant bit coding/ en az anlamlı bit kodlaması, echo hiding/yankı veri gizlemesi, cepstrum, spread spectrum/tayf yayılımı ve wavelet coding/dalgacık kodlaması kullanılarak steganografi işlemi gerçekleştirilmiştir.

Bu tez çalışmasında kullanılan steganografik teknikler Şekil 2.3'te gösterilmiştir.



Şekil 2.3: Çalışmada kullanılan ses steganografi teknikleri.

Tüm steganogarafik tekniklerde gömme işlemi tamamlandıktan sonra önem arz eden konu, alıcının orijinal dosyayı herhangi bir veri kaybı yaşamadan elde etmesidir. Kullanılan her teknik için stego ses dosyasından mesaj elde etme işlemi uygulanan işlem bazında farklılıklar gösterse de temelde uygulanan algoritma aynıdır. Şekil 2.4'te Stego sesten temel anlamda gizli mesajı elde etme işlemi şematik olarak gösterilmiştir.



Şekil 2.4: Stego sesten gizli mesaj elde etme işleminin şematik gösterimi.

3. MATERYAL VE YÖNTEM

Matlab programının bu tezdeki kullanımından ve 5 yöntemden ayrıntılı olarak bahsedilecektir.

3.1 LSB (En Az Önemli Bit) Yöntemi

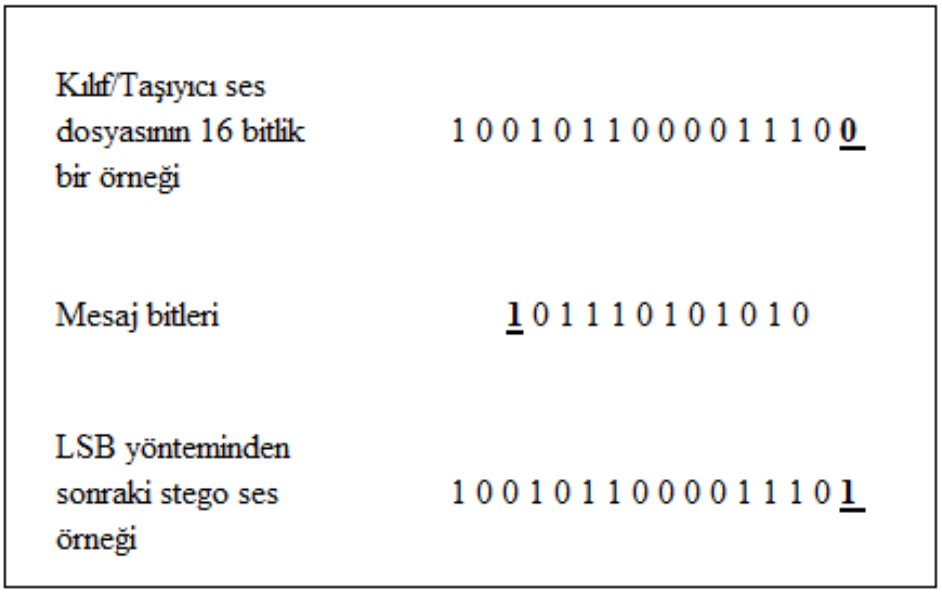
LSB metodu olarak bilinen en az önemli bit yöntemi, ses steganografisinde sıkça kullanılmaktadır. Kılıf/taşıyıcı ses dosyasındaki her bir örneğin son biti ile gizlenecek mesajın bitlerinin sırası ile yer değiştirmesi prensibine dayanır. Değiştirilecek bit sayısı, kılıf/taşıyıcı sesin örneklerinin son iki veya son üç biti olarak ayarlanabilir fakat bu işlem stego sesin kalitesini düşürmektedir. LSB kodlama yönteminde gömme kapasitesini belirleyen unsur örnekleme frekansıdır. Kanal kapasitesi, kilohertz başına 1 kilobittir [1].

Bu çalışmada, ses sinyali örnekleme frekansı 8 kHz'dir. Dolayısı ile saniye başına gömülebilecek bit sayısı 8000, yani 8 kbps'dir. Her bir örnekteki bit sayısı 16 olarak belirlenmiştir. Örneğin, 3 saniyelik bir ses sinyalinde saniyede 8000, toplamda 24000 adet 16 bitlik örnek bulunmaktadır. Bu çalışmada kullanılan ses dosyaları wav türünde, gizlenecek mesaj metin tipindedir. Ses sinyalinin ilk 40 baytı sinyal hakkında bilgi taşımaktadır. Bu yüzden mesaj gömme işlemi ilk 40 bayttan sonra başlatılmıştır. Metin mesajı, ses dosyasındaki ilk 40 bayt hariç, kalan en anlamsız olarak nitelendirilen bütün bitleri kullanacak uzunlukta seçilirse gömme kapasitesi %100 olmuş olur. Yapılan çalışmada LSB yöntemi uygulamak için, kılıf/taşıyıcı ses olarak 10 adet kadın, 10 adet erkek olmak üzere 20 farklı ses sinyali kullanılmıştır. Kullanılan seslerin dosya boyutları birbirlerinden farklıdır. LSB için ses dosyası seçildikten ve gömülecek metin mesajı belirlendikten sonra alıcı tarafından mesajın sağlıklı bir şekilde alınabilmesi için, literatürde stego key olarak adlandırılan stego anahtarının oluşturulması gerekmektedir. Stego anahtarı olarak 1x8'lik bir matris oluşturulmuştur. Aynı ses dosyasına farklı boyutlarda mesaj gömülmesinin sebebi, mesaj boyutu arttıkça sinyalin kalitesinin düştüğünü göstermektir. Stego anahtarı ve metin mesajı belirlendikten sonra kılıf/taşıyıcı ses dosyası dahil eldeki tüm veriler, binary (ikili) forma dönüştürülür. Binary forma dönüştürülen mesaj sinyali tek satırlık bir matris halindedir. Mesaj matrisindeki her bir eleman sırası ile 41. bayttan itibaren ses dosyasının 16 bitlik örneklerinin son bitleri ile yer değiştirir.

Mesaj bitleri ile kılıf/taşıyıcı ses dosyasındaki en anlamsız bitlerin yer değiştimesi sonucu oluşan ses, stego sestir. Stego ses yine wav dosya türündedir ve dosya boyutu orjinal ses dosyasının dosya boyutu ile aynıdır.

Bitlerin yer değiştirmesi prensibine dayandığı için oluşan stego sesin dosya boyutu ile kılıf/taşıyıcı sesin dosya boyutu ile her zaman aynı olacaktır.

Şekil 3.1'de 16 bitlik bir ses örneğinin son biti ile verilen mesaj bitlerinin birinci bitinin değiştirilmesi sonucu elde edilen stego ses örneği verilmiştir. Stego ses örneğinde altı çizili olarak gösterilen bit, mesaj bitlerinin ilk bitidir.



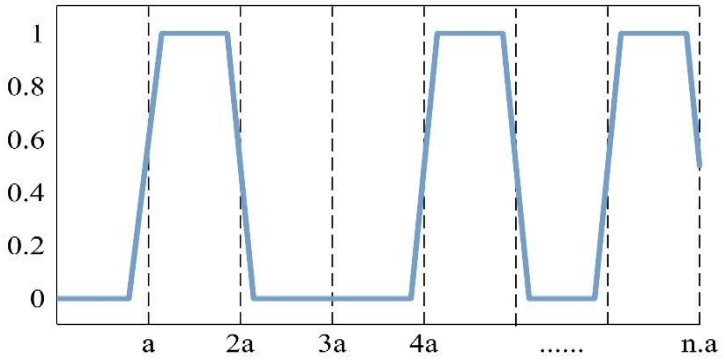
Şekil 3.1 : LSB yöntemi örnek gösterimi.

Stego ses, kılıf/taşıyıcı ses ile aynı dosya konumuna farklı bir wav dosyası olarak kaydedilir. Stego sesten, gömülen mesajı geri elde etmek için MATLAB ortamında ayrı bir kod dizini oluşturulmuştur. Bu kod dizini bir mesaj çözücü olarak düşünülebilir. Elde edilen stego seslerin kalitesini belirlemek için SNR değerleri hesaplanmıştır. SNR kavramından tezin teorik temeller başlığı altında detaylı olarak bahsedilmiştir.

3.2 Yankı Veri Gizleme Yöntemi

Yankı veri gizleme yöntemi, insan kulağının ses dosyasındaki kısa süreli yankıları tespit edemediği gerçeğini kullanan bir yöntemdir [36]. İlk olarak 1996 yılında orijinal ses dosyasına yankı ekleme fikri ortaya atılmıştır [18]. Yankı gizleme tekniğinde, gizlenecek mesaj ayrı bir sinyalde yankı olarak üretilir ve ardından yankı

ses sinyaline gömülür. Yankıyı ses sinyaline eklemek için, ses sinyali önce belirtilen çerçeve boyutuna sahip kısa çerçevelere bölünür. Şekil 3.2'de, orijinal sinyalin eşit parçalara bölünmüş bir örneği verilmiştir. Bu parçalara gömülebilecek maksimum bit sayısı, çerçeve boyutuyla aynıdır. Eşit parçalara bölündükten sonra oluşan yankılar kapak sesine eklenir.

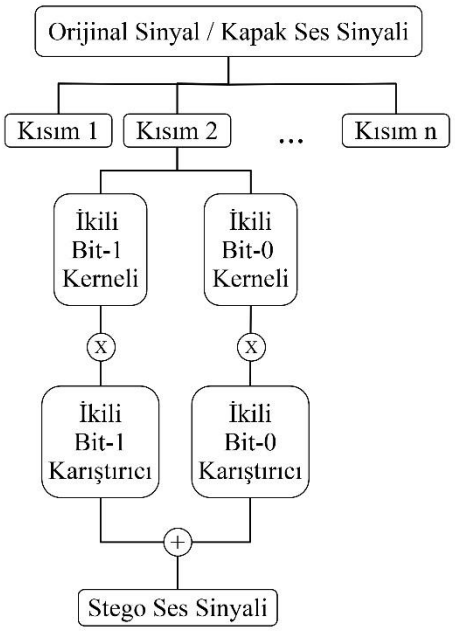


Şekil 3.2 : Eşit zaman aralıklarına bölünen örnek bir sinyal.

Yankı sinyali, orijinal ses sinyalinin ve yankı çekirdeğinin konvolüsyonu ile elde edilir. Gizlenecek bit 1 ise, ikili bir çekirdek gereklidir, oysa gizlenecek bit 0 ise, ikili sıfır çekirdek kullanılır. Yankı çekirdeği matematiksel olarak şu şekilde tanımlanır:

$$h(t) = \delta(t) + \alpha\delta(\mathrm{t} - \Delta\mathrm{t}) \qquad (3.2)$$

D enklem 3.2'de $\delta\,(t)$ birim dürtü fonksiyonu olup, $\Delta\,(t)$ gecikme süresini temsil eder ve α eko genliğidir. Yankılanan kısım 1, ikili bir çekirdeği ve ikili bir karıştırıcı kullanılarak oluşturulur. Aynısı, 0 biti bir yankı olarak eklendiğinde de geçerlidir ve bu durumda, ikili sıfır çekirdek ve ikili sıfır karıştırıcı kullanılarak yankılanan kısım 2 oluşturulur. Yöntemin akış şeması, Şekil 3.3'te gösterilmektedir. Stego sesi, oluşturulan yankılanan bölüm 1 ve yankılanan bölüm 2 birleştirilerek elde edilir.



Şekil 3.3: Yankı çekirdekleri ve karıştırıcılar ile stego sinyal üretimi.

Yankı verilerinin farklı şekillerde gizlenmesine izin veren üç farklı yankı çekirdeği vardır. Bunlara tek yankı, bipolar yankı ve bipolar ileri-geri yankı denir [37]. Bu çalışmada steganografi tek yankı gizleme yöntemi kullanılarak yapılmıştır. Bir ses çerçevesi $x(t)$ verildiğinde, ortaya çıkan yankılı ses sinyali $y(t)$ şu şekilde elde edilir:

$$y(t) = x(t) * \mathrm{h(t)} \tag{3.3}$$

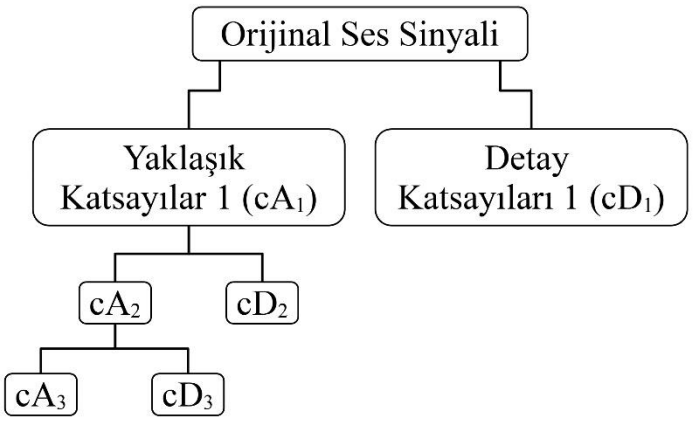
$$y(t) = x(t) + \alpha \mathrm{x(t - \Delta t)} \tag{3.4}$$

Bu yöntem, yaygın spektrum yöntemine paralel olarak yüksek veri aktarım hızına izin verir [34]. Veri aktarım hızının yanı sıra, stego ses kalitesi de önemlidir. Yüksek veri iletim hızında düşük SNR değerine sahip stego seslerinin veri gizlemede anlamsız olacağı açıktır.

Bilgiyi başarıyla depolamak için, genlik, düşüş oranı, orijinal sinyalden sapma (gecikme süresi) gibi üç yankı parametresi değiştirilir. Her üç parametre de insan kulağının algılama eşiğinin altına ayarlanır. Buna göre eşik seviyesinin altında olacak şekilde ayarlanan parametreler sayesinde stego sesini orijinal sesten ayırt etmek zorlaşır.

3.3 Dalgacık Kodlaması Yöntemi

Steganografi, sinyalin örneklerini herhangi bir dönüştürme olmadan doğrudan değiştirerek veya frekans alanındaki dönüştürme katsayılarını uygun alan dönüşümleriyle kullanarak gerçekleştirilebilir. Bununla birlikte, sinyal örneklerindeki doğrudan değişiklikler, bilgilerin gizlenmesini korsanlara karşı daha savunmasız hale getirebilir. Bu endişeleri ortadan kaldırmak için farklı yöntemler önerilmiştir. Dalgacık kodlaması yöntemi bahsedilen güvenlik kaygıları dikkate alınarak geliştirilen yöntemlerden biridir. İlk olarak Matematikçi Alfréd Haar, dalgacık yöntemini 1909 tezinde önermiştir [16]. Daha sonra 1988'de Ingrid Daubechies kompakt destek dik dalgasını oluşturmak için yeni bir dalgacık dönüşümü yöntemi önermiştir [5]. Aslında dalgacık dönüşümü, fonksiyon tanımı açısından Fourier Dönüşümü ile benzerdir. Fourier Dönüşümünden dalgacık dönüşümünü ayıran en önemli nokta, dalgacık dönüşümünün zamana bağlı olarak sinyalin frekans içeriğini oluşturmasıdır [19]. Şekil 3.4'te 3 seviyeli dalgacık dönüşümünün temel yapı diyagramı verilmiştir. Bu şekilde, cA yaklaşık katsayıları temsil ederken, cD detay katsayılarını temsil eder.



Şekil 3.4: 3 seviyeli dalgacık dönüşümünün temel yapı diyagramı.

Dalgacık dönüşümünü uygulamanın iki farklı yolu vardır. Bunlar ayrık dalgacık dönüşümü ve sürekli dalgacık dönüşümüdür [21] Ayrık dalgacık dönüşümünün temel amacı, sinyali ayırmak ve her dalgacığı ayrı ayrı örneklemektir [17].

Bir $f\,(t)$ sinyali için tek boyutlu ayrık dalgacık ayrıştırması denklem 3.5 'te verilmiştir [38].

$$W_f(j,k) = \int_{-\infty}^{\infty} f(t).\psi_{j,k}{}^{*}(t)dt\,, \psi_{j,k}(t) = a_0{}^{-\frac{j}{2}}.\psi(a_0{}^{-j}t - b_0k) \qquad (3.5)$$

$\psi\,(t)$ ana dalgacık, j ise dalgacık ayrışma seviyesidir. a_0 ve b_0 sabittir, k zaman kaydırma faktörü olarak tanımlanır ve ψ^{*}karmaşık eşleniktir. Genel olarak, a_0'ın 2, b_0'ın 1 olduğu denklem 3.6'te verilen form kullanılır.

$$W_f(j,k) = \int_{-\infty}^{\infty} f(t).\psi_{j,k}{}^{*}(t)dt\,, \psi_{j,k}(t) = 2^{-\frac{j}{2}}.\psi(2^{-j}t - k) \qquad (3.6)$$

Ayrıklaştırma tamamlandıktan sonra dönüşüm katsayıları hesaplanır. Mesaj bitlerini değiştirmek için tek boyutlu sinyalin hem yaklaşık hem de detay katsayıları hesaplanmalıdır. Tüm detaylar ve yaklaşık katsayılar hesaplandıktan sonra, toplam sinyal denklem 3.7 ile geri kazanılabilir.

$$f_j(t) = \sum_k W_f(j,k)\,\psi_{j,k}{}^{*}(2^{-j}t - k) \qquad (3.7)$$

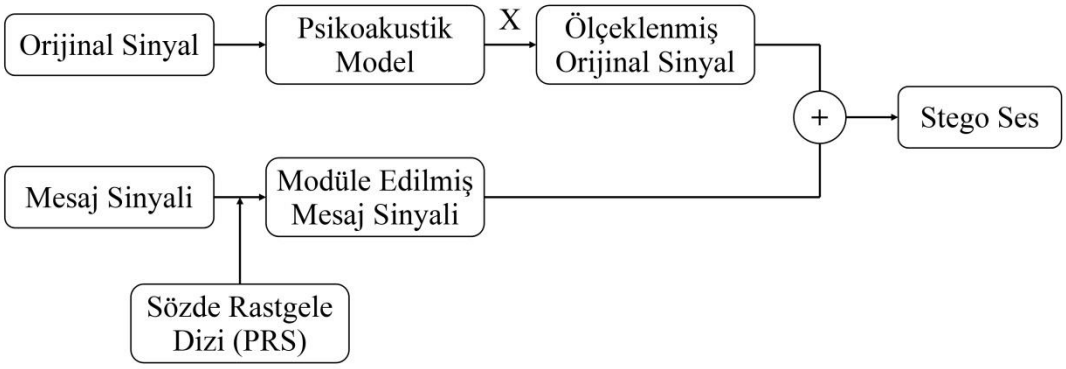
Gömme işlemi 3 seviyeli 1-D dalgacık ayrışması ile başlar. Seviye 3'teki yaklaşık katsayılar gömme için kullanılır. Mesaj bitlerine (1 veya 0) bağlı olarak 3. seviyedeki yaklaşık katsayılar yeniden oluşturulurken detay katsayılarında herhangi bir değişiklik yapılmamaktadır. Detay katsayılarında değişiklik yapılmayarak mesajın düşük fark edilebilir olması hedeflenir. Mesaj bitlerinin gömülü olduğu yeni üçüncü seviye yaklaşık katsayıları detay katsayıları ile birleştirilir. Stego sesi, elde edilen satır matrisine ters ayrık dalgacık dönüşümü kullanılarak elde edilir.

3.4 Tayf Yayılımı Yöntemi

Yayılı spektrum tekniği, steganografide en sık kullanılan tekniklerden biridir. Yaygın spektrumun amacı, gizlenecek bilgiyi mümkün olduğunca kapak ses sinyalinin frekans spektrumuna yaymaktır. Aslında, gizli bilgilerin yerleştirilmesi süreci LSB tekniğine benzer. Yaygın spektrum yönteminin LSB'den farkı, yayılmış spektrumun gizli bilgiyi örtme sinyalinin frekans spektrumuna gömülü hale getirmesidir.

Steganografiden sonra maksimum performans elde etmek için, kapak ses sinyali yerleştirmeden önce analiz edilmelidir. Bu amaçla psikoakustik model kullanılmıştır. Bu model sayesinde mesajların gömülmesi için hangi ses örneklerinin daha uygun olduğu belirlenebilir.

Psikoakustik model, mesajların spektrumda baskın olan sinyal kısımlarına gömülmesine izin verir. Bu şekilde, mesaj bitinin sinyalin önemsiz kısımlarına gömülmesini engeller ve ortaya çıkan stego kalitesinin artmasına izin vermektedir. Bu teknikte orijinal ses analiz edildikten sonra diğer tekniklerden farklı olarak sözde rastgele sıra (PRS) ile mesaj sinyali modüle edilir ve modüle edilmiş gizli mesaj sinyali oluşturulur. Sözde rasgele gürültü dizisi, 0 ve 1 bit dizisidir. Rastgele olarak adlandırılsalar da bir algoritmaya göre üretilirler. Çalışmadaki her çerçeve boyutu için, her çerçevede aynı sayıda bitten oluşan sözde rasgele diziler oluşturulmuştur. Bu modül sırasında mesajın yayılma süreci gerçekleşir. Ölçeklendirilmiş kapak sinyali ve modüle edilmiş mesaj sinyali birleştirilerek stego sesi elde edilir. Şekil 3.5, yayılı spektrum tekniğinin gömülme şemasını göstermektedir. Ölçekleme faktörü x, üretilen gizli mesajın fark edilebilirliğini azaltmak ve mesaj sinyalinin genliğini kontrol etmek için kullanılabilir [36].



Şekil 3.5: Tayf yayılımı tekniğinde gizli mesaj yerleştirme prosedürü.

Yaygın spektrum tekniği uygulandıktan sonra, stego sinyalinin bant genişliği, orijinal sinyalin bant genişliğinden daha büyüktür [18].

3.5 Kepstrum Yöntemi

Bu teknik aynı zamanda gömme işleminin frekans alanı katsayıları üzerine uygulandığı bir gizleme tekniğidir. Kepstrum aslında bir logaritma ile hesaplanan bir Fourier dönüşümü sonucunda ifade edilebilir [8]. Kepstrum için, Fourier dönüşümü önce kapak sinyaline uygulanır. İkinci işlem, sinyalin Fourier katsayılarının logaritması alınarak yapılır.

Logaritma işleminden sonra kepstrum, ters Fourier dönüşümü ile elde edilir. Ters Fourier Dönüşümünün matematiksel ifadesi 2. Bölümde denklem 2.4'te verilmiştir. Ters Fourier dönüşümünü uygulamadan önce, mesaj sinyali kapak sinyalinin kepstrum katsayılarına gömülür [13]. Bu yöntemde, gizliliği artırmak ve fark edilebilirliği azaltmak için mesaj bitleri rastgele kapak sesine yerleştirilir. Kapak sinyalinin önemli bileşenleri gömme için özel olarak seçilmemiştir.

Bu süreçte, kapak sesine yerleştirilmeden önce mesaj sinyali üzerinde istenen herhangi bir değişiklik yapılabilir. Bir x[n] sinyalinin kepstrum dizisi şu şekilde elde edilir [39]:

$$\hat{x}[n] = IDFT\ [\ \ln\{\ DFT\ (x[n])\ \}\ ] \tag{3.8}$$

Kepstrum katsayılarının varyansı daha küçük olduğundan, kepstrum katsayıları olası tehditlere karşı mesajları yerleştirmek için daha uygundur.

4. DENEYSEL SONUÇLAR VE TARTIŞMA

Bu çalışmada ses steganografiye ait tüm teknikler MATLAB programında icra edilmiştir. Kalite değerlendirmesi ilk aşamada SNR metriği ile yapılmıştır.

4.1 LSB Yönteminin Uygulanması

Steganografi işleminin uygulandığı birinci teknik olan en az anlamlı bit yönteminde ilk işlem kullanılacak ses dosyasının örneklenmesi olmuştur. Bir ses dosyası üzerinden örnek verilerek açıklanırsa .wav dosya türündeki ses kaydı 24096 örnek içermektedir. Oluşturulan tüm örneklerin uzunlukları birbirine eşit ve 16-bit olarak seçildiği için her örneğin en son biti ilgili değişikliğin yapıldığı bittir. Örnek ses dosyasının başlangıç örneğinden itibaren ilk 40 biti ses dosyasının temel özelliklerini ve ses ile ilgili bilgileri taşıdığı için başlık olarak nitelendirilmiş ve bu bitler üzerinde herhangi bir değişiklik yapılmamıştır. Değişiklik yapılamaması için bu bitler programa karakter olarak tanıtılmıştır. Ses dosyası ile ilgili işlemlerden sonra mesaj ve mesajın işlenmesi adımına geçilmiştir. Programda mesaj girişi doğrudan metin mesajı olarak yapılmıştır. Örneğin, " mesaj=' Bu komut dizini yardimi ile bir gizli mesaj örnek ses dosyasina gömülmüstür.' " şeklinde Türkçe karakter içermeyen bir mesaj oluşturulmuştur.

Örnekteki mesaj uzunluğu temsilidir. Tek bir karakter bir bayt uzunluğunda olduğundan dolayı mesajın gömülecek haline geldiğindeki uzunluğu denklem 4.1'de gösterildiği gibi,

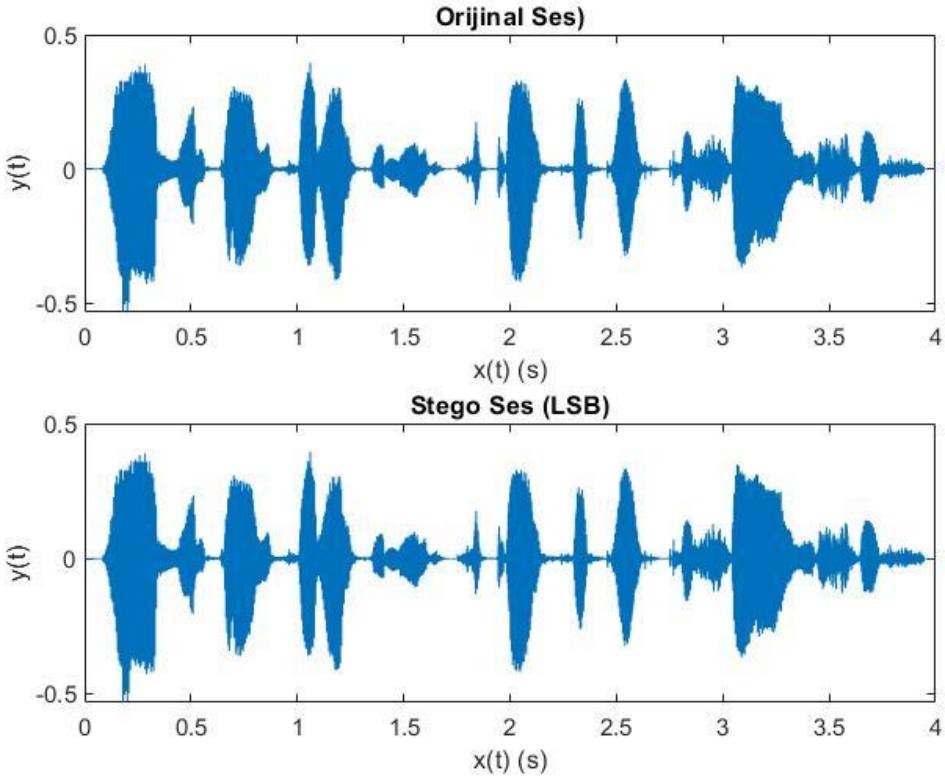
$$bit\ bazında\ mesajdaki\ örnek\ sayısı = \ mesajdaki\ karakter\ sayısı\ x\ 8 \quad (4.1)$$

olacaktır. Verilen örnekteki karakter sayısı 76 olduğundan ses dosyasına gömülecek bit sayısı;

$$bit\ bazında\ mesajdaki\ örnek\ sayısı = \ 76\ x\ 8 = 608$$ 'dir.

Bitlerin yer değiştirme işlemlerinden sonra dosya yeni bir isimle aynı dosya türünde kaydedilmiştir. LSB tekniği ile steganografi yapıldıktan sonra kaydedilen yeni dosya

ve orijinal ses dosyasının genlik karşılaştırmaları yapılmış ve gözle görülür bir değişiklik olmadığı Şekil 4.1' de görülmüştür.



Şekil 4.1: Orijinal ses dosyası ile LSB stego ses dosyasının karşılaştırılması.

Şekil 4.1' de yapılan karşılaştırmada gömme işlemi yapıldıktan sonra gözle görülür bir değişiklik olmadığı görülmektedir. Bu yüzden de SNR kalite değeri en yüksek çıkan teknik LSB tekniğidir. Bu teknikte SNR değerinin azalmasına yol açan faktör mesaj uzunluğudur ve Çizelge 4.1 yardımıyla açıklanmıştır.

Çizelge 4.1 : LSB tekniğine ait tüm mesaj uzunluklarındaki SNR değerleri.

	Mesaj uzunluğu (bit sayısı)													
Dosya	32	64	96	128	160	192	224	256	288	320	352	384	416	448
E1	97.139	95.275	93.285	92.745	92.068	90.855	90.275	90.149	89.937	89.306	88.892	88.347	88.127	87.826
E2	89.28	87.113	86.400	85.619	84.818	84.142	83.103	82.952	82.527	82.140	81.854	81.629	80.997	80.829
E3	93.737	92.545	90.961	90.292	89.241	89.491	88.362	87.631	87.205	86.863	86.190	85.936	85.608	85.486
E4	98.720	96.863	95.638	94.300	93.279	93.117	92.351	92.092	91.396	90.890	90.703	90.726	90.310	89.689
E5	90.441	88.191	87.059	85.670	84.956	84.498	83.545	83.359	82.981	82.737	81.968	81.711	81.195	81.371
E6	95.054	92.866	92.120	90.384	89.425	89.225	88.744	88.005	87.803	87.425	86.960	86.582	86.294	85.840
E7	85.555	83.166	81.938	80.981	80.370	79.834	79.571	78.743	78.178	77.846	77.360	77.042	76.597	76.579
E8	85.879	84.532	82.551	82.256	81.287	80.130	79.826	79.541	79.161	78.760	78.276	77.925	77.485	77.102
E9	85.616	84.067	82.094	81.057	80.403	79.481	78.785	78.982	77.993	77.707	77.121	76.743	76.490	76.126
E10	88.217	85.912	84.727	84.012	83.494	82.160	82.306	81.849	81.285	80.201	80.223	80.043	79.564	79.603
K1	97.268	95.557	93.763	93.084	92.115	91.137	90.719	90.493	90.278	89.613	89.197	88.796	88.448	87.844
K2	90.894	89.133	88.092	86.861	86.261	85.339	84.642	84.392	84.273	83.771	83.204	82.561	82.366	82.144
K3	90.698	88.638	87.846	86.193	85.392	84.795	84.306	83.678	83.021	82.545	81.948	81.825	81.496	81.208
K4	88.232	85.313	84.400	83.226	82.589	82.078	80.796	80.604	79.730	79.730	79.269	79.293	78.938	78.361
K5	86.551	83.963	83.083	81.944	81.322	80.451	80.037	79.435	79.342	78.878	78.612	78.123	77.602	77.267
K6	92.149	90.345	88.642	88.701	87.512	86.365	86.096	85.751	85.431	85.030	85.107	84.134	84.303	83.910
K7	85.337	83.228	82.535	81.815	80.565	80.260	79.316	78.958	78.774	78.320	77.983	77.488	77.356	76.828
K8	92.358	90.420	89.486	88.379	87.867	86.618	86.270	85.678	84.906	84.622	84.208	84.188	84.085	83.966
K9	88.153	85.227	84.821	83.060	82.618	81.928	81.475	80.719	80.181	79.823	79.447	79.122	78.592	78.136
K10	84.921	83.279	82.215	81.258	80.111	79.497	79.300	79.050	78.223	77.770	77.593	77.360	77.043	76.819
Ortalama	90.364	88.282	87.083	86.092	85.285	84.570	83.991	83.603	83.131	82.699	82.306	81.979	81.645	81.347

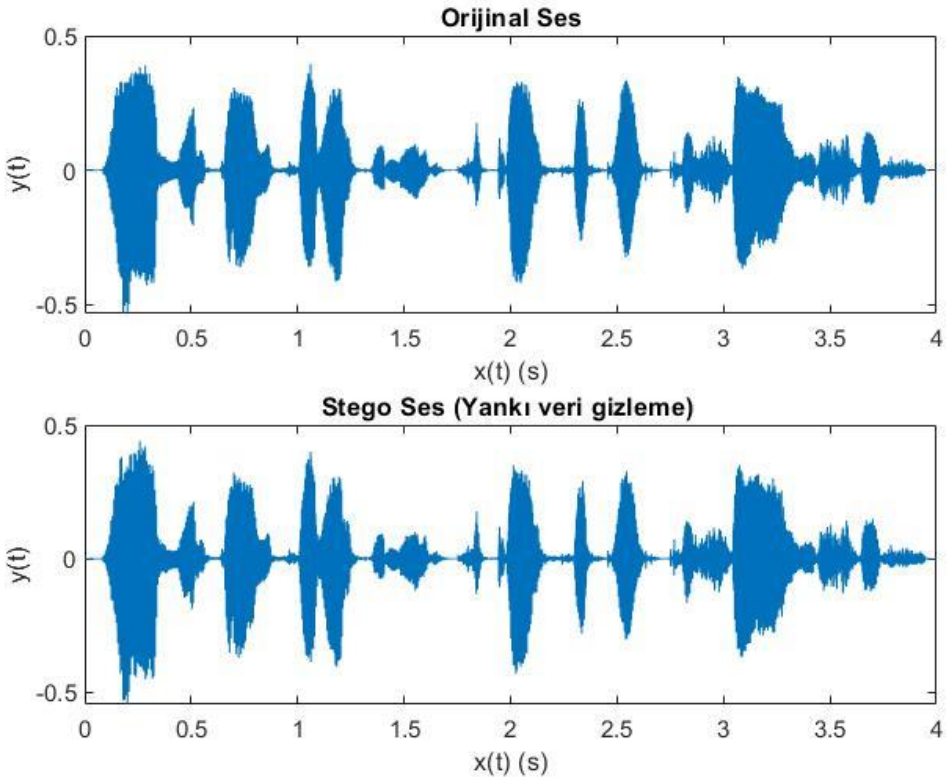
4.2 Yankı Veri Gizleme Yönteminin Uygulanması

Yankı veri gizleme yönteminde de teorik kısmın daha net aktarılabilmesini sağlamak amacıyla en az anlamlı bit yönteminin uygulaması başlığında bahsedilen ses dosyası üzerinden örnekler verilerek açıklanmıştır. Bit mertebesindeki değişim işleminin aksine yankı yöntemi kullanıldığı için uygulama aşamasında ilk olarak ses sinyalinin eşit parçalara bölünmesi gerekmektedir. Bu adımda çerçeve boyutu yine doğru bir kıyaslama için birbiriyle aynı ve 256 örnek olarak belirlenmiştir. Ortalama üç saniyelik örnek ses dosyasında toplamda 24000 bit bulunmaktadır. Çerçeve boyutu 256 ile bölüntülenerek eşit uzunluklu parçalara ulaşılmıştır. Bu teknikte metin mesajı gömme tekniğinden farklı olarak doğrudan rastgele 0'lar ve 1'ler içeren bit dizisi mesajlar üretilmiştir. Böylelikle gömülecek mesaj uzunluğu aynı olsa dahi (örneğin 32 ya da 64 bit) mesaj programda rastgele oluşturulduğu için yöntemin doğruluğunu test etmek daha elverişli olmuştur.

Mesaj üretiminden sonraki adım çerçeve boyutu ve örtüşmeye bağlı olan bir anahtar üretilmesidir. Anahtar olmadan alıcı tarafında mesajın çözülmesi mümkün değildir. Anahtarın mesaj ile bir bağı olmadığı için özgün olarak üretilmiştir. Gömülen mesaj bitlerinin hangi sıra ile 0 veya 1 içerdiği anahtar için önemsizdir. Anahtar uzunluğunu belirleyen faktör çerçeve boyutu ve örtüşme (overlap) miktarıdır. Bu çalışma için örtüşme 1/2'dir.

Yankı veri gizlemesi tekniğinde birinci amaç dinleyicinin yankıyı algılayamamasını sağlamaktır. Bu yüzden gömme kapasitesini aşmamak gerekir ve bu kapasite çalışmada kullanılan diğer steganografik tekniklere göre daha düşüktür. İnsan işitsel sisteminin ayırt edemeyeceği bir eşik belirlenerek buna uygun olarak yankı oluşturulur. Yankı oluşturabilmek için kapak ses sinyali ile yankı çekirdeğinin konvolüsyonun gerçekleştirilmesi gerekir. Yankı çekirdeği olarak pozitif tek yankı çekirdeği kullanılmış ve pozitif tek yankı veri gizleme işlemi yapılmıştır. Bölüm 3 içerisinde verilen denklem 3.2 kullanılarak işleme başlanır. Denklemdeki yankı genliği değeri (α) 0.2 olarak belirlenmiştir. Yankı sinyallerinin elde edilmesi ile birlikte bu yankıları ses dosyasına ekleyebilmek için karıştırıcılar (mikser) oluşturulur. 0 ve 1 biti için iki ayrı karıştırıcı oluşturulması gerekir. Bu karıştırıcılar da birer sinyaldir ve yankı sinyalleri ile çarpılarak kapak sesine eklenebilir hale gelir.

Yankı veri gizleme tekniği kullanılarak gerçekleştirilen ses steganografideki original ses ve stego ses dosyasının zamandaki görüntüsü Şekil 4.2'de verilmiştir.



Şekil 4.2: Orijinal ses dosyası ile Yankı Veri Gizleme stego ses dosyasının karşılaştırılması.

Şekil 4.2'de verilen karşılaştırmada da LSB tekniği ile eşit sayıda bit içeren bir mesaj gömüşmüştür. Genlik karşılaştırmaları detaylı olarak incelendiğinde örnekler arası farklar açıkça görülebilirken, ses dosyası normal olarak dinlenildiği zaman iki ses arasındaki fark ayırt edilebilir değildir. Sonraki sayfada verilen Çizelge 4.2'de 32 bit ile 448 bit arasında 32'şer bi artarak devam eden 14 mesaj uzunluğunda elde edilen SNR (dB) değerleri verilmiştir. LSB tekniği ile kıyaslandığında düşük SNR değerine sahip olarak gözükse de kalite seviyesi İnsan işitsel sisteminin algı seviyesine göre yüksektir.

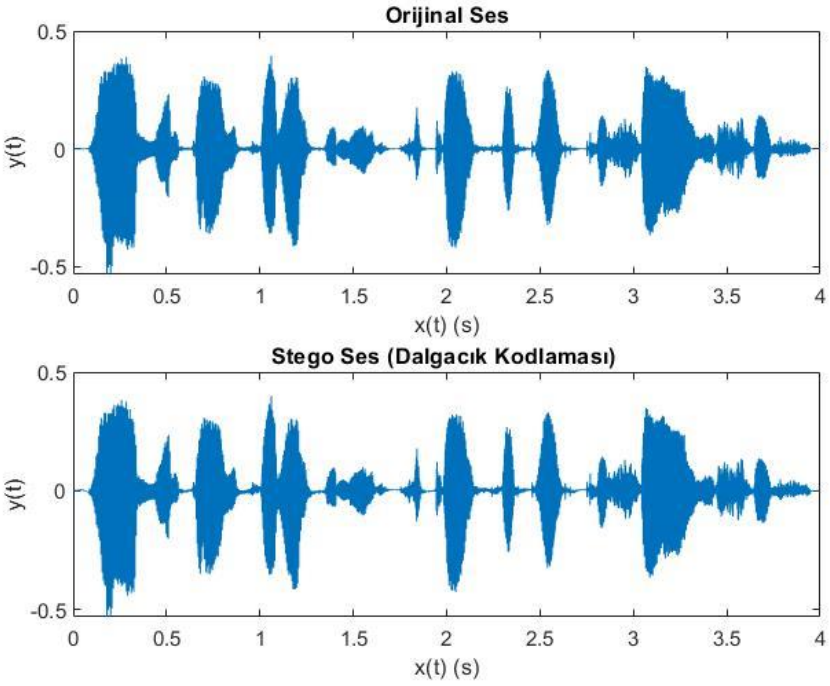
Çizelge 4.2 : Yankı Veri Gizleme tekniğine ait tüm mesaj uzunluklarındaki SNR değerleri.

	Mesaj uzunluğu (bit sayısı)													
Dosya	32	64	96	128	160	192	224	256	288	320	352	384	416	448
E1	27.967	22.203	19.955	19.362	17.719	16.905	16.673	16.689	16.630	16.584	16.631	16.707	16.609	16.657
E2	20.996	18.927	18.502	17.274	16.669	16.619	16.570	16.606	16.614	16.551	16.599	16.712	16.586	16.664
E3	20.583	17.233	16.705	16.687	16.533	16.556	16.586	16.615	16.552	16.524	16.600	16.564	16.483	16.576
E4	24.207	21.744	20.651	20.108	19.081	18.733	17.848	17.087	16.566	16.653	16.594	16.559	16.662	16.619
E5	19.366	18.237	17.354	16.675	16.636	16.647	16.574	16.606	16.632	16.639	16.668	16.591	16.678	16.722
E6	22.846	19.604	18.676	18.060	17.392	16.590	16.583	16.568	16.642	16.669	16.614	16.590	16.606	16.601
E7	21.472	18.766	18.418	17.217	16.940	16.650	16.606	16.616	16.612	16.660	16.668	16.617	16.713	16.608
E8	22.271	18.253	16.927	16.679	16.607	16.599	16.530	16.530	16.601	16.495	16.574	16.514	16.589	16.618
E9	20.387	18.800	17.693	16.917	16.635	16.521	16.621	16.697	16.600	16.575	16.610	16.742	16.578	16.577
E10	22.828	19.803	19.160	17.993	17.435	16.528	16.466	16.551	16.586	16.521	16.556	16.477	16.526	16.489
K1	22.392	19.485	19.128	17.838	16.740	16.651	16.587	16.627	16.612	16.593	16.597	16.558	16.612	16.640
K2	19.229	17.356	16.983	16.743	16.598	16.635	16.625	16.543	16.543	16.500	16.516	16.529	16.472	16.449
K3	19.377	18.316	17.221	16.939	16.567	16.665	16.628	16.529	16.537	16.462	16.591	16.603	16.495	16.564
K4	20.518	19.465	19.004	17.619	17.131	16.654	16.447	16.615	16.617	16.648	16.516	16.650	16.752	16.619
K5	21.465	19.184	18.822	17.563	17.251	16.489	16.591	16.592	16.503	16.447	16.589	16.535	16.512	16.460
K6	23.136	18.936	18.484	17.167	16.762	16.675	16.580	16.593	16.668	16.594	16.605	16.634	16.627	16.650
K7	21.346	19.769	18.641	17.717	17.136	16.586	16.605	16.554	16.590	16.482	16.538	16.541	16.517	16.611
K8	19.099	18.374	18.099	17.594	17.355	16.948	16.630	16.593	16.469	16.527	16.559	16.540	16.587	16.686
K9	22.037	18.573	17.591	17.115	16.561	16.557	16.502	16.608	16.570	16.541	16.544	16.452	16.469	16.600
K10	21.915	20.135	19.589	18.127	16.598	16.502	16.594	16.605	16.540	16.627	16.509	16.639	16.581	16.575
Ortalama	21.672	19.158	18.380	17.570	17.017	16.736	16.642	16.621	16.584	16.565	16.584	16.588	16.583	16.599

4.3 Dalgacık Kodlaması Tekniğinin Uygulanması

Dalgacık kodlaması tekniğinin uygulama safhasının ilk aşaması sinyali veri gizleme tekniğinde olduğu gibi belirlenmiş bir çerçeve boyutu ile eşit parçalara bölmektir. Çerçeve boyutu tüm tekniklerde (LSB) hariç olduğu gibi 512 bit olarak belirlenmiştir. 24096 örnek içeren ses dosyası orijinal ses dosyası olarak seçilmiştir. Bunun amacı yöntemler arasında yapılan kıyaslamanın kalitesini artırmaktır. Yine tüm yöntemlerde kapak ses dosyasına gömülen mesajlar eşit uzunlukta olduğu için programda dalgacık kodlaması tekniği iiçin de 32 bit ile 448 bit arasında farklı mesajlar üretilmiştir.

Kapak ses sinyaline 256 bit uzunluğunda bir mesaj 24096 örnek içeren mesaj sinyalininn gömülmesi ile elde edilen karşılaştırma Şekil 4.3'te verilmiştir. 256 bit mesaj uzunluğu tüm yöntemlerde karşılaştırma görseli kullanıldığı için aynıdır.



Şekil 4.3: Orijinal ses dosyası ile Dalgacık Kodlaması stego ses dosyasının karşılaştırılması.

Steganografi işlemi, kapak ses dosyasının ayrık dalgacık dönüşümü gerçekleştirildikten sonra sinyalin yaklaşık katsayıları ile yapılsa da alıcı tarafında geri çıkarma algoritmasında ters dalgacık dönüşümü yapılacağı için tüm katsayılarının elde edilmesi gerekir. Sinyalin yaklaşık ve detay katsayıları

kullanılarak alıcı tarafında stego anahtar ile geri çıkarma işlemi yapılacaktır. Stego ses sinyalinden mesaj sinyalinin çıkarılabilmesi için Buna uygun olarak da hem alıcı tarafındaki kullanıcını hem de verici tarafındaki kullanıcının bildiği binary sistemde bir stego anahtar oluşturulmalıdır. Bu çalışmada kullanılan steganografik teknikler arasında Dalgacık Kodlaması tekniği kalite anlamında 3. sıradadır. Tüm mesaj uzunluklarında elde edilen SNR (dB) değerleri Çizelge 4.3'te verilmiştir. Çizelgeye bakıldığında LSB yönteminin aksine 32 bit gömüldüğündeki SNR değeri ile 448 bit gömüldüğündeki SNR değerleri arasındaki fark Dalgacık Kodlaması tekniğinde daha azdır. Yani gömülen mesaj uzunluğunun artması ile sinyalde meydana gelen bozulmanın bu teknikte daha az olduğu görülmektedir.

Çizelge 4.3 : Dalgacık Kodlaması tekniğine ait tüm mesaj uzunluklarındaki SNR değerleri.

	Mesaj uzunluğu (bit sayısı)													
Dosya	32	64	96	128	160	192	224	256	288	320	352	384	416	448
E1	31.815	24.233	22.808	22.314	20.723	20.180	19.965	19.783	19.512	19.983	20.110	20.219	20.027	19.556
E2	24.444	22.574	21.343	19.599	18.909	18.721	18.658	18.581	18.705	18.165	19.142	19.527	18.422	18.981
E3	24.162	20.462	19.470	19.658	19.618	19.561	19.571	20.100	19.345	19.520	19.940	19.529	19.475	19.483
E4	29.011	25.549	23.892	23.954	23.051	22.042	21.090	20.415	20.030	19.923	20.461	19.588	20.123	20.153
E5	23.278	21.113	20.365	19.114	19.078	18.811	18.369	18.517	19.172	18.631	18.463	19.949	18.973	18.718
E6	27.487	22.462	21.829	20.278	18.476	18.983	19.123	19.588	19.446	19.557	19.045	19.621	19.019	19.353
E7	22.543	20.219	17.234	16.473	15.713	15.486	14.783	15.146	15.432	14.810	14.587	15.017	14.990	14.958
E8	22.106	19.620	17.632	16.910	16.470	16.375	16.483	16.662	16.692	16.865	17.156	16.697	16.425	16.798
E9	22.466	19.729	18.129	17.584	16.107	15.903	16.248	15.991	16.061	15.842	16.152	16.326	15.808	16.088
E10	24.482	21.563	19.768	18.852	18.529	16.911	16.068	16.221	16.911	17.373	17.035	16.475	16.820	16.747
K1	28.633	23.749	22.576	21.969	20.500	20.753	20.320	20.093	20.110	20.211	20.228	20.002	20.719	19.984
K2	27.152	23.558	21.678	21.103	19.978	19.989	19.924	19.849	20.477	19.622	20.563	19.605	20.200	20.166
K3	26.724	22.352	21.251	20.277	19.789	19.714	19.435	19.505	19.411	19.392	20.014	19.574	19.469	19.479
K4	25.331	22.295	20.728	19.272	18.425	17.079	16.931	17.191	16.893	16.931	16.846	16.983	16.968	17.028
K5	23.136	20.077	18.246	19.272	16.506	15.962	15.959	15.824	15.523	15.120	15.435	15.401	15.229	15.456
K6	25.473	21.572	20.977	17.544	19.907	19.609	19.827	19.470	19.450	19.951	19.339	19.411	19.393	19.268
K7	23.544	20.336	18.551	17.278	16.062	15.002	14.635	15.068	14.584	15.047	14.768	14.643	14.840	14.739
K8	25.436	24.548	23.261	22.450	21.102	20.922	19.883	20.166	20.344	19.741	20.143	19.779	19.939	19.517
K9	22.082	19.157	18.980	17.514	17.006	16.335	16.574	16.882	16.365	16.408	16.502	16.532	17.518	16.000
K10	22.794	20.830	17.985	17.156	16.586	15.588	15.358	15.443	15.167	15.388	15.181	15.084	15.674	15.565
Ortalama	25.105	21.800	20.459	19.429	18.627	18.196	17.960	18.025	17.982	17.924	18.056	17.998	18.002	17.902

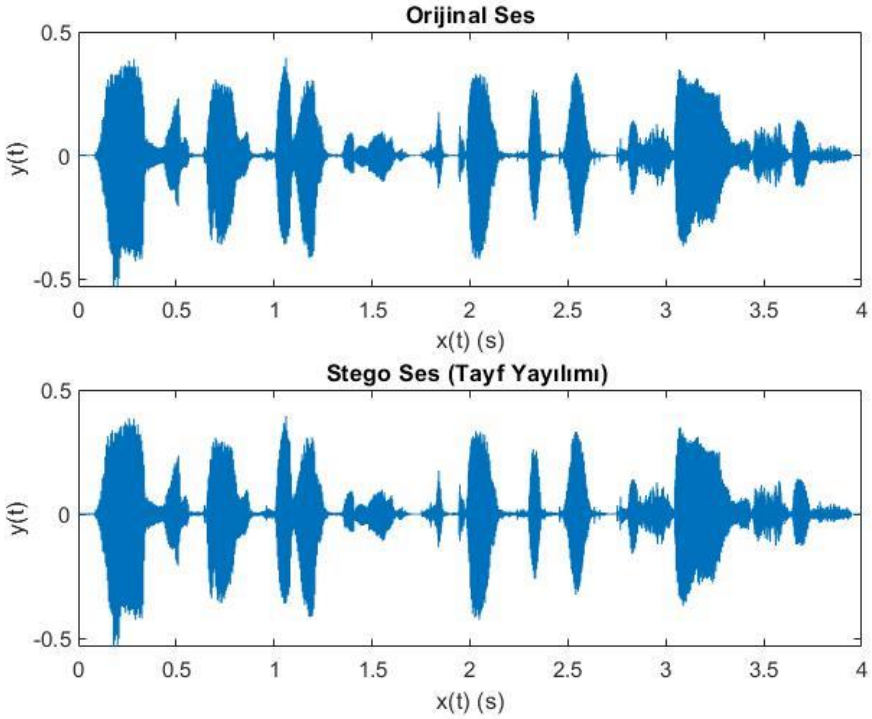
4.4 Tayf Yayılımı Tekniğinin Uygulanması

Tayf yayılımı tekniğinde gizlenecek mesaj diğer yöntemlerin aksine kapak sesi dosyasına bir gürültü olarak eklenir. Ancak bu gürültü spektruma yayıldığı için fark edilebilirliği oldukça düşüktür. LSB yöntemi hariç tüm tekniklerde olduğu gibi Tayf Yayılımı tekniğinde de birinci adım sinyalin çerçeve boyutu ile eşit parçalara bölünmesidir.

Bu teknikte güvenliğin artırılması için seçilen yöntem mesaj sinyalinin modüle edilmesi olduğu için programa bir PRS ürettirilir. Üretilen PRS'nin boyutu çerçeve boyutu ile aynıdır. Gömülecek bit sayısını belirlediği için sınırlayıcı bir faktör olarak sayılabilir. 512 bit uzunluğundaki PRS ile mesaj bitleri modüle edilir. Sağlamlığın artırılması için değişimleri kontrol eden bir sabit belirlenir. Bu çalışma için sağlamlık kontrol sabiti değeri 0.03 olarak seçilmiştir. Gömülecek bitin 1 veya sıfır olmasına göre sağlamlık kontrol sabitinin polaritesi değişmektedir. Bu işlem mesaj sinyalinin modülasyonu açısından önemlidir.

Mesaj bitleri bu işlemlerden sonra çerçeveler artık güncellenmiş ve ses dosyası stego parçaları içeren hale gelmiştir. Yeni çerçeveler birleştirilerek stego sesin tamamı elde edilebilir. Geri çıkarma algoritması diğer teknikler ile benzerdir. Yani Tayf Yayılımı tekniği için de alıcı tarafındaki kullanıcının mesajı stego ses dosyasından ayırabilmesi için stego anahtar ile veri gömme algoritmasını bilmesi gerekmektedir.

Şekil 4.4'te Orijinal ses dosyası ile tayf yayılımı tekniği ile elde edilen stego ses dosyasının karşılaştırması verilmiştir. Kıyaslaması yapılan teknikler arasında Tayf Yayılımı tekniği 2. sıradadır. Spektruma yayılan module edilmiş mesaj bitleri kaliteyi artıran bir yaklaşım göstermektedir.



Şekil 4.4: Orijinal ses dosyası ile Tayf Yayılımı stego ses dosyasının karşılaştırılması.

Şekil 4.4 dikkatlice incelenciğinde stego ses sinyalinin orijinal ses sinyaline oldukça yakın olduğu görülmektedir. Yine benzer yaklaşım Çizelge 4.4'te tüm mesaj uzunluklarında elde edilmiş SNR değerleri ile de desteklenmektedir. 32 bit ile 448 bit arasında mesaj uzunluklarını artması ile SNR değerinde meydana gelen azalma miktarı oldukça düşüktür. Kapak ses sinyaline 32 bit gömüldüğünde ortalama 37 dB SNR değeri elde edilirken mesaj uzunluğu 32 katına çıkarıldığında bu değer 32 dB civarında hesaplanmıştır.

Çizelge 4.4 : Tayf Yayılımı tekniğine ait tüm mesaj uzunluklarındaki SNR değerleri.

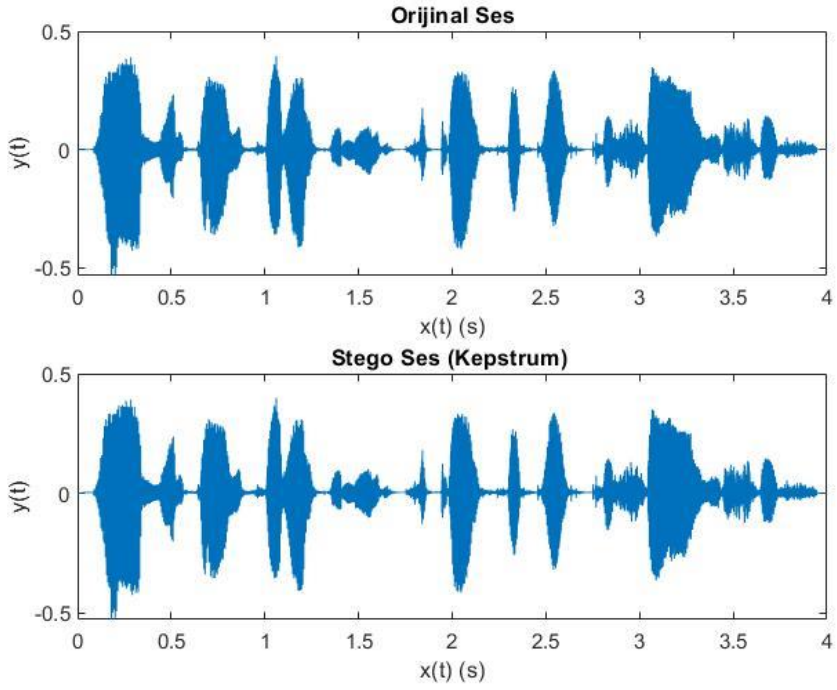
	Mesaj uzunluğu (bit sayısı)													
Dosya	32	64	96	128	160	192	224	256	288	320	352	384	416	448
E1	44.085	38.337	36.961	35.878	33.526	32.642	32.702	32.803	32.334	33.396	32.422	32.968	32.528	32.402
E2	35.880	33.751	33.278	32.190	32.021	32.102	32.454	31.658	30.900	31.643	31.799	31.873	32.181	32.008
E3	36.569	34.234	33.488	32.754	33.319	33.290	33.684	33.185	33.435	33.342	33.013	32.988	33.429	33.355
E4	41.567	39.383	37.718	36.720	35.789	35.305	35.260	35.083	33.876	33.962	33.565	33.061	33.453	33.317
E5	33.815	32.063	31.952	31.599	30.811	31.414	30.583	31.578	30.641	30.925	33.588	31.295	31.331	31.120
E6	38.945	35.712	34.748	33.554	33.272	32.714	32.946	33.045	32.994	33.162	32.597	32.159	33.576	32.216
E7	37.168	34.826	34.975	34.301	33.421	33.607	33.439	33.195	34.002	33.227	33.549	33.458	33.410	33.763
E8	38.284	33.297	32.136	31.045	31.383	31.364	31.000	31.376	31.258	30.669	31.308	30.910	31.769	31.098
E9	36.768	34.967	33.887	32.133	32.316	32.400	32.422	32.466	32.319	31.749	32.058	31.860	32.374	31.098
E10	38.403	34.774	33.676	33.602	32.418	31.381	31.984	31.638	32.172	31.332	31.681	32.440	31.272	31.098
K1	37.570	35.395	33.972	33.672	32.742	32.633	32.821	32.411	32.815	32.614	32.801	32.372	32.477	32.521
K2	35.131	32.776	32.272	32.694	31.691	32.005	32.898	32.309	31.760	31.451	31.123	31.681	31.798	32.105
K3	33.124	32.760	31.177	30.885	30.616	32.063	30.841	30.955	31.274	31.377	30.715	30.328	30.797	31.023
K4	36.659	35.044	35.572	33.658	33.407	32.252	32.275	31.848	32.301	32.200	32.468	32.086	32.497	31.733
K5	37.488	35.872	34.729	33.129	32.506	32.139	31.985	32.016	32.101	32.579	32.261	31.937	32.629	32.164
K6	37.369	34.405	34.069	31.999	30.879	31.200	31.166	31.474	32.102	32.840	31.147	31.634	31.962	31.467
K7	35.829	34.233	33.188	33.215	31.410	31.154	32.285	31.783	31.570	31.326	31.486	31.782	31.860	31.103
K8	35.937	35.010	34.563	33.352	33.303	32.504	33.367	32.989	32.980	32.851	32.644	32.830	32.784	33.358
K9	38.472	35.306	33.796	33.092	33.389	32.609	32.511	32.583	33.201	32.510	33.005	32.463	32.834	32.894
K10	37.343	34.704	34.534	33.842	32.296	33.093	32.529	32.765	32.944	31.978	32.339	32.525	32.220	32.996
Ortalama	37.320	34.842	34.035	33.166	32.526	32.394	32.458	32.358	32.349	32.257	32.275	32.133	32.359	32.142

4.5 Kepstrum Tekniğinin Uygulanması

Kepstrum tekniği de güvenlik kaygılarıyla ortaya çıkan bir teknik olduğu için işlem adımları karmaşıktır. Bu karmaşıklık matematiksel işlemlerin arka arkaya yapılmasından kaynaklanmaktadır. Uygulamanın ilk aşamsaında kapak ses sinyali birbiri ile eşit parçalara bölünmüştür. Çerçeve boyutu 512 bit olarak belirlenmiştir. Kapak ses dosyası 24096 örnek içermektedir. Mesaj uzunluğu 256 bit seçilerek Kepstrum tekniğinin diğer tekniklerde elde edilen karşılaştırma görselleri ile aynı mesaj uzunluğuna sahip olması hedeflenmiştir.

Mesaj bitleri kepstrum katsayılarına gömüldükten sonra Ters Fourier Dönüşümü (IDFT) uygulandığı için mesajın görünürlüğü ve fark edilebilirliği oldukça düşüktür. Mesaj bitlerinin 0 ya da 1 olması durumuna göre katsayılarda yapılan işlemlerde iki sabit değeri belirlenmiştir. Eğer mesaj biti 1 ise katsayılara 0.0015 eklenirken, mesaj biti 0 olduğunda katsayılardan 0.0015 değeri çıkarılmıştır. Elde edilen yeni değerler stego sinyale ait katsayılardır.

Şekil 4.5'te verilen şekilde Kepstrum tekniği ile elde edilen stego ses ile orijinal ses sinyalinin bir karşılaştırması verilmiştir.



Şekil 4.5: Orijinal ses dosyası ile Kepstrum stego ses dosyasının karşılaştırılması.

Bu çalışmada kepstrum tekniği diğer steganografik tekniklere göre 32 bit uzunluğunda mesaj gömüldüğünde ortalama 24 dB SNR değeri ile dördüncü sıraya yerleşmiştir. İnsan işitsel sisteminin ses sinyalindeki bozulmayı ayırt edebilme seviyesinin üstünde olduğu için mesaj gömmek için kaliteli bir yöntem olarak değerlendirilebilir.

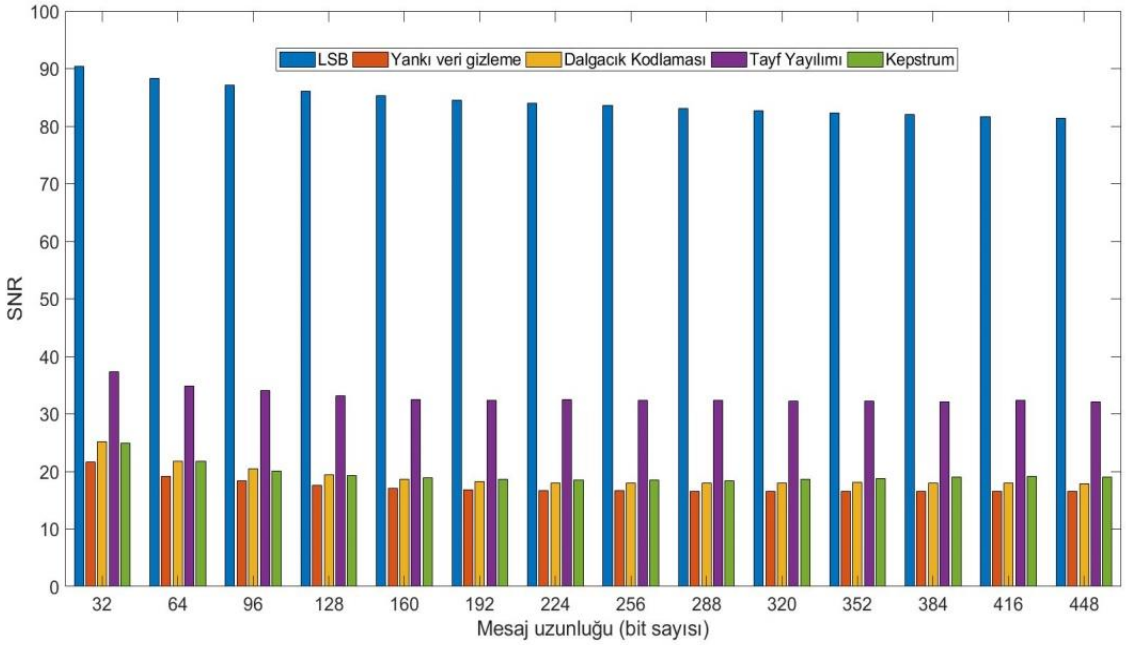
Çizelge 4.5'te Kepstrum tekniğine ait tüm mesaj uzunluklarında elde edilen SNR değerleri verilmiştir. Çizelgede ortalama SNR değerleri baz alınarak yorum yapılırsa 32 bit mesaj gömüldüğünde yaklaşık 25 dB (24.9 dB) SNR değeri elde edilmiştir. Bu değer Dalgacık Kodlaması tekniğinde yine aynı mesaj uzunluğundaki ortalama SNR değerine yakındır. Ancak dalgacık kodlaması tekniğinde mesaj uzunluğu artarak 448 bit uzunluğuna ulaştığında ortalama SNR değeri 16 dB olarak hesaplanırken Kepstrum tekniğinde maksimum mesaj uzunluğunda elde edilen SNR değerinin yaklaşık 19 dB olarak hesaplandığı görülmektedir. Bu da Kepstrum tekniğinin başlangıç mesaj uzunluğunda daha düşük SNR değerine sahip olsa da mesaj uzunluğu artışından daha az etkilendiğini göstermektedir.

Çizelge 4.5 : Kepstrum tekniğine ait tüm mesaj uzunluklarındaki SNR değerleri.

	Mesaj uzunluğu (bit sayısı)													
Dosya	32	64	96	128	160	192	224	256	288	320	352	384	416	448
E1	32.197	24.982	22.192	21.908	20.747	20.820	20.193	19.495	19.503	20.656	21.160	21.402	21.384	21.944
E2	25.725	22.522	20.945	19.874	18.617	18.635	18.781	18.316	19.104	18.638	18.971	19.669	19.802	19.284
E3	24.716	21.204	19.814	19.650	19.468	19.877	19.532	19.775	19.201	20.580	22.039	21.340	21.505	22.131
E4	29.498	25.765	24.016	24.023	23.168	22.323	21.282	20.400	19.906	21.140	20.960	22.036	21.698	21.762
E5	22.474	21.687	20.635	19.280	18.773	18.881	18.163	19.355	18.714	18.856	19.678	20.309	20.603	20.055
E6	26.724	22.272	21.762	21.160	20.967	19.541	19.218	19.480	19.395	20.925	20.501	20.421	20.736	20.547
E7	21.301	18.479	17.053	16.710	15.973	15.109	14.839	15.420	14.657	15.171	14.866	15.768	15.881	15.633
E8	24.170	20.443	18.490	17.875	16.743	17.076	16.575	17.108	16.585	16.924	17.112	17.304	17.975	17.570
E9	24.356	19.708	17.581	16.939	16.205	16.039	15.608	15.870	16.078	16.472	15.547	16.786	16.310	16.336
E10	24.729	22.092	19.408	18.938	18.239	17.838	16.787	16.894	16.572	16.742	17.198	17.429	17.838	17.978
K1	27.065	25.414	23.649	22.734	23.255	23.310	23.088	22.743	23.065	23.098	22.664	22.871	22.753	22.735
K2	26.074	23.379	22.023	20.724	20.067	20.898	20.614	21.430	20.837	20.652	21.166	20.578	20.474	20.086
K3	26.402	23.637	21.579	19.955	20.473	19.646	20.691	20.570	20.284	19.981	20.160	20.065	20.885	20.695
K4	24.203	20.759	18.817	17.748	17.972	17.604	17.219	17.120	17.037	17.232	17.226	17.274	17.122	17.399
K5	21.283	18.817	16.985	16.501	16.019	16.064	16.131	16.019	15.867	15.720	16.600	15.783	16.536	15.542
K6	27.173	24.675	22.026	20.667	20.425	21.147	21.007	21.180	20.808	20.854	20.499	20.674	22.407	21.218
K7	22.009	18.693	17.099	16.199	15.468	15.552	15.445	15.476	14.755	14.743	15.109	15.503	15.234	14.996
K8	26.499	23.405	22.999	21.451	20.993	20.750	20.516	20.061	21.097	20.894	21.052	20.867	21.246	21.103
K9	20.800	20.048	17.924	17.204	17.412	16.794	17.313	17.111	17.300	16.826	17.387	17.007	17.671	17.549
K10	21.205	18.304	17.274	15.581	16.201	15.537	16.363	15.726	15.896	16.448	16.287	16.182	15.790	16.318
Ortalama	24.930	21.814	20.114	19.256	18.859	18.672	18.468	18.477	18.333	18.628	18.809	18.963	19.193	19.044

5. SONUÇ VE ÖNERİLER

Değişik mesaj uzunluklarına sahip farklı steganografi teknikleri kullanılarak elde edilen ortalama SNR değerleri Şekil 5.1'de özetlenmiştir. Şekilden mesaj uzunluğu arttıkça, beklendiği gibi genel olarak daha düşük SNR değerlerinin elde edildiği görülmektedir. Bunun nedeni, mesaj uzunluğunun artırılmasının sonunda daha yüksek sayıda sinyal örneğini değiştirmesi ve dolayısıyla SNR değerinin azalmasıdır. Sinyal örneğinin değiştirilmesi her yöntem için farklı şekillerde olmuştur. SNR değerinin seviyesini mesajı gömme sırasında alınan güvenlik önlemi olarak yapılan işlem sayısının artırılması sağlamıştır.



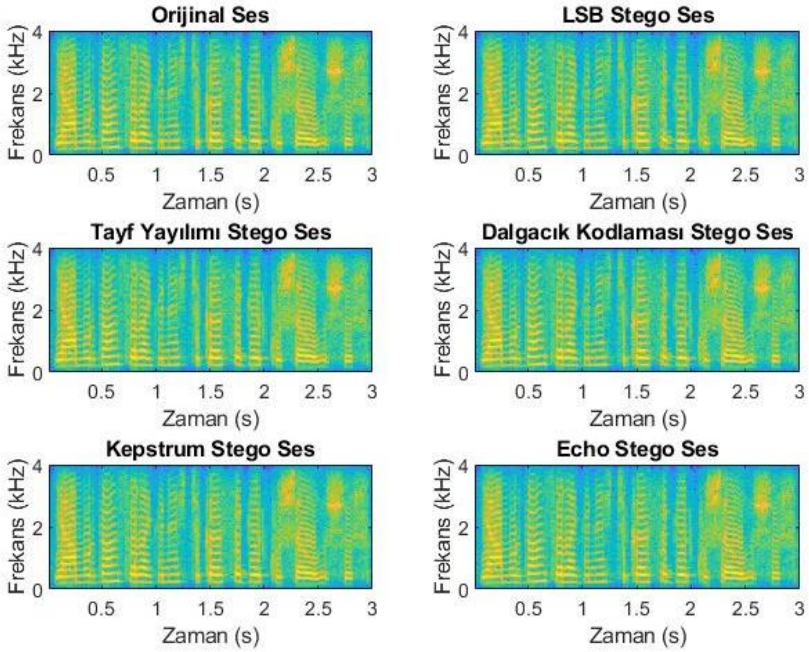
Şekil 5.1: 32–448-bit arası mesaj uzunluklarında SNR değerleri için yöntemlerin karşılaştırılması.

Beş farklı steganografi tekniği arasında LSB yöntemi en yüksek SNR değerlerini verir. Bunun nedeni muhtemelen LSB yöntemi her sinyal örneğinin yalnızca son bitini değiştirdiği için, orijinal sinyalde daha az distorsiyona neden olmasıdır. Şekilde, steganografik tekniklerin isimleri literatürde geçtikleri şekli ile verilmiştir. Buna göre LSB tekniği aynı kalırken, Yankı Veri Gizleme tekniği Echo olarak,

Dalgacık Kodlaması tekniği Wavelet olarak, Tayf Yayılımı tekniği Spread Spectrum olarak ve Kepstrum tekniği Cepstrum olarak ifade edilmiştir.

SNR değerlerine bakılarak yorum yapıldığında en yüksek SNR değerini veren LSB tekniği en mantıklı ses steganografi tekniği olarak gözükse de bu değerlendirmeyi yapmak için geçerli tek parametre kalite değeri değildir. Steganografi ile bir gizleme işlemi yapıldığı göz önünde bulundurulursa gizlilik ve sağlamlık çok önemlidir. Bu bağlamda değerlendirme yapıldığında kapak ses dosyasının frekansları ile ilgilenen teknikler ön plana çıkmaktadır.

Çalışmada kullanılan steganografik tekniklerin daha detaylı yorumlanabilmesi için zaman-frekans eksenlerinin aynı anda görüntülenebildiği spektrogramlar elde edilmiştir. Steganografik tekniklerin spektrogramları Şekil 5.2'de verilmiştir. Kapak sesi dosyaları 8 kHz ile örneklenmiştir ancak spektrogramdaki görüntünün daha net aktarılabilmesi için spektrogramlar 4 kHz' e kadar çizdirilerek elde edilmiştir.



Şekil 5.2: 5 Steganografik tekniğe ait Spektrogram görüntüleri.

Elde edilen veriler ve araştırmalar SNR değerini etkileyen 2 ana faktör olduğunu göstermektedir. Bunlar sırasıyla; kullanılan steganografik teknik ve gizlenecek mesaj uzunluğudur. Ancak bu faktörler ayrı ayrı değil, bir bütün olarak ele alınmalıdır.

Gelecek çalışmalarda yöntemleri test etmek için steganaliz yapılarak detaylı değerlendirmeler yapılabilir.

KAYNAKLAR

[1] **Dutta, P., Bhattacharyya, D., Kim, T.** (2009). Data Hiding in Audio Signal: A Review, International Journal of Database Theory and Application, 2(2):1-8.

[2] **Cox, I. J., Kalker, T., Pakura, G., & Scheel, M.** (2005, September). Information transmission and steganography. In *International Workshop on Digital Watermarking* (pp. 15-29). Springer, Berlin, Heidelberg.

[3] **Bandyopadhyay, S. K., Bhattacharyya, D., Ganguly, D., Mukherjee, S., & Das, P.** (2008, August). A tutorial review on steganography. In *International conference on contemporary computing* (Vol. 101, pp. 105-114).

[4] **Kumar, S., Barnali, B. A. N. D. Y. O. P. A. D. H. Y. A. Y., & Banik, G. U. P. T. A.** (2012). LSB modification and phase encoding technique of audio steganography revisited. *International Journal of Advanced Research in Computer and Communication Engineering*, *1*(4), 1-4.

[5] **Mishra, S., Yadav, V. K., Trivedi, M. C., & Shrimali, T.** (2018). Audio steganography techniques: A survey. In *Advances in Computer and Computational Sciences* (pp. 581-589). Springer, Singapore.

[6] **Sridevi, R., Damodaram, A., & Narasimham, S. V. L.** (2009). EFFICIENT METHOD OF AUDIO STEGANOGRAPHY BY MODIFIED LSB ALGORITHM AND STRONG ENCRYPTION KEY WITH ENHANCED SECURITY. *Journal of Theoretical & Applied Information Technology*, *5*(6).

[7] **Petrovic, R., Winograd, J. M., Jemili, K., & Metois, E.** (1999, October). Data hiding within audio signals. In *4th International Conference on Telecommunications in Modern Satellite, Cable and Broadcasting Services. TELSIKS'99 (Cat. No. 99EX365)* (Vol. 1, pp. 88-95). IEEE.

[8] **Wakiyama, M., Hidaka, Y., & Nozaki, K.** (2010, October). An audio steganography by a low-bit coding method with wave files. In *2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing* (pp. 530-533). IEEE.

[9] **Djebbar, F., Ayad, B., Hamam, H., & Abed-Meraim, K.** (2011, April). A view on latest audio steganography techniques. In *2011 International Conference on Innovations in Information Technology* (pp. 409-414). IEEE.

[10] **Asad, M., Gilani, J., & Khalid, A.** (2011, July). An enhanced least significant bit modification technique for audio steganography. In *International Conference on Computer Networks and Information Technology* (pp. 143-147). IEEE.

[11] **Bilgin, M.** (2013, Ocak). Steganografi. *XV. Akademik Bilişim Konferansı Bildirileri* (125-128).

[12] **Cao, X., & Zhang, L.** (2011, November). Researches on echo kernels of audio digital watermarking technology based on echo hiding. In *2011 International Conference on Wireless Communications and Signal Processing (WCSP)* (pp. 1-5). IEEE.

[13] **Tekeli, K., & Asliyan, R.** (2017). A comparison of echo hiding methods. *The Eurasia Proceedings of Science Technology Engineering and Mathematics*, (1), 397-403.

[14] **Cvejic, N., & Seppanen, T.** (2002, December). Increasing the capacity of LSB-based audio steganography. In *2002 IEEE Workshop on Multimedia Signal Processing.* (pp. 336-338). IEEE.

[15] **Kekre, H. B., Athawale, A., Rao, S., & Athawale, U.** (2010). Information hiding in audio signals. *International Journal of Computer Applications*, *7*(9), 14-19.

[16] **Kaur, N., & Behal, S.** (2014). A Survey on various types of Steganography and Analysis of Hiding Techniques. *International journal of engineering trends and technology*, *11*(8), 388-392.

[17] **Djebbar, F., Ayad, B., Meraim, K. A., & Hamam, H.** (2012). Comparative study of digital audio steganography techniques. *EURASIP Journal on Audio, Speech, and Music Processing*, *2012*(1), 1-16.

[18] **Bender, W., Gruhl, D., Morimoto, N., & Lu, A.** (1996). Techniques for data hiding. *IBM systems journal*, *35*(3.4), 313-336.

[19] **Tian, H., Zhou, K., Jiang, H., Liu, J., Huang, Y., & Feng, D.** (2009, June). An M-sequence based steganography model for voice over IP. In *2009 IEEE International Conference on Communications* (pp. 1-5). IEEE.

[20] **Kadhom, S. A., & Azize, S. A.** (2018, November). Embedding secrete message in transformed voices files using a new method for position selection. In *2018 1st Annual International Conference on Information and Sciences (AiCIS)* (pp. 159-163). IEEE.

[20] **Tura, A. D., Mamo, H. B., & Gemechu, W. F.** (2021). Mathematical modeling and parametric optimization of surface roughness for evaluating the effects of fused deposition modeling process parameters on ABS material. *International Journal of Advanced Engineering Research and Science*, *8*, 5.

[21] **Bhavana, D., Tej, D.R., Puneeth, M., Harini, A., Shankar, Y.M., Madhuri, T.S.** (2015). Steganography Using Matlab, International Journal of Advanced Engineering Research and Science (IJAERS) 19-24.

[22] **Tian, H., Zhou, K., Jiang, H., Huang, Y., Liu, J., & Feng, D.** (2009, May). An adaptive steganography scheme for voice over IP. In *2009 IEEE International Symposium on Circuits and Systems* (pp. 2922-2925). IEEE.

[23] **Shah, P., Choudhari, P., & Sivaraman, S.** (2008, December). Adaptive wavelet packet based audio steganography using data history. In *2008 IEEE Region 10 and the Third International Conference on Industrial and Information Systems* (pp. 1-5). IEEE.

[24] **Gupta, N., & Sharma, N.** (2014, February). DWT and LSB based Audio Steganography. In *2014 International Conference on Reliability Optimization and Information Technology (ICROIT)* (pp. 428-431). IEEE.

[25] **Bilal, I., Kumar, R., Roj, M. S., & Mishra, P. K.** (2014, December). Recent advancement in audio steganography. In *2014 International Conference on Parallel, Distributed and Grid Computing* (pp. 402-405). IEEE.

[26**] Kartheeswaran, T., Senthooran, V., & Pemadasa, T. D. D. L.** (2015, December). Multi agent based audio steganography. In *2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC)* (pp. 1-4). IEEE.

[27] **Siburian, R.** (2017, July). Steganography implementation on android smartphone using the LSB (least significant bit) to MP3 and WAV audio. In *2017 3rd International Conference on Wireless and Telematics (ICWT)* (pp. 170-174). IEEE.

[28] **Rajput, S. P., Adhiya, K. P., & Patnaik, G. K.** (2017, August). An efficient audio steganography technique to hide text in audio. In *2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA)* (pp. 1-6). IEEE.

[29] **Teotia, S., & Srivastava, P.** (2018, April). Enhancing Audio and Video Steganography Technique Using Hybrid Algorithm. In *2018 International Conference on Communication and Signal Processing (ICCSP)* (pp. 1059-1063). IEEE.

[30] **Anwar, M., Sarosa, M., & Rohadi, E.** (2019, March). Audio steganography using lifting wavelet transform and dynamic key. In *2019 international conference of artificial intelligence and information technology (ICAIIT)* (pp. 133-137). IEEE.

[31] **Sobin, C. C., & Manikandan, V. M.** (2019, November). A Secure Audio Steganography Scheme using Genetic Algorithm. In *2019 Fifth International Conference on Image Information Processing (ICIIP)* (pp. 403-407). IEEE.

[32] **Burrus, C. S., & Parks, T. W.** (1985). Convolution Algorithms. *Citeseer: New York, NY, USA*.

[33] **Bracewell, R. N., & Bracewell, R. N.** (1986). *The Fourier transform and its applications* (Vol. 31999, pp. 267-272). New York: McGraw-Hill.

[34] **Krenn, R.** (2004). Steganography and steganalysis.

[35] **Zamani, M., Manaf, A. B. A., Ahmad, R. B., Jaryani, F., Taherdoost, H., & Zeki, A. M.** (2009, November). A secure audio steganography approach. In *2009 International Conference for Internet Technology and Secured Transactions,(ICITST)* (pp. 1-6). IEEE.

[36] **YİĞİT, Y.** (2018). Sayısal imgelerde güvenli veri gizlemeye yönelik uygun maske belirleme/Determination of the appropriate mask for hiding secure data on digital images.

[37] **Tokur, Y., & Erçelebi, E.** (2005). Spread Spectrum Audio Watermarking Scheme Based On Psychoacoustic Model. *Gaziantep University, Electrical & Electronics Engineering*.

[38] **Lin, Y., Abdulla, W. H., M.** (2014). Audio Watermark: A Comprehensive Foundation Using MATLAB, Springer, 1-183.

[39] **Alp, H., Akıncı, T. Ç., Albora, M.** (2008). Comparıson Of Fourier And Wavelet Transforms In Geophysical Applicatıons, Journal Of Engineerıng Sciences, 14 (1), 67-76.

ÖZGEÇMİŞ

Ad-Soyad : Funda ASLANTAŞ BEYİN

ÖĞRENİM DURUMU:

- **Lisans :** 2018, Bursa Uludağ Üniversitesi, Mühendislik Fakültesi, Elektrik Elektronik Mühendisliği
- **Yüksek Lisans :** 2021, Bursa Teknik Üniversitesi, Fen Bilimleri Enstitüsü, Elektrik Elektronik Mühendisliği