T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YENİ BİR KAOS TABANLI KRİPTOLAMA SİSTEMİ VE UYGULAMASI

DOKTORA TEZİ

Ahmet Sertol KÖKSAL

Enstitü Anabilim Dalı	**:**	**ELEKTRONİK VE BİLGİSAYAR EĞİTİMİ**
Tez Danışmanı	**:**	**Yrd. Doç. Dr. Hayrettin EVİRGEN**

Kasım 2014

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

YENİ BİR KAOS TABANLI KRİPTOLAMA SİSTEMİ VE UYGULAMASI

DOKTORA TEZİ

Ahmet Sertol KÖKSAL

Enstitü Anabilim Dalı : ELEKTRONİK VE BİLGİSAYAR EĞİTİMİ

Bu tez 20/11/2014 tarihinde aşağıdaki jüri tarafından Oybirliği ile kabul edilmiştir.

Prof. Dr. **Feyzullah TEMURTAŞ** **Jüri Başkanı**	**Doç. Dr.** **Yılmaz UYAROĞLU** **Üye**	**Yrd. Doç. Dr.** **Hayrettin EVİRGEN** **Üye**
Doç. Dr. **Ahmet ZENGİN** **Üye**	**Yrd. Doç. Dr.** **Orhan ER** **Üye**	

ÖNSÖZ

Ağ güvenliği, geçmişten günümüze, üzerinde sürekli çalışılan, teknolojideki gelişmelerle paralel olarak yenilenen bir konudur. Günümüzde oldukça güvenli ağlar kurulmakla birlikte birçok ağa yapılan saldırılar sonucunda, bu konunun halen üzerinde çalışılması ve geliştirilmesi gerektiği görülmektedir. Ağ güvenliğinin sağlanmasında kriptolama sistemleri, güvenlik duvarları ve erişim denetimi, saldırı tespit sistemleri ve ağ izleme, antivirüs yazılımları, kimlik denetimi - sayısal imza vb. teknolojiler kullanılmaktadır. Gerek kablolu gerekse kablosuz ağlar için kullanılan bu teknolojiler için çok sayıda bilimsel çalışma yapılmıştır. Bu çalışmalar neticesinde farklı sistemler oluşturulmuş ve ağ güvenliği temin edilmeye çalışılmıştır.

Genel olarak, kriptolama sistemleri aktif ve pasif saldırılara karşı en iyi veri koruma yöntemi olarak kabul edilir. Son yıllarda kaos biliminin gelişimi ile birlikte kaos teorisi haberleşme sistemlerinde kullanılmaya başlanmış, veri gizleme ve kriptolama uygulamaları için farklı yaklaşımlarda bulunulmuştur.

Bu tez çalışmasında, modern ve hızlı ağlarda güvenliğin tesis edilmesi için kullanılabilecek yeni bir kaos tabanlı kriptolama sisteminin gerçekleştirilmesi amaçlanmaktadır.

Bu çalışmanın oluşmasında ve sonuçlandırılmasında her türlü bilgi ve desteğiyle yanımda olan değerli danışmanım Yrd. Doç. Dr. Hayrettin Evirgen'e; katkılarından dolayı Sayın hocalarım Prof. Dr. Feyzullah Temurtaş, Prof. Dr. Hüseyin EKİZ, Doç. Dr. Yılmaz Uyaroğlu, Doç. Dr. Ahmet Zengin'e; çalışmalarım boyunca maddi ve manevi desteğini hiç esirgemeyen Yrd. Doç. Dr. Orhan Er ve Dr. Can Yüzkollar'a; sabır ve destekleri ile her zaman yanımda olan aileme teşekkürü bir borç bilirim.

İÇİNDEKİLER

SİMGELER VE KISALTMALAR LİSTESİ

AES	: Advanced encryption standard
AH	: Authentication header
ASCII	: American standard code for information interchange
CCA	: Chosen-Ciphertext Attack
COOK	: Chaotic on-off keying
CSK	: Chaos shift keying
CSMA/CD	: Carrier sense multiple access with collision detection
DCSK	: Differential chaos shift keying
DDoS	: Distributed denial-of-service
DES	: Data encryption standard
DoS	: Denial-of-service
EBCDIC	: Extended binary coded decimal interchange code
ECG	: Electrocardiographic
EKL	: Erişim kontrol listesi
ESP	: Encapsulating security payload
FDDI	: Fiber distributed data interface
IKE	: Internet key exchange
IPSec	: Internet protocol security
ISO	: International standards organization
LAN	: Local area network
MD5	: Message-digest algorithm
MIMO	: Multiple-input and multiple-output
OCSK	: Orthogonal chaos shift keying
OFDM	: Orthogonal frequency-division multiplexing
OSI	: Open systems international
PCM	: Pulse code modulation
RNG	: Random number generator

SC : Synchronization code

SHA : Secure hash algorithm

STP : Shielded twisted pair

TCP : Transmission control protocol

TPDU : Transport protocol data unit

UDP : User datagram protocol

UTP : Unshielded twisted pair

ŞEKİLLER LİSTESİ

TABLOLAR LİSTESİ

ÖZET

Anahtar kelimeler: Yerel Alan Ağları, Kaos, Güvenli Haberleşme, Kriptoloji

Ağ güvenliği, geçmişten günümüze, üzerinde sürekli çalışılan, teknolojideki gelişmelerle paralel olarak yenilenen bir konudur. Günümüzde oldukça güvenli ağlar kurulmakla birlikte birçok ağa yapılan saldırılar sonucunda, bu konunun halen üzerinde çalışılması ve geliştirilmesi gerektiği görülmektedir.

Bu çalışmada güvenli bir haberleşme sistemi oluşturulması amacıyla, şifreleme ve şifre çözme işlemlerini gerçekleştirecek yeni bir kaos tabanlı kriptolama sistemi önerilmiştir. Önerilen bu sistem dört ana bölümden oluşmaktadır: Rastgele sayı üreteci, kaotik hesaplama katmanı, kuantalama katmanı ve lojik karıştırıcı katmanı. Kaotik hesaplama katmanı, şifreleme anahtarını üretir. Rastgele sayı üreteci ise kaotik hesaplama katmanı için başlangıç koşullarını belirler. Kuantalama katmanında ikili sembol dönüşümü yapılan şifreleme anahtarı, lojik karıştırıcı katmanında şifresiz veri ile karıştırılarak veri şifrelenir. Şifre çözme işlemi, belirlenen başlangıç koşullarının, güvenli bir kanaldan alıcıya gönderilmesiyle başlar. Daha sonra alıcıda bulunan özdeş kriptolama sistemi, verici ile aynı şifreleme anahtarlarını üreterek şifresiz veriyi elde eder. Önerilen kriptolama sistemi ile iki farklı uygulama geliştirilmiştir. Yapılan bilgisayar simülasyonları ile sistemin başarımı her iki uygulama için ayrı ayrı test edilmiştir.

A NEW CHAOS BASED CRYPTOSYSTEM AND APPLICATION

SUMMARY

Key Words: Local Area Network, Chaos, Secure Communication, Cryptology

Network security which is constantly worked on from past to present is a subject that is renewed with the parallel of the technological developments. With the build of secure networks today, this subject is seen that it should be worked and developed as a result of attacks on several networks.

In this study, a new chaos-based cryptosystem has been proposed to perform the encryption and decryption process in order to establish a secure communication system. The poposed cryptosystem consists of four main parts: Random Number Generator, Chaotic Calculation layer, Quantizer layer and Logical Mixer layer. Chaotic Calculation layer generates encryption key. Random Number Generator determines initial conditions for chaotic calculation layer. In Quantizer layer encryption key transformation with binary symbol, in Logical Mixer layer, the data is encrypted by mixing with the plaintext. Decryption process starts with the defined initial values are sent to the receiver over a secure channel. The identical cryptosystem on the receiver generates the same encryption keys with the transmitter and then the plaintext is recovered. Two different applications with the proposed chaos-based cryptosystem has been developed. The performance of the system was tested separately for both applications with computer simulations performed.

BÖLÜM 1. GİRİŞ

1990'lardan itibaren bilgisayarlar, hayatın her alanına girmiş ve vazgeçilmez bir biçimde kullanılmaya başlanmıştır. Teknolojideki gelişmeler ve sağladığı kolaylıklar açısından bilgisayarların birbiri ile haberleşmesi de bu süreçte bir ihtiyaç halini almıştır. Bu ihtiyaç, bilgisayar ağlarının tüm dünyayı kapsayacak şekilde tesis edilmesini gerektirmiştir. İletişim, kamu hizmetleri, bankacılık işlemleri, güvenlik ve savunma sistemleri ve daha birçok alanda bilgisayar ağları kullanılarak işlemler yapılmaktadır.

Günümüzde kurumlar, şirketler ve onların farklı coğrafi bölgelerdeki şubeleri kendilerine ait bir ağ üzerinde işlemlerini yapmakta, servislerini sunmaktadırlar. Yapılan tüm bu işlemler sırasında kişiye-şirkete özel ve üçüncü şahısların görmemesi gereken gizli bilgiler de ağ üzerinden iletilmektedir. Bu sebeple ağ güvenliği teknolojinin bu yeniliklerinden faydalanabilmenin olmazsa olmaz ilk şartı olarak gösterilebilir.

Ağ güvenliği, geçmişten günümüze, üzerinde sürekli çalışılan, teknolojideki gelişmelerle paralel olarak yenilenen bir konudur. Günümüzde oldukça güvenli ağlar kurulmakla birlikte birçok ağa yapılan saldırılar sonucunda, bu konunun halen üzerinde çalışılması ve geliştirilmesi gereken bir konu olduğu sonucunu çıkarabiliriz.

Ağ güvenliğinin sağlanmasında şifreleme, güvenlik duvarları ve erişim denetimi, saldırı tespit sistemleri ve ağ izleme, antivirüs yazılımları, kimlik denetimi - sayısal imza vb. teknolojiler kullanılmaktadır. Gerek kablolu gerekse kablosuz ağlar için kullanılan bu teknolojiler için çok sayıda bilimsel çalışma yapılmıştır. Bu çalışmalar neticesinde farklı sistemler oluşturulmuş ve ağ güvenliği temin edilmeye çalışılmıştır.

90'lı yıllardan itibaren haberleşme sistemlerinde gizliliği sağlamak üzere yeni bir şifreleme teknolojisi olarak kaos teorisi kullanılmaya başlanmıştır. Ağda güvenliği sağlamada kullanılan Kaos, kısaca düzensizliğin düzeni şeklinde tanımlanan, doğrusal olmayan (nonlineer) olayları açıklamaya yarayan bir bilim dalıdır [1]. Kaotik sistemler, düzen ve düzensizliğin bir kombinasyonu olarak tanımlanabilecek geniş yelpazeli davranışlar göstermektedir. Kaotik sistemlerin garip ve öngörülemez davranışlarının temelde üç nedeni vardır: Birincisi; kaotik sistemler, bir önceki periyottan elde edilen çıktının bir sonraki periyot için girdi olarak kullanıldığı geri beslemeli sistemlerdir. Değişkenler arasındaki ilişki nonlineer olduğundan neden ve etki arasındaki ilişki orantılı değildir. İkincisi; önemsiz gibi görülen girdiler zaman ilerledikçe sistemin davranışını büyük ölçüde etkileyebilirler. Kaotik sistemlerin üçüncü özelliği ise, başlangıç koşullarına olan hassas bağımlılıktır [2]. Kaotik sistemlerin genel blok diyagramı Şekil 1.1'de verilmiştir.

Şekil 1.1. Kaotik sistemlerin genel blok diyagramı.

Kaotik sistemin çıkışında elde edilen kaotik işaretler periyodik değildir. Ancak zamanla tekrar eden kararlı fakat düzensiz bir salınım gösterirler. Bunlara ek olarak, başlangıç koşullarına olan hassas bağımlılıklarından dolayı kaotik işaretlerin tahmin edilmesi çok güçtür.

Kaotik sistemler haberleşme sistemlerinde bilgi işaretinin fiziksel ortamda gizli olarak iletilmesi ve/veya bilginin kriptolanması için yeni yaklaşımlar getirmiş ve bu konularda çok sayıda bilimsel çalışma yapılmış; yapılmaya da devam etmektedir.

1990'da Pecora ve Carroll'un [3] yaptığı çalışmalar, kaos teorisinin haberleşme sistemlerinde kullanılmasında bir dönüm noktası olmuş ve bundan sonra bu konuda çok sayıda bilimsel çalışma yapılmıştır. Bu çalışmalardan bazıları şöyledir:

Cuomo ve arkadaşları 1993 yılında, kaotik Lorenz sisteminin bir devre gerçekleştirmesini yapmış, güvenli haberleşme için kaotik maskeleme ve senkronizasyon hatalarının algılanması prensibine dayanan iki farklı yaklaşımda bulunmuştur [4].

Beritelli ve arkadaşları, paket anahtarlamalı ağlarda güvenli sayısal iletişim için yeni bir algoritma önermiştir. Önerilen bu çok katmanlı kaotik şifreleme algoritması IP protokolü üzerinden güvenli veri iletimi sunmaktadır ve bu çalışmada geliştirilen algoritmanın TLS protokolü içinde verimli bir şekilde uygulandığı gösterilmiştir [5].

Chien ve Liao, yaptıkları çalışmada kriptografi ve kaotik senkronizasyon tekniklerine dayalı güvenli bir sayısal iletişim sistemi önermektedir. Bu sistemde veri, kaotik modülatör adı verilen verici tarafından gönderilmekte ve kaotik demodülatör adı verilen alıcı tarafından şifresi çözülerek alınmaktadır. Alıcı ve vericinin senkronizasyonu, doğrusal olmayan bir observer tarafından sağlanmaktadır [6].

2003 yılında yaptıkları bir çalışma ile Guojie ve arkadaşları, CCA (Chosen-Ciphertext Attack) saldırılarına karşı, kaotik senkronizasyon temelli kaotik haberleşme sistemlerinin güvenlik özelliklerini analiz etmiş ve bu yöntemle haberleşme sistemi parametrelerinin (anahtarlar gibi) elde edilebileceğini göstermişlerdir [7].

Abel ve Schwarz, kaotik haberleşme yöntemlerini kapsamlı olarak ele almış; farklı klasik ve kaotik modülasyon ve demodülasyon türlerini sınıflandırarak karşılaştırmalı bir performans analizi gerçekleştirmiştir [8].

Memon, kaos senkronizasyonunu kullanarak, ağ ortamında bir sinyal şifreleme uygulaması gerçekleştirmiş; hem çevrimiçi hem çevrimdışı çalışma ortamları için detaylı analizler yapmış ve ağlar arasında bilgi kodlaması için kaos kullanımını teşvik edici sonuçlar elde etmiştir [9].

Chee ve Xu, sayısal veriyi şifrelemek için, projektif senkronizasyon olarak tanımlanan farklı bir kaotik senkronizasyon yöntemi geliştirmişlerdir. Rastgele üretilen sayılarla

kaotik maskeleme yaptıkları bu sisteme ait özelliklerin, karakteristik kriptanaliz yöntemleriyle elde edilemeyeceğini göstermişlerdir [10].

Khadra ve arkadaşları ise daha farklı bir çalışma ile dürtüsel senkronizasyon kullanan kaos tabanlı güvenli haberleşme sistemlerindeki iletim ve örnekleme gecikmelerini incelemişlerdir. Bu çalışma sonucunda, haberleşme sistemlerinde kaçınılmaz olan gecikme olaylarını kontrol edebilecek matematiksel bir çözüm önerisinde bulunmuşlardır [11].

Alvarez ve Li, 2004 yılında yaptıkları çalışma ile, bir ağ içinde, kaotik maskeleme ile şifrelenmiş verilerin elde edilebileceğini göstermeye çalışmışlar; 1993 yılında Cuomo ve arkadaşlarının önerdikleri kaotik haberleşme sistemi [4] üzerinde yaptıkları ciphertext filtreleme saldırılarıyla bunu başarmışlardır [12].

Bowong ve arkadaşları, parametre modülasyonu yapılan kaotik haberleşme sistemlerinin problemleri üzerinde bir çalışma yapmışlardır. Bu sistemde bilgi sinyali, kaotik sistemin bir parametresini modüle etmek için kullanılmakta; daha sonra, elde edilen kaotik sinyal demodüle edilmekte ve bilgi sinyali adaptif bir demodülatör kullanılarak elde edilmektedir. Bu çalışmada kaotik Chua devresi üzerinde adaptif observer temelli bir senkronizasyon tekniği geliştirilmiştir [13].

Dronov, 2005 yılında Maryland Üniversitesi'nde yaptığı doktora tezinde bilgi iletimi sistemlerinde kaosun kontrolü ve senkronizasyonu üzerine bilgiler vermiş, dinamik sistemlerin kaotik davranışlarını matematiksel olarak kapsamlı bir şekilde açıklamış ve uydu haberleşmesi için güvenli bir kaotik haberleşme sistemi önermiştir [14].

Robilliard ve arkadaşları, analog ve sayısal kaotik sinyal üreteçlerini kıyaslamış, analog kaos işareti ile sayısal bilgi iletimini gerçekleştirecek hibrid bir sistem tasarlamış ve bu sistemin performans analizlerini yapmışlardır [15].

Chang, 2009 yılında yayınlanan makalesinde sayısal bilgi iletimi için yeni bir haberleşme sistemi sunmuş, kaotik modülasyon için üç farklı kaos durum değişkenini kullanarak daha güvenli bir sistem elde etmeye çalışmıştır. [16].

Illing, kaotik darbe konum modülasyonu kullanarak geliştirilen yüksek hızlı sayısal bir optik haberleşme sistemi üzerinde kanal gürültüsü ve diğer bozulmaları incelemiş, böyle bir sistem için güçlü kaos haberleşmesinin yapılabileceği sonucuna varmıştır [17].

Wren ve Yang, hem veri iletim hızını hem de güvenliği artırmak amacıyla dikey kaotik vektör kaydırmalı anahtarlama modülasyonu (OCSK) kullanarak yeni bir sayısal haberleşme sistemi önermişlerdir [18].

Stork, ayrık zamanlı kaotik sistemler konusunda bazı çalışmalar yapmış, bu sistemlerin de sürekli zamanlı sistemlere benzer şekillerde kontrol edilebileceğini ve senkronize olabileceğini göstermiştir [19].

Kaotik sistemler kullanılarak görüntü-video şifreleme, kaotik şifreleme anahtarlarının oluşturulması ve kaos tabanlı kriptolama mekanizmaları konusunda çeşitli çalışmalar yapılmıştır [20-29].

Çok yakın geçmişte yapılan diğer çalışmalarda;

- DCSK modülasyonu ile güvenli kaotik haberleşmenin gerçekleştirilmesi [30],

- Mobil iletişim için MIMO-OFDM tabanlı kaotik bir haberleşme sistemi üzerinde güvenliğin sağlanması [31],

- Çok yönlü yayılım ortamları için kaos tabanlı kablosuz kanal kapasitesinin artırılması [32],

- Yarı iletken halka lazerler kullanarak kaos tabanlı güvenli bir haberleşme sistemi uygulaması [33],

- Renkli görüntülerin kaotik bir blok şifreleyici sistem tarafından şifrelenmesi [34],

- Sayısal ses iletim ağlarında gizliliği sağlamak amacıyla simetrik bir akış şifreleyicinin kaos tabanlı gerçekleştirimi [35],

- Biyomedikal alanında, ECG sinyallerinin şifrelenmesi için kaotik tabanlı bir şifreleme algoritması [36],

- Ağa yapılacak DDoS ataklarının tespiti ve önlenmesi amacıyla ağ trafiğinin kaos tabanlı bir sistem ile izlenmesi [37] vb. konular araştırılmıştır.

Yukarıda verilen referans çalışmalarda da görüldüğü üzere kaos teorisinin haberleşme sistemlerinde kullanılması konusunda yeni yaklaşımlar araştırılmış olup hepsinin temel hedefi ağda güvenliği sağlamak yani en basit anlamıyla verinin sadece istenen noktalara gizli bir şekilde gönderilmesini sağlamaktır. Bu gizliliğin sağlanması için şifreleme yapmak kaçınılmazdır. İki düğüm arasındaki haberleşmenin şifreli olarak yapılabilmesi için öncelikle bu iki düğümün şifreleme algoritmasını ve gerekiyorsa şifreleme - şifre çözme anahtarlarını bilmesi gerekmektedir.

Günümüzde sıklıkla kullanılan kablolu yerel ağlarda iletişimin çoğunlukla şifresiz olarak yapıldığı bir gerçektir. Bu durum büyük bir risk oluşturmaktadır. Bu riski elimine etmek amacıyla yeni nesil ağlarda şifreli iletişimin zorunlu kılınması düşünülmüş ve IPSec protokolü geliştirilmiştir. Bu protokol yeni nesil IPv6 ağlarında zorunlu tutulmaktadır. IPSec protokolü, ağ içinde uçtan uca güvenli (şifreli) iletişimin her cihaz tarafından yapılması prensibine dayanmaktadır. IPSec ile kullanılacak şifreleme ve anahtar paylaşımı algoritmaları üzerinde halen çalışmalar sürdürülmekle birlikte henüz tam güvenli ve kabul edilebilir bir yapı sunulamamıştır [38].

IPv6 ile birlikte IPSec, güvenlik açıkları için tam bir çözüm değildir. IPSec tehdit ve güvenlik önlemlerini azaltmak için ağ katmanı ile uygulama katmanı arasında şifreleme dönüşümleri gibi işlevleri sunar. Ancak malware, spam, erişim denetimi, saldırı tespit ve bunun gibi diğer güvenlik işlevlerini yerine getirmez. DoS atakları ve kanal gizleme IPSec'te halen mevcuttur [39].

Günümüzün popüler ağ teknolojilerinden olan servis kalitesi (QoS), çoklu yayın (Multicast) ve gezgin IP (Mobil-IP); IPSec ile birlikte kullanıldığında birçok problem ortaya çıkmaktadır. Örneğin IPSec uygulandığında, IP başlığında bulunan servis kalitesi alanları şifrelenmekte dolayısıyla bu alan anlaşılamaz hale gelmektedir, IPSec noktadan noktaya tasarlandığı için çoklu yayın desteklenmemektedir ve gezgin IP ile dinamik biçimde kurulması gereken sanal tüneller için düğümlerin elle yapılandırılması gerekmektedir. Aynı zamanda IPSec yapan düğümler için otomatik ve güvenli anahtar dağıtma yöntemleri geliştirilmelidir. Çünkü IPSec'te kullanılan IKE gibi mevcut protokoller günümüz için yetersiz kalmaktadır. Tüm bu problemler IPSec kapsamında üzerinde çalışılması gereken araştırma alanlarından yalnızca bazılarıdır [55].

Bir çok ağda halen şifresiz haberleşme yapılması, yeni nesil Ipv6 ağlarının henüz yaygın olarak kullanılmaması, IPSec protokolünün henüz yeterince kararlı bir yapıya kavuşmamış olması nedenleriyle ağ güvenliğinin sağlanması hususunda bu çalışma ile yeni bir yaklaşımda bulunulmaktadır. Bu çalışmanın amacı, yüksek seviyeli güvenlik sunan bir ağ oluşturmaktır. Bu amaç doğrultusunda, yeni bir kaos tabanlı kriptolama sisteminin oluşturulması hedeflenmiştir.

Önerilen kaos tabanlı kriptolama sistemi, iki adet kaotik sistemin birleşiminden oluşan yapısıyla diğer kaos tabanlı kriptolama sistemlerinden ayrılmaktadır. Bu şekilde, kaosun güçlü şifreleme ve gizleme karakteristiklerinden daha etkin biçimde yararlanılabileceği bu tez çalışmasında gösterilmeye çalışılmıştır.

Önerilen kriptolama sisteminin diğer bir özelliği, yoğun matematiksel işlemler ve döngülere gerek duymaması ve bu nedenle yüksek hızlı ağlarda kullanılabilir olmasıdır. Bununla birlikte, önerilen sistem, daha hızlı ve daha güvenli yapıların oluşturulması amacıyla gelecekte yapılacak çalışmalara ışık tutabilir.

Bu amaçlar doğrultusunda, birinci bölümde tezde ele alınan problem anlatılmış, tezin yazılış amaçlarına değinilmiştir.

İkinci bölümde, bilgisayar ağlarının yapısı ve bu ağlarda güvenlik konusu incelenmiş, güvenliğin sağlanmasında kullanılan geleneksel kriptolama sistemleri tanıtılmıştır.

Üçüncü bölümde, kaos teorisi ve kaosun haberleşme sistemlerinde kullanılması ile ilgili temel kavramlar anlatılmış; kaos tabanlı kriptolama sistemlerinin özellikleri hakkında bilgiler verilmiştir.

Dördüncü bölümde, önerilen kaos tabanlı kriptolama sistemi tanıtılmıştır. Bu sistemin şifreleme-şifre çözme bölümlerinde yapılan işlemler adım adım resim, grafik ve tablolarla açıklanmıştır. Ayrıca geliştirilen sistemin mevcut sistemlerden farkı da bu bölümde detaylı bir şekilde anlatılmaktadır.

Beşinci bölümde, önerilen kriptolama sistemi ile iki farklı uygulama yapılmış ve uygulama sonuçları verilmiştir. İlk uygulama ile görüntü şifreleme; ikinci uygulama ile bilgisayar haberleşmesinde veri şifreleme ve şifre çözme işlemleri, önerilen kriptolama sistemi ile başarıyla gerçekleştirilmiştir.

Altıncı bölümde, önerilen sistem hakkında tartışma ve önerilere yer verilmiştir.

BÖLÜM 2. BİLGİSAYAR AĞLARINDA GÜVENLİK

2.1. Giriş

Ağ güvenliği, birçok sektördeki önemli gelişmeleri içeren bilgilerin gizliliği üzerinde geçmişten günümüze sürekli çalışılan, teknolojideki gelişmelerle paralel olarak yenilenen bir bilimdir. Günümüzde üst düzey güvenli ağlar kurulmakla birlikte birçok ağa yapılan saldırılar sonucunda, bu konunun halen üzerinde çalışılması ve geliştirilmesi gerektiği görülmektedir.

İletişim ortamlarının yaygınlaşması ve kullanımının artması sonucunda elektronik ortamlarda bulunan bilgilerin her geçen gün katlanarak artmasından dolayı bilgi güvenliğinin sağlanması ihtiyacı kişisel veya kurumsal olarak en üst seviyelere çıkmıştır. Bunun önemli sebepleri iş veya günlük yaşamın bir parçası haline gelen elektronik uygulamaların artması, ihtiyaç duyulan bilgilerin ağ sistemleri üzerinde paylaşımı, bilgiye her noktadan erişilebilirlik, bu ortamlarda meydana gelen açıkların büyük tehdit oluşturması ve en önemlisi kişisel ve kurumsal kayıplarda meydana gelen artışlar olarak sıralanabilir.

Günümüz dünyasında önemli kişisel veya kurumsal bilgilerin korunabilmesi, karşılaşabilecek risklerin en aza indirgenmesi ve iş sürekliliğinin sağlanması, bilgi paylaşımında kullandıkları ağların güvenliği ile paralellik göstermektedir. Kişisel ve kurumsal bilgi güvenliğinin yüksek seviyede sağlanması ile ilgili olarak literatürdeki mevcut kaynaklar araştırılıp incelendiğinde sınırsız bir güvenlik oluşmadığı görülmektedir. Amaç her zaman daha güvenli bir bilgi paylaşım ortamı sağlamaktır. Bu amaç doğrultusunda bu bölümde öncelikle yerel alan ağları tanıtılacaktır. Daha sonra bu ağlarda literatüre geçmiş mevcut güvenlik yöntemleri üzerinde durulacaktır.

2.2. Yerel Alan Ağları

Birden çok bilgisayarın birbirine bağlı olarak kullanılmasıyla oluşturulan çalışma biçimine bilgisayar ağı (computer network) denir [40]. Ağa bağlı tüm bilgisayarlar birbirleri ile iletişim kurabilirler, aynı kaynakları paylaşabilirler.

Bilgisayarlar bağlandıkları çalışma ortamlarının boyutlarına, eklenebilecek bilgisayar sayısına ve birim zamanda taşıdıkları bilgi miktarına göre farklı gruplar altında toplanır. Birkaç km boyunda ve belli bir organizasyona ait bilgisayarları birbirine bağlamak için kullanılan ağlara Yerel Alan Ağları (LAN - Local Area Network) adı verilir. LAN'lar adından da anlaşılacağı üzere belli bir lokasyon içerisinde oluşturulmuş ağ sistemidir. LAN ilk başlarda eş-eksenli bir kablonun bir sunucuya birkaç terminalle bağlandığı küçük bir sistemden oluşmaktaydı. Günümüzde ise LAN yüksek hızları destekleyen yüksek verimlilikte ağlar haline dönüştü ve geleneksel veri işlemenin yansıra ses ve video-konferans gibi işlevleri destekleyen ağlar haline gelmeye başladı. Şüphesiz bu gelişmenin ardında endüstriyel ve kişisel kullanıcı gereksinimlerinin gün geçtikçe artması, endüstriyel rekabet ve avantajlar (daha iyi, ucuz ve hızlı sistemler) önemli rol oynuyor. Küçük bir ağ iki bilgisayardan oluşabileceği gibi, büyük bir ağ yüzlerce bilgisayar, faks-modem, cd-rom sürücü, yazıcı ve bunları birbirine bağlayan ekipmanlardan oluşabilir.

Yerel alan ağlarında iletişim, genellikle bir bina veya binalar grubu, hastane, fabrika, üniversite kampüsü ve benzeri alanlar ile sınırlıdır.

Başarı için bir işletmenin öncelikle kendi içerisinde en hızlı, en verimli ve en etkin şekilde haberleşmesi gerekir. Bu da Yerel Alan Ağları ile mümkündür. Ayrıca bu altyapı sayesinde donanım sayısında azaltmalar yapılabilir. Paylaşım söz konusu olduğundan donanım tüm personel tarafından kullanılabilir, her bir birey için ek yazıcı, modem, disk ünitesi gerekmez. Benzer şekilde Internet erişimi de bir ağ üzerinde paylaştırılabilir. Yerel alan ağları, veri, yazılım ve donanım paylaşımı sağlamanın avantajlarını sunmaktadır.

Bir ağ tipi seçilirken göz önünde bulundurulması gereken temel kriterler:

- Yerel alan ağın boyutları
- Bu ağ üzerinde ne tip uygulamaların gerçekleştirileceği
- Kaç kullanıcının bulunacağı
- LAN'ın diğer hangi ağlarla bağlanabileceği
- Gelecekteki ağ beklentisi ve gelişmeye yönelik tahmin ve beklentiler

2.2.1. Yerel alan ağlarında kullanılan teknolojiler

2.2.1.1. Ethernet

İlk olarak XEROX firması tarafından geliştirilen, OSI tarafından IEEE 802.3 standardı olarak belirlenen bir standarttır. Yerel bir ağda bulunan bilgisayarların birbirleriyle haberleşmesini sağlar. Her bilgisayara ağ kartlarından bir tane takılır ve sonra da, kablo (ya da bazen telsiz) bağlantılarla bilgisayarlar arasında bir ağ oluşturulur. İletişim hızı, telefon ya da kablo hattı kullanan modemlere nazaran çok yüksektir. Yerel ağlarda günümüzde her bilgisayar HUB, SWITCH vb. denilen ve tüm bilgisayar bağlantıların tek bir noktada toplandığı ve böylece yerel ağın oluşturulduğu topolojiler sıkça kullanılır. Daha sonra, hub ya da switch, başka bir yerel ağ ya da internet bağlantı noktasına birleştirilerek ağdaki tüm bilgisayarların dış bağlantısı sağlanır [42].

Ethernet ağları, ağa giriş tekniği olarak 1960'lı yıllarda Hawaii Üniversitesi tarafından geliştirilen CSMA/CD (Carrier Sense Multiple Access With Collision Detection) tekniğini kullanırlar. Ethernet ağlar broadcast ile çalışan ağlardır. Yani ağdaki bir bilgisayarın gönderdiği bir veri ağdaki her bilgisayar tarafından görülmekte ama veri üzerinde MAC adresi bulunan bilgisayar tarafından işlenmektedir. Fakat bu, lokal ağın topolojisine göre değişir. Eğer ağ yıldız topoloji ise ve merkezde anahtar (switch) kullanıldıysa sadece ilgili bilgisayara anahtar tarafından yönlendirilir [42].

Ağa her bilgisayar istediği zaman girebilmektedir. Eğer aynı anda iki bilgisayar, ağın sessiz olduğunu düşünüp ağa bilgi bırakırsa bu bilgiler çarpışır (collision). CSMA/CD algoritmasını kullanarak tespit ettikleri bir zaman sonra tekrar aynı bilgiyi ağa bırakırlar ve iletişim gerçekleşir [42].

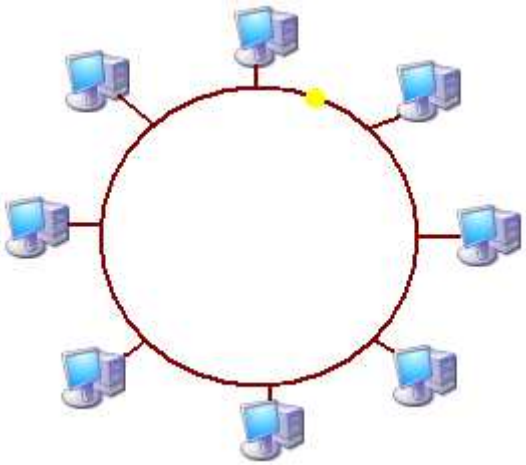
Ethernet ağlarında 4 farklı kategori vardır:

- Ethernet ve IEEE 802.3: 10 Mbps hızında koaksiyel ve UTP kablo üzerinde çalışır.
- Fast Ethernet: 100 Mbps hızında çift bükümlü (STP veya UTP) kablolar üzerinde çalışır.
- Gigabit Ethernet: 1000 Mbps (1 Gbps) hızında fiber kablo ve çift bükümlü kablolar üzerinde çalışır.
- 10 Gigabit Ethernet: 10.000 Mbps (10 Gbps) hızında fiber kablo üzerinde çalışır.

2.2.1.2. Jetonlu halka (Token ring)

Token Ring ağ protokolü yoğun trafiğe sahip ağlarda kullanılır. OSI tarafından IEEE 802.5 standardı olarak belirlenen bir standarttır. Bu sistemler pahalı fakat ağ problemleri az olan sistemlerdir. Bu ağ protokolü yapısında ağda bir jeton bulunur. Bu jeton ile birbirlerine ulaştıracakları bilgi paketleri taşınır [42].

Ağ ortamında bilgisayarlar arası bilgi alış - verişi sırasında, bilginin bozulmasını engellemek ve hızlı bir biçimde elektronik ortamda taşınmasını sağlamak için, bilgi belli byte uzunluklarında parçalara ayrılır. Çeşitli standartlara göre düzenlenen ve paket adı verilen yapılar halinde bilgisayarlar arası iletişim kanalında taşınır [42].



Şekil 2.1. Token ring ağ yapısı.

Token Ring ağ protokolü ile çalışan sistemlerinde, sistemde ilk açılan bilgisayar her zaman sistemin gözlemleyicisi görevini üstlenir ve bir sinyal (jeton) (Lojik 1 veya lojik 0 gibi) üretir. Bu sinyal ile ağda bilgi alış - verişi başlar. Sistemdeki başka bir bilgisayar diğer bir bilgisayara bilgi göndereceği zaman ağda dolaşan jetonun kendisine ulaşmasını bekler. Jeton kendine ulaştığında göndereceği bilgi paketini ve paketin ulaştırılacağı bilgisayarın adresini jetona ekler ve jetonu tekrar ağa bırakır. Bilgi paketi gidiş adresine ulaşana kadar ağdaki diğer bilgisayarlar bilgi alış verişi yapmaz dolayısıyla jetonu kullanamaz. Jeton boşalınca başka bir bilgisayar jeton aracılığıyla bir bilgi paketini başka bir bilgisayara iletebilir. Ağdaki iletişim bu şekilde devam eder [42, 43]. Şekil 2.1'de Token ring ağ yapısı verilmiştir.

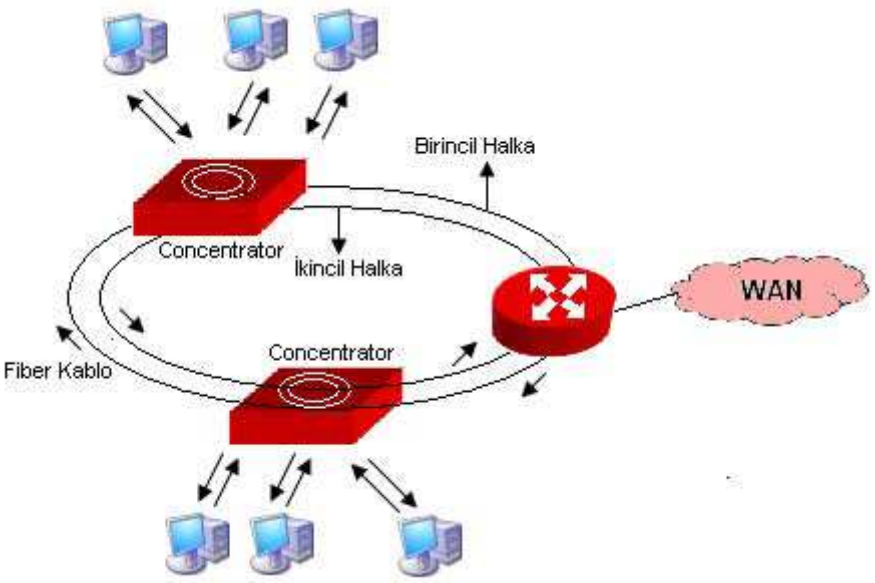
2.2.1.3. FDDI (Fiber distributed data interface)

1980'li yılların ortalarında yüksek hızlı bilgisayarların geliştirilmesiyle ortaya çıkmış bir standarttır. Bu standart günümüzde Ethernet kadar yaygın değildir.

Kullanılan fiber optik kablo sayesinde yüksek hızlarda çalışan (100 Mbps'nin üzerinde) token ring LAN'dır. FDDI kablolamada çift kablolama tekniği kullanılır. Bu durumda bir taraf saat yönünde iletim yaparken diğer taraf saatin tersi yönünde iletim yapar. FDDI'da A ve B sınıfı olmak üzere iki istasyon vardır. A sınıfı istasyonlar hayati önemli veriler ilettiğinden her iki fibere de bağlanır. B sınıfı istasyonlar ise fiberlerden sadece birine bağlanır. FDDI ile IEEE 802.5 Token Ring'in bir farkı vardır. 802.5'te bir istasyon yolladığı paket yerine gidip geri gelene kadar yeni jeton üretemezken FDDI'da istasyonun yeni bir jeton üretmek için eski jetonun geri gelmesini beklemesine gerek yoktur [42, 43].

Şekil 2.2'de verilen FDDI teknolojisi, uygulamalar için ideal olan gerçek zamanlı ağ bant aralığını (real time allocation) kullanma imkanı sunmaktadır. FDDI bunu iki farklı tipte trafik ile sağlamaktadır [43]. Bunlar;

Eş Zamanlı (Synchronous) : Eş zamanlı bant aralığı, ses ve video aktarımı gibi devamlı veri akışının gerektiği durumlarda kullanılır. Geri kalan bant aralığı eş zamanlılık gerektirmeyen uygulamalar için kullanılır.



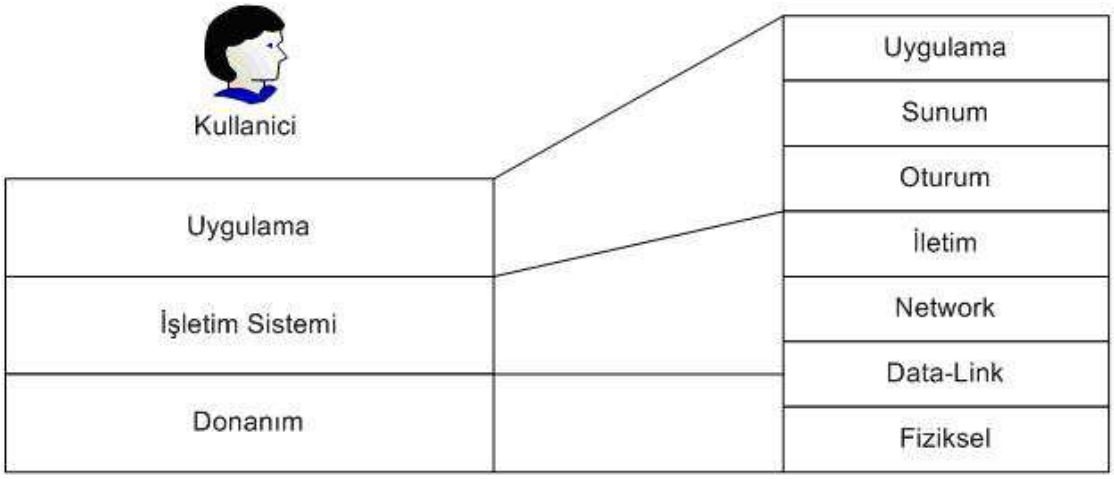
Şekil 2.2. FDDI teknolojisi.

Eş Zamanlı Olmayan (Asynchronous) : Bu tür trafikte sekiz seviyeli öncelik değerleri vardır. Bu öncelik değerine göre kendilerine ayrılan bant aralığını kullanır. Eş zamanlı bant aralığını kullanamayan ve öncelik değeri düşük olan bilgisayarlar FDDI öncelik mekanizması tarafında kilitlenerek iletişimi imkânsız hale gelebilmektedir [42, 43].

2.2.2. OSI referans modeli

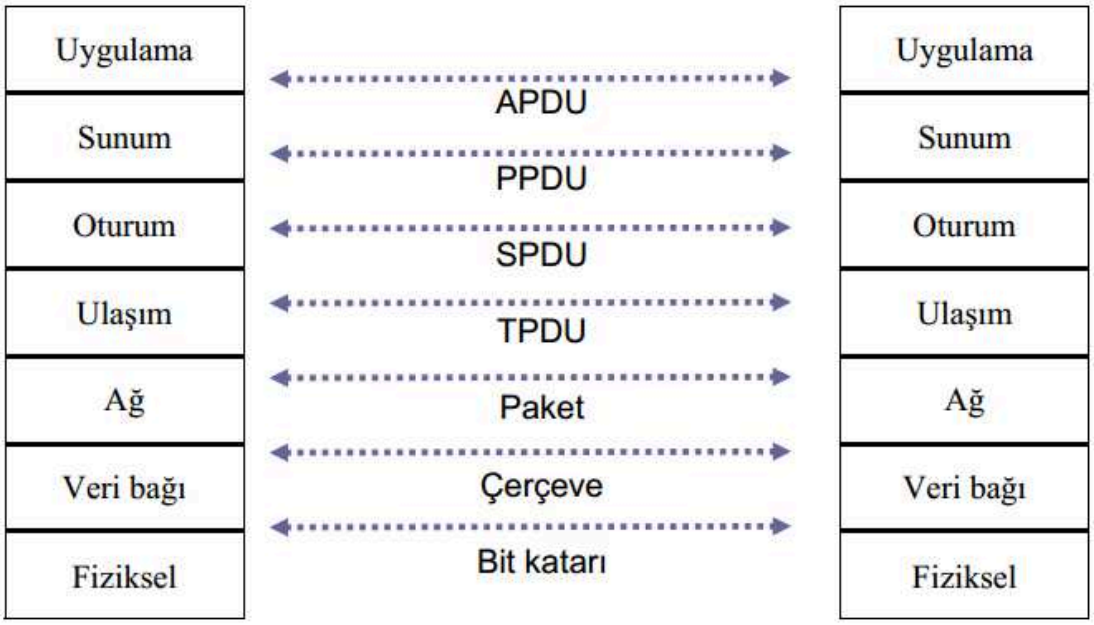
Haberleşme ağları karmaşık bir yapıya sahiptir. Ortamın fiziksel olarak yaratılması, bu ortam üzerinde veri aktarımı için gerekli kodlamanın yapılması, paketlerin oluşturulması, paketlerin varış noktasına yönlendirilmesi, veri aktarımı sırasında oluşan tıkanıklıkların giderilmesi, ağdaki bir hattın ya da birimin bozulması durumunda alternatif yolların bulunması, paketlerin birleştirilmesi, hataların fark edilmesi/düzeltilmesi, verinin bir uygulama protokolü aracılığı ile kullanıcıya sunulması gibi pek çok karmaşık işlemin yapılması gerekir.

Bunların hepsi haberleşme donanımı üzerinde çalışan haberleşme yazılım programları ile gerçekleştirilir. Bu işlemleri bir düzen içinde gerçeklemek için ISO (International Standards Organization) tarafından Şekil 2.3'de görülen OSI referans modeli önerilmiştir [44- 46].



Şekil 2.3. OSI referans modeli.

Şekil 2.3'de görüldüğü üzere OSI referans modeli yedi katmandan oluşmuştur. Bu katmanlarda işlenen veriler farklı isimler alır. Alt katmanlarda bit katarı, çerçeve, paket gibi isimler verilirken, üst katmanlarda ise ulaşım katmanı protokolü veri birimi (Transport Protocol Data Unit - TPDU) gibi katmana özel isimler alır [44]. Bu isimler Şekil 2.4'de verilmiştir.



Şekil 2.4. Katmanlara göre taşınan verinin isimlendirilmesi.

Bu katmanlarda yapılan işlemler aşağıda sırası ile açıklanmıştır.

1. Fiziksel Katman: Verinin fiziksel olarak hat üzerinden aktarılması için gerekli işlevleri kapsar. Veri, bu katman için sıradan bit dizisi olarak algılanır; bitlerin taşıdığı anlam bu katmanda yorumlanmaz. Bu katman için tanımlanan standartlar taşıyıcı işaretin şekli, verici ve alıcı konumdaki uç noktaların elektriksel ve mekanik özelliklerini belirler. Örneğin RS-232C, V.35 fiziksel katman standartlarıdır. Kablo standartları, tanımlamaları, işaret şekilleri, gerilim seviyeleri, işaret hızları bu katman için anlamlıdır [45-47].

2. Veri Bağı Katmanı: Bu katmanda hat kavramı oluşmaya başlar. Katmanın amacı verinin bir noktadan bir sonraki noktaya ulaştırılmasıdır. Bu katmanda veri çerçeve adı verilen bloklara bölünür. Gönderilecek bilginin hatalara bağışık bir yapıda mantıksal işaretlere dönüştürülmesi, alıcıda hataların sezilmesi, düzeltilemiyorsa doğrusunun elde edilmesi için göndericinin uyarılması ve hattın iki ucundaki birimin aynı hızlarda çalışmasını ayarlamak da bu katmanın görevidir [45, 47].

3. Ağ Katmanı: Veri paketlerinin bir uçtan diğer uca ağdaki çeşitli düğümler (yönlendirici, geçit yolu vs.) üzerinden geçirilip yönlendirilerek alıcısına ulaşmasını sağlayan işlevlere sahiptir. Veri paketinin alıcısına giderken ağ koşullarına, önceliklere ve diğer parametrelere göre hangi yolun uygun olacağı bu katmanda değerlendirilir. Bu amaçla düğümlere ağ adresi denilen numaralar verilir. Ağ adresi taşıyan bilgi bloklarına paket adı verilir. İnternet‘ in temel protokol kümesi olan TCP/IP‘nin IP protokolü bu katmanda yürütülen bir protokoldür. Heterojen alt ağların bulunduğu bir ortamda, alt ağlardan geçiş sırasında adresleme, paket boyu farklılığı gibi problemler bu katmanda çözülür [45, 47].

4. Ulaşım Katmanı: Bilginin son alıcıda her türlü hatadan arındırılmış olarak elde edilebilmesini sağlar. Ulaşım katmanının oluşturduğu bilgi bloklarına bölüm (bölüt) denir. Bölünen verinin numaralandırılması ve varış noktasında karışmış paketlerin tekrar sıralanması, yolda veri üzerinde oluşmuş hatalarla ilgili işlemlerin yapılması bu katmanın görevidir. Ulaşım katmanı uçtan-uca çalışır. Bu da kaynak ve varış düğümlerinde etkinlik göstermesi anlamına gelmektedir [45, 47].

5. Oturum Katmanı: Uç düğümler arasında gerekli oturumun kurulması, yönetilmesi ve sonlandırılması işlerini kapsar. İletişimin mantıksal sürekliliğinin sağlanması için, iletişimin kopması durumunda bir senkronizasyon noktasından başlayarak iletimin kaldığı yerden devam etmesini sağlar. Gönderilecek bilgi "senkronizasyon noktaları" ile sınırları belirlenmiş bloklara ayrılır. Karşı ucun oturum katmanı bir bloğun tamamını doğru olarak elde edip üst katmanına teslim ettikten sonra blokla ilgili işi tamamlamış olduğunu, veriyi gönderen tarafa bildirir. Gönderen taraf ise bloğu belleğinden silebilir. İletişim koparsa son senkronizasyon noktasından başlayarak bilgi gönderilir [45, 47].

6. Sunum Katmanı: Bilginin iletimde kullanılacak biçiminin düzenlenmesini sağlar: Sıkıştırma/açma, şifreleme/şifre çözme, EBCDIC-ASCII dönüşümü ve ters dönüşümü gibi işlevlerin yerine getirilmesini kapsar [45, 47].

7. Uygulama Katmanı: Uygulama programlarının ağa erişimi için gerekli işlevleri kapsar; kullanıcının etkileşimde bulunduğu uygulama programları doğrudan bu katmanla iletişim içindedir. Bu katman için dosya aktarımı, elektronik mektuplaşma, uzaktan dosya erişimi, ağ yönetimi, terminal protokolleri gibi standartlar geliştirilmiştir [45, 47].

2.2.3. TCP/IP referans modeli

Bir başka referans modeli de TCP/IP'dir. Bu modelin temelini ABD Savunma Bölümü tarafından desteklenerek geliştirilen ARPANET oluşturur. ARPANET'te amaç heterojen (telli, telsiz) alt ağların oluşturduğu bir ortamda kesintisiz bir bağlantı oluşturmaktı. Önem verilen bir diğer nokta ise bazı hatların kopması ya da düğümlerin bozulması sonrasında bile alternatif yolların bulunarak bağlantıların yaşatılmasını sağlamaktı. TCP/IP referans modelinin yapısı Şekil 2.5'de verilmiştir [44, 45].

TCP/IP referans modelindeki katmanların açıklaması aşağıdaki gibidir:

Ağ İşletim Katmanı: TCP/IP protokolünde düğümden-ağa katmanı hakkında fazla bir şey söylenmez. Bu katmanın amacı düğüm ile ağ arasında IP paketlerini gönderecek bir bağlantının kurulmasıdır.

TCI/IP Modeli
Uygulama (Application) Katmanı
Ulaşım (Transport) Katmanı
İnternet (Internet) Katmanı
Ağ İşletim (Network Access) Katmanı

Şekil 2.5. TCP/IP referans modeli.

İnternet Katmanı: Internet katmanı bir paket yapısı ve IP (Internet Protocol) adı verilen protokol tanımlar. Paketlerin oluşturulması, yönlendirilmesi, ortamdaki tıkanıklıkların giderilmesi bu protokolün görevidir.

Ulaşım Katmanı: Internet katmanının üzerinde ulaşım katmanı çalışır. Ulaşım katmanında kullanılmak üzere iki uçtan-uca protokol tanımlanmıştır. Bu protokoller: TCP (Transmission Control Protokol) ve UDP'dir (User Datagram Protocol).

Uygulama Katmanı: TCP/IP referans modelinde de uygulama katmanı tanımlanmıştır. Bu katman OSI referans modelinde olduğu gibi, ağa erişmek için gerekli uygulama protokollerini içerir. TCP/IP referans modeli sunuş ve oturum katmanlarına sahip değildir. OSI referans modelindeki veri bağı katmanı ve fiziksel katmanın işlevleri, TCP/IP referans modelinde düğümden-ağa katmanında gerçekleşmiştir [44, 45].

2.3. Bilgisayar Ağlarında Güvenlik

1990'lı yıllarda yaşanan hızlı teknolojik gelişmelerin bir sonucu olarak bilgisayarlar, modern hayatın her alanına girmiş ve vazgeçilmez bir biçimde kullanılmaya başlanmıştır. Hayatımızın birçok alanında bilgisayar ve bilgisayar ağı teknolojileri "olmazsa olmaz" bir şekilde yer almaktadır. İletişim, para transferleri, kamu

hizmetleri, askeri sistemler, elektronik bankacılık, savunma sistemleri, bu alanlardan sadece birkaçıdır. Teknolojideki bu gelişmeler, bilgisayar ağlarını ve sistemlerini, aynı zamanda, bir saldırı aracı haline, kullandığımız sistemleri de açık birer hedef haline getirmiştir [48].

Bilişim güvenliği konusunun, önümüzdeki dönemde de bilişim sektöründe giderek artan bir öneme sahip olacağı bilinmektedir. Bilişim Güvenliğinin birçok boyutu olmasına karşın, temel olarak üç prensipten söz edilebilir: gizlilik, veri bütünlüğü ve süreklilik.

Gizlilik (Confidentiality): Bilginin yetkisiz kişilerin eline geçmesinin engellenmesidir. Gizlilik, hem kalıcı ortamlarda (disk, tape, vb.) saklı bulunan veriler hem de ağ üzerinde bir göndericiden bir alıcıya gönderilen veriler için söz konusudur. Saldırganlar, yetkileri olmayan verilere birçok yolla erişebilirler: Parola dosyalarının çalınması, sosyal mühendislik, bilgisayar başında çalışan bir kullanıcının, ona fark ettirmeden özel bir bilgisini ele geçirme (parolasını girerken gözetleme gibi). Bunun yanında trafik analizinin, yani hangi gönderici ile hangi alıcı arası haberleşmenin olduğunun belirlenmesine karşı alınan önlemler de gizlilik hizmeti çerçevesinde değerlendirilir.

Veri Bütünlüğü (Data Integrity): Bu hizmetin amacı, veriyi göndericiden çıktığı haliyle alıcısına ulaştırmaktır. Bu durumda veri, haberleşme sırasında izlediği yollarda değiştirilmemiş, araya yeni veriler eklenmemiş, belli bir kısmı ya da tamamı tekrar edilmemiş ve sırası değiştirilmemiş şekilde alıcısına ulaşır. Bu hizmeti, geri dönüşümü olan ve olmayan şekilde verebiliriz. Şöyle ki; alıcıda iki tür bütünlük sınaması yapılabilir: Bozulma Sınaması ya da Düzeltme Sınaması. Bozulma Sınaması ile verinin göndericiden alıcıya ulaştırılması sırasında değiştirilip değiştirilmediğinin sezilmesi hedeflenmiştir. Düzeltme sınamasında ise, bozulma sınamasına ek olarak eğer veride değişiklik sezildiyse bunu göndericiden çıktığı haline döndürmek hedeflenmektedir.

Süreklilik (Availability): Bilişim sistemleri, kendilerinden beklenen işleri gerçekleştirirken, hedeflenen bir başarım (performans) vardır. Bu başarım sayesinde

müşteri memnuniyeti artar, elektronik işe geçiş süreci hızlanır. Süreklilik hizmeti, bilişim sistemlerini, kurum içinden ve dışından gelebilecek başarım düşürücü tehditlere karşı korumayı hedefler. Süreklilik hizmeti sayesinde, kullanıcılar, erişim yetkileri dâhilinde olan verilere, veri tazeliğini yitirmeden, zamanında ve güvenilir bir şekilde ulaşabilirler.

Sistem sürekliliği, yalnızca kötü amaçlı bir saldırganın, sistem başarımını düşürmeye yönelik bir saldırısı sonucu zedelenmez. Bilgisayar yazılımlarındaki hatalar, sistemin yanlış, bilinçsiz ve eğitimsiz personel tarafından kullanılması, ortam şartlarındaki değişimler (nem, ısı, yıldırım düşmesi, topraklama eksikliği) gibi faktörler de sistem sürekliliğini etkileyebilir.

Aşağıda, yukarıdaki üç temel prensibe ek olarak ikinci planda değerlendirilebilecek izlenebilirlik, kimlik sınaması, güvenilirlik ve inkâr edememe prensiplerinden bahsedilmiştir [48].

İzlenebilirlik ya da Kayıt Tutma (Accountability): Bu hizmetin hedefi sistemde gerçekleşen olayları, daha sonra analiz edilmek üzere kayıt altına almaktır. Burada olay dendiğinde, bilgisayar sistemi ya da ağı üzerinde olan herhangi bir faaliyeti anlayabiliriz. Bir sistemde olabilecek olaylara, kullanıcının parolasını yazarak sisteme girmesi, bir web sayfasına bağlanmak, e-posta almak göndermek ya da icq ile mesaj yollamak gibi örnekler verilebilir. Toplanan olay kayıtları üzerinde yapılacak analiz sonucunda, bilinen saldırı türlerinin örüntülerine rastlanırsa ya da bulanık mantık kullanılarak daha önce rastlanmayan ve saldırı olasılığı yüksek bir aktivite tespit edilirse alarm mesajları üretilerek sistem yöneticileri uyarılır.

Kimlik Sınaması (Authentication): Ağ güvenliği açısından kimlik sınaması; alıcının, göndericinin iddia ettiği kişi olduğundan emin olmasıdır. Bunun yanında, bir bilgisayar programını kullanırken bir parola girmek de kimlik sınaması çerçevesinde değerlendirilebilir. Günümüzde kimlik sınaması, sadece bilgisayar ağları ve sistemleri için değil, fiziksel sistemler için de çok önemli bir hizmet haline gelmiştir. Akıllı karta ya da biyometrik teknolojilere dayalı kimlik sınama sistemleri yaygın olarak kullanmaya başlanmıştır.

Güvenilirlik (Reliability - Consistency): Sistemin beklenen davranışı ile elde edilen sonuçlar arasındaki tutarlılık durumudur. Başka bir deyiş ile güvenilirlik, sistemden ne yapmasını bekliyorsak, sistemin de eksiksiz ve fazlasız olarak bunu yapması ve her çalıştırıldığında da aynı şekilde davranması olarak tanımlanabilir.

İnkâr Edememe (Non-repudiation): Bu hizmet sayesinde, ne gönderici alıcıya bir mesajı gönderdiğini ne de alıcı göndericiden bir mesajı aldığını inkâr edebilir. Bu hizmet, özellikle gerçek zamanlı işlem gerektiren finansal sistemlerde kullanım alanı bulmaktadır ve gönderici ile alıcı arasında ortaya çıkabilecek anlaşmazlıkların en aza indirilmesini sağlamaya yardımcı olmaktadır.

Bu hizmetler, zaman içinde bilgisayar sistemlerine karşı ortaya çıkmış tehditler ve yaşanmış olaylar sonucunda ortaya konmuştur. Yani her bir hizmet, belli bir grup potansiyel tehdide karşı sistemi korumaya yöneliktir, denilebilir [48].

2.3.1. Bilişim güvenliğinin sağlanması

Bir sistemin veya kurumun zarar görmesine neden olan istenmeyen bir olayın arkasındaki gizli nedene "Tehdit" adı verilir. Her tehdidin bir kaynağı (threat agent) ve bu kaynağın yararlandığı sistemdeki bir "güvenlik boşluğu" vardır. Tehditler, tehdit kaynağı açısından bakıldığında insan kaynaklı ve doğa kaynaklı tehditler olarak iki grupta incelenir [48].

İnsan Kaynaklı Tehditler: Kötü niyet olmayan davranışlar sonucu oluşanlar, bir kullanıcının, sistemi bilinçsiz ve bilgisizce, yeterli eğitime sahip olmadan kullanması sonucu sistemde ortaya çıkma olasılığı olan aksaklıklardır. Kötü niyetli davranışlar sonucu oluşanlar, Sisteme zarar verme amacıyla, sisteme yönelik olarak yapılacak tüm kötü niyetli davranışlardır. Bu tür tehditlerde, tehdit kaynağı, sistemde bulunan güvenlik boşluklarından yararlanır.

Doğa Kaynaklı Tehditler: Bu tür tehditler genellikle önceden tespit edilemezler ve büyük bir olasılıkla olmaları engellenemez. Deprem, yangın, su baskını, sel, ani sıcaklık değişimleri, toprak kayması, çığ düşmesi bu tür tehditlere örnek olarak

verilebilir. Tehdidin geliş yönüne göre de sınıflandırma yapılabilir. Buna göre iç tehditler, kurum içinden kuruma yönelik yapılabilecek saldırılar, dış tehditler ise kurum dışından kuruma yönelik olarak yapılabilecek saldırılar olarak tanımlanır.

Güvenlik boşluğu (Vulnerability), sistem üzerindeki yazılım ve donanımdan kaynaklanan ya da sistemin işletim kuralları ve/veya yönergelerindeki açık noktalar ve zayıf kalmış yönlerdir. Bir güvenlik boşluğu sayesinde bir saldırgan, sistemdeki bilgisayarlara ya da bilgisayar ağı üzerindeki kaynaklara yetkisiz olarak erişebilir. Bir sunucu bilgisayar üzerinde çalışan bir hizmet (örneğin web sunucu ya da e-posta alma/gönderme hizmeti), modem üzerinden içeri doğru sınırlandırılmamış arama hizmeti, bir güvenlik duvarı üzerinde açık unutulmuş bir erişim noktası (port), sunucu bilgisayarların bulunduğu odaya giriş çıkışlarda fiziksel erişim denetimi eksikliği, sunucular üzerinde belli bir politikaya dayandırılmadan belirlenen parolalar güvenlik boşluklarına örnek olarak verilebilirler.

Tehditler, bilgisayar sistemlerindeki güvenlik boşluklarına yönelik olarak tanımlanırlar. Yani bir güvenlik boşluğu ortadan kaldırılırsa ya da “yama program” yardımıyla düzeltilirse, söz konusu tehdit ortadan kaldırılır. Aşağıdaki tablodan da anlaşılacağı üzere, bir tehdidin oluşması için bir güvenlik boşluğuna ve bu güvenlik boşluğundan yararlanabilecek bir tehdit kaynağına ihtiyaç vardır.

Bir tehdit kaynağının, bir sistemdeki güvenlik boşluğundan yararlanarak sisteme yetkisiz erişimde bulunması olasılığı, bu tehdidin riski olarak ifade edilir. Tehdit kaynaklarının ya da güvenlik boşluklarının azaltılması, tehdide ait riskleri de aynı oranlarda azaltacaktır [48].

Bilişim sistemlerinin güvenli hale getirilmesi konusu, kapsamlı ve bütünleşik bir yaklaşımla ele alınmadığı takdirde, başarı kazanmak büyük olasılıkla mümkün olmayacaktır. Bilişim güvenliğinin sağlanması üç temel açıdan ele alınabilir. Bu üç süreç alanı şunlardır [48]:

- Yönetsel Önlemler
- Teknoloji Uygulamaları
- Eğitim ve Farkındalık Yaratma

2.3.2. Bilişim güvenliğinin sağlanmasında kullanılan teknolojiler

Bu çalışmada ağırlıklı olarak teknoloji uygulamaları ile bir ağın güvenliği hedeflenmiştir. Genel olarak ağ güvenliğinin sağlanmasında kullanılan teknolojiler aşağıdaki listede verilmiştir.

- Şifreleme (kriptoloji)
- Kimlik denetimi – Sayısal imza
- Güvenlik duvarları ve erişim denetimi
- Saldırı tespit sistemleri ve ağ izleme
- Antivirüs yazılımları

Genel olarak, kriptoloji aktif ve pasif saldırılara karşı en iyi veri koruma yöntemi olarak kabul edilir [41]. Bu nedenle bu bölümde bu teknolojilerden özellikle kriptoloji konusuna değinilecektir.

2.3.2.1. Şifreleme (Kriptoloji)

Kriptoloji, Latince “gizli” anlamına gelen “kryptos” ve “kelime” anlamına gelen “logos” sözcüklerinin birleşiminden oluşur. Kriptoloji bilgi güvenliğini inceleyen bilim dalıdır. Kriptoloji, haberleşen iki veya daha fazla tarafın bilgi alışverişini emniyetli olarak yapmasını sağlayan, temeli matematiksel zor problemlere dayanan tekniklerin ve uygulamaların bütünüdür. Kriptoloji biliminin kriptografi ve kriptanaliz olarak adlandırılan iki temel alt dalı bulunmaktadır. Kriptografi, belgelerin şifrelenmesi ve şifresinin çözülmesi için kullanılan yöntemleri araştırırken; kriptanaliz ise kriptolojik sistemlerin kurduğu mekanizmaları inceler ve kırmaya çalışır [45, 49, 50]. Kriptolojide daha çok bilginin güvenliği ve gizliliği üzerinde durulacaktır.

Bir bilginin içeriğinin, başkalarının anlayamayacağı bir hale getirilmesine "şifreleme" denir. Şifreleme işlemi, bilginin matematiksel yöntemler kullanılarak kodlanması ve başkalarının okuyamayacağı bir hale getirilmesidir. Yapılan bu kodlamaya kripto algoritması adı verilir. Şifre çözme ise, şifreli bilginin tekrar elde edilmesi işlemidir.

Şifrelenmemiş bir bilgiye "düz metin" (plain text) denir. Düz metin, bir insanın okuyabileceği bir yazı ya da bir bilgisayarın anlayabileceği çalıştırılabilir (.exe, .com) bir program ya da bir veri dosyası (.txt) olabilir. Bir kripto algoritması kullanılarak, herkesin okuyamayacağı bir şekilde kodlanmış bilgiye ise "şifreli metin" (cipher text) denir [45, 48].

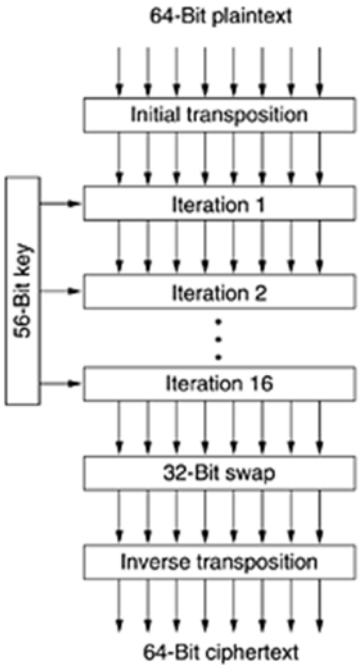
İlk bilinen kripto algoritmaları 4000 yıl kadar önce ortaya çıkmıştır. Zaman geçtikçe, kullanılan teknikler ve cihazlar gelişmiş ve her geçen gün yeni teknikler kullanılır ve yeni algoritmalar üretilir olmuştur. Bu teknoloji şu anda bilişim güvenliğinin vazgeçilmez bir parçasıdır [48]. Geçmişteki kripto algoritmalarının güvenliği, algoritmanın gizliliğine dayanmakta idi. Günümüzde ise kullanılan modern ve güçlü kripto algoritmaları artık gizli değildir. Bu algoritmalar güvenliklerini, kullandıkları farklı uzunluk ve yapılardaki anahtarlarla sağlarlar. Bir anahtar ile şifrelenen bilgi, kullanılan algoritmaya bağlı olarak, ilgili anahtar ile çözülebilir [54]. Kripto algoritmaları, temel olarak, kullandıkları anahtar yapısına göre "Simetrik" ve "Asimetrik" algoritmalar olarak ikiye ayrılmaktadır.

Simetrik Algoritmalar:

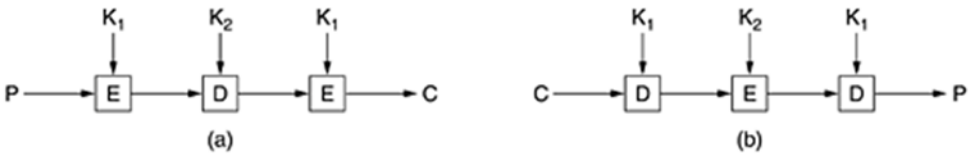
Simetrik algoritmalarda, şifreleme ve şifre çözme için gizli anahtar (secret key) olarak adlandırılan tek bir anahtar kullanılır. Gizli anahtar verinin iletimden önce şifrelenmesi, iletildikten sonra karşı tarafta şifresinin çözülmesi için kullanılmaktadır. Bu tip algoritmalarda anahtarın gizliliği çok önemlidir.

İki çeşit simetrik şifreleme yöntemi vardır: Blok şifreleme ve Akış şifreleme [45, 48, 54]. Blok şifrelemede; şifreleme ve şifre çözme işleminde metinler sabit uzunluklu dizilere bölünür ve blok blok işleme tabi tutulurlar. Anahtar uzunluğu sabittir.

En çok bilinen blok şifreleme algoritması 1977 yılında IBM tarafından geliştirilen DES algoritmasıdır. DES, mesajları 64 bitlik bloklar halinde şifreler. Şifreleme ve şifre çözme işlemlerinin her ikisinde de aynı algoritma kullanılır. DES, 56 bitlik şifreleme anahtarı kullanmaktadır. DES algoritmasının blok diyagramı Şekil 2.6'da gösterilmektedir. DES algoritmasının diğer bir çeşidi olan 3DES algoritması, 3 farklı anahtar değeri ile DES algoritmasının 3 defa ardışık olarak çalıştırılması esasına dayanır. 3DES algoritması ile şifreleme ve şifre çözme işlemleri Şekil 2.7'de gösterilmektedir [45, 54].



Şekil 2.6. DES algoritması 56 bitlik anahtar kullanarak 64 bitlik veriyi şifreler [45].



Şekil 2.7. 3DES algoritması ile a) şifreleme, b) şifre çözme işlemi [45].

Günümüzde kullanılan en önemli blok şifreleme algoritmalarından biri de AES'tir. DES'e göre daha güvenli bir algoritmadır. John Daemen ve Vincent Rijmen tarafından "Rijndael" adıyla geliştirilmiş ve 2002 yılında standart haline gelmiştir. AES

algoritması 128, 192 ya da 256 bitlik anahtarlar kullanır. DES'te 64 bit olan bloklar AES'te 128 bite çıkarılmıştır [45].

Diğer blok şifreleme algoritmalarına örnek olarak BLOWFISH, IDEA, FEAL ve RC5 algoritmaları verilebilir.

Akış şifrelemede ise, algoritmanın girdisi sadece anahtardır. Algoritma anahtardan rastgele bir diziye çok benzeyen kayan bir anahtar dizisi oluşturur. Daha sonra kayan anahtar dizisinin elemanları ile düz metin ve şifreli metin dizisinin elemanları ikili tabanda toplanarak şifreleme veya şifre çözme işlemi tamamlanır. Akış şifreleme algoritmalarına örnek olarak RC4 algoritması verilebilir.

Asimetrik Algoritmalar:

İki tarafta da biri gizli (private) diğeri açık (public) olarak tanımlanan iki farklı anahtar bulunur. Gizli anahtarlar sadece sahipleri tarafından bilinmektedir. Açık anahtarlar ise herkese açıktır (telefon numaraları gibi). Gönderen, mesajı alıcının açık anahtarı ile şifreler ve alıcı şifreli-mesajı gizli anahtarı ile çözer. Bu Diffie ve Hellman (Stanford Üniversitesi, 1975) tarafından keşfedilen, algoritmaların ve bir anahtarın şifrelemek, bir başka anahtarın çözmek için kullanılabileceği keşifleri sayesinde mümkün olmaktadır. Açık ve gizli anahtar bir anahtar çiftini oluşturur [49].

Bu şifreleme yöntemleri gerçekten çözülmesi zor olan sonlu alanların logaritmalarını almak (Diffie-Hellman), büyük sayıları asal çarpanlarına ayırmak (RSA) gibi matematiksel yöntemlerle tek-yönlü fonksiyonlardan yararlanır. Bu tip fonksiyonları tek yönde hesaplama diğer yönde hesaplamaya göre daha kolaydır. Bugünün işleme gücü ve bilgisayarlarıyla, brute-force saldırıları ile bu fonksiyonları çözmek sanal olarak imkânsızdır. Daha yeni eliptik eğriler, karışım üreticiler ("mixture generators") gibi teknikler daha hızlı açık anahtar sistemleri vadetmektedir [45, 49]. SHA-1, MD5, RSA gibi algoritmalar sıklıkla kullanılan açık anahtar şifreleme türleridir.
Asimetrik algoritmalar şu şekilde ifade edilebilir:

$$E_e(T) = C, D_d(C) = T$$

$E_e(T)$ şifreleme, $D_d(C)$ şifre çözme işlemini ifade etmektedir. *e* açık anahtar, *d* ise gizli anahtardır. Burada, *e* ile şifrelenen mesaj, *d* ile çözülmektedir. *e* ve *d* birbiri ile ilişkili değerlerdir ancak bu ilişki tek yönlü bir matematiksel fonksiyon tarafından belirlenir. $f: X \rightarrow Y$ şeklinde tanımlanan tek yönlü bir fonksiyonla, $x \in X$ için bütün *y* değerleri hesaplanabilirken; $y \in Y$ için ilişkili *x* değerlerini hesaplamak mümkün değildir. Açık anahtarlı bir kriptolama sisteminde, şifreleme algoritması herkes tarafından bilinir. Ancak şifre çözme algoritması ve anahtarı gizlidir. Böylece, sadece şifre çözme yetkisine sahip olan kişiler şifrelenmiş mesajı çözebilirler [45, 54].

Asimetrik algoritmalardan en çok kullanılan RSA, 1978 yılında Rivest, Shamir, Adleman tarafından geliştirilmiştir. RSA algoritması çok güçlü ve güvenli bir algoritmadır ve çeyrek yüzyıldan fazla zamandır kırılamamıştır [45]. RSA algoritmasının çalışması şu şekilde özetlenebilir:

- İki tane *p* ve *q* asal sayısı seçilir (örneğin 1024 bit uzunluğunda).
- $n = p \,.\, q$ ve $z = (p-1) \,.\, (q-1)$ değerleri hesaplanır.
- *z* ile aralarında asal olan bir *d* sayısı seçilir.
- $e \,.\, d = 1 \; (mod\; z)$ koşulunu sağlayan *e* değeri hesaplanır.

Bu değerler hesaplandıktan sonra şifreleme işlemine başlanır. Şifrelenecek P mesajı, $2^k < n$ koşulunu sağlayan k-bitlik bloklara ayrılır. Şifreli mesaj $C = P^e \; (mod\; n)$ formülü ile hesaplanır. Şifre çözme $P = C^d \; (mod\; n)$ formülü ile gerçekleştirilir. Bu formüllerden görüldüğü üzere; şifreleme işlemini yapmak için (*e, n*), şifre çözme işlemini yapmak için de (*d, n*) değerlerine ihtiyaç vardır. Bu nedenle, açık anahtar (*e, n*), gizli anahtar da (*d, n*) sayı çiftlerini içerir.

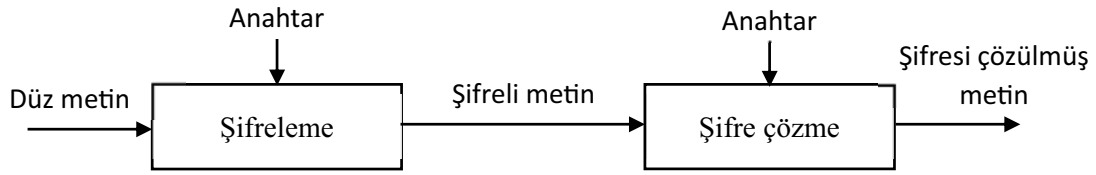
Örneğin, *p* = 3, *q* = 11 seçilirse *n* = 33 ve *z* = 20 olur. *z* ile aralarında asal olan *d* = 7 sayısı belirlenirse; $e \,.\, 7 = 1 \; (mod\; 20)$ formülünden *e* = 3 değeri hesaplanır. Bu durumda şifreli mesaj $C = P^3 \; (mod\; 33)$; şifresi çözülen mesaj da $P = C^7 \; (mod\; 33)$ şeklinde olacaktır [45]. Bu örneğe göre "SUZANNE" kelimesinin şifrelenmesi ve şifresinin çözülmesi Şekil 2.8'de gösterilmektedir.

Plaintext (P)			Ciphertext (C)		After decryption	
Symbolic	Numeric	P^3	P^3 (mod 33)	C^7	C^7 (mod 33)	Symbolic
S	19	6859	28	13492928512	19	S
U	21	9261	21	1801088541	21	U
Z	26	17576	20	1280000000	26	Z
A	01	1	1	1	01	A
N	14	2744	5	78125	14	N
N	14	2744	5	78125	14	N
E	05	125	26	8031810176	05	E
Sender's computation				Receiver's computation		

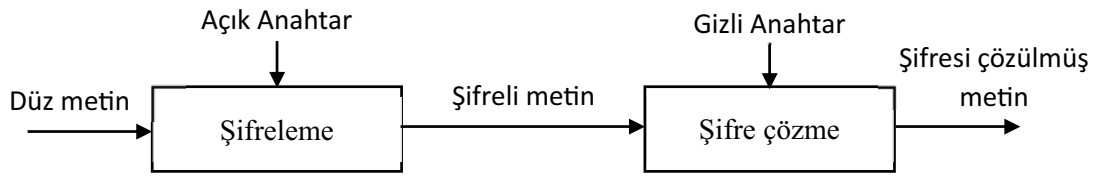
Şekil 2.8. Bir RSA algoritması örneği [45].

Simetrik algoritmalar, açık (public) anahtar kullanan rakiplerine göre çok daha hızlıdırlar. Ancak bu algoritmalarda, her iki taraf anahtarı bilmeli ve bu anahtarın paylaşımı için güvenli bir yol bulmalıdır.

Asimetrik algoritmalarda ise sadece gizli anahtar gizli tutulmalıdır. Açık anahtar için herhangi bir gizli kanal gereksinimi yoktur. Sadece açık anahtar, alıcıya bu anahtarın gerçek açık anahtar olduğundan emin olabileceği bir kanaldan gönderilmelidir. Ancak bu algoritmalar, matematiksel karmaşıklık içeren hesaplamalardan dolayı simetrik algoritmalara göre çok daha yavaş çalışmaktadır [45, 54]. Şekil 2.9 ve Şekil 2.10 simetrik ve asimetrik algoritmalarda anahtar kullanımını göstermektedir.



Şekil 2.9. Simetrik algoritmalarda anahtar kullanımı [54].



Şekil 2.10. Asimetrik algoritmalarda anahtar kullanımı [54].

Hashing/Mesaj Şekillendirme (Message Digest):

Bir hash fonksiyonu, bir blok veriden sabit uzunlukta karakter katarları oluşturur. Eğer fonksiyon tek yönlü ise ayrıca mesaj şekillendirme adını alır. Bu) fonksiyonlar bir mesajı alır, analiz eder ve sabit uzunlukta özetler (digest) oluşturur (pratik olarak bu özetler tektir, benzeri yoktur). Çok hızlı bilgisayarlarla bile bir hash yardımı ile mesajların elde edilmesi mümkün değildir. Aynı özete (digest'e) sahip bir başka mesajın elde edilmesi için bilinen bir makul yol yoktur. Bu algoritmalar genellikle mesajların bütünlüğünü onaylamak için imzalar hazırlamakta kullanılmaktadır [45, 49].

Avantajlar: Şifrelemeden daha hızlıdır ve sabit bir çıktı üretilir. Bunun anlamı, çok büyük dosyalar bile aynı digest'i oluşturur ve bu veri iletimi için çok verimli olur.
Dezavantajları: Sadece bütünlüğü garanti eder. Bazı makalelerde, bilinen bazı zayıflıkları anlatılmıştır [52].

Tipik Uygulamalar: Çoğu Internet sunucusu MD5 digestlerini önemli dosyaların indirilmesi durumlarında kullanır. Çoğu dijital imza sistemleri ve güvenli e-posta sistemleri bütünlük için bir digest fonksiyonu kullanır.

Bazı araştırmacılar kaotik sistemlerin gösterdikleri özel davranışlardan dolayı; kaos ve kriptoloji bilimleri arasında güçlü bir ilişki olduğunu vurgulamıştır [49, 51]. 1990'lardan beri blok şifreler, akan şifreler, özet (hash) fonksiyonları, görüntü şifreleme algoritmaları gibi birçok şifreleme sisteminin tasarlanmasında da kaotik sistemleri kullanmışlardır. Bu tez çalışmasında da bir ağın güvenliğinin, kaotik bir kriptolama sistemi ile sağlanmasına çalışılmıştır.

2.3.2.2. Kimlik doğrulama

Bir nesnenin kimliğinin doğrulanması yöntemidir. Nesne; kullanıcı, bilgisayar, makine ya da bir süreç olabilir. Doğrulama iki tarafın bildiği ama başkalarının bilmediği nitelikler kullanır. Bunlar biyolojik ölçüler (el tarama, DNA şekilleri, retina tarama, parmak izi tarama, el yazısı gibi), "passphrase"ler, şifreler, tek seferlik şifre listeleri,

kimlik kartları, akıllı tokenler, “challenge-response” listeleri, vb. olabilir. Bazı sistemler yukarıdakilerin kombinasyonlarını içerir [45, 49].

Günümüzde çok karşılaşılan güçlü doğrulama yöntemleri tek kullanımlık anahtarlar, otomatik şifre üreticileri ve zeki kimlik kartları olarak sıralanabilir.

2.3.2.3. Erişim kontrol listeleri (EKL)

Bir EKL (Erişim Kontrol Listesi) bir nesneye kimin (neyin), ne şekilde erişebileceğini tutan listelerdir. EKL’ler veri gizliliğini ve bütünlüğünü sağlamakta kullanılan birincil mekanizmadır. Akıllı erişim kontrollü sistemler kullanıcıları ayırt eder ve her nesne için EKL’yi yönetebilir. Eğer EKL kullanıcı (ya da veri sahibi) tarafından değiştirilebiliyorsa akıllı erişim kontrolü olduğu kabul edilir. Eğer EKL kullanıcı tarafından değiştirilemiyor, sistem tarafından belirleniyorsa zorunlu erişim kontrolü kullanılmaktadır [45, 49].

2.3.3. Mevcut güvenlik yöntemlerinden IPSec

IPSec, IP ağlarının güvenliği için IETF [53] tarafından tanımlanmış Internet Protokolü güvenlik standardıdır. Kendi içerisinde güvenli yerel alan ağlarının, güvensiz ağlar (örneğin İnternet) üzerinden güvenli olarak haberleşmesini sağlar.

Ağda güvenliği sağlamak, en basit anlamıyla verinin sadece istenen noktalara gizli bir şekilde gönderilmesi olarak tanımlanabilir. Bu gizliliğin sağlanması için şifreleme yapmak kaçınılmazdır. İki düğüm arasındaki haberleşmenin şifreli olarak yapılabilmesi için öncelikle bu iki düğümün şifreleme algoritmasını ve gerekiyorsa şifreleme - şifre çözme anahtarlarının bilinmesi gerekmektedir.

Günümüzde sıklıkla kullanılan kablolu yerel ağlarda iletişimin şifresiz olarak yapıldığı bir gerçektir. Bu durum büyük bir risk oluşturmaktadır. Bu riski elimine etmek amacıyla yeni nesil ağlarda şifreli iletişimin zorunlu kılınması düşünülmüş ve IPSec protokolü geliştirilmiştir. Bu protokol yeni nesil IPv6 ağlarında zorunlu tutulmaktadır.

IPSec protokolü, ağ içinde uçtan uca güvenli (şifreli) iletişimin her cihaz tarafından yapılması prensibine dayanmaktadır. IPSec ile kullanılacak şifreleme ve anahtar paylaşımı algoritmaları üzerinde çalışmalar halen sürdürülmektedir [28].

IPSec temelde iki ana parçadan oluşur. İlk parça; pakete eklenecek güvenlik tanımlayıcısı, bütünlük kontrol değeri ve diğer bilgileri taşıyan iki başlık yapısını tarif eder. İkinci parça ise anahtarların kurulması ile ilgilenen IKE'dir. IKE protokolü haberleşen uçlar arasında anahtarların dinamik olarak belirlenmesi ile ilgilenen bir protokoldür.

IPSec iletim kipi ve tünel kipi olmak üzere iki kipte kullanılabilir. İletim kipinde IPSec başlığı IP başlığından hemen sonra gelir ve IP başlığındaki protokol alanı, IPSec başlığının takip ettiğini gösterir. Tünel kipinde gerçek tüm IP paketi (IP başlığı, IPSec başlığı vs...) tamamen yeni bir IP başlığı tarafından kapsüllenir [45, 55].

IPSec protokolünün iki adet farklı güvenlik servis kipi bulunmaktadır. AH servisi sadece veri bütünlüğü sağlarken, ESP servisi hem gizlilik hem de veri bütünlüğünü sağlamaktadır [55].

Günümüzün popüler ağ teknolojilerinden olan servis kalitesi (QoS), çoklu yayın (Multicast) ve gezgin IP (Mobil-IP); IPSec ile birlikte kullanıldığında birçok problem ortaya çıkmaktadır. Örneğin IPSec uygulandığında, IP başlığında bulunan servis kalitesi alanları şifrelenmekte dolayısıyla bu alan anlaşılamaz hale gelmektedir, IPSec noktadan noktaya tasarlandığı için çoklu yayın desteklenmemektedir ve gezgin IP ile dinamik biçimde kurulması gereken sanal tüneller için düğümlerin elle yapılandırılması gerekmektedir. Aynı zamanda IPSec yapan düğümler için otomatik ve güvenli anahtar dağıtma yöntemleri geliştirilmelidir. Çünkü IKE gibi mevcut protokoller günümüz için yetersiz kalmaktadır. Tüm bu problemler IPSec kapsamında üzerinde çalışılması gereken araştırma alanlarından yalnızca bazılarıdır [55].

IPv6 ile birlikte IPSec, güvenlik açıkları için tam bir çözüm değildir. IPSec tehdit ve güvenlik önlemlerini azaltmak için ağ katmanı ile uygulama katmanı arasında şifreleme dönüşümleri gibi işlevleri sunar. Ancak malware, spam, erişim denetimi,

saldırı tespit ve bunun gibi diğer güvenlik işlevlerini yerine getirmez. DoS atakları ve kanal gizleme (karıştırma) IPSec'te halen mevcuttur [56]. IPSec tam bir güvenlik sunmadığı için bazı yazılımsal (saldırı tespit sistemleri) çözümler bilimsel olarak önerilmektedir [57].

BÖLÜM 3. KAOS VE KRİPTOLOJİ

3.1. Kaos Teorisi

1970'li yıllarda birkaç bilim adamı düzensizlik konusuna el atmaya başladı. Matematikçiler, fizikçiler, biyologlar, kimyacılar olarak hepsi de kural dışılığın çeşitli türleri arasında bağlantılar bulmak peşindeydi. Fizyologlar insan kalbinde oluşan ve izah edilemeyen ani ölümlerin belli başlı nedeni olan kaosta hayret verici bir düzey bulunduğunu tespit ettiler. Ekoloji uzmanları güve popülasyonlarının çoğalmalarını ve yok oluşlarını araştırdılar. Ekonomistler eski stok maliyeti verilerini inceleyip yeni bir analiz yöntemi denediler. Sonuçta ortaya çıkan bakış açısı, araştırıcıları, bulutların aldığı şekillere, yıldırımın izlediği yollara, kan damarlarının mikroskobik düzeylerde oluşturduğu ağlara, yıldızların galaksiler halinde kümelenmesine, yani doğrudan doğruya tabiata yöneltiyordu. On yıl kadar sonra, kaos kelimesi, bilimsel düzenin dokusunu yeniden şekillendirmeye yönelik hızlı gelişmeyi kısaca tanımlamak için kullanılan bir kavram haline geldi. Kaos, karmaşıklığın temelinde yatan muazzam ve hassas yapıyı yakalayabilmek için hem bilgisayar kullanımında özel bazı teknikler hem de birtakım özel grafik resim ve çizgi türleri icat etmiştir. Yeni bilim kendi dilini de üreterek fraktallar, çatallaşmalar, periyodiklikler gibi kendine özgü terimler kullanmaya başlamıştır [58].

Kaos, düzensizliğin düzeni şeklinde tanımlanan, doğrusal olmayan olayları açıklamaya yarayan bir bilim dalıdır. Kaos ile ilgili çalışmalar, doğrusal olmayan dinamik sistemler teorisinin bir kısmıdır. Bu durum daha çok “deterministik kaos” olarak bilinir. Aynı zamanda nedeni ve seyri bilinemeyen, hesaplanamaz olan “rastlantısal (stokastik) kaos” kavramı da mevcuttur. Fakat bilimin ilgilendiği daha ziyade deterministik kaostur [1]. Kaos teorisinin daha iyi anlaşılabilmesi için, determinizm, dinamik sistemler, nonlineer sistemler bu bölümde incelenecektir.

Kaosun ve kaotik işaretlerin başlıca önemli özellikleri; zaman boyutunda düzensizliği, başlangıç şartlarına hassas bağımlılığı, sınırsız sayıda değişik periyodik salınımlar içermesi, gürültü benzeri geniş güç spektrumuna sahip olması, limit kümesinin parçalı (fraktal) boyutlu olması, genliği ve frekansı tespit edilemeyen, ancak sınırlı bir alanda değişen işaretler içermesidir.

Kaos bilimindeki, determinizmin kaotik sistemleri önceden tahmin edemeyeceği keşfi bilimin deterministik bakış tarzlarını değiştirmiştir. Kaostaki bu buluş bilimlerde ve mühendislik sistemlerinde geniş olarak karşılaşılan karmaşık ve önceden kestirilemeyen olayların daha iyi anlaşılmasını sağlamaktadır. Düzenli bir hareketten, kaotik bir davranışa geçiş olayı, teorik ve deneysel olarak her iki alanda da geniş olarak çalışılmaktadır. Doğrusal olmayan sistem teorilerindeki ilerleme, yeni deneysel teknikler, pahalı ve işlem gücü yüksek bilgisayarların ucuzlayıp yaygınlaşması, karmaşık ve doğrusal olmayan davranışları daha iyi analiz etmeye ve anlamaya sebep olmuş ve sonuç olarak Kaos Bilimi gelişmiştir. Kaos ve karmaşıklıkla ilgili gözlemlere paralel olarak, bu olayın mekanizmasının anlaşılması, kaotik davranışın nitelendirilmesi, özelliklerinin belirlenmesi, deneysel verilerin ölçülmesi ve analizinin yapılması ile ilgili araştırmalarda çok hızlı gelişmeler kaydedilmiştir [1].

3.1.1. Determinizm

Determinizm, "bir fiziksel sistemin şimdiki durumu, önceki durumunun sonucudur" der. Dolayısıyla her olay ve hareketi önceden belirlemek mümkündür. Isaac Newton'un ortaya koyduğu hareketin üç temel yasası modern bilimi bütünüyle determinizme dayalı kılmıştır. Bu yasalar, determinizmi yalnız ileriye değil, geriye doğru da çalışan sağlam bir araç olarak görür. Newton'un hareket yasalarına göre, şu andaki olay ve hareket önceki olay ve hareketten çıktığı gibi, bundan sonra olacak olay veya hareket de şu andaki olay veya hareketin sonucu olacaktır. Determinizmin matematiksel dili çok açıktır. Başlangıç koşullarını bilince, ona uyan analitik çözümü, çözüm uzayından seçebiliriz. Bu çözüme *f* diyelim. Herhangi bir *t* anında sistemin durumunu biliyor isek, *f* fonksiyonunu biliyoruz demektir. *a* zaman aralığı olmak üzere, her *a* için *f(t+a)* ve *f(t-a)* değerlerini hesaplamak mümkündür. Matematiksel açıdan bakınca çözüm fonksiyonunun grafiği üstünde gerçekleşen bu olgu, fiziksel

açıdan bakınca söz konusu dinamik sistemin kendi yörüngesi üzerinde belli bir yerden ileriye ya da geriye doğru hareket ettirilebilmesi demektir.

Öyleyse, determinizmin uygulanabilmesi için, sistemin analitik çözümüne ve iyi belirlenmiş başlangıç koşullarına gereksinim vardır. Çok kolaymış gibi görünen bu iş, gerçekte pek çok sistem için imkansızdır. Bu imkansızlık kaos diye anılan fenomenleri ortaya çıkarır [59, 60].

3.1.2. Dinamik sistemler

Sistem kavramı, karşılıklı etkileşim içinde olan şeyler ve bunların arasındaki ilişkilerin anlaşılması olarak tanımlanabilir. Sistemler modellenebilir ve bu modeller orijinal sistemin davranışını deneysel olarak tekrarlayarak incelemekte kullanılabilir. Örneğin, doğadaki türler arasındaki etkileşimin modellenmesi bir sistemdir.

Dinamik sistem, zaman içinde değişen bir sistem olarak tanımlanır. Dinamik sistemler lineer ya da nonlineer olabilir. Bilindiği gibi lineer kavramı, basit bir şekilde, matematiksel modellerin grafik üzerinde doğru biçiminde gösterilebilmelerini belirtir. Lineer sistemler klasik bilimde, gerçeği iyi bir şekilde açıklamaktan ziyade, basit olmaları nedeniyle büyük ilgi görmüş ve yaygın olarak kullanılmıştır. Lineer olmayan sistemlerde girdi ve çıktı arasında bir orantı yoktur. Lineer modelden sapmalar, klasik bilimde deneysel "hatalar" veya gürültü (noise) olarak ele alınır. Fakat yapılan çalışmalar, deneysel hataların önemli bilgiler verebileceğini göstermektedir [2].

Matematiksel olarak dinamik bir sistem, bir durum (faz) uzayı ve dinamik olarak adlandırılan bir kuraldan oluşur. Sistemin herhangi bir zamandaki durumu bu kural vasıtasıyla belirlenir. Deterministik bir dinamik sistemin zamandaki durumu, sistemin başlangıç koşulları ve dinamiği tarafından tam olarak tanımlanmaktadır [61].

Deterministik bir dinamik sistem, sürekli veya ayrık bir durum uzayına ve sürekli zamanlı veya ayrık zamanlı bir dinamiğe sahip olabilir [62].

3.1.2.1. Sürekli zamanlı dinamik sistemler

Sürekli zamanlı deterministik bir dinamik sistem aşağıdaki diferansiyel denklem ile tanımlanmıştır.

$$\dot{X}(t) = F(X(t), t) \quad \textbf{(3.1)}$$

$$\dot{\emptyset}(t; X_0, t_0) = F(\emptyset(t; X_0, t_0), t) \quad \textbf{(3.2)}$$

$X(t)$ durum, $\dot{X}(t)$, $X(t)$'nin zamana göre türevi, $X(t_0) = X_0$ başlangıç koşuludur. $\emptyset(.; X_0, t_0)$ ise (3.1) diferansiyel denkleminin (X_0, t_0) yörüngesi veya çözümü olarak tanımlanır. $F(X, t)$ t zamanında X boyunca yörüngenin hızını ve yönünü tanımlayan bir vektör alanıdır. F vektörü $\emptyset$ akışını meydana getirir. t_0 anındaki X_0 noktası, t anında $X(t) = \emptyset_t(t; X_0, t_0)$ akışı tarafından haritalanmıştır.

Sürekli zamanlı deterministik bir dinamik sistemin vektör alanı sadece duruma bağımlı ve zamandan bağımsız ise bu sistem otonomdur denir ve aşağıdaki gibi ifade edilir.

$$\dot{X}(t) = F[X(t)] \quad \textbf{(3.3)}$$

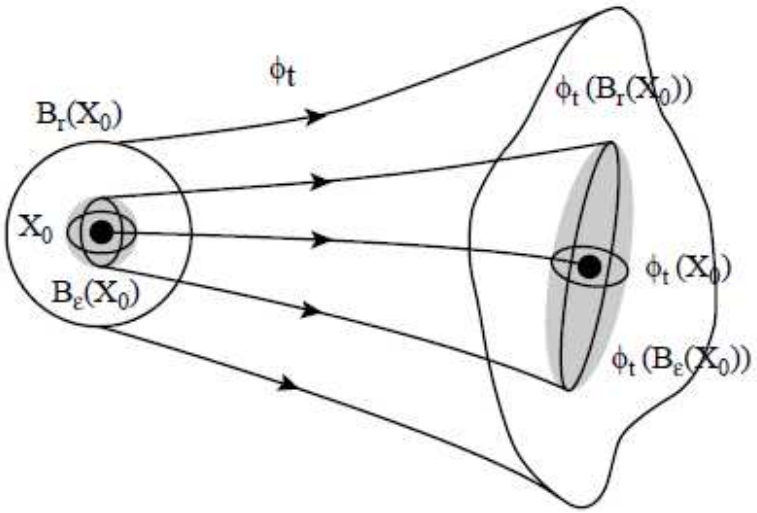
$$\dot{\emptyset}(t, X_0) = F[\emptyset(t, X_0)],\ \emptyset(t, X_0) = X_0 \quad \textbf{(3.4)}$$

Merkezi X_0, yarıçapı r olan $B_r(X_0)$ küresinden çıkan yörüngelerin bir kümesi t süre sonra $\emptyset_t[B_r(X_0)]$ alanı içinde akış tarafından haritalanmıştır. Burada önemli olan (Denklem 3.3) eşitliğinin eşsiz olması için dinamik sistemin yörüngesinin iki farklı yönde aynı iki noktadan geçmemesi gerektiğidir.

n-boyutlu otonom olmayan bir sürekli zamanlı dinamik sistem, ek bir durum değişkeni olarak zaman eklenerek (n+1) boyutlu otonom bir sisteme dönüştürülebilir.

$$\dot{X}(t) = F[X(t), X_{n+1}(t)] \quad \textbf{(3.5)}$$

$$X_{n+1}(t) = 1 \quad \textbf{(3.6)}$$



Şekil 3.1. Otonom bir sürekli zamanlı dinamik sistemin F vektör alanı, durum uzayındaki bir X_0 noktasından t zamanı kadar sonra $\emptyset_t(X_0)$ görüntüsü olarak haritalanan bir akış oluşturur [62].

Özel teknikler uygulanarak, periyodik davranış gösteren otonom olmayan sistemler, otonom sistemler gibi ele alınabilirler [62].

3.1.2.2. Ayrık zamanlı dinamik sistemler

Ayrık zamanlı deterministik bir dinamik sistem aşağıdaki fark denklemi ile tanımlanmıştır.

$$X(k+1) = G(X(k), k) \quad \textbf{(3.7)}$$

$X(k)$ durum, $X(k_0) = X_0$ başlangıç koşulu, $G(.;.)$ ise $X(k)$ durumundan bir sonraki durum olan $X(k+1)$ durumuna geçiş özelliklerini belirleyen haritadır.

(Denklem 3.7), sistemin geçerli olan (şu andaki) durumu verildiğinde, bir sonraki zaman diliminde sistemin durumunun ne olacağını bildirir. Sistemin durumu zamanla değiştiği için, herhangi bir andaki durumu tanımlayan bir notasyona ihtiyaç duyulur. k zamanındaki sistemin durumu $X(k)$ ile tanımlanır. (Denklem 3.7) eşitliği, sistemin başlangıç durumu belirsiz olduğundan, dinamik bir sistemin tam bir tanımı değildir. $X(k_0) = X_0$ başlangıç koşulu ile birlikte, sistemin tam tanımı yapılabilir.

Sürekli zamanlı dinamik sistemlerde olduğu gibi, $G(.;.)$ haritası sadece $X(k)$ durumuna bağlı ve k'dan bağımsız ise otonom bir sistem olarak tanımlanır ve (Denklem 3.8) eşitliği ile ifade edilebilir [2, 62].

$$X(k+1) = G[X(k)] \quad \textbf{(3.8)}$$

3.1.3. Nonlineer sistemler

Lineer ilişkiler grafik üzerinde bir doğru olarak ifade edilir ve bu ilişkilerin mantığını anlamak kolaydır. Nonlineer sistemler genellikle çözüme elverişli değillerdir. Akışkan ve mekanik sistemlerde, nonlineer şartlar, genellikle insanların konuyu basite indirip kolay anlaşılır hale getirmek istedikleri zaman devre dışı bırakmak istedikleri özellikler arasındadır. Bu tür sistemlerdeki karmaşık ilişkiler nonlineerliğin hesaplanmasını zorlaştırmaktadır. Aynı zamanda da lineer sistemlerde hiçbir zaman bulunmayan bir davranış biçimi zenginliği yaratmaktadır [63].

Etrafımızdaki hareketlerin bazıları, bir saat sarkacının sallanması gibi, düzenlidir, kolaylıkla anlaşılır ve ifade edilebilir. Fakat bazıları ise, bir şelalenin akışı gibi düzensizdir ve daha önce belirtilen kurallara aykırı olarak ortaya çıkarlar. Matematikçi Henri Poincare (1892) bu tür problemlerin gerçek kaynağını inceleyen ilk bilim adamıdır. Poincare, "Science and Method" adlı makalesinde şöyle yazmıştır [64]:

"Dikkatimizden kaçan çok küçük bir sebep, görmezden gelemeyeceğimiz çok büyük bir etkiye neden olabilir. Eğer doğanın kurallarını ve başlangıç aşamasında evrenin durumunu kesin olarak bilseydik, sonraki herhangi bir zamanda evrenin durumunu tam olarak tahmin edebilirdik. Doğa kanunlarının bizim için artık hiçbir gizliliğinin kalmadığı bir durumda bile başlangıç durumunu yaklaşık olarak bilmemiz, bir sonraki durumu tahmin etmede bize imkân verirse, kurallarla yönetilen bir olayın tahmin edilebildiğini söyleyebiliriz. Fakat bu anlattığımız gibi değildir. Başlangıç koşullarındaki küçük farklılıklar sonuçta çok büyüklerini üretir. Başlangıçtaki küçük bir hata sonuçta büyük bir hataya sebep olacaktır. Böylelikle tahmin yapmak imkânsız hale gelir ve biz tesadüfî bir olaya sahip oluruz..."

Nonlineer bir dinamik sistemin tanımı, lineer sistemlerde olduğu gibi bir diferansiyel denklem takımı şeklinde yapılabilir. Otonom sistemler için (Denklem 3.1), otonom olmayan sistemler için de (Denklem 3.3) eşitlikleri, nonlineer sistemler için de geçerlidir.

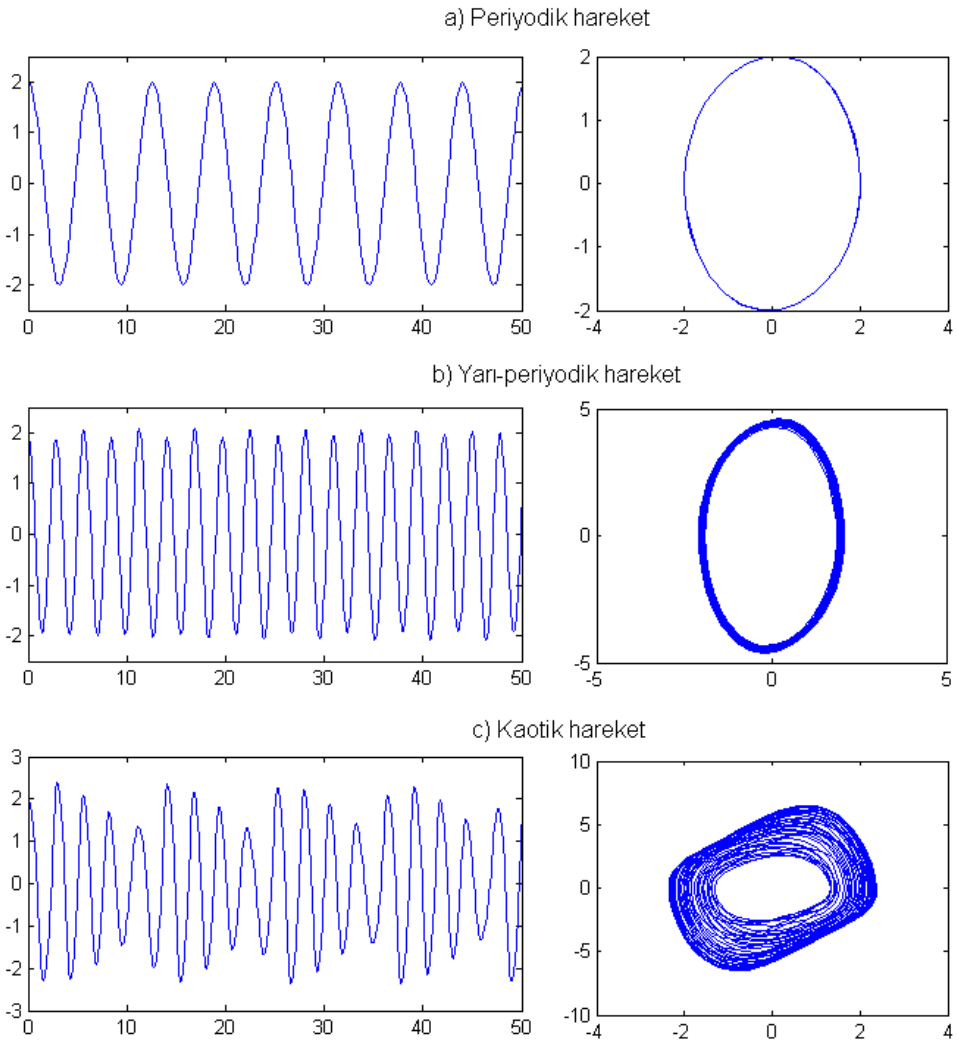
3.1.4. Faz uzayı

Faz uzayı bir dinamik sistemin mümkün olan tüm durumlarının birleşimidir [2]. Bir başka deyişle, durum değişkenleri ve onların türevlerinin oluşturduğu uzaya faz uzayı denir ve zaman ilerlerken faz uzayındaki bir nokta yörünge olarak adlandırılan bir yol izler [65]. Dinamik sistemlerin analiz edilmesinde, yörüngelerin davranışının nasıl olduğu çok önemlidir.

Sistemin dinamiğini tanımlayan yörüngenin oluşturduğu eğriler faz diyagramı veya harita olarak adlandırılır. Herhangi bir yörünge, zaman sonsuza giderken, asimptotik olarak faz uzayının bir alt kümesine yöneliyorsa, böyle bir altküme "çekici" olarak adlandırılır [1]. Çekicinin geometrik durumu, sistem karakteristiği hakkında önemli bilgiler verir. Kararlı periyodik sistemlerin zaman içindeki davranışları kestirilebilir ve faz uzayındaki eğriler kapalı bir göz şeklindedir. Bu durum limit döngü olarak adlandırılır. Eğer zaman serisinde iki frekans bileşeni varsa, çekici bir simidi (torus) gösterecektir. Daha fazla frekans bileşeninin olması durumunda, çekici n boyutlu bir simit olarak şekillenir. Bu tür sistemler yarı-periyodik sistemlerdir. Doğrusal olmayan kaotik bir sisteme ait çekici, simit ve limit döngüden oldukça farklı dinamiklere sahiptir. Bu durumda çekici, "tuhaf çekici" olarak adlandırılır ve sonsuz sayıda gözden meydana gelen karmaşık bir şekil olarak ortaya çıkar. Yörüngeler asla aynı nokta üzerinden birden fazla geçmezler, periyodik olmayan bir durumu ifade ederler ve bütün faz uzayını doldurmazlar.

Faz uzayında kapalı bir göz olarak ortaya çıkan limit döngüler düzenli modeller olduğundan, bu eğrilerin birbirine yakınsama ve ıraksamasının ortalama üstel oranı (Lyapunov üsteli) sıfır olacaktır [66]. Kaotik sistemlerde eğriler birbirini izlemez fakat sıfırdan büyük bir ortalama üstel ıraksama oranına sahiptir. Ayrıca doğrusal olmayan

kaotik sistemlerin çekicileri fraktal (parçalı) bir geometriye sahiptir [1, 67, 68]. Şekil 3.2 sırasıyla periyodik, yarı-periyodik ve kaotik bir sistemin zamana göre değişimini ve faz uzayını göstermektedir.



Şekil 3.2. Van Der Pol osilatörünün a) periyodik, b) yarı-periyodik ve c) kaotik durumları [67].

Dinamik sistemlerin anlaşılmasında, faz uzayındaki "denge noktası" önemli olan diğer bir kavramdır. Durum değişkenlerinin sayısı, faz uzayının boyutunu belirler. 3 boyutlu faz uzayına sahip olan bir dinamik sistem aşağıdaki diferansiyel denklem takımı ile ifade edilebilir.

$$\dot{x} = f(x, y, z)$$
$$\dot{y} = g(x, y, z) \quad \textbf{(3.9)}$$
$$\dot{z} = h(x, y, z)$$

f, g, h; x, y, z değişkenlerine bağlı fonksiyonlardır.

Denge noktaları; durum değişkenlerinin tümünün zamana göre türevlerinin sıfır olduğu, faz uzayındaki noktalar olarak tanımlanırlar. (Denklem 3.10) cebirsel denklem takımının çözümü ile sistemin denge noktaları tespit edilir [69].

$$f(x, y, z) = 0$$
$$g(x, y, z) = 0 \quad \textbf{(3.10)}$$
$$h(x, y, z) = 0$$

N boyutlu faz uzayına sahip bir dinamik sistem genelleştirilerek;

$$\frac{dx_i}{dt} = F_i(x) \quad \textbf{(3.11)}$$

şeklinde yazılabilir. i=1,2,…,N. $F_i(\vec{x}) = 0$ denklemi çözülerek, $\vec{x}$ sabit vektörleri hesaplanabilir. Hesaplanan $\vec{x}$ değerleri denge noktalarını vermektedir. Denge noktaları aynı zamanda kritik noktalar olarak da adlandırılırlar.

Kritik nokta civarındaki yörüngeler, bu noktaya yaklaşıyor ise sistem asimptotik olarak kararlıdır; kritik noktadan uzaklaşıyor ise sistem kararsızdır. Bu yörüngeler, kritik nokta civarında bir yörüngede kalıyorsa, bu sefer sistem kararlıdır ancak asimptotik olarak kararlı değildir. Eğer bir periyodiklik yok ise, kritik olmayan bir noktadan geçen bir yörünge, kendini asla kesmez [2, 69].

3.1.5. Lyapunov üstelleri

$\dot{x} = f(x)$ fonksiyonu x_0 denge noktasında Taylor serisine açılırsa;

$$f(x) = f(x_0) + (x - x_0)\frac{df}{dx} + \frac{1}{2}(x - x_0)^2\frac{d^2f}{dx^2} + \frac{1}{6}(x - x_0)^3\frac{d^3f}{dx^3} + \cdots \quad \textbf{(3.12)}$$

elde edilir. (Denklem 3.12)'de birinci mertebeden daha yüksek mertebeli türevler ihmal edilirse;

$$f(x) = f(x_0) + (x - x_0)\frac{df}{dx}\Big|_{x_0} + E(x - x_0) \quad \textbf{(3.13)}$$

yazılabilir. Burada E, hata fonksiyonudur ve $x \to x_0$ iken $E(x - x_0) \to 0$ olması beklenir. Hata fonksiyonunun $(x - x_0)$ 'dan küçük olması için;

$$\frac{E(x - x_0)}{x - x_0} \to 0$$

olmalıdır. (Denklem 3.13)'den;

$$\frac{f(x) - f(x_0)}{x - x_0} + \dot{f}(x_0) = \frac{E(x - x_0)}{x - x_0} \quad \textbf{(3.14)}$$

elde edilir. Türev tanımından;

$$\dot{f}(x_0) = \lim_{x \to x_0} \frac{f(x) - f(x_0)}{x - x_0}$$

olarak yazılırsa, $x \to x_0$ iken;

$$\frac{E(x - x_0)}{x - x_0} \to 0$$

olur [2, 63]. Yörüngelerin denge noktasından uzaklığı $\Delta x = x - x_0$ şeklinde tanımlanırsa (Denklem 3.15) elde edilir.

$$\frac{d}{dt}\Delta x = \dot{f}(x_0)\Delta x \tag{3.15}$$

$$\lambda = \left.\frac{df(x)}{dx}\right|_{x_0} \tag{3.16}$$

λ, denge noktasının karakteristik değeridir ve (Denklem 3.16) şartları altında, (Denklem 3.15)'in çözümü;

$$x(t) = x(0)e^{\lambda t} \tag{3.17}$$

olur. Buna göre $\lambda < 0$ iken, yörüngeler denge noktasına üstel olarak yaklaşır; $\lambda > 0$ olduğunda ise denge noktasından üstel olarak uzaklaşır. Denge noktasının bir civarı için λ, Lyapunov üsteli olarak adlandırılır. (Denklem 3.17)'nin çözümü ile;

$$\lambda = \lim_{t\to\infty} \frac{1}{t} ln \frac{x}{x_0} \tag{3.18}$$

Lyapunov üsteli bulunur [2, 69].

Ayrık zamanlı dinamik sistemler için de benzer bir analiz yapılabilir. Sürekli zamanlı dinamik sistemlerdeki diferansiyel denklemler, ayrık sistemlere dönüştürüldüğünde;

$$\lambda = \lim_{k\to\infty} \frac{1}{k} ln \frac{x_k}{x_0} \tag{3.19}$$

şeklinde yazılabilir.

Dinamik bir sistemin davranışlarının çözümünde Lyapunov üstelleri önemli bir kriterdir. Bir sistemin kaotik olup olmadığı Lyapunov üstellerine bakılarak söylenebilir. i boyutlu bir dinamik sistemin i adet Lyapunov üsteli vardır. Lyapunov

üsteli pozitif ise, başlangıç şartları arasındaki fark yörünge boyunca özel bir yönde büyüyecektir. Kararlı bir sürekli hal davranışı için daralma, genişlemeden fazla olmalıdır. Bu yüzden i boyutlu bir dinamik sisteme ait bütün Lyapunov üstellerinin toplamı sıfırdan küçüktür. Bununla birlikte, bir sistemin kaotik olması için en az bir λ değeri pozitif olmalıdır [1, 2, 59, 69].

Eğer λ negatif ise farklı başlangıç şartları aynı çıkış değerlerini vermeye meyillidir ve dolayısıyla gelişme kaotik değildir. Eğer λ pozitif ise farklı başlangıç değerleri farklı çıkış değerleri verir, yani hareket kaotiktir.

Bir kaotik sistemin temel karakteristiği, başlangıç şartlarına hassas bağımlılığıdır. Verilen iki farklı başlangıç durumu birbirine çok yakın bile olsa, bu iki noktada oluşan yörüngeler üstel olarak artan bir ayırımla birbirlerinden uzaklaşırlar. Lyapunov üstelleri, kaotik sistemler için başlangıç durumlarındaki hassas bağımlılığı ölçmek için kullanılır [1].

3.1.6. Çatallaşma

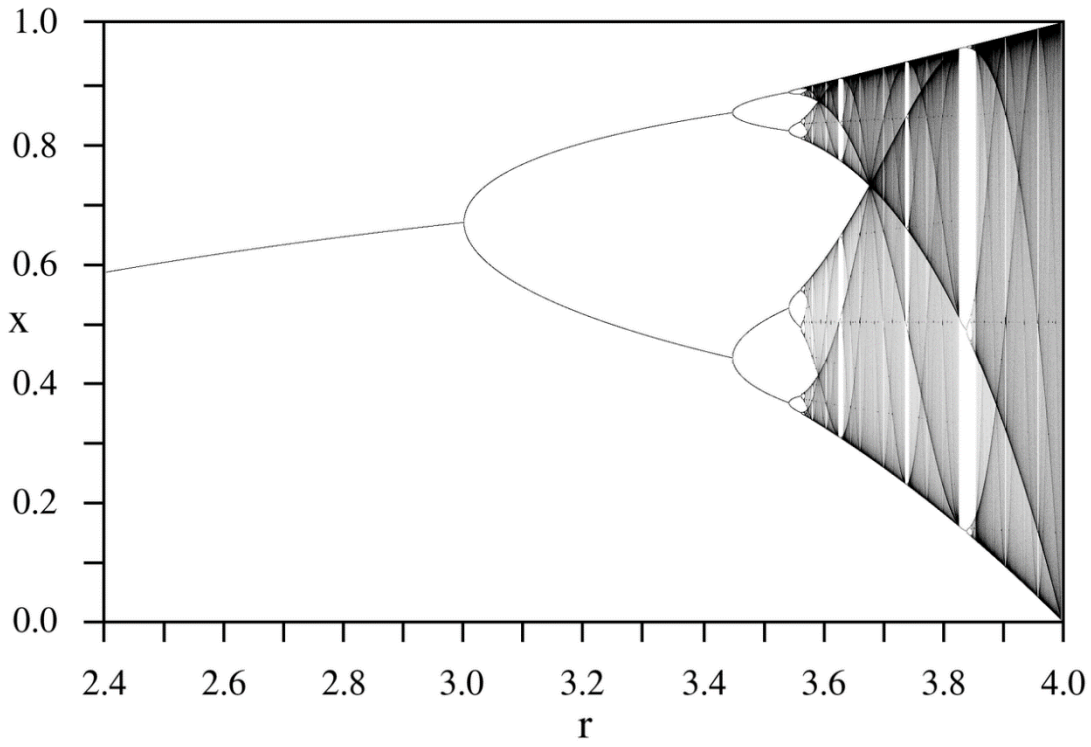
Çatallaşma (bifurcation) terimi, dinamik sistemlerde meydana gelen sistem parametrelerindeki en ufak değişimlerin, faz uzaylarındaki yapısal değişimlerine karşılık gelir. Böyle bir değişimde meydana gelen parametre değeri, kritik parametre değeri olarak adlandırılır. Çatallaşma terimi ilk olarak bir grup diferansiyel denklem eşitliklerinin denge çözümlerinin bulunduğunu tanımlamak için kullanılmıştır [70].

Çatallaşma teorisi, doğrusal olmayan sistemlerin çözümünde anahtar rol oynamaktadır. Sistemdeki anlık değişiklikler, sistemi kararlı normal durumundan artarak uzaklaştırmakta, bu da kaos olaylarını beraberinde getirmektedir. Bir sistemin dinamik davranışı bir parametre değişimiyle değiştirildiği zaman sistemde çatallaşmalar doğmaktadır [1].

Bir çizgi üzerindeki vektör alanlarının dinamiği çok sınırlıdır; tüm çözümler ya bir dengeye oturur ya da $\pm\infty$'a gider. Dinamiğin bu basitliği yanında tek boyutlu sistemlerin ilginçliği parametrelere olan bağlılıktır. Akışın nitel özellikleri

parametrelerdeki değişime bağlı olarak değişebilir. Yani sabit noktalar oluşturulabilir, yok edilebilir veya bu noktaların kararlılığı değişebilir. Dinamikteki bu değişmelere çatallaşma, değişimin görüldüğü parametre değerlerine de çatallaşma noktaları denir [70, 71].

Çatallaşma olaylarını sürekli hal ve süreksiz hal çatallaşma olayları olarak sınıflandırmak çok yararlıdır. Süreksiz çatallaşma olayları durumunda sistem nominal değerinden sonsuz bir değere ulaşmaktadır [58].



Şekil 3.3. Çatallaşma diyagramı [116].

Çatallaşmanın birçok çeşidi vardır. Çoğu pratik mühendislik sistemleri için en ilgi çekicisi, yerel çatallaşmadır. Bu yerel çatallaşma bir denge durumunda kararlılığını kaybetmesiyle oluşur. Global çatallaşma ise, durum uzayında bazı domenlerde meydana gelir. Sadece denge noktalarında oluşan çatallaşmalar, ikiye ayrılmalar, stasyoner ya da statik çatallaşma olarak bilinmektedir. Hopf çatallaşması gibi denge ve periyodik çözümleri içeren çatallaşmalar da bulunmaktadır.

Çatallaşma diyagramı bir veya daha fazla parametre değiştirildiğinde, kararlı-hal çözüm tipinin değişimini temsil eder. Kararlı-hal çözüm tipi genellikle, parametre değiştiğinde gözlenebilen uç noktaları göstermek yoluyla temsil edilir. Kararlı-hal çözümünün niteliksel değişimine karşılık gelen bir çatallaşma, çatallaşma diyagramında kolaylıkla ayırt edilebilir. Çatallaşma diyagramlarının ana kullanım amaçlarından biri de üzerinde düşünülen sistemin kaos rotalarını tespit etmektir [1].

3.1.7. Kaosun kuralları

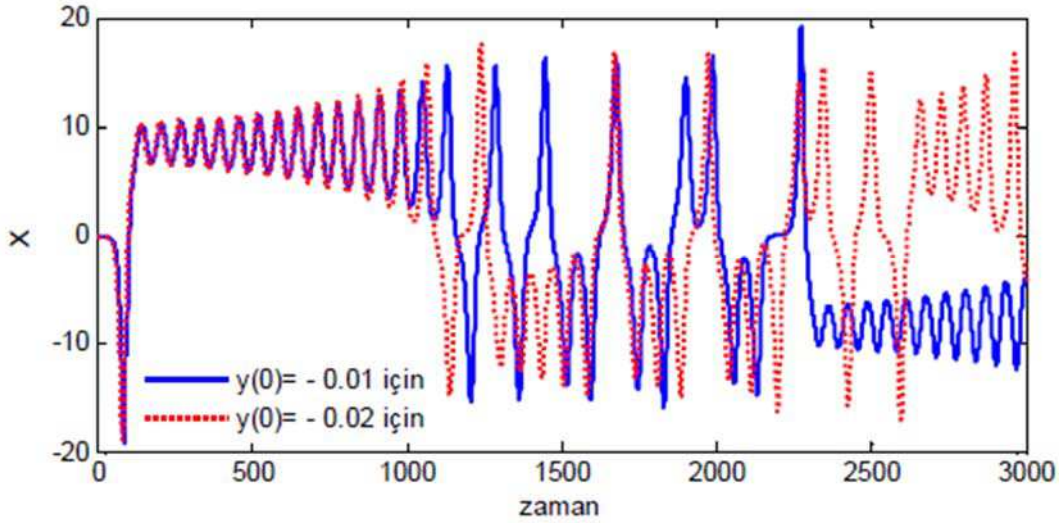
Kaotik bir davranışın temel özellikleri;

- Başlangıç şartlarına aşırı duyarlılık göstermesi,
- Rastgele değil deterministik tipte olması,
- Sınırsız sayıda değişik periyodik salınımlar içermesi,
- Gürültü sinyali veya benzeri güç spektrumuna sahip olması,
- Genliği ve frekansı tespit edilemeyen ancak sınırlı bir alan içerisinde değişen karmaşık davranışlar olmasıdır [72].

Bir sistemin kaotik olup olmadığına karar vermek için yukarıda sayılan kriterleri sağlayıp sağlamadığına bakılmalıdır. Başlangıç şartlarına aşırı duyarlılık, birçok alanda kaotik sistemlerin kullanılmasını teşvik etmektedir. Kaotik Lorenz sisteminin, başlangıç şartlarındaki çok küçük bir değişiklik ile nasıl farklılaştığı Şekil 3.4'te [1] gösterilmektedir.

Dinamik sistemlerde kaosun varlığını tespit için çeşitli yöntemler vardır. Bunlardan en çok kullanılanlar aşağıda sıralanmıştır [73].

- Zaman serileri analizi,
- Faz diyagramları (haritalar),
- Poincare haritaları,
- Güç spektrumu analizi,
- Lyapunov üstelleri,
- Çatallaşma diyagramları.



Şekil 3.4. Kaotik sistemlerin başlangıç şartlarına olan duyarlılığı için bir örnek [1].

3.1.7.1. Zaman serileri analizi

Bu yöntem, kaosun varlığını tespit etmek için kullanılan en basit ve görsel bir yöntemdir. Bu yöntemde, dinamik sistemin durum değişkenlerinin zamana göre değişimi gözlemlenir. Zaman serileri olarak adlandırılan bu değişime ait grafikler düzensiz ve tahmin edilemez davranışlar gösteriyorsa, sistem kaotiktir. Aksi halde sistem kaotik değildir. Şekil 3.5'de [74] kaotik ve kaotik olmayan zaman serilerine ait grafikler gösterilmektedir.

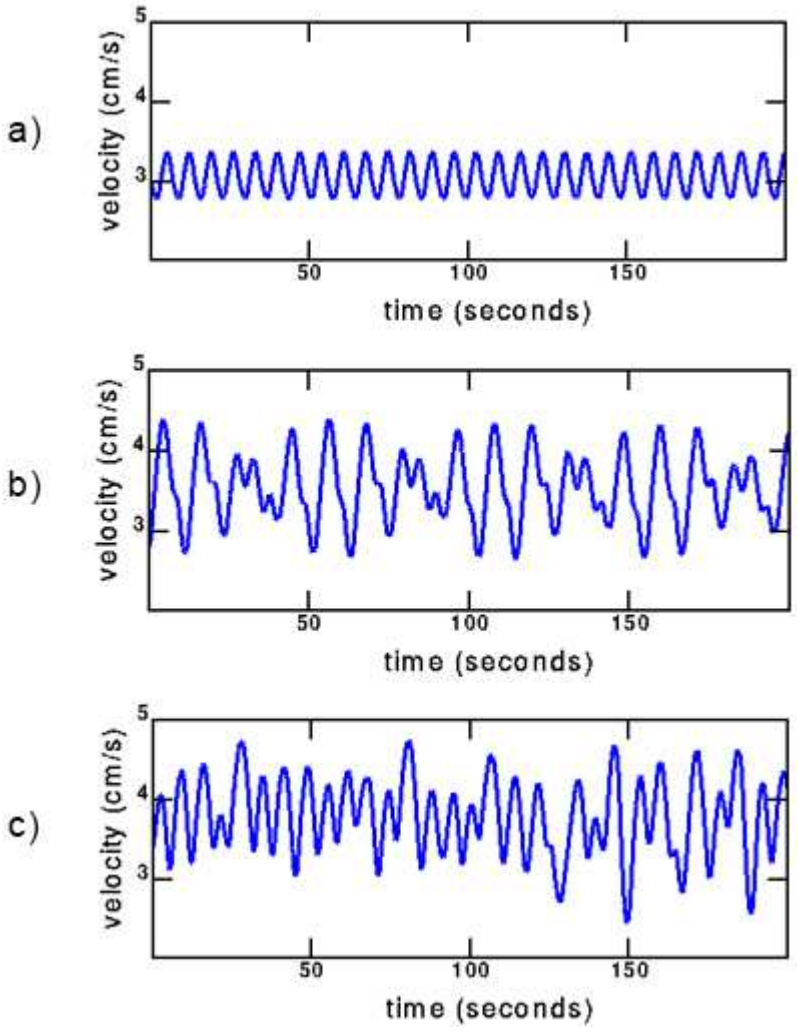
Bu yöntem her ne kadar en basit yöntem de olsa, genellikle bir sistemin kaotik olup olmadığını belirlemek için yeterli değildir. Çünkü bu yöntem ile yapılacak tespit, ancak analiz edilen zaman aralığı için geçerli olacaktır. Sistemin tamamının veya tamamını temsil eden bir kısmının incelenmesi genellikle mümkün değildir. Ayrıca, gözlemlenen grafiğin periyodik, yarı periyodik veya kaotik olup olmadığına karar vermek her zaman mümkün olmayabilir; karar verilse bile bu işaretin deterministik bir işaret mi yoksa rastgele bir işaret mi olduğunun belirlenmesi gerekir.

3.1.7.2. Faz diyagramları analizi

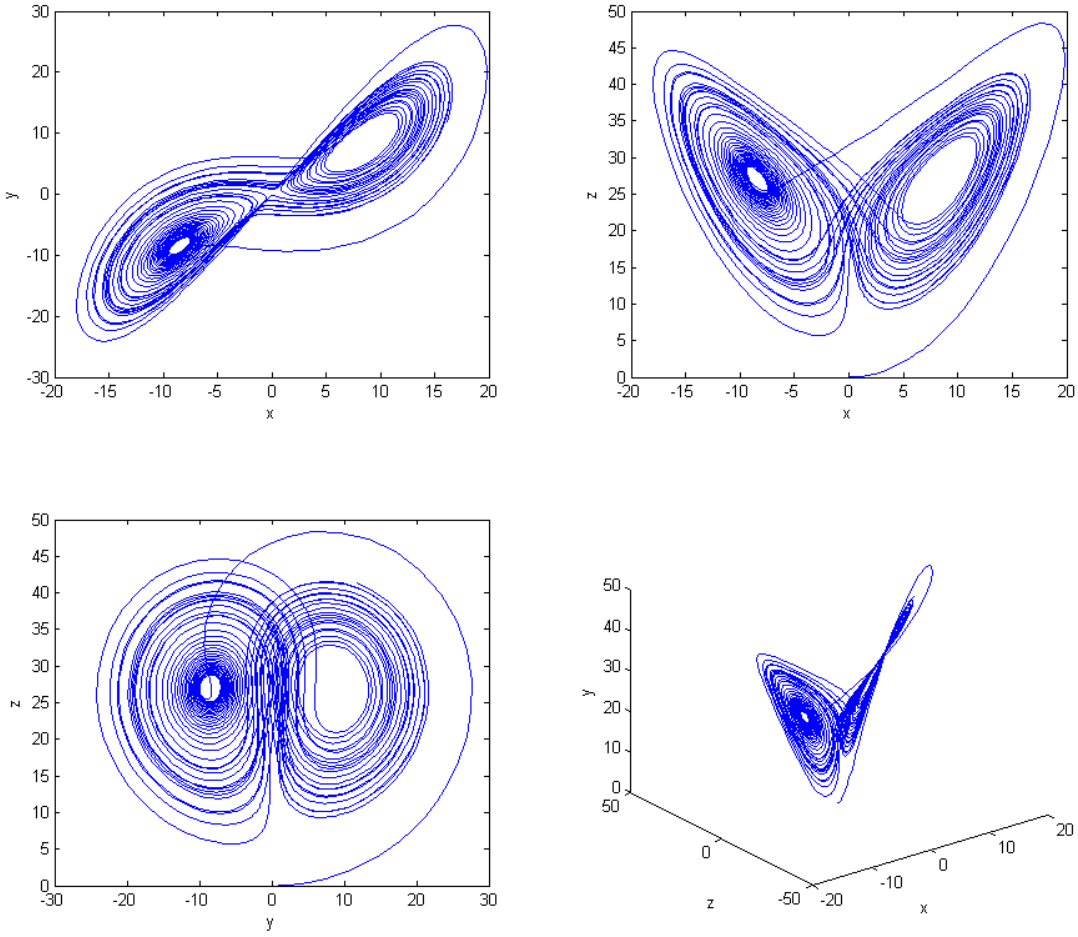
Faz diyagramı veya harita, sistemin bir durum değişkeninin diğerleri ile olan anlık ilişkilerinin bir görüntüsü olarak ifade edilebilir [75]. Faz diyagramının boyutu,

sistemin boyutu ile aynıdır. Örneğin, üç durum değişkeni olan üç boyutlu bir sistemin iki ve üç boyutlu faz diyagramları çizilebilir. Şekil 3.6'da, üç boyutlu Lorenz sistemine ait mümkün olan bütün faz diyagramları çizilmiştir. Bölüm 3.1.4'te açıklandığı üzere, faz diyagramları limit döngü, simit (torus) veya tuhaf çekici olarak adlandırılan karmaşık bir yapıda olabilir. Kaotik bir sistemin haritasını oluşturan yörüngeler, zaman ilerledikçe faz uzayını doldurmaya başlar ancak hiçbir zaman birbirini kesmeden tekrar ederler.

Faz diyagramları da, zaman serileri analizinde olduğu gibi, kaosun tespitinde tek başına yeterli olmayabilir. Bir sistemin hem zaman serisi analizinin yapılması hem de faz diyagramlarının çizilmesi, kaosun varlığını tespit etmede daha etkili olmasına rağmen yine de yetersizdir.



Şekil 3.5. a) Periyodik, b) yarı-periyodik, c) kaotik zaman serileri [74].



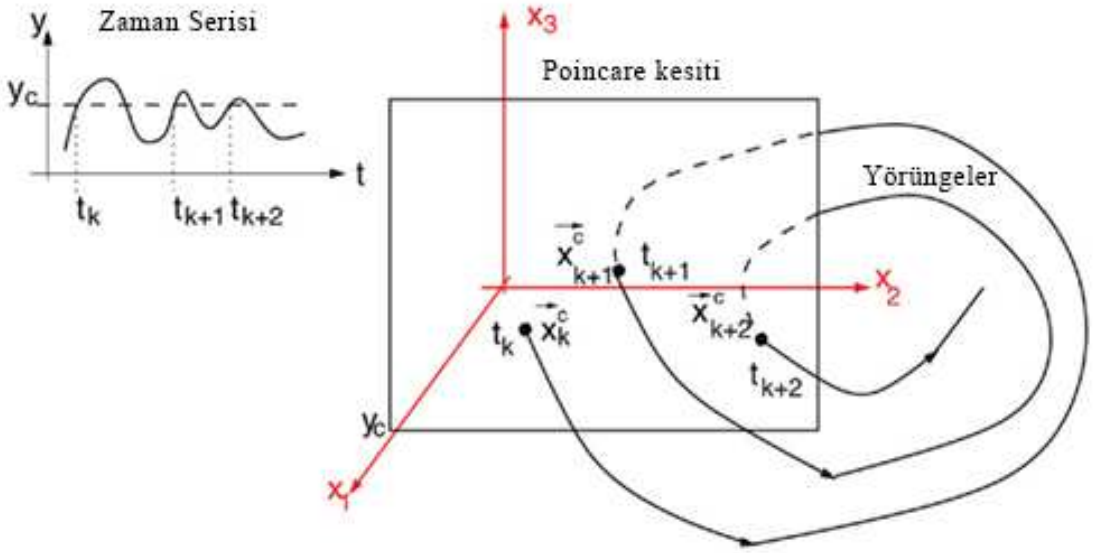
Şekil 3.6. Kaotik Lorenz sistemine ait faz diyagramları.

3.1.7.3. Poincare haritaları

Dinamik bir sistemin faz uzayındaki davranışı, faz uzayı belirli bir düzlemle kesilerek, yörüngelerin bu düzlemi kestiği noktaların oluşturduğu bir geometrik harita şeklinde de gözlemlenebilir. Bu yöntemde, n-boyutlu bir dinamik sistem, (n-1) boyutlu bir sisteme dönüştürülmektedir. Bu sayede, karmaşık sistemlerin analizi daha kolaylaşmaktadır. Zaman serisi verilmiş bir sistemin, faz diyagramından Poincare haritasının oluşturulması Şekil 3.7'de gösterilmektedir.

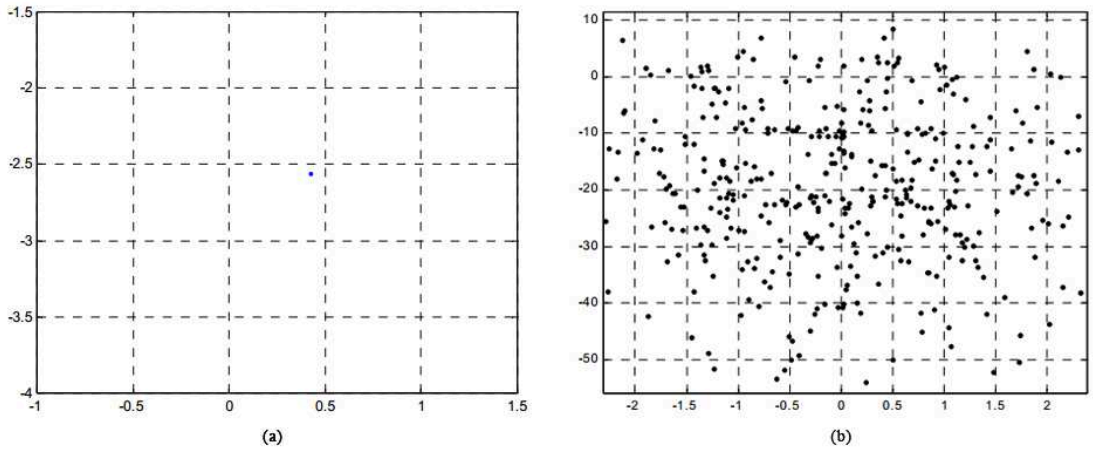
Poincare haritasını oluştururken belirlenecek düzlemin (Poincare kesiti) seçimi için belirli bir kural yoktur. Burada önemli olan, yörüngelerden belirli zaman aralıklarında örnek alabilmektir. Yörüngenin, Poincare kesiti ile kesiştiği noktalar kümesi, Poincare haritasını oluşturacaktır. Poincare haritası noktalardan oluşan bir harita olduğundan, sürekli zamanlı sistem, ayrık zamanlı bir sisteme dönüştürülmüş olacaktır. Çoğu

durumda, ayrık zamanlı bir sistemi analiz etmek, sürekli zamanlı bir sistemi analiz etmekten daha kolaydır.



Şekil 3.7. Poincare haritasının oluşturulması [76].

Poincare haritasına bakarak sistemin durumu hakkında yorum yapılabilir. Periyodik bir davranış Poincare haritalama yöntemi ile incelenirse, sabit bir nokta; yarı periyodik bir davranış, kapalı bir eğri; kaotik bir davranış ise kapalı olmayan, belirli alanlarda yoğunlaşmış fraktal (parçalı) bir şekilde olacaktır [67, 72, 73]. Şekil 3.8 periyodik ve kaotik sistemlere ait Poincare haritalarını göstermektedir.



Şekil 3.8. a) Periyodik, b) kaotik bir sisteme ait Poincare haritası [73].

Bu yöntem, daha önce anlatılan diğer iki yöntemi de kapsamaktadır. Yani, Poincare haritasını oluştururken hem zaman serileri hem de faz diyagramları bilinmektedir. Bu, üç yöntemin, aynı anda değerlendirilebileceği anlamına gelmektedir. Kısacası, bir sistemdeki kaos varlığı Poincare haritasına bakılarak büyük oranda tespit edilebilir.

3.1.7.4. Güç spektrumu analizi

Dinamik sistemler zaman ve frekans boyutunda analiz edilebilirler. Spektrum teknikleri veya Fourier dönüşümü ile bu iki boyut arasında bir ilişki kurulabilir. (Denklem 3.20) ve (Denklem 3.21) sırasıyla sürekli ve ayrık zamanlı sistemler için Fourier dönüşümünü göstermektedir.

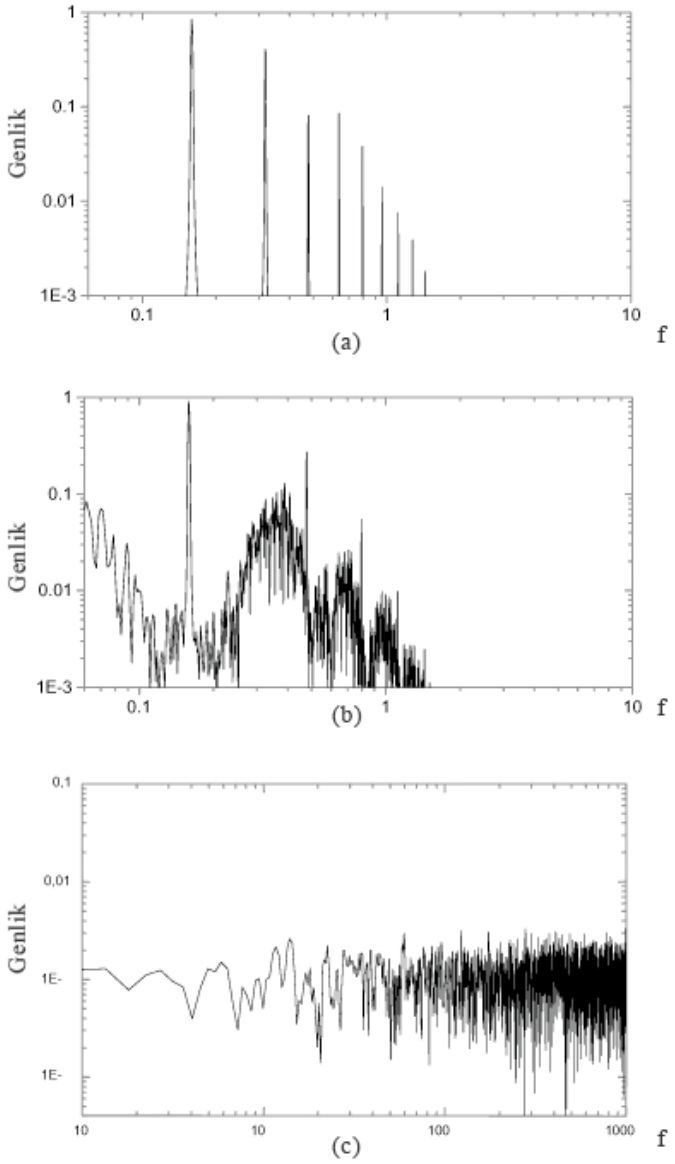
$$X(f) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} x(t) e^{j2\pi f t} dt \qquad \textbf{(3.20)}$$

$$X_k = \frac{1}{\sqrt{N}} \sum_{n=1}^{N} x_n e^{j2\pi kn/N} \qquad \textbf{(3.21)}$$

X, durum değişkeni; t, zaman; f, frekanstır. Ayrık zamanlı sistem için; k= - N/2,…,N/2 ve Δt örnekleme aralığı olmak üzere $f_k = k/N\Delta t$'dir.

Buna göre, güç spektrumu periyodik bir işaret için (f, 2f, 3f,…) frekanslarında ve genliği gittikçe zayıflayan piklerden oluşacaktır. Yarı periyodik bir işaret için ise (f_1, f_2 ve bunların tam katları) frekans bileşenleri benzer şekilde zayıflayan genliklerle gözlemlenecektir. Kaotik bir işaret için güç spektrumu ise geniş bir bant için yükseklik ve genişlikleri rastgele olan piklerden oluşur. Şekil 3.9, periyodik, kaotik ve rastgele bir işaret için güç spektrumlarını göstermektedir [72, 73, 77].

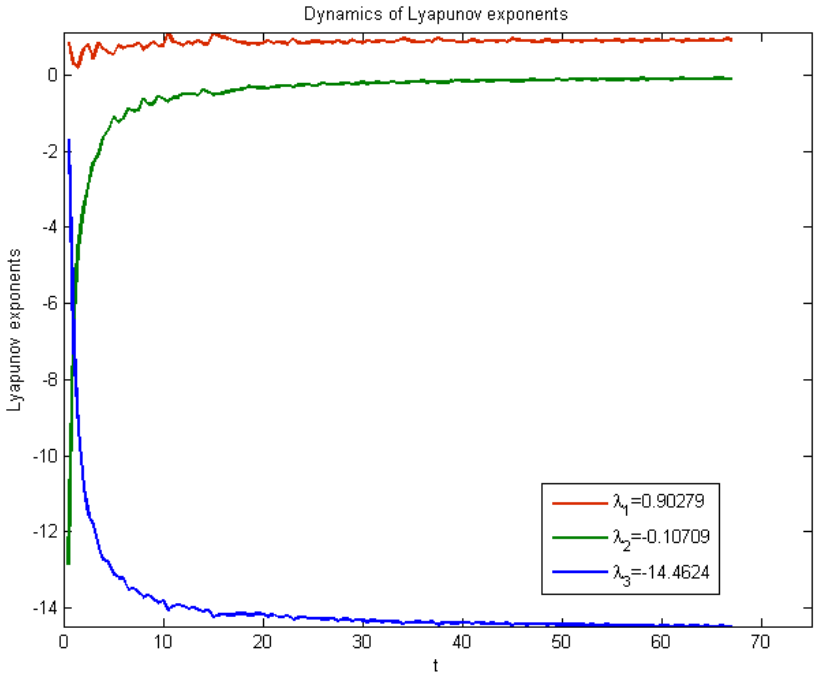
Güç spektrumu analizi ile periyodik, yarı-periyodik ve kaotik işaretleri ayırt etmek kolaydır. Ancak, gürültü benzeri rastgele işaretleri kaotik işaretlerden ayırt etmek güç olabilir. Kaotik işaretler deterministik bir yapıda oldukları için rastgele işaretlerden daha düzenli bir spektrum grafiğinin olması beklenir.



Şekil 3.9. a) Periyodik, b) kaotik, c) rastgele bir işaretin güç spektrumları [77].

3.1.7.5. Lyapunov üstelleri analizi

Bölüm 3.1.5'de kaotik sistemlerin varlığının tespiti için Lyapunov üstellerinin toplamının sıfırdan küçük, ancak en az bir tanesinin pozitif olması gerektiği açıklanmıştı. Burada, kaotik Lorenz sistemine ait Lyapunov üstelleri farklı başlangıç koşulları için analiz edilmiş x(0) = -14,772; y(0) = -4,6602; z(0) = 43,5162 değerleri için Şekil 3.10'da gösterilmiştir..



Şekil 3.10. x(0)=-14,772; y(0)=-4,6602; z(0)=43,5162 iken Lyapunov üstelleri.

Lyapunov üstelleri analizi, kaosun varlığının kesin olarak tespit edilmesinde çok etkili ve yeterli bir yöntemdir.

Bu yöntemlerin haricinde, çatallaşma diyagramlarına bakılarak da kaosun varlığı tespit edilebilir.

3.1.8. Kaotik Lorenz sistemi

Atmosfer olaylarını inceleyen meteorolojist Edward Lorenz, 1963'de havanın ısı değişimini belirlemek için bulduğu bir dizi denklem takımının çözümünü arıyordu. Lorenz, ele aldığı dinamik sistem için başlangıç koşullarında oluşacak küçük değişimlerin sonuca çok büyük etkiler yaptığını gözlemledi. Böylece, uzun süreli hava tahminleri yapmanın olanaksız olduğunu ortaya koydu. Lorenz'in bulmuş olduğu bu dinamik sistem, doğrusal olmayan, birinci dereceden üç diferansiyel denklem takımından (Denklem 3.22) oluşmaktaydı ve başlangıç şartlarına hassas bağımlılık ve kaos gösteren ilk sistemdi.

$$\dot{x} = \sigma.(y - x)$$
$$\dot{y} = a.x - y - x.z \quad \textbf{(3.22)}$$
$$\dot{z} = x.y - b.z$$

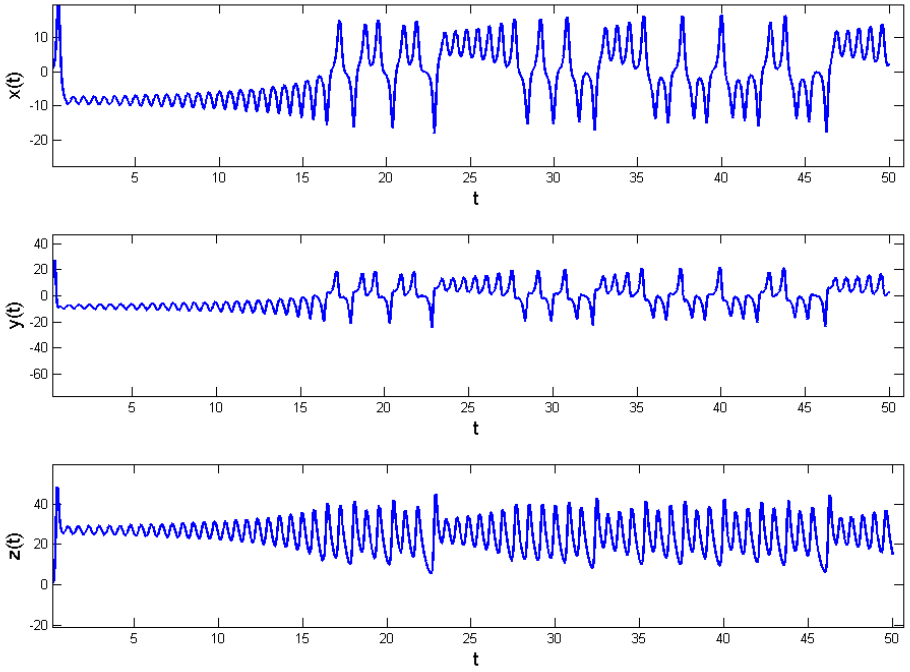
x, y, z durum değişkenleri, σ, a ve b skalar parametrelerdir. Lorenz, bu sistemin çözümü için, zaman Δt≈dt kadar değiştiğinde, x, y ve z değişkenlerinin aldığı yeni değerlerin (X,Y,Z noktalarının) üç boyutlu uzayda çizdiği yörüngeleri bilgisayarla çizdi. Lorenz, dt = 0,02, σ = 5, a = 15, b = 1 kabulüyle, (Denklem 3.23)'deki gibi bir analiz gerçekleştirmiştir.

$$X = x + \Delta x \approx x + dx = x + \sigma.(y.dt - x.dt))$$
$$Y = y + \Delta y \approx y + dy = y + a.x.dt - y.dt - x.z.dt \quad \textbf{(3.23)}$$
$$Z = z + \Delta z \approx z + dz = z + x.y.dt - b.z.dt$$

Ortaya çıkan grafik (Şekil 3.6), kendi kendisini hiç kesmiyor ve iki nokta civarına yığılıyordu. Bu yığılma noktalarına Lorenz Çekerleri (attractor) ya da Garip Çekerler denir [1, 2, 59, 78].

Kaos'u anlamak için, en temel sistem olan Lorenz sistemini incelemek yararlı olacaktır. Bu sistem kaos alanındaki teorik ve deneysel çalışmalara öncülük etmiştir. Baykuş gözlerini ya da kelebek kanatlarını andıran bu sihirli şekil kaosun ilk kaşifleri tarafından bir sembol olarak benimsenmiştir. Düzensiz bir veri akışının içinde sağlam ve güzel bir yapının saklı bulunduğu bu şekil sayesinde kaos açıklanmış olmaktadır. Sistem hiçbir zaman aynı şekilde tekrar etmediği için, sistem yörüngesi kendi kendisiyle asla kesişmez. Tam tersine sonsuza kadar kendi etrafında sarılmaya devam eder. Çekici üzerindeki bu hareket soyut olmasına rağmen, gerçek sistemin hareketi hakkında bir fikir vermektedir [1].

Lorenz'in bulduğu sistemin kaotik olduğu, Lyapunov üstelleri hesaplanarak Şekil 3.10 ve Tablo 3.1'de gösterilmektedir. Üç boyutlu kaotik Lorenz çekicisine ait zaman serileri Şekil 3.11'de verilmiştir.



Şekil 3.11. σ = 10, a = 8/3, b = 28, x(0)=0, y(0)=1, z(0)=0 iken Lorenz çekicisine ait zaman serileri.

Lorenz kaosu yeniden keşfedince, kaos örnekleri arayanlar çoğaldı. Farklı kaotik çekiciler geliştirildi. Bunlardan en çok bilinenleri, Rossler, Chua, Duffing, Chen, Van Der Pol, Rikitake, Colpits, Rucklidge, Henon, Horseshoe vb. olarak sayılabilir.

3.2. Haberleşme Sistemlerinde Kaos

Haberleşmede, "bilgi" enerjisi elektrik enerjisine dönüştürülür ve uzak mesafelere taşınır. Hedefte de bu gelen elektrik enerjisi tekrar orijinal şekline dönüştürülür. Orijinal bilgi enerjisi öncelikle elektronik bilgi sinyalini üretmek için elektriksel forma dönüştürülür. Bu işlem verilen herhangi bir enerji şeklini başka bir enerji şekline dönüştüren dönüştürücüler ile yapılır. Modern bir iletişim sisteminde, bilgi gönderilmeden önce sıraya konur, işlenir ve korunur. Gerçek anlamda gönderme işlemi gürültünün filtrelenmesi gerçekleştirildikten sonra sağlanır. Son safhada kod çözme, mesajı koruma ve bilgi algılama basamaklarından oluşan alma işlemi gelir.

Haberleşme sistemlerinde kaos dinamiğinin kullanılması, güvenli bilgi aktarımının araştırılması sonucu ortaya çıkmıştır. Kaos dinamiklerinin girişe olan hassas

bağımlılığı ve doğrusal olmayan yapıda olması, haberleşme sistemlerinde bilgi işaretinin kaotik işaretler ile taşınması fikrini ilgi çekici bir konu haline getirmiştir.

Kaotik sinyallerin karakteristiği olan geniş bantlılık ve gürültüye benzer özelliğe sahip olma, haberleşme sistemlerinde modülasyon için güvenli bir ortam oluşturmuştur. Haberleşme alanında oldukça popüler olan Code Division Multiple Access (Kod Bölmeli Çoklu Erişim)'e benzer bir yöntem ile kaotik dalga üzerinden bilgi sinyalinin modülasyonu güvenli ve gizli haberleşme amaçlı olmak üzere analog ve dijital sistemler üzerinde gerçekleştirilmektedir [79].

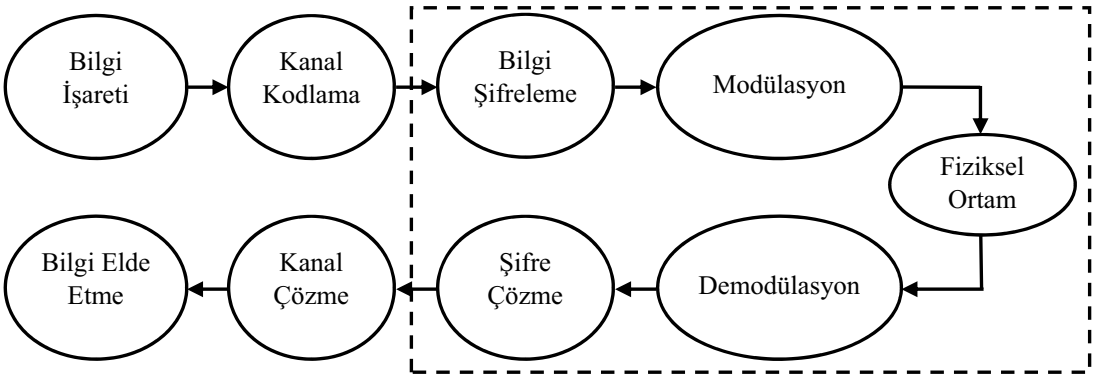
Elektronik devreler, sürekli zamanlı deterministik bir dinamik sistem olarak modellenebilirler. Devrenin karakteristikleri, durum denklemleri olarak adlandırılan tipik bir diferansiyel denklem takımı tarafından tanımlanır [62]. Kaotik sistemin dinamikleri de elektronik bir devrede tanımlanabilir. Böyle bir devre kaotik osilatör devresi olarak adlandırılmaktadır.

Haberleşme sistemlerinde kaos kullanarak veriyi taşıma ve şifreleme fikri, iki adet farklı kaotik osilatörde senkronizasyonun mümkün olabileceğinin Pecora ve Carroll tarafından gösterildiği 1990 yılında ortaya çıkmıştır [3]. Haberleşme konusunda yapılan ilk çalışma ise kaotik maskelemedir. 1993'de, Cuomo ve Oppenheim[4, 80], Lorenz denklem sistemini kullanarak güvenli haberleşme sistemini kurdular ve gösterdiler. Cuomo ve Oppenheim'ın Lorenz devresini kullanmalarına karşın, aynı kavramsal yaklaşımı Kocarev ve arkadaşları [81] kaotik sistem olarak Chua devresini kullanarak gerçekleştirmişlerdir. Bu çalışmaların, bir bilgi işaretine kaotik işaret ekleyerek, senkronizasyon kavramının bilgi işaretinin maskelenmesinde nasıl kullanılabileceğini göstermesi, kaotik haberleşme sistem tasarımında ilk uygulamalar olması açısından önemlidir. Bu ilk çalışmalardan sonra kaotik sistemlerin senkronizasyonu ve senkronize kaotik sistemlerin güvenilir haberleşme amaçlı kullanımı ile ilgili çok sayıda çalışma yapılmıştır [82-97].

3.2.1. Kaotik haberleşme sistemlerinin genel yapısı

Bilginin bu kadar önemli olduğu bir dönemde elbette bu bilginin güvenli bir şekilde taşınması istenmektedir. Bu nedenle gizli ve güvenilir haberleşme sistemleri için araştırmalar yapılarak şifreli haberleşme sistemleri geliştirilmiştir. Bu alanda, kaotik işaretlerin özellikleri önemli ilerlemelere neden olmuştur. Yapısal özelliği olan tahmin edilemezlik, bu işaretlerin bilgi iletiminde kullanılmasını uygun hale getirmiştir. Ayrıca haberleşme sistemlerinde de geniş bantlı sinyaller kullanılmaktadır. Bu sayede veri iletimi ve alımı daha kaliteli olmaktadır. Bunun paralelinde kaotik bir işaretin geniş bantlı bir karakteristiğe sahip olması taşıyıcı olarak kullanılmasını cazip hale getirmektedir. Kaotik haberleşme sistemleri ile bilgi iletimi daha güvenli bir ortamda gerçekleşmektedir. Bilgi, kaotik bir sistem tarafından şifrelenerek alıcıya ulaştırılmakta; alıcıda, gönderilen bilgi tekrar elde edilmektedir. Şekil 3.12 kaotik bir haberleşme sisteminin genel yapısını göstermektedir [79].

Kaotik haberleşme sistemlerinde iki önemli konu ön plana çıkmaktadır. Birincisi fiziksel ortamda iletilen kaotik sinyalin oluşturulması, ikincisi ise bu sinyalin alıcı ve vericide senkronizasyonunun sağlanmasıdır. Analog veya sayısal olabilecek bilgi işareti, fiziksel ortamın türüne göre istenen formata dönüştürülür. Bu işlem kanal kodlama aşamasında yapılır. Bilginin şifrelenmesi ve modüle edilerek fiziksel ortama verilme aşaması, kaotik sinyalin oluşturulduğu aşamalardır. Alıcı tarafından alınan bu kaotik sinyal, yine alıcıda mevcut olan özdeş veya benzer bir kaotik sistem kullanılarak bilgi işareti elde edilir.



Şekil 3.12. Kaotik haberleşme sisteminin genel yapısı.

3.2.1.1. Kaotik senkronizasyon

İki ya da daha fazla kaotik sistemin, aynı anda aynı davranışları göstermesi "kaotik senkronizasyon" olarak adlandırılır. Pecora ve Carroll, senkronizasyon ile ilgili yaptıkları çalışmada, sürücü-cevaplayıcı olarak adlandırdıkları yöntemle kaotik sistemlerin senkronize olabileceğini göstermişlerdir [3]. P-C yöntemi olarak adlandıracağımız bu yöntemde, n boyutlu otonom bir sistemin durum denklemi aşağıdaki gibi tanımlamaktadır:

$$\frac{dx}{dt} = f(x(t))$$

Bu otonom sistem keyfi olarak iki kısma ayrıldığında durum vektörü,

$$x = \begin{bmatrix} x_D \\ x_R \end{bmatrix}$$

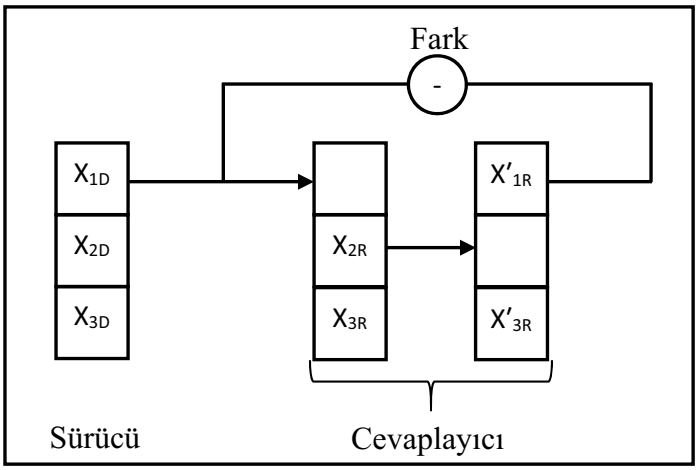
olacaktır. Burada D kısmı sürücü alt sistem; R kısmı ise cevaplayıcı alt sistem olarak tanımlanmaktadır. Bu iki alt sistemin dinamikleri,

$$\begin{aligned} \dot{x_D} &= g(x_D, x_R) \\ \dot{x_R} &= h(x_D, x_R) \end{aligned} \qquad \textbf{(3.24)}$$

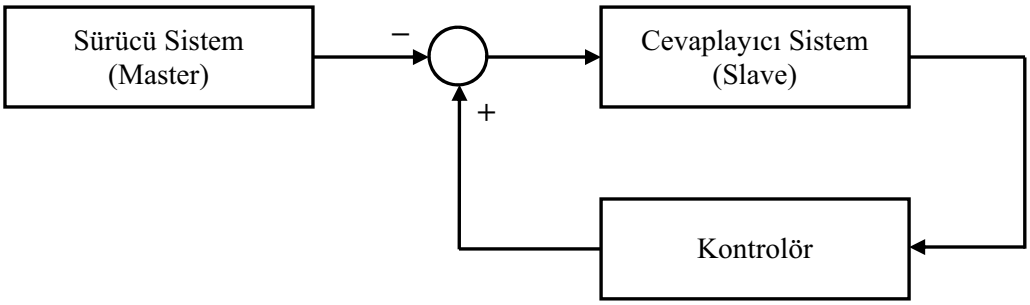
şeklinde ifade edilir. Daha sonra, cevaplayıcı alt sistemin bir kopyası oluşturulur ve $\acute{x_R}$ olarak adlandırılır. Bu durumda,

$$\begin{aligned} \dot{x_D} &= g(x_D, x_R) \\ \dot{x_R} &= h(x_D, x_R) \\ \dot{\acute{x_R}} &= h(x_D, \acute{x_R}) \end{aligned} \qquad \textbf{(3.25)}$$

denklem takımı elde edilir. Belirli bir süre sonra, x'_R değişkenleri, asimptotik olarak x_R değişkenlerine yakınsayacaktır. Bunun anlamı $x'_R - x_R$'nin sıfıra gitmesidir. Bu durumun oluşması için gerekli ve yeterli şart, x'_R alt sisteminin şartlı Lyapunov üstellerine ait işaretlerin durumudur. Lyapunov üstelleri, x_R alt sisteminin kararlılığını ve x'_R 'nin x_R'ye olan yakınlığını belirler. Bu üstellerin tümü negatif olduğu zaman x_R alt sistemi kararlıdır. Bu durum, x'_R'nin x_R'den farklı olmayacağını garanti eder. Bu işlem senkronizasyon için yeterli şartı sağlar [3]. Üç boyutlu kaotik bir sistem için, P-C yönteminin blok şeması Şekil 3.13'de gösterilmektedir.



Şekil 3.13. P-C kaotik senkronizasyon yöntemi [1].



Şekil 3.14. Kaotik senkronizasyon blok diyagramı.

Bu yöntemde, sürücü ve cevaplayıcı sistemlere ait başlangıç koşulları farklı olsa da senkronizasyon sağlanmaktadır [1, 98]. Senkronizasyon süresinin kontrolü için çoğu çalışmada bir kontrolör veya gözleyici (observer) tasarlanmıştır. Bu çalışmalar, sadece başlangıç koşulları değil, dinamik sistemin parametrelerinin de farklı olduğu

durumlarda kaotik senkronizasyonun sağlanabileceğini göstermektedir [13, 79, 99]. Kaotik senkronizasyonun bir kontrolör ile sağlanması Şekil 3.14'de gösterilmektedir.

Haberleşme sistemlerinde verici kısmına sürücü, alıcı kısmına da cevaplayıcı sistemler yerleştirilir. Vericiden gönderilen bilgiler, alıcı tarafında bir kontrolör vasıtasıyla tekrar elde edilmeye çalışılır. Kontrolörün çalışma prensibi, kaotik senkronizasyon esasına dayanır. Bu, vericinin gönderdiği ve fiziksel ortamdan geçerek alıcıya ulaşan sinyallerin cevaplayıcı sistem çıkışında üretilen sinyallerle senkron edilmesi anlamına gelir. Sürücü ve cevaplayıcı sistemler arasındaki fark, hata işareti olarak kabul edilir. Senkronizasyonun sağlanması için bu hatanın sıfır olması gerekir. Kontrolör tasarımı temel olarak şu şekilde yapılır. Sürücü sistem dinamiği,

$$\dot{X} = F(x)$$

olsun. Bu durumda, cevaplayıcı sistemin dinamiği,

$$\dot{\bar{X}} = F(\bar{x}) + \beta(t)$$

olarak yazılabilir. x gönderilen sinyal, $\bar{x}$ alınan sinyal, $\beta(t)$ kontrolün sağlanması için eklenen bir parametredir. Bu durumda hata işareti,

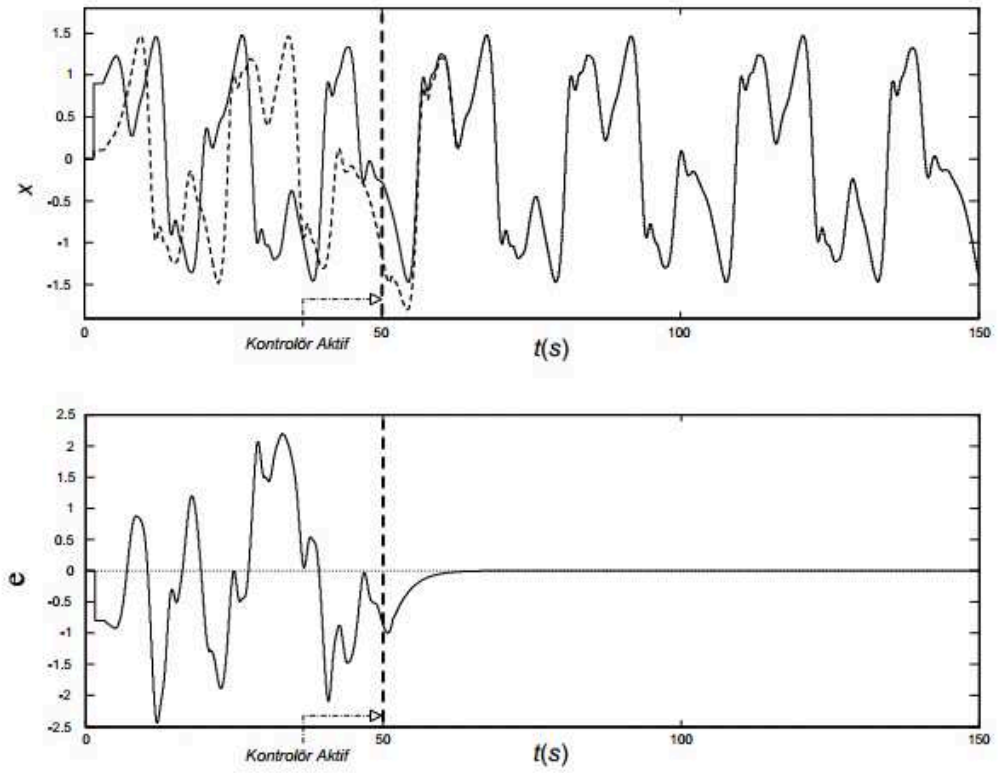
$$e = \bar{x} - x$$

olacaktır. Bundan sonra, hataya ait dinamik sistem,

$$\dot{e} = \dot{\bar{x}} - \dot{x} = G(\bar{x}, x, e, \beta)$$

olarak hesaplanır. Bundan sonra, hata dinamik sisteminin Lyapunov fonksiyonu belirlenir ve senkronizasyon koşullarını, dolayısıyla hatanın sıfıra yakınsamasını sağlayacak bir kontrol fonksiyonu üretilir [99-101]. Şekil 3.15, kontrolör kullanılan bir sistemdeki senkronizasyon süresi ve meydana gelen hata işaretini göstermektedir. Şekilden görüldüğü üzere kontrolör, kaotik sistemlerin çok daha hızlı bir şekilde

senkronize olmasını sağlamaktadır. Bununla birlikte, haberleşme sistemlerinde gürültünün etkisinin azaltılması da kontrolör tasarımlarında amaçlanan bir faktördür.



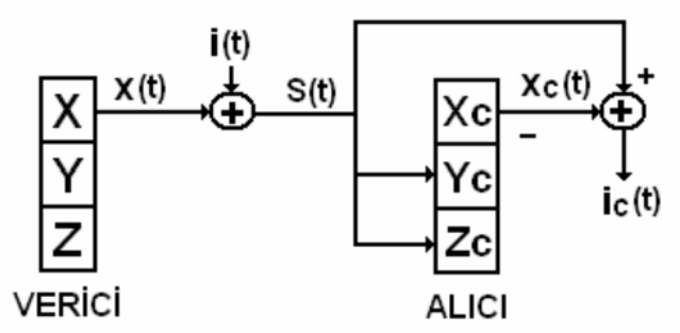
Şekil 3.15. Kaotik senkronizasyon için kontrolör kullanımı [102].

3.2.1.2. Kaotik sinyalin oluşturulması

Kaotik sinyallerin karakteristiği olan geniş bantlı olma ve gürültüye benzeme özelliği sayesinde, bilgi sinyalinin kaotik işaret üzerinden taşınması haberleşme sistemlerinde modülasyon için güvenli bir ortam oluşturur. Kaotik haberleşme ile ilgili kaotik gizleme, kaos kaydırmalı anahtarlama, kaos modülasyonu gibi farklı kodlama ve kod çözme yöntemleri geliştirilmiştir. Bu yöntemlerden biri kullanılarak kaotik sinyal oluşturulur ve haberleşme ortamına gönderilir.

Kaos tabanlı sinyal gizleme, analog iletişim sistemleri için geliştirilmiştir. Kaotik gizleme sistemi, göndericide oluşturulan bir kaotik sinyale doğrudan bilgi sinyalinin eklenmesidir. Bilgi sinyalinin iletilmesinden sonra, bilgi sinyali alıcıya ulaşır ve bazı sinyal işleme operasyonlarından sonra yeniden orijinal sinyal elde edilir [3, 103]. Kaotik sinyal gizlemenin mantığını gösteren blok diyagram Şekil 3.16'da

görülmektedir. Kaotik gizlemedeki temel prensip; analog olan i(t) bilgi işaretini, verici kısımdaki x(t) kaotik işaretiyle gizlemek ve bu şekilde iletmektir. Bu amaçla i(t) bilgi işareti, gizleyici x(t) kaotik işaretiyle toplanır ve iletim ortamına aktarılır. İletilen s(t) işareti ikisinin toplamıdır. Alıcı kısımda ise, bir önceki bölümde anlatılan P-C yöntemine göre gerçekleştirilen senkronizasyonla, gizleyici x(t) işaretinin aynı formu oluşturulmakta ve senkronize olmuş olan $x_c(t)$ kaotik işareti, iletim ortamından gelen s(t) işaretinden çıkartılarak tekrar bilgi işareti elde edilmektedir [98]. Kaotik gizleme yönteminde, alıcının kaosta kalması ve senkronizasyonun gerçekleşmesi için haber işaretinin genliğinin kaotik işaretin genliğinden 15-20dB az olması istenmektedir [1].



Şekil 3.16. Kaotik gizleme ile haberleşme blok diyagramı [1].

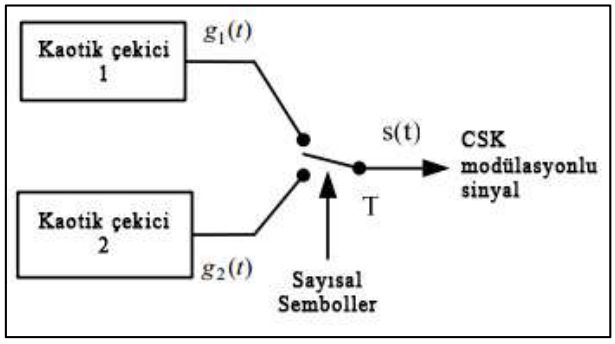
Sayısal haberleşme sistemlerinde, sembollerden oluşan sayısal bilgi, bir yerden başka bir yere analog işaretler ile modüle edilerek taşınır. Analog işaretler, sınırlı bir bant genişliğine sahip ve işareti bozucu etkileri olan analog bir kanaldan geçerler. Geleneksel haberleşme sistemlerinde, analog taşıyıcı işaret bir veya daha fazla sinüzoidal bileşenden oluşmaktadır. Kaotik haberleşme sistemlerinde ise taşıyıcı, kaotik bir işarettir. Alıcıda; eğer modülasyon sırasında kullanılan analog işaretlerin tamamı kesin olarak biliniyorsa evre uyumlu (coherent), bir veya birkaç karakteristiği tahmin edilebiliyorsa evre uyumsuz (non-coherent) algılama teknikleri ile semboller yeniden elde edilebilir. Evre uyumlu alıcılar için en sık kullanılan yöntem senkronizasyon tekniğidir. Bu teknikte, alıcı tarafından algılanan analog işaretler bir korelatör vasıtasıyla işlenir ve gönderilen bilgi elde edilir. Senkronizasyon tabanlı evre uyumlu alıcılar gürültü performansı, bant genişliğinin etkin kullanımı ve veri iletim hızı hususlarında evre uyumsuz alıcılara göre daha fazla avantaj sunar. Ancak, kötü yayılma koşulları gibi nedenlerden dolayı senkronizasyon sağlanamazsa bu avantajlar ortadan kalkar [104].

Kaotik taşıyıcı kullanarak sayısal modülasyon ve evre uyumlu alıcı devresi ilk defa 1992 yılında Kaos Kaydırmalı Anahtarlama (CSK) adı altında ortaya çıkmıştır. Sonraki yıllarda diğer kaotik modülasyon teknikleri sunulmuş ve 1996 yılında daha sağlam bir teknik olan Farksal Kaos Kaydırmalı Anahtarlama (DCSK) tanıtılmıştır [105]. CSK, her bir sembolün farklı bir kaotik çekici tarafından haritalandığı sayısal bir modülasyon türüdür. Örneğin, ikili sembollerin kullanıldığı bir haberleşme sisteminde, "1" ve "0" sembollerinin her biri farklı bir kaotik işaret tarafından anahtarlanır.

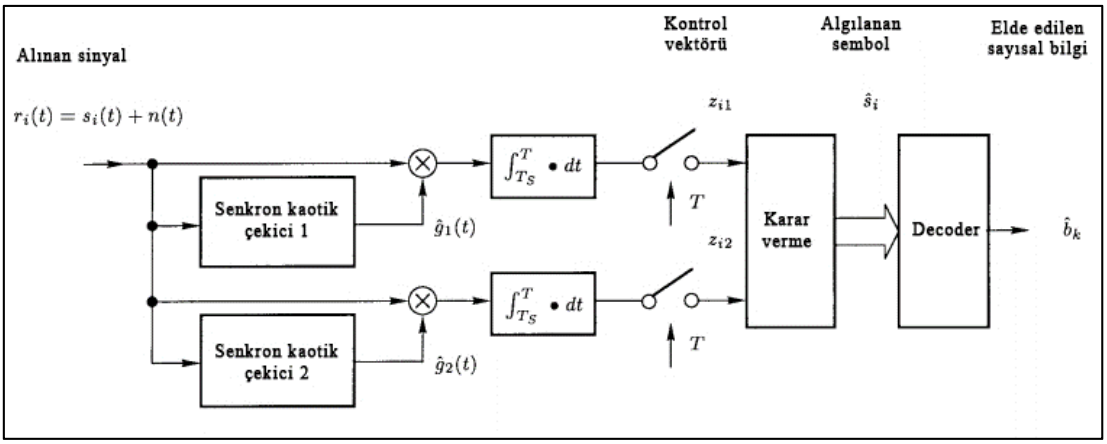
$$s(t) = \begin{cases} g_1(t), & \text{"1" sembolü için} \\ g_2(t), & \text{"0" sembolü için} \end{cases} \quad \textbf{(3.26)}$$

$s(t)$ gönderilen bilgi işareti, $g_1(t)$ birinci kaotik çekicinin, $g_2(t)$ ikinci kaotik çekicinin ürettiği işaretler olmak üzere, CSK modülasyonunun matematiksel ifadesi (Denklem 3.26), modülatörün şematik gösterimi de Şekil 3.17'de gösterildiği gibidir.

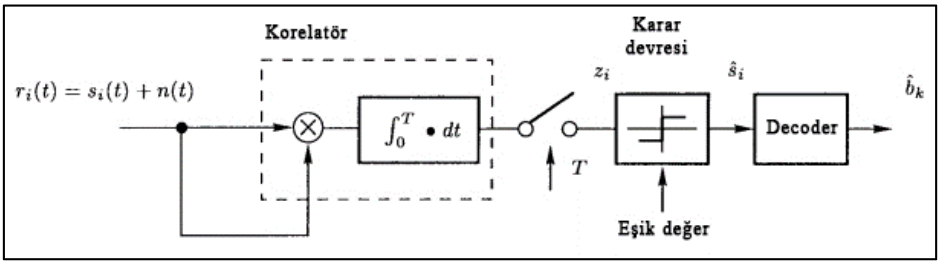
Evre uyumsuz alıcıda, gönderilen her bir sembolün temsil ettiği enerji seviyeleri birbirine yakındır. Bu yüzden hangi sembolün alındığını belirleyecek olan karar verme devresi hassas bir eşik değerine sahip olmalıdır [104, 105]. $n(t)$, kanal gürültüsü olmak üzere, evre uyumlu ve evre uyumsuz CSK alıcısı için blok diyagramlar sırasıyla Şekil 3.18 ve Şekil 3.19'da gösterilmektedir.



Şekil 3.17. CSK modülatörü [105].

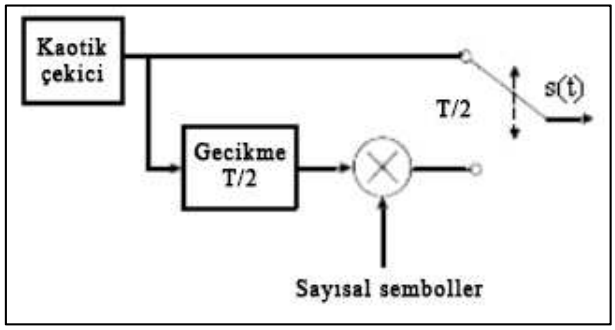


Şekil 3.18. Evre uyumlu CSK alıcı blok diyagramı [104].

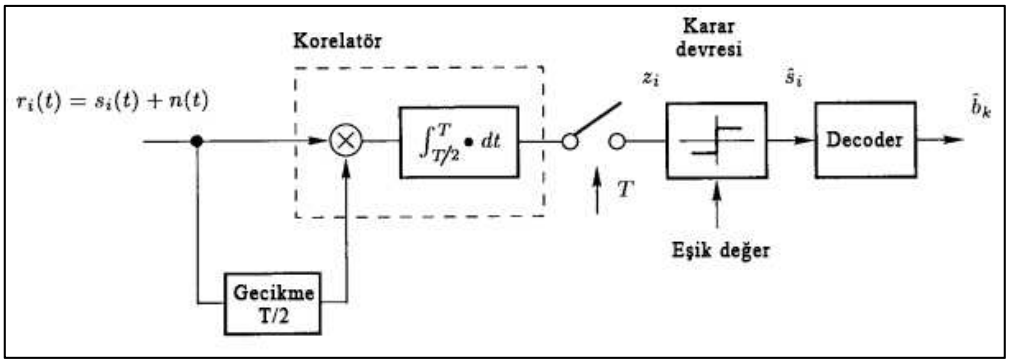


Şekil 3.19. Evre uyumsuz CSK alıcı blok diyagramı [104].

DCSK modülasyonunda, her bir sembol iki örnek işaretle temsil edilerek gönderilir. İlk işaret bir referans görevi yaparken ikincisi ise bilgiyi taşır. DCSK modülasyonunda kullanılan örnek işaretler tek bir kaotik çekici tarafından üretilir. İlk işaret ile ikinci işaret, kaotik işaretin sembol periyodunun yarısı (T/2) kadar zamanda ötelenmesiyle elde edilirler [104]. İkili sembollerin kullanıldığı bir haberleşme sisteminde, "1" sembolü için kullanılan kaotik işaretin ters kopyası, "0" sembolü için kullanılır. DCSK modülatör ve alıcı blok diyagramları sırasıyla Şekil 3.20 ve Şekil 3.21'de gösterilmektedir.



Şekil 3.20. DCSK modülatörü [105].



Şekil 3.21. DCSK alıcı blok diyagramı [104].

Kablolu, kablosuz veya optik sayısal haberleşme sistemlerinde gerek veri iletim hızı, gerek bit hata oranı, gerekse gürültü etkisi gibi faktörleri iyileştirmek için farklı modülasyon teknikleri geliştirilmiş ve geliştirilmeye devam edilecektir.

3.3. Kriptolama Algoritmaları ve Kaos

Bilimin birçok dalında uygulama alanı bulunan kaos teorisinin bilgisayar bilimlerindeki yaygın kullanım alanlarından biri de kaotik sistemleri kullanarak yeni kriptolojik sistemlerin tasarlanmasıdır. Kaos ve kriptoloji bilimleri arasında doğal bir ilişki bulunmaktadır. Bu ilişki Shannon'un [117] "herhangi bir şifreleme sisteminin güvenilir olması için sahip olması gereken karıştırma ve yayılma özelliklerinin" kaotik sistemlerin başlangıç koşullarına duyarlı olması ve doğrusal olmaması özellikleriyle örtüşmesinden ortaya çıkmaktadır.

Karıştırma özelliğine sahip şifreleme sistemlerinde; her anahtar için şifreleme algoritması öyle olmalıdır ki, açık metin ve şifreli metin arasındaki yapılar arasında istatistiksel bağlılık olmamalıdır. Bu özelliğin olabilmesi için anahtar ve açık metinin her bitinin şifreli metini etkilemesi gerekmektedir.

Yayılma özelliğine sahip bir şifreleme sistemi için ise; şifreli metin ile anahtar arasındaki ilişki mümkün olduğunca karmaşık olmalıdır. Diğer bir deyişle yayılma, anahtarın açık ve şifreli metinle olan ilişkisinin, analiz yöntemleriyle elde edilemeyecek kadar karmaşık olması demektir. Yani şifreleme sistemini tanımlayan

eşitlikler doğrusal olmayan karmaşık bir yapıda olmalı ve böylece şifreleme algoritmasından anahtar elde edilememelidir [49].

Karıştırma ve yayılma özellikleri dinamik sistemlerin sahip olduğu özelliklerdir. Kaotik sistemlerin başlangıç koşulları ve kontrol parametrelerine bağımlılığı bir kaotik sistemden üretilen yörüngeler boyunca yayılma özelliğini sağlar. Başka bir ifade ile herhangi bir yörünge üzerinde alınan her bir değer başlangıç koşulları veya kontrol parametrelerine bağımlıdır. Başlangıç koşulları ve kontrol parametrelerindeki en ufak bir değişiklik ile tamamen farklı yörüngeler oluşacağından bu bağımlılık çok güçlüdür. Bu nedenle, kaotik sistemlerin başlangıç koşulları ve kontrol parametrelerine bağımlılığı, kriptoloji sistemlerinin yayılma gereksinimini karşılayacak düzeydedir [49].

Kaotik bir sistemden üretilen yörüngelerin bir kümesi ile istatistiksel olarak, başlangıç koşulları ve kontrol parametrelerinin tam değerlerinin çıkarılması mümkün değildir. Ergodiklik olarak tanımlanan bu özellikleri sayesinde, kaotik sistemler kriptoloji sistemlerinin karıştırma gereksinimini de sağlamaktadır [20, 49].

Son yıllarda yapılan kaos tabanlı kriptoloji çalışmaları, geleneksel kriptoloji yöntemlerine kıyasla oldukça büyük etkiler yapmıştır. Öncelikle, hemen hemen tüm kaos tabanlı şifreleme algoritmaları gerçek sayılar kümesi üzerinde tanımlı dinamik sistemleri kullanır ve bu nedenle pratik olarak gerçekleştirilmeleri zordur. İkincisi, hemen hemen önerilen tüm kaos tabanlı yöntemlerin güvenlik ve performans analizi, geleneksel kriptoloji için geliştirilen teknikler ile yapılamamaktadır [22].

Kaos tabanlı kriptolama sistemleri, kaotik dinamikleri kullanırken; geleneksel kriptolama yöntemleri belli bir düzende rastgele sayılar üreten fonksiyonları (PRNG – Pseudo Random Number Generator) kullanır. Kaotik dinamikler, çıktı olarak sonsuz sayıda reel sayılar üretirler. PRNG tabanlı sistemde çıktı tam sayıdır ve sonlu miktardadır. Kaotik sistemler kendi kendini yineleyen geri beslemeli sistemlerdir ve her yinelemede yeni değerler üretirler; geleneksel kriptolojide ise döngüler oluşturularak yeni çıktılar üretilir. Kaotik sistemler başlangıç koşullarını ve sistem

parametrelerini kullanarak gizliliği sağlar; geleneksel sistemlerde ise gizlilik için bir anahtar kullanılır.

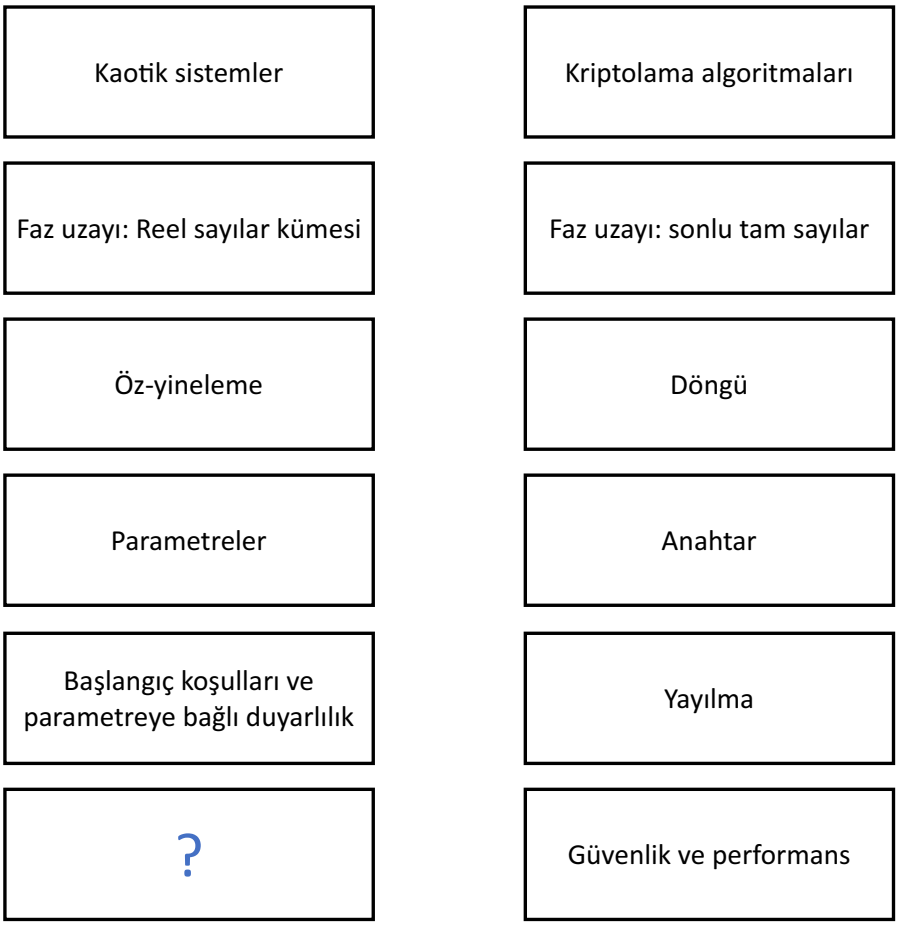
Tablo 3.1. Kaos teorisi ve kriptoloji karşılaştırması.

Kaos teorisi	**Kriptoloji**
Kaos tabanlı sistem	Pseudo-random tabanlı sistem
Sonsuz sayıda durum	Sonlu sayıda durum
Sonsuz sayıda tekrarlar	Sonlu sayıda tekrarlar
Başlangıç durumu	Açık metin
Bitiş durumu	Şifreli metin
Başlangıç koşulları / parametreler	Anahtar
Başlangıç/bitiş durumları arasında asimptotik bağımsızlık	Karıştırma
Başlangıç koşulları ve parametrelere bağlı karıştırma	Yayılma

Geleneksel kriptolama algoritmaları için söz konusu olan güvenlik ve performans kavramlarının kaos teorisinde bir karşılığı yoktur. Kaotik ve geleneksel kriptolama sistemlerine ait bir karşılaştırma Tablo 3.1'de verilmektedir. Yine kaotik ve geleneksel kriptolama sistemleri arasındaki benzerlikler ve farklılıklar Şekil 3.22'de gösterilmektedir [22, 29].

Analog sistemler radyo dalgalarının iletiminde sıklıkla kullanılmaktadır. RF bölgesinde, veriler bir uçtan bir uca gönderilirken modüle edilmek zorundadır. Veri ister sayısal ister analog olsun, taşıyıcı işaretler analogdur. Dolayısıyla iletilen işaret de analog olmaktadır. Alıcı tarafından alınan bu analog işaret demodülasyon işlemine tabi tutularak, veri işareti tekrar elde edilmektedir. Günümüzde kablosuz ağlar için tasarlanan kaotik sistemler de benzer şekildedir. Kaotik gizleme, kaotik anahtarlama veya kaos modülasyonu yapılarak işlenen işaret RF bölgesinde iletilmekte ve güvenli bir haberleşme sağlanmaya çalışılmaktadır.

Gönderilen ve alınan bilginin sayısal olduğu haberleşme sistemlerinde modülasyon yerine kodlama teknikleri kullanılmaktadır. Bu tür haberleşme sistemleri tam sayısal (full digital) olarak adlandırılabilir. Tam sayısal haberleşme sistemlerinde güvenlik, büyük ölçüde kriptolama algoritmaları ile sağlanmaktadır. Seçilen bir kriptolama algoritması kullanılarak, bilgi kodlanmakta bir başka deyişle şifrelenmektedir.

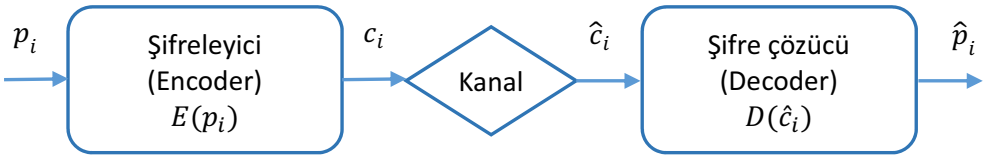


Şekil 3.22. Kaotik sistemler ve kriptolama sistemlerinin benzerlikleri ve farkları [22].

Kaotik kriptolama sistemlerinin güçlü özellikleri sayesinde, son yıllarda yapılan çalışmalarla birlikte kriptolama algoritmalarına yeni bir bakış açısı getirilmiş; güvenli haberleşmenin sağlanması konusunda yeni kaotik kriptolama sistemleri geliştirilmiştir. Özellikle tam sayısal haberleşme sistemlerinde, mevcut kriptolama sistemlerinin zayıf anahtar kullanımı, yavaş çalışma, kriptanaliz yöntemleriyle şifrelerinin kırılabilmesi gibi zayıflıklarını ve dezavantajlarını gidermek amacıyla, kaotik kriptolama sistemleri üzerinde yapılacak çalışılmalar teşvik edilmelidir.

BÖLÜM 4. ÖNERİLEN YENİ KAOS TABANLI KRİPTOLAMA SİSTEMİ

Kriptolama sistemlerinin genel blok diyagramı aşağıdaki şekilde verilmiştir.



Şekil 4.1. Kriptolama sistemi genel blok diyagramı.

$i = 1,2,3, \dots ,\ i \in Z^+$ ve p_i şifresiz veri (plaintext), c_i şifreli veri (ciphertext) olmak üzere E şifreleme (cipher) ve D şifre çözme fonksiyonları aşağıdaki gibi yazılabilir.

$$c_i = E(p_i) \quad \textbf{(4.1)}$$

$$\hat{p}_i = D(\hat{c}_i) \quad \textbf{(4.2)}$$

$\hat{p}_i$ şifresi çözülmüş, $\hat{c}_i$ algılanan şifreli veridir. Şifre çözme işleminin başarılı bir şekilde gerçekleşmesi için, her $\hat{p}_i = p_i$ iken, her $\hat{c}_i = c_i$ şartının sağlanması gerekir. Bu durumda (Denklem 4.2);

$$p_i = D(c_i)$$

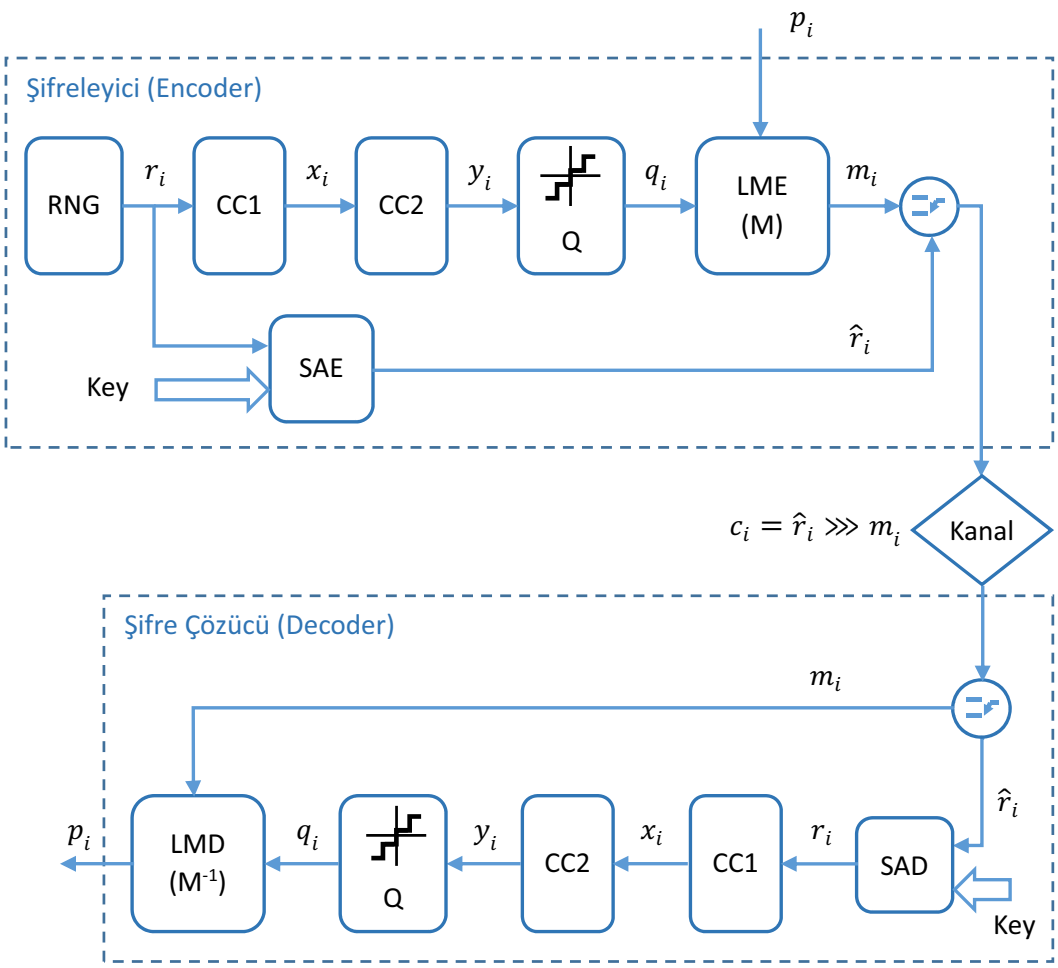
şeklinde yazılabilir. Bu ifade (Denklem 4.1)'de yerine yazılırsa;

$$c_i = E(D(c_i)) \quad \textbf{(4.3)}$$

$$p_i = D(c_i) = E^{-1}(c_i) \quad \textbf{(4.4)}$$

ifadesi elde edilir. Bu durumda $D \leftrightarrow E^{-1}$ lineer dönüşümü ile $p_i = E^{-1}(c_i)$ şeklinde yazılabilir ve şifresiz veri tekrar elde edilmiş olur.

Bu tez çalışmasında önerilen kaos tabanlı kriptolama sisteminin "şifreleyici" ve "şifre çözücü" bloklarının detaylı gösterimi Şekil 4.2'de verilmektedir.



Şekil 4.2. Önerilen yeni kaos tabanlı kriptolama sistemi detaylı blok diyagramı.

Bu sistem, "şifreleyici ve "şifre çözücü" tarafında yerleştirilmiş katmanlardan oluşmaktadır. Her bir katman, şifreleme ve şifre çözme fonksiyonlarını oluşturmak için farklı görevleri yerine getirmektedir. Şifreleyici sistem, Şekil 4.2'de görüldüğü gibi Rastgele Sayı Üreteci (RNG – Random Number Generator), iki adet art arda bağlanmış Kaotik Hesaplama katmanı (CC1, CC2 – Chaotic Computation 1-2), Kuantalama katmanı (Q - Quantizer), Lojik Karıştırıcı katmanı (LME – Logical Mixer

for Encoder) ve geleneksel bir şifreleyici (SAE - Symmetric or Asymmetric Encryption) katmanlarından oluşmaktadır. Şifre çözücü sistemde, geleneksel şifre çözücü (SAD - Symmetric or Asymmetric Decryption) ve LMD (Logical Mixer for Decoder) katmanı haricinde diğer katmanlar "şifreleyici" sistemdeki katmanlarla özdeştir. SAD, SAE tarafından şifrelenen verinin şifresini çözer. LMD, LME tarafından karıştırılan veriyi geri elde eder. Bu katmanların görevleri ve matematiksel ifadeleri bir sonraki bölümde detaylı olarak ele alınacaktır.

Artık, (Denklem 4.1) ve (Denklem 4.4) sırasıyla aşağıdaki gibi yazılabilir.

$$c_i = M(Q(G(F(r_i))), p_i, \hat{r}_i) \quad \textbf{(4.5)}$$

$$p_i = M^{-1}\left(Q\left(G(F(r_i))\right), m_i, \hat{r}_i\right) \quad \textbf{(4.6)}$$

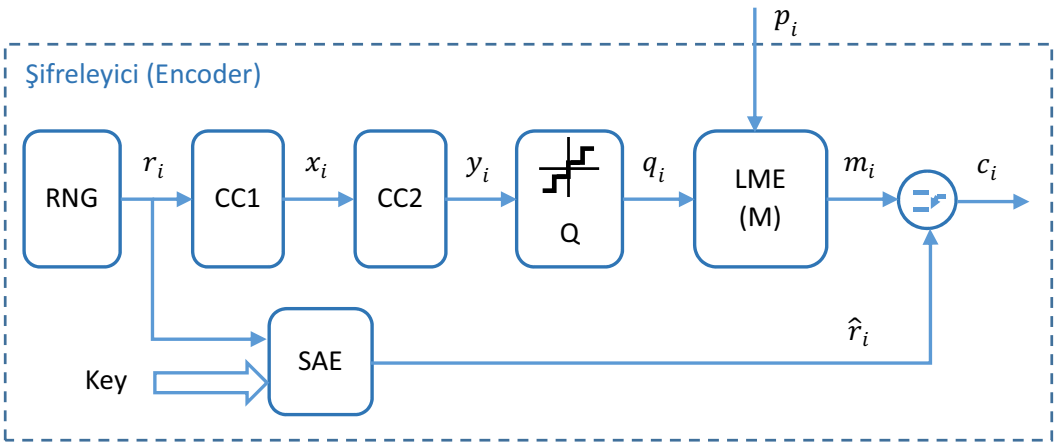
$i = 1,2,3, \dots,\ i \in Z^+$, r_i üretilen rastgele sayılar, $\hat{r}_i$ SAE katmanında şifrelenmiş r_i değerleri, m_i şifrelenmiş veri dizisi, M lojik karıştırıcı fonksiyonu, F ve G sırasıyla CC1 ve CC2 dinamiklerinin belirlediği fonksiyonlar ve Q kuantalama fonksiyonudur.

4.1. Şifreleme İşlemi

Şifreleyici, şifresiz p_i verisini, katmanlarının belirlediği, önerilen sistemde tasarlanan katmanların belirlediği ve (Denklem 4.5)'de açıklanan fonksiyon ile şifreler. Elde edilen şifreli c_i verisi, şifre çözme işlemi için bir kanaldan şifre çözücüye gönderilir. RNG tarafından üretilen r_i sayıları CC1 katmanında işlenir ve x_i değerleri hesaplanır. r_i sayıları aynı zamanda SAE bloğunda, geleneksel bir şifreleme yöntemiyle şifrelenerek şifre çözücü bloğuna gönderilir. CC2, hesaplanan bu x_i değerlerini kullanarak y_i değerlerini hesaplar. Hesaplanan y_i değerleri Q katmanında ikili sayılara dönüştürülür. Bu ikili sayılar, LME katmanında p_i veri dizisi ile karıştırılarak şifreli veri elde edilir.

Şifreleme işleminin nasıl yapıldığını anlamak için, şifreleyici bölümündeki katmanlar ayrı ayrı incelenecektir. Şekil 4.3'te, önerilen kaos tabanlı kriptolama sisteminin şifreleyici (encoder) blok diyagramı verilmiştir. Şekilde görülen çok katmanlı kaotik

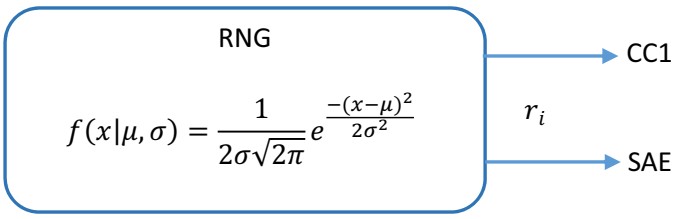
sistemin şifreleyici bölümünün sahip olduğu işlem adımları ve açıklamaları aşağıda detaylı olarak ifade edilmiştir.



Şekil 4.3. Önerilen yeni kaos tabanlı kriptolama sistemi, şifreleyici blok diyagramı

4.1.1. Rastgele sayı üreteci

Rastgele sayı üreteci (RNG), şifreleme algoritmasının ilk bölümüdür. Bu bölümün iki temel görevi vardır. Birincisi, ilk kaotik katman (CC1) için başlangıç koşullarını belirlemek; ikincisi ise ürettiği bu sayıları şifre çözme işleminde kullanılmak üzere SAE katmanına göndermektir.



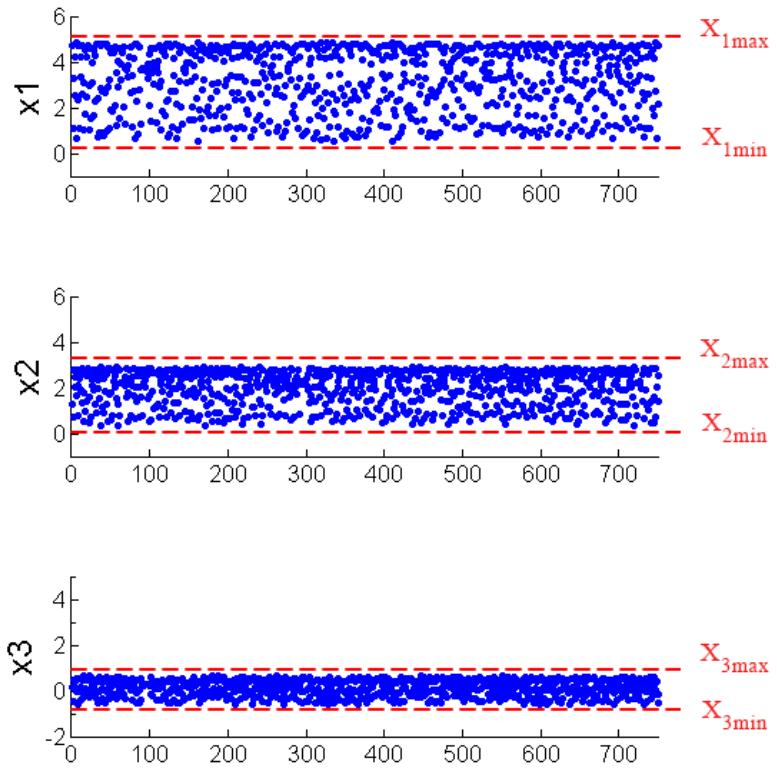
Şekil 4.4. RNG ve ilişkili olduğu katmanlar

RNG, CC1 kaotik hesaplama katmanının başlangıç koşullarını belirlemek üzere, "normal dağılım fonksiyonunu" kullanarak rastgele N adet reel sayı üretir. Normal dağılım fonksiyonu, Şekil 4.4'te f fonksiyonu ile gösterilmektedir. N, CC1 dinamik sisteminin boyutu ile aynıdır. CC1 katmanının dinamiği, $\dot{X}_i = F(x_1, x_2, \dots, x_N)$, $i = 1,2, \dots, N$ olsun. Bu durumda RNG'nin üreteceği sayılar $r_1, r_2, \dots, r_N$ olacaktır. Her bir

r_i değerinin hangi aralıkta olacağının belirlenmesi önemlidir. Çünkü kaotik sistemler başlangıç koşullarına aşırı duyarlıdır ve kaotik davranışın oluşması için başlangıç koşullarının da hassasiyetle belirlenmesi gereklidir. Bunun için, CC1 sisteminin zaman serileri incelenerek, kaotik davranışın gözlemlendiği çalışma bölgeleri belirlenir. 3-boyutlu kaotik bir sisteme ait çalışma bölgelerinin belirlenmesi Şekil 4.5'te gösterilmektedir. Bu durumda r_i değerleri;

$$x_{imin} \leq r_i \leq x_{imax} \tag{4.7}$$

aralığında seçilmelidir. x_{imin} durum değişkenlerinin alabileceği minimum, x_{imax} ise maksimum değerdir.



Şekil 4.5. Kaotik bir sistemin zaman serilerinin analizi ile durum değişkenlerinin alabileceği maksimum ve minimum değerler belirlenir.

4.1.2. SAE

SAE (Symmetric or Asymmetric Encryption) katmanı, üretilen r_i sayılarını, geleneksel şifreleme yöntemlerinden biri (DES, AES, RSA vb.) ile şifreler. Bu katmanda simetrik

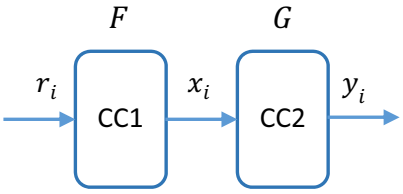
veya asimetrik şifreleme yöntemlerinden biri kullanılabilir. r_i sayıları, seçilen şifreleme yöntemine göre bir ya da iki anahtar (Key) kullanılarak şifrelenir. $\hat{r}_i$ şifrelenmiş sayılardır ve bu şifreli sayı dizisi, SC (Synchronization Code) olarak isimlendirildi. Bunun nedeni, "şifreleyici" ve "şifre çözücü" bloklarındaki kaotik katmanları, SC sayılarının senkron etmesidir.

Şekil 4.6. Asenkron haberleşme sistemlerinde şifreli veri paketinin yapısı.

SC'nin "şifre çözücü" bloğuna gönderilmesi iki şekilde gerçekleştirilebilir. Senkron haberleşme sistemleri için, SC, haberleşmenin öncesinde üretilir ve karşı tarafa gönderilir. Bu şekilde verici ve alıcıdaki (şifreleyici ve şifre çözücüdeki) özdeş kaotik katmanların başlangıç koşulları eşitlenmiş dolayısıyla senkronizasyon sağlanmış olur. Asenkron haberleşme sistemleri için, SC, Şekil 4.6'da gösterildiği gibi her bir veri paketinin önüne eklenir. Bu işlem bilgisayar ağları için, OSI referans modeline göre Oturum Katmanında icra edilir. Alıcı taraf, veri paketini aldıktan sonra öncelikle şifreli SC bilgisini kendi SAD katmanında çözer. Sonrasında, elde ettiği sayıları kullanarak veri paketinin geri kalan kısmını çözer.

4.1.3. Kaotik hesaplama katmanları

Kaotik hesaplama katmanları, art arda bağlanmış (cascade) iki farklı kaotik sistemden oluşur. Görevi, kriptolama sisteminin kullanacağı şifreleme anahtarlarını üretmektir. Bu yüzden, kaotik hesaplama katmanları önerilen yeni kriptolama sisteminin en önemli bölümünü oluşturmaktadır.



Şekil 4.7. Art arda bağlanmış kaotik hesaplama katmanları

Bu bölümdeki kaotik sistemler ayrık zamanlı dinamik sistemlerdir. Birinci kaotik sistem (CC1), RNG katmanından alınan r_i değerlerini, başlangıç koşulları olarak kabul eder. CC1'in dinamikleri bir F fonksiyonu ile tanımlıdır ve (Denklem 4.8)'de ifade edilmiştir.

$$X_i[n+1] = F(X_i[n]) \quad \textbf{(4.8)}$$

X_i durum değişkenleri $n = 0,1,2,\ldots$ ve $i = 1,2,\ldots,N \in Z^+$ iken $X_i[0] = [r_1 \quad r_2 \quad \ldots \quad r_N]$ şeklinde yazılabilir. CC1 tarafından hesaplanan ve bir sonraki anı ifade eden $X_i[n+1]$ değerleri CC1'in çıkışlarıdır. Bu çıkışlar, ikinci kaotik hesaplama katmanı olan CC2 için başlangıç koşullarını oluşturmaktadır. CC2 dinamikleri bir G fonksiyonu ile tanımlıdır ve (Denklem 4.9)'da gösterilmiştir.

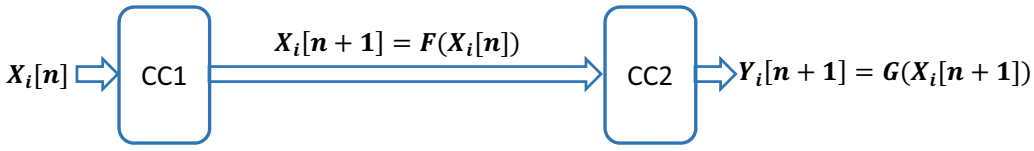
$$Y_i[n+1] = G(Y_i[n]) \quad \textbf{(4.9)}$$

Y_i durum değişkenleri $n = 0$ ve $i = 1,2,\ldots,K \in Z^+$ olmak üzere, $Y_i[n+1]$ değerleri CC2'nin çıkışlarıdır. Burada, dikkat edilmesi gereken CC2'nin başlangıç koşulları olan $Y_i[n]$ değerlerinin, CC1'in çıkışları olan $X_i[n+1]$ değerleri ile sürekli olarak değiştirildiğidir. Şekil 4.8'de gösterilen bu durumu matematiksel olarak aşağıdaki gibi ifade edebiliriz.

$$Y_i[n+1] = G(F(X_i[n])) \quad \textbf{(4.10)}$$

$$Y_i[n+1] = G(X_i[n+1]) \quad \textbf{(4.11)}$$

CC2 sistemi, yalın olarak kaotik bir sistemdir. Ancak, CC2'nin sürekli olarak CC1 ile sürülmesi sonucu, CC2 çıkışlarında gözlenecek davranışın kaotik olmayabileceği göz önünde tutulmalıdır. Tıpkı CC1'in kaotik davranışını garanti etmek için r_i değer aralığının belirlendiği gibi, CC2'nin kaotik davranışını garanti etmek için de $Y_i[n]$ değer aralığının belirlenmesi gereklidir. $Y_i[n]$, $X_i[n+1]$ tarafından belirlenmektedir ve bu yüzden CC1 ile CC2 arasında bir kontrolör tasarlanmalıdır. Bu kontrolör, $X_i[n+1] \overset{h}{\leftrightarrow} Y_i[n]$ şeklinde gösterilebilir.



Şekil 4.8. Kaotik sistemlerin art arda bağlanması

h kontrolörünün tasarlanması için öncelikle CC2 sisteminin zaman serileri incelenerek, durum değişkenlerinin alacağı maksimum ve minimum değerler belirlenmelidir. Bu değerlerin, sırasıyla y_{imax} ve y_{imin} olduğunu varsayalım.

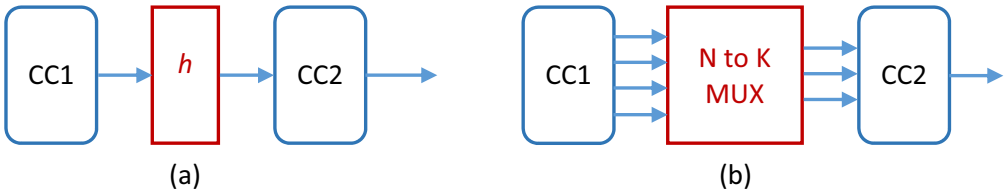
$h = A.X_i{}^T$ olsun. CC1 N-boyutlu, CC2 K-boyutlu sistemler olarak tanımlanmıştı. Bu durumda $X_i = [x_1, x_2, \dots, x_N]$, $Y_i = [y_1, y_2, \dots, y_K]$'dır ve A matrisi;

$$A = \begin{bmatrix} a_{11} & \cdots & a_{1N} \\ \vdots & \ddots & \vdots \\ a_{K1} & \cdots & a_{KN} \end{bmatrix}$$

şeklinde yazılır. Buradan da;

$$h = A.X_i{}^T = \begin{bmatrix} h_1 \\ \vdots \\ h_K \end{bmatrix}$$

ifadesi elde edilir. $i = 1,2, \dots, K$ olmak koşuluyla $y_{imin} \leq h_i \leq y_{imax}$ koşulu sağlandığı sürece CC2 çıkışında kaotik davranış gözlenir. CC1 ve CC2 arasında tanımlanan h kontrolörünün blok gösterimi Şekil 4.9'da gösterilmiştir. Şekil 4.9.b'de görüldüğü üzere, kontrolör bir çoklayıcı (multiplexer) şeklinde tasarlanabilir.



Şekil 4.9. Kontrolörün, a) blok gösterimi, b) çoklayıcı ile gerçekleştirilmesi.

CC2 kaotik sistemi yalın olarak çalıştığında, her bir $Y_i[n]$ için ayrı bir $Y_i[n+1]$ değeri üretecektir. Bu ilişki bir dizi değişkeni olarak ifade edilirse, $Array(a[n]) = [s_1, s_2, \dots, s_T]$ şeklinde yazılabilir. T hesaplamalar için yapılan adım sayısı, $n = 0,1, \dots, T$, s ise her bir adım sonunda hesaplanan sonuç değeridir. Belli bir başlangıç koşulunda, bu kaotik sistemin herhangi bir n anındaki çıkışı, bu dizi değişkenine bakılarak belirlenebilir. Örneğin, $a[158] = s_{158}$'dir. Ancak, CC2 çıkışında gözlenecek olan kaotik davranış, CC2'nin yalın olarak gösterdiği kaotik davranıştan farklıdır. Bu şekilde, iki farklı kaotik sistem birlikte kullanılarak üçüncü bir kaotik sistem elde edilmektedir. Bu birleşik kaotik sistemin davranışlarını belirleyebilmek için CC1 ve CC2'de tanımlanan her bir kaotik sistemin parametrelerinin ve başlangıç koşullarının bilinmesi gerekir. Birleşik sistemin giriş-çıkış ilişkisi, bir dizi değişkenine aktarılırsa bu durumda, $Array(b[n]) = [s_\alpha, s_\beta, \dots, s_T]$ şeklinde yazılabilir. Bunun nedeni, CC2'nin CC1 ile sürekli olarak sürülmesidir. CC1'in çıkışı, CC2'nin girişini sürekli olarak değiştirmekte, dolayısıyla a dizisinin değerlerini karıştırarak b dizisini oluşturmaktadır. Burada verilen örnekte, s_1, s_α; s_2, s_β ile yer değiştirmektedir. Kriptolama sistemlerinde yayılma veya dağılma (diffussion) olarak tabir edilen işlem burada gerçekleşmektedir.

Verinin şifrelenmesi için kullanılacak şifreleme anahtarları kaotik kurallara göre belirlenmekte dolayısıyla rastgele işaretlere benzeyen bir davranış göstermektedir. Bu yüzden, önerilen bu yeni kriptolama sistemindeki en önemli birimler kaotik hesaplama katmanlarıdır.

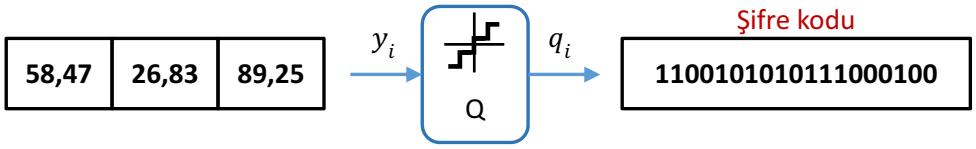
Bu kriptolama sistemi, farklı iki kaotik sistemi art arda bağlayarak daha da farklı üçüncü bir kaotik sistem oluşturmaktadır. Bu sistem ile hesaplanan değerler şifreleme anahtarlarıdır ve bu anahtarların elde edilme olasılığı, sadece bir tek kaotik sistem tarafından üretilen anahtarların elde edilme olasılığından daha düşüktür.

CC2 çıkışında elde edilen y_i değerleri bir sonraki katman olan Kuantalama katmanına gönderilir.

4.1.4. Kuantalama katmanı

Bu katmanın ana görevi, kaotik hesaplama katmanlarından gelen değerleri ikili (binary) sayılara dönüştürmektir. Dönüştürülen bu sayı "Şifre kodu" olarak isimlendirilecektir. "Şifre kodu" N-bitten oluşmaktadır.

Kuantalama katmanı, örneklenmiş bir sinyalin kuantalama seviyelerinin belirlenmesi ve ikili sayı sistemine kodlanması işlevlerini gerçekleştirir. y_i değerleri örneklenmiş sinyaller olarak kabul edilirse, bu sayıların hangi kuantalama seviyesine sahip olacağının belirlenmesi gerekir. Kuantalama seviyesi, şifreleme kodunun kaç bit olacağını belirler. $L = 2^N$ formülü ile hesaplanır. Şekil 4.10'da kuantalama katmanından gelen reel sayılardan Şifre kodu olarak isimlendirilen bit dizilerinin oluşturulması işlemleri görülmektedir.



Şekil 4.10. Kuantalama katmanına gelen reel sayılardan bit dizisinin oluşturulması.

Kuantalama seviyesinin belirlenmesi önemli bir konudur. Eğer L yeterince büyük seçilmezse, y_i'nin belirlediği kaotik değerler dizisi daralacak ve davranış kaotik olmaktan çıkacaktır. Ayrıca, burada orta yükseltili bir kuantalayıcı kullanılarak, lojik karıştırıcı katmanına gönderilecek şifreleme kodunun tamamen 0-bitlerinden oluşması engellenir ve bu sebeple oluşabilecek zayıflıklar giderilebilir.

Kuantalama işlemi, güvenliği artırıcı bir etken olarak belirli bir fonksiyonla kontrol edilebilir. Bu fonksiyonu CC2 çıkışlarından belirlemek mümkündür. Örneğin CC2 üç boyutlu bir sistem ise Y_1, Y_2, Y_3 çıkışlarına sahip olacaktır. Bu noktada, kuantalanacak sayıyı belirlemek üzere bu üç çıkışa bağlı bir fonksiyon, $f(y) = f(Y_1, Y_2, Y_3)$ şeklinde tanımlanabilir. Bu şekilde, kaotik hesaplama katmanları saldırgan tarafından deşifre edilmiş bile olsa, *f(y)* fonksiyonu bilinmedikçe şifreleme anahtarları ele geçirilemez. Bunun neticesinde önerilen *f(y)* fonksiyonu ile sisteme ilave bir güvenlik seviyesi kazandırılmış olur.

4.1.5. Lojik Karıştırıcı katmanı (LME)

LME (Logical Mixer for Encoder) şifresiz p_i verisi ile şifre kodunu, belirlenen bir M lojik fonksiyonuna göre karıştırarak kodlama görevini yerine getirir. Burada her seferinde N adet bit karıştırılır. Bu işlem yapılırken, eş zamanlı olarak önceki katmanlar ikinci bir şifre kodunu oluştururlar. Bu şekilde bir akış ile gönderilecek bütün veri kodlanır ve kodlanmış m_i paketleri haberleşme kanalına sunulur.

$m_i = M(p_i, q_i)$ şeklinde yazılarak (Denklem 4.5) aşağıdaki gibi yeniden düzenlenebilir.

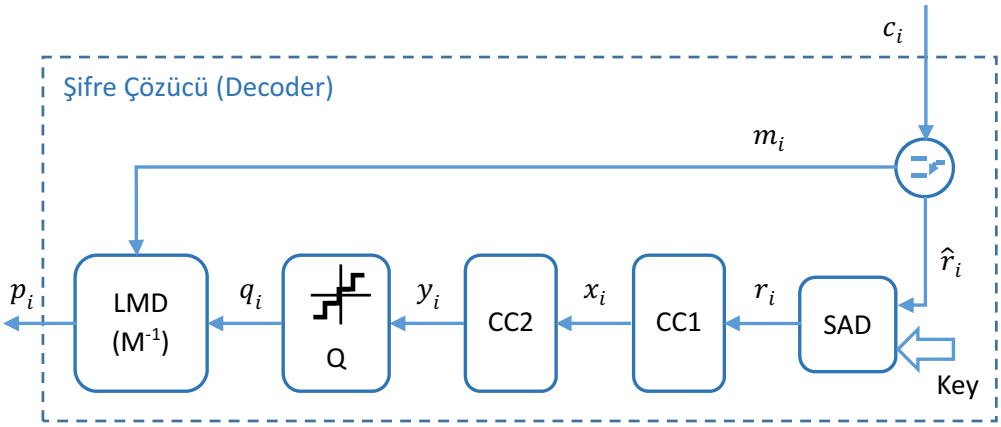
$$c_i = M(p_i, q_i, \hat{r}_i) \quad \textbf{(4.12)}$$

Bu ifadedeki $\hat{r}_i$, şifre çözücüye gönderilecek şifreli veridir ve (Denklem 4.12) $\hat{r}_i$'den bağımsız olarak aşağıdaki gibi yazılabilir.

$$c_i = M(p_i, q_i) \quad \textbf{(4.13)}$$

4.2. Şifre Çözme İşlemi

Şifre çözücü, şifreleyicide bulunan katmanların ters bir şekilde dizilişinden meydana gelmektedir. Şifre çözme bölümüne gelen c_i, SC ve kodlanmış m_i bilgilerinin toplamından oluşmaktadır. Bölüm 4.1.2'de açıklandığı üzere, SC ister ayrı olarak isterse şifreli paketle birlikte gönderilsin; şifre çözücü SAD katmanında, öncelikle bu SC bilgisinin şifresini çözer. SAD (Symmetric or Asymmetric Decryption), geleneksel bir simetrik veya asimetrik şifre çözme yöntemi olup SAE katmanı ile aynı yöntemi kullanmaktadır. Bu sayede SAD, SAE tarafından şifrelenen bilgiyi tekrar elde etmekte; elde ettiği r_i sayılarını kendi CC1 katmanına giriş olarak göndermektedir. Buradaki r_i sayıları, şifreleyicinin RNG katmanı tarafından üretilen rastgele reel sayılardır.



Şekil 4.11. Önerilen yeni kaos tabanlı kriptolama sistemi, şifre çözücü blok diyagramı

Şekil 4.11'de gösterilen CC1, CC2 ve Q katmanları, şifreleyicide bulunan aynı isimli katmanlarla özdeştir. Bu nedenle, her iki taraftaki kaotik sistem de aynı r_i başlangıç koşullarında çalışmaya başlayacak dolayısıyla aynı sonuç değerlerini üretecektir. Bu şekilde verici (şifreleyici) ile alıcı (şifre çözücü) arasında senkronizasyon garanti edilmektedir.

r_i'nin yeniden elde edilmesiyle başlayan süreç, kuantalayıcı çıkışındaki q_i değerlerinin oluşturulmasına kadar şifreleyici bölümle özdeş olarak devam eder. Elde edilen bu q_i değerleri LMD katmanında, şifreli c_i verisinden ayrıştırılan m_i verisiyle LME katmanındaki fonksiyonun tersi olan M^{-1} lojik fonksiyonuna göre karıştırılır. (Denklem 4.6)'da gösterilen bu işlem;

$$p_i = M^{-1}(m_i, q_i, \hat{r}_i) \quad \textbf{(4.14)}$$

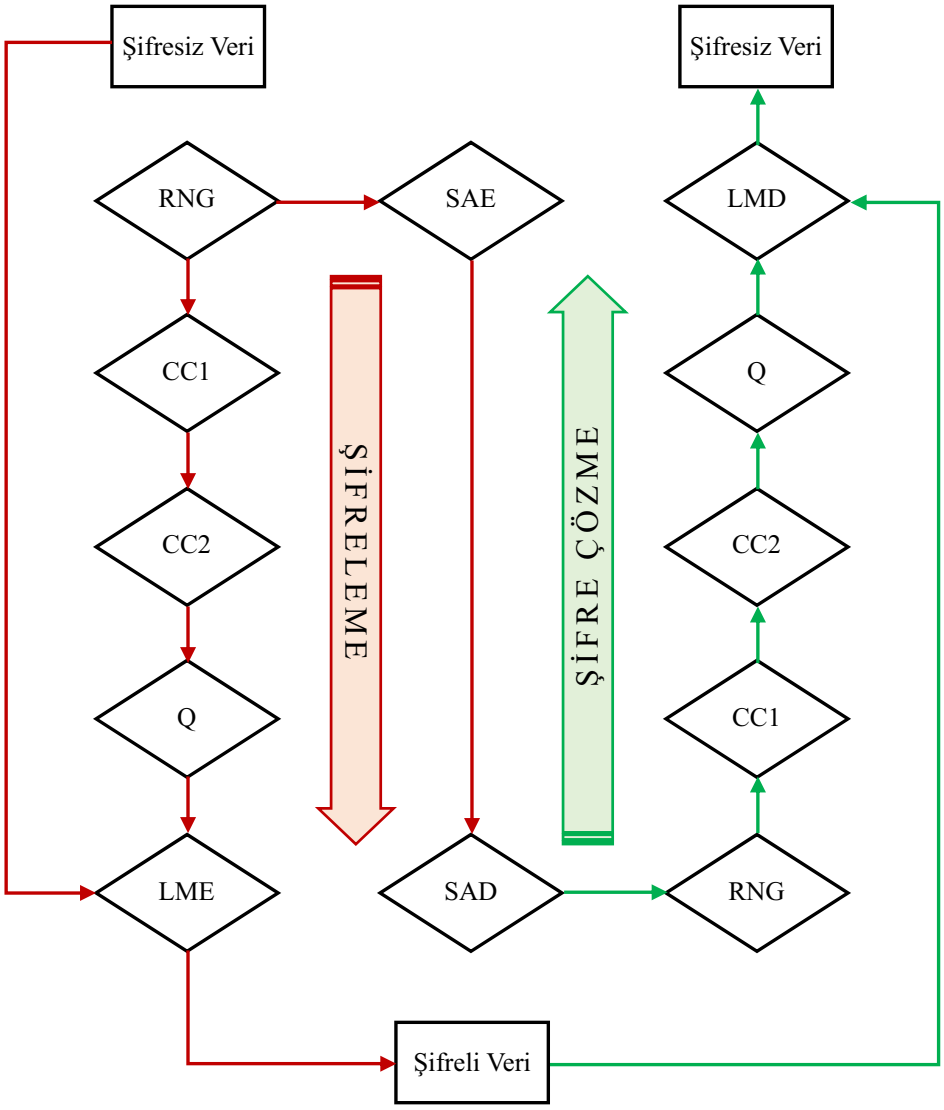
şeklinde yeniden düzenlenebilir. Bu ifadedeki $\hat{r}_i$, q_i'nin oluşturulmasında kullanılmaktadır ve (Denklem 4.14) $\hat{r}_i$'den bağımsız olarak aşağıdaki gibi yazılabilir.

$$p_i = M^{-1}(m_i, q_i) \quad \textbf{(4.15)}$$

q_i, N-bitlik şifre kodunu belirlemektedir. Her bir adımda N-bitlik m_i verisinin şifresi çözülmekte ve bu işlem tüm verinin şifresi çözülene kadar devam etmektedir.

Alıcı, SC kodunu bilmiyorsa (çözemezse) şifresiz veriyi elde edemez. Bu yüzden SC hem senkronizasyonu hem de güvenliğin bir seviye daha artırılmasını sağlamaktadır.

Gerçekleştirilen kaos tabanlı kriptolama sistemi ile verinin şifrelenmesi ve tekrar geri elde edilmesi Şekil 4.12'deki akış diyagramında gösterilmektedir.



Şekil 4.12. Önerilen yeni kaos tabanlı kriptolama sisteminin akış diyagramı.

BÖLÜM 5. UYGULAMA SONUÇLARI

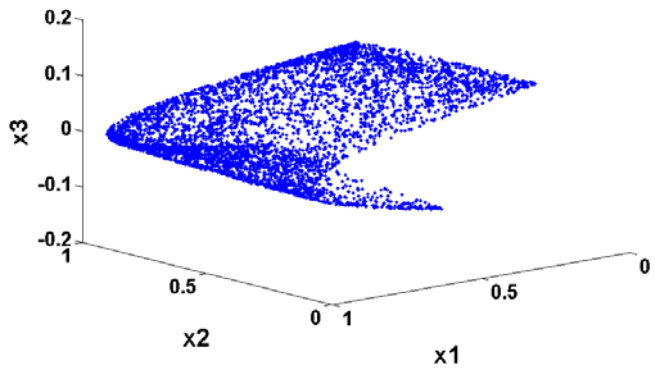
Önerilen yeni kaos tabanlı kriptolama sistemi iki ayrı uygulamada kullanılmıştır. Birincisi görüntü şifreleme; ikincisi ise bilgisayar haberleşmesi için bir veri şifreleme uygulamasıdır. Uygulamalarda kullanılan kaotik sistemler ve yapılan her iki uygulamaya ait bulgular ve sonuçlar bu bölümde verilecektir.

5.1. Uygulamalarda Kullanılan Kaotik Sistemler

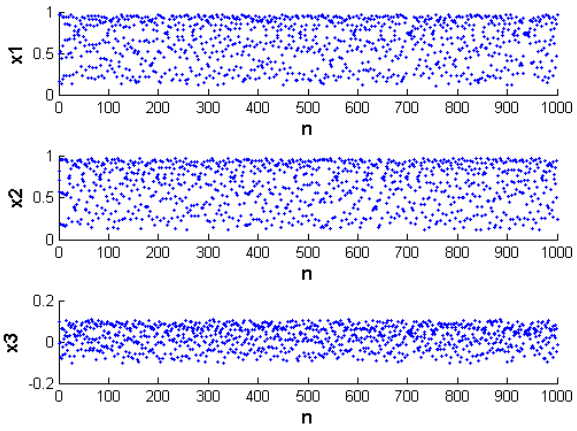
Bu bölümde, uygulamalarda kullandığımız ayrık zamanlı kaotik sistemler kısaca tanıtılacaktır. Sistemlerin matematiksel ifadelerinde verilen X_i, Y_i durum değişkenleri, $a, b, c, d, e, f, g, h, i$ sistem parametrelerdir.

Rossler kaotik sistemi [110]:

$$X_1[n+1] = aX_1[n](1 - X_1[n]) - b(X_3[n] + c)(1 - dX_2[n])$$
$$X_2[n+1] = eX_2[n](1 - X_2[n]) + fX_3[n] \quad \textbf{(5.1)}$$
$$X_3[n+1] = g(1 - hX_1[n])((X_3[n] + c)(1 - dX_2[n]) - i)$$



Şekil 5.1. Rossler sistemi 3D faz portresi.



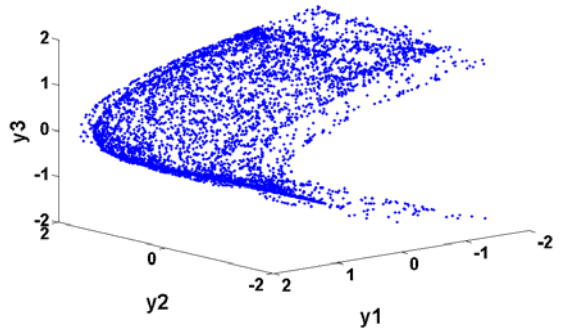
Şekil 5.2. Rossler sistemi zaman serileri.

Rossler kaotik sistemi (Denklem 5.1)'de verilen diferansiyel denklem takımı ile tanımlıdır. Sisteme ait faz portresi ve zaman serileri sırasıyla Şekil 5.1 ve Şekil 5.2'de verilmektedir. [a b c d e f g h i] = [3.8 0.05 0.35 2 3.78 0.2 0.1 1.9 1] ve ($x_1(0)$ $x_2(0)$ $x_3(0)$] = [0.2 0.6 0.1].

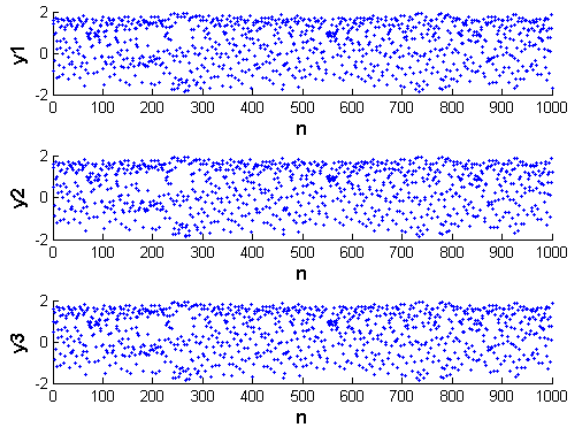
Henon kaotik sistemi [92]:

$$Y_1[n+1] = a - Y_2{}^2[n] - bY_3[n]$$
$$Y_2[n+1] = Y[n] \qquad \textbf{(5.2)}$$
$$Y_3[n+1] = Y_2[n]$$

Henon kaotik sistemi (Denklem 5.2)'de verilen diferansiyel denklem takımı ile tanımlıdır. Sisteme ait faz portresi ve zaman serileri sırasıyla Şekil 5.3 ve Şekil 5.4'de verilmektedir. [a b] = [1.76 0.1] ve ($y_1(0)$ $y_2(0)$ $y_3(0)$] = [1.6 0.5 1].



Şekil 5.3. Henon sistemi 3D faz portresi



Şekil 5.4. Henon sistemi zaman serileri.

5.2. Görüntü Şifreleme Uygulaması

Önerilen yeni kriptolama sistemi ile gerçekleştirilen ilk uygulama görüntü şifreleme (image encryption) uygulamasıdır. Bu uygulama ile görüntü dosyası kriptolanarak, ağ ortamına sunulmaktadır. Karşı tarafta alınan dosyanın kriptosu çözülerek, orijinal görüntü elde edilmektedir. Bu uygulamada, CC1 katmanında ayrık zamanlı kaotik Rossler sistemi, CC2 katmanında ise ayrık zamanlı kaotik Henon sistemi kullanılmıştır.

Yapılan uygulamada, öncelikle RNG katmanında üretilecek reel sayıların değer aralıkları belirlenmiştir. Bu aralığı belirleyebilmek için, CC1 katmanında kullanılan kaotik Rossler sisteminin zaman serileri, farklı parametrelerle ve farklı başlangıç koşullarında MATLAB programı kullanılarak analiz edilmiştir. Analizde 1000 farklı başlangıç koşulunda, durum değişkenlerinin aldığı minimum ve maksimum değerler $1x10^8$ örnekten oluşan zaman serileri incelenerek hesaplanmıştır. Hesaplanan bu değerler Tablo 5.1'de verilmektedir. 5 farklı parametre kombinasyonu için yapılan bu hesaplamaların sayısı artırılabilir. Kullanılacak parametrelere göre, bu tabloda verilen değer aralıkları, RNG katmanı tarafından üretilecek sayıların belirlenmesinde kullanılır.

Biz bu uygulama için, Tablo 5.1'deki 1 numaralı satırda verilen parametreleri kullanarak RNG değer aralıklarını aşağıdaki gibi belirledik.

$$0.020 \leq r_1 \leq 1$$
$$0.020 \leq r_2 \leq 1$$
$$-0.196 \leq r_3 \leq 0.196$$

Tablo 5.1. Rossler sistemi zaman serisi analiz sonuçları.

	Parametreler	$0.01 \leq X_1(0) \leq 1.1$ $0.01 \leq X_2(0) \leq 1.1$ $-0.2 \leq X_3(0) \leq 0.2$		
		X_1min **X_1max**	**X_2min** **X_2max**	**X_3min** **X_3max**
1	a=3.8; b=0.05; c=0.35; d=2; e=3.78; f=0.2; g=0.1; h=1.9; i=1	0.0200 1.0000	0.0200 1.0000	-0.1960 0.1960
2	a=3.9; b=0.05; c=0.05; d=2; e=3.78; f=0.2; g=0.2; h=1.9; i=1	0.0123 1.0000	0.0200 1.0000	-0.2212 0.1960
3	a=3.7; b=0.07; c=0.06; d=1.5; e=3.78; f=0.15; g=0.15; h=1.7; i=1	0.0090 1.0000	0.0200 1.0000	-0.1960 0.1960
4	a=3.5; b=0.053; c=0.09; d=4.9; e=2.55; f=0.15; g=0.2; h=1.5; i=1	0.0200 1.0000	0.0192 1.0000	-0.2125 0.2115
5	a=3.75; b=0.035; c=1; d=4.9; e=2.2; f=0.15; g=0.2; h=1.4; i=1	0.0200 1.0018	0.0137 1.0000	-0.5319 0.4532

RNG değerleri MATLAB programındaki "normrnd" komutu kullanılarak normal dağılım fonksiyonuna göre oluşturulmaktadır. RNG değer aralıkları belirlendikten sonra, CC2 kaotik sistemi için benzer bir zaman serisi analizi yapılmıştır. Bunun nedeni, CC1 ile CC2 arasında tasarlanacak kontrolörü belirlemek içindir. Bu kontrolör, CC1 çıkışlarını, CC2'nin kaotik davranış gösterdiği çalışma bölgeleri için ayarlayacaktır. CC2 çıkışında kaotik bir davranış gözlenebilmesi için, CC2 başlangıç koşullarının dikkatlice belirlenmesi gerekmektedir. Tablo 5.2'de, farklı parametreler kullanıldığında farklı başlangıç koşulları için CC2'de bulunan ayrık zamanlı kaotik Henon sisteminin üretmiş olduğu çıkışların minimum ve maksimum değerleri verilmektedir. Bu analiz de 1000 farklı başlangıç koşulu için yapılmıştır.

Zaman serisi analizlerinde, farklı başlangıç koşulları için ayrı ayrı hesaplamalar yapılmaktadır. Başlangıç koşulları için atanacak minimum ve maksimum değerler, ilgili kaotik sistemlerin kararlı çalışma bölgelerine bakılarak öncelikle kabaca seçilir.

Daha sonra seçilen bu sınırlar küçük aralıklarla genişletilir. Sistem hala kaotik davranış gösteriyorsa bu genişletmeye devam edilir; aksi halde genişletme durdurulur ve sınır değer belirlenir. Tablo 5.1 ve Tablo 5.2'den de görüldüğü üzere, başlangıç koşullarının minimum ve maksimum değerleri ile durum değişkenlerinin minimum ve maksimum değerleri farklıdır ve genellikle durum değişkenleri daha dar bir aralığa sahiptir. Yapılan uygulamada, daha dar olan aralıklara göre seçimler yapılmıştır. Bunun nedeni, oluşturulacak şifreleme anahtarlarının kaotik davranışın sınır bölgelerinden uzak tutulması içindir.

Tablo 5.2. Henon sistemi zaman serisi analiz sonuçları.

	Parametreler	$-1.9 \leq Y_1(0) \leq 1.9$ $-1.9 \leq Y_2(0) \leq 1.9$ $-2 \leq Y_3(0) \leq 2$		
		Y_1min **Y_1max**	**Y_2min** **Y_2max**	**Y_3min** **Y_3max**
1	a=1.76; b=0.1	-1.8900 1.9435	-1.8900 1.9435	-1.9960 1.9435
2	a=1.70; b=0.13	-1.8910 1.9443	-1.8910 1.9443	-1.9960 1.9443
3	a=1.5; b=0.2	-1.8900 1.7802	-1.8900 1.7802	-1.9960 1.7802
4	a=1.2; b=0.35	-1.8900 1.6959	-1.8900 1.6959	-1.9960 1.6959
5	a=0.95; b=0.4	-1.8900 1.5406	-1.8900 1.5406	-1.9960 1.5406

Tablo 5.2'deki 1 numaralı satırda verilen sınır değerleri, bizim bu uygulamada kullandığımız değerlerdir. Buna göre, CC2 sisteminin giriş sınırları aşağıdaki gibi olmalıdır.

$$-1.890 \leq y_1 \leq 1.9435$$
$$-1.890 \leq y_2 \leq 1.9435$$
$$-1.996 \leq y_3 \leq 1.9435$$

CC1 sisteminin çıkışları ise Tablo 5.1'de görüldüğü üzere aşağıda verilen sınırlar arasında olmaktadır.

$$0.020 \leq x_1 \leq 1$$
$$0.020 \leq x_2 \leq 1$$
$$-0.196 \leq x_3 \leq 0.196$$

Bu sonuçlardan görüldüğü üzere, CC1 çıkışındaki değerler CC2 girişinde olması gereken değerlerden daha küçüktür. Örneğin, CC2'nin y_1 değişkeninin başlangıç koşulları için (–1.89) ile (1.9435) arasında değer seçilebilirken, CC1'in x_1 değişkeni (0.02) ile (1) arasında değer üretmektedir. Eğer y_1 için başlangıç koşullarını x_1 çıkışlarına göre belirlersek, y_1 çıkışında üretilebilecek değerler kümesini de sınırlandırmış oluruz. Bu yüzden y_1 başlangıç koşulları mümkün olduğunca farklı sayılardan seçilmelidir. Bu noktada tasarlanacak bir kontrolör ile, x_i değerlerini y_i değer aralığına genişletebiliriz. Bu amaçla, aşağıdaki gibi bir kontrolör tasarlanmıştır.

$$A = \begin{bmatrix} 0.1 & 0 & 9 \\ 0 & 0.1 & 9 \\ -0.1 & 0 & 10 \end{bmatrix}$$

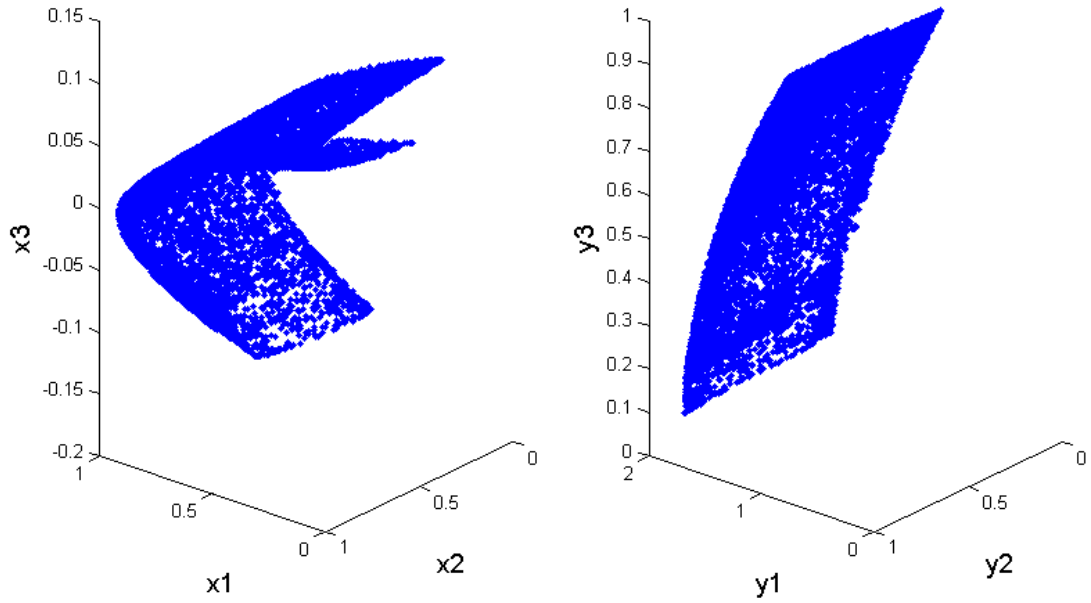
$$h = A.X_i{}^T = \begin{bmatrix} 0.1 & 0.1 & 8 \\ 0 & 0.2 & 9 \\ -0.1 & 0 & 10 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix}$$

Bu durumda CC2 girişlerinin değer aralıkları aşağıdaki gibi olur.

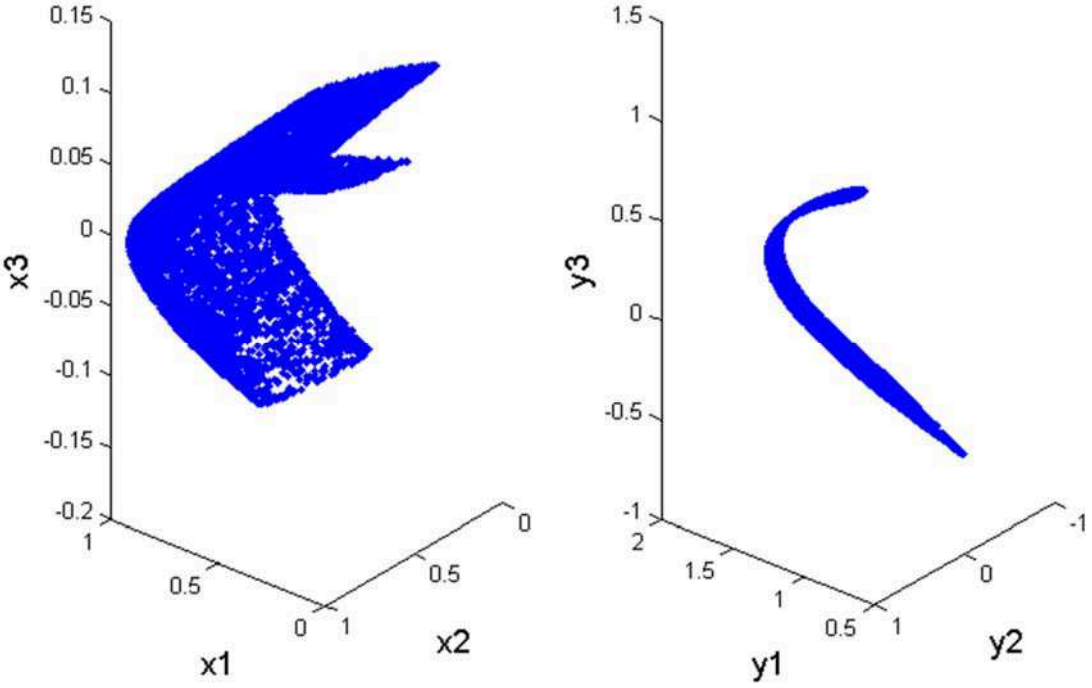
$$-1.762 \leq y_1 \leq 1.864$$
$$-1.762 \leq y_2 \leq 1.864$$
$$-1.962 \leq y_3 \leq 1.86$$

Kontrolör bu şekilde CC2 giriş aralığını genişletmekte ve çıkışta daha çok sayıda farklı değer üretilmesini sağlamaktadır. Daha çok sayıda değer, daha fazla şifreleme anahtarı, dolayısıyla daha güçlü bir kripto sistemi anlamına gelmektedir.

Bu aşamada, CC1 ve CC2 çıkışında meydana gelen davranışlar gözlemlenmiştir. CC1 ve CC2 sistemlerine ait faz portreleri; kontrolör olmadığı durumda Şekil 5.5'de, kontrolör kullanıldığı durumda ise Şekil 5.6'da gösterilmektedir.



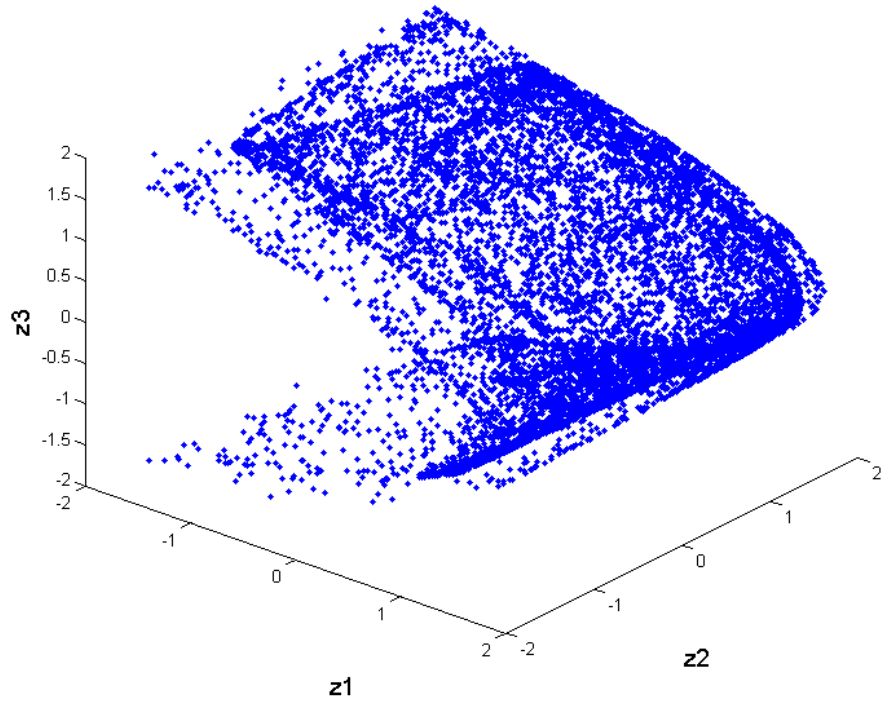
Şekil 5.5. CC1 ve CC2 sistemlerinin 3D faz portreleri (kontrolör yokken).



Şekil 5.6. CC1 ve CC2 sistemlerinin 3D faz portreleri (kontrolör varken).

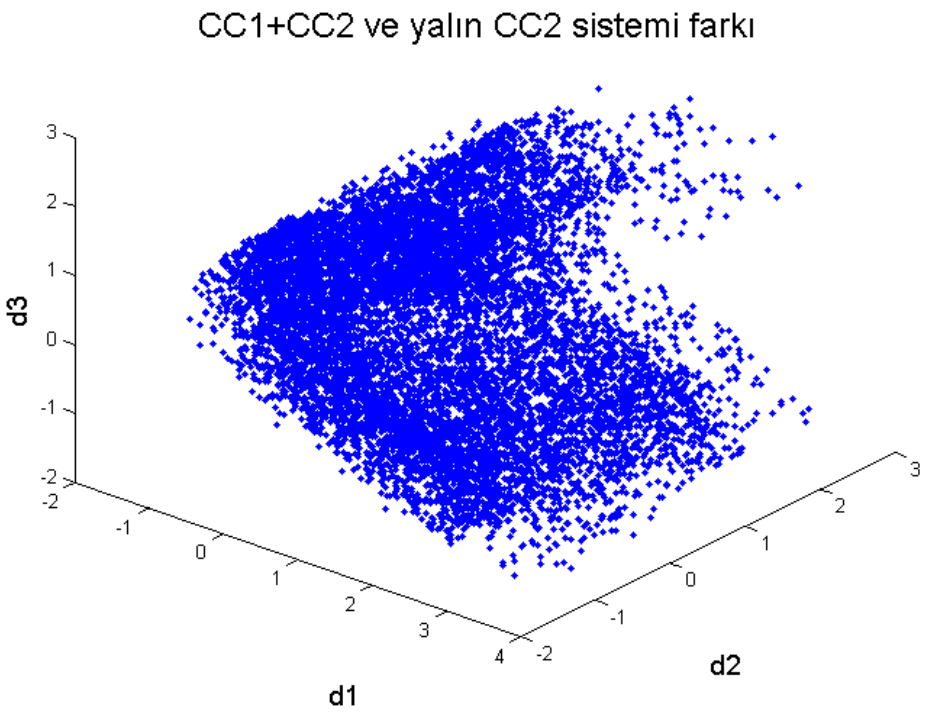
Kontrolör kullanıldığı durumda, çıkışta 3-kat daha fazla değer üretildiği görülmektedir. Ayrıca daha farklı bir kaotik davranış oluşmaktadır.

CC1+CC2 sistemi, CC2'nin sürekli olarak CC1 tarafından sürüldüğü; kaotik kriptolama sistemi içinde şifreleme anahtarlarının üretildiği yerdir. CC2'de bulunan ayrık zamanlı kaotik Henon sistemi, yalın olarak çalışmış olsaydı, yani sürekli olarak CC1 tarafından başlangıç koşulları değiştirilmeseydi Şekil 5.7'deki gibi bir faz portresine sahip olacaktı.

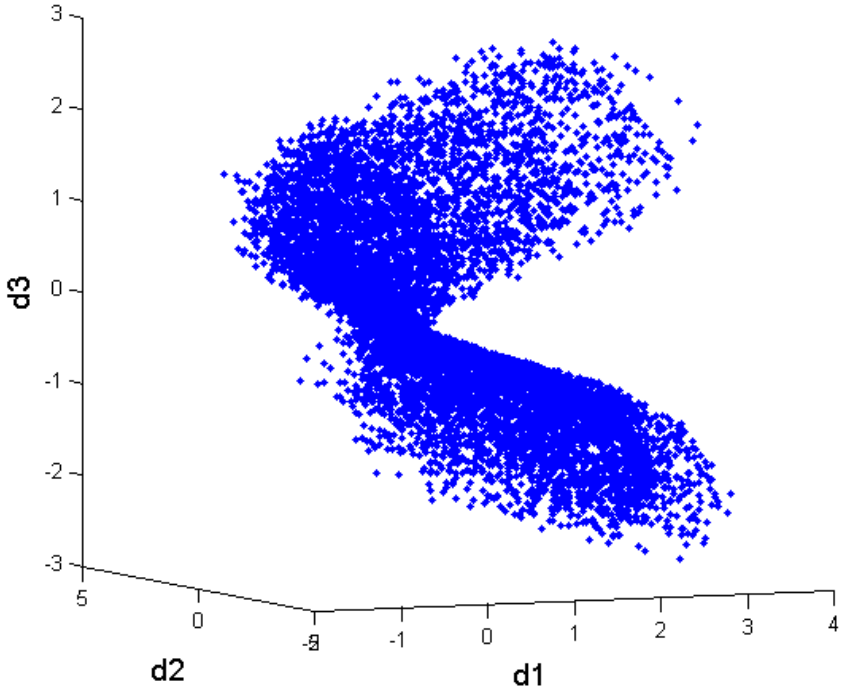


Şekil 5.7. CC2 sisteminin yalın 3D faz portresi.

CC1+CC2 sistemi ile yalın CC2 sistemi arasındaki fark Şekil 5.8 ve Şekil 5.9'da gösterilmektedir. Şekillerde de görüldüğü gibi, iki kaotik sistem arasındaki fark da kaotiktir. Bu şekilde, çalışma bölgeleri ve başlangıç koşulları birbirine adapte edilen iki farklı kaotik sistemden üçüncü bir farklı kaotik sistemin elde edilebileceği gösterilmektedir. Ayrıca, tasarlanacak lineer bir kontrolör ile daha da farklı kaotik davranışlar elde edilebilir.



Şekil 5.8. CC2 çıkışında meydana gelen değişime ait faz portresi (kontrolör yokken).



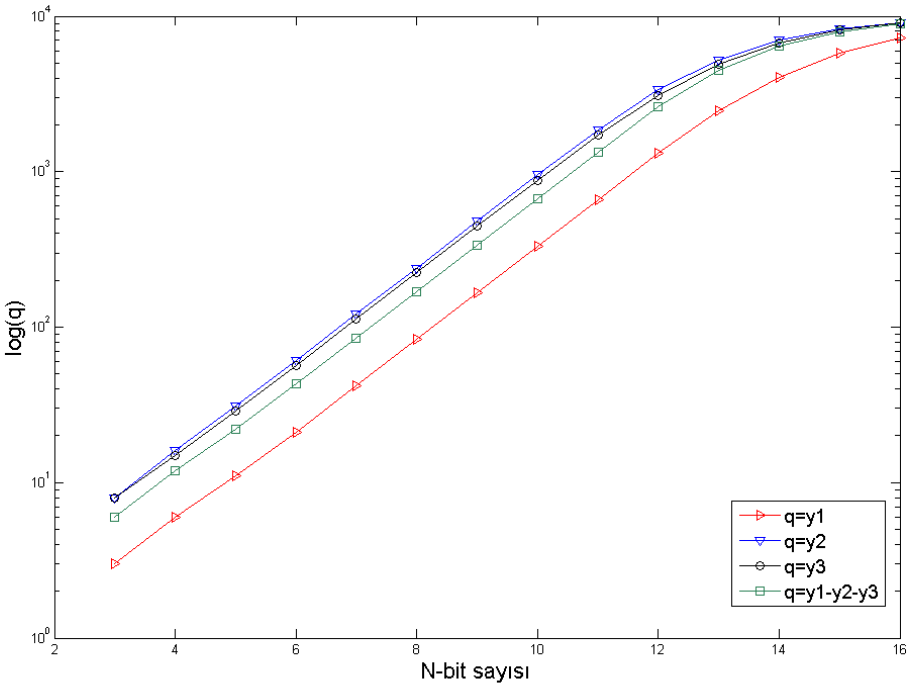
Şekil 5.9. CC2 çıkışında meydana gelen değişime ait faz portresi (kontrolör varken).

CC2 çıkışında elde edilen şifreleme anahtarları kuantalayıcı katmanında ikili sayılara dönüştürülmektedir. Bu ikili sayı dizisi "şifre kodu" olarak adlandırılmıştı. Bu aşamada, şifre kodunu oluşturmak için farklı seviyelerde kuantalama işlemi yapılarak sonuçlar karşılaştırılmıştır. Kuantalama seviyesi L, bit sayısı N olmak üzere, orta seviyeli doğrusal kuantalayıcı kullanılarak yapılan işlem sonuçları Tablo 5.3'de verilmiştir. q, üretilen şifre kodudur ve bu analizde her bir kuantalama seviyesi için kaç farklı q değerinin oluştuğu incelenmektedir. Tabloda $1x10^6$ döngü kullanılarak elde edilen sonuçlar ve bu sonuçların elde edilmesi için geçen süreler verilmektedir.

Tablo 5.3. Farklı bit sayıları için elde edilen şifre kodunun alabileceği farklı değerler.

Seviye sayısı L	**q-bit sayısı** $N = \log_2 L$	$q = y_1$ **(adet)**	**İşlem süresi (ms)**	$q = y_2$ **(adet)**	**İşlem süresi (ms)**	$q = y_3$ **(adet)**	**İşlem süresi (ms)**	$q = y_1 - y_2 - y_3$ **(adet)**	**İşlem süresi (ms)**
8	3	3	6.6	8	6.65	8	6.64	6	6.61
16	4	6	6.68	16	6.72	15	6.68	12	6.68
32	5	11	7.62	31	7.73	29	7.73	22	7.74
64	6	21	7.66	61	7.74	57	7.74	43	7.74
128	7	42	7.7	121	7.75	112	7.74	85	7.76
256	8	84	7.8	240	7.81	223	7.81	169	7.81
512	9	167	7.82	480	15.62	445	15.62	337	15.62
1024	10	331	15.62	956	23.43	882	23.43	673	23.43
2048	11	660	31.25	1859	39	1714	31.3	1341	39
4096	12	1308	54.68	3352	70.3	3098	70.3	2615	70.3
8192	13	2459	109.4	5235	140.6	4921	140.6	4506	140.62
16384	14	4030	203.1	7058	273.4	6770	273.43	6421	257.6
32768	15	5756	429.7	8329	539	8124	539	7983	515.6
65536	16	7269	882	9104	1085	9016	1039	8933	1029

Kriptolama sistemi, ne kadar çok q-şifre koduna sahip ise, yapılacak şifreleme o kadar güçlüdür. Kaotik katmanlar çıkışında elde edilen şifreleme anahtarlarının sayısı çok fazladır. Ancak bu sayıların çeşitliliği, kuantalama işlemi sonucunda azalmaktadır. Dolayısıyla farklı şifre kodu sayısı azalmaktadır. Kuantalama seviyesi ne kadar çok ise farklı şifre kodu sayısı da o kadar çoktur. Ancak tablodan da görüldüğü üzere, kuantalama seviyesi arttıkça, işlem süresi de artmaktadır. Bu süre, kriptolama sisteminin hızı ile doğrudan ilgilidir.



Şekil 5.10. Farklı şifre kodu sayısının, şifre kodu uzunluğu ile ilişkisi.

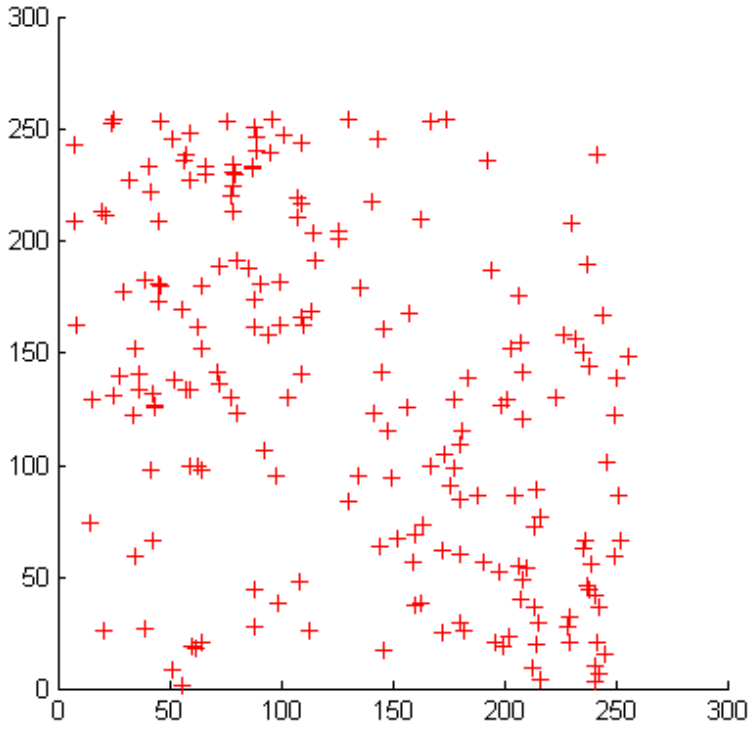
Şekil 5.10'da şifre kodunun, uzunluğuna (bit-sayısı) göre alabileceği farklı değerler grafiksel olarak gösterilmiştir. q değerleri, CC2 çıkışlarından türetilmektedir. Yapılan hesaplamalarda Tablo 5.3 ve Şekil 5.10'da gösterildiği gibi 4 farklı q değeri seçilmiştir.

Şifre kodları elde edildikten sonra, bu kodlar, şifresiz verinin N-adet biti ile lojik karıştırıcı katmanında karıştırılmaktadır. Lojik karıştırıcı katmanında M fonksiyonu olarak XOR işlevini kullandık. Buna göre şifrelenmiş veri, $m_i = p_i \, XOR \, q_i$ olmaktadır. p_i şifresiz veri, q_i elde edilen şifre kodlarıdır. Tablo 5.4, farklı şifre kodu uzunlukları için lojik karıştırıcı çıkışında elde edilen şifrelenmiş verileri göstermektedir.

N=8 bitlik şifre kodları tarafından şifrelenmiş veri ile şifresiz veri arasındaki bağıntının doğrusal olmadığı, Şekil 5.11'de verilen lojistik haritada gözlemlenmektedir.

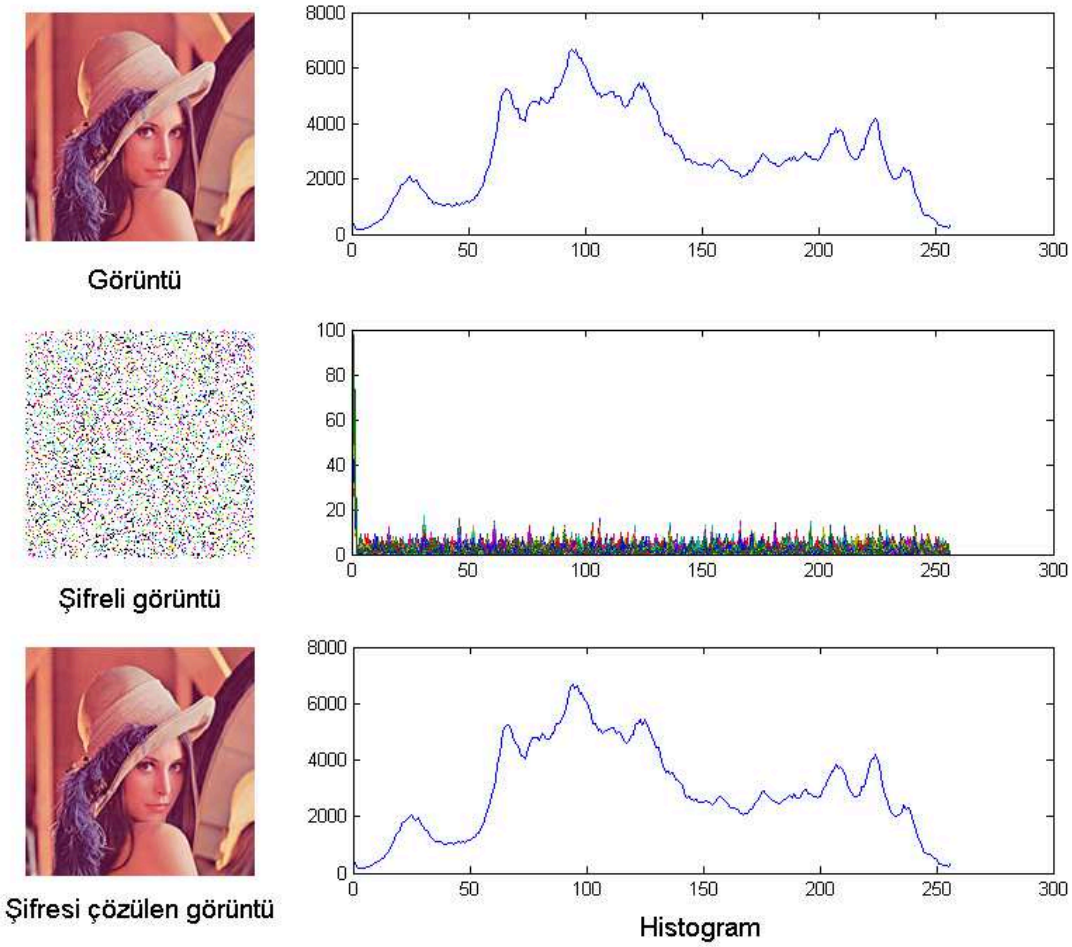
Tablo 5.4. Veri ile şifre kodunun XOR fonksiyonu ile karıştırılması ve şifreli verinin elde edilmesi.

N=8-bit			N=10-bit			N=12-bit			N=16-bit		
p_i	q_i	m_i	p_i	q_i	m_i	p_i	q_i	m_i	p_i	q_i	m_i
4E	FF	B1	38E	3FD	073	7F1	FF6	807	AE66	FF66	5100
1F	7E	61	2E4	1FA	31E	61D	7EA	1F7	C85C	7EA0	B6FC
E8	F0	18	030	3C2	3F2	90D	F09	604	FFFA	F091	0F6B
B2	44	F6	37B	112	269	B56	44A	F1C	5B03	44A7	1FA4
6D	B4	D9	26E	2D2	0BC	7E3	B49	CAA	51BC	B498	E524
FE	B9	47	2E4	2E6	002	434	B9A	FAE	7C96	B9A3	C535
CC	83	4F	134	20F	33B	78E	83E	FB0	BF7C	83E3	3C9F
AE	FC	52	3D2	3F0	022	226	FC1	DE7	6295	FC15	9E80
1F	54	4B	3A1	151	2F0	2E5	544	7A1	92CF	544F	C680
CB	97	5C	121	25F	37E	29F	97E	BE1	A1E3	97E7	3604
7A	F6	8C	33B	3D8	0E3	D75	F61	214	8F19	F612	790B
2F	5C	73	07A	171	10B	534	5C5	0F1	88BB	5C5F	D4E4
9A	BF	25	0E5	2FE	21B	2C1	BF8	939	854A	BF8D	3AC7
BA	BE	04	2DD	2FB	026	E96	BEE	578	EF75	BEE2	5197
38	C2	FA	0AC	30A	3A6	3D2	C2B	FF9	E0D9	C2B8	2261
99	BA	23	1E3	2EB	308	2C4	BAC	968	BD5D	BACE	0793
1C	B5	A9	25F	2D7	088	E3D	B5E	563	FC01	B5EB	49EA
DB	BE	65	364	2FB	19F	388	BEC	864	6B08	BEC2	D5CA
64	7C	18	2F2	1F1	303	3F1	7C4	435	825E	7C47	FE19
AA	F4	5E	111	3D1	2C0	5B5	F46	AF3	D2C9	F460	26A9



Şekil 5.11. Şifresiz ve şifrelenmiş verinin lojistik haritası (N=8-bit).

Yukarıda açıklandığı gibi üretilen şifreleme anahtarları ile $q = y_2$, L=256, N=8 seçerek elde edilen şifre kodları ile 500x500 piksel büyüklüğündeki 24-bit derinlikli bir görüntü şifrelenmiştir. Şifrelenen ve şifresi çözülen görüntüler Şekil 5.12'de gösterilmektedir.

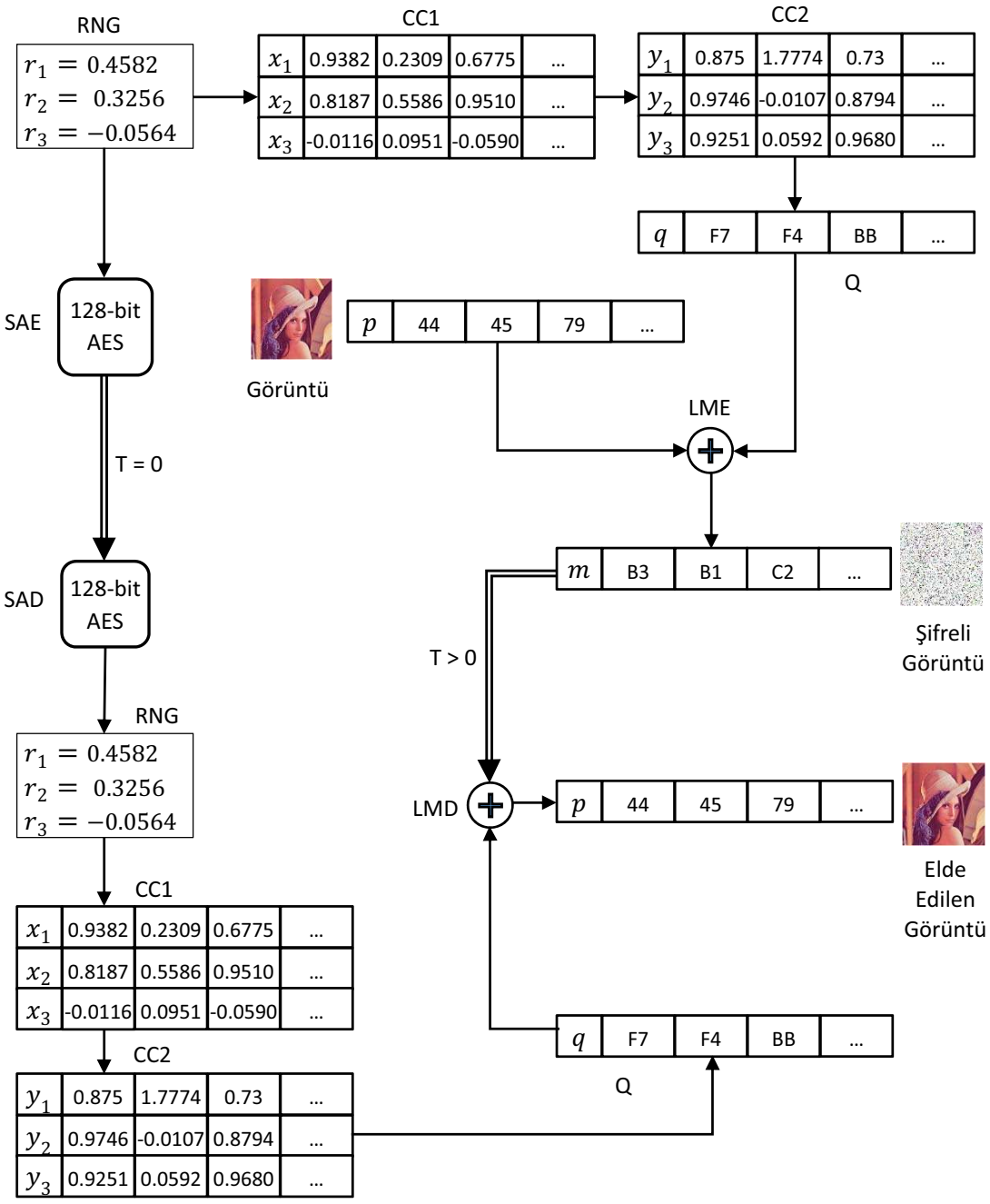


Şekil 5.12. Görüntünün şifrelenmesi ve şifresinin çözülmesi.

Şifre çözücü sistem, şifreleme sistemi ile aynıdır. Başlangıçta üretilen r_i değerleri, SAE katmanında, güçlü bir simetrik şifreleme algoritması olan 128-bit AES [106-109] algoritması ile şifrelenmiştir. Şifrelenen bu değerler ilk başta şifre çözücüye gönderilmiştir. Şifre çözücüde algılanan bu değerler, SAD katmanında çözüldükten sonra şifreleyici ve şifre çözücüdeki kaotik katmanlar aynı başlangıç koşullarına ayarlanmış, dolayısıyla aynı şifreleme anahtarlarını üretmişlerdir. Daha sonra algılanan şifrelenmiş görüntüye ait bitler şifre kodu ile yine XOR lojik fonksiyonundan geçirilmiş ve görüntünün şifresi başarıyla çözülmüştür. Görüntünün şifrelenmesi için

geçen süre 8.79ms olup, bu sistem ile 682Mbps hızında iletim yapılabileceği sonucuna varılmıştır. Tüm hesaplamalar, 2.5GHz işlemcili bir bilgisayarda MATLAB programı kullanılarak yapılmıştır.

Görüntünün şifrelenmesi ve şifresinin çözülmesi esnasında, önerilen yeni kriptolama sisteminin her bir katmanında gözlemlenen değişimler; katmanların giriş ve çıkışlarındaki işaretlere ait örnekler verilerek Şekil 5.13'de gösterilmiştir.



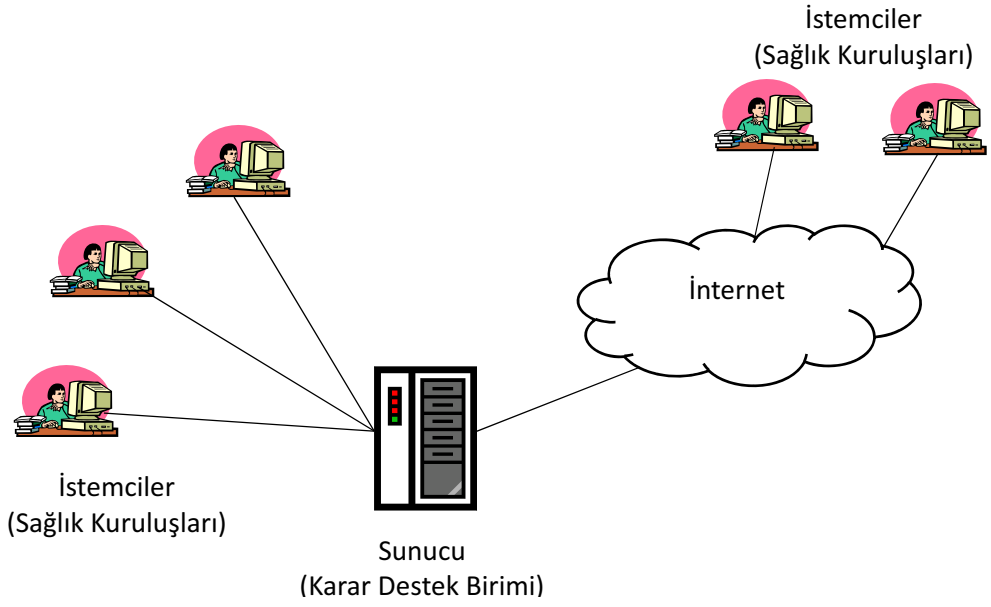
Şekil 5.13. Sayısal örneklerle görüntü şifreleme ve şifre çözme akış diyagramı.

5.3. Veri Şifreleme Uygulaması

Bu uygulamada, önerilen kaos tabanlı kriptolama sistemi ile bilgisayar ağlarında veri şifreleme işlemi gerçekleştirilmektedir. Bunun için, sağlık kuruluşlarında hastalık teşhisi için geliştirilmiş olan bir uzman sistemden yararlanılmıştır. Bu uzman sistem, yapay sinir ağı modelleri kullanılarak C# ortamında geliştirilmiş GOHAT [111-115] isimli bir yazılımdır. GOHAT yazılımı sunucu ve istemci tarafında çalışan iki modülden oluşmaktadır. İstemci modülü, sağlık kuruluşlarını; sunucu modülü ise bu sağlık kuruluşlarına hizmet veren "Karar Destek Birimini" temsil etmektedir.

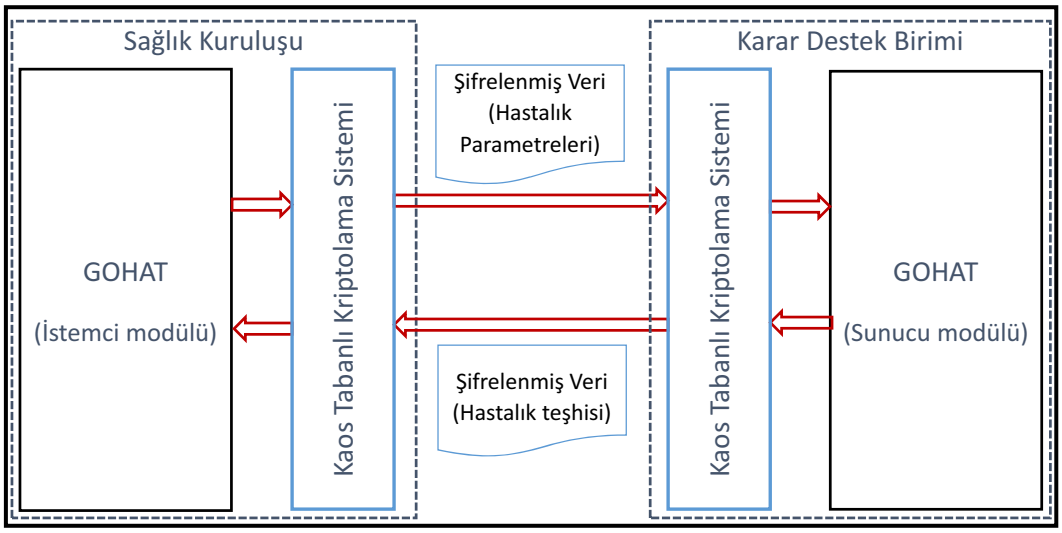
Sağlık kuruluşları, hastalarla ilgili yapmış oldukları test sonuçlarını karar destek birimine göndermekte; karar destek birimi de bu test sonuçlarını, kullandığı yapay sinir ağı modelleriyle değerlendirerek hastalık teşhisi yapmakta ve sonucu ilgili sağlık kuruluşuna bildirmektedir.

Kişisel sağlık bilgilerinin iletildiği ve bu yüzden güvenliğin önemli olduğu böyle bir haberleşme ağı senaryosu oluşturularak yapılan bu uygulamada, önerilen kaos tabanlı kripto sisteminin başarımı analiz edilmektedir. Bu amaçla oluşturulan ağın temsili gösterimi Şekil 5.14'te verilmektedir.



Şekil 5.14. Veri şifreleme uygulamasında kullanılan bilgisayar ağı yapısı.

Bu çalışmada önerilen kaos tabanlı kriptolama sistemi, şifreleme ve şifre çözme işlemlerini gerçekleştirmek üzere GOHAT yazılımının her iki modülüne de dahil edilmiştir. Böylelikle, sunucu ve istemci arasında iletilen mesajlar önerilen kriptolama sistemi ile şifrelenmektedir. Önerilen sistemin sunucu ve istemci modülüne entegrasyonunu ve düğümler arasındaki haberleşmeyi gösteren bir şema Şekil 5.15'de verilmiştir.



Şekil 5.15. Önerilen kaos tabanlı kriptolama sisteminin sunucu ve istemci tarafındaki yerleşim şeması.

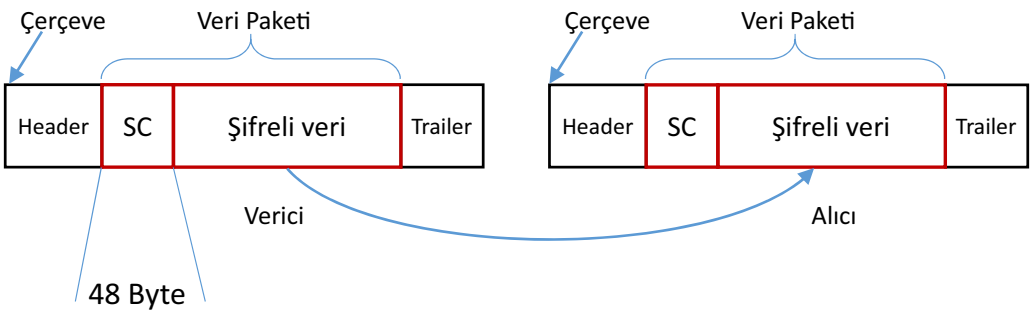
İstemci ve sunucunun haberleşmesi şu şekilde gerçekleşmektedir.

1. İstemci, test sonuçlarını paketler ve sunucuya gönderilmek üzere kriptolama sistemine gönderir.
2. Kriptolama sistemi, birinci uygulamada anlatıldığı şekilde rastgele reel sayıları üretir ve CC1 katmanına girdi olarak iletir. Aynı zamanda bu değerleri 128-bit AES algoritması ile şifreler, SC bilgisini oluşturur ve bunu sunucuya göndereceği veri paketinin başına ekler.
3. Kriptolama sistemi, birinci uygulamada yapılandan farklı olarak 16-bitlik şifre kodlarını üretir.
4. Üretilen şifre kodu, lojik karıştırıcı katmanında gönderilecek paketin ilk 16 biti ile XOR lojik fonksiyonuna göre karıştırılır. Elde edilen şifreli veri SC bilgisinin hemen devamına eklenir.

5. Tüm veri şifrelenene kadar bu işlem devam eder ve sonrasında şifreli veri paketi sunucuya gönderilir.
6. Sunucu öncelikle, almış olduğu paketin başındaki SC kodunu 128-bit AES algoritması ile çözer ve elde ettiği reel sayıları kendi CC1 katmanına girdi olarak iletir.
7. Alınan paketin diğer kısmını, istemcide oluşturulan aynı şifre kodunu oluşturduktan sonra bir akış şeklinde lojik karıştırıcı katmanında karıştırır ve şifreli paketi çözer.

Sunucu elde ettiği veriyi GOHAT modülünde değerlendirir ve elde ettiği sonucu yukarıdaki aynı işlemleri gerçekleştirerek istemciye gönderir. İstemci de benzer şekilde, almış olduğu paketin şifresini çözer ve GOHAT modülünün sonuç görüntüleme ekranında görüntüler. Bu şekilde sağlık kuruluşu test sonuçlarını güvenli bir şekilde karar destek merkezinde yorumlatmış ve hastalık teşhisi bilgisini elde etmiştir.

Bu uygulamanın görüntü şifreleme uygulamasından farkı, SC bilgisini, gönderilecek veri paketinin başına ekleyerek göndermesidir. Bu yapı Bölüm 4.1.2'de anlatılmıştır. Burada önemli olan, alıcı ile vericinin, SC bilgisinin uzunluğu konusunda anlaşmış olmalarıdır. Eğer alıcı, almış olduğu veri paketindeki SC bilgisini ayırabiliyorsa, bu sistem başarılı bir şekilde çalışacaktır. İstemci ve sunucu arasında iletilen veri paketi Şekil 5.16'da gösterilmiştir.



Şekil 5.16. İletilen veri paketinin yapısı

Uygulamalarda kullanılan kaotik Rossler sistemi 3-boyutlu bir sistem olduğu için 16 Byte büyüklüğünde 3 adet reel sayı, şifreleme işlemi öncesinde üretilmekte ve 128-bit

AES algoritması ile şifrelenmektedir. Bu yüzden SC bilgisi 48 Byte uzunluğundadır. Veri paketinde 48 Byte değerinde bir alan SC bilgisi için ayrılmaktadır.

Önerilen kriptolama sistemi bilgisayar ağları için bir üst katman uygulamasıdır ve çerçeve yapısına müdahale etmez. SC bilgisi için ayrılacak alanın belirlenmesi, SC bilgisinin gönderilmesi için çerçeve (frame) içinde rezerve edilen alanların kullanılması gibi konular, üzerinde çalışılması gereken konulardır. Bu yüzden bu çalışmalar IEEE 802.3, 802.6 gibi ilgili standartlarla birlikte yürütülmelidir.

Son olarak, gerçekleştirilen bu iki uygulama ile, önerilen kaos tabanlı kriptolama sisteminin başarımı test edilmiş; güvenli bir haberleşme sistemi oluşturmak için bu yapının kullanılabileceği sonucuna varılmıştır.

BÖLÜM 6. TARTIŞMALAR VE ÖNERİLER

Kaotik sistemler, karmaşık ve düzensiz dinamik yapıları sayesinde, rastgele işaretlere benzeyen şifreleme anahtarları üretebildiği için kriptolama sistemlerinde kullanılmaktadır. Bu şekilde üretilen anahtarlar gizliliğin sağlanması ve güvenliğin artırılmasında önemli rol oynarlar.

Önerilen kaos tabanlı kriptolama sistemini, diğer kaos tabanlı kriptolama sistemlerinden ayıran en belirgin özellik, katmanlı bir kaotik yapı kullanmasıdır. Bu katmanlı yapıda, şifreleme anahtarı öncelikle ilk kaotik sistem tarafından üretilmektedir. İkinci kaotik sistem ise, üretilen bu ilk şifreleme anahtarını kullanarak kendine özgü yeni bir şifreleme anahtarı üretmektedir. Böylelikle, gizliliği sağlayacak olan anahtarın kendisi de sistem tarafından gizlenmektedir. İki defa gizlenmiş bir şifreleme anahtarının, bir defa gizlenmiş bir şifreleme anahtarına göre daha fazla gizlilik sağlayacağı kabulüyle, katmanlı kaotik yapının daha fazla güvenlik sağlayacağı söylenebilir.

Önerilen sistem, rastgele seçilecek bir anahtarı kullanarak çalışmaya başlamaktadır. Rastgele seçilen bu anahtar, kaotik katmanlar tarafından iki defa gizlenerek asıl şifreleme anahtarı oluşturulmaktadır. Önerilen kriptolama sisteminin şifreli veriyi başarıyla çözebilmesi için, seçilen rastgele üretilmiş anahtarı bilmesi gerekmektedir. Bu yüzden, bu anahtarın şifre çözücü tarafa güvenli bir şekilde bildirilmesi gerekmektedir. Bu bildirimi yapabilmek için, geleneksel kriptolama yöntemlerinden biri kullanılmaktadır. Bunun nedeni, önerilen sistemde, her iki tarafta bulunan kaotik sistemlerin senkronizasyonu için bir kontrolörün bulunmamasıdır. Kaos senkronizasyonu için kullanılacak bir kontrolör, şifreleme ve şifre çözme işlemleri süresince sürekli icra edilmesi gereken matematiksel işlem ve hesaplamalardan oluşmaktadır. Bu işlem ve hesaplamaların getireceği yük ortadan kaldırılırsa, sistemin daha hızlı çalışacağı aşikardır. Kaos senkronizasyonunun, bu kriptolama sisteminde

kullanılmama nedeni budur. Ancak bu durumda, geleneksel şifreleme yöntemlerinde kullanılan gizli anahtarın, saldırgan tarafından ele geçirilmiş olabileceği göz önünde tutulmalıdır. Böyle bir durumda saldırgan, önemli bir bilgiyi elde etmiş olacaktır. Bu bilgi ile birlikte, sistemde kullanılan kaotik katmanları da tahmin edebilirse; saldırgan kripto sistemini rahatlıkla çözebilecektir. Böyle bir zayıflığın ortadan kaldırılması için, önerdiğimiz sistemde alınan önlemler mevcuttur. Birincisi, her iki kaotik katman arasındaki ilişkiyi belirleyen bir fonksiyon kullanılmaktadır. Bu fonksiyon basit bir lineer fonksiyondur ve kaotik sistemlerin davranışlarını önemli ölçüde değiştirmektedir. Yapılan uygulamalarda, bu fonksiyon ile bambaşka kaotik davranışların elde edilebileceği önceki bölümde gösterilmektedir. Bu nedenle, saldırganın her iki kaotik katmandaki sistemi tahmin etmesi, kripto sistemini çözmek için yeterli olmaz. Alınan diğer önlem, şifreleme anahtarının ikili sayılara dönüştürülmesi aşamasında, adaptif bir kuantalayıcı ile, farklı bit seviyelerinde dönüşüm yapılmasıdır. Yapılan uygulamalarda doğrusal kuantalayıcı kullanılmıştır. Doğrusal olmayan, daha karmaşık bir kuantalayıcı kullanılırsa bu katmanda alınan önlem daha etkin bir hale getirilebilir. Diğer bir önlem de, lojik karıştırıcı katmanında kullanılacak fonksiyon ile farklı şekillerde kodlama yapılmasıdır ki; saldırgan bu fonksiyonu bilmedikçe, diğer bütün bilgileri elde etmiş olsa dahi kriptoyu çözemez.

Önerilen kaos tabanlı kriptolama sistemi, yapılan ikinci uygulamada gösterildiği gibi, özellikle tam sayısal çalışan haberleşme sistemlerinde rahatlıkla kullanılabilir. Bununla birlikte, analog haberleşme sistemlerinde de şifreleyici/kodlayıcı bir sistem olarak kullanılabilir. Ancak bu sistem bir modülasyon tekniği olmadığı için, güvenliğin haberleşme kanalında tesis edilmesi için uygun değildir. Ancak bu çalışma, mevcut kaotik modülasyon sistemlerinde de katmanlı kaotik yapılar kullanılarak güvenliğin artırılması hususunda yapılacak çalışmalara zemin oluşturabilir.

Bu sistem, bilgisayar ağları için, OSI referans modeline göre üst katmanlarda tanımlanmıştır. Şifreleme ve şifre çözme işlemleri “Sunum Katmanında” gerçekleştirilmektedir. Üretilen rastgele sayının alıcıya gönderilmesi ve haberleşmenin başlatılması ise “Oturum Katmanında” gerçekleştirilmektedir.

Bilgisayar ağlarında oturum katmanı aynı zamanda kimlik denetiminin de gerçekleştirildiği yerdir. Önerilen kriptolama sistemi, bu noktada ekstra bir güvenlik sağlayıcı olarak kimlik denetimi yapılmasında da kullanılabilir. Şöyle ki; şifrelenerek alıcıya gönderilen SC bilgisi, haberleşme oturumunun başlatılması için alıcı ve verici arasında bir kimlik denetimi sağlayabilir. Ayrıca bu kimlik denetimi, aynı alıcı ve verici arasındaki her yeni haberleşme oturumunda tekrar yapılacağından, oturum süresi - zaman aşımı durumlarında meydana gelebilecek güvenlik açıkları için de bir önlem olabilir.

Yapılan görüntü şifreleme uygulaması sonuçlarında verildiği üzere, bu kriptolama sisteminin 682 Mbps iletim hızına sahip haberleşme sistemlerinde kullanılabileceği gösterilmiştir. Bu hızın artırılması için, önerilen kaos tabanlı kriptolama sistemi üzerinde iyileştirmeler yapılmalıdır.

Önerilen bu sistemin avantajları şu şekilde sıralanabilir:

- Kaosun güçlü şifreleme yapısından faydalanır,
- Katmanlı kaotik yapısı sayesinde daha güvenli şifreleme anahtarları üretilebilir,
- Farklı haberleşme sistemlerinde kullanılabilir,
- Mevcut Ethernet protokolleriyle uyumludur,
- Kablolu bilgisayar ağlarında rahatlıkla kullanılabilir,
- Her katmanı ayrı bir güvenlik sağlar,
- Hızlı bir sistemdir,
- Yüksek veri iletimi için uygundur.

Sistemin dezavantajı, şifre çözme işlemi için fazladan bir SC bilgisinin gönderilmesi gerekliliğidir. Her yeni haberleşme oturumu için bu bilginin gönderilmesi şarttır. Ancak bu bilgi, aynı zamanda kimlik denetiminde kullanılabileceği için, güvenliği artırıcı bir etken olarak da düşünülebilir.

Özetle, önerilen bu dört bölümlü kaos tabanlı kriptolama sisteminin her bir bölümü ayrı bir güvenlik imkanı sağlamaktadır. Bu sistem, yoğun matematiksel işlemler gerektirmediği için hızlı haberleşme sistemlerine adapte edilebilir. Özellikle ülkelerin

stratejik bilgilerinin yoğun kullanıldığı askeri savunma sanayii, endüstriyel üretim ve sağlık alanlarında tesis edilen haberleşme sistemlerinde kullanılabilir. Ayrıca, Gbit Ethernet, ATM, FrameRelay ağlarına; ses ve video haberleşmesi gibi senkron haberleşme sistemlerine uyarlanması için, gelecekte yapılacak çalışmalara zemin oluşturabilir.

Son olarak, gerçekleştirilen bu iki uygulama ile, önerilen kaos tabanlı kriptolama sisteminin başarımı test edilmiş; güvenli bir haberleşme sistemi oluşturmak için bu yapının kullanılabileceği sonucuna varılmıştır. Bununla birlikte, bu sistem ile ilgili yapılacak kriptanaliz çalışmaları ile gelecekte daha kararlı bir yapı elde edilecektir.

KAYNAKLAR

[1] PEHLİVAN, İ., Yeni kaotik sistemler: elektronik devre gerçeklemeleri, senkronizasyon ve güvenli haberleşme uygulamaları. Doktora tezi, SAÜ FBE, 2007.

[2] KARA, R., Nonlineer dinamik sistemlerde kaos, dallanma ve fraktaller. Yüksek lisans tezi, İTÜ FBE, 2006.

[3] PECORA, LM., CARROLL, TL., Synchronization in chaotic systems. Phys. Rev. Lett., 64(8):821-824, 1990.

[4] CUOMO, KM., OPPENHEIM, AV., STROGATZ, SH., Synchronization of Lorenz-based chaotic circuits with applications to communications. IEEE Transactions on Circuits and Systems II: Analog and Digital Signal Processing, 40(10):626-633, 1993.

[5] BERITELLI, F., DI COLA, E., FORTUNA, L., ITALIA, F., Multilayer chaotic encryption for secure communications in packet switching networks. Communication Technology Proceedings (WCC - ICCT 2000), IEEE: Beijing, 2:1575-1582, 2000.

[6] CHIEN TI., LIAO TL., Design of secure digital communication systems using chaotic modulation, cryptography and chaotic synchronization. Chaos, Solitons & Fractals, 24(1):241-255, 2004.

[7] GUOJIE, H., ZHENGJIN, F., RUILING, M., Chosen ciphertext attack on chaos communication based on chaotic synchronization. Circuits and Systems I: Fundamental Theory and Applications, 50(2):275-279, 2003.

[8] ABEL, A., SCHWARZ, W., Chaos communications-principles, schemes, and system analysis. Proceedings of the IEEE, 90(5):691-710, 2002.

[9] MEMON, AQ., Synchronized choas for network security. Computer Communications, 26(6):498-505, 2003.

[10] CHEE, CY., XU, D., Secure digital communication using controlled projective synchronisation of chaos. Chaos, Solitons & Fractals, 23(3):1063-1070, 2005.

[11] KHADRA, A., LIU, XZ., SHEN, X., Impulsively synchronizing chaotic systems with delay and applications to secure communication. Automatica, 41(9):1491-1502, 2005.

[12] ALVAREZ, G., LI, S., Breaking network security based on synchronized chaos. Computer Communications, 27(16):1679-1681, 2004.

[13] BOWONG, S., KAKMENI, FM., SIEWE, MS., Secure communication via parameter modulation in a class of chaotic systems. Communications in Nonlinear Science and Numerical Simulation, 12(3):397-410, 2007.

[14] DRONOV, V., Application of chaotic synchronization and controlling chaos to communications. Doktora tezi, University of Maryland, Faculty of the Graduate School, 2005.

[15] ROBILLIARD, C., HUNTINGTON, EH., FRATER, MR., Digital transmission for improved synchronization of analog chaos generators in communications systems. Chaos: An Interdisciplinary Journal of Nonlinear Science, 17(2): 023130, 2007.

[16] CHANG, WD., Digital secure communication via chaotic systems. Digital Signal Processing, 19(4):693-699, 2009.

[17] ILLING, L., Digital communication using chaos and nonlinear dynamics. Nonlinear Analysis: Theory, Methods & App., 71(12): e2958-e2964, 2009.

[18] WREN, TJ., YANG, TC., Orthogonal chaotic vector shift keying in digital communications. IET Communications, 4(6):739-753, 2010.

[19] STORK, M., Digital chaotic systems examples and application for data transmission. Electrical and Electronics Engineering (ELECO 2009), IEEE:Bursa, 5-8 Nov. 2009.

[20] ALVAREZ, G., LI, S., Some basic cryptographic requirements for chaos-based cryptosystems. International Journal of Bifurcation and Chaos, 16(08):2129-2151, 2006.

[21] JAKIMOSKI, G., KOCAREV, L., Chaos and cryptography: block encryption ciphers based on chaotic maps. IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 48(2):163-169, 2001.

[22] KOCAREV, L., Chaos-based cryptography: a brief overview. Circuits and Systems Magazine, IEEE, 1(3):6-21, 2001.

[23] WONG, KW., YUEN, CH., Embedding compression in chaos-based cryptography. Circuits and Systems II: Express Briefs, IEEE Transactions on, 55(11):1193-1197, 2008.

[24] AMIN, M., FARAGALLAH, OS., ABDEL-LATIF, AA., Chaos-based hash function (CBHF) for cryptographic applications. Chaos, Solitons & Fractals, 42(2):767-772, 2009.

[25] WONG, KW., Image encryption using chaotic maps. Intelligent Computing Based on Chaos, Studies in Computational Intelligence, Springer, 184:333-354, 2009.

[26] MISHKOVSKI, I., KOCAREV, L., Chaos-based public-key cryptography. Chaos-Based Cryptography, Studies in Computational Intelligence, Springer, 354:27-65, 2011.

[27] WANG, Y., WONG, KW., LIAO, X., CHEN, G., A new chaos-based fast image encryption algorithm. Applied soft computing, 11(1):514-522, 2011.

[28] LUI, OY., WONG, KW., CHEN, J., ZHOU, J., Chaos-based joint compression and encryption algorithm for generating variable length ciphertext. Applied Soft Computing, 12(1):125-132, 2012.

[29] KHARE, AA., SHUKLA, PB., SILAKARI, SC., Secure and fast chaos based encryption system using digital logic circuit. International Journal of Computer Network and Information Security (IJCNIS), 6(6):25, 2014.

[30] YANG, H., JIANG, GP., Reference-Modulated DCSK: A Novel Chaotic Communication Scheme. IEEE Transactions on Circuits and Systems II: Express Briefs, 60(4):232-236, 2013.

[31] OKAMOTO, E., A chaos mimo-ofdm scheme for mobile communication with physical-layer security. International Conference on Theory and Application in Nonlinear Dynamics (ICAND 2012), Springer, pp.203-212, 2014.

[32] REN, HP., BAPTISTA, MS., GREBOGI, C., Wireless communication with chaos. Phys. Rev. Lett. 110, 184101, 2013.

[33] LI, N., PAN, W., XIANG, S., LUO, B., YAN, L., ZOU, X., Hybrid chaos-based communication system consisting of three chaotic semiconductor ring lasers. Applied Optics, 52(7):1523-1530, 2013.

[34] LIU, H., KADIR, A., NIU, Y., Chaos-based color image block encryption scheme using S-box. AEU - International Journal of Electronics and Communications, 68(7):676-686, 2014.

[35] AHMAD, M, , ALAM, B., FAROOQ, O., Chaos based mixed keystream generation for voice data encryption. International Journal on Cryptography and Information Security, 2(1):36-45, 2012.

[36] KENFACK, G, TIEDEU, A., Chaos-based encryption of ECG signals: experimental results. Journal of Biomedical Science and Engineering, 7(6), 2014.

[37] MA, X., CHEN, Y., DDoS detection method based on chaos analysis of network traffic entropy. Communications Letters, IEEE, 18(1):114-117, 2013.

[38] CONVERY, S., MILLER, D., "Cisco IPv6 and IPv4 threat comparison and best practice evaluation (v1.0)", http://seanconvery. com/v6-v4-threats.pdf. Erişim Tarihi: 05.11.2014.

[39] FRANKEL, S., GRAVEMAN, R., PEARCE, J., Guidelines for the secure deployment of IPv6. National Institute of Standards and Technology, 2010.

[40] REİSOĞLU, E., Kablosuz Ağlarda Güvenlik. Bahçeşehir Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, İstanbul, Ocak 2008.

[41] MENEZES, A., VAN OORSCHOT, P., VANSTONE, S., Handbook of Applied Cryptography. CRC Press, Boca Raton, 1997.

[42] Bilişim Teknolojileri, LAN kablolama. Kitap, Milli Eğitim Bakanlığı Yayınları, Ankara, 2008.

[43] HALSHALL, F., Data communications, computer networks and OSI. Addison Wesley, 1988.

[44] OKTUĞ, S., BLG433-Bilgisayar haberleşmesi. İstanbul Teknik Üniversitesi, Bilgisayar Mühendisliği Bölümü, Ders Notları, 2006.

[45] TANENBAUM, A., Computer networks. Prentice Hall, Third Eddition, 1996.

[46] ÇÖLKESEN, R., ÖRENCİK, B., Bilgisayar haberleşmesi ve ağ teknolojileri, Papatya Yayınları, İstanbul, 1999.

[47] BAŞKAYA, O., OSI katman modelinde 3. katman güvenlik duvarı uygulaması. Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, Ankara, Mayıs 2010.

[48] Bilişim Güvenliği. Pro-G Bilişim Güvenliği ve Araştırma Ltd, Kitap, 2003.

[49] ÖZKAYNAK, F., ÖZER, AB., YAVUZ, S., Kaos tabanlı yeni bir blok şifreleme algoritması, IV. Ağ Ve Bilgi Güvenliği Sempozyumu, pp.108-112, Ankara, 2011.

[50] PAAR, C., PELZL, J., Understanding cryptography: A textbook for students and practitioners. Springer, 2010.

[51] AMIGO, JM., KOCAREV, L., SZCZAPANSKİ, J., Theory and practice of chaotic cryptography. Physics Letters A, 366:211-216, 2007.

[52] PRENEEL, B., VAN OORSCHOT, PC., On the security of two MAC algorithms. In Advances in Cryptology-EUROCRYPT'96, pp.19-32, Springer Berlin Heidelberg, January 1996.

[53] IETF, The Internet Engineering Task Force, http://www.ietf.org/. Erişim Tarihi: 01.10.2014.

[54] ERKOÇ, K., Kriptoloji ve bilgi güvenliği. Yüksek lisans tezi, SAÜ FBE, 2004.

[55] TEKİN, U., SOĞUKPINAR, İ., IPSec benzetim yazılımı: Tasarım ve gerçekleme. http://emo.org.tr, Erişim Tarihi: 01.11.2014

[56] FRANKEL, S., GRAVEMAN, R., PEARCE, J., ROOKS, M., Guidelines for the secure deployment of IPv6. NIST Special Publication 800-119, 2010.

[57] STAKHANOVA, N., LI, Y., GHORBANI, AA., Classification and discovery of rule misconfigurations in intrusion detection and response devices. In Privacy, Security, Trust and the Management of e-Business, World Congress on pp.29-37, IEEE 2009.

[58] UYAROGLU, Y., Elektrik güç sistemlerinde çatallaşma analizi ve kaotik olayların incelenmesi. Doktora tezi, SAU FBE, 2002.

[59] KARACAY, T., Determinizm ve kaos. II.Mantık, Matematik ve Felsefe Sempozyumu, Assos, 21-24 Eylül 2004.

[60] BROER, H., TAKENS, F., Dynamical systems and chaos. Applied Mathematical Sciences vol. 172, Springer, 2009.

[61] HIRSCH, MW., The dynamical systems approach to differential equations. Bull. Amer. Math. Soc., 11(1):1-64, 1984.

[62] CHEN, W-K., Nonlineer and distributed circuits. CRC Press, 2006.

[63] SCHEINERMAN, ER., Invitation to dynamical systems. Courier Dover Publications, 2012.

[64] TUFILLARO, N., ABBOTT, T., REILLY, J., An experimental approach to nonlinear dynamics and chaos. Redwood City, CA: Addison-Wesley, 1992.

[65] CAMBEL, AB., Applied Chaos Theory A Paradigm for Complexity. Academic Press, Boston, 1993.

[66] YAMAMOTO, Y.. Detection of chaos and fractals from experimental time series. Modern techniques in neuroscience research, Springer, Berlin Heidelberg, pp. 669-687, 1999.

[67] YILMAZ, D., GÜLER, NF., Kaotik zaman serisinin analizi üzerine bir araştırma. Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi, 21(4), 2006.

[68] STROGATZ, SH., Nonlinear dynamics and chaos: with applications to physics, biology and chemistry. Perseus publishing, 2001.

[69] HILBORN, R. C., COPPERSMITH, S., MALLINCKRODT, AJ., Chaos and nonlinear dynamics: an introduction for scientists and engineers. Computers in Physics, 8(6):689-689, 1994.

[70] ABACI, K., KÖSE, E., YALÇIN, MA., UYAROĞLU, Y., Kademe değiştirici transformatörlerin çatallaşma analizi ile dinamik gerilim kararlılığı. 3.Enerji Verimliliği ve Kalitesi Sempozyumu, Kocaeli, pp.52-56, 21-22 Mayıs 2009.

[71] AJJARAPU, V., LEE, B., Bifurcations theory and its application to nonlinear dynamical phenomena in an electrical power system. IEEE Trans. on Power Systems, 17(1):424-431, 1992.

[72] PAMUK, N., Dinamik Sistemlerde Kaotik Zaman Dizilerinin Tespiti. BAÜ Fen Bil. Enst. Dergisi, 15(1):77-91, 2013.

[73] ÖZER, AB., AKIN, E., Tools for detecting chaos. SAÜ Fen Bilimleri Enstitüsü Dergisi, 9(1):60-66, 2005.

[74] http://www.physics.emory.edu/faculty/weeks//research/tseries1.html. Erişim tarihi: 11.11.2014

[75] GIANNAKOPOULOS, K., DELIYANNIS, T., HADJIDEMETRIOU, J., Means for detecting chaos and hyperchaos in nonlinear electronic circuits. DSP 2002. 2002 14th International Conference on. IEEE, 2: 951-954, 2002.

[76] TAGLIAZUCCHI, E., BALENZUELA, P., FRAIMAN, D., CHIALVO, DR., Criticality in large-scale brain fMRI dynamics unveiled by a novel point process analysis. Front. Physiol., 2012.

[77] SAVI, MA., Chaos and order in biomedical rhythms. J. Braz. Soc. Mech. Sci. & Eng., 27(2):157-169, 2005.

[78] LORENZ, EN., Deterministic nonperiodic flow. J. Atmos. Sci., 20(2):130–141, 1963.

[79] KARAKAYİS, M., Kaotik osilatör devrelerinin analizi ve haberleşme sistemlerinde kullanımı. Yüksek lisans tezi, SAÜ FBE, 2005.

[80] CUOMO, KM., OPPENHEIM, AV., Circuit implementation of synchronized chaos with applications to communications. Physical review letters, 71(1): 65-68, 1993.

[81] KOCAREV, L., HALLE, KS., ECKERT, K., CHUA, LO., PARLITZ, U., Experimental Demonstration of Secure Communications via Chaotic Synchronization. International J. of Bifurcation&Chaos,, 2(3):709-713, 1992.

[82] SEKAR, AC., RADHIKA, S., ANAND, K., Secure communication using 512 bit key. Eur. J. Sci. Res, 52(1):61-65, 2011.

[83] GE, ZM., YANG, CH., Symplectic synchronization of different chaotic systems. Chaos, Solitons & Fractals, 40(5):2532-2543, 2009.

[84] YOO, W., JI, D., WON, S., Synchronization of two different non-autonomous chaotic systems using fuzzy disturbance observer. Physics Letters A, 374(11):1354-1361, 2010.

[85] CHEN, S., LÜ, J. Synchronization of an uncertain unified chaotic system via adaptive control. Chaos, Solitons & Fractals, 14(4):643-647, 2002.

[86] WANG, ZL., SHI, XR., Chaotic bursting lag synchronization of Hindmarsh–Rose system via a single controller. Applied Mathematics and Computation, 215(3):1091-1097, 2009.

[87] RYABOV, VB., USIK, PV., VAVRIV, DM., Chaotic masking without synchronization. International Journal of Bifurcation and Chaos, 9(6):1181-1187, 1999.

[88] CHENG, CJ., Robust synchronization of uncertain unified chaotic systems subject to noise and its application to secure communication. Applied Mathematics and Computation, 219(5): 2698-2712, 2012.

[89] YANG, T., CHUA, LO., Secure communication via chaotic parameter modulation. IEEE Trans Circuits Systems I: Fundam. Theory Appl., 43(9):817–819, 1996.

[90] MURAKAMI, H., New communication systems via chaotic synchronizations and modulations. Ieice Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 78(3):285-290, 1995.

[91] FALLAHI, K., LEUNG, H., A chaos secure communication scheme based on multiplication modulation. Communications in Nonlinear Science and Numerical Simulation, 15(2):368-383, 2010.

[92] FILALI, RL., BENREJEB, M., BORNE, P., On observer-based secure communication design using discrete-time hyperchaotic systems. Communications in Nonlinear Science and Numerical Simulation, 19(5):1424-1432, 2014.

[93] CHEN, M., HAN, Z., Controlling and synchronizing chaotic Genesio system via nonlinear feedback control. Chaos, Solitons & Fractals, 17(4):709-716, 2003.

[94] LIU, F., REN, Y., SHAN, X., QIU, Z., A linear feedback synchronization theorem for a class of chaotic systems. Chaos, Solitons & Fractals, 13(4):723-730, 2002.

[95] DELGADO-RESTITUTO, M., ACOSTA, AJ., RODRÍGUEZ-VÁZQUEZ, A., A mixed-signal integrated circuit for FM-DCSK modulation. Solid-State Circuits, IEEE Journal of, 40(7):1460-1471, 2005.

[96] RULKOV, NF., VOLKOVSKII, AR., Generation of broad-band chaos using blocking oscillator. Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions on, 48(6):673-679, 2001.

[97] GALIAS, Z., MAGGIO, GM., Quadrature chaos-shift keying: theory and performance analysis. Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions on, 48(12):1510-1519, 2001.

[98] ÇAVUŞOĞLU, Ü., UYAROĞLU, Y., PEHLİVAN, İ., Sürekli Zamanlı Otonom Kaotik Devre Tasarımı Ve Sinyal Gizleme Uygulaması. Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi, 29(1):79-87, 2014.

[99] EMİROĞLU, S., UYAROĞLU, Y., Kaotik Burke-Shaw çekicisinin aktif kontrol ile senkronizasyonu. NWSA: Engineering Sciences, 6(1):325-331, 2011.

[100] XIANG-JUN, W., A new chaotic communication scheme based on adaptive synchronization. Chaos: An Interdisciplinary Journal of Nonlinear Science, 16(4):043118, 2006.

[101] FEKI, M., An adaptive chaos synchronization scheme applied to secure communication. Chaos, Solitons & Fractals, 18(1):141-148, 2003.

[102] ÇETİNTAŞ, G., ÇELİK, V., Zaman Gecikmeli Kaotik Bir Sistemin Aktif Kontrol İle Senkronizasyonu. URSI-TÜRKİYE'2014 VII. Bilimsel Kongresi, Elazığ, 28-30 Ağustos, 2014.

[103] KURT, E., KASAP, R., Karmaşanın bilimi kaos. Nobel Yayınları, Ankara, Kasım 2011.

[104] KOLUMBAN, G., KENNEDY, MP., CHUA, LO., The role of synchronization in digital communications using chaos. II. Chaotic modulation and chaotic synchronization. Circuits and Systems I: Fundamental Theory and Applications, IEEE Transactions on, 45(11):1129-1140, 1998.

[105] OĞRAŞ, H., TÜRK, M., OĞRAŞ, S., Kaos tabanlı sayısal CSK ve DCSK modülasyon tekniklerinin matlab/simulink ortamında gerçekleştirilmesi, IV. İletişim Teknolojileri Ulusal Sempozyumu, Adana, 2009.

[106] CHOWN, P., Advanced encryption standard (AES) ciphersuites for transport layer security (TLS), RFC3268, IETF, 2002.

[107] OSVIK, DA., BOS, JW., STEFAN, D., CANRIGHT, D., Fast software AES encryption. In Fast Software Encryption, pp.75-93, Springer Berlin Heidelberg, January 2010.

[108] LU, CC., TSENG, SY., Integrated design of AES (Advanced Encryption Standard) encrypter and decrypter. In Application-Specific Systems, Architectures and Processors, 2002. Proceedings. The IEEE International Conference on pp.277-285, IEEE, 2002.

[109] FOROUZAN, BA., Cryptography & network security. McGraw-Hill, Inc., 2007.

[110] AN, HL., CHEN, Y., The function cascade synchronization scheme for discrete-time hyperchaotic systems. Communications in Nonlinear Science and Numerical Simulation, 14(4):1494-1501, 2009.

[111] KOÇ, E., ŞENGÜL, YA., ÖZKAYA, AU., GÖKÇE, B., Klinik Karar Destek Sistemleri Kullanımına Yönelik Bir Araştırma: Acıbadem Hastanesi Örneği, 2012.

[112] ÖZATA, M., ASLAN, Ş., Clinical Decision Support Systems and Model Applications. The Medical Journal of Kocatepe, 5(2)11-17, 2004.

[113] ER, O., TEMURTAŞ, F., A study on chronic obstructive pulmonary disease diagnosis using multilayer neural networks. Journal of Medical Systems, 32(5):429-432, 2008.

[114] ER, O., SERTKAYA, C., TEMURTAŞ, F., TANRIKULU, AC., A comparative study on chronic obstructive pulmonary and pneumonia diseases diagnosis using neural networks and artificial ımmune system. Journal of Medical Systems, 33(6):485-492, 2009.

[115] ER, O., TEMURTAŞ, F., TANRIKULU, AC., Tuberculosis disease diagnosis using artificial neural networks. Journal of Medical Systems, 34(3):299-302, 2010.

[116] http://en.wikipedia.org/wiki/Bifurcation_diagram. Erişim Tarihi: 01.11.2014.

[117] SHANNON, CE. Communication theory of secrecy systems. Bell Syst. Tech. J., vol. 28:656–715, 1949.

ÖZGEÇMİŞ

Ahmet Sertol Köksal, 1976 yılında Ordu'da doğdu. İlk, orta ve lise eğitimini Ordu'da tamamladı. 1994 yılında başladığı lisans eğitimini Karadeniz Teknik Üniversitesi, Elektrik Elektronik Mühendisliği bölümünde, 1998 yılında tamamladı. 1998-2002 yılları arasında özel sektörde mühendis olarak çalıştı. 2002-2012 yılları arasında Sakarya Üniversitesi Bilgi İşlem biriminde çalışan Ahmet Sertol, 2012 yılında Bozok Üniversitesi Bilgisayar Mühendisliği bölümünde Öğretim Görevlisi olarak çalışmaya başladı. Halen bu pozisyonda çalışmaktadır.