GÖRÜNTÜ ŞİFRELEMEDE KULLANILAN KAOTİK HARİTALARIN İNCELENMESİ VE HİBRİT BİR YÖNTEM ÖNERİSİ

Duygu GÜVENOĞLU
21 14 02 109

YÜKSEK LİSANS TEZİ
Bilgisayar Mühendisliği Anabilim Dalı
Bilgisayara Mühendisliği Tezli Yüksek Lisans
Danışman: Dr. Öğr. Üyesi Volkan TUNALI

İstanbul
T.C. Maltepe Üniversitesi
Lisansüstü Eğitim Enstitüsü
Nisan, 2023

GÖRÜNTÜ ŞİFRELEMEDE KULLANILAN KAOTİK HARİTALARIN İNCELENMESİ VE HİBRİT BİR YÖNTEM ÖNERİSİ

Duygu GÜVENOĞLU
21 14 02 109
ORCID: 0000-0002-6459-6953

YÜKSEK LİSANS TEZİ
Bilgisayar Mühendisliği Anabilim Dalı
Bilgisayar Mühendisliği Tezli Yüksek Lisans
Danışman: Dr. Öğr. Üyesi Volkan TUNALI

İstanbul
T.C. Maltepe Üniversitesi
Lisansüstü Eğitim Enstitüsü
Nisan, 2023



JÜRİ VE ENSTİTÜ ONAYI

Bu belge, Yükseköğretim Kurulu tarafından 19.01.2021 tarihli "Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge" ile bildirilen 6689 Sayılı Kişisel Verilerin Korunması Kanunu kapsamında gizlenmiştir.

ETİK İLKE VE KURALLARA UYUM BEYANI

Bu belge, Yükseköğretim Kurulu tarafından 19.01.2021 tarihli "Lisansüstü Tezlerin Elektronik Ortamda Toplanması, Düzenlenmesi ve Erişime Açılmasına İlişkin Yönerge" ile bildirilen 6689 Sayılı Kişisel Verilerin Korunması Kanunu kapsamında gizlenmiştir.

TEŞEKKÜR

Bu çalışmanın gerçekleştirilmesinde, tez çalışmam boyunca değerli bilgilerini bizlerle paylaşan, kullandığı her kelimenin hayatıma kattığı önemini asla unutmayacağım saygıdeğer danışman hocam Dr. Öğr. Üyesi Volkan TUNALI'ya ve desteklerini esirgemeyen aileme sonsuz teşekkürlerimi sunarım.

Duygu GÜVENOĞLU

Nisan, 2023

ÖZET

GÖRÜNTÜ ŞİFRELEMEDE KULLANILAN KAOTİK HARİTALARIN İNCELENMESİ VE HİBRİT BİR YÖNTEM ÖNERİSİ

Duygu Güvenoğlu
Yüksek Lisans Tezi
Bilgisayar Mühendisliği Anabilim Dalı
Bilgisayar Mühendisliği Tezli Yüksek Lisans
Danışman: Dr. Öğr. Üyesi Volkan Tunalı
Maltepe Üniversitesi Lisansüstü Eğitim Enstitüsü, 2023

Günümüz teknolojileri göz önüne alındığında günlük yaşantımızda en çok paylaşımda bulunulan verilerin multimedya verileri olduğu görülmektedir. Ağ üzerinden multimedya verileri farklı sunuculara iletilmektedir. Herkese açık olan bu ağlar üzerindeki verilerin güvenliğinin sağlanması gerekmektedir. Verilerin istenmeyen kişilerin eline geçmesini ve güvenlik sorunlarını ortadan kaldırmanın en etkili yolu şifreleme tekniklerinin kullanılmasıdır. Verilerin şifrelenmesi çoğunlukla ya kriptografik teknikler ile ya da kaotik teknikler ile sağlanmaktadır. Görüntü verilerinin güvenliğinin sağlanması sürecinde çoğunlukla kaotik teknikler kullanılmaktadır. Kaotik teknikleri yardımıyla görüntüye ait pikseller kaotik tekniğin yapısına göre karıştırılmakta, değerleri değiştirilmekte veya iki yöntem birlikte kullanılmaktadır.

Multimedya uygulamalarının ve mobil cihazlarda veri paylaşımının artması bilim insanlarının görüntü şifreleme alanında çalışmalar yapmasına olanak sağlamıştır. Görüntü şifreleme yöntemleri zaman içerisinde evrilmiş ve birbirinden farklı teknikler ortaya atılmıştır. Bu tekniklerin pek çoğunda kaotik tekniklerden faydalanılmıştır. Bu tez çalışmasında farklı çalışmalarda sıklıkla kullanılan kaotik tekniklerin detayları incelenmiş ve bir araya getirilmiştir. Bununla birlikte bilim insanları tarafından önerilecek yöntemlerin güvenilirliğini test edebilmek amacıyla literatürde kullanılan test tekniklerine de yer verilmiştir. Ayrıca yine kaotik teknikleri kullanan hibrit bir yöntem önerilmiş ve görüntü şifrelemede kullanımı gerçekleştirilmiştir. Yöntemin güvenilirliği çeşitli testler yapılarak ispatlanmıştır.

Anahtar Sözcükler: Şifreleme, Kaotik Haritalar, Görüntü Şifreleme, Test Teknikleri.

ABSTRACT

ANALYSIS OF CHAOTIC MAPS USED IN IMAGE ENCRYPTION AND SUGGESTION FOR A HYBRID METHOD

Duygu Güvenoğlu
Master Thesis
Computer Engineering Department
Computer Engineering with Thesis
Thesis Advisor: Assist. Prof. Dr. Volkan Tunalı
Maltepe University Graduate School, 2023

Considering today's technologies, it is seen that the most shared data in our daily life is multimedia data. Multimedia data are transmitted to different servers over the network. It is necessary to ensure the security of data on these networks that are open to everyone. The most effective way to prevent data from falling into the hands of unwanted people and to eliminate security problems is the use of encryption techniques. Encryption of data is mostly provided either by cryptographic techniques or by chaotic techniques. Chaotic techniques are mostly used in the process of ensuring the security of image data. With the help of chaotic techniques, the pixels of the image are mixed according to the structure of the chaotic technique, their values are changed or both methods are used together.

The increase in multimedia applications and data sharing on mobile devices has allowed scientists to work in the field of image encryption. Image encryption methods have evolved over time, and different techniques have been proposed. Chaotic techniques were used in most of these techniques. In this thesis, the details of the chaotic techniques frequently used in different studies were examined and brought together. In addition, test techniques used in the literature are also included in order to test the reliability of the methods proposed by scientists. In addition, a hybrid method using chaotic techniques has been proposed, and its use in image encryption has been realized. The reliability of the method has been proven by various tests.

Keywords: Encryption, Chaotic Maps, Image Encryption, Test Techniques.

İÇİNDEKİLER

JÜRİ VE ENSTİTÜ ONAYI ii
ETİK İLKE VE KURALLARA UYUM BEYANI iii
TEŞEKKÜR iv
ÖZET v
ABSTRACT vi
İÇİNDEKİLER vii
TABLOLAR LİSTESİ xiii
ŞEKİLLER LİSTESİ xiv
KISALTMALAR xvii
1. GİRİŞ 1
1.1 Problem 2
1.2 Amaç 3
1.3 Önem 3
1.4 Varsayımlar 4
1.5 Sınırlıklar 4
1.6 Tanımlar 4
2. LİTERATÜR ARAŞTIRMASI 6
3. MATERYAL VE YÖNTEM 24
3.1 Kaotik Sistemler 24
3.1.1 Tersine çevrilemeyen kaotik haritalar 25
3.1.1.1 Lojistik harita 25
3.1.1.2 Kübik harita 26

3.1.1.3 Doğrusal uyumlu üreteç haritası 27
3.1.1.4 Kaotik sinüs haritası 28
3.1.1.5 Çadır harita 29
3.1.1.6 Gauss harita 30
3.1.1.7 Kaotik Uç harita 31
3.1.1.8 Gaussian beyaz kaotik harita 31
3.1.1.9 Kıskaç harita 32
3.1.1.10 Spens harita 33
3.1.1.11 Sinüs çemberi harita 33
3.1.1.12 Parçalı kaotik harita 34
3.1.1.13 Kaotik şarkıcı haritası 35
3.1.1.14 Sinüzodial kaotik harita 36
3.1.1.15 Chebyshev kaotik harita 36
3.1.1.16 May kaotik harita 37
3.1.1.17 Gompertz kaotik harita 38
3.1.1.18 Trigonometrik kaotik harita 38
3.1.1.19 Bernoulli kaotik harita 39
3.1.1.20 Ricker kaotik harita 40
3.1.1.21 Aizawa kaotik harita 40
3.1.1.22 Beta kaotik harita 41
3.1.2 Dağıtıcı kaotik haritalar 42

3.1.2.1 Henon kaotik harita 42
3.1.2.2 Lozi kaotik harita 43
3.1.2.3 Gecikmeli lojistik harita 44
3.1.2.4 Tinkerbell kaotik harita 45
3.1.2.5 Burger'in kaotik haritası 46
3.1.2.6 Kaplan Yorke kaotik harita 47
3.1.2.7 Ikeda kaotik harita 48
3.1.2.8 Sinai kaotik harita 49
3.1.2.9 Ayrık zamanlı kaotik yırtıcı-av haritası 50
3.1.2.10 Holmes Kübik haritası 51
3.1.2.11 Baker kaotik harita 52
3.1.2.12 Bogdanov kaotik harita 53
3.1.2.13 Basin kaotik harita 54
3.1.2.14 Chialvo kaotik harita 55
3.1.2.15 Zaslavsky kaotik harita 56
3.1.3 Koruyucu kaotik haritalar 57
3.1.3.1 Chirikov kaotik harita 57
3.1.3.2 Hénon alan korumalı ikinci dereceden kaotik harita 58
3.1.3.3 Arnold'un kedi kaotik haritası 59
3.1.3.4 Gingerbreadman kaotik harita 60
3.1.3.5 Kaotik web haritası 61

3.1.3.6 Lorenz kaotik harita 62
3.1.3.7 Chua kaotik harita 63
3.1.3.8 Rossler'in kaotik haritası 64
3.2 Kaotik Haritalar ve Özellikleri 65
3.3 Değerlendirme Ölçütleri 66
3.3.1 Diferansiyel analizler 67
3.3.1.1 Piksel değişim oranı 67
3.3.1.2 Birleşik ortalama değişen yoğunluk 67
3.3.2 İstatistiksel analizler 68
3.3.2.1 Histogram analizi 68
3.3.2.2 Korelasyon katsayısı analizi 68
3.3.3 Diğer analiz teknikleri 69
3.3.3.1 Bilgi entropisi 69
3.3.3.2 Anahtar analizi 70
3.3.3.3 Gürültü saldırısı 70
3.3.3.4 Çalışma süresi 71
3.3.3.5 Bit geçerlik oranı 71
3.3.3.6 Ortalama karesel hata 71
3.3.3.7 Tepe sinyal gürültü oranı 72
3.3.3.8 Sinyal bozulma oranı 72
3.3.3.9 Yapısal benzerlik indeksi 73

3.3.3.10 Kök ortalama karekök hata 73
3.3.3.11 Ortalama mutlak hata 74
3.3.3.12 Sinyal gürültü oranı 74
3.3.4 NIST rastgelelik analizi 75
4. ÖNERİLEN HİBRİT GÖRÜNTÜ ŞİFRELEME YÖNTEMİ 76
4.1 Önerilen görüntü şifreleme algoritması 76
4.2 Önerilen algoritmanın deşifreleme işlemi 80
4.3 Deneysel sonuçlar ve güvenlik analizleri 80
4.3.1 Şifreleme ve deşifreleme sonuçları 80
4.3.2 Algoritmanın karmaşıklık analizi 81
4.3.3 Anahtar uzayı analizi 82
4.3.4 Anahtar hassasiyet analizi 82
4.3.5 Histogram analizi 83
4.3.6 Komşu pikseller arasında korelasyon analizi 84
4.3.7 Entropi analizi 86
4.3.8 Yapısal benzerlik testi analizi 87
4.3.9 NPCR ve UACI analizi 87
4.3.10 Dayanıklılık analizi 88
4.3.11 MSE ve PSNR testi 89
4.3.12 Bit geçerlik oranı testi 90
4.3.13 NIST testi 91

4.3.14 Çalışma süresi testi 92

5. SONUÇ ve ÖNERİLER 93

KAYNAKLAR 94

ÖZGEÇMİŞ 118

TABLOLAR LİSTESİ

Tablo 1. İncelenen kaotik haritalar ve özellikleri 65

Tablo 2. NIST test araçları 75

Tablo 3. Kaotik harita başlangıç değerlerinin elde edilmesi örneği 79

Tablo 4. Önerilen yöntemin korelasyon testi sonuçları 86

Tablo 5. Önerilen yöntemin entropi testi sonuçları 86

Tablo 6. Yapısal benzerlik testi sonuçları 87

Tablo 7. NPCR ve UACI testi sonuçları 87

Tablo 8. Orijinal ve deşifrelenmiş görüntüler arasındaki MSE ve PSNR değerleri 89

Tablo 9. Orijinal ve tahribata uğratılmış deşifreli görüntüler arasındaki MSE ve PSNR değerleri 90

Tablo 10. Orijinal ve deşifreli görüntüler arasındaki bit kayıp oranları 90

Tablo 11. Orijinal ve deşifreli gürültülü görüntüler arasındaki bit kayıp oranları 91

Tablo 12. Orijinal ve deşifreli tahribatlı görüntüler arasındaki bit kayıp oranları 91

Tablo 13. Şifrelenmiş "Lena" görüntü için NIST testi sonuçları 91

Tablo 14. Çalışma süresi testi sonuçları 92

ŞEKİLLER LİSTESİ

Şekil 1. Görüntü şifreleme yöntemlerinin sınıflandırılması 6

Şekil 2. Kaotik haritaların görüntü şifrelemede kullanılması süreci 7

Şekil 3. Kaotik haritaların sınıflandırılması 25

Şekil 4. Lojistik harita genlik dağılımı örneği 26

Şekil 5. Kübik harita genlik dağımı örneği 27

Şekil 6. Doğrusal uyumlu üreteç haritası genlik dağılımı örneği 28

Şekil 7. Sinüs kaotik harita örneği 29

Şekil 8. Kaotik çadır harita örneği 30

Şekil 9. Gauss harita örneği 30

Şekil 10. Uç harita örneği 31

Şekil 11. Gaussian beyaz kaotik harita örneği 32

Şekil 12. Kıskaç harita örneği 32

Şekil 13. Spens harita örneği 33

Şekil 14. Sinüs çemberi haritası örneği 34

Şekil 15. Parçalı kaotik harita örneği 35

Şekil 16. Kaotik singer haritası örneği 35

Şekil 17. Sinüzoidal kaotik harita örneği 36

Şekil 18. Chebyshev kaotik harita örneği 37

Şekil 19. May kaotik harita örneği 37

Şekil 20. Gompertz kaotik harita örneği 38

Şekil 21. Trigonometrik kaotik harita örneği 39

Şekil 22. Bernoulli kaotik harita örneği 39

Şekil 23. Ricker kaotik harita örneği 40
Şekil 24. Aizawa kaotik haritası örneği 41
Şekil 25. Beta kaotik harita örneği 42
Şekil 26. Henon kaotik harita örneği 43
Şekil 27. Lozi kaotik harita örneği 44
Şekil 28. Gecikmeli lojistik harita örneği 45
Şekil 29. Tinkerbell kaotik harita örneği 46
Şekil 30. Burger kaotik harita örneği 47
Şekil 31. Kaplan Yorke kaotik harita örneği 48
Şekil 32. Ikeda kaotik harita örneği 49
Şekil 33. Sinai kaotik harita örneği 50
Şekil 34. Ayrık zamanlı yırtıcı-av kaotik haritası örneği 51
Şekil 35. Holmes Kübik haritası örneği 52
Şekil 36. Baker kaotik harita örneği 53
Şekil 37. Bogdanov kaotik harita örneği 54
Şekil 38. Basin kaotik harita örneği 55
Şekil 39. Chialvo kaotik harita örneği 56
Şekil 40. Zaslavsky kaotik harita örneği 57
Şekil 41. Chirikov kaotik harita örneği 58
Şekil 42. Hénon alan korumalı ikinci dereceden harita örneği 59
Şekil 43. Arnold'un kedi kaotik haritası örneği 60
Şekil 44. Gingerbradman kaotik harita örneği 61
Şekil 45. Kaotik web haritası örneği 62
Şekil 46. Lorenz kaotik harita örneği 63
Şekil 47. Chua kaotik harita örneği 64

Şekil 48. Rossler'in kaotik harita örneği 65

Şekil 49. Önerilen yöntemin blok diyagramı..... 76

Şekil 50. Bit dizisinin matrise dönüşümü örneği..... 78

Şekil 51. Örnek KDSA dizisi 78

Şekil 52. Şifrelenmiş ve deşifrelenmiş görüntüler. (a) ~ (d) Orijinal görüntüler, (e) ~ (h) Şifreli görüntüler, (i) ~ (l) Deşifrelenmiş görüntüler..... 81

Şekil 53. Anahtar hassasiyeti analizi (a) doğru anahtar ile deşifrelenmiş görüntü (b)~(f) küçük farklı anahtarlar ile deşifrelenmiş görüntüler..... 83

Şekil 54. Orijinal ve şifrelenmiş görüntü histogramları 84

Şekil 55. Renkli Lena görüntüsü üzerinde gerçekleştirilen korelasyon testi sonuçları .. 85

Şekil 56. Gürültü saldırısı testi sonuçları (a) Tuz ve Biber gürültüsü değişiklik oranı 0.01 (b) Tuz ve Biber gürültüsü değişiklik oranı 0.05, (c) Gauss gürültüsü değişiklik oranı 0.01, (d) Gauss gürültüsü değişiklik oranı 0.1 88

Şekil 57. Dayanıklılık saldırısı testi sonuçları 89

KISALTMALAR

Kısaltma		Türkçe	İngilizce
ACM	:	Arnold'un Kedi Kaotik Haritası	Arnold's Cat Map
AES	:	Gelişmiş Şifreleme Standartı	Advanced Encryption Standard
AZCM	:	Aizawa Kaotik Haritası	Aizawa Chaotic Map
BACM	:	Baker Kaotik Harita	Baker Chaotic Map
BCM	:	Bernoulli Kaotik Harita	Bernoulli Chaotic Map
BCR	:	Bit Geçerlilik Oranı	Bit Correct Ratio
BECM	:	Beta Kaotik Harita	Beta Chaotic Map
BGCM	:	Burger Kaotik Harita	Burger's Chaotic Map
BOGCM	:	Bogdanov Kaotik Harita	Bogdanov Chaotic Map
BSCM	:	Basin Kaotik Harita	Basin Chaotic Map
CCM	:	Kaotik Uç Harita	Chaotic Cusp Map
CHCM	:	Chialvo Kaotik Harita	Chialvo Chaotic Map
CHRCM	:	Chirikov Kaotik Harita	Chirikov Chaotic Map
CM	:	Kübik Harita	Cubic Map
CSCM	:	Chebyshev Kaotik Harita	Chebyshev Chaotic Map
CSM	:	Kaotik Singer Haritası	Chaotic Singer Map
CUHCM	:	Chua Kaotik Harita	Chua Chaotic Map
CWM	:	Kaotik Web Haritası	Chaotic Web Map
DES	:	Veri Şifreleme Standartı	Data Encryption Standard
DTPPM	:	Ayrık Zamanlı Kaotik Yırtıcı-Av Haritası	Discrete-Time Chaotic Predatory-Prey Map

GCM	:	Gingerbreadman Kaotik Harita	Gingerbreadman Chaotic Map
GLM	:	Gecikmeli Lojistik Harita	Delayed Logistic Map
GM	:	Gauss Harita	Gauss Map
GPCM	:	Gompertz Kaotik Harita	Gompertz Chaotic Map
GWCM	:	Gaussian Beyaz Kaotik Harita	Gaussian White Chaotic Map
HAPQM	:	Hénon Alan Korumalı İkinci Dereceden Harita	Henon Area-Preserving Quadratic Map
HCM	:	Henon Kaotik Harita	Henon Chaotic Map
HLCM	:	Holmes Kübik Harita	Holmes Cubic Map
ICM	:	Ikeda Kaotik Harita	Ikeda Chaotic Map
KDSA	:	Knutt-Dustenfeld Karıştırma Algoritması	Knutt-Dustenfeld Shuffle Algorithm
KYCM	:	Kaplan Yorke Kaotik Harita	Kaplan Yorke Chaotic Map
LCGM	:	Doğrusal Uyumlu Üreteç Haritası	Linear Congruential Generator Map
LCM		Lozi Kaotik Harita	Lozi Chaotic Map
LM	:	Lojistik Harita	Logistic Map
LRCM	:	Lorenz Kaotik Harita	Lorenz Chaotic Map
LSM	:	Lojistik Sinüs Harita	Logistic Sine Map
MAE	:	Ortalama Mutlak Hata	Mean Absolute Error
MCM	:	May Kaotik Harita	May Chaotic Map
MSE	:	Ortalama Karesel Hata	Mean Squared Error
NIST	:	Ulusal Standartlar ve Teknoloji Enstitüsü	National Institute of Standards and Technology
NPCR	:	Piksel Değişim Oranı	Number of Changing Pixel Rate
PM	:	Kıskaç Harita	Pinchers Map
PSNR	:	Tepe Sinyal Gürültü Oranı	Peak Signal to Noise Ratio

PWM	:	Parçalı Kaotik Harita	Piecewise Chaotic Map
RCM	:	Ricker Kaotik Harita	Ricker Chaotic Map
RMSE	:	Kök Ortalama Karekök Hata	Root Mean Squared Error
ROCM	:	Rossler'in Kaotik Haritası	Rosler's Chaotic Map
RSA	:	Rivest–Shamir–Adleman	Rivest–Shamir–Adleman
SCM	:	Sinüs Çemberi Haritası	Sine-Circle Map
SDCM	:	Sinüzoidal Kaotik Harita	Sinusoidal Chaotic Map
SDR	:	Sinyal Bozulma Oranı	Signal to Distortion Ratio
SICM	:	Sinai Kaotik Harita	Sinai Chaotic Map
SM	:	Kaotik Sinüs Haritası	Chaotic Sine Map
SNR	:	Sinyal Gürültü Oranı	Signal to Noise Ratio
SPM	:	Spens Harita	Spence Map
SSIM	:	Yapısal Benzerlik İndeksi	Structural Similarity Index
TCM	:	Tinkerbell Kaotik Harita	Tinkerbell Chaotic Map
TGCM	:	Trigonometrik Kaotik Harita	Trigonometric Chaotic Map
TM	:	Çadır Harita	Tent Map
UACI	:	Birleşik Ortalama Değişen Yoğunluk	Unified Averaged Changed Intensity
ZCM	:	Zaslavsky Kaotik Harita	Zaslavsky Chaotic Map

1. GİRİŞ

Günümüzde internet hemen her alanda ve cihazda yaygın olarak kullanılmaktadır. İnternet kullanımı ve teknolojik gelişmelerin artması ile günlük hayatımızda görüntü paylaşımını da beraberinde getirmiştir. Günlük hayatımızın hemen her anında çekilen bir görüntü ya sosyal medyada paylaşılmakta ya da kullandığımız mobil telefonlarda depolanmaktadır. Mobil telefonlarda tıpkı bilgisayarlar gibi saldırıya açık haldedirler. Açık halde bulunan ve gizliliğe sahip görüntüleri üçüncü şahıslardan korumanın en güvenli yollarından birisi görüntülerin şifrelenmesidir.

Bilgi güvenliğinin en temel alanlarından birisi şifreleme bilimidir. İnternetin hayatımıza girmesi ve hemen her alanda ve cihazda yaygın olarak kullanılması beraberinde şifreleme alanına olan ihtiyacı da paralel olarak hızla arttırmıştır (Sakal ve Yıldırım, 2016). Şifreleme, günümüz bilgi sistemlerinde ve teknolojilerinde son derece hayati bir öneme sahiptir. Bir depolama biriminde kayıt altına alınan veriler veya güvensiz bir ağ ortamında iletilen tüm veriler şifreleme yardımıyla okunamaz hale getirilmektedir. Okunamaz haldeki bu verilere sadece doğru anahtara veya yetkiye sahip kişiler erişebilmektedirler. Doğru anahtara sahip kişi okunamaz haledeki bu veriyi doğru anahtarla orijinal hale geri döndürmektedir. Böylelikle güvensiz ortamlarda bulunan ya da iletilen veriler yetkisiz erişimlerden korunmuş olmaktadırlar (Sakal, 2016).

Veri şifreleme yaklaşımları kayıplı ve kayıpsız şifreleme olarak iki guruba ayrılmaktadır. Kayıplı şifreleme yöntemlerinin görüntüler üzerine uygulanması esnasında görüntüde yönteme göre az veya çok miktarda bozulma meydana gelebilmektedir. Kayıpsız şifreleme yöntemlerinde ise görüntünün şifrelenmesi ve ardından çözülmesinden sonra elde edilen sonuç görüntüsü ile orijinal görüntü arasında piksel kayıplarının olmaması beklenmektedir. Bir başka ifadeyle görüntü çözünürlüğü ve kalitesinde herhangi bir azalma olmayacaktır.

Metin türündeki verilerin şifrelenmesi için AES (Gelişmiş Şifreleme Standartı, Advanced Encryption Standard), DES (Veri, Şifreleme Standartı, Data Encryption Standard) ve RSA, Rivest–Shamir–Adleman) gibi geleneksel veri şifreleme yöntemleri kullanılmaktadır (Yüksel ve Özgün, 2021). Geleneksel veri şifreleme yöntemleri

görüntülerin şifrelenmesinde son derece yetersiz kalmaktadırlar. Bunun en temel iki nedeni bulunmaktadır. İlk nedeni, görüntü verilerinin boyut olarak metin verilere göre çok daha fazla veri içermesidir. İkinci nedeni ise metin türündeki verilerin çözülmesinde veri kayıpları çok az olurken görüntüler üzerinde renk ve bit gibi görüntünün yapısına zarar veren çok ciddi kayıplar yaşanabilmektedir. Bu durum bazen gözle fark edilemeyecek kadar küçük, bazı durumlarda da görüntüye bakıldığında kolaylıkla anlaşılabilecek boyutlarda olabilmektedir (Ceyhan ve Yolaçan, 2021).

1.1 Problem

İnternet kullanımının yaygın hale gelmesi ve teknolojik gelişmelere paralel olarak insanlar günlük hayatlarında yüzlerce fotoğraf çekmektedir. Zaman içerisinde artan fotoğraflar güvenlik problemlerini de beraberinde getirmektedir (Zolfaghari ve Koshiba, 2022). Görüntülerin telefon, bilgisayar, tablet ve taşınabilir belleklerde saklanması ve bunların kaybolması ya da istenmeyen kişilerin eline geçmesi durumlarında açık halde bulunmaktadırlar (Ceyhan ve Yolaçan, 2021). Dolayısı ile bu ortamlarda bulunan verilerin istenmeyen kişilerin eline geçmesi çok ciddi sonuçlara neden olabilecektir. Bu gibi durumların önüne geçilebilmesi ancak kişisel görüntülerin şifrelenerek saklanması ile mümkün olabilmektedir.

Şifreleme biliminin günümüzde büyük bir öneme sahip olmasının ana nedeni internet kullanımının artmasıdır (Elkandoz ve Alexan, 2022). Kullanıcılar arasında önemli olan verilerin karşı tarafa güvenli iletiminde şifreleme yöntemlerine ihtiyaç duyulmaktadır. Şifreleme, verileri okunamayan veya anlaşılamayan bir hale dönüştürerek koruma sağlamaktadır. Bu sayede verilere ancak yetkisi olan kullanıcılar erişebilmekte ve verilerin gizliliği ve güvenliği sağlanmaktadır. Gizlenmiş veriye sadece veriye erişim izni olan kullanıcılar ulaşabilmektedir. Günümüzde araştırmacıların karşılaştığı zorlukların başında, verilerin dijital ağlar üzerinden iletimi sırasında iletim kanallarının nasıl korunması gerektiği gelmektedir (Kumari, Gupta, ve Sardana, 2017). Veri türüne bağlı olarak kullanılan sistemlerin ve şirketlerin, güvenlik ihtiyacının artması bilim insanlarını kriptoloji alanında çalışma yönlendirmiştir. Verilerin güvenliğinin sağlanması, güvenli bir biçimde verilerin saklanması ve hedef alıcıya aktarılması şifreleme sistemlerinin en temel amaçlarındandır.

Benzer biçimde tıbbi ve askeri alanlarda kullanılan bilgiler ve görüntüler son derece değerli bilgilerdir. Bu tür veriler son derece gizli ve hem de kişisel veriler içermektedir. Bu nedenle verilerin bütünlüğünü ve güvenliğini sağlamak, olabilecek güvenlik saldırılarında ve bilgi kaybını önlemede şifreleme büyük öneme sahiptir. Şifreleme süreçleri için literatürde birbirinden farklı algoritmalara ve özelliklere sahip yöntemler bulunmaktadır. Bu yöntemlerin farklılıkları hız, karmaşıklık, yük, maliyet, bellek gereksinimi, bilgi kaybı, saldırılara karşı duyarlılık gibi durumlara göre çeşitlilik göstermektedir. Şifreleme algoritmaları, verilerin şifrelenmesi ve deşifrelenmesi (çözümlenmesi) algoritmalarını kullanılmaktadır. Şifreleme algoritmaları ile veriler anlaşılamaz bir hale getirilerek şifrelenmiş veri elde edilir. Şifre çözme (deşifreleme) algoritmaları ile şifrelenmiş veriler anlaşılır ve anlamlı hale getirilmektedir.

Verilerin şifrelenmesinde geleneksel yöntemler kullanılsa da bu yöntemlerin görüntülerde kullanılması uygun değildir (Kaur ve Kumar, 2020). Bunun temel nedeni görüntülerin çok yüksek oranda veri içermesinden kaynaklanmasıdır. Bu nedenle görüntülerin şifrelenmesi için farklı tekniklerin kullanılması gerekmektedir. Pek çok çalışmada bu tekniklerin sadece bazıları kullanılmaktadır. Ayrıca kullanılacak yöntemlerin bir arada yer aldığı çalışmalar bulunmamaktadır. Literatürde mevcut olan çalışmalarda bilinen kaotik haritalara yer verilmiş, var olan ve etkili olabilecek diğer kaotik haritaların göz ardı edildiği gözlemlenmiştir.

1.2 Amaç

Bu çalışmada, görüntülerin şifrelenmesi için yaygın olarak kullanılan kaotik haritalar ile az kullanım imkânı bulmuş kaotik haritalar incelenerek tüm özellikleri ayrıntılı olarak ortaya konacaktır. Kaotik haritaların avantaj ve dezavantajları göz önüne alınarak hibrit bir görüntü şifreleme yöntemi önerilecektir. Ayrıca görüntülerin şifrelenmesinin ardından önerilen yöntemlerin dayanıklılıklarını test etmek için kullanılan yöntemler de ayrıntılı olarak ele alınacaktır.

1.3 Önem

Bu çalışma ile görüntü şifrelemede kullanılan kaotik yöntemler ayrıntılı olarak incelenecek avantaj ve dezavantajları ortaya konacaktır. Kaotik yöntemler görüntü

şifreleme algoritmalarında son derece önemli bir yer tutmaktadır. Bu yöntemlerin bir arada yer aldığı ve incelendiği kaynaklar bulunmaması bu çalışmanın önemini arttırmaktadır. Ayrıca şifreleme sonrası güvenilirlik testlerinin de bu çalışma ile bir araya getirilmesi önerilecek yöntemlerin test edilmesinde bir kılavuz görevi görecektir.

1.4 Varsayımlar

Görüntü şifrelemede kaotik yapılar dışında yöntemlerde kullanılmaktadır ancak literatür çalışmaları incelendiğinde yapılan çalışmaların büyük bir çoğunluğunun kaotik haritaları kullandığı görülmektedir. Bu nedenle bu tez çalışmasında sadece kaotik yapılar ele alınmış ve diğer yöntemler kapsam dışı bırakılacaktır.

1.5 Sınırlıklar

Çalışmada varsayımlar bölümünde belirtilen kaotik yapılar incelenecek ve şifrelemede kullanılan diğer yöntemlere yer verilmeyecektir. Ayrıca kaotik yapıların performanslarını karşılaştırabilmek için standart ölçülerde ve aynı özelliklerde görüntüler kullanılacaktır.

1.6 Tanımlar

Çalışmada kullanılacak terimlerin ayrıntılı tanımlarına aşağıda yer verilmiştir.

Görüntü: Gerçekte var olmadığı hâlde gözümüze varmış gibi görünen ya da zihinde beliren, yer eden şeye verilen addır. Diğer bir anlamıyla görüntü, çeşitli araçlar yardımıyla insan gözünün görebilmesi için oluşturulan görünümdür.

Görüntü İşleme: Sayısal görüntü işleme, endüstriyel uygulamalarda bilgisayarla bütünleşik olarak kullanılabilen bilgisayar çalışmalarıdır. Görüntü işleme teknikleri ile nesne tanıma işlemleri yapılabilmekte, sayısal görüntü verileri iyileştirilebilmekte ve birbirinden farklı görüntüler elde edilebilmektedir. Görüntü işleme birbirini takip eden bir dizi işlemden meydana gelmektedir. Bu işlemler görüntünün elde edilmesi ile başlamakta ve amaca uygun farklı tekniklerin kullanılması ile devam etmektedir. Görüntü işleme uygulamaları kendi içerisinde matematik ve bilgisayar bilimi içermektedir. İmalat, tasarım, tıp, güvenlik, makine, mimari elektronik ve jeodezi gibi daha pek çok alanda yaygın olarak kullanılmaktadır (Samtaş ve Gülesin, 2011).

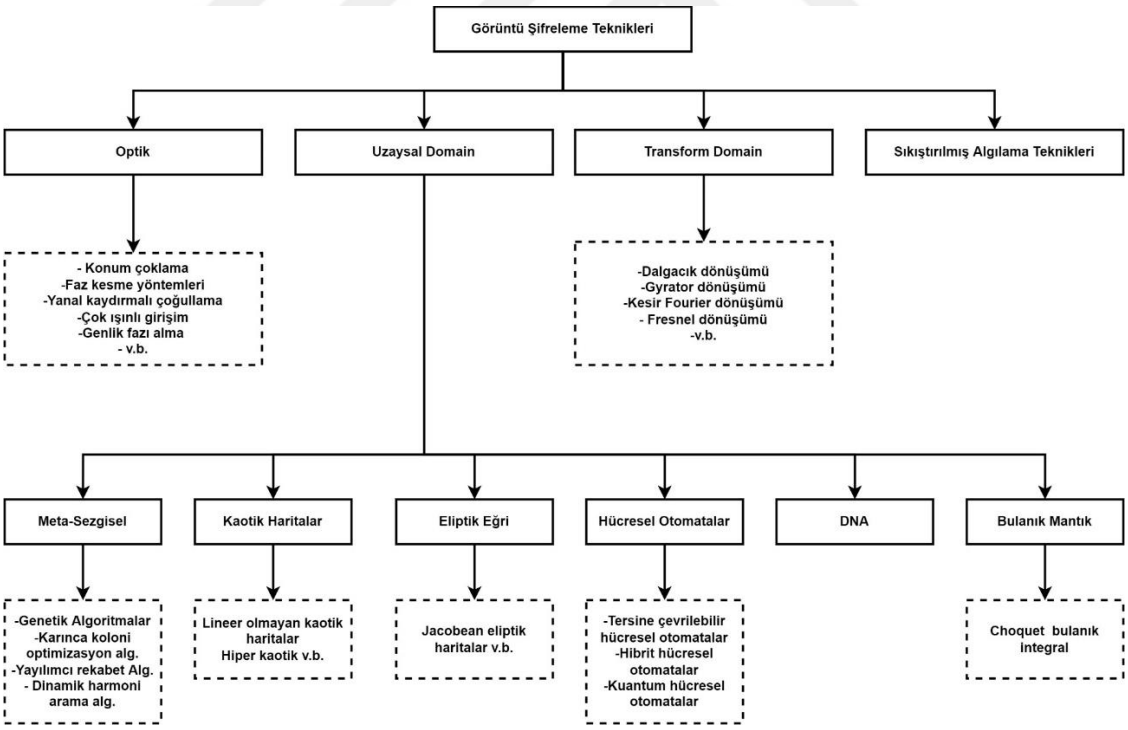
Şifreleme: Şifreleme bilimi kriptoloji olarak adlandırılmakta ve gönderilen özel mesajların güvenliğini sağlamak için gönderici ile alıcı arasına istenmeyen üçüncü kişilerin girmesini engelleyen bir bilim dalıdır. Başka bir ifadeyle kriptoloji, anlamlı halde olan bir verilerin şifreleme teknikleri kullanılarak istenmeyen kişilerin araya girmemesi için anlamsız hale getirilmesi sürecidir (Okuyucu, 2020).

Görüntü Şifreleme: Görüntü dosyalarında yer alan piksellerin belli yöntemler ile karıştırılması ve anlaşılmaz hale getirilmesidir (Sakal, 2016).

Kaotik Sistem: Kaotik sistem, kısaca, "başlangıç şartlarına bağlı olan yani hassas bağlılık gösteren ve ölçülemeyecek biçimde karmaşıklıkta sistemler" olarak tanımlanmaktadır. Kaos bilimine göre, kaotik sistemlerin başlangıç koşullarındaki çok küçük bir değişiklik, sistemin gelecekteki diğer durumlarında ölçülemeyecek kadar çok büyük değişikliklere neden olabilmektedir (Yardım ve Afacan, 2010).

2. LİTERATÜR ARAŞTIRMASI

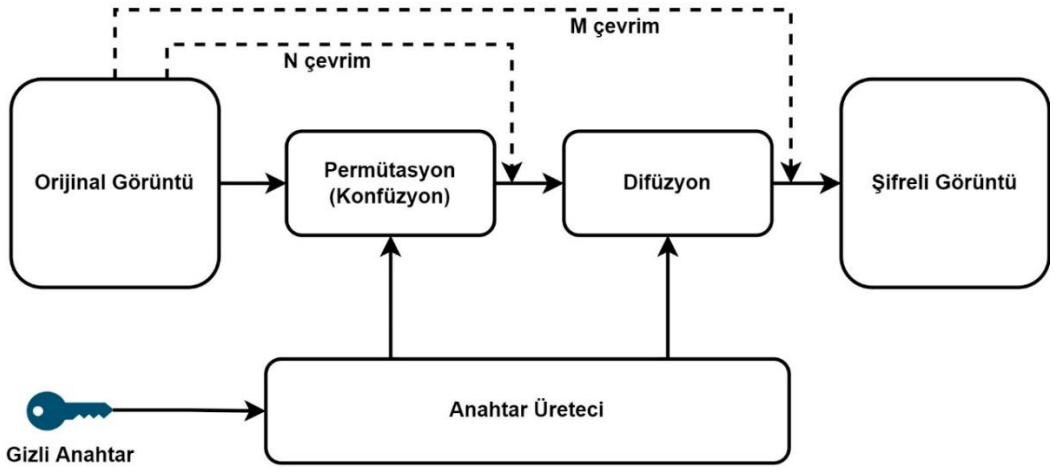
Günümüzde internet yaygın bir biçimde kullanım alanı bulmuştur. Bu durum mobil cihazlarda multimedya uygulamalarının kullanımını da arttırmıştır. Mobil cihazlar, görüntü elde edilmesini ve paylaşımını kolay hale getirmiştir. Bu durum çeşitli güvenlik problemlerinin ortaya çıkmasına neden olmuştur. Bu durumu ortadan kaldırmanın ve görüntü verilerinin istenmeyen kişilerin eline geçmesini engellemenin en etkili yolu görüntülerin şifrelenmesidir. Multimedya uygulamalarının artması ve mobil cihazlarda veri paylaşımının artması da bilim insanlarının görüntü şifreleme alanında çalışmalar yapmasına olanak sağlamıştır. Görüntü şifreleme yöntemleri zaman içerisinde evrilmiş ve birbirinden farklı teknikler ortaya atılmıştır. Bu teknikler kendi içinde sınıflandırılmıştır. Bu sınıflandırmalardan bir tanesi (Kaur ve Kumar, 2020) tarafından yapılmış ve Şekil 1'de verilmiştir.



Şekil 1. Görüntü şifreleme yöntemlerinin sınıflandırılması

Bu çalışmada görüntü şifreleme sınıflarından olan kaotik haritalar üzerinde durulmakta ve sadece kaotik sistem kullanan görüntü şifreleme tekniklerine ait literatür araştırmalarına yer verilmektedir. Görüntü şifreleme alanında geçmişten günümüze çok fazla sayıda çalışma bulunmaktadır. Bu nedenle bu bölümde bazı önemli çalışmalar hariç son beş yıl içerisinde yapılan ve en yüksek atıf alan çalışmalara yer verilmektedir.

Kaotik haritalar, kendi yapıları gereği kaotik bir davranış sergilemekte ve dinamik ortamlarda kullanılmaktadır. Bu sistemlerin başlangıç koşularında yapılacak çok küçük değişiklikler elde edilecek çıktılarda da yine büyük değişikliklere neden olmaktadır. Kaotik haritalar, görüntü şifreleme tekniklerinde kullanıldıklarında şifrenin görüntü üzerinde kullanılmasını sağlayabilmek için görüntü difüzyon ve permütasyon olmak üzere iki aşamaya bölünmektedir (Gu ve Ling, 2014). Gerçek zamanlı uygulamalarda kripto sistem geliştiricileri güvenilir bir yöntem elde edebilmek için permütasyon ve difüzyon aşamalarını geliştirdikleri sistemlere entegre etmektedirler (X. Huang ve Ye, 2014). Permütasyon veya karıştırma sürecinde düz görüntü, belirli bir yöntemden üretilen rastgele diziler kullanılarak karıştırılmaktadır. Rastgele dizinin üretilmesi gizli bir anahtara bağımlıdır. Difüzyon aşamasında ise karıştırılmış olan görüntü kendi içerisinde birkaç bloğa ayrıştırılmaktadır. Bunun nedeni kaotik haritanın başlangıç koşullarının belli aralıklar ile güncellenmesini sağlamaktır (Geetha, Punithavathi, Infanteena, ve Sindhu, 2018). Şekil 2'de kaos tabanlı görüntü şifreleme tekniklerinin süreci gösterilmektedir.



Şekil 2. Kaotik haritaların görüntü şifrelemede kullanılması süreci

Kaotik haritalar, güvenli iletişimde yaygın olarak kullanılmaktadır. Ayrıca veri güvenliği ile hesaplama hızı arasındaki dengeyi sağlayan bir unsur olarak kabul edilmektedir (Gu ve Ling, 2014). Bu nedenlerden dolayı kaotik haritalar farklı görüntü şifreleme uygulamalarında yaygın olarak kullanılmıştır. Kaos tabanlı görüntü şifreleme tekniklerini kullanan bazı çalışmalara ait literatür taraması aşağıda yer almaktadır.

Kaos tabanlı görüntü şifreleme yöntemlerine bakıldığında en sık kullanılan yöntemin lojistik harita (LM, Logistic Map) olduğu görülmüştür. LM'i kullanarak görüntülerin şifrelenmesini sağlayan bir yöntem (Ye ve Huang, 2017) tarafından önerilmiştir. Bu çalışmada standart LM geliştirilerek üç boyutlu LM haline getirilmiştir. Simetrik bir şifreleme yöntemidir. Yöntem gri seviye görüntüler üzerinde test edilmiş ve başarılı sonuçlar elde edildiği görülmüştür. Gri seviye görüntüler üzerinde LM'yi kullanarak şifreleme yapılan bir yöntem (Rostami, Shahba, Saryazdi, ve Nezamabadi-pour, 2017) tarafından önerilmiştir. Görüntü kendi içerisinde bloklara ayrılmış ve ayrılan bloklar LM'den elde edilen kaotik değerler ile XOR işlemine tabi tutularak şifrelenmiştir. Renkli görüntüler günlük hayatımızın her alanında karşımıza çıkmaktadır. Renkli görüntüleri ve LM'yi kullanan bir yöntem (H. Huang ve Yang, 2017) tarafından sunulmuştur. Görüntüyü karıştırmak için öncelikle LM elde edilmektedir. Ardından her bir renk katmanı (RGB) bu harita yardımıyla karıştırma işlemine tabi tutulmaktadır. Bazı çalışmalarda LM çift katmanlı olarak kullanılmıştır. (Safi ve Maghari, 2017) tarafından sunulan yöntemde aşamalı olarak LM elde edilmektedir. İlk aşamadan elde edilen harita ile başka bir anahtar yardımıyla elde edilen LM, XOR işlemine tutulmakta ve görüntü şifrelenmektedir. Yöntem gri seviye görüntüler üzerinde etkili sonuçlar vermektedir. LM farklı çalışma alanlarında kullanılmıştır. Biyomedikal alanında bir çalışma (Ismail vd., 2017) tarafından yapılmıştır. Çalışmada iki boyutlu LM kullanılmıştır. İki boyutlu LM'den elde edilen rastgele değerler yardımı ile biyomedikal görüntülerin karıştırılması ve şifrelenmesi sağlanmıştır. Birbirleri ile birlikte kullanılan kaotik haritalarda bulunmaktadır. LM ve Baker kaotik haritayı (BACM, Baker Chaotic Map) bir arada kullanan bir yöntem (Yuqin Luo, Yu, Lai, ve Liu, 2019) tarafından önerilmiştir. Yöntemde BACM'nin denklem sistemi LM denklemine ait parametrelere entegre edilmiş ve yeni kaotik bir harita sunulmuştur. Tek boyutlu LM, düzensiz dağılım, düşük güvenlik ve küçük parametre alanı gibi bazı dezavantajlara sahiptir. Bu dezavantajların üstesinden gelmek için (R. Li, Liu, ve Liu, 2019) tarafından rastgele seçilmiş bir ondalık sayı ile

gerçek zamanlı değişken LM temelli yeni bir kaotik harita yöntemi önerilmiştir. Yöntem ile tek boyutlu LM'nin dezavantajları ortadan kaldırılmış ve iki boyutlu bir harita geliştirilerek görüntü şifrelemeye uygulanmıştır. LM'lerin dezavantajlarını ortadan kaldırmak için bir başka çalışmada (Xiang ve Liu, 2020) tarafından yapılmıştır. Yöntemde LM, geri beslemeli kaotik sinüs haritası (SM, Chaotic Sine Map) ile desteklenerek daha kullanılabilir, güvenlik ve etkili bir şifreleme yöntemi geliştirilmiştir. Görüntü şifrelemede işlem yükünün azaltılması için bazı durumlarda görüntü bloklara ayrılmaktadır. Bloklara ayırma gerçek zamanlı uygulamalarda performansı arttırmaktadır. (A. A. Shah, Parah, Rashid, ve Elhoseny, 2020) tarafından önerilen bir yöntemde LM'ye dayalı ve verimli bir permütasyon kullanan bir yöntem önerilmiştir. Görüntü küçük bloklara ayrılmaktadır. Yöntem 192 bitlik bir anahtar kullanmakta ve her bir blokta görüntü piksellerinin dağıtılması için XOR işlemine başvurulmaktadır. Görüntü şifrelemenin belirli bir aşamasında XOR ve LM kullanan bir yöntem (Muñoz-Guillermo, 2021) tarafından önerilmiştir. Yöntemde öncelikle görüntü pikselleri XOR işlemine tutulmakta ardından satır ve sütun pikselleri LM'den elde edilen değerlere göre ötelenmektedir. Son aşamada da yine XOR operatörüne başvurularak şifreli görüntü elde edilmektedir.

Görüntülerin şifrelenmesi sürecinde farklı kaotik haritalarda kullanılmaktadır. Bu şifreleme sürecinde kullanılan kaotik haritalardan biride kübik haritadır (CM, Cubic Map). CM'yi kullanan çok fazla çalışma literatürde bulunmamaktadır. CM'yi kullanan yöntemlerden biri (Yang, Min, ve Wang, 2015) tarafından önerilmiştir. Yöntemde CM denkleminden elde edilen değerler yardımı ile görüntü pikselleri karıştırılarak şifrelenmiştir. Yöntem renkli görüntüler üzerinde uygulanmış fakat güvenlik testlerine yer verilmemiştir. CM'yi kullanan bir başka yöntem ise (Yahi, Bekkouche, Daachi, ve Diffellah, 2022) tarafından önerilmiştir. Üssel bir fonksiyon yardımı ile CM'den değerler elde edilerek renkli görüntü piksellerinin karıştırılması sağlanmıştır. Yöntemin performansı test edilmiş ve başarılı sonuçlar elde edildiği görülmüştür. (Xu ve Zhen, 2022) tarafından önerilen bir yöntemde ise CM ve henon kaotik harita (HCM, Henon Chaotic Map) birlikte kullanılmıştır. Yöntemde CM'den elde edilen değerler ve HCM'den elde edilen değerler görüntü şifreleme sürecinin farklı aşamalarında kullanılmıştır.

Rastgele sayılar görüntülerin şifrelenmesinde son derece önemli bir yere sahiptir. Görüntü şifrelemenin kalitesini arttırmak, iyileştirmek ve piksellerin karıştırılmasını sağlamak amacı ile kaos tabanlı doğrusal uyumlu üreteç haritası (LCGM, Linear Congruential Generator Map) kullanan bir yöntem (Sukhjeevan ve Shaveta, 2015) tarafından önerilmiştir. Önerilen algoritma, görüntülerde satır karıştırma, sütun karıştırma ve tüm pikselleri karıştırmada kullanılan rasgele sayılar üretmektedir. Rastgele sayıların kullanılması önerilen şifreleme tekniğinin kriptanalitik saldırılara karşı oldukça dirençli olmasını sağlamaktadır. LCGM'yi rastgele sayı üretmek ve görüntü şifrelemede kullanmak için bir başka yöntemde (AbdElHaleem, Abd-El-Hafiz, ve Radwan, 2022) tarafından önerilmiştir. Bu yöntemde benzer şekilde şifreleme sürecinde sadece rastgele sayıların üretilmesinde kullanılmış ve görüntüler şifrelenmiştir.

Kaotik Sinüs Haritası (SM, Chaotic Sine Map) görüntü şifrelemede kullanılan bir başka kaotik harita türüdür. SM kullanan bir çalışma (Yosefnezhad Irani, Ayubi, Amani Jabalkandi, Yousefi Valandar, ve Jafari Barani, 2019) tarafından önerilmiştir. Çalışmanın asıl amacı LM ve SM'deki anahtar uzayını arttırmaktır. Çalışmada tek boyutlu SM geliştirilmiş, anahtar uzayı genişletilmiş ve görüntülerin şifrelenmesinde kullanılmıştır. Şifreleme süreci görüntünün kendi içerisinde farklı bloklara ayrılması ile gerçekleştirilmiştir. Benzer bir biçimde SM'nin geliştirmesi ve kullanılması için bir çalışma (Y. Liu, Qin, Liao, ve Wu, 2020b) tarafından yapılmıştır. Yöntem, SM'den elde edilen değerler yardımıyla görüntü piksellerinin belirli aşamalarda XOR işlemine tabi tutulması ile şifreleme sürecini gerçekleştirmektedir. SM, görüntü şifrelemek amacıyla genellikle diğer kaotik haritalar ile birlikte hibrit bir şekilde kullanılmıştır. HCM ve SM (Wu, Liao, ve Yang, 2018) ve (M. Li, Xu, Luo, ve Fan, 2019) tarafından birlikte kullanılmıştır. Benzer şekilde LM ve SM hibrit bir şekilde lojistik sinüs harita (LSM, Logistic Sine Map) olarak literatüre girmiştir. LSM, (Elkandoz, Alexan, ve Hussein, 2019), (Zheng ve Liu, 2020), (Parameshachari, 2021), (Feng, He, Li, ve Li, 2019) ve (Hua, Jin, Xu, ve Huang, 2018) tarafından görüntü şifrelemek amacı ile kullanılmıştır. (Elkandoz vd., 2019) tarafından yapılan çalışmada Arnold kedi haritası (ACM, Arnold Cat Map) ile de yöntem daha güçlü hale getirilmiştir. Görüntü önce ACM ile karıştırılmış ardından SM ile 256 bitlik anahtar üretilmiş ve şifreleme yapılmıştır. (Zheng ve Liu, 2020), (Feng vd., 2019) ve (Hua vd., 2018) tarafından yapılan çalışmalarda tek boyutlu SM geliştirilerek iki boyutlu hale getirilmiş ve görüntülerin şifrelenmesi sağlanmıştır.

(Parameshachari, 2021) tarafından yapılan çalışmada ise görüntü önce bloklara ayrılmış ve ardından SM'den elde edilen değerler yardımıyla piksellerin karıştırılması sağlanmıştır. (H. Liu, Wen, ve Kadir, 2019) tarafından önerilen bir yöntemde ise Chebyshev kaotik haritası (CSCM, Chebyshev Chaotic Map), SM ile birlikte hibrit bir biçimde kullanılmıştır. Yöntemde her aşamadan sonra XOR işlemi kullanılmış ve görüntüde istenen şifreleme etkisinin elde edilmesi sağlanmıştır. Diğer hibrit yöntemlerden farklı bir hibrit yöntem ise (Sangavi ve Thangavel, 2020) tarafından önerilmiştir. Yöntemde Rossler kaotik sistemi (ROCM, Rossler Chaotic Map) ve SM birlikte kullanılmıştır. İlk aşamada görüntü parçalara ayrılmıştır. Parçalara ayrılan görüntüler, ROCM ve SM yardımıyla karıştırılarak görüntülerin şifrelenmesi sağlanmıştır.

Görüntülerin şifrelenmesi için literatürde çadır harita (TM, Tent Map) yöntemi de sıklıkla tercih edilmektedir. TM görüntü şifrelemek amacıyla (C. Li, Luo, Qin, ve Li, 2017) tarafından kullanılmıştır. Kaotik harita değerleri ile görüntüye ait her bir piksel XOR işlemine tabi tutulmakta ve görüntülerin şifrelenmesi sağlanmaktadır. Benzer bir çalışma (Naskar, Bhattacharyya, Nandy, ve Chaudhuri, 2020) tarafından yapılmıştır. Görüntü kendi içerisinde bloklara ayrılmış ve her bir blok TM'den elde edilen farklı anahtarlar ile şifrelenmektedir. TM'nin geliştirilmiş hali çarpık çadır haritadır. Bu harita türü (Mondal, Singh, ve Kumar, 2019), (J. Ahmad, Khan, Ahmed, ve Khan, 2018), (Essaid, Akharraz, Saaidi, ve Mouhib, 2018), (Elmanfaloty ve Abou-Bakr, 2020) ve (Roy, Chakraborty, ve Mali, 2020) tarafından gerçekleştirilen görüntü şifreleme yöntemlerinde kullanılmıştır. Bu yöntemlerin tamamında standart TM geliştirmiş ve literatüre kazandırılmıştır. (Mondal vd., 2019) tarafından yapılan çalışmada öncelikli olarak rastgele sayı üreteçleri yardımıyla bir sayı dizisi oluşturulmaktadır. Ardından elde edilen sonuç görüntüsü TM'den elde edilen 128 bitlik bir şifre yardımıyla şifrelenmektedir. (J. Ahmad vd., 2018) tarafından önerilen yöntemde görüntü öncelikle ortagonal bir matris yardımıyla bir dizi karıştırma işlemine tabi tutulmaktadır. Elde edilen sonuç görüntüsü ile TM'den elde edilen değerler yardımı ile tüm pikseller XOR işlemine tabi tutulmaktadır. (Essaid vd., 2018) tarafından sunulan yöntemde ise başlangıçta TM yardımıyla anahtar dizisi oluşturulmaktadır. Sonraki aşamada görüntü 1 x 256 boyutlarında bloklara ayrılmakta ve geleneksel karıştırma yöntemleri ile görüntü pikselleri karıştırılmaktadır. Tek boyutlu kaotik haritalar güvenlik açıkları nedeniyle tercih edilmemektedir. Bu sorunu ortadan

kaldırmak amacıyla (Elmanfaloty ve Abou-Bakr, 2020) tarafından yine tek boyutlu fakat daha güvenli bir yöntem önerilmiştir. Yöntemde başlangıç parametrelerine ek olarak beş parametre daha tanımlanarak yeni bir kaotik TM önerilmiştir. (Roy vd., 2020) tarafından sunulan TM'ye dayalı görüntü şifreleme yönteminde ise çarpık çadır harita yöntemi başlangıç parametrelerinin haricinde 72 bit uzunluğunda anahtar üretimi için kullanılmıştır. Bazı işlemlerden sonra bu uzunluk 64 bitlik dâhili anahtara indirgenmiş ve görüntünün her bir pikseli değişikliğe uğratılarak şifrelenmiştir. Dâhili anahtar bazı temel işlemlerde güvenliği arttırmak için kullanılmıştır.

Gauss harita (GM, Gauss Map), aynı zamanda sözde rasgele sayı üreten kaotik bir harita türüdür. Bu özelliğinden dolayı bazı görüntü şifreleme yöntemlerinde kullanılmıştır. GM, literatürde fare haritası (Mouse Map) olarak da adlandırılmaktadır. Bu harita türünü kullanan bir çalışma (Sahay ve Pradhan, 2017a) tarafından yapılmıştır. Yöntem renkli görüntüler üzerinde çalışmaktadır. İlk olarak görüntü RGB kanallarına ayrılmaktadır. Ardından her bir kanal GM'den elde edilen değerler ile XOR işlemine tabi tutularak şifrelenmektedir. Son aşamada ise birbirinden ayrık halde olan kanallar birleştirilerek sonuç görüntüsü elde edilmektedir. Benzer bir biçimde görüntü piksellerinin GM yardımıyla karıştırılmasını sağlayan bir yöntem de (Chandra ve Sharma, 2017) tarafından önerilmiştir. Başlangıç anahtarına bağlı olarak GM üretilmiş ve harita değerleri yardımıyla görüntü pikselleri karıştırılmıştır. Bu yöntemler tek boyutlu olduğundan saldırılara son derece açıktır. Yüksek boyutlu kaotik haritalar artan sistem parametreleri nedeniyle olağanüstü kaotik davranışa ve karmaşık yapıya sahiptirler. Bu nedenle, düşük dereceli kaotik haritanın eksikliklerinin üstesinden gelmek için bir yöntem (Salunke, Ahuja, Hashmi, Marriboyina, ve Bokde, 2022) tarafından önerilmiştir. Önerilen yöntem tek boyutlu GM'nin bir uzantısı ve beş boyuttan oluşmaktadır. İlk olarak orijinal görüntünün her bir satırı beş boyutlu GM'den elde edilen değerler ile karıştırılmaktadır. Ardından aynı işlem sütundaki pikselleri içinde uygulanmaktadır. Aynı süreç iki defa tekrarlanmaktadır. Son aşamada ise GM'den elde edilen bir değer ile XOR işlemine tabi tutularak görüntünün şifrelenmesi tamamlanmaktadır. Çok boyutlu GM kullanan bir başka çalışma (Sahay ve Pradhan, 2017b) tarafından yapılmıştır. Renkli görüntü RGB kanallarına ayrılmakta ve her bir kanalı şifrelemek için GM'den birbirinden farklı rastgele diziler elde edilmektedir. Her bir kanal bu diziler yardımıyla XOR işlemine tutularak piksellerin şifrelenmesi sağlanmaktadır.

Parçalı kaotik harita (PWM, Piecewise Chaotic Map), literatürde görüntü şifrelemede sıklıkla kullanılan haritalardan birisidir. (Yuling Luo, Zhou, Liu, Cao, ve Ding, 2018) tarafından önerilen bir yöntemde ilk olarak düz görüntü ve harici bir anahtar kullanılarak iki ondalık sayı elde edilmektedir. Bu elde edilen değerler parçalı kaotik harita için başlangıç değeri olarak kullanılmaktadır. Sonraki aşamada parçalı kaotik harita ve hiper kaotik harita yardımıyla bir şifreleme matrisi oluşturularak görüntülerin şifrelenmesi sağlanmaktadır. (Zhong, Liu, Sun, Lan, ve Luo, 2018) tarafından önerilen yöntemde PWM, SM ile birleştirilerek hibrit bir sistem ortaya atılmıştır. Yöntemde başlangıç değerlerine bağlı olarak her iki haritadan da kaotik bir dizi yaratılmış ve elde edilen dizi ile görüntünün şifrelenmesi sağlanmıştır. Fourier dönüşümü pek çok alanda yaygın olarak kullanılmaktadır. (Agarwal ve Patidar, 2018) tarafından önerilen bir yöntemde görüntü şifrelemek amacı ile Fourier dönüşümünden ve PWM'den faydalanılmıştır. Görüntü öncelikle Fourier dönüşümüne tabi tutulmuş ve ardından elde edilen sayısal sinyal değerleri PWM ile desteklenerek görüntülerin şifrelenmesi sağlanmıştır. (Sinha ve Sahu, 2018) tarafından yapılan bir çalışmada yarasa optimizasyon problemi PWM ile birlikte kullanılmıştır. Bu iki yöntem birlikte kullanılarak gizli anahtarın üretilmesi sağlanmıştır. Elde edilen 128 bitlik anahtar yardımıyla görüntü piksellerinin karıştırılması ve değerlerinin değiştirilmesi sağlanarak görüntü şifreleme yapılmıştır. PWM ile TM'nin birleştirilerek görüntülerin şifrelenmesini sağlayan hibrit bir sistem (X. Wang ve Yang, 2021) tarafından önerilmiştir. Yöntemde orijinal görüntüden SHA-512 anahtarlama algoritması ile 400 bitlik bir anahtar üretilmiştir. Üretilen bu anahtar parçalara ayrılarak kaotik haritaların başlangıç değerleri olarak sisteme verilmiş ve görüntü piksellerinin karıştırılması sağlanmıştır. SM ile PWM'nin birleştirilmesi ile kullanılan bir görüntü şifreleme yöntemi (J. Liu, Wang, Liu, ve Zhu, 2021) tarafından sunulmuştur. Birleştirilmiş SM ve PWM'nin başlangıç değerlerine bağlı olarak karıştırma dizisi değerleri elde edilmiş ve elde edilen dizi değerleri yardımıyla piksellerin karıştırılması sağlanmıştır. Tek boyutlu PWM kullanan bir yöntem (Elghandour, Salah, Elmasry, ve Karawia, 2021) tarafından önerilmiştir. Bu yöntem, PWM ve TM'yi kullanan hibrit bir yöntemdir. Öncelikle görüntü kendi içerisinde parçalara ayrılmış sözde rastgele sayı üreteçleri yardımıyla karıştırılmıştır. Son aşamada PWM ve TM'den elde edilen dizi değerleri ile XOR işlemine tutularak görüntünün şifrelenmesi sağlanmıştır. Anahtarlama algoritmaları pek çok şifreleme algoritmasında yaygın olarak kullanılmaktadır. RC4

anahtarlama algoritması ve PWM kullanılarak görüntülerin şifrelenmesini sağlayan bir yöntem (Ahmed, Jawad, ve Jawad, 2021) tarafından önerilmiştir. İlk olarak sözde rastgele sayı üreteci kullanılarak şifrelenecek görüntü boyutlarında bir anahtar dizisi oluşturmaktadır. İkinci bir anahtar dizisi ise RC4 anahtarlama algoritması kullanılarak üretilmektedir. Bu anahtar dizileri ve PWM değerleri yardımıyla görüntü pikselleri bir dizi karışık XOR işlemine tabi tutularak görüntünün şifrelenmesi sağlanmaktadır. Sözde rastgele sayı üreteçlerini ve PWM'i kullanan bir başka çalışma (Charalampidis, Volos, Moysis, Nistazakis, ve Stouboulos, 2022) tarafından yapılmıştır. Yöntemde PWM ve sözde rastgele sayı üreteci yardımıyla görüntü pikselleri karıştırılmakta ve ardından XOR işlemine tabi tutularak görüntüler şifrelenmektedir. S kutuları da benzer şekilde şifreleme alanında yaygın kullanılmaktadır. PWM yardımıyla S kutusu üretilen ve görüntü şifrelemede kullanılan bir yöntem (Hoseini, Behnia, Sarmady, ve Fathizadeh, 2022) tarafından önerilmiştir. Yöntemde PWM yardımıyla şifrelemede kullanılacak S kutuları elde edilmektedir. Elde edilen S kutuları yardımı ile görüntü pikselleri XOR işlemine tutularak görüntülerin şifrelenmesi sağlanmaktadır.

Kaotik şarkıcı haritası (CSM, Chaotic Singer Map)'nın görüntü şifrelemek amacıyla kullanımına ilişkin literatürde var olan tek çalışma (Karim, Abdalqader, Najim, Salhd, ve Abdulhammed, 2021) tarafından yapılmıştır. Yöntem dört aşamadan oluşmaktadır. İlk aşamada orijinal renkli görüntü sekiz parçaya bölünmekte ve karıştırılmaktadır. İkinci aşamada RGB renk kanallarına ait pikseller ikili koda dönüştürülmektedir. Üçüncü aşamada CSM ile gizli anahtarlar üretilmektedir. Dördüncü aşamada RGB katmanlarının her biri ayrı ayrı CSM'den elde edilen anahtar ile XOR işlemine tabi tutulmaktadır.

Benzer bir biçimde Sinüzoidal kaotik harita (SDCM, Sinusoidal Chaotic Map) ile görüntü şifreleme işlemi yapılan literatürdeki tek çalışma (F Abu-Amara ve Abdel-Qader, 2013) tarafından gerçekleştirilmiştir. Yöntem iki aşamadan oluşmaktadır. İlk aşamada kaotik harita yardımıyla görüntü piksellerinin konumları değiştirilmektedir. İkinci aşamada ise konumları değiştirilen piksel değerleri, yine kaotik harita ve rastgele sayı üreteci kullanılarak piksel değerlerinin değiştirilmesi sağlanmaktadır.

CSCM, görüntü şifrelemede kullanılan bir başka kaotik haritadır. Görüntü şifrelemek amacıyla CSCM kullanılarak S kutuları üreten bir yöntem (Hussain vd., 2019) tarafından

önerilmiştir. Bu yöntemde görüntü şifreleme kullanımına uygun olmayan ve metin şifrelemede sıklıkla kullanılan AES S kutularına benzer ve her biri 8 bitten oluşan S kutuları üretilmektedir. S kutuları belirli kombinasyonlar ile kullanılarak görüntülerin şifrelenmesi sağlanmıştır. HCM ve CSCM'nin hibrit bir şekilde kullanıldığı bir çalışma (Qi, Huang, Li, Yang, ve Kang, 2019) tarafından yapılmıştır. İki harita birlikte kullanılarak iki boyutlu hibrit bir sistem ortaya çıkartılmıştır. Böylelikle daha güçlü bir şifreleme yöntemi oluşturulmuştur. Yöntemde ortaya atılan iki boyutlu haritadan elde edilen dizi yardımıyla görüntü pikselleri karıştırılmaktadır. Ardından DNA hücresel otomatlar tekniği (Ping, Wu, Mao, Xu, ve Fan, 2018) ile şifreli görüntü elde edilmektedir. İki boyutlu HCM-CSCM kombinasyonunu kullanan bir başka çalışma ise (Y. Liu, Qin, Liao, ve Wu, 2020a) tarafından yapılmıştır. Yöntem, önerilen kaotik harita ve genetik rekombinasyon ile genetik mutasyonun temel ilkeleri kullanılmaktadır. Bir başka ifadeyle DNA hücresel otomatlar tekniğini kullanarak bit düzeyinde görüntü piksellerinin karıştırılmasını sağlamaktadır. CSCM'den elde edilen dizi değerlerinin kombinasyonunu kullanan bir çalışma (Gupta, Gupta, ve Shukla, 2021) tarafından önerilmiştir. Bu çalışmada tamamen CSCM'den yeni bir anahtarın nasıl üretileceği ele alınmıştır. Üretilen 64 bitlik anahtarlar yardımıyla görüntüler üzerinde şifreleme denemeleri yapılmıştır.

Görüntü şifreleme alanında sıklıkla tercih edilen kaotik haritalardan bir diğer ise HCM'dir. Byte dizilerinin karıştırılmasını sağlayan HCM'yi kullanan bir yöntem (Raghava ve Kumar, 2013) tarafından önerilmiştir. Yöntem metin şifrelemede de kullanılan simetrik şifrelemeyi kullanmaktadır. İlk olarak görüntü kendi içerisinde alt bölümlere ayrılmaktadır. Sonraki aşamalarda bu alt bölümlerin piksel değerlerine bakılarak karıştırma işlemi yapılmaktadır. Eğer piksel değeri çift ise bloklar saat yönünde, eğer tek ise saat yönünün tersi yönünde ötelenerek karıştırma işlemi yapılmaktadır. En son aşamada karıştırılan piksel değerleri HCM'den üretilen değerler ile XOR işlemine tabi tutularak görüntünün şifrelenmesi sağlanmaktadır. HCM'yi kullanan bir diğer yöntem ise (Mendua, 2013) tarafından sunulmuştur. Görüntü RGB katmanlarına ayrılmaktadır. Ardından HCM'den elde edilen dizi yardımıyla her bir katman XOR işlemine tutulmaktadır. Son aşamada bu katmanlar birleştirilerek şifreli görüntü elde edilmektedir. Görüntü şifreleme süreçlerinde hibrit sistemlerin kullanılması karmaşıklığı arttırmaktadır. Dolayısı ile beraberinde güvenlik problemlerini de en aza indirgemektedir. Hibrit bir görüntü şifreleme yöntemi (SJ Sheela, Suresh, ve Tandur, 2018) tarafından

HCM ve SM'i kullanılarak gerçekleştirilmiştir. İlk olarak gizli anahtarlar yardımıyla HCM'den bir dizi elde edilmektedir. Sonraki aşamada hibrit kaotik kaydırma dönüşü (W. Liu, Sun, ve Zhu, 2016) ve HCM'den elde edilen değerler yardımıyla görüntü pikselleri karıştırılmaktadır. Son aşamada ise başka bir gizli anahtar yardımıyla SM'den bir dizi üretilmekte ve bir önceki aşamada elde edilen karışık dizi ile XOR işlemine tutulmaktadır. HCM'nin ve ACM'nin birlikte kullanıldığı bir çalışma (Sinha, San, Asha, ve Sahu, 2018) tarafından önerilmiştir. HCM ve ACM değerleri yardımıyla rastgele değerlerden oluşan karışık bir dizi elde edilmektedir. Bu karışık dizi yardımıyla orijinal görüntü pikselleri kendi içerisinde karıştırılarak görüntülerin şifrelenmesi sağlanmaktadır. HCM'yi kullanan bir diğer çalışma (K. Mishra ve Saharan, 2019) tarafından gerçekleştirilmiştir. Çalışmada gizli anahtar olarak 128 bitlik bir anahtar ve HCM birlikte kullanılmıştır. Gizli anahtar yardımıyla görüntü pikselleri karıştırıldıktan sonra HCM'den edilen rastgele dizi değerleri XOR işlemine tutularak görüntülerin şifrelenmesi sağlanmıştır. Görüntü değerlerinin değiştirilmesini ve karıştırılmasını sağlamak amacıyla (Afifi, 2019) tarafından bir çalışma sunulmuştur. Yöntemde HCM ile ilk aşamada görüntü piksellerinin değerleri değiştirilmiştir. İkinci aşamada ise yine aynı harita kullanılarak görüntü piksellerinin konumlarının değiştirilmesi sağlanmıştır. Benzer bir biçimde görüntü piksellerinin konumlarının değiştirilmesi suretiyle görüntülerin şifrelenmesini sağlayan bir yöntem (Hussein, Mahmood, ve Abbass, 2019) tarafından önerilmiştir. Yöntem HCM'den elde edilen değerler ile piksellerin konumlarının değiştirilmesini sağlamakta ve son aşamada ise her bir piksel değeri buna karşılık gelen karışık dizi değerleri ile XOR işlemi uygulanmaktadır. (K. Zhou, Xu, Luo, Fan, ve Li, 2019) tarafından önerilen bir yöntem de ise öteme dönüşümü yardımıyla piksel değerlerinin karıştırılması sağlanmıştır. Sonraki aşamalarda ise HCM yardımıyla karışık dizi üretilmiş ve ilk aşamada ötelenen piksel değerleri ile XOR işlemine tabi tutulması sağlanmıştır. HCM, TM ve ortagonal (dik) matrislerin birlikte kullanıldığı bir çalışma (Kanwal vd., 2022) tarafından önerilmiştir. Görüntü şifreleme süreci üç aşamadan oluşmaktadır. İlk aşamada, kaotik bir HCM üretilmekte ve görüntünün karıştırılmasında kullanılmaktadır. İkinci aşamada gizli bir anahtar yardımıyla ortagonal bir matris ve genellikle metin şifrelemede kullanılan Hill şifreleme algoritması (F. H. Khan, Shams, Qazi, ve Agha, 2015) ile tekrar karıştırılmaktadır. Son aşamada ise TM'den üretilen değerler ile karıştırılan son görüntü XOR işlemine tabi tutulmaktadır.

Lozi kaotik harita (LCM, Lozi Chaotic Map) ile literatürde görüntü şifreleme alanında çok az sayıda çalışma bulunmaktadır. LCM ile ilgili bir çalışma (Rohith ve Sujatha, 2015) tarafından yapılmıştır. İlk olarak M x N boyutlarındaki görüntü tek boyutlu bir dizi haline getirilmektedir. İkinci aşamada LCM'den elde edilen dizi değerleri ile XOR işlemine tutulmaktadır. Son aşamada ise piksel değerleri değiştirilmiş görüntü tek boyutlu diziden iki boyutlu dizi haline getirilerek sonuç görüntüsü elde edilmektedir.

Kaotik sistemler başlangıç koşullarına göre çalışmaktadırlar. Tinkerbell kaotik haritası (TCM, Tinkerbell Chaotic Map) de benzer biçimde çalışmaktadır. Başlangıç değeri olarak onaltılık sayı sistemi kullanan bir çalışma (Krishna, Teja, ve Thanikaiselvan, 2018) tarafından gerçekleştirilmiştir. Anahtar olarak kullanılan onaltılık sayı sistemi kendi içerisinde parçalara ayrılarak TCM'nin başlangıç değerleri elde edilmiştir. Ardından bu başlangıç değerleri ile kaotik harita dizisi elde edilmiştir. Son aşamada kaotik dizi değerleri ile görüntü piksel değerleri XOR işlemine tutularak görüntülerin şifrelenmesi sağlanmıştır. TCM'yi kullanan bir çalışma (A. Kumar ve Raghava, 2020) tarafından yapılmıştır. Yöntemde iki boyutlu ayrık dalgacık dönüşümü (Shafique ve Ahmed, 2022) kullanılarak görüntü öncelikle dalgacık dönüşümü alanına ayrıştırılmaktadır. Ardından ayrılan alanların karıştırılması için ACM kullanılmaktadır. Son aşamada TCM ile görüntünün şifrelenmesi sağlanmaktadır. Kesirli Fourier alanında tekil değer ayrıştırmasını (Z. Wang vd., 2022) ve TCM'yi kullanan asimetrik tek kanallı renkli görüntü şifreleme sistemi (J. Kumar, Singh, ve Yadav, 2020) tarafından sunulmuştur. Giriş görüntüsü kırmızı, yeşil ve mavi kanallara bölünmüştür. Kırmızı bileşen düz metin olarak ve yeşil ve mavi bileşenler ise şifreleme sisteminde faz maskeleri olarak kullanılmıştır. Son aşamada TCM'den elde edilen dizi değerleri yardımıyla her bir renk bileşeni şifrelenmiştir. TCM, deoksiribo nükleik asit (DNA) (Chai, Chen, ve Broyde, 2017) ve hücresel otomatların (Ping vd., 2018) birlikte kullanıldığı bir yöntem ise (Enayatifar, Sadaei, Abdullah, Lee, ve Isnin, 2015) tarafından önerilmiştir. Yöntemde görüntü piksellerini şifrelemek için DNA kuralları, XOR operatörü ve hücresel otomatlar aynı anda kullanılmıştır. DNA dizisine ait kuralların ve hücresel otomatların belirlenmesinde iki boyutlu TCM'den faydalanılmıştır.

Burger kaotik harita (BGCM, Burger's Chaotic Map) ve LM kullanarak görüntülerin şifrelenmesini sağlayan bir yöntem (A. U. Rehman, Khan, Ahmad, ve Hwang, 2016)

tarafından önerilmiştir. Orijinal görüntüde pikseller arasındaki korelasyonu ortadan kaldırmak için iki boyutlu BGCM kullanılmıştır. Dinamik bir şekilde S kutuları LM kullanılarak üretilmiştir. Sonraki aşamalarda piksel değerlerinin değiştirilmesi için görüntü bloklara ayrılmış BGCM'den ve LM'den elde edilen S kutuları yardımıyla görüntülerin şifrelenmesi sağlanmıştır. BGCM ve HCM'nin birlikte kullanıldığı bir çalışma (M. Mishra ve Mankar, 2012) tarafından sunulmuştur. Çalışmada orijinal görüntü pikselleri ilk aşamada HCM'den elde edilen karışık dizi değerleri yardımıyla bozulmaktadır. Bu aşamanın çıkış değerleri benzer bir biçimde BGCM'den elde edilen dizi değerleri ile benzer bir işlemden geçirilerek şifrelenmiş görüntü elde edilmektedir. Çok katmalı bir görüntü şifreleme yöntemi (Al-Majdi vd., 2022) tarafından önerilmiştir. Yöntem çok katmanlı bir yapıya sahiptir ve görüntü piksellerini karıştırmak ve değerlerini değiştirmek için BGCM, şifrelemenin belirli bir aşamasında kullanılmıştır.

Kaplan Yorke haritasının (KYCM, Kaplan Yorke Chaotic Map) kullanıldığı ve FPGA donanımına uygulandığı bir çalışma (Tubola, 2017) tarafından sunulmuştur. Yöntemde görüntü şifrelemek amacı ile KTCM yardımıyla kaotik bir dizi üretilmektedir. Yöntemde daha yüksek bir güvenlik oluşturmak için FPGA donanımından faydalanılmıştır. Gyrator dönüşümü (Rodrigo, Alieva, ve Calvo, 2007) ve kaos teorisini kullanarak görüntü şifrelemeye yarayan bir yöntem (N. Singh ve Sinha, 2009) tarafından önerilmiştir. Kaos harita olarak sırasıyla LM, TM ve KYCM birlikte kullanılmıştır. Yöntemde gyrator dönüşümünün her aşamasında sonra bir kaotik haritadan üretilen değerler yardımıyla görüntü piksellerinin XOR işlemine tabi tutularak şifrelenmesi sağlanmıştır. (N. Singh ve Sinha, 2008) tarafından yapılan bir başka çalışmada ise Fourier dönüşümü ile birlikte benzer prensipte LM, TM ve KYCM birlikte kullanılmıştır. (N. Singh ve Sinha, 2010a) tarafından yapılan başka çalışmada ise üç doğrusal kanonik dönüşüm ve üç kaotik harita birlikte kullanılmıştır. Doğrusal kanonik dönüşüm olarak kesirli Fourier dönüşümü, genişletilmiş kesirli Fourier dönüşümü ve Fresnel dönüşümü, kaotik harita olarak ise TM, KYCM ve Ikeda kaotik haritası (ICM, Ikeda Chaotic Map) birlikte kullanılarak hibrit bir sistem oluşturulmuştur. Doğrusal kanonik dönüşümler sırasıyla kaotik haritalardan elde edilen karışık dizi değerleri ile XOR işlemine tabi tutulmuş ve görüntülerin şifrelenmesi sağlanmıştır. Uygun olmayan Hartley dönüşümü ve kaos teorisini kullanarak görüntü şifreleme için bir yöntem yine (N. Singh ve Sinha, 2010b) tarafından önerilmiştir. Bu yöntemde kaotik harita sayısı LM, TM, KYCM ve ICM kullanılarak dörde çıkarılmıştır.

Önerilen diğer yöntemlerden farklı olarak Hartley dönüşümünden elde edilen değerler anahtar olarak kullanılmıştır. Ayrık kesirli Mellin dönüşümü (M. m. Wang, Zhou, Li, ve Xu, 2022) ve KYCM'nin birlikte kullanıldığı bir yöntem (N. Zhou, Wang, ve Wu, 2011) tarafından önerilmiştir. Yöntemde görüntü pikselleri ayrık kesirli Mellin dönüşümü ile farklı bir forma dönüştürülmüş ve KYCM'den elde edilen rastgele dizi yardımıyla da bulundukları konumları değiştirerek görüntülerin şifrelenmesi sağlanmıştır.

ICM'yi kullanan bir görüntü şifreleme yöntemi (Jia, 2010) tarafından tanıtılmıştır. Yöntem, ICM'den elde edilen karışık dizi değerleri yardımıyla görüntü piksellerinin karıştırılmasını sağlamaktadır. Karıştırma işlemi satır ve sütunlarda ayrı ayrı tekrarlanarak gerçekleştirilmektedir. (C. Li, Luo, ve Li, 2018) tarafından önerilen bir yöntemde ise ICM'den elde edilen değerler yardımıyla görüntü pikselleri XOR işlemine tutularak görüntülerin şifrelenmesi sağlanmıştır. Yöntem piksel değerlerinin değiştirilmesinin ardından yine kaotik haritadan elde edilen değerlerden faydalanılarak piksellerin koordinatları da karıştırılmaktadır. Görüntülerin şifrelenmesi amacıyla ACM ve ICM'yi birlikte hibrit bir şekilde kullanan bir yöntem (Kapur ve Girdhar, 2019) tarafından önerilmiştir. Yöntemde ilk aşamada piksel değerlerinin bozulmasını sağlamak amacıyla ACM kullanılmıştır. Ardından ICM'den elde edilen değerler ile görüntü piksellerinin karıştırılması sağlanmıştır. HCM'yi ve ICM'yi birlikte kullanan hibrit bir sistem ise (Şekertekin ve Atan, 2016) tarafından önerilmiştir. Başlangıç parametreleri yardımıyla ICM'den dizi değerleri üretilmiş ve görüntü pikselleri karıştırılmıştır. Ardından HCM'den elde edilen değerler yardımıyla önceden karıştırılmış görüntü piksel değerleri XOR işlemine tabi tutularak şifrelenmiş görüntü elde edilmiştir.

Holmes kübik harita (HLCM, Holmes Cubic Map) literatürde Duffing harita olarak da bilinmektedir. HLCM'yi kullanan bit yöntem (Dhopavkar, Nayak, ve Roy, 2022) tarafından önerilmiştir. Yöntem, güvenliğin arttırılması amacı ile nesnelerin interneti (IOT) tabanlı olarak geliştirilmiştir. Yöntem, HLCM ve TCM'yi birlikte kullanan hibrit bir yöntemdir. Görüntülerin şifrelenmesi için Zigzag dönüşümü kullanmaktadır. Bu dönüşümün elde edilmesi ve görüntü piksellerin renk değerlerini karıştırılması için kaotik haritalardan faydalanılmıştır. Bir başka yöntem ise (Natiq, Roy, Banerjee, Misra, ve Fataf, 2020) tarafından önerilmiştir. Önerilen yöntem iki boyutlu bir yapıya sahiptir. Yöntemde, ilk aşamada düz görüntü piksellerinin karıştırılması için hiperkaotik diziler

oluşturulurken, ikinci aşamada eliptik eğriler, S-kutusu ve hiperkaotik dizilerden faydalanılmaktadır. Tek boyutlu haritalar kaotik görüntü şifreleme işlemlerinde güvenlik sıkıntıları nedeniyle pek tercih edilmemektedir. İki ve üç boyutlu HLCM kullanarak görüntülerin şifrelenmesini sağlayan bir yöntem (S. Singh, Parida, ve Pradhan, 2018) tarafından önerilmiştir. Gri seviye görüntülerin şifrelemesi için iki boyutlu ve renkli görüntülerin şifrelenmesi için ise üç boyutlu HLCM kullanılmıştır. Her iki durumda da kaotik haritadan elde edilen karışık dizi yardımıyla görüntü piksellerinin karıştırılması sağlanmaktadır.

Görüntü şifrelemek için kullanılan bir diğer kaotik harita türü Chirikov kaotik haritası (CHRCM, Chirikov Chaotic Map) dir. (M. Khan vd., 2021) tarafından önerilen bir yöntemde piksellerin karıştırılması için CHRCM kullanılmıştır. Yöntemde, piksellerin karıştırılması için ayrıca S kutuları ve Lorenz sisteminden de faydalanılmıştır. (Durafe ve Patidar, 2022) tarafından yapılan çalışmada ise iki boyutlu Gingerbreadman kaotik haritası (GCM, Gingerbreadman Chaotic Map) ve CHRCM birlikte kullanılmıştır. Yöntemde, standart GCM, CHRCM ile desteklenmiş ve görüntülerin şifrelenmesi sağlanmıştır. Bir başka hibrit sistem (J. Ahmad vd., 2020) tarafından önerilmiştir. Yöntem, SHA-512 anahtarlama algoritması, ayrık kosinüs dönüşümü, ortogonal matris ve ayrık CHRCM birlikte kullanılmıştır. Görüntüye ilk olarak ayrık kosinüs dönüşümü uygulanmış ve elde edilen değerler ortagonal matris ile çarpılmıştır. Son aşamada ise CHRCM ile görüntü piksellerinin karıştırılması sağlanmıştır.

Literatürde üzerinde en çok çalışma yapılan kaotik haritalardan birisi ACM'dir. ACM algoritması periyodikliği nedeniyle sınırlı bir alana sahiptir. Bu sınırlı alanın genişletilmesi ve görüntü şifrelemede kullanılabilmesi amacıyla (Brindha, 2017) tarafından bir yöntem önerilmiştir. Yöntemde ACM'in davranışı iki ve üç boyutlu haritalar önerilerek geliştirilmiştir. Görüntü piksellerinin karıştırılmasını sağlamak amacıyla ACM kullanan bir yöntem (Sinha vd., 2018) tarafından önerilmiştir. Yöntem piksellerin karıştırılması için ACM yardımıyla üretilen değerlerden yararlanmaktadır. Pikseller satır ve sütunda ayrı ayrı karıştırılmaktadır. Son aşamada ise karıştırılmış piksellerin değerlerinin değiştirilmesi için ise HCM'den faydalanmaktadır. (Das, Mondal, ve Sanyal, 2018) tarafından önerilen bir yöntemde görüntülerin şifrelenmesi üç aşamada gerçekleştirilmiştir. İlk aşamada genetik algoritmanın çaprazlama ve mutasyon

operatörleri görüntünün her pikseline uygulanmıştır. Burada geçiş noktalarına karar verebilmek için LM'den faydalanılmıştır. İkinci aşamada değiştirilmiş görüntünün pikselleri ACM yardımıyla yer değiştirme işlemine tabi tutulmaktadır. Son aşamada ise LM tarafından üretilen rastgele dizi ile değiştirilmiş görüntü pikselleri arasında XOR işlemi uygulanarak şifrelenmiş görüntüsü elde edilmektedir. ACM'in denklem yapısının değiştirilerek görüntülerin şifrelenmesini sağlayan bir yöntem (Subashini ve Poornachandra, 2018) tarafından önerilmiştir. Yöntemde klasik ACM yapısı değiştirilerek piksel değerlerinin iç içe ve rastgele bir şekilde konumlarının değiştirilmesi sağlanmıştır. Yöntem ile orijinal görüntünün elde edilmesi sürecindeki çevrim sayısı çok daha fazla hale getirilmiştir. ACM'nin üç boyutlu sürümü ve Eliptik Eğri Şifreleme (Yuling Luo, Ouyang, Liu, ve Cao, 2019) metodunun birlikte kullanıldığı bir çalışma (Parida ve Pradhan, 2022) tarafından yapılmıştır. İlk aşamada üç boyutlu ACM ile görüntü piksellerinin konumu ve piksel değerleri değiştirilmektedir. Son aşamada dönüştürülen piksel değerleri Eliptik Eğri Şifreleme algoritması kullanılarak şifrelenmiştir. Hibrit bir yapının kullanıldığı bir başka çalışma (Rashmi ve Supriya, 2020) tarafından önerilmiştir. Görüntü bloklara ayrılmış ve her bloğun karıştırılması için ortagonal tarama metodu uygulanmıştır. Karıştırılan bloklar ACM ile tekrar karıştırılmış ve son aşamada ise TM'den elde edilen karışık dizi ile XOR işlemine tabi tutulmuştur. İki boyutlu ACM'yi kullanarak gerçekleştirilen hibrit bir sistem ise (Masood vd., 2022) tarafından önerilmiştir. Yöntem, Newton-Leipnik dinamik sistemi (Leipnik ve Newton, 1981) ve Logistic Gaussian kaotik sistemini (Ali ve Khan, 2019), ACM ile birlikte kullanmaktadır. Kaotik haritaların parametreleri SHA-512 anahtarlama algoritması kullanılarak üretilmektedir. İlk olarak görüntü pikselleri ACM yardımıyla karıştırılmaktadır. Ardından Newton-Leipnik dinamik sisteminden elde edilen rastgele değerler ile karıştırılmış olan piksellerin değerleri değiştirilerek görüntülerin şifrelenmesi sağlanmaktadır. Piksellerin değiştirilmesi aşamasından S kutularından faydalanılmış ve bu kutular ise Logistic Gaussian kaotik sisteminden elde edilmiştir.

Literatürde en çok tercih edilen kaotik haritalardan bir diğeri ise Lorenz kaotik harita (LRCM, Lorenz Chaotic Map)'dır. Görüntü şifrelemek amacıyla LRCM kullanılan bir yöntem (Al-Hazaimeh, Al-Jamal, Alhindawi, ve Omari, 2019) tarafından önerilmiştir. Yöntemde ilk aşamada SHA-256 anahtarlama algoritması kullanılarak bir şifreleme anahtarı elde edilmektedir. Şifreleme anahtarları ve dört adet başlangıç değeri yardımıyla

LRCM'nin başlangıç değerleri elde edilmektedir. Bu başlangıç değerleri yardımıyla karışık dizi elde edilmekte ve görüntü piksellerini hem konumlarının hem de XOR işlemi ile değerlerinin değiştirilmesi sağlanmaktadır. (F. A. Khan, Ahmed, Khan, Ahmad, ve Khan, 2017) tarafından önerilen bir yöntemde anahtarlama algoritmaları yardımıyla 160 bitlik bir anahtar üretilmekte ve LRCM'nin başlangıç değerleri elde edilmektedir. Bir başlangıç değerleri yardımıyla satır ve sütunlarda piksellerin konumlarının ve beraberinde değerlerinin de değiştirilmesi sağlanmıştır. (Sankaradass, Murali, ve Tholkapiyan, 2018) tarafından önerilen bir yöntemde Sobel kenar belirleme operatöründen faydalanılmıştır. Sobel operatörü ile görüntü üzerinde kenar sayısına göre önemli ve önemsiz bölgeler olarak sınıflandırılmıştır. Daha sonra önemli bölgelerdeki pikseller LRCM ile elde edilen dizi değerleri ile hem değerleri hem de konumları değiştirilmektedir. Önemsiz bölgedeki pikseller ise sinüs haritası kullanılarak karıştırılmakta ve değerleri değiştirilmektedir. Son aşamada tüm görüntü LRCM dizi değerleri ile tekrar karıştırılmaktadır. LRCM ve Hadamard matrisi (S. Chen, Su, Sun, ve Zhang, 2022) yardımıyla görüntülerin şifrelenmesini sağlana bir yöntem (Lv, Bai, ve Sun, 2019) tarafından önerilmiştir. Yöntemde başlangıç değerleri yardımıyla Hadamard matrisinden ve LRCM sistemlerinden dizi değerleri üretilmiş bu üretilen değerler yardımıyla görüntülerin şifrelenmesi sağlanmıştır. Üç boyutlu LRCM ve iki boyutlu kesirli ayrık kosinüs dönüşümünü kullanan bir yöntem (Joshi, Kumar, Singh, ve Srivastava, 2021) tarafından önerilmiştir. Yöntemde görüntü RGB kanallarına ayrılmakta ve her kanal Üç boyutlu LRCM tarafından üretilen anahtarlar ile karıştırılmaktadır. Karıştırılan görüntü iki boyutlu kesirli ayrık kosinüs dönüşümünü yardımıyla piksel değerleri değiştirilerek şifrelenmektedir. Üç boyutlu LRCM kullanan bir başka yöntem (D. Kumar, Joshi, Singh, ve Mishra, 2021) tarafından önerilmiştir. Yöntemde ilk aşamada renkli görüntü pikselleri El-Gamal şifreleme algoritması yardımıyla şifrelenmiştir. Şifrelenen değerler bir matris haline getirilmiş ve üç boyutlu LRCM yardımıyla elde edilen dizi değerleri ile tekrar bir karıştırma ve değer değiştirme işlemine tabi tutulmuştur. Bir diğer üç boyutlu LRCM'yi kullanan yöntem (Masood, Ahmad, Shah, Jamal, ve Hussain, 2020) tarafından önerilmiştir. İlk olarak renkli görüntü RGB kanallarına ayrılmakta ve her bir kanaldaki piksel değerleri fraktal anahtarlı bir karıştırma algoritması ile karıştırılmaktadır. Ardından LRCM ile elde edilen dizi değerleri ile XOR işlemine tabi tutularak görüntülerin şifrelenmesi sağlanmaktadır.

Görüntü şifreleme algoritmalarında kullanılan bir diğer kaotik harita GCM'dir. GCM'in kullanıldığı bir yöntem (Alshibani, 2015) tarafından önerilmiştir. Yöntem, HCM, BGCM ve GCM'nin birlikte kullanıldığı hibrit bir yöntemdir. Görüntü pikselleri tek boyutlu bir dizi haline getirilerek her bir kaotik haritadan elde edilen dizi değerleri ile sırasıyla karıştırılarak görüntülerin şifrelenmesi sağlanmıştır. GCM kullanan bir başka yöntemde (Savitri, Johan, Firnanda Al Islama, ve Utaminingrum, 2019) tarafından önerilmiştir. Bu yöntemde başlangıç değerlerine bağlı olarak GCM ile elde edilen dizi değerleri ile görüntü piksellerinin karıştırılması ve değerlerinin değiştirilmesi sağlanmıştır. (Gaffar, Joshi, ve Kumar, 2020) tarafından önerilen bir yöntemde görüntü pikselleri GCM ile karıştırılmış ve elde edilen karışık görüntü pikselleri RC4 şifreleme algoritmasından elde edilen değerler ile XOR işlemine tabi tutularak şifrelenmiştir.

Literatür araştırmalarına dikkat edildiğinde bazı kaotik haritaların görüntü şifrelemede çok sık tercih edildiği, bazı kaotik haritaların ise çok az tercih edildiği yada hiç kullanılmadığı görülmüştür. Bu tez çalışması ile bu durumun daha net ortaya çıktığı görülmektedir. Bu tez çalışmasının sağladığı en önemli katkılardan birisi de çok az sayıda ya da hiç kullanılmayan kaotik haritalarında görüntü şifrelemede kullanılabileceğinin ortaya konması olarak düşünülmektedir.

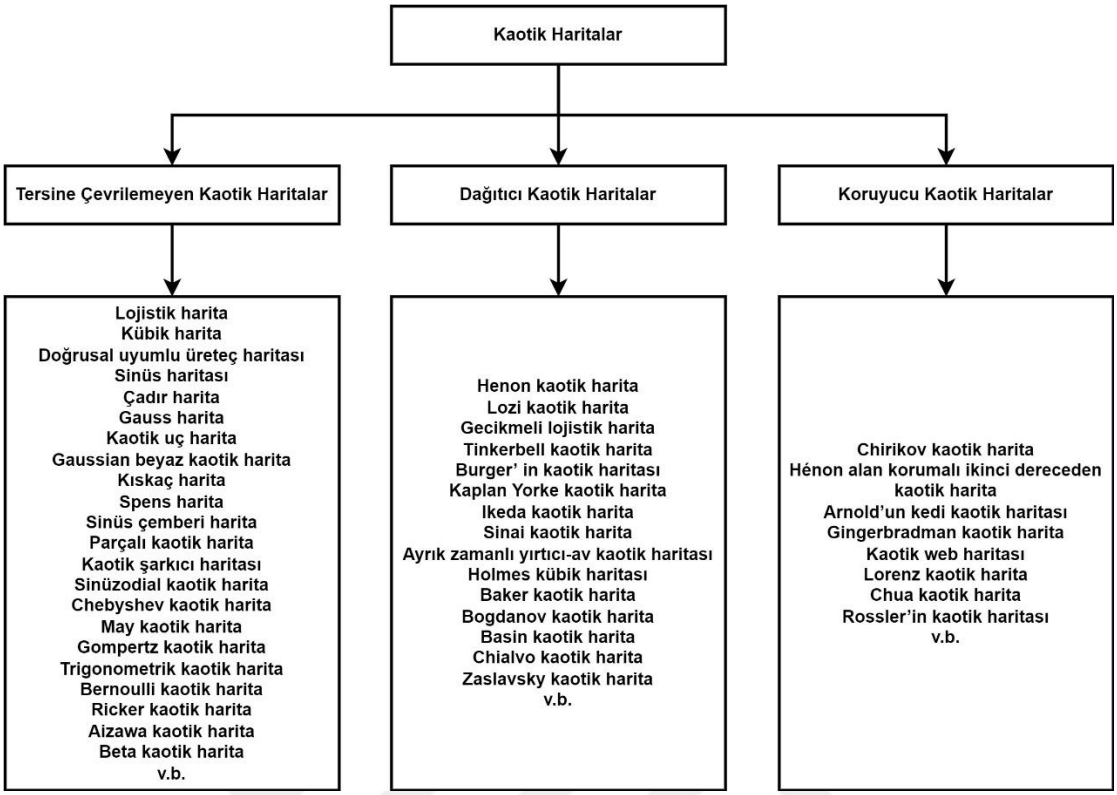
3. MATERYAL VE YÖNTEM

Bu bölümde literatürde görüntü şifreleme alanında yaygın olarak kullanılan 45 adet kaotik harita incelenmiş ve ayrıntılı özelliklerine yer verilmiştir. Görüntü şifrelemede çok az kullanım imkânı bulan yöntemler kapsam dışı bırakılmıştır. Ancak bazı yöntemlerin az kullanılmış olmasına rağmen bu alanda çalışacak bilim insanlarına yol göstermesi adına bu çalışmada yine de yer verilmiştir. İyi bir şifreleme algoritmasının bilimsel bir dayanağının olması gerekmektedir. Bu nedenle bu bölümde ayrıca hata ölçüm metriklerinin ayrıntılı özelliklerine de yer verilmiştir.

3.1 Kaotik Sistemler

Kaotik sistemler doğrusal olmayan bir davranış biçimi sergilemektedirler. Periyodik salınımları sınırsız sayıda olabilmektedir. Bu nedenlerden dolayı genliklerinin ve frekanslarının tespit edilmesi oldukça güçtür (Taşkıran, 2011). Genlik ve frekansları her ne kadar tespit edilemez ise de sınırlı bir alan içerisinde küçük dinamiklere de sahiptirler (Pehlivan, 2007). Bundan dolayı küçük dinamiklere sahip alanların tespit edilmesi nispeten mümkün olmaktadır. Dinamik sistemler elde edilebilecek tüm durumların kümesini içerebilmektedirler. Kaotik sistemler ayrık zamanlı ve sürekli zamanlı kaotik sistemler olarak ikiye ayrılmaktadır (Akgül, 2015). Kaotik sistemler ayrık işaret bağlamında incelendiğinde dinamik sistemlerin kuralı gereği ayrık zamanlı sistemler olarak adlandırılmaktadır. Benzer biçimde sürekli işaretler olarak incelendiğinde ise sürekli zamanlı dinamik sistemler olarak isimlendirilmektedir. Sürekli zamanlı kaotik sistemler diferansiyel denklem kümelerinden meydana gelmektedir (Pehlivan, 2007). Ayrık zamanlı yapılar ise tek boyutlu olup tek bir denklemden oluşabilmektedir. Sürekli zamanlı sistemler ise üç boyutlu ve en az üç denklem içeren ifadelerden meydana gelmektedir.

Kaotik haritaların bir başka sınıflandırılma biçimi (Mateos, Zozor, ve Olivares, 2020) tarafından yapılmıştır. Yapılan sınıflandırmaya göre kaotik haritalar tersine çevrilemeyen haritalar (non-invertible maps), dağıtıcı haritalar (dissipative maps) ve koruyucu haritalar (conservative maps) olarak üç sınıfta toplanmıştır. Bu sınıflamada yer alan ve literatürde yaygın bir şekilde kullanılan kaotik haritalar Şekil 3'de verilmiştir.



Şekil 3. Kaotik haritaların sınıflandırılması

Bu çalışmada kaotik haritalar incelenirken (Mateos vd., 2020) tarafından verilen sınıflandırma sistemi kullanılmıştır.

3.1.1 Tersine çevrilemeyen kaotik haritalar

Tersine çevrilemeyen kaotik haritalar, ayrık zamanlı kaotik sistemler olarak ta adlandırılmakta ve tek denklemden meydana gelmektedirler. Literatürde tersine çevrilemeyen kaotik haritalar genellikle iki boyutludur fakat üç boyutlu sistemlerde bulunmaktadır. Bu tür sistemler dijital ortamlarda doğrudan sayısal değer gerektiren durumlarda kullanılmaktadır. Literatürde basit, yüksek seviyede etkili ve tek boyutlu olan ayrık zamanlı pek çok kaotik sistem bulunmaktadır. Bunlardan bazılarına bu bölümde yer verilmiş ve elde edilen iterasyon adımları grafiksel olarak gösterilmiştir.

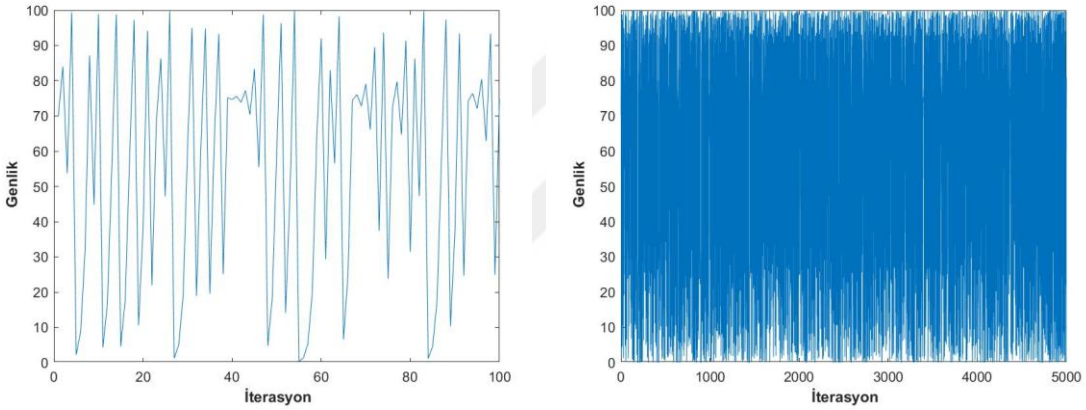
3.1.1.1 Lojistik harita

Lojistik harita (LM, Logistic Map), literatürde en sık kullanılan yöntemlerden biridir (Demir, Tuncer, ve Kocamaz, 2019b). Bu haritalar rastgele sayı üretiminde, görüntü

şifrelemede ve çeşitli optimizasyon problemlerinin çözümünde sıkça kullanılmaktadır (Demir, Tuncer, ve Kocamaz, 2019a). LM'ye ait matematiksel ifade Denklem 1 ile gösterilmektedir.

$$x_{n+1} = r x_n (1 - x_n) \quad (1)$$

Bu kaotik harita türünde 0 ve 1 aralığında rastgele sayılar türetilmekte ve edilen değerler görüntü şifrelemede kullanılmaktadır. Bu denklemde *x* sistem değişkeni ve *n* ise yineleme sayısını ifade etmektedir. Sistemde x_0 başlangıç değeri ve *r* sistem parametresi olmak üzere yinelemeli bir biçimde çalışmaktadır. Şekil 4'de kontrol parametresi $r = 4$ ve $x_0 = -0.35$ alındığında elde edilen kaos durumu gösterilmiştir. Bu değerler ile 100 ve 5000 adet değer üretilmiş ve her noktada bir kaos durumu olduğu gözlemlenmiştir.



a) 100 iterasyon b) 5000 iterasyon

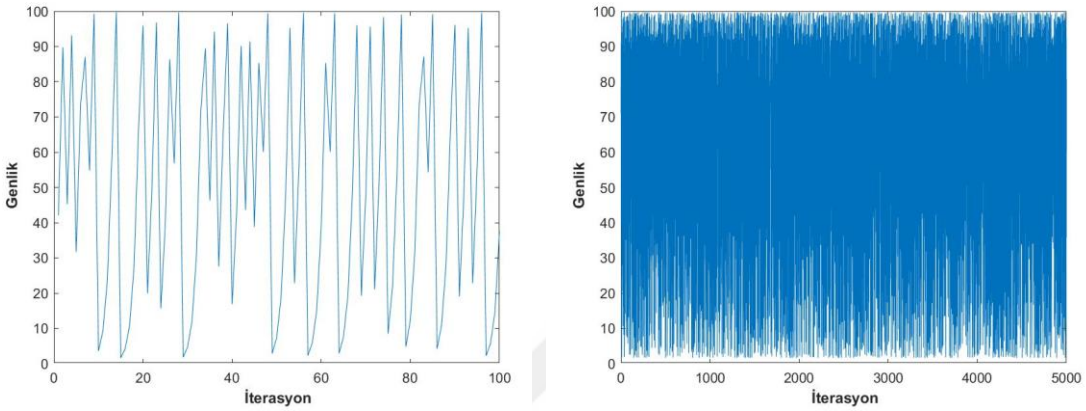
Şekil 4. Lojistik harita genlik dağılımı örneği

3.1.1.2 Kübik harita

Kübik harita (CM, Cubic Map), [0, 1] arasında bir dizi oluşturan kaotik yapılardan biridir. CM, kaotik dizilerin üretilmesi için yaygın olarak kullanılan haritalardan biridir (Özyön, Yaşar, ve Temurtaş, 2020). Bu kaotik harita türü [0, 1] arasında bir dizi oluşturmaktadır. CM'nin matematiksel gösterimi Denklem 2'de verilmiştir (Caponetto, Fortuna, Fazzino, ve Xibilia, 2003; Lu, Wang, Fei, ve Qiu, 2014).

$$X_{n+1} = pX_n(1 - X_n^2), \quad X_n \in (0,1), p = 2.59 \tag{2}$$

Bu kaotik yöntemden üretilen 100 ve 5000 adet değer için elde edilen dağılım Şekil 5'de gösterilmiştir.



a) 100 iterasyon b) 5000 iterasyon

Şekil 5. Kübik harita genlik dağımı örneği

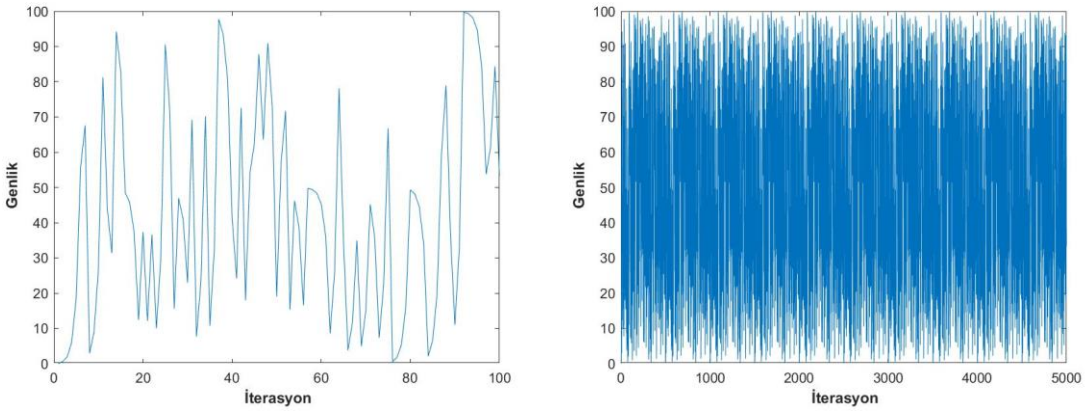
Şekil 5'de kontrol parametresi p = 2.59 alındığında elde edilen kaos durumu gösterilmiştir. Bu değerler ile farklı iterasyonlar için değer üretilmiş ve her noktada bir kaos durumu olduğu gözlemlenmiştir.

3.1.1.3 Doğrusal uyumlu üreteç haritası

Doğrusal uyumlu üreteç haritası (LCGM, Linear Congruential Generator Map), sürekli ve parçalı doğrusal bir denklem yardımıyla hesaplanmaktadır (Izotov, Velichko, ve Boriskov, 2021). LCGM denklemi ile sözde rastgele sayı dizisi elde edilmektedir. Yöntem en iyi bilinen ve en eski sözde rastgele sayı üreteçlerinden biridir (Bhowmik, Karforma, Dey, ve Sarkar, 2021). Uygulaması ve anlaşılması son derece kolay ve hızlı çalışan bir yöntemdir. LCGM, Denklem 3 ile ifade edilmektedir.

$$X_{n+1} = (aX_n + c)\ mod\ n \tag{3}$$

Burada X_0 başlangıç değerine, a ve c sabitlerine ihtiyaç duyulmaktadır. Üretilecek sayılar *0* ve *n-1* aralığında olabilmektedir. Dolayısı ile üretilebilecek rastgele sayıların sayısı sınırlıdır. Şekil 6'da a=37, c=91 ve x_0 = 7 için 100 ve 5000 adet değer üretilmiştir. Üretilen değerlerin rastgele bir dağılım gösterdiği görülmektedir.



a) 100 iterasyon b) 5000 iterasyon

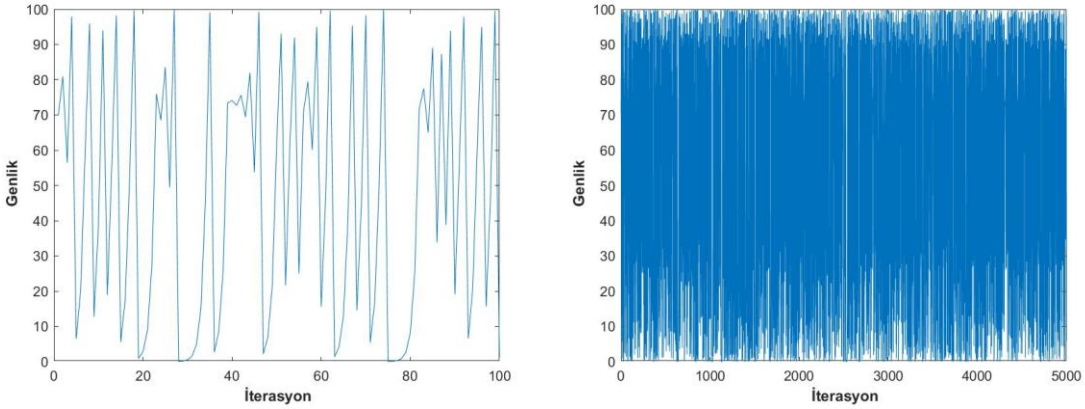
Şekil 6. Doğrusal uyumlu üreteç haritası genlik dağılımı örneği

3.1.1.4 Kaotik sinüs haritası

Kaotik sinüs haritası (SM, Chaotic Sine Map), dinamik bir sistemdir. SM fonksiyonu Denklem 4 ile ifade edilmektedir (Bilal, 2021).

$$X_{n+1} = \frac{\alpha}{4}\sin(\pi X_n), \quad 0 \leq \alpha \leq 4 \tag{4}$$

Burada $\alpha \leq 4$ olarak kontrol parametresini ve X_n ise başlangıç koşulunu ifade etmektedir (Belazi ve Abd El-Latif, 2017). Bu kaotik haritada α en fazla 4 olabildiğinden elde edilecek olan kaotik seri değerleri en fazla 0 ile $\alpha/4$ arasında olabilmektedir. SM'nin gerçekten kaotik olduğunu göstermek için (Griffin, 2013) tarafından pek çok deney yapılmıştır. Bu deneyler sonucunda SM'in LM'ye benzer biçimde bir diyagram oluşturduğu gözlemlenmiştir (Belazi ve Abd El-Latif, 2017). Ayrıca kaotik olma durumunun α değerine bağlı olarak 1'e yaklaştığı durumlarda gerçekleştiği görülmüştür. Şekil 7'de $\alpha = 1$ ve $X_0 = 0.7$ olduğu durumda elde edilen 100 ve 5000 adet değer için kaotik harita örneği gösterilmiştir. Kaotik haritanın her noktasında rastgele ve kaotik bir durum olduğu görülmektedir.



a) 100 iterasyon b) 5000 iterasyon

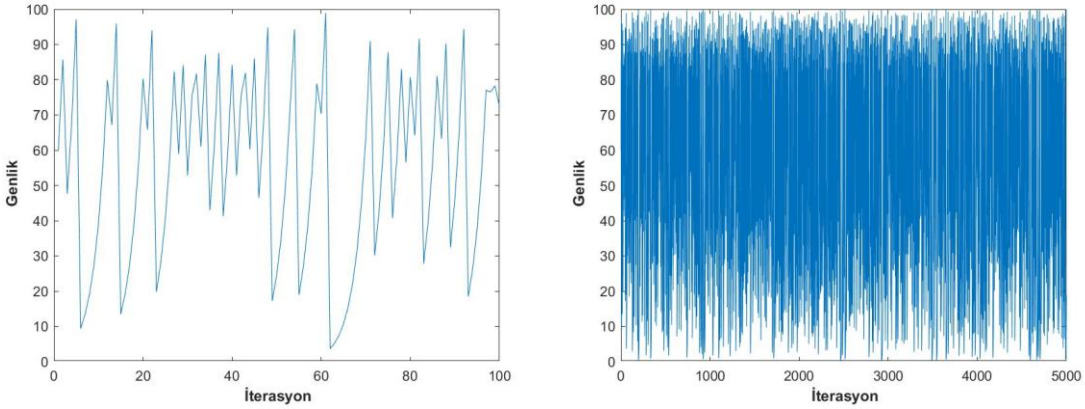
Şekil 7. Sinüs kaotik harita örneği

3.1.1.5 Çadır harita

Çadır harita (TM, Tent Map) kaotik haritası en sık kullanılan yöntemlerden birisidir (T. Tuncer, 2018). Görüntü şifrelemede, rastgele sayı üretiminde ve şifreleme yöntemleri için anahtar üretiminde kolay kullanımı nedeniyle sıklıkla tercih edilmektedir. TM'nin önemli özelliklerinden bir tanesi istatistiksel olarak en iyi sonuçları üreten bir fonksiyona sahip olmasıdır (Hua, Zhu, Yi, Zhang, ve Huang, 2021; X. Wang ve Guan, 2022). TM'nin matematiksel olarak tanımı Denklem 5'de verilmiştir.

$$x_{n+1} = \begin{cases} \dfrac{x_n}{0.7} & eğer\ x_n < 0.7 \\ \dfrac{10}{3} x_n(1 - x_n) & eğer\ x_n \geq 0.7 \end{cases} \quad (5)$$

Burada iki durum söz konusudur. Başlangıç değeri x_0'a göre iki farklı denklem üzerinde işlem yapılmaktadır. Yapılan işlemler tekrarlı bir şekilde gerçekleştirilmektedir. Şekil 8'de başlangıç değerinin $x_0 = 0.6$ olduğu durumda elde edilen 100 ve 5000 adet değer için kaotik harita örneği gösterilmiştir.



a) 100 iterasyon b) 5000 iterasyon

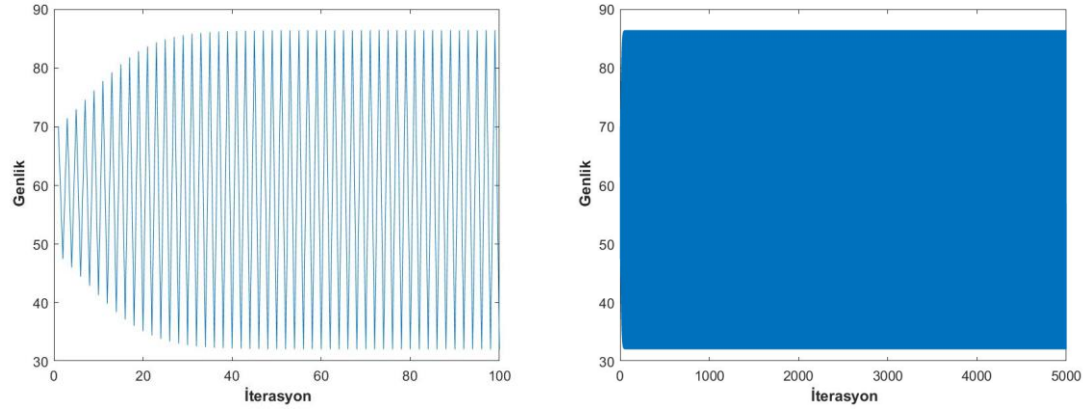
Şekil 8. Kaotik çadır harita örneği

3.1.1.6 Gauss harita

Gauss harita (GM, Gauss Map), literatürde ve matematikte fare harita (Mouse Map) olarak ta bilinmektedir. GM, gauss fonksiyonu yardımıyla belli bir aralıkta doğrusal olmayan ve yinelenen değerler üreten bir kaotik haritadır (Salunke vd., 2022). Üretilen değerler (0,1) aralığındadır. GM, Denklem 6 ile ifade edilmektedir (Al-Khasawneh vd., 2022).

$$x_{n+1} = e^{-\alpha(x_n)^2} + \beta \tag{6}$$

Burada α ve β değerleri gerçek sayılarıdır. $\alpha \geq 0$ olmak ve β değeri [-1, 1] aralığında olmak zorundadır aksi durumda GM sınırsız ve kaotik olmamaktadır. Şekil 9'da x_0 başlangıç değerinin 0.7 olduğu bir durum için elde edilen gauss kaotik haritası verilmiştir.



a) 100 iterasyon b) 5000 iterasyon

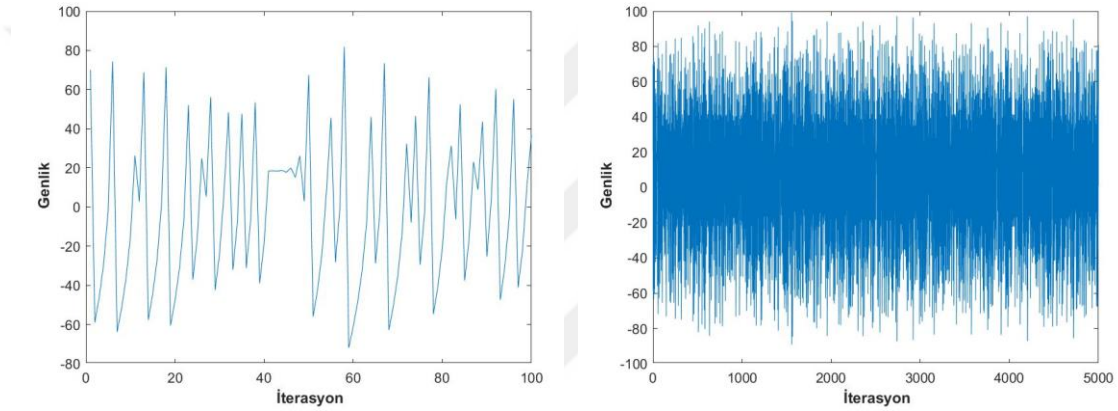
Şekil 9. Gauss harita örneği

3.1.1.7 Kaotik Uç harita

Kaotik uç harita (CCM, Chaotic Cusp Map), ayrık ve dinamik bir sistemdir (Antoniou, 2001). Yapısı gereği bir tepe noktası oluşturmaktadır. Tekrarlı, uniform dağılmayan ve tek boyutlu bir yapıya sahip kaotik bir ifadedir. CCM, Denklem 7 ile ifade edilmektedir.

$$X_{n+1} = 1 - A\sqrt{|X_n|} \tag{7}$$

Burada başlangıç şartı olan X_0 değeri $0 \leq X_0 \leq 1$ aralığında olmalıdır. Başlangıç değerin $X_0 = 0.7$ ve A=1.90 olduğu bir durum için elde edilen değerler Şekil 10'da gösterilmiştir.



a) 100 iterasyon b) 5000 iterasyon

Şekil 10. Uç harita örneği

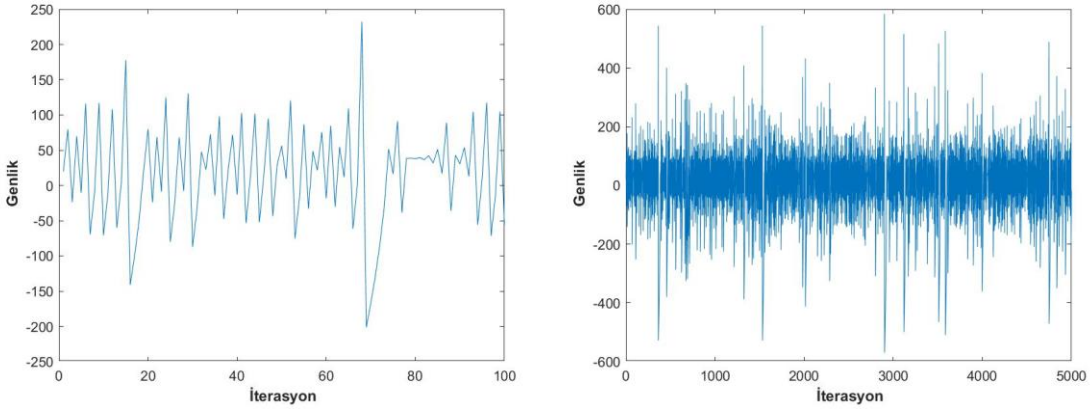
Burada aynı şartlar altında üretilen 100 ve 5000 adet değer için sistemin kaotik bir yapı sergilediği gözlemlenmektedir.

3.1.1.8 Gaussian beyaz kaotik harita

Gaussian beyaz kaotik harita (GWCM, Gaussian White Chaotic Map), ayrık zamanlı otokorelasyon işlevine sahip rastgele bir sürece sahiptir (Eisencraft, Monteiro, ve Soriano, 2017). GWCM, Denklem 8 ile ifade edilmektedir.

$$X_{n+1} = |X_n|^{-\frac{1}{4}} - \frac{1}{2} - |X_n| \tag{8}$$

Burada başlangıç şartı olan X_0 değeri $0 \leq X_0 \leq 1$ aralığında olmalıdır. $X_0 = 0.2$ başlangıç değeri ile 100 ve 5000 iterasyon için elde edilen dağılım grafiği Şekil 11'de gösterilmiştir.



a) 100 iterasyon b) 5000 iterasyon

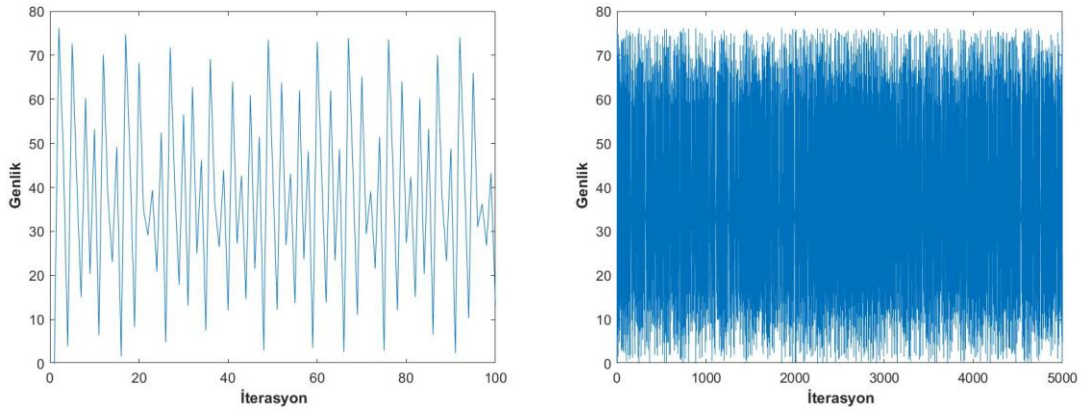
Şekil 11. Gaussian beyaz kaotik harita örneği

3.1.1.9 Kıskaç harita

Kıskaç harita (PM, Pinchers Map), tek boyutlu kaotik bir haritadır. PM, Denklem 9 ile ifade edilmektedir (Akgül, Kacar, Aricıoğlu, ve Pehlivan, 2013).

$$X_{n+1} = |\tanh S\ (X_n - C)| \tag{9}$$

Burada n tekrar sayısını, S ve C değerleri ise sistem değişkenlerini ifade etmektedir. Denklemin çalışabilmesi için X_0 başlangıç değerine ihtiyaç duyulmaktadır. X_0 = 0, S=2 ve C=0.5 için elde edilen 100 ve 5000 iterasyonlu dağılım grafiği Şekil 12'de gösterilmiştir.



a) 100 iterasyon b) 5000 iterasyon

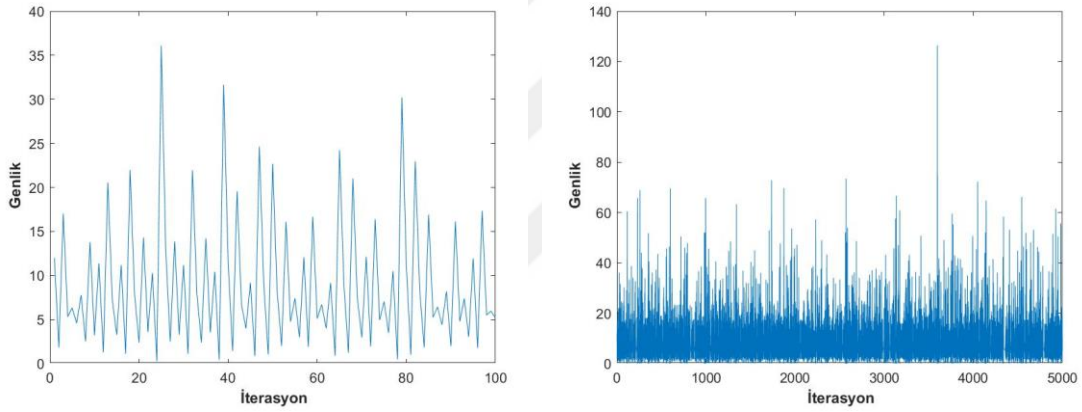
Şekil 12. Kıskaç harita örneği

3.1.1.10 Spens harita

Spens harita (SPM, Spence Map), Bill Spence tarafından ortaya atılan tek boyutlu basit kaotik bir haritadır. Yöntemin uygulanmasının basit olması ve denkleminin yapısı gereği elde edilecek çözümlerin küçük pozitif değerlerde kalması muhtemeldir. Ancak elde edilecek çözümlerin yüksek sayılara ulaşması da mümkündür (Shaw, 1981). SPM, *n* tekrar sayısını göstermek üzere Denklem 10 ile ifade edilmektedir.

$$X_{n+1} = |ln\, X_n)| \tag{10}$$

Denklemin çalışabilmesi için X_0 başlangıç değerine ihtiyaç duyulmaktadır. X_0= 1.2 için 100 ve 5000 iterasyon için elde edilen değerleri gösteren grafik Şekil 13'de verilmiştir.



a) 100 iterasyon b) 5000 iterasyon

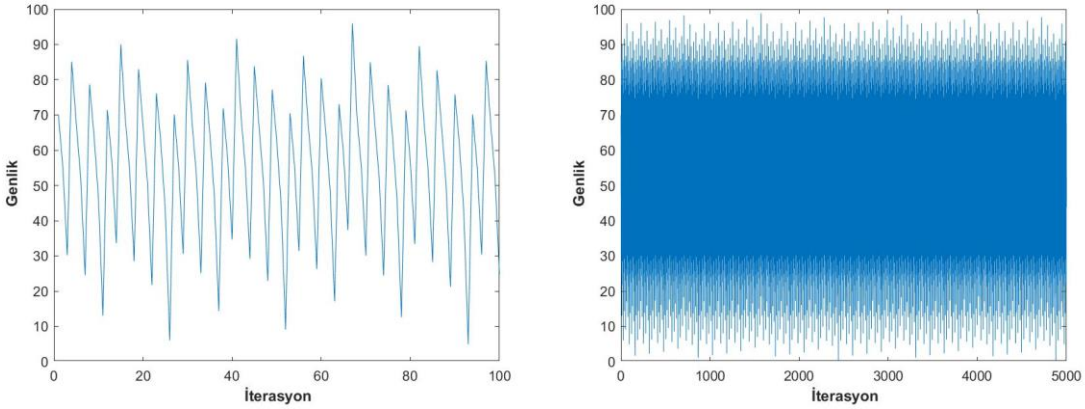
Şekil 13. Spens harita örneği

3.1.1.11 Sinüs çemberi harita

Sinüs çemberi haritası (SCM, Sine-Circle Map), tek boyutlu bir kaotik haritadır ve Denklem 11 ile ifade edilmektedir (Akgül vd., 2013).

$$X_{n+1} = mod(X_n + \Omega - \frac{K}{2\pi} sin2\pi X_n, 1) \tag{11}$$

Burada *n* tekrar sayısını, *K* ve *Ω* değerleri ise sistem parametrelerini ifade etmektedir. Denklemin çalışabilmesi X_0 başlangıç değerine bağlıdır. Şekil 14'de X_0=0.7, $\Omega = 0.7$ ve *k*=1 için elde edilen dağılım grafiği verilmiştir.



a) 100 iterasyon b) 5000 iterasyon

Şekil 14. Sinüs çemberi haritası örneği

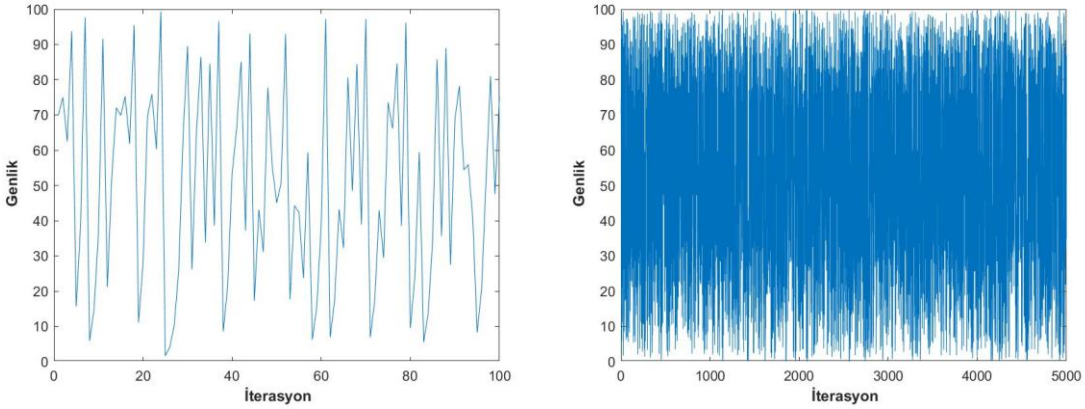
Bu yapı ile aynı şartlar altında 100 ve 5000 iterasyon yapılarak değerler üretilmiş ve üretilen değerlerin rastgele bir yapı sergiledikleri gözlemlenmiştir.

3.1.1.12 Parçalı kaotik harita

Parçalı kaotik harita (PWM, Piecewise Map), sözde rastgele diziler oluşturmak için kullanılan en basit ve tek boyutlu kaotik haritalardan birisidir. Tek tip dağılım işlemi iyi istatistiksel özelliklere sahip olmasından dolayı çeşitli görüntü şifreleme algoritmalarında yaygın olarak kullanılmaktadır (Ahmed vd., 2021). PWM denklemleri, Denklem 12 ile ifade edilmektedir.

$$x_{n+1} = \begin{cases} \dfrac{x_n}{p} & eğer\ 0 \le x_n \le p \\ \dfrac{x_n - p}{0.5 - p} & eğer\ p \le x_n \le 0.5 \\ \dfrac{(1 - p - x_n)}{0.5 - p} & eğer\ 0.5 \le x_n \le 1 - p \\ \dfrac{(1 - x_n)}{p} & eğer\ 1 - p \le x_n \le 1 \end{cases} \tag{12}$$

Burada x_i kaotik haritanın başlangıç değerini ifade etmekte $x_n \in [0, 1]$ aralığındadır. p kontrol parametresidir ve $p \in [0, 0.5]$ aralığında olması gerekmektedir. Şekil 15'de aynı şartlar altında üretilen 100 ve 5000 adet değerin dağılım grafiği gösterilmiştir.



a) 100 iterasyon b) 5000 iterasyon

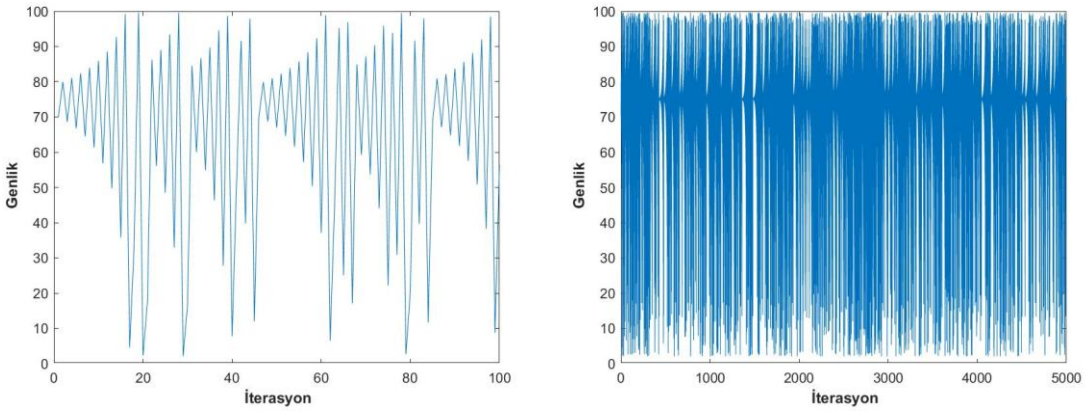
Şekil 15. Parçalı kaotik harita örneği

3.1.1.13 Kaotik şarkıcı haritası

Kaotik şarkısı haritası (CSM, Chaotic Singer Map), tek boyutlu kaotik bir sistemdir. Uygulanması ve kullanımı bakımından en kolay yöntemlerden birisidir. İteratif bir fonksiyon olma özelliğine sahiptir (Karim vd., 2021). CSM, Denklem 13 ile ifade edilmektedir.

$$x_{n+1} = \mu(7.86x_n - 23.31x_n^2 + 28.75x_n^3 - 13.30x_n^4) \quad (13)$$

Burada μ sistem parametresidir. Tipik olarak alabileceği değerler [0.90, 1.08] aralığındadır. Denklemin değer üretebilmesi için X_0 başlangıç değerine ihtiyaç duyulmaktadır. Şekil 16'da 100 ve 5000 iterasyondan elde edilen değerler grafiksel olarak gösterilmektedir.



a) 100 iterasyon b) 5000 iterasyon

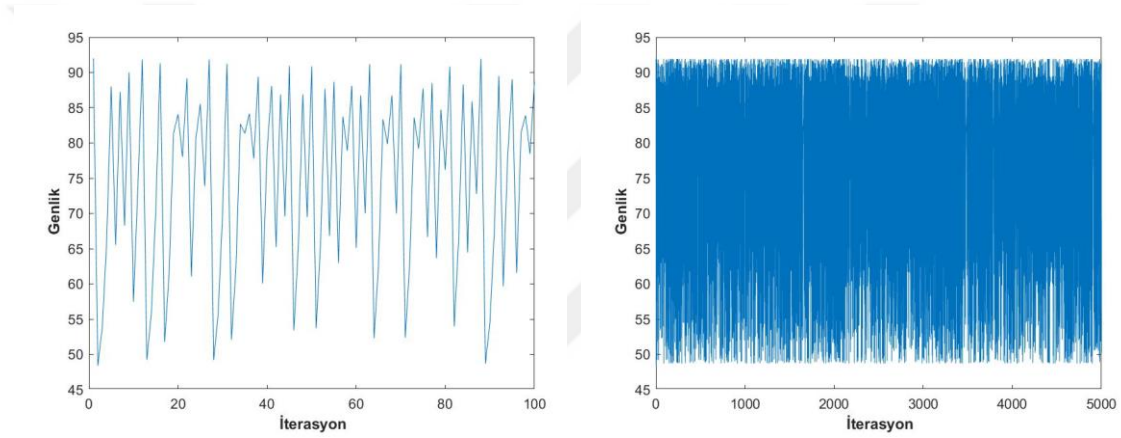
Şekil 16. Kaotik singer haritası örneği

3.1.1.14 Sinüzodial kaotik harita

Sinüzoidal kaotik harita (SDCM, Sinusoidal Chaotic Map), tek boyutlu dinamik değer üretebilen kaotik haritalardan birisidir. İteratif olarak değer üretmektedir. SDCM, Denklem 14 ile gösterilmektedir (Xie, Zhang, ve Lim, 2020).

$$x_{n+1} = 2.3x_n^2 \sin(\pi x_n) \tag{14}$$

Burada serinin üretilebilmesi için x_0 başlangıç değerine ihtiyaç bulunmaktadır. Kaotik seri üretilebilmesi için $x_0 \in [-0.92, 0.92]$ aralığında olması gerekmektedir. Şekil 17'de 100 ve 5000 iterasyondan sonra elde edilen değerlerin grafiksel gösterimi verilmiştir.



a) 100 iterasyon b) 5000 iterasyon

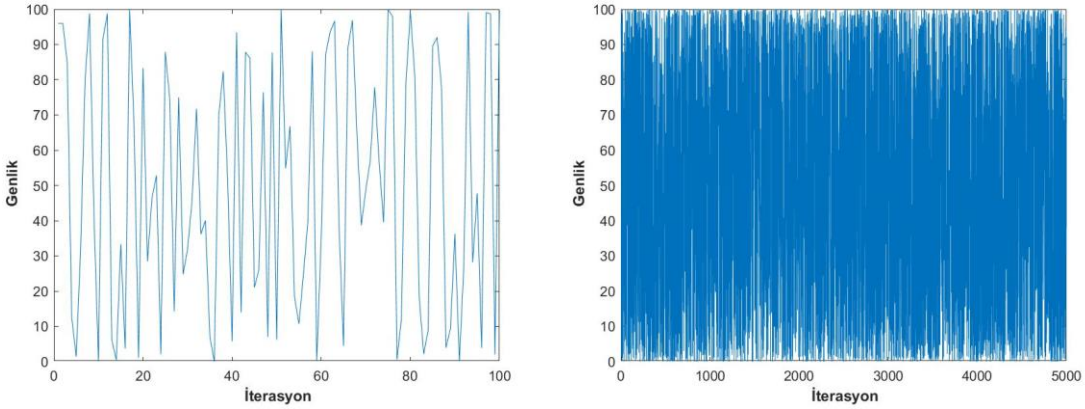
Şekil 17. Sinüzoidal kaotik harita örneği

3.1.1.15 Chebyshev kaotik harita

Chebyshev kaotik harita (CSCM, Chebyshev Chaotic Map), tek boyutlu kaotik harita olarak Denklem 15 ile tanımlanmaktadır (Qi vd., 2019).

$$x_{n+1} = \cos(w \times \cos^{-1} x_n) \tag{15}$$

Burada başlangıç olarak x_0 değerine ihtiyaç duyulmaktadır. w sistem parametresidir ve $w \in (2, +\infty)$ aralığındadır. Şekil 18'de 100 ve 5000 iterasyon ile elde edilen değerlerin grafiksel olarak gösterimi verilmiştir.



a) 100 iterasyon b) 5000 iterasyon

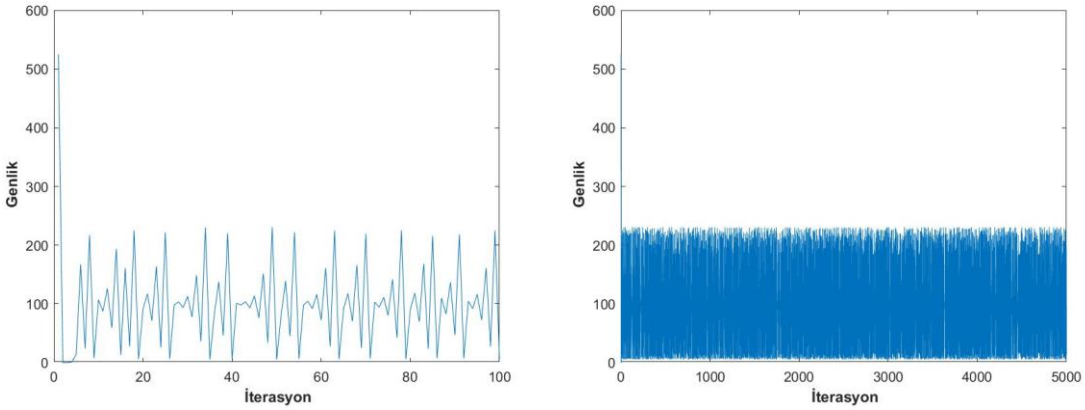
Şekil 18. Chebyshev kaotik harita örneği

3.1.1.16 May kaotik harita

May kaotik harita (MCM, May Chaotic Map) kaotik haritası, Robert May tarafından yayınlanmış ve LM'e benzer davranış ve özelliklere sahiptir ve Denklem 16 ile ifade edilmektedir (Ali ve Khan, 2019).

$$X_{n+1} = X_n e^{a(1-X_n)} \tag{16}$$

Burada $X_n \in [0, 10.9]$ ve kontrol parametresi olan a ise [0, 5] aralığında olmalıdır. Şekil 19'da başlangıç değerinin X_0=5.25 ve a = 2.9 olduğu durumda elde edilen 100 ve 5000 adet değer için kaotik harita örneği gösterilmiştir. Bu, haritanın yukarıda belirtilen başlangıç koşulu aralığında kaotik özellikler gösterdiği şekilde açıkça görülebilmektedir.



a) 100 iterasyon b) 5000 iterasyon

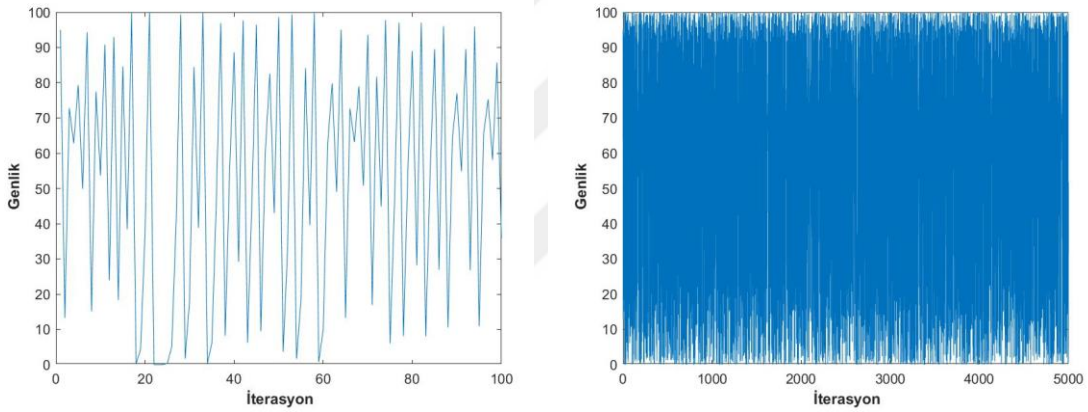
Şekil 19. May kaotik harita örneği

3.1.1.17 Gompertz kaotik harita

Gompertz kaotik harita (GPCM, Gompertz Chaotic Map), ilk olarak Gompertz tarafından önerilmiştir (Rusakov, Tikhonov, Nurieva, ve Medvinsky, 2021). GPCM, çok düşük düzeyde kaotik davranış ve özelliklere sahiptir. Denklem 17 ile gösterilmektedir.

$$X_{n+1} = -bX_n \ln(X_n) \tag{17}$$

Burada kontrol parametresi b ∈ [0,e] ve e = 2.71829 üstel fonksiyondur. Kaotik olma durumu diğer haritalara nazaran düşük kalmaktadır. Şekil 20'de başlangıç değerinin X_0=0.55 ve b = 2.71829 olduğu durumda elde edilen 100 ve 5000 adet değer için kaotik harita örneği gösterilmiştir.



a) 100 iterasyon b) 5000 iterasyon

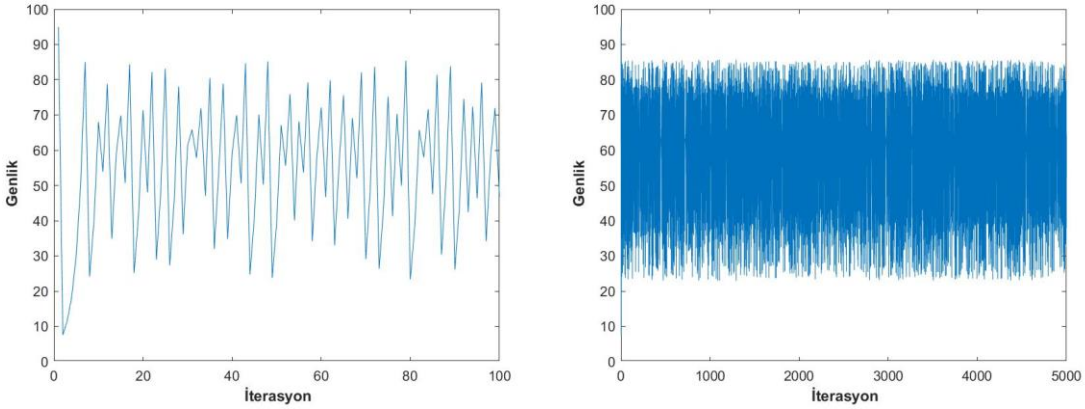
Şekil 20. Gompertz kaotik harita örneği

3.1.1.18 Trigonometrik kaotik harita

Trigonometrik kaotik harita (TGCM, Trigonometric Chaotic Map), tek boyutlu kaotik bir haritadır. TGCM, Denklem 18 ile ifade edilmektedir (Fadi Abu-Amara, 2018).

$$X_{n+1} = \begin{cases} \lambda X_n(\sin\left(\frac{\pi}{2}X_n\right) + \cos\left(\frac{\pi}{2}X_n\right)), & 0 \le X_n \le 0.5 \\ \lambda(1-X_n)(\sin\left(\frac{\pi}{2}(1-X_n)\right) + \cos\left(\frac{\pi}{2}(1-X_n)\right)), & 0 \le X_n \le 0.5 \end{cases} \tag{18}$$

Burada X_0 başlangıç değerinin ve λ kontrol parametresini ifade etmektedir. Ayrıca $X_{n+1} \in [0,1]$ aralığında olmalıdır. Şekil 21'de başlangıç değerinin X_0=0.95 ve λ = 2.71829 olduğu durumda elde edilen 100 ve 5000 adet değer için kaotik harita örneği gösterilmiştir.



a) 100 iterasyon b) 5000 iterasyon

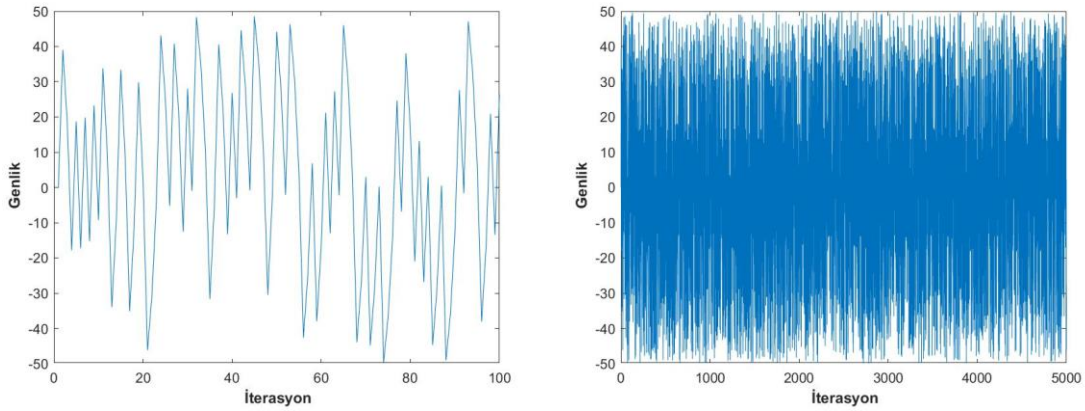
Şekil 21. Trigonometrik kaotik harita örneği

3.1.1.19 Bernoulli kaotik harita

Bernoulli kaotik harita (BCM, Bernoulli Chaotic Map), diyadik dönüşüm (dyadic transformation), iki katlı harita (doubling map) ve testere dişi haritası (saw tooth map) olarak da bilinmektedir (S Sheela ve Sathyanarayana, 2017). Denklem 19 ile ifade edilmektedir.

$$X_{n+1} = \begin{cases} r * X_n + 0.5, & X_n < 0 \\ r * X_n - 0.5, & X_n \geq 0 \end{cases} \quad (19)$$

İterasyonlu çalışan bir sistemdir ve bir başlangıç değerine bağlı olarak çalışmaktadır. r kontrol parametresidir. Şekil 22'de başlangıç değerinin X_0=-0.0625 ve r = 1.75 olduğu durumda elde edilen 100 ve 5000 adet değer için kaotik harita örneği gösterilmiştir.



a) 100 iterasyon b) 5000 iterasyon

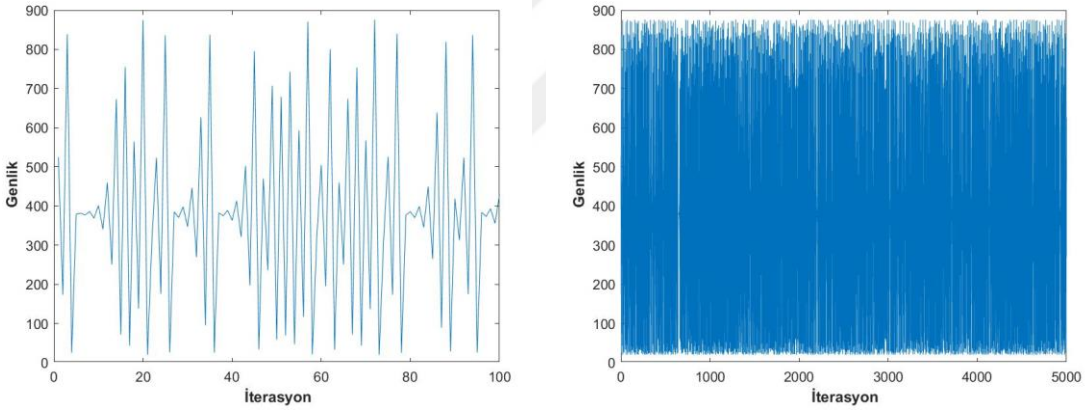
Şekil 22. Bernoulli kaotik harita örneği

3.1.1.20 Ricker kaotik harita

Ricker kaotik harita (RCM, Ricker Chaotic Map), W. E. Ricker tarafından 1954 yılında ortaya atılmıştır. Balıkçılık biliminin önemli bir kurucusudur. Balıkçılıkta bulunacak balık sayısını tahmin etmek için bu modeli öne sürmüştür (Al-Majdi vd., 2022). Denklem 20 ile ifade edilmektedir.

$$X_{n+1} = X_n e^{r(1-\frac{X_n}{k})} \tag{20}$$

Burada *r* ve *k* kontrol parametreleridir. Kontrol parametresi olan $r > 2$ olması durumunda sistem kararsız duruma gelmektedir. Bir başka ifade ile $r > 2$ olması durumunda sistem kararsız duruma gelmekte ve kaotik bir yapıya dönüşmektedir. Şekil 23'de başlangıç değerinin X_0=5.25, *r* = 2.9 ve *k*=3.8 olduğu durumda elde edilen 100 ve 5000 adet değer için kaotik harita örneği gösterilmiştir.



a) 100 iterasyon b) 5000 iterasyon

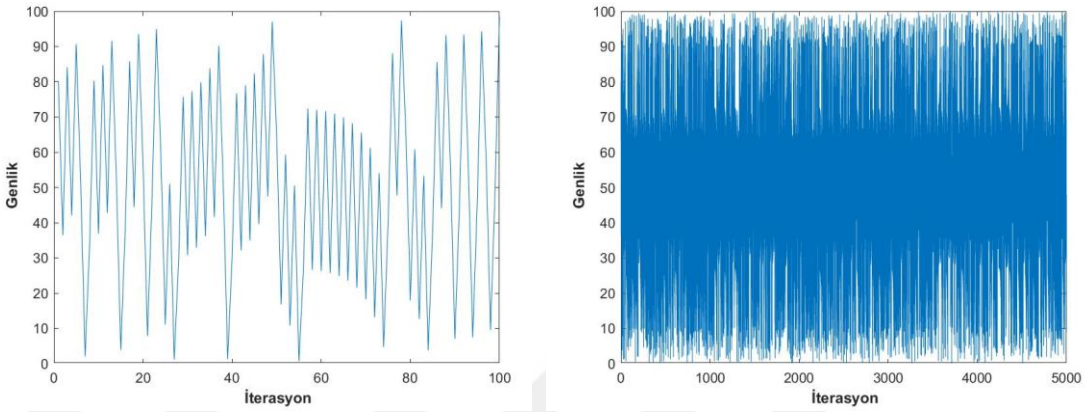
Şekil 23. Ricker kaotik harita örneği

3.1.1.21 Aizawa kaotik harita

Aizawa kaotik haritası (AZCM, Aizawa Chaotic Map), tek boyutlu kaotik bir sistem olmakla beraber üç boyutlu sürümü de bulunmaktadır (Kim, Naruse, Aono, Hori, ve Akimoto, 2016). Tek boyutlu AZCM Denklem 21 ile ifade edilmektedir.

$$X_{n+1} = \begin{cases} X_n + 2^{A-1}{X_n}^A, & 0 \le X_n \le 0.5 \\ X_n - 2^{A-1}(1-X_n)^A, & 0.5 < X_n \le 1 \end{cases} \tag{21}$$

Burada A kontrol parametresidir. Şekil 24'de başlangıç değerinin X_0=0.8 ve A = 0.15 olduğu durumda elde edilen 100 ve 5000 adet değer için kaotik harita örneği gösterilmiştir.



a) 100 iterasyon b) 5000 iterasyon

Şekil 24. Aizawa kaotik haritası örneği

3.1.1.22 Beta kaotik harita

Beta kaotik harita (BECM, Beta Chaotic Map), olasılık teorisinde ve matematiksel istatistiklerde sıklıkla bulunan beta işlevinden sentezlenen kaotik bir harita türüdür (Zahmoul, Ejbali, ve Zaied, 2017). BECM, Denklem 22 ile ifade edilmektedir.

$$X_{n+1} = k\ x\ Beta(X_n;\ x_1, x_2, p, q) \tag{22}$$

Burada;

$$p = b_1 + c_1 a \tag{23}$$

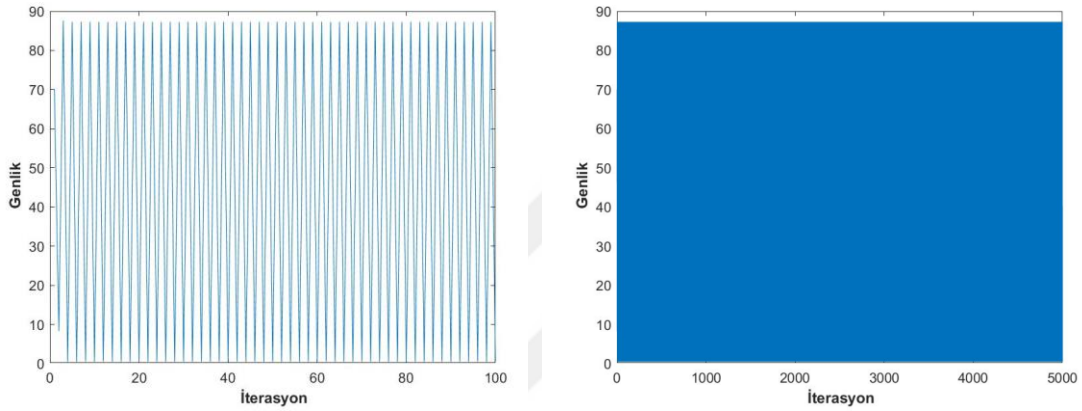
$$q = b_2 + c_2 a \tag{24}$$

ile elde edilmektedir. Beta değerlerinin hesaplanması ise Denklem 25 ve 26 ile elde edilmektedir.

$$Beta(X_n;\ x_1, x_2, p, q) = \begin{cases} \left[\frac{(X_n - x_1)}{(x_c - x_1)}\right]^p \left[\frac{(x_2 - X_n)}{(x_2 - x_c)}\right]^q & , Eğer\ x \in [x_1, x_2] \\ 0 & , Değilse \end{cases} \tag{25}$$

$$x_c = \frac{(px_2 + qx_1)}{(p+q)} \tag{26}$$

Burada, p, q, x_1, x_2, a, b_1, b_2, c_1, c_2 ve k sistem parametrelerini göstermektedir. Şekil 25'de başlangıç değerinin X_0=0.7, x_1=-1, x_2=1, a=-0.8, b_1=5, b_2=3, c_1=1, c_2=-1, p=4.2, q=3.8 ve k = 0.88 olduğu durumda elde edilen 100 ve 5000 adet değer için kaotik harita örneği gösterilmiştir.



a) 100 iterasyon b) 5000 iterasyon

Şekil 25. Beta kaotik harita örneği

3.1.2 Dağıtıcı kaotik haritalar

Bu tür kaotik haritalar edilen değerlerin pozitif ve negatif yönlerde dağıldığı bir yapıya sahiptir. Bu bölümde dağıtıcı kaotik haritalardan bazılarının detaylarına yer verilmiş ve grafiksel dağılımları gösterilmiştir.

3.1.2.1 Henon kaotik harita

Henon kaotik harita (HCM, Henon Chaotic Map) 1969 yılında Michel Henon tarafından tanıtılmıştır. Başlangıç koşullarına duyarlı olduğu için kaotik davranış sergileyen ayrık bir dinamik haritadır (Kanwal vd., 2022). Denklem 27 ve Denklem 28 ile ifade edilmektedir.

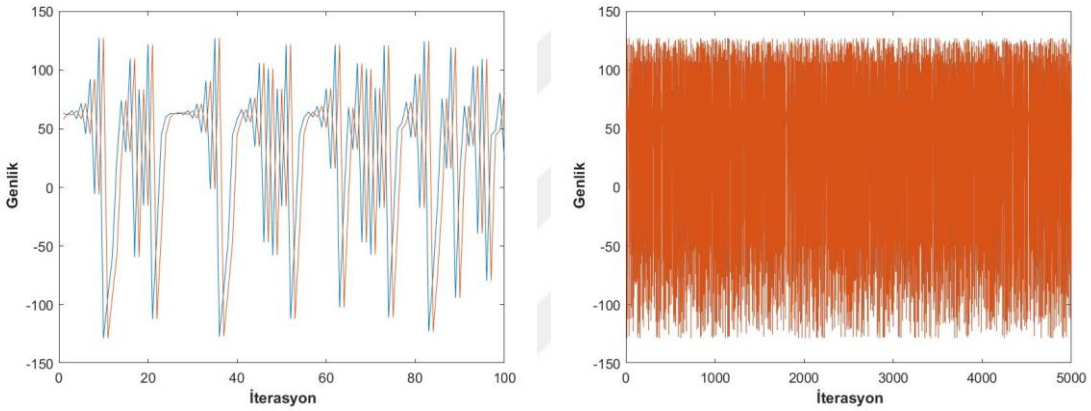
$$X(n+1) = 1 - aX(n)^2 + Y(n) \tag{27}$$

$$Y(n+1) = b(X(n)) \tag{28}$$

HCM sisteminin güçlü davranışı, kontrol parametreleri olarak adlandırılan a, b parametrelerinin değerlerine bağlıdır. HCM parametreleri ve koşulları aşağıdaki gibidir.

1. X_0 ve Y_0 başlangıç değerleridir.
2. a kontrol parametresidir ve [0, 1) aralığındadır.
3. b kontrol parametresidir.

HCM, davranışın rastgeleliği nedeniyle şifreleme alanındaki uygulamalar için sıklıkla tercih edilmektedir. HCM'de 100 ve 5000 iterasyon için elde edilen dağılım grafiği Şekil 26'da gösterilmiştir.



a) 100 iterasyon b) 5000 iterasyon

Şekil 26. Henon kaotik harita örneği

Bu yapı a=1.4, X_0 = 0.766, b = 0.3 ve Y_0 = 0.3432 için kaotiktir. Sonuç olarak, parametre değerlerindeki küçük bir değişiklik, bir sistemin farklı davranışlarına yol açabilmektedir.

3.1.2.2 Lozi kaotik harita

Lozi kaotik harita (LCM, Lozi Chaotic Map), HCM fonksiyonuna benzer bir davranış sergilemektedir (Öz, 2016). İki boyutlu parçalı doğrusal bir fonksiyondur. Denklem tanımı oldukça basit bir yapıya sahip olup gerçeklenmesi için Denklem 29 ve Denklem 30 ile ifade edilmektedir.

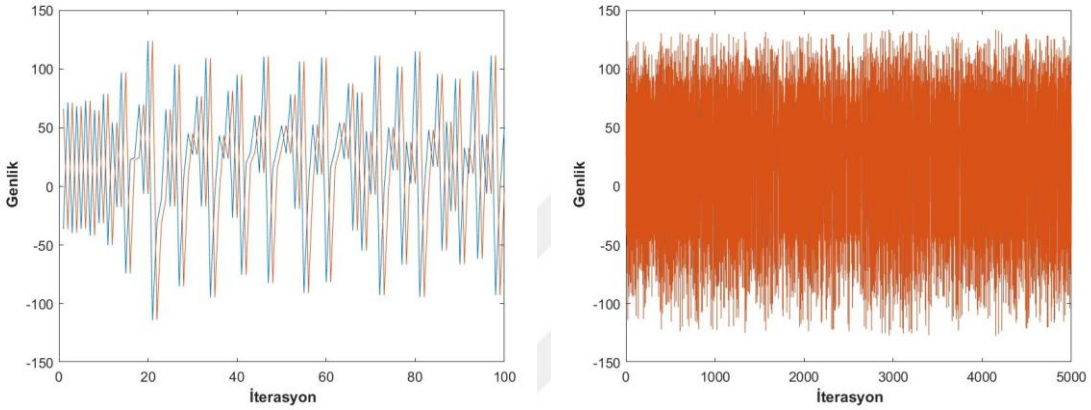
$$X(n+1) = 1 - a|X(n)| + bY(n) \tag{29}$$

$$Y(n+1) = X(n) \tag{30}$$

LCM parametreleri ve koşulları aşağıdaki gibidir.

1. X_0 ve Y_0 başlangıç değeri ve aynı zamanda permütasyon fazının gizli anahtarlarıdır.
2. a ve b kontrol parametreleridir.

Şekil 27'de 100 ve 5000 iterasyon için elde edilen dağılım grafiği gösterilmektedir.



a) 100 iterasyon b) 5000 iterasyon

Şekil 27. Lozi kaotik harita örneği

Bu yapı a=1.7, X_0 = -0.2, b = 0.5 ve Y_0 = 0.1 için kaotiktir. Her bir parametre değişikliğinde sistem farklı davranışlara neden olmaktadır.

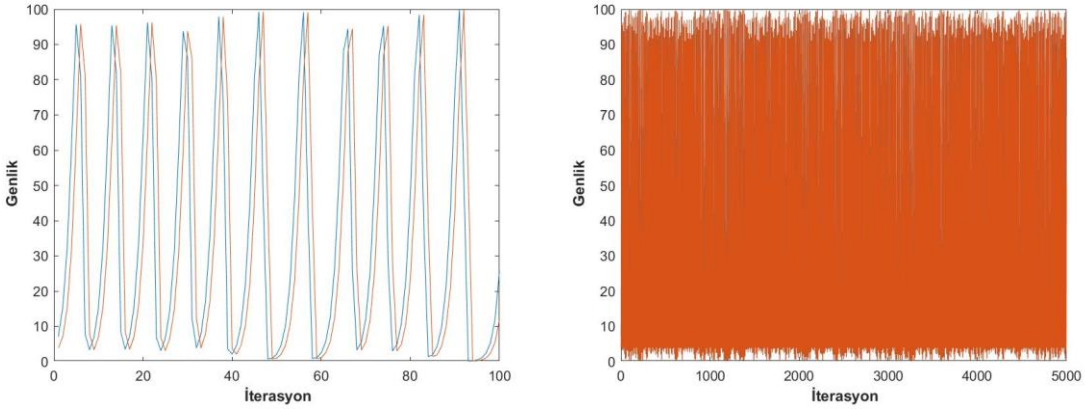
3.1.2.3 Gecikmeli lojistik harita

Gecikmeli lojistik harita (GLM, Delayed Logistic Map), geleneksel LM'in farklı bir versiyonudur (Dudás ve Krisztin, 2021). GLM'in geciktirilmiş biçimini Denklem 31 ve Denklem 32'de verilmiştir.

$$X_n = aX_{n-1}(1 - Y_{n-1}) \tag{31}$$

$$Y_n = X_{n-1} \tag{32}$$

Burada a sistem parametresini ifade etmektedir. GLM, başlangıç değeri ve gizli anahtar olan X_1 ve Y_1 değerlerine ihtiyaç duymaktadır. Şekil 28'de 100 ve 5000 iterasyon için GLM'in dağılımı gösterilmektedir.



a) 100 iterasyon b) 5000 iterasyon

Şekil 28. Gecikmeli lojistik harita örneği

Bu yapı *a*=2.27, X_1 = 0.001 ve Y_1 = 0.01 için kaotiktir. Her bir parametre değişikliğinde sistem farklı davranışlara neden olmaktadır.

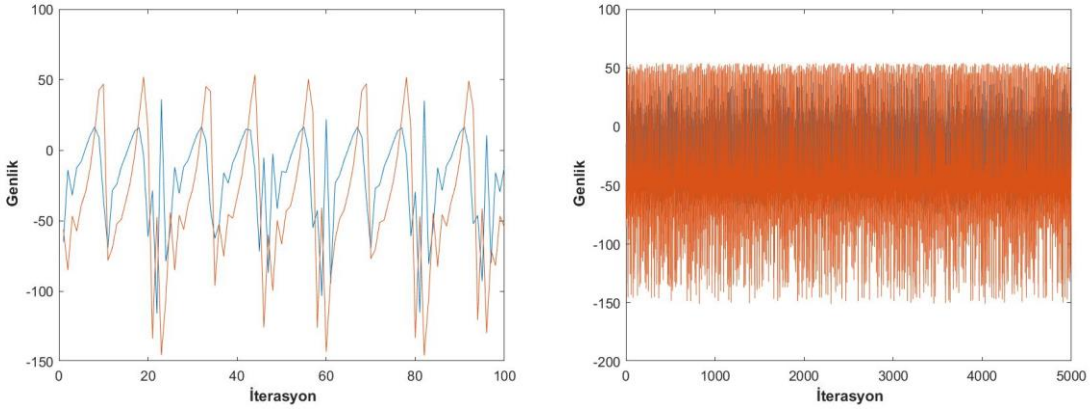
3.1.2.4 Tinkerbell kaotik harita

Tinkerbell kaotik harita (TCM, Tinkerbell Chaotic Map), ayrık zamanlı dinamik bir kaotik sistemdir (Stoyanov, 2014). Tinkerbell adının kökeni bilinmemektedir ancak, sistemin grafik resmi, bilindik Disney çizgi filmlerinin başında gösterildiği gibi, Tinker Bell'in Cinderella Kalesi üzerindeki hareketine benzerlik göstermektedir (Yuan, Jiang, ve Jing, 2011). TCM, Denklem 33 ve Denklem 34 ifade edilmektedir.

$$X_{n+1} = X_n^2 - Y_n^2 + aX_n + bY_n \tag{33}$$

$$Y_{n+1} = 2X_nY_n + cX_n + dY_n \tag{34}$$

Burada *n*, sistemin ayrık zaman evrimine karşılık gelen yineleme adımlarını temsil etmektedir. *a, b, c,* ve *d* parametreleri ise kontrol parametreleridir. TCM'nin 100 ve 5000 adet iterasyonundan elde edilen dağılım grafiği Şekil 29'da gösterilmiştir.



a) 100 iterasyon b) 5000 iterasyon

Şekil 29. Tinkerbell kaotik harita örneği

Bu yapının a=0.9, b=-0.6, c=2, d=0.5, X_0 = 0.1 ve Y_0 = 0.4 için kaotik olduğu görülmektedir. Her bir parametre değişikliğinde sistem farklı davranışlara neden olacaktır.

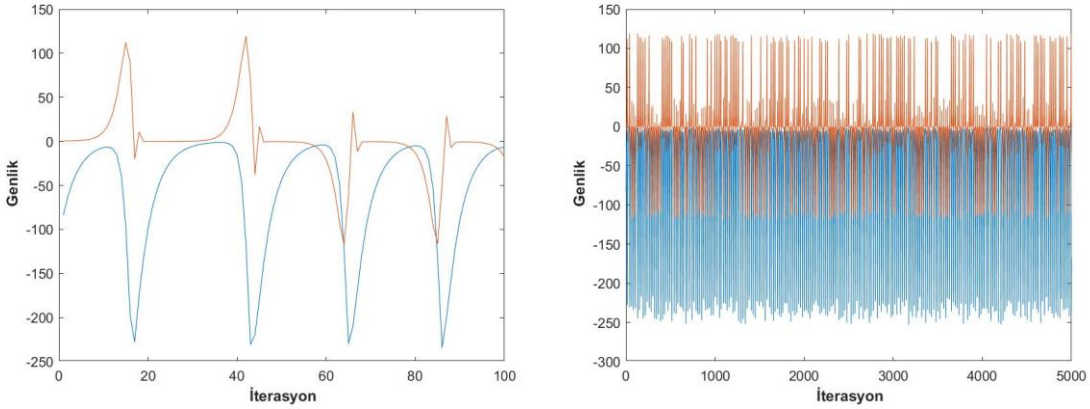
3.1.2.5 Burger'in kaotik haritası

Burger kaotik harita (BGCM, Burger's Chaotic Map), Burgers tarafından ortaya konmuştur. Bir çift birleştirilmiş diferansiyel denklemin ayrıştırılmış halidir. Bu denklemler aslında bir tür Lorenz modelidir (Elabbasy, Agiza, El-Metwally, ve Elsadany, 2007). BGCM denklemleri Denklem 35 ve Denklem 36 ile gösterilmektedir (Ran, 2020).

$$X(n+1) = (1-a)X(n) - Y(n)^2 \tag{35}$$

$$Y(n+1) = (1+b)Y(n) + Y(n)X(n) \tag{36}$$

Burada a, ve b parametreleri kontrol parametreleridir. Denklemin çalışabilmesi için başlangıçta X_0 ve Y_0 değerlerine ihtiyaç duyulmaktadır. Şekil 30'da 100 ve 5000 iterasyon için elde edilen dağılım verilmektedir.



a) 100 iterasyon b) 5000 iterasyon

Şekil 30. Burger kaotik harita örneği

Bu haritanın *a*=0.75, *b*=1.75, X_0 = -0.2 ve Y_0 = 0.1 için kaotik olduğu görülmektedir. Her bir parametre değişikliğinde sistem farklı davranışlara neden olacaktır.

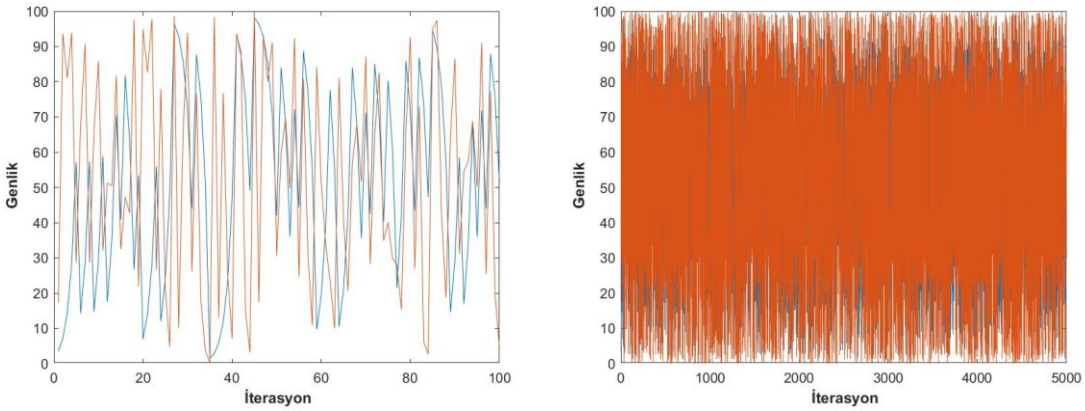
3.1.2.6 Kaplan Yorke kaotik harita

Kaplan Yorke kaotik harita (KYCM, Kaplan Yorke Chaotic Map), ayrık zamanlı bir dinamik sistemdir. Kaotik davranış sergileyen dinamik sistem örneklerinden biridir. James L. Kaplan ve James A. Yorke tarafından ortaya atılmıştır (Kordov, 2021). KYCM, Denklem 37 ve Denklem 38 ile ifade edilmektedir.

$$X_{i+1} = aX_i \; mod \; 1 \tag{37}$$

$$Y_{i+1} = bY_i + \cos\left(4\pi X_i\right) \tag{38}$$

Burada *a* ve *b* kontrol parametreleri $0 \leq a \leq 2$ ve $0 \leq b \leq 1$ aralığında yer almaktadır. Kaotik değerlerin elde edilebilmesi için X_0 ve Y_0 başlangıç değerlerine ihtiyaç duyulmaktadır. Bu değerler aynı zamanda gizli anahtar çiftini temsil etmektedir. Şekil 31'de 100 ve 5000 iterasyon için elde edilen dağılım verilmektedir.



a) 100 iterasyon b) 5000 iterasyon

Şekil 31. Kaplan Yorke kaotik harita örneği

Bu haritanın a=1.99999999, b=0.2, X_0 = 0.7071 ve Y_0 = -0.4 için kaotik olduğu görülmektedir. Her bir parametre değişikliğinde sistem farklı davranışlara neden olacaktır.

3.1.2.7 Ikeda kaotik harita

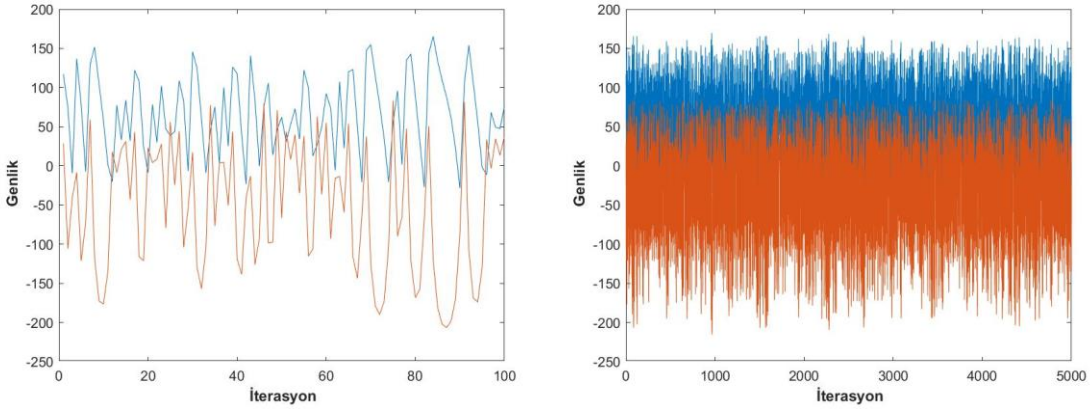
Ikeda kaotik harita (ICM, Ikeda Chaotic Map), iki boyutlu ayrık yapıya sahip kaotik bir haritadır (Stoyanov ve Ivanova, 2019). K. Ikeda tarafından 1979 yılında ortaya atılmıştır. ICM, aşağıdaki denklemler ile ifade edilmektedir.

$$X_{n+1} = 1 + u(X_n cost_n - Y_n sint_n) \tag{39}$$

$$Y_{n+1} = u(X_n sint_n + Y_n cost_n) \tag{40}$$

$$t_n = 0.4 - \frac{6}{1 + X_n^2 + Y_n^2} \tag{41}$$

Burada denklemde yer alan u sisteme ait parametredir ve [0.5, 0.95] aralığında olması gerekmektedir. Bu aralık dışında kaotik bir sistem elde edilememektedir. Kaotik değerlerin elde edilebilmesi için X_0 ve Y_0 başlangıç değerlerine ihtiyaç duyulmaktadır. Şekil 32'de 100 ve 5000 iterasyon için değer dağılımları gösterilmiştir.



a) 100 iterasyon b) 5000 iterasyon

Şekil 32. Ikeda kaotik harita örneği

Bu haritanın u=0.9, X_0 = 0.005 ve Y_0 = 0.0 için kaotik olduğu görülmektedir. Her bir parametre değişikliğinde sistem farklı davranışlara neden olacaktır.

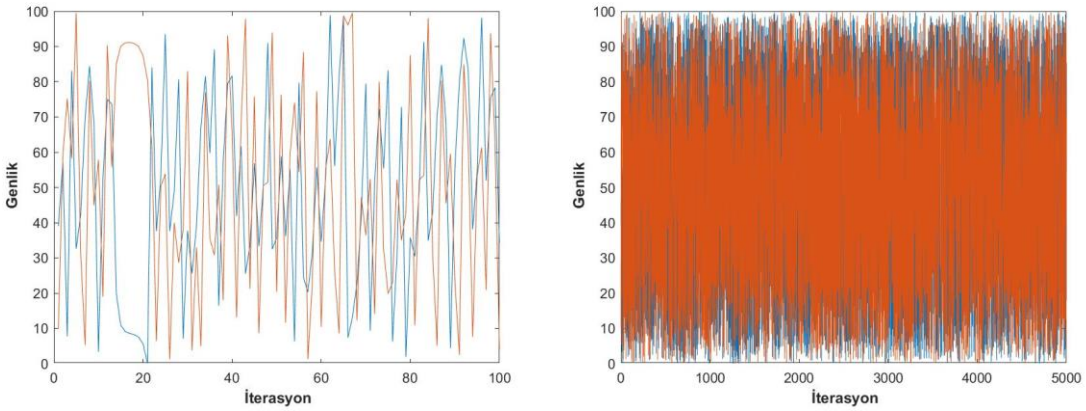
3.1.2.8 Sinai kaotik harita

Sinai kaotik harita (SICM, Sinai Chaotic Map), ACM ile benzer olan iki boyutlu ayrık yapıya sahip kaotik bir sistemdir (Pluhacek, Senkerik, Viktorin, ve Kadavy, 2020). SICM, Denklem 42 ve Denklem 43 ile gösterilmektedir.

$$X_{n+1} = X_n + Y_n + \delta\cos 2\pi Y_n \ (mod\ 1) \tag{42}$$

$$Y_{n+1} = X_n + 2Y_n \ (mod\ 1) \tag{43}$$

Burada, δ sistem parametresidir. Kaotik harita değerlerinin elde edilebilmesi için X_0 ve Y_0 başlangıç değerlerine ihtiyaç duyulmaktadır. Şekil 33'de 100 ve 5000 iterasyon için dağılım grafiği verilmiştir.



a) 100 iterasyon b) 5000 iterasyon

Şekil 33. Sinai kaotik harita örneği

Bu haritanın δ =0.10, X_0= 0.5 ve Y_0 = 0.5 için dağılımın kaotik olduğu görülmektedir. Her bir parametre değişikliğinde sistem farklı davranışlara neden olacaktır.

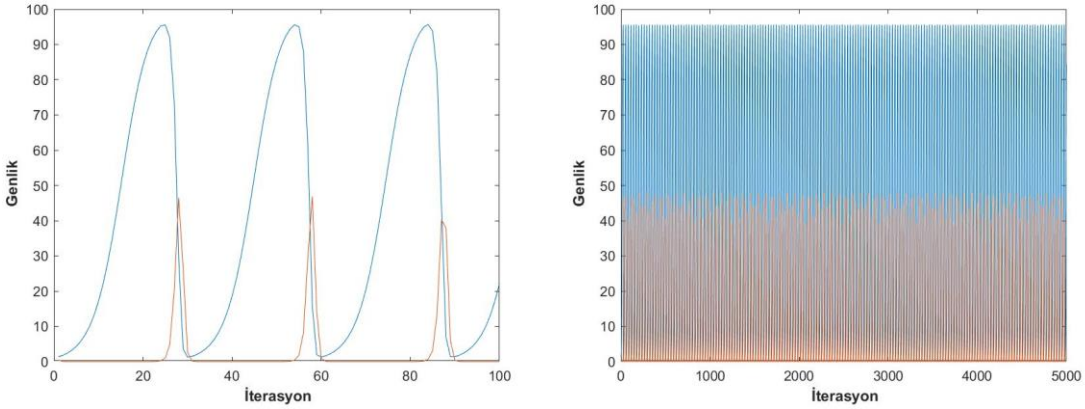
3.1.2.9 Ayrık zamanlı kaotik yırtıcı-av haritası

Ayrık zamanlı kaotik yırtıcı-av haritası (DTPPM, Discrete-Time Chaotic Predatory-Prey Map), (X.-w. Chen, Fu, ve Jing, 2013) tarafından önerilmiş ayrık zamanlı ve iki boyutlu kaotik bir sistemdir. DTPPM, Denklem 44 ve Denklem 45 ile gösterilmektedir.

$$x_{n+1} = ax_n(1 - x_n) - bx_n y_n \tag{44}$$

$$y_{n+1} = -cy_n + dx_n y_n \tag{45}$$

Burada, *x* ve *y* sırasıyla bir avın ve bir avcının popülasyon yoğunluklarını temsil etmektedir. Denklemde *a, b, c* ve *d* pozitif parametrelerdir. Burada *a*, avcının yokluğunda avın doğal büyüme hızını, *b* yırtıcılığın av üzerindeki etkisini, *c* avın yokluğunda avcının doğal ölüm oranını ve *d*, yırtıcı hayvanın verimini ve yayılma hızını temsil etmektedir (Zhao, Xuan, ve Li, 2016). Şekil 34'de 100 ve 5000 iterasyonlu dağılım grafiği gösterilmektedir.



a) 100 iterasyon b) 5000 iterasyon

Şekil 34. Ayrık zamanlı yırtıcı-av kaotik haritası örneği

Bu haritanın *a*=0.3, *b*=1, *c*=5, *d*=0, x_0 = 0.5 ve y_0 = 0.5 için dağılımın kaotik olduğu görülmektedir. Her bir parametre değişikliğinde sistem farklı davranışlara neden olacaktır.

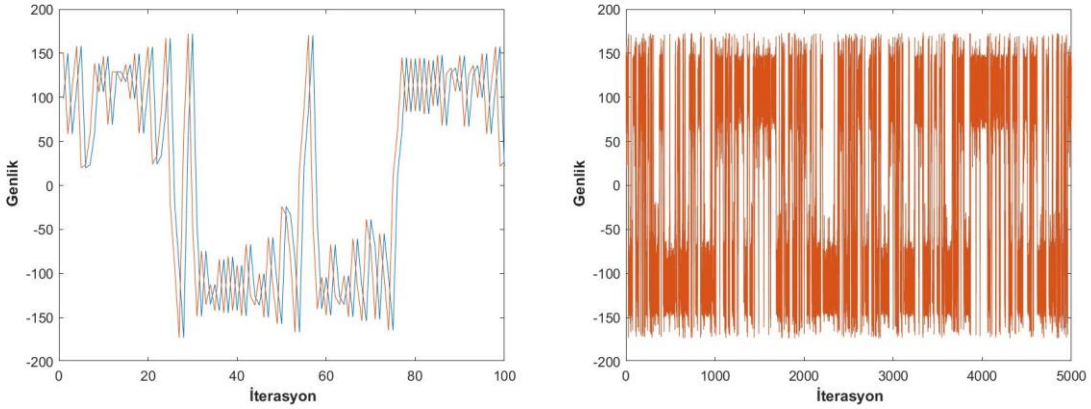
3.1.2.10 Holmes Kübik haritası

Holmes Kübik haritası (HLCM, Holmes Cubic Map), literatürde Duffing kaotik haritası (DF, Duffin Map) olarak ta geçmektedir. Ayrık zamanlı dinamik bir kaotik sistemdir. HLCM, ifadesi Denklem 46 ve Denklem 47 ile ifade edilmektedir (Rabie, Ahmad, ve Alghazzawi, 2022).

$$x_{n+1} = y_n \tag{46}$$

$$y_{n+1} = -bx_n + ay_n - y_n^3 \tag{47}$$

Burada a ve b sistem parametrelerini temsil etmektedir. Yöntemin çalışabilmesi ve seri üretebilmesi için x_0 ve y_0 değerlerine ihtiyaç duyulmaktadır. Bu ifadeler aynı zamanda gizli anahtar olarak kullanılmaktadır. Şekil 35'de 100 ve 5000 iterasyon için elde edilen sayı dizisi dağılımı grafiksel olarak gösterilmiştir.



a) 100 iterasyon b) 5000 iterasyon

Şekil 35. Holmes Kübik haritası örneği

Bu haritanın a=2.77, b=0.2, x_0 = 1.7 ve y_0 = 0 için dağılımın kaotik olduğu görülmektedir. Her bir parametre değişikliğinde sistem farklı davranışlara neden olacaktır.

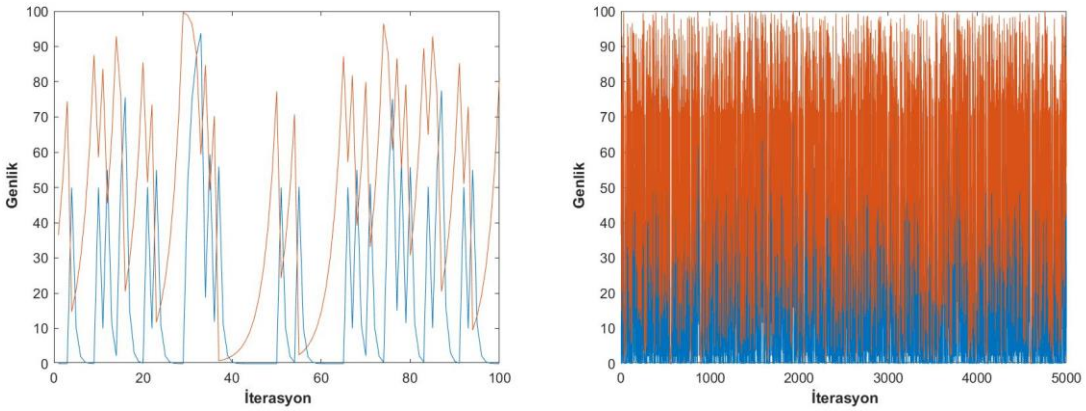
3.1.2.11 Baker kaotik harita

Baker kaotik harita (BACM, Baker Chaotic Map), yaygın kullanılan kaotik haritalardan birisidir. BACM, Denklem 48 ve Denklem 49 ile elde edilmektedir.

$$x_{n+1} = \begin{cases} \lambda_a x_n & y_n < \alpha \\ (1-\lambda_b) + \lambda_b x_n & y_n > \alpha \end{cases} \quad (48)$$

$$y_{n+1} = \begin{cases} \dfrac{y_n}{\alpha} & y_n < \alpha \\ \dfrac{y_n - \alpha}{\beta} & y_n > \alpha \end{cases} \quad (49)$$

Burada kontrol parametreleri $\beta = 1 - \alpha$ ve $\lambda_a + \lambda_b \leq 1$ olduğu durumlarda kaotik durumlar elde edilebilmektedir. x_0 ve y_0 başlangıç parametreleridir. Şekil 36'da 100 ve 5000 iterasyon için elde edilen sayı dizisi dağılımı grafiksel olarak gösterilmiştir.



a) 100 iterasyon b) 5000 iterasyon

Şekil 36. Baker kaotik harita örneği

Bu haritada α=0.7, β=0.3, x_0 = 0.1, y_0 = 0.5, λ_a=0.2 ve λ_b=0.5 için dağılımın kaotik olduğu görülmektedir. Her bir parametre değişikliğinde sistem farklı davranışlara neden olacaktır.

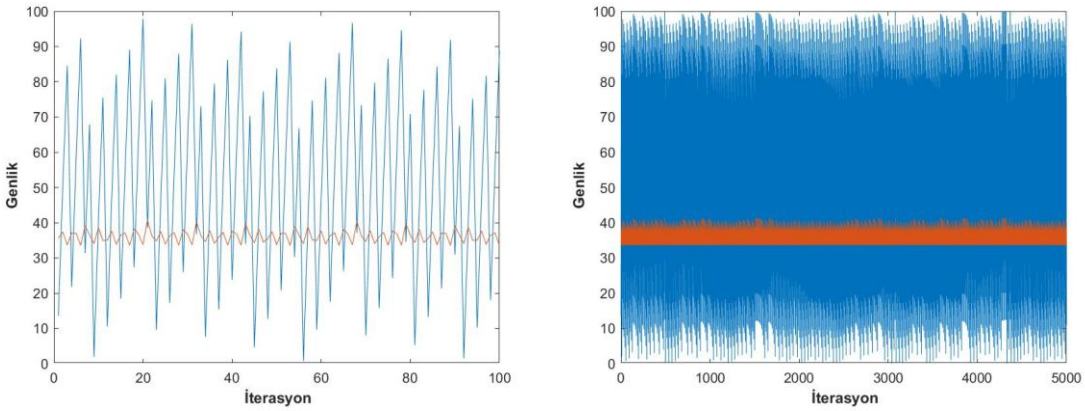
3.1.2.12 Bogdanov kaotik harita

Bogdanov kaotik harita (BOGCM, Bogdanov Chaotic Map), piksel konumlarının karıştırılması için (Arrowsmith, Cartwright, Lansbury, ve Place, 1993) tarafından önerilmiştir. BOGCM, Denklem 50 ve Denklem 51 ile ifade edilebilen iki boyutlu bir sistemdir (Cheroiu, Răducanu, ve Nitu, 2022).

$$x_{n+1} = x_n + y_{n+1} \tag{50}$$

$$y_{n+1} = y_n + \varepsilon y_n + k x_n (x_n + 1) + \mu x_n y_n \tag{51}$$

Burada, x_0 ve y_0 başlangıç parametrelerini k, ε ve μ sistem parametrelerini ifade etmektedir. Şekil 37'de 100 ve 5000 iterasyon için elde edilen sayı dizisi dağılımı grafiksel olarak gösterilmiştir.



a) 100 iterasyon b) 5000 iterasyon

Şekil 37. Bogdanov kaotik harita örneği

Bu haritada k=0.30, μ=-1.70, x_0= 1.8, y_0 = 0 ve ε = 0.15 için dağılımın kaotik olduğu görülmektedir. Her bir parametre değişikliğinde sistem farklı davranışlara neden olacaktır.

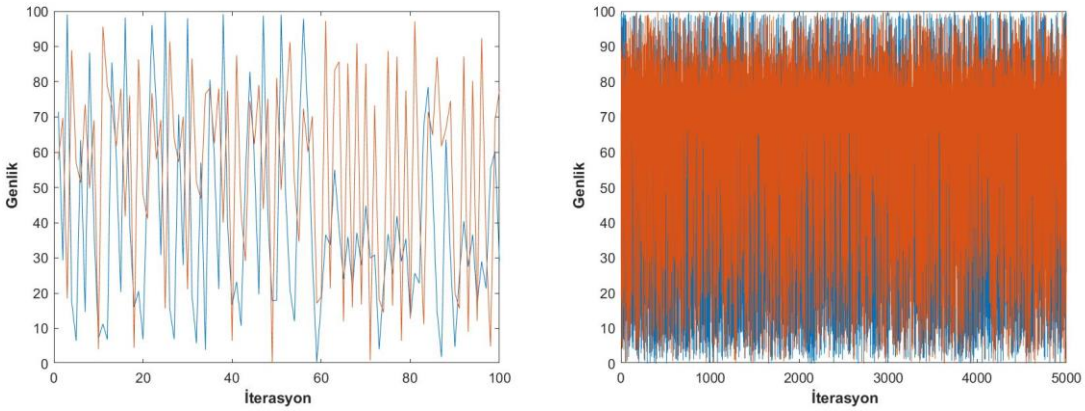
3.1.2.13 Basin kaotik harita

Basin kaotik harita (BSCM, Basin Chaotic Map), iki boyutlu bir kaotik haritadır. Denklem sistemi olarak BOGCM denklemine benzemektedir. BSCM, Denklem 52 ve Denklem 53 ile ifade edilmektedir (M. Khan, Masood, Alghafis, Amin, ve Batool Naqvi, 2019).

$$x_{n+1} = x_n + y_n \tag{52}$$

$$y_{n+1} = y_n + \varepsilon y_n + k x_n (x_n - 1) + \mu x_n y_n \tag{53}$$

Burada, x_0 ve y_0 başlangıç parametrelerini k, ε ve μ sistem parametrelerini ifade etmektedir. Şekil 38'de 100 ve 5000 iterasyon için elde edilen sayı dizisi dağılımı grafiksel olarak gösterilmiştir.



a) 100 iterasyon b) 5000 iterasyon

Şekil 38. Basin kaotik harita örneği

Bu haritada k=1.30, μ=-1.70, x_0 = -1.5, y_0 = 1.5 ve ε = 0.15 için dağılımın kaotik olduğu görülmektedir. Her bir parametre değişikliğinde sistem farklı davranışlara neden olacaktır.

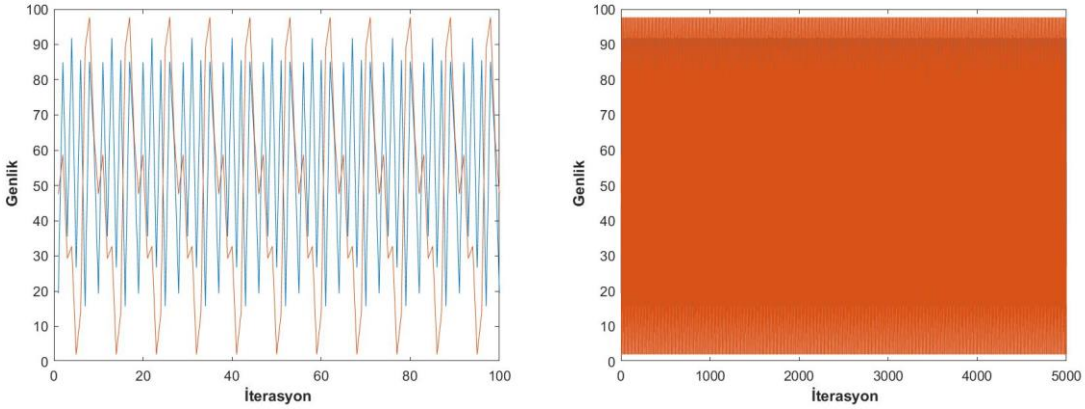
3.1.2.14 Chialvo kaotik harita

Chialvo kaotik harita (CHCM, Chialvo Chaotic Map), iki boyutlu kaotik haritadır. D. Chialvo tarafından önerilmiş ve Denklem 54 ve Denklem 55 ile ifade edilmektedir (Chialvo, 1995).

$$x_{n+1} = x_n^2 \exp(y_n - x_n) + k \tag{54}$$

$$y_{n+1} = a y_n - b x_n + c \tag{55}$$

Burada, x_0 ve y_0 başlangıç parametrelerini k, a, b ve c sistem parametrelerini ifade etmektedir. Şekil 39'da 100 ve 5000 iterasyon için elde edilen sayı dizisi dağılımı grafiksel olarak gösterilmiştir.



a) 100 iterasyon b) 5000 iterasyon

Şekil 39. Chialvo kaotik harita örneği

Bu haritada *k*=0.80, *a*=0.89, *b*=0.6, *c*=0.28, x_0 = 2, ve y_0 = 2.3 için dağılımın kaotik olduğu görülmektedir. Her bir parametre değişikliğinde sistem farklı davranışlara neden olacaktır.

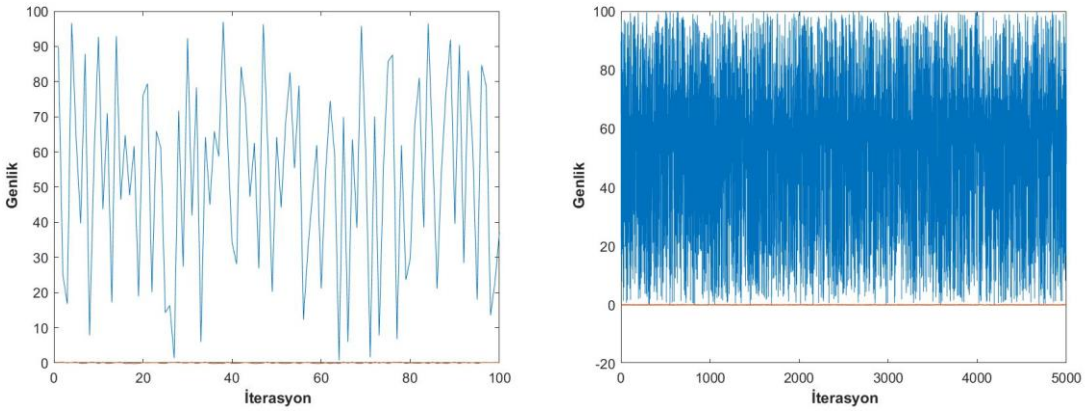
3.1.2.15 Zaslavsky kaotik harita

Zaslavsky kaotik harita (ZCM, Zaslavsky Chaotic Map), ZCM, George M. Zaslavsky tarafından ortaya atılan ayrık zamanlı bir dinamik bir kaotik sistemdir (Hamza ve Titouna, 2016). ZCM, Denklem 56 ve Denklem 57 ile ifade edilmektedir.

$$x_{n+1} = \left[x_n + v\left(1 + \left(\frac{1-e^{-r}}{r}\right)y_n\right) + \epsilon v\left(\frac{1-e^{-r}}{r}\right)\cos(2\pi x_n)\right](mod\ 1) \qquad (56)$$

$$y_{n+1} = e^{-r}(y_n + \epsilon\cos(2\pi x_n)) \qquad (57)$$

Burada, x_0 ve y_0 başlangıç parametrelerini ϵ, v ve r sistem parametrelerini ifade etmektedir. Şekil 40'da 100 ve 5000 iterasyon için elde edilen sayı dizisi dağılımı grafiksel olarak gösterilmiştir.



a) 100 iterasyon b) 5000 iterasyon

Şekil 40. Zaslavsky kaotik harita örneği

Bu haritada *k*=9, *a*=1.885, *e*=0.3, *v*=0.2, *r*=5, $\epsilon = 100$, x_0 = 0.1, ve y_0 = 0.1 için dağılımın kaotik olduğu görülmektedir. Her bir parametre değişikliğinde sistem farklı davranışlara neden olacaktır.

3.1.3 Koruyucu kaotik haritalar

Koruyucu kaotik haritalar yapıları gereği kendi açısal momentum gibi korunan bazı özel niceliklere sahiptir. Bulundukları uzayda kendi hacimlerini korumaktadırlar. Bu bölümde koruyucu kaotik haritalardan bazılarının detaylarına yer verilmiştir. Kaotik haritalar farklı iterasyon adımları ile test edilmiş ve dağılımları grafiksel olarak gösterilmiştir.

3.1.3.1 Chirikov kaotik harita

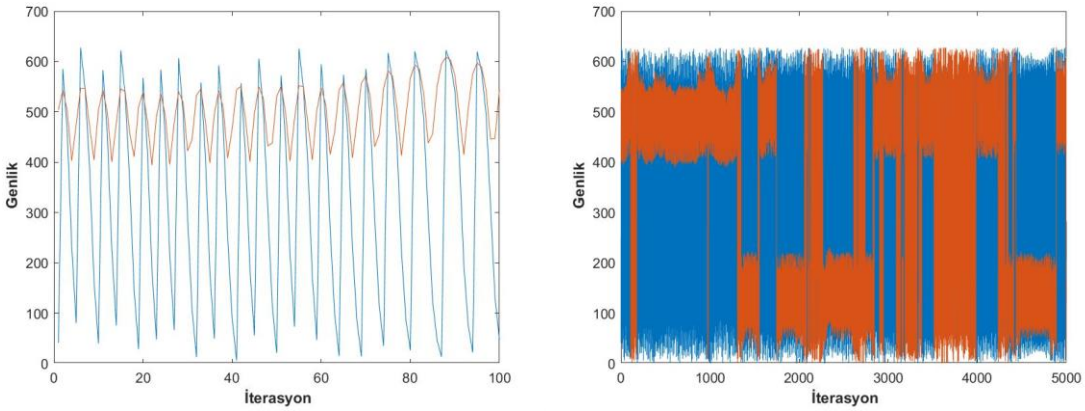
Chirikov kaotik harita (CHRCM, Chirikov Chaotic Map), kenarı 2π olan bir kareden iki adet dinamik değişken için kare alanını koruyan tersine çevrilebilen kaotik bir haritadır (Y. Zhang ve Xiao, 2013). CHRCM, Denklem 58 ve Denklem 59 ile gösterilmektedir (Durafe ve Patidar, 2022).

$$x_{i+1} = (x_i + y_i)\ mod 2\pi \tag{58}$$

$$y_{i+1} = (x_i + \delta \sin(x_i + y_i)) mod 2\pi \tag{59}$$

Burada, $\delta > 0$ kontrol parametresidir. x_i ve y_i'nin her ikisi de tüm *i* için [0, 2π) aralığında gerçel değerler almaktadırlar. Bu değerler aynı zamanda kaotik değerlerin elde

edilebilmesi için gerekli değerlerdir. 100 ve 5000 iterasyon için değer dağılımını gösteren bir grafik Şekil 41'de gösterilmiştir.



a) 100 iterasyon b) 5000 iterasyon

Şekil 41. Chirikov kaotik harita örneği

Bu haritanın kontrol parametresi δ = 0.3 ve başlangıç değerleri x_0 = 0.1 ve y_0 = 6 için dağılımın kaotik olduğu görülmektedir. Her bir parametre değişikliğinde sistem farklı davranışlara neden olacaktır.

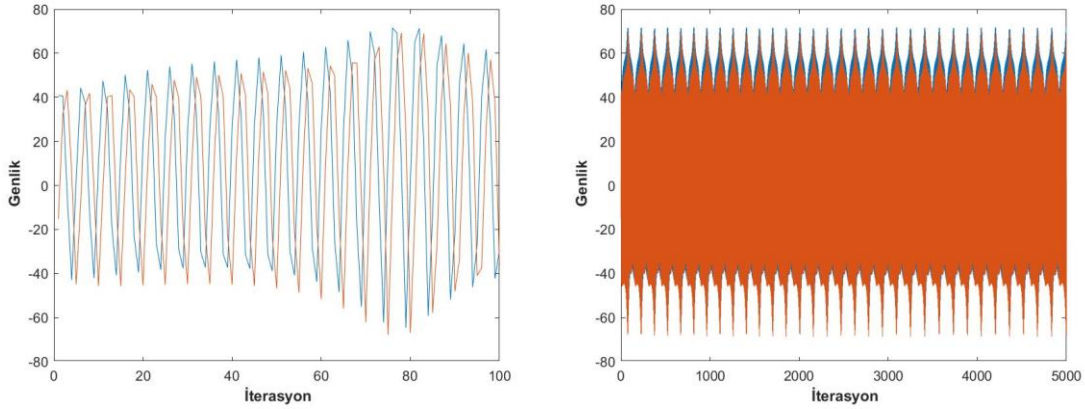
3.1.3.2 Hénon alan korumalı ikinci dereceden kaotik harita

Hénon alan korumalı ikinci dereceden harita (HAPQM, Henon Area-Preserving Quadratic Map), M. Hénon tarafından ortaya atılmıştır. HAPQM'e ait denklemler Denklem 60 ve Denklem 61 ile gösterilmektedir (Yin ve Min, 2010).

$$x_{n+1} = x_n cos\alpha - (y_n + x_n^2) sin\alpha \tag{60}$$

$$y_{i+1} = x_n sin\alpha + (y_n + x_n^2) cos\alpha \tag{61}$$

Burada, $0 \leq \alpha \leq \pi$ arasında sistem parametresidir. Kaotik harita değerlerinin elde edilebilmesi için x_0 ve y_0 başlangıç değerlerine ihtiyaç duyulmaktadır. Şekil 42'de 100 ve 5000 iterasyon için elde edilen dağılım grafiği gösterilmektedir.



a) 100 iterasyon b) 5000 iterasyon

Şekil 42. Hénon alan korumalı ikinci dereceden harita örneği

Bu haritanın kontrol parametresi α = 1.3284 ve başlangıç değerleri x_0 = 0.6 ve y_0 = 0.13 için dağılımın kaotik olduğu görülmektedir. Her bir parametre değişikliğinde sistem farklı davranışlara neden olacaktır.

3.1.3.3 Arnold'un kedi kaotik haritası

Arnold'un kedi kaotik haritası (ACM, Arnold's Cat Map), 1968 yılında Vladimir Arnold tarafından ortaya atılmıştır. Çalışmalar bir kedi resmi üzerinde yapıldığından bu ismi almıştır (Özyön vd., 2020). Kaotik görüntü şifrelemede en çok kullanılan tekniklerden biridir. ACM, iki boyutlu ters çevrilebilir kaotik bir haritadır. ACM, Denklem 62 ile ifade edilmektedir (Zareai, Balafar, ve Feizi Derakhshi, 2021).

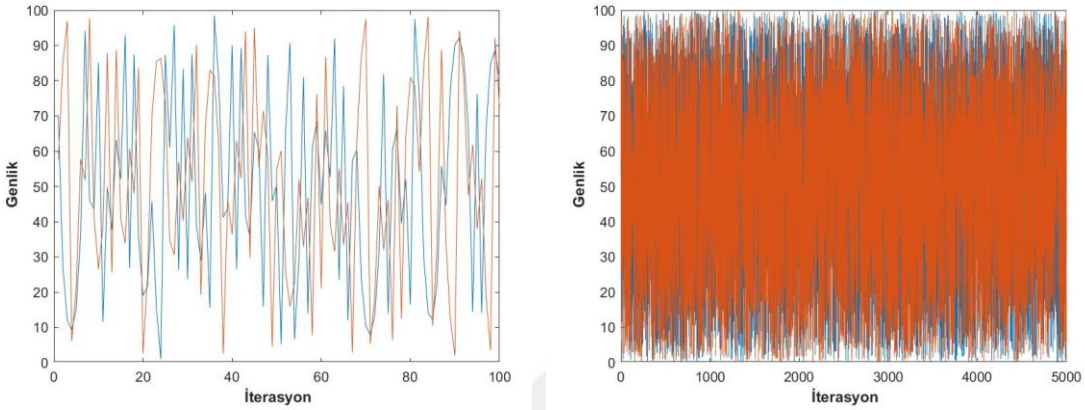
$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} mod\ N \tag{62}$$

Burada p ve q ifadeleri kontrol parametrelerini göstermektedir. *(N × N)* görüntü boyutunu, *(x, y)* orijinal görüntü piksel konumunu ve *(x′, y′)* Arnold dönüşümü uygulandıktan sonra karıştırılan görüntü içindeki yeni piksel konumunu belirtmektedir. Bu yeni piksel konumları ise Denklem 63 ve Denklem 64 ile elde edilmektedir.

$$x' = (x + py)\ mod\ N \tag{63}$$

$$y' = (px + (pq+1)y)\ mod\ N \tag{64}$$

Bu işlem görüntü piksel değerlerini değiştirmemekte sadece piksellerin mevcut konumlarını değiştirmektedir. Şekil 43'de 100 ve 5000 iterasyon için elde edilen dağılım grafiği verilmiştir.



a) 100 iterasyon b) 5000 iterasyon

Şekil 43. Arnold'un kedi kaotik haritası örneği

Bu haritanın kontrol parametresi p = 1, q=1.3284 ve başlangıç değerleri x_0 = 0 ve y_0 = 0.7071 için dağılımın kaotik olduğu görülmektedir. Her bir parametre değişikliğinde sistem farklı davranışlara neden olacaktır.

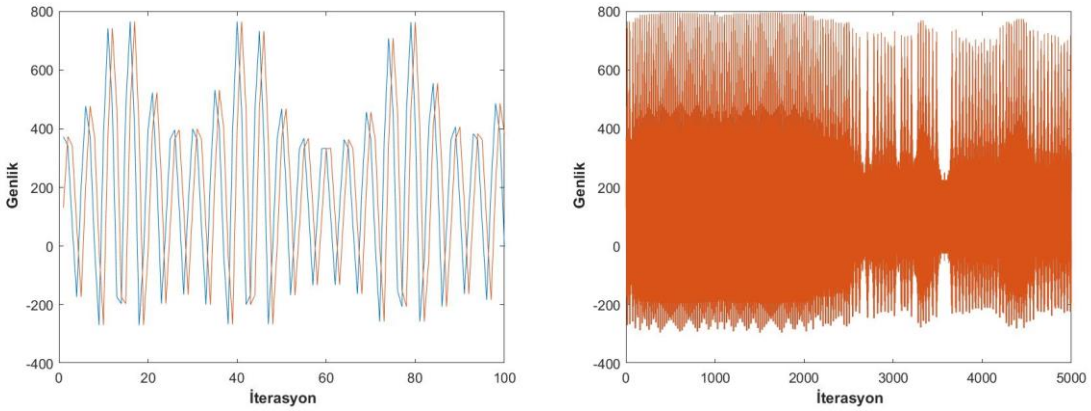
3.1.3.4 Gingerbreadman kaotik harita

Gingerbreadman kaotik harita (GCM, Gingerbreadman Chaotic Map), iki boyutlu kaotik bir haritadır. Parçalı doğrusal bir denklem olarak ifade edilmekte ve Denklem 65 ve Denklem 66 ile gösterilmektedir (Hassan, Aladhami, ve Mahdi, 2022).

$$x_{n+1} = 1 - y_n + |x_n| \tag{65}$$

$$y_{n+1} = x_n \tag{66}$$

Burada, başlangıç için x_0 ve y_0 değerlerine ihtiyaç duymaktadır. Şekil 44'de 100 ve 5000 iterasyon için dağılım grafiği verilmiştir.



a) 100 iterasyon b) 5000 iterasyon

Şekil 44. Gingerbradman kaotik harita örneği

Bu haritanın başlangıç değerleri x_0 = 0.51 ve y_0 = 3.7 için dağılımın kaotik olduğu görülmektedir. Her bir parametre değişikliğinde sistem farklı davranışlara neden olacaktır.

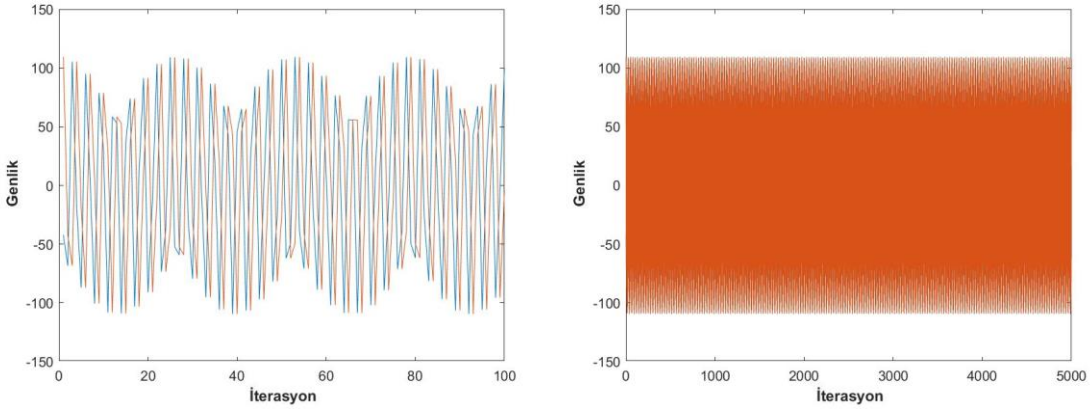
3.1.3.5 Kaotik web haritası

Kaotik web haritası (CWM, Chaotic Web Map), tekrarlanan ve doğrusal olmayan bir kaotik harita türüdür. CWM denklemi Denklem 67 ve Denklem 68 ile aşağıdaki gibi verilmiştir (Rueda, Vera, Rodríguez, ve Torroba, 2008).

$$x_{n+1} = x_n cos\alpha - (y_n + ksinx_n)sin\alpha \quad (67)$$

$$y_{n+1} = x_n sin\alpha + (y_n + ksinx_n)cos\alpha \quad (68)$$

Burada, k sistem parametresidir. Başlangıç olarak (x_0, y_0) değerlerine ihtiyaç duyulmaktadır. Şekil 45'de 100 ve 5000 iterasyondan elde edilen dağılım grafiği gösterilmiştir.



a) 100 iterasyon b) 5000 iterasyon

Şekil 45. Kaotik web haritası örneği

Bu haritanın kontrol parametresi α = 1.5708, k=1 ve başlangıç değerleri x_0 = 0 ve y_0 = 0.98 için dağılımın kaotik olduğu görülmektedir. Her bir parametre değişikliğinde sistem farklı davranışlara neden olacaktır.

3.1.3.6 Lorenz kaotik harita

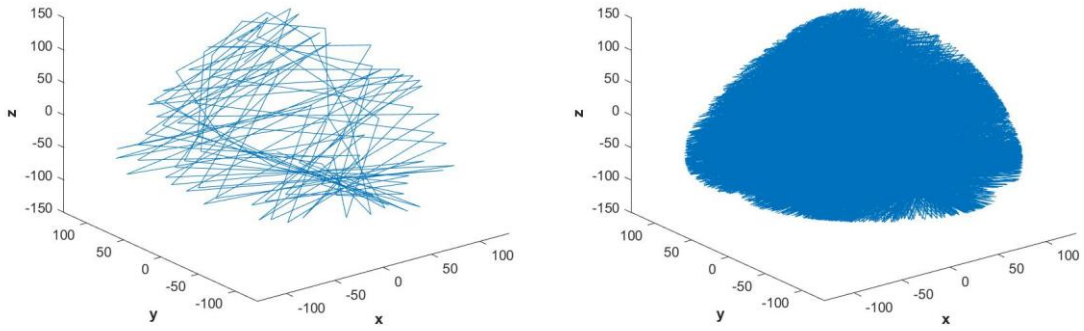
Lorenz kaotik harita (LRCM, Lorenz Chaotic Map), 1963 yılında Edward Lorenz tarafından önerilmiştir. Bu model atmosferik değişimlerin incelenmesi için üretilmiştir. Model diferansiyel denklem sistemleri yardımıyla tanımlanmaktadır (Munir, Khan, Jamal, Hazzazi, ve Hussain, 2021). LRCM, Denklem 69, Denklem 70 ve Denklem 71 ile aşağıdaki biçimde ifade edilmektedir.

$$x' = a(y - x) \tag{69}$$

$$y' = cx - xz - y \tag{70}$$

$$z' = xy - bz \tag{71}$$

Burada, sistemin kaotik davranışı, *x*, *y* ve *z* değişkenlerinin bazı başlangıç değerleri ile *a*, *b* ve *c* kontrol parametrelerine bağlıdır. Başlangıç değerlerinde ve sistem parametrelerindeki çok küçük değişiklikler kaotik sistem üzerinde büyük sonuçlara neden olabilmektedir. Şekil 46'da 100 ve 5000 iterasyon için elde edilen dağılım grafiği gösterilmiştir.



a) 100 iterasyon b) 5000 iterasyon

Şekil 46. Lorenz kaotik harita örneği

Bu haritanın kontrol parametresi a=1, b=1, c=1 ve başlangıç değerleri x_0 = 0.5, y_0 = 0.51 ve z_0 = -0.99 için dağılımın kaotik olduğu görülmektedir. Her bir parametre değişikliğinde sistem farklı davranışlara neden olacaktır.

3.1.3.7 Chua kaotik harita

Chua kaotik harita (CUHCM, Chua Chaotic Map), üç boyutlu kaotik bir sistemdir. Literatürde Chua devresi (Chua Circuit) olarak ta anılmaktadır. Üç parçalı doğrusal bir fonksiyona sahiptir. CUHCM, Denklem 71, Denklem 73 ve Denklem 74 ile ifade edilmektedir (AlMutairi ve Bonny, 2020).

$$x' = \alpha(y - x - f(x) \tag{71}$$

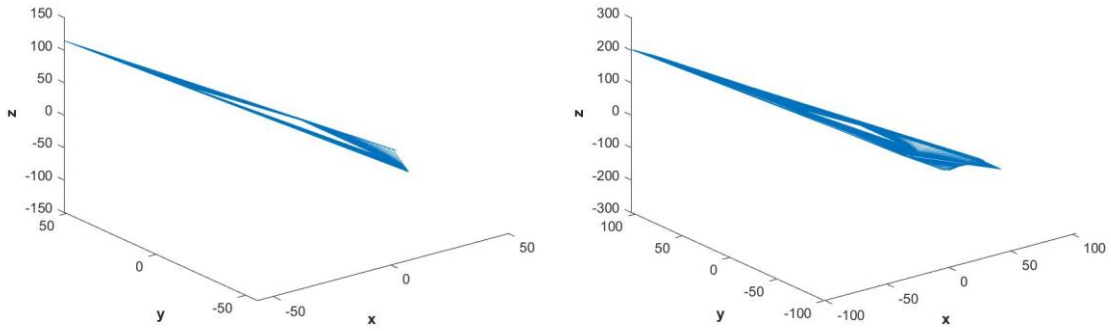
$$y' = x - y + z \tag{72}$$

$$z' = -\beta y \tag{73}$$

Denklem 75'de verilen $f(x)$ fonksiyonu Denklem 74 ile ifade edilmektedir.

$$f(x) = bx + 0.5(a - b)(|x + 1.0| - |x - 1.0|) \tag{75}$$

Burada α, β, a ve b sistem parametrelerini ifade etmektedir. Şekil 47'de 100 ve 5000 iterasyon için elde edilen dağılım grafiği gösterilmiştir.



a) 100 iterasyon b) 5000 iterasyon

Şekil 47. Chua kaotik harita örneği

Bu haritanın sistem parametresi α=1.000056, β=2.000008, a=-0.00714, b=-1.0143 ve başlangıç değerleri x_0 = 0.07, y_0 = 0.03 ve z_0 = 0.08 için dağılımın kaotik olduğu görülmektedir. Her bir parametre değişikliğinde sistem farklı davranışlara neden olacaktır.

3.1.3.8 Rossler'in kaotik haritası

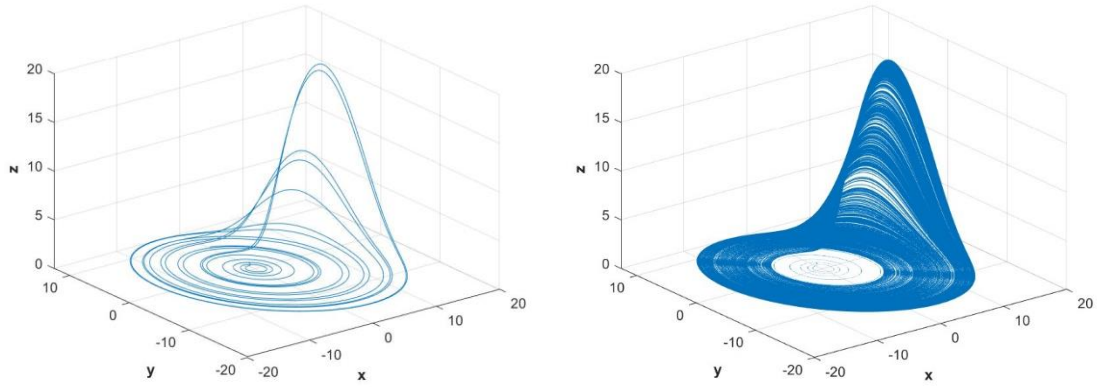
Rossler'in kaotik haritası (ROCM, Rossler's Chaotic Map), üç boyutlu kaotik bir sistemdir. Lorenz sistemine göre oldukça basit üç parçalı doğrusal olmayan denklem sistemine sahiptir. ROCM, Denklem 76, Denklem 77 ve Denklem 78 ile ifade edilmektedir (Alsafasfeh ve Arfoa, 2011).

$$x' = -y - z \tag{76}$$

$$y' = x + ay \tag{77}$$

$$z' = b + z(x - c) \tag{78}$$

Burada x, y, z, a, b ve c sistem parametrelerini ifade etmektedir. Şekil 48'de 100 ve 5000 iterasyon için elde edilen dağılım grafiği gösterilmiştir.



c) 100 iterasyon d) 5000 iterasyon

Şekil 48. Rossler'in kaotik harita örneği

Bu haritanın kontrol parametresi a=0.5, b=0.2, c=10 ve başlangıç değerleri x_0 = 0.5, y_0 = 1.5 ve z_0 = 0.1 için dağılımın kaotik olduğu görülmektedir. Her bir parametre değişikliğinde sistem farklı davranışlara neden olacaktır. İterasyon sayısı arttıkça süre karmaşıklık grafiğinin elde edilmesi süresi de uzamaktadır.

3.2 Kaotik Haritalar ve Özellikleri

Bu bölümde incelenen 45 adet kaotik haritanın tüm özellikleri bir arada Tablo 1'de verilmiştir. İncelenen kaotik haritalar başlangıç parametrelerine ihtiyaç duymaktadırlar. Bu nedenle parametre sayısı verilirken başlangıç parametreleri de hesaplamaya dâhil edilerek tüm parametre sayıları verilmiştir.

Tablo 1. İncelenen kaotik haritalar ve özellikleri

Kaotik Harita	Türü	Zaman Domaini	Uzay Domaini	Boyutu	Parametre Sayısı
Lojistik harita	Tersine çevrilemeyen kaotik haritalar	Ayrık	Gerçek	1	2
Kübik harita		Ayrık	Gerçek	1	2
Doğrusal uyumlu üreteç haritası		Ayrık	Gerçek	1	4
Sinüs haritası		Ayrık	Gerçek	1	2
Çadır harita		Ayrık	Gerçek	1	1
Gauss harita		Ayrık	Gerçek	1	3
Kaotik Uç harita		Ayrık	Gerçek	1	2
Gaussian beyaz kaotik harita		Ayrık	Gerçek	1	1
Kıskaç harita		Ayrık	Gerçek	1	3
Spens harita		Ayrık	Gerçek	1	1
Sinüs çemberi harita		Ayrık	Gerçek	1	3
Parçalı kaotik harita		Ayrık	Gerçek	1	2
Kaotik singer haritası		Ayrık	Gerçek	1	2

Sinüzodial kaotik harita		Ayrık	Gerçek	1	1
Chebyshev kaotik harita		Ayrık	Gerçek	1	2
May kaotik harita		Ayrık	Gerçek	1	2
Gompertz kaotik harita		Ayrık	Gerçek	1	2
Trigonometrik kaotik harita		Ayrık	Gerçek	1	2
Bernoulli kaotik harita		Ayrık	Gerçek	1	2
Ricker kaotik harita		Ayrık	Gerçek	1	3
Aizawa kaotik harita		Ayrık	Gerçek	1	2
Beta kaotik harita		Ayrık	Gerçek	1	11
Henon kaotik harita	Dağıtıcı kaotik haritalar	Ayrık	Gerçek	2	4
Lozi kaotik harita		Ayrık	Gerçek	2	4
Gecikmeli lojistik harita		Ayrık	Gerçek	2	3
Tinkerbell kaotik harita		Ayrık	Gerçek	2	6
Burger'in kaotik haritası		Ayrık	Gerçek	2	4
Kaplan-Yorke kaotik harita		Ayrık	Gerçek	2	4
Ikeda kaotik harita		Ayrık	Gerçek	2	3
Sinai kaotik harita		Ayrık	Gerçek	2	3
Ayrık zamanlı kaotik yırtıcı-av haritası		Ayrık	Gerçek	2	6
Holmes Kübik haritası		Ayrık	Gerçek	2	4
Baker kaotik harita		Ayrık	Gerçek	2	6
Bogdanov kaotik harita		Ayrık	Gerçek	2	5
Basin kaotik harita		Ayrık	Gerçek	2	5
Chialvo kaotik harita		Ayrık	Gerçek	2	6
Zaslavsky kaotik harita		Ayrık	Gerçek	2	8
Chirikov kaotik harita	Koruyucu kaotik haritalar	Ayrık	Gerçek	2	3
Hénon alan korumalı ikinci dereceden kaotik harita		Ayrık	Gerçek	2	3
Arnold'un kedi kaotik haritası		Ayrık	Gerçek	2	4
Gingerbradman kaotik harita		Ayrık	Gerçek	2	2
Kaotik web haritası		Ayrık	Gerçek	2	4
Lorenz kaotik harita		Sürekli	Gerçek	3	6
Chua kaotik harita		Sürekli	Gerçek	3	7
Rossler'in kaotik haritası		Sürekli	Gerçek	3	6

3.3 Değerlendirme Ölçütleri

Görüntü şifreleme tekniklerinin başarısı ve etkinliğini doğrulamak için değerlendirme ölçütleri son derece büyük bir öneme sahiptir. Bu sayede ortaya atılan yöntemlerde açıklar mevcut ise kolaylıkla tespit edilebilmekte ve önlemler alınabilmektedir. Literatürde görüntü şifreleme yöntemlerini analiz etmek için çeşitli analiz teknikleri bulunmaktadır. Bu teknikler diferansiyel analizler, istatistiksel analizler ve diğer analizler olarak üç sınıfta toplanabilmektedir (Kaur ve Kumar, 2020). Buna ek olarak NIST rastgelelik testide bulunmaktadır.

3.3.1 Diferansiyel analizler

Diferansiyel saldırıları analiz etmek için literatürde yaygın olarak iki yöntem kullanılmaktadır. Bunlardan birincisi Piksel Değişim Oranı (NPCR, Number Of Changing Pixel Rate) ikincisi ise Birleşik Ortalama Değişen Yoğunluk (UACI, Unified Averaged Changed Intensity) parametreleridir. Diferansiyel saldırılar, şifreleme algoritmalarının düz görüntüdeki en küçük değişikliklere karşı duyarlılığını test etmek için kullanılmaktadır. Saldırganlar genellikle orijinal görüntüler üzerinde çok küçük bir değişiklik yapmaktadırlar. Ardından orijinal ve değiştirilmiş görüntüleri ortak gizli anahtarı kullanarak şifrelemektedirler. Son aşamada ise orijinal ve değiştirilmiş görüntülerin şifrelenmiş görüntüleri arasındaki ilişkiyi tespit etmeye çalışmaktadırlar.

3.3.1.1 Piksel değişim oranı

NPCR, düz görüntüleri sadece bir piksellik farka sahip olan iki görüntü arasındaki farklı piksel sayılarının yüzdesi olarak tanımlanmaktadır. Başka bir ifadeyle tüm piksellerin yüzde kaçının değiştiğini tespit etmek için kullanılmaktadır. NPCR değerinin %99.61'e yakın olması önerilen algoritmanın diferansiyel saldırılara karşı dayanıklı olduğu anlamına gelmektedir (Belazi, Abd El-Latif, ve Belghith, 2016). NPCR Denklem 79 ile hesaplanabilir (Saidi, Cherrid, Bentahar, Mayache, ve Bentahar, 2020).

$$NPCR = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)}{MxN} x100 \qquad D(i,j) = \begin{cases} 0 & eğer\ C_1 = C_2 \\ 1 & eğer\ C_1 \neq C_2 \end{cases} \tag{79}$$

Burada, *M* ve *N* şifrelenmiş görüntülerin genişlik ve yüksekliğini, C_1, piksel değişiminden önce şifrelenen görüntüyü ve C_2 piksel değişiminden sonra şifrelenen görüntüyü temsil etmektedir. Her iki görüntüde aynı koordinatlara karşılık gelen piksel değerleri aynı ise 0 farklı ile 1 değeri üretilmektedir.

3.3.1.2 Birleşik ortalama değişen yoğunluk

UACI, iki görüntü arasındaki ortalama yoğunluğu hesaplamak için tercih edilen diferansiyel analiz tekniklerinden biridir. Bir başka ifadeyle UACI, piksellerin yüzde kaç oranında değiştiğini hesaplamak için kullanılmaktadır. İdeal UACI değerinin %33.46'ya yakın olması beklenmektedir (Budiman, Andono, ve Setiadi, 2022). *M* ve *N* şifrelenmiş

görüntülerin genişlik ve yüksekliğini, C_1, piksel değişiminden önce şifrelenen görüntüyü ve C_2 piksel değişiminden sonra şifrelenen görüntüyü temsil etmek üzere UACI, Denklem 80 ile hesaplanmaktadır.

$$UACI = \frac{1}{MxN}\left[\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(C_1(i,j) - C_2(i,j))}{255}\right]x100 \quad (80)$$

3.3.2 İstatistiksel analizler

İstatistiksel analizler, şifrelenmiş görüntülerin kırılması için sıklıkla tercih edilmektedir. Dolayısı ile şifreleme tekniklerinin istatistiksel saldırılara karşı dayanıklılığının test edilmesi gerekmektedir. Bir şifreleme tekniğinin sağlamlığını doğrulamak amacıyla histogram analizi ve korelasyon katsayısı analizi en çok tercih edilen yöntemler arasında yer almaktadır.

3.3.2.1 Histogram analizi

Histogram analizi, bir görüntüdeki piksel değerlerinin dağılımını ortaya çıkaran bir yöntemdir. Orijinal görüntülere ait histogramların şifrelenmiş görüntülerin histogramından tamamen farklı olması gerekmektedir. Orijinal yani düz görüntülerin piksel dağılımı histogramları doğası gereği tek tip bir yapıya sahip değillerdir. Buna karşılık şifrelenmiş görüntülerin piksel dağılım histogramlarının tek tipte olması gerekmektedir (Sivakumar ve Venkatesan, 2015). Şifrelemiş görüntülerde histogramların tek tip olması hem piksellerin uzayda eşit olarak dağıldığını hem de şifreleme tekniğinin sağlamlığını göstermektedir.

3.3.2.2 Korelasyon katsayısı analizi

Korelasyon katsayısı analizi, orijinal ve şifreli bir görüntünün birbirlerine karşılık gelen pikselleri arasındaki benzerliği tespit etmek için kullanılmaktadır. Orijinal bir görüntüde görüntünün komşu piksel değerleri yatay, çapraz ve dikey olmak üzere üç farklı yönde güçlü bir şekilde ilişki bulunmaktadır. İyi bir görüntü şifreleme tekniğinde, şifrelenmiş görüntüye ait bu ilişkilerin en aza indirilmesi gerekmektedir (Abd El-Samie vd., 2013). Korelasyon katsayısı Denklem 81'de yardımıyla hesaplanmaktadır (Chai, Gan, Yang, Chen, ve Liu, 2017).

$$r_{x,y} = \frac{C(x,y)}{\sqrt{D(x)}.\sqrt{D(y)}} \tag{81}$$

Burada;

$$C(x,y) = \frac{\sum_{i=1}^{K}(x_i - E(x))(y_i - E(x))}{K} \tag{82}$$

$$D(x) = \frac{1}{K}\sum_{i=1}^{K}(x_i - E(x))^2 \tag{83}$$

$$D(y) = \frac{1}{K}\sum_{i=1}^{K}(y_i - E(y))^2 \tag{84}$$

Burada *C(x, y)*, x ve y örnekleri arasındaki kovaryansı ifade etmektedir. Denklemde verilen *x* ve *y* bir görüntünün koordinatlarıdır. *K*, (x_i, y_i) piksel çiftlerinin sayısıdır. *D(x)* ve *D(y)*, sırasıyla x ve y'nin standart sapmasıdır. *E(x)*, x_i piksel değerlerinin ortalamasıdır. Korelasyon katsayısı [-1, 1] aralığında ve şifrelenmiş görüntüde ise korelasyon katsayısının 0'a yakın olması beklenmektedir (Gupta, Singh, Gupta, ve Shukla, 2022).

3.3.3 Diğer analiz teknikleri

İyi bir şifreleme tekniğinin gerçek anlamda dayanıklılığını ispat etmek için farklı tekniklere de ihtiyaç duyulmaktadır. Bu bölümde diferansiyel analizler ve istatistiksel analizler dışında kalan ve herhangi sınıflandırmaya giremeyen görüntü şifreleme tekniklerinin ayrıntılarına yer verilmiştir.

3.3.3.1 Bilgi entropisi

Bilgi entropisi, bir görüntüde bit başına düşen ortalama bilginin ölçülmesi için kullanılmaktadır. Bir görüntüde yer alan olası bilgileri ölçmeye yardımcı olmaktadır. Görüntüde yer alan her bir pikselin değeri birbirinden farklıdır. Bu durum, şifrelenmiş bir görüntünün entropi değerinin eşit olasılığa sahip olması gerektiği anlamına gelmektedir (W. Zhang, Wong, Yu, ve Zhu, 2013). Şifrelenmiş görüntülerde ideal entropi değerinin 8 olması beklenmektedir. Bir başka ifadeyle, şifrelenmiş bir görüntünün entropi değeri 8'e

ne kadar yakınsa önerilen şifreleme yönteminin de o kadar iyi olduğu anlamına gelmektedir. Bir görüntünün entropisi Denklem 85 ile hesaplanmaktadır.

$$H(s) = -\sum_{S}(P(s_i)\ x\ \log_2 P(s_i)) \tag{85}$$

Burada *S* mesajının entropisi *H(S)* ile gösterilmektedir. $P(s_i)$, s_i'nin görüntü veri dizisi içerisindeki olasılığını ifade etmektedir. Entropi değeri [0, 8] aralığındadır (M. Ahmad vd., 2022). Şifreli 8 bitlik bir görüntünün ideal entropi değeri 8'e yakın olmalıdır.

3.3.3.2 Anahtar analizi

Anahtar analizi, herhangi bir şifreleme algoritmasının en temel parçalarından birisidir. Bir şifreleme algoritmasının gücü buna bağlıdır. Şifrelemede kullanılacak olan gizli anahtarların her türlü saldırıya direnecek kadar güçlü olması gerekmektedir. Güçlü bir gizli anahtar yüksek hassasiyete ve çok geniş bir anahtar uzayına sahip olmalıdır (Ghebleh, Kanso, ve Noura, 2014). Anahtar uzayı gizli anahtarın boyuna bağlıdır. Gizli anahtarın boyutu ne kadar büyük olursa bir saldırganın doğru anahtarı tahmin etmesi de o kadar zor olmaktadır. Şifrelemede kullanılacak olan anahtarın hassasiyeti de son derece önemlidir. Anahtar hassasiyeti, saldırganın orijinal anahtardaki tek bir pikseli bile değiştirmesi durumunda orijinal görüntünün kurtarılamayacağı anlamına gelmektedir. Bu nedenlerden dolayı önerilecek bir şifreleme algoritmasında anahtar analizinin mutlaka yapılması ve saldırılara açık halde olmaması gerekmektedir.

3.3.3.3 Gürültü saldırısı

Gürültü, görüntüler üzerinde meydana gelen parazitlerdir. Bir başka ifadeyle, dijital ortamlarda görüntülerin elde edilmesi veya iletilmesi sırasında meydana gelen istenmeyen bilgilere gürültü adı verilmektedir. Görüntüler üzerinde istenmeyen benekli bir görünüm meydana getirirler (Küpeli ve Bulut, 2020). Bu gürültüler görüntülerdeki detayların kaybolmasına ve görüntü işleme uygulamalarında verimin düşmesine sebep olmaktadırlar.

Gürültü saldırısında, saldırgan şifreli görüntü üzerinde faydalı bilgileri yok etmek amacıyla parazitler oluşturabilmektedir. Bu parazitlerin amacı hedeflenen kullanıcıya

görüntünün bozularak iletilmesi ve şifre çözme işleminden sonra orijinal görüntüyü kurtarılamaz hale getirmektir (Güvenoğlu ve Tunalı, 2023). Saldırgan, şifrelenmiş görüntülere tuz-biber gürültüsü, Gauss gürültüsü ve Poisson gürültüsü gibi yöntemler ile gürültü ekleyebilmektedir (Sivakumar ve Venkatesan, 2015). İyi bir şifreleme algoritmasının gürültü saldırılarına karşı dayanıklı olması gerekmektedir. İletilen görüntüye saldırgan tarafından gürültü eklense dahi şifre çözme işleminden sonra görüntünün gözle görülür bir şekilde kurtarılabilmesi gerekmektedir.

3.3.3.4 Çalışma süresi

Çalışma süresi, belirli bir görüntü şifreleme tekniğini yürütmek için gereken süre olarak ölçülmektedir. Derleme ve çalışma zamanının toplamıdır. Görüntü şifrelemenin etkili ve verimli olması için çalışma süresinin kısa olması gerekmektedir. Çalışma süresi, genellikle saniye, milisaniye veya dakika cinsinden ölçülmektedir (Abd El-Latif ve Niu, 2013).

3.3.3.5 Bit geçerlik oranı

Bit geçerlik oranı (BCR, Bit Correct Ratio), şifresi çözülmüş görüntü ile orijinal görüntü arasındaki farkı tahmin etmek amacıyla kullanılmaktadır. Şifresi çözülmüş görüntünün doğruluğunu kontrol etmektedir (Habek vd., 2022). Bit geçerlik oranı Denklem 86 ile hesaplanmaktadır.

$$BCR = (1 - \frac{\sum_{x,y}^{MxN} O(x,y) \oplus R(x,y)}{M\ x\ N}) \tag{86}$$

Burada, x ve y, $M\ x\ N$ boyutuna sahip görüntünün piksek koordinatlarını ifade etmektedir. O orijinal görüntüyü ve R ise şifresi çözülmüş görüntüyü temsil etmektedir. $\oplus$ ifadesi XOR işlemini göstermektedir. Bit geçerlik oranı [0, 1] aralığında olmalıdır. Bu geçerlik testi ile şifreli görüntünün iletimi sırasında herhangi bir saldırıya uğrayıp uğramadığı tespit edilebilmektedir.

3.3.3.6 Ortalama karesel hata

Ortalama karesel hata (MSE, Mean Squared Error), orijinal görüntü piksel değerlerinin şifrelenmiş görüntü piksel değerleri ile karşılaştırılmasını sağlamaktadır. Buradaki hata

değeri, orijinal görüntünün değerlerinin şifresi çözülen görüntüden farklı olma miktarıdır (M. U. Rehman, Shafique, Khalid, ve Hussain, 2021). MSE, Denklem 87 ile hesaplanmaktadır.

$$MSE = \frac{1}{MxN}\sum_{x=1}^{M}\sum_{y=1}^{N}[O(x,y) - R(x,y)]^2 \quad (87)$$

Burada *x* ve *y, M x N* piksel boyutundaki görüntülerin piksel koordinatlarıdır. *O* ve *R,* sırasıyla orijinal ve şifresi çözülmüş görüntülerdir. MSE değeri [0, ∞] aralığında olabilmektedir. Orijinal ile şifresi çözülen görüntü arasındaki MSE değeri minimum olmalıdır. Başka bir ifadeyle, etkili bir şifreleme algoritması için daha yüksek MSE değerlerinin gerekli olduğu anlamına gelmektedir.

3.3.3.7 Tepe sinyal gürültü oranı

Tepe sinyal gürültü oranı (PSNR, Peak Signal to Noise Ratio), orijinal ve şifresi çözülmüş görüntüler arasında bir kalite ölçümü olarak kullanılmaktadır. Başka bir ifadeyle, orijinal ve şifresi çözülmüş görüntüler arasındaki bozulmayı ölçmek için kullanılan metriklerden biridir (Yasser, Khalil, Mohamed, Samra, ve Khalifa, 2021). PSNR matematiksel olarak Denklem 88 ile hesaplanmaktadır.

$$PSNR = 10\log_{10}\frac{(2^n - 1)^2}{MSE} \quad (88)$$

Burada *n*, piksel başına düşen bit sayısını temsil etmektedir. PSNR, desibel (dB) cinsinden ölçülmektedir. PSNR [0, ∞] aralığında olabilmektedir. İyi bir şifreleme algoritmasında PSNR değeri, orijinal ve şifresi çözülmüş görüntüler arasında minimum olmalıdır.

3.3.3.8 Sinyal bozulma oranı

Sinyal bozulma oranı (SDR, Signal to Distortion Ratio), orijinal ve şifresi çözülmüş görüntülerin piksel değerleri arasındaki bozulma oranını ölçmek için kullanılmaktadır (K. N. Singh ve Singh, 2022). Denklem 89'da SDR ifadesi verilmektedir.

$$SDR = 10\log_{10}\frac{\sum_{x,y} O(x,y)^2}{\sum_{x,y}(O(x,y) - D(x,y))^2} \quad (89)$$

Burada *O(x, y)* ve *D(x, y)* sırasıyla orijinal ve şifresi çözülmüş görüntüleri temsil etmektedir. *x* ve *y*, *M x N* boyutundaki görüntülerin piksel koordinatlarıdır. SDR ölçü birimi desibel (dB)'dir. SDR değeri [0, ∞] aralığındadır. İyi bir şifreleme algoritmasında orijinal ve şifresi çözülmüş görüntüler arasındaki SDR değeri minimum olmalıdır.

3.3.3.9 Yapısal benzerlik indeksi

Yapısal benzerlik indeksi (SSIM, Structural Similarity Index), orijinal ve şifresi çözülmüş görüntüler arasındaki benzerliği ortaya çıkarmak için kullanılmaktadır. Şifresi çözülen görüntünün kalitesinin ortaya koymak için kullanılan bir parametredir. Benzerlik indeksi hesaplanmak istenen görüntülerin aynı ölçülerde olması gerekmektedir (K. Kumar, Roy, Rawat, ve Mishra, 2022). SSIM değeri Denklem 90 ile hesaplanmaktadır.

$$SSIM = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \quad (90)$$

Burada *x* orijinal görüntüyü ve *y* işlenmiş görüntüyü μ_x ve μ_y, *x* ve *y*'nin ortalamalarını, σ_x^2 ve σ_y^2, *x* ve *y*'nin varyanslarını, σ_{xy}, *x* ve *y*'nin kovaryanslarını, C_1 ve C_2, görüntüleri dengelemek için kullanılan değişkenleri temsil etmektedir. SSIM değerleri [-1, 1] aralığındadır. SSIM değerinin 1'e yakın ya da eşit olması orijinal ve deşifrelenmiş görüntülerin yapısal olarak birbirlerine çok benzediğini göstermektedir. Buna karşılık SSIM değerinin 0'a yakın veya eşit olması yapısal olarak bir benzerliğin olmadığı anlamına gelmektedir (Güvenoğlu, 2016).

3.3.3.10 Kök ortalama karekök hata

Kök ortalama karekök hata (RMSE, Root Mean Squared Error), MSE'nin karekökünün alınması ile elde edilmektedir. RMSE, deşifreli görüntü ile orijinal görüntü pikselleri arasındaki hatanın büyüklüğünü ölçmek için kullanılan hata ölçüm metriklerinden biridir (Anusree ve Rahiman, 2022). RMSE, Denklem 91 ile ifade edilmektedir (T. Shah, Qureshi, ve Usman, 2021).

$$RMSE = \sqrt{\frac{\sum_{x=1}^{M}\sum_{y=1}^{N}[O(x,y)-D(x,y)]^2}{MxN}} \quad (91)$$

Burada *x* ve *y*, *M x N* boyutundaki görüntülerin piksel koordinatlarıdır. *O* ve *D*, sırasıyla orijinal ve şifresi çözülmüş görüntülerdir. RMSE değerleri [0, ∞] aralığındadır. RMSE değerinin sıfıra yakın veya eşit olması öne sürülen görüntü şifreleme yönteminin iyi bir performansa sahip olduğunu göstermektedir.

3.3.3.11 Ortalama mutlak hata

Ortalama mutlak hata (MAE, Mean Absolute Error), şifrelenmiş ve orijinal görüntüler arasındaki farkı ölçmek için kullanılmaktadır. MAE, Denklem 92 ile elde edilmektedir.

$$MAE = \frac{1}{M\ xN}\sum_{x=1}^{M}\sum_{y=1}^{N}|O(x,y) - E(x,y)| \quad (92)$$

Burada *O(x, y)* ve *E(x, y)* sırasıyla orijinal ve şifreli görüntüleri temsil etmektedir. *x* ve *y*, *MxN* boyutunda görüntünün piksel koordinatlarını göstermektedir. MAE aralığı [0, $2^n - 1$]. Bu ifadede *n* değeri piksel başına bit sayısıdır. MAE değeri öne sürülen bir şifreleme algoritmasında orijinal ve şifreli görüntüler arasında yüksek bir değere sahip olmalıdır. Başka bir ifadeyle MAE ne kadar büyükse, önerilen şifreleme sisteminin güvenilirliği de o kadar yüksek olmaktadır (Nazir, Bajwa, Abdullah, Kazmi, ve Samiullah, 2022).

3.3.3.12 Sinyal gürültü oranı

Sinyal gürültü oranı (SNR, Signal to Noise Ratio), bir şifreleme algoritmasının sonuçlarının nicel bir şekilde değerlendirilmesi için kullanılan metriklerden biridir (B. Wang ve Sun, 2001). SNR, Denklem 93 ile hesaplanmaktadır.

$$SNR = \frac{\sum_{m,n}[O(m,n)]^2}{\sum_{m,n}[O(m,n)-D(m,n)]^2} \quad (93)$$

Burada *O(m, n)* ve *D(m, n)*, orijinal ve deşifrelenmiş görüntüyü, *m* ve *n* ise görüntülere ait piksel koordinatlarını temsil etmektedir. SNR değerleri [1, ∞] aralığındadır. SNR değeri, orijinal ile şifresi çözülmüş görüntü arasında maksimum olmalıdır. Yani SNR

değeri ne kadar yüksek ise önerilen görüntü şifreleme algoritması da o kadar güçlü demektir.

3.3.4 NIST rastgelelik analizi

NIST (Ulusal Standartlar ve Teknoloji Enstitüsü, National Institute of Standards and Technology) testi kaotik sistemler tarafından üretilen rastgele sayıların rastgelelik durumlarını test etmek için ortaya atılmıştır. Bir başka ifade ile rastgele sayı üreteçlerinden elde edilen rastgele sayıların bit dizilerinin rastgelelik durumlarını ölçmek ve değerlendirmek için kullanılmaktadır (Avaroğlu, 2014). NIST testi 15 adet istatistiksel değerlendirme içermektedir. Bu testler Tablo 2'de sırasıyla verilmiştir (Abas ve Arulmurugan, 2022).

Tablo 2. NIST test araçları

No	Test Adı	Türkçesi
1	Frequency (Monobits) Test	Frekans (Monobitler) Testi
2	Frequency Test within a Block	Bir Blok İçinde Frekans Testi
3	Runs Test	Çalıştırma Testi
4	Test for the Longest Run of Ones in a Block	Bir Bloktaki En Uzun Süreli Koşu Testi
5	Binary Matrix Rank Test	İkili Matris Sıra Testi
6	Discrete Fourier Transform Test	Ayrık Fourier Dönüşümü (Spekral) Testi
7	Non-Overlapping Template Matching Test	Örtüşmeyen Şablon Eşleştirme Testi
8	Overlapping Template Matching Test	Örtüşen Şablon Eşleştirme Testi
9	Maurer's "Universal Statistical" Test	Maurer'in "Evrensel İstatistik" Testi
10	Linear Complexity Test	Doğrusal Karmaşıklık Testi
11	Serial Test	Seri Test
12	Approximate Entropy Test	Yaklaşık Entropi Testi
13	Cumulative Sums Test	Kümülatif Toplamlar Testi
14	Random Excursions Test	Rastgele Gezinti Testi
15	Random Excursions Variant Test	Rastgele Gezinti Varyant Testi

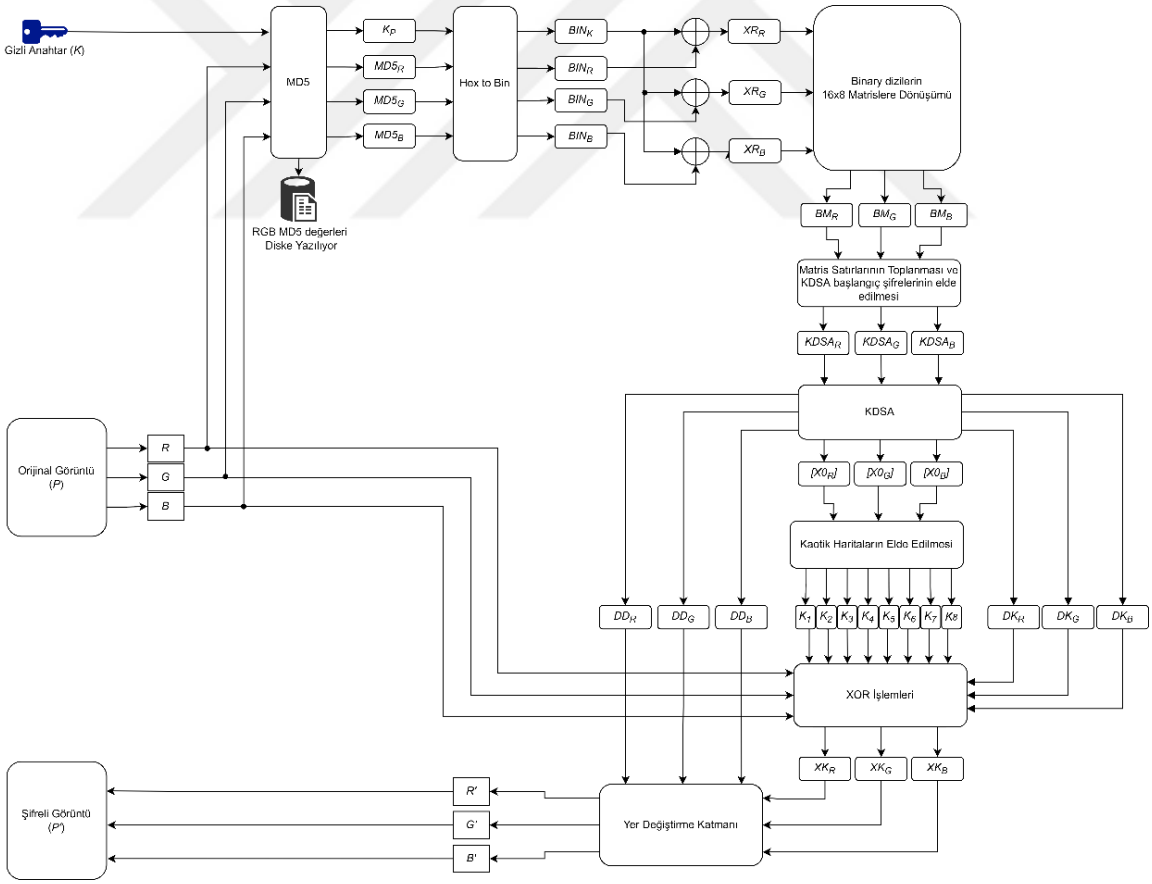
Her test, belirli bir anlamlılık düzeyine sahiptir. Testler sonucunda olarak *P* değeri üretilmektedir. Burada $P = 0.01$ ayarlanmaktadır. *P* değerinin 0.01 olarak seçilmesi test edilen sayıların rastgelelik durumunun %99 güvenilirlikte olduğunu işaret etmektedir. *P* değerinin 1'e eşit olması durumunda ise rastgeleliğin mükemmel olduğu anlamına gelmektedir (S. A. Tuncer ve Yeliz, 2019). Başka bir ifadeyle *P* değerinin 0.01'den büyük olması sistemin rastgele olduğunu göstermektedir (Güvenoğlu ve Tunalı, 2023). Kaotik bir sistemin iyi olarak kabul edilebilmesi için 16 testin tümü geçmesi gerekmektedir.

4. ÖNERİLEN HİBRİT GÖRÜNTÜ ŞİFRELEME YÖNTEMİ

Bu bölümde kaotik haritalar yardımıyla görüntülerin şifrelenmesini sağlayan hibrit bir görüntü şifreleme yöntemi önerilmiştir. Önerilen şifreleme yönteminin tüm detayları ayrıntılı olarak anlatılmış ve güvenlik testleri gerçekleştirilmiştir.

4.1 Önerilen görüntü şifreleme algoritması

Görüntülerin şifrelenmesi amacıyla önerilen yöntemde literatürde az kullanım imkânı bulan sekiz adet kaotik harita seçilmiştir. Bu kaotik haritalar Kübik, Sinüs, Tent, Cusp, May, Aizawa, Bernoulli ve Gompertz kaotik haritalarıdır. Önerilen yöntemin blok diyagramı Şekil 49'da verilmiştir.



Şekil 49. Önerilen yöntemin blok diyagramı

Önerilen görüntü şifreleme yöntemi dokuz adımdan oluşmaktadır. Bu adımların detayları aşağıda verilmiştir.

Adım 1: Önerilen yöntem renkli ve gri seviye görüntülerin şifrelenmesini sağlamaktadır. İlk adımda şifrelenecek görüntü R (Red, Kırmızı), G (Green, Yeşil) ve B (Blue, Mavi) renk kanallarına ayrılmaktadır.

Adım 2: RGB renk kanallarından ve kullanıcı tarafından belirlenen gizli anahtardan MD5 (Message Digest 5) anahtarlama algoritması kullanılarak 128 bitlik birer anahtar değeri (Hash) elde edilmektedir. MD5, bir mesaj veya dosyanın kendine özgü bir parmak izinin elde edilmesini sağlamaktadır. Bu adımda gizli anahtardan elde edilen MD5 değeri K_P ve RGB kanallarından elde edilen MD5 değerleri $MD5_R$, $MD5_G$ ve $MD5_B$ olarak temsil edilmektedir. Bu değerlerden gizli anahtara ait K_P hariç $MD5_R$, $MD5_G$ ve $MD5_B$ değerleri bir dosyada tutulmaktadır. Bu değerlerin herkese açık olmasında herhangi bir sakınca bulunmamaktadır. Şifreli görüntünün çözülebilmesi için bu değerler tek başına yeterli olmamaktadır.

Adım 3: Bir önceki adımda üretilen MD5 değerleri BIN_K, BIN_R, BIN_G ve BIN_B ikili sayı değerlerine dönüştürülmektedir.

Adım 4: Kullanıcının gizli anahtarından elde edilen BIN_K ikili sayı dizisi sırası ile RGB kanallarından elde edilen BIN_R, BIN_G ve BIN_B ikili sayı dizileri ile XOR işlemine tabi tutulmaktadır. Bu anahtar güvenliğinin arttırılması için yapılan bir işlemdir. Bu adıma ait denklemler Denklem 94, Denklem 95 ve Denklem 96 ile elde edilmektedir.

$$XOR_R = BIN_K \oplus BIN_R \tag{94}$$

$$XOR_G = BIN_K \oplus BIN_G \tag{95}$$

$$XOR_B = BIN_K \oplus BIN_B \tag{96}$$

Adım 5: Bir önceki adımdan elde edilen her bir 128 bitlik ikili sayı dizisi 16 x 8 boyutlarında BM_R, BM_G ve BM_B matrislerine dönüştürülmektedir. Bit değerleri sırasıyla 8'er bit okunarak 16 satır ve 8 sütundan oluşan matrisler haline getirilmektedir. Örnek bir matris dönüşümü Şekil 50'de gösterilmektedir.

Bit Dizisi

00111101011101010011001011010011
11011000111001110100101010101001
10100000000011101001111010001110
10000111011000010111010011011110

	1	2	3	4	5	6	7	8
1	0	0	1	1	1	1	0	1
2	0	1	1	1	0	1	0	1
3	0	0	1	1	0	0	1	0
4	1	1	0	1	0	0	1	1
5	1	1	0	1	1	0	0	0
6	1	1	1	0	0	1	1	1
7	0	1	0	0	1	0	1	0
8	1	0	1	0	1	0	0	1
9	1	0	1	0	0	0	0	0
10	0	0	0	0	1	1	1	0
11	1	0	0	1	1	1	1	0
12	1	0	0	0	1	1	1	0
13	1	0	0	0	0	1	1	1
14	0	1	1	0	0	0	0	1
15	0	1	1	1	0	1	0	0
16	1	1	0	1	1	1	1	0

Şekil 50. Bit dizisinin matrise dönüşümü örneği

Adım 6: RGB kanallarına ait BM_R, BM_G ve BM_B matrislerinin her bir satırın tamsayı değerleri elde edilerek toplanmakta ve her kanal için $KDSA_R$, $KDSA_G$ ve $KDSA_B$ değerleri elde edilmektedir. Bu değerler 1-16 arasındaki sayıların karıştırılması için Knutt-Dustenfeld Karıştırma Algoritmasının (KDSA, Knutt-Dustenfeld Shuffle Algorithm) başlangıç değerleri olarak kullanılmaktadır (Güvenoğlu ve Esin, 2009). KDSA, 1..N arasındaki tamsayıların konumlarının değiştirilmesi için yaygın kullanılan bir algoritmadır. KDSA'dan elde edilen karışık tamsayı dizisi yardımıyla Şekil 50'de verilen satır çiftleri XOR işlemine tabi tutulmaktadır. Örnek bir KDSA dizisi Şekil 51'de verilmiştir.

İndis	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Satır	8	10	9	5	13	15	2	11	1	12	7	3	6	16	14	4

Şekil 51. Örnek KDSA dizisi

Burada dizi değerleri sırasıyla okunmaktadır. Okunan bu değerler matrisin satır numarasını temsil etmektedir. Örneğin 1. indisteki 8 değeri ve 2. indisteki 10 değeri matrisin 8 ve 10. satırlarının XOR işlemine tutulacağını göstermektedir. Benzer biçimde 3 ve 4 numaralı indisler, 5 ve 6 numaralı indisler şeklinde devam ederek sırasıyla XOR işlemi uygulanmaktadır.

Adım 7: Önceki adımın ardından her kanal için 8 satırdan oluşan matrisler elde edilmektedir. Bu matrislerin her satırındaki 8 bitlik diziler tamsayılara dönüştürülmekte $[X0_R]$, $[X0_G]$ ve $[X0_B]$ dizileri elde edilmektedir. Bu dizilerdeki tamsayı değerleri 1000'e bölünerek yöntemde kullanılan kaotik haritaların başlangıç değerlerinin [0, 1] aralığında olması sağlanmaktadır. Bu başlangıç değerleri Tablo 3'de bir örneği verilen biçimde sırasıyla kaotik haritaların başlangıç değerleri olarak atanmaktadır.

Tablo 3. Kaotik harita başlangıç değerlerinin elde edilmesi örneği

	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**Tamsayı**	**Başlangıç Değeri**	**Kaotik Harita**	**Simge**
1	0	1	1	1	1	0	1	1	123	0.123	Cubic Map	K_1
2	1	0	0	0	0	0	1	1	131	0.131	Sine Map	K_2
3	1	1	1	1	0	0	0	1	241	0.241	Tent Map	K_3
4	1	1	1	1	0	1	1	0	246	0.246	Cusp Map	K_4
5	0	1	0	1	0	1	0	1	85	0.085	May Map	K_5
6	1	0	0	0	0	0	1	0	130	0.130	Aizawa Map	K_6
7	0	1	1	1	1	1	1	1	127	0.127	Bernoulli Map	K_7
8	0	0	0	1	0	0	1	1	19	0.019	Gompertz Map	K_8

Kaotik haritaların başlangıç değerleri ve denklem parametreleri yardımıyla K_1, K_2, K_3, K_4, K_5, K_6, K_7 ve K_8 kaotik haritaları elde edilmektedir. Denklem parametreleri her kaotik harita için literatürde kaotik olduğu noktalardaki değerler alınmıştır. KDSA yardımıyla ayrıca hangi kaotik haritanın hangi sırada uygulanacağını belirlemek amacı ile 1…8 arasında DK_R, DK_G ve DK_B karışık dizileri elde edilmektedir. Bununla birlikte şifrelemenin son adımında piksellerin yer değiştirilmesini ve daha da karmaşık hale getirilebilmesi için KDSA yardımıyla 1…M × N arasında karıştırılmış DD_R, DD_G ve DD_B dizileri elde edilmektedir.

Adım 8: Kaotik haritalar yardımıyla RGB katmanları ayrı ayrı XOR işlemine tabi tutulmaktadır. XOR işlemi sırasıyla yapılmamakta Adım 6'da kullanılan KDSA ile 1..8 arasında karışık bir dizi elde edilerek gerçekleştirilmektedir. KDSA dizilerinin

oluşturulması için $KDSA_R$, $KDSA_G$ ve $KDSA_B$ başlangıç anahtar değerleri ile elde edilmektedir. Elde edilen dizi değerleri kullanılarak her bir kaotik harita RGB kanalları XOR işlemine tabi tutularak XK_R, XK_G ve XK_B matrisleri elde edilmektedir.

Adım 9: Bu adımda bir önce adımda elde edilen XK_R, XK_G ve XK_B matris değerlerinin konumları Adım 7'de elde edilen DD_R, DD_G ve DD_B dizileri yardımıyla yer değiştirme işlemine tabi tutularak şifreli görüntü katmanları *R', G'* ve *B'* elde edilmektedir. Bu katmanlar birleştirilerek şifreli renkli görüntü oluşturulmaktadır.

4.2 Önerilen algoritmanın deşifreleme işlemi

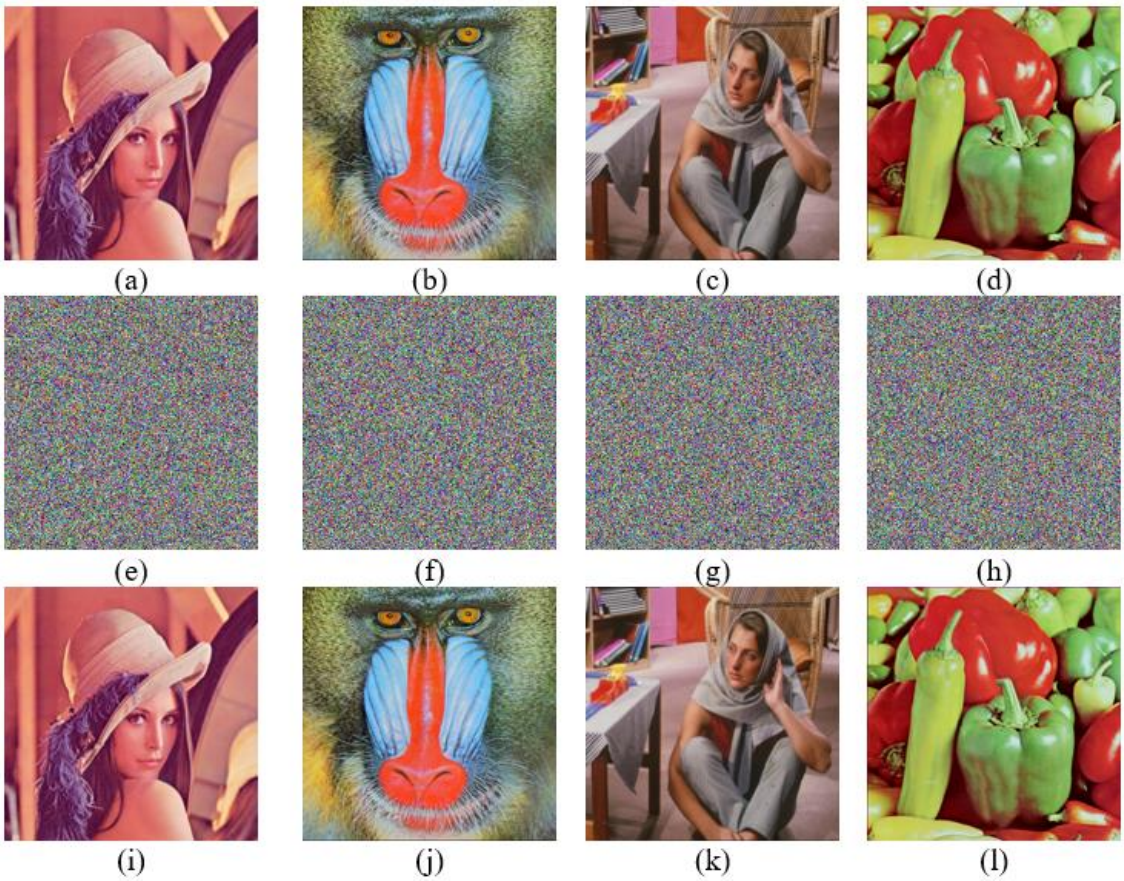
Şifreli görüntünün çözülebilmesi için ilk yedi adımdan sonra Adım 8'deki işlemlerin tersten uygulanması gerekmektedir. Orijinal görüntünün elde edilebilmesi ancak gizli anahtarın elde edilebilmesi ile mümkündür. Benzer biçimde kaotik haritaların başlangıç değerlerinin belirlenebilmesi ve beraberinde orijinal görüntü katmanlarına hangi sırada hangi haritanın XOR işlemine tutulduğunun tespit edilebilmesi içinde gizli anahtara ihtiyaç duyulmaktadır.

4.3 Deneysel sonuçlar ve güvenlik analizleri

Bu bölümde önceki kısımlarda önerilen görüntü şifreleme algoritmasının güvenlik analizi sonuçlarına yer verilmiştir. Yöntemin geçerliliği yapılan testler ile kanıtlanmıştır.

4.3.1 Şifreleme ve deşifreleme sonuçları

Önerilen yöntem, literatürde görüntülerin şifrelenmesi amacıyla sıklıkla kullanılan 256 x 256 boyutlarında "Lena", "Pepper", "Baboon" ve "Barbara" görüntüleri üzerinde denenmiştir. Ayrıca yöntem Intel Core i7-4700 CPU 2.4 GHz 4 çekirdek, 16 GB RAM ve MS Windows 10 Pro 64 bit işletim sistemi üzerinde test edilmiştir. Algoritmanın geliştirilmesinde MATLAB 2020b sürümü kullanılmıştır. Şifreleme yönteminde gizli anahtar olarak "maltepe@" anahtarı kullanılmış, şifreleme ve deşifreleme işlemi sonucunda elde edilen sonuç görüntüleri Şekil 52'de gösterilmiştir. Farklı anahtarlar ile farklı sonuçlar da elde edilebilmektedir.



Şekil 52. Şifrelenmiş ve deşifrelenmiş görüntüler. (a) ~ (d) Orijinal görüntüler, (e) ~ (h) Şifreli görüntüler, (i) ~ (l) Deşifrelenmiş görüntüler

Şifrelenmiş ve deşifrelenmiş görüntüler dikkate alındığında gözle görünür herhangi bir piksel kaybının olmadığı görülmektedir.

4.3.2 Algoritmanın karmaşıklık analizi

Önerilen yöntem dokuz adımdan oluşmaktadır. Bu nedenle her bir adımın karmaşıklık oranları birbirinden farklıdır. Yöntemin ilk adımında görüntü renk kanallarına ayrılmakta ve karmaşıklığa bir etkisi bulunmamaktadır. Bu nedenle dikkate alınmamıştır. İkinci adımda, MD5 anahtarlama algoritması kullanılarak gizli anahtarların elde edilmesinde kullanılmaktadır. Dolayısı ile toplam karmaşıklığa çok küçük ve eşit miktarda katkı sağladığından göz ardı edilmiştir. Benzer şekilde üçüncü, dördüncü, beşinci ve altıncı adımlar da anahtar üretim sürecinin bir parçasıdır ve toplam karmaşıklığı etkisi çok düşüktür. Yedinci adımda $M \times N$ büyüklüğünde kaotik haritalar her bir kanal için ayrı ayrı üretildiğinden her bir harita için karmaşıklık $3 \times M \times N$ olmaktadır. Bu adım için 8 farklı kaotik harita üretildiğinden $8 \times (3 \times M \times N)$ yani toplam karmaşıklık $24 \times M \times N$

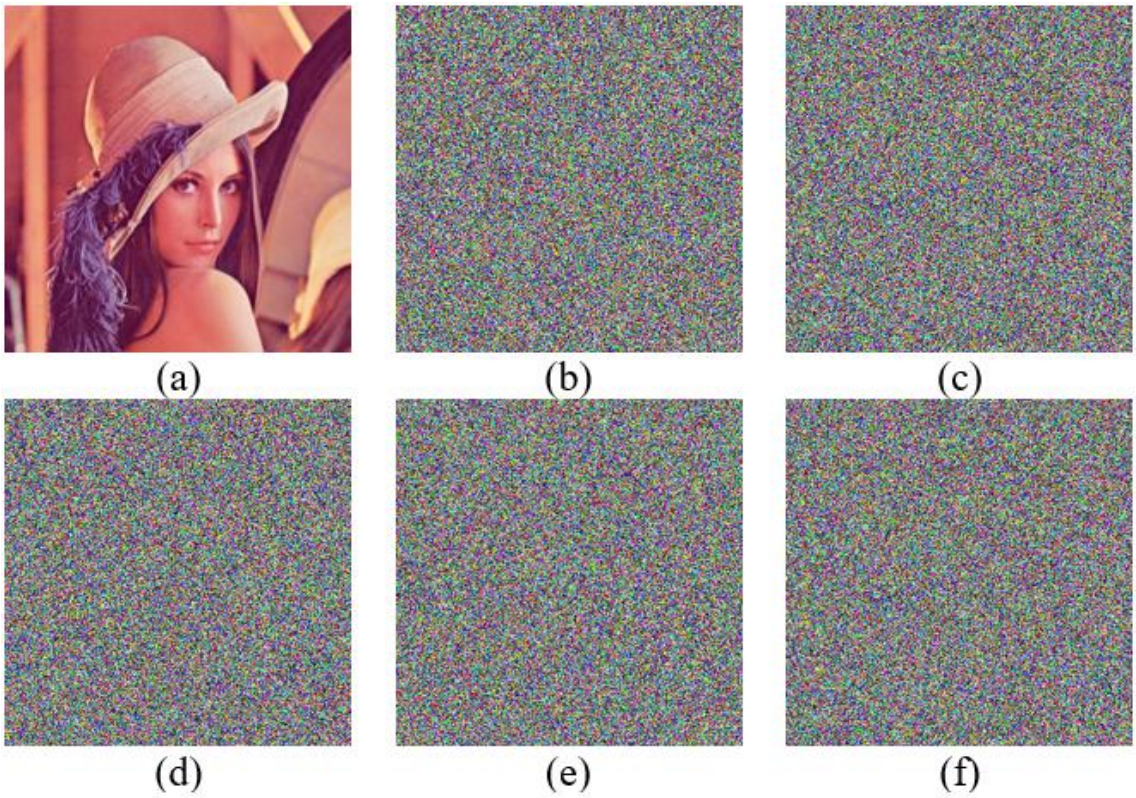
olmaktadır. Son adımda elde edilen pikseller her kanalda yer değiştirme işlemine tabi tutulmakta ve karmaşıklığı $3 \times M \times N$ olmaktadır. Şifreleme sürecinin hesaplama karmaşıklıkları birleştirildiğinde önerilen yöntemin karmaşıklığının $27 \times M \times N$ olduğu görülmektedir. Buradan yöntemin karmaşıklığı basitçe $O(M \times N)$ ifade edilebilmektedir. Sonuç olarak, önerilen yöntem düz metin görüntülerdeki piksel sayısına göre doğrusal bir zaman karmaşıklığına sahiptir. Bununla birlikte verimliliğin önemli bir gereksinim olduğu gerçek dünya senaryolarında etkin bir şekilde uygulanabilecektir.

4.3.3 Anahtar uzayı analizi

Önerilen yöntemde MD5 anahtarlama algoritması kullanılmıştır. MD5 algoritması 128 bitlik bir yapıya sahiptir ve anahtar uzayı 2^{128} olmaktadır. Bununla birlikte yöntemin sonraki adımlarında alt anahtarlar da elde edilmekte ve anahtar uzayı çok daha büyük olmaktadır. Güçlü bir yöntemin anahtar uzayının 2^{100} den büyük olması beklenmektedir (Alvarez ve Li, 2006). Dolayısı ile önerilen yöntemin anahtar uzayı belirtilen değerden büyük ve oldukça güçlü olduğu söylenebilmektedir.

4.3.4 Anahtar hassasiyet analizi

Önerilen yöntemde 256 x 256 boyutlarında renkli “Lena” görüntüsü “maltepe@” anahtarı ile şifrelenmiştir. Ardından anahtar üzerinde çok küçük değişiklikler yapılarak görüntü deşifrelenmeye çalışılmıştır. Kullanılan anahtarlar “Maltepe&”, “maltePe&”, “mAltepe&”, “maltepe?” ve “ma3tepe&” biçiminde çok küçük değişikliklerden oluşmaktadır. Elde edilen sonuçlar Şekil 53’de gösterilmektedir.

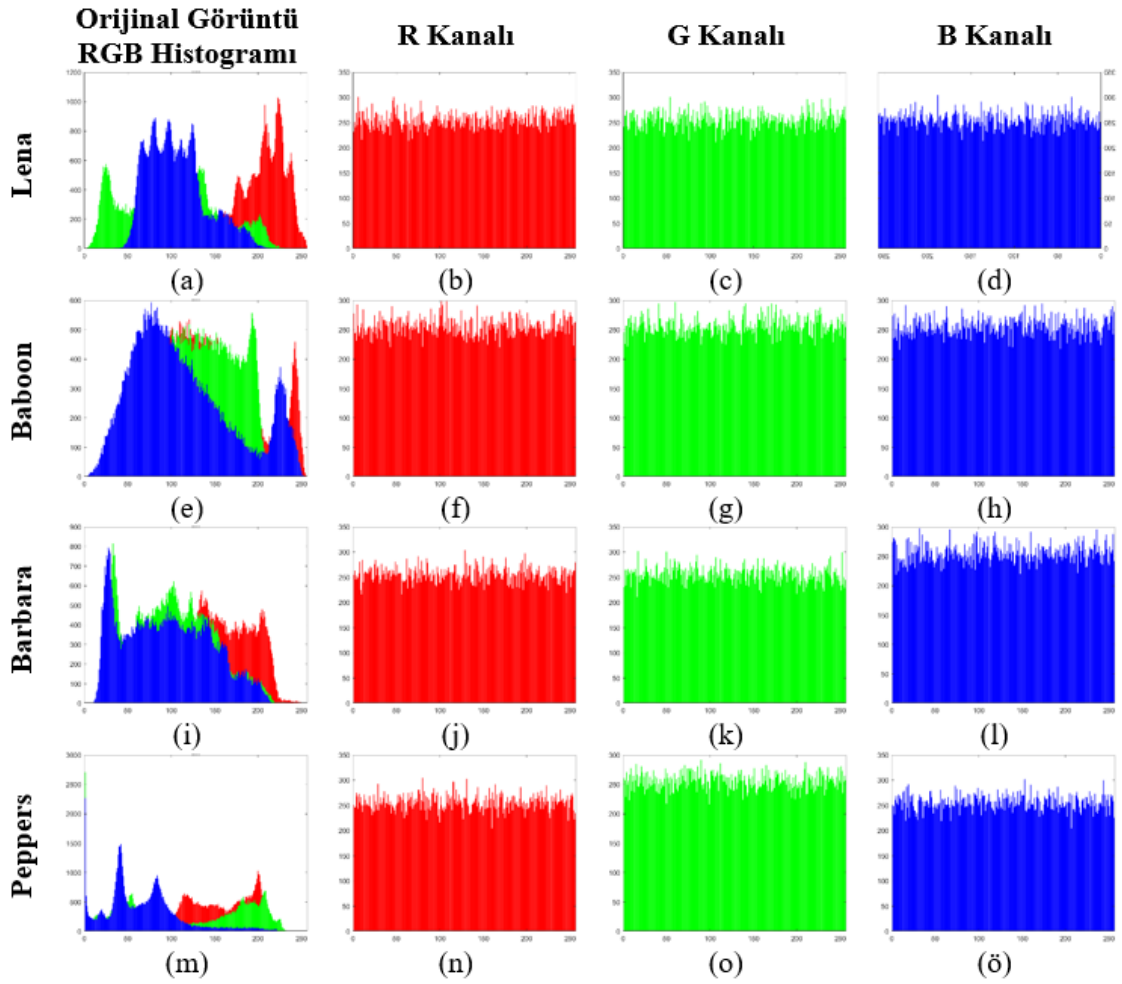


Şekil 53. Anahtar hassasiyeti analizi (a) doğru anahtar ile deşifrelenmiş görüntü (b)~(f) küçük farklı anahtarlar ile deşifrelenmiş görüntüler

Deneysel sonuçlar dikkate alındığında doğru görüntüye ulaşmanın tek yolunun ancak ve ancak doğru anahtar ile mümkün olduğu görülmektedir. Bu durum önerilen yöntemin anahtara karşı oldukça hassas olduğunu göstermektedir.

4.3.5 Histogram analizi

Histogramlar, görüntülere ait piksel dağılımını gösteren grafiklerdir. Şifreli görüntülerden orijinal görüntülerin elde edilebilmesi için frekans analizi yapılabilmektedir. Frekans analizi ile saldırganın orijinal görüntülere ulaşılabilmesinin engellenmesi gerekmektedir. Bu nedenle şifrelenmiş görüntülerde piksel dağılımının nispeten düz olması gerekmektedir. Düz bir yapıya sahip görüntülerde frekans analizi tekniği ile orijinal görüntüye ulaşabilmek oldukça güçtür. Şekil 54'de orijinal ve şifrelenmiş görüntülerin histogramları gösterilmektedir.



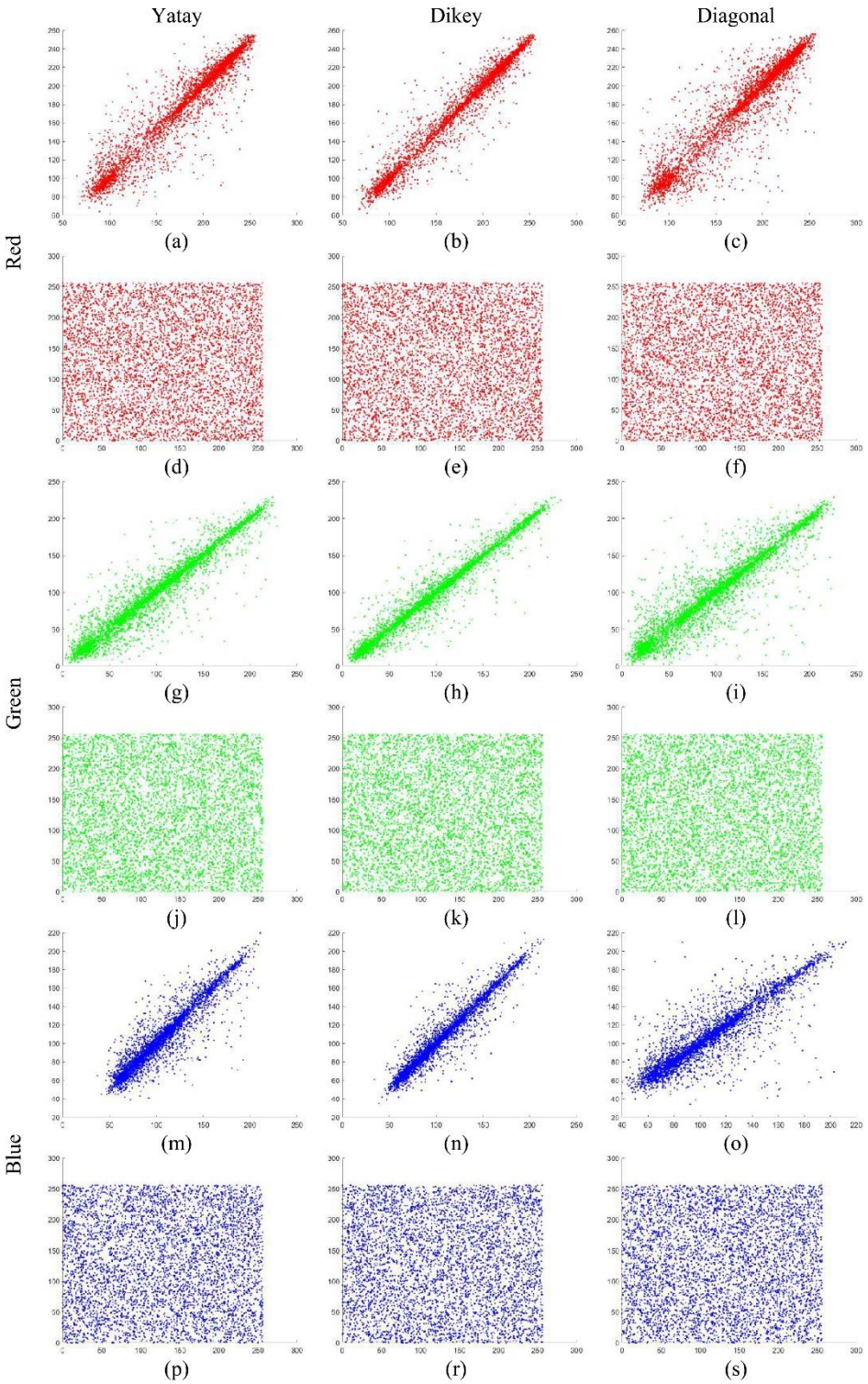
Şekil 54. Orijinal ve şifrelenmiş görüntü histogramları

Önerilen yöntemde şifrelenmiş görüntü histogramına dikkat edildiğinde düz bir dağılımın sağlandığı görülmektedir. Bu durum önerilen yöntemin frekans analizi saldırılarına karşı dayanıklı olduğu anlamına gelmektedir.

4.3.6 Komşu pikseller arasında korelasyon analizi

İki görüntü arasındaki ilişkinin belirlenmesinde korelasyon teknikleri kullanılmaktadır. Şifrelenmiş görüntülerde pikseller arasındaki korelasyonu yatay, dikey ve çapraz yöndeki komşu pikseller kullanılarak elde edilmektedir. Önerilen yöntemin korelasyon testi işlemi orijinal ve şifreli görüntüler arasında yapılmıştır. Üç farklı yönde rastgele 5000 adet piksel kullanılmıştır. Yöntemin korelasyon analizi ve performansını değerlendirmek amacıyla renkli "Lena" seçilmiştir. İlgili testler farklı görüntüler üzerinde de

gerçekleştirilmiştir. Şekil 55'de renkli "Lena" görüntüsünde farklı yönlerde gerçekleştirilmiş korelasyon analizi sonuçları gösterilmiştir.



Şekil 55. Renkli Lena görüntüsü üzerinde gerçekleştirilen korelasyon testi sonuçları

Renkli “Lena” ve çalışmada kullanılan diğer görüntülerin korelasyon testi sonuçlarından elde edilen korelasyon değerleri Tablo 4’de verilmiştir.

Tablo 4. Önerilen yöntemin korelasyon testi sonuçları

	Yatay			Dikey			Diagonal		
Resim	**R**	**G**	**B**	**R**	**G**	**B**	**R**	**G**	**B**
Lena Orijinal	0.9578	0.9554	0.9303	0.9799	0.9792	0.9621	0.9361	0.9349	0.9001
Lena Şifreli	0.0009	0.0002	-0.0049	0.0020	0.0133	-0.0004	0.0041	-0.0014	-0.0009
Barbara Orijinal	0.9526	0.9444	0.9526	0.9611	0.9542	0.9623	0.9182	0.9029	0.9182
Barbara Şifreli	-0.0040	-0.0011	0.0048	-0.0038	0.0026	-0.0002	0.0001	-0.0076	-0.0014
Baboon Orijinal	0.9474	0.8727	0.9215	0.9207	0.8380	0.9138	0.9033	0.7924	0.8762
Baboon Şifreli	0.0057	0.0033	0.0029	0.0011	-0.0014	0.0029	0.0020	-0.0016	0.0034
Peppers Orijinal	0.9645	0.9698	0.9645	0.9679	0.9750	0.9679	0.9369	0.9465	0.9369
Peppers Şifreli	0.0018	0.0017	0.0018	-0.0057	0.0004	-0.0057	-0.0021	-0.0032	-0.0021

Saldırılara karşı dayanıklı bir yöntemde piksellerin dağılımının her yönde olması ve korelasyon değerinin sıfıra çok yakın olması gerekmektedir. Şekil 55 ve Tablo 4’e dikkat edildiğinde piksel dağılımının her yönde ve korelasyon değerlerinin sıfıra çok olduğu görülmektedir. Bu değerler dikkate alındığında önerilen yöntemin güçlü olduğu söylenebilmektedir.

4.3.7 Entropi analizi

Bir sistemdeki rastgelelik ve düzensizlik entropi olarak tanımlanmaktadır. Bir sistemde ideal entropi değeri 8’dir. Şifreli bir görüntüde entropi değerinin 8’e eşit ya da çok yakın olması pikseller arasında düzensizliğin çok fazla olduğu anlamına gelmektedir. Tablo 5’de çalışmada kullanılan görüntülerin entropi testi sonuçları verilmiştir.

Tablo 5. Önerilen yöntemin entropi testi sonuçları

	Orijinal Görüntü			Şifreli Görüntü		
Görüntü	**R**	**G**	**B**	**R**	**G**	**B**
Lena	7.2432	7.5638	6.9558	7.9971	7.9969	7.9972
Barbara	7.5518	7.3756	7.4773	7.9973	7.9970	7.9973
Baboon	7.6058	7.3581	7.6665	7.9974	7.9975	7.9973
Peppers	7.3009	7.5570	7.0929	7.9972	7.9977	7.9973

Entropi testinden elde edilen sonuçlara dikkat edildiğinde şifreli görüntülerin entropi değerlerinin 8'e çok yakın olduğu görülmektedir. Bu durum pikseller arasındaki düzensizliğin fazla ve saldırılara karşı dayanıklı olduğu anlamına gelmektedir.

4.3.8 Yapısal benzerlik testi analizi

Yapısal benzerlik testi iki görüntü arasındaki benzerliği ölçülmek amacıyla kullanılan yöntemlerden biridir. Bu test aynı zamanda iki görüntü arasındaki kalite farkının tespit edilmesi amacıyla da kullanılmaktadır (Güvenoğlu, 2016). Tablo 6'da çalışmada kullanılan orijinal ve şifreli görüntüler arasındaki yapısal benzerlik testi sonuçları verilmiştir.

Tablo 6. Yapısal benzerlik testi sonuçları

Görüntü	Orijinal ve Şifreli Görüntü Arasındaki Benzerlik Oranı (%)
Lena	0.0114
Barbara	0.0093
Baboon	0.0086
Peppers	0.0079

Yapısal benzerlik testi sonuçlarına göre şifreli ve orijinal görüntüler arasında benzerliğin çok düşüktür. Bu nedenle önerilen yöntemin oldukça güvenilir olduğu sonucu ortaya çıkmaktadır.

4.3.9 NPCR ve UACI analizi

NPCR ve UACI diferansiyel analiz teknikleridir. İdeal NPCR değerinin %99.61'e ve UACI değerinin %33.46'ya yakın olması beklenmektedir. Tablo 7'de önerilen yöntemin orijinal ve şifreli görüntüler arasındaki NPCR ve UACI testi sonuçları verilmiştir.

Tablo 7. NPCR ve UACI testi sonuçları

	NPCR (%)			UACI (%)		
Görüntü	R	G	B	R	G	B
Lena	99.61	99.62	99.62	33.38	33.29	33.35
Barbara	99.60	99.66	99.61	33.45	33.09	33.34
Baboon	99.62	99.62	99.60	33.35	33.02	33.69
Peppers	99.60	99.64	99.58	33.36	33.27	33.29

NPCR ve UACI testleri renkli görüntüler üzerinde ve her bir RGB kanalında ayrı ayrı gerçekleştirilmiştir. Elde edilen sonuçlar dikkate alındığında ideal UACI ve NPCR değerlerine çok yakın olduğu görülmektedir. Bu durum önerilen yöntemin diferansiyel saldırılara karşı dayanıklı olduğunu göstermektedir.

4.3.10 Dayanıklılık analizi

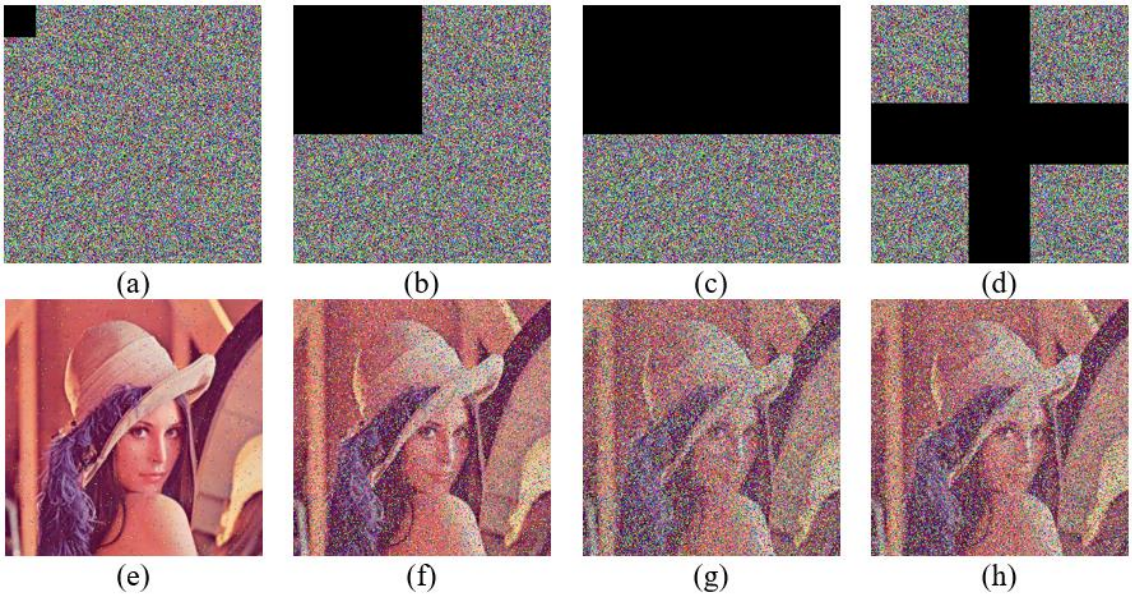
Görüntülerin iletimi sırasında istenmeyen üçüncü kişiler tarafından görüntüler tahribata uğratılabilmektedirler. Başka bir ifade ile görüntülerin belirli bir bölümü saldırgan tarafından ortadan kaldırılabilmektedir. Bu işlem genellikle görüntüye gürültü ekleme veya görüntünün belli bir bölümünün ortadan kaldırılması şeklindedir. Yöntemin dayanıklılığın test edilmesi için ilk olarak şifreli görüntülere belirli oranlarda gürültü eklemiş ve doğru şifre ile çözülmeye çalışılmıştır. Şifreli görüntülere gürültü eklemek için literatürde bilinen ve çok sık kullanılan Tuz ve Biber Gürültüsü ve Gauss Gürültüsü ekleme yöntemleri kullanılmıştır. Gürültünün eklenmesinden sonra elde edilen deşifrelenmiş görüntü sonuçları Şekil 56'da gösterilmektedir.



Şekil 56. Gürültü saldırısı testi sonuçları (a) Tuz ve Biber gürültüsü değişiklik oranı 0.01 (b) Tuz ve Biber gürültüsü değişiklik oranı 0.05, (c) Gauss gürültüsü değişiklik oranı 0.01, (d) Gauss gürültüsü değişiklik oranı 0.1

Gürültü eklenmiş görüntülerin doğru anahtar ile deşifrelenmesinden sonra elde edilen sonuçlar dikkate alındığında, veri iletiminde şifreli görüntünün saldırıya uğramış olmasına rağmen çok ciddi kayıpların olmadığı görülmektedir.

Bir diğer dayanıklılık testi ise şifreli görüntünün bazı bölümlerinin yok edilmesi ve ardından doğru anahtar ile deşifrelenmeye çalışılması biçiminde yapılmıştır. Şifreli görüntü üzerinde saldırgan tarafından görüntünün bazı bölümlerinin yok edildiği bir yapı düşünülmüştür. Ardından doğru anahtar ile deşifreleme işlemi yapılmıştır. Elde edilen sonuçlar Şekil 57'de gösterilmektedir.



Şekil 57. Dayanıklılık saldırısı testi sonuçları

Elde edilen sonuçlara dikkat edildiğinde tahribata uğrayan bölgeler bulunmasına rağmen doğru anahtar ile şifreli görüntülerin doğru bir şekilde deşifrelendiği görülmektedir. Bu durum, görüntülerin iletilmesi esnasında saldırgan tarafından şifreli görüntüler tahrip edilse dahi görüntü içerisindeki verilere sadece doğru anahtar ile ulaşılabileceğini göstermektedir. Görüntülere dikkat edildiğinde görüntü verisinin gözle algılanabildiği ve yöntemin saldırılara karşı oldukça dayanıklı olduğu sonucu ortaya çıkmaktadır.

4.3.11 MSE ve PSNR testi

Yöntemin dayanıklılığının test edilebilmesi için MSE ve PSNR testleri de yapılmıştır. İyi bir şifreleme yönteminde orijinal ve şifresi çözülmüş görüntüler arasında MSE değerinin yüksek ve PSNR değerinin ise düşük olması beklenmektedir. Tablo 8'de gürültülü görüntülerin deşifrelenmesi ile elde edilen sonuç görüntüsü ve orijinal görüntü arasında elde edilen MSE ve PSNR değerleri verilmiştir.

Tablo 8. Orijinal ve deşifrelenmiş görüntüler arasındaki MSE ve PSNR değerleri

	MSE			**PSNR**		
Gürültü	**R**	**G**	**B**	**R**	**G**	**B**
Tuz ve Biber (0.01)	9.8459	9.4457	8.3374	28.2657	28.6261	29.7102
Tuz ve Biber (0.05)	22.8096	21.3508	18.9488	20.9684	21.5425	22.5792
Gaussian (0.01)	51.6146	47.7090	41.0847	13.8753	14.5588	15.8572
Gaussian (0.1)	77.4804	71.8110	65.2467	10.3470	11.0070	11.8396

Benzer bir test tahribata uğratılmış görüntüler ve orijinal görüntüler arasında gerçekleştirilmiştir. Elde edilen sonuçlar Tablo 9'da verilmiştir.

Tablo 9. Orijinal ve tahribata uğratılmış deşifreli görüntüler arasındaki MSE ve PSNR değerleri

	MSE			PSNR		
Maske	**R**	**G**	**B**	**R**	**G**	**B**
Maske 1 (1/8)	13.0645	11.8933	10.3488	25.8090	26.6248	27.8330
Maske 2 (1/4)	51.7801	47.4944	41.5196	13.8476	14.5980	15.7657
Maske 3 (1/2)	73.2636	67.0660	59.0454	10.8330	11.6008	12.7071
Maske 4 (Artı)	67.0952	61.0160	54.2058	11.5970	12.4219	13.4499

Yukarıdaki tablolarda verilen MSE ve PSNR değerlerine dikkat edildiğinde MSE değerlerinin tahribat arttıkça arttığı ve buna karşılık PSNR değerlerinin ise azaldığı görülmektedir. Bu durum görüntülerin saldırılara karşı oldukça dayanıklı olduğunu göstermektedir.

4.3.12 Bit geçerlik oranı testi

BCR, orijinal görüntü ve deşifrelenmiş görüntüler arasındaki piksel kayıplarının olup olmadığının tespit edilmesi için yapılmıştır. Gizli kullanıcı anahtarı ile görüntüler önce şifrelenmiş ve ardından deşifrelenmiştir. Bu adımların ardından BCR testi yapılmış ve elde edilen sonuçlar Tablo 10'da verilmiştir.

Tablo 10. Orijinal ve deşifreli görüntüler arasındaki bit kayıp oranları

	BCR (%)			
Görüntü	R	G	B	**Ortalama (%)**
Lena	0	0	0	0
Barbara	0	0	0	0
Baboon	0	0	0	0
Peppers	0	0	0	0

Benzer testler saldırgan tarafından gürültü eklenmiş ve tahribata uğratılmış görüntüler üzerinde de gerçekleştirilmiştir. Elde edilen sonuçlar sırasıyla Tablo 11 ve Tablo 12'de verilmiştir.

Tablo 11. Orijinal ve deşifreli gürültülü görüntüler arasındaki bit kayıp oranları

	BCR (%)			
Gürültü	**R**	**G**	**B**	**Ortalama (%)**
Tuz ve Biber (0.01)	0.0051	0.0051	0.0046	0.0049
Tuz ve Biber (0.05)	0.0241	0.0255	0.0252	0.0249
Gaussian (0.01)	0.4003	0.4004	0.4019	0.4008
Gaussian (0.1)	0.4487	0.4479	0.4477	0.4481

Tablo 12. Orijinal ve deşifreli tahribatlı görüntüler arasındaki bit kayıp oranları

	BCR (%)			
Maske	**R**	**G**	**B**	**Ortalama (%)**
Maske 1 (1/8)	0.0078	0.0079	0.0079	0.0078
Maske 2 (1/4)	0.1245	0.1247	0.1249	0.1247
Maske 3 (1/2)	0.2496	0.2502	0.2500	0.2499
Maske 4 (Artı)	0.2103	0.2097	0.2102	0.2100

Önerilen yöntemde bit kayıp oranları incelendiğinde saldırılara karşı oldukça dayanıklı olduğu görülmektedir. Bu durum arada saldırganın şifreli görüntüyü ele geçirip üzerinde tahribatlara neden olsa da elde edilen görüntüde çok ciddi kayıpların olmadığı ve doğru anahtar ile görüntünün büyük bir kısmının elde edilebileceğini göstermektedir. Dolayısı ile saldırılara karşı dayanıklı olduğu söylenebilmektedir.

4.3.13 NIST testi

Önerilen yöntemde şifrelenmiş görüntü piksellerinin rastgelelik durumunun test edilmesi için NIST testi uygulanmıştır. NIST testi şifreli “Lena” görüntüsüne uygulanmış ve elde edilen rastgelelik sonuçları Tablo 13’de verilmiştir.

Tablo 13. Şifrelenmiş "Lena" görüntü için NIST testi sonuçları

No	**Test Adı**	**P Değeri**	**Sonuç**
1	Frequency (Monobits) Test	0.0073	Rastgele değil
2	Frequency Test within a Block	0.4294	Rastgele
3	Runs Test	0.7815	Rastgele
4	Test for the Longest Run of Ones in a Block	0.1370	Rastgele
5	Binary Matrix Rank Test	0.4419	Rastgele
6	Discrete Fourier Transform Test	0.7823	Rastgele
7	Non-Overlapping Template Matching Test	0.8978	Rastgele
8	Overlapping Template Matching Test	0.5596	Rastgele
9	Maurer’s “Universal Statistical” Test	0.1546	Rastgele
10	Linear Complexity Test	0.1148	Rastgele

11	Serial Test	0.3520	Rastgele
12	Approximate Entropy Test	0.1713	Rastgele
13	Cumulative Sums Test	0.0138	Rastgele
14	Random Excursions Test	0.3695	Rastgele
15	Random Excursions Variant Test	0.1456	Rastgele

Bu test yönteminde *P* değerinin 0.01'den büyük olması değerlerin rastgele olduğunun bir işaretidir. Elde edilen test sonuçlarına dikkat edildiğinde önerilen yöntemin 15 adet rastgelelik testinden sadece bir tanesini geçemediği görülmüştür. Dolayısı ile önerilen yöntemin 14 farklı rastgelelik testinden geçmiş olması nedeniyle oldukça güvenilir ve piksel dağılımının rastgele olduğu sonucuna varılabilmektedir.

4.3.14 Çalışma süresi testi

Önerilen yöntemin çalışma süresi iki farklı özellikte bilgisayar üzerinde test edilmiştir. İlk bilgisayar Intel Core i7-4700 CPU 2.4 GHz 4 çekirdek, 16 GB RAM ve MS Windows 10 Pro 64 bit işletim sistemi ve ikinci bilgisayar ise Intel(R) Core(TM) i7-7700 CPU @ 3.60 GHz 8 çekirdek, 32 BG RAM ve MS Windows 10 Pro 64 bit işletim sistemi özelliklerine sahiptir. Çalışma süresi için her bir bilgisayarda 100 deneme yapılmış ve ortalama çalışma süresi elde edilmiştir. Elde edilen ortalama şifreleme ve deşifreleme süreleri Tablo 14'te verilmiştir.

Tablo 14. Çalışma süresi testi sonuçları

	Bilgisayar 1		**Bilgisayar 2**	
Görüntü	Şifreleme Süresi (sn)	Deşifreleme Süresi (sn)	Şifreleme Süresi (sn)	Deşifreleme Süresi (sn)
Lena	1.4121	1.4733	0.3339	0.3273
Barbara	1.4719	1.4934	0.3315	0.3308
Baboon	1.4664	1.4713	0.3285	0.3313
Peppers	1.4445	1.4114	0.3383	0.3703
Ortalama	1.4487	1.4623	0.3330	0.3399

Önerilen yöntemin şifreleme ve deşifreleme sürelerine dikkat edildiğinde oldukça hızlı olduğu ve sektörde her alanda kullanılabileceği sonucuna varılabilmektedir.

5. SONUÇ ve ÖNERİLER

Günümüzde internet ve mobil teknolojilerinin kullanımının yaygınlaşması beraberinde çeşitli güvenlik problemlerini de beraberinde getirmektedir. Özellikle mobil teknolojiler ile birlikte sosyal medya kullanımının ve görüntü paylaşımının yaygınlaşması görüntü şifreleme alanındaki çalışmalarında popüler hale gelmesini sağlamıştır. Görüntü verilerinin saklanması ve karşı alıcıya iletilirken istenmeyen şahısların ele geçirememesi, ele geçirse bile orijinal veriyi elde edememesi gibi konular görüntü şifreleme yöntemlerinin en temel ve önemli konuları arasındadır. Görüntü şifrelemek amacıyla kullanılan en yaygın yöntemlerin kaotik haritalardan faydalanılarak gerçekleştirilen yöntemler olduğu görülmüştür. Ancak bu kaotik haritalar farklı kaynaklarda yer almakta ve dağınık durumdadırlar. Bu sebepten dolayı bu çalışma ile bu kaotik haritalar içerisinde literatürde kullanımı yaygın olan ve literatürde az yer bulmuş kaotik haritalar bir araya getirilmiştir. Her bir kaotik haritanın sergiledikleri dağılım davranışları grafikler ile gösterilmiştir. Literatürde bu çalışmada verilen haritalardan başka kaotik haritalarda bulunmaktadır. Ancak süre performansları nedeni ile görüntü şifreleme algoritmalarında kullanımlarının tercih edilmediği gözlemlenmiş ve tez çalışmasında bu kaotik haritalara yer verilmemiştir.

Bu tez çalışmasında yer verilen kaotik haritalar kullanılarak bir görüntü şifreleme yöntemi de önerilmiştir. Önerilen yöntem farklı kaotik haritalardan oluşmaktadır. Böylelikle literatürde az kullanım olanağı bulmuş kaotik haritaların da kullanımına imkân verilmiştir. Yöntem, farklı test teknikleri ile test edilmiş ve her bir test yönteminden elde edilen sonuçlar değerlendirilmiştir. Yöntemden elde edilen test sonuçları dikkate alındığında oldukça başarılı sonuçlar elde edilmiştir. Yöntemin görüntü şifreleme amacıyla kolaylıkla her ortama uygulanabileceği ve kullanılabileceği öngörülmektedir.

Sonuç olarak bu tez çalışması ile görüntü şifreleme alanında kullanılan kaotik haritaların bir araya getirilmesi sağlanarak, görüntü şifreleme alanında çalışacak bilim insanlarına kılavuz olacağı düşünülmektedir. Ayrıca önerilen yöntemin esnekliği sayesinde de aynı yöntemde farklı kaotik haritalar kullanılarak bilim insanları tarafından farklı çalışmalar yapılabilecektir.

KAYNAKLAR

Abas, F. S., ve Arulmurugan, R. (2022). Radix Trie improved Nahrain chaotic map-based image encryption model for effective image encryption process. *International Journal of Intelligent Networks*, 3, 102-108.

Abd El-Latif, A. A., ve Niu, X. (2013). A hybrid chaotic system and cyclic elliptic curve for image encryption. *AEU-International Journal of Electronics Communications*, 67(2), 136-143.

Abd El-Samie, F. E., Ahmed, H. E. H., Elashry, I. F., Shahieen, M. H., Faragallah, O. S., El-Rabaie, E.-S. M., vd. (2013). *Image encryption: a communication perspective*: CRC Press.

AbdElHaleem, S. H., Abd-El-Hafiz, S. K., ve Radwan, A. G. (2022). A generalized framework for elliptic curves based PRNG and its utilization in image encryption. *Scientific reports*, 12(1), 1-16.

Abu-Amara, F. (2018). Image Encryption using Trigonometric Chaotic Map. *Jour of Adv Research in Dynamical & Control Systems*, 10(13), 230-237.

Abu-Amara, F., ve Abdel-Qader, I. (2013). Chaotic image encryption via convex sinusoidal map. *WSEAS Transactions on Signal Processing*, 9(4), 177-184.

Afifi, A. (2019). A chaotic confusion-diffusion image encryption based on Henon map. *International Journal of Network Security Applications Vol*, 11.

Agarwal, R., ve Patidar, V. (2018). *Double Image Encryption Based on 2D Discrete Fractional Fourier Transform and Piecewise Nonlinear Chaotic Map*. Paper presented at the International Conference on Advanced Informatics for Computing Research.

Ahmad, J., Khan, M. A., Ahmed, F., ve Khan, J. S. (2018). A novel image encryption scheme based on orthogonal matrix, skew tent map, and XOR operation. *Neural Computing Applications*, 30(12), 3847-3857.

Ahmad, J., Tahir, A., Khan, J. S., Jameel, A., Abbasi, Q. H., ve Buchanan, W. (2020). *A novel multi-chaos based compressive sensing encryption technique.* Paper presented at the 2019 International Conference on Advances in the Emerging Computing Technologies (AECT), DOI: 10.1109/AECT47998.2020.9194220.

Ahmad, M., Agarwal, S., Alkhayyat, A., Alhudhaif, A., Alenezi, F., Zahid, A. H., vd. (2022). An image encryption algorithm based on new generalized fusion fractal structure. *Information Sciences,* 592, 1-20.

Ahmed, D. W., Jawad, T. M., ve Jawad, L. M. (2021). An effective color image encryption scheme based on double piecewise linear chaotic map method and RC4 algorithm. *Journal of Engineering Science Technology*, 16(2), 1319-1341.

Akgül, A. (2015). *Yeni kaotik sistemler ile rasgele sayı üreteci tasarımı ve çoklu-ortam verilerinin yüksek güvenlikli şifrelenmesi,* (Yayın no: 387525) [Doktora Tezi\ Sakarya Üniversitesi, Fen Bilimleri Enstitüsü], https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp

Akgül, A., Kacar, S., Aricıoğlu, B., ve Pehlivan, I. (2013). *Text encryption by using one-dimensional chaos generators and nonlinear equations.* Paper presented at the 2013 8th International Conference on Electrical and Electronics Engineering (ELECO), DOI: 10.1109/ELECO.2013.6713853.

Al-Hazaimeh, O. M., Al-Jamal, M. F., Alhindawi, N., ve Omari, A. (2019). Image encryption algorithm based on Lorenz chaotic map with dynamic secret keys. *Neural Computing Applications*, 31(7), 2395-2405.

Al-Khasawneh, M. A., Uddin, I., Shah, S. A. A., Khasawneh, A. M., Abualigah, L., ve Mahmoud, M. (2022). An improved chaotic image encryption algorithm using Hadoop-based MapReduce framework for massive remote sensed images in parallel IoT applications. *Cluster Computing,* 25(2), 999-1013.

Al-Majdi, K., Salman, A., Abbas, N. A., Hashim, M. M., Taha, M., Nahi, A. A., vd. (2022). MLCM: An efficient image encryption technique for IoT application

based on multi-layer chaotic maps. *International Journal of Nonlinear Analysis Applications*.

Ali, K. M., ve Khan, M. (2019). Application based construction and optimization of substitution boxes over 2D mixed chaotic maps. *International Journal of Theoretical Physics*, 58(9), 3091-3117.

AlMutairi, F., ve Bonny, T. (2020). *Image Encryption Based on Chua Chaotic Oscillator*. Paper presented at the 2020 3rd International Conference on Signal Processing and Information Security (ICSPIS), DOI: 10.1109/ICSPIS51252.2020.9340157.

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

Alshibani, D. R. (2015). A new RGB image encryption based on a combination of 2D chaotic maps. *International Journal of Computer Application*, 975, 8887.

Alvarez, G., ve Li, S. (2006). Some basic cryptographic requirements for chaos-based cryptosystems. *International Journal of bifurcation chaos*, 16(08), 2129-2151.

Antoniou, I. (2001). The time operator of the cusp map. *Chaos, Solitons Fractals*, 12(9), 1619-1627.

Anusree, L., ve Rahiman, M. A. (2022). A New Highly Secure Optical Image Security Technique Using Gyrator Transform for Image Security-Related Applications. *International Journal of Optics*, 2022.

Arrowsmith, D. K., Cartwright, J. H., Lansbury, A. N., ve Place, C. M. (1993). The Bogdanov map: Bifurcations, mode locking, and chaos in a dissipative system. *International Journal of bifurcation chaos*, 3(04), 803-842.

Avaroğlu, E. (2014). *Donanım tabanlı rasgele sayı üretecinin gerçekleştirilmesi.* (Yayın No:355498), [Doktora Tezi\, Fırat Üniversitesi, Fen Bilimleri Enstitüsü, Elazığ], https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp.

Belazi, A., ve Abd El-Latif, A. A. (2017). A simple yet efficient S-box method based on chaotic sine map. *Optik,* 130, 1438-1444.

Belazi, A., Abd El-Latif, A. A., ve Belghith, S. (2016). A novel image encryption scheme based on substitution-permutation network and chaos. *Signal Processing,* 128, 155-170.

Bhowmik, A., Karforma, S., Dey, J., ve Sarkar, A. (2021). Linear Congruence Generator and Chaos Based Encryption Key Generation for Medical Data Security in IoT Based Health Care System. In *Advanced Soft Computing Techniques in Data Science, IoT and Cloud Computing* (pp. 53-79): Springer.

Bilal, H. (2021). *Kaotik kril sürüsü optimizasyon yönteminin geliştirilmesi ve süspansiyon parçasının optimizasyonu.* (Yayın no: 701017), [Doktora Tezi\Uludağ Üniversitesi, Bursa], https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp.

Brindha, M. (2017). *Periodicity analysis of Arnold Cat Map and its application to image encryption.* Paper presented at the 2017 International Conference on Inventive Computing and Informatics (ICICI), DOI: 10.1109/ICICI.2017.8365401.

Budiman, F., Andono, P., ve Setiadi, D. (2022). Image encryption using double layer chaos with dynamic iteration and rotation pattern. *Int. J. Intell. Eng. Syst,* 15, 57-67.

Caponetto, R., Fortuna, L., Fazzino, S., ve Xibilia, M. G. (2003). Chaotic sequences to improve the performance of evolutionary algorithms. *IEEE transactions on evolutionary computation,* 7(3), 289-304.

Ceyhan, M., ve Yolaçan, E. (2021). Görüntü Dosyalarının Şifrelenerek Güvenli Şekilde Saklanması. *Eskişehir Osmangazi Üniversitesi Mühendislik ve Mimarlık Fakültesi Dergisi,* 29(1), 28-42.

Chai, X., Chen, Y., ve Broyde, L. (2017). A novel chaos-based image encryption algorithm using DNA sequence operations. *Optics Lasers in Engineering,* 88, 197-213.

Chai, X., Gan, Z., Yang, K., Chen, Y., ve Liu, X. (2017). An image encryption algorithm based on the memristive hyperchaotic system, cellular automata and DNA sequence operations. *Signal Processing: Image Communication,* 52, 6-19.

Chandra, M., ve Sharma, P. (2017). Image encryption based on random scrambling and chaotic gauss iterative map. *Int J Comp Appl*, 157(3), 18-23.

Charalampidis, N., Volos, C., Moysis, L., Nistazakis, H. E., ve Stouboulos, I. (2022). *A Novel Piecewise Chaotic Map for Image Encryption.* Paper presented at the 2022 11th International Conference on Modern Circuits and Systems Technologies (MOCAST), DOI: 10.1109/MOCAST54814.2022.9837545.

Chen, S., Su, Q., Sun, Y., ve Zhang, X. (2022). A blind color image watermarking algorithm using the energy concentration principle of Hadamard matrix. *Optik,* 249, 168231.

Chen, X.-w., Fu, X.-l., ve Jing, Z.-j. (2013). Dynamics in a discrete-time predator-prey system with Allee effect. *Acta Mathematicae Applicatae Sinica, English Serie,* 29(1), 143-164.

Cheroiu, D.-G., Răducanu, M., ve Nitu, C. M. (2022). *Fast Image Encryption Algorithm Based on Multiple Chaotic Maps.* Paper presented at the 2022 14th International Conference on Communications (COMM), DOI: 10.1109/COMM54429.2022.9817317 .

Chialvo, D. R. (1995). Generic excitable dynamics on a two-dimensional map. *Chaos, Solitons Fractals,* 5(3-4), 461-479.

Das, S., Mondal, S. N., ve Sanyal, M. K. (2018). Image encryption based on Arnold cat map and GA operator. In *Intelligent Engineering Informatics* (pp. 19-28): Springer.

Demir, F. B., Tuncer, T., ve Kocamaz, A. F. (2019a). Lojistik-Gauss Harita Tabanlı Yeni Bir Kaotik Sürü Optimizasyon Yöntemi. *Computer Science,* 4(1), 47-53.

Demir, F. B., Tuncer, T., ve Kocamaz, A. F. (2019b). *Lojistik-Singer Harita Tabanlı Yeni Bir Kaotik Sürü Optimizasyon Yöntemi.* Paper presented at the 2019 International Artificial Intelligence and Data Processing Symposium (IDAP), DOI: 10.1109/IDAP.2019.8875984.

Dhopavkar, T. A., Nayak, S. K., ve Roy, S. (2022). IETD: a novel image encryption technique using Tinkerbell map and Duffing map for IoT applications. *Multimedia Tools Applications*, 1-40.

Dudás, J., ve Krisztin, T. (2021). Global stability for the three-dimensional logistic map. *Nonlinearity*, 34(2), 894.

Durafe, A., ve Patidar, V. (2022). *Comparative Analysis of Chaotic Image Encryption Using Improved 2D Gingerbreadman Map and Chirikov Standard Map.* Paper presented at the 2022 International Conference for Advancement in Technology (ICONAT), DOI: 10.1109/ICONAT53423.2022.9725986.

Eisencraft, M., Monteiro, L. H., ve Soriano, D. C. (2017). White Gaussian chaos. *IEEE Communications Letters*, 21(8), 1719-1722.

Elabbasy, E., Agiza, H., El-Metwally, H., ve Elsadany, A. (2007). Bifurcation analysis, chaos and control in the Burgers mapping. *International Journal of Nonlinear Science*, 4(3), 171-185.

Elghandour, A. N., Salah, A. M., Elmasry, Y. A., ve Karawia, A. A. (2021). An image encryption algorithm based on bisection method and one-dimensional piecewise chaotic map. *IEEE Access*, 9, 43411-43421.

Elkandoz, M. T., ve Alexan, W. (2022). Image encryption based on a combination of multiple chaotic maps. *Multimedia Tools Applications*, 1-22.

Elkandoz, M. T., Alexan, W., ve Hussein, H. H. (2019). *Logistic sine map based image encryption.* Paper presented at the 2019 Signal Processing: Algorithms, Architectures, Arrangements, and Applications (SPA), DOI: 10.23919/SPA.2019.8936718.

Elmanfaloty, R. A., ve Abou-Bakr, E. (2020). An image encryption scheme using a 1D chaotic double section skew tent map. *Complexity,* 2020.

Enayatifar, R., Sadaei, H. J., Abdullah, A. H., Lee, M., ve Isnin, I. F. (2015). A novel chaotic based image encryption using a hybrid model of deoxyribonucleic acid and cellular automata. *Optics Lasers in Engineering,* 71, 33-41.

Essaid, M., Akharraz, I., Saaidi, A., ve Mouhib, A. (2018). A new image encryption scheme based on confusion-diffusion using an enhanced skew tent map. *Procedia Computer Science*, 127, 539-548.

Feng, W., He, Y., Li, H., ve Li, C. (2019). Cryptanalysis and improvement of the image encryption scheme based on 2D logistic-adjusted-sine map. *IEEE Access,* 7, 12584-12597.

Gaffar, A., Joshi, A., ve Kumar, D. (2020). Image Encryption using Gingerbreadman Map And RC4A Stream Cipher. *Applications Applied Mathematics: An International Journal*, 15(2), 30.

Geetha, S., Punithavathi, P., Infanteena, A. M., ve Sindhu, S. S. S. (2018). A literature review on image encryption techniques. *International Journal of Information Security Privacy*, 12(3), 42-83.

Ghebleh, M., Kanso, A., ve Noura, H. (2014). An image encryption scheme based on irregularly decimated chaotic maps. *Signal Processing: Image Communication,* 29(5), 618-627.

Griffin, J. (2013). The sine map. Erişim Tarihi: 19.08.2022 https://people.maths.bris.ac.uk/~macpd/ads/sine.pdf, adresinden alındı.

Gu, G., ve Ling, J. (2014). A fast image encryption method by using chaotic 3D cat maps. *Optik*, 125(17), 4700-4705.

Gupta, M., Gupta, K. K., ve Shukla, P. K. (2021). Session key based novel lightweight image encryption algorithm using a hybrid of Chebyshev chaotic map and crossover. *Multimedia Tools Applications*, 80(25), 33843-33863.

Gupta, M., Singh, V. P., Gupta, K. K., ve Shukla, P. K. (2022). An efficient image encryption technique based on two-level security for internet of things. *Multimedia Tools Applications*, 1-21.

Güvenoğlu, E. (2016). Resim şifreleme amacıyla dinamik S kutusu tasarımı için bir yöntem. *El-Cezeri,* 3(2).

Güvenoğlu, E., ve Esin, E. M. (2009). Knutt/Durstenfeld shuffle algoritmasının resim şifreleme amacıyla kullanılması. *Politeknik Dergisi,* 12(3), 151-155.

Güvenoğlu, E., ve Tunalı, V. (2023). ZigZag transform with Durstenfeld shuffle for fast and secure image encryption. *Connection Science*, 1-23.

Habek, M., Gene, Y., Aytas, N., Akkoc, A., Afacan, E., ve Yazgan, E. (2022). *Digital Image Encryption Using Elliptic Curve Cryptography: A Review.* Paper presented at the 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), DOI: 10.1109/HORA55278.2022.9800074.

Hamza, R., ve Titouna, F. (2016). A novel sensitive image encryption algorithm based on the Zaslavsky chaotic map. *Information Security Journal: A Global Perspective,* 25(4-6), 162-179.

Hassan, N. F., Aladhami, A., ve Mahdi, M. S. (2022). Digital Speech Files Encryption based on Hénon and Gingerbread Chaotic Maps. *Iraqi Journal of Science*, 830-842.

Hoseini, R., Behnia, S., Sarmady, S., ve Fathizadeh, S. (2022). Construction of dynamical S-boxes based on piecewise map: Image encryption approach. *Reseach Square*.

Hua, Z., Jin, F., Xu, B., ve Huang, H. (2018). 2D Logistic-Sine-coupling map for image encryption. *Signal Processing,* 149, 148-161.

Hua, Z., Zhu, Z., Yi, S., Zhang, Z., ve Huang, H. (2021). Cross-plane colour image encryption using a two-dimensional logistic tent modular map. *Information Sciences,* 546, 1063-1083.

Huang, H., ve Yang, S. (2017). Colour image encryption based on logistic mapping and double random-phase encoding. *IET Image Processing*, 11(4), 211-216.

Huang, X., ve Ye, G. (2014). An efficient self-adaptive model for chaotic image encryption algorithm. *Communications in Nonlinear Science Numerical Simulation*, 19(12), 4094-4104.

Hussain, I., Anees, A., Alkhaldi, A. H., Aslam, M., Siddiqui, N., ve Ahmed, R. (2019). Image encryption based on Chebyshev chaotic map and S8 S-boxes. *Optica Applicata*, 49(2).

Hussein, K. A., Mahmood, S. A., ve Abbass, M. A. (2019). *A New Permutation-Substitution Scheme Based on Henon Chaotic Map for Image Encryption.* Paper presented at the 2019 2nd Scientific Conference of Computer Sciences (SCCS), DOI: 10.1109/SCCS.2019.8852590.

Ismail, S. M., Said, L. A., Rezk, A. A., Radwan, A. G., Madian, A. H., Abu-ElYazeed, M. F., vd. (2017). *Biomedical image encryption based on double-humped and fractional logistic maps.* Paper presented at the 2017 6th international conference on modern circuits and systems technologies (MOCAST), DOI: 10.1109/MOCAST.2017.7937642.

Izotov, Y., Velichko, A., ve Boriskov, P. (2021). *Method for fast classification of MNIST digits on Arduino UNO board using LogNNet and linear congruential generator*. Paper presented at the Journal of Physics: Conference Series, DOI: 10.1088/1742-6596/2094/3/032055.

Jia, X. (2010). *Image Encryption using the Ikeda map.* Paper presented at the 2010 International conference on intelligent computing and cognitive informatics, DOI: 10.1109/ICICCI.2010.124.

Joshi, A. B., Kumar, D., Singh, S., ve Srivastava, K. (2021). *A New Algorithm for Color-Image Encryption Using 3D-Lorenz Chaotic Map and Random Modulus Decomposition in Transform Domain.* Paper presented at the Proceedings of

International Conference on Scientific and Natural Computing, DOI: 10.1007/978-981-16-1528-3_3.

Kanwal, S., Inam, S., Othman, M. T. B., Waqar, A., Ibrahim, M., Nawaz, F., vd. (2022). An Effective Color Image Encryption Based on Henon Map, Tent Chaotic Map, and Orthogonal Matrices. *Sensors*, 22(12), 4359.

Kapur, H., ve Girdhar, A. (2019). Image encryption approach using ikeda map and vertical and horizontal blocks. *Asian Journal of Multidimensional Research*, 8(3), 81-90.

Karim, A. B., Abdalqader, P. S., Najim, Z. T., Salhd, A. M., ve Abdulhammed, O. Y. (2021). Color Image Encryption with a Novel Technique and Chaotic Singer Map. *Science Journal of University of Zakho*, 9(3), 158-162.

Kaur, M., ve Kumar, V. (2020). A comprehensive review on image encryption techniques. *Archives of Computational Methods in Engineering*, 27(1), 15-43.

Khan, F. A., Ahmed, J., Khan, J. S., Ahmad, J., ve Khan, M. A. (2017). A novel image encryption based on Lorenz equation, Gingerbreadman chaotic map and S 8 permutation. *Journal of Intelligent Fuzzy Systems*, 33(6), 3753-3765.

Khan, F. H., Shams, R., Qazi, F., ve Agha, D. (2015). Hill cipher key generation algorithm by using orthogonal matrix. *Int. J. Innov. Sci. Mod. Eng*, 3(3), 5-7.

Khan, M., Jamal, S. S., Hazzazi, M. M., Ali, K. M., Hussain, I., ve Asif, M. (2021). An efficient image encryption scheme based on double affine substitution box and chaotic system. *Integration*, 81, 108-122.

Khan, M., Masood, F., Alghafis, A., Amin, M., ve Batool Naqvi, S. I. (2019). A novel image encryption technique using hybrid method of discrete dynamical chaotic maps and Brownian motion. *PLoS One*, 14(12), e0225031.

Kim, S.-J., Naruse, M., Aono, M., Hori, H., ve Akimoto, T. (2016). Random walk with chaotically driven bias. *Scientific reports*, 6(1), 1-9.

Kordov, K. (2021). Text Encryption Algorithm For Secure Communication. *International Journal of Applied Mathematics,* 34(4), 705.

Krishna, P. R., Teja, C. V. S., ve Thanikaiselvan, V. (2018). *A chaos based image encryption using tinkerbell map functions.* Paper presented at the 2018 Second International Conference on Electronics, Communication and Aerospace Technology (ICECA), DOI: 10.1109/ICECA.2018.8474891.

Kumar, A., ve Raghava, N. (2020). *Wavelet Based Selective Image Encryption Scheme Using Tinkerbell Chaotic Map.* Paper presented at the International Conference on Communication, Networks and Computing, DOI: 10.1007/978-981-16-8896-6_16.

Kumar, D., Joshi, A. B., Singh, S., ve Mishra, V. N. (2021). *Digital color-image encryption scheme based on elliptic curve cryptography ElGamal encryption and 3D Lorenz map.* Paper presented at the AIP Conference Proceedings, DOI: 10.1063/5.0062877.

Kumar, J., Singh, P., ve Yadav, A. (2020). *Asymmetric color image encryption using singular value decomposition and chaotic Tinkerbell map in fractional Fourier domain.* Paper presented at the Optics and Photonics for Information Processing XIV, DOI: 10.1117/12.2568447.

Kumar, K., Roy, S., Rawat, U., ve Mishra, I. (2022). *An Efficient Image Encryption Technique Using Logistic Map and 2D-TCLM.* Paper presented at the International Conference on Cyber Warfare, Security and Space Research, DOI: 10.1007/978-3-031-15784-4_7.

Kumari, M., Gupta, S., ve Sardana, P. (2017). A survey of image encryption algorithms. *3D Research,* 8(4), 1-35.

Küpeli, C., ve Bulut, F. (2020). Görüntüdeki Tuz Biber ve Gauss Gürültülerine Karşı Filtrelerin Performans Analizleri. *Haliç Üniversitesi Fen Bilimleri Dergisi,* 3(2), 211-239.

Leipnik, R., ve Newton, T. (1981). Double strange attractors in rigid body motion with linear feedback control. *Physics Letters A*, 86(2), 63-67.

Li, C., Luo, G., ve Li, C. (2018). A Novel Scheme for the Preview of the Image Encryption Based on Chaotic Ikeda Map. *Int. J. Netw. Secur.*, 20(6), 1105-1114.

Li, C., Luo, G., Qin, K., ve Li, C. (2017). An image encryption scheme based on chaotic tent map. *Nonlinear Dynamics*, 87(1), 127-133.

Li, M., Xu, M., Luo, J., ve Fan, H. (2019). Cryptanalysis of an image encryption using 2D henon-sine map and DNA approach. *IEEE Access*, 7, 63336-63345.

Li, R., Liu, Q., ve Liu, L. (2019). Novel image encryption algorithm based on improved logistic map. *IET Image Processing*, 13(1), 125-134.

Liu, H., Wen, F., ve Kadir, A. (2019). Construction of a new 2D Chebyshev-Sine map and its application to color image encryption. *Multimedia Tools Applications*, 78(12), 15997-16010.

Liu, J., Wang, Y., Liu, Z., ve Zhu, H. (2021). A chaotic image encryption algorithm based on coupled piecewise sine map and sensitive diffusion structure. *Nonlinear Dynamics*, 104(4), 4615-4633.

Liu, W., Sun, K., ve Zhu, C. (2016). A fast image encryption algorithm based on chaotic map. *Optics Lasers in Engineering*, 84, 26-36.

Liu, Y., Qin, Z., Liao, X., ve Wu, J. (2020a). A chaotic image encryption scheme based on Hénon–Chebyshev modulation map and genetic operations. *International Journal of bifurcation chaos*, 30(06), 2050090.

Liu, Y., Qin, Z., Liao, X., ve Wu, J. (2020b). Cryptanalysis and enhancement of an image encryption scheme based on a 1-D coupled Sine map. *Nonlinear Dynamics*, 100(3), 2917-2931.

Lu, H., Wang, X., Fei, Z., ve Qiu, M. (2014). The effects of using chaotic map on improving the performance of multiobjective evolutionary algorithms. *Mathematical Problems in Engineering*, 2014.

Luo, Y., Ouyang, X., Liu, J., ve Cao, L. (2019). An image encryption method based on elliptic curve elgamal encryption and chaotic systems. *IEEE Access*, 7, 38507-38522.

Luo, Y., Yu, J., Lai, W., ve Liu, L. (2019). A novel chaotic image encryption algorithm based on improved baker map and logistic map. *Multimedia Tools Applications*, 78(15), 22023-22043.

Luo, Y., Zhou, R., Liu, J., Cao, Y., ve Ding, X. (2018). A parallel image encryption algorithm based on the piecewise linear chaotic map and hyper-chaotic map. *Nonlinear Dynamics*, 93(3), 1165-1181.

Lv, W., Bai, R., ve Sun, X. (2019). *Image encryption algorithm based on hyper-chaotic lorenz map and compressed sensing theory.* Paper presented at the 2019 Chinese Control Conference (CCC), DOI: 10.23919/ChiCC.2019.8866148.

Masood, F., Ahmad, J., Shah, S. A., Jamal, S. S., ve Hussain, I. (2020). A novel hybrid secure image encryption based on julia set of fractals and 3D Lorenz chaotic map. *Entropy*, 22(3), 274.

Masood, F., Boulila, W., Alsaeedi, A., Khan, J. S., Ahmad, J., Khan, M. A., vd. (2022). A novel image encryption scheme based on Arnold cat map, Newton-Leipnik system and Logistic Gaussian map. *Multimedia Tools Applications*, 1-29.

Mateos, D. M., Zozor, S., ve Olivares, F. (2020). Contrasting stochasticity with chaos in a permutation Lempel–Ziv complexity—Shannon entropy plane. *Physica A: Statistical Mechanics its Applications*, 554, 124640.

Mendua, B. R. B. I. (2013). A new approach of colour image encryption based on Henon like chaotic map. *Journal of Information Engineering Applications*, 3(6).

Mishra, K., ve Saharan, R. (2019). A fast image encryption technique using Henon chaotic map. In *Progress in advanced computing and intelligent engineering* (pp. 329-339): *Springer.*

Mishra, M., ve Mankar, V. (2012). *Design and Analysis of Cipher Based on Henon And Burger Maps.* Paper presented at the Proceedings of IEEE 4th International Conference on Electronics Computer Technology (ICECT-2012), DOI: 978-1-4673-1850-1/12/.

Mondal, B., Singh, S., ve Kumar, P. (2019). A secure image encryption scheme based on cellular automata and chaotic skew tent map. *Journal of Information Security Applications,* 45, 117-130.

Munir, N., Khan, M., Jamal, S. S., Hazzazi, M. M., ve Hussain, I. (2021). Cryptanalysis of hybrid secure image encryption based on Julia set fractals and three-dimensional Lorenz chaotic map. *Mathematics Computers in Simulation,* 190, 826-836.

Muñoz-Guillermo, M. (2021). Image encryption using q-deformed logistic map. *Information Sciences,* 552, 352-364.

Naskar, P. K., Bhattacharyya, S., Nandy, D., ve Chaudhuri, A. (2020). A robust image encryption scheme using chaotic tent map and cellular automata. *Nonlinear Dynamics,* 100(3), 2877-2898.

Natiq, H., Roy, A., Banerjee, S., Misra, A., ve Fataf, N. (2020). Enhancing chaos in multistability regions of Duffing map for an asymmetric image encryption algorithm. *arXiv preprint arXiv:.02347*.

Nazir, H., Bajwa, I. S., Abdullah, S., Kazmi, R., ve Samiullah, M. (2022). A Color Image Encryption Scheme Combining Hyperchaos and Genetic Codes. *IEEE Access,* 10, 14480-14495.

Okuyucu, H. H. (2020). *Hash Fonksiyonlarının Adli Bilişimde Uygulamaları ve C++ İle Şifreleme Algoritması Tasarımı,* (Yayın no: 649174), [Yüksek Lisans Tezi\

Karabük Üniversitesi, Lisansüstü Eğitim Enstitüsü], https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp.

Öz, D. (2016). Göç Eden Kuşlar Algoritmasinda Kaos Fonksiyonlarinin Kullanilmasi. *Gazi Üniversitesi Fen Bilimleri Dergisi Part C: Tasarım ve Teknoloji,* 4(4), 225-233.

Özyön, S., Yaşar, C., ve Temurtaş, H. (2020). Test Fonksiyonları için Kaos Tabanlı Yerçekimsel Arama Algoritmaları (CbGSA-X). *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, 8(3), 1771-1793.

Parameshachari, B. (2021). *Logistic sine map (LSM) based partial image encryption.* Paper presented at the 2021 National Computing Colleges Conference (NCCC), DOI: 10.1109/NCCC49330.2021.9428854 .

Parida, P., ve Pradhan, C. (2022). *Improved ECC-Based Image Encryption with 3D Arnold Cat Map.* Paper presented at the International Conference on Innovative Computing and Communications, DOI: 10.1007/978-981-16-2594-7_62.

Pehlivan, İ. (2007). *Yeni kaotik sistemler: elektronik devre gerçeklemeleri, senkronizasyon ve güvenli haberleşme uygulamaları.* (Yayın no: 212246) [Doktora Tezi\Sakarya Üniversitesi, Fen Bilimleri Enstitüsü]. https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp.

Ping, P., Wu, J., Mao, Y., Xu, F., ve Fan, J. (2018). Design of image cipher using life-like cellular automata and chaotic map. *Signal Processing*, 150, 233-247.

Pluhacek, M., Senkerik, R., Viktorin, A., ve Kadavy, T. (2020). Chaos-enhanced multiple-choice strategy for particle swarm optimisation. *International Journal of Parallel, Emergent Distributed Systems*, 35(6), 603-616.

Qi, F., Huang, S., Li, T., Yang, H., ve Kang, X. (2019). *2D henon-chebyshev chaotic map for image encryption.* Paper presented at the 2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on

Data Science and Systems (HPCC/SmartCity/DSS), DOI: 10.1109/HPCC/SmartCity/DSS.2019.00114.

Rabie, O., Ahmad, J., ve Alghazzawi, D. (2022). Modified SHARK Cipher and Duffing Map-Based Cryptosystem. *Mathematics,* 10(12), 2034.

Raghava, N., ve Kumar, A. (2013). Image encryption using henon chaotic map with byte sequence. *International Journal of Computer Science Engineering Information Technology Research,* 3(5), 11-18.

Ran, J. (2020). Identification of chaos in fractional chaotic map. *Advances in Difference Equations*, 2020(1), 1-9.

Rashmi, P., ve Supriya, M. C. (2020). Self Adaptive Image Encryption Based on Orthogonal Scan Patterns Using Arnold Cat Map and Tent Map. *SSAHE-JIR*, 36.

Rehman, A. U., Khan, J. S., Ahmad, J., ve Hwang, S. O. (2016). A new image encryption scheme based on dynamic s-boxes and chaotic maps. *3D Research,* 7(1), 1-8.

Rehman, M. U., Shafique, A., Khalid, S., ve Hussain, I. (2021). Dynamic substitution and confusion-diffusion-based noise-resistive image encryption using multiple chaotic maps. *IEEE Access,* 9, 52277-52291.

Rodrigo, J. A., Alieva, T., ve Calvo, M. L. (2007). Gyrator transform: properties and applications. *Optics express,* 15(5), 2190-2203.

Rohith, S., ve Sujatha, B. (2015). *Image encryption and decryption using combined key sequence of Logistic map and Lozi map.* Paper presented at the 2015 International Conference on Communications and Signal Processing (ICCSP), DOI: 10.1109/ICCSP.2015.7322662.

Rostami, M. J., Shahba, A., Saryazdi, S., ve Nezamabadi-pour, H. (2017). A novel parallel image encryption with chaotic windows based on logistic map. *Computers Electrical Engineering,* 62, 384-400.

Roy, M., Chakraborty, S., ve Mali, K. (2020). A robust image encryption method using chaotic skew-tent map. In *Applications of advanced machine intelligence in computer vision and object recognition: emerging research and opportunities* (pp. 1-29): IGI Global.

Rueda, E., Vera, C. A., Rodríguez, B., ve Torroba, R. (2008). Synchronized chaotic phase masks for encrypting and decrypting images. *Optics communications*, 281(23), 5750-5755.

Rusakov, A., Tikhonov, D., Nurieva, N., ve Medvinsky, A. (2021). Emergence of Self-Organized Dynamical Domains in a Ring of Coupled Population Oscillators. Mathematics 2021, 9, 601. In: s Note: MDPI stays neutral with regard to jurisdictional claims in published.

Safi, H. W., ve Maghari, A. Y. (2017). *Image encryption using double chaotic logistic map.* Paper presented at the 2017 International Conference on Promising Electronic Technologies (ICPET), DOI: 10.1109/ICPET.2017.18.

Sahay, A., ve Pradhan, C. (2017a). *Gauss iterated map based RGB image encryption approach.* Paper presented at the 2017 International Conference on Communication and Signal Processing (ICCSP), DOI: 10.1109/ICCSP.2017.8286437.

Sahay, A., ve Pradhan, C. (2017b). *Multidimensional comparative analysis of image encryption using gauss iterated and logistic maps.* Paper presented at the 2017 International Conference on Communication and Signal Processing (ICCSP), DOI: 10.1109/ICCSP.2017.8286603.

Saidi, R., Cherrid, N., Bentahar, T., Mayache, H., ve Bentahar, A. (2020). Number of Pixel Change Rate and Unified Average Changing Intensity for Sensitivity Analysis of Encrypted inSAR Interferogram. *Ingénierie des Systèmes d Inf.,* 25(5), 601-607.

Sakal, H. (2016). *Görüntü şifreleme teknikleri ve bir uygulama tasarımı.* (Yayın No: 455545), [Yüksek Lisans Tezi\Kocaeli Üniversitesi, Fen Bilimleri Enstitüsü], https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp.

Sakal, H., ve Yıldırım, M. (2016). Görüntü şifreleme için scan paternlerini kullanan hibrit bir yöntem. *Selçuk-Teknik Dergisi,* 15(3), 264-283.

Salunke, S., Ahuja, B., Hashmi, M. F., Marriboyina, V., ve Bokde, N. D. (2022). 5D Gauss Map Perspective to Image Encryption with Transfer Learning Validation. *Applied Sciences,* 12(11), 5321.

Samtaş, G., ve Gülesin, M. (2011). Sayısal görüntü işleme ve farklı alanlardaki uygulamaları. *Ejovoc,* 2(1), 85-97.

Sangavi, V., ve Thangavel, P. (2020). An exotic multi-dimensional conceptualization for medical image encryption exerting Rossler system and Sine map. *Journal of Information Security Applications,* 55, 102626.

Sankaradass, V., Murali, P., ve Tholkapiyan, M. (2018). *Region of Interest (ROI) based image encryption with sine map and lorenz system.* Paper presented at the International Conference on ISMAC in Computational Vision and Bio-Engineering, DOI: 10.1007/978-3-030-00665-5_49.

Savitri, N., Johan, A. W. S. B., Firnanda Al Islama, A., ve Utaminingrum, F. (2019). *Efficient Technique Image Encryption with Cipher Block Chaining and Gingerbreadman Map.* Paper presented at the 2019 International Conference on Sustainable Information Engineering and Technology (SIET), DOI: 10.1109/SIET48054.2019.8986084.

Shafique, A., ve Ahmed, J. (2022). *A Color Image Encryption Algorithm Based on Chaotic Map and Discrete Wavelet Transform.* Paper presented at the 2022 Global Conference on Wireless and Optical Technologies (GCWOT), DOI: 10.1109/GCWOT53057.2022.9772906.

Shah, A. A., Parah, S. A., Rashid, M., ve Elhoseny, M. (2020). Efficient image encryption scheme based on generalized logistic map for real time image processing. *Journal of Real-Time Image Processing,* 17(6), 2139-2151.

Shah, T., Qureshi, A., ve Usman, M. (2021). A Novel Color Image Encryption Scheme Based on Arnold's Cat Map and 16-Byte S-box. *Applications Applied Mathematics: An International Journal,* 16(1), 33.

Shaw, R. (1981). Strange attractors, chaotic behavior, and information flow. *Zeitschrift für Naturforschung A,* 36(1), 80-112.

Sheela, S., ve Sathyanarayana, S. (2017). Application of chaos theory in data security-a survey. *ACCENTS Trans Inf Secur,* 2(5), 1-15.

Sheela, S., Suresh, K., ve Tandur, D. (2018). Image encryption based on modified Henon map using hybrid chaotic shift transform. *Multimedia Tools Applications,* 77(19), 25223-25251.

Singh, K. N., ve Singh, A. K. (2022). Towards integrating image encryption with compression: a survey. *ACM Transactions on Multimedia Computing, Communications, Applications,* 18(3), 1-21.

Singh, N., ve Sinha, A. (2008). Optical image encryption using fractional Fourier transform and chaos. *Optics Lasers in Engineering,* 46(2), 117-123.

Singh, N., ve Sinha, A. (2009). Gyrator transform-based optical image encryption, using chaos. *Optics Lasers in Engineering,* 47(5), 539-546.

Singh, N., ve Sinha, A. (2010a). Chaos based multiple image encryption using multiple canonical transforms. *Optics Laser Technology*, 42(5), 724-731.

Singh, N., ve Sinha, A. (2010b). Optical image encryption using improper Hartley transforms and chaos. *Optik,* 121(10), 918-925.

Singh, S., Parida, R., ve Pradhan, C. (2018). *Comparative analysis of image encryption using 2d and 3d variations of duffing map.* Paper presented at the 2018

International Conference on Communication and Signal Processing (ICCSP), DOI: 10.1109/ICCSP.2018.8524385.

Sinha, R. K., ve Sahu, S. (2018). Secure image encryption based on improved bat optimized piecewise linear chaotic map through integrated permutation-confusion and double diffusion. *Journal of Intelligent Fuzzy Systems*, 35(2), 1567-1578.

Sinha, R. K., San, N., Asha, B., ve Sahu, S. (2018). *Chaotic image encryption scheme based on modified arnold cat map and henon map.* Paper presented at the 2018 International Conference on Current Trends towards Converging Technologies (ICCTCT), DOI: 10.1109/ICCTCT.2018.8551137.

Sivakumar, T., ve Venkatesan, R. (2015). A novel image encryption using calligraphy based scan method and random number. *KSII Transactions on Internet Information Systems*, 9(6), 2317-2337.

Stoyanov, B. (2014). Pseudo-random bit generation algorithm based on Chebyshev polynomial and Tinkerbell map. *Applied Mathematical Sciences*, 8(125), 6205-6210.

Stoyanov, B., ve Ivanova, T. (2019). *CHAOSA: Chaotic map based random number generator on Arduino platform.* Paper presented at the AIP Conference Proceedings, DOI: 10.1063/1.5133578.

Subashini, V., ve Poornachandra, S. (2018). A New Transformation for Chaotic Image Encryption based on the Arnold Cat Map. *Applied Mathematics Information Sciences An International Journal*, 12(4), 797-805.

Sukhjeevan, K., ve Shaveta, A. (2015). Image Encryption Using Chaotic Map and Prime modulo Multiplicative Linear Congruential Generator. *International Journal of Innovative Research in Computer Communication Engineering*, 3(3), 2339-2345.

Şekertekin, Y., ve Atan, Ö. (2016). *An image encryption algorithm using Ikeda and Henon chaotic maps.* Paper presented at the 2016 24th Telecommunications Forum (TELFOR), DOI: 10.1109/TELFOR.2016.7818872.

Taşkıran, A. (2011). *Burke-shaw ve T (Tıgan) kaotik osilatörlerinin tasarımı: güvenli haberleşme amaçlı senkronizasyon uygulamaları.* (Yayın No: 283330), [Yüksek Lisans Tezi \Sakarya Üniversitesi, Fen Bilimleri Enstitüsü], https://tez.yok.gov.tr/UlusalTezMerkezi/tezSorguSonucYeni.jsp.

Tubola, O. D. (2017). *Kaplan-Yorke map Implementation on FPGA for a highly secured image encryption system.* (Master Thesis), Gokongwei College of Engineering, Philippines, Erişim Tarihi: 15.12.2022. URL: https://animorepository.dlsu.edu.ph/etd_masteral/5800/ adresinden alındı.

Tuncer, S. A., ve Yeliz, G. (2019). İnsan Hareketleri Tabanlı Gerçek Rasgele Sayı Üretimi. *Bitlis Eren Üniversitesi Fen Bilimleri Dergisi,* 8(1), 261-269.

Tuncer, T. (2018). Çadır Haritası Tabanlı Kaotik Optimizasyon Yöntemi. *Gazi University Journal of Science Part C: Design Technology,* 6(4), 909-918.

Wang, B., ve Sun, C.-C. (2001). Enhancement of signal-to-noise ratio of a double random phase encoding encryption system. *Optical Engineering,* 40(8), 1502-1506.

Wang, M. m., Zhou, N.-r., Li, L., ve Xu, M.-t. (2022). A novel image encryption scheme based on chaotic apertured fractional Mellin transform and its filter bank. *Expert Systems with Applications,* 207, 118067.

Wang, X., ve Guan, N. (2022). 2D sine-logistic-tent-coupling map for image encryption. *Journal of Ambient Intelligence Humanized Computing,* 1-21.

Wang, X., ve Yang, J. (2021). A privacy image encryption algorithm based on piecewise coupled map lattice with multi dynamic coupling coefficient. *Information Sciences,* 569, 217-240.

Wang, Z., Su, Y., Wang, X., Wang, B., Li, S., Liu, C., vd. (2022). Security-enhanced multiple-image encryption based on quick response codes and modified double random phase encoding in the fractional Fourier transform domain. *Applied Optics,* 61(24), 7255-7264.

Wu, J., Liao, X., ve Yang, B. (2018). Image encryption using 2D Hénon-Sine map and DNA approach. *Signal Processing,* 153, 11-23.

Xiang, H., ve Liu, L. (2020). An improved digital logistic map and its application in image encryption. *Multimedia Tools Applications,* 79(41), 30329-30355.

Xie, H., Zhang, L., ve Lim, C. P. (2020). Evolving CNN-LSTM models for time series prediction using enhanced grey wolf optimizer. *IEEE Access,* 8, 161519-161541.

Xu, Y., ve Zhen, X. (2022). *Image encryption using improved Cubic map and Henon map.* Paper presented at the ITM Web of Conferences, DOI:10.1051/itmconf/20224502011.

Yahi, A., Bekkouche, T., Daachi, M. E. H., ve Diffellah, N. (2022). A color image encryption scheme based on 1D cubic map. *Optik,* 249, 168290.

Yang, X., Min, L., ve Wang, X. (2015). A cubic map chaos criterion theorem with applications in generalized synchronization based pseudorandom number generator and image encryption. *Chaos: An Interdisciplinary Journal of Nonlinear Science,* 25(5), 053104.

Yardım, F., ve Afacan, E. (2010). Lorenz-Tabanli Diferansiyel Kaos Kaydirmali Anahtarlama (DCSK) Modeli Kullanilarak Kaotik Bir Haberleşme Sisteminin simülasyonu. *Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi,* 25(1).

Yasser, I., Khalil, A. T., Mohamed, M. A., Samra, A. S., ve Khalifa, F. (2021). A Robust Chaos-Based Technique for Medical Image Encryption. *IEEE Access,* 10, 244-257.

Ye, G., ve Huang, X. (2017). An efficient symmetric image encryption algorithm based on an intertwining logistic map. *Neurocomputing,* 251, 45-53.

Yin, P., ve Min, L. (2010). *A color image encryption algorithm based generalized Chaos synchronization for bidirectional discrete systems for audio signal communication.* Paper presented at the 2010 International Conference on

Intelligent Control and Information Processing, DOI: 10.1109/ICICIP.2010.5565244.

Yosefnezhad Irani, B., Ayubi, P., Amani Jabalkandi, F., Yousefi Valandar, M., ve Jafari Barani, M. (2019). Digital image scrambling based on a new one-dimensional coupled Sine map. *Nonlinear Dynamics,* 97(4), 2693-2721.

Yuan, S., Jiang, T., ve Jing, Z. (2011). Bifurcation and chaos in the Tinkerbell map. *International Journal of bifurcation chaos,* 21(11), 3137-3156.

Yüksel, T., ve Özgün, B. (2021). RSA ve RC4 Algoritmalarının Performans Karşılaştırması. *AURUM Journal of Engineering Systems,* 5(1), 29-40.

Zahmoul, R., Ejbali, R., ve Zaied, M. (2017). Image encryption based on new Beta chaotic maps. *Optics Lasers in Engineering,* 96, 39-49.

Zareai, D., Balafar, M., ve Feizi Derakhshi, M. R. (2021). A new Grayscale image encryption algorithm composed of logistic mapping, Arnold cat, and image blocking. *Multimedia Tools Applications,* 80(12), 18317-18344.

Zhang, W., Wong, K.-w., Yu, H., ve Zhu, Z.-l. (2013). An image encryption scheme using reverse 2-dimensional chaotic map and dependent diffusion. *Communications in Nonlinear Science Numerical Simulation,* 18(8), 2066-2080.

Zhang, Y., ve Xiao, D. (2013). Double optical image encryption using discrete Chirikov standard map and chaos-based fractional random transform. *Optics Lasers in Engineering,* 51(4), 472-480.

Zhao, M., Xuan, Z., ve Li, C. (2016). Dynamics of a discrete-time predator-prey system. *Advances in Difference Equations,* 2016(1), 1-18.

Zheng, J., ve Liu, L. (2020). Novel image encryption by combining dynamic DNA sequence encryption and the improved 2D logistic sine map. *IET Image Processing,* 14(11), 2310-2320.

Zhong, Y.-R., Liu, H.-Y., Sun, X.-Y., Lan, R.-S., ve Luo, X.-N. (2018). *Image encryption using 2D sine-piecewise linear chaotic map.* Paper presented at the 2018 international conference on wavelet analysis and pattern recognition (ICWAPR), DOI: 10.1109/ICWAPR.2018.8521240.

Zhou, K., Xu, M., Luo, J., Fan, H., ve Li, M. (2019). Cryptanalyzing an image encryption based on a modified Henon map using hybrid chaotic shift transform. *Digital Signal Processing,* 93, 115-127.

Zhou, N., Wang, Y., ve Wu, J. (2011). Image encryption algorithm based on the multi-order discrete fractional Mellin transform. *Optics communications,* 284(24), 5588-5597.

Zolfaghari, B., ve Koshiba, T. (2022). Chaotic Image Encryption: State-of-the-Art, Ecosystem, and Future Roadmap. *Applied System Innovation,* 5(3), 57.

ÖZGEÇMİŞ

Duygu GÜVENOĞLU

Eğitim

Yüksek Lisans	2023	Maltepe Üniversitesi, Lisansüstü Eğitim Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı
Lisans	2010	Maltepe Üniversitesi, Mühendislik ve Doğa Bilimleri Fakültesi Bilgisayar Mühendisliği
Önlisans	2007	İstanbul Ticaret Üniversitesi, Meslek Yüksekokulu, Bilgisayar Teknolojisi Ve Programlama

İş/İstihdam (Varsa)

Yıl	Görev
2022	Yazılım Mühendisi (Bilmed Bilgisayar ve Yazılım A.Ş.)
2023	Veri Yönetim Ofisi Uzmanı (Bupa Acıbadem Sigorta)

Mesleki Birlik/Dernek Üyelikleri (Varsa)

Yıl	Kurum
-	-

Alınan Burs ve Ödüller (Varsa)

Yıl	Burs/Ödül
-	-

Yayınlar ve Diğer Bilimsel/Sanatsal Faaliyetler

1) Atasever, V., Arslan, D., Güvenoğlu, E. (2010). Mobil cihazlarda online görüntü işleme yazılımının geliştirilmesi. Akademik Bilişim Konferansı, Muğla.
2) Arslan, D., Atasever, V., Güvenoğlu, E., Erdoğan, Ş. Z. (2010). Çizgi Barkod Sistemleri ve HCCB Barkod Sisteminin Karşılaştırılması. Akademik Bilişim Konferansı, Muğla.
3) Atasever, V., Arslan, D., Erdoğan, Ş. Z. (2010). Tag Teknolojisi Kullanarak E-Kupon Sisteminin Geliştirilmesi. Çankaya Üniversitesi Mühendislik ve Teknoloji Sempozyumu, 2010, Ankara.