T.C.
KASTAMONU ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BİR DİRENÇ- İKİ BOBİN - İKİ DİYOTLU KAOTİK DEVRE ARACILIĞIYLA GÜVENLİ İMGE İLETİŞİMİNİN ARAŞTIRILMASI

Khaled Mohamed EL HADAD

Danışman	**Doç. Dr.Aybaba HANÇERLİOĞULLARI**
II. Danışman	**Prof. Dr Erol KURT**
Jüri Üyesi	**Prof. Dr. Fatma KANDEMİRLİ**
Jüri Üyesi	**Dr. Öğr.Üyesi Hüseyin DEMİREL**
Jüri Üyesi	**Dr. Öğr. Üyesi Seçil KARATAY**
Jüri Üyesi	**Dr. Öğr. Üyesi Javad RAHEBI**

DOKTORA TEZİ
MALZEME BİLİMİ VE MÜHENDİSLİĞİ ANABİLİM DALI

KASTAMONU – 2018

TEZ ONAYI

Khaled Mohamed EL HADAD tarafından hazırlanan "**Bir Direnç- İki Bobin-İki Diyotlu Kaotik Devre Aracılığıyla Güvenli İmge İletişiminin Araştırılması**" adlı tez çalışması aşağıdaki jüri üyeleri önünde savunulmuş ve **oy birliği** ile Kastamonu Üniversitesi, Fen Bilimleri Enstitüsü **Malzeme Bilimi ve Mühendisliği Ana Bilim Dalı**'nda **DOKTORA TEZİ** olarak kabul edilmiştir.

Danışman	Doç.Dr. Aybaba HANÇERLİOĞULLARI Kastamonu Üniversitesi	.....
Jüri Üyesi	Prof. Dr. Fatma KANDEMİRLİ Kastamonu Üniversitesi	.....
Jüri Üyesi	Dr. Öğr. Üyesi Hüseyin DEMİREL Karabük Üniversitesi	.....
Jüri Üyesi	Dr.Öğr. Üyesi Seçil KARATAY Kastamonu Üniversitesi	.....
Jüri Üyesi	Dr. Öğr. Üyesi Javad RAHEBI Türk Hava Kurumu Üniversitesi	.....

16 /07/2018

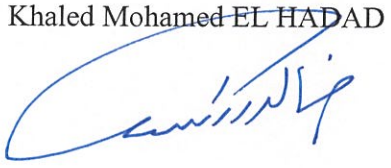
Enstitü Müdür V.	Doç. Dr. Mehmet Altan KURNAZ	.....

TAAHHÜTNAME

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada bana ait olmayan her türlü ifade ve bilginin kaynağına eksiksiz atıf yapıldığını bildirir ve taahhüt ederim.

İmza

Khaled Mohamed EL HADAD



ÖZET

Doktora Tezi

BİR DİRENÇ- İKİ BOBİN - İKİ DİYOTLU KAOTİK DEVRE ARACILIĞIYLA GÜVENLİ İMGE İLETİŞİMİNİN ARAŞTIRILMASI

Khaled Mohamed EL HADAD

Kastamonu Üniversitesi
Fen Bilimleri Enstitüsü
Malzeme Bilimi ve Mühendisliği Ana Bilim Dalı

Danışman: Doç. Dr. Aybaba HANÇERLİOĞULLARI
II. Danışman: Prof. Dr. Erol KURT

Bu tezde, kaotik bir devre olarak bir direnç - iki bobin ve iki diyot içeren R2L2D devresi kullanılarak önce eşzamanlılık çalışması yapılmış, bu devrenin benzeri ile kaotik eşzamanlı duruma getirilmiştir. Sonra bir imgenin sayısal-anolog dönüştürücü kullanılarak bu kaotik devre üzerine bir toplayıcı devre ile modüle edilip analog devreden başka bir alıcı analog devreye güvenli olarak imgenin gönderilip şifresinin çözülerek gizlenen imgenin eldesi sağlanmıştır. Metot olarak eşzamanlılıkta OGY (Ott-Grebogi-Yorke) metodu ve güvenli haberleşme kısmında ise hakim-esir metodu kullanılmıştır. Literatürde burada tasarlanıp gerçekleştirildiği şekilde ilgili kaotik devreyi kullanarak imge gizleyip eşzamanlı olarak bunu çözebilen analog bir güvenli haberleşme sistemi yoktur. Hem teorik hem de deneysel açıdan gerçek zamanlı güvenli iletişimin analog devreler üzerinden sağlanması internet veya diğer bilgisayar bazlı uygulamalardan daha üstündür, çünkü internet ve bilgisayar ortamındaki veriler kopyalanmaya açıkken analog eşzamanlı devrelerde bu olasılık yoktur. Deneylerde anolog/sayısal ve sayısal/analog dönüştürücüler görüntünün gri seviyelerinin okunması ve iletimi aracılığıyla kullanıldığından işlem sonunda ilgili imgeler imha edilebilirler. Geleneksel teknikler, bilgisayar ortamında depolanan ve işlenen verileri kullanmaktadır ve bu da günümüzün gelişmiş internet ağı ortamında güvenlik sorunlarına neden olabilirken önerilen eşzamanlı kaotik güvenli imge haberleşmesi tekniği bu alandaki önemli bir açığı dolduracaktır.

Anahtar kelimeler: Güvenli İmge Sistemi, R2L2D Kaotik Devre, İmge Şifreleme ve Çözme, Eşzamanlılık, Hakim-Esir Kaotik Devreler.

2018, 76 Sayfa
Bilim Kodu: 91

ABSTRACT

Ph.D. Thesis

EXPLORATION OF SECURE IMAGE COMMUNICATION VIA A RESISTOR-TWO INDUCTORS-TWO DIODES CHAOTIC CIRCUIT

Khaled Mohamed EL HADAD

Kastamonu University
Institute of Sciences
Department of Material Science and Engineering

Supervisor: Assoc. Prof. Dr. Aybaba HANÇERLİOĞULLARI
Co-Supervisor: Prof. Dr. Erol KURT

In this thesis, first a synchronization study has been performed by using a R2L2D circuit including one resistor 2 inductors and 2 diodes and that circuit has been synchronized with the same other chaotic circuit. Then, the images are modulated on a chaotic signal by a signal from an adder circuit via a digital-anolog converter and the summed chaotic and gray-level signal is sent to the receiver circuit for the encyrption of the summed signal in a secure way. As the methods, OGY (Ott-Grebogi-Yorke) and master-slave methods are used for synchronization and secure communication, respectively. In the literature, there exists no secure image communication system by using the present chaotic circuit, encryption and decrytion the images, synchronously. That providing the secure communication theroretically and experimentally by real-time analog circuits is superior over the internet and other computer-based applications, because the data in internet and computer media are open to be copied, there is no such possibility in analog circuits. In the experiments, analog/digital and digital/analog converters are used for the read of gray levels of images and the communication issues, these images can be destroyed just after the transfer at the end of process. The conventional techniques operate with the stored and processed data in the computer media and while that procedure can be a security problem in today's developed internet web media, the proposed synchronized secure image communication technique will fill the gap in that field.

Keywords: Secure Image System, R2L2D Choatic Circuit, Image Encryption and Decryption, Synchronization, Master–Slave Chaotic's Circuits.

2018, 76 pages
Science Code: 91

TEŞEKKÜR

Tez çalışmam boyunca her türlü desteği ve imkânı sağlayarak değerli bilgilerinden yararlandığım, danışman hocam Doç. Dr. Aybaba HANÇERLİOĞULLARI'na, Tezimin içeriğindeki özel ölçümlerin düzenlemesi ve devreler tasarımında bana sürekli desdeklerini ve emeğini esirgemeyen eş danışmanım Prof.Dr.Erol KURT hocama,Tez İzleme Komitesi üyeleri Dr.Öğr.Üyesi Seçil KARATAY ve Dr.Öğr.Üyesi Javad RAHABİ ve Kastamonu Üniversitesi Malzeme Bilimi ve Mühendisliği Bölümü öğretim üyelerine, Labratuvar imkanlarını bana sağlayan ,Gazi Üniversitesi Teknoloji Fakültesi Elektrik-Elektronik Bölümü öğretim üyelerine en kalbı duygularımla teşekkür ederim. Ayrıca Türkiye'de bulunduğum süre içinde eğitim ve araştırma faaliyeleri süresince maddi ve manevi desteğini esirgemeyen Libya Hükümeti'ne şükranlarımı sunarım. Bu çalışmayı benim için hayati önem arz eden aileme ithaf ediyorum.

Khaled Mohamed EL HADAD
Kastamonu, Temmuz,2018

İÇİNDEKİLER

Sayfa

ÖZET iv
ABSTRACT v
TEŞEKKÜR vi
İÇİNDEKİLER vii
ŞEKİLLER DİZİNİ xiii
TABLOLAR DİZİNİ xii
GRAFİKLER DİZİNİ xi
FOTOĞRAFLAR DİZİNİ ix
SİMGELER VE KISALTMALAR LİSTESİ x
1. GİRİŞ 1
1.1. Problemin Açıklanması 4
1.2. Literatürdeki Çalışmaların Değerlendirilmesi 6
1.3. Şifrelemede Kaotik Devreler 11
1.4. Kaotik Yöntemin Önemi 12
2. KURAMSAL BILGI 15
2.1. Kaotik Maskeleme 15
2.2. Kaotik Kaydirmali Anahtarlama (CSK) 16
2.3. Kaotik Modülasyon 17
2.4. Kaotik şifreleme sistem 18
2.4.1. Kaos Temelli Şifreleme Sistem Türleri 20
2.4.2. Kaotik İmge Şifreleme Sistemleri Yapısı 20
2.4.3. Kaotik sistemler ve şifreleme sistem arasindaki ilişki 21
2.5. Şifreleme Algoritması 24
2.5.1. Geleneksel Şifrelemesi 24
2.5.2. Açık Anahtar Şifreleme 25
2.6. Şifreleme Yöntemleri 26
2.6.1. Kaotik şifreleme şemaları için parametreler 27
2.6.2. İmge Şifreleme/Şifre çözme Tekniği 28
2.6.3. Şifreleme/Şifre çözme Tekniği 29
2.7. R2D2L Kaotik Devrede Eşzamanlılık ve Güvenli İletişim 29

2.7.1. R2L2D devresinin eşzamanlılığı 31
2.7.2. R2L2D devresinin güvenli iletişim sistemi 34
3. MALZEME VE ÖLÇME YÖNTEMLERİ..... 37
3.1. Malzemelerinin özellikleri..... 37
3.2. Anolog ve imge sinyalinin ölçümleri 42
3.2.1. Anolog sinyalinin ölçülmesi 42
3.2.2. İmge sinyalinin iyileştirilmesi..... 44
3.2.3. R2L2D Devresinde Kaos Devresi ile Giriş/Çıkış Sinyalinin Ölçülmesi .. 45
3.2.4. Dönüştürülen ve Gönderilen İmge Gri Şifreleme Aşamaları..... 47
3.2.5. Şifre çözme aşamaları 50
4. BULGULAR VE DEĞERLENDİRMELER 53
4.1. Imge Şifreleme Çözümleme Analizi..... 53
4.2. Histogram Analizi 57
4.3. Piksel Korelasyonu 58
4.4.Bilgi Entropisi Analizi 66
4.5. Hata Ölçümü 68
5. SONUÇ VE ÖNERİLER..... 69
KAYNAKLAR 71
ÖZGEÇMİŞ 76

ŞEKİLLER DİZİNİ

Sayfa

Şekil 1.1. İletişim sistemlerinin temel elemanları 13
Şekil 1.2. Chau kaotik RCD devresi 13
Şekil 2.1. Analog kaotik maskeleme devresi 15
Şekil 2.2. Analog kaotik anahtarlama şeması 16
Şekil 2.3. (a) Kaotik parametre modülasyonu 17
Şekil 2.3. (b) Kaotik özerk olmayan modülasyon 18
Şekil 2.4. Kaotik şifreleme sistem şeması 19
Şekil 2.5. Standart yapılı kaos temelli imge şifreleme sistemleri 21
Şekil 2.6. Geleneksel şifreleme 24
Şekil 2.7. Açık Anahtar Şifreleme 25
Şekil 2.8. Şifreleme ve şifre çözüm aşamaları 28
Şekil 2.9. R2L2D devresi 29
Şekil 2.10. Özerk olmayan kaotik blok diyagramı 33
Şekil 2.11. Güvenli imge sistemi 35
Şekil 2.12. Güvenli iletişim sistemi şeması 36
Şekil 3.1. Mikrokontrol PIC18F4550 programlama 37
Şekil 3.2. İkili ağırlıklı R-2R dirençlerden oluşmuş merdivenler 38
Şekil 3.3. 8 bitlik bir D/A dönüştürücü simülasyon şeması 40
Şekil 3.4. 32x32 matrisinin 1x1024 vektörüne dönüşümü 48
Şekil 3.5. 32x32 matrisinin 1x1024 vektörüne dönüşümü 49
Şekil 3.6. Imge 1x1024 voltaj vektörünün 32x32 matrisine dönüştürülmesi 50
Şekil 4.1. (a) Bir kameramanın asıldan şifre ve şifre çözümüne ulaşması 54
Şekil 4.1. (b) Bir bayanın (Lena) yüz imagenin asıldan şifre ve şifre çözümüne ulaşması 54
Şekil 4.1. (c) Bir adamın fotoğraf portesinin asıldan şifre ve şifre çözümüne ulaşması 54
Şekil 4.1. (d) Bir köpeğin asıldan şifre ve şifre çözümüne ulaşması 55
Şekil 4.1. (e) Birördeğin asıldan şifre ve şifre çözümüne ulaşması 55
Şekil 4.1. (f) Monalisa portesinin asıldan şifre ve şifre çözümüne ulaşması 55
Şekil 4.2. (a,b) Bir kameramanın ait asıl-şifre / asıl-şifreçözümlerinin histogramı 59
Şekil 4.2. (c,d) Bayan Lina ya ait asıl-şifre / asıl-şifreçözümlerinin histogramı 59
Şekil 4.2. (e,f) Bir adama ait asıl-şifre / asıl-şifreçözümlerinin histogramı 60
Şekil 4.2. (g,h) Bir köpeye ait asıl-şifre / asıl-şifreçözümlerinin histogramı 60
Şekil 4.2. (i,j) Bir ördeğe ait asıl-şifre / asıl-şifreçözümlerinin histogramı 61
Şekil 4.2. (k,l) Bir ördeğe ait asıl-şifre / asıl-şifreçözümlerinin histogramı 61
Şekil 4.3. (a,b) Açık gri tonlamalı imge kameraman korelasyon diyagramları .. 63
Şekil 4.3. (c,d) Açık gri tonlamalı imge Lena'nın korelasyon diyagramları 64
Şekil 4.3. (e,f) Açık gri tonlamalı imge fotoğrafçı korelasyon diyagramları 64
Şekil 4.3. (g,h) Açık gri tonlamalı imge köpeğin korelasyon diyagramları 65
Şekil 4.3. (i,j) açık gri tonlamalı imge ördeğin korelasyon diyagramları 66
Şekil 4.3. (k,l) açık gri tonlamalı imge Mona Lisa'nın ilgileşim diyagramları .. 66

TABLOLAR DİZİNİ

Sayfa

Tablo 2.1. Kaos temelli şifreleme sistem türleri 22
Tablo 2.2. Kaotik sistemin özelliklerinin karşılaştrılması 23
Tablo 2.3. Anahtar şıfer Alanı..... 27
Tablo 4.1. Verilerin şifre çözme imgesinde hata yüzdesi 56
Tablo 4.2. Çeşitli imgelere ait korelasyon katsayısıların karşılaştırılması 62
Tablo 4.3. Örneklere ait Entropi bilgisi ve gerçek imgelerin bit değerlerinin karşılaştırılması..... 68
Tablo 4.4. Test imgelerine ilişkin hata ölçümleri 68

GRAFİKLER DİZİNİ

Sayfa

Grafik 3.1. D/A dönüştürücü için genliğe karşı gri değerleri…..... 41

FOTOĞRAFLAR DİZİNİ

Sayfa

Fotoğraf 2.1. R2D2L devre sistemi 36
Fotoğraf 3.1. DAC R-2R anolog/sayısal çevirici basamak devresi 39
Fotoğraf 3.2. Donanım yükleyici programlama -pic18f4550 41
Fotoğraf 3.3. Hex dosyasını PIC -18 F4550 için kullanılan USB yazılımı..... 42
Fotoğraf 3.4. Arduino Uno -6 giriş kapısı. 44
Fotoğraf 3.5. İmge sinyalinin iyileştrilmesi 44
Fotoğraf 3.6. R2L2D devresinde kaos sinyalinin ölçüm düzeneği 46
Fotoğraf 3.7. Master devresinde sinüs sinyalinin uygulanması 46
Fotoğraf 3.8. Osilaskopta çıkış kaos sinyalini elde edilişi 47
Fotoğraf 3.9. Toplayıcı ve D/A dönüştürücüsü verici devresi 49
Fotoğraf 3.10. Çıkarma devresinden analog sinyalinin ölçülmesi 51

SİMGELER VE KISALTMALAR LİSTESİ

3DES	Üçlü Veri Şifreleme Standardı
ADC	Analog Sayısal Dönüştürücü
AES	İleri Şifreleme Standardı
ARDUINO UNO	ATmega328 dayalı Mikro Denetim Birimi Kartı
BWR	İkili Ağırlıklı Rezistans
DAC	Sayısal Analog Dönüştürücü
DES	Veri Şifreleme Standardı
FPGA	Alanda programlanabilir kapı dizisi
GHS	Genel Hamiltonian sistemleri
GPS	Genel İzdüşümsel Eşzamanlılık syon
IDEA	Uluslararası Veri Şifreleme Algoritması
LFSR	Doğrusal Geri besleme Kaydırma Yazmacı
LSB	En Az Anlamlı Bit
MSB	En Anlamlı Bit
NCD	Özerk olmayan Chua diyotu
NSA	Ulusal Güvenlik Teşkilatı
OGY	Ott-Grebogi-Yorke
PRNG	Sözde Rastgele Sayı Üreteci
R2L2D	Bir Direnç (R), 2 Bobin (L) ve 2 Diyot (D) içeren Elektrikli devre
RLC	Bir Direnç (R), bir Bobin (L) ve bir Kapasitör (C) içeren Elektrikli devre
TRNG	Gerçek Rastgele Sayı Üreteçleri

1. GİRİŞ

Araştırmacılar, bilgi güvenliği ve bilgi depolama bakımından özellikle iletişim alanında anolog/sayısal dönüşümüne ait sayısal sisteme geçerken, yeni matematiksel algoritma ve ileri düzeyde elektronik devreler yapılarına ihtiyaç duymuştur. Bilgisayar donanım ve yazılım kullanarak veri ağlarında ve elektronik sistemlerin veri iletimi, doğrusal olmayan sistemler yardımıyla gerçekleştiğinden bu alanda yeni çalışmalara ve yoğun bir matematiksel işlemlere başvurulmuştur. Böylelikle bu alanda, matematiksel olarak, çok katlı diferansiyel denklemler ve doğrusal olmayan sistemlerin anlaşılması yönünde eşzamanlı bir kaotik devre çalışmaları ön plana gelmiştir (Kasap ve Kurt, 1998; Kiers, Schmidt ve Sprott, 2004; E Kurt, Acar ve Kasap, 2000; Murali, Lakshmanan ve Chua, 1994).

Kaotik yapı, başlangıç koşullarına bağlılık gösteren belirsiz bir sistemdeki uzun vadeli bir davranıştır (Strogatz, 1994). Özellikle çoğu elektronik devrelerde, Chua'nun geliştirdiği model doğrusal olmayan diyot (NCD) devre sistemleri hem senkorize olmada zorlukları hemde kaotik durumlara sebep olduğundan uygulmalarda zorluklara sebep olmaktadır (Murali et al., 1994). Chua'nun modeli, doğrusal olmayan dirençler ve diyotlarının karmaşıklığını arttıran,RDL(Direnç-Diyot-Bobin) seri halde birleştirildiği zaman, kaos olası hale gelir. Bunlara ek olarak, girişler için çekim noktalarını parametreler olarak nitelendiren değişmezleri kullanarak (Hanias, Avgerinos, ve Tombras, 2009) ,RLD devrelerini kontrol ederek, kaotik zaman serisinin tek kademeli ve çok kademeli tahminlerini elde etmek mümkün hale getirilir.

Kaosa dayalı şifreleme, internet iletişimi, aktarım, tıbbi görüntüleme, tıp ve askeri İletişim gibi farklı alanlarda pek çok uygulamaya sahiptir. Bu alandaki gelişme hala devam etmektedir. Geleneksel olarak, kaotik şifreleme sistemlerde şifreleme "Gerçek Rastgele Üreteç (TRG)" olarak bilinen kaotik devre anahtarlama ile üretilen rastgele sayıların oluşturulması ile yapılmaktadır. Aynı zamanda, sözde "Rastgele Sayı Üreteçler (RNG)" ile yapılmaktadır.

Bir diğer yandan, çoğu sözde RNG çeşitli nedenlerle şifrelemegrafi için uygun değildir. İlk olarak, sözde RNG ürünleri üzerinde yapılacak özelleştirilmiş istatistiksel testler ürünün tam olarak rastgele olmadığını kanıtlamıştır. Çıkan sayılar istatistiksel testlerde görüldükleri gibi değildir. Bunlar tersine mühendislik ile belirlenebilmektedir.

İkinci olarak, sözde RNG üreteci için algoritma belirlendiği zaman üretilecek bütün rastgele sayılar tahmin edilebilir. Bu dezavantaj, bir çekim noktasının şifreleme mesajlarını okumasına olanak verir. Aksi halde, kaotik bir sayı üreteci (doğru) ile bu mümkün olmayacaktır, bu sebeple, Chua devreleri bu şifreleme analizi türüne direnç göstermektedir.

Son zamanlarda elektronik sistemlerin kolay kontrol ve uygulanabilir olması için sürülmüş olan yeni kaotik devre, bir direnç, iki bobin ve iki ters bağlı diyottan (R2L2D) oluşmaktadır. Eşzamanlı bir kaotik devreye dayalı olarak yeni güvenli bir imge iletişimi sistemi tasarlanmış ve uygulanmıştır. Eksiksiz bir biçimde, en basit devreler süreci ikiye katlayan kaosa neden olan, direnç R, bobin L ve diyot D içermektedir (Linsay, 1981). Daha sonra, bu analog araç bir analog/sayısal dönüştürücü yoluyla bir bilgisayara iletilir ve saklı bir imge elde edilir (Baptista, 1998; Belkhouche ve Qidwai, 2003).

Bu çalışmada, R2L2D devresinde, yeni devre geniş bir besleme genliği ve frekans rejimleri için keşfedilmiştir. Bu da yukarı/aşağı süpürme etkisinin periyodik ve kaotik rejimler açısından dinamiklerin tespit edilmesini kontrol ettiğini kanıtlamaktadır (Erol ve Bingöl, 2016). Bu tekniğin diğer güvenli haberleşme yöntemlerine göre üstünlüğü, gerçek zamanlı olduğu için sayısal verilerin herhangi bir kayıtlı kopyasına, alıcıya imge olarak göndermek için bile ihtiyaç duymamasıdır. Kaotik eşzamanlılı, güvenli iletişim açısından araştırma alanı olarak son zamanlarda daha fazla ilgi görmektedir. Bazı kaotik eşzamanlılık ile ilgili faktörler burada ele alınmaktadır (Feki, 2003).

Kaotik sistemler arasında eşzamanlılık güvenli iletişim yeni bulunan bir iletişim güvenliği yoluydu. Bu “donanım anahtarı” hızlı bir şekilde vuku bulan iletişimin

güvenliğini sağlar. Bu eşzamanlılık türü ilk olarak 1990 yılında gözlemlenmiş ve dosyalanmıştır (Pecora ve Carroll, 1990). Bilim adamları ve mühendisler eşsiz parametrelerinden dolayı iletişim güvenliğinin oluşturulmasına yardım edebileceğini hissetmişlerdir.

Daha sonra, tüm dünyadan araştırmacılar, mühendisler ve uzmanlar bu kaotik donanım anahtarı türünün faydalı olduğunu kabul etmiştir. Özellikle yakın zamanlarda iletişim güvenlik sistemlerinde, üç analog kaotik şifreleme tekniği kullanılmıştır. İlk olarak, sürekli kaotik sinyale dayanan kaotik maskeleme girdi analog sinyaline eklenir. İkinci olarak, girdi analog sinyaline dayanan kaotik modülasyon kaotik taşıyıcı tarafından değiştirilir. Üçüncü olarak, girdi sayısal sinyaline dayanan kaotik kaydırmalı anahtarlama (CSK) olarak da bilinen kaotik Aktarma Anahtarı, iki farklı çekim noktası arasında anahtarlayarak şifrelenir. Dahası, kaotik kaydırmalı anahtarlama tekniği, M-senkronize faz kaotik sistemlere (M-CPSK) dayalı eszamanlilik temelli kaotik faz kaydırmalı anahtarlama (CPSK) için geliştirilmiştir. Birinci ve ikinci tekniklerin prensibi, şifrelenmiş bir analog sinyalidir (Yang, 2004).

İletişim alanında çok yönlü şifreleme ve düşük maliyetli sistemleri güvenlik sistemleri bilgisayar donanım için kullanılmıştır. Buda, şifreleme kullanan iletişim güvenliği bir verici yardımıyla verileri anlaşılamayan bir formata dönüştürerek başarılı olmaktadır. Verici, iletişim/aktarım işlemleri esnasında verileri görünmez ve oldukça okunmaz bir hale getirir. Bu şifreleme herhangi bir emniyetsiz bağlantı kullanılarak aktarılır. Alıcı bölümünde, şifreli veriler tekrardan anlaşılabilir formata dönüştürülür ve dolayısıyla bilgiler güvenli bir şekilde aktarılır.

Verilerin gizlenmesi için, konumsal bölge, frekans bölgesi ve sıkıştırılmış veri bölgesi gibi çeşitli yöntemler bulunmaktadır. Bunlar arasında, doğrudan yöntemler bütün imge bazlı verileri kullanmaları bakımından bazı avantajları sahiptirler ve gayet kesin kayıt sağlamaktadırlar (Shelke, Dongre, ve Soni, 2014). Bir dezavantajı da vardır ve bu da hafıza gereksinimleridir ve buna ek olarak, gizli başlatmanın ve tekniklerin uygulanması kolay olmayabilir (Celik ve Kurt, 2016). Konumsal bölge, frekans bölgesi ve sıkıştırılmış veri bölgesi gibi şifrelenmiş veriler için çeşitli

yöntemler bulunmaktadır. Veri şifreleme standardı (DES), uluslararası veri şifreleme algoritması (IDEA),ileri şifreleme standardı (AES) ve doğrusal geri besleme kaydırma yazmacı (LFSR) en yaygın şekilde kullanılan analog algoritmalardan biridir (Daemen ve Rijmen, 2013, Schneier, 2007). Bunlar, şifresiz belgeyi blok şifresi veya veri akışı olarak gören yüksek bilişimsel güvenliğe sahiptir.

1.1. Problemin Açıklanması

İmge şifreleme gizliliğinden dolayı bilgi güvenliğinin temeli olan, bilgi güvenliği alanında özel bir yeri vardır. Mesajı alması istenen kişinin dışında herhangi başka biri tarafından okunamayan mesajları paylaşmak için tarih boyunca şifreleme kullanılmıştır. İmge şifreleme, imge bilgi verilerini okunabilir bir imge verisinden, okuyucuya bilgi vermeyen yararsız bir veri gibi tamamen okunamaz bir imge verisine dönüştürmektir. Araştırmacılar aynı zamanda verileri veya başka bir imgeyi imgenin içerisine yerleştiren teknikler de geliştirmiştir. Görsel şifreleme için pek çok teknik geliştirilmiştir. Aslında, bunlar imge steganografisinde (metin içi şifreleme) daha önce kullanılmıştır. Fakat imge pikselleri arasındaki büyük veri hacminden ve güçlü ilintiden dolayı hızları yavaş olduğu için gerçek zamanlı olarak görüntü ve video şifrelemesi için uygun değillerdir. Bunlara ek olarak, ticari yazılımla uygulandığı zaman görüntü video şifreleme için bu algoritmaların uygulanması çok karmaşıktır. Bir diğer yandan, pek çok araştırma çalışması bunların güvenliksiz olduğunu göstermiştir.

Bunların arasında, doğrudan yöntemler, bütün imge verilerini kullanmaları ve böylece gayet kesin kayıt sağlamaları bakımından bazı avantajlara sahiptir.Fakat bu yöntemlerin dezavantajı gizli bir başlatmaya ihtiyaç duymalarıdır. Şifrelenmiş imge için çeşitli sistemler mevcuttur.Fakat bunların bazı eksiklikleri vardır.Örneğin, ya mesajı şifrelemezler ya da şifrelemegrafiyi gerçekleştirmek için çok zayıf bir algoritma kullanırlar. Buda hacker gibi bilgi çalma hırsızların önünü açar.

Bu çalışmada, gerçek zamanlı olarak, kaotik devreye dayanarak videyo ve imge sistemlerin doğrudan şifrelenmesi için güvenli bir şifreleme sistemi geliştirdik. Kaotik devre sadece dirençler,bobinler, kondansatörler,diyotlar ve opamplar ile

oluşturulabilir Özel bir kaotik devre R2D2L'ye dayanarak güvenli bir imge iletişimi sistemini tasarlamak ve uygulamak bu tezin kapsamıdır.

Tez kapsamında, kaotik devre gürültü üreticisine dayanan bir imge şifreleme sistemi sunmaktayız. Bu imge, sayısal gri değerden analog değere dönüştürülür. Dolayısıyla, analog değerler ana kaotik devretarafından üretilen kaotik sinyal $N(t)$ ile maskelenir. Şifrelenen imge daha sonra güvenliksiz kanal yoluyla aktarılır. Alıcı cihazda, ters işlem kullanılarak kaos ilaveli sinyalden kaldırılması için, özdeş kaotik bir gürültü $N\ (t)$ oluşturulmalıdır. Daha sonra, gri düzeyli değerleri imge olarak okumak için sinyal geri verilebilir ve geri alınabilir.Böylece şifre çözme imgesi elde edilir. Bu yöntem, uygulanması nispeten kolay olduğu için tercih edilmiştir

Bu tezde, geliştirilmiş bir güvenliği olan bir kaotik devreye (Gerçek Rastgele Üreteçler) dayanan güvenli bir imge iletişimi sistemini sunulmaktadır.Önerilen sistem, donanım açısından kolaylıklar ve yazılım ile de daha esnek olarak uygulanabilir. Kullanılan teknik karmaşık değildir ve uygundur. Kaotik devre, düşük maliyetle kolaylıkla uygulanabilir. Bu da makul, hızlı ve düşük maliyetli uygulamaya yol açar. Kaotik durum değişkenlerinin başlangıç koşulları güvenli anahtar parçalarını temsil ederse, bir şifreleme sistemi açısından, başlangıç koşullarına karşı bir duyarlılık olabildiğince büyük olmalıdır. Bu sebeple, rastgele sayı üreteci için R2L2D kaotik devresini tercih edilmişitr. Kaotik faz altında bu devrelerden çoğaltılabilecek veriler mevcut değildir ve ürünler tamamen öngörülemez hale gelmektedir. Bu durum, güvenli ve dayanıklı bir imge iletişiminin "Gerçek zamanlı" olarak yapılabileceğini garanti etmektedir. Ortak şifreleme sistem saldırılarına karşı sisteminizi pek çok analiz ile incelenmiştir.

Bu tez beş bölümde incelenmiştir. Birinci bölümde probem çözümü ve tezin amacı açıklanmıştır. Bununla birlikte, literatür taraması ayrıntılı olarak gösterilmiştir. Geliştirilen (R2D2L) kaotik devreler üzerine yoğunlaşan çalışmalardan önemli noktaları ortaya koyarak, bu devrelerin çeşitlerini ve avantajlarını açıklanmıştır. Bununla birlikte, tez kapasamında, şifreleme ve şifre çözme imgesi için maskeli kaotik sinyal(MSK), eszamanlilik kaotik sinyali ve kaotik kaydırmalı anahtarlama sistemleri detaylı açıklanmıştır.

İkinci bölümde, R2L2D kaotik devrelerdeki eşzamanlılık uyumlu açıklayan temel matematiksel denklemler için temel kuralları ve güvenli iletişim tasarımları açıklanmıştır.

Üçüncü bölümde, tez için gerekli olan malzeme ve metotlar , şifreleme bilimi ve şifre çözme tekniği şemaları ayrıntıları ile ele alınmıştır. Şifreleme ve şifre çözme imgesi için önemli araçlar ve fazlar, Şekiler ve fotoğraflar ile birlikte açıklanmıştır.

Dördüncü bölümde, deneysel ve analiz teknikleri başlangıç koşuları ve diğer parametreler image fotoğraflarla birlikte gösterilmiştir. Ayrıca, güvenli imge iletişimi başka donanımlar ile birlikte lisanlı,MatLab,Proteus-8, Prpton Ide yazılım programı kullanılmıştır. İmge üzerinde pikselerin nasıl dağıtıldığını göstermek için şifreleme histogramlarını hesaplayarak istatistiksel analizleri yapılmıştır. Ayrıca, bu bölümde güvenlik açığı için önerilen şifreleme yapısının analiz işlemleri yapılmıştır.

Beşinci bölümde sonuç ve önerleri değerlendirilmiştir.

1.2. Literatürdeki Çalışmaların Değerlendirilmesi

Lorenz (1963), tarafından yapılan çalışmada, kaos veya dayanıklı bir fiziksel olayı göstermek için devrelerin matematiksel denklemlerini ve eksik yönlerini ortaya koymuştur.

Matsumoto (1984), tarafından yapılan çalışmada kaotik dinamik sistemlerin, çekim noktalarının varlığını şekilsel olarak bir dizi matematiksel denklemlerle ispatlamıştır.

Ayrom ve Zhong (1986), tarafından yapılan çalışmalarda, Chua nın çalışmalarını deneysel olarak gözlemlemişler ve bu alanda teoriler geliştirmişlerdir.

Matthews (1989), tarafından yapılan çalışmada ilk kaotik şifreleme algoritması geliştirilmiştir. Daha sonra, kaos temelli şifrelemeye dayalı araştırmalar yapılmıştır. Lojistik denklemde tamsayılı tekrarlamalar için, bir metin iletisinin her bir karakterini şifrelemeye dayalı basit tek boyutlu lojistik denklemler geliştirmişlerdir.

Carroll ve Pecora (1991), tarafından yapılan çalışmada belirli şartlar altında farklı başlangıç koşullarından başlayan senkronize iki kaotik sisteme sahip olmanın olası olduğunu göstermiştir.

Kocarev, Halle, Eckert, Chua ve Parlitz (1992), tarafından yapılan çalışmada, doğrusal olmayan ve iki taraflı olan üçüncü derece bir devre tasarlamıştır (RDL), çift kaydırmalı bir çekim noktasını ve 3 bölümlü parçalı doğrusal bir direnci ortaya koymaktadır. Çalışmalarında çok sayıda tarama yolu ,alan doldurma eğrileri, resmi dile dayalı 2-D ,SCAN tarafından üretilebilir durumuna dayanmaktadır.

Kolumban, Vizvári, Schwarz ve Abel (1996), tarafından yapılan çalışmada faz kilitli döngülü hibrit sistemini (SPLL) doğrusal olmayan dinamik ve kaotik sistemler için kullanmışlardır. Eğer döngü filtre geçemese bifurcations (iki kola ayrılma) ve kaotik davranışlar gözlenebilir.

Lu ve He (1996), tarafından yapılan çalışmada basit kaotik devreler için tek değişkenli zamana bağlı diferansiyel denklemeler geliştirmişlerdir.Uygun paremeteler seçerek sinyal gecikmesini azaltmışlardır.

Ogorzalek (1997), tarafından yapılan çalışmada seçilmiş parametreler, girdi sinyalleri ve başlangıç koşulları gibi belirli durumlarda, bütün elektrik ve elektronik devrelerin davranışlarını kaotik şekilde açıklamıştır.

Yen ve Guo (1999), tarafından yapılan çalışmada, imgeleri yedi aşamaya dayanan ayna gibi şifreleme algoritma geliştirmişlerdir. Öncelikli olarak, tek boyutlu (1D) kaotik sistem belirlenmiş ve başlangıç noktası x=0 ve kümeleri belirlenmiştir. Sonrasında, kaotik sistem için ikili dizi geliştirmişlerdir. Son olarak, değiş-tokuş fonksiyonu ikili diziye göre 4 aşamalı imge piksellerini yeniden düzenlemişlerdir.

Hilborn (2000), tarafından yapılan çalışmada giderek artan yoğun desen formasyon alanlarını kuantum kaotik sitemler için hem differansiyel denklemler topluluğu hemde ynelemeli harita modelemesi geliştrmişlerdir.

Chang, Hwang ve Chen (2001), tarafından yapılan çalışmada imgeler için vektör niceleme (VQ) metodu kullanarak, şifreleme sistemi tasarlamışlardır.Vektör nicemleme (VQ) şifreleme şemasına ve birkaç diğer sayı teoremine dayanmaktadır. Bir vektör nicemlemedeki (VQ) ilk şey, imgelerin vektörler içerisinde ayrıştırılmasıdır, daha sonra vektörden vektöre sıralı olarak şifrelenirler.

Shin, Seo, Cho, Lee ve Kim (2003), tarafından yapılan çalışmada çok katmanlı ve imge bölme tekniğini kullanarak bir imge şifreleme tekniğini kullanmışlardır. Bir imgeyi şifrelemek için imgenin çok katmanlı bir formu olan bir algoritma ileri sürmüşlerdir. İmge bölme tekniğinin takip ettiği harici (XOR) işlemi ile gerçekleştirilmiştir. Bu yöntem, ikili Şekiler, ikili faz şifreleme için yeniden oluşturulur ve daha sonra bu imgeler ikili faz şifrelenir.

Belkhouche ve Qidwai (2003), tarafından yapılan çalışmada, kaotik eşlem kullanan imge şifreleme tekniğini kullanmıştır. Bu yöntem ile çeşitli anahtarların ikili imge şifreleme için kullanılabilir durumları iyleştirilmiştir.

Sprott ve Sprott (2003), tarafından yapılan çalışmada kaotik durumlar için basit doğrusal olmayan elektriksel devreler önermiştir. Devrelerde direnç, bobin ve diyot gibi işlevsel devre elemenlarını kullanmıştır. Çalışmalarında teori ve deneysel durumları doğrusal olmayan denklemlerle desteklemiştir.

Maniccam ve Bourbakis (2004), tarafından yapılan çalışmada yeni bir algoritma geliştirilmiştir. Modelleri; ikili ve gri ölçekli Şekilerin şifrelenmesi ve yitimsiz sıkıştırma, şifreleme ve sıkıştırma şemaları, bilgisayar tarama (SCAN) dayanmaktadır.

Xiao ve Zhang (2006), tarafından yapılan çalışmada iki kaotik sistemi kullanarak bir algoritma hazırlanmıştır; ilk kaotik sistem, bir başlangıç fonksiyonu kullanarak ikili bir akış içerisindeki değişime karşılık veren kaotik bir dizi oluşturur. İkinci kaotik sistem, bir atlama metrisi meydana getirecek şekilde karşılık vermiştir. İkili akışı bir anahtar akışı olarak kullanarak gerçekleştirilir, rastgele şekilde imgelerin piksel değerleri değiştirilmiş ve şifrelenmiştir.

Gu ve Han (2006),tarafından yapılan çalışmada hazırlanan yeni bir algoritma, ayırma ve yerleştirme yöntemlerine kullanılmıştır. İmge şifreleme için son derece optimize olduğu belirlenmiştir. Sözde rastgele kaotik dizileri arttırarak gerçekleştirilmiştir.

Gao, Zhang, Liang ve Li (2006), tarafından yapılan çalışmda sunulduğu gibi sıralı olarak değiştirilir. Gücüyle ve teğet fonksiyonları ile kaotik algoritma, XOR işleminin meydana getirdiği kaotik biz dizi kullanır

Pisarchik ve Zanin (2008), tarafından yapılan çalışmada bileşik kaotik şifreleme dizisini dinamik olarak değiştirmiştir. Yeni pikselleri orijinal piksellerin değiştirilmesi için hareket ettiren, yerleştirme ve devşirim yapılarak 2D kaotik eşlemden bütün pikselleri geçirmişlerdir.

Xiangdong, Junxing, Jinhai ve Xiqin (2008), tarafından yapılan çalışmada kaos teorisi sıralanmış dönüşümleri kullanan bir başka algoritma sunmuşlardır. Sayısal medikal imge koruma için piksel temelli şifrelemeyi kullanmıştır.

Tong ve Cui (2009), tarafından yapılan çalışmada dinamik şifre kaydırmayı kullanan imge şifrelemeyi öne sürmüştür.

Alsafasfeh ve Arfoa (2011), tarafından yapılan çalışmada "Lorent Kaotik Sistemini" "Rossler Kaotik Sistemine" ekleyerek yeni bir kaotik sisteme dayanan yeni bir imge şifreleme ileri sürmüştür. Deneysel analizden yola çıkarak, bu yeni algoritmanın geniş anahtar alanı ve yüksek düzeyli güvenlik ve yüksek hız avantajlarına sahip olduğunu açıklamışlardır. Analog kaotik sistemlerin yerine sayısal kaotik sistemler önerilmiştir.

Patidar, Pareek, Purohit ve Sud (2011) tarafından yapılan çalışmada devşirime dayalı imge şifreleme tekniğini önermişlerdir. İmge kalitesini devam eşzamanlılık ile birlikte rastgele piksel devşirimine dayalı olarak bir algoritma ileri sürmüşlerdir. Şifreleme için üç aşama uygulanmıştır. İlk aşama imge şifrelemedir. İkinci aşama anahtar üretimi aşamasıdır. Son aşama da, tanımlama süreci olarak bilinen küçük hesaplar ile bir renk imgesi özelliği sağlamaktadır.

Nag et al. (2011), tarafından yapılan çalışmda ilk olarak dönüşümün kullanılmasını işaret eden yeni bir algoritma sunmuştur ve bu algoritma aynı zamanda imge piksellerinin yerlerinin değiştirilmesine dayanmaktadır. Algoritma iki aşamada işe yaramaktadır. Birinci aşamada şifreleme,XOR işlemini kullanan imgeler ile sonuçlanır. Daha sonra, ikinci aşamada, ilgin dönüşümü kullanarak, piksel değerleri 4-bitlik anahtarlar ile farklı yerlere yeniden dağıtılmıştır. Dönüştürülen imge daha sonra 2 piksel ve 2 piksel gruplarına ayrılmıştır ve her bir blok dört tane 8-bitlik anahtarlar ile birlikte XOR işlemi kullanılarak şifrelenmiştir. Sonuçlar, piksel değerleri arasındaki ilgileşim analizinin, ilgin dönüşümün uygulanmasından sonra anlamlı derecede azaltılmış olduğunu göstermiştir.

Wang ve Shen (2011), tarafından yapılan çalışmada gerçekleştirilen paralel imge şifreleme algoritması, iki aşamada gerçekleştirilen kesikli kolmogorov eşleminin kullanılmasını önermiştir

Šalamon (2012), tarafından yapılan çalışmada devrelerin kaotik davranışlarını elektronik devre simülatörleriyle analiz etmiştir. Devredeki akım ve voltajların zamana bağlı olarak analizleri için bu simülatörler kullalınabileceğini göstermiştir.Yine yapılan modelemede bifurcation diagramını kullanmışlardır.

Jain, Bansal, Sharma, Kumar ve Gupta (2016), tarafından yapılan çalışmada çeşitli imge şifreleme mekanizmalarının ayrıntılı bir kıyaslamasını sağlamıştır.

Yukarıdaki tekniklerin hepsi, kaotik şemalara dayalı olan uzamsal alanı veya frekans alanını kapsamaktadır. Özetlemek gerekirse, şifreleme ve şifre çözme teknikleri gerçek zamanlı imge şifreleme için farklılık göstermektedir. Her bir tekniğin, farklı uygulamalar için uygun olabilecek, tek bir şifreleme ve şifre çözme yolu vardır. Her gün, yeni bir şifreleme tekniği geliştirilmektedir.

Bu çalışma, analog temelli kaotik şifreleme sistemlerini farklı bir model için geliştirlmiştir. Kaotik şemalar ile güvenlik düzeyini de iyileştiren yeni bir imge şifreleme tekniği ve modeli geliştirdik. Bu model güvenli iletişimi gerçekleştirmek için kaotik sinyal özelliklerinden yararlanmak üzere tekniklerin keşfedilmesi ile elde edilmiştir Ayrıca bağlı devrede, imge gri düzeylerinin çıkarma işleminde kullanmak

üzere bu kaotik diziler geliştrilmiştir. Sayısal kaotik imge, etkili bir yöntemle bir sayısal/analog dönüştürücü yoluyla bağlı devreye aktarılmış ve çözülmüş imge gerçek zamanlı olarak elde edilmiştir. Bu tekniğin diğer güvenli haberleşme yöntemlerine göre üstünlüğü, gerçek zamanlı olduğu için sayısal verilerin herhangi bir kayıtlı kopyasına, alıcıya imge olarak göndermek için bile ihtiyaç duymamasıdır.

1.3. Şifrelemede Kaotik Devreler

Kaotik dinamik özellikler sınırlı hassasiyet uygulamasında bozulabileceği için, güvenlik açısından bozulmaya yol açılabilir. Küçük şifre alanı, şifreleme analiz sistemleri dışardan saldırılarına karşı savunmasız bir durumdayken, daha yüksek boyutlu sistemler pek çok durumda imge şifrelemede kullanılmaktadır. Burada, yüksek rastgeleliğin ve daha karmaşık dinamik davranışın meydana getirdiği birden fazla yapının yanı sıra imge şifreleme için daha yüksek boyutlu kaotik sistemlerin kullanılması önerilmektedir.

Kaos temelli şifreleme sistemlerinin tasarlanmasına yönelik analog ve sayısal olmak üzere iki ana yaklaşım bulunmaktadır. Bu yaklaşımlar olarak Analog temelli kaotik şifreleme sistemleri, tek yönlü kaotik eşzamanlılık syona dayanan güvenli iletişim bağlantılarıdır.

Analog temelli kaotik şifreleme sistem, sürekli bir zaman kaotik sistemi veya zamanda ayrık kaotik haritaları bünyesinde uygulanabilir. Sayısal kaos temelli şifreleme sistemleri ise açık mesajı çeşitli şekillerde şifrelemek için mutlak hesaplama duyarlılığı olan bir veya daha fazla kaotik haritanın uygulandığı sayısal bilgisayarlar için tasarlanmıştır. Sayısal kaotik şifreleme sistem kaotik eşzamanlılık syona bağlı değildir fakat gizli bir anahtar olarak kullanılan başlangıç koşullarına ve kaotik parametrelerine sahiptirler. Şifrelemegrafide, gerçek rastgele sayı üreteçlerinden (TRNG) yararlanılabilir. Tam olarak kaotik sinyalleri sadece analog kaotik devreler üretebilir (Andreatos ve Leros, 2013).

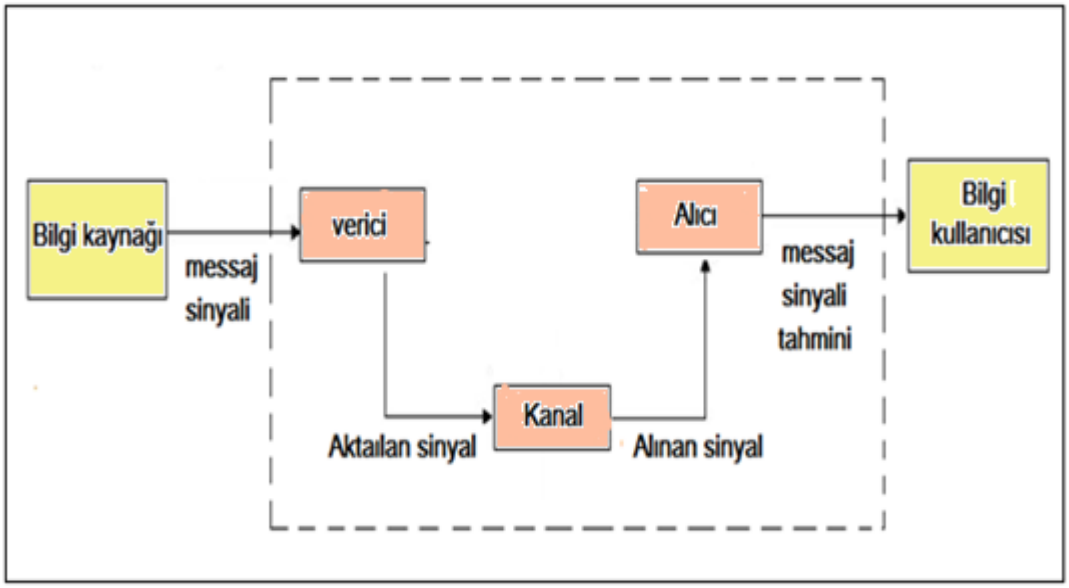
Genel olarak, kaotik analog devre normalde sayısal bir kaotik şifreleme sistemindeki uygun bir matematik modeli tarafından değiştirilir (Koh ve Ushio, 1997) Bilgisayarlar, denk düşen sayısal algoritmayı çözmek için kullanılır. Aslında, gerçek

rastgele sayı üreteçlerinden (TRNG) farklı olarak, sayısal kaotik devre modeli sadece bir analog değişken yaklaşımını sunmakta ve Rastgele Sayı Üreteci (PRNG) olarak çalışmaktadır.

Farklı değerlerin sayısı, sınırlı bit sayısının değerlerin kendisini temsil ettiği bir bilgisayarda her zaman nihaidir. Her iletişim sistemi, Şekil 1.1 de iletişim sistemlerinin temel yapısı gösterilmiştir. Sistem genel olarak verici, kanal ve alıcı olmak üzere üç temel öğeden oluşmaktadır. Vericinin amacı, kaynağın oluşturduğu bilgi sinyalini kanal üzerinden aktarılmaya uygun bir şekle dönüştürmektir (Sprott ve Sprott, 2003) Kanal, verici ve alıcıyı bağlayan fiziksel ortamdır. Bununla birlikte, kanalda, iletilen sinyal kanal boyunca yayılır. Dahası, gürültü ve karıştırıcı sinyaller de kanal çıktısına eklenir. Bunun sonucunda da bu alınan sinyal verilen sinyalin bozuk bir versiyonu olur.

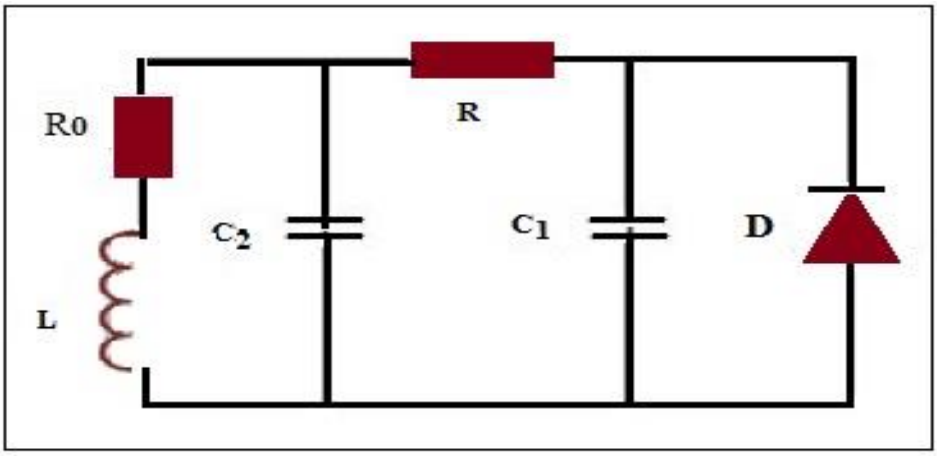
1.4. Kaotik Yöntemin Önemi

Kaotik yöntemin, aşağıdaki nedenlerle çeşitli imge şifreleme yöntemlerinin hepsi açısından en iyisi olduğu kanıtlanmıştır .Kaotik teknik, yüksek dağıntı değerinde net olan yüksek rastgelelik sağlamaktadır; Kaotik tekniğinin, orijinal pikseldeki tek bir bit değişimine çok yüksek hassasiyeti vardır; Şifreleme sistemimizin güvenlik özellikleri, bilinmeyen Kaotik devre topolojisine ve de kaotik devre davranışını değiştiren bileşenlerin farklılaşan toleransına dayanmaktadır; Bilinmeyen denetleyici türü; Kaotik teknikteki Pikseller, yüksek derecece ilintisiz olduğu için en iyileridir. Tek düze dağıtım, kaotik mekanizmasının en yüksekte durmasını sağlayan niteleyici bir özelliktir.



Şekil 1.1. İletişim sistemlerinin temel elemanları

Alıcının,bir kullanıcı için orijinal bilgi sinyalinin tanımlanabilen bir biçimini yeniden oluşturmak amacıyla, alınan sinyal üzerinden çalışması gerekir. Şekil 1.2 de Chua'nun doğrusal olmayan RCD basit devresi gösterilmektedir. Bu devre iki taraflı olan üçüncü derece bir devredir (Lu ve He, 1996) Chua devresi iletişim sistemlerinde kaotik eşzamanlılık sistemine sahiptir.



Şekil 1.2. Chau nun kaotik RCD devresi

Elektronik devreler doğrusal (DC) ve doğrusal olmayan (AC) şekilde teorik olarak iki durumda diferansiyel çözümler verilirken, deneysel olarak tam doğrusallık için mevcut değildir. Aslında, bütün devreler gerçek zamanlı olarak doğrusal değildirler.

Doğrusal olmayan türevsel denklemlerin çözülmesi gerektiğinden, analiz matematiksel olarak zordur.Bağımlı doğrusal olmayan devreler, işlevlerine göre farklı çözümlerde karşımıza çıkar (Ogorzałek, 1997). Çözümler sırasıyla, periyodik ve yarı periyodik (osilatör, sinyal üreteci), asimptotik olarak kararlı (iki kararlı devreler, hafıza tutucu devreler) ve hiperbolik olarak kararlı devreler (RLC-filtreli, yükselteçli v.b) şeklinde devrelerdir.

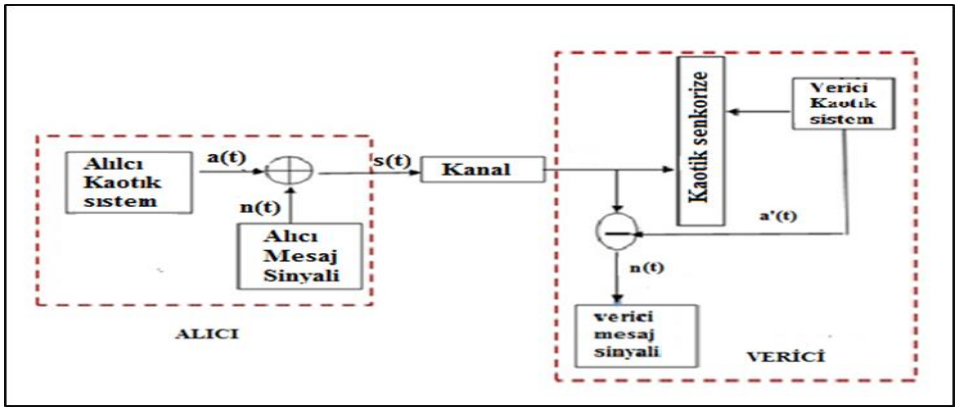
2. KURAMSAL BILGI

Genel olarak, elektronik kaotik devreler anolog ve sayısal olmak üzere iletişimde doğrusal olmayan sayısal algoritmalar için kullanılır. Doğrusal olmayan güvenli analog temelli kaotik şifreleme sistemleri dört temel başlık altında incelenmiştir. Bunlar sırasıyla, kaotik maskeleme, kaotik kaydırmalı (anahtarlama), kaotik eszamanlilik ve kaotik karışık devrelerdir (Yang, 2004).

2.1. Kaotik Maskeleme

Kaotik maskeleme methodun temel prensibi genel olarak verici-alıcı eşzamanlılık sistemine dayanır. Vericiteki I(t), giriş sinyali kaotik sistemin kaynağını oluşturmaktadır. Alıcıda ise, çıkış sinyalinin kaotik eş zamanlılık ve taşıyıcı senkroniz oluşturmaktdır.Şekil 2.1 de hem verici hemde alıcı kaotik maskeleme durumuna ait şema verilmiştir.

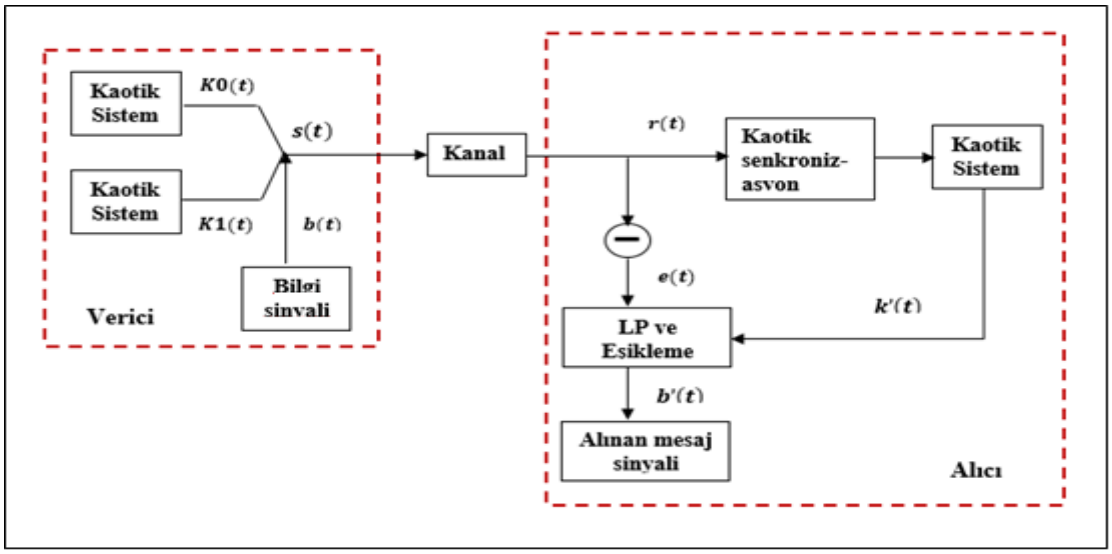
Burada $a(t)$, zamana bağlı vericideki kaotik sistem parametresi değeri 20 desibel-30 desibel arasında değişir $n(t)$, mesaj sinyali parametresi ve $s(t)$, vericiden aktarılan toplam sinyal $s(t) = a(t) + n(t)$ dir. Kaotik sinyal $a(t)$ çok karmaşık olduğu ve $n(t)$ de $a(t)'$den daha küçük olduğu için, mesaj sinyalinin $n(t)$ gerçek $a(t)$ değeri bilinmeden $s(t)$'den ayrılamayacağı beklenebilir.



Şekil 2.1. Analog kaotik maskeleme devresi

2.2. Kaotik Kaydirmali Anahtarlama (CSK)

Kaotik anahtarlama (CSK) yöntemi, kaotik çekim noktaları ile eszamanlilikun en basit şeklini göstermektedir. Sayısal mesaj sinyalini aktarmak için tasarlanmıştır. Sayısal sinyallerin deşifre edilmesi için uygundur.Güvenlik derecesini bir dereceye kadar geliştirir.Ancak yine de yetersiz bulunmaktadır. Şekil 2.2 de gösterildiği üzere, ikili bir girdi sinyalini şifreleme durumunu gözlemleyelim.



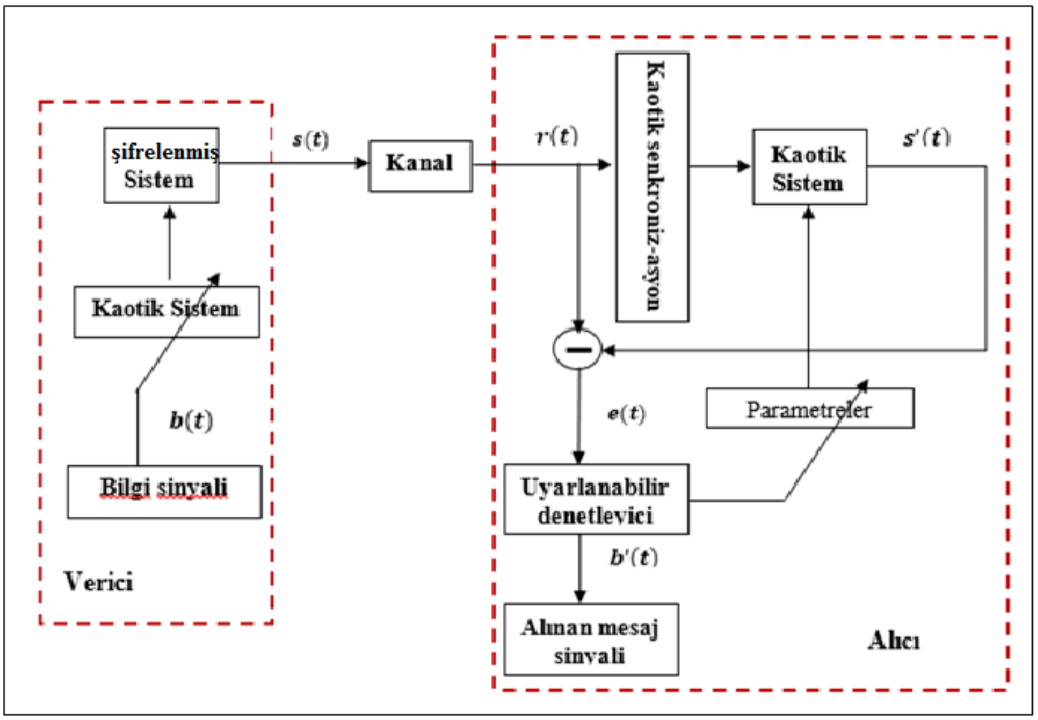
Şekil 2.2. Analog kaotik anahtarlama şeması

Verici, parametreleri olan iki kaotik alt sistemden oluşmakta ve farkı parametreleri olan kaotik sistemler arasında değiştirme yapan anahtarı kullanarak alt sistemleri kontrol etmektedir. Bu mesaj sinyali b(t)şemasındaki, statik olarak benzer iki kaotik çekim noktası olan k_0(t) ve $k_1(t)$ arasında aktarılan sinyali anahtarlamak için, sayısal bir sinyal kullanılır.

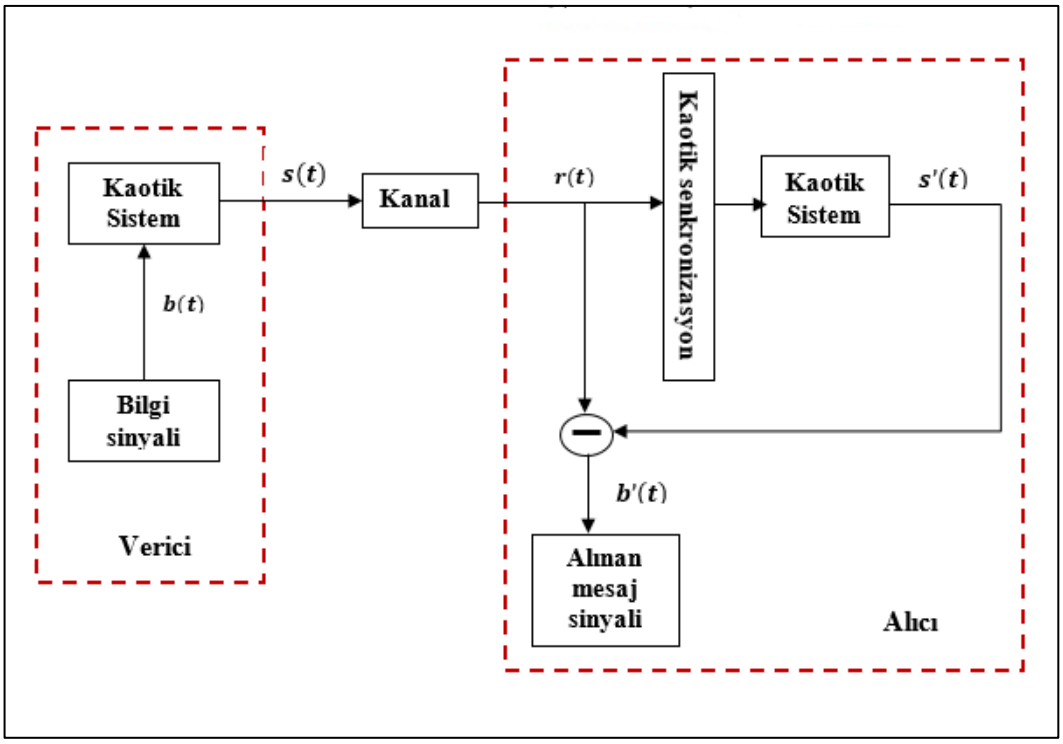
Mesaj sinyali 0 ve 1 bit şifrelemek için sırayla kullanılır.Farklı parametreler ve aynı yapı ile birlikte, her iki çekim noktası iki kaotik sistem tarafından üretilir.Alıcıda alınan sinyal, herhangi bir kaotik sistem vericisine kayıtsızca benzer olan bir kaotik sistemi yönlendirecek şekilde kullanır. Eşzamanlılık syon hata sinyalini alçak iletimli filtreleme ve sonrasında eşikleme,mesaj sinyalini $e(t)$ kurtaracaktır.

2.3. Kaotik Modülasyon

Kaotik taşıyıcılar için mesaj sinyallerinin değiştirilmesi için iki yöntem kullanırlar. Şekil 2.3.a gösterildiği üzere kaotik parametre modülasyonu olarak adlandırılır. Diğeri ise Şekil 2.3.b gösterildiği şekilde kaotik özerk olmayan modülasyondur. Kaotik parametre modülasyonunda, sinyal p(t) bir mesaj sinyalini temsil eder ve kaotik sistemin vericisi dahilinde ve aynı zamanda bazı parametreleri değiştirir; yörüngeleri farklı kaotik çekim noktalarını değiştirmeye devam eder. Kaotik sistem dahilindeki çatallaşma alanı o kadar karmaşıktır ki parametrelerindeki değişikliklerin çözülmesi çok zordur. Uyarlanabilir bir kontrol birimi, eşzamanlılık syon süreci boyunca kaotik sistemi uyarlanabilir şekilde ayarlar.



(a)



(b)

Şekil 2.3.(a) Kaotik parametre modülasyonu (b) Kaotik özerk olmayan modülasyon

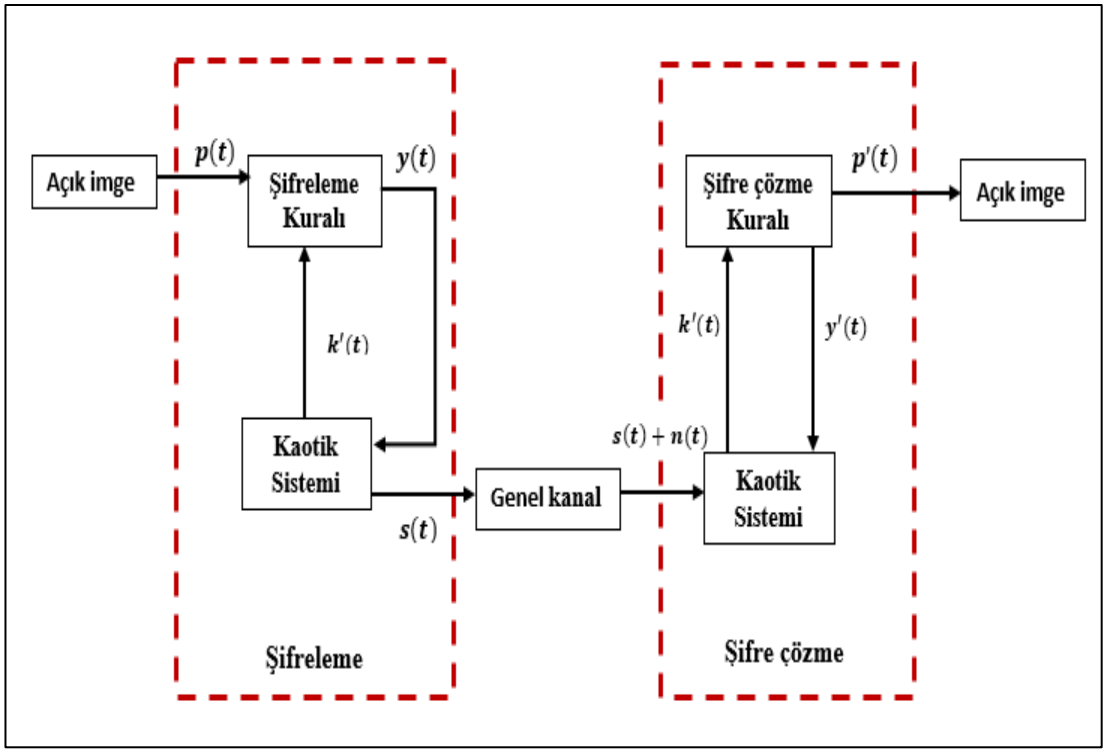
Şekil 2.3.b de gösterildiği üzere, kaotik özerk olmayan modülasyon, doğrudan bu evre uzayında kaotik çekim noktasını sarsıma uğratacak şekilde kaotik vericinin parametrelerini değiştirmek yerine mesaj sinyalini kullandığını göstermektedir. Verici, bir kaç kaotik çekim noktasında bir takım yörüngeler arasında anahtarlanır. Aynı kaotik çekim noktalarının çeşitli yörüngeleri vasıtasıyla, kaotik özerk olmayan modülasyon gönderici cihazda anahtarlanır. Teoride ise, kaotik özerk olmayan modülasyon herhangi bir hata şeması sayesinde kesin doğruluğa sahiptir.

2.4. Kaotik şifreleme sistemi

Kaotik güvenli iletişim şemalarının, düşük kanal kullanımı gibi bazı dezavantajları dolayı ,güvenlik derecesinin artırılması için kaotik şifreleme sistem gelişlmiştir.Bu sistemlerde güvenlik derecesini arttırmak için, kaotik eşzamanlılık ve klasik şifreleme tekniğinin kombinasyonu kullanılmaktadır (Yang, 2004).Yine de, bütün kaotik güvenli iletişim sistemlerinde, bu kaotik sistem türü şimdiye kadar bozulmamış olan en yüksek güvenliğe sahiptir.

Şekil 2.4 de Kaotik şifreleme sistemine ait vericide kaotik sistem tarafından meydana getirilen düz metin sinyalini şifrelemek için anahtar bir sinyal $c(t)$ ile şifreleme kuralından yararlanan analog kaotik şifreleme sistemini göstermektedir. Kaotik sistemi yönlendirmek için, kaotik dinamiklerin açık kanal üzerinden aktarıldığı vericideki kaotik sistemi değiştirdiği karıştırılmış sinyal kullanılır. Aslında izinsiz giren, kaotik donanım anahtarına erişemeyeceği için, $s(t)$ değerinden $p(t)$ değerini bulmak oldukça zordur.

Alıcıda, alınan sinyal $r(t) = s(t) + n(t)$ şeklindedir.Vericide alıcıyı ve kaotik sistemi senkronize etmek için, kanal gürültüsünü $n(t)$ kullanırlar. $k(t)$ ve $y(t)$ sinyali, $k'(t)$ ve $y'(t)$.,ile ifade edilen bazı gürültüler ile alıcıda geri kazanılabilir. Kaotik eşzamanlılık meydana getirildikten sonra şifre çözümü içinde $k'(t)$ ve $y'(t)$ beslenir.



Şekil 2.4. Kaotik şifreleme sistem şeması

2.4.1. Kaos Temelli Şifreleme Sistem Türleri

Kaos teorisi için, sayısal benzeşim açısından fiziksel devre sisteminde belirli bir sapma bulunmaktadır. Büyük sinyal koşulları altında, çoğu kaotik güvenli iletişim şemalarının uygunluğu ve güvenliği açısından bazı eksiklikler bulunmaktadır. Güvenlik sorunlarını çözmek için, dinamik araştırma ve modern genişletme alanlarının anlaşılması ve uygun kaynakların tasarlanması ile mevcuttur (Wu ve Chua, 1993).

Kaotik dizilerin oluşturulması için basit yapı ve yüksek hız da imge şifrelemede kullanılması büyük çapta zaman ve uygulanabirlirlik açısından kolaylık sağlayacaktır.

Diğer yandan düşük boyutlu kaotik şifreleme sistemlerin birkaç dezavantaj kullanılmaktadır.İlk dezavantaj, düşük boyutlu kaotik kaotik dizilerin, herhangi bir kaotik yörüngenin sınırlı bir hassasiyete sahip bilgisayar gerçekleşmelerinde daha kısa dönemselliğe sahip olmasıdır.

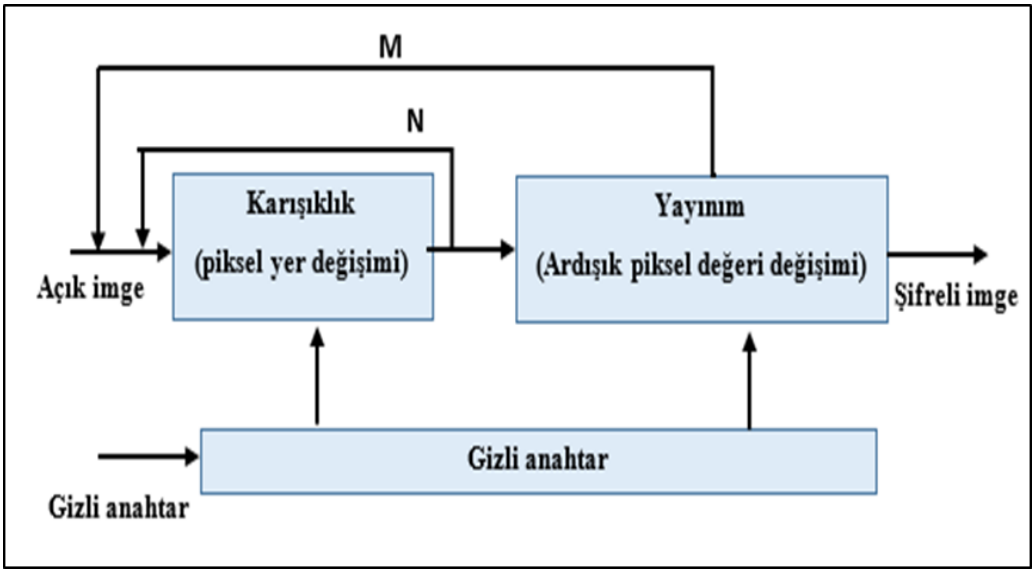
Kaotik dinamik özellikler sınırlı hassasiyet uygulamasında bozulabileceği için, sonuç olarak güvenlik açısından bozulmaya yol açılabilir.Diğer bir dezavntaj, küçük şifre alanı sahip olduğundan , şifreleme analiz saldırılarına karşı savunmasız olmasıdır.Bu önemli durumlardan dolayı,daha yüksek boyutlu sistemler pek çok durumda imge şifrelemede kullanılmaktadır.Burada,yüksek rastgeleliğin ve daha karmaşık dinamik davranışın meydana getirdiği birden fazla yapının yanı sıra imge şifreleme için daha yüksek boyutlu kaotik sistemlerin kullanılması önerilmektedir.

2.4.2. Kaotik İmge Şifreleme Sistemleri Yapısı

Şekil2.5 de kaos temelli imge şifreleme sistemlerinin yapısal tasarımını göstermektedir.Karışıklık ve yayınım olmak üzere iki aşamadan oluşur. Bu aşamalardan; karışıklık durumuda, gizli bir talebin olduğu durumda, imge piksellerininleri yer değişimi şifreleme açısından önmelidir.Buna ek olarak, tüm imgeyi bekleyerek, bir pikselde küçük bir değişim birkaç piksele yansıtılır.Aslında,

karışıklık aşamasında gereken zaman n olarak bilinir, n değeri genellikle 1 değerinden daha büyüktür ve yayınım aşaması tarafından da gözlemlenir.

Tatmin edici bir güvenlik düzeyi elde etmek için, kapsamlı n-devirli karışıklık ve tek devirli yayınım, çoğu durumda m değerinin 1'den daha yüksek olduğu sürelerden başlayarak çoğalır. Yayınım ve değiştirme, Şekil 2.5 de gösterildiği gibi, birincil kaotik planların kısıtlamaları gibi farklı devirlerde karışık ve yayınım şifreleme arasındaki ilişki gösterilmektedir. Burada, bir devirli anahtar üreteci bunu girdi gibi çekirdek bir gizli anahtar ile bunu başarabilir. Tablo 2.1 de kaos tabanlı anolog ve sayısal şifreleme sistemlerini hakkında bilgi vermektedir.



Şekil 2.5. Standart yapılı kaos temelli imge şifreleme sistemleri

2.4.3. Kaotik sistemler ve şifreleme sistem arasindaki ilişki

Pek çok açıdan, geleneksel şifreleme sistem ve kaotik sistemler arasındaki yakın ilişkide bir çıkış mevcuttur. Bunlara ek olarak, şifreleme sistemde ihtiyaç duyulanlara benzer şekilde denk düşenler ile aynı şekilde, kaotik sistemler pek çok üstün dinamik özelliklere sahip olabilir. Parametre ve başlangıç koşulları için rastgele davranışla birlikte duyarlılık, avantajlar sağlayan kaostur. Aslında, hız, güvenlik, hesaplama gücü, karmaşıklık ve hesaba dayalı ek yük, kaos temelli şifreleme algoritmasının olağandışı iyi özellikleri olarak sınıflandırılır. Tablo 2.2'de.

Tablo 2.1.*Kaos temelli şifreleme sistem türleri*

KATEGORİ	YÖNTEM	AÇIKLAMA	
Analog Şifreleme sistem	Kaos maskeleme	Mesaja kaotik bir sinyal eklenmiştir.	
	Kaotik kaydırmalı anahtarlama	Mesaja eklenecek farklı kaotik sistem arasındaki sayısal bir mesaj sinyali anahtarlama.	
	Kaotik Modülasyon	Kaotik vericinin parametrelerini veya faz uzayını değiştirmek için bir mesaj sinyali kullanılır.	
	Kaotik Kontrol	Bir mesaj sinyali, klasik bir şekilde şifrelenir ve kaotik sistemi alt üst etmek için kullanılır.	
Sayısal Şifreleme sistem	Kesintisiz şifreleme	Kaotik PRNG	Bir kaotik sinyal, XOR Kırmızı mesaja göre sözde rastgele bir dizi meydana getirir.
		Kaotik Ters Sistem Yaklaşımı	Bir mesaj sinyali, verilmiş bir uyarıdaki şifreli mesaj sinyalinin beslemiş olduğu kaotik sinyal çıktısına eklenir.
	Blok şifreleme	Tersine doğru yinelemeli	Tersine kaotik sistem kullanılarak açık bir mesajın bir bloğu şifrelenir.
		İleriye doğru yinelemeli	Kaotik sistemden elde edilen sözde rastgele değiştirme ile açık bir mesajın bir bloğu elde edilir.
		S -Kutuları	S-Kutuları, kaotik sistemden oluşturulur.

Şifreleme sistemlerde, dönemsellik kavramı karışıklık kavramı arasındaki durum ilişiklendirilebilir. Geleneksel şifreleme sistemlerindeki karışıklık kavramı, düz imgenin rastgele şifreli imgeye, şifreli imgedeki modele dönüştürülmesine neden olur. Genel olarak, tek biçimli dağıtım ile birlikte, kaotik sistemin yörüngeleri faz uzayının her noktasından geçer;burada, başlangıç koşulundan itibaren, bir noktanın son konumunu tahmin etmek oldukça zordur.

Yayınımın özelliği, iyi bir şifreleme sistem geliştirebilecek başka bir temel tasarım prensibidir. Bir bitin, düz imge veya anahtarı nasıl değiştirdiğinin bir öneminin olmaması ile sonuçlanarak, çok zor bir şifreli imge ile gerçekleştirilebilir.Bu bölümden yola çıkarak, sistemin şifreleme anahtarının yanı sıra düz imgeye de duyarlı olduğu açıktır.

Tablo 2.2.*Kaotik sistemin özelliklerin karşılaştırılması*

Kaotik sistem	Geleneksel şifreleme sistemler
Döngelik	Karışıklık
Başlangıç koşullarına ve sistem parametrelerine duyarlılık	Yayınım
Parametreler	Şifreleme anahtarı
Yinelemeler	Şifre

Fakat bir diğer yandan, yörüngelerin birbirinden anlamlı derecede uzaklaştığı başlangıç koşulları veya başlangıç noktası tarafından kaotik sistemlerin yavaşça etkilendiğini göstermektedir. Buna ek olarak, şifreleme sistemlerin şifreli devrelerin üyeleri ile düz imgeyi karıştırdığı ve yaydığı yerde, şifreleme sistemler ve kaotik sistemler doğal olarak hesaba katılabilir.

Kaotik sistemdeki başlangıç bölgesi, sonuç olarak yinelemeler aracılığıyla tüm faz uzayı üzerinden dağıtılır, dolayısıyla, kaos teorisine şifrelemegrafi alanında yatırım

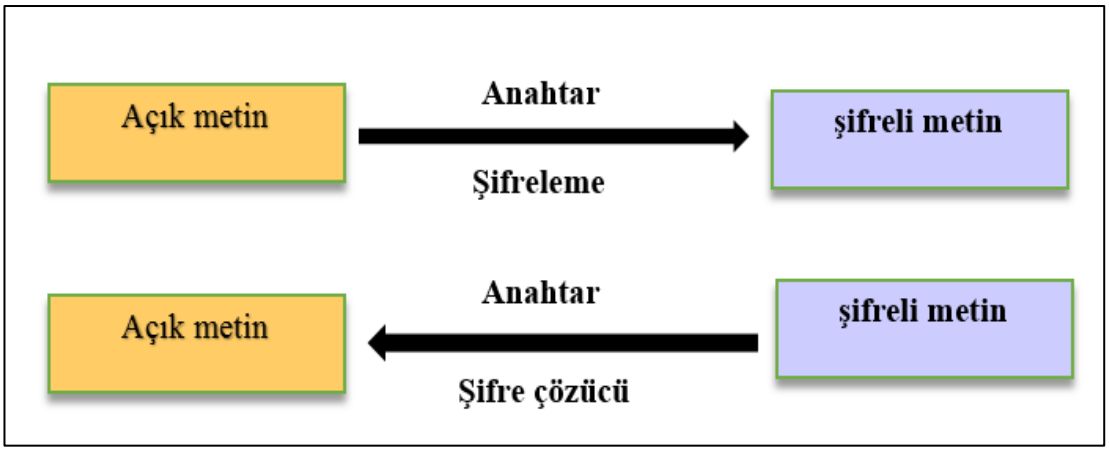
yapılabileceğine dair bir beklenti bulunmaktadır. Başlangıç koşulu ve sistem parametreleri gizli anahtar *s* olarak kullanılır.

2.5. Şifreleme Algoritmasi

Şifrelemegrafi algoritmasının matematiksel fonksiyonu, aynı zamanda şifre olarak da bilinen veri şifre çözümü olarak adlandırılır.Burada şifrelemegrafi algoritması; bir anahtar, bir kelime, bir sayı veya düz metni şifreleyecek bir ifadenin karışımı olan mekanizmadır.Farklı anahtarlar ile, özdeş düz metin veri güvenliğini etkileyerek, farklı metnini şifreler. Aslında, şifreleme yüksek güvenlik açısından iki durum bakımından önemlidir.Sırasıyla, şifrelemegrafik algoritmanın gücü ve şifreleme anahtarın güvenirliliğir.

2.5.1. Geleneksel Şifreleme

Geleneksel şifrelemegrafi Şekil 2.6 da gösterildiği gibi hem şifre çözme hem de şifreleme için tek bir anahtar ile ilerleyen, simetrik anahtarlı şifreleme ve gizli anahtarlı olarak da bilinmektedir.



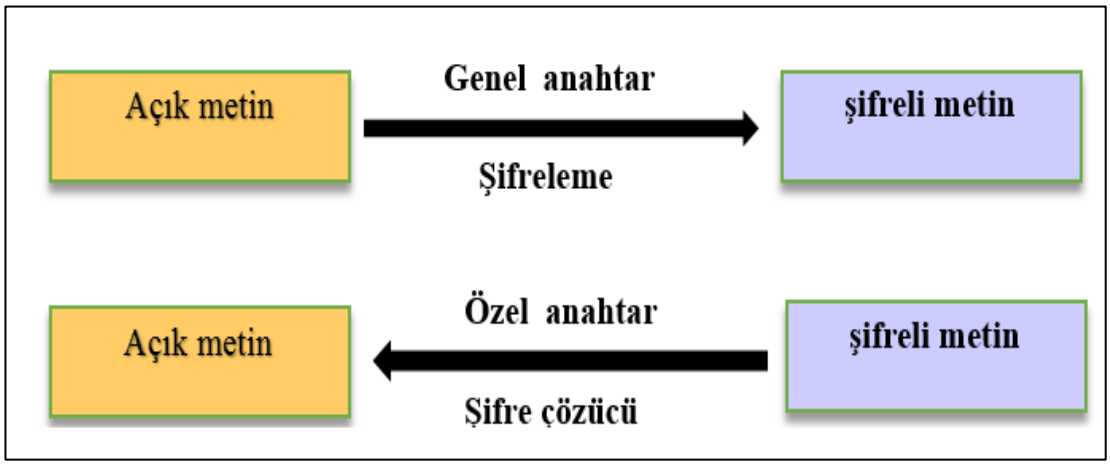
Şekil 2.6.Geleneksel şifreleme

Geleneksel şifreleme hızlı olması, aynı yerde kalan verilerin şifrelenmesine yönelik avantaja sahip iken, güvenli verilerin aktarılması için bir araç olarak, geleneksel şifrelemeyi nispeten pahalı hale getiren, güvenli anahtar dağıtımı zorluğundan dolayı işlem maliyeti açısından da bir dezavantajdır.

Bir diğer yandan, gönderici ve alıcının haberciye veya aktarım boyunca gizli anahtarın açığa çıkarılmasını engelleyecek bir araç olan başka bir iletişim yöntemine güvenmesi gerekir; bu durumda, her ikisi de farklı fiziksel konumlarda mevcut olur. Diğer bir dezavantaj da eğer aktarım esnasında anahtarı dinler veya yarıda keserse, bu anahtar ile şifreli veya denetli bütün bilgileri herhangi biri teslim edebilir, değiştirebilir veya saptırabilir.

2.5.2. Açık Anahtarın Şifreleme

Şekil 2.7 de şifreleme için bir çift anahtarı uyarlayan asimetrik bir yapı gösterilmiştir. Burada, verilerin şifrelenmesi için açık anahtar ve şifre çözümü için uygun gizli özel anahtar dağıtımı mekanizmasını belirtilmiştir.Özel anahtarın sırrını koruması ile birlikte, açık anahtar bütün dünyaya açık hale gelir; burada, her bireyin sadece kendisinin okuyabileceği bilgileri şifreleyebilecek bir açık anahtar çiftine sahiptir.



Şekil 2.7. Açık Anahtar Şifreleme

Açık anahtarın en önemli temel özelliklerinden, mesajları güvenli şekilde değiş-tokuş edecek önceden var olan bir güvenliğin olmadığı genel kamu izinleri, güvenli kanal kullanılırken bile alıcının yanı sıra gönderici için de gizli anahtarların paylaşılmasını reddetmesidir.Aslında, herhangi bir gizli anahtarın aktarılmadığı veya paylaşılmadığı halde bütün iletişimler açık anahtarları kapsamaktadır.

Buna ek olarak, bazı açık anahtarlı şifreleme sistem özellikleri şöyledir;DSA (sayısal imza algoritması),RSA (asimetrik algoritma).

2.6. Şifreleme Yöntemleri

Veri şifreleme için çeşitli metotlar vardır. Bu metotlardan DES (Veri şifreleme standartı (DES), ortak gizli şifreleme uygulayan şifrenin bloke edilmesidir. DES, en yaygın blok şifre algoritması, Qian Gong-canister v.d. tarafından ileri sürülen imge şifreleme için kullanılan alternatif bir yazılı şifreleme sistem olan 64 bitlik anahtar kullanır. DES, uluslarası kapsamlı, Amerikada federal bilgi işleme standardı (FIPS) olarak bilinmektedir. Bu şifreleme stantdartı,56-bitlik anahtara sahip simetrik bir algoritma sistemidir. Daha önceleri şifreleme anahtarlarının uzun ve güvensiz olmasından dolayı sorunlar yaşanıyordu,ancak şifreleme analizlerinin modern anlamda iyleştiştirimesi DES sayesinde avantajlı duruma gelmiştir.Daha sonra geliştirilen,Üçlü DES (3DES) sistemi sistemi üç kez tamamlayarak daha güvenli olmuştur. Buda şifreleme olayının 256 kat daha fazla güvenli olacağı anlamımna gelir.

Yine diğer method olan AES (Geliştirilmiş şifreleme standartı), izin verilen üç anahtar uzunluğu şöyledir; 128-bit, 192-bit ve 256-bit. AES 197 standart sayısı ile, Federal Bilgi İşleme (FIPS) içerisinde iyi tanımlanan simetrik ve buna Amerikan federal hükümeti tarfından destekli şifreleme algoritmasıdır.

Genel olarak algoritmanın, herhangi bir mesajı şifrelemek ve şifresini çözmek için doğru anahtarın bilinmesi gerekir. Tablo 2.3’ de tüm şifreleme çeşitlerine göre anahtar alanı ve anahtar uzunluğu gösterilmiştir. Anahtar alanı veya boyutuna dikkat edilmesi gerekir çünkü olası bir anahtarla yakalanan bir mesajın şifresini çözmeye çalışmak herhangi biri için bir şifreyi çözmek için en basit yoldur. Şifreleme için kullanılan anahtarların yanı sıra başlangıç parametreleri de, imge şifreleme aşamasında oldukça duyarlıdır.

Anahtar alanı, anahtarı deşifre etmek için gereken zamanı etkilemiştir. Buna ek olarak, birtakım imge şifreleme mekanizmalarının önemle kıyaslanması (Yang ve Chua, 1996) çalışmada verilmiştir. Anahtar boyutunun kareler algoritmasının yerinde olduğu, toplam anahtar boyutu ile kıyaslandığında şifreleme sistem üstsel bir hale gelir. Bir örnek olarak, anahtar boyutu olarak 128 bit dahilindeki şifreleme

algoritması, 2^{128}'lik bir anahtar alanını nitelemektedir; bu da, yaklaşık 1021 yıl ihtiyaç duyulabilecek tüm olası anahtarların denetimini son derece etkilemiştir.

Tablo 2.3. *Anahtar şifer Alanı*

Şifre	Anahtar uzunluğu	Anahtar alanı
DES	56	2^{256}
3DES	168	2^{168}
AES	128	2^{128}
ELİPTİK	2x64	2^{128}
KAOTİK	6x64	2^{384}

2.6.1. Kaotik şifreleme şemaları için parametreler

Farklı çalışmalarda, araştırmacılar imge şifreleme için geçerli olacak kaotik şifrelemegrafik sistemin performansını değerlendirmek için birçok parametre önermiştir. Genel olarak, şifrelemegrafik teknikler rastgele sayı teorisine ve cebirsel formüller üzerine odaklanmaktadır. Fakat kaotik prosedürler, doğrusal olmayan dinamikler alanına uygun olacak büyük sayılar (kaos) ile belirlenmektedir. Kaotik şifreleme, belirleyici dinamikler, doğrusal olmayan fonksiyonları ve kaos özellikleri olan tahmin edilemez davranış gibi önemli özelliklere dayanmaktadır. Performans, bütün şifrelemegrafik teknikler için bir nebze en önemli faktördür. Buradaki dikkate değer endişe, farklı yazarların kaotik şifreleme tekniklerinin tahmin edilmesi için farklı düşüncelere sahip olmasıdır, hatta faktörlerin sayısı ve bunların yapısı da bireyden bireye sapar.

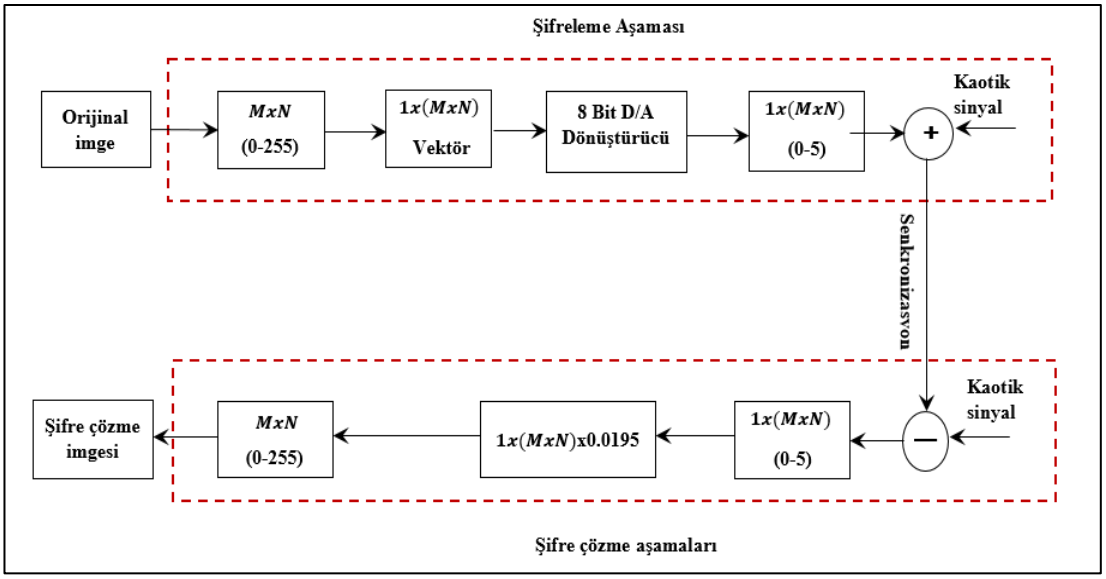
Kaotik şifreleme için temel parametreler (Ahmad ve Alam, 2009; Ahmed, Kalash, ve Allah, 2007; Awad ve Saadane, 2010;Gao, Zhang, Liang, ve Li, 2006;Jakimoski ve Kocarev, 2001; Lee, Pei, ve Chen, 2003; Liu, Sun, ve Xu, 2009; Mao, Chen, ve Lian, 2004; Maung ve Sein, 2008;Rao ve Gangadhar,2007;Socek, Li, Magliveras, ve Furht, 2005; Wang, Zhang, ve Cao, 2009; Zhu ve Li,2010) raporlarında

gösterilmektedir; burada, hız, anahtar alanı, histogram (çubuk grafik), ilgileşim katsayısı, piksel katsayısı, bilgi yitimi ve rastgele bir sayıyı ele almışlardır.

2.6.2. İmge Şifreleme/Şifre çözme Tekniği

Önceki çalışmalardan yola çıkarak, bütün imge şifreleme teknikleri, yerleştirme ve devşirim ile bir piksel bloğunu şifrelemek için, karmaşık matematiksel adımlara dayanan matematiksel algoritma ile birlikte sayısal rastgele üretimi veya kaotik eşlemleri kullanmaktadır.Bir blok içerisindeki pikseller dizisini okunabilir hale getirmek için değiştirmektedir. Küçük anahtar alanları, yavaş performans ve daha zayıf güvenlik gibi dezavantajları bulunmaktadır.

Şekil 2.8 de yeni bir güvenli imge şifreleme /şifre çözme tekniği adımlarıyla gösterilmiştir.Dolayısıyla, araştırmacılar, sadece açık ve şifreli imge arasında iyi rastgele sağlayabilecek değil aynı zamanda geniş anahtar alanına sahip olması gereken çalışmalara dikkatlerini yönlendirmiştir.Ayrıca, işlem süresi olabildiğince düşük olmalıdır.



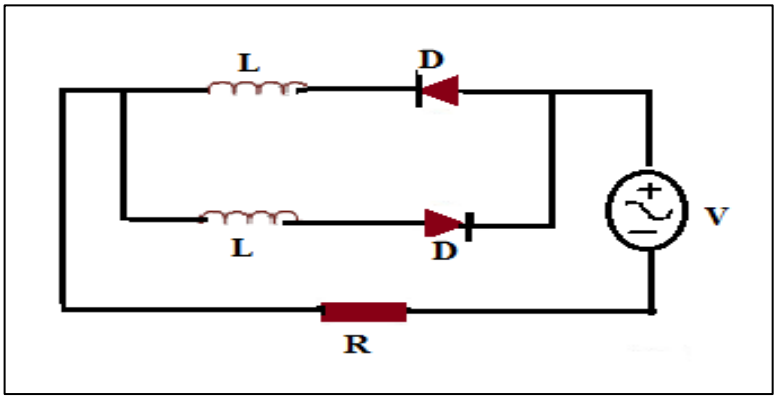
Şekil 2.8. Şifreleme ve şifre çözüm aşamaları

2.6.3.Şifreleme/Şifre çözme Tekniği

Şifreleme aşamasında; Şifreleme ve şifre çözme tekniği için Şekil 2.8'e göre;imge metrisi piksek boyutunu (MxN) bulmak için imgenin okunması ile başlamaktadır; burada, M ve N imgenin satır ve sütun dizimini temsil etmektedir. Daha sonra, bir imge verisi (0-255) arasında onlu gri tonlamalı değer biçiminde olmalıdır. Son olarak, MxN metrisi bir tane bir boyutlu vektör boyutuna dönüştürülür, 1x(MxN) üretilir.i,.aşamda, üretilen gri tonlamalı dizi olan 1x(MxN) vektör,8-bitlik Sayısal/Analog devre kullanılarak analog voltaj değerlerine dönüştürülür.ii.,aşamada, üretilen 1x(MxN) vektörü, güvenli olmayan kanal üzerinden alıcıya gönderilecek kaotik sinyal ile maskelenir.iii.,aşamada,Şifre çözme, ters işlem gerçekleştirilecektir, sadece farklı olarak,Analog bu formül voltaj değeri /0.0195 kullanılarak sayısala dönüştürülecektir.Son aşamalarda, MxN matrisi imgenin Şifresinin çözülmesi için kullanılmaktadır.iv.aşamada,.sayısaldan/analoga dönüştürücü (DAC), digital formdaki girdi sinyalinin analog formdaki bir çıktı sinyaline dönüştürmek için kullanılan bir cihazdır.

2.7. R2D2L Kaotik Devrede Eşzamanlılık ve Güvenli İletişim

Bu çalışmada iletişim algoritması için daha güvenli şifreleme R2L2D olarak (E Kurt, 2006) tarafından önerilen bağımlı (non-autonomous) kaotik bir devredir.Devrenin temel akım-voltaj yapısı Şekil 2.9 de gösterilmiştir. Devre nin giriş gerilimi alternatife gerilim olup sinüzal olarak; $V = \mathrm{V}_0 \sin(wt)$ şeklinde verilmektedir.



Şekil 2.9. R2L2D devresi

Burada, devrenin toplam gerilimi V; direnç (VR) ve bobin-diyot ikilisinden (VLD) den kaynaklanmaktadır.

$$V_R + V_{LD} = V \tag{2.1}$$

Şekil 2.8 de gösterildiği gibi, ters konumda iki diyot ve iki bobin birbirlerine bağlanmıştır. Ana koldan I akımı, her kolda I_1 ve I_2 olarak ayrılırken, negatif ve pozitif sinusoidal voltaj alternatifleri bütün süreç boyunca kolların içerisinden geçer. Dolayısıyla, devrenin voltaj kalitesi aşağıdaki gibi ifade edilebilir:

$$V_{LD} = V_{D1} + L\,\frac{dI_1}{dt} \tag{2.2}$$

$$V_{LD} = V_{D2} - L\,\frac{dI_2}{dt} \tag{2.3}$$

Buradan denklemler ele alınırken, şu sonuca ulaşılır;

$$\frac{\mathrm{dI_1}}{\mathrm{dt}} = \frac{\mathrm{V_{D1}}}{\mathrm{L}} + \frac{\mathrm{V}}{\mathrm{L}}\sin(\mathrm{wt}) - \frac{\mathrm{R}}{\mathrm{L}}\,(\mathrm{I_1} + \mathrm{I_2}) \tag{2.4}$$

$$\frac{\mathrm{dI_2}}{\mathrm{dt}} = \frac{\mathrm{V_{D2}}}{\mathrm{L}} + \frac{\mathrm{V}}{\mathrm{L}}\sin(\mathrm{wt}) - \frac{\mathrm{R}}{\mathrm{L}}\,(\mathrm{I_1} + \mathrm{I_2}) \tag{2.5}$$

Burada, I_1ve I_2 kol devrelerini simgelemektedir ve $I = I_1 + I_2$ geçerlidir.

V_{D1} ve V_{D2}'nin diyotlar üzerindeki voltajlar için kullanıldığını dikkate alınız. Tam anlamıyla anlatırsak, şu şekilde yazılabilirler:

$$V_{D1} = \frac{kT}{e}\ln\left(\frac{I_1}{I_s} + 1\right) \tag{2.6}$$

$$V_{D2} = \frac{kT}{e}ln\left(\frac{I_2}{I_s} + 1\right) \tag{2.7}$$

Böylelikle, diyotların doğrusal olmayan davranışı devrelerin dinamikleri için önemlidir. Burada, doygunluk devresi dönemi I_s de, diyotun karakteristik bir özelliği olarak dahil edilmiştir. Denklem sisteminin boyutsuz biçimi aşağıdaki şekilde yazılabilir;

$$\frac{dI_1}{dt'} = \frac{kT}{eL} + \frac{V}{L}\sin(\Omega t) - \frac{R}{L}\,(I_1 + I_2) \tag{2.8}$$

$$\frac{dI_2}{dt'} = \frac{kT}{eL}\ln\left(\frac{I_1}{I_s} + 1\right) + \frac{V}{L}\sin(\Omega t) - \frac{R}{L}\,(I_1 + I_2) \tag{2.9}$$

Burada, zaman ölçeklemesi $t' = \tau t$ olarak ele alınabilir ve $\tau = L / R$ gibi devre elemanlarının özellikleri ile τ belirlenir. Burada, τ devrenin doğal süresini temsil etmektedir ve $\Omega = \omega / \tau = \omega R / L$ şeklinde verilir.

2.7.1. R2L2D devresinin eşzamanlılığı

Belirli şartlar altında farklı başlangıç koşullarından başlayan senkronize iki kaotik sistemin olma olasılığı, eşzamanlılık senkorinazyona karşı koyan dinamik sistemlere bağlıdır. Her bir faz alanında aynı çekim noktasını ayrıntılarıyla planlandığı halde, faz alanındaki nerdeyse aynı başlangıç noktalarında başlatılan iki özdeş özerk kaotik sistemin, hızlıca ilintisiz hale gelen yörüngelere sahiptir. Dolayısıyla laboratuar ortamında özdeş, kaotik, senkronize sistem oluşturmak uygulamalı olarak imkansızdır (Pecora ve Carroll). Dolayısıyla, başlangıç koşulları ne olursa olsun kaotik eşzamanlılık senkronize elde etmek mümkündür. Kaotik eşzamanlılığı gerçekleştirmek için, iki kaotik sistem arasında bulunan bir birleştirme düzeninin olması gerekmektedir. Tek yönlü birleştirme olması halinde, bir kaotik devreden gelen sinyal (ana devre) ikinci bir kaotik devreye (bağlı devre) aktarılmaktadır. Dolayısıyla, kaotik sinyaller analog iletişim sistemlerinde olduğu gibi taşıyıcı sinyal olarak kullanılabilir.

R2L2D devresi, yukarı/aşağı süpürme davranışından dolayı genlik ve frekans rejimleri için ayarlanmıştır.(Erol Kurt ve Bingol, 2017).Bu anlamda, periyodik ve kaotik rejimler farklı frekanslar için birbirlerine karışırlar. Bu sebeple, besleme voltajlarına bağlı olarak dinamik rejimlerinin eşikleri için bir belirsizlik bölgesi tanımlamaktadır. Besleme voltajları rejimi etkilediği için, bu etki eşzamanlılık ve şifreleme çalışmaları açısından önemlidir. (Pecora ve Carroll, 1990).

Açık bir şekilde ifade edersek;(R2L2D)'nin eşzamanlılık senkorinazyonu sıradan RLD devresine göre, bizim çalışmamızda kullandığımız devre daha geniş bir

parametre bölgesine sahiptir. Literatürden açıkça görülüyor ki (B. KURT; Pecora ve Carroll, 1990), en iyi eşzamanlılık senkorinize performansı daha düşük frekanslar ve genlikler için elde edilebilir.

Deneylere göre, kaotik rejimler (Chua, Wu, Huang, ve Zhong, 1993) tarfından yapılan çalışmalardan da görüldüğü gibi maskeli sinyalin geri kazanımınıda etkilemektedir. Eşzamanlılık senkonizenin belirlenmesi, aşağıdaki gibi ana devre aracılığıyla tanımlanmıştır.

Ana fonksiyonun (M) sistem denklemleri aşağıdaki gibi oluşturulur,

$$\frac{d_x}{d_t}=f\big(x(t)\big) \tag{2.10}$$

Bağlı bir esir fonksiyon(S), aşağıdaki şekilde ulaşılan master ve durum denklemleri ile birlikte yazılabilir,

$$x=\begin{bmatrix}x_m\\x_s\end{bmatrix} \tag{2.11}$$

Bu sistemlerin dinamik formu aşağıdaki gibi özetlenebilir;

$$\dot{x}_m = g(x_m , x_s) \tag{2.12}$$

$$\dot{x}_s = h(x_m , x_s) \tag{2.13}$$

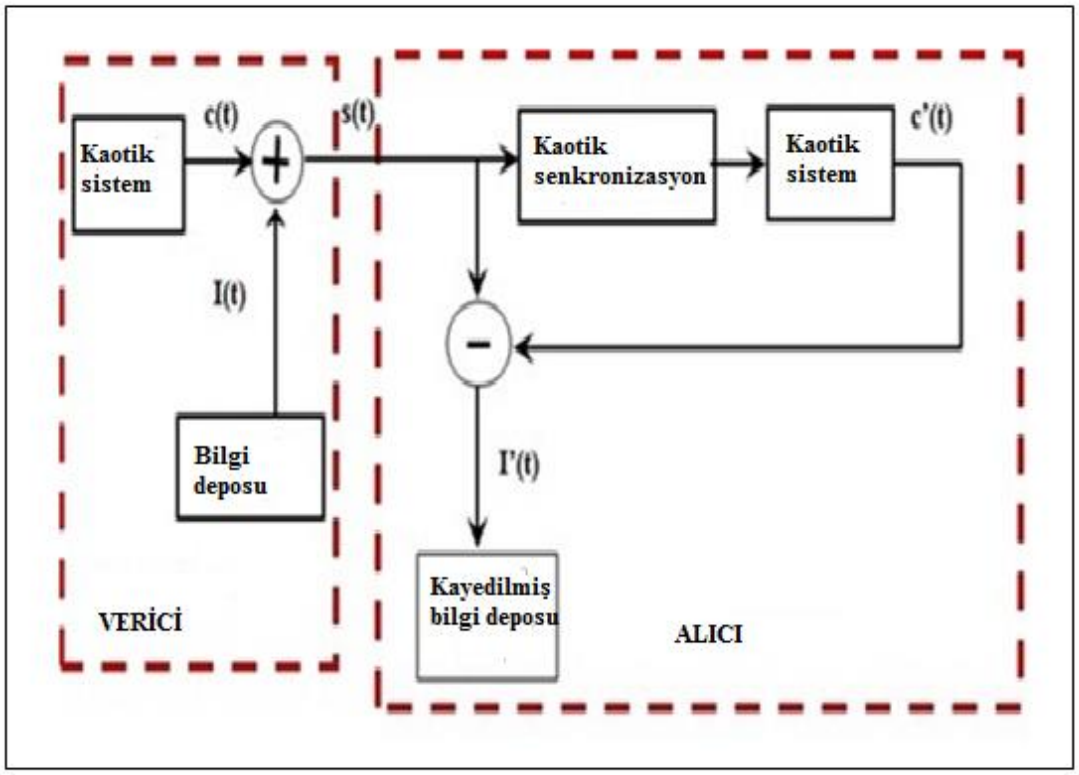
(Pecora ve Carroll, 1990) yöntemine göre, bağlı devrenin bir kopyası aşağıdaki gibi h ve g fonksiyonlarıyla ana devre ile birlikte çalıştırılabilir:

$$\dot{x}_m = g(x_m , x_s) \tag{2.14}$$

$$\dot{x}_s = h(x_m , x_s) \tag{2.15}$$

$$\dot{x}_s{}' = h(x_m , x_s{}') \tag{2.16}$$

Zaman sonsuza gittiğinde ve farklılık $|x_s - x_s'|$ sıfıra yaklaşırsa, x_s ve x_s' özdeş hale gelir ve eşzamanl senkorinazyon sağlanır.Kaotik maskeleme ve şifre çözme düzeni, Şekil 2.10 da gösterildiği gibi kaotik sinyal $c(t)$, imge pikselleri değerleri olan "Bilgi Verilerinin" düzenli dizisine eklenir, daha sonra da kaotik verinin çıkarılması ve imgenin şifresinin çözülmesi için alıcıya iletilir.



Şekil 2.10.Özerk olmayan kaotik blok diyagramı

Kaotik maskeleme bölümünde, bilgi sinyalini ve kaotik taşıma sinyalini birleştirmek için genellikle iki yöntem kullanılır Bunlardan biri, kaotik parametre modülasyonu ve diğeri ise mevcut çalışmada kullanıldığı üzere kaotik özerk olmayan modülasyondur.I(t) sinyali kaotik sistemin vericisi dahilinde bilgi sinyal ve maskelemesinin bazı parametrelerin ifade etmektedir.Alıcı kısmında, bağlı parça denklemine göre senkronize edilir.Dolayısıyla, eşzamanlılık syon hatası sıfıra yaklaşır.

Ana (m) master devre denklemleri şöyle verilmiştir;

$$\begin{aligned} \dot{x}_m &= \alpha \ln(x_m + 1) + \beta \sin(u_m) - z_m \\ \dot{y}_m &= -\alpha \ln(y_m + 1) + \beta \sin(u_m) - z_m \\ \dot{q}_m &= \left(\frac{L}{R} I_s\right) z_m \\ \dot{u}_m &= \Omega \frac{L}{R} \end{aligned} \tag{2.17}$$

Burada, *x* ve y devre akan akımları simgeler ve *z* besleme voltajının fazıdır.

Benzer şekilde, bağlı(esir) devre (s) için denklemler;

$$\begin{aligned} \dot{x}_s &= \alpha \ln(x_s + 1) - z_s \\ \dot{y}_s &= -\alpha \ln(y_s + 1) - z_s \\ \dot{q}_m &= \left(\frac{L}{R} I_s\right) z_s \end{aligned} \tag{2.18}$$

Bağlı devre (S), bağlı devrelerin iki dalı üzerindeki ana daldan q yük miktarını alır. Dolayısıyla, bu işlem şöyle açıklanabilir:

$$\begin{aligned} \dot{x}_s &= \alpha \ln(x_s + 1) - z_m \\ \dot{y}_s &= -\alpha \ln(y_s + 1) - z_m \\ \dot{q}_s &= \left(\frac{L}{R} I_s\right) z_s \end{aligned} \tag{2.19}$$

Güvenli iletişim, sinyalin şifresini çözmek için yüksek bir düzen eşzamanlılık syonu gerektirdiği için, x_s, y_s ve q_s ana devrenin ana akım kolu tarafından kontrol edilir. Bilgi sinyali sisteme iletildiği zaman, denklemler şu şekilde ifade edilebilir:

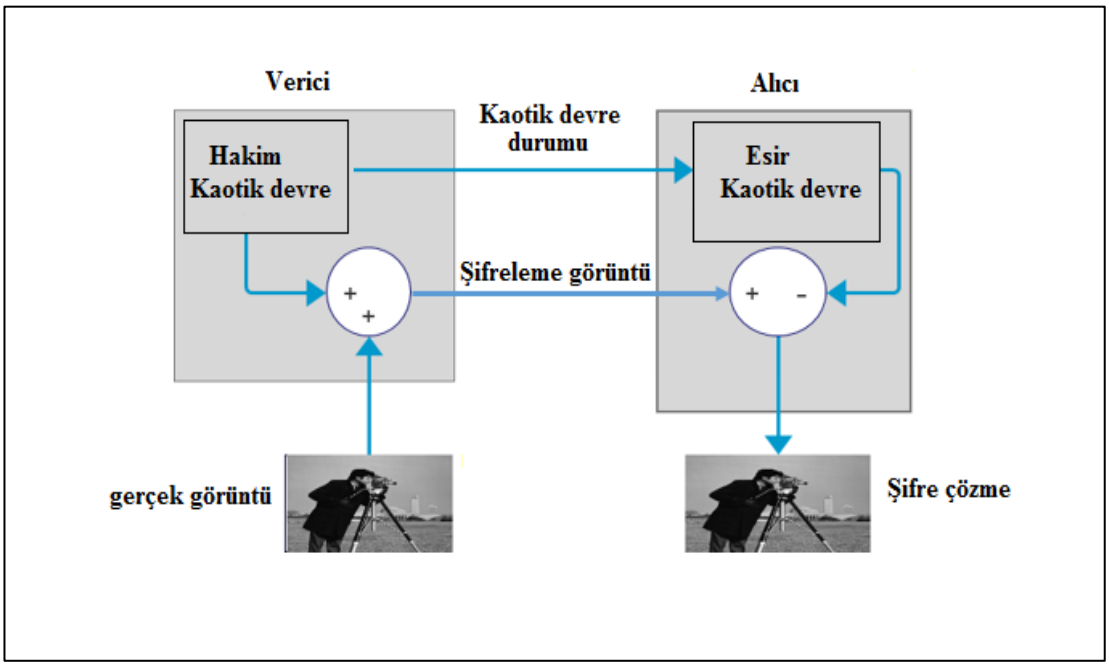
$$\begin{aligned} \dot{x}_s &= \alpha \ln(x_s + 1) - s(t) \\ \dot{y}_s &= -\alpha \ln(y_s + 1) - s(t) \\ \dot{q}_s &= \left(\frac{L}{R} I_s\right) z_s \end{aligned} \tag{2.20}$$

2.7.2. R2L2D devresinin güvenli iletişim sistemi

Bu çalışmada, herhangi bir imge verisi kaydetmeden (güvenli anahtarlar) güvenli imge transferinin gerekliliklerini yerine getirmek için (R2L2D) kaotik devresine dayanan yeni bir güvenli iletişim sistemi oluşturulmuştur.Bu çalışmada önerilen yeni

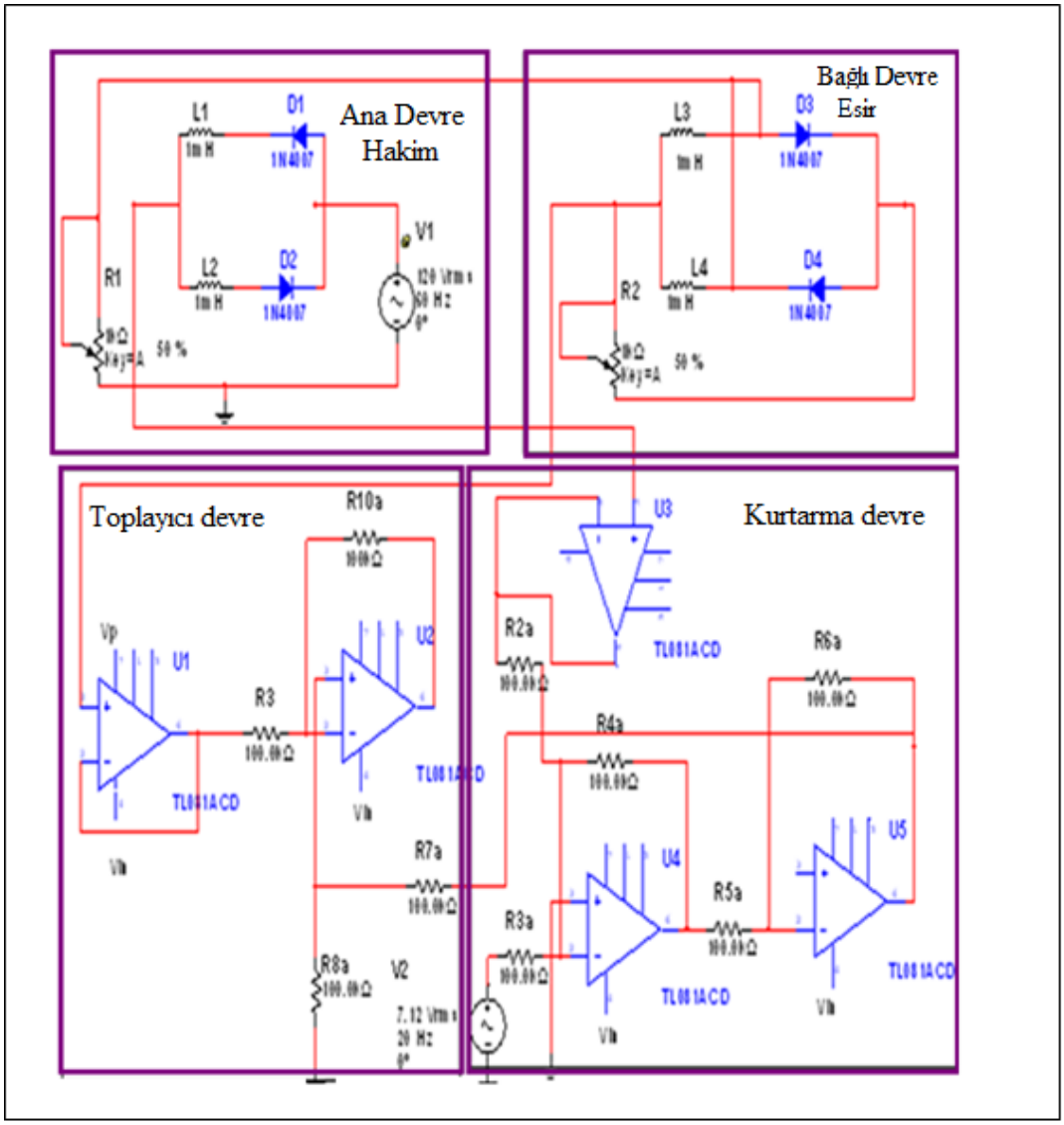
imge şifreleme tekniği, gerçek zamana dayalı bir teknik olduğu için, herhangi bir imgeyi veya güvenli anahtarı kaydetmeden güvenli imge aktarımına yönelik bir R2L2D kaotik devresine dayanmaktadır. Devre parametreleri, verileri geri kurtarmak için yeterlidir ve karşılayan tarafta başka hiçbir parametre, imge veya güvenli anahtara gerek duyulmamaktadır.

Kaos sistemi için sadece başlangıç parametreleri vardır ve orijinal değer için mantıklıdır ve öngörülemezdir. Şekil 2.11ve Şekil 2.12 de gösterilen güvenli imge şifreleme için yeni bir devre şema gösterilmiştir.

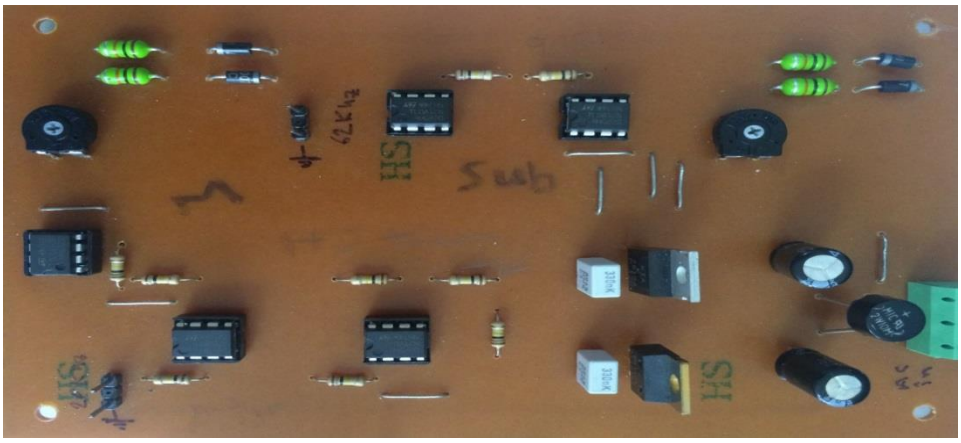


Şekil 2.11.Güvenli imge sistemi

Kaotik sinyal, Ana devrenin ana kolundan (M) başlamaktadır.Toplayıcı devre (Au) Ana Devreden (M) kaotik sinyal biçimi alır ve bunu bilgi sinyali I(t) ile birleştirir ve daha sonra maskeli sinyal kurtarma devresine (Su) aktarılır ve kaotik parça bağlı devre (S) vasıtasıyla çıkarılır ve temiz bir bilgi sinyali I(t) elde edilir.Şekil 2.12 da gösterildiği gibi, güvenli R2L2D sistem devresi için baskı devre Kartlarını (PCB) ifade etmektedir. Ana devre (M) ve bağlı devre (S), toplayıcı devre (Au) ve Kurtarma devresi (Su) gösterilmiştir. R2L2D analog kaotik devreleri NI Multisim yazılımında benzeştirilmiştir.Şekil 2.12 de uygun olarak deneysel devre sistemi ve Fotoğraf 2.1 de göstermektedir.



Şekil 2.12.Güvenli iletişim sistemi şeması



Fotoğraf 2.1.R2D2L devre sistemi

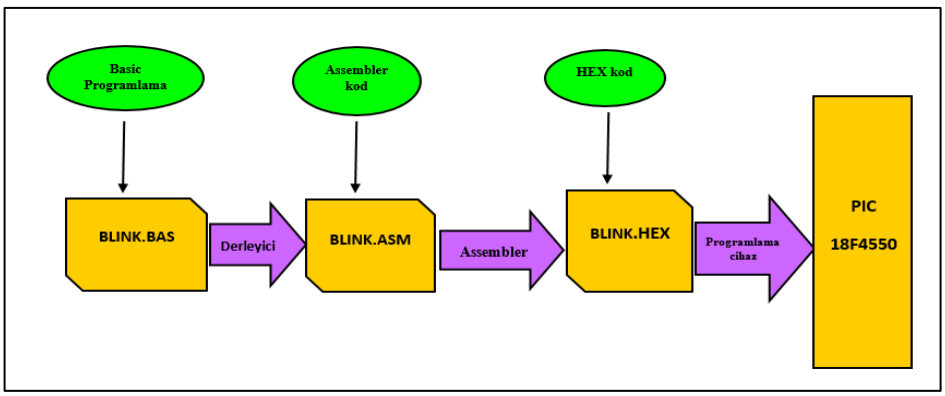
3. MALZEME VE ÖLÇME YÖNTEMLERİ

3.1.Malzemelerinin özellikleri

Öncelikle günümüzde bilgi iletimi ve yüksek güvenlik için şifreleme ve şifre çözme algoloritmaları sürekli ihtiyaç duyulmaktadır. Bu tezde önerilen yeni görüntü şifreleme tekniği, herhangi bir görüntüyü kaydetmeden güvenli görüntü aktarım için bir R2L2D kaotik devresine ya da gerçek zamanlı bir teknik olduğu için güvenli tuşlara bağlıdır.

Burada kullanılan devre elemanları veriler için yeterlidir. Alıcı için başka hiçbir parametre, görüntü veya güvenli anahtara ihtiyaç yoktur. Tez için gerekli olan 8 bitlik bir D/A (sayısal/anolog) çevirici olan DAC,sayısal formdaki girdi sinyalinin analog formdaki bir çıktı sinyaline dönüştürmek için kullanılan bir cihazdır.

Yine sayısal/anolog programlama için PIC18F4550 mikrokontrol sistemi temin edilmiştir Güvenli kaotik şifreleme sistemi için lisanslı Proton- BasiC- IDE programını satın alıp Şekil 3.1 de Fotoğraf 3.1 de gösterildiği gibi mikrokontol PIC18F4550 yükleyici yardımıyla transfer edilmiştir. Dönüşümü gerçekleştirmek için anahtar, dirençler , işlemsel yükselteçler ,BWR(ikili 0-1) durumu için özel direnç ve Şekil 3.2 de gösterilen ağırlıklı portatif dirençler(R-2R) ,DAC devresiyle birlikte temin edilmiştir.



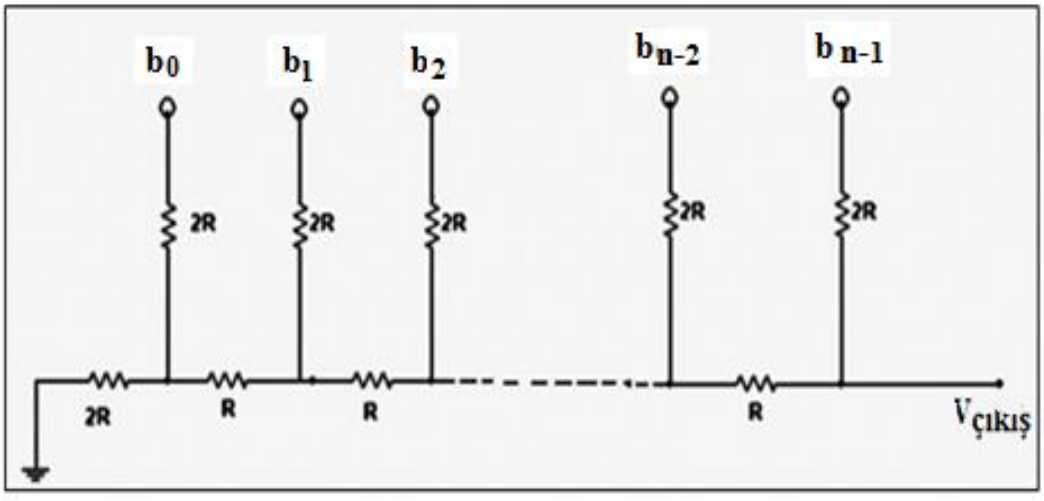
Şekil 3.1. Mikrokontrol PIC18F4550 programlama

Fotoğraf 3.1 de şifreleme sisteminin test edilmesi deneyleri esnasında, sadece program 32x32 gri imge değerleri için PIC 18F4550'i kullanılmıştır.

Programın mikrokontrolü PIC18F4550 aktarımı ise, Hex-dosyasının 18F4550 Pic mikro denetleyicisine eklenmesi ile gerçekleştirilmiştir. Burada Hex; ASCII metin formunda ikili sistemi ileten bir dosya formatıdır (Mohrem, Chetate, Guıa, ve Bougara).

R-2R (Singh, Sharma , 2017) devrenin analiz edilmesi için burada eşdeğer devreler uygulanmaktadır. Dolayısıyla, R-2R devresinin nasıl çalıştığı kolayca anlaşılabilir. R-2R devresi, paralel bir sayısal ismi veya kelimeyi analog bir voltaj değerine doğrudan dönüştürmektedir. Her bir sayısal girdi (b0, b1, v.b.), analog girdisine kendi ağırlıklı katkısını eklemektedir.

R-2R şebekesinin eşsiz ve ilginç özellikleri bulunmaktadır. İhtiyacımız olduğu Kadar herhangi bir gerekli sayıya göre ölçeklendirilebilir.Devrenin çıktısını kesin bir hale getiren sadece iki R ve 2R direnç değerlerini kullandığı için kolay oluşturulur. Bitlerin sayısının filtrelemeyi ve hatta analog sinyali işleyen devre tasarımını basitleştirmesi halinde, çıkış eşdeğer direnç R'ye eşit olur.

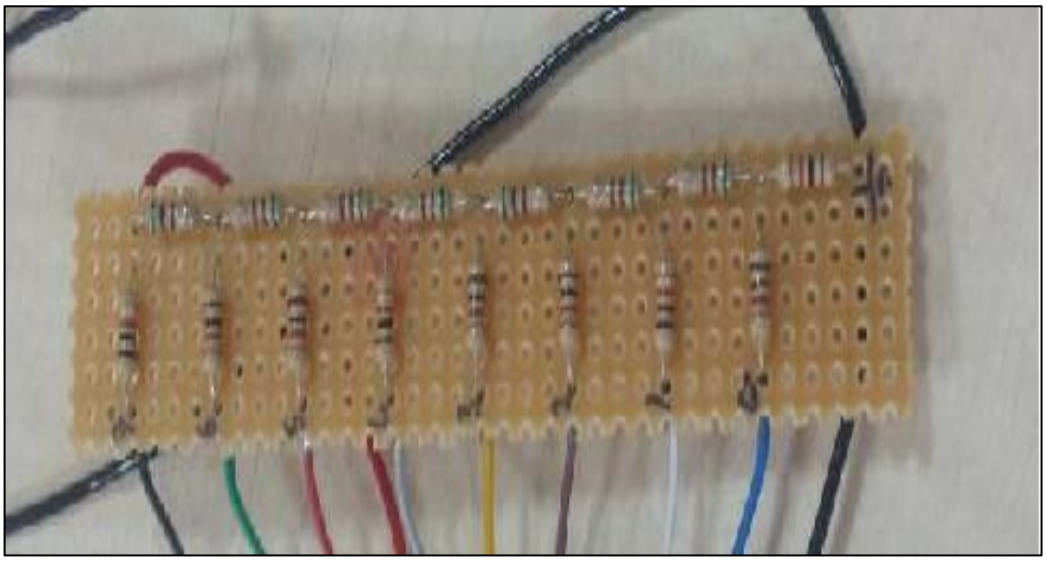


Şekil 3.2. İkili ağırlıklı R-2R dirençlerden oluşmuş merdivenler

Şekil 3.2 de devrede voltaj bölücü olan, çıkış gerilim ($V_{çıkış}$) değeri , b_i bit sayısı ve giriş gerilim($V_{giriş}$) değerine bağlı kalacak şekilde denklem 3.1 de belirlenmektedir.

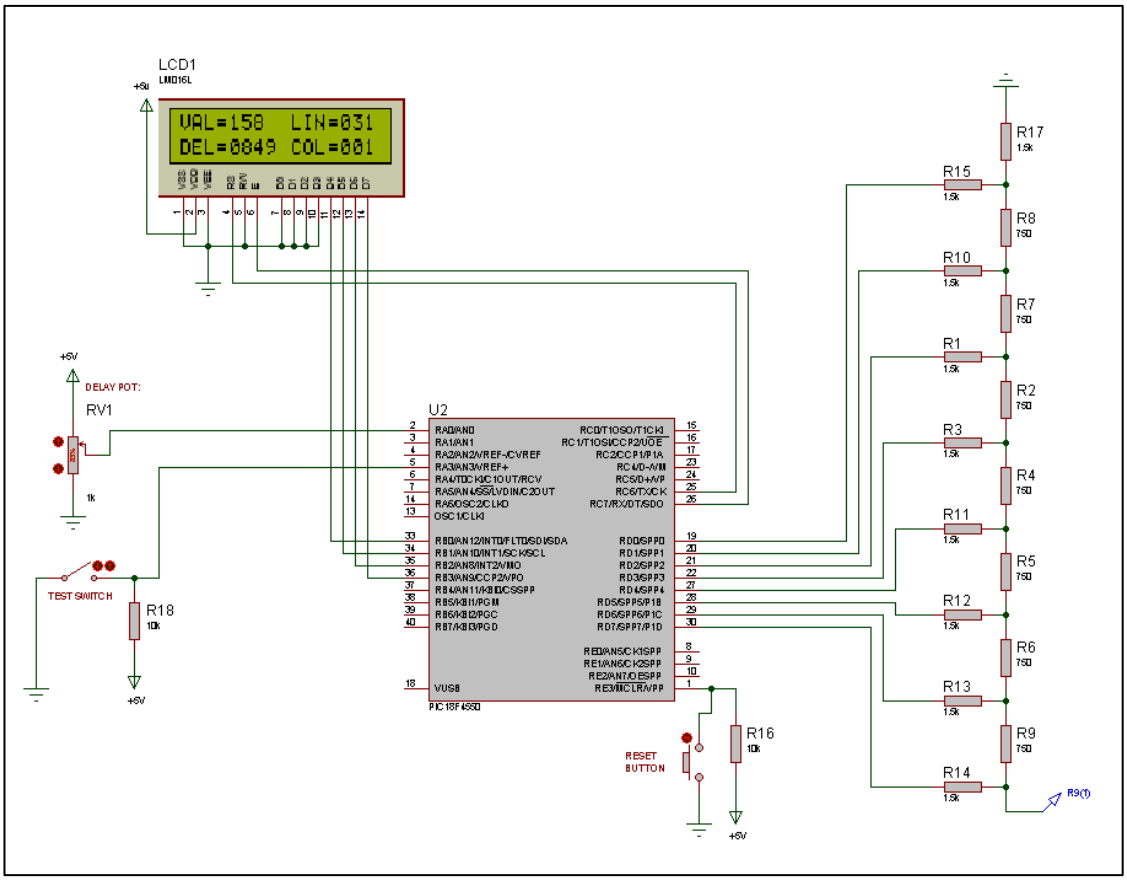
$$V_{out} = V_{giriş} \sum_{i=0}^{n} b_i \frac{1}{2^{i+1}} \quad (3.1)$$

Fotoğraf 3.1 de DAC (sayısal /anolog çevirici) 8bit (0-255) arasında imge durumunu gri tonlamalı piksellerle temsil etmektedir. Devremiz (R-2R) için burada R=0.5 KΩ ve 2R=1 KΩ şeklindedir.



Fotoğraf 3.1. DAC R-2R anolog/sayısal çevirici basamak devresi

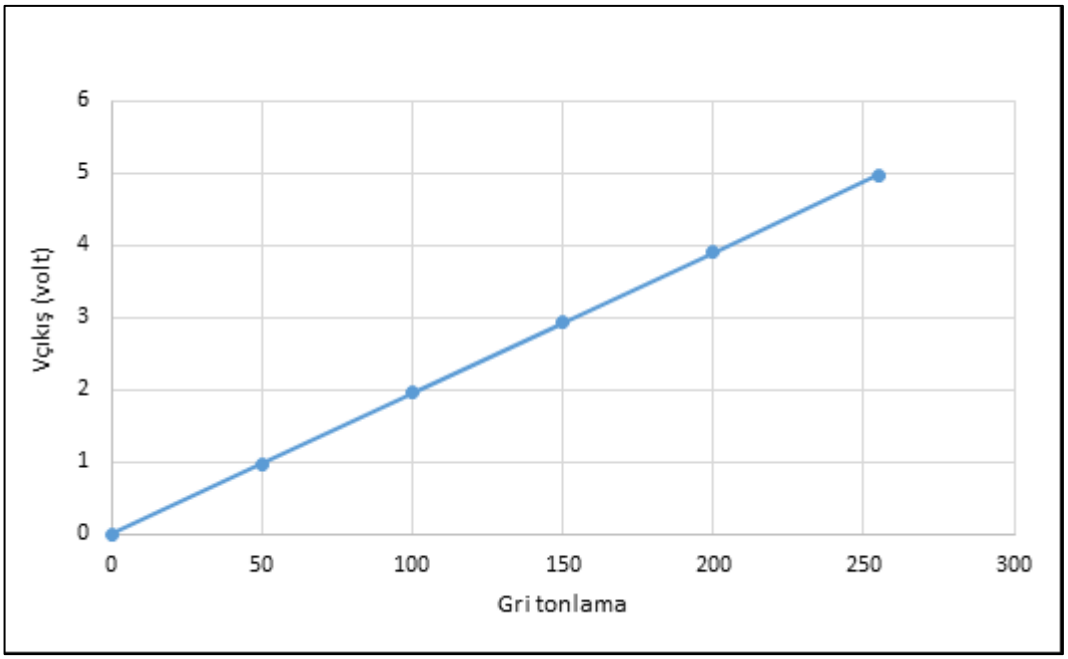
Girdi ölçeğindeki belirli bir değişimin ardından final değerinin (± 0.5) LSB (en az anlamlı bit) içine yerleşecek çıktı sinyali için süre gerekmektedir. İdeal şekilde, yeni bir ikil kelime DAC içerisine girdiği zaman analog voltajda anlık bir değişim meydana gelecektir. İmge gri tonlamalı pikselleri, Şekil 3.3 de gösterilen D/A simülasyon dönüştürücüsü kullanılarak (0-255) aralığında çıkış gerilimi (0-5V) aralığına dönüştürülür.



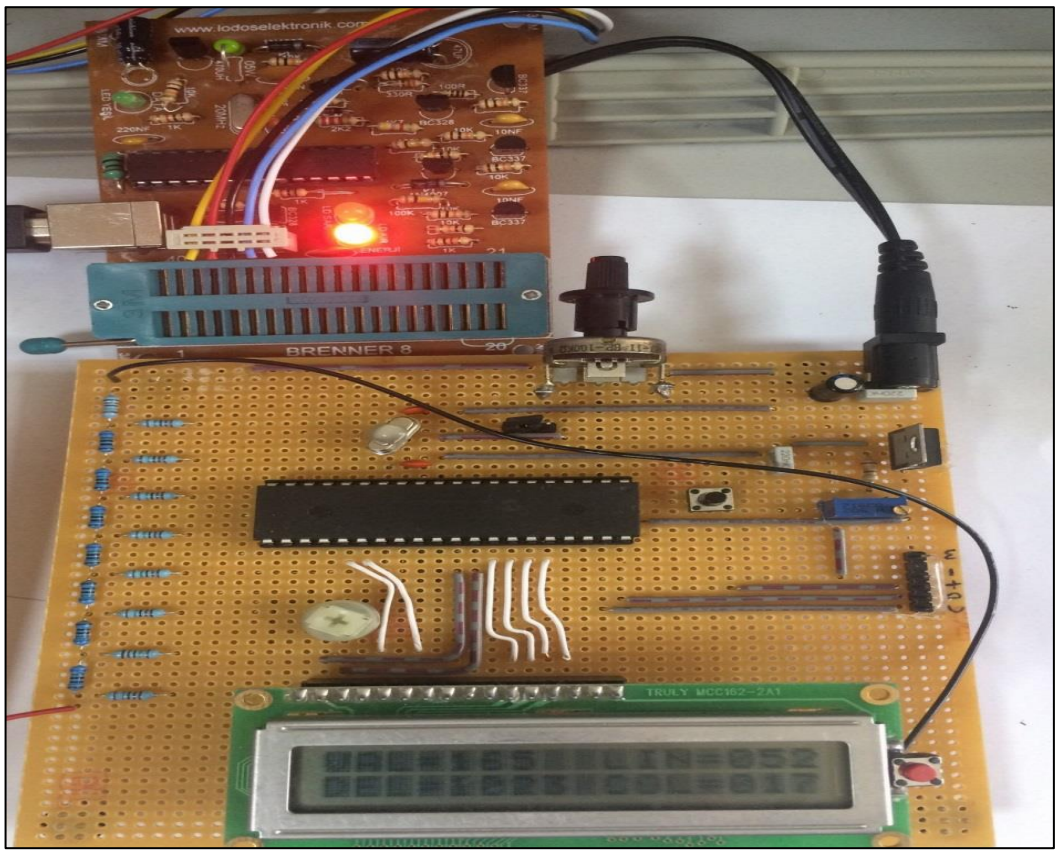
Şekil 3.3. 8 bitlik bir D/A dönüştürücü simülasyon şeması

Dönüştürücü, 5/255 = 0.0195 V olan bir aşama değeri ile 255 griden 5 volt değerine dönüştürmektedir.Çıktı genliği, ikili girdinin çoğalttığı aşama voltajı değerine eşit olmalıdır. Örneğin, Şekil 3.3 de binary sistemde verilen (129 =1000 0001) sayısı değerinden Vçıkış =129 x 0.0195 = 2.451V gerilim değerine ulaşırız.

Grafik 3.1. de D/A dönüştürücü için genliğe karşı gri değerleri gösterilmiştir.Burada, 8 bitlik D/A dönüştürücü simülasyon çıktı voltajına göre sonuçlanmıştır.Grafik 3.1 de gösterildiği üzere D/A dönüştürücü için voltaja bağlı olarak gri değerleri arasında doğrusal bir ilişkinin olduğu görülmektedir.

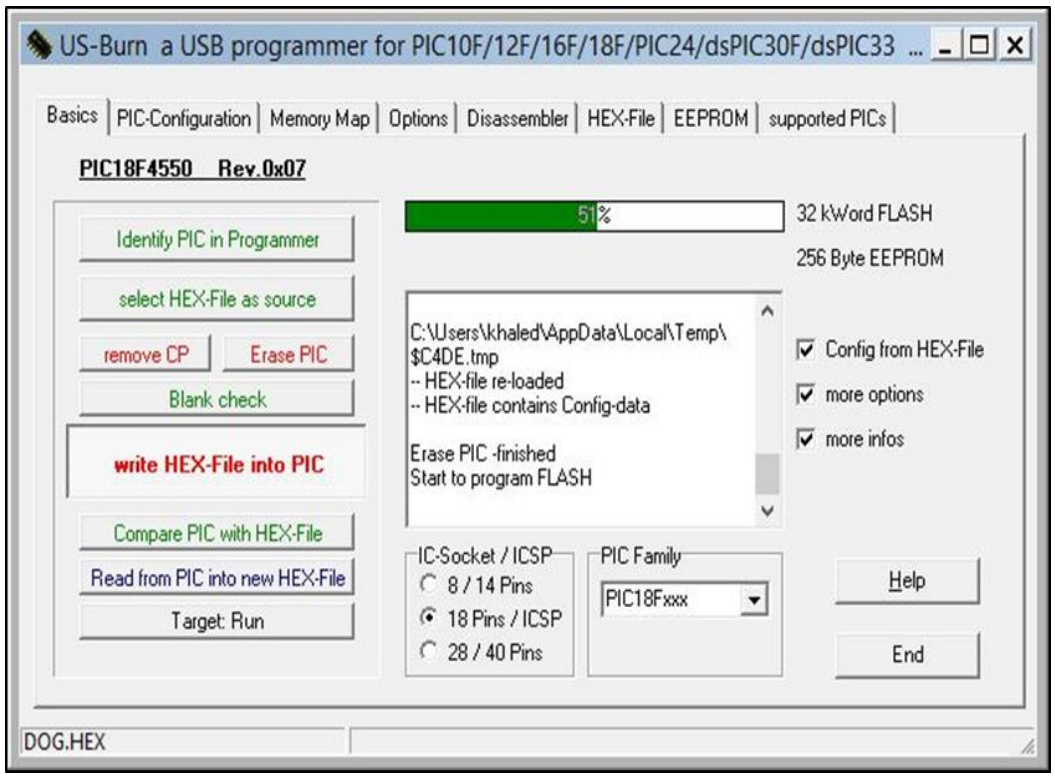


Grafik 3.1. D/A dönüştürücü için genliğe karşı gri değerleri



Fotoğraf 3.2. Donanım yükleyici programlama -pic18f4550

Bu forum EPROM ve diğer progranabilir mantık cihazlarını programlamak için yaygın olarak kullanılır.Hex- dosyasını Pıc 18f4550 ‘e yüklemek için kullanılan USB yazılımı Fotoğraf 3.2 de ve Fotoğraf 3.3 de 10F/12F/16F modelleri ayrı ayrı gösterilmiştir.



Fotoğraf 3.3.Hex dosyasını PIC -18 F4550 için kullanılan USB yazılımı

3.2.Anolog ve imge sinyalinin ölçümleri

3.2.1. Anolog sinyalinin ölçülmesi

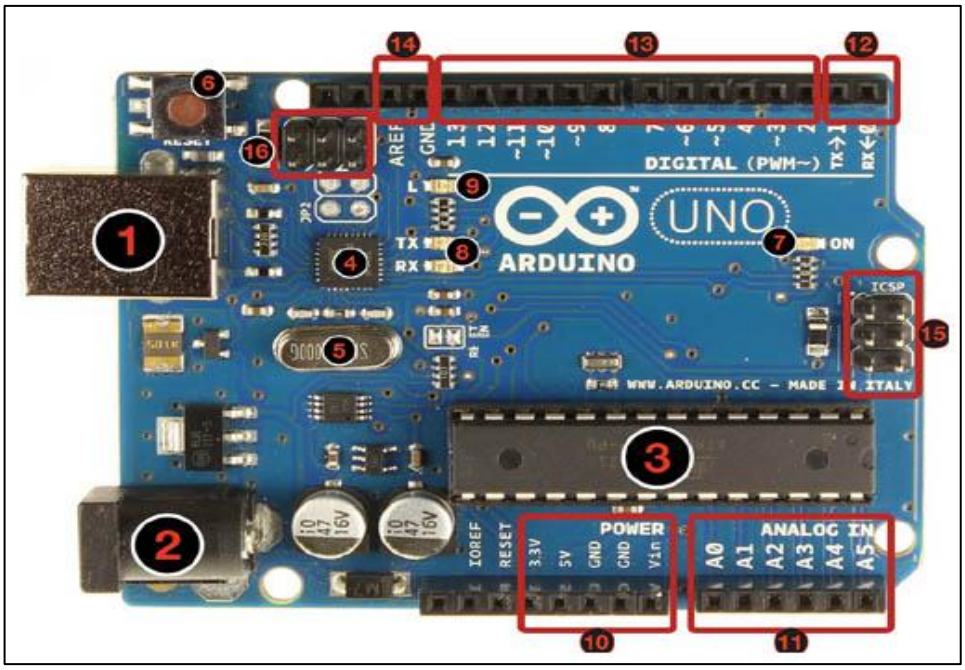
Tez çalışmasında, önerilen analog ölçümünün gerçekleştirilmesi için ARDUINO /UNO mikrokonrtrol devresi kullanılmıştır. Bu denetleyici ATmega328P tabanlı bir karttır.14 adet sayısal giriş/çıkış pini 6 anolog girişi, çıkışı 6 ve 16 Mhz kuvars kristeli USB ye sahiptir. Çalışmada kullanılan ARDUINO ön modeli, pek çok sinyal kontrolü türündeki çok kullanılan açık kaynak platformudur.Bu çalışmada, önerilen analog ölçümünün gerçekleştirilmesi için Arduino seçilmiştir.

Çünkü, bütün diğer avantajların arasında, MATLAB programında kullanmamızı olanak veren daha basit bir derleyiciye sahiptir. Bu da muhtemelen, çok sayıda uygulamada kullanılan en ticari platformdur. Fotoğraf 3.3 de gösterildiği gibi, Arduino Uno 6 giriş kapısına sahiptir. Arduino Uno bir USB kablosu ile bilgisayar bağlanarak çalıştırılabilir ya da harici bir güç kaynağından beslenebilir.

Harici güç kaynağı bir AC yada DC adaptör ya da batarya olabilir. Arduino Uno bir bilgisayar ile, başka bir Arduino ile ya da diğer mikrodenetleyiciler ile haberleşme için çeşitli imkanlar sunar. AT mega328 mikrodenetleyici, RX ve TX pinlerinden erişilebilen UART TTL (5V) seri haberleşmeyi destekler. Kart üzerindeki bir ATmega16U2 seri haberleşmeyi USB üzerinden kanalize eder ve bilgisayardaki yazılıma sanal bir com portu olarak görünür. 16U2 standart USB sürücülerini kullanır ve harici sürücü gerektirmez. Ancak, windows dosyası gereklidir.Kart üzerindeki RX ve TX ledleri USB den seri çipe ve USB den bilgisayara veri giderken yanıp söner.

Software-serial kütüphanesi Arduino Uno 'nun digital pinlerinden herhangi biri üzerinden seri haberleşmeye imkan sağlar. Ayrıca, ATmega328 I2C (TWI) ve SPI haberleşmelerini destekler.Kapıların sayısı, Arduino modeliniz ile çeşitlenmektedir. Fakat kodlama aynı kalmaktadır.

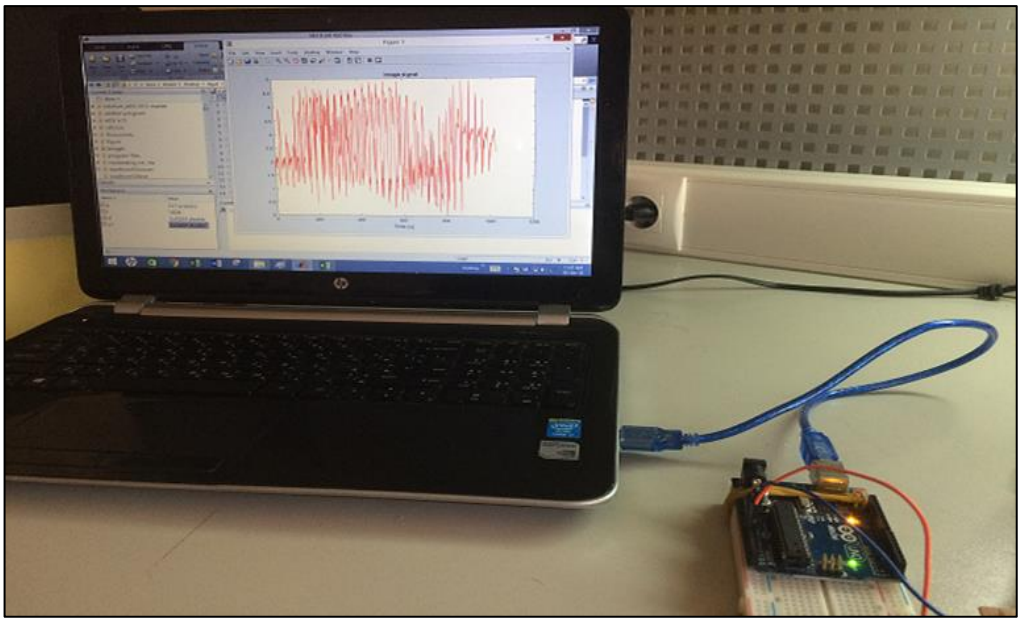
Analog girdilerindeki analog okuma uygun 10 bitlik (0-1023) sayısal değerlere dönüştürülür.Fotoğraf 3.4 de numarandırılan parçalar sırasıyla ;1- USB jakı, 2 - Power jakı(7-12v dc),3 -Mikrokontrol ATmega328, 4 - Haberleşme çipi, 5 – kristal 16 MHz,6 -Reset butonu, 7 - Power ledi,8 -TX / NX ledleri, 9 -Led, 10 -Power pinleri, 11 - Analog girişler, 12 - TX / RX pinleri,13 - Sayısal giriş / çıkış pinleri , 14 -Ground ve AREF pinleri, 15 -ATmega328 için ICSP ve 16 -USB arayüzü için ICSP ayrı ayrı gösterilmiştir (Banzi ve Shiloh, 2014).



Fotoğraf 3.4. Arduino Uno -6 giriş kapısı.

3.2.2. İmge sinyalinin iyileştirilmesi

İmge şifresini çözmek için, alıcı ortam için hiçbir koşul gerekli değildir. Sistem gerçek zamanlı olarak çalıştığı için, alıcı da maskeli imge sinyalinin doğrudan şifresini çözer.



Fotoğraf 3.5.İmge sinyalinin iyileştrilmesi

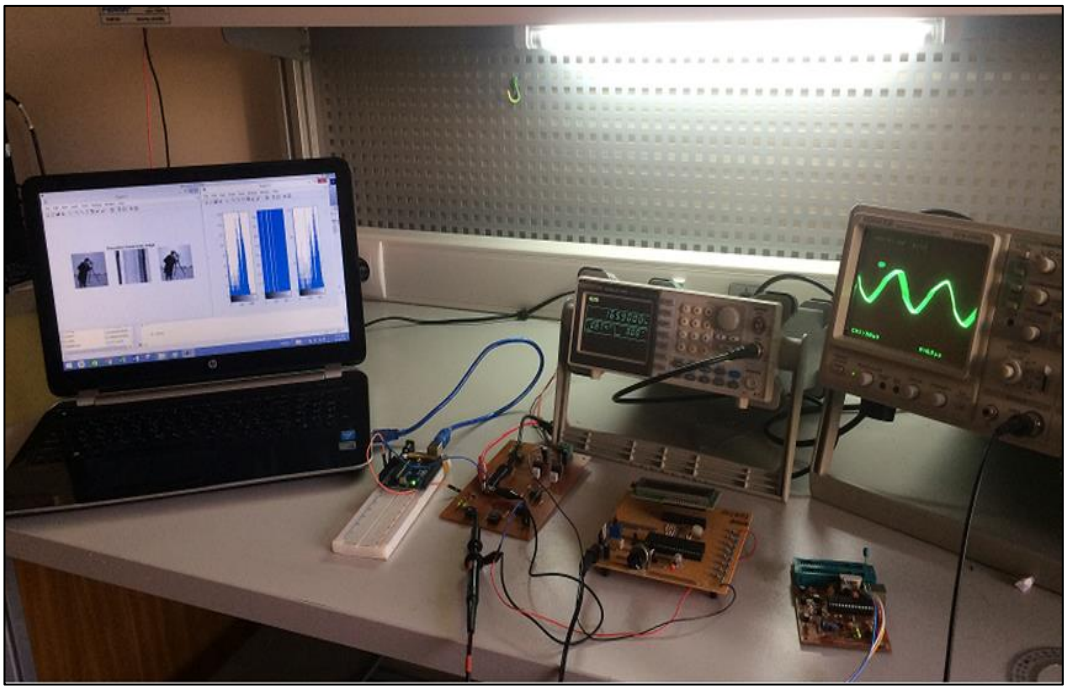
İmge sinyalinin kurtarılması, analog ölçümü olarak Fotoğraf 3.5 de gösterilen ARDUNINO/UNO -6 sistemi ile gerçekleştirilmiştir.

İmgenin şifresini çözmek için, alıcı ortam için hiçbir koşul gerekli değildir. Sistem gerçek zamanlı olarak çalıştığı için, alıcı da maskeli imge sinyalinin doğrudan şifresini çözer. İmge sinyalinin kurtarılması, analog cihaz ölçümü olarak "Arduino Uno" ile gerçekleştirilir. Fotoğraf 3.5 de gösterildiği şekilde MATLAB programı üzerinden sayısal değer dönüştürülür ve kurtarılır.

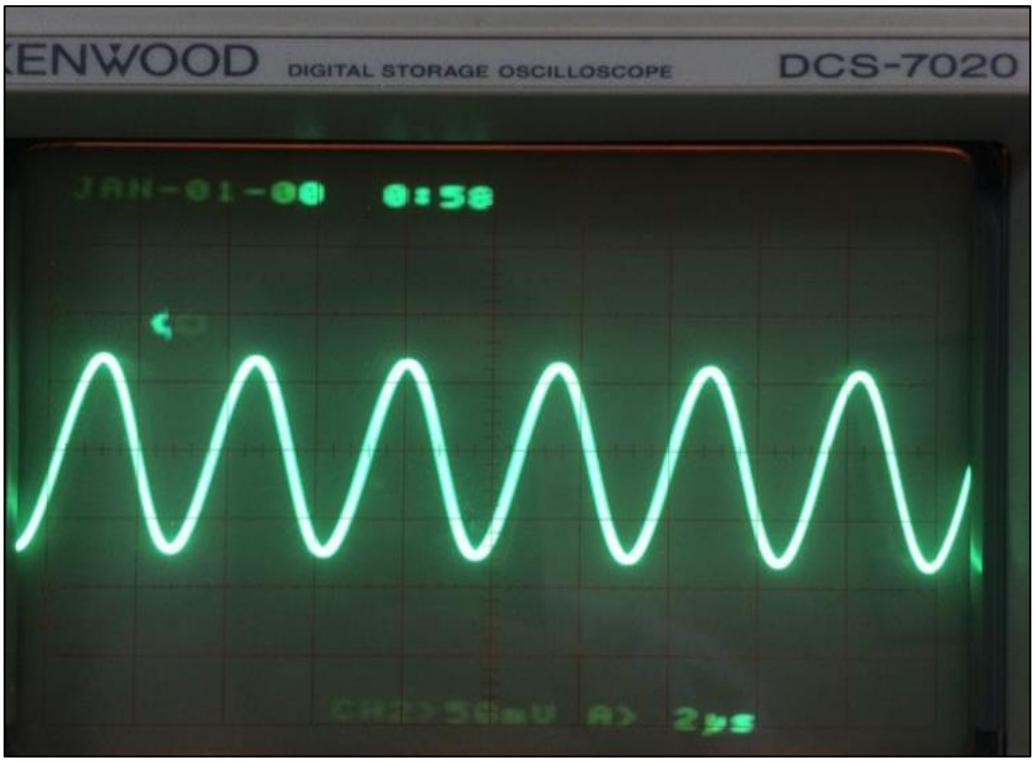
3.2.3.R2L2D Devresinde Kaos Devresi ile Giriş/Çıkış Sinyalinin Ölçülmesi

Bu çalışmada kullandığımız Anolog/Sayısal şifre çözücü deney düzeneği Fotoğraf 3.6gösterilmiştir.Deneydüzeneğimizde sinus dalgasının görünümü için *Kenwood-Dsb-7020* Osilloskop, anaolog sinyal ölçümü için *Ardunıno/Uno* mikrokontrol devre düzeneği, şifre çözücü için kullanılmıştır.

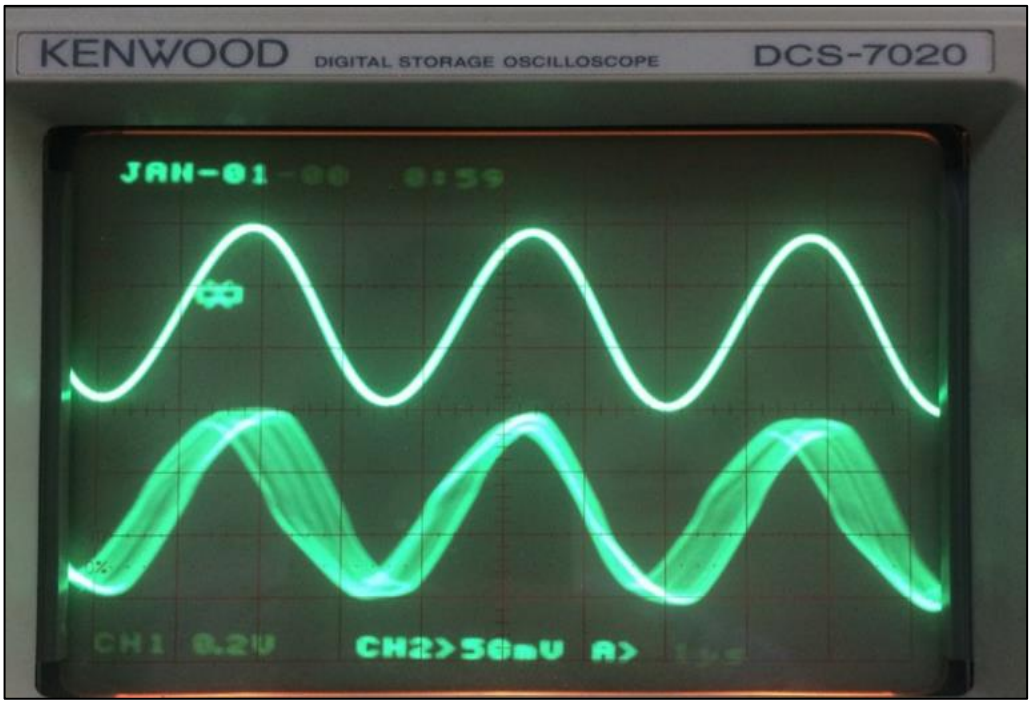
(R2L2D) bağımlı non-autonomous kaotik devre düzeneği, mikrokontrol için program sağlayıcı *Brenner-8/Usb Pıc* programalyıcı, güç kaynağı (AC) kullanılmıştır. Sayısal/Anolog çevirici kaos sinyalini c(t) elde etmek için R2L2D devresinde kaos sinyali için başlangıç koşulu (frekans, genlik voltajı ve rezistans değeri) ana birimde yapılandırılmıştır.Başlangıç koşulu değeri,$c(\mathrm{t})$ sinüs dalgası ($\mathrm{f} = 195.9\ \mathrm{kH}\ , \mathrm{V} = 0.944\mathrm{v}$), R1=1kΩ, R2=1kΩ şeklindedir.Fotoğraf 3.5 de ana devre için girdi sinyali iken ve Fotoğraf 3.6 de ise hem giriş hemde kaotik sinyali göstermektedir.



Fotoğraf 3.6. R2L2D devresinde kaos sinyalinin ölçüm düzeneği



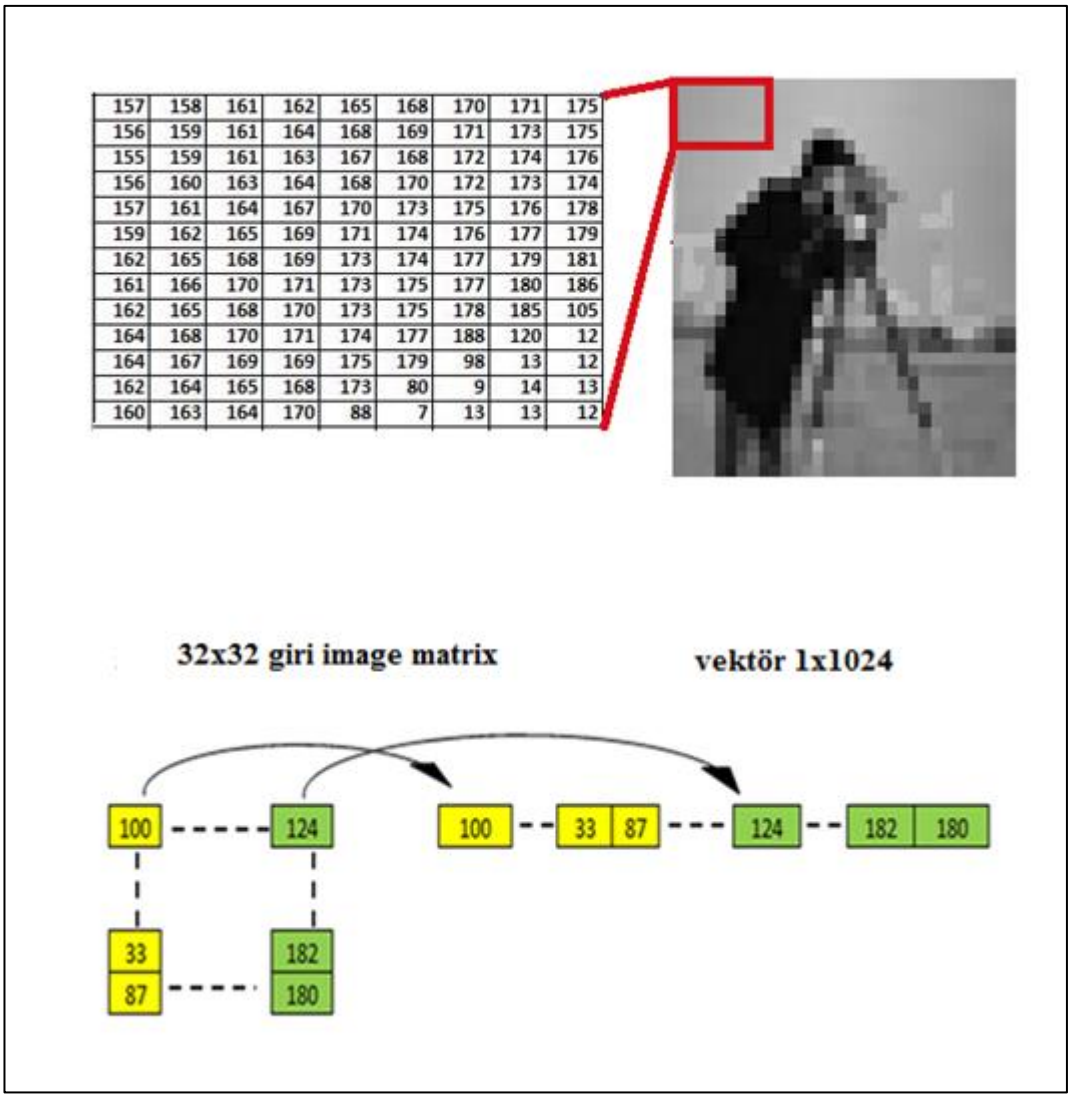
Fotoğraf 3.7.Master devresinde sinüs sinyalinin uygulanması



Fotoğraf 3.8.Osilaskopta çıkış kaos sinyalini elde edilişi

3.2.4. Dönüştürülen ve Gönderilen İmge Gri Şifreleme Aşamaları

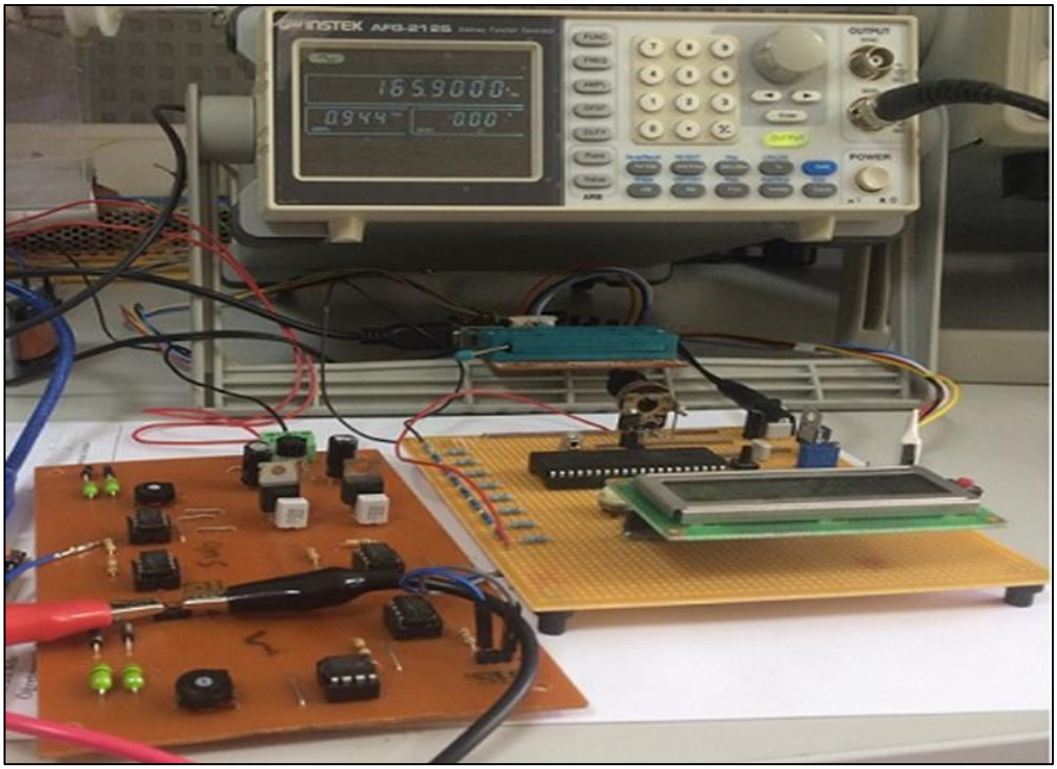
Bu bölümde, 32x32 olan imge boyutu için giri imge değerlerini okumak için lisanslı MatLab-R2016 programı kullanılmıştır.MatLab-R2016 programında imgeler kullanıldığı zaman, uygunsuz bir sorun meydana gelebiliyor. "Imread", kullanılmadan önce çift ve yeniden ölçeklendirilmiş hale dönüştürülmesi gereken 8 bitlik imge verilerine çevrilir. MxN metrisinin 1x(MxN) vektörüne dönüştürülmesi, sütuna göre metris sütununu okuyarak gerçekleştirilir. Şekil 3.4 de herhangi bir imgenin,32x32 olan matrix giri çift numaralı boyut değerlerini göstermektedir. Şekil 3.4'de 32x32 gri image matrisinin 1x1024 tipi vektöre dönüştürülmesini göstermektedir.



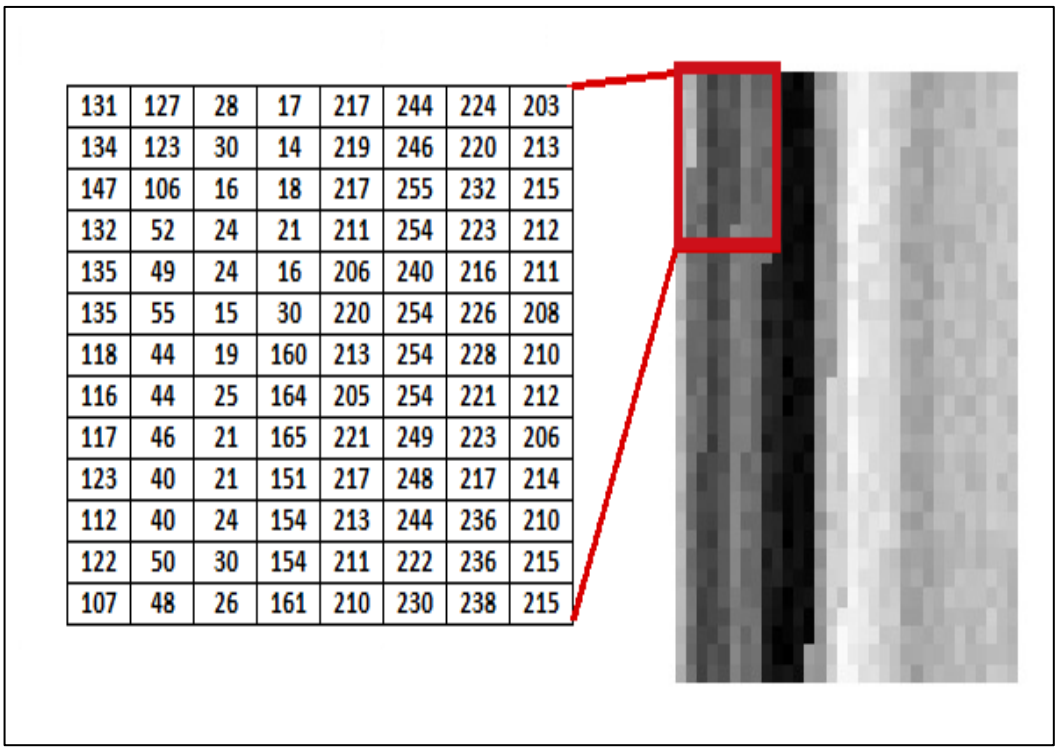
Şekil.3.4.32x32 matrisinin 1x1024 vektörüne dönüşümü

Fotoğraf 3.10 de 8.bit D/A dönüştürücü, R2D2L güvenli devre, dalga üreteçini göstermektedir.Sinyal jenatöründen görülen sayısal değerler başlangıç koşullarını göstermektedir.Başlangıç da; f=195.9 KHz, V=0.944 volt olup dirençler sırasıyla hakim (R1=1 KΩ) ve esir (R2=1 KΩ) verilmiştir.Bu değerler sistemin şifresidir.Eğer başlanğıç değerler değişirse sistemin kaotik durumu bozulmaktadır.

Ekleme işleminden sonra, şifreli sinyal s(t) güvensiz kanal üzerinden gönderilir. Şekil 3.5 de şifreleme için çıktı değerleri sinyal olarak gösterilmiştir.Bu matrisin MatLab-R2016 programının uygulanmasının sonucu gösterilen imge ortaya çıkmıştır.



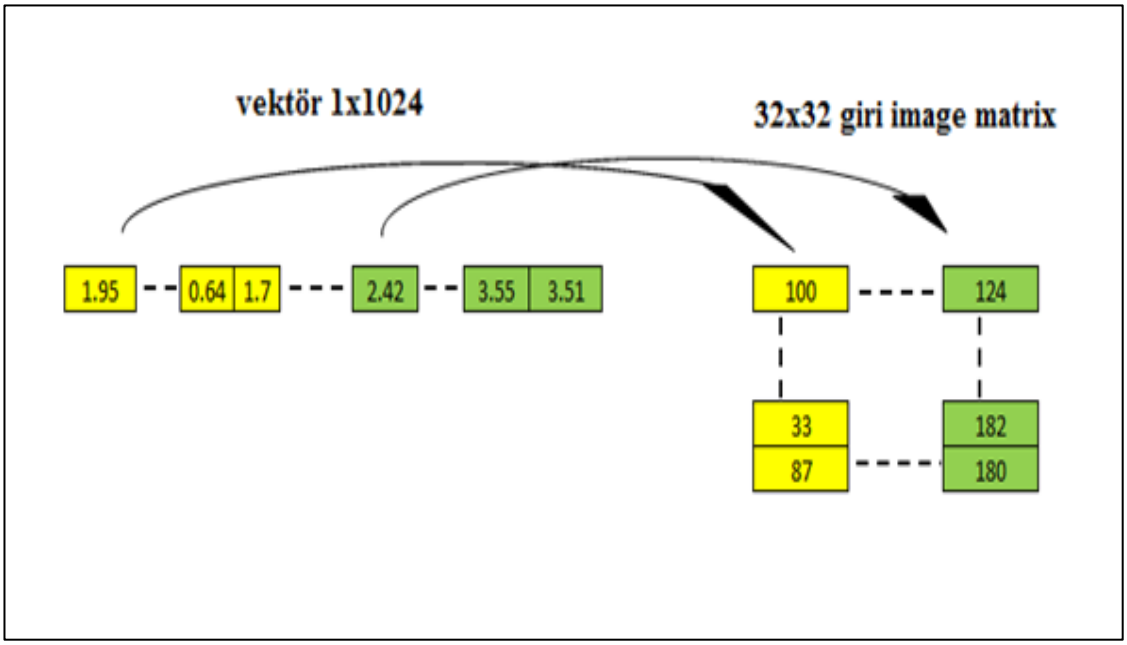
Fotoğraf 3.9.Toplayıcı ve D/A dönüştürücüsü verici devresi



Şekil 3.5.32x32 matrisinin 1x1024 vektörüne dönüşümü

3.2.5.Şifre çözme aşamaları

Şifre çözme, şifreli imgenin orijinal açık imgeye dönüştürülmesi aşaması olan, şifrelemenin ters yapısıdır. Şifreli imge alıcı ortama aktarıldıktan sonra, şifresinin çözülmesi gerekir. İmgenin şifresini çözmek için, alıcı ortam için hiçbir koşul gerekli değildir. Sistem gerçek zamanlı çalıştığı için, alıcı da maskeli imgeyi doğrudan deşifre edecektir. Şekil 3.6 da gösterilen imge voltaj vektörü 1x1024 voltajları, 32x32 imge gri matris boyutuna dönüştür.



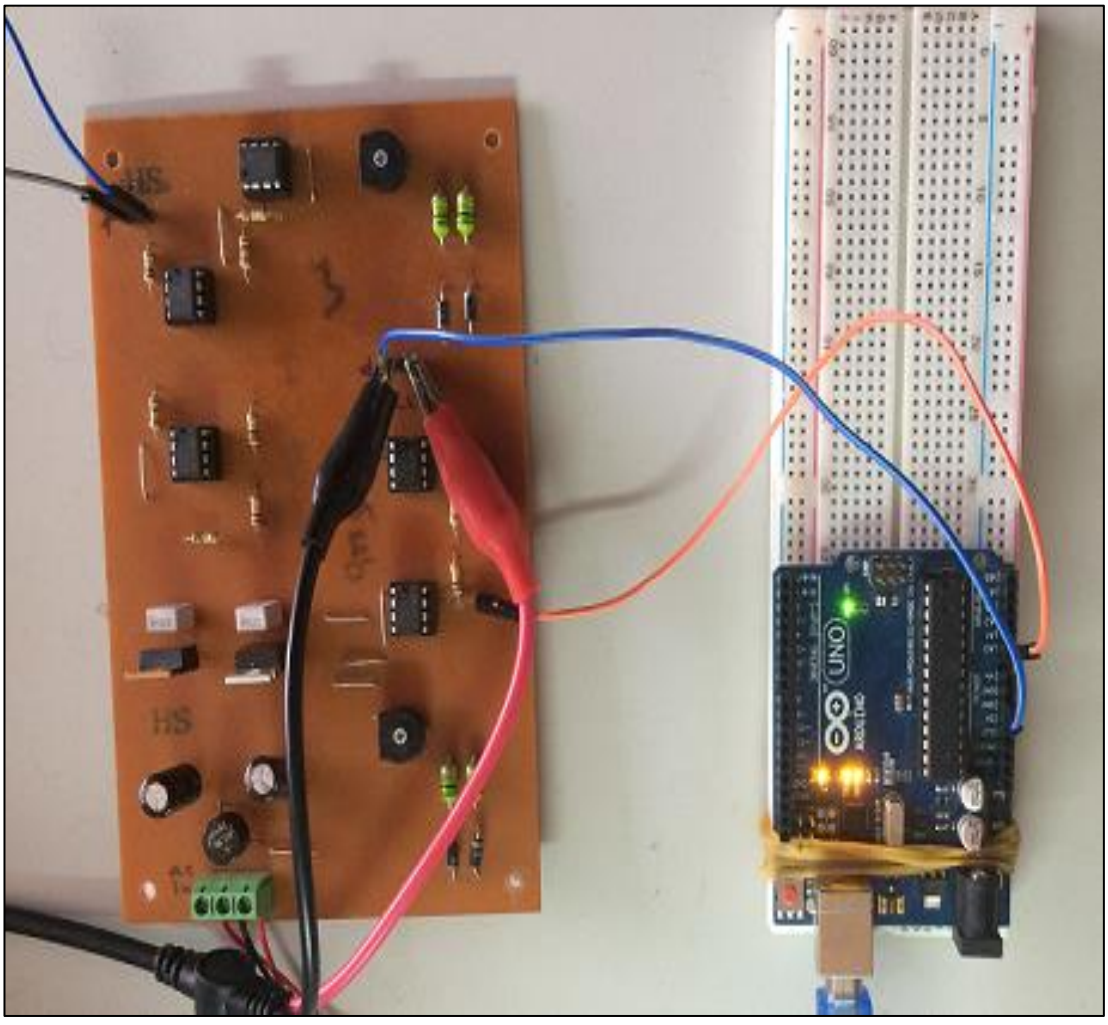
Şekil 3.6. Imge 1x1024 voltaj vektörünün 32x32 matrisine dönüştürülmesi

Fotoğraf 3.12 da Matlab R2016 program yardımıyla şifre çözmek için çıkarma devresinden analog sinyalinin ölçülmesini göstermektedir.Analog voltaj değeri, çıktının çıkarma biriminden çıkarma biriminden alınan analog sinyal çıkarılır ve MatLab tarafından hazırlanan veri dosyasında saklanır.Bu aşamadaki önemli nokta ise, aynı girdi değerleri türüne sahip olacak doğru analog sinyali değeri sıralamasını elde etmek için, Arduino ve MathLab programı arasında eşzamanlı kılmak gerekliliğidir. Analog gri imge ölçeği metrisinin sayısı, imge boyutuna dayalıdır bu

nedenle de imgenin şifresinin çözülmesi için bilmeniz gereken bir diğer koşul olarak görülmelidir. Bir diğer yandan, Arduino Uno kullanımının bazı dezavantajları vardır.

Analog sinyalini okuma “voltajı oku ( )” bazı hata değerleri veren aynı gürültüyü vermektedir.Bu nedenle gri imge değerlerini ölçerken % 5-8 aralığında hatayla karşilaşma olasılığımız vardir.

Bu şifre çözme imgesine yansımaktadır. Ancak bu durum maliyet ve programlama açısından iyi bir seçenektir. Gelecekte daha fazla doğruluk ile analog sinyalini ölçmek için kullanılabilecek daha başka pahalı bir cihaz bulunabilir.



Fotoğraf 3.10.Çıkarma devresinden analog sinyalinin ölçülmesi

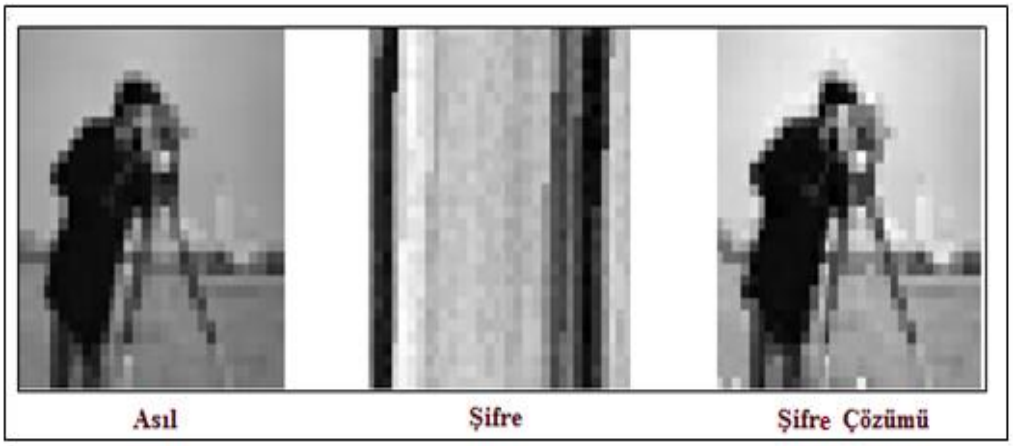
Veri dosyasını elde ettikten sonra, gri düzeyli değerlere dönüştürülür ve şifresi çözülmüş imge eldedilir. Gri düzeyler için voltaj değerlerinin bulunmasından sonra, gerçek gri düzeyli değerlere dönüştürülür, bu şekilde de şifresi çözülmüş imge son aşamada elde edilir.

4. BULGULAR VE DEĞERLENDİRMELER

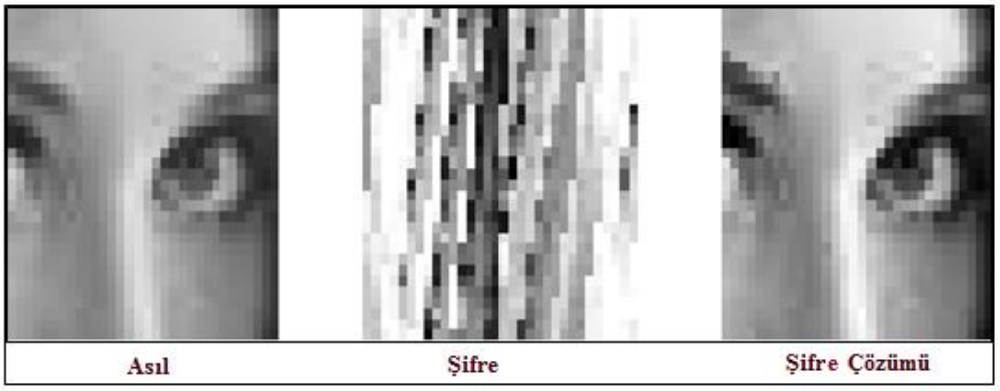
Bu bölümde, tez kapsamında yapılan herhangi bir gıri image (şekil ,fotoğraf v.b) durumlarını lisaslı MATLab R2016 bilgisayar programlamasına uygun hale getirilmiştir.Daha sonra R2L2D devresinde kaos sinyalinin ölçüm düzeneğiyini kullanarak ,D/A gıri imageleri 0-5 voltaj türüne 8 bitlik bilgisayar kodlarını Arduino UNO board yardımıyla ölçülrek uygun sinyallere dönüştürülmüştür.Şifreli imgelerle ve histogram analiziyle ilgili testler, açık kanaldan güvenli bir yolla iletişimi gerçekleştirmek için önemlidir. Ana devre olan (R2L2D) Hakim kaotik sinyal olarak başlangıç koşullarında sinyal oluşturak esir alicisina gönderdildi.Başlanğıç koşulu olarak (genlik, frekans, gerilim v.b), $c(\mathrm{t})$ sinüs dalgası ($\mathrm{f} = 195.9\ \mathrm{kH}$, $\mathrm{v} = 0.944\mathrm{v}$), R1=1kΩ, R2=1kΩ şeklindedir. Ayrıca şifre çözülmesi 32x32 matris dönüşümlerini ve gerekli bulgulara ilişkin elde edilen veriler, tablolar halinde sunulmuş ve tartışılmıştır.

4.1. Imge Şifreleme Çözümleme Analizi

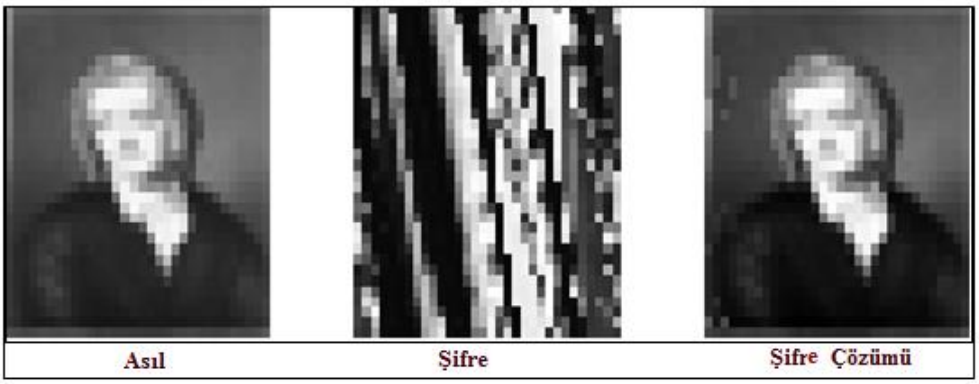
Bir imgenin şifresinin çözülmesi, çıkarma devresi aracılığıyla bir sinyal çıktısının okunmasının ardından gerçekleştirilir. Bu sinyalin gri değerlere dönüştürülmesi ve tam imgenin elde edilmesi, R2L2D kaotik image şifreleme yardımıyla Şekil 4.1a, 4.1b, 4.1c, 4.1d, 4.1e ve 4.1f de herbir fotoğrafın durumları gösterilmiştir. Dahası, 32x32 pikselli dağıtım ile birlikte diğer imgeler ile dikkate alınmıştır. Aşağıda gösterilen tüm imglerin boyutu 32x32 pikseldir.



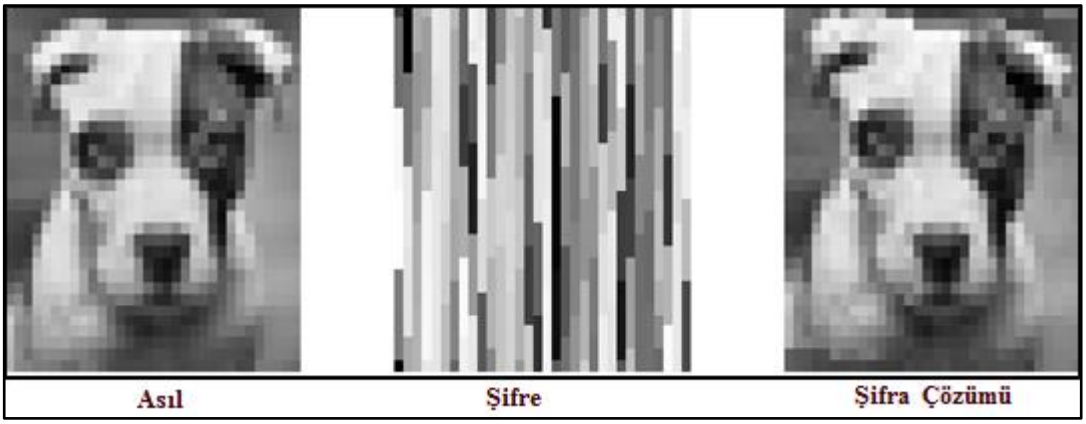
Şekil 4.1.a.Bir kameramanın asıldan şifre ve şifre çözümüne ulaşması



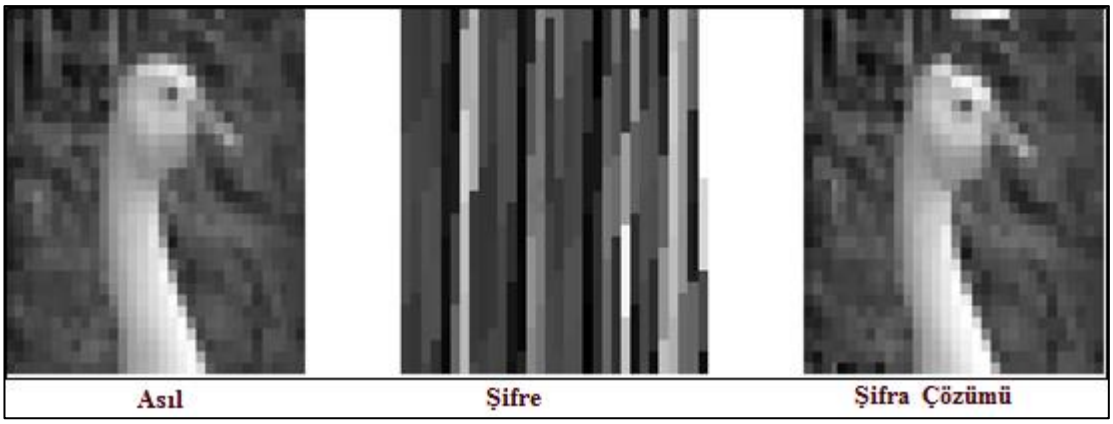
Şekil 4.1.b. Bir bayanın (Lena) yüz imagenin asıldan şifre ve şifre çözümüne ulaşması



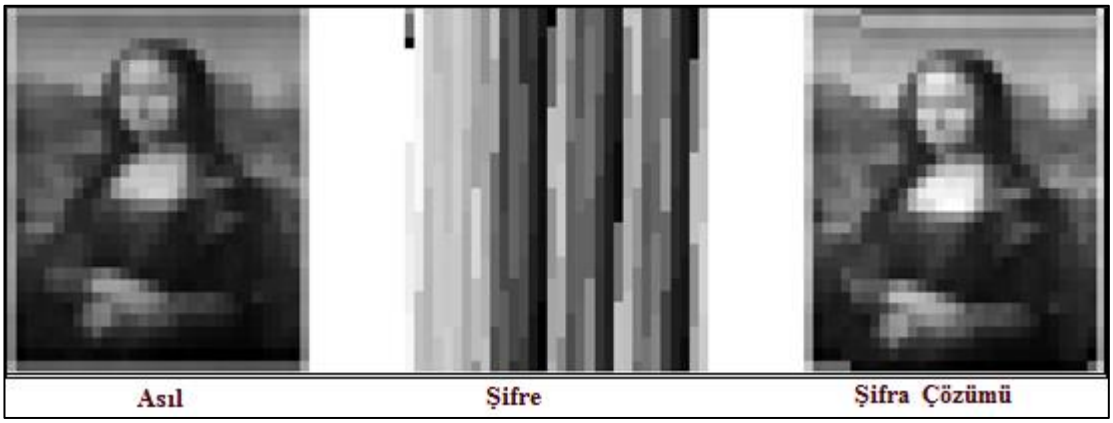
Şekil 4.1.c.Bir adamın fotoğraf portesinin asıldan şifre ve şifre çözümüne ulaşması



Şekil 4.1.d. Bir köpeğin asıldan şifre ve şifre çözümüne ulaşması



Şekil 4.1.e. Birördeğin asıldan şifre ve şifre çözümüne ulaşması



Şekil 4.1.f. Monalisa portesinin asıldan şifre ve şifre çözümüne ulaşması

Şekil 4.1.b de Bayan Lena nın imgesi 32x32 piksel değerlerinde bir kısmının, % 5 gürültü ile görülen imgeyi şifrelendiği gösterilmektedir.Şekil 4.1.c. de bir adamın imgesi 32x32 piksel değerlerinde bir kısmının, %7 gürültü ile görülen imgeyi

şifrelendiği gösterilmektedir. Şekil4.1.d. de bir köpeğin imgesi 32x32 piksel değerlerinde bir kısmının, % 4 gürültü ile görülen imgeyi şifrelendiği gösterilmektedir Şekil 4.1.d de bir ördeğin kafasının imgesi 32x32 piksel değerlerinde bir kısmının, %4 gürültü ile görülen imgeyi şifrelendiği gösterilmektedir.

Yine, Şekil 4.1.f. de Monalisa imgesi 32x32 piksel değerlerinde bir kısmının, %4 gürültü ile görülen imgeyi şifrelendiği gösterilmiştir.Tablo 4.1 de sıradağımız Şekil 4.1(a,b,c,d,e ve f) ye ait olan şifre çözme imgesindeki Piksel sayısı, doğru değer, yanlış değer ve % hatalarını göstermektedir.

Tablo 4.1.*Verilerin şifre çözme imgesinde hata yüzdesi*

İmge ismi	Piksel sayısı	Doğru değer	Yanlış değer	Hata yüzdesi
Kameraman imgesi	1024	1008	16	2%
Lena imgesi	1024	1015	9	1%
İnsan imgesi	1024	1003	21	2%
Ördek imgesi	1024	909	115	11%
Köpek imgesi	4095	3975	120	3%
Mona Liza	4095	3958	137	3%

İmgelerin şifrelenmesinin kalitesi, işlemlerin gönderilmesine ve okunmasına bağlıdır. Aslını söylemek gerekirse, analog devresinden verilen ve alınan sinyal orijinalliğini kaybedebilir, bu sebeple de, belirli bir hataya neden olabilir. Dolayısıyla, dönüşüm devresinin kalitesi ve bağlantısı, maskeleme ve yeniden kurtarma açısından imge kalitesini karşılamak için çok önemlidir.

4.2. Histogram Analizi

Bu bölümde, histogram analizler, piksel ilgileşim testleri ve hata ölçümleri gerçekleştirilmiştir. Histogram analizi, imge şifrelemeyi ölçen unsurların güvensiz kaynaklara ve rakiplere bilgi sızıntılarını engellemesi bakımından önemlidir. Bir görüntü işlemi analizinde görüntünün histogramı normal olarak piksel yoğunluğu değerlerine bağlıdır. Histogramı test etmek için, asıl (orjinal) ve şifreli imgeler ele alınmıştır. 8-BİT giri tonlamalı görüntü için 256 (0-255) farklı olası yoğunluk vardır.

Böylece gri tonlama değerleri arasında piksel dağılımını gösteren 256 rakamlı grafiksel durum söz konusudur. Şifreli imgelerin histogramları, orijinal imgelere ilişkin herhangi bir bilgi türü getirmez. Herhangi bir yetkisiz kişinin bu imgelerin şifresini çözme çabası bu anlamda başarılı olamayacağı için, iletişimde güvenli imgeler olarak kabul görebilirler.

Histogram ölçümlerinden sonra, Şekil 4.2a, 2b, 2c, 2d, 2e, 2f, 2g, 2h, 2i, 2j, 2k ve 2l de MATLab R2016 bilgisayar programı ve kaotik R2D2L şifreleme devresinde (Hakim-Esir) eşzamanlı sinyal analiz sonuıçları nın istatistik analizleri histogram şeklinde asıl ve şifre çözülmesi durumları gösterilmiştir.

Şifreli imgelerin, iyi şifrelemeyi kanıtlayan daha fazla dağıtılmış histograma sahip olduğu dikkate alınmalıdır. Histogramlardan yola çıkarak,özellikle Şekil 4.2d ve Şekil 4.2g için çoğu güçlü şifrelemelerin gerçekleştirildiği görülmektedir. Aslına bakarsak, asıl imge kümelenmiş ani gürültüler şeklindedir, şifreli imgeler bütün gri düzeylere daha kapsamlı biçimde dağıtılmaktadır.

Ayrıca, bu kümelenmiş görüntüler yok edilerek asıl imgelerin histogramlarından farklı bir hal alır. Şekil 4.2 de yatay eksen, giri seviyesini (0=siyah - 255=Beyaz) belirlerken,düşey eksen image durumunun şiddetini vermektedir.Şekil 4.2a asil (orjinal) iken Şekil 4.2b de şifre çözülmüş halini göstermektedir.Burada Şekil 4.2a, 4.2c, 4.2e, 4.2g, 4.2i ve 4.2k asıl (orjinal) histogram dağılımları gösterirken, Şekil 4.2b, 4.2d, 4.2f, 4.2h, 4.2j ve 4.2l ise şifrelerin histogramlarını göstermektedir. Bu Şifrelenmiş görüntülerin histogramları asıl (orjinal) görüntülerle ilgili herhangi bir bilgi vermez. Çünkü histogram dağılımları normal bir dağılımdır.

4.3. Piksel Korelasyonu

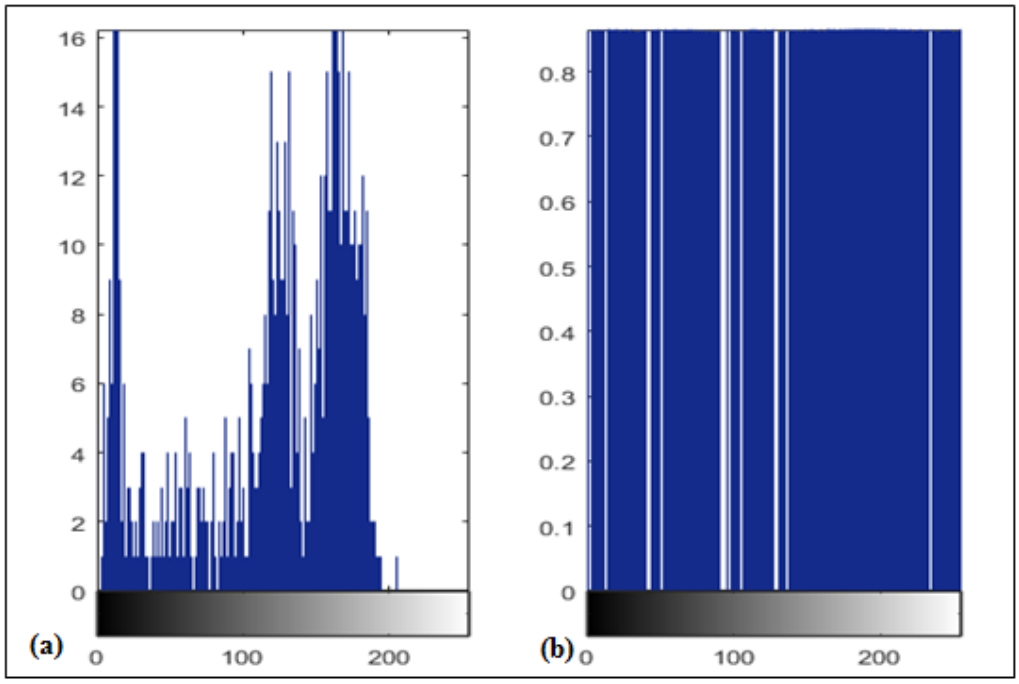
Korelasyon (ilgileşim) iki değişken arasındaki ilişkiyi değerlendirmek yollarından en sık karşılaşılanıdır. Bir değişken arttığında diğeri de artıyorsa pozitif, birinin artıp diğerinin azaldığı durumda ise negatif ilşki söz konusudur. Sayısal (sayısal) imgelerde genellikle, civardaki pikseller arasında yüksek bir korelasyon ilişki sözkonusudur. Tanıma göre, iyi şifreleme sistemler bu korelesyon azaltmaktadır, bu da istatistiksel saldırılara karşı büyük bir savunma haline gelmektedir.

Kovaryans değişkenlerin hareket yönünü gösterirkenkorelasyon iki değişkenin birbirine ne kadar benzerlikte hareket ettiğini gösterir. Farklı imge boyutları için şifreli piksellerin ilgileşim katsayıları, hem orijinal hem de şifreli imgeler için hesaplanmıştır. Veri korelesyon, korelesyon katsayısı olan ρxy olarak tanımlanır, x (bağımsız) ve y (bağımlı) veri gruplarıdır ve μ ise standart sapma açısından ortalama değerdir, Bu nedenle x,y değişkenleri ile ilişkilidir, p değeri bire daha yakın olacaktır. (Pozitif bir ilgileşim, bir değişken yükseldikçe, diğerinin de artacağını ve ya tam tersi düşeceğini ifade etmektedir).

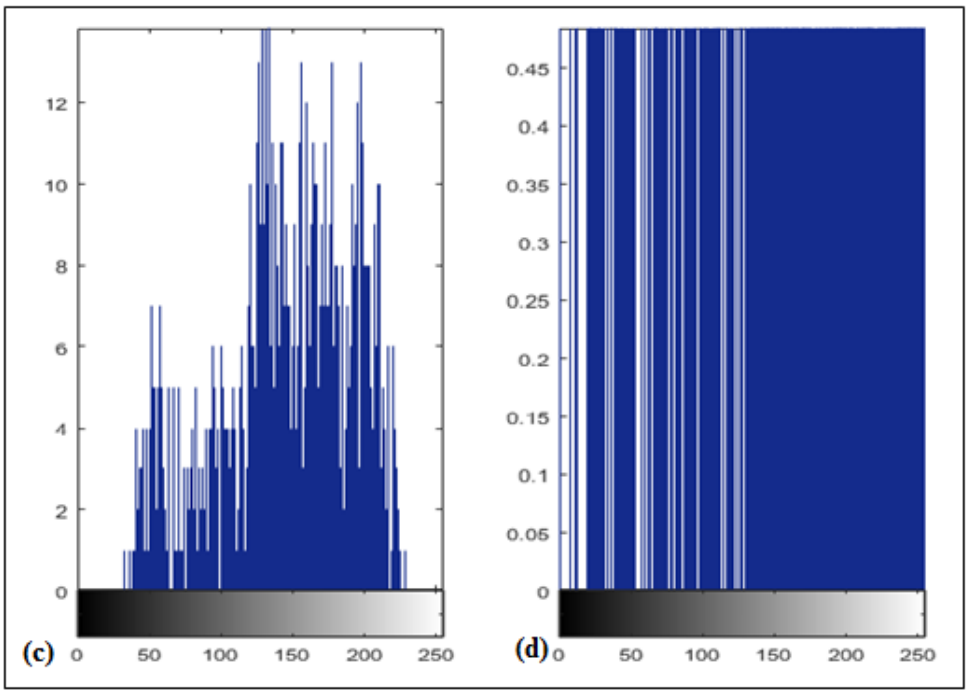
p değeri sıfıra daha yakın olursa aksi doğru olur (sıfır, değişkenlerin ilişkili olmadığını göstermektedir). Korelasyon bağıntısı aşağıdaki denklemle verilmiştir.

$$\rho_{x,y} = \mathrm{Cor}(X, Y) = \frac{\mathrm{cov}(X,Y)}{\sigma_X \sigma_Y} = \frac{E((X-\mu_X)(Y-\mu_Y))}{\sigma_X \sigma_Y} \quad (4.1)$$

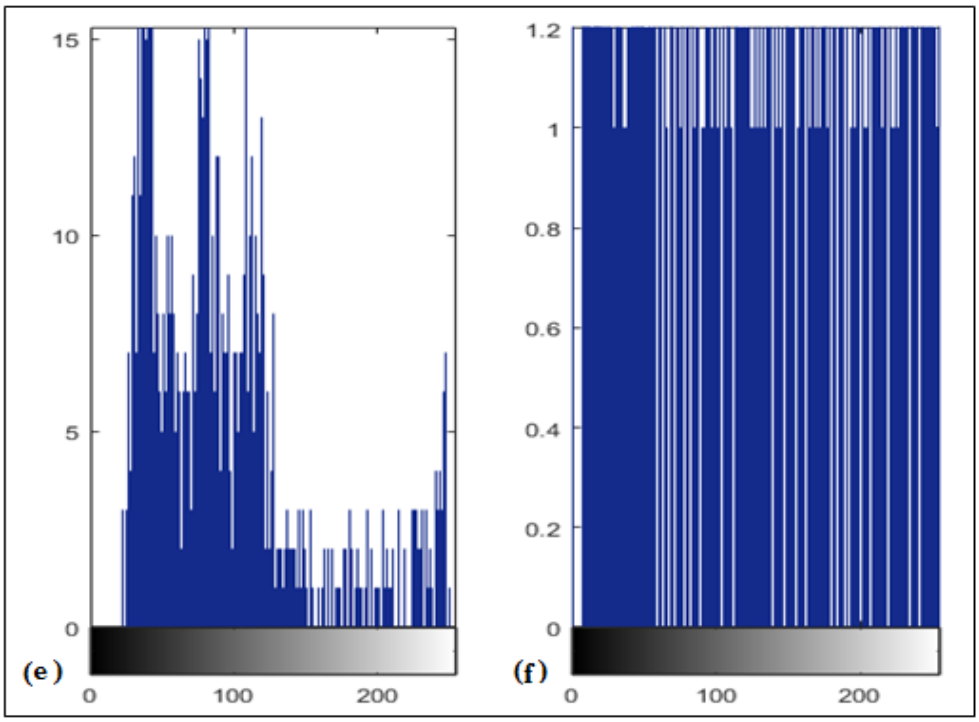
Yukarıda ifade edilen formülde, E beklenen değerdir. Burada, Cor korelesyon temsil ederken Cov ise kovaryansı temsil etmektedir.



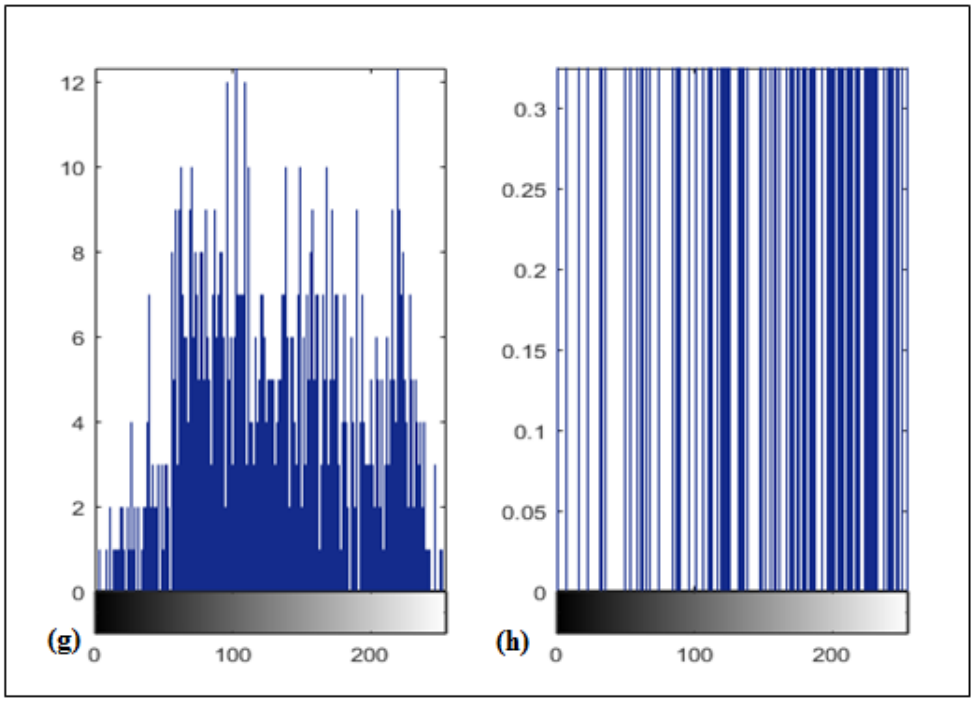
Şekil 4.2.(a,b).Bir kameramanın ait asıl-şifre /asıl-şifre çözümlerinin histogramı



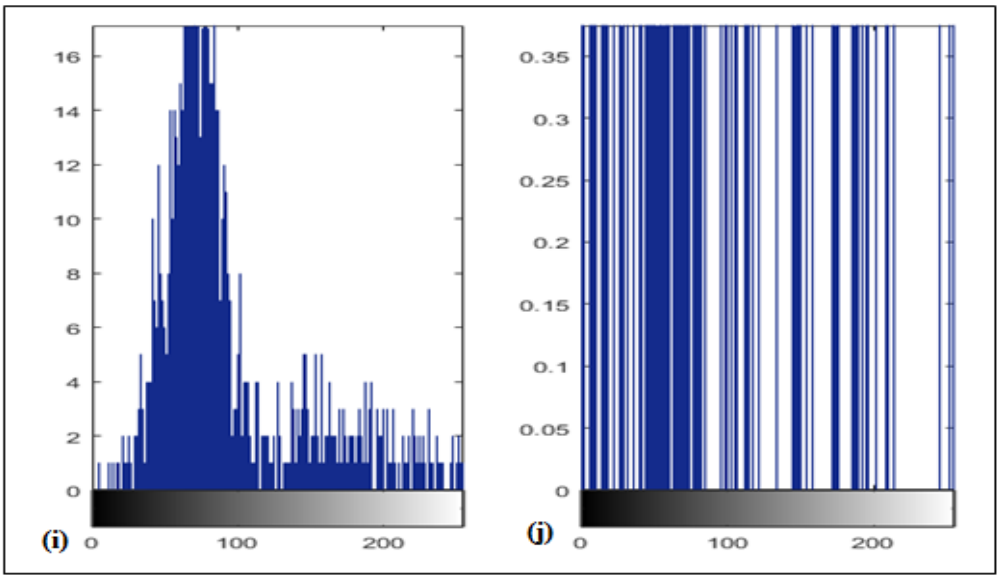
Şekil 4.2.(c,d).Bayan Lina ya ait asıl-şifre / asıl-şifreçözümlerinin histogramı



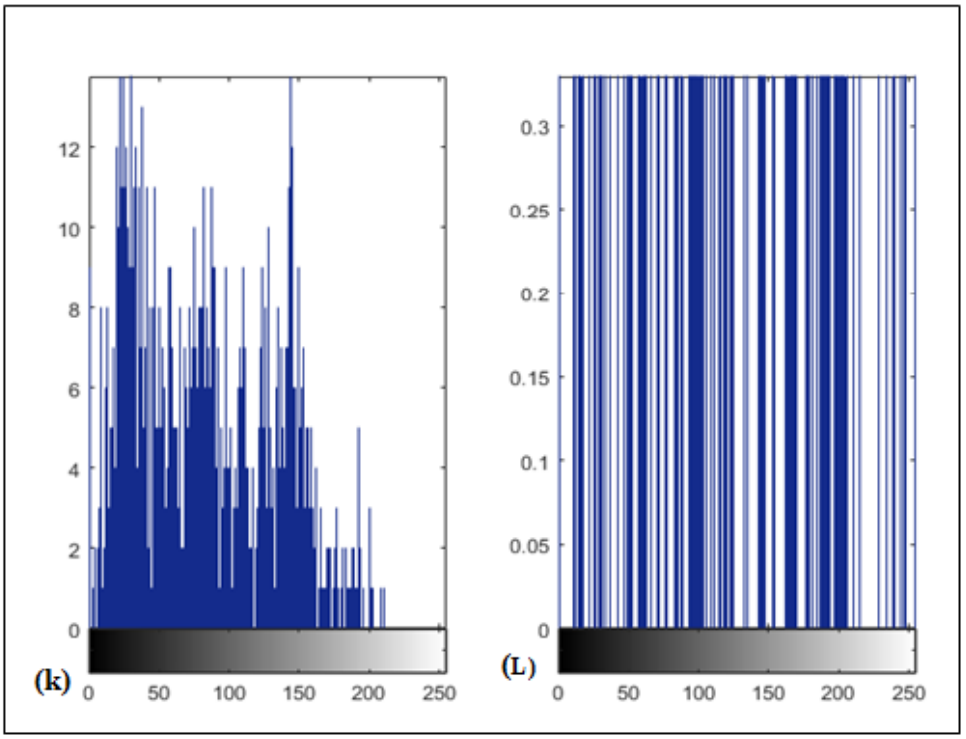
Şekil 4.2.(e,f).Bir adama ait asıl-şifre /asıl-şifre çözümlerinin histogramı



Şekil 4.2.(g,h).Bir köpeye ait asıl-şifre / asıl-şifreçözümlerinin histogramı



Şekil 4.2.(i,j).Bir ördeğe ait asıl-şifre / asıl-şifreçözümlerinin histogramı



Şekil 4.2.(k,l).Bir ördeğe ait asıl-şifre /asıl-şifreçözümlerinin histogramı

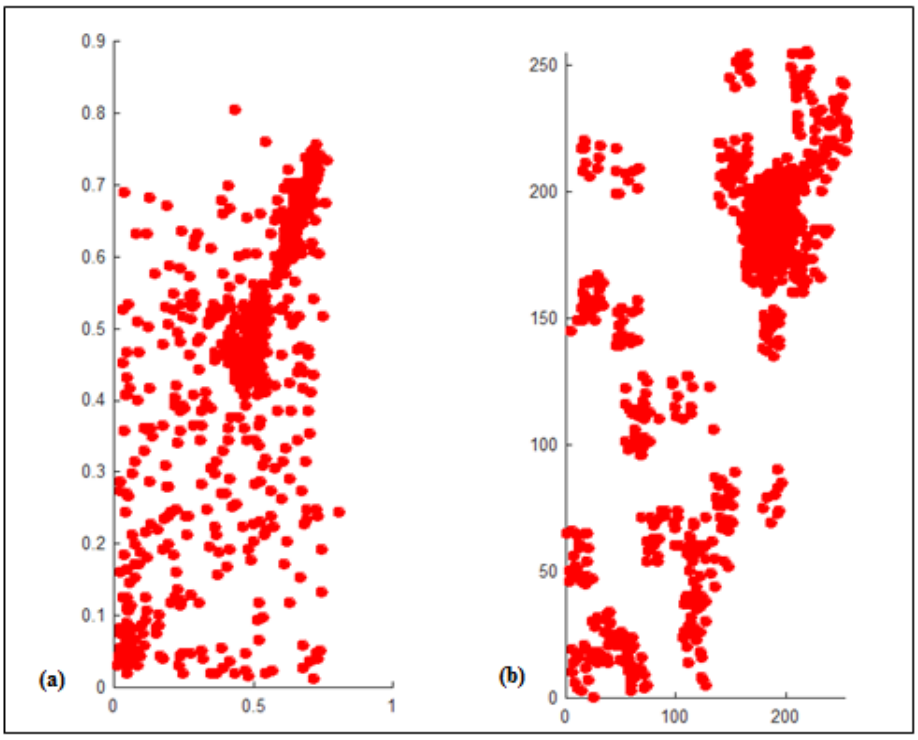
Orijinal ve şifreli imge arasında ilişki olduğunu keşfedilmiştir.İmgelere ait orjinal - şifre ve orjinal-şifre çözümleri ile ilgili korelasyon Tablo 4.2 de gösterilmiştir.

Tablo 4.2 incelendiğinde Şekil 4c e ait orjinal-şifre çözücüsüne ait korelesyon katsayısının en büyük olduğu (0.998) görülür iken , orjinal-şifre çözücüsüne ait en küçük korelesyon ilşkisinin Şekil 4k ya ait olan Monalisa ya ait olduğu (0.846) görülmektedir.Şekil 4.3.a., 4.3.b, 4.3.c, 4.3.d, 4.3.e, 4.3.f, 4.3.g, 4.3.h, 4.3.i, 4.3.j, 4.3.k ve 4.3.L de gri düzeyde korelasyon ilşkilerinin yakınlık ve uzaklık dereceleri ana(orjinal) ve şifrelenmiş hallerine ait ilşkiler histogram halinde gösterilmiştir.

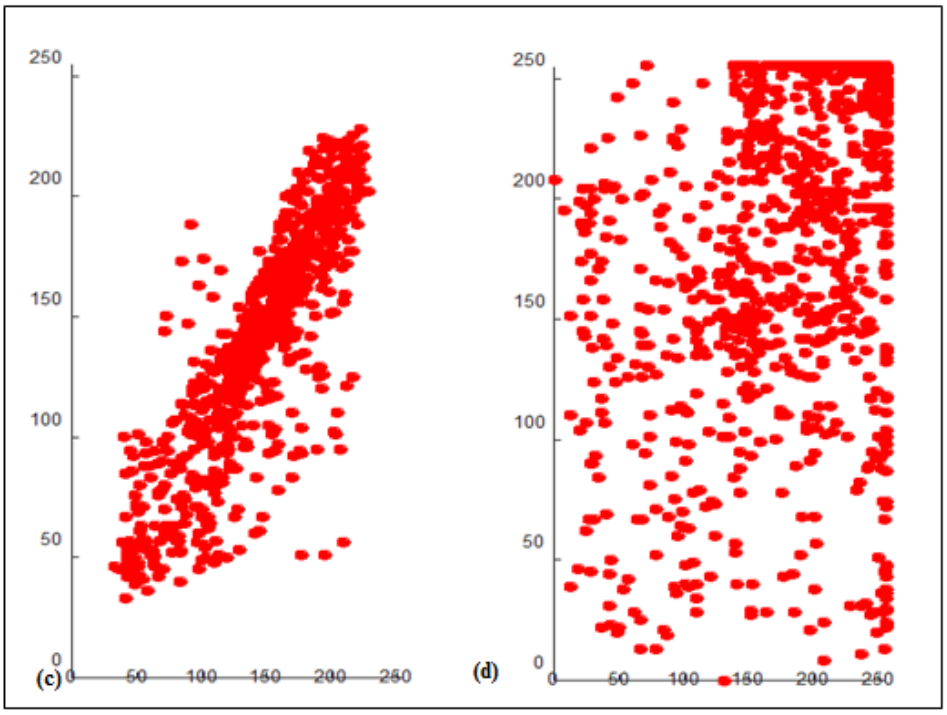
Genel olarak, orijinal ve şifresi çözülmüş imgeler arasında ilgileşimler daha yüksek olduğu halde, orijinal ve şifreli imgeler arasında ise ilgileşimler beklendiği üzere 0.35 veya daha düşük değerlere düşmektedir.

Tablo 4.2. *Çeşitli imgelere ait korelasyon katsayısıların karşılaştırılması*

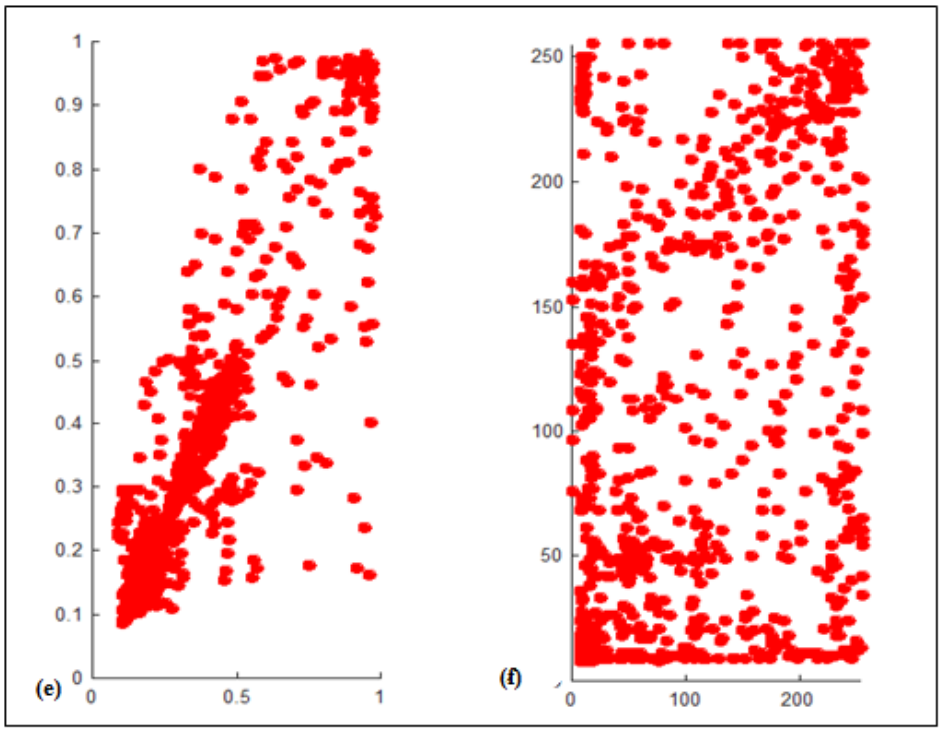
İmge ismi Boyut (32x32)	koveryans katsayı imgeleri	
	Koveryans $\rho_{x,y}$ Orijinal-Şifre	Koveryans $\rho_{x,y}$ Orijinal- Şifre çözümü
Kameraman	-0.334	0.991
Lena	-0.374	0.996
İnsan	0.215	0.998
Köpek	0.0497	0.885
Ördek	-0.094	0.899
Mona Liza	0.113	0.846



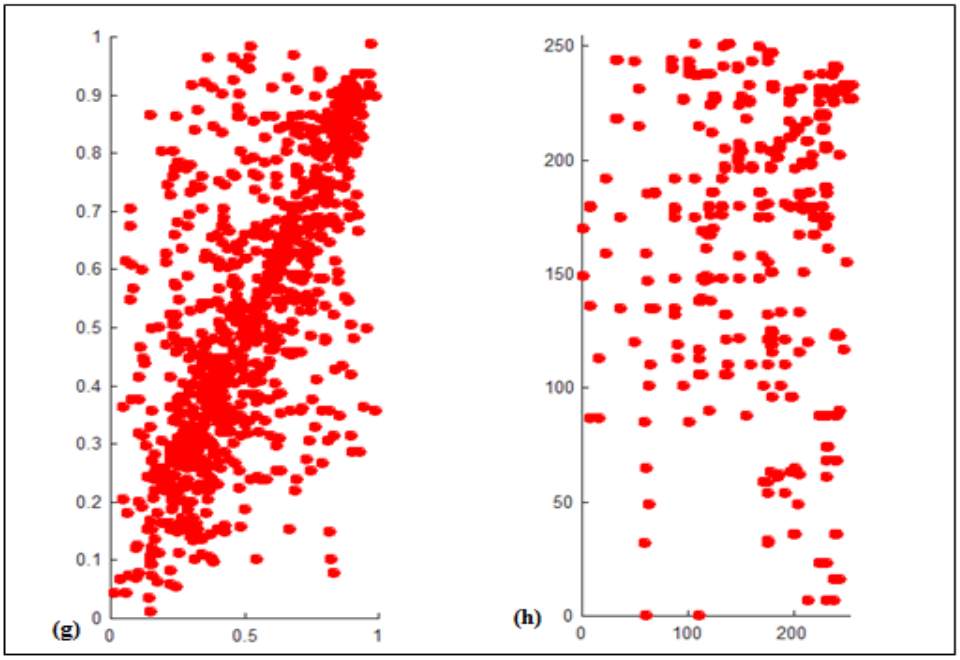
Şekil 4.3.(a,b).Açık gri tonlamalı imge kameraman korelasyon diyagramları



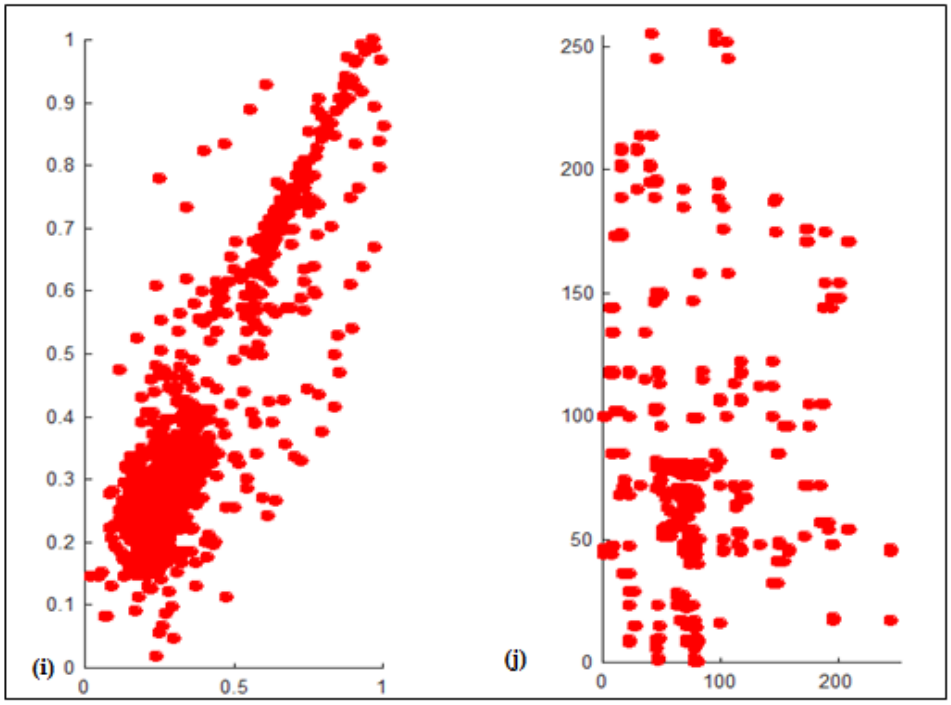
Şekil 4.3.(c,d).Açık gri tonlamalı imge Lena'nın ilgileşim diyagramları



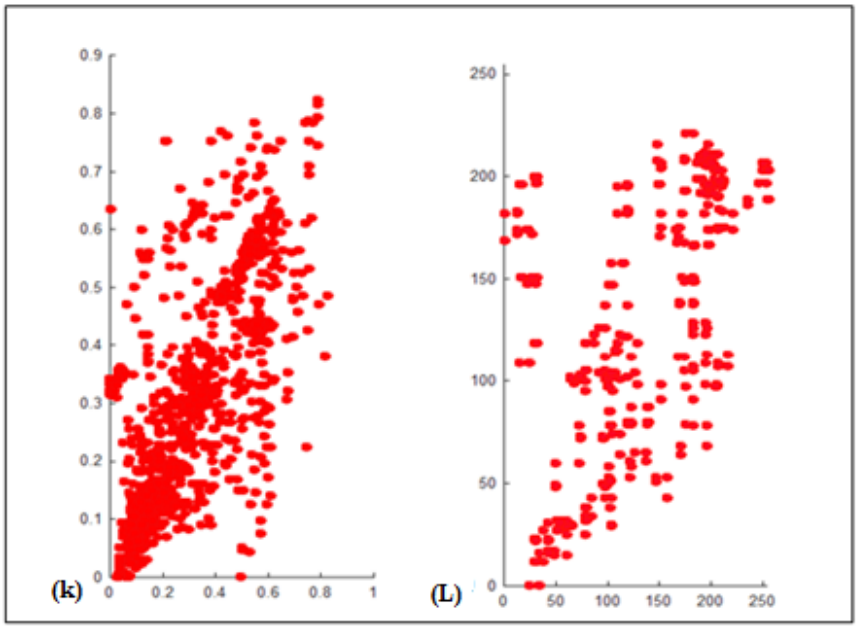
Şekil 4.3.(e,f).Açık gri tonlamalı imge insanın ilgileşim diyagramları



Şekil 4.3.(g,h).Açık gri tonlamalı imge köpeğin ilgileşim diyagramları



Şekil 4.3.(i,j).Açık gri tonlamalı imge ördeğin ilgileşim diyagramları



Şekil 4.3.(k,l).Açık gri tonlamalı imge Mona Lisa'nın ilgileşim diyagramları

Şekil 4.3(a,b,c,d,e,f,g,h,I,j,k ve l) durumları açık imge ve şifreli imge yönünden piksellerin ilgileşim dağıtımını göstermektedir. İlgileşim katsayıları, hem açık imge hem de şifreli imge için Tablo 4.2 de gösterilmiştir. Şekil 4.3(a,b,c,d,e,f,g,h,I,j,k ve l) ve Tablo 4.2 den yola çıkarak, şifreli imgedeki iki yakın piksel arasında önemsiz bir korelasyon bulunduğu belirgindir.

4.4. Bilgi Entropisi Analizi

Bilgi Entropi teorisi, bilgi içeriğini veya bir düzensizlik dağılımını temsil edilen rastgele bir değişkenin belirsizliğidir (Cover ve Thomas,2012). Matematiksel olarak, x alfabesi ve olasılık yoğunluk fonksiyonu (OYF) ile birlikte x,kesikli rastgele değişken olsun $p(x)$,$x \in X$.

X'in *Shannon bağıntısı* aşağıdaki denklemle verilir. Entropi bilgi birimi ' bit' olarak adlandırılr.

$$\text{Entropi bilgisi} = -\sum_{x\in X} P_i(x_i)\log_2 P_i(x_i) \qquad (4.2)$$

Burada, $p(x) \in [0,1]$, $\sum_{x\in X} P_i(x_i) = 1.0$ ve $-\log p(x)$ ise tek bir x oluşumu ile ilşkilidir.

Entropi bilgisi, rastgele değişkeni elde etmek için gerekli olan ortalamaya göre bitlerin sayısını ifade etmektedir. Bunun için, her zaman negatif olmayan bir değerdir. Entropi değeri daha yüksek olduğu zaman, bu durum değişkenin daha fazla bilgi içerdiği anlamına gelmektedir.

Entropının anlamlı bir özelliği, her zaman içbükey bir işlev sunmaktadır ve eğer ve sadece p(x) fonksiyonu tüm X'e eşit olursa, bu özellik |X | kaydında maksimum seviyesine ulaşır; bu da, olasılık dağıtımının tek biçimli olduğu anlamına gelir. Şifreleme sistemin gücünü ölçmek için bilgi entropisı kullanılır ve iyi bir imge şifreleme algoritmasını imgeye uygulayarak eşit derecede olası gri düzeyler sağlamaktadır(Wu ve v.d,2013).

Tablo 4.3 imgeler için ana (orjinal) ve bilgi entropi arasındaki ilişki göstermektedir.Tablo 4.3 de iki orijinal imgenin ve bunların şifreli olanlarının dağıtım değerlerini vermektedir. Gri düzeyde, eşit olasılığa sahip 256 olası değer çıktısı bulunmaktadır ve bu rastgele olarak ele alınmaktadır. Bu durumda, entropi=8 ideal bir değerdir.

Bu çalışmada, 32 bit kullanılmıştır ve dolayısıyla entropi için ideal değer 8'den daha az olmalıdır. Tablo 4.4. Örneklere ait Entropi bilgisi ve ana (orjinal) imgelerin bit değerlerinin karşılaştırılması gösterilmiştir.

Tablo 4.3 inceleniğinde, Şekil 4.2 ye göre Şekil 4.3c en büyük bilgi entropisine sahip iken en küçük Şekil 4.3i görülmektedir. Genel olarak ,bilgi entropisı şifreleme sistemi ile arttırılır ve şifreli imgelerin bilgi entropiları yaklaşık olarak 6.5'dir.

Bu önerilen şifreleme algoritmasının bilgi sızıntısına oldukça dirençli olduğunu kanıtlamaktadır.

Tablo 4.3. *Örneklere ait Entropi bilgisi ve ana (orjinal) imgelerin bit değerlerinin karşılaştırılması*

İmgeler	Ana(orjinal)	Entropi bilgisi
Kameraman	6.34929	6.35640
Lena	6.39117	5.48926
İnsan	5.93559	6.46618
Köpek	6.53661	5.66985
Ördek	6.45983	4.7336
Mona Liza	6.33432	5.30373

4.5. Hata Ölçümü

Ana hata kaynağı, analoga /sayısal platform aracılığıyla imgelerin gerçek zamanlı dönüştürülmesidir. Aslında, çıktı analog sinyallerinin deneysel ölçümlerinin de gerçek zamanlı bütün cihazlarda olduğu gibi mutlak bir hatası vardır. Bu gibi hatalar,Tablo 4.4 de ölçülmüş ve hesaplanmıştır.

En düşük değer Lena için elde edilirken, en büyük ölçek koyun için hesaplanmıştır. Bununla birlikte, gerçek zamanlı bir şifreleme sistemi için yaklaşık %5 olan hata miktarı, ana/bağımlı biçimdeki kabul edilebilir sınırlar eşzamanlılık devresi dahilindedir ve kaotik sinyallerin içindeki açık imge gri düzeylerini maskeler, onları açık kanal ile aktarılır ve gerçek zamana dayalı bir ortamda %5 dahilinde yeterli bir güvenlik ile yeniden kurtarılır.

Tablo 4.4. *Test imgelerine ilişkin hata ölçümleri*

İmgeler	Hata (Orijinal- Şifre çöz)
Kameraman	4%
Lena	3.7%
İnsan	3.9%
Köpek	4.2%
Ördek	3%
Mona Liza	3%

5. SONUÇ VE ÖNERİLER

Tez kapsamında ilk olarak,güvenli iletişimi gerçekleştirmek için kaotik sinyal özelliklerinden yararlanmak üzere R2D2L kaotik şifreleme algoritması geliştirilmiştir.Çalışmamızda kaotik bir devre (R2L2D) kullanan yeni bir gri imge şifreleme tekniğinin diğer tekniklerden olan üstünlüğü deneysel olarak ve MatLap program yardımıyla simülasyonu gerçekleştilerek ispatlanmıştır.

Tezin ikinci aşamasında,farklı başlangıç koşullarından başlayarak iki kaotik sistemi eşzamanlı (Hakim-Esir) ilişkisi gerçekleştirilmiştir.Kaotik ve kaos sistemleri başlangıç koşullarına/parametre uyumsuzluklarına hassasiyet, belirleyici dinamikler, karıştırma özelliği ve yapı karmaşıklığı gibi pek çok özelliğe sahiptir.Bununla birlikte,kaotik eşzamanlılık olasılığı, analog temelli güvenli iletişimde uygulanmaları için şifreleme ve şifre çözümündeki uygulanabilirliği belirlenmiştir. Ek olarak, kaos yöntemi daha sağlam güvenliğin sunulmasının yanı sıra, güvenilir, hızlı ve basit bir imge şifreleme zemininin sağlanması için çok iyi bir alternatif yöntem olduğunu deneysel gözlemlerle belirlenmiştir.Gerçek rastgele üreteçler, gürültü gibi tahmin edilemeyen doğal süreçlerin ölçülmesinden kaynaklanır. Şifreleme sistemi, güvenli bir anahtar bulmak amacıyla temel olarak seçilmiş bir şifreli imge saldırısı olan farklı saldırılara direnebilmektedir.

Tezin üçüncü ve son aşamasında,verilerin deneysel ve teorik karşılaştırılması yapılarak şifreleme sisteminin çok sağlam bir güvenlik sağladığı sonucuna varılmıştır.Önerilen imge şifreleme tekniğinin, istatistiksel saldırılara dayanacak güçlü bir kabiliyetinin olduğu nettir. Bu teknik, alınan şifre çözme imgesindeki, şifresi çözülen imgede büyük bir farklılık meydana getiren ve iyi bir şifreleme sistemine yol açan küçük değişimlere zaman açısından daha duyarlı olduğu anlaşılmıştır.

Gri imgeleri, fiziksel katman ile yerlerinin değiştirildiği alıcıya göndererek herhangi bir sayısal veriyi kaydetmediği için bu tasarımın çok faydalı olduğu belirtilmelidir.Buna ek olarak, “donanım anahtarı” konfigürasyonu her ne zaman daha kesin olursa, deneysel amaçlarla tasarlanmış olan devre de daha kesin olacaktır.

Bu teknikte karşılaştığımız tek eksiklik şifresi çözülen imgedeki çok az gürültü miktarı oluşturulmasıdır.

Bununla birlikte, Bölüm 4.3 de gösterildiği şekilde, renkli imgeler işlenirken imge verilerinin dönüştürülmesi için geniş hafızaya ihtiyaç vardır. Gelecekteki araştırmacılara öneri için, bu alanda yeni bir yöntem olacak, renkli bir imge sinyalinin gönderilmesi için bu tekniğin geliştirlmesi düşünülmelidir.

Gelecekte daha güvenli yöntem olması için, saldırılara karşı artan sağlamlık ve azalan süre karmaşıklığı açısından daha iyi sonuçlar elde etmek için önemli bazı frekans alanı ve başlangıç koşulu şifreleme aralık teknikleri geliştirilebilir.

KAYNAKLAR

Alsafasfeh, Q. H., , Arfoa, A. A. (2011). Image encryption based on the general approach for multiple chaotic systems. *J. Signal and Information Processing, 2*(3), 238-244.

Andreatos, A., , Leros, A. (2013). Secure Image Encryption Based On a Chua Chaotic Noise Generator. *Journal of Engineering Science and Technology Review, 6*(4).

Ayrom, F., , Zhong, G.-Q. (1986). *Chaos in Chua's circuit.* Paper presented at the IEE Proceedings D-Control Theory and Applications.

Banzi, M., , Shiloh, M. (2014). *Getting started with Arduino: the open source electronics prototyping platform*: Maker Media, Inc.

Baptista, M. (1998). Cryptography with chaos. *Physics Letters A, 240*(1-2), 50-54.

Belkhouche, F., , Qidwai, U. (2003). *Binary image encoding using 1D chaotic maps.* Paper presented at the IEEE Region 5, 2003 Annual Technical Conference.

Carroll, T. L., , Pecora, L. M. (1991). Synchronizing chaotic circuits. *IEEE Transactions on Circuits and Systems, 38*(4), 453-456.

Celİk, K., , Kurt, E. (2016). *A new image encryption algorithm based on lorenz system.* Paper presented at the Electronics, Computers and Artificial Intelligence (ECAI), 2016 8th International Conference on.

Chang, C.-C., Hwang, M.-S., , Chen, T.-S. (2001). A new encryption algorithm for image cryptosystems. *Journal of Systems and Software, 58*(2), 83-91.

Chua, L. O., Wu, C. W., Huang, A., , Zhong, G.-Q. (1993). A universal circuit for studying and generating chaos. I. Routes to chaos. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 40*(10), 732-744.

Daemen, J., , Rijmen, V. (2013). *The design of Rijndael: AES-the advanced encryption standard*: Springer Science , Business Media.

Erol, K., , BİNGÖL, C. (2016). A New Sweep Up/Down Phenomenon between the Chaotic and Regular Regions in a New R2L2D Circuit, page: 305-310. *Politeknik Dergisi, 19*(3).

Feki, M. (2003). An adaptive chaos synchronization scheme applied to secure communication. *Chaos, Solitons , Fractals, 18*(1), 141-148.

Gao, H., Zhang, Y., Liang, S., , Li, D. (2006). A new chaotic algorithm for image encryption. *Chaos, Solitons , Fractals, 29*(2), 393-399.

Gu, G., , Han, G. (2006). *An enhanced chaos based image encryption algorithm.* Paper presented at the Innovative Computing, Information and Control, 2006. ICICIC'06. First International Conference on.

Hanias, M., Avgerinos, Z., , Tombras, G. (2009). Period doubling, Feigenbaum constant and time series prediction in an experimental chaotic RLD circuit. *Chaos, Solitons , Fractals, 40*(3), 1050-1059.

Hilborn, R. C. (2000). *Chaos and nonlinear dynamics: an introduction for scientists and engineers*: Oxford University Press on Demand.

Jain, Y., Bansal, R., Sharma, G., Kumar, B., Gupta, S. (2016). Image encryption schemes: a complete survey. *International Journal of Signal Processing, Image Processing and Pattern Recognition, 9*(7), 157-192.

Kasap, R., , Kurt, E. (1998). An investigation of chaos in the RL-diode circuit using the BDS test. *Advances in Decision Sciences, 2*(2), 193-199.

Kiers, K., Schmidt, D., , Sprott, J. C. (2004). Precision measurements of a simple chaotic circuit. *American Journal of Physics, 72*(4), 503-509.

Kocarev, L., Halle, K., Eckert, K., Chua, L. O., , Parlitz, U. (1992). Experimental demonstration of secure communications via chaotic synchronization. *International Journal of Bifurcation and Chaos, 2*(03), 709-713.

Koh, C. L., , Ushio, T. (1997). Digital communication method based on M-synchronized chaotic systems. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 44*(5), 383-390.

Kolumban, G., Vizvári, B., Schwarz, W., , Abel, A. (1996). *Differential chaos shift keying: A robust coding for chaos communication.* Paper presented at the Proc. NDES.

Kurt, E. (2006). Nonlinearities from a non-autonomous chaotic circuit with a non-autonomous model of Chua's diode. *Physica Scripta, 74*(1), 22.

Kurt, E., Acar, S., , Kasap, R. (2000). A comparison of chaotic circuits from a statistical approach. *Mathematical and Computational Applications, 5*(2), 95-103.

Kurt, E., , Bingol, C. (2017). *Synchronization and secure communication in a resistor double inductor and diode circuit.* Paper presented at the Power and Electrical Engineering of Riga Technical University (RTUCON), 2017 IEEE 58th International Scientific Conference on.

Linsay, P. S. (1981). Period doubling and chaotic behavior in a driven anharmonic oscillator. *Physical Review Letters, 47*(19), 1349.

Lorenz, E. N. (1963). Deterministic nonperiodic flow. *Journal of the atmospheric sciences, 20*(2), 130-141.

Lu, H., , He, Z. (1996). Chaotic behavior in first-order autonomous continuous-time systems with delay. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 43*(8), 700-702.

Maniccam, S. S., , Bourbakis, N. G. (2004). Image and video encryption using SCAN patterns. *Pattern Recognition, 37*(4), 725-737.

Matsumoto, T. (1984). A chaotic attractor from Chua's circuit. *IEEE Transactions on Circuits and Systems, 31*(12), 1055-1058.

Matthews, R. (1989). On the derivation of a "chaotic" encryption algorithm. *Cryptologia, 13*(1), 29-42.

MOHREM, A., CHETATE, B., GUIA, H. E., , Bougara, M. H.(2015), Design, simulation and realization of voltage measurement and monitoring system with real time data logging based on microcontroller.

Murali, K., Lakshmanan, M., , Chua, L. O. (1994). The simplest dissipative nonautonomous chaotic circuit. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 41*(6), 462-463. doi: https://doi.org/10.1109/81.295246

Nag, A., Singh, J. P., Khan, S., Biswas, S., Sarkar, D., , Sarkar, P. P. (2011). *Image encryption using affine transform and XOR operation.* Paper presented at the Signal Processing, Communication, Computing and Networking Technologies (ICSCCN), 2011 International Conference on.

Ogorzalek, M. J. (1997). Chaos and complexity in nonlinear electronic circuits. *Chaos and Complexity in Nonlinear Electronic Circuits. Edited by OGORZALEK MACIEJ J. Published by World Scientific Publishing Co. Pte. Ltd.,. ISBN# 9789812798626.*

Ogorzałek, M. J. (1997). *Chaos and complexity in nonlinear electronic circuits*: World Scientific.

Patidar, V., Pareek, N., Purohit, G., , Sud, K. (2011). A robust and secure chaotic standard map based pseudorandom permutation-substitution scheme for image encryption. *Optics Communications, 284*(19), 4331-4339.

Pecora, L. M., , Carroll, T. L. (1990). Synchronization in chaotic systems. *Physical Review Letters, 64*(8), 821.

Pisarchik, A., , Zanin, M. (2008). Image encryption with chaotically coupled chaotic maps. *Physica D: Nonlinear Phenomena, 237*(20), 2638-2648.

Šalamon, M. (2012). *Chaotic electronic circuits in cryptography.* Paper presented at the Applied cryptography and network security.

Schneier, B. (2007). *Applied cryptography: protocols, algorithms, and source code in C*: john wiley , sons.

Shelke, F. M., Dongre, A. A., , Soni, P. D. (2014). Comparison of different techniques for Steganography in images. *International Journal of Application or Innovation in Engineering , Management, 3*(2), 171-176.

Shin, C.-M., Seo, D.-H., Cho, K.-B., Lee, H.-W., , Kim, S.-J. (2003). *Multilevel image encryption by binary phase XOR operations.* Paper presented at the Lasers and Electro-Optics, 2003. CLEO/Pacific Rim 2003. The 5th Pacific Rim Conference on.

Singh, S., Sharma, S., , Dev, A. (2017), Very Low Power 3 Bit R-2R Ladder Based Digital to Analog Converter and Comparative Analysis with other Types of Dacs at 180nm. ISSN: 2394-9333 IJTRD | Available Online@www.ijtrd.com

Sprott, J. C., , Sprott, J. C. (2003). *Chaos and time-series analysis* (Vol. 69): Citeseer.

Strogatz, S. (1994). Nonlinear Dynamics and Chaos: With applications to physics, biology, chemistry, and engineering Perseus Books Publishing: Massachusetts.

Tong, X., , Cui, M. (2009). Image encryption scheme based on 3D baker with dynamical compound chaotic sequence cipher generator. *Signal Processing, 89*(4), 480-491.

Wang, C., , Shen, H.-W. (2011). Information theory in scientific visualization. *Entropy, 13*(1), 254-273.

Wu, C. W., , Chua, L. O. (1993). A simple way to synchronize chaotic systems with applications to secure communication systems. *International Journal of Bifurcation and Chaos, 3*(06), 1619-1627.

Xiangdong, L., Junxing, Z., Jinhai, Z., , Xiqin, H. (2008). Image scrambling algorithm based on chaos theory and sorting transformation. *IJCSNS International Journal of Computer Science and Network Security, 8*(1), 64-68.

Xiao, H.-P., , Zhang, G.-J. (2006). *An image encryption scheme based on chaotic systems.* Paper presented at the Machine Learning and Cybernetics, 2006 International Conference on.

Yang, T. (2004). A survey of chaotic secure communication systems. *International Journal of Computational Cognition, 2*(2), 81-130.

Yang, T., , Chua, L. O. (1996). Secure communication via chaotic parameter modulation. *IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, 43*(9), 817-819.

Yen, J.-C., , Guo, J.-I. (1999). *A new image encryption algorithm and its VLSI architecture.* Paper presented at the Signal Processing Systems, 1999. SiPS 99. 1999 IEEE Workshop on.

ÖZGEÇMİŞ

Adı Soyadı : Khaled Mohamed EL HADAD
Doğum Yeri ve Yılı : 03.04. 1968 Tripoli-Libya
Medeni Hali : Evli
Yabancı dil :Arapça,İngilizce ve Türkçe
E-posta : khaledhadadtr@gmail.com



EĞITIM DURUMU

Lise : Alhathba Triopli/Libya
Lisans : Higher Education Center/Elektrik-Bilgisayar Mühendisliği Zilten\Libya
Yüksek Lisans : Brno Teknoloji Üniversitesi/Prag-Çek cumhuriyeti Elektronik ve Bilgisayar Mühendisliği Elektronik ve iletişim Ana Bilim Dalı

YAYINLAR VE KONFERANS

K. M. El hadad (2018), A New Technique for Secure Image Communication via Chaotic Circuit, IJCST . 9:1, Issn online : 0976-8491 .

K. M. El hadad, E. Kurt, A.Hançerlioğulları (2017), New Technıque For Secure Image Communıcatıon Vıa A Resıstor-Two Inductors-Two Dıodes Chaotıc Cırcuıt international conference on advanced enginnering Technologies, 21-23 sempteber,Bayburt/Turkey.

S. A. A. Shufat, E. Kurt, **K. M. El hadad,** A. Hancerlioğulları (2018). A numerical. model for a Stirling engine. Journal of Energy Systems, 2(1), 1-12.

S. A. A. Shufat, E. Kurt, **K. M. El hadad**, A. Hancerlioğulları (2017), A stirling engine modeling study for solar energy of parabolic dish systems", Fourth European Conference on Renewable Energy Systems. Sarajevo, Bosnia and Herzegovina. Isbn: 978-605-86911-5-5

A. Hançerlioğullari, A. Kurnaz, Y. G. Ali MADEE, L. A. Abdalsmd, S. A. A. Shufat, **K. M. El hadad,** H.Almezogi, M. M. A. Mansur (2017), Estimates of the Fast and Termal Flux inBlanket of Critical Reactors by Using Multi-Group Methods, Open Journal of Applied Sciences, 7, 68-81, http://www.scirp.org/journal/ojapps, ISSN Online: 2165-3925, Issn Print: 2165-3917.