T.C.
ULUDAĞ ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

KAOTİK ÖZELLİKLERİN KONUŞMA SESLERİ STEGANALİZİNDE KULLANIMI

Emrah YÜRÜKLÜ

Prof.Dr. Erdoğan DİLAVEROĞLU
(Danışman)

DOKTORA TEZİ
ELEKTRONİK MÜHENDİSLİĞİ ANABİLİM DALI

BURSA-2013

TEZ ONAYI

Emrah Yürüklü tarafından hazırlanan "Kaotik özelliklerin konuşma sesleri steganalizinde kullanımı" adlı tez çalışması aşağıdaki jüri tarafından oy birliği/oy çokluğu ile Uludağ Üniversitesi Fen Bilimleri Enstitüsü Elektrik-Elektronik Mühendisliği Anabilim Dalı'nda **DOKTORA TEZİ** olarak kabul edilmiştir.

Danışman : Prof.Dr. Erdoğan DİLAVEROĞLU

Başkan :	Prof.Dr. Erdoğan DİLAVEROĞLU Uludağ Üniversitesi Mühendislik-Mimarlık Fakültesi, Elektrik-Elektronik Mühendisliği Anabilim Dalı	İmza
Üye :	Prof.Dr. Osman KOPMAZ Uludağ Üniversitesi Mühendislik-Mimarlık Fakültesi, Makine Mühendisliği Anabilim Dalı	İmza
Üye :	Doç.Dr. Fahri VATANSEVER Uludağ Üniversitesi Mühendislik-Mimarlık Fakültesi, Elektrik-Elektronik Mühendisliği Anabilim Dalı	İmza
Üye :	Yrd.Doç.Dr. Osman H. KOÇAL Yalova Üniversitesi Mühendislik Fakültesi, Bilgisayar Mühendisliği Anabilim Dalı	İmza
Üye :	Yrd.Doç.Dr. Ersen YILMAZ Uludağ Üniversitesi Mühendislik-Mimarlık Fakültesi, Elektrik-Elektronik Mühendisliği Anabilim Dalı	İmza

Yukarıdaki sonucu onaylarım

Prof. Dr. Ali Osman DEMİR

Enstitü Müdürü

(…./……../2013)

U.Ü. Fen Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında;

- tez içindeki bütün bilgi ve belgeleri akademik kurallar çerçevesinde elde ettiğimi,
- görsel, işitsel ve yazılı tüm bilgi ve sonuçları bilimsel ahlak kurallarına uygun olarak sunduğumu,
- başkalarının eserlerinden yararlanılması durumunda ilgili eserlere bilimsel normlara uygun olarak atıfta bulunduğumu,
- atıfta bulunduğum eserlerin tümünü kaynak olarak gösterdiğimi,
- kullanılan verilerde herhangi bir tahrifat yapmadığımı,
- ve bu tezin herhangi bir bölümünü bu üniversite veya başka bir üniversitede başka bir tez çalışması olarak sunmadığımı

beyan ederim.

30/Kasım/2013

Emrah YÜRÜKLÜ

ÖZET

Doktora Tezi

KAOTİK ÖZELLİKLERİN KONUŞMA SESLERİ
STEGANALİZİNDE KULLANIMI

Emrah YÜRÜKLÜ

Uludağ Üniversitesi

Fen Bilimleri Enstitüsü

Elektrik-Elektronik Mühendisliği Anabilim Dalı

Danışman: Prof. Dr. Erdoğan DİLAVEROĞLU

Bu tezde kaotik özelliklerin, kaydedilmiş konuşma seslerinin steganalizinde kullanım alanları ve olanakları araştırılmıştır. Veri gizleme işleminin konuşma sesleri üzerine gürültü eklediği ve böylelikle orijinal ses sinyallerine ait kaotik özelliklerin değiştiği varsayımını kullanarak, Hatalı-Komşular Oranı, Lyapunov üstelleri, vekil veriler tabanlı Gecikmeli-Vektör varyans analizi gibi kaotik özellikleri kullanan yeni bir ses steganalizörü önerilmiştir. Bu tezde ayrıca önerilen steganalizörün, dolayısıyla kaotik özellik vektörünün yalnızca konuşma seslerine değil tüm ses kayıtları için uygulanabilirliği araştırılmıştır. Önerilen steganalizörün başarımı pek çok farklı benzetim şartlarında denenmiş ve elde edilen nümerik sonuçlar literatürdeki benzer steganalizörler ile karşılaştırılmıştır.

Bu tezdeki çalışmalar TUBITAK tarafından 104E056 nolu proje numarası altında desteklenmiştir.

Anahtar Kelimeler: Steganografi, steganaliz, konuşma, kaos, hatalı komşular, Lyapunov üsteli, vekil veri, kesirli boyutlar.

2013, xii + 91 sayfa.

ABSTRACT

PhD Thesis

USING CHAOTIC FEATURES FOR SPEECH STEGANALYSIS

Emrah YÜRÜKLÜ

Uludağ University

Graduate School of Natural and Applied Sciences

Department of Electric-Electronic Engineering

Supervisor: Prof. Dr. Erdoğan DİLAVEROĞLU

The use of chaotic-type features for recorded speech steganalysis is investigated by this thesis. Considering that data hiding within a speech signal distorts the chaotic properties of the original speech signal, a new steganalyzer that uses chaotic features like Lyapunov exponents and fraction of false neighbors as chaotic features to detect the existence of a stego-signal has been designed. Also the applicability of the proposed method to general audio has been discussed. Proposed steganalyzer has been tested by various conditions of simulators and also numerical results have been compared to other steganalyzers which have been proposed by academic literature.

This thesis is supported in part by TUBITAK Project 104E056.

Key Words: Steganography, steganalysis, speech, chaos, false-neighbors, Lyapunov exponent, surrogate data, fractal dimension.

2013, xii + 91 pages.

TEŞEKKÜR

Doktora tez çalışmalarım sırasında bana her konuda yardımcı olan ve teze yaptığı katkılarından dolayı danışmanım sayın Prof.Dr. Erdoğan Dilaveroğlu'na, sayın Yrd. Doç. Dr. Osman H. KOÇAL ve sayın Prof.Dr. İsmail Avcıbaş'a, ayrıca pek çok teknik konuda yardımlarını esirgemeyen arkadaşlarım Yrd.Doç.Dr. A. Emir Dirik, Sevinç Bayram ve Erhan Dinar'a teşekkürü bir borç bilirim.

Tezde kullanılan veri setlerinin temininde yardımlarını esirgemeyen TUBİTAK UEKAE Konuşma Grubu'ndan sayın Dr. Hamza Özer'e teşekkürlerimi sunarım.

Ayrıca hayatımı kolaylaştıran sevgili eşim Çiğdem YÜRÜKLÜ'ye, yaşamım boyunca bana her zaman destek olan annem, babam ve kardeşlerime, bugüne kadar bana emeği geçen tüm öğretmenlerime ve her zaman yanımda bulunan arkadaşlarıma içtenlikle teşekkür ederim.

Emrah YÜRÜKLÜ

30/Kasım/2013

İÇİNDEKİLER

Sayfa

SİMGELER ve KISALTMALAR DİZİNİ

Simgeler	Açıklama
A:	*(Anma) A = DP / (DP + HN)*
ANOVA:	(*Analysis Of VAriance*) Varyans Analizi
AQM	(*Audio Quality Metrics*) Ses Kalitesi Metrikleri
BO:	*(yüzdesel Başarım Oranı)* BO=(1-(YA+TM)/2*N*)x100
CI-AQM:	(*Content Independent - Audio Quality Metrics*) İçerik-Bağımsız Ses Kalitesi Metrikleri
COX:	Cox ve ark. Tarafından 1997 yılında önerilen sudamgalama yöntemi
D:	*(Duyarlılık) D = DP / (DP+HP)*
DN:	*(Doğru Negatif)* Negatif (Gizli mesajın yokluğu) olarak etiketlenen gizli mesaj içermeyen örnek sayısı
DNO:	*(Doğru Negatif Oranı) DNO = DN / (DN + HP)*
DP:	*(Doğru Pozitif)* Pozitif (Gizli mesajın varlığı) olarak etiketlenen gizli mesaj içeren örnek sayısı
DPO:	*(Doğru Pozitif Oranı) DPO = DP / (DP + HN)*
DSSS:	Direct Sequence Spread Sprectrum (Bender ve ark. 1996) sudamgalama tekniği
DVV:	(*Delay Vector Variance*) Gecikmeli Vektör Varyans
ECHO :	Bender ve arkadaşları tarafından 1996 yılında önerilen Eko-Veri Gizleme ve sudamgalama Tekniği
FHSS:	Frequency Hopping Spread Spectrum (Bender ve ark. 1996) sudamgalama tekniği
FNF:	(*False Neighbourhood Fraction*) Hatalı Komşular Oranı
HIDE4PGP:	(HIDE4PGP. 2006) kaynağındaki veri gizleme tekniği
HN:	*(Hatalı Negatif)* Negatif (Gizli mesajın yokluğu) olarak etiketlenen gizli mesaj içeren örnek sayısı (TM-Tespit Edilemeyen Mesaj)
HNO:	*(Hatalı Negatif Oranı) HNO = HN / (DP + HN)*

HP: *(Hatalı Pozitif)* Pozitif (Gizli mesajın varlığı) olarak etiketlenen gizli mesaj içermeyen örnek sayısı (YA-Yanlış Alarm)

HPO: *(Hatalı Pozitif Oranı) HPO = HP / (DN + HP)*

LAR: *(Log-Area Ratio)* Logaritmik Alan Oranı

LLR: *(Log-Likelihood Ratio)* Logaritmik Benzerlik Oranı

LR (*Lineer Regression*) Lineer Sınıflandırıcı

MP3: (MP3STEGO. 2006) kaynağındaki veri gizleme tekniği

NTIMIT: (*Noisy TIMIT*) Telefon konuşmaları ses kayıtlarından oluşan veri tabanı

PAQM: *(Perceptual Audio Quality Measure)* Algısal Ses Kalite Metriği

ROC: *(Receiver Operating Characteristics)* Algısal İşlem Karakteristikleri

SFFS: (*Sequential Forward Floating Searching*) Ardışıl İleri Yönde Kayan Arama

SPD: *(Spectral Phase Distortion)* Spektral Faz Bozulması

STEGA: (STEGANOS. 2006) kaynağındaki veri gizleme tekniği

STEGHIDE: (STEGHIDE. 2006) kaynağındaki veri gizleme tekniği

STOMOD: Fridrich ve Goljan tarafından 2003 yılında önerilen veri gizleme ve sudamgalama tekniği

SVM: (*Support Vector Machine*) Destek Vektör Makinesi; Bir nonlineer sınıflandırıcı

SWR: *(Signal-to-Watermark Ratio)* Sinyal gücünü gizlenen veri ile oluşan gürültü gücüne oranı

TIMIT: (*Texas Instruments- Massachusetts Institute of Technology*) Literatürde sıklıkla kullanılan konuşma sesleri veri tabanı

TM: (*Tespit edilemeyen Mesaj*) İçerisinde gizli mesaj olmasına rağmen tespit edilemeyen veri sinyallerinin sayısı

YA: *(Yanlış Alarm) İ*çerisinde herhangi bir gizli veri olmamasına rağmen gizli mesaj taşıyor şeklinde etiketlenen veri sinyalleri sayısı

Kısaltmalar	**Açıklama**
F_{xxx}	Steganalizde kullanılmak üzere *xxx* tekniğine ait özellik vektörü
T	Faz uzayı eksenleri arasındaki gecikme değeri
D_E	Faz uzayı gömme boyutu
$\mathbf{s}(n)$	Faz uzayında işlem yapılan referans nokta
$\mathbf{s}(m)$	Faz uzayında referans noktaya en yakın komşu noktası
$x(n)$	**s** sinyaline ait zaman serisi
λ	Lyapunov üsteli
p	ANOVA analizi sonrasında ortaya çıkan bağımsızlık değeri
t	Sınıflandırıcılarda kullanılan karar eşik değeri
n_{surr}	DVV metodunda kullanılan vekil veri sayısı

ŞEKİLLER DİZİNİ

Sayfa

ÇİZELGELER DİZİNİ

Sayfa

1. GİRİŞ

Steganografi bilgi gizleme yöntemlerinin önemli bir alt dalıdır (Petitcolas ve ark. 1999). Bu yaklaşım, bir nesnenin içerisine bir verinin gizlenmesi olarak tanımlanabilir. Bu yaklaşımla ses, sayısal resim, video görüntüleri üzerine veri saklanabilir. Görüntü dosyaları içerisine saklanacak veriler metin dosyası olabileceği gibi, başka bir görüntü dosyası, video dosyası veya ses dosyası da olabilir. Bu yaklaşımda içine bilgi gizlenen ortama örtü sinyali veya nesnesi (cover-signal; cover-object), oluşan yeni veriye de stego sinyali veya nesnesi (stego-signal; stego-object) denilmektedir.

Steganografi kelimesi Yunanca "steganos: gizli, saklı" ve "grafi: çizim ya da yazım" kelimelerinden gelmektedir. Steganografi, Antik yunan ve Heredot zamanına kadar uzanan oldukça eski bir veri gizleme yöntemidir. Heredot, İran Savaşları sırasında, kafasını kazıtıp kafa derisinin üzerine, gizli bir mesajın dövmesinin yapılmasına izin veren bir ulaktan bahsetmektedir. Mesaj yazıldıktan sonra ulak saçının uzamasını beklemekte, daha sonra ulak mesajı bekleyen kişiye ulaşmakta, kafasını tekrar tıraş etmekte, böylelikle mesaj ortaya çıkmaktadır. Bu yöntem bilinen ilk steganografi uygulamasıdır. Daha sonraki zamanlarda steganografi, harflere müzik notalarının atanması, II. Dünya savaşı esnasında başarıyla uygulanan görünmez mürekkeplerin kullanımı gibi uygulamalarla karşımıza çıkmaktadır (Katzenbeisser ve Petitcolas. 2000). II. Dünya savaşında yaşanan bir başka örnek ise savaş sırasında, New York'taki bir Japon ajanının (Velvalee Dickinson) oyuncak bebek pazarlamacısı kılığı altında saklanmasıdır. Bu ajan, Amerikan ordusunun hareketlerini bebek siparişi içeren mektuplar içine saklayarak Güney Amerika'daki adreslere göndermekte idi (Şahin ve ark. 2006).

Steganografi için pek çok örnek verilebilir. Örneğin aşağıdaki metin steganografinin oldukça basit bir örneğidir. Gönderilen veri içerisine saklanan veriye ulaşabilmek için yalnızca tek satırları (1., 3., 5., …) okumak gerekmektedir (Şekil 1.1).

Benim için futbolda önemli olan centilmenlik
ve dostluktur. Hedefim illa ki kazanmak
falan değildir. Ben sadece kendi reklamını düşünen
kişiliğe sahip olsam başka olurdu. Ben net
birisiyim arkadaş. Takımım kazanırsa mal-
zemecisine kadar mutlu oluruz. Ben de sporcu
varlığımı geliştiririm. Hakemlere baskı uygulamak
sportmenliğe yakışmaz. Fair-play için mücadele
gerekirse onu da yaparım. Medyayı da bağ-
rıma basmışım, spor uğruna gülmüşüm ve ağ-
lamışım, kafam rahat!

Şekil 1.1. Metin steganografi örneği (Tek satırlar okunduğunda gizli mesaj ortaya çıkmaktadır).

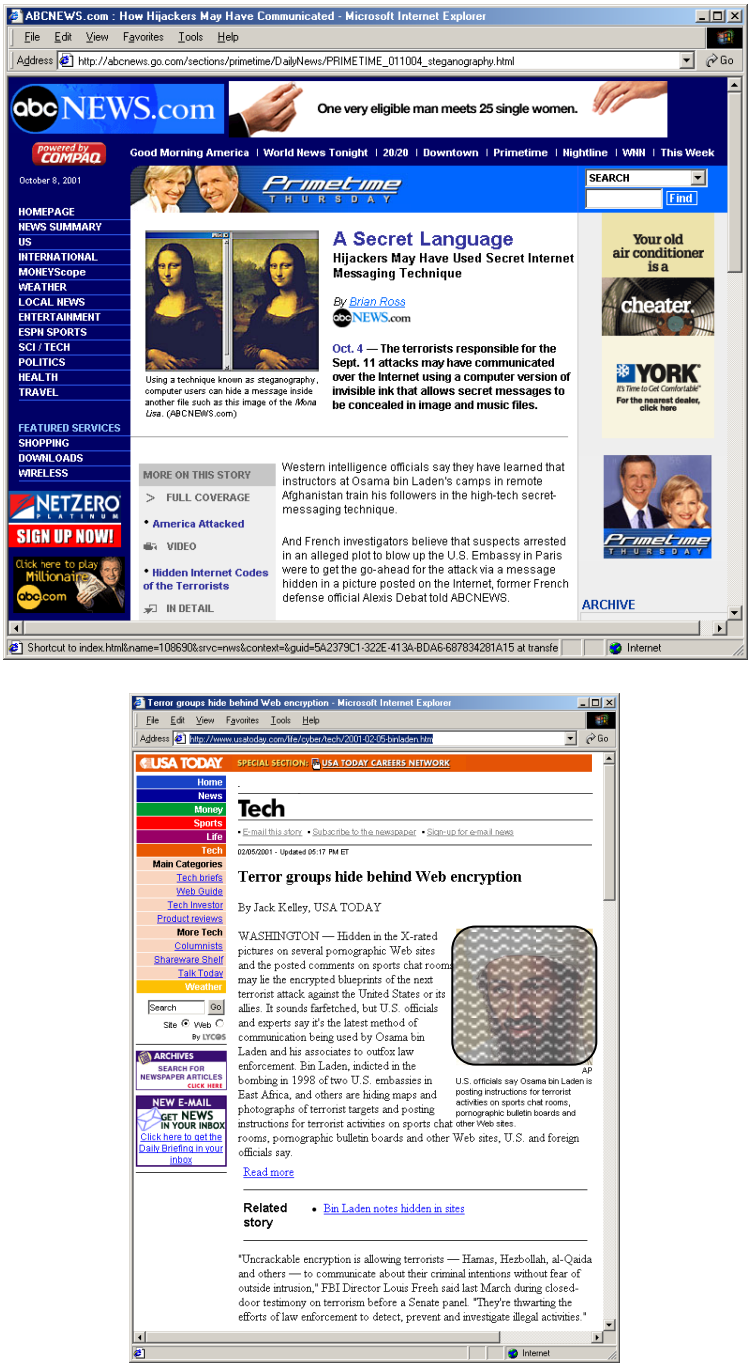
Günümüzde ise sayısal (dijital) nesneler üzerinde steganografi uygulamaları yapılmaktadır ve gelişen teknoloji nedeniyle, verilerimizi korumak amacıyla son yıllarda sıklıkla kullanılmaya başlanmıştır. Steganografi, Dilbilim ve Teknik Steganografi olmak üzere kendi içerisinde ikiye ayrılmaktadır. Dilbilim steganografi, taşıyıcı verinin metin olduğu steganografi koludur. Teknik Steganografi ise birçok konuyu içine almaktadır. Bunlar; görünmez mürekkep, gizli yerler, mikro noktalar ve bilgisayar tabanlı yöntemler gibi başlıklar altında toplanabilmektedir. Bu tezde dilbilim steganografi ele alınacaktır. Bilgisayar tabanlı yöntemler metin, ses ve görüntü dosyalarını kullanarak veri gizleme yöntemleridir.

Veri gizleme yöntemlerinin önemi, son yıllarda artan terör gruplarının bu yöntemle haberleştiğinin anlaşılmasıyla daha da fazla artmıştır (Şekil 1.2). Özellikle 11. Eylül. 2001'de İkiz Kuleler'e gerçekleştirilen saldırıda veri gizleme teknikleri kullanıldığının anlaşılmasından sonra Amerikan Haber Alma Teşkilatı (CIA) ve Federal Araştırma Bürosu (FBI) gizli veri içeren sinyallerin tespit edilmesini sağlayan steganaliz yöntemleri ile ilgili çalışmaları desteklemeye başlamıştır. Özellikle 1999 yılında FBI tarafından kurulan "Forensic Science Communications"[1] araştırma dergisinde steganaliz üzerine çalışmalar yayınlanmaktadır.

Bu tez ile de ses sinyalleri içerisine gizlenen verileri tespit etmek üzere kaotik özellik vektörleri kullanan bir steganaliz yöntemi literatürde ilk defa önerilmiş, performans testleri pek çok farklı şart altında gerçekleştirilmiş ve nümerik sonuçlar ile işe yararlılığı

[1] www.fbi.gov/about-us/lab/forensic-science-communications/

kanıtlanmıştır. Çalışmanın bilime olan katkısı da bu noktadadır. Literatürde çalışmanın yapıldığı tarih itibariyle önerilen ses steganalizörleri ile karşılaştırmalı sonuçlar ile önerilen kaotik özellikler tabanlı steganalizörün örtü ve stego sinyali ayırt etmedeki başarısı desteklenmiştir.



Şekil 1.2. Teröristlerin steganografi tekniklerini kullandığını bildiren haberler

Önerilen özellik vektörü, literatürde ilk defa ses steganalizi için kullanılan kaotik özellikler analiz araçları yardımıyla oluşturulmuştur. *Kaos*; mutlak evrensel düzen anlamına gelen *kozmo*s kelimesinin tersi; Eski Yunanca'da mutlak anarşi, kargaşa ve düzensizlik anlamına gelmektedir. M.Ö. 8. yüzyılda yaşayan Hesiodos, Theogonia adlı eserinde "Her şeyden önce kaos vardı" demektedir. Eski Yunanlılar kaosun kuralsızlık olmasının yanında, düzeni doğuran bir özelliğe de sahip olduğunu düşünüyorlardı. Fakat 20. yüzyıla kadar bu anlamda kayda değer fikir üretilmedi.

Kaos sözcüğünün yaygın olarak çağrıştırdığı anlam, evrenin matematiksel denklemlerle modellenip öngörülemeyecek denli karışık, rasgele kuvvetlerin etkisi altında olduğudur. Günümüzde bilimciler kaos deyince bu ifadeden farklı olarak görünüşte düzensiz ve öngörülemez olarak sınıflandırılabilen çoğu sistemin ve davranışın üst düzeyde matematiksel bir düzene sahip olduğu anlamında kullanmaktadır (Canan. 2011). Özellikle 1990'lı yılların başların oldukça popüler olan kaos teorisi üzerine yapılan çalışmalarda kaosun ölçülebilirliği ve analizi üzerine pek çok yayın yayınlanmıştır (Abarbanel. 1996, Hilborn. 2000). Bu çalışmalar sonucu ortaya konulan nümerik kaos ölçme metotlarını kullanarak ses steganalizinde kullanılması önerisi bu çalışmanın ana çıkış noktasıdır.

Yapılan tezin takip eden bölümlerindeki konuları sıralayacak olursak;

Bölüm 2'de bugüne kadar ses steganografisi, ses steganalizi, kaos ölçme ve analiz araçları üzerine yapılan çalışmaların özeti verilmiştir.

Bölüm 3'de genel olarak steganografi ve kaos teorimi disiplinlerine ait genel bilgi verilmekle beraber, Bölüm 3.1'de steganografi ve steganalizin tanımları, Bölüm 3.2'de ses steganografisi ve steganalizi, ses steganalizörü tasarımı, Bölüm 3.3'de kaos kuramı, kaos ölçme yöntemleri ve hesaplama şekilleri, elde edilen kaotiklerden oluşan özellik vektörünün ses steganalizinde kullanılması anlatılmaktadır.

Bölüm 4 tez çalışmasının sonuçlarına ve tartışmaya ayrılmakla birlikte detay olarak, Bölüm 4.1'de önerilen kaotik özellik vektörünü kullanan steganalizörün başarım değerlerini görebilmek için gerçekleştirilecek pek çok farklı altyapı kullanan benzetimin şartları ortaya konulmuştur. Bölüm 4.2'de ise ortaya konan benzetim şartlarında gerçekleştirilen benzetimlerin sonuçları iletilmiştir.

Ayrıca Ekler kısmında yapılan çalışmada kullanılan MATLAB kodları verilmiştir. .

2. KAYNAK ARAŞTIRMASI

Literatürde özellikle 1990'lı yılların başlarından itibaren sayısal veri gizleme metotları önerilerinin sayısı hızla artmıştır. Bu steganografi tekniklerinin bir kısmı nesne bağımsız (metin, ses, görüntü, video) olarak tüm sayısal veriler içerisine istenilen veriyi gizleyebilen (görüntü içerisine gizlenen ses veya video içerisine gizlenen metin gibi) teknikler olmakla birlikte bir kısmı da bazı sayısal veri tiplerine özel olarak uygulanabilmektedir (yalnızca ses içerisine gizlenebilen metin gibi). Bu çalışmaların büyük bir kısmı özel olarak görüntü içerisine veri gizleme teknikleri önerilerine ayrılmıştır (Fridrich ve Goljan. 2003). Göreceli olarak ses içerisine veri gizleme önerileri daha sınırlı sayıda kalmıştır (Mp3Stego. 2006) Ses sinyali içerisine veri gizleme teknikleri genel olarak biraz önce bahsedilen nesne bağımsız steganografi önerilerine dâhil olarak sunulmuştur (Bender ve ark. 1996, Cox. 1997, Fridrich ve Goljan. 2003, Steganos. 2006, Steghide. 2006, Hide4pgp. 2006). Bu tezde pek tabii ki bugüne kadar önerilen tüm ses veya nesne bağımsız steganografi tekniklerinin incelenmesi mümkün olmamıştır. Bunun yerine literatürde genel olarak sıklıkla atıf alan teknikler çalışmada incelemeye ve önerilen steganalizörün performans testlerinde kullanılmıştır. Performans testlerine tabii tutulan steganografi teknikleri kısaca şöyledir:

COX → Cox ve ark. Tarafından 1997 yılında önerilen sudamgalama yöntemi

DSSS → Direct Sequence Spread Sprectrum (Bender ve ark. 1996) sudamgalama tekniği

FHSS → Frequency Hopping Spread Spectrum (Bender ve ark. 1996) sudamgalama tekniği

ECHO → Bender ve arkadaşları tarafından 1996 yılında önerilen Eko-Veri Gizleme ve sudamgalama Tekniği

STEGA → (STEGANOS. 2006) kaynağındaki veri gizleme tekniği

HIDE4PGP → (HIDE4PGP. 2006) kaynağındaki veri gizleme tekniği

STEGHIDE → (STEGHIDE. 2006) kaynağındaki veri gizleme tekniği

STOMOD → Fridrich ve Goljan tarafından 2003 yılında önerilen veri gizleme ve sudamgalama tekniği

MP3 → (MP3STEGO. 2006) kaynağındaki veri gizleme tekniği

Tez boyunca, bahsedilen steganografi teknikleri bu kısaltmalar ile anılacaktır. Bu tekniklerin ilk 3 tanesi steganografik tekniklerin bir alt grubu olan sudamgası teknikleri grubuna aittir[2]. Sudamgası tekniklerinde veri gizleme işleminin stego veriye ulaşan herkes tarafından bilinmesi istenir. Bu gruptaki steganografi tekniklerinde gizli haberleşme amacı gütmeksizin veri gizleme (gömme) işlemi örtü verisini özel olarak işaretlemek (orijinalliğinin bozulmadığını garantilemek, verinin sahipliğini ifade etmek gibi) amacıyla gerçekleştirilmektedir. Sudamgasında önemli olan gizli verinin fark edilmemesi değil, stego sinyali üzerinde yapılacak sayısal işlemler ile (filtreleme, düşük frekansta örnekleme, vb.) gömülen verinin yok edilememesidir. Bu yüzden bu amaçlarla elde edilmiş stego sinyallerinin, içerisinde herhangi gizli veri barındırmayan orijinal sinyallerden ayırt edilmesi bilimi olan steganalizde önemli bir yeri yoktur. Gizlenen verinin keşfedilememesi gibi bir amaç gütmediği için bu yöntemler için oldukça yüksek başarımlar elde edilmektedir. Fakat yine de bu tekniklerin literatürde gerçekleştirilmiş steganaliz çalışmalarında kullanılması ve bu tezde elde edilen sonuçlar ile literatürde elde edilen sonuçların doğru bir platformda karşılaştırması gereği nedenleriyle bu tezde ki gerçekleştirilen steganaliz çalışmalarında da kullanılmıştır.

Yıllar boyunca önerilen ve kabul edilen her steganografi tekniği ile birlikte bu teknik ile gizlenen veriyi ortaya çıkarmak üzere steganaliz önerileri ortaya konulmuştur. Ses steganografi teknikleri için özel veya tüm steganografi tekniklerini kapsayan evrensel (universal) steganalizörler literatürde yerini almıştır. Bu çalışmalardan kısaca bahsetmek gerekirse, bunlar arasında literatürde önemli yer tutan bir çalışma olan Westfeld'in önerdiği steganaliz yöntemi (Westfeld 2003) LSB steganografi yöntemi kullanılarak saklanmış verilerin algılanmasına yöneliktir. Westfeld ve Pfitzman'ın önerdiği diğer bir steganaliz çalışması ise MP3 ses sinyallerinin içerisine gizlenmiş verilerin algılanması üzerine yapılmış bir çalışmadır (Westfeld ve Pfitzman 1999). Johnson ve arkadaşlarının yaptığı başka bir öneri ise LSB ve Hide4Pgp steganografi

[2] ECHO ve STOMOD sudamgalama olarak da kullanılabilen steganografi teknikleridir.

algoritmalarına göre gizlenmiş verilerin algılanması üzerinedir (Johnson ve ark. 2005). Ayrıca DSSS sudamgası ve stokastik modülasyon steganografi yöntemleri için Altun ve arkadaşları tarafından çeşitli steganaliz çalışmaları gerçekleştirilmiştir (Altun ve ark. 2005). Hem sudamgalama hem de steganografik saklama yöntemleri için evrensel bir steganaliz yaklaşımının geliştirilmeye çalışılan çalışmalar Özer ve ark. ve Koçal ve ark. tarafından gerçekleştirilmiştir (Özer ve ark. 2003, Avcıbaş. 2006, Özer ve ark. 2006, Koçal ve ark. 2008).

Konuşma sinyalleri yıllar boyunca yalnızca lineer modelleme teknikleri ile modellenmiştir. Gerek nonlineer modelleme tekniklerinin gelişmesindeki gecikme, gerekse lineer modellerin işlemlerde sağladığı kolaylık nedeniyle uzun süre nonlineer modeller gereken önemi kazanamadı. Fakat özellikle 1990'lı yılların başlarından itibaren gerçekleştirilen çalışmalar yıllar boyunca kabul edilen konuşma seslerinin durağan (stationarity) ve lineer olduğu varsayımlarını çürütmüştür. Kokkinos ve Maragos tarafından 2005 yılında, Banbrook ve McLaughlin tarafından 1999 yılında, Martinez ve arkadaşları tarafından 2002 yılında ve Pitsikalis ve Maragos tarafından 2002 yıllarında gerçekleştirilen çalışmalar konuşma sesinde var olan nonlineer fenomene işaret etmekte ve bu nonlineer dinamiklerin lineer modelleme ile kapsanamayacağını belirtmektedirler. Bu çalışmalarda ayrıca konuşma sesleri içerisinde bulunan nonlineer dinamiklerin kaotik sistemler ile benzerlik gösterdiğini, yapılan denemeler ile de konuşma seslerinin kaotik olarak kabul edilebileceği ifade edilmiştir (Banbrook ve McLauglin. 1994 ve 1999, Kokkinos ve Maragos. 2005, Martinez ve ark. 2002, Pitsikalis ve Maragos. 2002). Bu çalışmalardan Martinez ve arkadaşları tarafından 2002 yılında ve Pitsikalis ve Maragos tarafından 2002 yıllarında gerçekleştirilen bu varsayıma dayanarak analizlerde bulunmuş ve başarılı olmuşlardır.

Konuşma seslerinin kaotik olduklarını ve örtü sinyali içerisine veri gizleme işleme işleminin sinyale gürültü eklenmesi varsayımları kullanarak gerçekleştirilen bu çalışma literatürde bir ilki teşkil etmektedir. Bu varsayımlar yardımıyla örtü sinyallerine ait kaotik özelliklerin aynı sinyalin stego versiyonunun kaotik özelliklerine göre farklılık göstereceği yaklaşımı benimsenmiştir. Literatürde yer alan kaotik sistemlerin ölçülebilirliğini araştıran ve analizlerini gerçekleştiren Hatalı Komşular Oranı (Kennel ve Abarbanel. 2002), Lyapunov Üstelleri (Martinez ve ark. 2002), Vekil veriler (Theiler ve ark. 1992) ve kesirli boyut tahmin edicileri (Abarbanel. 1996, Hilborn. 2000) gibi

araçlar bu amaçla kullanılmıştır. Sayısal değer üreten bu yöntemleri kullanılarak örtü ve stego sinyallerin kaotik özellikleri incelenmiş, stego sinyalleri ayırt etmede başarılı olanlar ile detaylı performans testleri gerçekleştirilmiştir.

3. MATERYAL VE YÖNTEM

3.1 Steganografi

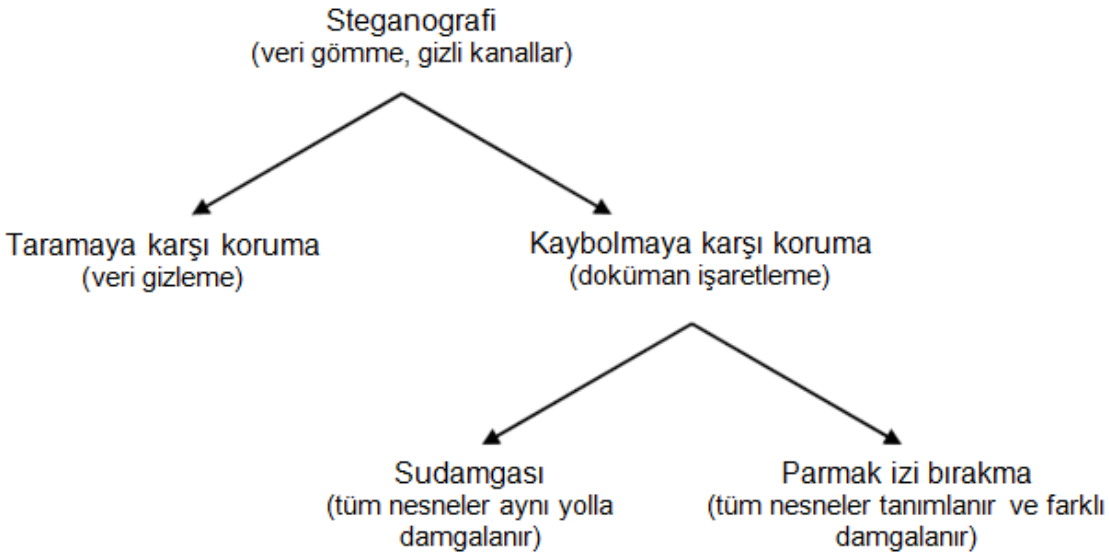
Steganografi, gizli mesajların sayısal sinyaller (veriler) içerisine saklanması yolu ile haberleşme bilgisinin var olduğunun gizlenmesi bilimidir (Steganografi veri gizleme, veri saklama, veri gömme bilimi adı altında Türkçe'ye çevrilebilir). Bir başka deyişle steganografi veri içine veri gömerek gömülen verinin varlığını saklar. Gizli verinin varlığını saklamak için gömme işlemi sonucunda örtü-sinyalin (herhangi bir gizli bilgi içermeyen ses, görüntü, metin veya video verileri gibi sayısal sinyaller) en az bozulmaya uğraması hedeflenir. Ayrıca örtü-sinyaline maksimum büyüklükte gizli veri saklamaya çalışılır. Steganografi bilim dalında saklanmak istenen gizli mesaj sinyallerine stego-sinyal denilmektedir ve örtü-sinyal gibi ses, görüntü, metin veya video verileri gibi sayısal sinyallerden oluşur.

Gerçek anlamda güvenilir ve keşfedilemez haberleşmenin sağlanması için stego-sinyaller ile örtü-sinyaller arasında herhangi bir farkın bulunmaması gerekmektedir. Fakat bu durum ancak ideal bir steganografi yöntemi için geçerlidir. Gizli verinin gömülmesi ile örtü-sinyal üzerinde mutlaka bazı değişiklikler yapılmıştır ve uygun yöntemlerle örtü-sinyal ve stego-sinyal arasındaki bu farklılıklar ortaya çıkartılabilir. İşte örtü-sinyal ile stego-sinyal arasındaki bu farklılıkların ortaya çıkartılması, diğer anlamda gizli mesaj içeren sayısal sinyallerin ayırt edilmesi işlemine *steganaliz* denilmektedir. Steganaliz ile sadece sinyalin içerisinde herhangi bir gizli mesajın bulunup bulunmadığını algılanmaktadır. Algılama sonrası gizli mesajın deşifre edilmesi başka bir bilim dalı olan kriptografiye aittir.

Steganografinin kriptografiden (şifreleme) en önemli farkı steganografide saklı mesajın varlığının gizlenmesidir. Yani saklı verinin örtü-sinyal içine gömüldüğü bilgisi sadece mesajın alıcısı tarafından bilinir ve örtü-sinyale sahip olan bir başkası saklı verinin varlığını fark edemez. Kriptografide ise gönderilen verinin gizli olduğu herkes tarafından bilinir. İçeriği gizli anahtar olmadan anlaşılamaz ve gizli verinin anlaşılabilmesi için çok büyük çabanın ve zamanın harcanması gerekir. Eğer birbirleri ile gizli olarak haberleşen iki kişiyi gözetleyen üçüncü bir kişi haberleşmenin gizliliğini fark edecek olursa steganografi esas amacına ulaşamamış olacaktır.

Burada ayrıca steganografi ile sürekli karıştırılan steganografinin bir alt dalı olan sudamgası (watermarking) yöntemlerinin arasındaki farkı belirtmekte fayda bulunmaktadır. Sudamgası yöntemleri genelde bir kaynak tarafından ortaya konan verinin orijinal (bozulmamış veya sahte olmayan) olduğunu veya veri kaynağı hakkında bilgi sunabilmek için örtü-sinyalin üzerine herhangi bir gizlilik amacı gütmeden işitme organlarıyla hissedilemeyecek kadar küçük bir veri koymaktadır. Sudamgasına en iyi örnekler şunlar olabilir; Banknot içerisindeki filigran ile banknotun sahte olmadığı, çekilen bir fotoğrafın kendisine ait olduğunu ispat etmek isteyen fotoğrafçının fotoğrafı sayısal olarak imzalaması (içerisine kendi bilgilerini gömmesi), bir videonun bozulmadan kesintisiz saklandığını garantilemek isteyen arşiv görevlisinin videonun tamamına belli bir bilgiyi gömmesi, vb. Sudamgasında, steganografide olduğu gibi örtü-sinyalin bozulmamasına yüksek hassasiyetle dikkat edilmediği için steganaliz yöntemleri sudamgası ile gizlenmiş verileri yüksek doğrulukla algılamaktadır.

Şekil 3.1'de Steganografinin farklı yaklaşımları görülebilmektedir.



Şekil 3.1. Farklı steganografi metotları.

3.1.1 Stego-sistem

Steganografik bir sistemin modeli (bu stego-sistem olarak ta bilinir), veriler ve aralarındaki ilişkileri içeren süreçleri tanımlar. Bir stego-sistem genel olarak Şekil 3.2'de gösterilmiştir. Stego-sistem aşağıdaki bileşenleri içerir (Kutucu ve Kaya. 2002).

Mesaj: Gömülecek olan gizli mesaj.

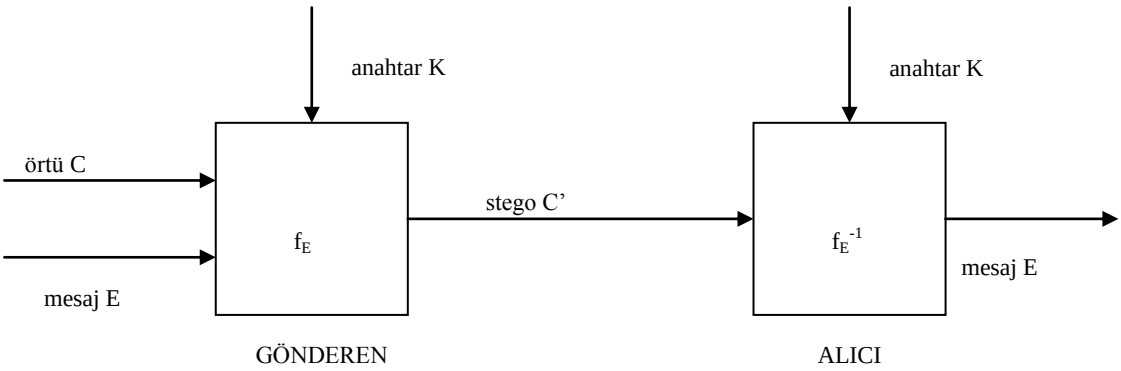
Örtü-sinyal: İçerisine mesaj gömülecek olan temiz veri (Cover-signal).

Stego-sinyal: Gömülmüş olan bir mesajı içeren görünüşte örtü-sinyal ile ayırt edilemeyen, örtü-sinyalin değiştirilmiş versiyonu (Stego-signal).

Anahtar: Gönderici ve alıcı tarafından da bilinmesi gereken gömme ve açma işlemleri için gerekli olan anahtar gizli veri.

f_E : Girdi olarak anahtar, mesaj ile örtü-sinyale sahip ve çıktı olarak stego-sinyali üreten steganografik fonksiyon.

f_E^{-1} : Girdi olarak anahtar ile stego-sinyale sahip olan çıktı olarak mesajı üreten bir steganografik fonksiyon (f_E^{-1} fonksiyonu f_E fonksiyonun ters fonksiyonudur).



Şekil 3.2. Stego-sistemin genel yapısı (Kutucu ve Kaya. 2002).

Günümüzde ise sayısal (dijital) nesneler üzerinde steganografi uygulamaları yapılmaktadır ve gelişen teknoloji nedeniyle, verilerimizi korumak amacıyla son yıllarda sıklıkla kullanılmaya başlanmıştır. Steganografi, Dilbilim Steganografi ve Teknik Steganografi olmak üzere kendi içerisinde ikiye ayrılmaktadır. Dilbilim

steganografi, taşıyıcı verinin metin (text) olduğu steganografi koludur. Teknik Steganografi ise birçok konuyu içine almaktadır. Bunlar; görünmez mürekkep, gizli yerler, microdot'lar ve bilgisayar tabanlı yöntemler gibi başlıklar altında toplanabilmektedir. Bilgisayar tabanlı yöntemler metin, ses, görüntü, resim dosyalarını kullanarak veri gizleme yöntemleridir.

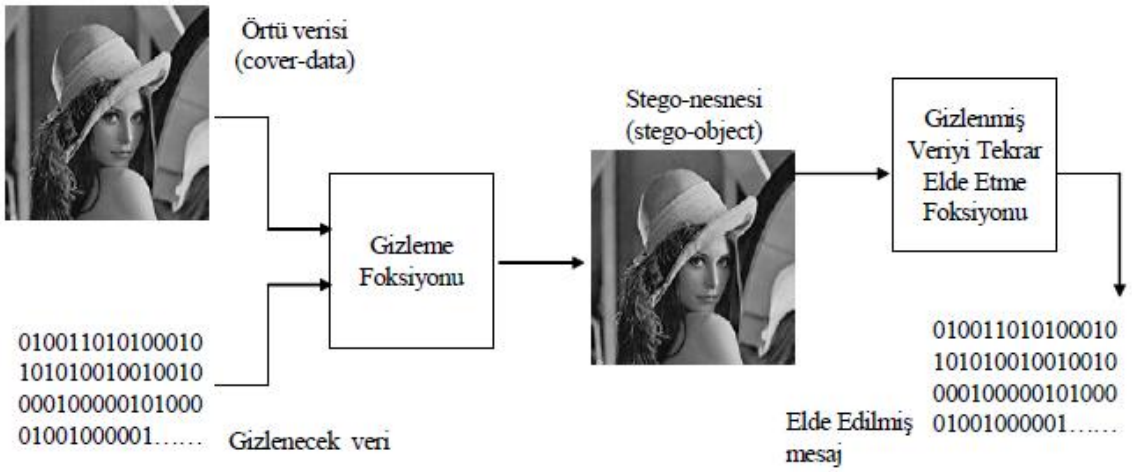
Steganografi kullanım alanları açısından üçe ayrılmaktadır. Bunlar aşağıdaki gibidir:

- Metin (text) steganografi

- Görüntü (image) steganografi

- Ses (audio) steganografi.

Görüntü dosyaları için bir steganografik sistem Şekil 3.3'de gösterilmektedir. Gönderici bir gizleme fonksiyonu kullanarak bir steganogram yaratır. Gizleme fonksiyonu, verinin saklanacağı taşıyıcı ortam ve gizlenecek veri olmak üzere iki parametreye sahiptir (Westfeld ve Pfitzmann. 1999).



Şekil 3.3. Görüntü Stego-sistemi

3.1.2 Steganaliz

Steganaliz, steganografik sistemlerin gizliliğini kırma sanatı ve bilimi olarak tanımlanabilir. Bu bilimle uğraşanlara ise steganalist (steganalyst) denir (Kutucu ve Kaya. 2002).

Elektronik ortamda bilgiyi saklama ortam özelliklerinin değişmesini birlikte getirir. Bu değişiklikler gömülü mesajın varlığını ortaya çıkaran bir imza, gürültü ya da bir parmak izi olabilir. Bu değişiklikler de steganografinin amacını bozmakla birlikte kaçınılmazdır.

Saldırılar steganalistin elinde var olan bilgilere bağlı olarak farklı formlarda olabilir (Çizelge 3.1).

Çizelge 3.1. Steganografi için farklı saldırı yaklaşımları

Stego saldırısı	Sadece stego-sinyal elimizde
Seçili stego saldırısı	Stego-tekniği (algoritması) biliniyor ve stego-nesne elimizde
Bilinen örtü saldırısı	Stego-sinyal ve örtü-sinyalin orijinal bir kopyası elimizde
Bilinen stego saldırısı	Stego-tekniği (algoritması) biliniyor, stego-sinyal ve orijinal sinyal (örtü-sinyal) elimizde.
Bilinen mesaj saldırısı	Gizli mesaj ve stego-sinyal elimizde
Seçili mesaj saldırısı	Steganalist bu yöntemde stego-nesnesini analiz edebilmek için çeşitli mesajlar seçer, steganografik araçlar kullanır ve algoritmayı bulmaya çalışır.

Steganalizde saldırı tipleri iki ana başlık altında incelenir. Bunlar;

- Aktif Saldırı: Yok Etme/Bozma (Distortion)
- Pasif Saldırı: Tarama (Detection)

Aktif Saldırı: Gizli mesajı ortaya çıkarmanın önemli olmadığı durumlarda veya sudamgasının ortadan kaldırmak istenildiği durumlarda sinyalin bir filtreden geçirilmesi veya yeniden oluşturulması (rendering) gibi yollar ile sinyalin bozulmasıdır. Böylece sinyalin içerisinde gizli bir mesaj veya sudamgası olması durumunda bu bilgiler geri dönülemez bir biçimde yok edilecektir. Bu işlem pasif saldırıya göre hızlı bir işlem olmasına karşın, hangi sinyallerde gizli bilgi taşındığı bilgisinin kaybedilmesi sebebiyle

(dolayısıyla kimler, ne amaçla, hangi gizli bilgiyi iletiyor bilgileri yok olacaktır) genellikle tercih edilmeyen bir yöntemdir.

Pasif Saldırı: Bu tür saldırı ile sayısal sinyal öncelikle içerisinde gizli bir mesaj var olup olmadığını tespit etmek üzere taranır. İçerisinde gizli mesaj var olmasından şüphelenilen sinyallerde şifre çözme (decoding) işlemi gerçekleştirilebilir veya sadece mesajı gönderen ve alan taraflar takip altına alınabilir.

3.2 Ses Steganografisi

İnsan kulağı ses düzenindeki değişiklikleri algılamada oldukça hassas olmasına rağmen fakat birbirine göre farklı seviyedeki ve yaklaşık aynı frekansları birbirinden ayırt etmede o kadar iyi değildir. Buna örnek olarak yüksek genlikli sesle altındaki daha sessiz olan gürültü benzeri sesleri algılayamamaktadır. Steganografideki gibi bir haberleşme ortamına veri gizleme söz konusu olduğunda, kulağımızın bu tip sesleri ayırt edememe dezavantajını kullanmak oldukça faydalı olmaktadır. Ses steganografisindeki diğer önemli bir taraf ise gizli veriyi taşıyacak stego-sinyalin kesinlikle herhangi bir sayısal işleme (filtreleme, ses iyileştirme, vb.) tabi tutulmamasını garanti etmektir. Çünkü bu şekilde sinyalin herhangi bir sayısal sinyal işleme algoritmasına tabi tutulması ses sinyalinin yapısını bozacak ve gizlenen verinin bir daha tekrar elde edilmesine (decoding) imkân vermeyecektir (Wohlgemuth. 2002).

3.2.1 Ses stego-sistemleri

Tezin ilgi alanı olan ses stego-sistemleri 4 ana veri saklama yaklaşımı altında incelenebilir. Bunlar;

- En Değersiz Bit (LSB-Least Significant Bit) Veri Saklama
- Spektruma Yayarak Gizleme Tekniği ile Veri Saklama
- Eko Veri Gizleme Tekniği ile Veri Saklama
- Algısal Maskeleme Tekniği ile Veri Saklama

3.2.1.1 En değersiz bit (LSB-Least Significant Bit) veri saklama

En önemsiz bite ekleme yöntemleri (Least Significant Bit Insertion Methods) yaygın olarak kullanılan ve uygulaması basit yöntemlerdir. Fakat yöntemin dikkatsizce uygulanması durumunda veri kayıpları ortaya çıkmaktadır. Bu yöntemde; ses sinyalini oluşturan her örnekteki (sample) her sekizlinin (byte) en önemsiz biti olan son biti değiştirilerek o bitin yerine gizlenmesini istediğimiz verinin bitleri sırasıyla verinin başlangıcından itibaren birer birer yerleştirilmektedir. Burada her sekiz bitin en fazla bir biti değişikliğe uğratıldığından ve eğer değişiklik olmuşsa da değişiklik yapılan bitin sekizlisinin en az anlamlı biti olmasından dolayı, ortaya çıkan stego-sinyaldeki (= örtü sinyali + gizlenen veri) değişimler insan tarafından algılanamaz boyutta olmaktadır. Son bite ekleme işlemi ses sinyalinin başından ya da sonundan olmak üzere sıralı bir şekilde olabileceği gibi, bir rasgele fonksiyon üreteci (random function generator) kullanılarak belirlenen sinyal dizisi elemanları üzerinde değişiklik yapılması şeklinde gerçekleştirilebilmektedir (Şahin ve ark. 2006).

Bazı steganografik sistemler bazı gizli anahtarlar da kullanabilmektedir. Bu anahtarlar ikiye ayrılırlar:

1. *Steganografik anahtarlar;* mesajı ses sinyalinin içine gizleme ve tekrar elde etme işlemini kontrol etme için kullanılırlar.

2. *Kriptografik anahtarlar;* Mesajın ses sinyalinin içine gizlenmeden önce şifrelenmesi ve daha sonra deşifrelenmesinde kullanılırlar (Westfeld ve Pfitzmann. 1999).

LSB veri saklama tekniği sudamgalama tekniklerinde daha çok steganografi uygulamalarında kullanılmıştır. Özellikle kriptografik anahtarlar ile uygulanan versiyonları günümüzde en çok kullanılan ses steganografi uygulamalarıdır. Bu tezde ses stego-sistemleri arasında literatürde en sıklıkla karşımıza çıkan Steghide (Steghide. 2006), Hide4PGP(Hide4PGP. 2006), Stokastik Modülasyon (Fridrich ve Goljan. 2003), Steganos (Steganos. 2006) ve MP3Stego (MP3Stego. 2006) veri saklama teknikleri incelenecektir.

3.2.1.2 Spektruma yayarak gizleme tekniği ile veri saklama

Spektruma yayarak (Spread-Spectrum) şifreleme tekniği, dar-bantlı bir sinyali (mesajı) daha geniş-bantlı sinyaller içerisine gizlemek anlamına gelmektedir. Bu metot genel

anlamda bir gürültü kaynağı tarafından üretilen gürültüyü ses sinyaline eklemektedir. Bu durumda mesaj, ses sinyalinin neredeyse tüm frekans spektrumuna yayılmış (gürültünün frekans spektrumunun olabildiğince tamamına yayılması istenmektedir) gürültü şeklinde taşınmış olacaktır. Literatürde spektruma yayarak gizleme teknikleri en çok sudamgalama tekniği olarak kullanılmış ve özellikle Bender ve arkadaşlarının 1996 yılındaki çalışmaları ile ivme kazanmıştır. Bu çalışmalarında DSSS(Direct-Sequence Spread Spectrum) ve FHSS(Frequency-Hopping Spread Spectrum) yöntemleri ile sudamgalama uygulamaları yapmışlardır. Ayrıca farklı bir sudamgalama ve veri gizleme tekniğini Cox ve arkadaşları 1997 yılında önermişler ve literatürde önemli bir yer edinmişlerdir.

3.2.1.3 Eko veri gizleme tekniği ile veri saklama

Bu teknik, veriyi gizlemede ses akışında yer alan ekoları kullanmaktadır. Ekolar eğer doğru kullanılırsa genellikle, sesin kalitesini bozmak bir yana dinleyenler açısından kalitesini arttırmaktadır. Sinyale eklenecek ekolar, sesin başlangıç genliği, azalma eğimi ve offset değerlerine göre değişim göstermektedir. Diğer taraftan orijinal ses ile eko arasındaki zaman gecikmesi azaldıkça kulağın bu ekonun gerçek dışı olmasını (doğal olmaması) durumunu algılaması güçleşmektedir. İşte bu zaman gecikmesi aslında sayısal verinin "1" veya "0" olması anlamına gelmekte ve ses sinyali boyunca var olacak bu zaman gecikmeleri, hepsinin birlikte çözülmesi durumunda gizlenen veriyi ortaya çıkaracaktır. Eko veri gizleme tekniği, eğer ses kalitesiz (gürültülü, bozulmuş, düşük örnekleme frekansı ile örneklenmiş) değilse ve boşluklu (uzun veya kısa sessiz boşluklar) olmaması durumlarında oldukça işe yarar sonuçlar ortaya koymuştur (Bender ve ark. 1996).

3.2.1.4 Algısal maskeleme tekniği ile veri saklama

Kulağın farklı sesleri eğer yaklaşık aynı frekanslarda ve farklı genliklerde olursa algılamada zorluklar yaşadığından bahsetmiştik. Algısal maskeleme, bir sesi daha yüksek ve yaklaşık aynı frekanstaki başka bir sesin arkasına saklama tekniğidir. Bu teknik aslında toplum tarafından da oldukça sık kullanılmaktadır. Örneğin ne konuştuklarının duyulmasını istemeyen kişilerin televizyon veya radyonun sesini açması gibi bu tekniğe uygun bir örnektir. Bu teknik aslına LSB veri saklama tekniğinin gizlenecek verinin karakteristiğine göre yeniden düzenlenmesini içeren özel bir

durumudur. Bu teknik kriptografik anahtarlamalı LSB tekniğinin kullanımındaki kolaylığı sebebiyle literatürde ağırlık kazanamamış ve daha çok 2000 yılı öncesinde yapılmış çalışmalar ile sınırlı kalmıştır.

3.2.2 Ses steganalizörü tasarımı

3.2.2.1 Ses steganalizörlerinin literatürdeki durumu (State-of-art)

Ses sinyalleri içerisinde herhangi bir gizli veri var olup olmadığını kontrol etmek üzerine literatürde bazı steganografi yöntemlerine özel veya herhangi bir steganografi yöntemine özel olmayan genel (universal) steganalizörler tasarlanmıştır. Bu çalışmalardan kısaca bahsetmek gerekirse, bunlar arasında literatürde önemli yer tutan bir çalışma olan Westfeld'in önerdiği steganaliz yöntemi (Westfeld 2003) LSB steganografi yöntemi kullanılarak saklanmış verilerin algılanmasına yöneliktir. Westfeld ve Pfitzman'ın önerdiği diğer bir steganaliz çalışması ise MP3 ses sinyallerinin içerisine gizlenmiş verilerin algılanması üzerine yapılmış bir çalışmadır (Westfeld ve Pfitzman 1999). Johnson ve arkadaşlarının yaptığı başka bir öneri ise LSB ve Hide4Pgp steganografi algoritmalarına göre gizlenmiş verilerin algılanması üzerinedir (Johnson ve ark. 2005). Ayrıca DSSS sudamgası ve stokastik modülasyon steganografi yöntemleri için Altun ve arkadaşları tarafından çeşitli steganaliz çalışmaları gerçekleştirilmiştir (Altun ve ark. 2005). Hem sudamgalama hem de steganografik saklama yöntemleri için evrensel bir steganaliz yaklaşımının geliştirilmeye çalışılan çalışmalar Özer ve ark. ve Koçal ve ark. tarafından gerçekleştirilmiştir (Özer ve ark. 2003, Avcıbaş. 2006, Özer ve ark. 2006, Koçal ve ark. 2008).

Tezde yalnızca Çizelge 3.1'de gösterilen farklı steganografi saldırı tekniklerinden birinci sıradaki yani elimizde yalnızca stego-sinyalin bilindiği, gizleme tekniğinin bilinmediği durum ele alınacaktır. Gizli verinin tespiti sonrasında gerçekleştirilecek saldırı tekniği tamamen uygulamayı yapacak kişiye bırakılmıştır.

Tezin bu kısmından sonra ses steganalizörlerinin tasarımı gerçek örneklerle adım adım anlatılacak, önerilen steganalizörün başarımının literatür tarafından kabul edilir şekilde

ölçülmesi ve mevcut steganalizörler ile aynı zeminde karşılaştırmasının gereklilikleri iletilecektir.

3.2.2.2 Özellik vektörünün oluşturulması

Bir steganalizörün yüksek doğrulukta çalışmasını sağlayan en önemli etken, özellik vektörünün örtü ve stego sinyalleri birbirinden ayırt edecek elemanlardan oluşmasıdır. Örneğin bir ses sinyalinin ortalaması, sinyal içerisinde herhangi bir veri gömülmesi (bir nevi gürültü eklenmesi) ile kolaylıkla değişebilecek bir özellik değildir. Bu yüzden böyle bir özelliğin özellik vektöründe yer alması steganalizörün doğru çalışmasına fayda vermeyecek aksine işlem süresini uzatacağı için farklı steganalizörlere karşı verimsiz duruma düşürecektir. Buna karşılık bulunabilecek tek bir özellik ki bu özellik örtü ve stego sinyallerin durum uzayında çok farklı bölgelerde yer almasını sağlayabildiği takdirde, tek başına yüksek başarımla gizli veri varlığını tespit edebilir. Özellik vektörü aşağıdaki şekilde genel olarak ifade edilebilir;

(3.1)

Önerilen özellik vektörünün başarılı bir steganalizör olup olmadığını yapılacak bazı testler sonrasında anlaşılabilmektedir. Yapılacak bu testlerin dünya literatürü tarafından kabul edilebilmesi bakımından genel olarak kabul edilmiş araçlardan oluşması gerekmektedir. Aksi halde önerilen özellik vektörünün diğer özellik vektörleri ile doğru bir karşılaştırması yapılamaz, dolayısıyla başarılı bir steganalizör olduğu kanıtlanamaz olmaktadır.

3.2.2.3 Veri setinin seçilmesi

Önerilen steganalizörün başarım ölçümünün kabul edilebilmesi için öncelikle üzerinde çalışılacak veri setinin literatür tarafından kabul görmesi gerekmektedir. Bu set, konuşma sesleri için başarım ölçümü yapılması gerektiğinde konuşma seslerinin yer aldığı TIMIT (TIMIT. 2006) veya telefon görüşmeleri seslerinin yer aldığı NTIMIT olabilir. Bunun dışında müzik aletleri veya şarkılar ile de test edilmesi gerektiğinde genel olarak ulaşılabilir sanatçıların albümlerindeki ses verileri kullanılabilmektedir.

3.2.2.4 Stego-sinyal veri setinin oluşturulması

Veri setinin seçimi sonrasında, tüm verilere veya alt veri gruplarına steganalizörün test edileceği steganografi teknikleri ile farklı gömme oranlarında veriler saklanarak stego-sinyal veri setleri oluşturulabilir. Alt stego-sinyal veri setlerine örnek olarak DSSS tekniği ile 30dB oranında SWR (Signal-to-Watermarking Ratio) oluşturacak şekilde veri gömülmüş bir alt veri seti verilebilir. Bu veri setleri eğer evrensel bir steganalizör önerisinde bulunuluyor ise literatürde kabul görmüş steganografi tekniklerinin çoğunluğunu kapsaması gerekmektedir. Yine farklı steganalizör teknikleri ile doğru bir karşılaştırma yapılabilmesi için mutlaka sabit ve bilinen bir SWR ile veri gömülmesi istenilmektedir. Burada orijinal veri seti, steganalizör için örtü-sinyal veri setini oluşturacaktır. Örtü sinyali enerjisinin, gömülecek verinin enerjisine oranını belirleyen SWR aşağıdaki gibi hesaplanmaktadır;

(3.2)

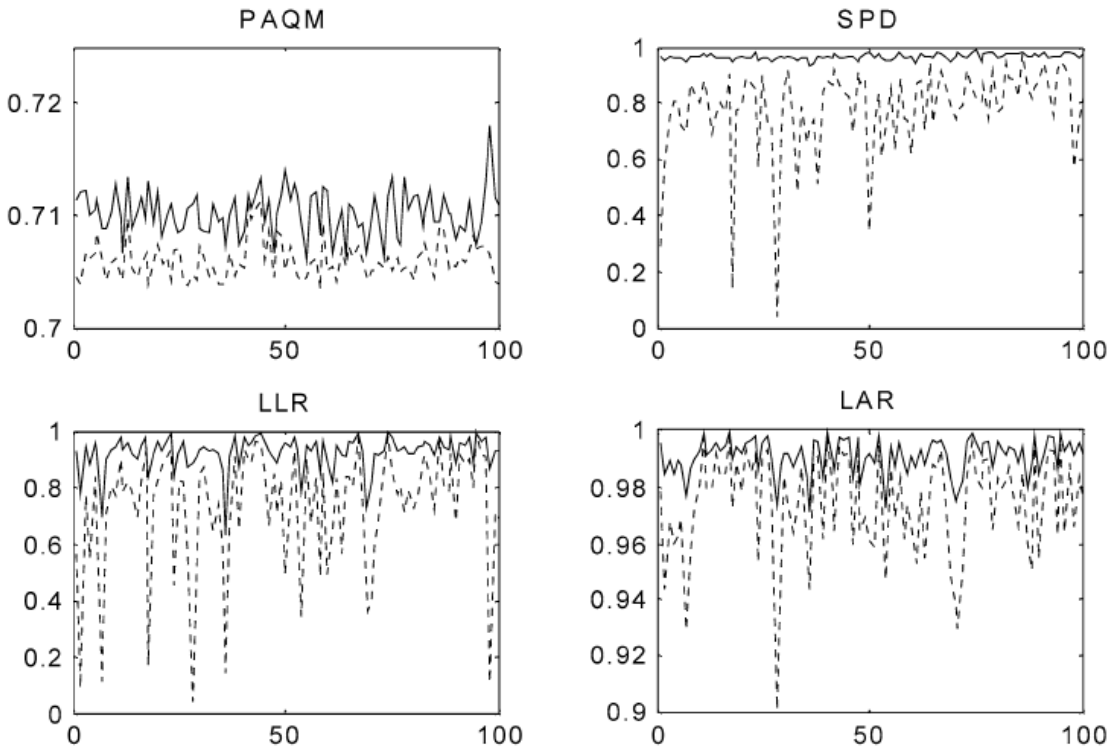
Burada *x(n)* örtü sinyalini, *y(n)* ise stego-sinyalini temsil etmektedir. Bu oran sadece sudamgalama tekniklerinde kullanılabilir olup, diğer steganografik tekniklerde kullanılmamaktadır. Sudamgası olmayan steganografik tekniklerde gömülen verinin boyutu ile alakalı olan gömme kapasitesi kullanım oranına göre veri gömme işlemi gerçekleşmektedir. Gömme kapasitesi tamamen algısal olup, gizlenen veri boyutunun küçük adımlarda arttırılması durumunda, sesin kalitesinin bozulduğunun hissedilmeye başlandığı durumdaki gizlenen verinin boyutu, %100 gömme kapasitesi kullanım oranına karşılık düşmektedir. Bu veri boyutunun yarısı kadar bir verinin aynı sinyal içerisine gömülmesi durumunda ise %50 gömme kapasitesi kullanım oranı ile veri gömülmüş olacaktır.

SWR değerini hesaplayan MATLAB Kodu, Ek-1'de verilmiştir.

3.2.2.5 Veri setleri için özellik vektörlerinin oluşturulması

Elimizde artık hazır bulunan veri setlerinin içerisinde bulunan her bir ses sinyali için, **F,** özellik vektörünün oluşturulması gerekmektedir. Böylelikle her bir ses sinyali bir vektör

ile temsil edilmiş olacak ve tüm sınıflandırma işlemleri bu vektör üzerinden gerçekleştirilecektir. Özellik vektörlerinin oluşturulması sonrasında, seçtiğimiz özelliklerin iyi bir steganalizör için uygun olup olmadığını aslında bu aşamada ilk kontrollerini yapabilmekteyiz. Şekil 3.4'de 100 ses sinyalinden oluşan bir veri seti üzerinde yapılan iyi bir özellik ve kötü bir özelliğin ayırt ediciliği görülmektedir. Burada PAQM ve SPD oldukça iyi ayırt edici özellikler olup, LLR ve LAR ortalama seviyede ayırt ediciliği bulunan özelliklerdir.



Şekil 3.4. 100 adet ses sinyalinden oluşan veri kümesi üzerinde PAQM, SPD, LLR ve LAR özelliklerinin ayırt ediciliği (Düz çizgiler örtü sinyalleri, kesikli çizgiler stego-sinyalleri temsil etmektedir) (Özer ve ark. 2003).

3.2.2.6 Sınıflandırıcı seçimi

Her bir ses sinyaline ait özellik vektörlerinin elde edilmesi sonrasında Şekil 3.4'de gözle yaptığımız ayırt etme işlemini bir sınıflandırıcı tasarlayarak otomatik hale getirmeliyiz. Bu sebeple nesne tanıma algoritmalarından yaptığımız çalışmanın hassasiyetine ve hızına uygun olanını seçmeliyiz. Yüksek hız ve düşük hassasiyet istenen durumlarda

lineer sınıflandırıcılar, yüksek hassasiyet istendiği ve hızın çok önemli olmadığı durumlarda SVM (Support Vector Machine) gibi nonlineer sınıflandırıcılar kullanılabilmektedir (SVM. 2011).

3.2.2.7 Özellik vektörünün rafine edilmesi

Aslında bu kısma kadar anlatılan aşamalar ile artık önerilen steganalizörün tasarımı bitmiş ve önerilen özellik vektörünün başarımını öğrenebilir durumdadır. Fakat tam da bu adımdan önce önerilen özellik vektöründeki bağımlı elemanlar keşfedilerek elenmeli ve özellik vektörü rafine bir hale getirilmelidir. Ancak bu şekilde steganaliz sürecinde gereksiz geçen zaman sarfiyatından kurtulabilinmektedir. Steganalizde belirli bir süre içerisinde yapılması gereken işlemlerin çokluğu düşünülürse kazanılabilecek her zaman tasarrufuna ihtiyaç bulunmaktadır. Bu yolla aynı zamanda, sınıflandırıcının sınıflandırma süreci karmaşası basitleştirilmiş olacaktır. Yapılan rafine edilme işlemine "Temel Bileşenler Analizi" (PCA-Principal Component Analysis veya ICA-Independent Component Analysis) işlemi denilmektedir ve nesne sınıflandırma uygulamalarının vazgeçilmez adımlarından biridir. Ardışıl İleri Yönde Kayan Arama (SFFS-Sequential Forward Floating Searching) örnek bir PCA algoritmasıdır (Pudil ve ark. 1994).

3.3 Kaotik Özelliklerin Ses Steganalizinde Kullanımı

3.3.1 Kaos kuramı

Kaos, deterministik bir sistemin düzensiz yani hiç beklenmedik bir şekilde davranabilmesidir. Örneğin, düzgün bir borudan akan bir sıvının akışında bazen kaotik durumlar görülebilir. Newton kanunlarından elde edilen dinamik denklemler düzgün akışları ifade edebilirken, akışkanın akış hızı belirli bir değeri aştıktan sonra akışta girdaplar oluşur ve Newton kanunları geçerliliğini yitirir. Yani artık akış kaotiktir.

Kaosun meydana gelmesi, belirli parametrelere bağlı olduğu gibi sistemin yapısına da bağlıdır. Kaos genellikle kararsız, karmaşık ve doğrusal olmayan sistemlerde ortaya çıkmaktadır. Karmaşık sistemler, çok sayıda elemanın birbiriyle etkileştiği, pek çok serbestlik derecesi olan yani çeşitli davranış şekilleri gösterebilen, genellikle de dışarıyla madde ve enerji alışverişi yapan, incelenmesi zor sistemlerdir. Doğrusal

olmayan bir sistem, değişim anında değişim kurallarının da değiştiği bir sistemdir ve sistem, dışarıdan gelebilecek etkilere karşı açıksa sistemden beklenmeyen davranış biçimleri görülebilir. Örneğin hava direncinin hızın küpüyle değiştiği bir sarkaç deneyinde, dışarıdan periyodik bir kuvvetin etkisiyle sürtünme katsayısının belli bir değerinden sonra kaotik bir davranış görülmektedir. Kaotik sistemlerin en önemli özelliği başlangıç şartlarına hassas duyarlılıklarıdır. Deterministik bir sistemin başlangıç durumu ve denklemleri biliniyorsa, sistemin sonraki davranışı belirlenebilir. Kaotik sistemlerde, sistemin zaman içindeki gelişimini tam olarak belirleyebilmek için başlangıç değerlerini sonsuz hassasiyetle bilmek gerekmektedir. Çünkü kaotik sistemler doğrusal olmadıkları için hata zamanla üstel olarak artacaktır (Yılmaz ve Güler. 2006).

Kaotik dinamikleri şekillendiren süreçlerin temelde değişken olması sebebiyle, sistemin durum uzayını, sinyal uzayı (vektörü), **s***(n)*'in skaler ölçümlerinden elde etmek zorundayız. Bu prosedür dinamik yeniden inşa edilme adıyla bilinir. Yeniden inşa edilme, dinamik modellemenin geçerliliğini doğrulamasının yanında, sinyali üreten dinamikler hakkında bilgi edinilmesini de sağlar.

Packard ve arkadaşlarının (1980) önerdiği gibi, dinamik sistemlerin gözlemlenebilir bir değişkeni, *x(n)*, geciktirilmiş versiyonları (*x(n+T), x(n+2T),...*) Öklid Uzayında çizilen yörüngenin koordinatları olarak kullanılabilirler. Yapılan tez çalışmasında, yeniden inşa yöntemi olarak, gecikme koordinatları adıyla bilinen metot kullanılmıştır. *T* sabit *zaman gecikmesi, D_E* durum uzayının *gömme boyutu* olmak üzere;

$$\mathbf{s}(n) = [x(n)\, x(n+T) \ldots x(n+(D_E - 1)T)] \tag{3.3}$$

Böyle bir dinamik sinyali, istenen gecikme ile istenen boyutlarda temsil eden uzaya *faz uzayı* da denilmektedir. Burada Takens'ın teoremine göre, gömme boyutu (D_E), sistemin gerçek boyutunun (*d*) (bağımsızlık derecesi-degrees of freedom) iki katından bir fazla olması durumda ($D_E \geq 2d+1$), sinyaldeki tüm dinamikler faz uzayına yansıyabilmektedir (Takens. 1980).

Eğer zaman gecikmesi, *T*, olması gerekenden daha küçük olursa her bir veri noktası zamanda kendinden bir önce gelen noktaya çok yakın olacak ve bu durumda sinyalin,

s*(n),* faz-uzayı geometrisi gömme uzayında diyagonal bir doğruyu oluşturacaktır. Bu durum birbirine çok yakın iki örneğin birbirlerine bağımlı olmalarından kaynaklanmaktadır. Tam tersine zaman gecikmesi çok büyük olursa, bu durumda örnekler birbirinden tamamen bağımsız hale gelecek, sinyal neredeyse stokastik bir sinyalin özelliklerini taşımaya başlayacaktır. Doğru bir faz-uzayının yeniden oluşturulması işlemi için optimum zaman gecikmesi ortalama ortak enformasyon bilgisi kullanılarak hesaplanabilmektedir (Abarbanel. 1996). Shannon tarafından yapılan ortak enformasyonun tanımı şöyledir;

$$I_{AB} = \log_2 \left[\frac{P_{AB}(a_i, b_j)}{P_A(a_i).P_B(b_j)} \right] \tag{3.4}$$

Burada, *A* ve *B* olaylar, *a* ile *b* ise *A* ve *B* olaylarının sonuçları olmak üzere, $P_{AB}(a,b)$ birleşik olasılık, $P_A(a)$ ve $P_B(b)$ ise tek olayların olasılıklarıdır. *A* olayı *a* ile sonuçlanmış iken, *B* olayı da *b* ile sonuçlanmışsa, bu durumda elde edilen enformasyon eşitlik (3.4)'te verilen formül sonucu kadardır. *A* ve *B* olaylarının sonuçlarının tüm kombinasyonları değerlendirilir ve elde edilebilecek enformasyon miktarları hesaplanabilirse, A ve B olayları için bir ortalama ortak enformasyon hesaplanabilir. Ortalama ortak enformasyon eşitlik (3.5)'te verilmiştir.

$$I_{AB} = \sum_{a_i, b_j} P_{AB}(a_i, b_j).\log_2 \left[\frac{P_{AB}(a_i, b_j)}{P_A(a_i).P_B(b_j)} \right] \tag{3.5}$$

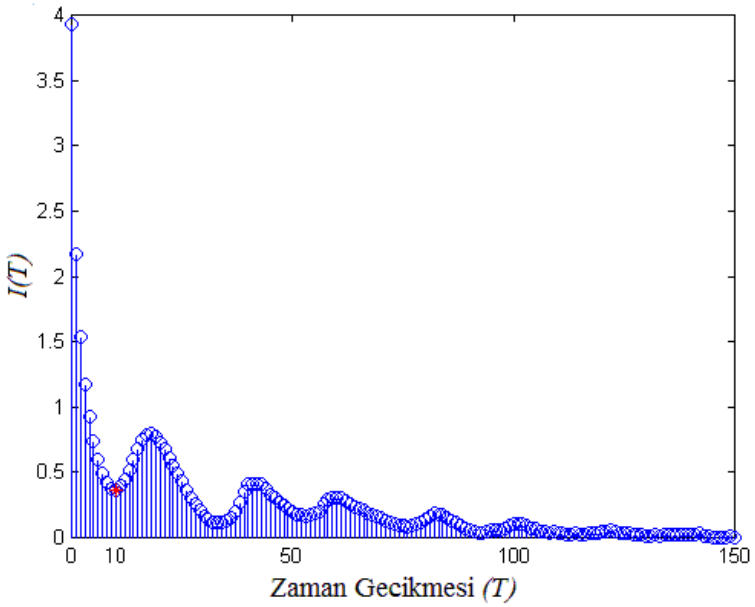
Bu nicelik, olayların lineer ya da nonlineer değişimleri ile bağıntılı değildir. Tamamen iki sonucun ya da değişkenin birbirlerine olan bağımlılıkları ile ilgilidir. Buradan yola çıkılarak, gecikme süresi değiştirilerek eksenlerin birbirleriyle olan bağımlılıkları incelenerek en uygun gecikme süresi seçilebilir. *T*=1'den başlayarak (*T*=0 sinyalin kendisi, maksimum bağımlılık) arttırılarak bağımlılığın en büyük olduğu *T* katsayısı seçilerek, gecikme süresi belirlenmiş olur.

Eşitlik (3.5)'i vektör uzaylarının elemanlarına uygun şekilde değiştirecek olursak, *T* gecikme süresine göre ortak enformasyon şu şekilde hesaplanabilir;

$$I(T) = \sum_{\mathbf{s}(n),\mathbf{s}(n+T)} P(\mathbf{s}(n),\mathbf{s}(n+T)).\log_2\left[\frac{P(\mathbf{s}(n),\mathbf{s}(n+T))}{P(\mathbf{s}(n)).P(\mathbf{s}(n+T))}\right] \quad (3.6)$$

I(T), ortalama ortak enformasyon değeri, *T* değerinin büyümesiyle *x(n)* ile *x(n+T)* arasındaki bağımlılığın azalmasından ötürü sıfıra yaklaşacaktır. Bu sebeple pratik çalışmalar yardımıyla da *I(T)* değerinin ilk minimum yaptığı değer gömme işleminde gecikme süresi olarak tayin edilir.

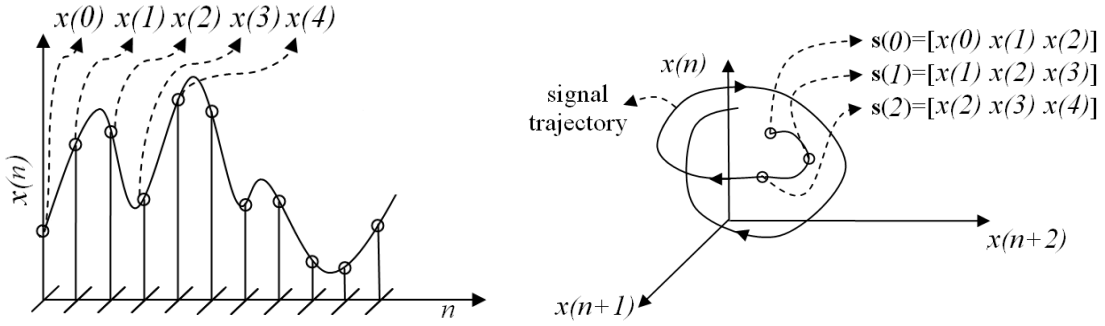
Şekil 3.5'te bir ses sinyalinin *x* değişkeni için hesaplanan ortalama ortak enformasyon miktarı grafiği verilmektedir. Şekilden de görüldüğü üzere sinyalin *x* değişkeni için bağımsızlığın maksimum olduğu ilk nokta olan *T*=10, gömme işleminde kullanılacak olan gecikme süresi olarak kullanılabilir.



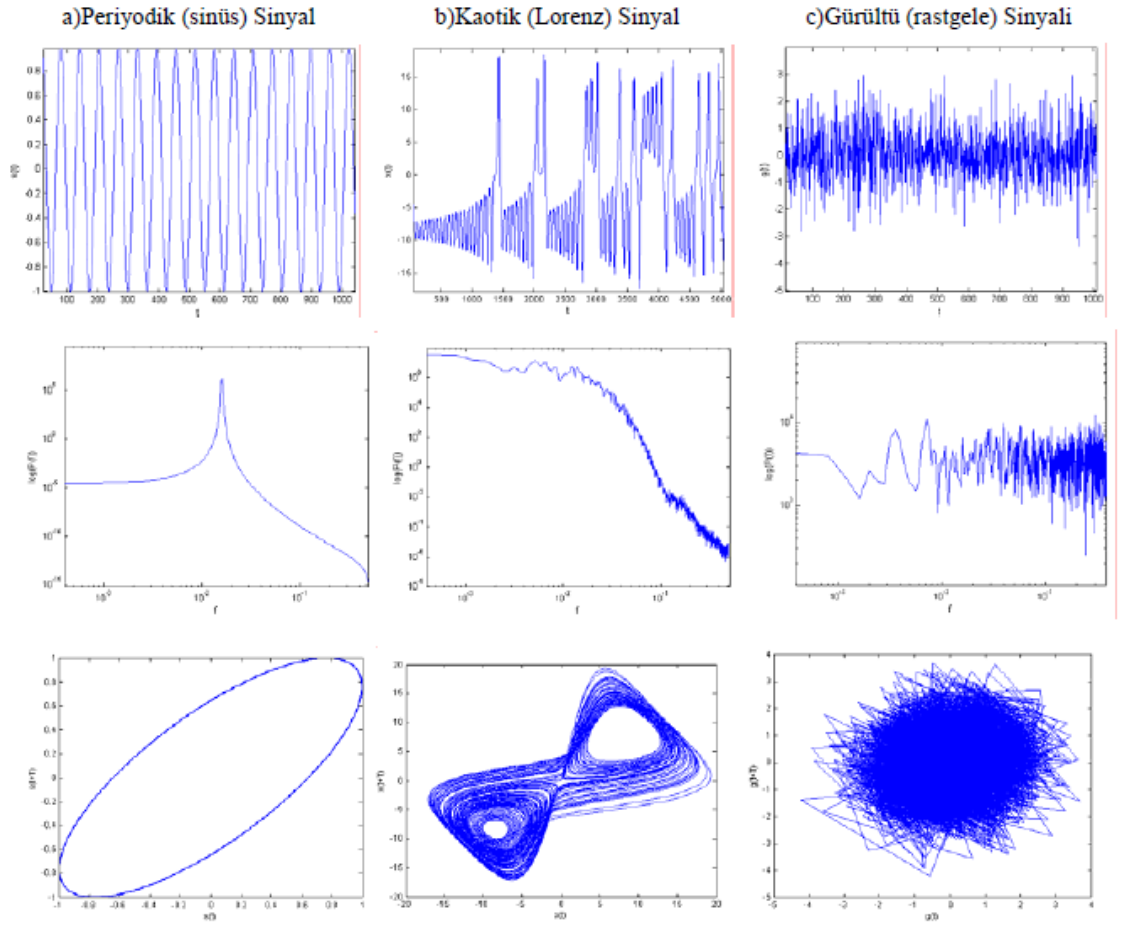
Şekil 3.5. Bir ses sinyalinin *x* değişkeni için ortalama ortak enformasyonun zaman gecikmesi ile değişimi

Şekil 3.6'da *T*=1 ve D_E=3 için *x* zaman sinyaline ait oluşturulan faz uzayı görülebilmektedir. Burada faz uzayındaki her bir nokta **s** faz uzayı elemanı olarak ifade edilmektedir. Faz uzayında sinyal takip ettiği yola sinyalin yörüngesi denilmektedir ve kaotik sinyaller için bu yörünge genel olarak belli şekil oluşturacak şekilde ilerler.

Ortalama ortak enformasyon değerini hesaplayan MATLAB kodu Ek-2'de verilmiştir.



Şekil 3.6. Bir zaman serisinden T=1 ve D_E=3 için faz uzayının oluşturulması.

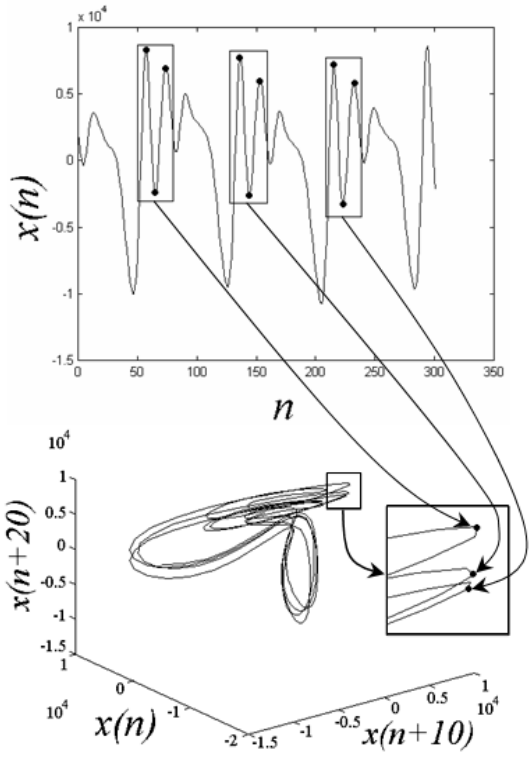


Şekil 3.7. Periyodik (sinüs) (a), kaotik (Lorenz) (b) ve gürültü (rastgele) (c) sinyallerinin güç spektrumları ve faz uzayındaki çekerleri. Yukarıdan aşağıya her bir sütun, zaman serisi şeklindeki sinyali, sinyalin güç spektral yoğunluğunu ve iki boyutlu faz uzayını göstermektedir

Farklı sinyaller için oluşturulmuş faz uzaylarının görünümleri Şekil 3.7'de görülebilmektedir. Burada tüm sinyallerin faz uzayları T=1 ve D_E=2 şartları ile

oluşturulmuştur (Yılmaz ve Güler. 2006). Görüldüğü üzere periyodik (deterministik) bir sinyalin yörüngesi tamamen aynı yolu takip ederek çok belirgin bir şekil oluşturmuştur. Buna rağmen yarı-periyodik (pseudo-periodic) diyebileceğimiz kaotik bir sinyal belirgin bir yörünge üzerinden küçük sapmalar ile belli bir şekli oluşturmuştur. Bu durum kaotik sinyallerin ayırt edici bir özelliğidir. Deterministik sinyallerin tersine stokastik (rasgele) bir sinyal olan gürültü sinyali tamamen karmaşık bir yörünge izleyerek belirsiz bir faz uzayı şekli oluşturmuştur.

Ses sinyallerinin de özellikle konuşmadaki sesli harflerin veya müzik aletlerinden çıkan seslerin kaotik olduğuna dair literatürde araştırmalar bulunmaktadır (Banbrook ve McLaughlin. 1994). Gerçekten de ses sinyalleri ilerideki bölümlerde görülecek kaos ölçme yöntemlerine tabi tutulduğunda kaotik bir yapı sergilediği görülmektedir. Sesin bu özelliğini kullanarak birçok ses analizi, ses sentezleme, ses ve konuşma tanıma gibi uygulamalar geliştirilmiştir. Hatta bu açıdan bakıldığında yapılan çalışmanın da çıkış noktası yine aynı şekilde sesin kaotik özellikler sergilemesi varsayımıdır.



Şekil 3.8. Gerçek bir konuşma ses sinyali parçasının T=10 ve D_E=3 için faz uzayı. Zaman serisinde farklı bölgelerde bulunan üç noktanın faz uzayında yakın bölgelerde bulunarak komşu olması.

Şekil 3.8'de gerçek bir konuşma ses sinyali parçası faz uzayının yeniden oluşturulması görülebilmektedir. Zaman serisinde gözlemlenmesi neredeyse imkânsız benzer dinamiklerin faz uzayında yakın bölgelere düşerek komşu oldukları gözlenebilmektedir.

Daha önceden de bahsedildiği üzere Taken'ın gömme teorisi'ne göre (Takens. 1980) doğru zaman gecikmesi, *T*'nin seçilmesinden başka tüm dinamiklerin faz uzayına aktarılabilmesi için doğru gömme boyutu, D_E seçilmelidir. Doğru gömme boyutunu seçmenin birçok farklı yöntemi vardır. Aslında bu yöntemler de kaos ölçme tekniklerinin temellerini oluşturmaktadır. Bilindiği gibi kaotik sistemlerin sistem boyutu kesirlidir (fraktal). Doğru gömme boyutunu hesaplamak için sistem boyutu hesaplanabilir ve sonrasında kendisine $+\infty$ yönündeki en yakın tamsayıya yuvarlanması ile gömme boyutu belirlenebilir. Ancak sistem boyutunu kesin olarak hesaplayabilmek mümkün olmadığı ve önerilen sistem kesirli boyutu kestirim tekniklerinin çok uzun hesaplama sürelerinde belirli bir hassasiyette tahmin yapabilmesi sebebiyle tercih edilmemektedir. Bunun yerine daha doğrudan ve daha basit bir şekilde uygun gömme boyutu hesaplama tekniği olan *Hatalı Komşular Oranı* (*FNF*-False Neighbours Fraction) tekniği en çok kullanılan yöntem olmuştur (Abarbanel. 1996). Yöntemin temel mantığı, sistemin kesirli boyutunu hesaplamak yerine gömme boyutu, D_E'yi 1'den başlayarak arttırarak ilerlerken, hatalı komşular oranının belirli bir seviyenin altında kaldığı gömme boyutunun, faz uzayının gömme boyutu olarak belirlenmesidir.

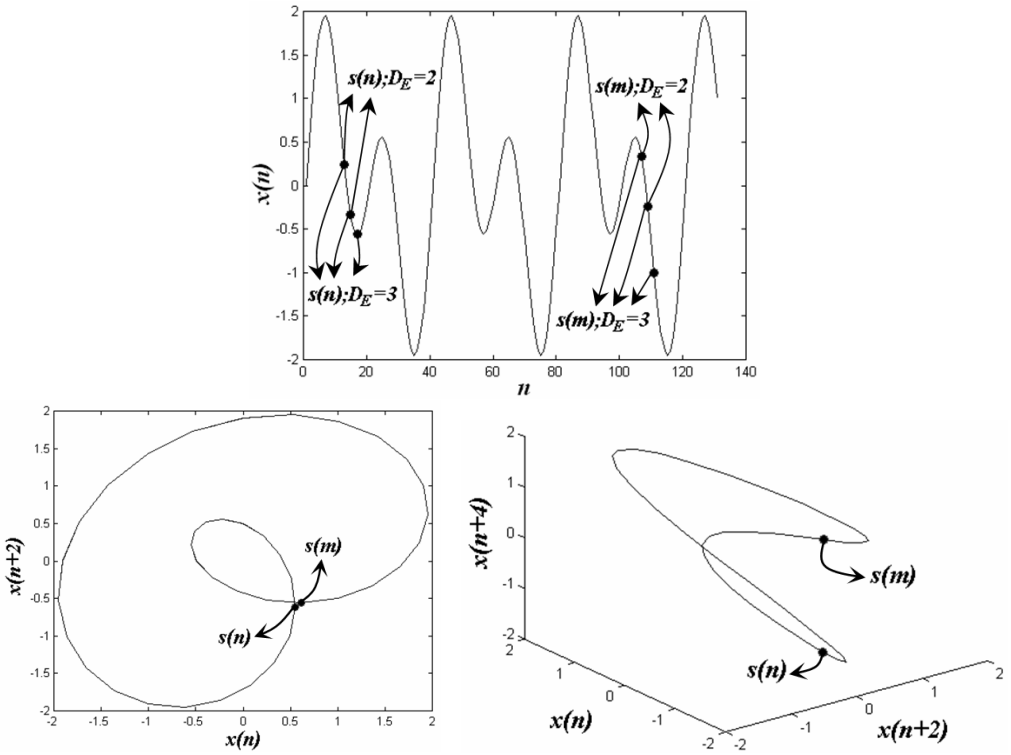
Faz uzayının gömme boyutunu belirlemekte kullanılan *FNF* ve diğer sistem kesirli boyutunu tahmin eden teknikler gibi diğer kaos ölçme teknikleri detaylı olarak bir sonraki bölümde anlatılacaktır.

3.3.2 Kaos ölçme yöntemleri

3.3.2.1 Hatalı komşular oranı yöntemi

Hatalı Komşular Oranı (*FNF*) yöntemi verilen belirli bir faz uzayı boyutu için, *D*, hatalı komşulukların oranını hesaplamaktadır. Bir komşuluğun hatalı veya doğru olarak etiketlenmesinin kriteri, iki komşu nokta, $\mathbf{s}(n)$ ve $\mathbf{s}(m)$, arasındaki öklid mesafesinin, bir fazla faz uzayı boyutunda, $D+1$, komşuluğun devam edip etmemesidir. Komşuluğun bir fazla boyutta da devam etmesi durumunda doğru, etmemesi durumunda ise hatalı

komşuluk olarak etiketlenir. Şekil 3.9'da D_E=2 için hatalı bir komşuluğun etiketlenmesini gösterilmektedir.



Şekil 3.9. İki boyutta komşu olan iki noktanın (**s***(n)* ve **s***(m)*) üç boyutta faklı bölgelerde yer alması sebebiyle hatalı komşuluk olarak atanması

Eğer *D* boyuttaki iki komşu nokta (**s***(n)* ve **s***(m)*) arasındaki mesafe

$$\mathrm{d}_D(\mathbf{s}(n),\mathbf{s}(m)) = \sqrt{\sum_{k=0}^{D-1}(x(n+k.T)-x(m+k.T))^2} \qquad (3.7)$$

D+1 boyuttaki mesafeden

$$\mathrm{d}_{D+1}(\mathbf{s}(n),\mathbf{s}(m)) = \sqrt{(x(n+T.D)-x(m+T.D))^2+\sum_{k=0}^{D-1}(x(n+k.T)-x(m+k.T))^2} \qquad (3.8)$$

belirgin bir şekilde farklı ise, bu iki nokta hatalı komşu olarak etiketlenir (Abarbanel. 1996). Bu iki mesafe (ve ( ) arasındaki fark terimi

, komşuluğun hatalı veya doğru olarak etiketlenmesinde asıl rol oynayan faktördür. Bu durumda hatalı komşuluğun etiketlenmesinde özel bir şart oluşturulabilir;

$$\frac{\mathrm{d}_{D+1}(\mathbf{s}(n),\mathbf{s}(m))}{R_A} < \rho_a \tag{3.9}$$

Burada R_A tüm sinyal üzerinden hesaplanan bir sayısal bir değerdir. Bu değer için kullanılması mantıklı olan uygun değer *x(n)* sinyal dizisinin varyansıdır. ρ_A ise genellikle 1 ile 2 arasında seçilen sabit bir parametredir (Abarbanel. 1996).

Faz uzayındaki tüm komşulukların doğru veya hatalı olarak etiketlenmesi sonrasında hatalı komşuluklar oranı (*FNF*) aşağıdaki gibi hesaplanır;

(3.10)

Uygun faz uzayı gömme boyutu, D_E değerinin seçilmesi için birden fazla faz uzayı boyutu, *D* için *FNF* değerinin hesaplanması gerekmektedir. Üzerinde gürültü bulunmayan temiz bir sinyal için %1'in altında *FNF* değeri veren en küçük faz uzayı boyutu, yeniden oluşturulan faz uzayının gömme boyutu, D_E olarak seçilir. Fakat veri gürültülü ise uygun gömme boyutunu seçmek oldukça güç bir iştir. Fakat eğer gürültünün genliği, δ, biliniyorsa denklem (3.9)'da ki kriteri aşağıdaki gibi güncelleyerek daha uygun bir kriter elde edilmiş olunur.

$$\frac{|x(n+D)-x(m+D)|}{R_A} > \rho_a + 2\delta \tag{3.11}$$

Özetlemek gerekirse, gömme boyutunun, D_E seçimi için aşağıdaki algoritma kullanılmaktadır;

BAŞLA: $D=1$;NFN (Hatalı Komşu Sayısı)=0; ρ_a=1.2; $x(n)$ için R_A'yı hesapla;

ADIM 1: $\mathbf{s}(m)$'i bul // $\mathbf{s}(n)$'in en yakın komşusu

ADIM 2: EĞER $\frac{|x(n+D)-x(m+D)|}{R_A} < \rho_a$

İSE ADIM3'e GİT // $\mathbf{s}(n)$ ve $\mathbf{s}(m)$ gerçek komşular

DEĞİLSE NFN = NFN + 1 // $\mathbf{s}(n)$ ve $\mathbf{s}(m)$ hatalı komşular

ADIM 3: ADIM1 ve ADIM2'yi tüm n'ler için YÜRÜT

ADIM 4: *FNF*'i HESAPLA

EĞER $FNF < 0.01$

İSE $D_E = D$ DUR // Uygun gömme boyutu bulundu.

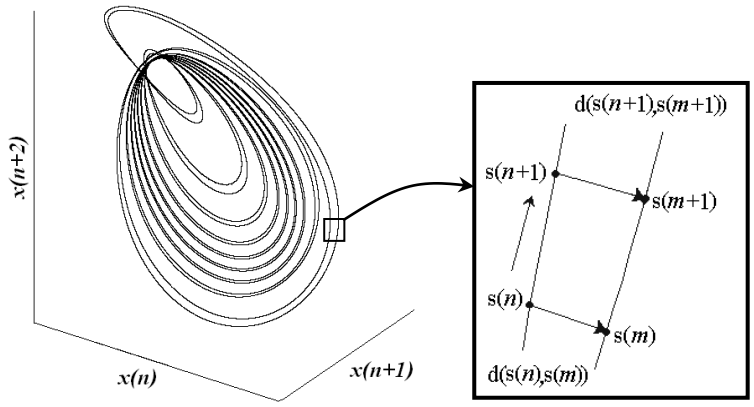
DEĞİLSE

$D=D+1$; NFN = 0; ADIM1'e GİT.

3.3.2.2 Lyapunov üstelleri

Lyapunov Üsteli (Lyapunov Exponent) faz uzayında birbirine yakın seyreden yörüngelerin birbirlerinden ıraksamasını (yakınsamasını) niceliksel olarak ölçen bir yöntemdir. Iraksamanın büyüklüğü faz uzayının farklı eksenleri farklı durumlarda olacaktır. Bu yüzden her bir faz uzayı ekseni farklı bir ortalama Lyapunov üsteli hesaplanmaktadır. Sonuç olarak gömme boyutu, D_E, adedince elimizde Lyapunov üsteli bulunacaktır.

Pozitif bir üstel başlangıçta birbirine yakın iki yörüngenin zaman ile birlikte birbirinden ayrılması (ıraksama) anlamına gelmektedir. Pozitif üstelin büyüklüğü ıraksamanın ne kadar hızlı olduğunun göstergesidir. Benzer şekilde negatif bir üstel başlangıçta uzak olan yörüngelerin birbirine yakınsadığını göstermektedir (yakınsama). Büyük Lyapunov üsteline sahip bir sistem daha fazla tahmin edilemez olmaktadır (Abarbanel. 1996, Hilborn. 2000). Lyapunov üstellerinin hesaplanmasında kullanılan terimler Şekil 3.10'da görülmektedir.



(a) (b)

Şekil 3.10. (a) Sinyalin faz uzayı, (b) iki yörüngenin birbirinden zaman ile ayrılması (ıraksama)

Her bir eksendeki (boyuttaki) Lyapunov üsteli aşağıdaki formül ile hesaplanmaktadır:

$$\lambda = \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \ln \frac{\mathrm{d}(\mathbf{s}(n+1), \mathbf{s}(m+1))}{\mathrm{d}(\mathbf{s}(n), \mathbf{s}(m))} \tag{3.12}$$

Burada $\mathbf{s}(n)$ referans noktası, $\mathbf{s}(m)$ ise $\mathbf{s}(n)$'in en yakın komşusudur.

başlangıçta iki nokta arasındaki mesafe olmak üzere, iki noktanın ayrık zamanda bir adım sonraki durumları, $\mathbf{s}(m+1)$ ve $\mathbf{s}(n+1)$, arasındaki mesafedir. Lyapunov üstelini hesaplarken, her yeni $\mathbf{s}(n)$ noktası için yeni bir $\mathbf{s}(m)$ noktası bulmaktadır (n=1,2,..,N). Her bir eksen için Lyapunov üstelinin hesaplanması sonrasında D_E adet Lyapunov üsteli büyükten küçüğe doğru sıralanır ( ).

λ_1 Lyapunov üsteli, en büyük Lyapunov üsteli olarak bilinir ve kaosun mevcudiyeti pozitif bir en büyük Lyapunov üsteli ile tanımlanmaktadır. Aslında Şekil 3.14'de de görüldüğü üzere, deneme amaçlı Lyapunov üstelleri hesaplanan ses sinyallerinin hepsinin en büyük Lyapunov üsteli pozitiftir. Her bir nokta için Lyapunov üstellerinin hesaplanması sonrasında, sinyale ait Lyapunov üstelleri her bir nokta için hesaplanan değerlerin ortalaması şeklinde hesaplanmaktadır.

3.3.2.3 Vekil veri (Surrogate data)

Zaman serileri fizyolojik, biyolojik, mekanik gibi gerçek yaşamsal sistemlerden elde edilen bilgilerle oluşturulurlar. Bu sinyallerin periyodik, yarı periyodik, kaotik veya rastgele ya da tamamıyla gürültülerden ibaret olup olmadığı yukarıda açıklanan hesaplamalar yapılarak ortaya çıkarılabilir ancak bu zor bir süreçtir. Kaotik bir sistem düşük boyutlu doğrusal olmayan bir sistemdir ve doğrusalsızlığın tespiti kaos için gerekli bir şarttır. Bu nedenle verinin doğrusalsızlığını tespit etmek için çeşitli metotlar geliştirilmiştir. En çok kullanılan metot vekil veri (surrogate data) metodudur (Theiler ve ark. 1992). Bu metot zaman serisindeki doğrusalsızlığı tespit etmek için istatistiksel bir yaklaşıma dayanır. Önce bazı doğrusal işlemler bir hükümsüz hipotez (null hypothesis) olarak belirlenir. Sonra belirlenen bu hükümsüz hipoteze uygun vekil veriler üretilerek, orijinal veri ile vekil veri kümeleri arasında bir istatistik fark hesaplanır. Bu istatistiksel karşılaştırma sonucunda, orijinal veri için hesaplanan değer, vekil verilerden hesaplanan değerlerden önemli derecede farklı ise hükümsüz hipotez reddedilir ve doğrusalsızlık tespit edilir.

Vekil veriler, verilen verinin fazının rastgele veya belli bir düzenle karıştırılmasından oluşturulmaktadır. Böylelikle orijinal veri ile vekil verilerin spektral özellikleri (ortalama değer, varyans değeri, otokorelasyon fonksiyonu, güç spektrumu) birebir aynı olmaktadır. Farklı olan sadece ve sadece faz spektrumlarıdır (Theiler ve ark. 1992).

Bu tezde literatürde en çok kabul gören Schreiber ve Shmidtz tarafından 1996 yılında önerilmiş olan Genlik Ayarlamalı Fourier Transformu (Amplitude Adjusted Fourier Transform-AAFT) yöntemini kullanarak vekil verileri elde edeceğiz. Bu yöntem rastgele bir faz spektrumu oluşturmakta ve bu faz spektrumunun değerlerini orijinal verinin frekans genlik spektrumu ile frekans bölgesinde çarpması ile vekil verinin faz spektrumu elde edilmektedir. Bu açıdan bakıldığında AAFT yöntemi, yukarıda anlatılan vekil veri elde etme yöntemlerinden ilk tipteki yöntemler arasında yer almaktadır.

Vekil verinin oluşturulmasını sağlayan MATLAB kodu Ek-3'de verilmiştir.

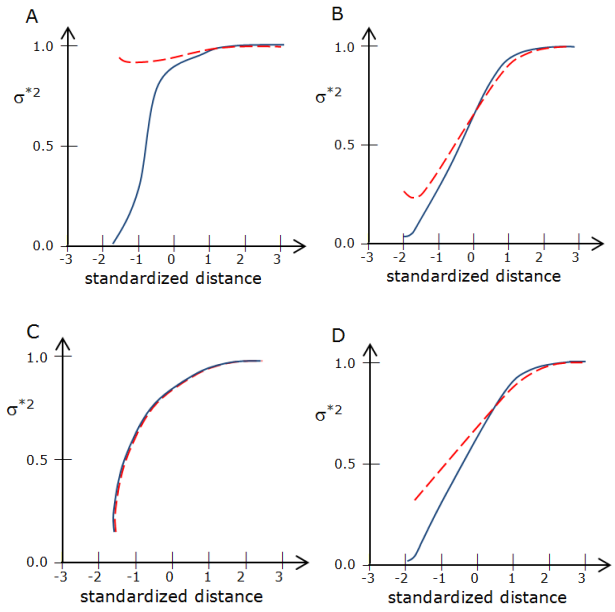
Gecikmeli vektör varyans metodu (DVV-Delay Vector Variance)

Wold ayrıştırma yöntemine göre (Wold. 1938) herhangi ayrık bir sinyal, birbiri ile ilişkili olmayan deterministik ve stokastik bileşenlerine ayrıştırılabilir. Bu yüzden, bir sinyalin deterministik veya stokastik olmasına karar vermek yerine, sinyalde bulunan deterministik bileşen(ler) ile çok yakından ilişkili olan sinyalin tahmin edilebilirliğini ölçmek genellikle daha çok kabul edilen bir yaklaşımdır. Ayrıca sinyalin tahmin edilebilirliği için geliştirilecek her ölçek diğer taraftan sinyalin doğrusallığına karar vermemiz sırasında geçerli bir ölçek olacaktır.

Tezde önerilen steganaliz yönteminde özellik vektörü olarak kullanılacak DVV analiz yöntemi, "hedef varyans", σ^{*2}, üzerine temellendirilmiş olup, belli bir gömme boyutu, D_E, sinyalin tahmin edilebilirliğinin tersidir. $\Omega_n(D_E,r_d)$ seti, $\mathbf{s}(n)$ vektörüne belli bir öklid mesafesi, r_d, dahilinde bulunan komşu -gecikme- vektörlerinin gruplanması ile oluşmaktadır. Burada r_d, tüm gecikmeli vektör çiftleri için aralarında bulunan Öklid mesafesinin dağılımına göre normalize edilir ve ortalama r_d değeri sıfır olarak kabul edilir. Burada $\mathbf{s}(n)$ vektörü, D_E gömme boyutu ve T gecikme süresi için denklem (3.3)'deki gibidir.

Belirlenen bir gömme boyutu için, D_E, Gecikmeli Vektör Varyans (DVV) metodu şöyle özetlenebilir;

- Ortalama, μ_d, ve standart dağılım, σ_d, tüm gecikmeli vektör çiftleri için hesaplanır.
- Kapsama genişliği, r_d, $[\mu_d - n_d\sigma_d; \mu_d + n_d\sigma_d]$ aralığında seçilir. Burada n_d DVV hesaplamasında kapsama genişliğini kontrol etmekte kullanılan bir parametredir. $\Omega_n(D_E,r_d)$ seti $\mathbf{s}(n)$ vektörüne r_d veya daha yakın bulunan tüm vektörleri içermektedir.
- Her $\Omega_n(D_E,r_d)$ seti için varyans değeri hesaplanır. Sonrasında tüm setlerin ortalaması, zaman serisinin varyansına bölünerek, tahmin edilebilirliğin tersi olan parametreye yani "hedef varyans", $\sigma^{*2(D_E,r_d)}$, değerine ulaşılır. Burada hesaplama yapılırken içerisinde en az 30 gecikmeli vektörün bulunduğu setler göz önüne alınır ve ortalamaya katılırlar.



Şekil 3.11. Düz çizgiler Henon-Map (A), Mackey-Glass (B), renkli gürültü (C) ve lazer zaman serileri (D) için DVV-grafiklerini göstermektedir. Aralıklı çizgiler ise aynı zaman serilerinin 99 vekil verisinin ortalama DVV-grafikleridir.

Kapsama genişliği, r_d, normalize edilmesi sayesinde Şekil 3.11'de de görüldüğü üzere grafikleri okumak oldukça kolaylaşmaktadır. DVV-grafikleri r_d'nin fonksiyonu $\sigma^{*2(D_E,r_d)}$değerleri üzerinden çizilmektedir. Sinyallerdeki deterministik bileşenlerin varlığı, DVV-grafiklerinde özellikle küçük r_d değerleri için (0'dan küçük) ortaya çıkmaktadır. Eğer orijinal sinyalin hedef varyansı ile vekil verisinin hedef varyansı yakın değerlerde ise, her iki sinyalin de tahmin edilebilirliği aynıdır denir. Bu durumda Şekil 3.11-C'de görülen renkli gürültüye ait DVV-grafiği göre renkli gürültünün tahmin edilebilirliği oldukça düşüktür. Diğer taraftan Henon-Map verisinin tahmin edilebilirliği oldukça yüksektir (Schreiber ve Schmitz. 2000).

3.3.2.4 Kesirli boyut kestirim metotları

Kaotik sistemlerde gözlemlenen yapı (tezde, faz uzayı içerisindeki konuşma sesi sinyali yapısı) ne faz uzayını dolduran bir sinyal ne de basit bir eğridir. Böyle karmaşık bir geometri, ancak tamsayı olmayan bir sinyal boyutu ile karakterize edilebilinmektedir. Bu durumda sinyalin boyutu kesirli olmaktadır (fraktal) ve bu türdeki yapılara da kesirli (fraktal) yapılar denilmektedir (Abarbanel. 1996, Hilborn. 2000). Literatürde kabul

görmüş ve teoride hepsinin aynı değere yakınsaması gereken kesirli boyut tahmin etme yaklaşımları kısaca şöyle özetlenebilir.

Kaplan-Yorke (Lyapunov) boyutu

Lyapunov veya diğer adıyla Kaplan-Yorke boyutu, D_{KY}, Lyapunov üstellerini kullanarak aşağıdaki gibi hesaplanmaktadır. Burada k. sıradaki Lyapunov üstelidir.

$$D_{KY} = D_E + \frac{1}{\left|\lambda_{D_E+1}\right|}\sum_{k=1}^{D_E}\lambda_k \tag{3.13}$$

Korelasyon boyutu

Korelasyon boyutu her bir (komşu olsun veya olmasın) $\mathbf{s}(m)$ ve $\mathbf{s}(n)$ nokta çiftleri arasındaki mesafeler kullanılarak hesaplanmaktadır. D_E, gömme boyutu ve N ise nokta sayısını temsil etmek üzere $C(r)$, korelasyon fonksiyonu şöyke hesaplanır;

— (3.14)

Burada , $\mathbf{s}(m)$ ve $\mathbf{s}(n)$ nokta çiftleri arasındaki öklid mesafesi olup, r ise D_E, gömme boyutlu hiper-uzayın yarıçapıdır. $\theta(\bullet)$ fonksiyonu ise *Heaviside* step fonksiyonudur;

$$\theta(r - \mathrm{d}_{D_E}(\mathbf{s}(n),\mathbf{s}(m))) = \begin{matrix} 1\,,\ 0 \le\ (r - \mathrm{d}_{D_E}(\mathbf{s}(n),\mathbf{s}(m))) \\ 0\,,\ 0 \ge\ (r - \mathrm{d}_{D_E}(\mathbf{s}(n),\mathbf{s}(m))) \end{matrix} \tag{3.15}$$

Sonuç olarak $C(r)$ korelasyon fonksiyonunu kullanarak D_{corr} korelasyon boyutu şu şekilde hesaplanır;

$$D_{corr} = \lim_{r\to 0}\frac{\log(C(r))}{\log(r)} \tag{3.16}$$

Enformasyon boyutu

Bir sinyale ait faz uzayının, eşit büyüklükte ve bir kenarı ε olan hiper-küpler ile tamamen doldurulduğunu varsayalım. N_i *i.* küp içerisindeki toplam nokta sayısı, N faz uzayı içerisindeki toplam nokta sayısı olmak üzere; bir noktanın *i.* kübün içerisinde bulunma olasılığı; ’dir. Bu durumda enformasyon boyutu, D_I, aşağıdaki formül ile hesaplanmaktadır;

$$D_I = \lim_{\varepsilon \to 0} \frac{-\sum_i p_i \log p_i}{-\log \varepsilon} \tag{3.17}$$

3.3.3 Ses steganalizinde kaotik özelliklerin başarısı

Kaotik Özelliklerin ses steganalizinde kullanılabilmesinin temel mantığı sesin kaotik özellikler göstermesi olduğunu Bölüm 3.3.1 Kaos kuramında bahsedilmişti. Fakat bu varsayımın yanı sıra Steganalizde genel olarak kabul edilen bir diğer varsayım olan örtü sinyaline mesaj gizlemenin sinyal üzerine gürültü eklendiği varsayımıdır (Koçal ve ark. 2008). Bu varsayımı ses sinyallerinin kaotik özelliklerindeki etkisini incelediğimizde kaotik özelliklerin Steganalizde kullanılabilmesi konusunda oldukça cesaret verici çıkarımlar ortaya çıkmaktadır. Bilindiği gibi gürültü eklenmesi ile sinyallerin belli olan sistem boyutu önlenemez bir şekilde artacaktır. Diğer bir deyişle sinyali oluşturan sistemin boyutu d ise, üzerine herhangi bir şekilde gürültü eklenmesi veya orijinal sinyalin bozulması ile bu boyut $d_{gürültülü} \geq d$ olacaktır. İşte bu iki varsayım sayesinde kaotik özelliklerin ses steganalizinde kullanılması fikri ortaya çıkmış, gelecek bölümlerde de görüleceği üzere fikrin doğruluğu kanıtlanmıştır.

3.3.3.1 Hatalı komşular oranının ses steganalizinde kullanılması

ve (eşitlik (3.7)ve (3.8)) arasındaki fark terimi ’dir. Bu fark terimi aslında komşuluk çiftinin doğru veya hatalı olmasında asıl etkili olan terimdir. Bir sinyal içerisine veri gizleme işleminin, sinyale rasgele bir gürültü eklenmesine karşılık geldiği varsayımını kullanarak Δ teriminin örtü ve stego sinyalleri *FNF* değerlerinin nasıl değiştiği, dolayısıyla *FNF* değerlerinin steganalizde kullanılabilirliğinin teorik altyapısı çalışmamızın bu kısmında

açıklanacaktır. örtü sinyalinin kendisini, ise stego sinyali versiyonunu temsil etmek üzere, Δ fark terimi, örtü (Δ_C) ve stego sinyali (Δ_S) için sırasıyla eşitlik (3.18) ve (3.19)'daki gibi olur. Burada bağımsız özdeşçe dağılmış (independent identicaly distributed-*i.i.d.*) sıfır ortalamalı ve varyansa sahip beyaz gürültüdür.

$$\Delta_C = (x(n+D) - x(m+D))^2 \tag{3.18}$$

$$\Delta_S = (x(n+D) + \varepsilon(n+D) - x(m+D) - \varepsilon(m+D))^2 \tag{3.19}$$

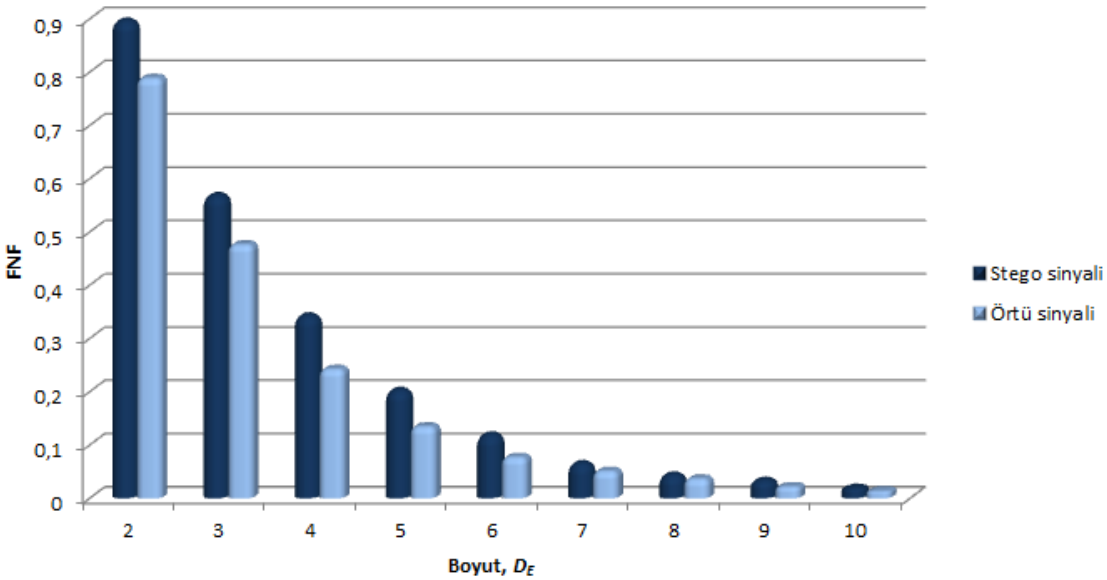
Δ_s teriminin beklenen değeri eşitlik (3.20)'deki gibi hesaplanabilir. Bu değer bizim gelecek işlemlerimiz için gerekli olacaktır.

$$\begin{aligned} E[\Delta_S] = {} & [x(n+D) - x(m+D)]^2 - 2[x(n+D) - x(m+D)]E[\varepsilon(n+D) \\ & - \varepsilon(m+D)] + E[\varepsilon(n+D)^2] + E[\varepsilon(m+D)^2] - 2E[\varepsilon(n+D)\varepsilon(m+D)] \end{aligned} \tag{3.20}$$

ve değerlerinin istatistiksel olarak bağımsız özdeşçe dağılmış olmaları ve sıfır ortalama, varyansa sahip olmaları sebebiyle, eşitlik (3.18)'deki Δ_c terimini de kullanmamız durumunda, eşitlik (3.20), şeklinde sadeleşecektir. Örtü sinyalleri ve stego sinyalleri versiyonlarının *FNF* değerlerine baktığımızda her zaman için stego sinyallerinin daha büyük olduğunu görmekteyiz (Şekil 3.13 ve Şekil 3.12). Aslında yapılan detaylı incelemelerde gizlenen verinin büyüklüğünün arttıkça stego sinyallere ait *FNF* değerlerinin de arttığını görebilmekteyiz. Teorik olarak gizlenen veri büyüdükçe, değeri de artmaktadır. Burada eğer ve değerleri istatistiksel olarak bağımsız özdeşçe dağılmış değilse terimi, değeri 'in inci korelasyon katsayısı olmak üzere, olacaktır. Bu durumda *FNF* değerleri steganalizde çok daha az ayırt edici olacaktır (Koçal ve ark. 2008).

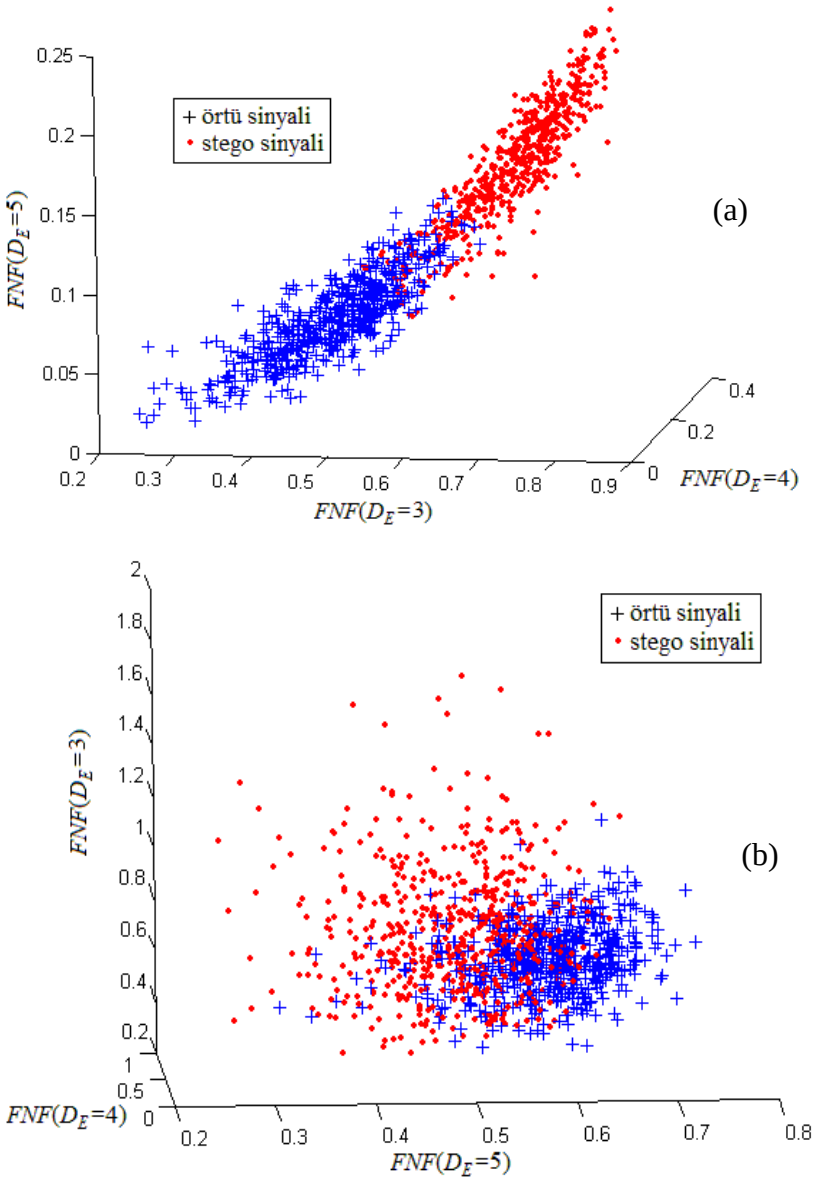
Şekil 3.12, örtü sinyalleri ve stokastik modülasyon (Fridrich ve Goljan. 2003) tekniği ile veri gizlenmiş stego sinyallerinin *FNF* değerleri için bir örnek görülmektedir. Şekilde kolaylıkla görüldüğü üzere stego sinyallerinin *FNF* değerleri her gömme boyutu için

örtü sinyallerine göre daha büyüktür. Bu durumda diyebiliriz ki, veri saklama işlemi örtü sinyalinin gömme boyutunu dolayısıyla sinyal boyutunu (bağımsızlık derecesi) arttırmaktadır. Bu örnek için gizlenen verinin büyüklüğünü dolayısı ile örtü sinyaline eklenen gürültünün genliğini bilinmesine rağmen bu bilgi *FNF* değerlerinin hesaplanmasında (eşitlik (3.11)) kullanılmamıştır. Eğer bu şekle bakarak yeniden faz uzayının inşası için doğru bir gömme boyutu seçilmek istenirse, *FNF* değerinin belli bir değere yakınsamaya başladığı ilk değer gömme boyutu, D_E, olarak seçilmelidir. Yakınsamaya başlanan bu *FNF* değeri tamamen *SNR* (Signal-to-Noise Ratio) değeri ile ilgili olup, gürültü sebebiyle daha önceden bahsetmiş olduğumuz 0.01 değerinin altına düşmek ancak çok yüksek gömme boyutları için mümkün olacaktır. Bu durumda örtü sinyali için D_E=8, stego sinyali için D_E=9 seçmek oldukça mantıklı olacaktır. Burada tez çalışmamızda *FNF* değerlerini gömme boyutunu belirlemek için kullanmadığımızı, bu değerleri direkt olarak önerilen steganalizör için özellik vektöründe kullanıldığını belirtmekte fayda görülmektedir. Tez çalışmasında belli bir gömme boyutundan, belli bir gömme boyutuna kadar hesaplanmış ve bu değerler özellik vektöründe kullanılmıştır (Koçal ve ark. 2008).



Şekil 3.12. Örtü ve Stego sinyaller için *FNF* değerleri (Stokastik Modülasyon)

Örtü ve stego sinyallerinin *FNF* değerleri arasındaki fark Şekil 3.13'de açık bir şekilde görülebilmektedir. Şekilde üç farklı gömme boyutu için (D_E=3,4,5), 2000 adet örtü sinyali ve bu sinyallerin iki popüler steganografi yöntemi DSSS (Direct Sequence Spread Spectrum) (Bender ve ark. 1996) ve Stokastik Modülasyon (Fridrich ve Goljan. 2003) için 2000 adet stego sinyal versiyonlarının durum uzayında ayrışması görülebilmektedir. Sınıflandırma işlemi için oldukça kolaylık sağlanacak bu ayrışma *FNF* değerlerinin ses steganalizinde kullanılabilmesi konusunda umut vaat etmektedir.



Şekil 3.13. Üç farklı boyut için (D_E=3,4,5) DSSS (a) ve Stokastik Modülasyon (b) yöntemleri ile steganografi işlemi yapılmış 2000 adet örtü ve stego sinyallerinin *FNF* değerleri. SWR değeri DSSS için 38dBve Stokastik Modülasyon için 40dB'dir.

3.3.3.2 Lyapunov üstellerinin ses steganalizinde kullanılması

mesafesi yalnızca tüm faz uzayının büyüklüğü ile etkilenmekte ve sinyaldeki bozulma (distorsiyon) ile faz uzayının genel şeklinin değişmemektedir. Faz uzayının ortalama mesafesi bu durumda hem örtü, hem de stego sinyalleri faz uzayları için yaklaşık olarak aynı olacaktır. Çünkü referans noktası olan , veri gizleme ile oluşan distorsiyonun etkisi ile en yakın komşusundan uzak bir noktaya düşmesi durumunda kendisine yeni bir en yakın komşu bulacaktır. Yani mesafesi distorsiyon ile büyük değişiklikler göstermeyecektir. Fakat her iki noktanın yörüngelerindeki bir sonraki noktalarının arasındaki mesafe olan mesafesinin distorsiyondan doğan bozulmayı kompanze edebilecek herhangi bir şansı bulunmamaktadır. Bu durumda distorsiyondan oluşan bozulmanın etkileri daha çok mesafesi üzerinde görülmektedir (Koçal ve ark. 2008).

Örtü sinyali faz uzayında D_E gömme boyutu için bu mesafe;

$$\mathrm{d}(\mathbf{s}(n+1),\mathbf{s}(m+1))_C = \sqrt{\sum_{k=0}^{D_E-1}(x(n+k+1)-x(m+k+1))^2} \tag{3.21}$$

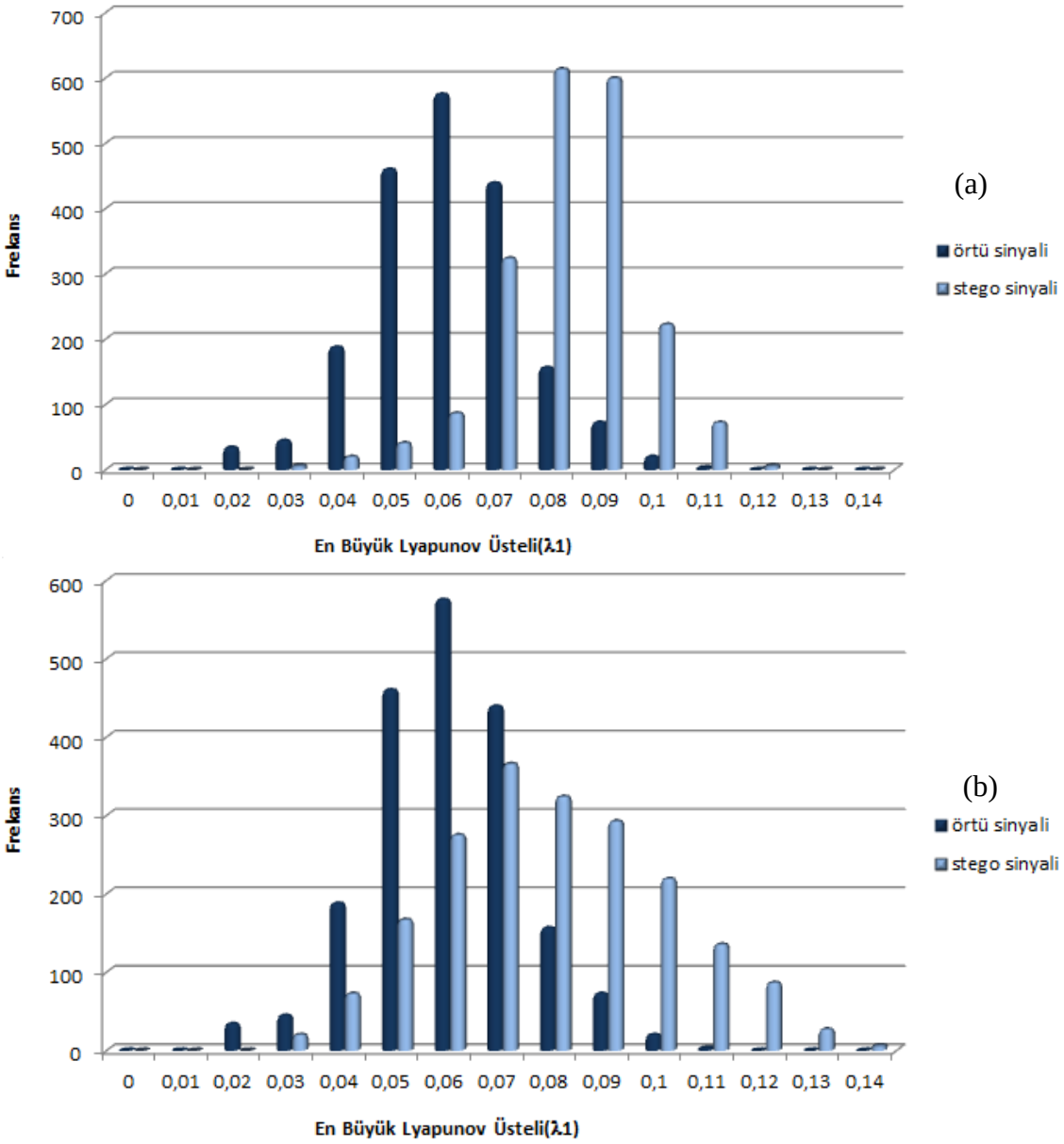
olacaktır. Aynı mesafe, aynı gömme boyutundaki stego sinyal faz uzayı için;

$$\mathrm{d}(\mathbf{s}(n+1),\mathbf{s}(m+1))_S = \sqrt{\sum_{k=0}^{D_E-1}(x(n+k+1)+\varepsilon(n+k+1)-x(m+k+1)-\varepsilon(m+k+1))^2} \tag{3.22}$$

olacaktır. değerinin beklenen değeri şu şekilde elde edilir;

$$E[\mathrm{d}(\mathbf{s}(n+1),\mathbf{s}(m+1))_S{}^2] = \mathrm{d}(\mathbf{s}(n+1),\mathbf{s}(m+1))_C{}^2 + 2\sigma^2 D_E \tag{3.23}$$

Eşitlik (3.23)'den görüldüğü üzere, örtü sinyallerine ait Lyapunov üstelleri stego sinyaller için hesaplananlardan daha küçük olacaktır. Bu durumda stego sinyaller için örtü sinyallerine göre daha az tahmin edilebilir denilebilmektedir (Koçal ve ark. 2008).



Şekil 3.14. DSSS (a) ve Stokastik Modülasyon (b) ile veri saklanmış 2000 adet örtü ve stego sinyaline ait D_E=7 için en büyük Lyapunov üstellerinin, λ_1, histogramları.

Şekil 3.14'de, D_E=7 için, 2000 adet ses örtü sinyalinin ve bu sinyallere ait DSSS ve Stokastik Modülasyon veri gizleme teknikleri ile oluşturulmuş stego sinyal versiyonlarına ait en büyük Lyapunov üstellerinin, λ_1, dağılımı görülmektedir. Bu

şekilden de görüldüğü üzere, stego sinyallere ait en büyük Lyapunov üstelleri neredeyse her zaman örtü sinyallerine ait en büyük Lyapunov üstellerinden daha büyüktür. Ayrıca her iki Lyapunov üstelleri dağılımının birbirlerinden farklı olduğu yine aynı şekilde görülebilmektedir. Bu durum *FNF* değerleri gibi Lyapunov üstellerinin de ses steganalizinde ayırt edici özellikler olarak kullanılabileceğini göstermektedir (Koçal ve ark. 2008)

3.3.3.3 DVV yönteminin ses steganalizinde kullanılması

Bölüm 3.3.2.3'de anlatıldığı üzere, DVV grafiklerine bakılarak orijinal sinyalin nonlineerliği konusunda fikir yürütülebilmekteydi. Fakat bu durumu sübjektif bir yaklaşımdan objektif (bakış açısına göre değişmeyen) bir yöntem ile değerlendirmek gerekmektedir. Bu sebeple sayısal değer üreten aşağıda anlatılan yöntem tanımlanmıştır (Schreiber ve Schmitz. 2000);

1. Öncelikle kaç adet vekil verisinin oluşturulacağı seçilmelidir. Bu değer, *n_surr*, az olursa yapılan değerlendirme anlamsız olabilmekte, gerektiğinden fazla olursa ise yeterinden daha fazla süre sürecek analiz çalışmaları ve bilgisayar hesaplamaları anlamına gelecektir. Bu değerin alt sınırı anlamlılık seviyesi, (genelde 0.05 seçilir), olmak üzere

– (3.24)

olmalıdır.

2. Seçilen vekil veri sayısı adedince, orijinal verinin vekil verisi oluşturulur, $\mathbf{s}_1$, $\mathbf{s}_2$,… $\mathbf{s}_{n\_surr}$,

3. Orijinal verinin ve vekil verilerin, DVV eğrisi oluşturulur.

4. Vekil verilerin DVV eğrisi ile orijinal verinin arasındaki fark *RMSE (Hatanın Karesel Ortalaması-Root Mean Square Error)* cinsinden hesaplanır, $RMSE_1$, $RMSE_2$,..., $RMSE_{n\_surr}$.

5. Vekil veri adedince elde edilen *RMSE* değeri üzerinden ortalama, varyans, çarpıklık (skewness) ve basıklık (kurtosis) (1., 2., 3. ve 4. merkez moment değerleri) hesaplanarak, steganalizör için özellik vektörü oluşturulur;

; (3.25)

ölüm 3.3.2.3 Vekil veri (Surrogate data) kısmında bahsedilen *n.* sinyale ait $\Omega_n(D_E,r_d)$ seti; D_E gömme boyutu, r_d ise komşuluk yarıçapı olmak üzere Ω_n olarak kısaca belirtilebilir. Ω_n vektör seti şöyle ifade edilebilir;

; *m=1,2,..N* (3.26)

Burada *N* zaman serisinde bulunan örnek sayısıdır. Ω_n setindeki gecikmeli vektör komşulukları arasındaki mesafelerin karesi;

$$\mathrm{d}(x(n), x(m))^2 = \|x(m) - x(n)\|^2 = \sum_{k=1}^{D_E} (x(n+k) - x(m+k))^2 \quad (3.27)$$

olacaktır. Ω_n setindeki ortalama, μ_d ve varyans, değerleri ise;

$$\mu_d \quad (3.28)$$

olacaktır. Bu eşitlikleri ve veri gizlemenin sinyale $\varepsilon(k)$ genliğinde sıfır ortalamalı ve varyanslı beyaz gürültü eklenmesi anlamına geldiği varsayımını kullanarak eşitlik (3.27)'yi sırasıyla örtü ve stego sinyaller için tekrar düzenlersek;

$$\mathrm{d}_C(x(n), x(m))^2 = \mathrm{d}_C{}^2 = \sum_{k=1}^{D_E} (x(n+k) - x(m+k))^2 \quad (3.29)$$

$$\mathrm{d}_S(x(n), x(m))^2 = \mathrm{d}_S{}^2 = \sum_{k=1}^{D_E} \left([x(n+k) + \varepsilon(n+k)] - [x(m+k) + \varepsilon(m+k)]\right)^2 \quad (3.30)$$

Stego sinyaller için kullanılan $\mathrm{d}_S{}^2$ terimini açarsak;

$$d_S^2 = \sum_{k=1}^{D_E} x^2(n+k) + 2x(n+k)\varepsilon(n+k) + \varepsilon^2(n+k) + x^2(m+k) + 2x(m+k)\varepsilon(m+k) \quad (3.31)$$
$$+ \varepsilon^2(m+k) - 2\left[x(n+k)x(m+k) + x(n+k)\varepsilon(m+k) + \varepsilon(n+k)x(m+k) + \varepsilon(n+k)\varepsilon(m+k)\right]$$

Bu terimde $d_C^2 = \sum_{k=1}^{D_E} x^2(n+k) + 2x(n+k)x(m+k) + x^2(m+k)$ terimini yerine koyarsak;

$$d_S^2 = d_C^2 + \sum_{k=1}^{D_E} 2x(n+k)\varepsilon(n+k) + \varepsilon^2(n+k) + 2x(m+k)\varepsilon(m+k) + \varepsilon^2(m+k) \quad (3.32)$$
$$- 2\left[x(n+k)\varepsilon(m+k) + \varepsilon(n+k)x(m+k) + \varepsilon(n+k)\varepsilon(m+k)\right]$$

olacaktır. , , , ve çiftlerinin bağımsız özdeşçe dağılmış (independent identically distributed) olmaları sebebiyle, stego sinyale ait eşitlik(3.32)'de verilen terimin ortalama değeri sade bir yolla şu şekilde hesaplanabilir;

(3.33)

ε(k)'nın sıfır ortalamalı ve varyanslı beyaz gürültü olması sebebiyle;

(3.34)

olacaktır. DVV analizinde kullanılan ve eşitlik (3.28)'de görülen varyans değeri örtü ve stego sinyalleri için şöyle ifade edilebilir;

(3.35)

(3.36)

Eşitlik (3.34) kullanılırsa terimi şu şekilde olacaktır;

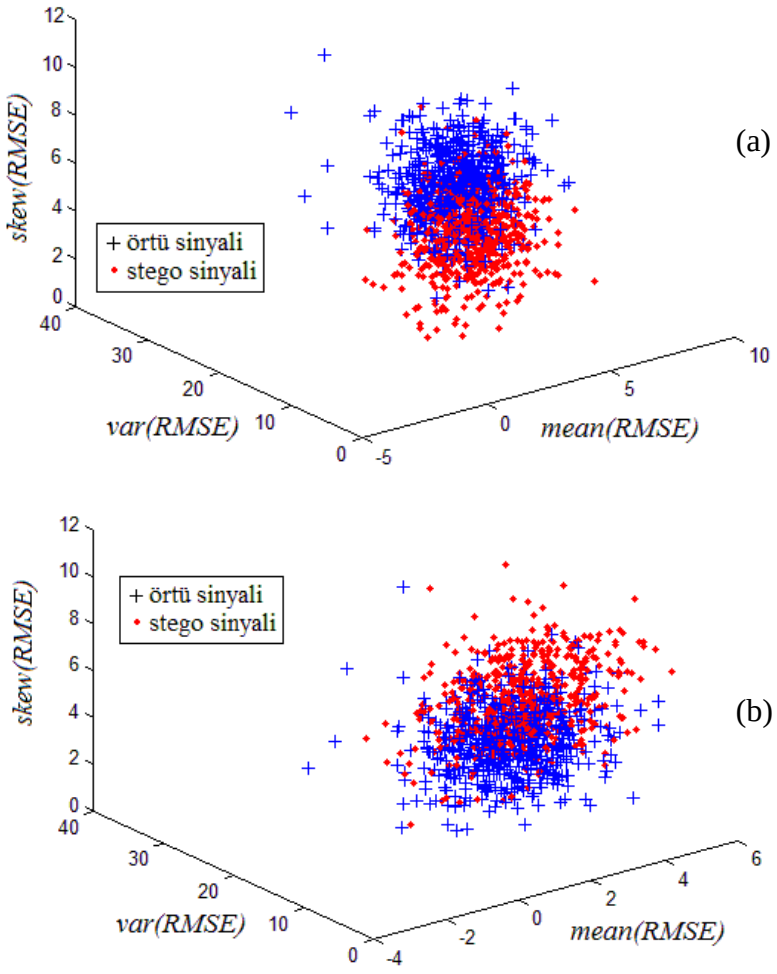
+ (3.37)

yaklaşık eşitliğini kullanırsak;

(3.38)

olacaktır. Bu durumda DVV analizinde kullanılan stego sinyaline ait varyans değeri her zaman için örtü sinyaline ait varyans değerinden büyük olacaktır.

Önerilen $\mathbf{F}_{surr}$ özellik vektörünün ilk üç elemanının, DSSS ve stokastik modülasyon teknikleri ile veri gizlenmiş 2000 adet stego sinyali ve bu sinyallerin orijinal versiyonu olan örtü sinyalleri için hesaplanmış değerlerini Şekil 3.15'de görebilmekteyiz. Burada vekil veri sayısı, n_{surr}=20 olarak seçilmiştir. Şekilden de görüldüğü üzere, örtü ve stego sinyalleri *FNN* ve Lyapunov üstelleri kadar olmasa bile yine de belli bir farkla ayrışmaktadır.

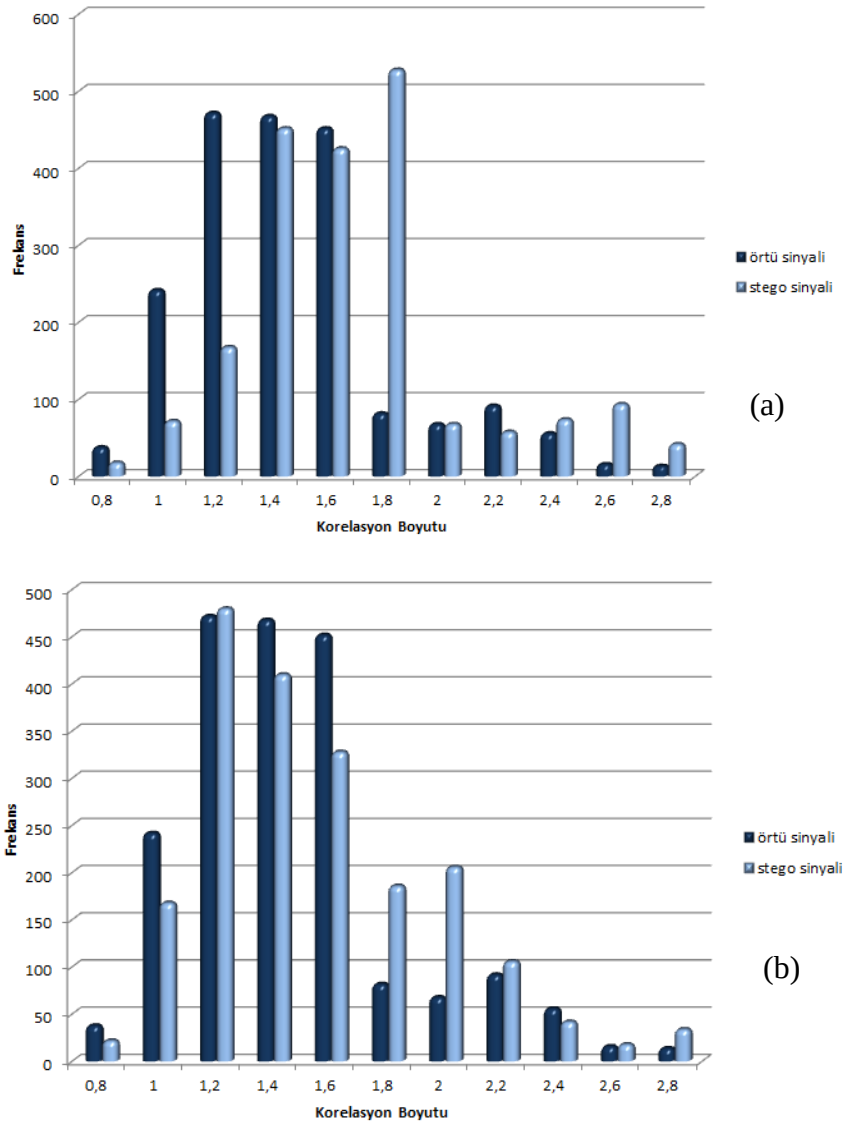


Şekil 3.15. DSSS (a) ve Stokastik Modülasyon (b) ile veri saklanmış 2000 adet örtü ve stego sinyalinin, n_{surr}=20 için F_{surr} özellik vektörünün ilk 3 elemanı değerleri

3.3.3.4 Kesirli boyut kestirim metotlarının ses steganalizinde kullanılması

Bölüm 3.3.2.4'de belirtildiği üzere bir sinyalin kaotik olup olmadığı ve kaotikliğinin derecesini ölçmek için literatürde birden fazla kesirli boyut kestirim yöntemleri önerilmiştir (Abarbanel. 1996, Hilborn. 2000). Bu yöntemler arasında korelasyon boyutu en göze çarpan ve literatürde en çok kullanılan yöntemdir (Pitsikalis ve Maragos. 2002). Literatürde önerilen farklı yaklaşımlar arasında en doğru tahmin sonuçlarını veren korelasyon boyutu tahmin değerleri örtü ve stego sinyaller için Şekil 3.16'de görülmektedir. Şekilde de görüldüğü üzere, örtü ve stego sinyaller için korelasyon boyutu değerleri büyük farklar oluşturmamaktadır. Bu durumun altında

yatan asıl sebep boyut tahmini yapan yaklaşımların gürültüyü otomatik olarak süzmeleridir. Kestirim algoritması ile birlikte gelen bu gürültü filtreleme algoritması ana algoritmadan ayrıştırılamamaktadır. Bu durum kesirli boyut kestirim metotlarının ses steganalizinde kullanımı için uygun olmadığı varsayımını doğurmaktadır. Tezin gelecek bölümünde, Bölüm "3.3.2 Kaos ölçme yöntemleri"nde anlatılan tüm yöntemler ses steganalizinde önerilecek ve sayısal değerler ile her bir yöntemin başarım sonuçları verilecektir. Tezin bu kısmında elde edilecek sayısal değerler ile diğer kaos ölçme yöntemleri ile birlikte kesirli boyut tahmin yöntemlerinin de başarımı karşılaştırmalı olarak incelenebilecektir.



Şekil 3.16. DSSS (a) ve Stokastik Modülasyon (b) teknikleri ile veri gizlenmiş 2000 adet örtü ve stego ses sinyallerinin korelasyon boyutu (D_{corr}) değerleri histogramı.

4. BULGULAR VE TARTIŞMA

Tezin bu kısmında bir önceki bölümde ses steganalizörü olarak kullanıldığında başarılı olma olasılığı yüksek olan kaotik özelliklerin performansları farklı veri setleri ve koşullar için irdelenecektir. Evrensel steganalizör olarak önerilen kaotik özellikler konuşma, müzik ve enstrümantal (sözsüz) sesler için denenmiş ve farklı ses kaynakları için farklı özelliklerin çok daha uygun sonuçlar verdiği anlaşılmıştır. Bu bölümde öncelikle benzetim şartları ortaya konularak, literatürde önerilen diğer ses steganalizörleri ile doğru bir karşılaştırma ortamının sağlanması garanti edilmiştir. Sonrasında ortaya konan benzetim şartları ile gerçekleştirilen performans testlerinin sonuçları paylaşılarak literatürdeki diğer ses steganalizörleri ile karşılaştırmaları gerçekleştirilmiştir. Doğru karşılaştırma altyapısının oluşturulması amacıyla, Çizelge 3.1'de verilen Steganografi için farklı saldırı yaklaşımlarından "Seçili stego saldırısı", yani steganografi yönteminin bilindiği ve elimizde yalnızca stego sinyalin bulunduğu yaklaşım benimsenmiştir.

4.1 Benzetim Şartlarının Oluşturulması

Önerilen ses steganalizörü performans sonuçlarının literatür ve benzer çalışma çevrelerinde kabul görebilmesi ve çalışmayı yapanın da önerdiği steganalizör özelliklerinin performansını doğru bir şekilde ölçebilmesi için doğru şartlarda performans testlerini gerçekleştirmesi gerekmektedir. Bu kapsamda doğru veri setleri, doğru veri saklama oranları ve doğru steganografi yöntemleri için önerilen özellikler test edilmelidir. Bu bölümde adım adım benzetim şartlarının oluşturulması anlatılacaktır.

4.1.1 Veri setinin oluşturulması

Yapılan tezde konuşma sesleri, müzik sesleri (şarkı) ve enstrümantal müzik sesleri için performans testleri yapılmıştır. Konuşma sesleri için iki farklı veri seti kullanılmıştır. Bunlardan ilki; her biri 3-4 saniye süreli erkeklerin konuştuğu 200 adet farklı ses parçasından oluşmuştur. Bu veri setinde kayıtların hepsi 16 kHz frekansında ve akustik

olarak korunmalı ortamda kaydedilmiştir. İkinci veri seti ise literatürde otomatik konuşma ve/veya konuşmacı tanıma algoritmalarının değerlendirilmesinde geniş kullanım olanağı bulan TIMIT (TIMIT. 2006) veri seti içerisinden hiçbir şart gözetilmeden tamamen rastgele seçilmiş 2000 adet konuşma sesinden oluşan bir alt kümesidir. TIMIT veri seti, 16 kHz frekansında kaydedilmiş, 630 farklı erkek ve kadın konuşmacı tarafından 8 ana Amerikan lehçesini temsil eden 6300 konuşma kaydından oluşmuştur.

Müzik (şarkı) veri seti ise popüler şarkıların resmi müzik kayıtlarından oluşmuştur. Bu set, U2 grubunun "One" ve "Even Better Than The Real Thing", Rolling Stones grubunun "Paint It, Black", Roger Sanchez'in Rap tarzında ve sürekli ritmik müzik ve konuşmalardan oluşan "Again" ve Londra Filarmoni Orkestrası tarafından çalınmış Korsakov bestesi "Şehrazat"ın kayıtlarının 44.1 kHz'den 16 kHz'e aşağı örneklenmesi ve 4 saniyelik parçalar bölünmesi ile oluşturulmuştur. Aşağıdaki tabloda her bir kayıt için toplam ses kaydı sayısı görülmektedir.

Çizelge 4.1. Müzik Veri Setlerindeki Kayıt Sayıları

Veri Seti	**Kayıt Sayısı**
Şehrazat (Klasik Müzik)	52
U2 "One"	52
U2 "Even Better"	44
Rolling Stones	44
Again (Rap Müzik)	92
TOPLAM	**284**

Müzik enstrümanları veri seti için MIT'nin (Massachusetts Institute of Technology) SQAM (SQAM. 2006) adı altında yayınladığı ses kayıtları kullanılmıştır. Bu set yine müzik sinyalleri veri seti gibi 44.1 kHz'den 16 kHz'e aşağı örneklenmesi ve 4 saniyelik parçalar bölünmesi ile oluşmuş çeşitli müzik enstrümanların 70 adet ses verisi parçasından oluşmuştur.

4.1.2 Ses steganalizinde kullanılmak üzere kaotik özelliklerden oluşan yeni bir özellik vektörü

Ses steganalizörü için önerilen özellik vektöründe yer alan Hatalı Komşular Oranı (*FNF*) ve Lyapunov üstelleri yöntemleri ile ilgili hesaplamalar Hegger ve arkadaşlarının 1999 yılında yayınlamış olduğu TISEAN (TIme SEries ANalysis) adındaki paket programın yardımıyla hesaplanmışlartır. Vekil veriler ile ilgili hesaplamalar ise Schreiber ve Schmitz tarafından 2000 yılında yayınlanmış olan çalışmanın ışığında gerçekleştirilen MATLAB kodları yardımıyla hesaplanmıştır. *FNF* değerlerinin hesaplanması ile *FNF* değerlerini kullanan aşağıdaki özellik vektörü önerilmiştir:

(4.1)

Her bir vektörü üç elemandan oluşmaktadır; Hatalı komşular oranı, ortalama en yakın komşuların mesafesi ve en yakın komşular mesafesinin *RMS* değeri.

Eşitlik (4.1)'de ki *FNF* özelliklerini içeren vektör, =7 için hesaplanan Lyapunov üstelleri ve eşitlik (3.25)'de önerilen vekil verilerden elde edilen *RMSE* değerleri yardımı ile oluşturulan özelliklerin tümünü içeren 26 elemanlı özellik vektörü aşağıdaki gibidir.

∪ ∪ (4.2)

Yapılan tez çalışmasındaki tüm vekil veri özellik vektörleri (eşitlik (3.25)) n_{surr}=20 adet vekil verinin kullanılmasıyla hesaplanmıştır.

Önerilen özellik vektörünün (eşitlik (4.2)) ilk 15 elemanı *FNF* oranı yardımıyla, ikinci 7 elemanı Lyapunov üstellerinin yardımıyla, kalan 4 eleman ise vekil veriler yardımıyla elde edilen değerlerden oluşmuştur.

Tezde Bölüm 3.3.2.4 Kesirli boyut kestirim metotlarında anlatılan kesirli boyut kestirim metotlarından alınan değerler önerilen özellik vektörü içerisine dâhil edilmemiştir. Bunun nedeni bu yöntemlerden elde edilen özelliklerin ses steganalizinde olumlu bir etkisinin bulunmamasıdır. Bu durumun kanıtı olarak kaotik özelliklerin tamamında

yapılan Varyans Analizi (*ANOVA*-ANalysis Of VAriance) sonuçlarıdır. Bu analiz sonrasında ses steganalizi için ayırt edici olmayan özellikler önerilen özellik vektörü içerisinde yer almamıştır. Genel olarak *ANOVA* analizi sonucunda 0.05 değerinden daha düşük *p* değerleri, iki kümenin farklı ortalamalara ve dağılımlara sahip olduğunu dolayısıyla ayırt edici özellikler oldukları kabul edilmektedir (Avcibas. 2006, Koçal ve ark. 2008). Çizelge 4.2'de tüm steganografi metotları için, =3 ve =4 gömme boyutları için *FNF* değerleri, en büyük Lyapunov üsteli, vekil veriler için hesaplanan *RMSE* değerlerinin ortalaması, Enformasyon Boyutu, Korelasyon Boyutu ve Kaplan-Yorke Boyutu için *ANOVA* analizi sonrasında elde edilen *p* değerleri görülmektedir. Bu tablodan da görüldüğü üzere Enformasyon Boyutu, Korelasyon Boyutu ve Kaplan-Yorke Boyutu'nun *p* değerleri 0.05 değerinin oldukça üstündedir. Diğer metotlar için oluşturulan özellik vektörlerinden alınan örnek değerler için ise *p* değerleri 0.05 değerinin altında kalmakta, dolayısıyla bu tekniklerin ses steganalizinde ayırt edici bir özellik olarak kullanılabilirliği anlaşılmaktadır (Rencher. 1995).

Çizelge 4.2. Kaotik Özelliklerin ayırt edici gücünü gösteren istatistiksel *ANOVA* analizi sonucunda elde edilen *p* değerleri ($p \leq 0.05 \Rightarrow$ ayırt edici özellik).

Method	***FNF*** ***(D_E=3)***	***FNF*** ***(D_E=4)***	λ_1	***mean(RMSE)*** ***n_{surr}=20***	D_I	D_{KY}	D_{CORR}
COX	0,0882	0,0921	0,1128	0,1866	0,4821	0,3598	0,4584
DSSS	**0,0000**	**0,0000**	**0,0012**	**0,0019**	**0,0023**	**0,0001**	**0,0003**
FHSS	**0,0000**	**0,0000**	**0,0023**	**0,0106**	**0,0433**	**0,0373**	**0,0314**
ECHO	**0,0241**	**0,0283**	0,1432	0,1526	0,2183	0,2502	0,1871
STEGANOS	**0,0238**	**0,0328**	**0,0030**	**0,0632**	0,3492	0,2893	0,2860
HIDE4PGP	**0,0000**	**0,0001**	0,0623	0,1165	0,2493	0,2702	0,3218
STEGHIDE	**0,0043**	**0,0101**	0,0891	0,1328	0,2849	0,2684	0,3511
STOMOD	**0,0468**	**0,0327**	**0,0021**	**0,0054**	0,2983	0,2792	0,2128
MP3	**0,0016**	**0,0347**	0,1437	0,0872	0,4122	0,3509	0,4532

Bu çizelgedeki steganografi tekniklerinin ilk üç tanesi (*COX*, *DSSS* ve *FHSS*), sudamgalama tekniği olması sebebiyle, gizlenen verinin alıcılar tarafından tespit edilmesinin önemi yoktur. Dolayısıyla sudamgalama tekniklerinin algoritmalarının geliştirilmesine böyle bir amaç güdülmediği için steganalizde bu teknikler için, örtü ve stego sinyalin kolaylıkla ayırt edilmesi, diğer bir deyişle yüksek performans değerleri beklenen bir durumdur. Fakat bunun tersine diğer altı steganografi tekniğinde gizlenen verinin tespit edilememesi istenmekte, dolayısıyla bu tekniklere ait algoritmalar bu yönde geliştirilmiştir. Bu durumda bu teknikler için örtü ve stego sinyallerin ayırt edilmesi zorlayıcı olmalı, sudamgalama tekniklerine göre daha düşük performans değerleri beklenmelidir.

4.1.3 Steganalizörün tasarımı

Ses steganalizinde kullanılmak üzere kaotik özelliklerden oluşmuş önerilen yeni özellik vektörünün başarımını test etmek üzere bir nonlineer sınıflandırıcı olan *SVM* (Destek Vektör Makinesi - Support Vector Machine) sınıflandırıcı yardımı ile performans testleri gerçekleştirilmiştir. Bu kapsamda Ohio-State Üniversitesi'nin geliştirmiş olduğu MATLAB için *SVM* paketi kullanılmıştır(OSU-SVM Matlab Toolbox. 2011). Kullanılan *SVM* sınıflandırıcıda radyal tabanlı fonksiyon, Gamma=4.0 değeri ile kullanılmıştır. Yapılan tezde, literatürde daha önceden yapılmış bulunan bazı çalışmalar ile doğru karşılaştırmayı yapabilmek adına gerekli görülen durumlarda lineer sınıflandırıcı kullanılmıştır.

Seçilen sınıflandırıcı ile birleştirilmiş olarak çalışacak olan özellik vektörü elemesi (temel bileşen analizi-*PCA*) algoritması olarak Pudil ve arkadaşlarının 1994 yılında önermiş oldukları Ardışıl İleri Yönde Kayan Arama (*SFFS*-Sequential Forward Floating Searching) algoritması kullanılmıştır. Böylelikle önerilmiş özellik vektörü içerisinde yalnızca birbirinden bağımsız vektör elemanları bırakılmış, başka bir vektör elemanına lineer bağımlı olan elemanlar elenmiştir. Bu eliminasyon işlemi her bir performans testi öncesinde uygulanmış ve yalnızca en uygun vektör elemanları ile sınıflandırma işlemi gerçekleştirilmiştir. Bu yolla önerilen özellik vektörü için ses steganalizinde maksimum performansa ulaşmak hedeflenmiştir.

Kullanılan *SFFS* özellik elemesi (seçimi) yönteminin çalışma prensibi özet olarak aşağıdaki akışta görülebilmektedir. Temel olarak boş bir küme olarak başlatılan Y elenmiş özellik vektörü bağımsız özelliklerin seçilerek eklenmesi ile genişleyecek, eklenecek yeni bir bağımsız eleman kalmayınca da son haline ulaşacaktır. Aşağıdaki döngünün sonsuza ıraksamasını engellemek amacıyla akıllı bir geçmişi saklama algoritması ile aynı elemanın sürekli olarak eklenip çıkartılması durumu fark edilmeli ve algoritma durdurulmalıdır. Burada objektif fonksiyon, her alt özellik vektörü için değerlendirme yaparak alt özellik vektörünün ne kadar iyi bir ayırt edici olduğunu tanımlayan sayısal bir değer geri döndüren fonksiyondur.

1. Boş bir Y kümesi ile başla.
2. En iyi özelliği seç; (J: Objektif Fonksiyon)

   ; k=k+1
3. En kötü özelliği seç ;
4. Eğer > ise

   ; k=k+1; Adım 3'e git

   Değilse

   Adım 2'ye git.

Tasarlanan steganalizörde, örtü ve stego-sinyal veri setinde bulunan veri sayısının ($2N$), yarısı (N) eğitim için diğer yarısı (N) ise test için kullanılmaktadır. Örtü ve stego sinyal veri setlerinin rasgele yarısı alınarak oluşturulan set ile sınıflandırıcının eğitimi gerçekleştirilmektedir. Eğitimde kullanılmayan diğer veriler ise eğitilmiş sınıflandırıcının performansını test etmekte kullanılmaktadır. Örneğin 2000 adetlik ses sinyali bulunduran örtü ve stego-sinyalleri veri setinin 1000'er adet ses verisi önce özellik vektörünün rafine edilmesi (*SFFS*) ve sınıflandırıcının eğitilmesi için kullanılmakta, geri kalan 1000'er adet ses verisi ile test gerçekleştirilmektedir. Önerilen steganalizörün performans testi sonrasında elimizde Yanlış Alarm (*YA*; False Alarm) dediğimiz içerisinde herhangi bir gizli veri olmamasına rağmen gizli mesaj taşıyor

şeklinde etiketlenen veri sinyalleri sayısı ve Tespit Edilemeyen Mesaj (*TM*) taşıyan sinyal sayısı ve yüzdesel başarım oranı (*BO*=(1-(*YA*+*TM*)/2*N*)x100) gibi değerler ve *ROC* (Alıcı İşlem Karakteristikleri - Receiver Operating Characteristics) eğrileri olacaktır. Burada *YA* ve *TM* değerlerinin düşük, *BO* (%) değerinin yüksek olması önerilen steganalizörün daha başarılı olmasını işaret etmektedir.

ROC eğrileri, bir sınıflandırma testine ilişkin duyarlık ve seçicilik değerleri arasındaki ilişkiyi grafiksel olarak göstermektedir. Farklı sınıflandırıcıların performanslarını karşılaştırmak için bize kolay bir yöntem sunan *ROC* eğrisi ile ilgili açıklamalara geçmeden önce sınıflandırıcılarda sıklıkla kullanılan bazı terimlerin açıklamalarını görmekte fayda bulunmaktadır.

Doğru Pozitif (DP): Pozitif (Gizli mesajın varlığı) olarak etiketlenen gizli mesaj içeren örnek sayısı

Doğru Negatif (DN): Negatif (Gizli mesajın yokluğu) olarak etiketlenen gizli mesaj içermeyen örnek sayısı

Hatalı Pozitif (HP): Pozitif (Gizli mesajın varlığı) olarak etiketlenen gizli mesaj içermeyen örnek sayısı (YA-Yanlış Alarm)

Hatalı Negatif (HN): Negatif (Gizli mesajın yokluğu) olarak etiketlenen gizli mesaj içeren örnek sayısı (TM-Tespit Edilemeyen Mesaj)

Doğru Pozitif Oranı (DPO): DPO = DP / (DP + HN)

Hatalı Pozitif Oranı (HPO): HPO = HP / (DN + HP)

Doğru Negatif Oranı (DNO): DNO = DN / (DN + HP)

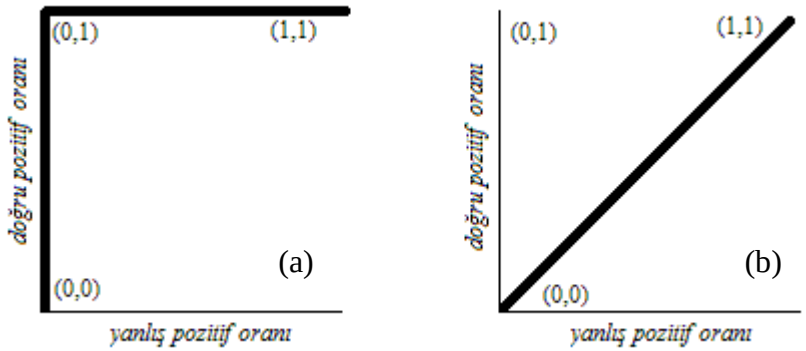
Hatalı Negatif Oranı (HNO): HNO = HN / (DP + HN)

Duyarlılık(D): D = DP / (DP+HP)

Anma (A): A = DP / (DP + HN)

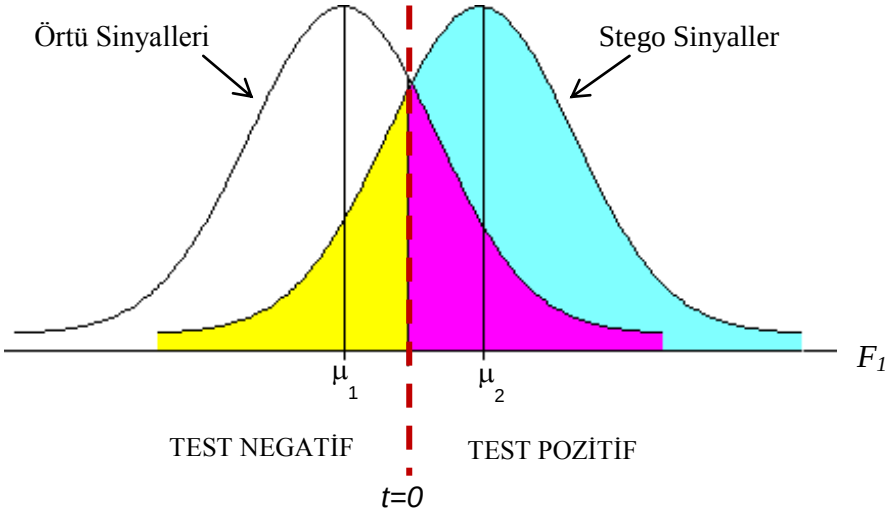
ROC eğrisi *DPO*'na karşın *YPO*'ın noktalanarak çizilmesiyle elde edilir. Bu eğri sayesinde sınıflandırıcının seçim yaparken kullandığı eşik değerinin değişmesi ile

performans değerlerinin nasıl değiştiği hızlı bir şekilde öğrenilebilir. Bilindiği gibi çoğunlukla, tespit etme algoritmaları yanlış alarmlara müsamaha gösterirken, tespit edilemeyen gizli mesaj haberleşmesi durumlarına müsamaha göstermemek mantığı üzerine tasarlanmaktadır. Duyarlılık denilen bu değeri arttırmak için, *ROC* eğrileri sayesinde istenilen gizli mesajların tespit edilememe durumunu azaltacak yönde eşik değeri değiştirilebilmektedir. *ROC* eğrisi üzerindeki her nokta faklı bir eşik değerine sahip sınıflandırıcının oluşturduğu bir modele karşı düşmesi sebebiyle istenilen *DPO* ve *HPO* değerleri için *ROC* eğrisini kullanarak gerekli eşik değeri bilgisine ulaşabiliriz.



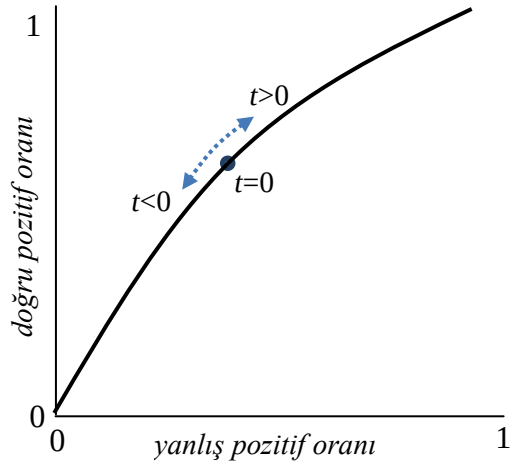
Şekil 4.1. İdeal (a) ve en kötü (b) sınıflandırıcıları gösteren *ROC* eğrileri.

Şekil 4.1'de (0,0) noktası bütün örneklerin negatif olarak sınıflandırıldığı, (1,1) noktası bütün örneklerin pozitif olarak sınıflandırıldığı, (0,1) noktası ise her örneğin doğru küme ile sınıflandırıldığı ideal durumun noktaları temsil etmektedir. Bu durumda, ROC eğrisi (0,1) noktasına ne kadar yakın ise o kadar iyi bir sınıflandırıcıya sahibiz anlamına gelmektedir.



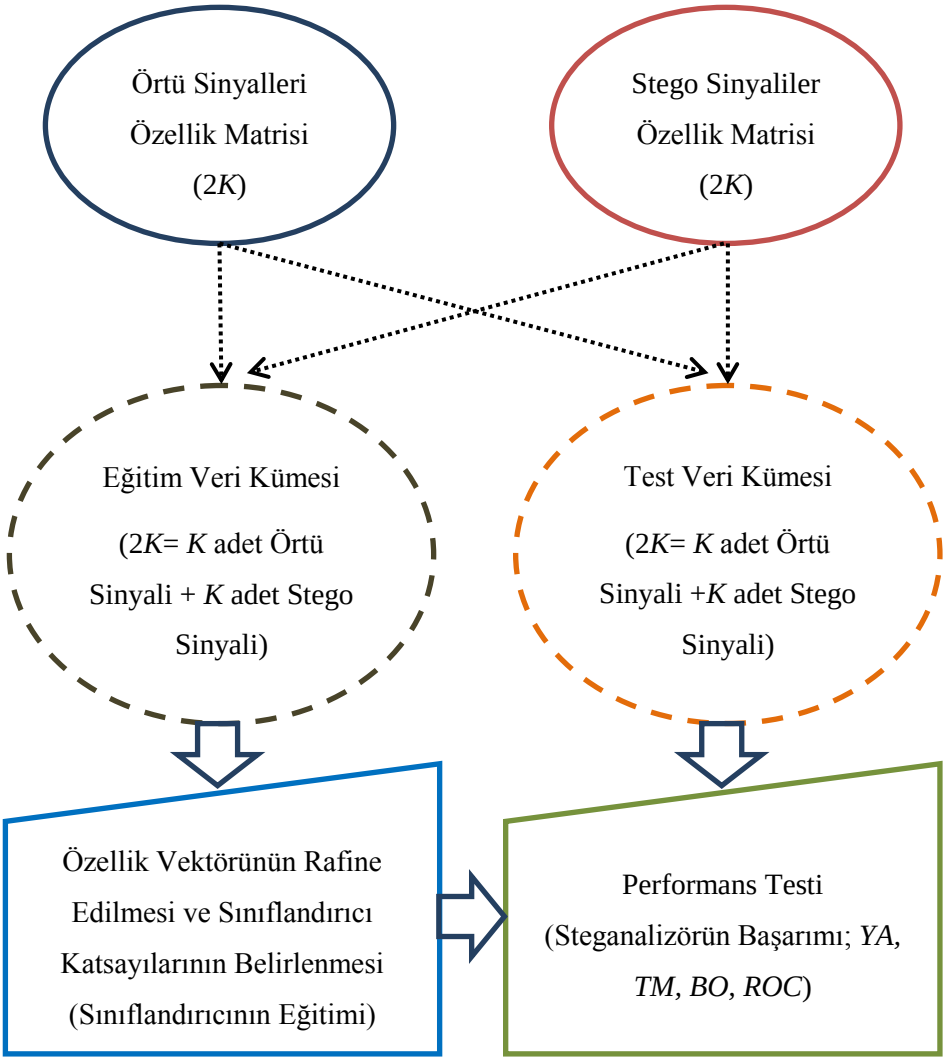
Şekil 4.2. Örtü ve Stego sinyalleri F_1 özellik değerlerinin temsili olasılık dağılımı ve $t=0$ karar eşik değerine göre performans testi sonucu.

Şekil 4.2'de temsili örtü ve stego sinyallerinin temsili özellik değeri F_1'in olasılık dağılımları ve seçilen $t=0$ karar eşik değerine göre performans testi (sınıflandırma) sonucu görülmektedir. Burada karar eşik değeri, t, pozitif veya negatif yönde değiştirilmesi yardımıyla *DPO* ve *HPO* değerleri de değiştirilebilmektedir. Farklı karar eşik değerlerine karşılık gelen ROC eğrisi üzerindeki noktaların temsili gösterimi Şekil 4.3'de görülebilmektedir.



Şekil 4.3. *ROC* eğrisinde farklı karar eşik değerlerine, t, karşılık gelen noktaların temsili gösterimi

Önerilen özellik vektörünün performans testinin şekilsel ve özet olarak nasıl gerçekleştiği Şekil 4.4'de görülebilmektedir.



Şekil 4.4. Önerilen özellik vektörünün performans testinin akış şeması

Yapılan tezde aksi belirtilmediği takdirde, *DSSS* tekniği için 38dB, *FHSS* tekniği için 34dB, *ECHO* tekniği için 18dB, *STOMOD* için 40dB ve *COX* tekniği için 20dB'lik *SWR* değerlerine uyularak seçilen gizli verilerin örtü sinyaline saklanması ile oluşturulmuştur. Benzer şekilde diğer steganografi yöntemleri için stego-sinyal veri seti %100 veri saklama kullanım kapasitesini kullanmaya yönelik boyuttaki verilen örtü sinyallerine gizlenmesi ile meydana getirilmiştir.

SFFS ve performans testini gerçekleştirmek için yazılmış MATLAB kodu Ek-4'te verilmiştir.

4.2 Benzetim Sonuçları

4.2.1 Konuşma ses kayıtları için karşılaştırmalı benzetim sonuçları

Tezde ses steganalizörü için önerilen özellik vektörünün performansının görülebilmesi amacıyla pek çok farklı denemeler yapılmıştır. Yapılan denemelerin geçerli olabilmesi amacıyla literatürde daha önceden önerilmiş steganaliz yöntemleri ve benzetim şartları ile uyumlu performans testleri gerçekleştirilmiştir. Gerçekleştirilen steganaliz testlerinde eşitlik (4.2)'de verilmiş olan özellik vektörü kullanılmıştır.

Gerçekleştirilen ilk performans testi Özer ve arkadaşları tarafından 2003 yılında önerilen Ses Kalitesi Metriklerine (*AQM*-Audio Quality Metrics) ve Avcıbaş tarafından 2006 yılında önerilen İçerik-Bağımsız Ses Kalitesi Metriklerine (*CIAQM* – Content Independent Audio Quality Metrics) dayanan steganalizörler ile karşılaştırılması amacıyla Bölüm 4.1.1'de bahsedilen ilk konuşma veri seti ile gerçekleştirilmiştir. Yine aynı amaçla gerçekleştirilen testte lineer sınıflandırıcı kullanılmıştır.

Çizelge 4.3'de görüldüğü gibi, önerilen özellikler ile sudamgası teknikleri için elde edilen başarım değerleri *AQM* ve *CIAQM* steganalizörleri başarım değerleri ile yaklaşık aynı olmasına rağmen, diğer steganografi teknikleri için elde edilen başarım karşılaştırmalı olarak daha iyidir. Bu durumun sebebi daha önceden de bahsedildiği üzere sudamgası teknikleri gizlenen verinin fark edilmesi endişesi taşınmamasıdır. Bu sebeple sudamgası algoritmaları saklanan verinin gizli kalmasını değil, yok edilememesini amaçlamaktadırlar. Bu durumda sudamgası teknikleri ile saklanan verileri ayırt etmek diğer steganografi tekniklerine göre çok daha kolay hale gelmektedir.

Yapılan ikinci denemede ise, TIMIT veri setinin 2000 adetlik alt-seti ve *SVM* sınıflandırıcı kullanılarak performans testi gerçekleştirilmiştir. Bu denemenin sonuçları ve Dalgacık temelli özellikler (Johnson ve ark. 2005) ile yapılan steganaliz sonuçları karşılaştırması Çizelge 4.4'de görülebilmektedir. Bu tabloda *SVM* temelli nonlineer sınıflandırıcının etkisi görülebilmekte, *SVM* sınıflandırıcı ile Çizelge 4.3'de verilen lineer sınıflandırıcı ile elde edilen başarım sonuçlarına göre daha iyi sonuçlar elde edilmektedir.

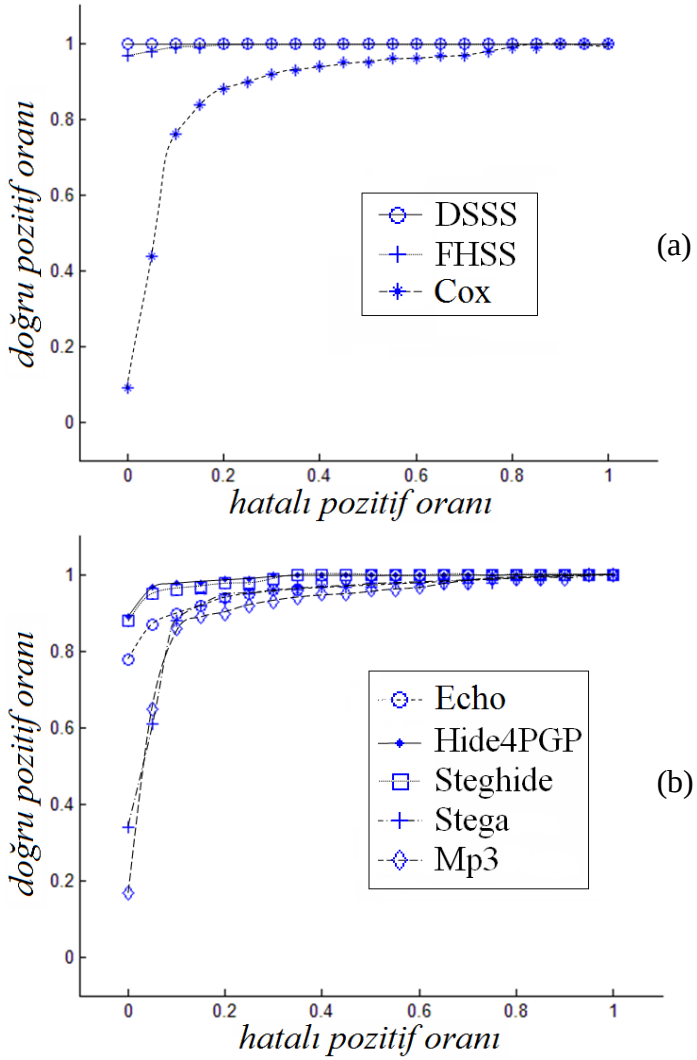
Çizelge 4.3. Kaotik Özellikler ile *AQM* ve *CIAQM* özelliklerin karşılaştırılması.

	AQM			**CIAQM**			**KAOTİK**		
Metot	TM	YA	%	TM	YA	%	TM	YA	%
DSSS	0/50	0/50	100,0	0/50	0/50	100,0	0/100	0/100	100,0
FHSS	2/50	1/50	97,0	0/50	0/50	100,0	0/100	0/100	100,0
ECHO	3/50	5/50	92,0	0/50	0/50	100,0	6/100	17/100	88,5
STEGA	4/50	4/50	92,0	3/50	1/50	96,0	7/100	8/100	92,5
HIDE4PGP	14/50	10/50	76,0	4/50	8/50	88,0	2/100	3/100	97,5
STEGHIDE	11/50	8/50	81,0	8/50	6/50	86,0	2/100	6/100	96,0
COX	1/50	5/50	94,0	-	-	-	21/100	33/100	73,0
STOMOD	-	-	-	-	-	-	15/100	9/100	88,0
MP3	-	-	-	-	-	-	19/100	14/100	83,5

Çizelge 4.4. Dalgacık temelli özellikler ve önerilen kaotik özelliklerin performansları

	DALGACIK			**KAOTİK**		
Metot	**TM**	**YA**	**%**	**TM**	**YA**	**%**
COX	463/1000	446/1000	54,6	227/1000	245/1000	76,4
DSSS	46/1000	69/1000	94,3	2/1000	1/1000	99,9
FHSS	143/1000	162/1000	84,8	5/1000	5/1000	99,5
ECHO	396/1000	418/1000	59,3	63/1000	154/1000	89,2
STEGA	269/1000	275/1000	72,8	51/1000	84/1000	93,2
HIDE4PGP	167/1000	210/1000	81,2	29/1000	55/1000	95,8
STEGHIDE	255/1000	218/1000	76,4	33/1000	48/1000	95,9
MP3	284/1000	235/1000	74,1	154/1000	114/1000	86,6
STOMOD	195/1000	221/1000	79,2	118/1000	71/1000	90,5

TIMIT veri setinin alt-kümesinden oluşan veri seti için yapılan *SVM* sınıflandırıcı tabanlı performans testleri farklı karar eşik değerleri, *t*, için gerçekleştirildiğinde ortaya çıkan *ROC* eğrileri Şekil 4.5'de görülebilmektedir. Bu şekilde özellikle sudamgası ve diğer steganografik yöntemler ayrı olarak gösterilmiştir. Bu eğrilerde hem sudamgası hem de diğer steganografik yöntemler için önerilen kaotik özellikler tabanlı özellik vektörünün düşük *HPO* değerleri için bile yüksek *DPO* değerleri vermekte, yani ayırt edici bir sınıflandırıcı tablosu çizmektedir.



Şekil 4.5. Sudamgası (a) ve diğer steganografik yöntemler (b) için SVM tabanlı sınıflandırıcı ve 2000 adetlik TIMIT alt veri seti ile gerçekleştirilen steganaliz testleri sonucunda elde edilen ROC eğrileri

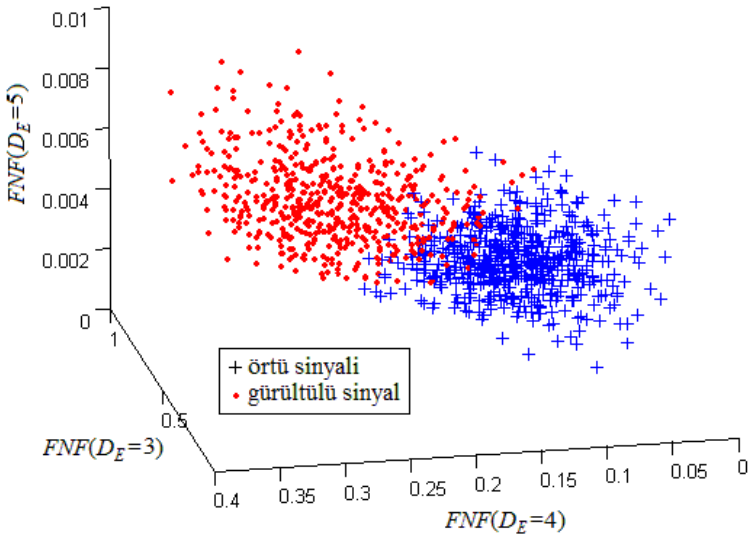
Çizelge 4.5'de her bir steganografi yöntemi için, Çizelge 3.1'de verilen steganografi saldırı yaklaşımlarından "seçili stego saldırısı" yaklaşımı ile gerçekleştirilen steganaliz öncesinde yürütülen özellik vektörü rafine edilmesi (*SFFS*) sonrasında seçilen özelliklerle ile gerçekleştirilen steganaliz sonuçları görülmektedir. Aynı tabloda tezde genel olarak benimsenen "seçili stego saldırısı" yaklaşımı dışında, "Hepsi" satırında "Stego Saldırısı" yaklaşımı, yani elimizde yalnızca stego-sinyalin bulunduğu, veri gizleme metodunun bilinmediği yaklaşım ile gerçekleştirilen steganaliz öncesindeki *SFFS* algoritmasının yürütülmesi sonrasında seçilen özellikler görülebilmektedir. Bu tablo seçili olan özellik elemanları ile maksimum performans elde edildiğini, seçili olmayan diğer elemanların steganaliz performansına katkısının bulunmadığını anlatmaktadır. Daha önceden de bahsedildiği aynı başarım sonuçlarını veren en az sayıda özellik kullanmak steganalizin çok uzun olabilecek işlem süresini kısaltmak adına gerçekleştirilen önemli bir adımdır.

Çizelge 4.5. Her bir steganografik yöntem için ayrı ve yöntemlerin tümünü içeren *SVM* tabanlı sınıflandırıcı ve 2000 adetlik TIMIT alt veri setinde yapılan özellik vektörünün rafine edilmesi (*SFFS*) sonrasında kullanılan özellikler

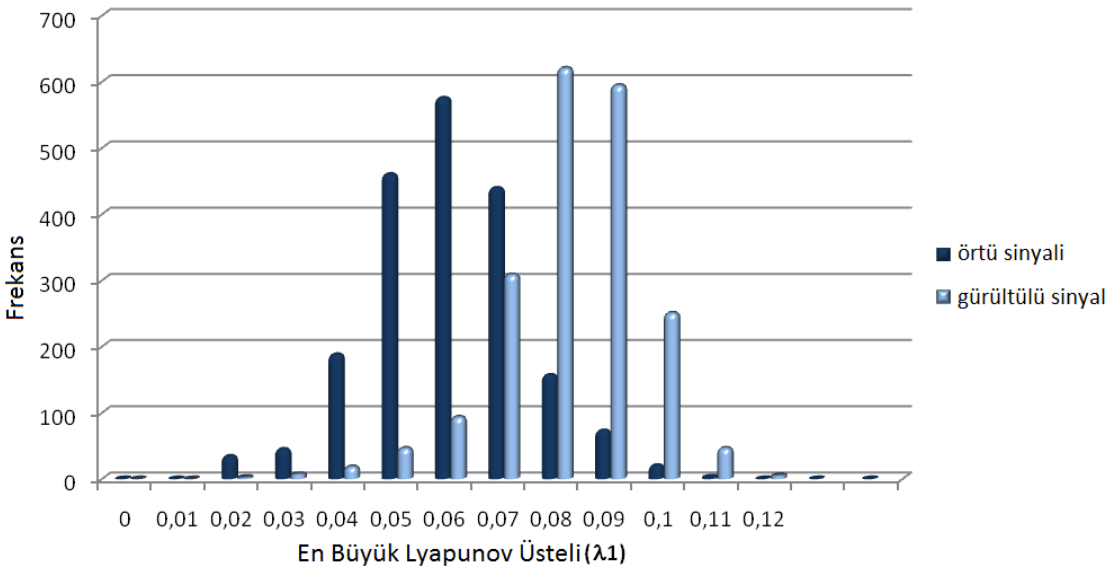
YÖNTEM	**RAFİNE EDİLMİŞ ÖZELLİK VEKTÖRÜ**	**TM**	**YA**	**%**
COX	{1,2,6,7,8,9,10,11,12,13,14,16,17, 19,20,23}	227/1000	245/1000	76,4
DSSS	{1,10,16,23}	2/1000	1/1000	99,9
FHSS	{1,7,10,13,17,19,21,24}	5/1000	5/1000	99,5
ECHO	{1,5,10,13,24,25}	63/1000	154/1000	89,2
STEGA	{2,3,10,13,16,17,18,19,20,22,23}	51/1000	84/1000	93,2
HIDE4PGP	{1,2,7,10,17,18,20,23,25}	29/1000	55/1000	95,8
STEGHIDE	{2,4,10,11,17,20,23,24}	33/1000	48/1000	95,9
MP3	{2,3,5,6,8,9,10,11,14,16,18,19,20, 22,24}	154/1000	114/1000	86,6
STOMOD	{2,10,13,14,17,19,23,25}	118/1000	71/1000	90,5
HEPSİ	{2,4,10,12,13,15,16,17,18,19,20,21, 23,24}	1651/9000	1854/9000	80,5

4.2.1.1 *Gürültünün etkisi*

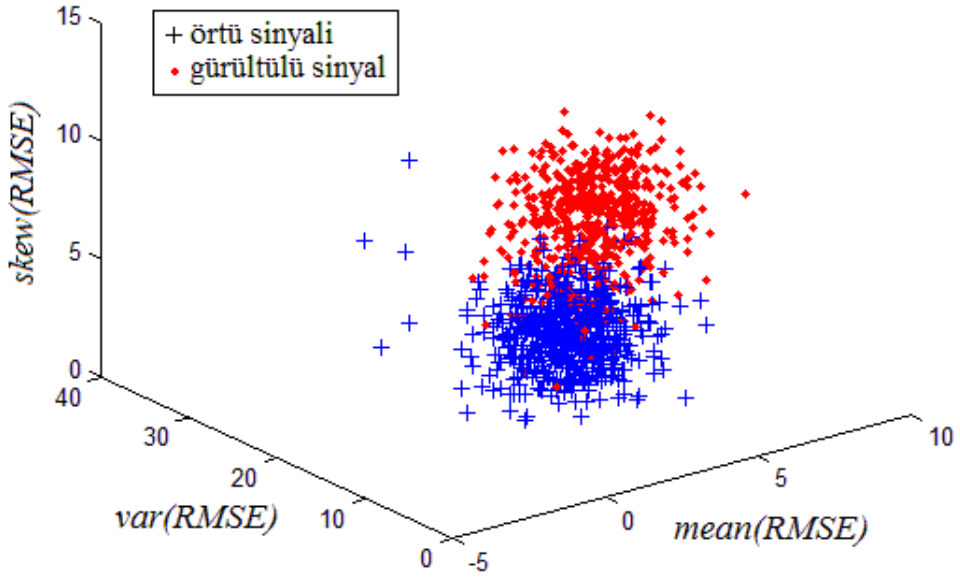
Tezde önerilen özelliklerin gürültüye karşı ayırt ediciliğini test etmek üzere 2000 adetlik TIMIT alt setine *SWR*=40dB olmak üzere beyaz gürültü eklenerek, bir önceki kısımda *STOMOD* steganografi tekniği ile yapılmış olan benzetim şartlarında performans testleri gerçekleştirilmiştir. Çizelge 4.4'de görülmekte olan sonuçları veren steganaliz testlerinde de benzer şekilde gizlenen verinin büyüklüğü ile orantılı şekilde örtü sinyalinde *SWR*=40dB'lik bir gürültü oluşturmaktadır. Tezin bu kısmında aynı gürültü oranını veri gizlenmesi ile değil, doğrudan doğruya beyaz gauss gürültüsü eklenmesi suretiyle sağlanmıştır. Şekil 4.6 ve Şekil 4.7'de kaotik özelliklerin gürültüye ne kadar hassas olduğu görülebilmektedir. Üzerinde gürültü bulunmayan örtü sinyalleri ve bu sinyallerin gürültülü versiyonlarının kaotik değerleri oldukça ayırt edici olmaktadır. Şekil 3.13 (b), Şekil 3.14(b) ve Şekil 3.15 (b) ile Şekil 4.6, Şekil 4.7 ve Şekil 4.8'nin karşılaştırılması bize veri gizlemenin sinyale bağımsız gürültü eklenmesi ile yakın anlamlar taşıdığı varsayımını kuvvetlendirmektedir. Çizelge 4.6. ise *SWR*=70dB için bile önerilen kaotik özellik vektörünün yüksek performans ile ayırt etme görevini sürdürdüğünü göstermektedir.



Şekil 4.6. 2000 adet TIMIT konuşma sesini temel alan örtü ve 40dB gürültülü sinyallerin farklı boyutlardaki (D_E=3, 4, 5) *FNF* değerlerinin dağılımı.



Şekil 4.7. 2000 adet TIMIT konuşma sesini temel alan örtü ve 40dB gürültülü sinyallerin D_E=7 için hesaplanan en büyük Lyapunov üsteli değerlerinin dağılımı.



Şekil 4.8. 2000 adet TIMIT konuşma sesini temel alan örtü ve 40dB gürültülü sinyallerin n_{surr}=20 için F_{surr} özellik vektörünün ilk 3 elemanı değerleri

Çizelge 4.6. Gürültülü Konuşma Sinyallerinin Performansı

SWR	**TM**	**YA**	**%**
20dB	1/1000	2/1000	99,9
30dB	4/1000	5/1000	99,5
40dB	12/1000	11/1000	98,9
50dB	37/1000	38/1000	96,3
60dB	111/1000	99/1000	89,5
70dB	235/1000	241/1000	76,2
80dB	387/1000	398/1000	60,8
90dB	472/1000	443/1000	54,3

4.2.1.2 Saklanan verinin boyutunun etkisi

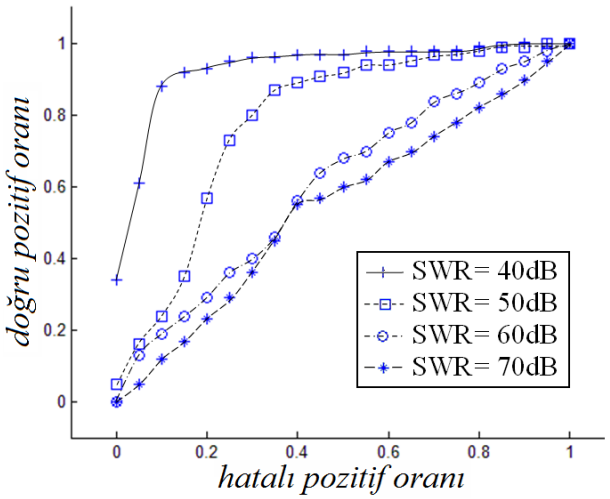
2000 adetlik TIMIT alt seri seti üzerinde ayrıca önerilen kaotik özelliklerin başarımının gizlenen verinin büyüklüğü ile nasıl değişildiği incelendi. Sudamgalama yöntemleri için 20dB, 30dB ve 40dB'lik farklı *SWR* oranları, diğer steganografi yöntemleri için ise %10, %50 ve %100'lük kapasite kullanım oranları için yapılan steganaliz performans testleri tekrar edildi. Bölüm 4.2.1'de yapılan steganaliz testleri ses sinyalindeki bozulmanın fark edildiği *DSSS* tekniği için 38dB, *FHSS* tekniği için 34dB, *ECHO* tekniği için 18dB, *STOMOD* için 40dB ve *COX* tekniği için 20dB'lik *SWR* değerleri, diğer steganografi teknikleri için %100 kapasite kullanım oranı ile gerçekleştirilmiştir.

Farklı gizli veri boyutları için elde edilen steganaliz performans sonuçları Çizelge 4.7'de görülebilmektedir. Burada ses sinyalindeki bozulmanın fark edilebildiği sınırın altındaki gizlenen veri boyutları için (daha düşük *SWR*, daha düşük kapasite kullanım oranı) performans değerlerinin kötüleştiği fark edilmektedir. Tez çalışmasında ayrıca *STOMOD* steganografi tekniği için farklı gömme oranları için *ROC* eğrileri hesaplanmıştır. Elde edilen *ROC* eğrileri Şekil 4.9'da görülebilmektedir.

Çizelge 4.7. *SVM* tabanlı steganalizörün farklı gömme oranları için önerilen kaotik özellikler ile elde ettiği performans değerleri

Metot	**SWR**	**TM**	**YA**	**%**
DSSS	20dB	0/1000	0/1000	100,0
	30 dB	0/1000	0/1000	100,0
	40 dB	2/1000	2/1000	99,8
FHSS	20 dB	0/1000	0/1000	100,0
	30 dB	4/1000	3/1000	99,7
	40 dB	13/1000	9/1000	99,0
ECHO	20 dB	74/1000	148/1000	88,9
	30 dB	132/1000	295/1000	78,7
	40 dB	212/100	437/1000	67,6
COX	20 dB	227/1000	245/1000	76,4
	30 dB	435/1000	442/1000	56,2
	40 dB	471/1000	483/1000	52,3
STOMOD	20 dB	7/1000	5/1000	99,4
	30 dB	45/1000	21/1000	96,5
	40 dB	118/1000	71/1000	90,5

Metot	**Kapasite Kull.**	**TM**	**YA**	**%**
STEGA	%10	243/1000	274/1000	74,2
	%50	105/1000	117/1000	88,9
	%100	51/1000	84/1000	93,2
HIDE4PGP	%10	111/1000	202/1000	84,4
	%50	32/1000	143/1000	91,3
	%100	29/1000	55/1000	95,8
STEGHIDE	%10	173/1000	234/1000	79,7
	%50	85/1000	124/1000	89,6
	%100	33/1000	48/1000	95,9
MP3	%10	365/1000	251/1000	69,2
	%50	239/1000	127/1000	81,7
	%100	154/1000	114/1000	86,6



Şekil 4.9. *STOMOD* steganografi tekniği ve *SVM* sınıflandırıcı ile farklı gizli veri boyutları için elde edilen *ROC* eğrileri.

4.2.2 Genel ses sinyalleri için uygulama

Önerilen kaotik özelliklerin genel ses sinyallerinin steganalizinde kullanılabilirliğini göstermek amacıyla Bölüm 4.1.1 Veri setinin oluşturulması kısmında bahsedilen müzik kayıtlarından oluşan iki adet veri seti kullanılmıştır. Bunlardan ilki 284 adet ses parçasından oluşan popüler şarkılardan, diğeri ise 70 adet ses parçasından oluşan müzik enstrümanları kayıtlarından oluşmaktadır. Popüler şarkı kayıtlarına ait 284 parçadan oluşan alt veri set ve lineer tabanlı sınıflandırıcı içeren steganalizör ile gerçekleştirilen performans testleri ve aynı şartlarda gerçekleştirilen *AQM* (Özer ve ark. 2003) özellikleri ile gerçekleştirilen performans testlerinin karşılaştırmalı sonuçları Çizelge 4.8'de görülebilmektedir.

Çizelge 4.8. Kayıtlı müzik sinyallerinin *AQM* ve önerilen kaotik özellikler ile gerçekleştirilen steganaliz sonuçları

	AQM			**KAOTİK**		
Metot	***HNO***	***HPO***	**%**	***HNO***	***HPO***	**%**
DSSS	9,8	14,1	88,1	21,1	42,8	68,1
FHSS	1,4	2,8	97,9	22,4	47,3	65,2
ECHO	16,9	20,1	81,5	27,2	41,0	65,9
STEGA	12,6	14,1	86,7	42,5	27,0	65,3
HIDE4PGP	16,9	19,7	81,7	29,4	42,6	64,0
STEGHIDE	26,7	26,7	73,3	28,5	44,0	63,8
MP3	-	-	-	32,6	47,6	59,9
STOMOD	-	-	-	41,1	36,6	61,2

Çizelge 4.8'de görülen *HNO* ve *HPO* değerleri sırasıyla *YA* ve *TM* sinyal sayısının yüzdesel oranıdır. Bu tablodaki sonuçlar, önerilen kaotik özelliklerin konuşma seslerinde olduğu gibi müzik kayıtlarında başarılı olmadığını göstermektedir. Performans değerlerindeki bu keskin düşüşün açıklaması, müzik seslerinde kaotik fenomenin konuşma seslerine göre daha az görülmesidir. Müzik seslerinde ayrıca aynı

anda kayıtta olan ve farklı sinyal boyutlarına sahip birden fazla enstrüman ve insan sesi verisi, kaotik özelliklerin ses verisinde görülememesi anlamına gelmektedir. Sonuç olarak, müzik sesi sinyalinin boyutu, her bir ses kaynağının boyutları toplamına eşit olacaktır. Bu durumda, önerilen kaotik özellikler düşük boyutlu ses sinyalleri için ayırt edici olmakta, müzik sinyalleri gibi yüksek boyutlu ses sinyalleri için ayırt edici olmamaktadır.

Çizelge 4.9'da örnek olarak *ECHO* ve *STEGHIDE* steganografi yöntemleri için *SVM* tabanlı sınıflandırıcı kullanan farklı tipte müzik eserleri için gerçekleştirilen steganaliz performans sonuçları görülmektedir. Bu tablodan, eğer müzik kaydı sözlü ise, insan sesi ne kadar baskın ise başarım değerlerinin de o kadar arttığı çıkarımını elde etmek mümkündür. İnsan sesinin kaotikliği daha önceki bölümlerde de görüldüğü üzere ses steganalizinde önemli bir ayırt edici olarak görev yapmaktadır. Sözsüz bir klasik müzik eseri olan "Şehrazat" parçası için başarım değerleri oldukça düşerken, ritim ve sürekli konuşma seslerinden oluşan "Again" isimli müzik eseri için gerçekleşen başarım değerleri "Bölüm 4.2.1 Konuşma ses kayıtları için karşılaştırmalı benzetim sonuçları"nda elde edilen başarım sonuçlarına yaklaşmaktadır. Sonuç olarak insan sesinin eksikliği ses steganalizinin performansında negatif etkide bulunmaktadır.

Çizelge 4.9. Farklı tiplerdeki müzik kayıtlarından oluşan veri setlerinde *ECHO* ve *STEGHIDE* steganografi yöntemleri için SVM tabanlı sınıflandırıcı kullanan steganalizör performans sonuçları

	ECHO			**STEGHIDE**		
Veri Seti	**TM**	**YA**	**%**	**TM**	**YA**	**%**
Şehrazat (Klasik Müzik)	8/26	7/26	71,2	9/26	8/26	67,3
U2 "One"	5/26	6/26	78,8	8/26	6/26	73,0
U2 "Even Better"	5/22	5/22	77,3	7/22	5/22	72,7
Rolling Stones	6/22	5/22	75,0	7/22	6/22	70,5
Again (Rap Müzik)	6/46	7/46	85,9	8/46	6/46	84,8
TÜM VERİ SETİ	31/142	30/142	78,6	32/142	33/142	77,1

4.2.2.1 Müzik enstrümanları kayıtları

Müzik enstrümanlarının genelde tek bir nota veya tek bir vuruştan oluşan seslerinden oluşan veri seti (SQAM. 2006) ile gerçekleştirilen *SVM* tabanlı sınıflandırıcı kullanan steganalizörün performans testlerinin sonuçları Çizelge 4.10'da görülmektedir. Bu veri tabanındaki ses kayıtlarının ortalama olarak %20'sinin sessiz boşluklardan oluştuğu göz önüne alınarak, kayıtların sessiz kısımlarını çıkartarak performans testi tekrar edilmiş ve aynı tabloda paylaşılmıştır.

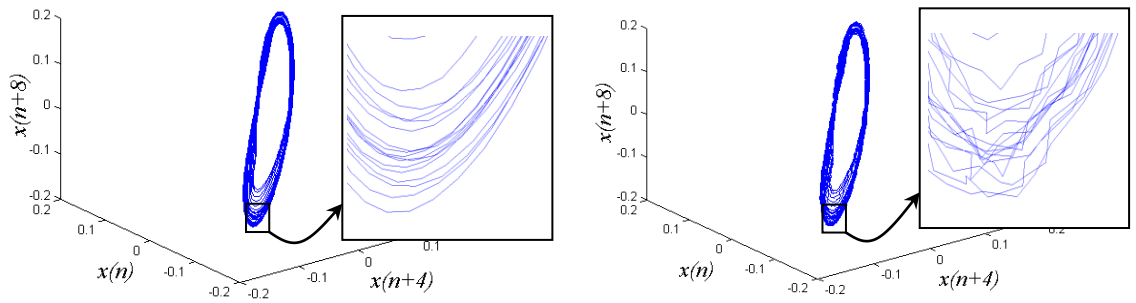
Çizelge 4.10. Müzik enstrümanları kayıtlarının bütün halde ve sessiz kısımları çıkartılmış halde önerilen kaotik özellikler ile gerçekleştirilen *SVM* tabanlı sınıflandırıcı kullanan steganalizörün performansı

	Sessiz Kısımlar Dâhil			**Sessiz Kısımlar Hariç**		
Metot	**TM**	**YA**	**%**	**TM**	**YA**	**%**
COX	15/35	16/35	55,7	14/35	14/35	60,0
DSSS	12/35	13/35	64,3	6/35	7/35	81,4
FHSS	13/35	15/35	60,0	7/35	7/35	80,0
ECHO	15/35	18/35	52,9	9/35	10/35	72,9
STEGA	15/35	16/35	55,7	8/35	7/35	78,6
HIDE4PGP	15/35	17/35	54,3	9/35	10/35	72,8
STEGHIDE	14/35	16/35	57,1	10/35	12/35	68,6
MP3	14/35	16/35	57,1	10/35	13/35	67,1
STOMOD	15/35	14/35	58,6	8/35	10/35	74,3

Çizelge 4.10'daki sonuçlardan açıkça görülmektedir ki, müzik aletlerinin seslerine ait kayıtlar ile yapılan steganaliz sonuçları, konuşma sesleri ile yapılanlardan daha kötüdür. Kayıtlardaki sessiz boşluklar hatalı *FNN*, Lyapunov Üstelleri ve vekil verilerin hesaplanmasına ve oluşturulmasına neden olmaktadır. Bu durum ise sınıflandırıcının hatalı kararlar almasına neden olmaktadır. Sessiz kısımlarının kayıtlardan çıkartılması ile steganaliz performansında gözle görülür bir artış gözlenmesi de bu durumun bir kanıtıdır. Fakat bu durumda bile, konuşma seslerinde görülen ayırt edicilik müzik

aletleri seslerinde görülmemektedir. Bunun nedeni müzik aletleri seslerinin kaotik değil harmonik olmasıdır. Bu durum kaotik özelliklerin örtü sinyali ve stego sinyal arasında büyük farklılıklar göstermemesine neden olmaktadır. Yine de küçümsenmeyecek bir başarım olan bu sonuçların kaotik olmayan bir sinyalde nasıl elde edildiğini Şekil 4.10'da açıklamaktadır.

Şekil **4.10** (a)'da görülen obua müzik enstrümanına ait ses sinyalinin faz uzayı, sinyal üzerine *DSSS* sudamgalama yöntemi ile veri gizlenmesi ile bozulmakta ve Şekil **4.10** (b)'de görülen şekil ortaya çıkmaktadır. Bu durum, neden kaotik olmasa bile bir sinyalin faz uzayındaki değişikliklerin, bu değişikliklere sıkı sıkıya bağlı kaotik özellikler üzerinde değişiklikler ortaya çıkaracağını açıklamaktadır.



(a) **(b)**

Şekil 4.10. Veri gizlemenin bir müzik enstrümanı ses kaydının faz uzayı üzerindeki etkisi. (a) Örtü sinyalinin faz uzayı, (b) *DSSS* steganografi yöntemi ile oluşturulmuş stego sinyalin faz uzayı.

4.2.3 Performans iyileştirme çalışmaları

Önerilen kaotik özellik vektörünün konuşma sesini üreten sistemin tüm nonlineer dinamiklerini kapsaması tabii ki düşünülemez. Konuşma sesleri analizleri için geliştirilen nonlineer sinyal işleme araçlarının hepsi, konuşma ses sinyallerinin durağan (stationarity) oldukları varsayımına dayanmaktadır. Tezde kullandığımız ses sinyallerinin 4 saniyelik parçalara bölünüp özelliklerinin çıkartılmasına çalışılmasının sebebi daha kısa süreli ses parçaları ile bu varsayımın doğrulanmaya çalışılmasıdır. Konuşma sesinin 250ms süre ile yarı-durağan, 20 ms ile durağan olduğu varsayılmakla (JPL's. 2011) birlikte bu kadar kısa süreli ses sinyalleri kaotik özelliklerin çıkartılmasına yeterli olmamaktadır. Performansın maksimumda tutulması için

belirlenen 4 saniyelik optimum süreden başka, performansı iyileştirmek için başka yaklaşımlar da geliştirilmiştir.

4.2.3.1 Yalnızca sesli harflerin kullanılması

Konuşma sesinin dinamiklerinin daha iyi kapsanmasını sağlamak amacıyla, yalnızca kayıttaki sesli harflerin bulunduğu kısımlar için kaotik özelliklerin hesaplanarak steganaliz testleri tekrar edilmiştir. TIMIT veri setinden rasgele seçilen 250 adet ses kaydından Goldwave (Goldwave. 2011) programı yardımıyla manuel olarak ortalama 200 ms uzunluğunda 1000 adet yalnızca sesli harflerden oluşan yeni ses kayıtları oluşturulmuştur.

1000 adetlik yeni veri seti ile yeniden yapılan *SVM* tabanlı steganaliz testlerinin sonuçları Çizelge 4.11'de görülebilmektedir. Bu çizelgeden da görüldüğü üzere, 4 saniye uzunluktaki orijinal ses kayıtları ile yapılan steganaliz sonuçlarına göre ortalama %5'lik bir iyileşme sağlanmıştır. Çizelgedeki ilk 3 sütun, Çizelge 4.4'de verilmiş olan performans sonuçları kullanılarak oluşturulmuştur. Burada *TM* ve *YA* değerlendirme kriterleri yerine farklı veri setlerinden oluşan iki steganalizörü doğru bir şekilde karşılaştırabilmek amacıyla *HNO* ve *HPO* istatistiksel değerlendirme kriterleri kullanılmıştır.

Çizelge 4.11. Yalnızca sesli harflerden oluşan ses kayıtlarının önerilen kaotik özellikler ile gerçekleştirilen performans testlerinin karşılaştırmalı sonuçları

	4 s'lik ses kayıtları			**Yalnızca Sesliler**		
Metot	**HNO**	**HPO**	**%**	**HNO**	**HPO**	**%**
COX	22,7	24,5	76,4	19,4	21,2	79,7
DSSS	0,2	0,1	99,9	0,0	0,0	100,0
FHSS	0,5	0,5	99,5	0,0	0,0	100,0
ECHO	6,3	15,4	89,2	3,8	12,2	92,0
STEGA	5,1	8,4	93,2	1,6	5,6	96,4
HIDE4PGP	2,9	5,5	95,8	1,4	3,4	97,6
STEGHIDE	3,3	4,8	95,9	1,8	2,8	97,7
MP3	15,4	11,4	86,6	11,4	6,8	90,9
STOMOD	11,8	7,1	90,5	7,4	2,6	95,0

4.2.3.2 Kayıtlardaki sessiz boşlukların elenmesi

Ses kayıtlarında genellikle sessiz boşluklar bulunabilmekte ve durum da performansı etkilemektedir. Özellikle kayıtlardaki uzun sessizlikler, kaotik özellikler ile steganaliz işlemini imkânsız kılabilmektedir. Bunun nedeni sessiz kısımlar için kaotik özelliklerin hesaplanamaması veya gerçek dışı değerler hesaplanmasıdır. Bu kısımlar gürültü gibi davrandığından bu sinyaller için kaotik denilmesi mümkün değildir. Bu durumda çok yüksek boyutlardaki bu sinyaller için önerilen kaotik özelliklerin ses steganalizinde işe yaraması mümkün değildir.

Çizelge 4.12'ün ilk sütunu Çizelge 4.4'de verilmiş konuşma seslerine ait yüzdesel başarım oranlarını veren steganaliz sonuçlarını göstermektedir. Aynı tablonun üçüncü ve dördüncü sütunları ise daha önceden Çizelge 4.10'de verilmiş olan müzik aletlerine ait sessiz kısımlar dâhil ve hariç yüzdesel başarım oranlarını veren performans sonuçlarıdır. Oransal olarak çok daha az sessizlik barındıran konuşma sinyalleri (ortalama %4 sessizlik), çok daha fazla sessizlik içeren müzik aletleri sinyallerine (ortalama %20 sessizlik) göre sessiz kısımların çıkartılmasından çok daha fazla etkilenmiştir. Konuşma sinyalleri ile yapılan SVM tabanlı steganaliz sonuçları ortalama % 0.8 artış gösterirken, müzik aletleri sesleri ile yapılan steganaliz sonuçlarında ortalama %16'lık bir artış gözlenmiştir.

Çizelge 4.12. Kayıtlardaki sessiz boşlukların performansa etkisi

	Konuşma		**Müzik Enstrümanları**	
Metot	**Sessiz Kısımlar Dâhil**	**Sessiz Kısımlar Hariç**	**Sessiz Kısımlar Dâhil**	**Sessiz Kısımlar Hariç**
COX	76,4	76,6	55,7	60,0
DSSS	99,9	99,9	64,3	81,4
FHSS	99,5	99,6	60,0	80,0
ECHO	89,2	90,6	52,9	72,9
STEGA	93,2	94,3	55,7	78,6
HIDE4PGP	95,8	96,1	54,3	72,8
STEGHIDE	95,9	96,4	57,1	68,6
MP3	86,6	88,6	57,1	67,1
STOMOD	90,5	92,5	58,6	74,3

5. SONUÇ

Bu tez çalışmasında, kaosun analizinde sıklıkla kullanılan kaos analiz araçlarının ilk defa ses steganalizinde kullanılması önerilmiştir. Konuşma ve müzik seslerinde kaotik görüngünün (fenomenin) bulunduğuna dair kanıtları araştıran bugüne kadar yapılan teorik ve pratik çalışmalardan ilham alınan bu tez ile ses sinyallerinin kaotik özelliklerindeki değişimin ses steganalizindeki kullanılabilirliği araştırılmıştır.

Hatalı komşular yöntemi, Lyapunov üstelleri, vekil veriler, kesirli boyut tahmin edicileri gibi kaos araçlarını kullanarak elde edilen özellik vektörü, konuşma, müzik eserleri, müzik aletleri gibi pek çok farklı ses verisi için ses steganalizindeki kullanım alanları ve performans değerleri hesaplanmıştır. Performans testleri bugün için bilinen tüm ses steganografi yöntemleri için gerçekleştirilmiş, özellikle sudamgası tekniği denilen gruptaki steganografi teknikleri için neredeyse tam başarım (%100 ayırt etme) sağlanmıştır. Sudamgalama tekniklerinde elde edilen bu yüksek başarımın sebebi, tezde de anlatıldığı üzere sudamgası tekniklerinin gizlenen verinin fark edilmemesi gibi bir kaygısının bulunmamasıdır. Diğer steganografi tekniklerindeki algoritmalar gizli verinin fark edilmemesi üzerine kurulduğu için, bu yöntemler ile gizlenen verilerin tespit edilmesi çok daha zordur. Bu durum elde edilen performans testleri sonuçlarında da görülebilmektedir. Tezde performans testleri, tasarlanan akademik çevrelerin kabul ettiği, genelde tüm literatürde steganaliz testlerinde kullanılan öğrenme tabanlı lineer veya SVM sınıflandırıcı kullanan steganalizör ile gerçekleştirilmiştir.

Önerilen kaotik özellik vektörün geçerliliğini kanıtlamak üzere, literatürde bugüne kadar yapılmış olan çalışmalar ile karşılaştırmalar gerçekleştirilmiştir. Bu karşılaştırmalar, önerilen kaotik özellik vektörünün ses steganalizinde kullanılabilirliğini göstermek bir yana, ses steganalizinde bugün için özellikle *HIDE4PGP*, *STEGHIDE*, *MP3* ve *STOMOD* steganografi teknikleri için bilinen en başarılı sonuçlar olduğunu göstermektedir. Önerilen özellik vektörüne, örneğin *CIAQM* (Avcibas. 2006) özellik vektöründeki elemanların eklenmesi ile bu başarım çok daha yüksek seviyelere gelecektir. Hali hazırda önerilen kaotik özellik vektörünün tek başına *COX* ve *ECHO* gibi steganografi teknikleri için orta seviyede başarılı olması sebebiyle, bu eksikliğin *CIAQM* veya daha başka bir steganalizör özellik elemanlarının da önerilen özellik vektörüne eklenmesi ile bu engel giderilmiş olacaktır.

Önerilen özellik vektörü genel olarak konuşma seslerinden oluşan stego sinyalleri tespit etmek üzere önerilmiş olsa da tüm ses sinyalleri türleri için performans testleri gerçekleştirilmiştir. Kaotik özellik vektörü TIMIT konuşma veri seti gibi erkek ve bayanlara ait pek çok farklı aksanı barındıran zorlu veri setleri için bile oldukça yüksek başarıma sahip değerler elde edilmiştir. Fakat aynı başarım seviyeleri, müzik eserleri ve müzik aletleri için geçerli değildir. Bu durumun sebebi, müzik eserlerinin birden fazla ses kaynağından oluşması sebebiyle, sinyal boyutunun (d, degrees-of-freedom) çok yüksek seviyelerde olmasıdır. Çok yüksek boyutlu sinyaller içerisine gizlenen veri örtü sinyalini birkaç derece kadar arttıracaktır. Bu durum ise kaotik özellikler tarafından örtü sinyali ile stego sinyalin ayırt edilebilirliğini kötü yönde etkileyecektir. Zira kaotik özellikler konuşma seslerindeki gibi, 3 ila 7 arasında boyutlara sahip ses sinyallerinde birkaç derece artışları hissedebilmektedir.

Ayrıca müzik aletleri ile yapılan performans testlerinde, ses sinyalindeki sessiz boşlukların steganaliz performansını kötü yönde oldukça etkilediği ortaya çıkmıştır. Bu durumun birinci sebebi, sessiz kısımların kaotik özelliklerin hesaplanmasında hatalara sebep (çok büyük veya çok küçük değerlerin hesaplanması ve sıfıra bölünme hataları gibi) olmasıdır. Örtü sinyali ve stego sinyal için oluşabilen bu durum iki sinyalin ayırt ediciliğini azaltmaktadır. Benzer şekilde sessiz boşluklar örtü sinyali ve stego sinyal için kaotik özelliklerin yakın değerlerde hesaplanmasına dolayısı ile iki sinyalin ayırt ediciliği negatif yönde etkilenmektedir. Müzik aletleri ses kayıtlarından sessiz kısımların çıkartılması ile, beklenen performans değerlerine yakın başarım değerleri elde edilmiş fakat yine de konuşma sesleri için elde edilen performans değerlerine ulaşılamamıştır. Bunun nedeni ise, boşlukların çıkartılması ile çok daha kısa sinyaller (konuşma sesleri 4 saniye uzunluğunda idi) üzerinden kaotik özelliklerin hesaplanmasıdır. Tezin başında da belirtildiği üzere optimum değer olan 4 saniye süresi, kaotik özelliklerin hesaplanabilmesi için yeterince uzun, yarı periyodikliğin sağlanması için yeterince kısa olan optimum değerdir. Bu sürenin kısalması ile kaotik özellik değerleri tam olarak hesaplanamadan (uygun değere oturmadan) işlem yarıda kesilmiş gibi olmaktadır.

Önerilen steganalizörün müzik aletleri kayıtlarında yaşanan düşük performans değerlerinin arttırılması için yapılan özel çalışma, ses kayıtlarındaki sessiz boşlukların

elenmesidir. Gerçekten de ses sinyallerinden boş kısımların elenmesi ile %20'lere ulaşan başarım iyileştirmeleri görülmüştür.

Konuşma sesleri için önerilen bir iyileştirme de kaotik fenomenin asıl olarak görüldüğü sesli harflerin seçilerek yalnızca bu kısımlar üzerinde kaotik özellik değerlerinin hesaplanmasıdır. Bu yaklaşımda başarım değerlerinin yaklaşık %2 iyileştiği gözlemlenmiştir. Fakat bu iyileştirme önerisinin hayata geçebilmesi için, ses kayıtlarındaki yarı-periyodik veya kaotik kısımları otomatik olarak algılayan ve diğer kısımları eleyen bir işleme ihtiyaç duyulmaktadır. Yapılan çalışmada bu işlem, manuel olarak gerçekleştirilmiştir.

Önerilen kaotik özellik vektörü, şüpheli sinyalin elimizde olduğu ve steganografi yönteminin bilindiği steganaliz saldırı tipi için önerilmiş bir özellik vektörüdür. Yapılan çalışma boyunca da performans değerleri bu şekilde hesaplanmış ve her bir steganografi tekniği için başarım değerleri ayrı ayrı verilmiştir. Önerilen özellik vektörünün evrensel steganalizör olarak test edildiği çalışmalar Çizelge 4.5 ve Çizelge 4.9'da verilmektedir. Evrensel steganalizör (Steganografi yönteminin bilinmediği, elimizde sadece şüpheli sinyalin bulunduğu durum) olarak orta seviyede başarım sonuçları veren önerilen özellik vektörü, özellikle *COX* ve *ECHO* gibi steganografi tekniklerinde yaşadığı düşük başarım değerlerinin kaotik olmayan özellik elemanlarının (örneğin; *AQM* veya *CIAQM*) eklenerek yok edilmesi ile, oluşturulan bu yeni özellik vektörü rahatlıkla evrensel steganalizör olarak kullanılabilecektir. Hattı zatında bugün için evrensel steganalizör olarak tek başına yüksek değerlerde başarım değerleri üretebilen tek bir kaynak bulunmamaktadır.

Sonuç olarak özetle günümüzde oldukça popüler olan steganaliz çalışmalarının ses verisi için yapılan tespit çalışmalarında kullanılmak üzere konuşma sesi ve müzik aletleri sesleri için sinyallerin kaotik özelliklerini kullanan bir özellik vektörü önerilmiştir. Önerilen özellik vektörünün ayırt ediciliği yapılan benzetimler sonucunda elde edilen nümerik sonuçlar ile de geçerliliği literatürde önerilmiş diğer ses steganalizörleri ile karşılaştırmalı olarak ortaya konulmuştur. Ayrıca tezde ortaya konulan sonuçların bir kısmı Koçal ve arkadaşları tarafından 2005 ve 2008 yıllarında, Yürüklü ve arkadaşları tarafından 2012 ve 2013 yıllarında yapılan yayınlar ile bilim dünyasında yayınlanmıştır.

KAYNAKLAR

Anonim, 2006-a. Mp3Stego. http://www.petitcolas.net/fabien/steganography/mp3stego.-(Erişim Tarihi: 16.Şubat.2006).

Anonim, 2006-b. SQAM (Sound Quality Assessment Material). http://sound.media.mit.edu/mpeg4/audio/sqam/ -(Erişim Tarihi: 12.Kasım.2006).

Anonim, 2006-c. Steganos. www.steganos.com.-(Erişim Tarihi: 15.Ekim.2006).

Anonim, 2006-d. TIMIT Speech Database. http://www.ldc.upenn.edu/Catalog/CatalogEntry.jsp?catalogId=LDC93S1.-(Erişim Tarihi: 03.Kasım.2006).

Anonim, 2011-a. Goldwave. http://www.goldwave.com/ -(Erişim Tarihi: 20.Ağustos.2011).

Anonim, 2011-b. JPL's Wireless Communication Reference Website. http://wireless.per.nl/reference/chaptr04/speech.htm.-(Erişim Tarihi: 20.Ağustos.2011).

Anonim, 2011-c. OSU-SVM Matlab Toolbox. http://sourceforge.net/projects/svm/ -(Erişim Tarihi: 16.Ağustos.2011).

ABARBANEL, H. D. I. 1996. Analysis of Observed Chaotic Data. New York: Springer-Verlag.

ALTUN, O., G. SHARMA, M. CELIK, M. STERLING, E. TITLEBAUM, M. BOCKO. 2005. Morphological Steganalysis of Audio Signals and the Principle of Diminishing Marginal Distortions. *IEEE Int. Conf. on Acoustics, Speech, and Signal Processing, Proceedings. (ICASSP '05).* 18-23 Mart 2005. Vol.2: 21-24.

AVCIBAŞ, İ. 2006. Audio Steganalysis with Content-Independent Distortion Measures. *IEEE Signal Processing Letters,* Vol.13, No.12, pp. 92-95.

BANBROOK, M., S. McLAUGHLIN. 1994. Is speech chaotic?: invariant geometrical measures for speech data. *IEE Colloquium on Exploiting Chaos in Signal Processing*. 8/1 – 810.

BANBROOK, M., S. McLAUGHLIN. 1999. Speech Characterization and Synthesis by Nonlinear Methods. *IEEE Transactions on Speech and Audio Processing,* Vol. 7, No. 1, pp. 1-17.

BENDER, W., D. GRUHL, N. MORIMOTO, A LU. 1996. Techniques for data hiding. *IBM Systems Journal,* vol. 35, no: 3&4, pp. 313-336.

CANAN, S., **2011.** Kaos: Kendinle Karışık mısın?. NTV Bilim Dergisi: 22-27.

COX, I. J., J. KILIAN, F.T. LEIGHTON, T. SHAMOON. 1997. Secure spread spectrum watermarking for multimedia. *IEEE Tr. Image Proc.*, vol 6, pp. 1673 – 1687.

FRIDRICH, J., M. GOLJAN. 2002. Practical Steganalysis of Digital Images - State of the Art. *Proc. SPIE Photonics West*, Vol. 4675, 1-13.

FRIDRICH, J., M. GOLJAN. 2003. Digital Image Steganography Using Stochastic Modulation. *Proc. SPIE Electronic Imaging,* Santa Clara, CA, pp. 191-202.

HEGGER, R., H. KANTZ, T. SCHREIBER. 1999. Practical Implementation of Nonlinear Time Series Methods: The TISEAN Package. Chaos, Vol. 9, pp. 413-435.

HETZL, S. 2006. Steghide. http://steghide.sourceforge.net.-(Erişim Tarihi: 22.Aralık.2006).

HILBORN, R. 2000. Chaos and Nonlinear Dynamics. Oxford University Press, 2. ed.

JOHNSON, M.K., S. LYU, H. FARID. 2005. Steganalysis of Recorded Speech. *Proc. SPIE Symposium on Electronic Imaging,* San Jose, CA.

KATZENBEISSER S., F.A.P. PETITCOLAS. 2000. Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, INC. 685 Canton Street Norwood, MA 02062.

KENNEL, M. B., H. D. I. ABARBANEL. 2002. False neighbors and false strands: A reliable minimum embedding dimension algorithm. *Physical Review E,* Vol. 66, 026209.

KOÇAL, O.H., E. YURUKLU, I. AVCIBAS. 2008. Chaotic-type features for Speech Steganalysis. *IEEE Transactions on Information Forensics and Security.* Vol:3-4 : 651-661.

KOÇAL, O.H., E. YURUKLU, I. AVCIBAS. 2005. Speech Steganalysis Usıng Chaotic-Type Features. *13th European Signal Processing Conference, EUSIPCO' 2005.* Antalya.

KOKKINOS, I., P. MARAGOS. 2005. Nonlinear Speech Analysis Using Models for Chaotic Systems. *IEEE Transactions on Speech and Audio Processing,* Vol. 13, No. 6, pp. 1098-1109.

KUTUCU, H., M. KAYA. 2002. Steganography. Cryptography and Network Security Term Project. Ege University International Computer Institute.

MARTINEZ, F., A. GUILLAMON, J.C. ALCARAZ, M.C. ALCARAZ. 2002. Detection of Chaotic Behaviour in Speech Signals Using the Largest Lyapunov Exponent. *14th International Conference on Digital Signal Processing 2002, DSP 2002,* Vol. 1, pp. 317-320, 1-3.

OZER, H., I. AVCIBAS, B. SANKUR, N. MEMON. 2003. Steganalysis of Audio Based on Audio Quality Metrics. *Proc. SPIE, Security and Watermarking of Multimedia Contents V,* Vol.5020: 55-66.

ÖZER, H., B. SANKUR, N. MEMON, İ. AVCIBAŞ. 2006. Detection of Audio Covert Channels Using Statistical Footprints of Hidden Messages. *Digital Signal Processing, Vol.*16, pp. 389-401.

PACKARD, N. H., J. P. CRUTCHFIELD, R. S. SHAW, J. D. FARMER. 1980. Geometry from time series. *Phys. Rev. Lett.,* Vol. 45, p. 712.

PETITCOLAS F.A.P., R.J. ANDERSON, M.G. KUHN. 1999. Information Hiding– A Survey. *Proceedings of the IEEE, Special Issue on Protection of Multimedia Content,* 87(7):1062-1078.

PITSIKALIS, V., P. MARAGOS. 2002. Speech Analysis and Feature Extraction Using Chaotic Models. *IEEE International Conference on Acoustics, Speech, and Signal Processing Proceedings. (ICASSP '02).* Vol.1, pp. 533-536.

PUDIL, P., J. NOVOVICOVA, J. KITTLER. 1994. Floating Search Methods in Feature Selection. *Pattern Recognition Lett.* Vol 15, pp. 1119-1125.

REPP, H. 2006. Hide4PGP. www.heinz-repp.onlinehome.de/Hide4PGP.htm.-(Erişim Tarihi: 04.Kasım.2006).

RENCHER, A. C. 1995. Methods of Multivariate Analysis. New York, John Wiley. ch. 6, 10.

SCHREIBER, T, A. SCHMITZ. 1996. Improved surrogate data for nonlinearity tests. *Phys. Rev. Lett.* vol.77:635-638.

SCHREIBER, T, A. SCHMITZ. 2000. Surrogate time series. *Physica D,* vol.142(3-4):346-382.

ŞAHİN, A., E. BULUŞ, M.T. SAKALLI. 2006. 24-Bit Renkli Resimler Üzerinde En Önemsiz Bite Ekleme Yöntemini Kullanarak Bilgi Gizleme. *Trakya Univ J Sci*, 7(1): 17-22.

TAKENS, F. 1980. Detecting strange attractors in turbulence. *Dynamical Systems and Turbulence,* vol. 898, p. 365.

THEILER, J., S. EUBANK, A. LONGTIN, B. GALDRIKIAN, J. FARMER. 1992. Testing for nonlinearity in time series: the method of surrogate data. *Physica D,* vol.58:77-94.

WESTFELD, A.P., A. PFITZMANN. 1999. Attacks on steganographic systems. Information Hiding, LNCS 1768, Springer-Verlag Heidelberg, 1999, 61-66.

WESTFELD, A.P. 2003. Detecting Low Embedding Rates. *Fabien A. P. Petitcolas (Ed.): Information Hiding. 5th International Workshop, IH 2002 Noordwijkerhout,* pp. 324–339, The Netherlands, 7-9 Ekim 2002. Springer-Verlag Berlin Heidelberg, 2003.

WOHLGEMUTH, S. 2002. Steganography and Watermarking. Lecture to University of Freiburg. http://www.informatika.org/~rinaldi/Kriptografi/20020108Steganography Watermarking.4on1.pdf-(Erişim Tarihi: 08.Temmuz.2011).

WOLD, H.O.A. 1938. A Study in the Analysis of Stationary Time Series, Almqvist and Wiksell: Uppsala.

YILMAZ, D., N.F. GÜLER. 2006. Kaotik Zaman Serisinin Analizi Üzerine Bir Araştırma. *Gazi Üniv. Müh. Mim. Fak. Der.* Cilt 21, No 4, 759-779.

YÜRÜKLÜ, E., O. H. KOÇAL, E. DİLAVEROĞLU. 2012. Speech Steganalysis Using Delay Vector Variance Based Features. *International Conference on Applied and Computational Mathematics (ICACM) – 2012.* Ankara.

YÜRÜKLÜ, E., O. H. KOÇAL, E. DİLAVEROĞLU. 2013. A New Approach for Speech Audio Steganalysis Using Delay Vector Variance Method. *Uludağ University Journal of The Faculty of Engineering and Architecture*, basım aşamasında.

EKLER

EK-1

```
%% file: swr.m
function swr=swr(a,b)
a=wavread(a);
b=wavread(b);
sizea=prod(size(a));
sizeb=prod(size(b));
absfark=min(sizea, sizeb);
payda=mean((b(1:absfark)-a(1:absfark)).^2);
pay=mean(a(1:absfark).^2);
swr=10*log10(pay/payda);
```

EK-2

```
%% file: mutin.m
function I=mutin(wavedata)
[sizex sizey]=size(wavedata);
if sizex==1
  wavedata=wavedata';
end

data=wavedata*20;
%data=ind;
%data=data-min(data)+1;
data=round(data-min(data))+1;
N=length(data);
data=data';
I=0;
for T=0:500
  prx=zeros(1,max(data));
for i=1:N
  prx(data(i))=prx(data(i))+1;
end

matris=[data(1:N-T) ; data(T+1:N)];

prxy=zeros(max(data),max(data));

for i=1:N-T
  prxy(matris(1,i),matris(2,i))=prxy(matris(1,i),matris(2,i))+1;
end
I(T+1)=0;
[indx indy]=find(prxy);
for i=1:length(indx)
  prxytemp=prxy(indx(i),indy(i));
  I(T+1)=I(T+1)+(prxytemp*log2(prxytemp/(prx(indx(i))*prx(indy(i)))));
end
end
I=I-min(I)+1;



figure
stem((0:length(I)-1),I);
```

EK-3

```
%% file: surdatafft.m
function [vectorout]=surrdatafft(vectorin)

vectorln=length(vectorin);
vectorfft=fft(vectorin);
nrel=ceil((vectorln-1)/2)+1;
nchange=vectorln-nrel;
relvector=zeros(nrel,1);
relvector=vectorfft(1:nrel);
randangles=rand(nchange,1)*2*pi;
relvector(2:nchange+1)=(cos(randangles)+sin(randangles)*i).*...
  abs(vectorfft(2:nchange+1));
vectorrandom(1:nrel)=relvector;
for l=vectorln:-1:nrel+1
  j=vectorln-l+2;
  vectorrandom(l)=conj(relvector(j));
end

vectorout=real(ifft(vectorrandom));
```

EK-4

```
%%file: denelin_feat.m
clear all;
hangi=input('Steganaliz Türü:');
str1=strcat('wd',hangi,'.txt');
str2=strcat('wd',hangi,'emb.txt');
FEAT=input('FEAT=');
sinif1=[];
sinif1temp=load(str1);
sinif2=[];
sinif2temp=load(str2);
sinif1=sinif1temp(:,FEAT);
sinif2=sinif2temp(:,FEAT);
clear sinif1temp;
clear sinif2temp;
ln=length(FEAT);
[sizex1 sizey1]=size(sinif1);
[sizex2 sizey2]=size(sinif2);
if (sizex1~=sizex2)
   disp('Sınıfların boyutları eşit değil, Kontrol ettikten sonra tekrar deneyiniz...');
   break;
end
if mod((sizex1),2)==1
   disp('Dizinin uzunluğu ikiye tam bölünebilir olmalıdır')
   sinif1temp=sinif1(1:sizex1-1,:);
    sinif2temp=sinif2(1:sizex1-1,:);
    clear sinif1;
   clear sinif2;
   sinif1=sinif1temp;
   sinif2=sinif2temp;
   clear sinif1temp;
   clear sinif2temp;
   sizex=(sizex1-1)/2;
else
   sizex=sizex1/2;
end

order=randperm(sizex*2);
%pause

clear sizex1,sizex2,sizey1,sizey2;
%sizex=150;
%karistir;

% TR=[1:sizex]     %egitimde kullanilacak veri sayisi
% TS=[(sizex+1):2*sizex]   %testte kullanilacak veri sayisi
```

```
TR=[order(1:sizex)]     %egitimde kullanilacak veri sayisi
TS=[order((sizex+1):2*sizex)]   %testte kullanilacak veri sayisi
dataor=[sinif1(TR,:);sinif2(TR,:)]
datadg=[sinif1(TS,:);sinif2(TS,:)]

oznitelik_sayisi=ln.....; %Secmek istedigin maksimum oznitelik sayisi. Benim
oznitelik vektorum 118 oznitelikten olusuyordu.Ben
                % en fazla 60 oznitelik secildiginde durumun ne oldugunu gormek cin 60
yazdim.

fp_cs=fopen('Sonuclar.txt','w'); % Sonuclar bu dosyaya yaziliyor.


 for i=1:oznitelik_sayisi

    fprintf('%d Öznitelik seçildiginde Sonuç',i)
    [fa,miss,out(i)]=fSFSbyLin1_feat(dataor,datadg,i,ln,sizex)
    fprintf(fp_cs,'%d.) fa=%d miss=%d basarim=%f\n',i,fa,miss,out(i)); %fa yanlis alarm,
miss kacirma

end
fclose('all');
```

```
%% file: fSFbyLin1_feat.m
function [falsealarm,misdec,out,features] =
fSFSbyLin1(dataor,datadg,kfinal,nfeat,sizex)

tot = 2*sizex; % Eğitim ve test için kullanılacak toplam veri sayisi (bir sınıf için)
Ntrn = sizex; % Eğitimci veri sayisi (bir sınıf için)
%nfeat=42;  %oznitelik sayisi


tektek = zeros(1,nfeat);
for kk = 1:nfeat, % her bir öznitelik için teker teker eğitim ve test yaparak başarım
oranlarını hesaplama
    tektek(kk) = lin(dataor(:,kk),datadg(:,kk),sizex);
end;

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
% en iyi ikiliyi secme
k1 = find(tektek==max(tektek)); % en iyisi
eklenen(1) = k1(1,1);
eklenen = eniyieklelin(eklenen,dataor,datadg,nfeat,Ntrn,tot,sizex); % en iyi ikinciyi ekle
```

```
if length(eklenen)==kfinal % eğer sadece iki öznitelik seçilmesi istenmişse
    step1 = 0;
    step2 = 1;
    step3 = 1;

    indx = length(eklenen);
    or = dataor(:,eklenen(1:indx));
    dg = datadg(:,eklenen(1:indx));
    testor = lin(or,dg,sizex);

    features = eklenen
    out = testor;

    [rate,cordecdg,cordecor] = lin(or,dg,sizex);
    falsealarm =  cordecdg
    misdec =cordecor
%    sonuc=[falsealarm misdec ]
    return;
else
    step1 = 1;
    step2 = 1;
    step3 = 1;
end;
cnt = 1;


while ( (step1 == 1) | (step2 == 1) | (step2 == 1) )



%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
    % STEP1:en iyi n.ciyi ekle
    if step1==1
        eklenen = eniyieklelin(eklenen,dataor,datadg,nfeat,Ntrn,tot,sizex);
        indx = length(eklenen);
        or = dataor(:,eklenen(1:indx));
        dg = datadg(:,eklenen(1:indx));
        testor = lin(or,dg,sizex); %testh(or,dg,Ntrn,tot,0); % en son eklenenle beraber
basari.

        step1=0;
        step2=1;
        step3=1;
    end;

    % end of STEP1
```

```
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
    cnt = cnt+1;
    if cnt>12*kfinal
        disp('Break...')
        break;
    end;


%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
        % STEP2
        % en son eklenen haricidekiler birer birer cikarak test et
        while ( (step2 == 1) | (step3 == 1) )
            step2 = 0;

            indx = length(eklenen);
            testka = zeros(1,indx-1);
            or = dataor(:,eklenen(2:indx));
            dg = datadg(:,eklenen(2:indx));
            testka(1) = lin(or,dg,sizex); %testh(or,dg,Ntrn,tot,0); % ilki cikariyoruz
kalanlarla test

            for ii=2:indx-1 % birer birer cikarma ve kalanlarla test (son eklenen haric)
                or = [dataor(:,eklenen(1:ii-1)) dataor(:,eklenen(ii+1:indx))];
                dg = [datadg(:,eklenen(1:ii-1)) datadg(:,eklenen(ii+1:indx))];
                testka(ii) = lin(or,dg,sizex); %testh(or,dg,Ntrn,tot,0);
            end;

            if max(testka) > testor % herhangi biri (en iyisi), originalden daha iyi ise

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
                % once onu kumeden cikar
                ttemp = find(testka == max(testka));
                ttemp = ttemp(1,1);
                if ttemp == 1
                    ektemp = eklenen(2:indx);
                else
                    ektemp = [eklenen(1:ttemp-1) eklenen(ttemp+1:indx)];
                end;
                eklenen = ektemp;

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

                if length(ektemp) == 2 % sonra eger k=2 ise bir nolu stepe don
```

```
        step1 = 1;
        step2 = 0;
        step3 = 0;
        %continue; % go to step1
      else
        step1 = 0;
        step2 = 0;
        step3 = 1; % go to step3
      end;

    else  % if max(teska), yani hic birini cikarinca daha iyi olmuyorsa

      if length(eklenen) == kfinal, % eger k son degere ulasmissa sonlandir
        step1 = 0;
        step2 = 0;
        step3 = 0;
        break;
      else
        step1 = 1; % eger hic biri iyi degilse eklenenle beraber tekrar step1'e don
        step2 = 0;
        step3 = 0;
        %continue;
      end;

    end % if max(teska)
  %% end of STEP2

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

  if step1 == 1
    step2 = 0;
    step3 = 0;
   % continue; % step1'e don
  end

  while (step3 == 1)
      % write step3
      indx = length(eklenen);
      or = dataor(:,eklenen(1:indx));
      dg = datadg(:,eklenen(1:indx));
      testor = lin(or,dg,sizex); %testh(or,dg,Ntrn,tot,0);
      st3kalan = birercikarlin(dataor,datadg,eklenen,Ntrn,tot,sizex); % birer birer
cikar

      if max(st3kalan)>testor % eger herhangi biri (en kotusu) cikinca daha iyi
oluyorsa
```

```
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
          % once onu kumeden cikar
          ttemp = find(st3kalan == max(st3kalan));
          ttemp = ttemp(1,1);
          if ttemp == 1,
            ektemp = eklenen(2:indx);
          else if ektemp == indx,
              ektemp = eklenen(1:indx-1);
            else
              ektemp = [eklenen(1:ttemp-1) eklenen(ttemp+1:indx)];
            end;
          end;
          eklenen = ektemp;

%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
          if length(eklenen) == 2,
            step1 = 1; % step1 e git,
            step2 = 0;
            step3 = 0;
            %continue;
          else
            step1 = 0;
            step2 = 0; % step2'ye git,
            step3 = 1; % step3'ye git,
          end
        else  % hic biri iyi degilse hepsi kalsin ve step1'e git

          if length(eklenen) == kfinal % ise sonlandir
            step1=0;
            step2=0;
            step3=0;
            break;
          else
            step1=1; % step1'e don
            step2=0;
            step3=0;
            %continue;
          end

        end; % if max(st3kalan)

    end; % while step3==1

  end; % while step2
```

```
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
end; % while step1

indx = length(eklenen);
or = dataor(:,eklenen(1:indx));
dg = datadg(:,eklenen(1:indx));
testor = lin(or,dg,sizex);

features = eklenen
out = testor;

[rate,cordecdg,cordecor] = lin(or,dg,sizex);
falsealarm = cordecdg;
misdec = cordecor;

%sonuc=[falsealarm misdec]
%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
```

```
%% file: lin.m (SVM)
function [basarim,fa,miss]=lin(TrainSteganos,TestSteganos,sizex),
labels=[-1*ones(1,sizex) ones(1,sizex)];

Gamma=4; %RBF
Degree = 4; %Polinom 9
C=1;  % 0.3
net = svml('echo.txt', 'Kernel', 0, 'C', 1);
%net = svml('echo.txt', 'Kernel', 1, 'C', C, 'KernelParam', Degree);
%net = svml('echo.txt', 'Kernel', 2, 'C', 1,'KernelParam',Gamma);
%net = svml('echo.txt', 'Kernel', 3, 'C', 1, 'KernelParam', [1, 2]);

net = svmltrain(net, TrainSteganos, labels');

Ypred = svmlfwd(net, TestSteganos,labels');


fa=length(Ypred(1:sizex)>0);
md=length(Ypred((sizex+1):(2*sizex))<0);
basarim=1-(fa+md)/(2*sizex);
```

```
%% file: lin.m (Lineer Sınıflandırıcı)
function [basarim,fa,miss]=lin(TrainSteganos,TestSteganos,sizex),
```

```
TR=[1:sizex];
y=ones(1, 2*max(TR));
y(TR)=-1;

ZZ=TrainSteganos'*TrainSteganos;
alfa=inv(ZZ)*(TrainSteganos'*y');

for i=1:2*sizex
  deger(i)=alfa'*TestSteganos(i,:)';
end

TH=0;
fa=size(find(deger(1:sizex)>=TH),2);
miss=size(find(deger((sizex+1):2*sizex)<TH),2);
basarim=1-((fa+miss)/(2*sizex));
```

ÖZGEÇMİŞ

Adı Soyadı : Emrah Yürüklü

Doğum Yeri ve Tarihi : Bursa, 28.Ekim.1979

Yabancı Dili : İngilizce, İtalyanca

Eğitim Durumu (Kurum ve Yıl)

Lise : Bursa Erkek Lisesi, 1993-1997

Lisans : Uludağ Üniversitesi, 1997-2001

Yüksek Lisans : Uludağ Üniversitesi, 2001-2004

Doktora : Uludağ Üniversitesi, 2006-2013

Çalıştığı Kurum/Kurumlar ve Yıl :

Uludağ Üniversitesi Mühendislik-Mimarlık Fakültesi Elektronik Mühendisliği Bölümü, 2002-2008

TOFAŞ Türk Otomobil Fab. A.Ş. ArGe Departmanı, 2008-

İletişim (e-posta) : emrah.yuruklu@gmail.com

Tez ile İlgili Yayınları :

KOÇAL, O.H., E. YÜRÜKLÜ, İ. AVCIBAŞ. 2005. Speech Steganalysis Using Chaotic-Type Features. *13th European Signal Processing Conference, EUSIPCO' 2005.* Antalya.

KOÇAL, O.H., E. YÜRÜKLU, İ. AVCIBAŞ. 2008. Chaotic-type features for Speech Steganalysis. *IEEE Transactions on Information Forensics and Security.* Vol:3-4 : pp.651-661.

YÜRÜKLÜ, E., O. H. KOÇAL, E. DİLAVEROĞLU. 2012. Speech Steganalysis Using Delay Vector Variance Based Features. *International Conference on Applied and Computational Mathematics (ICACM) – 2012.* Ankara.

YÜRÜKLÜ, E., O. H. KOÇAL, E. DİLAVEROĞLU. 2013. A New Approach for Speech Audio Steganalysis Using Delay Vector Variance Method. *Uludağ University Journal of The Faculty of Engineering and Architecture*, basım aşamasında.

Tez ile İlgili Olmayan Yayınları :

KOÇYİĞİT, İ., E. YÜRÜKLÜ. 2001. The ERICA Algorithm for ABR Service in ATM Networks. *ELECO 2001*. Bursa.

YAĞIMLI, M., E. YÜRÜKLÜ. 2006. Fiber Optik Sensörler ve Optik Jiroskop. *Deniz Harp Okulu Bülteni.*

YÜRÜKLÜ, E, B. ÇAYIR, T. ACARMAN. 2009. Low Cost Driver Monitoring and Warning System Development. *Intelligent Vehicles Symposium.* China.

ÇAYIR, B., T. ACARMAN, E. YÜRÜKLÜ. 2009. Driver Monitoring and Warning System Development. *16th Intelligent Transport Systems World Congress 2009.* Stockholm.

ACARMAN, T., B. ÇAYIR, E. YÜKSEL, E. YÜRÜKLÜ. 2010. Development of an Active Safety System. *Otomotiv Teknolojileri Kongresi - OTEKON 2010.* Bursa.

YENİKAYA, G., E. DÜVEN, A. ÜZGEÇ, E. YÜRÜKLÜ. 2010. Sürücü Davranış Karakteristiklerinin Tanılanması için Görü Temelli Bir Sürüş Sisteminin Tasarlanması. *Otomotiv Teknolojileri Kongresi - OTEKON 2010.* Bursa.

DEMİRCİ, A., E.G. SCHMIDT, E. YURUKLU, U. KARAKAYA. 2010. FlexRay Araçiçi Haberleşme Ağlarının Deneysel Başarım Değerlendirmesi. *Otomotiv Teknolojileri Kongresi - OTEKON 2010.* Bursa.

SCHMIDT, K., E.G. SCHMIDT, A. DEMIRCI, E. YURUKLU, U. KARAKAYA, 2010. An Experimental Study of the FlexRay Dynamic Segment. *IFAC Symposium Advances in Automotive Control, AAC2010.*

SCHMIDT, E. G., M. ALKAN, K. SCHMIDT, E. YURUKLU, U. KARAKAYA. 2010. Performance Evaluation of FlexRay/CAN Networks Interconnected by a Gateway. *IEEE Symposium on Industrial Embedded Systems - SIES 2010.*

YÜRÜKLÜ, E., O. H. KOÇAL. 2012. Kendi Kendini Düzenleyen Haritalar Yöntemiyle Sesli Harflerin Sınıflandırılması ve Tanınması. *Uludağ Üniversitesi Mühendıslık-Mımarlık Fakültesı Dergısı, pp.1-6, Cilt 17, Sayı 1, Haziran 2012.*