

154672

İSTANBUL TEKNİK ÜNİVERSİTESİ ★ FEN BİLİMLERİ ENSTİTÜSÜ

**SES İŞARETLERİ İÇİN GERÇEK ZAMANLI BİR
TÜMLESİK DAMGA CÖZME TEKNİĞİ**

**YÜKSEK LİSANS TEZİ
Müh. Yusuf YASLAN
(504021307)**

**Tezin Enstitüye Verildiği Tarih : 26 Nisan 2004
Tezin Savunulduğu Tarih : 1 Temmuz 2004**

Tez Danışmanı : Prof.Dr. Bilge GÜNSEL *B. Günel*

Diğer Jüri Üyeleri Prof.Dr. Serhat ŞEKER (İ.T.Ü.) *Şeker*

Doç.Dr. M. Ertuğrul ÇELEBİ (İ.T.Ü.) *M. E. Çelebi*

TEMMUZ 2004

ÖNSÖZ

Akademik çalışmalarım sırasında her türlü desteğini esirgemeyen değerli hocam Prof. Dr. Bilge GÜNSEL' e ve bugünlere gelmemi sağlayan aileme ve yakınlarıma teşekkürü bir borç bilirim. Ayrıca proje çalışma arkadaşlarım Kadir Herkiloğlu ve Sait Şener'e teşekkür ederim.

Bu tez çalışması kapsamında geliştirilen ses damgalama ve damga çözme sistemi İ.T.Ü. Çoğulortam Sinyal İşleme ve Örüntü Tanıma Laboratuvarına aittir ve Prof. Dr. Bilge Günsel yöneticiliğinde yapılan İ.T.Ü. Geliştirme Vakfı “Sayısal Ses Damgalama Projesi” tarafından desteklenmiştir.

Temmuz 2004

Yusuf YASLAN

İÇİNDEKİLER

KISALTMALAR	iv
TABLO LİSTESİ	v
ŞEKİL LİSTESİ	vi
SEMBOL LİSTESİ	ix
ÖZET	xi
SUMMARY	xii
1. GİRİŞ	1
1.1 Damgalamanın Tarihçesi	2
1.2 Sayısal Damgalama Sistemleri	4
2. UYARLANIR SES DAMGALAMA SİSTEMİ	6
2.1 Geliştirilen Uyarlanırlı Damgalama Sistemi	8
2.1.1 Kanal Kodlayıcı	9
2.1.2 Ses Damgalama	12
2.1.2.1 Gizli Anahtar Üretimi	13
2.1.2.2 Damga Ekleme	13
2.1.3 Damga Çözme Bloğu	14
3. GERÇEK ZAMANLI TÜMLEŞİK DAMGA ÇÖZME	15
3.1 Dalgacık Gürültü Süzme ve Damga Çıkarımı	16
3.2 Damga Çözme ve Veri Senkronizasyonu	17
3.3 Damga Senkronizasyonu	19
3.4 Yayılı İzge Yöntemi ile Damgalanmış Ses Verisinde Damga Çözme	19
3.5 Damga-Sinyal-Oranı ve Gürültü-Sinyal-Oranı	26
3.6 Uyarlanırlı Damgalama ile Damgalanmış Ses Verisinde Damga Çözme	31
4. TESTLER	41
4.1 Farklı Örnekleme Frekansında Damgalamaya Karşı Gürbüzlük	42
4.2 Stereo-Mono Dönüşümler	43
4.3 Eklenebilir Beyaz Gauss Gürültüsü Atağı	44
4.4 Belirli Bir Frekansta Sinüs Atağı	48
5. SONUÇLAR VE TARTIŞMA	50
KAYNAKLAR	52
ÖZGEÇMİŞ	55

KISALTMALAR

DAVIC	:The Digital Audio Visual Council
DVD	:Digital Versatile Disk
SDMI	:The Secure Digital Music Initiative
MPEG	:Moving Pictures Expert Group
WIPO	:World Intellectual Property Organization
PN	:Pseudo Noise
WSR	:Watermark to Signal Ratio
SNR	:Signal to Noise Ratio
BDO	:Bit Doğruluk Oranı



TABLO LİSTESİ

	<u>Sayfa No</u>
Tablo 2.1. BCH kod kelimeleri üreteç polinomları tablosu.....	11
Tablo 4.2. Stereo-Mono dönüşümlerine karşı gürbüzlük.....	44



ŞEKİL LİSTESİ

	<u>Sayfa No</u>
Şekil 2.1 : Damgalama ve damga çözme sistemi blok çizelgesi.....	7
Şekil 2.2 : Yayılı izge yöntemine dayalı damgalama ve damga çözme işlemi.....	8
Şekil 2.3 : Geliştirilen ses damgalama- damga çözme sisteminin blok çizelgesi.....	9
Şekil 2.4 : Uyarlanır damgalama yönteminin blok şeması	12
Şekil 3.1 : (a) Orijinal ses işareti zaman uzayı gösterimi. (b) Orijinal ses işareti frekans uzayı gösterimi. (c) Eklenen gizli anahtar işareti zaman uzayı gösterimi. (d) Eklenen gizli anahtar işareti frekans uzayı gösterimi. (e) Damgalanmış ses işareti zaman uzayı gösterimi. (f) Damgalanmış ses işareti frekans uzayı gösterimi.....	21
Şekil 3.2 : (a) Dalgacık dönüşümü ile ayrıştırılan gizli anahtar işareti. (b) (a)'da görülen ayrıştırılmış anahtar işaretinin frekans uzayı gösterimi. (c) Kestirilmiş orijinal ses işaretinin zaman uzayı gösterimi. (d) Kestirilmiş orijinal ses işaretinin frekans uzayı gösterimi.....	22
Şekil 3.3 : (a) Damgalı ses işareti ile damgalamada kullanılan gizli anahtar arasındaki ötilinti fonksiyonunun τ ya bağılı değışimi. (b) Dalgacık gürültü süzme ile ayrıştırılan gizli anahtar işareti ile damgalamada kullanılan orijinal anahtar arasındaki ötilinti fonksiyonunun τ ya bağılı değışimi.....	23
Şekil 3.4 : (a) 16 bit lik damga bloğı eklenecek orijinal ses işareti. (b) (a)'daki ses işaretinin frekans uzayı gösterimi. (c) 16 bitlik damga bloğı içeren anahtar işareti. (d) (c)'deki anahtar işaretinin frekans uzayı gösterimi. (e) Damgalanmış ses işareti. (f) Damgalanmış ses işaretinin frekans uzayı gösterimi.....	25
Şekil 3.5 : (a) Dalgacık dönüşümü ile ayrıştırılan damga işareti. (b) Damgalanmış işareten kestirilen orijinal ses işareti. (c) Orijinal ses işareti. (d) (a)'daki işaretin frekans uzayı gösterimi. (e) (b)'deki işaretin frekans uzayı gösterimi. (f) (c)'deki işaretin frekans uzayı gösterimi	26
Şekil 3.6 : Dalgacık ayrıştırma ile elde edilen damga işareti ile orijinal ses işareti arasındaki WSR ların 16 ses çerçevesi boyunca değışimi. Orijinal damgalı işaret ile orijinal ses işareti arasındaki WSR lerin 16 ses çerçevesi boyunca değışimi.....	27
Şekil 3.7 : (a) Damgalanmış ses işareti ve gizli anahtar arasındaki ötilintilerin enbüyüklediğı noktaların τ 'ya bağılı histogramı. Gürültülü damgalanmış ses işareti ve gizli anahtar arasındaki enbüyüklediğı noktaların τ 'ya bağılı histogramı (b) SNR=10 dB, (c) SNR=5 dB, (d) SNR = 0 dB.....	29

Şekil 3.8	: (a) Damgalanmış ses işaretinden dalgacık ayrıştırma ile elde edilen anahtar ve orijinal gizli anahtar arasındaki ötilintilerin enbüyüklediđi noktaların τ 'ya bađlı histogramı. Gürültülü damgalanmış ses işaretinden dalgacık ayrıştırma ile elde edilen anahtar ve gizli anahtar arasındaki ötilintilerin enbüyüklediđi noktaların τ 'ya bađlı histogramı (b) SNR=10 dB, (c) SNR=5 dB, (d) SNR = 0 dB.....	30
Şekil 3.9	: Orijinal ses çerçevesi. (b) (a)'daki ses çerçevesine ait frekans uzayı gösterimi. (c) 9 özyineleme sonucu eklenen toplam gizli anahtar işareti (d) (c)'deki gizli anahtar işaretinin frekans uzayı gösterimi. (e) (a)'daki ses çerçevesine (c)'deki damga işaretinin eklenmesi sonucu elde edilen damgalanmış ses çerçevesi. (f) Damgalanmış ses çerçevesinin frekans uzayı gösterimi.....	32
Şekil 3.10	: (a) Dalgacık dönüşümü ile ayrıştırılan gizli anahtar işareti. (b) Kestirilen orijinal ses çerçevesi. (c) Orijinal ses çerçevesi. (d) (a)'daki işaretin frekans uzayı gösterimi. (e) (b)'deki işaretin frekans uzayı gösterimi. (f) (c)'deki işaretin frekans uzayı gösterimi.....	33
Şekil 3.11	: (a) Damgalı ses işareti ile damgalamada kullanılan gizli anahtar arasındaki ötilinti fonksiyonunun τ ya bađlı deđişimi. (b) Dalgacık gürültü süzme ile ayrıştırılan anahtar ile damgalamada kullanılan orijinal anahtar arasındaki ötilinti fonksiyonunun τ ya bađlı deđişimi.....	34
Şekil 3.12	: (a) 16 bit lik damga blođu eklenecek orijinal ses işareti. (b) (a)'daki ses işaretinin frekans uzayı gösterimi. (c) 16 bitlik damga blođu içeren gizli anahtar işareti. (d) (c)'deki anahtar işaretinin frekans uzayı gösterimi. (e) Damgalanmış ses işareti. (f) Damgalanmış ses işaretinin frekans uzayı gösterimi.....	35
Şekil 3.13	: (a) Dalgacık dönüşümü ile ayrıştırılan damga işareti. (b) Dalgacık dönüşümü ile kestirilen orijinal ses işareti. (c) Damgalanmamış orijinal ses işareti. (d) (a)'daki işaretin frekans uzayı gösterimi. (e) (b)'deki işaretin frekans uzayı gösterimi. (f) (c)'deki işaretin frekans uzayı gösterimi.....	36
Şekil 3.14	: Dalgacık ayrıştırma ile elde edilen damga işareti ile orijinal ses işareti arasındaki WSR ların 16 ses çerçevesi boyunca deđişimi . Orijinal damgalı işaret ile orijinal ses işareti arasındaki WSR lerin 16 ses çerçevesi boyunca deđişimi.....	37
Şekil 3.15	: (a) Damgalanmış ses işareti ve gizli anahtar arasındaki en büyük ilinti deđerini sađlayan τ histogramı. (b) Gürültülü ses işareti için elde edilen τ histogramı (SNR=10 dB). (c) Gürültülü ses işareti için elde edilen τ histogramı (SNR=5 dB). (d) Gürültülü ses işareti için elde edilen τ histogramı (SNR=0 dB).....	38
Şekil 3.16	: (a) Damgalanmış ses işareti üzerinde dalgacık dönüşümü ile ayrıştırılmış anahtar bilgisinin eklenen gizli anahtar ile arasındaki en büyük ötilintilerin τ 'ya bađlı histogramları. (b) Gürültülü ses işareti için dalgacık gürültü süzme ile elde edilen τ histogramı (SNR=10 dB). (c) Gürültülü ses işareti için dalgacık gürültü süzme ile elde edilen τ histogramı (SNR=5 dB). (d) Gürültülü ses işareti için dalgacık gürültü süzme ile elde edilen τ histogramı (SNR=0 dB).....	39

Şekil 4.1	: WSR' ye bağlı farklı frekans bantlarında başarımlar (a) Konuşma L=15 bit. (b) Müzik L=15 bit.....	42
Şekil 4.2	: 32kHz'de örneklenmiş ses işaretleri için elde edilen WSR' ye bağlı BDO (a) Konuşma işareti için (b) Müzik işareti için.....	43
Şekil 4.3	: SNR' a bağlı damga çözme başarımları. (a) Konuşma işareti için. (b) Müzik işareti için.....	45
Şekil 4.4	: SNR' a bağlı damga çözme başarımları (dalgacık dönüşümü ve BCH hata düzeltme ile). (a) Konuşma işareti için. (b) Müzik işareti için.....	46
Şekil 4.5	: Uyarlanabilir damgalama yönteminin SNR' a bağlı BDO damga çözme başarımları (Dalgacık dönüşümü ve BCH kullanılarak). (a) Konuşma işareti için. (d) Müzik işareti için.....	47
Şekil 4.6	: 300Hz Sin işareti SNR' ına bağlı BDO damga çözme başarımları (Yayıllı izge damgalama için). (a) Konuşma işareti için. (b) Müzik işareti için.....	48
Şekil 4.7	: 300Hz Sin işareti SNR' ına bağlı BDO damga çözme başarımları.(Uyarlanırlı damgalama için) (a) Konuşma işareti için. (b) Müzik işareti için.....	49



SEMBOL LİSTESİ

k_{m_i}	: i . Ses çerçevesine eklenecek modüle gizli anahtar işareti
k	: gizli anahtar işareti
w_j	: j . damga bilgisi
L	: eklenen damganın uzunluğu
$f()$	: doğrusal olmayan damgalama fonksiyonu
s_i	: orijinal i . ses çerçevesi
$s_{i_{wm}}$	: damgalanmış i . ses çerçevesi
$g()$	: doğrusal olmayan damga çözme algoritması
$\hat{w}_j$	: öngörü ile çözülen j . damga biti
s_{i_R}	: kanaldan alınan damgalı ses işareti
w	: damga katarı
$g(x)$	: BCH kodları üreteç polinomu
n	: BCH kod kelimesi uzunluğu
k	: BCH kod kelimesi bilgi biti uzunluğu
m	: galois field uzunluğu
t	: bir kod kelimesi üzerinde düzeltilebilecek hata sayısı
$d_{\min}$	: minimum Hamming uzaklığı
σ_K	: gizli anahtar işaretinin standart sapması
r	: PN yazmaç sayısı
s_i^t	: i . ses çerçevesinin t . yinelemedeki değeri
N	: bir ses çerçevesindeki örnek sayısı
$s_{i_{wm}}^t$	: i . ses çerçevesinin t . yinelemedeki damgalanmış değeri
t	: yineleme sayısı
n	: kanal gürültüsü
RP	: damga çözücünde incelenen ses işaretinin periyot sayısı
Λ_h	: dalgacık eşikleme işlevi
h	: eşik değeri
W	: dalgacık dönüşümü
W^{-1}	: ters dalgacık dönüşümü
$\hat{s}_i^t$	: kestirilmiş orijinal ses işareti
$\hat{e}$	: dalgacık dönüşümüyle ayrıştırılan gizli anahtar işareti
τ	: özilinti indisi
M	: gizli anahtar işaretinin uzunluğu
$\hat{k}_{m_i}$	: kestirilmiş anahtar işareti
$r_i(\cdot)$	: her bir τ değerine karşı düşen özilinti değeri
τ_{sync}	: veri senkronizasyonunun sağlandığı τ değeri
R_i	: incelenen ses çerçevesindeki en büyük özilinti değeri

$\hat{\mathbf{d}}$	: olası damga bitlerini içeren vektör
$\hat{d}_i$	: olası i . damga biti
$\hat{\mathbf{w}}$	: olası damga bitlerini içeren vektör
$\hat{\mathbf{w}}_{BCH}$	: güncellenmiş damga bitlerini içeren vektör



SES İŞARETLERİ İÇİN GERÇEK ZAMANLI BİR TÜMLEŞİK DAMGA ÇÖZME TEKNİĞİ

ÖZET

Bu tez çalışması kapsamında, gerçek zamanlı bir tümleşik damga çözme sistemi gerçekleştirilmiştir. Geliştirilen sistemde, damga çözme işlemi sırasında, orijinal damgalanmamış veriye gerek duyulmamaktadır. Önerilen damga çözme tekniği veri senkronizasyonunu sağlarken damga çözme işlemini de gerçekleştirmektedir. Damga çözücüde karar verici, ses işaretine gömülen gizli anahtar ve alınan ses işaretinden dalgacık dönüşümü ile ayrıştırılan gizli anahtar işareti arasındaki ötilintiye göre çalışmaktadır. Geliştirilen ses damgalayıcıda MPEG Katman 1 Model 1 uyumlu psikoakustik frekans maskeleme kullanılmaktadır. Damga çözücüde dalgacık dönüşümüne dayalı gürültü süzme gerçekleştirilmektedir. Damga çözme başarımı, farklı damga uzunluklarında, farklı işaret-gürültü oranlarında, farklı frekans bantlarında ses işaretine stereo-mono dönüşümler de uygulanarak incelenmiş ve sonuçlar literatürdeki standart yöntemle karşılaştırılmıştır. Gerçeklenen tekniğin özellikle gürültülü kanal iletimlerinde, standart tekniklerden daha yüksek bir başarıml sağladığı gözlenmiştir. Geliştirilen damga çözme algoritması gerçek zamanda işlem yapabilmekte ve senkronizasyon kayıplarından doğan hataları en küçüklemektedir.

A REALTIME INTEGRATED AUDIO WATERMARK DECODING TECHNIQUE

SUMMARY

In this thesis a real time integrated audio watermark decoding technique is proposed. The method performs blind decoding thus does not require the original audio data at the receiver. The proposed audio watermark extraction technique, performs watermark decoding while installing data synchronization. At the decoder site, decision making is achieved by calculating the correlation between the secret key and the extracted key obtained by wavelet denoising. The developed audio watermark encoder uses MPEG Layer 1 Model 1 compatible psychoacoustic frequency masking. Watermark decoding performance analysis is performed at different SNRs and WSRs within different frequency bands. The developed audio watermarking system robusts to channel noise as well as stereo-to-mono conversions. It is observed that the implemented technique outperforms the standard technique especially under channel noise. The developed algorithm is capable of decoding in real time and minimizes the synchronization errors.

1. GİRİŞ

Günümüzde internette, dijital TV ve radyo yayınlarında, CD ve DVD gibi çoğul ortam veri saklayıcılarında görülen hızlı teknolojik gelişmeler, bu medyalar aracılığı ile müzik, resim ve video gibi çoğul ortam verilerinin aitlik haklarına uyulmadan kolaylıkla dağıtımına olanak tanımaktadır. Sayısal sistemlerin gelişmesi imge, video, ses gibi verilerin sayısal olarak kodlanması ve saklanması olanağını da beraberinde getirmiştir. Sayısal veriler kopyalandığında, elde edilen kopya orijinal verinin aynısıdır. MP3.com, Kazaa, Emule vb gibi program ve internet siteleri, kullanıcılarına herhangi bir ücret ödmeden; müzik, resim ve video gibi dosyaların paylaşımını sağlamakta, bu durum bu ürünleri üreten ticari şirketlerin büyük maddi kayıplara uğramasına neden olmaktadır. 90'lı yılların başından itibaren aitlik haklarının korunması problemi hızla yaygınlaşmış ve bu problemin çözümü üzerinde çalışmalar başlatılmıştır. Bu maddi kayıpları azaltmak için; sayısal verilerin kopyalanmasını önleyici sistemler üzerinde yıllardır çalışılmasına rağmen, bu sistemlerin çoğu günümüz koşullarında yetersiz kalmaktadırlar. Sayısal damgalama sistemleri aitlik haklarının korunabilmesi problemine bir çözüm olarak önerilmiştir.

Tez kapsamında kullanılan sayısal damgalar; silinemeyen, gürbüz, eklendiği veri içerisinde algılanamayan ve genellikle eklendiği veri ile ilgili kaynak ve yasal bilgi gibi içeriğe sahip sayısal kodlardır [1]. Damga; imge, ses, video, metin ve hatta program kaynak kodu içerisine orijinal veriyi bozmayacak şekilde eklenebilir. Eklenen damga doğrudan kopyalamayı önleyici olamamakla beraber, kanuni olmayan dağıtım ve kopyalamanın gerçekleştirildiği kaynağı saptamada kullanılabilir. Benzer bir kavram olan steganografi kelime olarak eski Yunanca' da "gizli yazım" anlamına gelmektedir. Steganografiyi kriptografiden ayıran en önemli nokta; steganografide eklenen damganın iletilmek istenen bilgiyi taşıması ve orijinal veriyi bozmadığı için fark edilememesi, kriptografinin ise mesajın formatını değiştirerek içeriğini gizlemesidir. Öte yandan, steganografiden farklı olarak, damgalamada orijinal veriye aitlik haklarını belirleyici bilgi eklenmektedir.

Sayısal damgalamanın kullanım alanları sadece telif haklarının korunmasıyla sınırlı kalmamakta; veri indeksleme, veri getirme, TV ve radyo kanalları izlenme oranları ölçümleri gibi birçok değişik alanda kullanılabilmektedir. Farklı kullanım alanları göz önüne alındığında, damgalama yöntemlerinin işlem karmaşıklığının düşük, gerçek zamanda çalışabilmeye uygun yöntemler olması gerektiği açıktır.

1.1 Damgalamanın Tarihçesi

Gizli haberleşme kavramının temeli antik çağlara kadar dayanmaktadır [2]. Eski Yunan eserlerinden İliada' da Homer gizli haberleşmeden bahsetmiştir. Benzer olarak Herodot'un hikâyelerinde de metin tabletine gizli mürekkeple mesaj yazılmasından bahsedilmiştir. 1586 yılında İngiliz kraliçesi Elizabeth' in tahtına göz koymuş olan İskoç kraliçesi Mary, kraliçeyi öldürtmek için katil kiralamış fakat iletişim için kullandığı şifre İngiliz gizli polisi tarafından çözülmüştür. Bu olayla ilgisi bulunan kişiler yakalanmış ve İskoç kraliçesi idam edilmiştir.

Sayısal damgalamanın ilk kullanım alanlarından biri olan; kâğıt, para ve pullara yerleştirilen ve ancak ışığa tutulunca görülebilen damgaların geçmişi 700 yıl kadar geriye gitmektedir [1]. Bugün bilinen en eski damgalanmış kâğıt; 1292 yılında, kâğıt damgalamanın ana vatanı olarak kabul edilen İtalya'nın Fabriano kentinde üretilmiştir. 19. yy sonlarına doğru Fabriano' da yaklaşık 40 tane kâğıt üreticisi değişik kalitede ve ebatlarda kâğıtlar üretebilmekteydi. Önceleri kâğıtlara eklenen damga; kâğıdın boyut, cins ve üreticisini belirtirken daha sonraları bunlara üretim tarihi, yeri gibi bilgilerde eklenmiştir. Kâğıt damgalar İtalya'dan tüm Avrupa'ya yayılmış ve resmi anlamda değer kazanmıştır. Öyle ki; damgalı kâğıtlara yazılmış iki mektup, 1887 yılında Fransa' da cumhurbaşkanı Grèvy'nin istifa etmesine neden olan olaylarda delil olarak kullanılmıştır [1].

Günümüzde de buna benzer olaylar meydana gelmektedir. 1980'lerde İngiltere başbakanı Margaret Thatcher'in kabinesinde, kabine içi bilgilerin basına sızdırılmasından sorumlu bakanın bulunması için; kararların yazıldığı kelime işlem programı her bir bakan için ayrı bir tanımlayıcı bilgi ekleyecek şekilde programlanmış ve sorumlu bakan bu sayede bulunmuştur [2]. Buna benzer içerik

bilgisi veya seri numarası ekleme işlemleri; bugün sıkça kullanılan elektronik dokümanlarda da kullanılmaktadır.

Günümüzdeki anlamda sayısal damgalama ile ilgili en önemli çalışma ilk olarak 1954 yılında; Emil Hembrooke' un sahip olduğu Muzak şirketinin, müzik kayıtları içerisine sahiplik bilgisini içeren kod yerleştirmek için almış olduğu patenttir [3,4]. 1980'li yılların başlarında videobandı etkin koruyucu sistemleri geliştirilmiş ve bazı firmalar tarafından kullanılmıştır. Macrovision olarak adlandırılan bu sistemin temeli; TV'ler tarafından ihmal edilen fakat video kayıt cihazlarının devrelerinde bozucu etki gerçekleştiren ve kopyalamayı önleyen ek sinyal göndermeye dayanmaktadır. Macrovision Amerikan sinema filmi yapım şirketleri tarafından hala kullanılmakta ve DVD'lere adapte edilmeye çalışılmaktadır. 1990'ların başında imge damgalama kavramı gelişmiş; Tanaka ve arkadaşları faks gibi ikili imgelerin korunması kavramını ortaya atmışlardır [5,6]. 1993 yılında Tirkel ve arkadaşları gerçekleştirdikleri damgalamaya; daha sonra "watermark" olarak birleştirilecek "water mark" ismini vermişlerdir [1]. Bilim çevreleri bu yıllarda konu üzerine daha fazla eğilmeye başlamış ve sayısal damgalama (watermarking) ile ilgili ilk seminer 1996 yılında gerçekleşmiştir.

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

birçok uluslararası projenin oluşturulmasına destek sağlayarak; konu ile ilgili şirket ve kişilerin bir araya gelmesini sağlamıştır. Dünya çapında telif haklarını korunması ve düzenlenmesi ile ilgili çalışmalar yapan ve hükümetler üstü bir kuruluş olan WIPO (World Intellectual Property Organization) sayısal damgalamanın yasal alanlarıyla ilgili çalışmalarını sürdürmektedir [7]. Günümüzde DICOM gibi imge formatları; hastalara ait resimlerden, hasta ismi, tarih, şikâyet ve hastalıklar gibi birçok bilgiyi çıkarabilmekte ve medikal güvenliği sağlayabilmektedir.

Bugün sayısal damgalama; endüstriden, standardizasyon kuruluşlarından ve kanuni birçok kuruluştan ilgi görmesine rağmen konu ile ilgili en geniş çalışmalar üniversitelere ve araştırma enstitülerine bağlı imge ve işaret işleme grupları tarafından gerçekleştirilmektedir.

1.2 Sayısal Damgalama Sistemleri

Bugün haberleşmede sayısal haberleşme yöntemleri kullanılmaktadır. Analog haberleşmede olduğu gibi, sayısal haberleşmede de gizli bilgi iletimi veya başka bir veri içerisine gizlenmiş veri iletimi üzerinde çalışılmaktadır. Damgalamada mesaj gizli bir anahtar yardımıyla eklenmekte ve bu anahtar olmaksızın eklenen mesaj çözülememektedir. Günümüzde gerçekleştirilen sayısal damgalama sistemlerinin çoğu birbirlerine yakın fikirler içermelerine rağmen ayırt edici en önemli özellikleri ataklara karşı dayanıklılıklarıdır. Steganografi ile sayısal damgalamayı (watermarking) birbirinden ayıran temel nokta; steganografinin genel olarak ataklara karşı gürbüz olmaması fakat sayısal damgalamanın gürbüz olmasıdır [1]. Steganografi; eklenen bilginin üçüncü kişiler tarafından bilinmediği karşılıklı gizli iletişimlerde kullanılır. Fakat gizli bilginin eklendiği veri üzerinde herhangi bir değişiklik olduğu zaman, gizli bilgiyi elde edebilmek genellikle mümkün değildir.

Sayısal damgalama steganografiye ek olarak ataklara karşı dayanıklılık içermektedir. Kriptografide Kerkhoff kanunu olarak bilinen ve sayısal damganın varlığı, eklenme algoritması bilinse dahi; damganın yok edilmesinin çok zor veya nerdeyse imkânsız olması prensibi sayısal damgalamayı steganografiden ayırmaktadır.

Sayısal damgalama sistemleri genel olarak şu temel özellikler altında gerçekleştirilmelidir [1,8]:

- Eklenen damga mümkün olduğu kadar fazla bilgi içermeli, veri iletim kapasitesi yüksek olmalıdır.
- Eklenen damga genellikle gizli olmalıdır ve yetkili kişiler dışındaki kişiler tarafından erişilememelidir. Buda genellikle kriptografik anahtarlar sayesinde gerçekleştirilebilmektedir.
- Damga, gürbüz olmalı yani eklendiği veri üzerinde; yetkisiz kişilerin kasti veya kasti olmayan atakları, stereo-mono dönüşümler, dijital-analog / analog-dijital dönüşümler, kanal gürültüleri, filtreleme, yeniden örnekleme, kırılma, kayıplı sıkıştırma, yazdırma, tarama ve kanal iletimleri gibi işlemler sonucunda eklendiği veri üzerinde kalabilmeli ve tekrar elde edilebilmelidir.
- Damga silinemez ve algılanamaz olmalıdır.
- Damga eklendiği veri üzerinde algılanabilecek değişimlere neden olmamalıdır. İmge ve video üzerine eklenen damga görülmemeli, ses içerisine eklenen damga duyulmamalıdır.
- Damga veri içerisine doğrudan eklenmeli, herhangi bir başlık (header) içerisine eklenmemelidir. Bu sayede çok farklı veri formatlarında bile eklenen damga kalabilmelidir.
- Damgalanmış verinin belirli bir kısmından dahi olsa eklenen damga bulunabilmelidir.

Bunların dışında ek olarak gereksinim duyulabilecek başka özelliklerde vardır:

- Eklenen damganın bulunması; orijinal veriye gereksinim duyabileceği gibi (non-blind decoding), orijinal veriye gereksinim duyulmadan da (blind decoding) damga bulunabilir.
- Uygulamaların özelliklerine göre damga ekleme ve çözme işlemleri gerçek zamanda gerçekleştirilebilir olmalı ve yine uygulamaya göre sıkıştırılmış uzayda çalışılabilmelidir.
- Bazı uygulamalarda damga sürekli bilgi taşımak zorunda olabilir. Diğer uygulamalarda ise sadece belirli damgalar veri içerisine gömülmek zorundadır. Damga çözme aşamasında sadece eklemenin yapıldığı kısımlara bakmak yeterli olabilmelidir.

2. UYARLANIR SES DAMGALAMA SİSTEMİ

Ses damgalama sistemleri iki modülden oluşmaktadır:

- Damga ekleme modülü
- Damga çözme modülü

Şekil 2.1 'de bir sayısal damga ekleme ve damga çözme sisteminin genel blok çizelgesi görülmektedir. Damgalamada gizli veya açık anahtar kullanılarak damga bilgisi eklenebilmektedir. Geliştirilen damgalama sistemlerinde genel olarak; damga ekleme ve damga çözme aşamalarında, anahtar bilgisi bilinmektedir. Ses damgalamada duyulamazlığı sağlamak için çeşitli ölçütler kullanılmaktadır. Bunun bir sonucu olarak her bir ses örneği algılanamazlık kriterine uygun olarak değiştirilmektedir. Damgalama ve damga çözme işlemleri üç temel adımla özetlenebilir.

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

Ses çerçevesine gömülecek anahtar işareti tipik olarak; k gizli anahtar bilgisi ve w_j damga bilgisinin bir fonksiyonu olarak üretilir [1].

$$k_{m_i} = f(w_j, k) \quad j=1,2,\dots,L \quad (2.1)$$

(2.1) ifadesinde, L eklenecek damganın uzunluğunu belirtmekte olup, w_j i . çerçeveye eklenecek j . damga bitini göstermektedir. $f()$ fonksiyonu sadece k ve w_j 'nin değil, damga eklenen orijinal ses çerçevesi s_i 'nin de bir fonksiyonu olarak tanımlanabilir [9]. Tez kapsamında geliştirilen sistemde $f()$ üç değişkenli doğrusal olmayan bir fonksiyondur.

$$k_{m_i} = f(w_j, k, s_i) \quad (2.2)$$

- 2) k_{m_i} modüle edilmiş gizli anahtar işaretinin taşıyıcı s_i işaretine gömülmesiyle damgalanmış $s_{i_{NM}}$ işaretinin elde edilmesi.

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

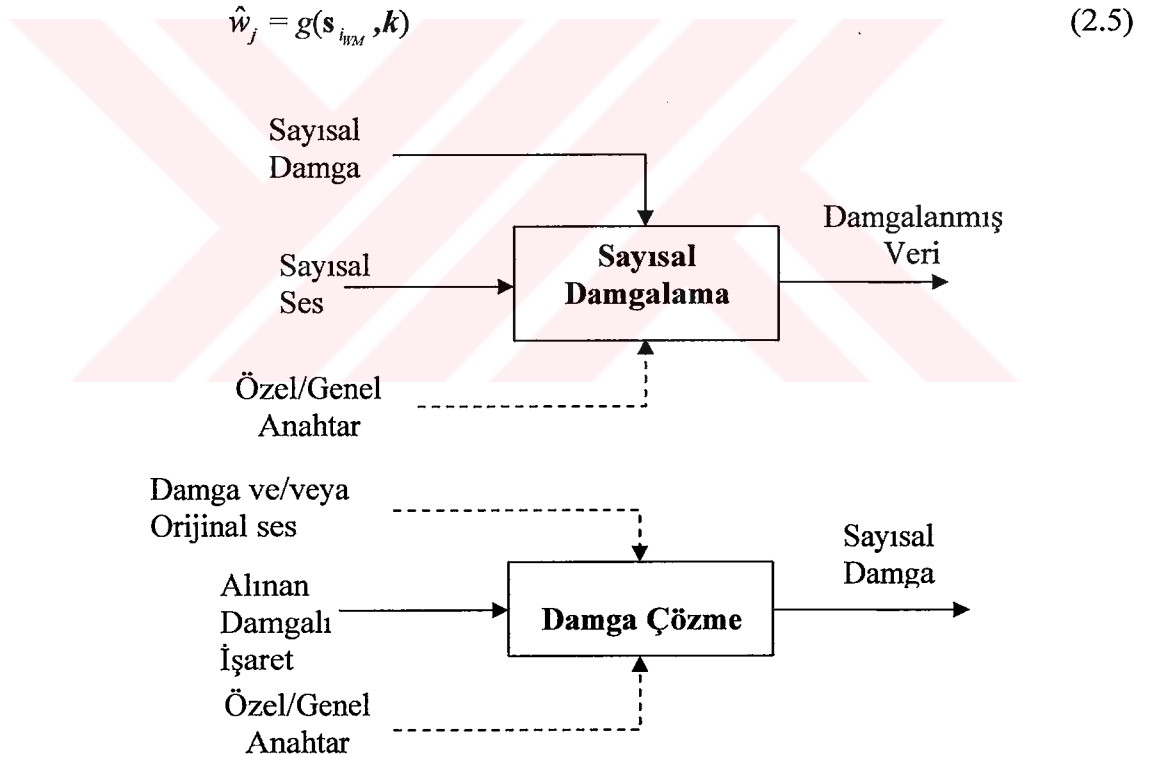
$$s_{i_{WM}} = f_i(s_i, k_{m_i}) \quad (2.3)$$

3) Gizli anahtar ve orijinal taşıyıcı işaret yardımıyla damga bilgisinin elde edilmesi, bir başka deyişle damga çözme.

$\hat{w}_j$ öngörü ile çözülen j . damga biti olmak üzere, (2.4) eşitliğinde $g(\cdot)$ doğrusal olmayan fonksiyonu damga çözme işlemini modellemektedir.

$$\hat{w}_j = g(s_i, s_{i_{WM}}, k) \quad (2.4)$$

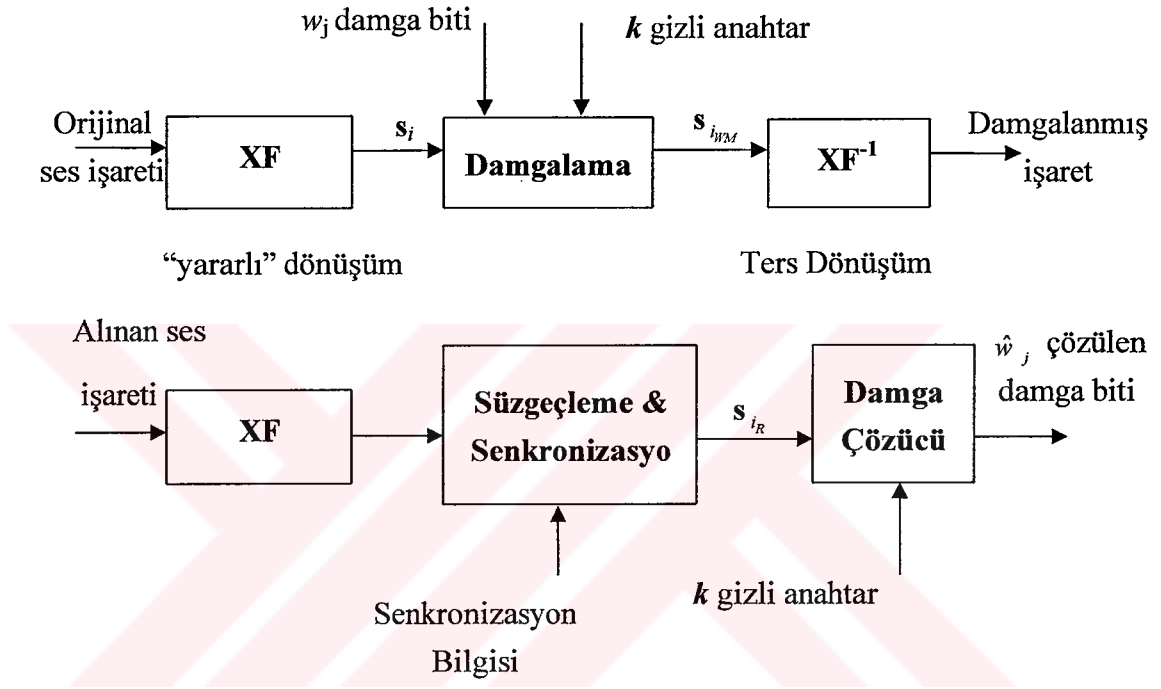
Alıcıda orijinal ses işaretinin bilinmemesi durumunda $g(\cdot)$ fonksiyonu (2.5) eşitliğinde görüldüğü gibi iki değişkenli bir fonksiyon olarak tanımlanır.



Şekil 2.1. Damgalama ve damga çözme sistemi blok çizelgesi.

Şekil 2.2 'de yaygın olarak kullanılan yayılı izge yöntemine dayalı bir damga ekleme ve damga çözme sisteminin blok çizelgesi görülmektedir [9]. Şekilde s_i dönüşüm uzayında damgalanacak ses çerçevesini, k gizli anahtar bilgisini, w_j damga bitini, $s_{i_{WM}}$ damgalanmış ses çerçevesini, s_{i_R} kanaldan alınan damgalı ses işaretini,

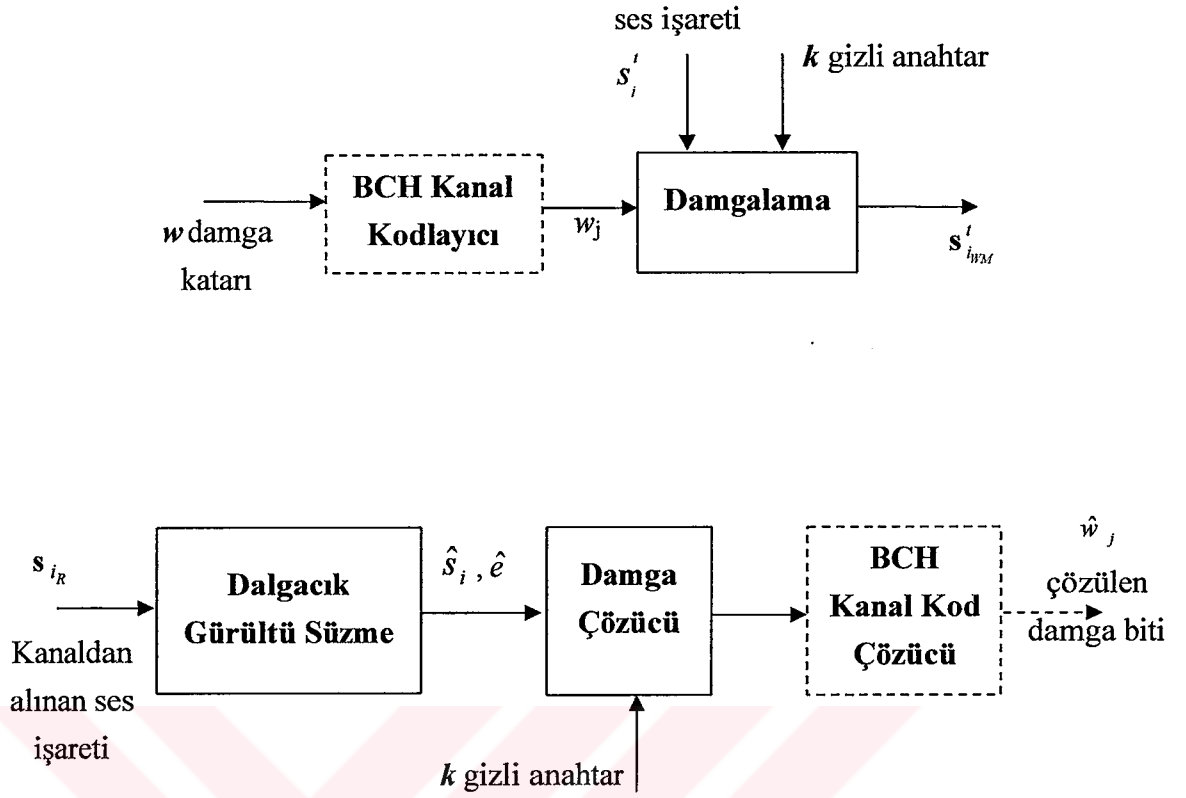
$\hat{w}_j$ damga çözücünde çözülen damga bitini belirtmektedir. Bu sistemde, [1]'de önerilen damgalayıcı ve damga çözücünden farklı olarak, damgalama doğrudan ses işareti üzerinde yapılmamakta, dönüşüm uygulanmış sayısal ses üzerinde gerçekleştirilmektedir. Burada amaçlanan damga çözme aşamasında performansı arttırmaktır [9]. Çizelgede “yararlı dönüşüm” olarak adlandırılan işlem kosinüs dönüşümü [10], dalgacık dönüşümü [11] ya da amaca uygun bir başka dönüşüm olabilir. Tez kapsamında damgalama orijinal ses örnekleri üzerinde yapılmaktadır.



Şekil 2.2. Yayılı izge yöntemine dayalı damgalama ve damga çözme işlemi.

2.1 Geliştirilen Uyarlanır Damgalama Sistemi

Şekil 2.3 de tez kapsamında geliştirilen ses damgalama-damga çözme sisteminin blok çizelgesi görülmektedir. Sisteme eklenen kanal kodlayıcı ile gerçek iletim ortamlarında veri iletim hatalarının enküçüklenmesi amaçlanmaktadır. Benzer kodlayıcılar literatürde kullanılmıştır [12,13].



Şekil 2.3. Tez kapsamında geliştirilen ses damgalama-damga çözme sisteminin blok çizelgesi.

2.1.1 Kanal Kodlayıcı

Geliştirilen damgalama sisteminde; w damga katarı BCH (Bose Chaudhuri Hocuenghem) kanal kodlayıcı [14] kullanılarak, kanal kod kelimelerine dönüştürülmektedir. Bu sayede damga çözme aşamasında kanal kod kelimelerinin sağlamış olduğu hata düzeltme kapasitelerinden yararlanılabilmektedir. Ayrıca kanal kodlarında; aynı uzunluktaki iki kod kelimesi arasında belirli bir Hamming uzaklığının bulunması, damga bitlerinin yanlış çözülme olasılığını azaltmaktadır. BCH kanal kodlayıcılar teknik yazında imge damgalamada [12, 15, 16] ve dalgacık uzayında gerçekleştirilen ses damgalamada kullanılmıştır [17].

BCH kodları çevrimsel kodlar olup, belirli bir $g(x)$ üreteç polinomuna göre farklı uzunlukta üretilebilirler. Bu kodlar, kod kelimeleri arasındaki en küçük Hamming uzaklığına bağlı sayıda hata düzeltme kapasitelerine sahiptirler. Kodlar zaman uzayında üretilebildikleri gibi kod kelimesinin üretiminde kullanılan Galois field'ların (GF) Fourier transformu alınarak frekans uzayında da üretilebilirler. Tez

çalışması kapsamında eklenecek damga bitleri olarak zaman uzayında üretilen kodlar kullanılmıştır.

En genel anlamda (n,k) bir BCH kodunda n kod kelimesi uzunluğunu, k bilgi bitlerinin uzunluğu göstermekte olup, n Galois field'in derecesi m 'ye bağımlı olarak bulunur. n ve m arasındaki ilişki (2.6) eşitliğinde görülmektedir.

$$n = 2^m - 1, \quad m \geq 3 \quad (2.6)$$

(n,k) lık bir BCH kodu k uzunluklu bir bit katarını n uzunluğundaki bit katarına (kod kelimesi) dönüştürür ve k , n değerleri (2.7) eşitliği ile birbirlerine bağlıdır.

$$k = n - \text{derece}(\text{GF}) \quad (2.7)$$

BCH kod kelimelerinin iletimi sırasında oluşan belirli sayıdaki hatalı bit alıcıda otomatik olarak düzeltilebilmektedir. Bir kod kelimesi üzerindeki düzeltilebilecek hatalı bit sayısı t ile gösterilmek üzere, n , k ve t değerleri arasındaki ilişki (2.8) eşitsizliği ile tanımlanır.

$$n - k \leq mt \quad (2.8)$$

Üretilen kod kelimeleri arasındaki $d_{\min}$ minimum Hamming uzaklığı ile düzeltilebilecek hata sayısı t arasındaki ilişki aşağıdaki gibidir.

$$d_{\min} \geq 2t + 1 \quad (2.9)$$

Geliştirilen ses damgalama sisteminde damga bilgisi BCH kodlayıcı tarafından üretilmekte, böylelikle damga çözmede iletim hatalarından doğabilecek başarımla azalması enküçüklenmektedir. Tez çalışması sırasında damga üretiminde (15,11) ve (63,16) lık BCH kod kelimeleri kullanılmıştır. BCH (15,11) kod kelimeleri için $m=4$, $k=11$, $t=1$ ve $d_{\min} = 3$ olarak alınmıştır. Bu kod tek bir hata düzeltme kapasitesine sahiptir. Benzer olarak tez çalışması sırasında damga biti uzunluğunun başarıma etkilerini inceleyebilmek açısından 63 bit uzunluğundaki damga bitleri BCH(63,16) kodlayıcı ile üretilmiştir. BCH(63,16)'lık kod kelimeleri için $m=6$, $k=16$, $t=11$ ve $d_{\min} = 23$ olup, bu kod kelimelerinde oluşan hatalı bitlerden en fazla 11 tanesi düzeltilebilmektedir. 15 bitlik damga bilgisi kullanılarak gerçekleştirilen damgalamada, her bir damga bloğunda hatalı iletilen bitlerin ancak blok uzunluğunun %6 sı kadarı düzeltilebilmedir. Buna karşın 63 bitlik damgalamada her bir blokta blok uzunluğunun %17'si kadar hatalı bit düzeltilebilmektedir.

Tablo 2.1'de, 63 bit uzunluğa kadar BCH kod kelimelerinin oluşturulması için [18]'de verilen üreteç polinomları görülmektedir.

Tablo 2.1. BCH kod kelimeleri üreteç polinomları tablosu.

n	k	t	$g(x)$ [Octal]
7	4	1	13
15	11	1	23
	7	2	721
	5	3	2467
31	26	1	45
	21	2	3551
	16	3	107657
	11	5	5423325
	6	7	313365047
63	57	1	103
	51	2	12471
	45	3	1701317
	39	4	166623567
	36	5	1033500423
	30	6	157464165547
	24	7	17323260404441
	18	10	1363026512351725
	16	11	6331141367235453
	10	13	472622305527250155
	7	15	5231045543503271737

(15,11)'lik BCH koduna ait $g(x)$ polinomu için $(23)_{\text{octal}}$ değeri verilmiştir. İkili kod olarak bu polinom $(23)_{\text{octal}} = (010011)_{\text{binary}}$ şeklindedir. Bu kod kelimesine ait $g(x)$ fonksiyonu (2.10) eşitliğinde görülmektedir.

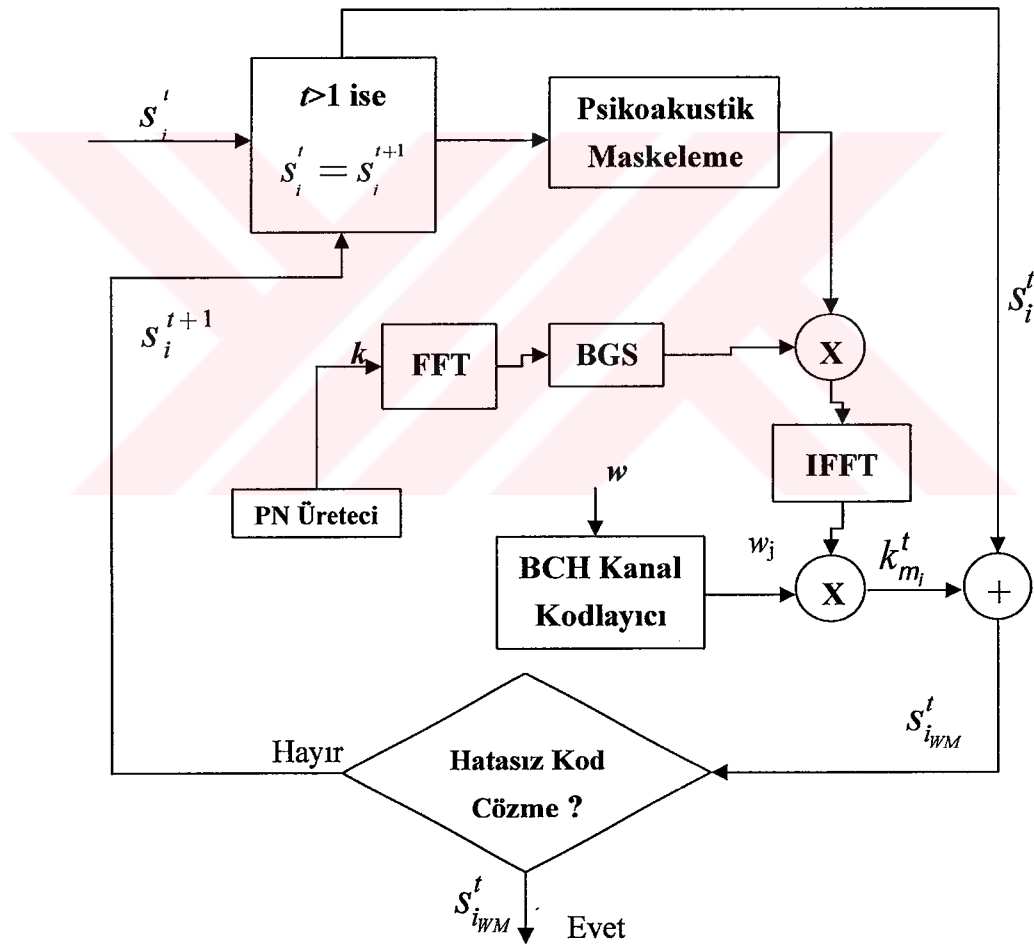
$$g(x) = 1 + x + x^4 \quad (2.10)$$

k bitlik katardan $g(x)$ üreteç polinomu kullanılarak n bitlik kod kelimesi, bir başka deyişle, n uzunluklu damga bilgi katarı üretilmektedir. Yapılan tez çalışmasında

BCH kodlarının üretiminde ve kod çözmede [19]'teki internet adresinde kullanıma sunulan kodlayıcı yazılımı temel alınmıştır.

2.1.2 Ses Damgalama

Geliştirilen ses damgalayıcıda uyarlanabilir psikoakustik frekans maskeleme kullanılmaktadır ve gerçekleştirilen damgalamanın duyulamazlık kriterini sağladığı gösterilmiştir [20]. Şekil 2.4' de geliştirilen ses damgalama sisteminin blok çizelgesi görülmektedir. Sistemde, kanal kod kelimelerinin sağlamış olduğu hata düzeltme yeteneğinden yararlanabilmek amacıyla iletilmek istenen damga katarı w , BCH kanal kodlayıcılar kullanılarak, belirli bir üreteç polinomu ile üretilmiş kod kelimesine dönüştürülmektedir.



Şekil 2.4. Uyarlanır damgalama yönteminin blok şeması.

2.1.2.1 Gizli Anahtar Üretimi

Damgalama sistemlerinde genel olarak damgalama sistemlerinde sözde gürültü üretici (pseudo noise generator) ile üretilen sıfır ortalamalı ve standart sapması $+\sigma_K$ ve $-\sigma_K$ değerlerini alan anahtar işaretleri kullanılmaktadır [9]. PN sözde gürültü dizileri, doğrusal geri beslemeli kaydırmalı yazmaçlarla üretilmektedir [21]. Eklenen damganın gizliliğinin önemli olduğu uygulamalarda PN dizisinin üretimi daha da önem kazanmakta ve damgalamada kript algoritmaları kullanılarak üretilen anahtarlar kullanılmaktadır.

r yazmaçlı sözde gürültü üretici ile üretilen anahtarın, içerisindeki r bitlik dizinin tekrarı ancak N bit sonra gerçekleşmektedir. N sayısı (2.11) ilişkisi ile belirlenmektedir.

$$N = 2^r - 1 \quad (2.11)$$

Sözde gürültü üretici ile üretilen gizli anahtar bilgisi işareten ilintisiz olup eklendiği işaretin istatistiksel özelliklerini değiştirmemesi amacıyla sıfır ortalamalı üretilmektedir. Tez kapsamında geliştirilen sistemde k gizli anahtar işareti sözde gürültü üretici ile üretilmiş ve $+1$ ve -1 değerlere sahip sıfır ortalamalı bir işarettir. Sayısal damgalayıcıda gizli anahtar işareti, ses işaretine bağlı olarak psikoakustik frekans maskeleye ile şekillendirilmekte ve bant geçiren süzgeçten geçirilerek bant frekans uzayında veri gömülmek istenen bölgeyle sınırlandırılmaktadır. Bantı sınırlı anahtar işareti zaman uzayında sese eklenecek damga bilgisi ile çarpılmakta ve modüle edilmiş anahtar, $k_{m_t}^t$, elde edilmektedir (Bkz Şekil 2.4). t üst indisi yineleme sayısını göstermektedir ve ileriki bölümde açıklanmaktadır.

2.1.2.2 Damga Ekleme

Tezde damga ekleme amacıyla geliştirilen uyarlanırlı damgalama algoritması kullanılmaktadır [20,22]. Damgalanacak sayısal ses işaretinin i . ses çerçevesinin t . yinelemedeki değeri s_i^t ile gösterilsin. $s_i^t(n)$, $n=1,...,N$ i . çerçevedeki bir ses örneğini göstermekte olup N , çerçevedeki örnek sayısıdır. Tez kapsamında N , MPEG 1 Model 1 Katman 1 e uyumlu olarak 512 örnek/çerçeve şeklindedir. Ses işareti; 44.1 kHz' de örneklenmiş ses işaretleri için yaklaşık 11.6 msn ve 32 kHz' de örneklenmiş ses işaretleri için 16 msn uzunluğundaki ses çerçevelerine bölünerek damgalanmıştır. Damgalayıcıda her bir çerçeveye 1 bit damga bilgisi eklenmekte olup 44.1 kHz 'de örneklenmiş ses işaretleri için en yüksek damga iletim hızı 86 bit/sn ve 32 kHz' de örneklenmiş ses işaretleri için 62 bit/sn dir.

Sınırlandırılmış ve damga biti ile çarpılmış $k_{m_i}^t$ gizli anahtar işareti zaman uzayında s_i^t ses işaretine eklenmekte ve damgalanmış ses işareti $s_{i_{wm}}^t$ elde edilmektedir. $s_{i_{wm}}^t$ (2.12) eşitliği ile ifade edilebilir.

$$s_{i_{wm}}^t = s_i^t + f(s_i^t, w_j) k_{m_i}^t = s_i^t + w_j k_{m_i}^t \quad j=1, \dots, L \quad (2.12)$$

(2.12) eşitliğinde k , Söзде Gürültü (PN) üretici ile üretilen sıfır ortalamalı gizli anahtar işaretini, w_j i . ses çerçevesine eklenecek damga bitini, L damga uzunluğunu, $k_{m_i}^t$, psikoakustik frekans maskeleye ile modüle edilmiş ve eklenecek damga biti ile çarpılmış t . özyinelemedeki gizli anahtar işaretini göstermekte olup, bu işaret zaman uzayında orijinal ses işaretine eklenmektedir. $f(s_i^t, w_j)$ fonksiyonu; $k_{m_i}^t$ yi belirleyen ve giriş ses işareti s_i^t ile damga biti w_j 'nin doğrusal olmayan bir fonksiyonudur.

Gizli anahtar bilgisi eklendiği ses çerçevesine bağlı modüle edildiği için damga çözücüde doğru çözülemeyebilmektedir. Geliştirilen damgalamada; damga gömüldükten sonra damganın doğru çözümünün gerçekleşip gerçekleşmediği kontrol edilmekte ve damgalayıcıda oluşacak hatalar, yinelemeli damgalama ile, enküçüklenmektedir. Böylelikle WSR oranını enbüyükleyen, ses işaretine uyarlanır bir damgalama gerçekleştirilmektedir.

2.1.3 Damga Çözme Bloğu

Bu tez kapsamında gözükapalı bir damga çözme sistemi geliştirilmiş olup Şekil 2.3 'te görülen BCH kanal kod çözücü isteğe bağlı olarak kullanılmaktadır. Geliştirilen sayısal ses damga çözücü sistemi Bölüm 3'te ayrıntılı olarak anlatılmaktadır.

3. GERÇEK ZAMANLI TÜMLEŞİK DAMGA ÇÖZME

Teknik yazında yayınlanan çalışmalarda damga çıkarma amacıyla kullanılan sistemler gözükapalı (blind) damga çözücüler ve orijinal işarete gerek duyan damga çözücüler olmak üzere iki gruba ayrılmaktadır [21]. Gözükapalı damga çözücülerde damga çözme işlemi sırasında damga işaretinin eklendiği orijinal ses işaretine gereksinim duyulmaz. Buna karşın diğer sistemlerde damga çözücülerde orijinal ses işareti gerekmekte olup, bu tür sistemlerin pratikte kullanımı aslına uygunluğun belirlenmesi (authentication) amaçlı uygulamalarla sınırlıdır. Gözü kapalı sistemlerde kabaca orijinal işarete gereksinim duyan damga çözme sistemlerinin yarısı kadar depolama ve iletim kanalı kapasitesi gerekmektedir ki bu durum uygulamalarda tercih nedenidir. Öte yandan alıcıda orijinal işaretin bilinmemesi damga çözücü yapısını karmaşıktırmakta, başarımı azaltmaktadır.

Damga çıkarımı genel olarak alınan işaret ve eklenen gizli anahtar arasındaki özilinti analizine göre gerçekleştirilmektedir [9]. Özilinti analizi gerçekleştirilecek işaret üzerinde filtreleme, gürültü süzme gibi çeşitli ön işleme teknikleri başarımı arttırmak amacıyla kullanılabilir. Teknik yazındaki çalışmaların çoğunda, gönderici ve alıcı arasında veri kaybı veya gecikmesinden dolayı ortaya çıkan senkronizasyon probleminden söz edilmemekte, damga çözümü basit özilinti analizi ile gerçekleştirilmektedir. Gerçek kanal iletimlerinde alıcıda senkronizasyon problemi dikkate alınmadığından, damga çözücülerde başarımlar çok büyük oranlarda düşmektedir. Tez çalışmasında bu problem dikkate alınarak, veri senkronizasyonunu sağlayan ve aynı zamanda damga çıkarımını gerçekleyen tümleşik bir damga çözücü sunulmuş ve birçok durumda başarımlar incelenmiştir [23].

Geliştirilen sistemde damga çözücülerde alınan ses işareti dalgacık gürültü süzme ön işleminden geçirilmekte böylelikle damga çözme başarımı artırılmaktadır [23]. Teknik yazında dalgacık gürültü süzme ile ilgili; temel dalgacık eşikleme (basic wavelet thresholding) [24], çevrim döndürme (cycle spinning), dalgacık ayak izleri (wavelet footprints) gibi özyineli olmayan (non-iterative) teknikler sunulmuş ve çevrim döndürme yönteminin özyineli (iterative) ve pencerelemeli yapıları geliştirilmiştir [25]. Özyineli dalgacık gürültü süzme işlemlerinin daha iyi sonuç verdiği belirtilmekle birlikte, özyineleme işleminin getirmiş olduğu işlem karmaşası göz önüne alındığında gerçek zamanlı işlem yapabilme açısından, dalgacık gürültü

süzme bloğunda yaygın olarak temel dalgacık eşikleme işlemi kullanılmıştır. Dalgacık gürültü süzme tekniği daha önce imgelerde gözü kapalı (blind) damga çözme amacıyla kullanılmıştır [11]. Ancak Lu ve arkadaşları çalışmalarında [11] damgalamayı ve damga çözme dalgacık uzayında gerçekleştirmektedirler. Bu tez kapsamında damgalama aşamasında dalgacık uzayında çalışılmamış damga çözme aşamasında bir ön işlem olarak dalgacık gürültü süzme kullanılmıştır.

Teknik yazında yayınlanan bazı çalışmalarda damga çözme başarımını yükseltmek amacıyla alıcıda da psikoakustik frekans maskeleye yapılmıştır [26]. Bu çalışmalarda alıcıya gelen damgalı ve gürültülü ses bir frekans maskeleyiciden geçirilmekte ve maske eşiklerinin üzerinde kalan değerler atılarak elde edilen ses işareti üzerinde damga çözme gerçekleştirilmektedir. Bu sayede kanal iletimi sırasında oluşan gürültü etkileri en aza indirilerek damga çözme başarımı artırılmaya çalışılmıştır.

3.1 Dalgacık Gürültü Süzme ve Damga Çıkarımı

Kanaldan alınan gürültülü damgalı ses işareti çerçevesi (3.1) ile modellenmektedir.

$$\mathbf{s}_{i_R}^t = \mathbf{s}_{i_{WM}}^t + \mathbf{n} = \mathbf{s}_i^t + \mathbf{w}_j \mathbf{k}_{m_i} + \mathbf{n}, \quad i=1,..., (L \times RP), j=1,...,L. \quad (3.1)$$

Eşitlikte $\mathbf{n}$ kanal gürültüsünü, $\mathbf{s}_{i_R}^t$ kanaldan alınan i . ses işareti çerçevesini belirtirken $\mathbf{s}_{i_{WM}}^t$ damgalı ses çerçevesini belirtmektedir. Burada L damga uzunluğu olup, ses işareti damga çözme RP 'lik periyotlar halinde işlenmektedir.

Damga çözme kanaldan alınan ses işaretine 1. seviyeden dalgacık dönüşümü uygulanarak, işaret detay ve yaklaşım katsayıları olmak üzere iki parçaya ayırılır. Bu bölme işlemi frekans uzayında iki eşit frekans aralığına karşı düşmekte olup; yüksek frekans bölgelerini içeren kısım detay katsayılarından, alçak frekans bölgelerini içeren kısım ise yaklaşım katsayılarından oluşmaktadır. Kanal iletimi sırasında eklenen gürültüler, genellikle yüksek frekanslı bileşenler içerir. Bu bakımdan dalgacık dönüşümü ile ayrıştırma sonucunda, gürültü bileşenleri ve damga bilgisinin büyük bir kısmı yüksek frekans bileşenleri içerisinde kalacağından, orijinal damgalanmamış ses işareti yaklaşım katsayıları ile modellenabilir. Kanaldan alınan ses işareti üzerinde dalgacık dönüşümü uygulayarak, orijinal damgalanmamış ses işaretini kestirmek mümkündür. Orijinal ses işaretinin kestirimi; dalgacık dönüşümü

ile elde edilen detay katsayılarının üzerinde eşikleme işlemi gerçekleştirildikten sonra ters dönüşüm uygulanarak (3.2)'deki gibi elde edilmektedir.

$$\hat{s}_i^t = W^{-1}(\Lambda_h(W(s_{i_R}^t))), \quad i=1,...,(L \times RP) \quad (3.2)$$

(3.2) eşitliğinde Λ_h , belirli bir h eşik değerinin altında kalan detay katsayılarını sıfırlayan dalgacık eşikleme işlevini, $s_{i_R}^t$ kanaldan alınan i . ses işaretini çerçevesini, $\hat{s}_i^t$ kestirilmiş orijinal ses işaretini belirtirken, W dalgacık dönüşümünü ve W^{-1} ters dalgacık dönüşümünü göstermektedir [25].

Orijinal ses işaretinin kestirim değeri kullanılarak, eklenen gizli anahtar işaretine ulaşılabilir. Bu aşamada eklenen gizli anahtar işaretinin ayrışımı (3.3)'teki gibi gerçekleştirilir.

$$\hat{e} = s_{i_R}^t - \hat{s}_i^t = \hat{w}_j \hat{k}_{m_j} + \mathbf{n}, \quad j=1,...,L. \quad (3.3)$$

(3.3) de $\hat{e}$ ayrıştırılan gizli anahtar işaretini, $\hat{s}_i^t$ i . ses çerçevesine ait orijinal ses işaretinin kestirilmiş değerini, $s_{i_R}^t$ kanaldan alınan i . ses çerçevesi işaretini, $\mathbf{n}$ kanal gürültüsünü, $\hat{w}_j$ kestirilmiş damga bitini, $\hat{k}_{m_j}$ kestirilmiş anahtar bilgisini, L damga uzunluğunu göstermektedir.

Tez çalışması sırasında önerilen damga çözücüde; dalgacık dönüşümü kullanılarak ayrıştırılan gizli anahtar işareti kullanılarak damga çözme işlemi gerçekleştirilmektedir. Bölüm 2.1.3' te damga çözme işleminin özilinti ile yapıldığı belirtilmişti. Bundan sonraki bölümde özilinti analizine göre damga çözme ve buna bağlı olarak gerçekleştirilen veri senkronizasyonu anlatılacaktır.

3.2 Damga Çözme ve Veri Senkronizasyonu

Damga çözücüde özilinti analizinden önce; kanaldan alınan ses işaretine (3.2)'deki dalgacık gürültü süzme ve (3.3)'teki ayrıştırma uygulanarak gizli anahtar işaretinin çıkarımı gerçekleştirilir. Çıkarılan bu işaret ve eklenen gizli anahtar arasında (3.4)'te belirtilen özilinti analizi gerçekleştirilmektedir. Ses işaretinde oluşan bozulmalar, kayıplar veya kayıt sırasındaki gecikmeler senkronizasyon problemini ortaya çıkarmaktadır. Bu nedenle (3.4)'te belirtilen özilinti fonksiyonu, senkronizasyon

problemini ortadan kaldırmak amacıyla, gönderici ve alıcı arasındaki gecikme değerini veren τ indisinin bir fonksiyonu olarak hesaplanmaktadır.

$$r_i(\tau) = \frac{\sum_{n=0}^{M-1} (k(n) - \langle k \rangle) (\hat{w}_j \hat{k}_{m_i}(n+\tau) - \langle \hat{w}_j \hat{k}_{m_i}(\tau) \rangle)}{\sqrt{\sum_{n=0}^{M-1} (k(n) - \langle k \rangle)^2} \sqrt{\sum_{n=0}^{M-1} (\hat{w}_j \hat{k}_{m_i}(n+\tau) - \langle \hat{w}_j \hat{k}_{m_i}(\tau) \rangle)^2}} \quad (3.4)$$

(3.4)' teki formül kanal gürültüsünün sıfır ortalamalı ve i.i.d.(ideally identically distributed) olduğu varsayımı ile elde edilmiş olup, $\hat{w}_j$ kestirilmiş damga bitini, M gizli anahtar işaretinin uzunluğunu, $\hat{k}_{m_i}$ kestirilmiş anahtar işaretini, $k(n)$ gizli anahtar işaretine ait her bir örnek değerini, k orijinal gizli anahtar işaretini göstermektedir. $r_i(.)$ her bir τ değerine karşı düşen ötilinti değerini belirtmekte olup, +1, -1 arasında normalize değerler içermektedir. $\langle . \rangle$ ortalama değer işlemi olup (3.5)'teki gibi hesaplanır.

$$\langle \hat{w}_j \hat{k}_{m_i}(\tau) \rangle = \frac{1}{M} \sum_{n=0}^{M-1} \hat{w}_j \hat{k}_{m_i}(n+\tau) \quad (3.5)$$

Veri iletimi sırasında gönderici ve alıcı arasında herhangi bir senkronizasyon problemi söz konusu değilse $r_i(0)$ ' daki ötilinti değerini hesaplamak damga çözmek için yeterli olacaktır. Fakat genellikle kayıpsız ve gecikmesiz iletim mümkün olmamaktadır. Bu durumda damga çözücünde veri senkronizasyonu aranır. Veri senkronizasyonu gönderilen ve alınan bitler arasındaki gecikmeyi veren τ değerinin hesaplanması işlemidir. Bu değer (3.4)' deki formüle göre $\tau=0,1,...,M-1$ için bulunur. Veri senkronizasyonunu sağlayan olası τ değeri; her bir çerçeve içerisindeki en büyük $r_i(\tau)$ değerlerini veren, $i=1,...(L \times RP)$, τ 'ların histogramından elde edilir. Histogramda belirli bir t , tolerans değerine göre en büyük değeri sağlayan τ değeri veri senkronizasyonunun sağlandığı τ_{sync} olarak belirlenir. İncelenen ses çerçevesi için R_i , en büyük ötilinti değeri; t , tolerans değeri kullanılarak (3.6)' daki gibi hesaplanır.

$$R_i = \max_t (r_i(\tau_{synch} \pm t)) \quad (3.6)$$

Damga çözme (3.6)' da hesaplanan en büyük ötilinti değerlerine göre gerçekleştirilmektedir. En büyük ötilinti değerlerinin işaretine göre eklenen damga biti çözülmektedir. Olası damga bitlerini içeren vektör $\hat{d} = [\hat{d}_i]_{L \times RP}$ şeklindedir ve olası her bir damga biti $\hat{d}_i$, (3.7)'deki gibi hesaplanır.

$$\hat{d}_i = \begin{cases} 1 & \text{if } \text{sign}(R_i) > 0 \\ -1 & \text{if } \text{sign}(R_i) < 0 \end{cases} \quad (3.7)$$

Veri senkronizasyonu sağlandıktan sonra damga çözme işlemi gerçekleştirilebilir. Fakat burada damga senkronizasyonu adı verilen ve bir sonraki bölümde açıklanacak ikinci bir senkronizasyonun daha sağlanması gerekmektedir.

3.3 Damga Senkronizasyonu

Damga çözme işlemi; iletim sırasındaki gecikme veya veri kaybından dolayı, eklenen damga katarının başından itibaren gerçekleştirilemez. Bu durumda çözülen olası damga bitleri üzerinde damga senkronizasyonu aranır. Tez çalışması sırasında senkronizasyon biti olarak damga katarının başına sekiz tane 1 içeren senkronizasyon bitleri yerleştirilmiştir. Damga senkronizasyonu $\hat{d}$ vektörü üzerinde birer bit sağa kaydırarak senkronizasyon bitlerini aramayla gerçekleştirilir. $(L \times RP)$ ' lik dizi içerisinde senkronizasyon bilgisi arama işlemi, sekiz tane 1 verisi ard arda bulunana kadar devam eder. Senkronizasyon bilgisi bulununca eklenen damga bitlerini çözme işlemine geçilir. Senkronizasyon arama işlemi ile damga çözme işlemlerin daha hızlı gerçekleştirilmesi ve yanlış damga çözme olasılığının düşürülmesi amaçlanmaktadır.

Damga senkronizasyonu sağlandıktan sonra, damga çözme $\hat{d}$ vektörü içerisinde L tane biti olası damga bitlerini içerecek $\hat{w}$ vektörü içerisine atar. Eğer damgalama sırasında BCH (n, k) kod kelimesi kullanılmış ise bu kod kelimesinde oluşabilecek $(d_{min}-1)/2$ hata düzeltilebilecektir. Dolayısı ile $\hat{w}$ vektöründe hata analizi gerçekleştirilip $\hat{w}$ vektörü güncellenmektedir. $\hat{w}_{BCH}$ güncellenmiş damga bitlerini içeren vektör ile damgalama sırasında kullanılan damga bitleri karşılaştırılıp, çözülen damga katarının veri tabanındaki hangi damga katarına ait olduğu belirlenir.

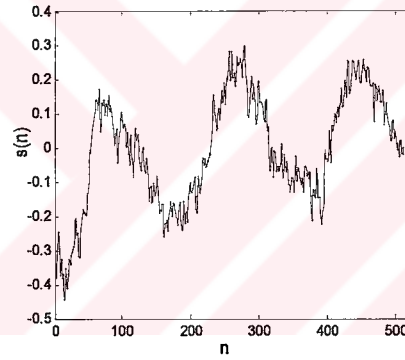
Önerilen damga çözme yönteminin başarımları Testler kısmında belirtileceğinden tezin bundan sonraki kısmında dalgacık gürültü süzme işleminin farklı damgalama yöntemleri ile damgalanmış ses işaretleri üzerindeki damga çıkarımı başarımına etkileri incelenecektir.

3.4 Yayılı İzge Yöntemi ile Damgalanmış Ses Verisinde Damga Çözme

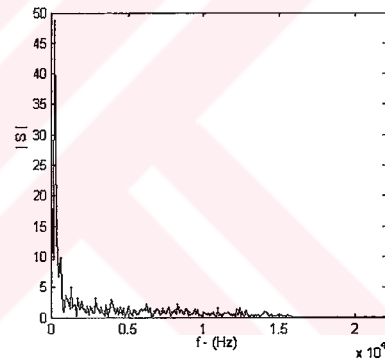
Teknik yazında “yayılı izge” yöntemi olarak adlandırılan [9] damgalama yöntemi; Bölüm 2.1.2’de belirtilen damgalama sisteminde $t=1$ alınarak, psikoakustik frekans maskeleyme yardımıyla gerçekleştirilmekte ve duyulmazlık kriterini sağlamaktadır.

Literatürde sıkça karşılaşılan yayılı izge damgalama yönteminin zaman uzayı damgalama ve uyarlanır damgalama yöntemleri ile olan karşılaştırmaları [27]'de irdelenmiştir. Tez çalışmasında sunulan damgalama ve damga çözme yöntemlerinin başarımı, yayılı izge yöntemi ile elde edilen sonuçlarla karşılaştırılacaktır.

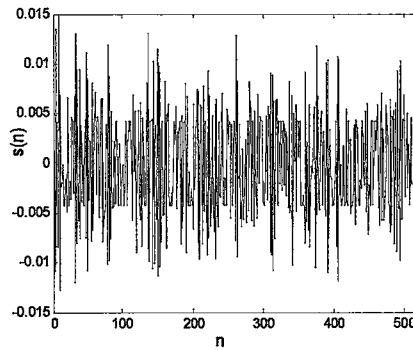
Şekil 3.1 (a)'da içerisine bir damga bitinin ekleneceği, 512 örneklilik orijinal ses işareti görülmektedir. Orijinal ses işaretinin frekans uzayı gösterimi Şekil 3.1 (b)'de görülmekte olup; bu işarete yayılı izge yöntemiyle gömülen gizli anahtarın zaman uzayı gösterimi Şekil 3.1 (c)'de, frekans uzayı gösterimi Şekil 3.1 (d)'de görülmektedir. Damgalanmış ses çerçevesine ait zaman uzayı gösterimi Şekil 3.1 (e)'de ve frekans uzayı gösterimi Şekil 3.1 (f)'de görülmektedir. Eklenen gizli anahtar işareti, duyulamazlık kriterini sağlamak açısından, düşük genlikli olup orijinal ses çerçevesi üzerinde zaman ve frekans uzayında büyük değişikliklere yol açmamaktadır.



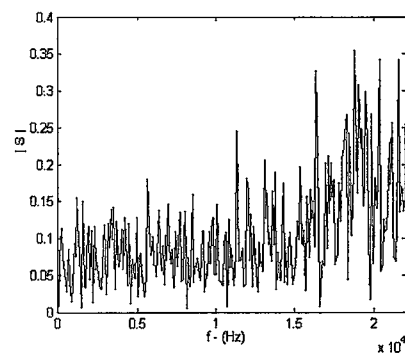
(a)



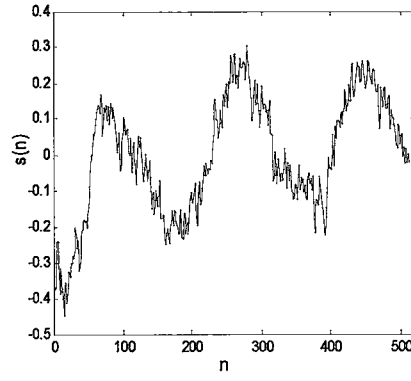
(b)



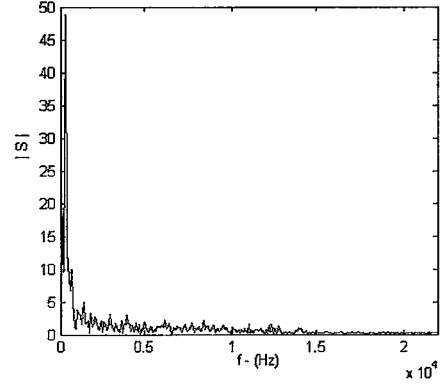
(c)



(d)



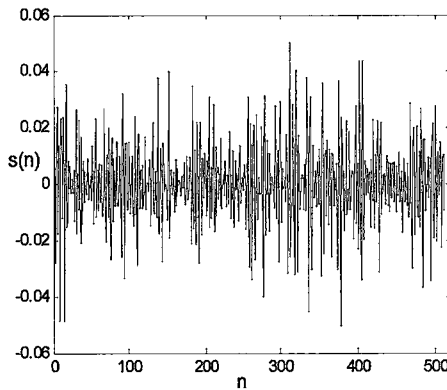
(e)



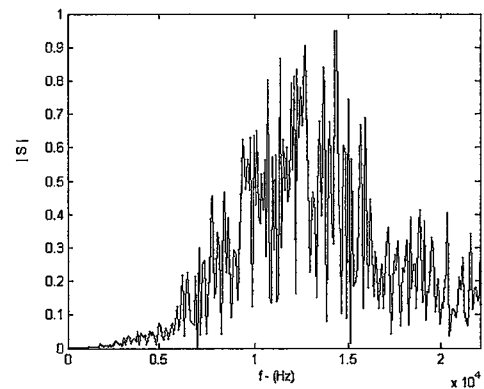
(f)

Şekil 3.1. (a) Orijinal ses işareti zaman uzayı gösterimi. (b) Orijinal ses işareti frekans uzayı gösterimi. (c) Eklenen gizli anahtar işareti zaman uzayı gösterimi. (d) Eklenen gizli anahtar işareti frekans uzayı gösterimi. (e) Damgalanmış ses işareti zaman uzayı gösterimi. (f) Damgalanmış ses işareti frekans uzayı gösterimi.

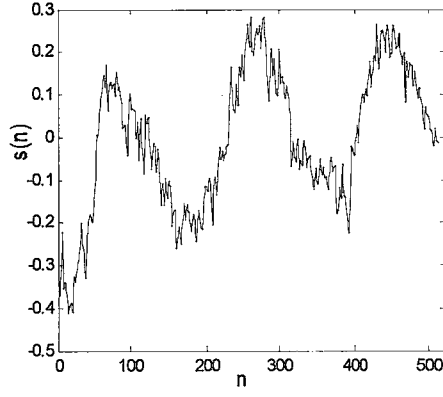
Şekil 3.1 (e)'deki damgalanmış ses işaretine (3.2) ile tanımlı dalgacık gürültü süzme ve (3.3) ile tanımlı gizli anahtar işareti ayrıştırma işlemlerinin uygulanmasıyla elde edilen gizli anahtar işaretinin zaman uzayı gösterimi Şekil 3.2 (a)'da, frekans uzayı gösterimi Şekil 3.2 (b)'de görülmektedir. Benzer olarak (3.2) ile tanımlı dalgacık gürültü süzme ile elde edilen orijinal ses işaretinin kestiriminin zaman uzayı gösterimi Şekil 3.2 (c)'de ve frekans uzayı gösterimi Şekil 3.2 (d)'de görülmektedir. Orijinal ses işaretinin kestiriminin zaman ve frekans uzayı değerleri sırasıyla, Şekil 3.1 (a) ve Şekil 3.1 (b)'de görülen damgalanmamış orijinal ses işaretinin zaman ve frekans uzayı değerlerine çok yakındır. Şekillerden görüldüğü gibi, tek bir damga bitinin eklendiği ses çerçevesinde, dalgacık gürültü süzme ile orijinal ses işaretine çok yakın bir işaret elde edilebilmektedir.



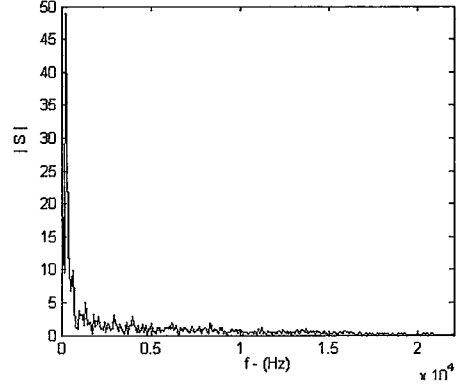
(a)



(b)



(c)



(d)

Şekil 3.2. (a) Dalgacık dönüşümü ile ayrıştırılan gizli anahtar işareti. (b) (a)' da görülen ayrıştırılmış anahtar işaretinin frekans uzayı gösterimi. (c) Kestirilmiş orijinal ses işaretinin zaman uzayı gösterimi. (d) Kestirilmiş orijinal ses işaretinin frekans uzayı gösterimi.

Damga çözme; özilinti analizine göre gerçekleştirildiğinden yayılı izge yöntemine göre damgalanmış ses işaretlerinde alınan damgalı işaret ile orijinal gizli anahtar arasındaki özilinti fonksiyonlarının τ bağlı değişimi elde edilmiştir. Damgalanmış ses çerçevesi ile eklenen gizli anahtar arasındaki özilinti değerlerinin τ ' ya bağlı değişimi (3.8) formül kullanılarak hesaplanmaktadır.

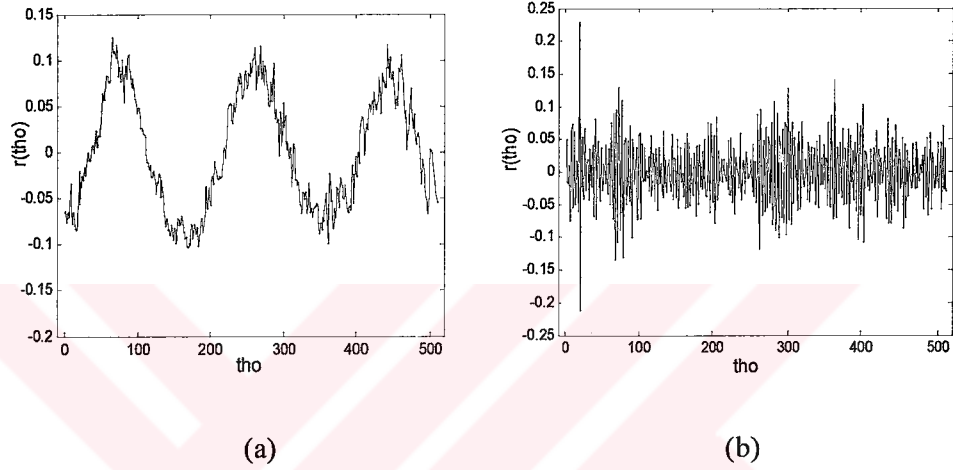
$$r_i(\tau) = \frac{\sum_{n=0}^{M-1} (k(n) - \langle k \rangle) (s_{i_R}^t(n + \tau) - \langle s_{i_R}^t(\tau) \rangle)}{\sqrt{\sum_{n=0}^{M-1} (k(n) - \langle k \rangle)^2} \sqrt{\sum_{n=0}^{M-1} (s_{i_R}^t(n + \tau) - \langle s_{i_R}^t(\tau) \rangle)^2}} \quad (3.8)$$

(3.8)' de $s_{i_R}^t(n)$ kanaldan alınan ses işaretinin her bir örneğini gösterirken, $k(n)$ gizli anahtar işaretine ait her bir örnek değerini, k gizli anahtar vektörünü göstermektedir. $r_i(\tau)$ her bir τ değerine karşı düşen özilinti değerini belirtmekte olup, +1,-1 arasında normalize değerler almaktadır. $\langle \cdot \rangle$ ortalama değer işlemi olup (3.9)'daki gibi hesaplanır.

$$\langle s_{i_R}^t(\tau) \rangle = \frac{1}{M} \sum_{n=0}^{M-1} s_{i_R}^t(n + \tau) \quad (3.9)$$

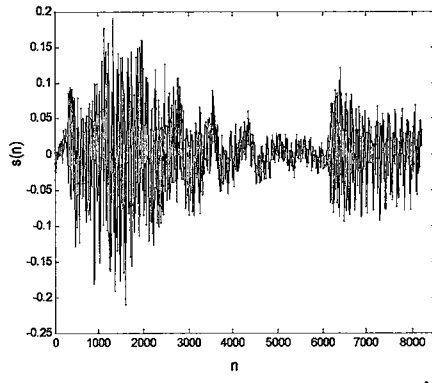
İçerisine bir bit damga bilgisi gömülmüş ses işareti için (3.8)'deki formüle göre elde edilen özilinti fonksiyonunun τ ya bağlı değişimi Şekil 3.3 (a)'da görülmektedir. Şekildeki özilinti değerlerinden hiç biri ayırt edici tepe noktası oluşturmamaktadır. Bu

da veri senkronizasyonunun sağlanmasında kullanılan τ_{sync} değerinin bulunmasını güçleştirmektedir. Bu problemi ortadan kaldırmak amacıyla (3.2) ile tanımlı dalgacık gürültü süzme ve (3.3) ile tanımlı ayrıştırma işlevleri kullanılarak, gizli anahtar işareti ayrıştırılmış ve eklenen gizli anahtar işareti arasındaki ötilinti değlerlerinin τ ya bağıl değışimi (3.4) formülüne göre hesaplanarak Şekil 3.3 (b)'deki değışim elde edilmiştir. Şekil 3.3 (b)'den görüldüğü gibi, τ 'ya bağıl ötilinti grafiğinde Şekil 3.3 (a)'da görülen veri senkronizasyonunda kullanılacak τ_{sync} değlerinin bulunamaması sorunu ortadan kalkmıştır ve incelenen çerçeve boyunca ötilinti tek bir τ_{sync} değeri için enbüyüklenmektedir.

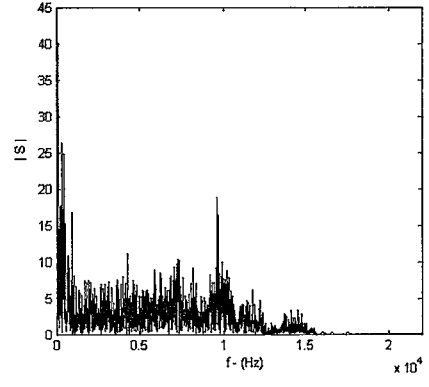


Şekil 3.3. (a) Damgalı ses işareti ile damgalamada kullanılan gizli anahtar arasındaki ötilinti fonksiyonunun τ ya bağıl değışimi. (b) Dalgacık gürültü süzme ile ayrıştırılan gizli anahtar işareti ile damgalamada kullanılan orijinal anahtar arasındaki ötilinti fonksiyonunun τ ya bağıl değışimi.

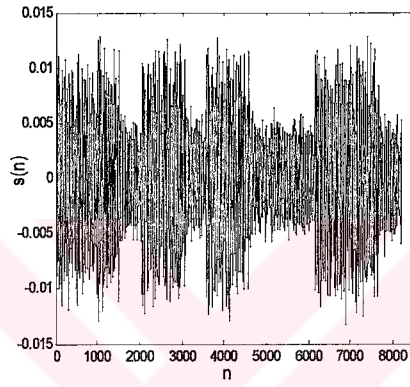
Tez kapsamında yapılan çalışmalarda; dalgacık dönüşümü yardımıyla gizli anahtar işaretinin ayrıştırılması, eklenen bir damga katarının tamamı uzunluğundaki ses işaretleri üzerinde de incelenmiştir. 16 bit uzunluğundaki damga katarının ekleneceği orijinal ses işareti Şekil 3.4 (a)'da ve bu ses işaretine ait frekans uzayı gösterimi Şekil 3.4 (b)'de görülmektedir. 16 bit uzunluğundaki damga katarı, Şekil 3.4 (c)'de zaman uzayı gösterimi, Şekil 3.4 (d)'de de frekans uzayı gösterimi görülen gizli anahtar işareti yardımıyla yayılı izge yöntemine göre orijinal ses işaretine eklenmiştir. Damgalanmış ses işaretine ait zaman uzayı gösterimi Şekil 3.4 (e)'de ve frekans uzayı gösterimi Şekil 3.4 (f)'de görülmektedir.



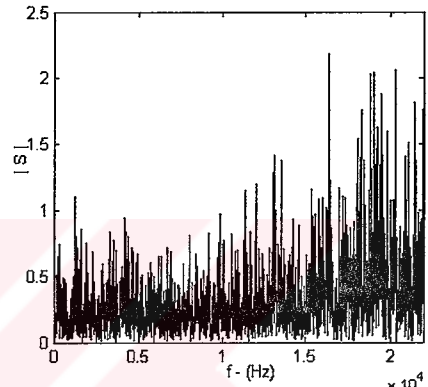
(a)



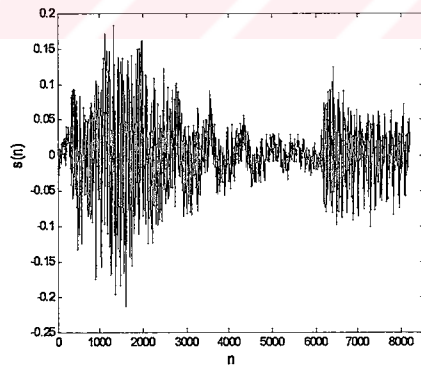
(b)



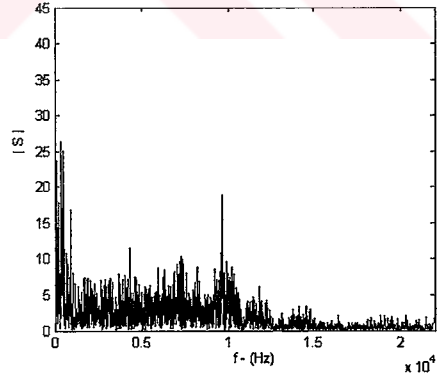
(c)



(d)



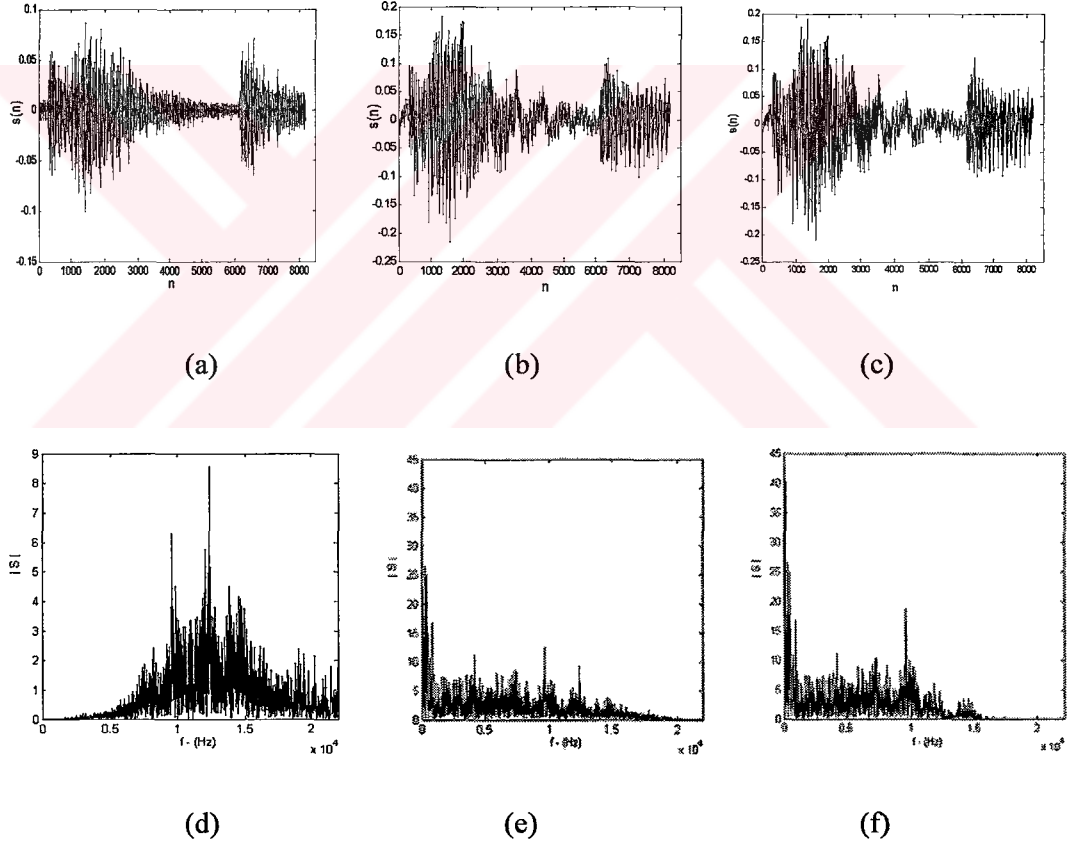
(e)



(f)

Şekil 3.4. (a) 16 bit lik damga bloğu eklenecek orijinal ses işareti. (b) (a)'daki ses işaretinin frekans uzayı gösterimi. (c) 16 bitlik damga bloğu içeren anahtar işareti. (d) (c)'deki anahtar işaretinin frekans uzayı gösterimi. (e) Damgalanmış ses işareti. (f) Damgalanmış ses işaretinin frekans uzayı gösterimi.

Şekil 3.4 (e)'de gösterilen damgalanmış ses işaretinden eklenen gizli anahtar işaretini çıkarmak için, (3.2) ile tanımlı dalgacık gürültü süzme ve (3.3) ile tanımlı ayrıştırma işlemleri uygulanmıştır. Ayrıştırılan gizli anahtar işaretinin zaman uzayı gösterimi Şekil 3.5 (a)'da ve kestirilmiş orijinal ses işaretinin zaman uzayı gösterimi Şekil 3.5 (b)'de görülmektedir. Kestirilmiş orijinal ses işaretinin zaman uzayı bileşenleri, Şekil 3.5 (c)'de zaman uzayı bileşenleri gösterilen orijinal damgalanmamış ses işaretine yakın değerler içermektedir. Benzer olarak, dalgacık dönüşümü ile ayrıştırılan gizli anahtar işaretinin frekans uzayı gösterimi Şekil 3.5 (d)'de görülmektedir. Kestirilen orijinal ses işaretinin frekans uzayı gösterimi Şekil 3.5 (e)'de görülürken, Şekil 3.5 (f)'de orijinal damgalanmamış ses işaretinin frekans uzayı görülmektedir. Kestirilen orijinal ses işareti frekans uzayında da, zaman uzayında olduğu gibi, damgalanmamış orijinal ses işaretine yakın değerlere sahiptir.



Şekil 3.5 (a) Dalgacık dönüşümü ile ayrıştırılan damga işareti. (b) Damgalanmış işareten kestirilen orijinal ses işareti. (c) Orijinal ses işareti. (d) (a)'daki işaretin frekans uzayı gösterimi. (e) (b)'deki işaretin frekans uzayı gösterimi. (f) (c)'deki işaretin frekans uzayı gösterimi.

3.5 Damga-Sinyal-Oranı ve Gürültü-Sinyal-Oranı

Belirli bir damga katarı için ayrıştırılan gizli anahtar işaretinin gücünün orijinal ses işaretinin gücüne oranı olarak tanımlanabilen WSR (damga-sinyal oranı) ve eklenen damga işaretinin gücünün orijinal ses işaretinin gücüne oranı olarak tanımlanabilen WSR değerleri damga çözme analizinde önem taşımaktadır.

$\hat{e}$ ayrıştırılan damga işareti ve orijinal ses işareti arasındaki WSR, 16 bit uzunluğundaki damga katarındaki her bir ses çerçevesi için (3.10)' deki formül kullanılarak hesaplanır.

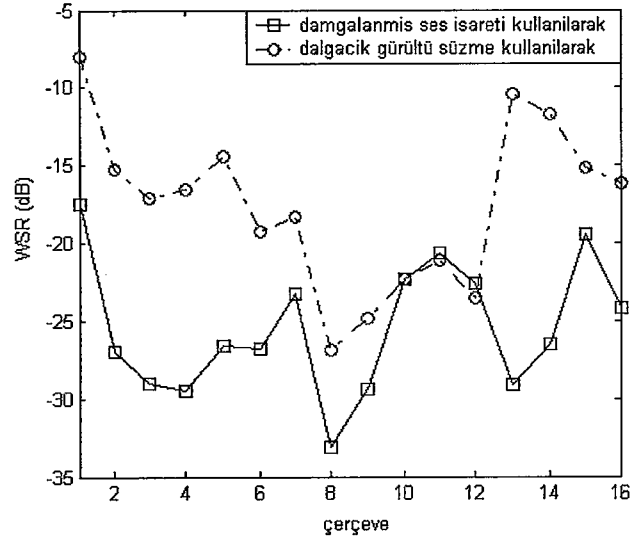
$$WSR(s'_i, \hat{e}) = 10 \log_{10} \left\{ \frac{\sum_{n=0}^{N-1} [\hat{e}(n)]^2}{\sum_{n=0}^{N-1} [s'_i(n)]^2} \right\} \text{ dB} \quad (3.10)$$

(3.10)'da $s'_i(n)$ orijinal işaretin i . çerçevesine ait t . yinelemedeki her bir ses örneğinin değerini, $\hat{e}(n)$ ayrıştırılan damga işaretinin her bir çerçevedeki örnek değerlerini, N çerçeve uzunluğunu göstermektedir.

Damgalı işaret ve orijinal ses işareti arasındaki WSR, damga katarındaki her bir çerçeve için (3.11) formülü kullanılarak hesaplanır.

$$WSR(s'_i, s'_{iM}) = 10 \log_{10} \left\{ \frac{\sum_{n=0}^{N-1} [s'_i(n) - s'_{iM}(n)]^2}{\sum_{n=0}^{N-1} [s'_i(n)]^2} \right\} \text{ dB} \quad (3.11)$$

(3.11)'de $s'_i(n)$ orijinal işaretin i . çerçevesine ait t . yinelemedeki örnek değerlerini gösterirken $s'_{iM}(n)$ damgalanmış örnek değerlerini, N çerçeve uzunluğunu göstermektedir.



Şekil 3.6. Dalgacık ayrıştırma ile elde edilen damga işareti ile orijinal ses işareti arasındaki WSR ların 16 ses çerçevesi boyunca değişimi (kesik çizgi). Orijinal damgalı işaret ile orijinal ses işareti arasındaki WSR lerin 16 ses çerçevesi boyunca değişimi (düz çizgi).

Şekil 3.6'da eklenen gizli anahtar işaretinin ve dalgacık dönüşümü ile ayrıştırılan gizli anahtar işaretinin, orijinal ses işaretine oranı olan WSR değerlerinin 16 bitlik çerçeveler için dB cinsinden değerleri görülmektedir. Eklenen gizli anahtar ve orijinal ses işareti arasındaki WSR düz (-) çizgiler ile gösterilmiş olup, dalgacık dönüşümü ile ayrıştırılan gizli anahtar işareti ve orijinal ses işareti arasındaki WSR kesik çizgilerle (-.-) belirtilmiştir. Şekil 3.6'da görüldüğü gibi, dalgacık dönüşümü ile ayrıştırılan gizli anahtar işaretinin enerjisi, damgalama sırasında eklenen gizli anahtar işaretinin enerjisinden daha fazladır.

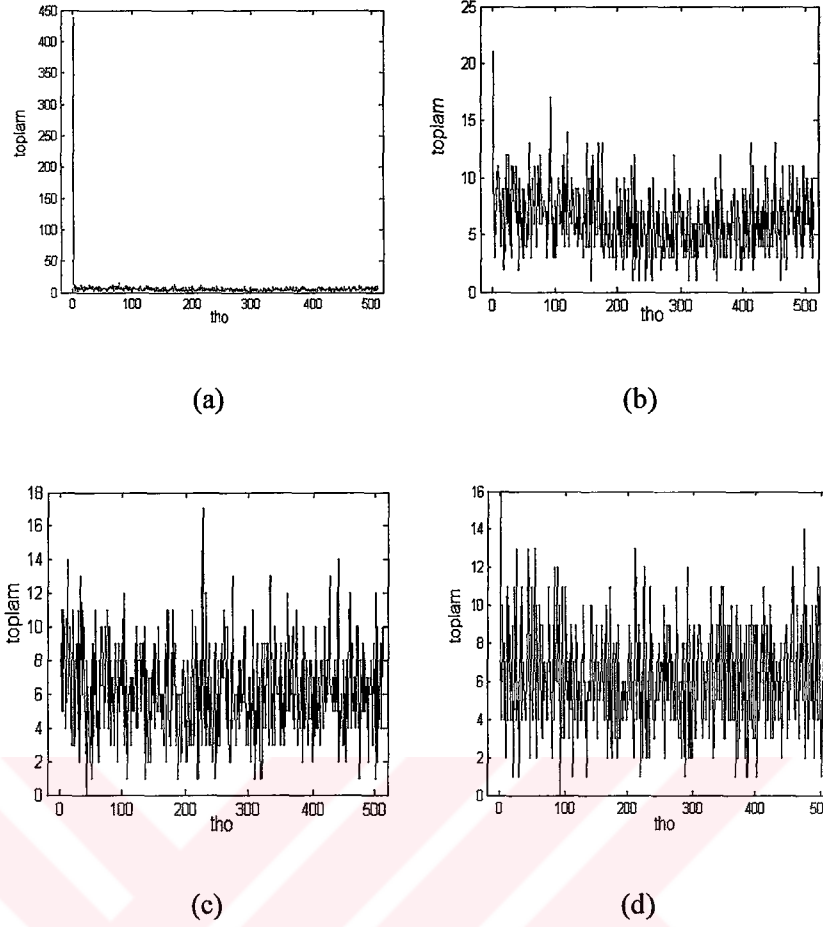
Bölüm 3.2'de veri senkronizasyonunun; eklenen gizli anahtar işareti ve dalgacık dönüşümü ile ayrıştırılan gizli anahtar işareti arasındaki en büyük ötilinti değerlerini veren τ' ların histogramı yardımıyla elde edildiği belirtilmişti. Tez çalışmasının bu bölümünde yayılı izge yöntemine göre damgalanmış ses işaretleri için τ histogramlarının değişimi incelenmiştir. 36 sn' lik ses işareti yayılı izge yöntemine dayalı damgalama ile ortalama WSR=-21 dB olacak şekilde damgalanmıştır. Şekil 3.7 (a)'da damgalanmış ses işareti ile gizli anahtar işareti arasında (3.8) formülü kullanılarak elde edilen ötilinti fonksiyonunda, en büyük ötilinti değerlerini veren τ' ların histogramı görülmektedir. Histogramdaki en büyük değer $\tau=0$ için bulunmuştur.

Şekil 3.7 (a)' da görüldüğü gibi herhangi bir dönüşüm uygulamadan hesaplanan özilinti değeri senkronizasyon bilgisini doğru bir şekilde verebilmektedir. Fakat önceki bölümlerde de belirtildiği üzere (Bkz Bölüm 3.2) gürültüsüz kanal iletimleri genellikle mümkün olmamaktadır. Bu açıdan histogram değerlerinin eklenebilir beyaz Gauss gürültüsü ile değişimi irdelenmelidir. Şekil 3.7 (a)'da τ histogramı görülen damgalanmış ses işareti üzerine SNR değeri (3.12)'deki formüle göre 10 dB olacak şekilde beyaz Gauss gürültüsü eklenmiştir.

$$SNR = 10 \log_{10} \left\{ \frac{\sum_{n=0}^{N-1} [s'_{i_{MM}}(n)]^2}{\sum_{n=0}^{N-1} [n(n)]^2} \right\} \quad (3.12)$$

(3.12)'de $n(n)$ beyaz Gauss gürültüsüne ait her bir örnek değerini gösterirken, $s'_{i_{MM}}(n)$ damgalanmış ses işaretine ait her bir örneği göstermektedir.

Damgalanmış gürültülü ses işareti ve eklenen gizli anahtar işareti arasında elde edilen özilinti fonksiyonu içerisinde en büyük özilinti değerlerini veren τ ' ların histogramı Şekil 3.7 (b)'de görülmektedir. Gürültü, histogramda bozulmalara yol açmakta ve en büyük değere sahip τ 'nun ayrımını güçleştirmektedir. Bu durum damga çözme aşamasında veri senkronizasyonu problemini ortaya çıkarmaktadır. Şekil 3.7 (c)'de damgalanmış ses işareti üzerine SNR değeri 5 dB ve Şekil 3.7 (d)'de SNR değeri 0 dB olacak şekilde beyaz Gauss gürültüsü eklenmiş ses işaretleri ve eklenen gizli anahtar işareti arasında elde edilen özilinti fonksiyonunda en büyük özilinti değerlerini veren τ 'ların histogramları görülmektedir. Eklenen gürültünün enerjisi arttıkça, histogramda en büyük değere sahip τ değerinin ayrımı zorlaşmaktadır.

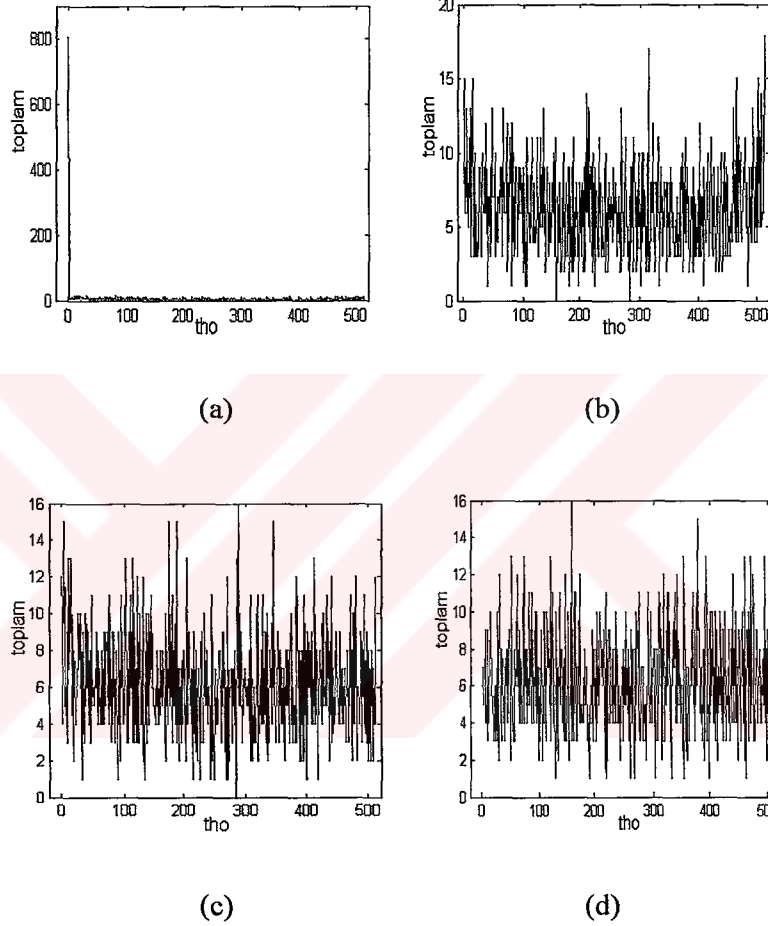


Şekil 3.7. (a) Damgalanmış ses işareti ve gizli anahtar arasındaki özilintilerin enbüyük olduğu noktaların τ 'ya bağlı histogramı. Gürültülü damgalanmış ses işareti ve gizli anahtar arasındaki enbüyük olduğu noktaların τ 'ya bağlı histogramı (b) SNR=10 dB, (c) SNR=5 dB, (d) SNR = 0 dB.

Tez kapsamında, doğrudan damgalanmış ses işaretleri yerine, yayılı izge yöntemine dayalı damgalanmış ses işaretlerinin dalgacık gürültü süzme işleminden geçirilmesi sonucunda elde edilen gizli anahtar işareti kullanılmasının τ histogramına etkisi de incelenmiştir. Ayırıştırılan gizli anahtar işareti ile eklenen gizli anahtar arasındaki (3.8) formülü ile bulunan özilinti fonksiyonunda en büyük özilinti değerlerini veren τ 'ların histogramları bulunmuştur. Şekil 3.8 (a)'da; Şekil 3.7 (a)'da τ histogramı elde edilen ses işareti üzerinde (3.2) ile tanımlı dalgacık gürültü süzme ve (3.3) ile tanımlı ayırıştırma ile elde edilen gizli anahtar işareti ve eklenen orijinal gizli anahtar işareti kullanılarak bulunan τ histogramı görülmektedir. Ayırıştırılan gizli anahtar işareti için elde edilen τ histogramının $\tau=0$ daki değeri, orijinal damgalanmış işaret için elde edilen τ histogramının $\tau=0$ daki değerinin yaklaşık iki katıdır. Şekil 3.8 (b), (c) ve (d) de sırasıyla, SNR=10 dB ve SNR=5 dB, ve SNR=0 dB için aynı işlemler tekrarlanarak elde edilen histogramlar görülmektedir. Histogramlardaki τ

değerlerinin ayırt edici tepe değere sahip olmaması; doğru damga çözme olasılığını azaltmakta ve senkronizasyon bilgisinin kaybolmasına neden olmaktadır.

Yayılı izge yöntemine dayalı damgalama-damga çözme, gürültülü ortamlarda damga çözme performansını düşürecek sorunlara neden olmaktadır. Bundan sonraki bölümde yayılı izge yöntemi için gerçekleştirilen damga çıkarımları kullanılan uyarlanırlı damgalama yöntemi için tekrarlanacak ve başarımın nasıl değiştiği irdelenecektir.

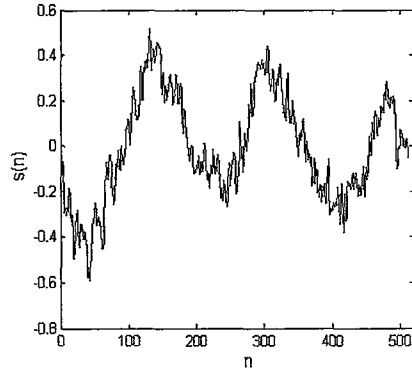


Şekil 3.8. (a) Damgalanmış ses işaretinden dalgacık ayrıştırma ile elde edilen anahtar ve orijinal gizli anahtar arasındaki özilintilerin enbüyük olduğu noktaların τ 'ya bağlı histogramı. Gürültülü damgalanmış ses işaretinden dalgacık ayrıştırma ile elde edilen anahtar ve gizli anahtar arasındaki özilintilerin enbüyük olduğu noktaların τ 'ya bağlı histogramı (b) SNR=10 dB, (c) SNR=5 dB, (d) SNR = 0 dB.

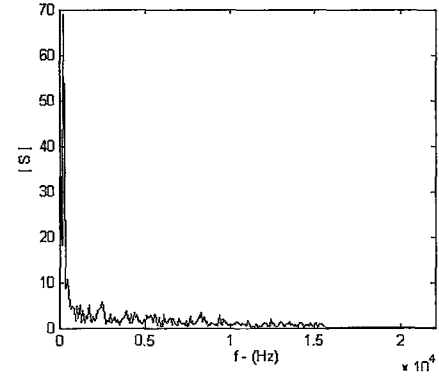
3.6 Uyarlanır Damgalama ile Damgalanmış Ses Verisinde Damga Çözme

Yayılı izge yöntemine dayalı damgalamada dalgacık gürültü süzme gürültüsüz veri iletimlerinde başarıyı arttırmakta, ancak gürültülü iletimlerde aynı başarıya ulaşılamamaktadır. Önceki bölümlerde de belirtildiği gibi, telli, telsiz, akustik, ve benzeri iletişim kanallarından gürültüsüz veri iletimi yapmak çok zor ve nerdeyse imkânsızdır. Bunun yanında, tezin giriş kısmında damgalama sistemlerinin kanal gürültüsüne, dijital-analog / analog-dijital dönüşümlere, filtrelemeye, yeniden örnekleme, kırılma ve kayıplı sıkıştırma gibi ataklara karşı dayanıklı olması gerektiğine değinilmişti. Tez kapsamında kullanılan uyarlanır damgalama yöntemi hem iletim hatalarına hem de belirtilen ataklara karşı gürbüzdür.

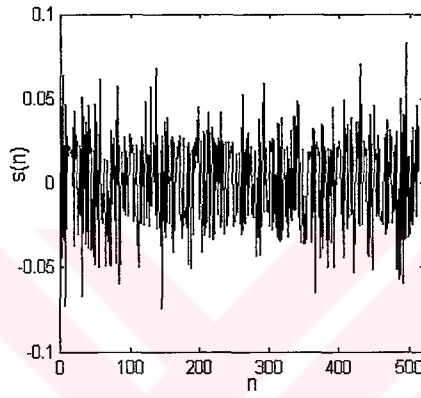
Bölüm 2.1' de belirtildiği gibi, uyarlanır damgalama yöntemi eklenen damganın doğru çözülüp çözülmediğini damgalama sırasında kontrol etmekte ve bu sayede alıcıdaki damga çözme hatasını enküçükmektedir. Damgalama işlemi sırasında herhangi bir ses çerçevesi 1'den fazla maskelenebilmekte ve her bir aşamada düşük WSR değerlerinde ekleme yapılarak ses bozulmamaktadır. Tezin bu aşamasında uyarlamalı damgalama sırasında birden fazla özyinelemenin olduğu ses çerçevelerinde, eklenen damganın gürültü süzme işlemi ile ayrıştırılması irdelenmiştir. Şekil 3.9 (a)' da 1 damga bitinin ekleneceği 512 örneklilik orijinal ses işaretinin zaman uzayı gösterimi ve Şekil 3.9 (b)'de de frekans uzayı gösterimi görülmektedir. Uyarlanır damgalama yöntemi kullanılarak Şekil 3.9 (a)'daki ses çerçevesine 9 özyineleme sonucunda Şekil 3.9 (c)'de zaman uzayı gösterimi ve Şekil 3.9 (d)'de frekans uzayı gösterimi görülen gizli anahtar işareti eklenmiştir. 9 özyineleme işlemi sonucunda elde edilen damgalanmış ses işaretine ait zaman uzayı gösterimi Şekil 3.9 (e)'de ve frekans uzayı gösterimi Şekil 3.9 (f)'de görülmektedir. Damgalama sırasında her bir özyineleme işleminde WSR nin düşüklüğü korunabilmekte bu durum duyulmazlık kriterine uyulmasını garantilemektedir. Özyineleme işlemi aynı zamanda toplam WSR oranında çıkılabilecek en yüksek kapasiteye erişilmesini sağlamaktadır.



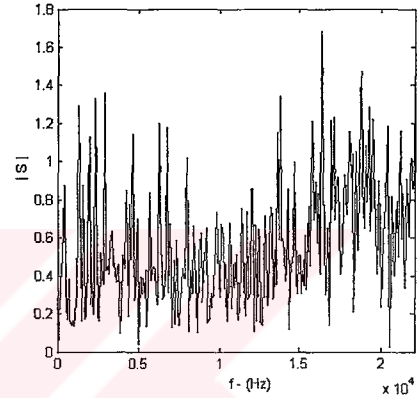
(a)



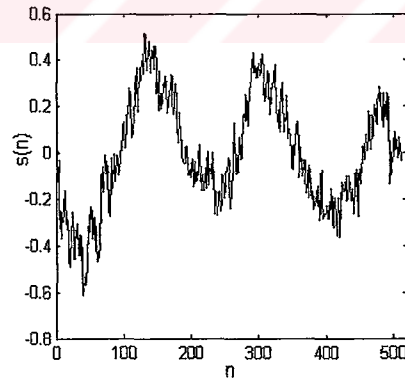
(b)



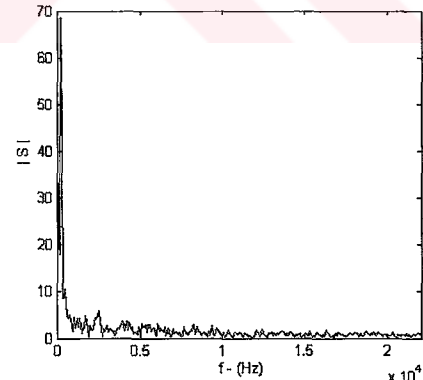
(c)



(d)



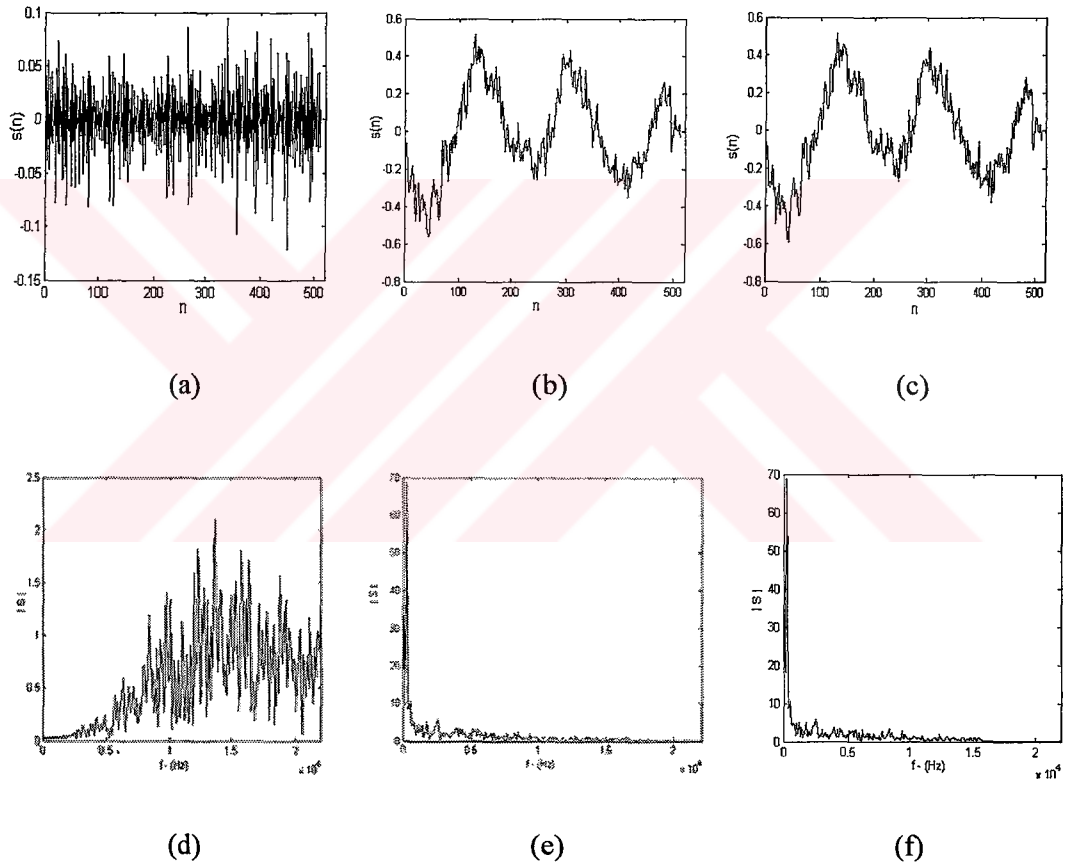
(e)



(f)

Şekil 3.9. (a) Orijinal ses çerçevesi. (b) (a)'daki ses çerçevesine ait frekans uzayı gösterimi. (c) 9 özyineleme sonucu eklenen toplam gizli anahtar işareti (d) (c)'deki gizli anahtar işaretinin frekans uzayı gösterimi. (e) (a)'daki ses çerçevesine (c)'deki damga işaretinin eklenmesi sonucu elde edilen damgalanmış ses çerçevesi. (f) Damgalanmış ses çerçevesinin frekans uzayı gösterimi.

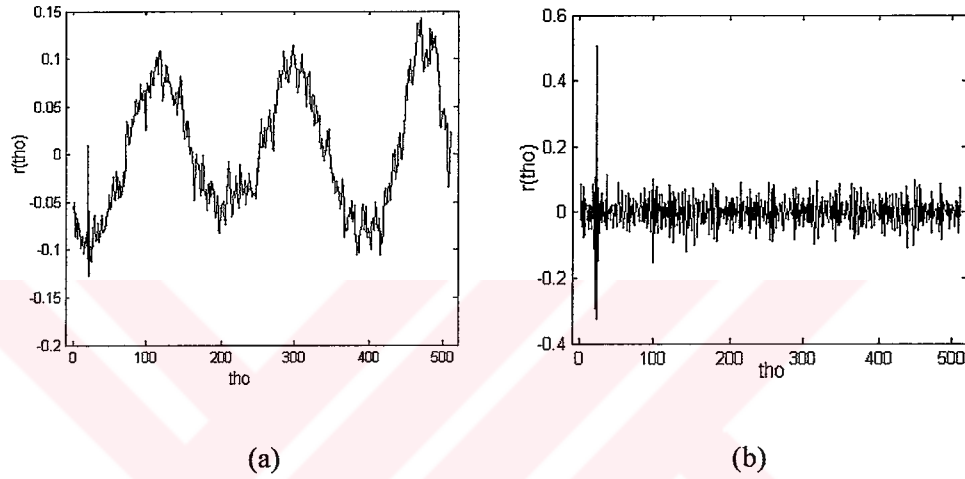
Şekil 3.9 (e)'deki damgalanmış ses çerçevesine dalgacık gürültü süzme ve gizli anahtar ayrıştırma uygulandıktan sonra elde edilen gizli anahtar işareti Şekil 3.10 (a)'da görülmektedir. (3.2) formülü ile kestirimi gerçekleştirilen orijinal ses işareti Şekil 3.10 (b)'de ve orijinal damgalanmamış ses işareti Şekil 3.10 (c)'de görülmektedir. Benzer olarak Şekil 3.10 (d)'de ayrıştırılan gizli anahtar işaretine ait frekans uzayı görülürken, kestirilen orijinal ses işareti ve damgalanmamış orijinal ses işaretine ait frekans uzayı gösterimleri sırasıyla, Şekil 3.10 (e) ve Şekil 3.10 (f)'de görülmektedir. Zaman ve frekans uzayı gösterimlerinden görülebileceği gibi; dalgacık ayrıştırma sonucunda kestirilen orijinal ses çerçevesi, damgalanmamış orijinal ses işaretine yakın değerler içermektedir.



Şekil 3.10. (a) Dalgacık dönüşümü ile ayrıştırılan gizli anahtar işareti. (b) Kestirilen orijinal ses çerçevesi. (c) Orijinal ses çerçevesi. (d) (a)'daki işaretin frekans uzayı gösterimi. (e) (b)'deki işaretin frekans uzayı gösterimi. (f) (c)'deki işaretin frekans uzayı gösterimi.

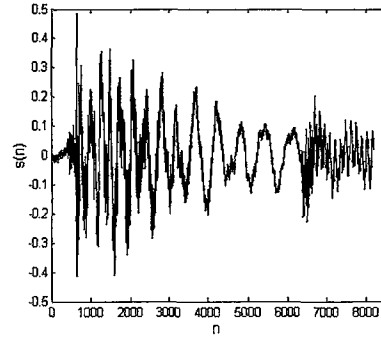
Uyarlanır damgalama yöntemi ile damgalanmış ses işaretinden ayrıştırılan gizli anahtar işareti üzerinde özilinti analizi gerçekleştirilmektedir. Daha iyi karşılaştırma yapabilmek açısından öncelikle damgalanmış ses işareti kullanılarak elde edilen

özilinti fonksiyonunun değişimi gösterilecektir. Şekil 3.11 (a)' da damgalanmış ses çerçevesi ve eklenen gizli anahtar arasında (3.8) formülü kullanılarak elde edilen özilinti fonksiyonunun τ ya bağlı değişimi görülmektedir. Grafikte görüldüğü gibi özilinti fonksiyonunda veri senkronizasyonunu sağlayacak herhangi bir tepe noktası bulunmamaktadır. Şekil 3.11 (b)' de dalgacık gürültü süzme ile ayrıştırılan gizli anahtar işareti ve eklenen gizli anahtar işareti arasında (3.4) formülü kullanılarak elde edilen özilinti değişimi görülmektedir. Grafikteki özilinti fonksiyonunda veri senkronizasyonunun sağlanması için gerekli τ değeri kolaylıkla bulunabilmektedir.

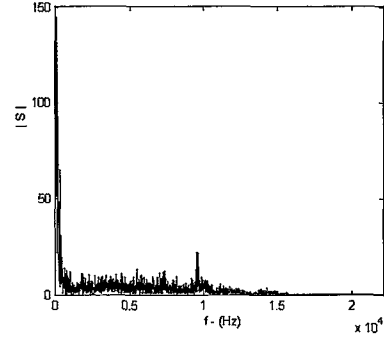


Şekil 3.11. (a) Damgalı ses işareti ile damgalamada kullanılan gizli anahtar arasındaki özilinti fonksiyonunun τ ya bağlı değişimi. (b) Dalgacık gürültü süzme ile ayrıştırılan anahtar ile damgalamada kullanılan orijinal anahtar arasındaki özilinti fonksiyonunun τ ya bağlı değişimi.

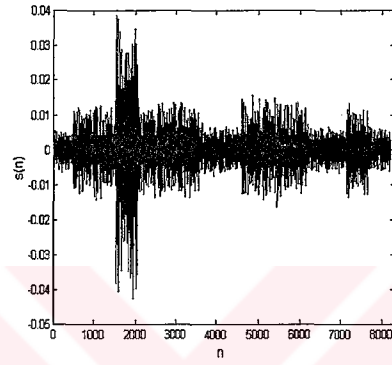
Bir sonraki adımda, uyarlanır damgalama yöntemiyle damgalanmış bir damga biti taşıyan ses işareti için gerçekleştirilen dalgacık gürültü süzmeye dayalı gizli anahtar bilgisi ayrıştırma, 16 bitlik damga katarı ile damgalanmış ses işareti için incelenmiştir. Şekil 3.12 (a)'da 16 bitlik damga bilgisinin ekleneceği orijinal ses işaretinin zaman uzayı gösterimi, Şekil 3.12 (b)'de frekans uzayı gösterimi görülmektedir. Şekil 3.12 (c)'de görülen 16 bitlik damga bilgisi taşıyan gizli anahtar işareti, uyarlanır damgalama yöntemine göre Şekil 3.12 (a)'daki ses işaretine gömülmüştür. Eklenen gizli anahtar işaretine ait frekans uzayı gösterimi Şekil 3.12 (d)'de görülmektedir. Eklenen gizli anahtar işaretinin 3. çerçevesinde 5 kez özyineleme işlemi gerçekleştirilmiş olup, damgalanmış ses işaretinin zaman uzayı gösterimi Şekil 3.12 (e)'de ve frekans uzayı gösterimi Şekil 3.12 (f)'de görülmektedir.



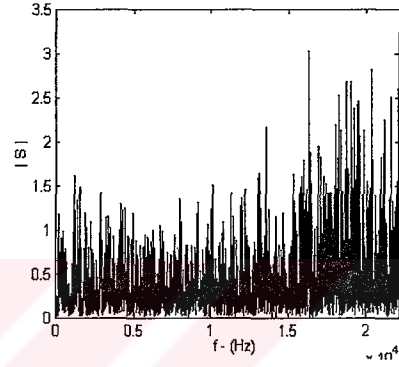
(a)



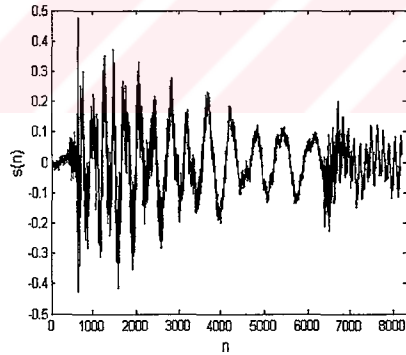
(b)



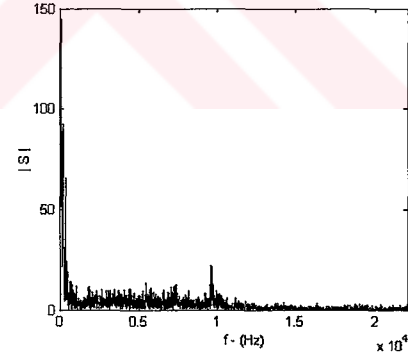
(c)



(d)



(e)

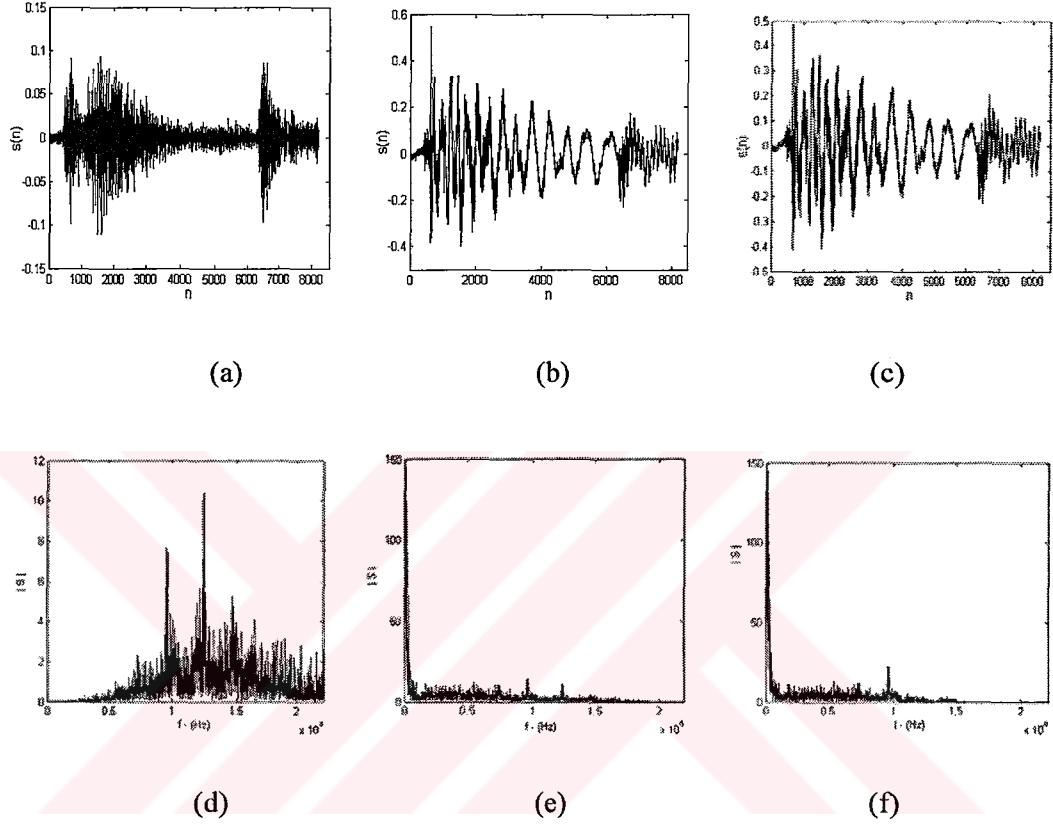


(f)

Şekil 3.12. (a) 16 bit lik damga bloğu eklenecek orijinal ses işareti. (b) (a)'daki ses işaretinin frekans uzayı gösterimi. (c) 16 bitlik damga bloğu içeren gizli anahtar işareti. (d) (c)'deki anahtar işaretinin frekans uzayı gösterimi. (e) Damgalanmış ses işareti. (f) Damgalanmış ses işaretinin frekans uzayı gösterimi,

Damgalanmış ses işaretine dalgacık gürültü süzme ve gizli anahtar işaretini ayrıştırma işlemleri uygulanarak eklenen gizli anahtar işareti ayrıştırılmıştır. Ayrıştırılan gizli anahtar işaretinin zaman uzayı gösterimi Şekil 3.13(a)'da frekans

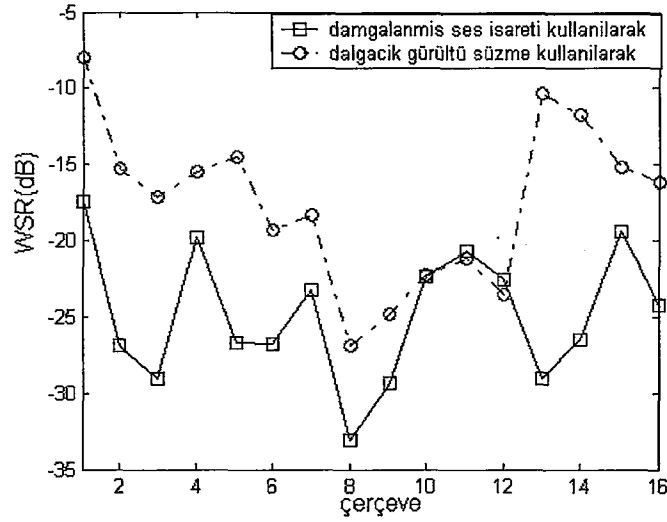
uzayı gösterimi Şekil 3.13(d)'de görülmektedir. Dalgacık dönüşümü yardımıyla kestirilen orijinal ses işareti Şekil 3.13(b)'de, bu ses işaretine ait frekans uzayı gösterimi Şekil 3.13 (e)'de görülmektedir. Kestirilen ses işareti Şekil 3.13(c)'de zaman uzayı ve Şekil 3.13 (f)'de de frekans uzayı gösterilen orijinal ses işaretine çok yakın değerler içermektedir.



Şekil 3.13. (a) Dalgacık dönüşümü ile ayrıştırılan damga işareti. (b) Dalgacık dönüşümü ile kestirilen orijinal ses işareti. (c) Damgalanmamış orijinal ses işareti. (d) (a)'daki işaretin frekans uzayı gösterimi. (e) (b)'deki işaretin frekans uzayı gösterimi. (f) (c)'deki işaretin frekans uzayı gösterimi.

Dalgacık dönüşümü ile ayrıştırılan gizli anahtar işareti ve orijinal ses işareti kullanılarak hesaplanan WSR değerlerinin değişimleri 16 bitlik çerçeveler için irdelenmiştir. Ayrıştırılan gizli anahtar işareti ve orijinal ses işareti arasındaki WSR değerleri (3.10) formülü kullanılarak hesaplanmış olup bulunan değerler Şekil 3.14'de kesik çizgilerle(-.-) belirtilmiştir. Eklenen damga ve orijinal ses işareti arasındaki WSR oranları (3.11) formülü kullanılarak hesaplanmış olup bulunan değerler Şekil 3.14' de düz (-) çizgiler ile gösterilmiştir. Dalgacık dönüşümü ile ayrıştırılan gizli anahtar işareti; çerçevelerin çoğunda, eklenen orijinal gizli anahtar

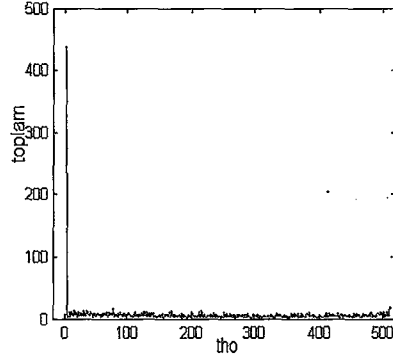
işaretinden daha fazla enerjiye sahip olup 10, 11 ve 12. çerçevelerde ayrıştırılan gizli anahtar işreti ve eklenen gizli anahtar işreti birbirine yakın enerjilere sahiptir.



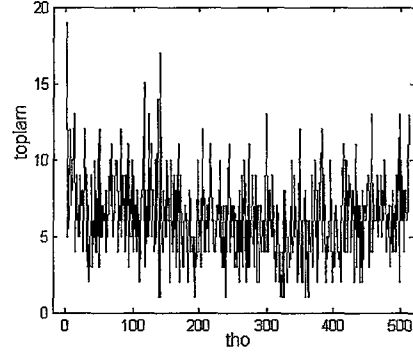
Şekil 3.14. Dalgacık ayrıştırma ile elde edilen damga işreti ile orijinal ses işreti arasındaki WSR ların 16 ses çerçevesi boyunca değişimi (kesik çizgi). Orijinal damgalı işaret ile orijinal ses işreti arasındaki WSR lerin 16 ses çerçevesi boyunca değişimi (düz çizgi).

Klasik yayılı izge damgalama yöntemi ile karşılaştırma yapabilmek amacıyla, uyarlanır damgalama yöntemi kullanılarak damgalanmış ses işaretlerinden dalgacık dönüşümü yardımıyla ayrıştırılan gizli anahtar işaretleri kullanılarak özilinti ve τ histogramı analizi yapılmıştır. Bu amaçla 36 sn' lik ses işreti ortalama WSR oranı -21 dB olacak şekilde uyarlanır damgalama yöntemiyle damgalanmıştır. Damgalanmış ses işreti ve eklenen gizli anahtar işreti arasındaki özilinti fonksiyonu (3.8) formülü kullanılarak hesaplanmıştır. Şekil 3.15 (a)'da, damgalanmış ses işreti ile eklenen gizli anahtar işreti arasında, her bir çerçevede elde edilen en büyük özilinti değerlerini sağlayan τ değerlerinin histogramı görülmektedir. Herhangi bir senkronizasyon kaybı gerçekleşmediği için histogramda en büyük değer $\tau=0$ için sağlanmaktadır. Aynı ses işreti üzerine SNR değeri 10 dB olacak şekilde beyaz Gauss gürültüsü eklenerek elde edilen ses işaretine ait τ histogramı Şekil 3.15 (b) görülmektedir. Benzer şekilde SNR=5 dB ve SNR=0 dB için elde edilen histogramlar sırasıyla, Şekil 3.15 (c) ve Şekil 3.15 (d) de görülmektedir. Şekil 3.15 (b), (c) ve (d) de görüldüğü gibi, beyaz Gauss gürültüsünün eklenmesiyle birlikte; histogramlarda her bir çerçeve için en büyük

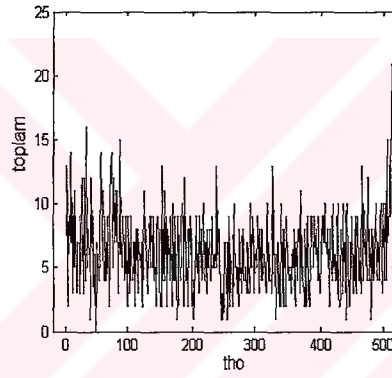
özilinti değerini sağlayan τ değerleri ayırt edilememektedir. Bu da veri senkronizasyonunu sağlayan τ_{sync} değerinin bulunmasını zorlaştırmakta ve doğru damga çözme olasılığını azaltmaktadır.



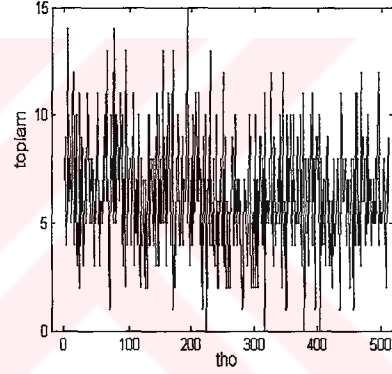
(a)



(b)



(c)

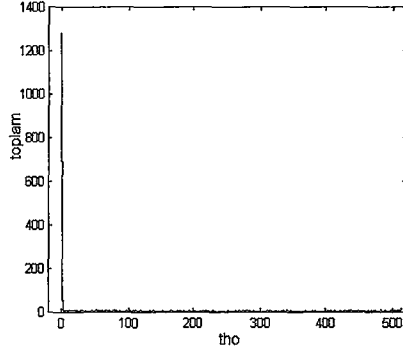


(d)

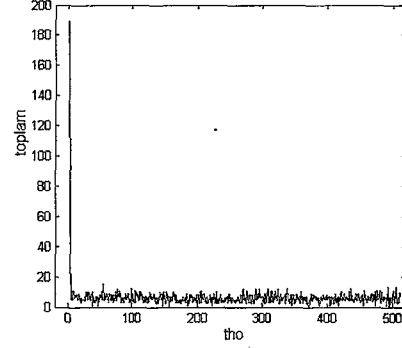
Şekil 3.15. (a) Damgalanmış ses işareti ve gizli anahtar arasındaki en büyük ilinti değerini sağlayan τ histogramı. (b) Gürültülü ses işareti için elde edilen τ histogramı (SNR=10 dB). (c) Gürültülü ses işareti için elde edilen τ histogramı (SNR=5 dB). (d) Gürültülü ses işareti için elde edilen τ histogramı (SNR=0 dB).

Dalgacık gürültü süzmenin etkisini gözlemlemek amacıyla, Şekil 3.15 teki sonuçların alındığı uyarlanır damgalama yöntemiyle damgalanmış ses işareti üzerinde, (3.2) formülü ile modellenen dalgacık gürültü süzme ve (3.3) formülü ile modellenen gizli anahtar ayrıştırma işlemleri gerçekleştirilerek ayrıştırılan gizli anahtar işareti için τ histogramları çıkarılmıştır. Histogramlar, ayrıştırılan gizi anahtar işareti ve eklenen gizli anahtar işareti arasında (3.4) formülü ile elde edilen özilinti fonksiyonunda en büyük özilinti değerlerini sağlayan τ değerleri için elde edilmiştir. Şekil 3.16 (a)'da; Şekil 3.15 (a)'da τ histogramı elde edilen damgalanmış ses işaretinden dalgacık

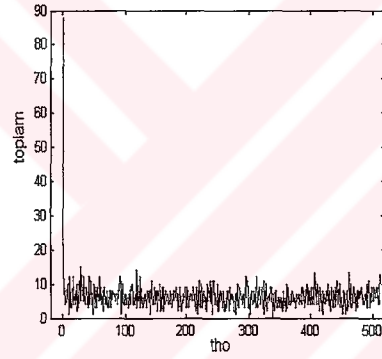
dönüşümü uygulanarak ayrıştırılan gizli anahtar işareti için elde edilen τ histogramı görülmektedir. $\tau=0$ da; dalgacık dönüşümü ile ayrıştırılan gizli anahtar işareti için elde edilen τ histogramı, herhangi bir dönüşüm gerçekleştirilmeden damgalanmış ses işareti için elde edilen τ histogramından daha büyük değerler içermektedir.



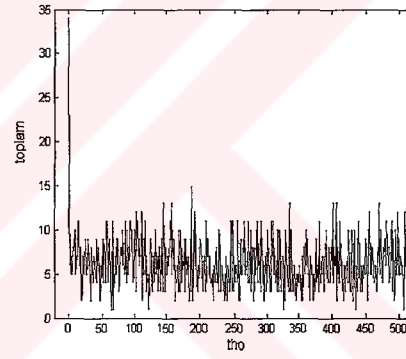
(a)



(b)



(c)



(d)

Şekil 3.16. (a) Damgalanmış ses işareti üzerinde dalgacık dönüşümü ile ayrıştırılmış anahtar bilgisinin eklenen gizli anahtar ile arasındaki en büyük özilintilerin τ 'ya bağlı histogramları. (b) Gürültülü ses işareti için dalgacık gürültü süzme ile elde edilen τ histogramı (SNR=10 dB). (c) Gürültülü ses işareti için dalgacık gürültü süzme ile elde edilen τ histogramı (SNR=5 dB). (d) Gürültülü ses işareti için dalgacık gürültü süzme ile elde edilen τ histogramı (SNR=0 dB).

Gürültülü damgalanmış ses işaretleri için; dalgacık gürültü süzmenin, τ histogramlarına olan etkileri sırasıyla, Şekil 3.16 (b), (c) ve (d) de irdelenmiştir. Şekil 3.16 (b) de SNR değeri 10 dB, Şekil 3.16 (c)'de SNR değeri 5 dB ve Şekil 3.16 (d)'de de SNR değeri 0 dB olacak şekilde beyaz Gauss gürültüsü eklenerek elde edilen ses işaretlerinden dalgacık gürültü süzme ile ayrıştırılan gizli anahtar işareti ve eklenen gizli anahtar işareti arasında (3.4) formülü kullanılarak elde edilen özilinti

fonksiyonunda, en büyük özilinti değerlerini veren τ 'ların histogramları görülmektedir. Dalgacık gürültü süzme ile elde edilen histogramlarda, SNR=0 dB olacak şekilde beyaz Gauss gürültüsü eklenmiş ses işaretinde bile veri senkronizasyonunun sağlanması için kullanılacak olası τ_{sync} değeri rahatlıkla ayırt edilebilmektedir. Bu durum gürültülü iletimlerde bile veri senkronizasyonunun sağlanmasına, dolayısıyla doğru damga çözebilmeye olanak tanımaktadır. Dalgacık gürültü süzme ile gerçekleştirilen gizli anahtar bilgisi ayrıştırma işlemi uyarlanır damgalamanın gürültüye karşı gürbüzlüğü artırırken, senkronizasyon problemini ortadan kaldırmaktadır. Bu sayede veri senkronizasyonu ile damga çözme işlemleri başarılı bir şekilde birleştirilebilmektedir.

Bölüm 3'te tez kapsamında sunulan damga çözme yöntemlerinden bahsedildi. Bu yöntemler öncelikli olarak literatürdeki yayılı izge yöntemine dayalı ses damgalama yöntemi üzerinde irdelendi ve damga çözme aşamasında oluşan sorunlardan bahsedildi. Benzer olarak uyarlamalı damgalamanın bu sorunlara getirdiği çözümlerden ve önerilen uyarlanır damgalama-damga çözme yönteminin veri senkronizasyonuna olan katkılarından bahsedildi. Bu bağlamda tez kapsamında incelenen damgalama-damga çözme tekniklerinin başarımlarını bir sonraki bölümünde verilen test sonuçları ile daha ayrıntılı irdelenecektir.

4. TESTLER

Tez kapsamında gerçekleştirilen testlerde 44.1 kHz' de örneklenmiş radyo kayıtlarından alınmış ses verileri kullanılmıştır. Bu veriler konuşma ve müzik kategorisi olmak üzere iki grupta ayrı damgalanmış ve damga çözme başarımları incelenmiştir. Testlerde damgalama 2-22050 Hz frekans bandında yapılmıştır.

Eklenen damganın başarımının damga-işaret oranına (WSR) bağlı değişimi, (3.11)'deki eşitlik kullanılarak müzik ve konuşma verileri üzerinde incelenmiştir.

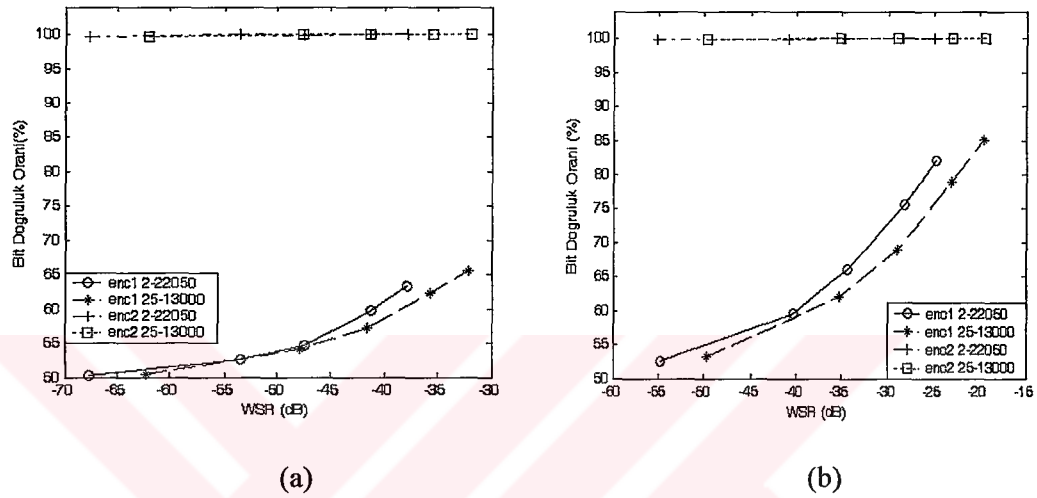
Test sonuçları (4.1) e göre hesaplanan yüzde Bit Doğruluk Oranı (BDO) şeklinde verilmektedir.

$$BDO = 100 \times \frac{\text{Doğru _ Çözülen _ Bit _ Sayısı}}{\text{Toplam _ Bit _ Sayısı}} \quad (4.1)$$

Farklı uzunluktaki damga bitlerinin damgalama başarımına etkisini incelemek amacıyla; $L=15$, BCH(15,11) ve $L=63$, BCH(63,16) damga bitleri kullanılmıştır. Yayılı izge yöntemine dayalı damgalama sonuçları, şekillerde enc1 olarak görülürken, tez kapsamında açıklanan uyarlanabilir damgalama yöntemiyle elde edilen sonuçlar enc2 olarak görülmektedir.

Şekil 4.1 (a)'da konuşma ses işaretinin (44.1kHz ve $L=15$) yayılı izge damgalama yöntemi ve uyarlanabilir damgalama yöntemi ile 25-13000 ve 2-22050 Hz frekans bandlarında damgalanması sonucunda elde edilen WSR' ye bağlı damga çözme başarımları görülmektedir (yayılı izge sonuçları enc1 25-13000 ve enc1 2-22050, uyarlanabilir damgalama sonuçları enc2 25-13000 ve enc2 2-22050 şeklinde görülmektedir). Gerçekleştirilen damgalamalarda, duyulmazlık kriterini sağlamak amacıyla WSR değerleri düşük tutulmuştur. Uyarlanabilir damgalama yöntemi 2-22050Hz frekans bandında -67 dB gibi düşük WSR oranlarında bile %100' e yakın damga çözme başarımına sahiptir. Damgalama sırasında, özyineli olarak düşük WSR değerlerindeki eklemelerle damga çözücünde bu başarımın yakalanması sağlanmaktadır. Buna karşın yayılı izge yöntemine dayalı damgalamada başarım; 2-22050 Hz frekans bandında WSR=-67 dB'de %50 değerine ulaşabilmektedir. Damgalamanın gerçekleştiği frekans bandının değişmesi başarımı değiştirmemekte ve uyarlanabilir damgalama yöntemi %100' e yakın başarım sağlamaktadır. Konuşma

işareti için elde edilen sonuçların bir benzeri müzik işareti (44.1kHz ve $L=15$) için de elde edilmiş olup; sonuçlar Şekil 4.1 (b)'de görülmektedir. Müzik işaretinde de uyarlanabilir damgalama yöntemi sonuçları, yayılı izge yöntemi ne dayalı damgalamadan çok daha yüksek değerler içermekte olup -55 dB gibi düşük WSR' da bile %100' e yakın damga çözme gerçekleştirilebilmektedir. Müzik işareti için 2-22050 Hz frekans bandında elde edilen yayılı izge yöntemi sonuçları, 25-13000 Hz frekans bandında elde edilen sonuçlara göre daha iyi olmasına rağmen en yüksek başarımlar %85'lere çıkmaktadır.

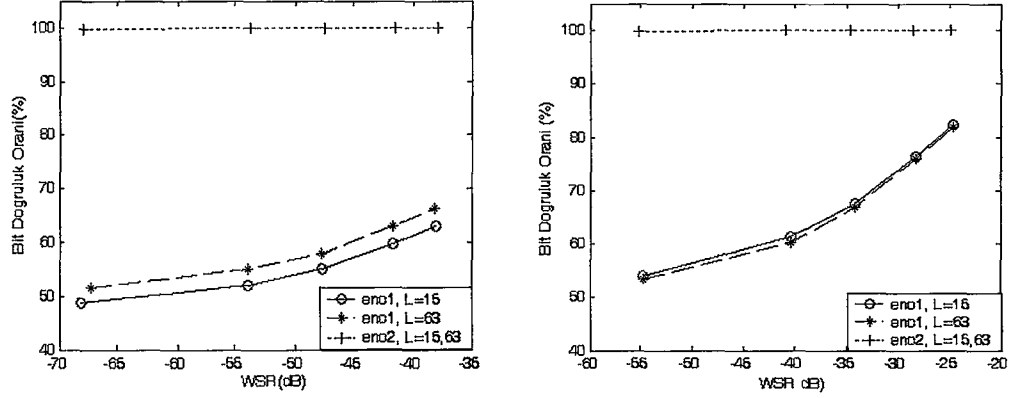


Şekil 4.1. WSR' ye bağlı farklı frekans bantlarında başarımlar (a) Konuşma $L=15$ bit. (b) Müzik $L=15$ bit.

4.1 Farklı Örnekleme Frekansında Damgalamaya Karşı Gürbüzlük

Bu bölümde yayılı izge damgalama yöntemi ve uyarlanırlı damgalama yönteminin farklı örnekleme frekansında örneklenmiş ses işaretleri üzerinde damgalama ve damga çözme başarımları incelenmiştir. 32 kHz de örneklenmiş ses işaretleri $L=15$, $L=63$ bit seçilerek yayılı izge damgalama ve uyarlanırlı damgalama yöntemleriyle ayrı ayrı damgalanarak damga çözme başarımları WSR' ye bağlı irdelenmiştir. Şekil 4.2 (a)' da yayılı izge damgalama ve uyarlanırlı damgalama ile damgalanmış konuşma işareti ($L=15$ ve $L=63$) için elde edilen başarımlar görülmektedir. Yayılı izge damgalama yönteminde $L=63$ için elde edilen sonuçlar, $L=15$ için elde edilen sonuçlara göre daha iyi olmakla birlikte, uyarlanırlı damgalama yöntemi $L=15$ ve $L=63$ için %100 başarıma sahiptir. 32 kHz' de örneklenmiş müzik işareti $L=15$ ve $L=63$ olarak yayılı izge damgalama ve uyarlanırlı damgalama yöntemleriyle damgalanmış olup, WSR' ye bağlı edilen sonuçlar Şekil 4.2 (b)'de gösterilmiştir. Yayılı izge damgalama yöntemi için elde edilen sonuçlar $L=15$ ve $L=63$ için yaklaşık

aynıdır. Yayılı izge damgalama yöntemi için WSR -25 dB’ de %80’nin üzerinde BDO elde edilirken, uyarlanır damgalama yöntemi için -55 dB gibi düşük WSR oranlarında bile $L=15$ ve $L=63$ değerlerinde %100 başarımla sağlanmaktadır.



Şekil 4.2. 32kHz’de örneklenmiş ses işaretleri için elde edilen WSR’ ye bağlı BDO
(a) Konuşma işareti için (b) Müzik işareti için.

4.2 Stereo-Mono Dönüşümler

Damgalanmış ses işareti veri iletimi sırasında stereo-mono dönüşümü gibi çeşitli dönüşümlere uğrayabilir. Bu bölümde stereo-mono dönüşümlere karşı damga çözme başarımları incelenmiştir. Ses işaretleri sol ve sağ kanal bilgileri ayrı damgalanarak profesyonel bir yazılım aracılığı ile stereo ses işaretleri oluşturulmuştur. Stereo ses işaretleri aynı yazılım kullanılarak mono ses işaretlerine çevrilmiş ve sonuçlar sadece mono olarak damgalanan ses işaretleri ile karşılaştırılmıştır. Tablo 4.1’de stereo-mono dönüşüm sonucu elde edilen damga çözme başarımları (S-M) sütunu altında, önceki testlerde olduğu gibi, mono damgalanıp mono damga çözme işlemi sonucu elde edilen başarımları (Mono) sütununda yüzde BDO olarak raporlanmaktadır. Sonuçlar farklı damga uzunluğu ve farklı damgalama yöntemlerine göre elde edilmiş olup, yayılı izge damgalama konuşma işareti için damga uzunluğu $L=15,63$ bit için stereo-mono dönüşümüne gürbüz değildir. Buna karşın uyarlanabilir damgalama stereo-mono dönüşümlerine karşı gürbüz olup en yüksek başarımları göstermektedir.

Tablo 4.1: Stereo-Mono dönüşümlerine karşı gürbzlük (yüzde BDO)

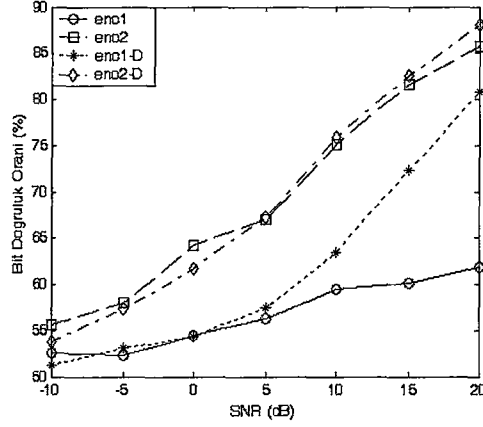
	Konuşma		Müzik	
$L = 15\text{bit}$	S-M	Mono	S- M	Mono
enc1	57	62	75	75
enc2	100	100	100	99
$L = 63\text{bit}$	S-M	Mono	S- M	Mono
enc1	62	63	74	74
enc2	100	100	100	100

4.3 Eklenebilir Beyaz Gauss Gürültüsü Atağı

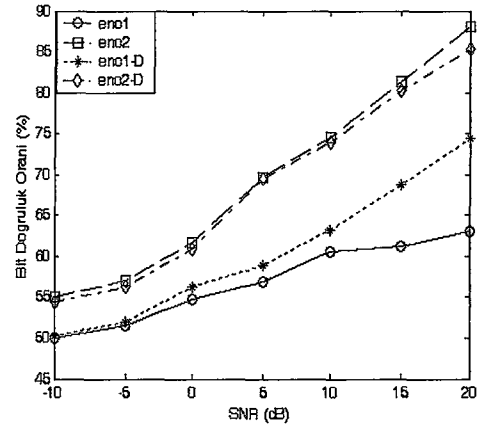
Gürültüsüz veri iletiminin ne denli güç olduğu önceki bölümlerde vurgulanmıştı. Damgalanmış ses işareti üzerinde gürültü ataklarını modelleyebilmek açısından bu işaretlere beyaz Gauss gürültüsü eklenip damga çözme performansı irdelenmiştir. Damgalanmış ses işaretleri için eklenebilir gürültü atağı sonucunda elde edilen damga çözme başarımları (3.12)'deki formüle göre hesaplanan SNR değerine bağlı verilmiştir.

Şekil 4.3 (a)'da yayılı izge damgalama ve uyarlanır damgalama yöntemi ile damgalanmış konuşma işaretinin ($L=15$ bit ve $WSR= -38$ dB) eklenebilir beyaz Gauss gürültüsünün SNR değerine bağlı damga çözme başarımları görülmektedir. Başarımlar yayılı izge yöntemi ile damgalama için (3.8)'deki klasik özilinti formülüne (enc1) ve (3.4)'teki dalgacık dönüşümü ile ayrıştırılan işaret için kullanılan özilinti formülüne (enc1-D) göre incelenmiş olup, eklenen gürültünün enerjisi 0 dB'nin üzerindeyken dalgacık dönüşümü damga çözme başarımını arttırmaktadır. SNR değeri 5 dB'nin üzerinde, uyarlanır damgalama ile damgalanmış gürültülü ses işaretinde dalgacık gürültü süzme ve (3.4)'teki özilinti formülüyle (enc2-D) elde edilen damga çözme başarımı, (3.8)'deki klasik özilinti formülüyle (enc2) elde edilen damga çözme başarımından daha iyidir. Buna karşın dalgacık

gürültü süzme işlemi yayılı izge yöntemiyle damgalanmış gürültülü işaretlerde damga çözme başarımını çok daha fazla arttırmaktadır. Benzer sonuçlar müzik işareti ($L=15, WSR=-35$ dB) için 4.3 (b)'de elde edilmiş olup, yayılı izge damgalama için dalgacık dönüşümü SNR=-5 dB, uyarlanır damgalama için SNR=10 dB'nin üzerindeki değerler için performansı arttırmaktadır.



(a)



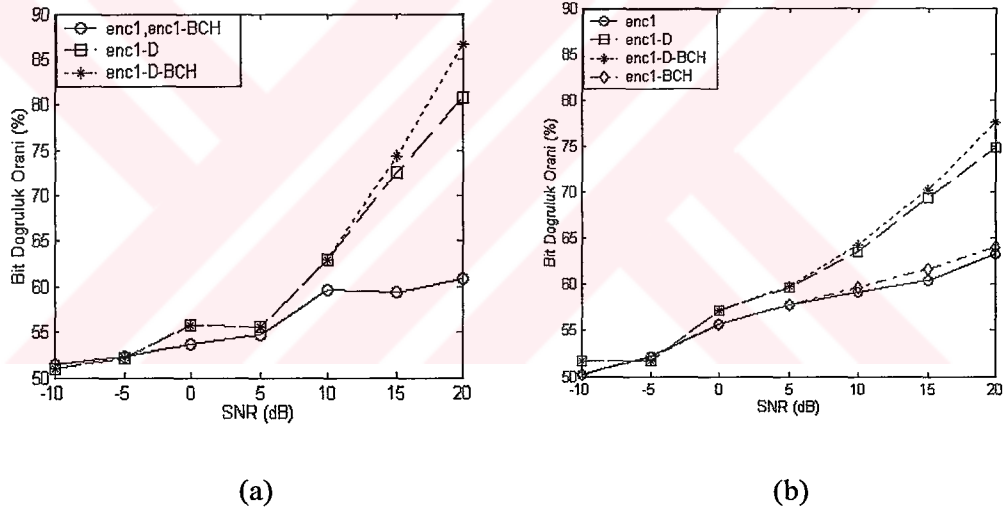
(b)

Şekil 4.3. SNR' a bağlı damga çözme başarımı. (a) Konuşma işareti için. (b) Müzik işareti için.

Damgalı ses işaretlerinde dalgacık dönüşümünün damga çözme başarımını arttırdığı testlerde görüldü. Daha önce damga çözücüde BCH kodlarının hata düzeltme kapasitelerinden faydalanılabileceğinden bahsedilmişti. Bu aşamada dalgacık dönüşümü ile artırılan başarımlar, BCH kodlarının hata düzeltme kapasiteleri de kullanılarak daha da artırılabilir. Bu amaçla damga çözücüde alınan ses işaretlerinde dalgacık gürültü süzme işlemi ve (3.4)'teki formüle göre özilinti analizi gerçekleştirilerek damga bitleri çözülür. Çözülen damga bitleri üzerinde hata düzeltme işlemi gerçekleştirilerek damga çözme başarımı artırılır. Benzer olarak başarımlar (3.8)'de verilen klasik özilinti formülüne dayalı damga çözme işlemi sonrasında hata çözme işlemi gerçekleştirilerek artırılabilir.

Şekil 4.4 (a)'da yayılı izge yöntemi ile damgalanmış ($L=63, WSR=-38$ dB) konuşma işaretine ait SNR' a bağlı damga çözme başarımları görülmektedir. Dalgacık gürültü süzme işlemine dayalı damga çözme işlemi sonuçları (enc1-D), (3.8)'de verilen klasik özilinti formülüne dayalı damga çözme işlemi (enc1) ile elde edilen sonuçlardan daha yüksek başarımla sahiptir. Klasik damga çözme işlemi ardından gerçekleştirilen BCH hata düzeltme işlemi (enc1-BCH) yayılı izge damgalama yöntemi

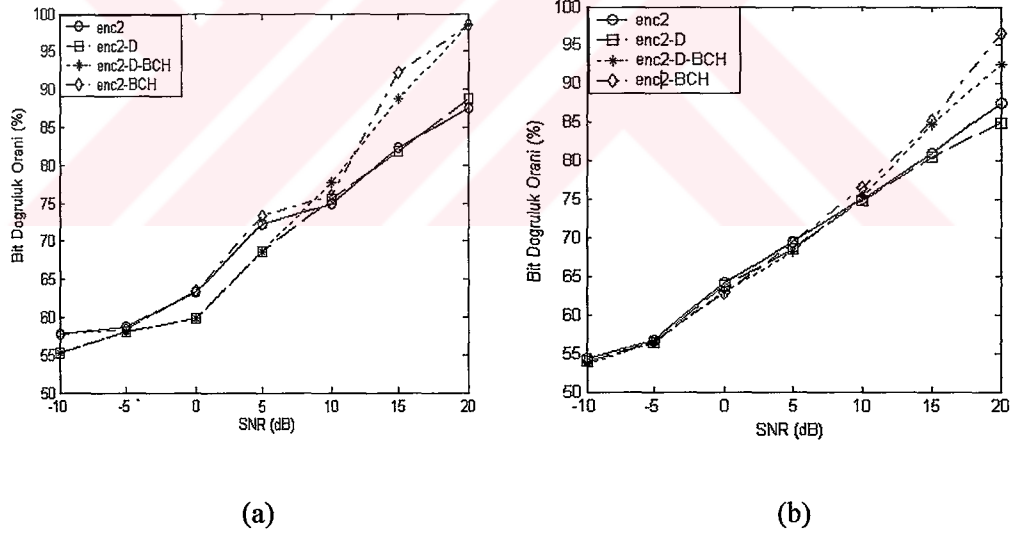
için başarımı değiştirmemektedir. Dalgacık dönüşümüne dayalı damga çözme SNR=20 dB’de, klasik damga çözücünden yaklaşık %20 oranında daha iyi sonuç vermektedir. Dalgacık dönüşümü yardımıyla çözülen damga bitlerinde, BCH hata düzeltme yapılarak Şekil 4.4 (a)’da görüldüğü gibi damga çözme başarımı artırılmıştır. SNR=20 dB gürültüde, klasik özilinti analizine göre %60 oranında elde edilen başarımlar, dalgacık dönüşümü ve ardından BCH hata düzeltme yapılarak %85’lere çıkmaktadır. Benzer sonuçlar yayılı izge yöntemi ile damgalanmış ($L=63$, WSR=-35 dB) müzik işareti içinde elde edilmiş olup sonuçlar Şekil 4.4 (b)’de gösterilmiştir. Dalgacık dönüşümü (enc1-D) ve dalgacık dönüşümü ardından yapılan BCH hata düzeltme (enc1-D-BCH) ile elde edilen başarımlar çok farklı olmamakla birlikte, dalgacık dönüşümü ardından yapılan BCH hata düzeltme en iyi sonucu vermektedir. Klasik damga çözme (enc1) ve klasik damga çözme işlemi ardından BCH hata düzeltme (enc1-BCH) başarımları SNR 20 dB için %65’lerdedir. Buna karşın dalgacık dönüşümü ardından yapılan BCH hata düzeltme (enc1-D-BCH) başarımı SNR 20 dB için %75 dir.



Şekil 4.4. SNR’ a bağlı damga çözme başarımı (dalgacık dönüşümü ve BCH hata düzeltme ile). (a) Konuşma işareti için. (b) Müzik işareti için.

Yayılı izge yöntemi için elde edilen sonuçların bir benzeri uyarlamalı damgalama için de edilmiş olup sonuçlar Şekil 4.5’te gösterilmiştir. Şekil 4.5 (a)’da konuşma işareti için klasik damga çözme (enc2), klasik damga çözme ardından BCH hata düzeltme (enc2-BCH), dalgacık dönüşümüne dayalı damga çözme (enc2-D) ve dalgacık dönüşümü ardından BCH hata düzeltmeye dayalı damga çözme (enc2-D-BCH) sonuçları görülmektedir. Konuşma işareti için SNR 10 dB’nin üzerinde klasik damga çözme ve dalgacık gürültü süzmeye dayalı damga çözme işlemleri yaklaşık aynı sonuçları vermektedir. SNR 10 dB’nin üzerinde klasik damga çözme işlemi

ardından gerçekleştirilen BCH hata düzeltme (enc2-BCH), dalgacık gürültü süzme işlemi ardından gerçekleştirilen BCH hata düzeltme (enc2-D-BCH) sonuçlarına yakın sonuçlar vermekle birlikte, SNR 15 dB’ de klasik damga çözme işleminin ardından gerçekleştirilen BCH hata düzeltme daha yüksek başarıma sahiptir. SNR=10 dB’nin altındaki değerlerde dalgacık gürültü süzmeye dayalı damga çözme işlemi, dalgacık gürültü süzme işlemi ardından gerçekleştirilen BCH hata düzeltmeye dayalı damga çözme işlemi ile yaklaşık aynı sonuçları vermektedir. Benzer olarak SNR 10 dB’nin altında klasik damga çözme işlemi, klasik damga çözme işlemi ardından gerçekleştirilen BCH hata düzeltmeye dayalı damga çözme işlemi ile yaklaşık aynı sonuçları vermektedir. SNR 20 dB’de BCH hata düzeltme işlemini kullanan damga çözücüler yaklaşık %100 başarıma ulaşmaktadırlar. Her dört damga çözme yöntemi müzik verisinde de denenmiş olup sonuçlar Şekil 4.5 (b)’de görülmektedir. Müzik işareti için SNR=10 dB’nin altındaki değerlerde başarımlar dört yöntem için yaklaşık aynıdır. Dalgacık dönüşümü ardından gerçekleştirilen BCH hata düzeltme işlemi performansı arttırmaktadır. Buna karşın klasik damga çözme işlemi ardından gerçekleştirilen hata düzeltme başarımları SNR=20 dB için en iyi sonucu vermektedir.

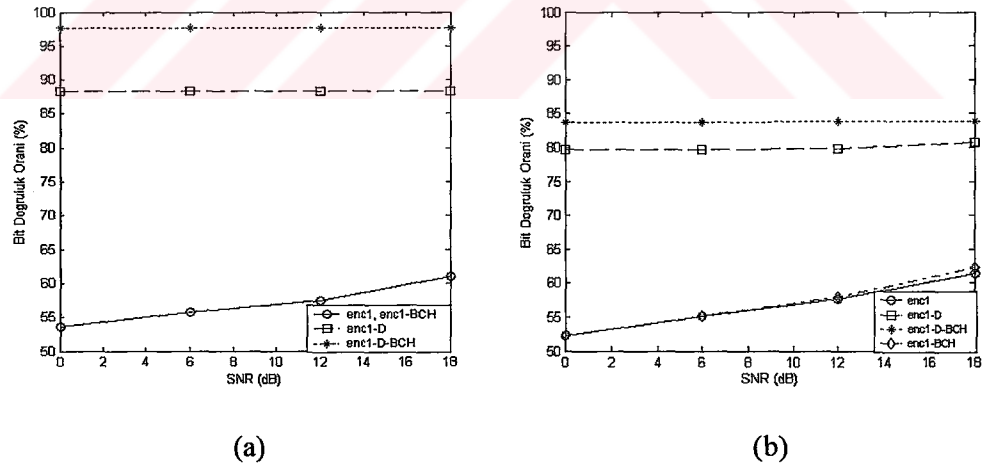


Şekil 4.5. Uyarlanabilir damgalama yönteminin SNR’ a bağlı BDO damga çözme başarımları (Dalgacık dönüşümü ve BCH kullanılarak). (a) Konuşma işareti için. (b) Müzik işareti için.

4.4 Belirli Bir Frekansta Sinüs Atağı

Testlerin bu aşamasında damgalanmış ses işaretlerine 300 Hz de farklı güçlerdeki sinüs işareti eklenmiş ve damga çözme başarımları irdelenmiştir.

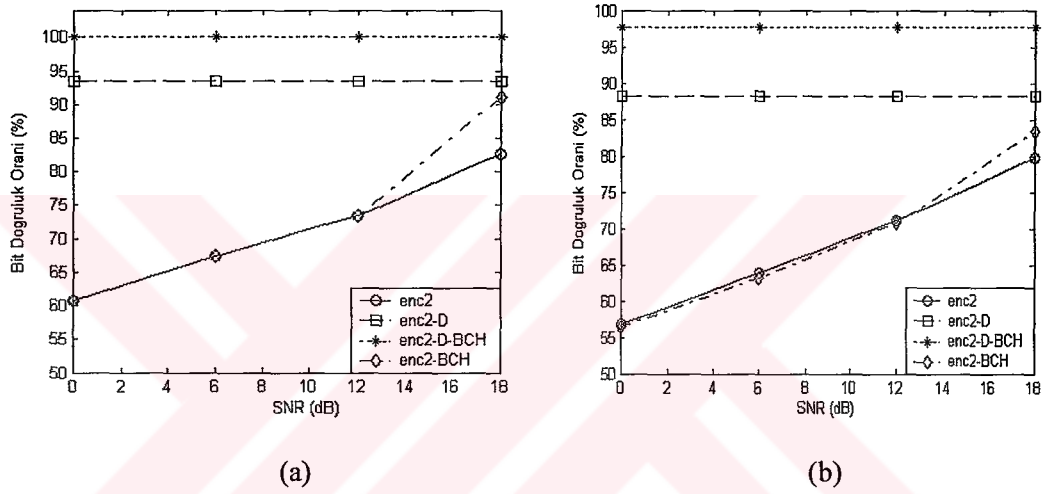
Şekil 4.6 (a)'da yayılı izge damgalama ile damgalanmış konuşma işaretinin ($L=63$, $WSR=-38$ dB), klasik damga çözme (enc1), dalgacık dönüşümüne dayalı damga çözme (enc1-D), dalgacık dönüşümü ardından BCH hata düzeltmeye dayalı damga çözme (enc1-D-BCH) ve klasik damga çözme işleminin ardından BCH hata düzeltmeye dayalı damga çözme (enc1-BCH) yöntemleriyle elde edilen başarımlarının SNR' a bağlı grafiği görülmektedir. Dalgacık dönüşümü yardımıyla gerçekleştirilen damga çözmede 300 Hz sinüs işareti eklenmiş gürültülü işarete damga çözme başarımları %90'a çıkarken, ardından gerçekleştirilen BCH hata düzeltme başarımları %97'e çıkarmaktadır. Klasik damga çözme ve klasik damga çözme işlemi ardından BCH hata düzeltmeye dayalı damga çözme işlemlerinde başarımlar aynı sonuçlar vermektedir ve bu değer SNR 18 dB' de %60 dır. Yayılı izge damgalama ile damgalanmış ($L=63$, $WSR=-35$ dB) müzik işareti içinde benzer sonuçlar Şekil 4.6 (b)' de görülmekte olup, klasik damga çözme işlemi (enc1) ve klasik damga çözme işlemi ardından gerçekleştirilen BCH hata düzeltmeye (enc1-BCH) dayalı damga çözme işlemleri yaklaşık aynı sonuçları vermektedir. Dalgacık dönüşümü ile damga çözme işleminden sonra gerçekleştirilen BCH hata düzeltme başarımları %85'lere çıkarmaktadır.



Şekil 4.6. 300Hz Sin işareti SNR' na bağlı BDO damga çözme başarımları (Yayılı izge damgalama için). (a) Konuşma işareti için. (b) Müzik işareti için.

Yayılı damgalama için gerçekleştirilen 300 Hz de sinüs işareti ekleme atağı uyarlanırlar damgalama ile damgalanmış konuşma ($L=63$, $WSR=-38$ dB) ve müzik işareti ($L=63$, $WSR=-35$ dB) içinde gerçekleştirilmiş olup sonuçlar Şekil 4.7' de görülmektedir. Şekil

4.7 (a)'da konuşma işareti için, klasik damga çözme (enc2), dalgacık dönüşümü yardımıyla damga çözme (enc2-D), dalgacık dönüşümü ardından BCH hata düzeltmeye dayalı damga çözme (enc2-D-BCH) ve klasik damga çözme işlemi ardından gerçekleştirilen BCH hata düzeltmeye dayalı (enc2-BCH) damga çözme yöntemleriyle elde edilen başarımlarının SNR'a bağlı grafiği görülmektedir. SNR 12 dB'nin altındaki değerlerde klasik damga çözme (enc2) ve klasik damga çözme işleminin ardından BCH hata düzeltmeye dayalı damga çözme (enc2-BCH) aynı sonuçları vermektedir. Dalgacık dönüşümü yardımıyla gerçekleştirilen damga çözmenin ardından yapılan BCH hata düzeltme, başarımları %100'e çıkarmaktadır. Benzer sonuçları müzik işaretleri içinde elde edilmiş olup sonuçlar Şekil 4.7 (b)'de görülmektedir.



Şekil 4.7. 300Hz Sin işareti SNR' ına bağlı BDO damga çözme başarımları.(Uyarlanırlı damgalama için) (a) Konuşma işareti için. (b) Müzik işareti için.

Geliştiren damgalama-damga çözme yönteminin farklı frekanslarda damga gömmeye, stereo-mono dönüşümlerine, gürültü ataklarına ve belirli frekansta sinüs işareti ekleme gibi çeşitli ataklara karşı gürbüz olduğu gösterilmiştir. Sunulan yöntem sıkıştırılmaya dayalı ataklarda oluşan büyük veri kayıplarından dolayı bu tür ataklara gürbüz değildir.

5. SONUÇLAR VE TARTIŞMA

Bu tez çalışmasında ses işaretleri için bir gerçek zamanlı damga çözme tekniği sunulmuştur. Damga çözme aşamasında dalgacık gürültü süzme yöntemi ön işlem olarak eklenen gizli anahtar bilgisinin ayrıştırılması amacıyla kullanılmıştır. Ayrıca damga çözücü BCH hata düzeltme bloğuna da sahip olup, dalgacık gürültü süzme ve hata düzeltme işlemi gerçek zamanda yapılabilir. Damga çözücüde gerçekleştirilen veri ve damga senkronizasyonu sistemin işlem karmaşıklığını azaltmaktadır. Damga çözücü gerçek zamanda çalışabilmektedir. Önerilen yöntemin başarımı literatürdeki standart yayılı-spektrum ses damgalama yöntemi başarımı ile karşılaştırılmış sonuçlar karşılaştırmalı olarak raporlanmıştır. Ses damgalayıcılar MPEG Katman 1 Model 1 psikoakustik frekans maskeleye dayalı olarak 512 örneklik çerçeveler üzerinde damgalama gerçekleştirmektedir.

İletilen ses iletişim kanallarında kanal gürültülerine maruz kalacağından, geliştirilen damga çözme sisteminin başarımı, damgalanmış ses verilerine gürültü eklenerek incelenmiştir. Damgalama-damga çözme yönteminin farklı frekans bandına damga gömme, stereo-mono dönüşümler, eklenebilir beyaz Gauss gürültüsü, belirli bir frekansta sinüs ekleme gibi çeşitli ataklara karşı gürbüz olduğu gösterilmiştir. Önerilen uyarlanabilir frekans maskeleye dayalı damgalama yöntemi klasik psikoakustik frekans maskeleye dayalı damgalamadan daha başarılı sonuçlar vermektedir. Damga çözme aşamasında dalgacık dönüşümünün gürültülü iletimlerde performansı arttırdığı görülmüştür. Yayılı izge damgalama için Beyaz Gauss gürültüsü eklenerek yapılan testlerde; dalgacık dönüşümü yardımıyla çözülen damga bitleri üzerinde BCH hata düzeltme işlemi gerçekleştirilerek elde edilen başarımlar diğer damga çözme yöntemlerine oranla daha yüksektir. Uyarlanabilir damgalama için Beyaz Gauss gürültüsü eklenerek yapılan testlerde de dalgacık dönüşümü yardımıyla çözülen damga bitleri üzerinde BCH hata düzeltme işlemi gerçekleştirilerek elde edilen başarımlar yüksek olmakla birlikte, klasik damgalama işlemi ardından gerçekleştirilen BCH hata düzeltmeye dayalı damga çözme işlemi daha yüksek performansa sahiptir. Belirli bir frekansta sinüs işareti eklenerek yapılan testlerde en iyi sonuçlar, dalgacık

dönüşümü yardımıyla çözülen damga bitleri üzerinde BCH hata düzeltme işlemi gerçekleştirilerek elde edilmiştir. Sunulan damga çözme yöntemi aynı zamanda senkronizasyon kayıplarını en küçükmekte ve doğru damga çözme olasılığını arttırmaktadır.

Önerilen sistemin hesaplama işlem karmaşıklığı düşük olup, gerçekleştirilen yazılımla gerçek zamanda damga çözme yapabilmektedir.



KAYNAKLAR

- [1] **Hartung, F., Kutter, M.**,1999. Multimedia Watermarking Techniques, *Proceedings of the IEEE*, vol. 87,no.7, pp 1079–1107.
- [2] **Anderson, R. J., Petitcolas, F. A. P.**,1998. On the Limits of Steganography, *IEEE Journal of Selected Areas in Communications*, vol. 16,no.4, pp 474-481.
- [3] **Cox, I. J., Miller, M. L.**, 2002. The First 50 Years of Electronic Watermarking, *Journal of Applied Signal Processing*, vol. 16,no.4, pp 126-132.
- [4] **03004104**, 1961. Identification of Sound and like Signals, United States Patent Office, USA.
- [5] **Tanaka, K., Nakamura, Y., and Matsui, K.**, 1990. Embedding a Secret Information into a Dithered Multil-level Image, *Proceedings of IEEE Military Communications Conference*, pp 216-220.
- [6] **Matsui, K., Tanaka, K., and Nakamura, Y.**, 1989. Digital Signature on Facsimile Document by Recursive MH Coding, *International Symposium on Cryptography and Information Security (CIS89)*.
- [7] **Delaigle, J. K.**, 2000. Protection of Intellectual Property of Images by Perceptual Watermarking, *Phd Thesis, Université Catholique de Louvain*.
- [8] **Bemder, W., Gruhl, D., Norimoto, N., and Lu, A.**, 1996. Techniques for Data Hiding, *IBM Systems Journal*, vol. 35,no.3&4, pp 313–336.
- [9] **Malvar, H. S., and Florêncio, D. A. F.**, 2003. Improved Spread Spectrum: A New Modulation Technique fo Robus Watermarking, *IEEE Transactions on signal Processing*, vol. 51,no.4, pp 898–905.
- [10] **Tao, B. , Dickinson, B.**, 1997. Adaptive Watermarking in the DCT Domain, *IEEE International Conference on Acoustics Speech and Signal Processing, Munich, Germany (ICASSP 97)*,, 21-24 April 1997.
- [11] **Lu, C. S., Liao, H. Y. M. and Kutter, M.**, 2002. Denoising and Copy Attacks Resilient Watermarking by Exploiting Prior Knowledge at Detector, *IEEE Transactions on Image Processing*, vol 11 no 3, 280-292.
- [12] **Baudry, S. , Delaigle, J. F., Sankur, B., Macq, B., and Maitre, H.**, 2001. Analyses of Error Correction Strategies for Typical Communication Channels in Watermarking, *Signal Processing*, vol. 81, pp. 1239-1250.

- [13] **Kesal, M. , Mihcak, K., Koetter, R., and Moulin, P.,** 2000. Iteratively Decodable Codes for Watermarking Applications, *Proceedings of the 2nd Symposium on Turbo Codes and Their Applications*, Brest, France, September 2000.
- [14] **Bose, R. C., and Ray-Chaudhuri, D. K.,** 1960. On a Class of Error Correcting Binary Group Codes, *Information Control*, vol. 3, pp. 68-79.
- [15] **Hernandez, J. R. , Gonzalez, F. P., and Rodriguez, J. M.,** 1998. The Impact of Channel Coding on the Performance of Spatial Watermarking for Copyright Protection, *IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP 98)*, Seattle, USA, May 1998.
- [16] **Chen, P. C. , Hsu, W. H., and Chen, Y. S.,** 1999. Modeling Performance Analysis and Applications of Digital Image Watermarking Systems, *IPPR Conference on Computer Vision, Graphics and Image Processing (CVGIP'99)*, Taipei, Taiwan, August 1999.
- [17] **Li, W. , Xue, X., Li, X., and Lu, P.,** 2003. A Novel Feature-Based Robust Audio Watermarking for Copyright Protection, *Proceedings of the International Conference on Information Technology: Computers and Communications (ITCC03)*, Las Vegas, USA, April 2003.
- [18] **Michelson, M. , and Levesque, A. H.,** 1985. Error-Control Techniques for Digital Communication, *a Wiley-Interscience publication*, New York, USA.
- [19] www.eccpage.com, Robert Morelos-Zaragoza.
- [20] **Günsel, B., Sener, and S., Yaslan, Y.,** 2003. An Adaptive Encoder for Audio Watermarking, *WSEAS Transactions on Computers*, issue 4, vol. 2, pp 1044–1048.
- [21] **Kim, H. J.,** 2003. Audio Watermarking Techniques, *Pacific Rim Workshop on Digital Steganography*, Kitakyushu, Japan, July 2003.
- [22] **Şener, S.,** 2004. Uyarlanırsı Psikoakustik Maskeleye Kullanarak Gürbüz Ses Damgalama, *Yüksek Lisans Tezi*, İ.T.Ü. Bilişim Enstitüsü, İstanbul.
- [23] **Yaslan, Y. , Günsel, B.,** 2004. An Integrated Decoding Framework for Audio Watermark Extraction, *17th International Conference on Pattern Recognition*, Cambridge, UK, 23-26 August 2004. (Kabul edildi)
- [24] **Fletcher, A. K., Goyal, V. K. and Ramchandran, K.,** 2002. Wavelet Denoising by Recursive Cycle Spinning, *International Conference on Image Processing (ICIP 2002)*, Rochester ,New York, USA, September 2002.

- [25] **Fletcher, A. K., Goyal, V. K. and Ramchandran, K.,** 2003. Iterative Projective Wavelet Methods for Denoising, *Proceedings of the Wavelets X* , part of the 2003 SPIE Int. Symp. on Optical Sci. & Techn. San Diego, USA, August 2003.
- [26] **Garcia, R.A.,** 1999. Digital Watermarking of Audio Signals Using A Psychoacoustic Auditory Model, and Spread Spectrum Theory, *Master Thesis*, School of Music Engineering Technology, University of Miami, Coral Gables, Florida.
- [27] **Herkiloğlu, K. ,Yaslan, Y. , Şener, S. , Günsel , B.,** 2004. Uyarlanırs Psikoakustik Maskeleye Kullanılarak Gürbüz Ses Damgalama, IEEE 12. Sinyal İşleme ve İletişim Uygulamaları Kurultayı, Kuşadası, Türkiye, 28-30 Nisan 2004.



ÖZGEÇMİŞ

Yusuf Yaslan 2001 yılında İstanbul Üniversitesi Bilgisayar Bilimleri mühendisliği bölümünden mezun olmuştur. 2001-2002 yılları arasında 6 ay süreyle Almanya Federal Cumhuriyetinde FGAN-FOM araştırma enstitüsünde bursiyer olarak bulunmuştur. 2002 yılından bu yana İstanbul Teknik Üniversitesi Fen Bilimleri Enstitüsü Telekomünikasyon mühendisliği programında yüksek lisans yapmaktadır. Örüntü tanıma, sayısal damgalama konuları üzerinde çalışmakta, 3 tanesi yurt içi ve 2 tanesi yurt dışında olmak üzere yayınlanmış 5 bilimsel bildirisi bulunmaktadır. İ.T.Ü. ROTAM (Rotorlu Hava Araçları Tasarım ve Mükemmeliyet Merkezi) da HAGU projesi Aviyonik iş paketinde çalışmaktadır.

