T.C.
İSTANBUL ATLAS ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

AYRIK DALGACIK DÖNÜŞÜMÜ (ADD) KULLANILARAK SES STEGANOGRAFİSİ

Hamidah Saleh Abdullah Mohammed ZOLAAT

DANIŞMAN
Dr. Öğr. Üyesi Recep DURANAY

Bilgisayar Mühendisliği Anabilim Dalı

Bilgisayar Mühendisliği (Türkçe) Programı

İSTANBUL, 2026

T.C.
İSTANBUL ATLAS ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ

AYRIK DALGACIK DÖNÜŞÜMÜ (ADD) KULLANILARAK SES STEGANOGRAFİSİ

Hamidah Saleh Abdullah Mohammed ZOLAAT

DANIŞMAN
Dr. Öğr. Üyesi Recep DURANAY

Bilgisayar Mühendisliği Anabilim Dalı

Bilgisayar Mühendisliği (Türkçe) Programı

İSTANBUL, 2026

T.C.
İSTANBUL ATLAS ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
TEZ ONAY SAYFASI

ÖĞRENCİ ADI -SOYADI	Hamıdah Saleh Abdullah Mohammed ZOLAAT
ÖĞRENCİ NUMARASI	232114004
PROGRAM ADI	Bilgisayar Mühendisliği Tezli Yüksek Lisans Programı

İstanbul Atlas Üniversitesi Bilgisayar Mühendisliği Anabilim Dalında Hamıdah Saleh Abdullah Mohammed ZOLAAT tarafından hazırlanan "Ayrık Dalgacık Dönüşümü (ADD) Kullanılarak Ses Steganografisi" adlı tez çalışması jüri tarafından Yüksek Lisans tezi olarak kabul edilmiştir.

Tez Savunma Tarihi: 23 /02 /2026

Jüri Üyesinin Unvanı, Adı, Soyadı	**Çalıştığı Kurum**	**İmzası**
Dr. Öğr. Üyesi Recep DURANAY	İstanbul Atlas Üniversitesi	
Doç. Dr. Ahmet GÜRHANLI	İstanbul Topkapı Üniversitesi	
Doç. Dr. Oğuz ATA	İstanbul Atlas Üniversitesi	

İstanbul Atlas Üniversitesi Lisansüstü Eğitim-Öğretim ve Sınav Yönetmeliği'nin ilgili maddeleri uyarınca bu tez jüri tarafından onaylanmış ve Enstitü Yönetim Kurulu kararıyla kabul edilmiştir.

Prof. Dr. Hafize UZUN
Lisansüstü Eğitim Enstitüsü Müdürü

BEYAN

Bu tezin bana ait, özgün bir çalışma olduğunu; çalışmamın hazırlık, veri toplama, analiz ve bulguların sunumu olmak üzere tüm aşamalarında bilimsel etik ilke ve kurallara uygun davrandığımı; bu çalışma kapsamında elde edilmeyen tüm veri ve bilgiler için kaynak gösterdiğimi ve bu kaynaklara kaynakçada yer verdiğimi; çalışmanın İstanbul Atlas Üniversitesinde kullanılan "bilimsel intihal tespit programı" ile tarandığını ve öngörülen standartları karşıladığını beyan ederim.

Herhangi bir zamanda, çalışmamla ilgili yaptığım bu beyana aykırı bir durumun saptanması durumunda, ortaya çıkacak tüm ahlaki ve hukuki sonuçlara razı olduğumu bildiririm.

Hamıdah Saleh Abdullah Mohammed ZOLAAT

İTHAF

Bu çalışmayı, sabrı, sevgisi ve desteğiyle her zaman yanımda olan aileme ithaf ediyorum..

BÜTÇE DESTEKLERİ

AYRIK DALGACIK DÖNÜŞÜMÜ (DWT) KULLANILARAK SES STEGANOGRAFİSİ

Bu tez çalışması için herhangi bir kurumdan bütçe desteği alınmamıştır.

TEŞEKKÜR

Bu tez çalışmasının hazırlanması sürecinde, değerli akademik rehberliği, titiz danışmanlığı ve yapıcı metodolojik geri bildirimleri için tez danışmanım **Dr. Öğr. Üyesi Recep DURANAY'a** en içten teşekkürlerimi sunarım. Bilimsel titizlik, analitik açıklık ve sistematik araştırma yaklaşımına verdiği önem, bu çalışmanın yönünü ve teknik derinliğini belirlemede önemli bir rol oynamıştır.

Ayrıca, akademik süreç boyunca sağladığı değerli destek, rehberlik ve teşvikleri için Prof. Dr. **Naim Mahmood Musleh AJLOUNI'ye** teşekkür ederim. Tavsiyeleri ve sürekli desteği, akademik gelişimime önemli katkılar sağlamıştır.

Mühendislik ve Doğa Bilimleri Fakültesi'nin değerli akademik kadrosuna, eleştirel düşünmeyi teşvik eden ve bu çalışmanın tamamlanmasına olanak sağlayan destekleyici akademik ortam için teşekkür ederim.

Her zaman duaları ve manevi desteğiyle yanımda olan anneme, mesafeye rağmen bana güç veren varlığı için minnettarım.

Son olarak, bu süreçteki iş birliği, desteği ve yapıcı tartışmalarıyla karşılaştığım birçok zorluğun üstesinden gelmeme yardımcı olan değerli arkadaşım ve meslektaşım Mühendis **Abdelrahman Almassri'ye** teşekkür ederim.

TEŞEKKÜR EDERİM…

Şubat 2026 Hamıdah Saleh Abdullah Mohammed ZOLAAT

İÇİNDEKİLER

Sayfa no

SİMGE/SEMBOL VE KISALTMALAR LİSTESİ

cA	Yaklaşım katsayıları
cD	Detay katsayıları
Δ	Nicemleme adım büyüklüğü
x[n]	Ayrık zamanlı sinyal
h[n]	Yüksek geçiren filtre
g[n]	Alçak geçiren filtre
$\oplus$	XOR işlemi
$GF(2^8)$	Sonlu alan
IV	Başlatma Vektörü
ADD	Ayrık Dalgacık Dönüşümü
DWT	Discrete Wavelet Transform
NİM	Nicemleme İndeks Modülasyonu
QIM	Quantization Index Modulation
GŞS	Gelişmiş Şifreleme Standardı
AES	Advanced Encryption Standard
ŞBZ	Şifre Blok Zincirleme
CBC	Cipher Block Chaining
PSNR	Tepe Sinyal-Gürültü Oranı
BER	Bit Hata Oranı
LSB	En Az Anlamlı Bit
DCT	Ayrık Kosinüs Dönüşümü
HAS	İnsan İşitsel Sistemi

ŞEKİL VE RESİMLER LİSTESİ

Sayfa no

TABLOLAR LİSTESİ

Sayfa no

ÖZET

Zolaat,H. (2025). Ayrık Dalgacık Dönüşümü (ADD) Kullanılarak Ses Steganografisi Yüksek Lisans Tezi, İstanbul Atlas Üniversitesi Lisansüstü Eğitim Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, İstanbul.

Dijital iletişimin hızla yaygınlaşması, hassas bilgilere yetkisiz erişim riskini artırmıştır. Geleneksel kriptografik teknikler veri gizliliğini sağlasa da iletişimin varlığını gizlemez ve bazı bağlamlarda şüphe uyandırabilir. Ses steganografisi bu sınırlamayı, gizli bilgiyi ses sinyalleri içine gömerek aşmayı amaçlar; ancak mevcut birçok yaklaşım saydamlık, dayanıklılık ve kapasite arasında yapısal ödünleşimlerle karşı karşıyadır.

Bu tezde, dönüşüm alanında gömme için Ayrık Dalgacık Dönüşümü (ADD) ve Nicemleme İndeks Modülasyonu (NİM) yöntemlerini birleştiren ve mesaj gizliliğini gömme öncesinde korumak amacıyla GŞS-ŞBZ şifrelemesini kullanan hibrit bir ses steganografisi çerçevesi sunulmuştur. Şifrelenmiş metinsel veriler, algısal kaliteyi korumak amacıyla insan işitsel sisteminin özelliklerinden yararlanılarak sıkıştırılmamış WAV sesinin yüksek frekanslı dalgacık katsayılarına gömülmüştür.

Python ortamında bir prototip gerçekleştirilmiş ve sistem Tepe Sinyal-Gürültü Oranı (PSNR) ile Bit Hata Oranı (BER) ölçütleri kullanılarak değerlendirilmiştir. Deneyler, algoritmik davranışı izole etmek amacıyla özellikle kontrollü ve sıkıştırılmamış ses koşullarına odaklanmıştır. Sonuçlar çok yüksek algısal saydamlık sağlandığını, ancak özellikle şifreleme uygulandığında çözücü tarafında kalıcı bit hatalarının ortaya çıktığını göstermiştir. Bu bulgular, mesaj geri kazanımının tam değil kısmi olduğunu ve güvenilir çıkarımdan ziyade dönüşüm ve yeniden yapılandırma aşamalarındaki sayısal etkilerle sınırlı kaldığını; dolayısıyla algısal duyulmazlık ile bit düzeyinde geri kazanılabilirlik arasında yapısal bir gerilim bulunduğunu ortaya koymaktadır.

Genel olarak çalışma, dönüşüm alanı steganografisini modern kriptografi ile bütünleştiren yorumlanabilir bir temel çerçeve sunmaktadır. Sistem özellikle saydamlığın önceliklendirildiği kontrollü veya çevrimdışı senaryolar için uygundur ve dayanıklılık odaklı geliştirmeler ile daha geniş gerçek dünya değerlendirmeleri için bir başlangıç noktası oluşturmaktadır.

Anahtar Kelimeler: Ses Steganografisi, ADD, NİM, AES-ŞBZ, Dönüşüm Alanında Gömme, Güvenli Veri Gizleme, PSNR, BER, Algılanamazlık, Dayanıklılık

ABSTRACT

Zolaat, H. (2025). Discrete Wavelet Transform (ADD) and Quantization Index Modulation (NİM) for transform-domain embedding. Master's Thesis, İstanbul Atlas University Postgraduate Education Institute, Department of Computer Engineering, İstanbul.

The rapid growth of digital communication has increased the risk of unauthorized access to sensitive information. While traditional cryptographic techniques ensure data confidentiality, they do not conceal the existence of communication and may therefore raise suspicion in certain contexts. Audio steganography addresses this limitation by embedding secret information into audio signals; however, many existing approaches face inherent trade-offs between transparency, robustness, and capacity. This thesis presents a hybrid audio steganography framework that combines Discrete Wavelet Transform (ADD) and Quantization Index Modulation (NİM) for transform-domain embedding, together with GŞS-ŞBZ encryption to protect message confidentiality prior to insertion. Encrypted textual data are embedded in high-frequency wavelet coefficients of uncompressed WAV audio, exploiting properties of the human auditory system to preserve perceptual quality. A prototype implementation was developed in Python and evaluated using Peak Signal-to-Noise Ratio (PSNR) and Bit Error Rate (BER). The experiments deliberately focused on controlled, uncompressed audio conditions in order to isolate algorithmic behaviour. The results indicate very high perceptual transparency but also reveal persistent bit errors at the decoder, particularly when encryption is applied. These findings indicate that message recoverability is partial and constrained by numerical effects in the transform and reconstruction stages, highlighting a structural tension between perceptual inaudibility and bit-level recoverability rather than reliable extraction. Overall, the work provides an interpreTablo baseline framework that integrates transform-domain steganography with modern cryptography. The system is primarily suited for controlled or offline scenarios where transparency is prioritised, and it serves as a foundation for future research targeting robustness-oriented enhancements and broader real-world evaluation.

Keywords: Audio Steganography, DWT, QIM, AES-CBC, Transform-Domain Embedding, Secure Data Hiding, PSNR, BER, Imperceptibility, Robustness

1. GİRİŞ VE MOTİVASYON VE PROBLEM TANIMI

1.1.GİRİŞ

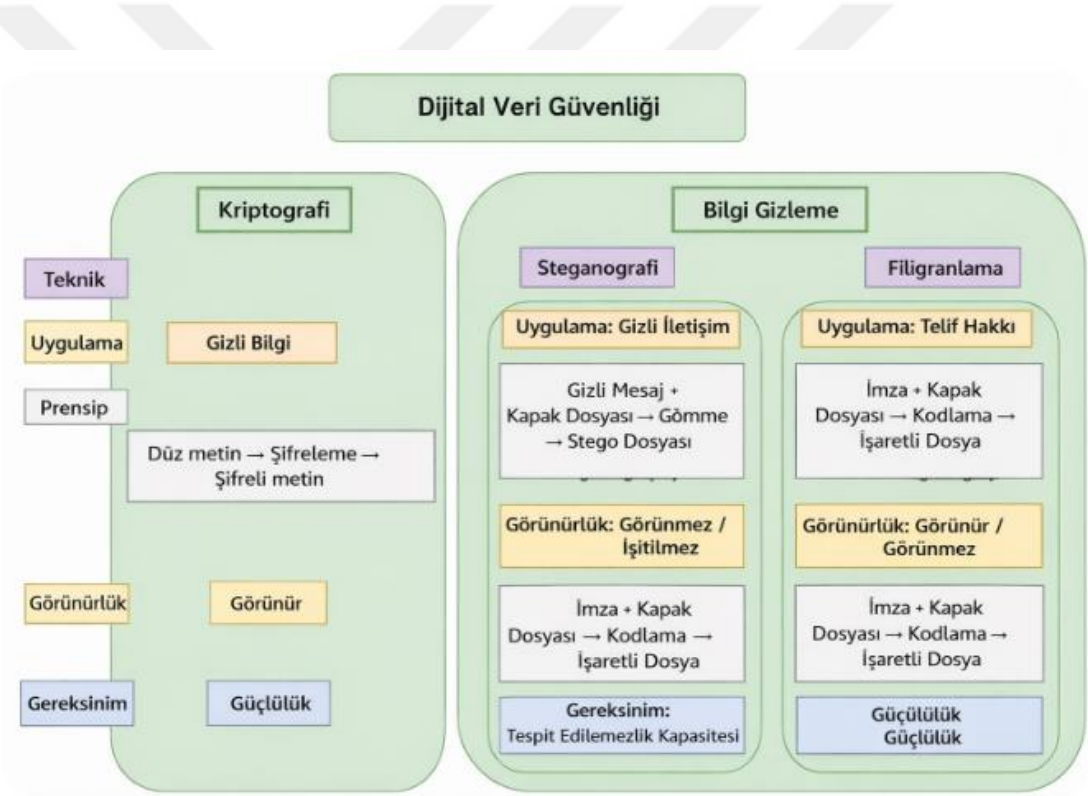
Dijital iletişim teknolojileri, iletilen bilginin hem miktarını hem de hassasiyetini önemli ölçüde artırmış ve güvenliği modern bilişim ortamlarının temel bir gereksinimi hâline getirmiştir. Kriptografik yöntemler gizliliği, açık metni şifreli metne dönüştürerek sağlar; ancak şifrelenmiş trafik dışarıdan bakıldığında yine de korumalı içerik olarak ayırt edilebilir durumdadır. Bazı ortamlarda yalnızca şifreleme kullanılması bile şüphe uyandırabilir veya adli incelemelerin odağına girebilir. Bu nedenle, gizleme ihtiyacı gizlilik kadar önemli hâle gelmektedir. Ses steganografisi, gizli veriyi sıradan ses sinyalleri içine algısal olarak fark edilmeyecek biçimde gömerek hem tespit edilme olasılığını azaltmayı hem de ses kalitesini korumayı amaçlar (Bender et al., 1996; Petitcolas et al., 1999).

Dönüşüm uzayı temelli yaklaşımlar, özellikle Ayrık Dalgacık Dönüşümü (**ADD**) kullanan yöntemler, sinyal bilgisini hem zaman hem de frekans boyutunda konumlandırarak düzenli veri gömme imkânı sunar. Bu çok çözünürlüklü gösterim sayesinde veri, ham ses örneklerine doğrudan müdahale etmek yerine insan işitme sistemi açısından daha az hassas bileşenlere yerleştirilebilir. Klasik En Önemsiz Bit (**LSB**) değiştirme yöntemleriyle karşılaştırıldığında **ADD** tabanlı teknikler, algılanamazlık ile veri kapasitesi arasında daha esnek bir denge kurabilmektedir (Mallat, 1989; Johnson & Katzenbeisser, 2000). Bununla birlikte literatürdeki çalışmaların önemli bir kısmı bu sistemleri çoğunlukla ideal ve sıkıştırılmamış koşullar altında değerlendirmekte ve tasarım tercihlerinin saydamlık, veri boyutu ve mesajın geri elde edilebilirliği üzerindeki etkisini her zaman açık biçimde ortaya koymamaktadır. Ayrıca bazı araştırmalar gizlemeye ağırlık verirken kriptografik korumayı ihmal etmekte ve veri ortaya çıkarıldığında içeriğin doğrudan okunabilir olmasına neden olmaktadır (Chan & Cheng, 2004).

Bu eksikliklerden hareketle bu tezde, **ADD** alanında Nicemleme İndeks Modülasyonu (**NİM**) ile veri gömme işlemini, Blok Zincirleme Kipinde (**ŞBZ**) çalışan Gelişmiş Şifreleme Standardı (**GŞS**) ile birleştiren hibrit bir yapı incelenmektedir. Amaç evrensel bir dayanıklılık iddiası ortaya koymak değil; açıkça tanımlanmış varsayımlar altında deneysel olarak analiz edilebilen, anlaşılır ve tekrarlanabilir bir işlem süreci geliştirmektir. Bu kapsamda sistem davranışı, sıkıştırılmamış ve kontrollü **WAV** ortamında algısal saydamlık, veri kapasitesi ve geri elde etme kararlılığı açısından değerlendirilmiştir. Şifreleme uygulandığ

ında çözme aşamasında ortaya çıkabilecek küçük hatalar bile elde edilen mesajı kullanılamaz hâle getirebildiğinden Bit Hata Oranı'na (**BER**) özellikle önem verilmiştir. Bu nedenle geri kazanım süreci kesin sonuç veren bir işlem olarak kabul edilmemiş; dönüşüm uzayındaki sayısal etkilerden etkilenen, sınırlı ve hata oluşumuna açık bir süreç olarak ele alınmıştır (Petitcolas et al., 1999).Bu nedenle deneysel kapsam bilinçli olarak sınırlı tutulmuştur. Bu sınırlar içerisinde tezin temel katkısı yöntemsel açıklıktır.

Çalışmada tasarım kararları açık biçimde belgelenmiş, ortaya çıkan ödünleşimler ortaya konmuş ve sistem davranışı Tepe Sinyal-Gürültü Oranı (**PSNR**) ile Bit Hata Oranı (**BER**) gibi yerleşik ölçütler kullanılarak nicel olarak raporlanmıştır. Tamamlanmış ve doğrudan kullanıma hazır bir ürün sunmak yerine önerilen yapı, ileride dayanıklılık odaklı geliştirmelere temel oluşturabilecek şeffaf bir referans yapılandırma olarak sunulmuştur.



Şekil 1.1: Ses steganografisinde tezin motivasyonu ve problem bağlamının genel görünümü.

1.2. MOTİVASYON VE PROBLEM TANIMI

Ses steganografisi, bilgiyi ses sinyallerinin içine algısal kaliteyi bozmayacak ve şüphe uyandırmayacak biçimde gizlemeyi amaçlar. Ancak uygulamada her steganografik sistem üç temel hedef arasında denge kurmak zorundadır: sesin saydamlığını korumak, makul bir veri kapasitesi sunmak ve mesajın kısmen de olsa geri elde edilebildiği koşulları incelemek. Mevcut birçok yaklaşım özellikle Ayrık Dalgacık Dönüşümü (**ADD**) gibi dönüşüm uzayı tekniklerini kullananlar genellikle yalnızca temiz ve sıkıştırılmamış ortamlarda değerlendirilmekte ve kimi zaman açıkça tanımlanmış ya da tekrarlanabilir değerlendirme süreçleri olmadan tek seferlik sonuçlar raporlamaktadır.

Öte yandan yalnızca steganografi kullanılması, gizli veri ortaya çıkarıldığında içeriğin gizliliğini garanti etmez; benzer şekilde kriptografik yöntemler de çoğu zaman şifrelemenin ses taşıyıcısı içine gömme kararlarıyla nasıl etkileştiğini ele almaz. Bu nedenle dalgacık ayrışım seviyesi, nicemleme gücü ve veri boyutu gibi tasarım parametrelerinin ses kalitesi ve çıkarım güvenilirliği üzerindeki etkilerini ölçülebilir biçimde açıklayan, açıkça belgelenmiş ve tekrarlanabilir çerçevelere hâlen ihtiyaç duyulmaktadır.

Bu tezde ele alınan problem, evrensel olarak dayanıklı ya da gerçek zamanlı çalışan bir sistem geliştirmek veya sıkıştırma ile saldırgan ortamlara karşı direnç iddiasında bulunmak değildir. Bunun yerine amaç, kontrollü ve sıkıştırılmamış **WAV** koşulları altında **GŞS-ŞBZ** şifreleme ile **ADD–NİM** gömme yöntemini birleştiren hibrit bir yapıyı sistematik biçimde inceleyerek saydamlık, kapasite ve geri elde edilebilirlik arasındaki somut ödünleşimleri açıkça ortaya koymaktır.

1.3. AMAÇLAR VE KATKILAR

1.3.1. Araştırma Amaçları

Bu tezin genel amacı, açıkça tanımlanmış deneysel koşullar altında **GŞS-ŞBZ** şifreleme ile **ADD–NİM** gömme yöntemini birleştiren hibrit bir ses steganografisi yapısı tasarlamak ve analiz etmektir. Daha özel olarak tez şu hedeflere odaklanmaktadır:

- Mevcut ses steganografisi yaklaşımlarını, özellikle **ADD** ve **LSB** tabanlı tekniklere odaklanarak incelemek ve bütüncül biçimde sentezlemek.
- Asarım kararları açıkça belirtilmiş hibrit bir **GŞS-ŞBZ** + **ADD–NİM** yapısı geliştirmek.
- Belgelenmiş parametreler ve tekrarlı deneyleri içeren, tekrarlanabilir bir deney protokolü tanımlamak.

- Algısal saydamlığı değerlendirmek için Tepe Sinyal-Gürültü Oranı (**PSNR**) ve mesajın geri elde edilebilirliğinin sınırlarını belirlemek için Bit Hata Oranı (**BER**) kullanarak performansı değerlendirmek.
- Saydamlık, kapasite ve geri elde edilebilirlik arasındaki gözlenen ödünleşimleri analiz etmek.
- Gerçekçi sınırlamaları belirlemek ve gelecekte dayanıklılık odaklı araştırmalar için yönelimler ortaya koymak.

1.3.2 Özgün Katkılar

Evrensel ve doğrudan kullanıma hazır bir steganografi sistemi önermek yerine bu tez, kontrollü koşullar altında şifreleme ile dönüşüm uzayı tabanlı gömme yöntemlerinin nasıl etkileştiğini anlamaya yönelik açık ve tekrarlanabilir bir temel çerçeve sunmaktadır. Başlıca katkılar şunlardır:

- **Hibrit temel çerçeve**: **GŞS-ŞBZ** şifreleme ile **ADD** tabanlı **NİM** gömme ve çıkarma süreçlerini uçtan uca içeren, belgelenmiş bir işlem hattı.
- **Açık tasarım gerekçesi**: Dalgacık seviyesi, katsayı seçimi ve nicemleme adım büyüklüğü gibi tercihlerin beklenen sistem davranışını nasıl etkilediğinin tartışılması.
- **Tekrarlanabilir yapı**: Parametre düzeyinde deneylere ve genişletmelere imkân verecek şekilde gömme ve çıkarma işlemlerinin yapılandırılmış sunumu.
- **Değerlendirilmiş referans temeli**: Sıkıştırılmamış **WAV** sesleri üzerinde PSNR ve BER kullanılarak yapılan sistematik değerlendirme ile gelecekte dayanıklılık odaklı çalışmalar için izlenebilir bir referans noktası oluşturulması.

1.4. KAPSAM VE SINIRLILIK

Bu tez, bilinçli olarak kontrollü ve açık biçimde tanımlanmış bir problem çerçevesine odaklanmaktadır. Önerilen hibrit yapı yalnızca sıkıştırılmamış **16-bit PCM WAV** sesleri üzerinde, çevrimdışı deneyler ve kısa metinsel yükler kullanılarak değerlendirilmiştir. Gerçek zamanlı senaryolar, kayıplı sıkıştırma (**örneğin MP3**), saldırgan ortamlar, otomatik steganaliz ve derin öğrenme tabanlı yaklaşımlar bu çalışmanın kapsamı dışındadır. Amaç evrensel olarak dayanıklı bir sistem iddiasında bulunmak değil; daha zorlu ve gerçekçi koşullara ileride genişletilebilecek tekrarlanabilir bir temel çerçeve oluşturmaktır.

1.5. TEZ ORGANİZASYONU

Tezin geri kalanı şu şekilde düzenlenmiştir: Bölüm 2, önerilen yapının anlaşılması için gerekli kuramsal arka planı sunmakta; dijital sesin temel kavramları, steganografi ve Ayrık Dalgacık Dönüşümü ele alınmaktadır. Bölüm 3'te ses steganografisi alanındaki ilgili çalışmalar incelenerek literatürde bildirilen güçlü yönler, sınırlılıklar ve açık problemler ortaya konulmaktadır. Bölüm 4, **GŞS-ŞBZ** şifreleme ile **ADD–NİM** gömme yönteminin bütünleştirildiği önerilen hibrit yapıyı ve gömme–çıkarma süreçlerini ayrıntılı biçimde açıklamaktadır. İzleyen geliştirme bölümlerinin ardından Bölüm 7'de kontrollü koşullar altında gerçekleştirilen deney düzeni, değerlendirme ölçütleri ve elde edilen sonuçlar sunulmakta, gözlenen ödünleşimler yorumlanmaktadır. Son olarak Bölüm 8'de temel bulgular özetlenmekte, çalışmanın sınırlılıkları tartışılmakta ve gelecekteki araştırmalar için olası yönelimler önerilmektedir.

2. ARKA PLAN

2.1. STEGANOGRAFİ: GÜVENLİ İLETİŞİMDE TEMELLERİ VE ROLÜ

Steganografi, gizli iletişimin varlığı fark edilmeyecek şekilde bilginin bir dijital ortamın içine saklanması uygulamasıdır. Kriptografi, hassas bir iletişim gerçekleştiğini açıkça gösterse de mesaj içeriğini korumaya odaklanırken; steganografi mesajı görüntü, ses kaydı veya video dosyası gibi sıradan görünen bir sinyalin içine yerleştirerek şüphe oluşmasını tamamen ortadan kaldırmayı hedefler (Katzenbeisser & Petitcolas, 2000).

Günümüz dijital ortamlarında bu iki teknik çoğunlukla birlikte kullanılmaktadır: kriptografi içeriği korurken steganografi iletişimin varlığını gizler. Bu katmanlı yaklaşım, görünür şifrelemenin adli inceleme başlatabileceği veya dikkat çekebileceği uygulamalar açısından özellikle önem taşımaktadır.

Steganografik sistemler üç temel ilke ile tanımlanır (Johnson & Katzenbeisser, 2000):

- **Alıglanamazlık(Saydamlık)**: Gömme işlemi işitsel veya görsel olarak fark edilebilir bozulmalara neden olmamalıdır.
- **Kapasite**: Sistem, sinyal kalitesini düşürmeden anlamlı miktarda veri taşıyabilmelidir.
- **Dayanıklılık**: Gizli mesaj mümkün olduğunca yaygın sinyal işlemlerine karşı dirençli olmalıdır.

Bu ilkeler, bu tezde geliştirilen ses steganografisi çerçevesinin kavramsal temelini oluşturmaktadır.

2.2. SES STEGANOGRAFİSİ TEKNİKLERİ

Ses steganografisi, dinleyici açısından algısal kaliteyi koruyarak gizli bilgiyi dijital ses sinyalleri içine yerleştirir. İnsan İşitsel Sistemi (**HAS**), özellikle düşük frekans bölgelerindeki bozulmalara oldukça duyarlı olduğundan, gömme stratejilerinin algısal maskeleme etkilerinden ve daha az hassas frekans bileşenlerinden yararlanması gerekir.

Mevcut yaklaşımlar genel olarak şu gruplara ayrılabilir:

- En Önemsiz Bit (**LSB**) değiştirme gibi zaman alanı teknikleri
- Yankı gizleme teknikleri
- Yayılı spektrum yöntemleri
- **ADD** ve **DCT** tabanlı gömme gibi dönüşüm alanı yaklaşımları (Johnson & Katzenbeisser, 2000).

Zaman alanı yöntemleri basit yapılıdır ve çoğu zaman yüksek veri kapasitesi sunar; ancak sıkıştırma, yeniden nicemleme ve istatistiksel steganaliz karşısında oldukça hassastır. Buna karşılık dönüşüm alanı yöntemleri bilgiyi frekans açısından yerelleşmiş bileşenlere gömerek algısal saydamlık ve dayanıklılık üzerinde daha iyi kontrol sağlar (Mallat, 1989). Bu nedenle önerilen yapıda dönüşüm alanı tabanlı gömme tercih edilmiştir; çünkü bu yaklaşım ses sinyali içinde değişikliklerin nasıl ve nerede yapılacağını düzenli ve kontrollü biçimde yönetmeye imkân tanır.

2.3. SES STEGANOGRAFİSİ İÇİN DEĞERLENDİRME ÖLÇÜTLERİ

Ses steganografisi sistemleri genellikle birbirini tamamlayan üç ölçüt kullanılarak değerlendirilir (Johnson & Katzenbeisser, 2000; Petitcolas et al., 1999).

2.3.1. Algılanamazlık (Saydamlık)

Stego-sesin, orijinal sesten ayırt edilememesi gerekir. Saydamlığı nicel olarak değerlendirmek için bu tezde nesnel bir ölçüt olarak Tepe Sinyal-Gürültü Oranı (**PSNR**) kullanılmakta; genel olarak daha yüksek PSNR değerlerinin daha düşük algısal bozulmaya karşılık geldiği kabul edilmektedir.

2.3.2. Kapasite

Kapasite, işitsel bozulma oluşturmadan gömülebilecek bit sayısını ifade eder. Kapasitenin artırılması çoğu zaman bozulmayı da artırdığından, pratik sistemlerde veri miktarı ile saydamlık gereksinimleri arasında denge kurulmalıdır.

2.3.3. Dayanıklılık

Dayanıklılık, gömülü verinin yaygın sinyal işlemlerinden ne ölçüde etkilenmeden korunabildiğini gösterir. Bu tezde dayanıklılık, çıkarım sonrası elde edilen bitlerin doğruluğunu ölçen Bit Hata Oranı (**BER**) kullanılarak değerlendirilmiştir.

2.4. AYRIK DALGACIK DÖNÜŞÜMÜ (ADD)

Ayrık Dalgacık Dönüşümü (**ADD**), bir sinyalin çok çözünürlüklü bir gösterimini sağlayarak hem zaman hem de frekans alanında eşzamanlı konumlandırma sunar; bu özellik klasik Fourier tabanlı analizlere göre önemli bir üstünlük sağlar (Mallat, 1989).

Bir ses sinyaline uygulandığında **ADD**, sinyali şu bileşenlere ayrıştırır:

- **Yaklaşım katsayıları (cA):** Düşük frekans bileşenlerini temsil eder.
- **Detay katsayıları (cD):** Yüksek frekans değişimlerini temsil eder.

İnsan İşitsel Sistemi yüksek frekans bölgelerindeki küçük değişimlere genellikle daha az duyarlı olduğundan, gizli verinin detay katsayılarına yerleştirilmesi algısal saydamlığın korunmasına katkı sağlar. Ayrıca **ADD**, gömme işleminin belirli spektral bantlarla sınırlandırılmasına olanak tanıyarak yerleştirme konumu üzerinde düzenli bir kontrol sunar.

Önerilen yapıda, hesaplama basitliğini korurken yeterli gömme kapasitesi ve saydamlık sağlamak amacıyla Seviye-1 Haar tabanlı **ADD** ayrışımı tercih edilmiştir (Daubechies, 1992).

2.5. NİCEMLEME İNDEKSİ MODÜLASYONU (NİM)

Nicemleme İndeksi Modülasyonu (**NİM**), gömülecek bitin değerine göre belirlenen farklı nicemleme bölgelerine dönüşüm katsayılarını eşleyerek bilgiyi gömer (Chen & Wornell, 2001).

Tek tek en az anlamlı bitleri değiştirmek yerine NİM, bir katsayının nicemleme indeksini ayarlar:

- Gizlenecek her bit (**0 veya 1**) için ayrı bir nicemleme kümesi tanımlanır.
- Sinyaldeki katsayı değeri, ilgili bitin kümesindeki en yakın nicemleme seviyesine kaydırılır.
- Böylece bilgi, katsayının tam değeriyle değil hangi aralığa ait olduğu üzerinden temsil edilir.

Bu yaklaşım üç temel avantaja sahiptir:

- Nicemleme adımı delta ile ayarlanabilen kontrollü bozulum
- Küçük işleme gürültüsüne karşı kararlılık
- Ayrık Dalgacık Dönüşümü tabanlı gömme ile doğal uyumluluk

Bu tezde **NİM**, sağlamlık ile saydamlık arasında ilkesel bir denge sağladığı için temel gömme mekanizması olarak kullanılmaktadır.

2.6. ŞİFRELEMEYE GENEL BAKIŞ: GŞZ VE ŞBZ MODU

Steganografi bir mesajın varlığını gizlerken, gizli yük çıkarıldığında gizliliği garanti etmez. Bu nedenle bu tezde gizli veri gömmeden önce şifrelenmektedir.

Gelişmiş Şifreleme Standardı (**GŞS**), sabit boyutlu veri blokları üzerinde çalışan yaygın olarak kullanılan simetrik bir şifreleme algoritmasıdır (Daemen & Rijmen, 2002). Bu çalışmada Gelişmiş Şifreleme Standardı (**GŞS**), Şifre Bloku Zincirleme kipi (**ŞBZ**) ile birlikte kullanılmaktadır:

- Her şifreli metin bloğu bir öncekine bağlıdır.
- Rastgele bir Başlatma Vektörü **(BV**), aynı açık metinlerin farklı şifreli metinler üretmesini sağlar.
- Ortaya çıkan şifreli veri akışı istatistiksel olarak rastgele görünür.
- Bu özellik steganografi için özellikle önemlidir; çünkü gürültüye benzeyen şifreli metin, dönüşüm katsayılarına tanınabilir desenler yerleştirme olasılığını azaltır.

Bu nedenle önerilen çerçevede **GŞS-ŞBZ** gizlilik sağlarken, **ADD–NİM** gömme işlemi gizleme sağlar böylece birbirini tamamlayan katmanlı bir koruma stratejisi oluşur.

3. KURUMSAL ARKA PLAN

3.1. AYRIK DALGACIK DÖNÜŞÜMÜ (ADD) KURAMI:

Ses gibi durağan olmayan sinyallerle çalışırken temel öneme sahip olan ortak zaman-frekans yerelleştirmesi sağlayabilmesi nedeniyle bu tezde kullanılmıştır. Yalnızca küresel frekans analizi yapan ve zamansal bilgiyi kaybeden Fourier Dönüşümü'nün aksine, **ADD** yerel sinyal ayrıştırmasına izin verir; bu da hassas ve fark edilemez gömme gerektiren steganografik uygulamalar için daha uygun hale getirir (Mallat, 1989).

Bu araştırmada ses sinyaline Seviye-1 Haar (**Daubechies-1**) dalgacık ayrıştırması uygulanmıştır. Haar, hesaplama basitliği (Daubechies, 1992), ortogonallik ve hızlı işleme sağlaması nedeniyle hafif ve verimli bir uygulama gereksinimiyle uyumlu olduğundan seçilmiştir. Sinyal **ADD** işleminden geçtiğinde şu bileşenlere ayrılır:

- **Yaklaşım katsayıları (cA)** – düşük frekans bileşenlerini temsil eder,
- **Ayrıntı katsayıları (cD)** – yüksek frekans değişimlerine karşılık gelir.

Yüksek frekanslı sinyal bölgeleri İnsan İşitsel Sistemi tarafından daha az algılandığından, verinin **cD** alt bandına gömülmesi yapılan değişikliklerin akustik olarak saydam kalmasını sağlar (Johnson & Katzenbeisser, 2000). Bu nedenle bu tezde, algılanan ses kalitesini etkilemeden gizli veri eklenmesini desteklemek amacıyla gömme bölgesi olarak **cD** katsayıları seçilmiştir.

3.2. ADD vs. FOURİER DÖNÜŞÜMÜ

Tablo 3.1: Ses sinyali analizi için Fourier Dönüşümü ile Ayrık Dalgacık Dönüşümü (ADD) arasındaki karşılaştırma

Özellik	**Fourier Dönüşümü**	**Dalgacık Dönüşümü (ADD)**
Zaman Yerelleştirmesi	Hayır	Evet
Frekans Çözünürlüğü	Sabit	Ölçeğe bağlı değişir (çok çözünürlüklü)
Sinyal Uygunluğu	Durağan sinyaller	Durağan olmayan sinyaller
Analiz Türü	Küresel	Yerel

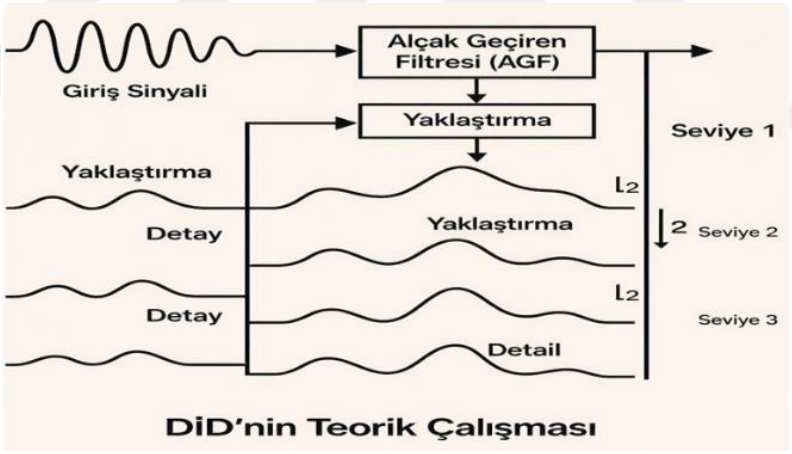
Zaman yerelleştirmesi, sinyalde değişimlerin ne zaman gerçekleştiğini belirleyebilme yeteneğini ifade eder; bu özellik Fourier Dönüşümü'nde bulunmazken **ADD**'nin doğasında vardır. Frekans çözünürlüğü Fourier analizinde sabit kalırken, **ADD** farklı frekans bileşenlerine uyum sağlayan ölçeğe bağlı çok çözünürlüklü bir gösterim sunar. Fourier Dönüşümü ile **ADD** arasındaki yapılandırılmış karşılaştırma Tablo 3.1'de özetlenmiştir.

3.3. ADD'NİN KURAMSAL ÇALIŞMA PRENSİBİ

ADD, giriş sinyalini birbirini tamamlayan iki filtreden geçirerek çalışır:

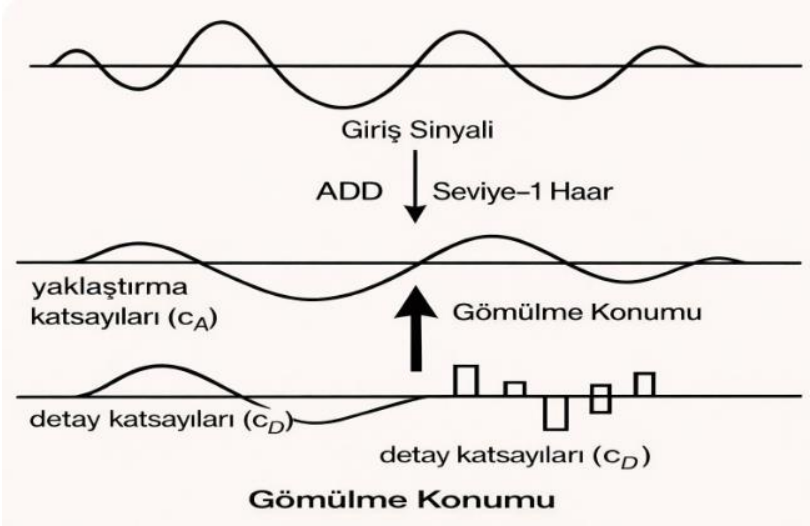
- **Alçak Geçiren Filtre** (**AGF**) – Sinyalin kaba yaklaşımını (düşük frekansları) çıkarır.
- **Yüksek Geçiren Filtre** (**YGF**) – İnce ayrıntıları (yüksek frekansları) yakalar.

Bu filtrelerin çıktıları daha sonra iki kat azaltılarak örneklenir (her ikinci örnek korunur). Bu işlem, sinyalin çok seviyeli ayrıştırmasını elde etmek için düşük frekans bileşeni üzerinde yinelemeli olarak tekrarlanabilir.



Şekil 3.1: Çok seviyeli Ayrık Dalgacık Dönüşümü (**ADD**) ayrışımı: ardışık seviyelerde yaklaşık (approximation) ve detay alt bantlarının gösterimi.

"Çok seviyeli **ADD** ayrışımı, sinyalin giderek daha düzgün yaklaşık bileşenlere ve ince ayrıntılara sahip detaylara daha derin biçimde ayrılmasını sağlar. Şekil 3.1'de gösterildiği gibi yalnızca düşük frekanslı yaklaşık bant yinelemeli olarak ayrıştırılır; bu durum, dönüşüm alanı steganografisinde gömme bölgelerinin bilinçli biçimde seçilebilmesine imkân tanıyan hiyerarşik bir analiz olanağı sağlar.".



Şekil 3.2: Seviye-1 Haar ayrıştırmasından sonra detay katsayılarına (**cD**) veri yerleştirilmesini gösteren **ADD** çerçevesinde gömme konumu.

"Şekil 3.2, **ADD** çerçevesi içerisindeki gömme konumunu göstermektedir. Seviye-1 Haar ayrıştırmasından sonra giriş ses sinyali yaklaşık (**cA**) ve detay (**cD**) katsayılarına ayrılır. Gizli veri, insan işitsel sistemi tarafından daha az algılanabilir olduğu için yüksek frekans bölgelerinde yapılan değişikliklerin fark edilmesi zor olduğundan, saydamlık ve gizliliği artırmak amacıyla **cD** bileşenine gömülmektedir."

3.4. MATEMATİKSEL GÖSTERİM

Orijinal ayrık sinyal x[n]olsun. **ADD** aşağıdaki işlemleri uygular:

3.4.1. Yaklaştırma katsayıları (A)

$$\boldsymbol{A(n) = \sum_{k=1}^{N} x\,[k].\,g[2n-k]}$$

ADD'nin matematiksel formülasyonu, filtreleme ve aşağı örnekleme işlemlerini kompakt bir şekilde ifade eder.

$x[k] \cdot g(2n-k)$ terimi alçak geçiren filtre ile yapılan evrişimi temsil ederken, $2n$ ifadesi yalnızca her ikinci örneğin tutulduğunu gösterir; böylece sinyal yapısı korunurken fazlalık (**redundancy**) azaltılır.

3.4.2. Detay Katsayıları (D)

$$\boldsymbol{D(n) = \sum_{k=1}^{N} x\,[k].\,h[2n-k]}$$

ADD'de detay katsayılarının matematiksel ifadesi, yüksek geçiren filtreleme ardından aşağı örnekleme işlemini temsil eder. Terim :

$$\boldsymbol{x[k] \cdot h\,(2n-k)}$$

Burada Ndalgacık filtresinin uzunluğunu temsil eder ve k, evrişim sırasında sinyal örnekleri boyunca değişir.

Yüksek geçiren filtre ile yapılan evrişime karşılık gelir; burada h[n]hızlı sinyal değişimlerini ve ince varyasyonları yakalar. 2nterimi ise iki kat aşağı örneklemeyi ifade eder ve yalnızca her ikinci örneğin tutulmasını sağlar. Bu işlem, sinyalin yüksek frekans bileşenlerini çıkararak geçici davranışları ve ince detayları vurgularken gereksiz veriyi azaltır.

Burada g[n]ve h[n]sırasıyla alçak geçiren ve yüksek geçiren filtrelerin dürtü yanıtlarını temsil eder ve 2naşağı örnekleme işlemini gösterir (Mallat, 1989).

Daha derin seviyeli ayrıştırmalar mümkün olsa da, bu tezde yalnızca Seviye-1 **ADD** ayrıştırması kullanılmıştır; çünkü daha ileri seviyeler çoğu zaman gömme kapasitesini azaltmakta ve yeniden oluşturma sırasında duyulabilir bozulma olasılığını artırmaktadır (Selesnick, 2001).

Not: Steganografik uygulamalarda bu yüksek frekans bileşenleri genellikle veri gömme için tercih edilir; çünkü insan işitsel sistemi tarafından daha az algılanırlar ve bu nedenle güvenli ve saydam bilgi gizleme için idealdir (Johnson & Katzenbeisser, 2000; Petitcolas vd., 1999).

3.5. STEGANOGRAFİ İLE İLİŞKİSİ

Katzenbeisser ve Petitcolas'a (2000) göre, özellikle Seviye-1 cD alt bandında olmak üzere frekans alanı katsayıları içerisine veri gömmenin aşağıdaki avantajları vardır:

- Algısal saydamlık – yüksek frekans bantlarındaki değişiklikler daha az algılanır.
- Dayanıklılık – dönüşüm alanında gömme, sıkıştırma ve yeniden örnekleme gibi işleme operasyonlarına karşı daha dirençlidir.

- Yüksek gömme kapasitesi – ses kalitesini bozmadan yeterli miktarda veri gömülebilir.

Bu özelliklere dayanarak, bu tezde veriyi **ADD** katsayıları içerisine gömmek için Nicemleme İndeks Modülasyonu (**NİM**) tekniği uygulanmış, böylece gömme kararlılığı ve bozulmaya karşı direnç artırılmıştır. **NİM**'in **ADD** içerisindeki kuramsal ve uygulamalı entegrasyonu bir sonraki bölümde ele alınmaktadır (Chen & Wornell, 2001).

3.6. YAYGIN UYGULAMALAR

Görüntü sıkıştırma (örneğin JPEG2000), ses ve görüntü steganografisi, sinyal gürültü giderme, tıbbi görüntüleme ve konuşma işleme alanlarında özellik çıkarımı ile veri şifreleme ve biyometrik sinyal analizi yaygın kullanım alanları arasındadır.

4. İLGİLİ ÇALIŞMALAR (STEGANOGRAFİ)

4.1. STEGANOGRAFİNİN KAVRAMSAL TEMELLERİ

Bu tezde steganografi, yalnızca mesajın içeriğini değil, aynı zamanda bir mesajın iletildiği gerçeğini de gizlemeyi amaçlayan gizli bir iletişim tekniği olarak kullanılmaktadır. Kriptografiden farklı olarak — ki kriptografi verinin anlamsal içeriğini korurken şifreleme varlığını açıkça belli eder — steganografi, bilgiyi görüntü, ses veya video sinyali gibi zararsız görünen bir örtü ortamı içerisine gömerek çalışır (Katzenbeisser & Petitcolas, 2000). Bu özellik, şifrelemenin görünürlüğünün dahi yakalama, şüphe veya adli analiz tetikleyebileceği ortamlarda özellikle değerlidir (Petitcolas, Anderson & Kuhn, 1999).

Bilgi güvenliği perspektifinden bakıldığında, steganografik sistemleri değerlendirmek için genellikle üç temel tasarım ölçütü kullanılmaktadır:

- **Algılanamazlık (Imperceptibility)** – gömmenin insan algısı veya otomatik analiz tarafından tespit edilemez olma derecesi;
- **Kapasite (Capacity)** – örtü sinyalini önemli ölçüde bozmayacak şekilde gömülebilecek bilgi miktarı;
- **Dayanıklılık (Robustness)** – gömülü verinin sıkıştırma, filtreleme veya yeniden örnekleme gibi sinyal işleme işlemlerine karşı direnci (Johnson & Katzenbeisser, 2000).

Dolayısıyla bu tezde ele alınan steganografik model yalnızca tanımsal bir yaklaşım olmayıp, özellikle ses sinyali işleme bağlamında bu üç ölçüt arasında etkili bir denge kurmayı hedeflemektedir.

4.2. SAYISAL STEGANOGRAFİ TÜRLERİ

Dijital steganografik yöntemler, kullanılan örtü ortamının (cover medium) türüne göre sınıflandırılabilir. Giriş niteliğindeki birçok çalışmada metin, görüntü, ses ve video steganografisi yalnızca kategoriler hâlinde sıralanırken, bu tez her bir ortamı sağlam ve gizli iletişime uygunluk açısından daha analitik bir yaklaşımla değerlendirmektedir.

- **Metin steganografisi** genellikle boşlukların, noktalama işaretlerinin, yazı tipi özelliklerinin veya dilsel yapıların değiştirilmesine dayanır. Görsel olarak fark

edilmesi zor olsa da veri kapasitesi oldukça sınırlıdır ve biçim dönüştürme, yeniden kodlama ve düzenleme işlemlerine karşı son derece hassastır.

- **Görüntü steganografisi**, piksel alanındaki fazlalık (**redundancy**) nedeniyle en yaygın araştırılan alanlardan biridir. Ancak görüntüler sıklıkla kayıplı sıkıştırmaya (örn. **JPEG**) maruz kaldığından, sağlamlık özel olarak ele alınmadığı takdirde gömülü bilgi kolayca bozulabilir (Chan & Cheng, 2004).
- Bu tezin temel odağını oluşturan ses **steganografisi**, İnsan İşitsel Sistemi'nin (**HAS**) maskeleme etkisi gibi özelliklerinden yararlanarak veriyi sinyalin algısal olarak daha az hassas bölgelerine gömer (Johnson & Katzenbeisser, 2000). Bu nedenle, iletim kanallarının zaten yoğun ses içeriği taşıdığı durumlarda ses etkili bir örtü ortamı sunar.
- **Video steganografisi**, görüntü ve ses steganografisinin özelliklerini birleştirir ve yüksek kapasite sağlar; ancak zamansal ve çok kipli (**multimodal**) yapısı nedeniyle ek karmaşıklıklar ortaya çıkarır.

Bu değerlendirmeler ışığında, gizlenebilirlik, kapasite ve dijital iletişim sistemlerinde pratik uygulanabilirlik arasında gerçekçi bir denge sunması nedeniyle bu tezde odak noktası olarak ses steganografisi seçilmiştir.

4.3. SES STEGANOGRAFİ

Şekil 4.1: Ses steganografisi tekniklerinin zaman alanı, dönüşüm alanı, yayılı spektrum, yankı gizleme ve uyarlamalı yaklaşımlar kapsamında sınıflandırılması.

4.3.1. Ses Steganografisi Teknikleri: Analitik Bir Genel Bakış

Ses steganografisi yöntemleri, verinin hangi alanda gömüldüğüne bağlı olarak çeşitli teknik kategorilere ayrılabilir. Bu bölümde, teknik aileler güçlü ve zayıf yönleri ile birlikte, bu tezde geliştirilen **ADD–NİM** yaklaşımıyla ilişkileri açısından incelenmektedir.

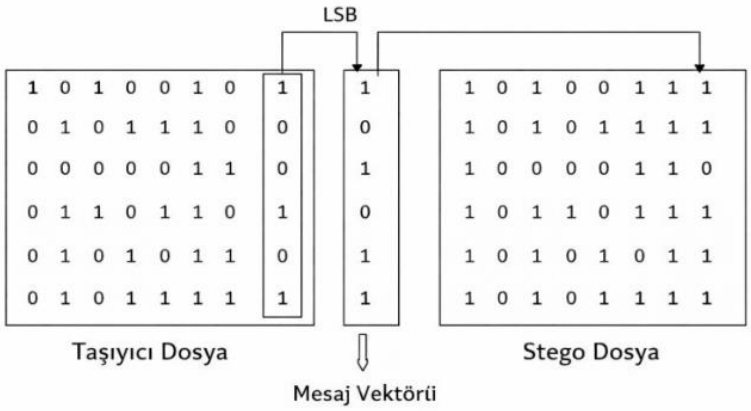
4.3.2. Zaman Alanı Teknikleri (örn. LSB Yerine Koyma)

Zaman alanı yöntemleri doğrudan ayrık ses örnekleri üzerinde çalışır. Bunun en temel örneği, seçilen örneklerin en düşük anlamlı bitlerinin gizli mesajın bitleriyle değiştirildiği En Düşük Anlamlı Bit (**LSB**) yerine koyma yöntemidir.

- **Avantajlar**:
  LSB kavramsal olarak basit, uygulanması kolaydır ve görece yüksek gömme kapasitesi sağlayabilir.

- **Dezavantajlar:**
  Yeniden nicemleme (re-quantization), sıkıştırma veya filtreleme gibi küçük sinyal işleme işlemlerine karşı oldukça hassastır. Ayrıca **LSB** desenleri istatistiksel steganaliz yöntemleriyle tespit edilebilir (Chan & Cheng, 2004).

Bu nedenle **LSB**, daha çok kontrollü ortamlarda kullanıma uygundur ve bu tezde nihai gömme yöntemi olarak değil, referans tekniği olarak ele alınmıştır.



Şekil 4.2: Zaman alanında En Az Anlamlı Bit (LSB) yerine koyma örneği; bir ses örneğinin bit düzeyinde doğrudan değiştirilmesini göstermektedir.

Orijinal örnek: 10110100

Gömülü Bit (1): 10110101

4.3.3. Dönüşüm Alanı Teknikleri (ADD, DCT, NİM)

Dönüşüm alanı yöntemleri, ses sinyalini Ayrık Kosinüs Dönüşümü (**DCT**) veya Ayrık Dalgacık Dönüşümü (**ADD**) gibi matematiksel bir dönüşüm kullanarak farklı bir gösterime dönüştürdükten sonra veriyi gömer.

- **ADD** tabanlı gömme, çok çözünürlüklü zaman–frekans ayrışımından yararlanır ve gizli verinin algısal olarak daha az hassas frekans bantlarına karşılık gelen katsayılara yerleştirilmesine olanak tanır (Mallat, 1989).
- **DCT** tabanlı yöntemler genellikle sıkıştırma standartlarıyla uyumludur ve dayanıklılık ile algısal kalite arasında denge kurmak amacıyla veriyi orta frekans katsayılarına gömer (Bender ve ark., 1996).
- Nicemleme İndeks Modülasyonu (**NİM**), gömülecek bite bağlı olarak dönüşüm katsayılarının nicemleme seviyelerini değiştirir ve böylece dayanıklılık–bozulma dengesi üzerinde sistematik kontrol sağlar (Chen & Wornell, 2001).

Dönüşüm alanı yaklaşımları genellikle zaman alanı yöntemlerine göre daha dayanıklıdır; ancak daha yüksek hesaplama karmaşıklığına sahiptir ve hem ileri hem de ters dönüşümlerin uygulanmasını gerektirir.

NİM Örneği

Orijinal Katsayı: 5.72

Gömülecek Bit: 1

NİM: floor(5.72 / delta) + delta/2 => 5.5 (if delta = 1.0)

4.3.4. Yayılı Spektrum Teknikleri

Yayılı spektrum teknikleri, gömülü mesajı sahte rastgele diziler kullanarak geniş bir frekans bandına dağıtır ve bu yönüyle yayılı spektrum haberleşme sistemlerine benzer. Doğrudan Dizili Yayılı Spektrum (**DSSS**) ve frekans atlamalı yöntemler bu yaklaşıma örnek olarak verilebilir. Bu yöntemlerin başlıca avantajı, gürültülü veya düşmanca ortamlarda yüksek dayanıklılık ve düşük tespit edilme olasılığı sağlamasıdır. Bununla birlikte gömme kapasitesi görece düşüktür ve uygulama karmaşıklığı daha yüksektir (Petitcolas et al., 1999). Bu nedenle bu yaklaşımlar, yüksek kapasiteli steganografiden ziyade daha çok sağlam sayısal damgalama (watermarking) uygulamalarıyla ilişkilendirilir ve bu tez kapsamında tercih edilmemiştir.

[Mesaj Biti] → [Sahte Rastgele Dizi] → [Sinyalde Geniş Bantlı Yayılım]

4.3.5. Yankı Gizleme Teknikleri

Yankı gizleme yöntemleri, gizli veriye göre yankı gecikmesi, genliği veya fazı gibi parametreleri değiştirerek ses sinyaline çok hafif yankılar eklenmesi prensibine dayanır. Bu yaklaşımın avantajı, yankıların orta düzey sinyal işleme ve sıkıştırma işlemlerinden sonra bile korunabilmesi sayesinde gürültü ve sıkıştırmaya karşı iyi bir dayanıklılık sağlamasıdır. Ancak gömme hızı sınırlıdır ve algılanamaz kalabilmesi için yankı parametrelerinin çok hassas biçimde ayarlanması gerekir (Bender et al., 1996). Bu nedenle bu yöntemler sağlam sayısal damgalama uygulamaları için uygun olsa da yüksek veri yükü gerektiren durumlar için daha az elverişlidir.

[Orijinal Ses] + [Gecikmesi = Veri Bitini Gösteren Zayıf Yankı]

4.3.6. Uyarlamalı ve İstatistiksel Teknikler

Uyarlamalı steganografik yöntemler, gömme stratejisini yerel sinyal özelliklerine veya istatistiksel modellere göre dinamik olarak ayarlar. Uyarlamalı **LSB** ve modele dayalı gömme bu yaklaşıma örnek verilebilir. Bağlama duyarlı gömme sayesinde istatistiksel izler azaltıldığı için tespit edilmeleri daha zordur. Ancak yüksek hesaplama maliyeti ve uygulama karmaşıklığına sahiptir ve bu durum hafif Python tabanlı sistemler ile gerçek zamanlı kısıtlar açısından uyumsuzluk oluşturabilir (Fridrich, 2009). Bu nedenle uyarlamalı stratejiler algılanabilirliği azaltma açısından güçlü olsa da hesaplama açısından yoğun yöntemlerdir.

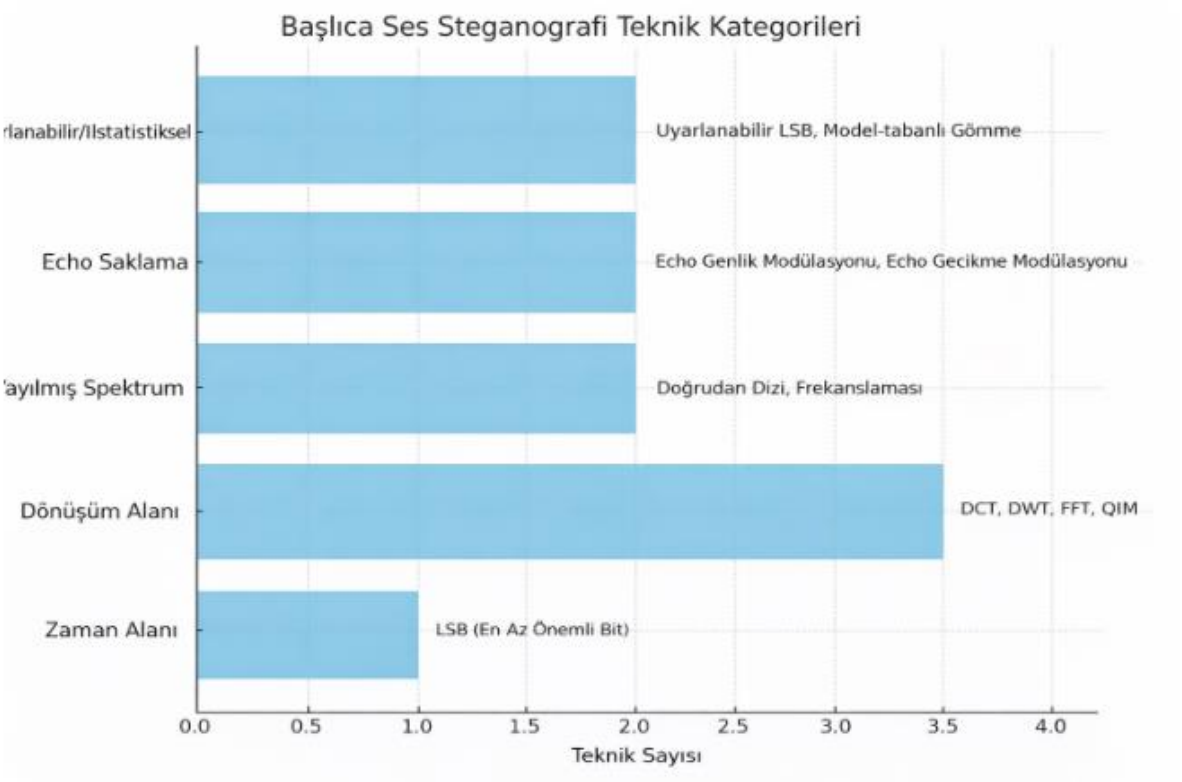
4.4. TEKNİKLER ARASINDAKİ ÖDÜNLEŞİMLERİN ÖZETİ

Yukarıda incelenen teknikler; dayanıklılık, kapasite ve karmaşıklık açısından özetlenebilir. Bu ödünleşimlere ilişkin karşılaştırmalı özet Tablo 4.1'de sunulmaktadır.

Tablo 4.1: Ses steganografisi tekniklerinin dayanıklılık, kapasite ve hesaplama karmaşıklığı açısından karşılaştırmalı özeti. Petitcolas ve ark. (1999), Johnson & Katzenbeisser (2000), Chan & Cheng (2004) çalışmalarından uyarlanmıştır

Kategori	Temel Teknikler	Dayanıklılık	Kapasite	Karmaşıklık
Zaman Alanı	LSB	Düşük	Yüksek	Düşük
Dönüşüm Alanı	ADD, DCT, NİM	Yüksek	Orta	Orta–Yüksek
Yayılı Spektrum	DSSS, Frekans Atlamalı	Çok Yüksek	Düşük	Yüksek
Yankı Gizleme	Yankı Gecikmesi/Genlik Modülasyonu	Yüksek	Düşük	Orta
Uyarlamalı/İstatistiksel	Uyarlamalı LSB, Modelle Tabanlı	Orta	Orta	Yüksek

Bu analitik karşılaştırma, bu tezde dönüşüm alanı tabanlı bir yöntemin tercih edilmesinin gerekçesini ortaya koymaktadır; özellikle **ADD** ve **NİM** kullanılarak dayanıklılık, kapasite ve algısal şeffaflık arasında pratik bir denge elde edilmesi amaçlanmıştır.



Şekil 4.3: ADD alanındaki gömme stratejilerinin kavramsal karşılaştırması; **LSB** tabanlı yöntemlerin sınırlamalarını ve NİM'in avantajlarını vurgulamaktadır.

4.5. ADD ALANINDA GÖMME STRATEJİLERİ

(Bu bölümde "**LSB + ADD** Sınırlamaları" artık sonuçlar kısmı olarak değil, deneylerin ileriki bir bölümde verileceği belirtilerek kuramsal bir analiz olarak ele alınmaktadır.)

Bu tezde önerilen sistem, gizli veriyi **ADD** alanında gömmektedir. Kavramsal olarak iki temel yaklaşım mümkündür: **LSB** yerine koyma yönteminin dönüşüm alanına genişletilmesi ve Nicemleme İndeks Modülasyonu (**NİM**) kullanımı. Bu bölüm, **ADD** katsayıları üzerinde çalışılırken **NİM**'in LSB'ye tercih edilmesinin kuramsal gerekçesini ortaya koymaktadır. Şekil 4.3'te kavramsallaştırıldığı üzere, **NİM** doğrudan **LSB** manipülasyonuna kıyasla dönüşüm alanında daha kararlı bir gömme stratejisi sunmaktadır.

4.5.1. ADD Alanında LSB'nin Kuramsal Sınırlamaları

LSB yerine koyma yöntemi zaman alanında uygulanması kolay ve cazip olsa da, **ADD** katsayılarına genişletilmesi kuramsal açıdan sorunludur. Dalgacık katsayıları genellikle kayan noktalı sayılarla temsil edilir ve bu katsayıların en düşük anlamlı bitlerine veri gömmek çeşitli problemlere yol açar. Öncelikle, **ADD** ve ters dönüşüm süreçlerinde uygulanan filtreleme ve aşağı örnekleme işlemleri yuvarlama ve yaklaşım hataları üretir; bu durum katsayıların en düşük anlamlı bitlerini değiştirerek ileri ve geri dönüşümler arasında gömülü verinin kararsız hâle gelmesine neden olur (Mallat, 1989; Selesnick, 2001). Ayrıca dalgacık filtreleri enerjiyi katsayılar arasında yeniden dağıttığından, **LSB** düzeyindeki değişiklikler katsayı uzayındaki doğal dalgalanmalar tarafından maskelenebilir veya bozulabilir ve güvenilir çıkarımı zorlaştırır. Bunun yanında **LSB** gömme yaklaşımı katsayıları yalnızca bit taşıyıcı kaplar olarak ele alır ve dönüşüm alanındaki yapısal anlamlarını göz ardı eder; bu uyumsuzluk sağlamlık ve güvenilirlik açısından düşük kuramsal güvence doğurur (Fridrich, 2009). Bu nedenlerle literatürde **LSB** gömme yönteminin dönüştürülmüş katsayı alanlarından ziyade ham örnek alanları için daha uygun olduğu kabul edilmektedir.

4.5.2. ADD Alanında NİM'in Avantajları

Nicemleme İndeks Modülasyonu (**NİM**), **ADD** katsayılarına veri gömmek için daha ilkeli bir çerçeve sunar. En düşük anlamlı bitleri doğrudan değiştirmek yerine, gömülecek bit değerlerine göre katsayıların nicemlenmesini modüle eder. Nicemleme indeksleri düzeyinde çalıştığı için işlem sırasında oluşan küçük bozunumların gömülü bilgiyi değiştirme olasılığı daha düşüktür (Chen & Wornell, 2001). Ayrıca nicemleme, dönüşüm alanı tabanlı birçok kodlama şemasında zaten kullanılan standart bir işlemdir; bu nedenle kontrollü nicemleme ile gömme yaklaşımı **ADD** katsayılarının istatistiksel yapısıyla doğal biçimde uyumludur. Bunun yanında nicemleyici adım büyüklüğü **Δ** ayarlanarak dayanıklılık ile algısal bozulma arasında dengeli bir ödünleşim sağlanabilir ve gömme süreci sistematik olarak kontrol edilebilir. Bu özellikler **NİM**'i dönüşüm alanı steganografisi için özellikle uygun kılmakta ve bu tezde temel gömme tekniği olarak seçilmesini gerekçelendirmektedir.

4.5.3. Kavramsal Karşılaştırma: ADD + LSB ve ADD + NİM

Yukarıda sunulan teorik analiz temel alındığında; **ADD** tabanlı LSB ve **ADD** tabanlı NİM olmak üzere iki gömme stratejisi; dayanıklılık, kapasite, saptanabilirlik ve pratik ses stegonografisine uygunluk gibi birkaç temel boyut üzerinden sistematik olarak karşılaştırılabilir. Bu karşılaştırma Tablo 4.2'de özetlenmiştir.

Tablo 4.2: Ses stegonografisinde **ADD** tabanlı LSB gömme ile **ADD** tabanlı NİM gömme yöntemlerinin kavramsal karşılaştırması

Özellik	**ADD + LSB**	**ADD + NİM**
Uygulama Basitliği	Basit ve uygulanması kolaydır.	Nispeten daha karmaşıktır; kuantalama (quantization) ve hassas hesaplamalar gerektirir.
Kapasite	Nispeten yüksek (çok sayıda bit gömülebilir).	Orta ile düşük arası; kuantalama adımına Δ bağlıdır.
Gürültüye Karşı Dayanıklılık	Zayıf – küçük değişiklikler veriyi bozabilir.	Güçlü – sıkıştırma veya bozulmadan sonra bile mesaj geri kurtarılabilir.
Saptanabilirlik (Steganaliz)	Spektral veya istatistiksel analiz araçlarıyla kolayca tespit edilebilir.	Sistematik kuantalama gömme yapısı nedeniyle tespit edilmesi daha zordur.
ADD ile Entegrasyon	Zayıf – LSB zaman etki alanında (time domain) daha iyi çalışır.	Güçlü – ADD katsayı yapısıyla doğal olarak uyumludur.
Gömme Sonrası Ses Kalitesi	Küçük mesajlar için iyi, büyük verilerde kalite düşer.	Kontrollü gömme sayesinde genel kalite daha iyidir.
Geri Getirme Doğruluğu	Güvenilmez – yuvarlama ve dönüşümlerden etkilenir.	Yüksek – eğer Δ (kuantalama adımı) iyi seçilirse, veri güvenilir bir şekilde geri kurtarılabilir.
Gerçek Uygulamalar İçin Uygunluk	Güvenli veya kritik kullanımlar için önerilmez.	Güvenli ve dayanıklı uygulamalar için uygundur.

Bu tez çalışmasında, yukarıda belirtilen nedenlerle ana gömme stratejisi olarak **ADD** + **NİM** yöntemi benimsenmiştir. Yukarıda ana hatları çizilen tasarım tercihleri, önerilen sistemin performansının **PSNR** (**Tepeden Tepeye Sinyal-Gürültü Oranı**), **BER** (**Bit Hata Oranı**) ve gömme kapasitesi parametreleri kullanılarak nicel olarak değerlendirildiği bir sonraki bölümde sunulan deneysel sonuçlarla da desteklenmektedir.

5. ŞİFRELEME

5.1. SES STEGANOGRAFİSİNDE ŞİFRELEMENİN ROLÜ

Tezinizin bu bölümü için verdiğiniz metni, akademik üslubu ve teknik terimleri koruyarak Türkçeye çevirdim. **GŞS** (**AES**) ve **ŞBZ** (**CBC**) gibi kısaltmaları, Türkçe literatürdeki karşılıklarıyla (**Gelişmiş Şifreleme Standardı ve Şifre Blok Zincirleme**) uyumlu hale getirdim.

Steganografi tek başına gizli mesajın varlığını gizler, ancak gömülen verinin açığa çıkması durumunda mesajın gizliliğini garanti etmez. Bu nedenle, saptanma durumunda mesaj güvenliğini sağlamak amacıyla gömme işleminden önce şifreleme sürece dahil edilir. Önce şifreleme, ardından steganografi uygulanan bu katmanlı güvenlik modeli, yüksek güvenlikli bilgi gizleme sistemlerinde yaygın olarak kullanılmaktadır (Katzenbeisser & Petitcolas, 2000).

Bu tez çalışmasında, **ADD–NİM** steganografik gömme işleminden önce **ŞBZ (CBC)** modunda **GŞS (AES)** şifrelemesi uygulanmıştır; böylece gizli veri ayıklansa bile, şifreleme anahtarı ve başlatma vektörü (**IV**) olmadan anlamsız kalması sağlanmıştır (Daemen & Rijmen, 2002).

Steganografi mesajı gizler, şifreleme ise onu korur. Bu iki yöntem birlikte "derinlemesine savunma" (**defense-in-depth**) stratejisini oluşturur. Sadece steganografi kullanımı ile şifreleme destekli steganografi arasındaki kısa bir karşılaştırma Tablo 5.1'de sunulmuştur.

Tablo 5.1: Gizlilik ve pratik güvenlik açısından yalnızca steganografi ile şifreleme destekli steganografinin karşılaştırması

Özellik	**Yalnızca Steganografi**	**Steganografi + Şifreleme**
Gizli mesaj keşfedilirse	Mesaj okunabilir	Anahtar olmadan içerik anlaşılamaz
Mesaj koruması	Sadece gizlemeye dayanır	Keşfedilse bile güvenliğini korur
Sıkıştırma/değişikliklere karşı dayanıklılık	Mesaj bitleri bozulabilir	Bitler bozulsa bile anahtar olmadan veri anlamsız kalır
Hassas uygulamalara uygunluk	Tek başına yeterli değildir	Güvenli ve gizli iletişim için önerilir

Steganografinin şifreleme ile birleştirilmesi, gizli veri tespit edilse bile anahtar olmadan içeriğinin anlaşılamaz kalmasını sağlar ve yalnızca gizlemeye dayanan yaklaşıma göre daha güçlü bir gizlilik koruması sunar. Bu katmanlı tasarım, bu nedenle hassas veya güvenli iletişim için tek başına steganografi kullanımına kıyasla daha uygundur.

5.2. GŞS (GELİŞMİŞ ŞİFRELEME STANDARDI)

GŞS, NIST tarafından standartlaştırılmış simetrik bir blok şifreleme algoritmasıdır ve **128** bitlik bloklar üzerinde **128, 192** veya **256** bit uzunluğunda anahtarlarla çalışacak şekilde tasarlanmıştır. Bu tezde, hesaplama verimliliği ile yüksek güvenlik arasında dengeli bir yapı sunduğu için **GŞS-128** kullanılmıştır.

5.2.1. Sonlu Alan Gösterimi GF(2^8)

GŞS'de tüm aritmetik işlemler sonlu alan **GF**(2^8) içinde gerçekleştirilir. Bu alanda her bayt (**8** bit), ikili katsayılara (yani katsayıları $\mathbb{Z}_2$ içinde olan) sahip en fazla yedinci dereceden bir polinom olarak temsil edilir. Alan aşağıdaki şekilde tanımlanır:

$$\mathbf{GF(2^8) = \mathbb{Z}_2[x] / (x^8 + x^4 + x^3 + x + 1)}$$

Bu ifade, polinomların ikili alan üzerinde oluşturulduğunu ve indirgenemez (**irreducible**) aşağıdaki polinom ile mod alınarak sadeleştirildiğini belirtir:

$$\mathbf{x^8 + x^4 + x^3 + x + 1}$$

Bu polinom onaltılık (**hexadecimal**) gösterimde **0x11B** değerine karşılık gelir. Bu polinomun kullanılması, alandaki her sıfırdan farklı elemanın tekil bir çarpımsal tersi olmasını garanti eder. Bu özellik, **GŞS**'de tersinir dönüşümlerin gerçekleştirilebilmesi için kritik öneme sahiptir; özellikle SubBytes ve MixColumns adımlarında gereklidir. Bu polinom tabanlı alan yapısı olmadan **GŞS** tersinirliği garanti edemez ve güvenli çözme işlemi matematiksel olarak mümkün olmazdı.

5.3. GŞS İÇ ŞİFRELEME İŞLEMLERİ

5.3.1. Matematiksel İfadeler

AddRoundKey:

State_new = State $\oplus$ RoundKey

Burada $\oplus$ işleci bit düzeyinde XOR işlemini ifade eder.

SubBytes:

State[i][j] = SBox(State[i][j])

(Rijndael S-Box kullanılarak)

MixColumns:

NewColumn =

NewColumn =

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \cdot \begin{bmatrix} s_0 \\ s_1 \\ s_2 \\ s_3 \end{bmatrix}$$

Buradaki çarpma işlemi **GF(2^8)** alanında polinom çarpımıdır.

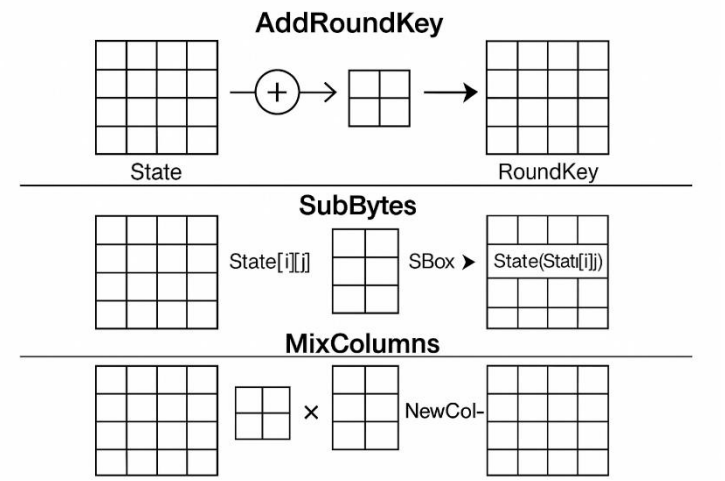
GŞS algoritmasındaki tur sayısı, güvenlik ile hesaplama verimliliği arasında denge kurmak amacıyla anahtar uzunluğu ile doğrudan ilişkilidir. Daha uzun anahtarlar, kriptanalitik saldırılara karşı direnci artırmak için ek turlar gerektirirken, daha kısa anahtarlar daha az tur ile yeterli güvenlik sağlayabilir. Bu çalışmada, steganografik gömme sırasında çalışma süresini optimize ederken yeterli kriptografik dayanıklılığı korumak amacıyla **GŞS-128** tercih edilmiştir. Anahtar uzunluğu ile şifreleme tur sayısı arasındaki ilişki Tablo 5.2'de özetlenmiştir.

Tablo 5.2: Anahtar uzunluğuna bağlı **GŞS** şifreleme tur sayısı.

Tur Sayısı	**Anahtar Uzunluğu**	**GŞS Sürümü**
10 tur	128 bit	GŞS-128
12 tur	192 bit	GŞS-192
14 tur	256 bit	GŞS-256

Bu çalışmada, steganografik gömme sırasında çalışma süresini optimize etmek amacıyla **GŞS-128** kullanılmıştır.

GŞS şifreleme algoritması, hem karmaşıklığı (confusion) hem de yayılımı (diffusion) artırmak için doğrusal ve doğrusal olmayan dönüşümlerin bir dizisini uygular. SubBytes adımı S-Box tablo araması kullanarak doğrusal olmayanlık kazandırır, MixColumns **GF(2^8)** alanında matris çarpımı ile her baytın etkisini bulunduğu sütun boyunca yayar ve AddRoundKey bit düzeyinde **XOR** işlemi ile şifreleme anahtarını güvenli biçimde entegre eder.



Şekil 5.1: GŞS şifreleme sürecinin iç dönüşüm aşamalarını gösteren, durum matrisi üzerinde uygulanan SubBytes, ShiftRows, MixColumns ve AddRoundKey işlemlerinin şematik gösterimi.

Şekil 5.1, şifreleme turları sırasında **GŞS** durum matrisinin iç dönüşüm aşamalarını göstermektedir. Her turda doğrusal olmayanlığı sağlamak için SubBytes, tüm sütunları dönüştürerek yayılımı artırmak için MixColumns ve tur anahtarını bit düzeyinde **XOR** ile güvenli biçimde birleştirmek için **AddRoundKey** uygulanır. Bu işlemler birlikte, **GŞS**'nin kriptanalize karşı dayanıklılığının temelini oluşturur.

GŞS, her turda bir dizi dönüşüm aşaması uygulayan ve State adı verilen 4×4 baytlık bir matris üzerinde çalışır; bu aşamalar Tablo 5.3'te özetlenmiştir.

Tablo 5.3: GŞS şifreleme algoritmasının temel dönüşüm aşamaları ve işlevsel rolleri.

Dönüşüm	**İşlevi**
SubBytes	S-Box kullanılarak doğrusal olmayan yer değiştirme
ShiftRows	Satır bazlı döngüsel kaydırmalar
MixColumns	GF(2^8) alanında matris çarpımı
AddRoundKey	Tur anahtarı ile **XOR** işlemi

5.4. GŞS'DE ÇALIŞMA MODLARI VE SES STEGANOGRAFİSİ İLE İLİŞKİLERİ

Gelişmiş Şifreleme Standardı (**GŞS**)'nin pratik uygulamalarında, blok tabanlı şifreleme belirli çalışma modları kullanılarak daha büyük veri dizilerine genişletilir. Bu modlar, her bir **128** bitlik şifrelenmiş bloğun komşu bloklarla nasıl etkileşime girdiğini belirler ve sistemin gizliliğini ile dayanıklılığını doğrudan etkiler.

En yaygın kullanılan çalışma modları şunlardır:

• **Electronic Codebook (ECB):** Her bloğu, önceki şifreleme çıktısına başvurmadan bağımsız olarak şifreler. Hesaplama açısından basit olmasına rağmen bu bağımsızlık tekrarlayan desenlerin ortaya çıkmasına neden olur ve bu nedenle güvenli uygulamalar için uygun değildir (Ferguson vd., 2010).

• **Cipher Block Chaining (ŞBZ):** Her açık metin bloğu, rastgele bir Başlatma Vektörü (**IV**) kullanılarak önceki şifreli blok ile birleştirilir ve birlikte işlenir. Bu bağımlılık, aynı açık metin girişlerinin farklı şifreli çıktılar üretmesini sağlayarak istatistiksel düzenlilikleri bastırır ve trafik analizine karşı direnci artırır.

• **CFB, OFB ve CTR:** Genellikle gerçek zamanlı veya düşük gecikmeli ortamlarda uygulanan akış yönelimli yapılandırmalardır. Belirli uygulamalar için uygun olmakla birlikte, bu tez kapsamında uygulama ve senkronizasyon kısıtları nedeniyle tercih edilmemiştir.

5.5. ŞBZ MODUNUN SEÇİLME GEREKÇESİ

Ses steganografisinin örtük doğası ve gizli verinin çıkarılma olasılığı göz önüne alındığında, veri keşfedildikten sonra bile şifrelemenin etkili kalması gerekir. Bu nedenle şifreleme modunun seçimi, gizliliğin korunması ve istatistiksel sızıntının önlenmesi açısından kritik bir rol oynar. Bu bağlamda Cipher Block Chaining (**ŞBZ**) modu, Electronic Codebook (**ECB**) moduna kıyasla önemli avantajlar sunar.

ŞBZ'nin **ECB**'ye göre uygunluğunu vurgulayan karşılaştırmalı analiz Tablo 5.4'te sunulmuştur.

Tablo 5.4: Güvenlik ve veri bağımlılığı açısından ECB ve ŞBZ çalışma modlarının karşılaştırılması.

Kriter	**GŞS-ECB**	**GŞS-ŞBZ**
Blok Bağımlılığı	Yok – bağımsız şifreleme	Her blok önceki şifreli bloğa bağlıdır
Güvenlik Seviyesi	Desen açığa çıkmasına karşı zayıf	Yüksek – tekrar eden şifreleme izlerini engeller
IV Kullanımı	Gerekli değil	Her şifreleme için gereklidir
İstatistiksel Analize Karşı Dayanıklılık	Düşük	Yüksek
Ses Steganografisine Uygunluk	Sınırlı, temel koruma sağlar	Güvenli gömme için yüksek derecede önerilir

ECB tabanlı şifreleme, şifrelenmiş çıktı içinde tekrar eden desenlerin tanınmasına izin vererek örtük iletişimin temel amacını zayıflatır. Buna karşılık **ŞBZ** modu, zincirleme yapıyı ve rastgele oluşturulan bir başlatma vektörünü (**IV**) entegre ederek istatistiksel izlerin ortadan kaldırılmasını sağlar ve mesaj çıkarılsa bile gizliliğin korunmasına olanak tanır.

ŞBZ modu, aynı açık metin bölümleri için farklı şifreli metin değerleri üreterek korelasyonu etkili biçimde gizler ve tespit edilme olasılığını önemli ölçüde azaltarak steganografik gizliliği daha da artırır.

Bu nedenlerle, bu tezde **ADD-NİM** kullanılarak gerçekleştirilen gömme işleminden önce **GŞS-ŞBZ** tercih edilmiş ve böylece steganografinin gizleme özelliklerini tamamlayan kriptografik olarak güvenli bir çerçeve sağlanmıştır.

5.6. GÜVENLİK VARSAYIMLARI VE TEHDİT MODELİ

Bu tez, önerilen ses steganografisi çerçevesinin hangi güvenlik varsayımları altında değerlendirildiğini açıklığa kavuşturmak amacıyla açık bir tehdit modeli benimsemektedir. Modelin amacı, tüm saldırı senaryolarına karşı evrensel direnç iddiasında bulunmak değil, raporlanan sonuçları bağlam içine yerleştirmektir.

Ele alınan saldırganın pasif bir saldırgan olduğu varsayılmaktadır; yani stego-ses sinyaline erişimi vardır ancak **GŞS-ŞBZ** şifreleme aşamasında kullanılan gizli anahtara veya başlatma vektörüne (**IV**) sahip değildir. Kerckhoffs ilkesine uygun olarak saldırganın gömme ve çıkarma algoritmalarının tamamını bildiği kabul edilir, ancak uyarlamalı ya da seçilmiş mesaj oracle'larına erişimi yoktur.

Bu tehdit modeli kapsamında steganografinin rolü, gizli mesajın varlığını saklayarak tespit edilme olasılığını azaltmaktır; **GŞS-ŞBZ** şifrelemesi ise gömülü verinin kısmen ya da tamamen çıkarılması durumunda mesaj gizliliğini korumak için kullanılmaktadır. Dolayısıyla gizliliğin esas olarak kriptografik katmana dayandığı, saklamanın ise dönüşüm alanı tabanlı gömme yöntemi ile sağlandığı varsayılmaktadır.

Önerilen sistemin aktif saldırılara (kasıtlı sinyal manipülasyonu, uyarlamalı steganaliz veya anahtar yönetimini hedef alan kriptografik saldırılar gibi) karşı dayanıklı olacak şekilde tasarlanmadığı özellikle belirtilmelidir. Ayrıca kayıplı sıkıştırma, yeniden örnekleme, filtreleme veya gürültü ekleme gibi işlemlere karşı dayanıklılık bu tehdit modeli kapsamında ele alınmamış olup, gelecekteki çalışmalar için bir araştırma yönü olarak belirlenmiştir.

6. ÖNERİLEN YÖNTEM VE GERÇEKLEŞTİRİM

Önerilen ses steganografisi çerçevesi, kriptografik gizliliği (**GŞS-ŞBZ**) dalgacık dönüşüm alanında algısal gömme (**ADD–NİM**) ile bütünleştirir. Bu bölüm, bilgi saklama ve işaret işleme literatüründe önerildiği üzere (Mallat, 1989; Daemen & Rijmen, 2002; Petitcolas vd., 1999; Chen & Wornell, 2001) sistem mimarisi diyagramları, akış şemaları ve sinyal ayrışım gösterimleri ile desteklenen kapsamlı bir yöntemsel genel bakış sunmaktadır.

6.1. YAZILIM ORTAMI VE KÜTÜPHANELER

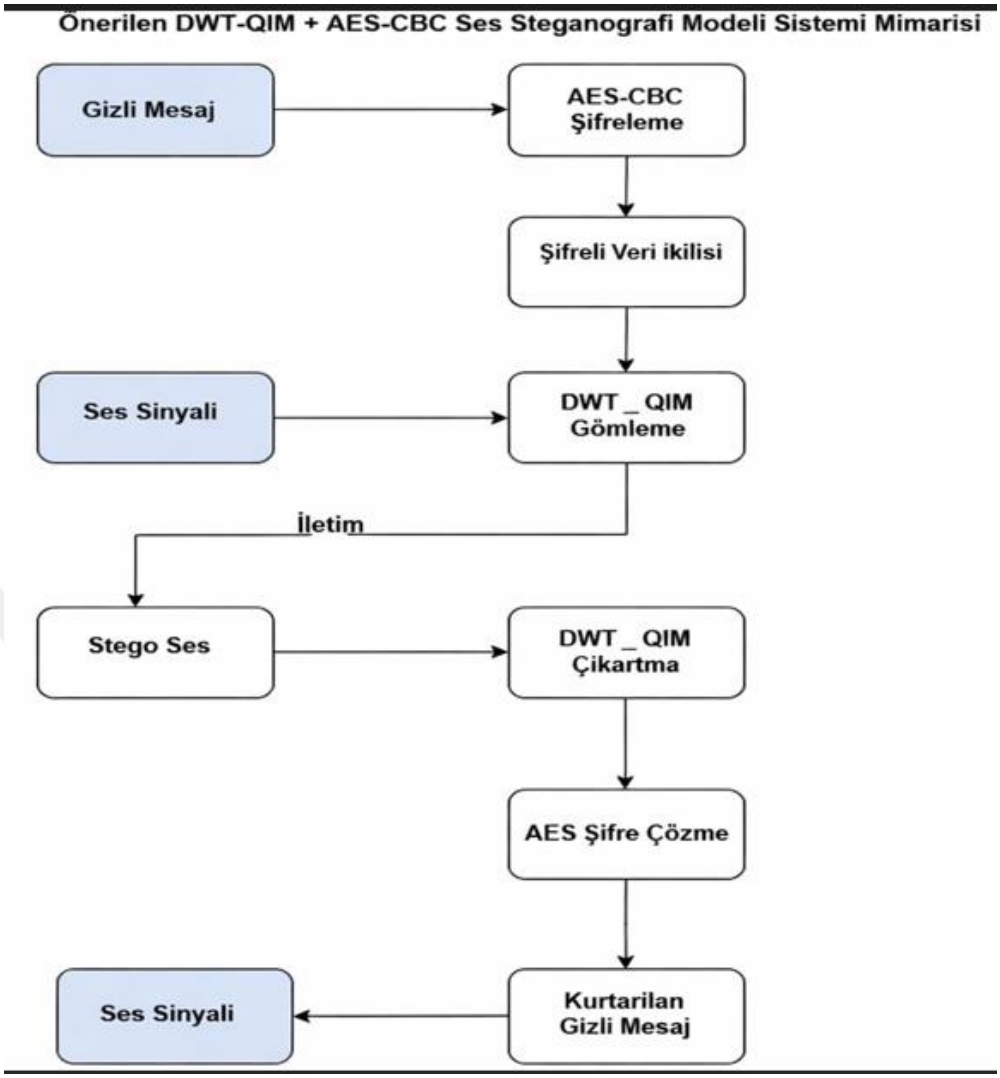
Önerilen çerçeve **Python 3.x** ortamında gerçekleştirilmiş olup, olgun bilimsel ekosistemi ve açık modüler yapısından yararlanılmıştır. Birden fazla kütüphane koordineli biçimde kullanılmıştır. PyWavelets, ses sinyalleri üzerinde Ayrık Dalgacık Dönüşümü (**ADD**) ve ters **ADD** işlemlerini gerçekleştirmek için kullanılmıştır. NumPy, örnek dizileri ve dalgacık katsayıları üzerindeki sayısal işlemleri yürütmüştür. PyCryptodome, dolgulama, anahtar yönetimi ve **IV** üretimi dâhil olmak üzere Şifre Blok Zincirleme (**GŞS-128**, **ŞBZ** modu) şifrelemesini uygulamıştır. Standart **WAV** giriş/çıkış araçları **16-bit PCM** ses dosyalarının okunması ve yazılması için kullanılmış, Matplotlib ise geliştirme sürecinde ara sonuçların görselleştirilmesi ile **PSNR** ve **BER** grafiklerinin oluşturulmasında kullanılmıştır.

Bu bileşenlerin modüler tutulması, kriptografik katmanın, dalgacık alanı gömme yönteminin ve değerlendirme hattının birbirinden bağımsız biçimde değiştirilmesine veya genişletilmesine olanak sağlamaktadır.

6.2. SİSTEMİN MİMARİSİ

Genel sistem mimarisi Şekil 6.1'de gösterilmekte olup, şifreleme, dalgacık alanı sinyal işleme, Kuantalama İndeks Modülasyonu (**NİM**) ile gömme ve alıcı tarafındaki karşılık gelen çıkarma ile çözme süreçleri arasındaki etkileşimi ortaya koymaktadır.

Sistem, gizli mesajın önce Şifre Blok Zincirleme (**GŞS-ŞBZ**) modunda şifrelenmesiyle başlayan çok aşamalı bir işlem hattı olarak çalışır. Elde edilen şifreli bit akışı daha sonra ses dosyasının seçilen **ADD** detay katsayıları içerisine gömülür. Alıcı tarafında ise gizlenen mesajı geri elde etmek için ters işlemler uygulanır.



Şekil 6.1: Önerilen ses steganografisi çerçevesinin sistem mimarisi: **GŞS-ŞBZ** şifrelemesinin **ADD–NİM** gömme ve çıkarma süreçleriyle bütünleştirilmesi

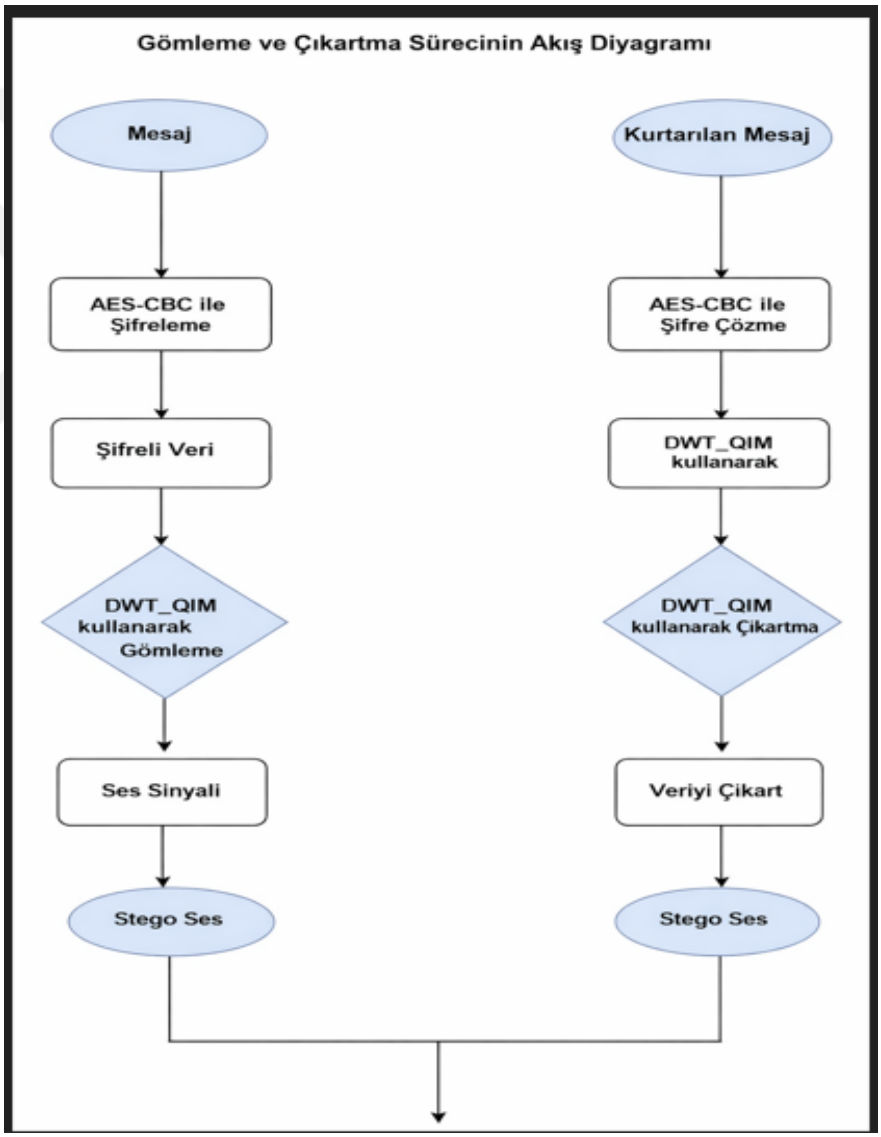
Önerilen sistem, kriptografik ve dönüşüm alanı işlemlerini birleşik bir mimari içinde bütünleştirir.

Şekil 6.1, **GŞS-ŞBZ** şifrelemesi ile **ADD–NİM** gömme ve çıkarma süreçlerini entegre eden önerilen ses steganografisi çerçevesinin genel mimarisini göstermektedir. Süreç, giriş gizli mesajıyla başlar; bu mesaj gömme işleminden önce veri gizliliğini sağlamak amacıyla öncelikle **GŞS-ŞBZ** algoritması kullanılarak şifrelenir. Bu adım sonucunda ikili (binary) bir şifreli yük elde edilir.

The encrypted data is then embedded into the cover audio signal using the **ADD–NİM** method, which relies on wavelet-domain decomposition and Quantization Index Modulation. Şifrelenmiş veri daha sonra dalgacık alanı ayrıştırmasına ve Nicemleme İndeks

Modülasyonu'na dayanan **ADD–NİM** yöntemi kullanılarak örtü ses sinyali içine gömülür. Bu işlem sonucunda iletişim kanalı üzerinden iletilen stego ses elde edilir.

Alıcı tarafında sistem, stego sesten gizlenmiş şifreli bitleri çıkarmak için ters **ADD–NİM** sürecini gerçekleştirir. Elde edilen veri daha sonra **GŞS** kullanılarak çözülür ve özgün gizli mesaj geri kazanılır. Mimari diyagramda gösterildiği gibi, önerilen gömme stratejisi algısal kaliteyi korurken sistem hattının işlevsel doğruluğunu sürdürmeyi amaçlamaktadır. Bu davranışın nesnel değerlendirmesi bir sonraki bölümde sunulmaktadır.



Şekil 6.2: GŞS-ŞBZ şifrelemeli önerilen **ADD–NİM** ses steganografisi çerçevesinde gömme ve çıkarma süreçlerinin akış diyagramı .

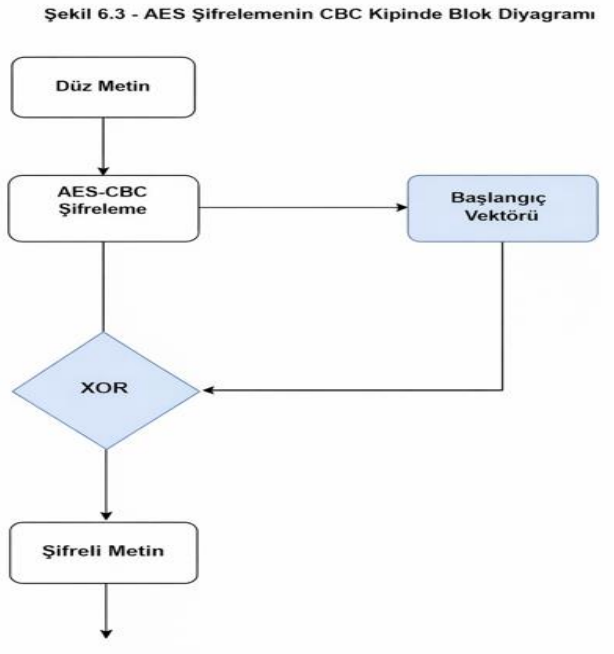
- **Akış Diyagramı Açıklaması**

Süreç, açık metin mesajı ile başlar ve bu mesaj öncelikle güvenli bir ikili veri yükü elde etmek amacıyla **GŞS-ŞBZ** algoritması kullanılarak şifrelenir. Elde edilen şifreli veri daha sonra **ADD–NİM** yöntemi ile ses sinyali içerisine gömülerek iletime hazır stego ses üretilir. Şekil 6.2'de görüldüğü üzere gömme ve çıkarma işlemleri simetrik ve düzenli bir işlem hattını takip etmektedir.

Çıkarma aşamasında sistem, alınan stego sese ters **ADD–NİM** sürecini uygulayarak gömülü bitleri geri elde eder. Kurtarılan ikili veri daha sonra **GŞS-ŞBZ** ile çözülür ve özgün mesaj yeniden oluşturulur. Akış diyagramı, gömme ve çıkarma aşamaları arasındaki simetriyi vurgulayarak kriptografik gizlilik ile kontrollü koşullar altında yapılandırılmış ve tekrarlanabilir bir çıkarma sürecinin birlikte çalıştığı tutarlı ve geri döndürülebilir bir sistem hattı sunulduğunu göstermektedir.

- **GŞS-ŞBZ Şifreleme Süreci**

ŞBZ (Cipher Block Chaining) kipinde çalışan **GŞS**, her şifreli metin bloğunun hem karşılık gelen açık metne hem de bir önceki şifreli metin bloğuna bağlı olmasını sağlayarak kriptografik güvenlik sunar. Böylece **ECB** gibi daha zayıf kiplerde görülen tekrar örüntülerinin oluşması engellenir (Ferguson, Schneier & Kohno, 2010).



Şekil 6.3: GŞS-ŞBZ şifreleme sürecinin blok diyagramı: blok zincirleme yapısı, başlatma vektörü (**IV**) ile **XOR** işlemleri ve ardışık şifreli metin üretimini göstermektedir.

ŞBZ kipi, yayılımı artıran ve istatistiksel sızıntıyı bastıran kriptografik bir zincirleme yapısı sağlar.

GŞS-ŞBZ Şifreleme Blok Diyagramının Açıklaması

Şekil 6.3'te, Şifre Blok Zincirleme (**ŞBZ**) kipinde çalışan **GŞS** şifreleme sürecinin işleyişi gösterilmektedir.

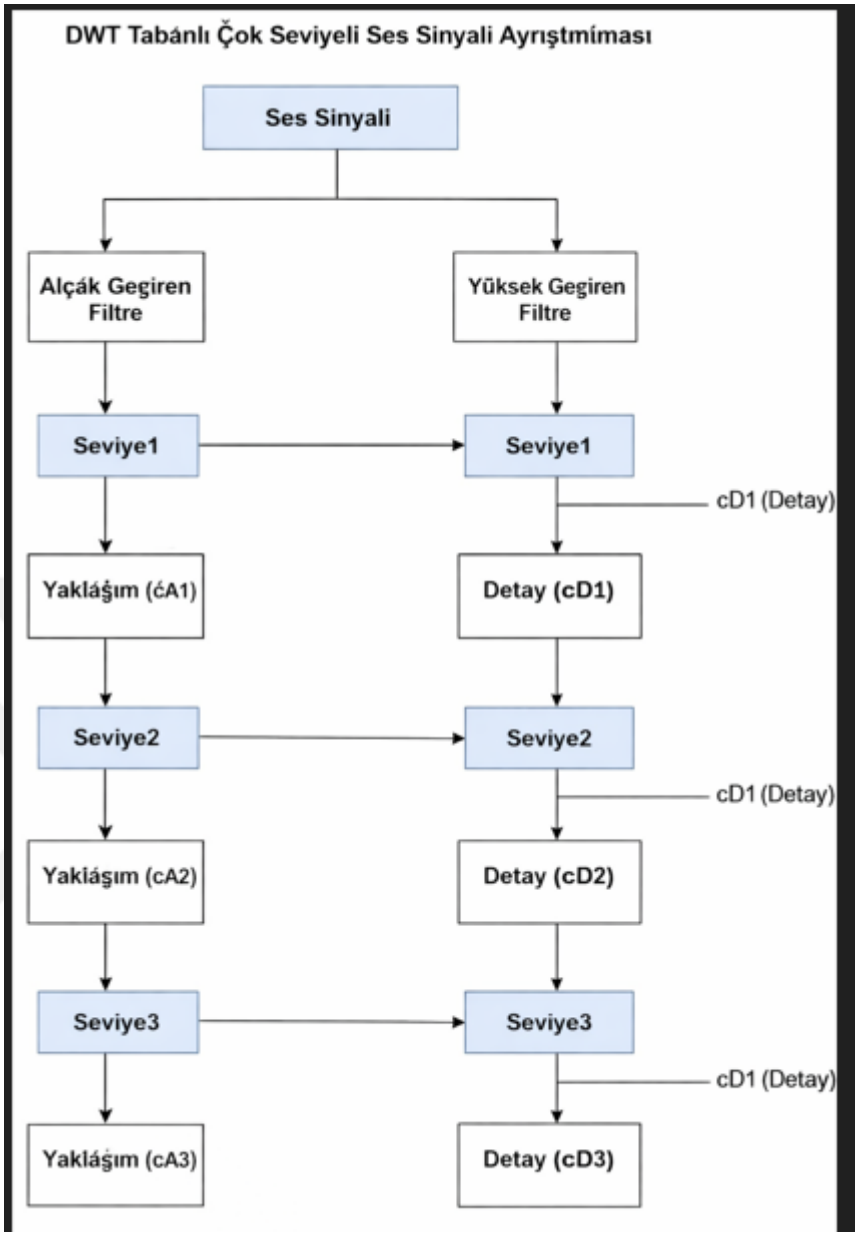
Şifreleme işlemi, açık metnin sabit boyutlu bloklara ayrılmasıyla başlar. Her açık metin bloğu, bit düzeyinde **XOR** işlemi kullanılarak önceki şifreli metin bloğu ile birleştirilir. İlk blok için bu **XOR** işlemi rastgele üretilmiş bir Başlatma Vektörü (**IV**) ile gerçekleştirilir; böylece aynı açık metin mesajlarının farklı şifreli çıktılar üretmesi sağlanır.

Şekil 6.3'te gösterildiği üzere Şifre Blok Zincirleme yapısı ardışık bloklar arasında bağımlılık oluşturarak şifreli çıktıda tekrar örüntülerinin oluşmasını engeller.

XOR işleminden sonra elde edilen blok, standart **GŞS** yer değiştirme–permütasyon dönüşümlerini uygulayan **GŞS-ŞBZ** şifreleme fonksiyonundan geçirilir. Bu adımın çıktısı şifreli metin bloğunu oluşturur ve bir sonraki açık metin bloğunun **XOR** işleminde kullanılır. Bu zincirleme yapı, tüm şifreleme turları boyunca bağımlılığı yayarak örüntü temelli kriptoanaliz saldırılarına karşı direnci artırır ve güvenliği güçlendirir.

6.3. ADD SİNYAL AYRIŞTIRMA DİYAGRAMI

Ayrık Dalgacık Dönüşümü (**ADD**), ses sinyalini çok çözünürlüklü bileşenlere ayrıştırarak algısal gömme için uygun zaman–frekans yerelleştirmesi sağlar. Hiyerarşik ayrıştırma süreci, Mallat (1989) tarafından tanımlanan dalgacık analizi kuramsal çerçevesini izleyerek Şekil 6.4'te gösterilmektedir.



Şekil 6.4: Ardışık ayrıştırma aşamalarında yaklaşım (**cA**) ve detay (**cD**) katsayılarını gösteren çok seviyeli Ayrık Dalgacık Dönüşümü (**ADD**) ayrıştırması.

Yinelemeli ayrıştırma yalnızca yaklaşım katsayılarına uygulanırken, yüksek frekanslı detay bantları gömme bölgeleri olarak kullanılır.

ADD Çok Seviyeli Ayrıştırma Diyagramının Açıklaması

Bir ses sinyalinin Ayrık Dalgacık Dönüşümü (**ADD**) kullanılarak çok seviyeli ayrıştırılması şu şekilde gerçekleşir: Süreç, giriş sesine iki tamamlayıcı filtrenin uygulanmasıyla başlar. Alçak geçiren filtre (**low-pass**), yavaş değişen spektral bileşenleri

korurken; yüksek geçiren filtre (**high-pass**), hızlı değişimleri ve yüksek frekans detaylarını yakalar.

Şekil 6.4'te gösterildiği üzere yinelemeli ayrıştırma yalnızca yaklaşım katsayılarına uygulanır; detay alt bantları ise olası gömme bölgeleri olarak kullanılır.

Her ayrıştırma seviyesinde alçak geçiren kol bir yaklaşım katsayısı (**cA**), yüksek geçiren kol ise bir detay katsayısı (**cD**) üretir. Elde edilen yaklaşım katsayıları ardışık seviyelerde yeniden ayrıştırılarak **cA1 → cA2 → cA3** biçiminde ilerler. Buna karşılık detay katsayıları (**cD1**, **cD2**, **cD3**) kendi seviyelerinde kalır ve ses sinyalinin giderek daha ince ayrıntı bileşenlerini temsil eder.

Bu hiyerarşik yapı, **ADD**'nin ses sinyalini farklı frekans özelliklerini yakalayan çoklu alt bantlara ayırdığını gösterir. Bu temsil steganografi açısından özellikle avantajlıdır; çünkü belirli alt bantlar genellikle detay katsayıları içine veri gömülmesine olanak tanırken algısal saydamlık ve dayanıklılık korunur.

6.4. GŞS-ŞBZ'NİN ADD–NİM İLE BÜTÜNLEŞTİRİLMESİ

GŞS-ŞBZ ve **ADD–NİM** bütünleşmesi iki katmanlı bir güvenlik mekanizması oluşturur:

6.4.1. Gizlilik (Confidentiality):

GŞS-ŞBZ, kriptografik anahtar ve **IV** olmadan çıkarılan verinin çözülememesini sağlayarak veri gizliliğini garanti eder.

6.4.2. Gizlilik ve Saydamlık (Stealth and Transparency):

ADD detay katsayıları içinde gerçekleştirilen **NİM** gömme işlemi, İnsan İşitsel Sisteminin yüksek frekanslara sınırlı duyarlılığı nedeniyle işitsel bozulmayı en aza indirir (Johnson & Katzenbeisser, 2000).

6.4.3. Dayanıklılık (Robustness):

Steganografi literatüründe dönüşüm alanında nicemleme tabanlı gömme yöntemlerinin, kontrollü koşullar altında basit **LSB** yer değiştirmesine kıyasla genellikle daha kararlı davrandığı rapor edilmektedir.

Bu bileşenler birlikte, kriptografik korumayı algısal saydamlık ile birleştiren bir steganografik çerçeve oluşturur. Sistem performansı, bir sonraki bölümde **PSNR** ve **BER** gibi nesnel ölçütler kullanılarak değerlendirilmektedir.

6.5. VERİ YÜKÜ ÇERÇEVELEME VE UZUNLUK YÖNETİMİ

Gizli mesajın doğru şekilde yeniden elde edilebilmesi için alıcının, stego ses sinyali içine tam olarak kaç bit gömüldüğünü bilmesi gerekir. Bu bilgi olmadan çıkarma işlemi ya erken durabilir ya da ilgisiz katsayıları okumaya devam ederek bozuk bir çıktı üretir. Bu sorunu önlemek amacıyla önerilen sistemde açık başlık (header) tabanlı bir çerçeveleme stratejisi benimsenmiştir.

Sabit bir veri yükü boyutu varsaymak yerine, gömülü bit akışının ilk kısmı toplam veri uzunluğunu N olarak kodlayan bir başlığa ayrılmıştır. Gerçekleştirimde başlık 32 bitten oluşur; bu değer büyük mesaj boyutlarını temsil etmek için yeterli olmakla birlikte düşük ek yük oluşturur. Bit akışının geri kalan kısmı ise **GŞS-ŞBZ** şifreleme aşamasında üretilen şifreli metni içerir.

Çıkarma sırasında alıcı önce **32** bitlik başlığı okur, bunu tekrar tamsayıya dönüştürerek N değerini elde eder. Sistem daha sonra **ADD–NİM** gömme alanından tam olarak **N** bit geri alır ve böylece katsayı uzayının gereğinden fazla okunması engellenerek gizli verinin deterministik ve senkronize biçimde kurtarılması sağlanır.

Bu tasarım iki temel avantaj sunar. Birincisi, değişken uzunluklu mesajları destekleyerek kısa veri yüklerinde gömme kapasitesinin boşa harcanmasını önler. İkincisi, sabit uzunluklu sistemlerde sıkça görülen senkronizasyon hatalarını ortadan kaldırır. Bu nedenle başlık tabanlı çerçeveleme stratejisi önerilen çerçevede benimsenmiş ve gömme ile çıkarma arasındaki hizalamayı korumak amacıyla Algoritma 6.1 ve 6.2'ye tutarlı biçimde entegre edilmiştir.

6.6. GÖMME VE ÇIKARMA ALGORİTMALARI

Bu bölümde önerilen ses steganografisi çerçevesinin biçimsel algoritmik tanımı sunulmaktadır. Yöntem, hem kriptografik gizliliği hem de algısal saydamlığı sağlamak amacıyla **GŞS-ŞBZ** şifrelemesini **ADD–NİM** gömme yöntemiyle bütünleştirir. Gömme ve çıkarma süreçleri simetrik olup alıcı tarafında gizli mesajın deterministik biçimde geri elde edilmesine olanak tanır. Algoritmalar, sistemin çalışma akışını açık biçimde göstermek amacıyla sözde kod (pseudocode) biçiminde ifade edilmiştir.

6.6.1. Gömme Algortiması

Gömme Sürecine Giriş : Gömme işlemi önerilen sistemin ana operasyon hattını oluşturur. Açık metin mesajı, gömülü veri kısmen açığa çıksa bile gizliliği garanti etmek amacıyla önce Şifre Blok Zincirleme (**ŞBZ**) kipinde çalışan **GŞS** ile şifrelenir. Ardından elde edilen şifreli bit akışı, Nicemleme İndeks Modülasyonu (**NİM**) kullanılarak yüksek frekanslı **ADD** detay katsayıları içerisine gömülür. Bu gömme stratejisi, İnsan İşitsel Sisteminin yüksek frekanslara düşük duyarlılığından ve nicemleme tabanlı filigranlama yöntemlerinin dayanıklılığından yararlanır. Şekil 6.5'te gösterildiği üzere gömme iş akışı şifrelemeden ters **ADD** yeniden yapılandırmasına kadar sıralı bir işlem hattını takip eder.

Algoritma 6.1, gömme sürecinin adım adım işleyişini biçimsel olarak tanımlar.

Gömme Algoritması: GŞS-ŞBZ Şifrelemeli ADD–NİM

Girdi:

x[n] : Örtü ses sinyali (16-bit PCM WAV)

M : Açık metin gizli mesaj

K : GŞS-128 şifreleme anahtarı

IV : GŞS-ŞBZ için Başlatma Vektörü

ψ : Dalgacık tabanı (örn. Haar)

Δ : NİM nicemleme adımı

Çıktı:

xs[n] : Stego ses sinyaliExplanation

Adımlar

1. **Mesajın Şifrelenmesi**

1.1 Mesaj M baytlara dönüştürülür ve PKCS#7 dolgulama uygulanır.

1.2 GŞS-ŞBZ ile şifrelenir:

$C = GŞS\_ŞBZ\_Encrypt(M, K, IV)$

1.3 Şifreli metin ikili dizine dönüştürülür:

$B = \{ b_1, b_2, \ldots, b\_N \}$

2. **Veri Yükü Çerçeveleme (Başlık Oluşturma)**

2.1 Veri uzunluğu N, 32 bitlik başlık olarak kodlanır:

$H = Binary32(N)$

2.2 Başlık ve veri birleştirilir:

$B' = H \parallel B$

3. **Örtü Sesin ADD Ayrıştırması**

3.1 x[n] yüklenir ve gerekirse normalize edilir.

3.2 Seviye-1 ADD uygulanır:

$(cA_1, cD_1) = ADD(x[n], \psi)$

4. **Kapasite Doğrulaması**

4.1 Eğer length(B′) > length(cD_1) ise işlem sonlandırılır ve kapasite yetersizliği raporlanır.

5. **NİM Gömme**

5.1 i = 1 → length(B′) için tekrarla:

coeff = $cD_1[i]$

q_index = floor(coeff / Δ)

Eğer B′[i] = 0 ise:

q_even = 2 * floor(q_index / 2)

$cD_1[i]$ = q_even * Δ

Eğer B′[i] = 1 ise:

q_odd = 2 * floor(q_index / 2) + 1

$cD_1[i]$ = q_odd * Δ

6. **Stego Sesin Yeniden Oluşturulması**

6.1 $cA_1' = cA_1$ (değiştirilmez)

6.2 Ters ADD uygulanır:

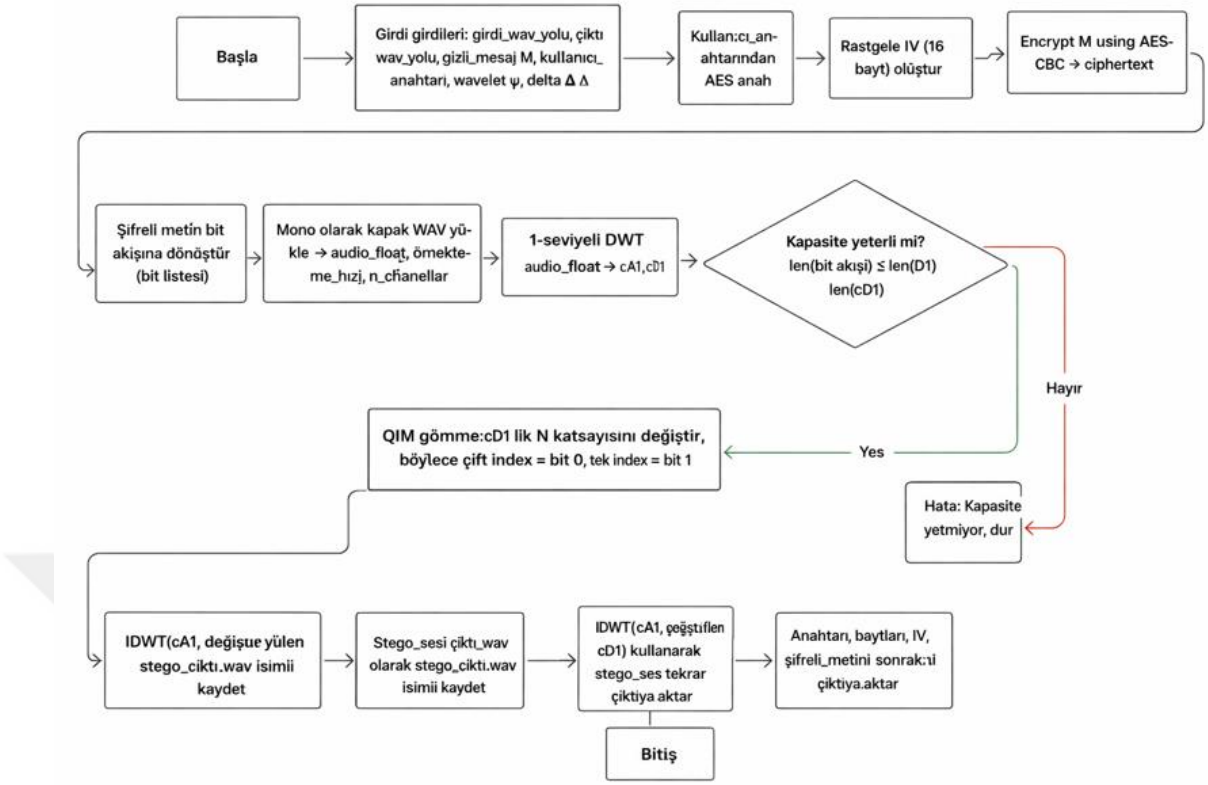
$xs[n] = IADD(cA_1', cD_1, \psi)$

7. **Çıktı**

7.1 xs[n] stego ses dosyası olarak kaydedilir.

8. **Son**

Algoritma 6.1, şifreleme ile dönüşüm alanı gömme işlemlerinin ses sinyali üzerinde birlikte nasıl uygulandığını göstermektedir. **GŞS-ŞBZ**, anahtar ve **IV** olmadan gizli mesajın okunamaz kalmasını sağlarken; **ADD** detay katsayıları içinde gerçekleştirilen NİM gömme işlemi algısal saydamlığı korumayı ve temiz, sıkıştırılmamış koşullar altında mesajın yeniden elde edilebilmesini amaçlar. **ADD**'de yaklaşım (**cA**) ve detay (**cD**) katsayılarının ayrılması, değişikliklerin daha az fark edilebilir olduğu frekans bölgelerinde gömme yapılmasına olanak tanıyarak gizliliği artırır ve ses bozulmasını en aza indirir.



Şekil 6.5: Ters **ADD, NİM** tabanlı bit geri kazanımı ve **GŞS-ŞBZ** çözme adımlarını gösteren ses steganografisi çıkarma sürecinin akış diyagramı.

6.6.2. Çıkarma Algoritması

Çıkarma Sürecine Giriş: Çıkarma işlemi, gizlenen bilginin geri elde edilmesi için gömme hattının tersini uygular. Stego ses, değiştirilmiş detay katsayılarını elde etmek amacıyla aynı dalgacık tabanı kullanılarak ayrıştırılır. Daha sonra gömülü bitleri yeniden oluşturmak için ters **NİM** nicemlemesi uygulanır. Elde edilen şifreli metin doğru anahtar ve **IV** kullanılarak **GŞS-ŞBZ** ile çözülür. Tasarım, sayısal etkiler dışında ek bir bozulma olmadığı varsayımıyla, temiz kanal koşullarında açık metnin geri kazanılmasını hedeflemektedir.

Algoritma 6.2 ayrıntılı çıkarma iş akışını sunar. Şekil 6.6'da gösterildiği üzere çıkarma hattı gömme sürecini yansıtır ancak dönüşüm alanındaki sayısal sapmalara karşı hassastır.

Algoritma 6.2 – Ters NİM + GŞS-ŞBZ Çıkarma Süreci

Girdi:

xs[n] : Stego ses sinyali

K : GŞS-128 çözme anahtarı

IV : Gömme sırasında kullanılan Başlatma Vektörü

ψ : Dalgacık tabanı (gömme ile aynı)

Δ : NİM nicemleme adımı

Çıktı:

M* : Geri elde edilen açık metin mesajı

Adımlar:

1.ADD Ayrıştırması

1.1 xs[n] yüklenir.

1.2 Seviye-1 ADD uygulanır:

$(cA_1^*, cD_1^*) = ADD(xs[n], \psi)$

2.Ters NİM ile Bit Geri Kazanımı

2.1 Boş bit dizisi B* oluşturulur.

2.2 $i = 1 \rightarrow length(cD_1^*)$ için:

$coeff = cD_1^*[i]$

$q\_index = round(coeff / \Delta)$

Eğer $q\_index \bmod 2 = 0$ ise $b_i^* = 0$, aksi halde $b_i^* = 1$

b_i^* değeri B* dizisine eklenir.

3.Başlık Çözme (Veri Uzunluğu)

3.1 B* dizisinin ilk 32 biti okunur: H* = B*[0 : 32]

3.2 Başlık tamsayıya dönüştürülür: N = Binary32_To_Int(H*)

3.3 Yalnızca veri yükü bitleri alınır: B_payload* = B*[32 : 32 + N]

4.Şifreli Metnin Yeniden Oluşturulması

4.1 B_payload* bayt gruplarına ayrılır.

4.2 Gruplar şifreli metne dönüştürülür: C*

5.Çözme İşlemi

5.1 GŞS-ŞBZ ile çözülür: M_padded* = GŞS_ŞBZ_Decrypt(C*, K, IV)

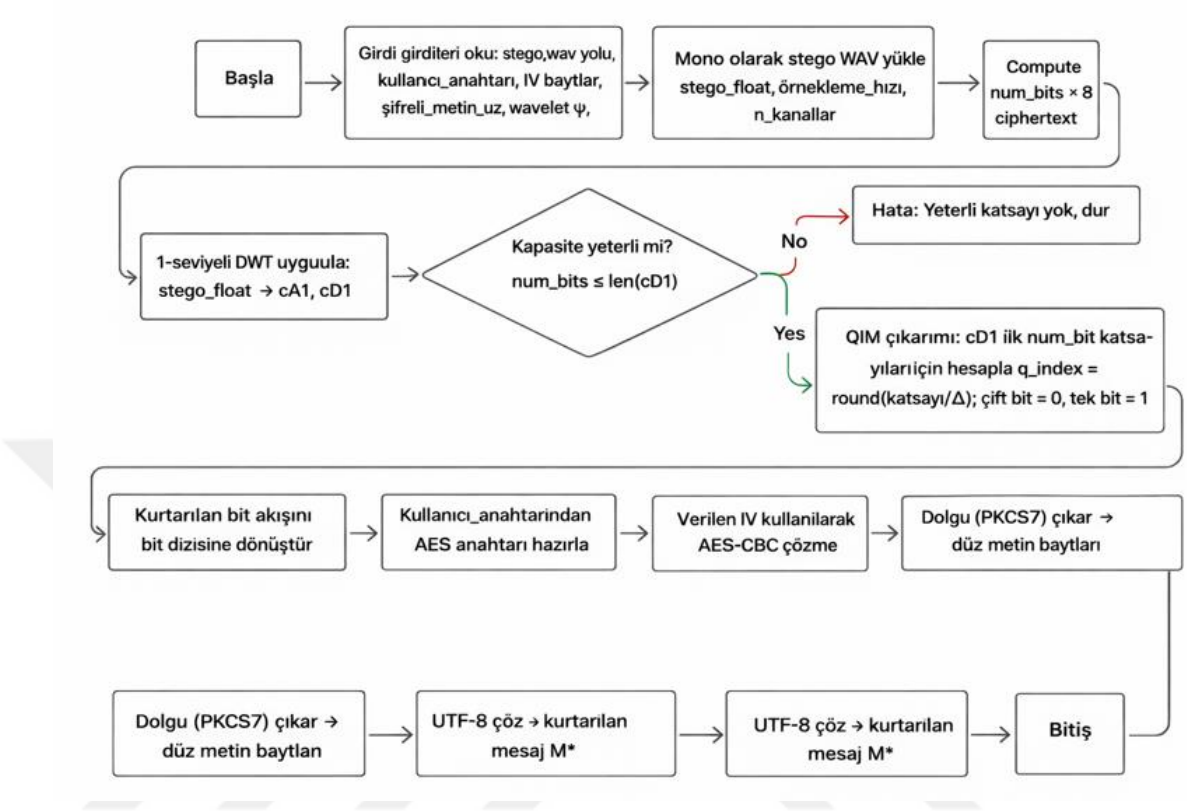
5.2 Dolgulama kaldırılır: M* = RemovePadding(M_padded*)

6.Geri elde edilen mesaj M* çıktı olarak verilir.

7. Son.

Algoritma 6.2, gömme sürecini yansıtır ve dalgacık alanında **NİM** tabanlı gömmenin yapılandırılmış fakat tam anlamıyla deterministik olmayan doğasını ortaya koyar. Her katsayıyı karşılık geldiği çift veya tek nicemleme aralığına eşleyerek algoritma, temiz kanal koşulları altında bitleri yeniden elde etmeye çalışır; geri kazanım başarımı ise dönüşüm ve yeniden yapılandırma aşamalarındaki sayısal kararsızlıklarla sınırlıdır. **GŞS-ŞBZ** çözme aşaması özgün açık metni tamamen geri yükleyerek hibrit steganografi modelinin doğruluğunu doğrular.

Bu algoritmik temel, Bölüm 7'de sunulan deneysel değerlendirmelerin dayanağını oluşturur.



Şekil 6.6: Ses Steganografisi Çıkarma Akış Diyagramı

7. DENEYSEL SONUÇLAR VE DEĞERLENDİRME

Bu bölümde, **GŞS-ŞBZ** şifrelemesi ile **ADD–NİM** gömme yöntemini birleştiren önerilen ses steganografisi çerçevesi değerlendirilmektedir. Amaç yalnızca sayısal performans ölçütlerini raporlamak değil; sistemin kontrollü koşullar altında nasıl davrandığını karakterize etmek, belirli tasarım tercihlerinin ortaya çıkardığı ödünleşimleri belirlemek ve elde edilen sonuçların gerçekçi ve kısıtlı kullanım senaryoları açısından ne ifade ettiğini incelemektir.

Analiz, nicel ölçümleri algoritmik davranışın nitel yorumuyla birlikte ele almakta ve özellikle algısal saydamlık ile mesajın geri kazanılabilirliği arasındaki ilişkiye odaklanmaktadır. Deterministik ya da tamamen güvenilir çıkarım varsaymak yerine değerlendirme, Bit Hata Oranı (**BER**) ölçümleriyle yansıtılan geri kazanımın kapsamını ve sınırlılıklarını; ayrıca Tepe Sinyal-Gürültü Oranı (**PSNR**) ile değerlendirilen algısal saydamlıkla birlikte eleştirel biçimde incelemektedir. Bu yaklaşım, önerilen çerçevenin hem güçlü yönlerinin hem de doğasında bulunan sınırlamaların dengeli biçimde değerlendirilmesini sağlar.

7.1. DENEYSEL KURULUM

7.1.1. Ses Veri Seti

Deneysel çalışmada iki adet mono **WAV** ses dosyası kullanılmıştır. Kayıtların örnekleme frekansı **44.1 kHz**, çözünürlüğü **16-bit PCM** olup her birinin süresi yaklaşık **10 saniyedir**. Veri kümesi, tek konuşmacının baskın olduğu konuşma benzeri bir sinyal ile daha zengin spektral değişim içeren müzik benzeri bir sinyalden oluşmaktadır. Bu seçimin amacı geniş ölçekli bir karşılaştırma veri tabanı oluşturmak değil, birbirinden farklı fakat temsil gücü yüksek iki akustik bağlamda sistem performansını değerlendirmektir.

7.1.2. Gömme Yapılandırılması

Gömme ve çıkarma işlemleri Bölüm 6'da sunulan algoritmalarla birebir uyumlu olarak gerçekleştirilmiştir. Açık metin mesajı dolgulandıktan sonra **GŞS-ŞBZ** ile şifrelenmiştir. Elde edilen şifreli metin bit dizisine dönüştürülmüş ve veri uzunluğu 32 bitlik bir başlık ile kodlanmıştır. Böylece oluşturulan son çerçevelenmiş veri yükü aşağıdaki yapıdadır:

$$\boldsymbol{B' = H \parallel B}$$

Seviye-1 ADD, Haar dalgacıkları kullanılarak uygulanmış ve **NİM** yöntemi, bit **"0"** için çift nicemleme aralıklarını, bit **"1"** için tek nicemleme aralıklarını kullanacak şekilde detay katsayıları **cD_**1üzerinde **Δ = 1** sabit adım değeri ile gerçekleştirilmiştir. Bu uygulamadan elde edilen deneysel yapılandırma Tablo 7.1'de özetlenmiştir.

Tablo 7.1: Deneysel Yapılandırma

Parametre	**Değer**
Örnekleme frekansı	44.1 kHz
Bit derinliği	16-bit PCM
Biçim	Mono WAV
Dalgacık	Haar (Db1)
ADD seviyesi	1
Gömme bandı	cD1
Nicemleme adımı (Δ)	1
Başlık uzunluğu	32 bits
GŞS kipi	GŞS-ŞBZ
GŞS anahtar uzunluğu	128-bit
IV üretimi	Random per run
Veri yükü boyutları	500, 1000, 1500, 2000 bits
Tekrar sayısı	10 per configuration

İstatistiksel değişkenliği sağlamak amacıyla her çalıştırmada farklı **GŞS** anahtarları ve **IV**'ler üretilmiştir..

7.1.3. Değerlendirme Ölçütleri

İki ölçüt kullanılmaktadır:

- **Tepe Sinyal-Gürültü Oranı (PSNR)**

$$PSNR = 10 \cdot \log_{10} (MAX^2 / MSE)$$

burada MAX = 32767 (16-bit PCM için).

PSNR algısal saydamlığı ölçer.

- **Bit Hata Oranı (BER)**

BER = (incorrect bits) / (total embedded bits)

BER, başlık dâhil olmak üzere tüm bit akışı B′ üzerinde hesaplanır.

7.2. NİCEL SONUÇLAR

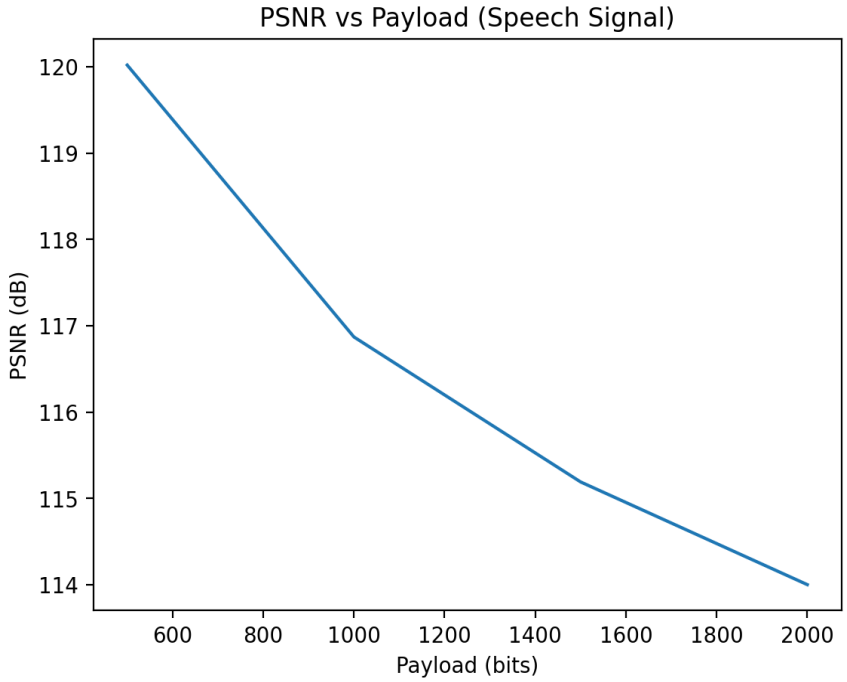
7.2.1. PSNR Sonuçları

- **PSNR Sonuçları (Konuşma Sinyali)**

Stego ses sinyallerinin algısal saydamlığını farklı veri yükü boyutları altında değerlendirmek amacıyla Tepe Sinyal-Gürültü Oranı (**PSNR**) kullanılmıştır. Daha yüksek **PSNR** değerleri, daha düşük algısal bozulmaya ve ses kalitesinin daha iyi korunmasına karşılık gelir.Konuşma sinyali için elde edilen **PSNR** sonuçları Tablo 7.2'de özetlenmiştir.

Tablo 7.2: Farklı veri yükü boyutları altında konuşma sinyali için **PSNR** sonuçları.

Veri yükü (bit)	Ortalama (dB)	Std (dB)	Min (dB)	Maks (dB)
500	120.02	0.23	119.75	120.46
1000	116.87	0.06	116.77	116.96
1500	115.19	0.08	115.06	115.34
2000	114.00	0.07	113.91	114.10



Şekil 7.1: Konuşma sinyali için veri yükü boyutuna karşı **PSNR.**

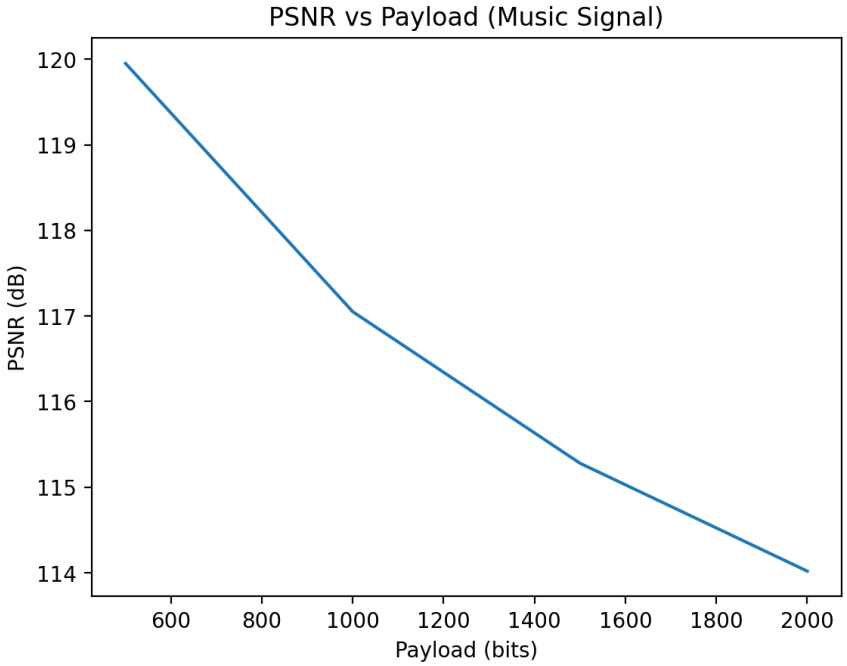
Veri yükü boyutu arttıkça daha fazla **ADD** detay katsayısı değiştirildiğinden **PSNR** kademeli olarak azalmaktadır. Buna rağmen değerler oldukça yüksek kalmakta ve konuşma sinyali için mükemmel algısal saydamlığa işaret etmektedir.

- **PSNR Sonuçları (Müzik Sinyali)**

Farklı içerik özellikleri altında algısal saydamlığı daha kapsamlı değerlendirmek amacıyla **PSNR**, müzik ses sinyali üzerinde de hesaplanmıştır. Müzik sinyali için elde edilen **PSNR** sonuçları Tablo 7.3'te özetlenmiştir.

Tablo 7.3: Farklı veri yükü boyutları altında müzik sinyali için **PSNR** sonuçları

Veri yükü (bit)	Ortalama (dB)	Std (dB)	Min (dB)	Maks (dB)
500	119.95	0.11	119.78	120.09
1000	117.05	0.10	116.90	117.16
1500	115.28	0.10	115.13	115.46
2000	114.02	0.10	113.90	114.16



Şekil 7.2: Müzik sinyali için veri yükü boyutuna karşı **PSNR**.

Müzik sinyali için de benzer bir azalma eğilimi gözlenmiş, daha yüksek veri yüklerinin daha fazla bozulma oluşturduğunu doğrulamıştır; ancak algısal saydamlık korunmaya devam etmektedir.

Yorum (PSNR)

NİM gömme işlemi tarafından değiştirilen **ADD** detay katsayılarının sayısı arttıkça PSNR değerleri monoton biçimde azalmaktadır. Bununla birlikte hem konuşma hem de müzik sinyalleri için raporlanan tüm **PSNR** değerleri 110 dB'in üzerinde kalmıştır. Bu durum, önerilen yöntemin sıkıştırılmamış ses koşulları altında ihmal edilebilir düzeyde işitsel bozulma oluşturduğunu ve yüksek algısal saydamlığı koruduğunu göstermektedir.

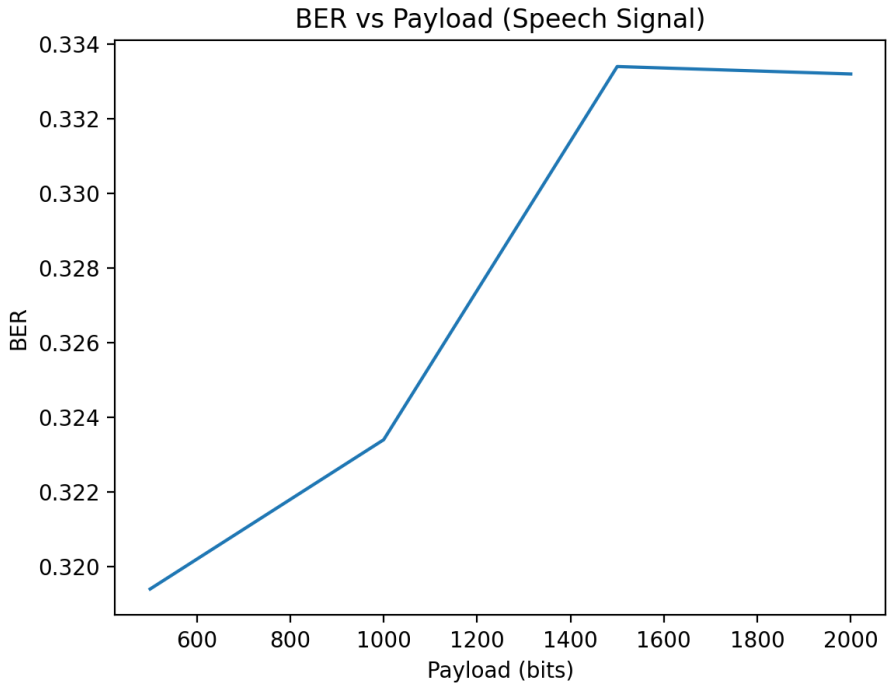
7.2.2. BER Sonuçları

- **BER Sonuçları (Konuşma Sinyali)**

Farklı veri yükü boyutları altında konuşma sinyali için mesaj çıkarımının güvenilirliğini değerlendirmek amacıyla Bit Hata Oranı (**BER**) kullanılmıştır.

Tablo 7.4: Farklı veri yükü boyutları altında konuşma sinyali için **BER** sonuçları

Veri yükü (bit)	Ortalama (dB)	Min (dB)	Maks (dB)
500	0.3194	0.284	0.350
1000	0.3234	0.304	0.344
1500	0.3334	0.314	0.352
2000	0.3332	0.318	0.352



Şekil 7.3: Konuşma sinyali için veri yükü boyutuna karşı **BER.**

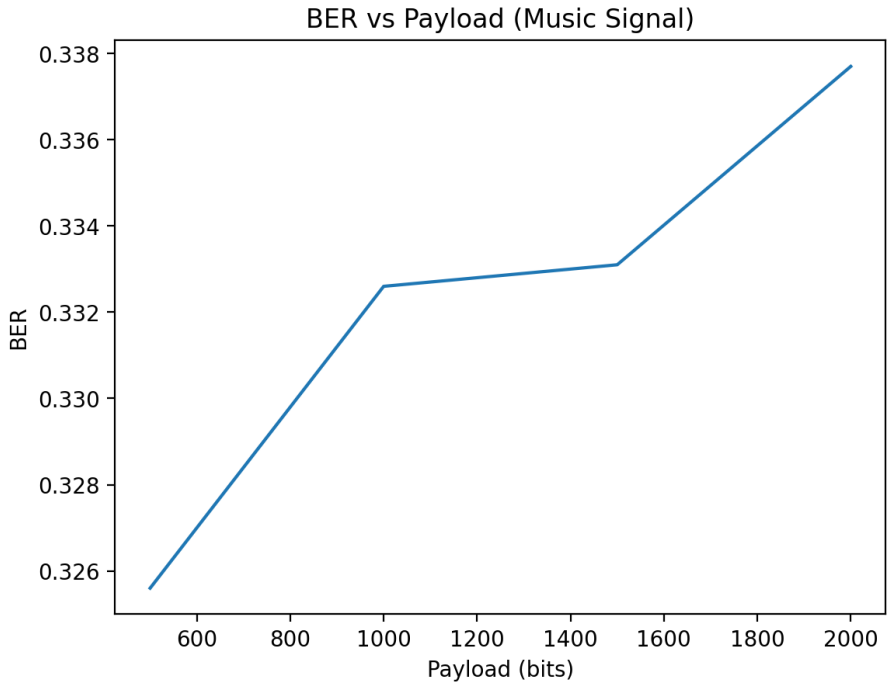
BER, farklı veri yükü boyutları boyunca yaklaşık **0.32–0.34** aralığında görece sabit kalmaktadır; bu durum bit hatalarının esas olarak gömme kapasitesinden değil, dönüşüm alanı işlemleri sırasında ortaya çıkan sayısal etkilerden kaynaklandığını göstermektedir. Bu **BER** düzeyi, mesaj geri kazanımının doğası gereği kısmi olduğunu ve deterministik ya da tamamen güvenilir bir çıkarım olarak yorumlanmaması gerektiğini ortaya koymaktadır.

- **BER Sonuçları (Müzik Sinyali)**

Farklı ses içerikleri arasında çıkarım güvenilirliğinin tutarlılığını değerlendirmek amacıyla **BER**, müzik sinyali kullanılarak da hesaplanmıştır.

Tablo 7.5: BER results for the music signal under varying payload sizes

Veri yükü (bit)	Ortalama (dB)	Min (dB)	Maks (dB)
500	0.3256	0.302	0.350
1000	0.3326	0.318	0.352
1500	0.3331	0.314	0.348
2000	0.3377	0.326	0.354



Şekil 7.4: Farklı veri yükü boyutları altında müzik sinyali için BER sonuçları.

Müzik sinyali, konuşma sinyaline benzer **BER** davranışı sergilemekte ve çıkarım hatalarının veri yükü uzunluğundan ziyade dönüşüm alanındaki pertürbasyonlardan kaynaklandığı gözlemini güçlendirmektedir.

Yorum (BER)

PSNR'den farklı olarak **BER,** veri yükü boyutu arttıkça yükselmemektedir. Bunun yerine hem konuşma hem de müzik sinyalleri için yaklaşık 0.33 civarında sabitlenmektedir. Bu durum, çıkarım hatalarının esas olarak gömme yoğunluğundan değil sayısal etkilerden kaynaklandığını göstermektedir. Bu etkiler arasında **ADD/IADD** sırasında oluşan sayısal

kaymalar, **16-bit** sinyal yeniden yapılandırmasındaki yuvarlama işlemleri ve **NİM** nicemleme aralıklarının neden olduğu parite değişimleri bulunmaktadır. Dolayısıyla **BER** davranışı, veri yüküne bağlı bir bozulmadan ziyade dönüşüm alanının doğasında bulunan sınırlamaları yansıtmaktadır. Nicemleme adım büyüklüğü **Δ** tüm deneylerde sabit tutulduğundan ve BER veri yükü boyutuna göre değişmediğinden, baskın hata kaynağının gömme yoğunluğu veya veri uzunluğu değil dönüşüm alanındaki sayısal pertürbasyonlar olduğu sonucuna varılmaktadır.

7.3. BÜTÜNLEŞİK ANALİZ

Deneysel sonuçlar, önerilen sistemin soyut bir fikirden ziyade teknik bir yapı olarak nasıl davrandığını ortaya koymaktadır. **PSNR** ve **BER** birlikte yorumlandığında, algısal saydamlık ile kontrollü koşullar altında mesajın geri kazanılabilirliğinin sınırları hakkında açık bir tablo ortaya çıkmaktadır.

7.3.1. Saydamlık ve Güvenilirlik

Çerçeve açık biçimde algısal görünmezliği önceliklendirmektedir. Saydamlık, tek seviyeli **ADD** kullanımı**, cD_1** alt bandında gömme yapılması ve çok küçük bir nicemleme adımı Δ seçilmesi sayesinde elde edilmiştir. Bu tasarım tercihi, tüm deneylerde gözlenen ve **110 dB'in** üzerinde kalan sürekli yüksek **PSNR** değerlerini açıklamaktadır.

Ancak aynı tasarım doğası gereği kırılganlığı artırmaktadır. **ADD/IADD** yuvarlama işlemleri, sinyalin tekrar **16-bit** tamsayı aralığına dönüştürülmesi ve çıkarım sırasında dönüşümün yeniden uygulanmasıyla oluşan küçük sayısal sapmalar katsayıları komşu **NİM** aralıklarına kaydırabilir ve gömülü paritenin değişmesine neden olabilir.

Kısacası algısal saydamlık, bit düzeyinde geri kazanılabilirlik pahasına elde edilmektedir. Bu ödünleşim rastlantısal değil yapısaldır ve aşırı görünmezlik ile kararlı mesaj yeniden elde etme arasındaki temel gerilimi yansıtır.

7.3.2. Δ'nın Merkezi Rolü (örnekleyici açıklama)

Δ parametresi **NİM** nicemleme aralıkları arasındaki mesafeyi belirler.

Küçük Δ → minimum işitsel bozulma

Küçük Δ → birbirine çok yakın NİM aralıkları → artan bit değişimleri

Örnekleyici gözlem

Bir katsayının ideal olarak aşağıdaki değere eşit olduğunu varsayalım:

12.45

$\Delta = 1$ için değer 12 (çift) veya 13 (tek) aralığına nicemlenebilir.

Ters **ADD** ve yuvarlama sonrasında oluşan çok küçük bir sayısal sapma:

$12.45 \rightarrow 12.62$

değerin komşu aralığa geçmesine ve kodlanan bitin değişmesine yol açmak için yeterlidir. Bu durumun gerçekleşmesi için gürültü, sıkıştırma ya da herhangi bir saldırı gerekmez — yalnızca normal aritmetik sürüklenme yeterlidir.

Dolayısıyla, küçük (koruyucu) Δ değeri saydamlığı sağlar, ancak güvenilir geri kazanımı garanti etmez. Bu nedenle çözüm, Δ değerini kör biçimde büyütmekten ziyade uyarlamalı Δ stratejileri ve fazlalık (redundancy) kullanımıdır.

7.3.3. Şifreleme ve Hata Yayılımı

GŞS-ŞBZ gizliliği sağlar ancak dayanıklılığı artırmaz. Şifreli metin rastgele göründüğünden tek bir bit hatası bile çözülmüş bir bloğun tamamını bozarak okunamaz çıktı üretebilir. Bu nedenle görece düşük **BER** değerleri dahi çözme işleminden sonra orantısız derecede ciddi sonuçlar doğurur. Gözlenen **BER** düzeylerinde (yaklaşık 0.33) ek hata düzeltme mekanizmaları olmadan **GŞS-ŞBZ** çözme işlemi pratik olarak mümkün değildir; çünkü zincirleme yapısı nedeniyle seyrek bit hataları şifre blokları boyunca yayılır. Bu nedenle gizlilik ve dayanıklılık ayrı ayrı tasarlanması gereken özelliklerdir.

7.3.4. Konuşma ve Müzik

Konuşma ve müzik sinyalleri benzer eğilimler göstermektedir: **PSNR** farkları düşük kalmakta ve **BER** değerleri aynı aralıkta seyretmektedir. Bununla birlikte bu benzerliğin altında yatan nedenler farklıdır. Müzik sinyallerinde enerji daha homojen yayıldığından oluşan bozulmalar yayılma eğilimi gösterirken, konuşma sinyalleri formant yapıları ve sessizlik bölgeleri içerdiğinden bazı bölümler değişimlere daha duyarlıdır. Bu durum sinyal yapısının önemli olduğunu ve içerik farkındalıklı gömme stratejilerinin dayanıklılığı artırabileceğini göstermektedir.

7.3.5. Pratik Çıkarımlar

Yöntemin uygun olduğu durumlar; sesin sıkıştırılmadan iletildiği, görünmezliğin önceliklendirildiği ve zaman zaman oluşabilecek hataların tolere edilebilir olduğu senaryolardır. Buna karşılık sıkıştırma veya yeniden örnekleme olasılığının bulunduğu, mesajın

eksiksiz geri elde edilmesinin zorunlu olduğu ya da şifreli içeriğin tamamen korunmasının gerektiği durumlarda yöntem daha az uygundur. Bu değerlendirme, yöntemin gerçekçi çalışma sınırlarını tanımlamaktadır.

7.3.6. Mevcut Bulguların Sınırları

Bu deneyler henüz **MP3** sıkıştırma, yeniden örnekleme, gürültü ekleme veya filtreleme, steganaliz ve daha geniş veri kümeleri gibi durumları değerlendirmemiştir. Gözlenen hassasiyet dikkate alındığında, bu tür dönüşümlerin **BER** değerini önemli ölçüde artırması beklenmektedir ve sistematik olarak incelenmeleri gerekmektedir.

7.3.7. Çıkarılan Dersler (Gelecek Çalışmalarla İlişkilendirme)

Bu bölümde elde edilen bulgular birkaç temel çıkarımı ortaya koymaktadır. Öncelikle, korumacı **ADD–NİM** parametreleri kullanıldığında yüksek algısal saydamlığın sağlanabildiği görülmüştür. Bununla birlikte, yalnızca sayısal sürüklenmenin dahi kalıcı bit hatalarına yol açabildiği ve şifreleme sürecinin **BER'in** pratik etkisini belirgin biçimde artırdığı anlaşılmıştır. Bu nedenle dayanıklılığın sistemde kendiliğinden ortaya çıkmadığı; uyarlamalı Δ seçimi, fazlalık ekleme ve hata düzeltme kodları gibi yöntemlerle açıkça tasarlanması gerektiği ortaya konmuştur. Ayrıca daha geniş kapsamlı dayanıklılık testlerinin yapılmasının zorunlu olduğu anlaşılmaktadır. Bu çıkarımlar, sonuç ve gelecek çalışmalar bölümünde tartışılan tasarım yönelimlerine doğrudan temel oluşturmaktadır.

Gözlenen **BER** değerleri sistemin hatalı çalıştığını göstermemekte, aksine kanal gürültüsü bulunmasa bile tersinir dönüşümler altında ince taneli nicemlemenin doğasında bulunan kararsızlığı nicel olarak ortaya koymaktadır.

7.4. SINIRLILIK

Sunulan sonuçlar açıkça tanımlanmış bir kapsam içinde yorumlanmalıdır. Bu sınırlılıkların belirtilmesi çalışmanın katkısını azaltmaz; aksine aşırı genellemenin önüne geçer ve bulguların gerçekte neyi gösterdiğini netleştirir.

İlk olarak tüm deneyler sıkıştırılmamış 16-bit **PCM WAV** sesleri üzerinde gerçekleştirilmiştir. Bu kontrollü ortam, gereksiz değişkenlikleri ortadan kaldırarak algoritmik davranışı izole etmek amacıyla özellikle seçilmiştir. Ancak gerçek uygulamalarda sesler çoğu zaman sıkıştırılmakta (**MP3/AAC**), yeniden örneklenmekte, filtrelenmekte veya akış halinde iletilmektedir. Temiz ve sıkıştırılmamış koşullarda dahi ölçülebilir bit hataları gözlendiğinden,

bu tür işlemlerin BER'i daha da artırması beklenmektedir. Bu nedenle gerçekçi işlem zincirleri altında sistematik bir dayanıklılık değerlendirmesine ihtiyaç vardır.

İkinci olarak veri kümesi yalnızca iki temsili sinyalden oluşmaktadır: biri konuşma benzeri, diğeri müzik benzeri kayıt. Bu sınırlı kurulum eğilimlerin daha açık yorumlanmasını sağlamış ve karıştırıcı etkenleri azaltmıştır; ancak genellenebilirliği kısıtlamaktadır. Farklı türler, kayıt ortamları, süreler ve ses şiddeti profilleri üzerinde daha geniş bir değerlendirme yapılması, saydamlık–güvenilirlik ödünleşiminin daha genel geçerli olup olmadığını ortaya koymak açısından gereklidir.

Üçüncü olarak gerçekleştirim sabit bir yapılandırmaya dayanmaktadır: **seviye-1 ADD**, Haar dalgacıkları ve sabit nicemleme adımı $\Delta = 1$. Bu tercihler analizi basitleştirmiş ve içsel davranışın yorumlanmasını kolaylaştırmıştır; ancak çok seviyeli ayrıştırma, algısal ağırlıklandırma veya uyarlamalı Δ gibi alternatif stratejilerin araştırılmasını engellemiştir. Dolayısıyla elde edilen bulgular tüm tasarım uzayını değil, belirli bir tasarım noktasını karakterize etmektedir.

Dördüncü olarak dayanıklılık mekanizmaları bilinçli olarak dâhil edilmemiştir. Sistem fazlalık, yeniden senkronizasyon veya hata düzeltme kodları kullanmamaktadır. **GŞS-ŞBZ** şifrelemesi ile birlikte değerlendirildiğinde bu durum, görece küçük **BER** değerlerinin bile tüm çözülmüş mesajı geçersiz kılabilmesine yol açmaktadır. Bu tercih kapsam sınırlaması açısından bilinçli olsa da güvenilirliğin gelecek sürümlerde açık biçimde tasarlanması gerektiğini göstermektedir.

Son olarak herhangi bir steganaliz veya karşıt (adversarial) test yapılmamıştır. Değerlendirme saydamlık (**PSNR**) ve geri kazanılabilirlik (**BER**) üzerine odaklanmış, ancak istatistiksel veya makine öğrenmesi tabanlı steganaliz araçlarına karşı tespit edilebilirlik incelenmemiştir. Bu nedenle "güvenlik" ile ilgili çıkarımlar, tespit edilebilirlik titizlikle değerlendirilene kadar eksik kalmaktadır.

Özetle bu çalışma kontrollü koşullar altında bir temel karakterizasyon olarak görülmelidir. Temel değeri dayanıklılık gösteriminde değil, gelecekteki steganografik tasarımların ele almak zorunda olduğu saydamlık–güvenilirlik ödünleşimini açık biçimde ortaya koymasındadır.

.

8. SONUÇ VE GELECEK ÇALIŞMALAR

8.1. SONUÇ

Bu tez, **GŞS-ŞBZ** şifrelemesi ile **ADD–NİM** gömme yöntemini birleştiren hibrit bir ses steganografisi çerçevesini incelemiştir. Değerlendirme, algoritmik davranışı izole etmek ve saydamlık–güvenilirlik ödünleşimini açık biçimde analiz edebilmek amacıyla özellikle kontrollü ve sıkıştırılmamış **WAV** sesleri üzerinde gerçekleştirilmiştir. Elde edilen sonuçlar, bu kontrollü koşullar altında çok yüksek algısal saydamlık sağlandığını, ancak çözücü tarafında ölçülebilir bit hatalarının da ortaya çıktığını göstermiştir. Bu hataların başlıca nedeni, dönüşüm ve yeniden yapılandırma aşamalarında oluşan sayısal sürüklenme etkileridir. Şifreleme katmanı mevcut olduğunda bu tür hatalar bloklar boyunca yayılabilmekte ve çözülmüş verinin geçerliliğini etkileyebilmektedir. Bu durum, gizlilik, saydamlık ve dayanıklılık özelliklerinin kendiliğinden hizalanan değil, çoğu zaman birbirinden bağımsız tasarım eksenleri olduğunu göstermektedir. Bu bağlamda çalışma, doğrudan uygulanabilir bir iletişim sistemi önermekten ziyade, önerilen yaklaşımın hangi koşullar altında etkili olduğunu ve güvenilirliğin hangi durumlarda ek mühendislik gerektirdiğini ortaya koyan analitik bir temel karakterizasyon sunmaktadır. Dolayısıyla önerilen çerçeve, kontrollü deney ortamında saydamlık–geri kazanılabilirlik ödünleşimini incelemek amacıyla oluşturulmuş yorumlanabilir bir referans yapı olarak değerlendirilmelidir.

Bu çalışma, literatürde yaygın olarak kullanılan zaman alanı tabanlı **LSB** yöntemleri ve dönüşüm alanı tabanlı yaklaşımlar ile karşılaştırıldığında, katmanlı güvenlik yaklaşımı sunması bakımından ayrışmaktadır. **LSB** tabanlı yöntemler genellikle yüksek veri kapasitesi sağlamakla birlikte sıkıştırma, yeniden örnekleme ve benzeri sinyal işleme adımlarına karşı düşük dayanıklılık göstermektedir (Chan & Cheng, 2004). Dönüşüm alanı tabanlı yöntemler, özellikle **Ayrık Dalgacık Dönüşümü** (**ADD**) kullanan çalışmalar, algısal saydamlık açısından avantaj sağlasa da çoğu çalışmada kriptografik koruma katmanı sistematik biçimde entegre edilmemektedir (Petitcolas et al., 1999). Bu tezde önerilen **GŞS-ŞBZ + ADD–NİM** hibrit yapısı, gizleme ve şifreleme süreçlerini birlikte ele alarak saydamlık, kapasite ve geri elde edilebilirlik arasındaki yapısal ödünleşimi açık biçimde ortaya koymaktadır. Bulgular, yüksek algısal kalite korunurken dönüşüm alanındaki sayısal etkilerin bit hata oranını etkileyebildiğini göstermekte ve literatürde çoğu zaman açık biçimde tartışılmayan saydamlık–geri kazanım

gerilimini görünür hale getirmektedir. Bu yönüyle çalışma, dayanıklılık odaklı gelecekteki araştırmalar için referans niteliğinde yorumlanabilir bir temel çerçeve sunmaktadır.

8.2. GELECEK ÇALIŞMALAR

Bu gözlemler önerilen çerçevenin geçersiz olduğunu göstermemekte, aksine tasarımın hangi yönlerde geliştirilmesi gerektiğini ortaya koymaktadır. Öncelikle **MP3/AAC** sıkıştırma, yeniden örnekleme, filtreleme ve gürültü ekleme gibi gerçekçi işleme zincirleri altında dayanıklılık sistematik biçimde incelenmelidir. Ayrıca çok seviyeli **ADD** kullanımı, algısal ağırlıklandırma ve uyarlamalı **Δ seçimi** gibi yaklaşımları içeren uyarlamalı gömme stratejileri değerlendirilmelidir. Özellikle şifreli veri yükleri söz konusu olduğunda BER değerini düşürmek amacıyla fazlalık ekleme ve ileri hata düzeltme kodlarının entegrasyonu önem taşımaktadır. Buna ek olarak klasik steganaliz yöntemleri ve modern makine öğrenmesi tabanlı tespit yaklaşımları kullanılarak algılanabilirlik analiz edilmeli, veri kümesi farklı türler, kayıt ortamları ve sinyal dinamiklerini kapsayacak şekilde genişletilerek genellenebilirlik artırılmalıdır. Gelecek çalışmalarda hata yayılımını azaltırken şifreli metin rastgeleliğini koruyan **CTR** gibi akış yönelimli kipler veya **GCM** gibi kimlik doğrulamalı kipler de araştırılabilir.

Bu tez, önerilen yöntemin mutlak dayanıklılık sağladığı iddiası olarak değil; algısal saydamlık ile kriptografik güvenliğin aynı anda önceliklendirildiği durumda dayanıklılığın nerede ve neden sınırlı kaldığını kontrollü biçimde ortaya koyan bir çalışma olarak değerlendirilmelidir.

9. KAYNAKLAR

Bender, W., Gruhl, D., Morimoto, N., & Lu, A. (1996). Techniques for data hiding. IBM Systems Journal, 35(3–4), 313–336.

Chan, C. K., & Cheng, L. M. (2004). Hiding data in images by simple LSB substitution. Pattern Recognition, 37(3), 469–474. https://doi.org/10.1016/j.patcog.2003.08.007.

Chen, B., & Wornell, G. W. (2001). Quantization index modulation: A class of provably good methods for digital watermarking and information embedding. IEEE Transactions on Information Theory, 47(4), 1423–1443.

Daemen, J., & Rijmen, V. (2002). The design of Rijndael: GŞS—The advanced encryption standard. Springer.

Daubechies, I. (1992). Ten lectures on wavelets. Society for Industrial and Applied Mathematics.

Ferguson, N., Schneier, B., & Kohno, T. (2010). Cryptography engineering: Design principles and practical applications. Wiley.

Fridrich, J. (2009). Steganography in digital media: Principles, algorithms, and applications. Cambridge University Press.

Johnson, N. F., & Katzenbeisser, S. (2000). A survey of steganographic techniques. In S.

Katzenbeisser & F. A. P. Petitcolas (Eds.), Information hiding techniques for steganography and digital watermarking (pp. 43–78). Artech House.

Katzenbeisser, S., & Petitcolas, F. A. P. (Eds.). (2000). Information hiding techniques for steganography and digital watermarking. Artech House.

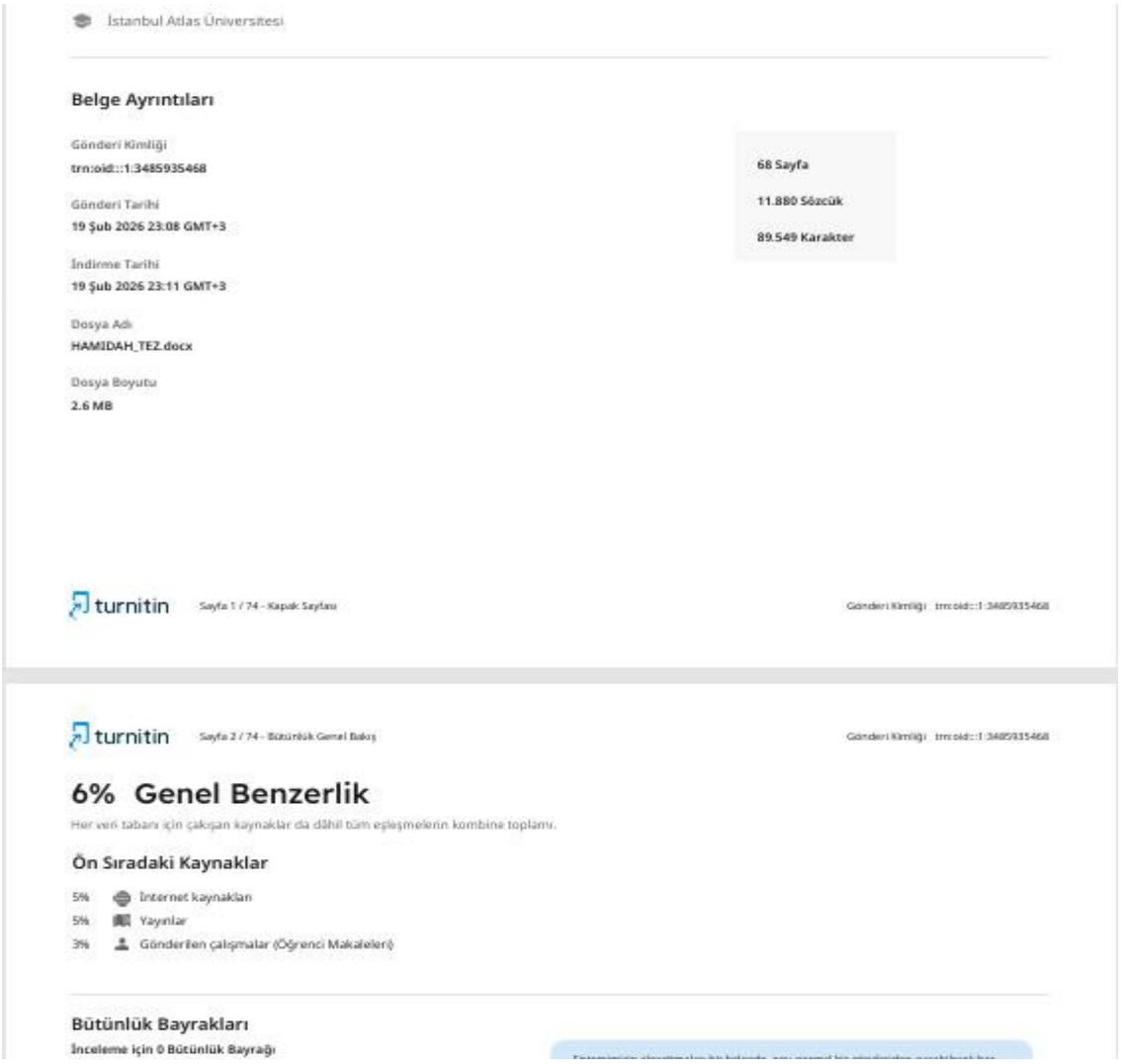
Mallat, S. (1989). A theory for multiresolution signal decomposition: The wavelet representation. IEEE Transactions on Pattern Analysis and Machine Intelligence, 11(7), 674–693. https://doi.org/10.1109/34.192463

Petitcolas, F. A. P., Anderson, R. J., & Kuhn, M. G. (1999). Information hiding—A survey. Proceedings of the IEEE, 87(7), 1062–1078.

Selesnick, I. W. (2001). Smooth wavelet tight frames with zero moments. Applied and Computational Harmonic Analysis, 10(2), 163–181. https://doi.org/10.1006/acha.2000.0324

İNTİHAL RAPORU

Dr. Öğr. Üyesi Recep DURANAY, Hamidah Saleh Abdullah Mohammed ZOLAAT - AYRIK DALGACIK DÖNÜŞÜMÜ (ADD) KULLANILARAK SES STEGANOGRAFİSİ



İstanbul Atlas Üniversitesi

Belge Ayrıntıları

Gönderi Kimliği
trn:oid:::1:3485935468

Gönderi Tarihi
19 Şub 2026 23:08 GMT+3

İndirme Tarihi
19 Şub 2026 23:11 GMT+3

Dosya Adı
HAMIDAH_TEZ.docx

Dosya Boyutu
2.6 MB

68 Sayfa

11.880 Sözcük

89.549 Karakter

turnitin Sayfa 1 / 74 - Kapak Sayfası Gönderi Kimliği trn:oid:::1:3485935468

turnitin Sayfa 2 / 74 - Bütünlük Genel Bakış Gönderi Kimliği trn:oid:::1:3485935468

6% Genel Benzerlik

Her veri tabanı için çakışan kaynaklar da dâhil tüm eşleşmelerin kombine toplamı.

Ön Sıradaki Kaynaklar

5% İnternet kaynakları
5% Yayınlar
3% Gönderilen çalışmalar (Öğrenci Makaleleri)

Bütünlük Bayrakları

İnceleme için 0 Bütünlük Bayrağı

10. ÖZGEÇMİŞ

ADI SOYADI: HAMİDAH ZOLAAT

Öğrenim Durumu:

Derece	Okul Adı ve Bölümü	Mezuniyet Yılı
Lisans	Dhamar Üniversitesi YEMEN – Computer Science	2015-2016
Yüksek Lisans	İstanbul Atlas Üniversitesi – Computer Engineering ISTANBUL	2025 - Devam

İş Deneyimi :

Unvan	Görev Yeri	Yıl
Araştırma Asistanı	İstanbul Atlas Üniversitesi	2024–2025
IT Uzmanı	Sukoon Media, İstanbul	2023–2024
Öğretim Görevlisi	Hadramut Üniversitesi YEMEN	2019–2020

Yayınları

Yüksek Lisans Tezi:
DWT–QIM ve AES Şifreleme Yöntemleri Kullanılarak Güvenli Ses Steganografisi Üzerine Bir Çalışma, İstanbul Atlas Üniversitesi, 2025 (Beklenen).

Araştırma Katılımı:
Yapay zeka ve veri analizi alanlarında araştırma çalışmalarına katılım sağlanmıştır.