Araştırma Makalesi

MANDELBROT VE LOJİSTİK KAOTİK HARİTA KULLANILARAK GÖRÜNTÜ ŞİFRELEME

Gülseren KİBAR[†], Mustafa Cem KASAPBAŞI[††]

[†] İstanbul Ticaret Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Ana Bilim Dalı, İstanbul, Türkiye

[††]İstanbul Ticaret Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Ana Bilim Dalı, İstanbul, Türkiye

gulserennkibar@gmail.com, mckasapbasi@ticaret.edu.tr

0000-0001-9413-658X, 0000-0001-6444-6659

Atıf/Citation: KİBAR, G., KASAPBAŞI, M. C., (2022). Mandelbrot ve Lojistik Kaotik Harita Kullanılarak Görüntü Şifreleme, Journal of Technology and Applied Sciences 5(2), s. 79-95, DOI: 10.56809/icujtas.1150309

ÖZ

Son yıllarda, görüntü şifreleme popüler ve önemli bir araştırma alanı olmuştur. İnternet ve ağlar üzerinden iletişime olan bağımlılığın gün geçtikçe artmasıyla birlikte, verilerin iletimi güvenlik ihlaline karşı açık hale geliyor. Bu güvenlik ihlallerine karşı en iyi çözümlerden biri de verinin şifrelenmesidir. Günümüzde kullanılan geleneksel algoritmalar, düşük güvenlik seviyesi göstermesi sebebiyle kaos tabanlı kripto sistemler fazlasıyla ilgi çekici hale gelmiştir. Buraya olan yoğun ilgiden sonra çeşitli kaotik haritalar kriptografi alanına kazandırılmıştır. Eski şifreleme yöntemlerinin kullanılmasıyla ortaya çıkan düşük güvenlik seviyesi problemi kaos şifrelemesi kullanılarak çözülmüştür. Bunun yanı sıra kaos şifrelemede anahtarın rastgeleliğinin ve boyutunun büyüklüğünün de görüntü şifrelemedeki önemi ortaya çıkmıştır. Bu araştırma makalesi görüntüleri işlemek için çeşitli türleri olan kaotik haritalar ile Mandelbrot fraktallarını içeren yeni bir hibrit şifreleme algoritması sunmaktadır. Bunun sebebi fraktal görüntülerin rastgeleliğinin fazla olması nedeniyle, şifreleme için güçlü bir anahtar olarak kullanılabilmesidir. Araştırmacıların çalışmaları sonucu literatürde de yer alan pek çok kaotik metot ortaya çıkmıştır. Makalede de bunlardan birisi olan Lojistik kaotik harita metodunda oluşturulan anahtar ile Mandelbrot fraktal setlerinden elde bir başka anahtarın işleme tabi tutularak ortaya çıkan anahtar ile görüntü şifrelemesi yapılmıştır. Ayrıca makalede bu kaotik harita ile fraktalların birlikte kullanılmasının sonucu elde edilen şifreli görüntülerin analizi ve karşılaştırılması yapılmıştır. Bu analiz yapılırken oluşturulan şifreli görüntünün ve görüntünün orijinal halinin görsel değerleri karşılaştırılarak algoritmanın başarısı PSNR, Entropi, SSIM, MSE, Korelasyon Katsayısı, Histogram Analizi, NPCR ve UACI yöntemleri ile ölçülmüştür.

Anahtar Kelimeler: Kaos Teorisi, Kaotik Görüntü Şifreleme, Lojistik Harita, Mandelbrot Set, Performans Analizi

IMAGE ENCRYPTION USING MANDELBROT AND LOGISTIC CHAOTIC MAP

ABSTRACT

In recent years, image encryption has been a popular and important research area. With the increasing dependence on communication over the Internet and networks, the transmission of data becomes vulnerable to security breaches. One of the best solutions against these security breaches is data encryption. Chaos-based cryptosystems have become very interesting because of the low security level of traditional algorithms used today. After the intense interest here, various chaotic maps have been brought to the field of cryptography. The low security level problem caused by using old encryption methods has been solved by using chaos encryption. In addition, the importance of the randomness and size of the key in image encryption has emerged in chaos encryption. This research paper presents a new hybrid encryption algorithm for processing images, including several types of chaotic maps and Mandelbrot fractals. This is because fractal images are so random that they can be used as a strong key for encryption. As a result of the studies of the researchers, many chaotic methods have emerged in the literature. In the article, image encryption was made with the key created in the logistic chaotic map method, which is one of them, and another key obtained from the Mandelbrot fractal sets was processed. In addition, the analysis and comparison of the encrypted images obtained as a result of the use of this chaotic map

Geliş/Received : 28.07.2022
Gözden Geçirme/Revised : 02.08.2022
Kabul/Accepted : 05.08.2022

and fractals were made in the article. The success of the algorithm was measured by PSNR, Entropy, SSIM, MSE, Correlation Coefficient, Histogram Analysis, NPCR and UACI methods by comparing the visual values of the encrypted image and the original state of the image created during this analysis.

Keywords: Chaos Theory, Chaotic Image Encryption, Logistic Map, Mandelbrot Set, Performance Analysis

1. GİRİŞ

Günümüzde multimedya teknolojisinin yaygın olarak kullanılmasıyla birlikte, dijital görüntü paylaşımı en fazla kullanılan içerik biçimlerinden biri halini almıştır. Paylaşımın güvenliğini sağlamak için görüntü şifreleme etkili bir teknik olarak kullanılır. Ancak görüntü iletiminin ve saklanmasının güvenli bir şekilde olması için kriptografi yaklaşımına ihtiyaç duyulur. Kriptografi, verilere yetkisiz erişimden kaçınmak için kullanılan bir tekniktir (Menezes ve ark, 1996). İki ana bileşeni vardır; a) Şifreleme algoritması ve b) Anahtar (Stallings, 2006). Bazen, şifreleme için birden fazla anahtar da kullanılabilir. Piyasada DES, AES, TDES ve RSA gibi bir dizi geleneksel kriptografik algoritma mevcuttur. Geleneksel şifreleme algoritmalarının çoğu, metin verileri veya ikili veriler için kullanılır ve yüksek hesaplama karmaşıklığına sahiptir. Multimedya görüntüleri özel kodlama yapılarına ve büyük hacimli verilere sahip olduğundan, geleneksel şifreleme algoritmasının gerçek zamanlı gereksinimleri karşılaması zordur ve veri formatını değiştirebilirler.

Şifreleme algoritmasının güvenli olması için algoritmada kullanılan şifrenin karmaşıklık, rastgelelik ve yayılma gibi kriptografi alanındaki temel koşulları karşılaması beklenir. Kaotik sistemler, rastgeleliğin avantajını kullanmakla birlikte başlangıç koşullarına daha fazla hassasiyet sunar, bu nedenle kaba kuvvet ve istatistiksel saldırılara direnmek için çok geniş bir alan sunar. Sayısal görüntülerin doğası gereği fazla verisi, komşu pikseller için yüksek benzerliği ve piksel özniteliğinde küçük bir değişikliğe karşı daha az duyarlılığı olduğundan, sayısal görüntülerin güvenlik gereksinimleri, kaos tabanlı şifreleme yöntemlerinin önemini artırmaktadır (Chen ve ark, 2004).

Bu çalışmada, mevcut kaotik harita şemalarına katkıda bulunmak için Fraktal-Kaos hibrit görüntü şifreleme algoritması ele alınmıştır. Literatürde yer alan görüntüler kullanılarak performans metrikleri ve güvenlik analizleri yapıldığında teorik değerler elde edilmiştir. Bölüm 2'de görüntü şifrelemesi ile ilgili literatür taraması yapılmıştır. Bölüm 3'te Lojistik harita ve fraktal setin bir ön incelemesi yapılmıştır. Bölüm 4'te önerilen şifreleme yaklaşımı ayrıntılı olarak açıklanmıştır. Bölüm 5'te algoritmanın önceki çalışmalarda da yer alan güvenlik analizleri ve performans değerlendirmeleri sonuçları ile birlikte sunulmuştur. Tartışma kısmında, literatürde yer alan mevcut şifreleme yöntemleri ile önerilen yaklaşım sonucu elde edilen sonuçların karşılaştırması yapılmıştır. Son bölümde ise sonuçlara yer verilmiştir.

2. LİTERATÜR TARAMASI

Görüntü şifreleme hayatımızda önemli bir kavram haline geldiğinden bu konu ile ilgili önerilen birçok algoritma bulunmaktadır. Son yıllarda özellikle kaotik haritaların bu denli popülerliğinin artması sebebiyle farklı çalışmaların yapıldığı görülmektedir. Bunlara ilk olarak, görüntü şifresi ve çözülmesi için kaotik haritaları birleştirerek hibrit bir algoritma öneren çalışma (Shubo ve ark., 2009) örnek olarak verilebilir. Geliştirilen algoritmada iki kaotik sistem olan Lorenz ve Baker haritaları kullanılır. Karıştırma ve yayılma aşamasında piksel konumları ve değerleri kaotik sistemlere dayalı olarak değiştirilir. Her iki aşama için ayrı anahtarlar üretilip kullanılarak görüntü şifreleme yapılır. Şifreli görüntünün çözülmesi aşamasında ise yapılan işlemlerin tersi yapılarak orijinal görüntü elde edilir. Birleştirilmiş kaotik haritalara dayanan deneysel sonuçlar, önerilen yöntemin etkinliğini onaylar ve geniş anahtar alanı ve yüksek seviyeli güvenliğin avantajlarını gösterir. İnternet üzerinden güvenli iletimde pratik olarak kullanım için uygun olduğunu belirtir.

Kaotik haritanın kullanıldığı bir görüntü karıştırma algoritmasının önerildiği makalede (Dong ve ark., 2010) lojistik harita metodu kullanılarak piksellerin bir karıştırma matrisi aracılığı ile değiştirilmesi sağlanır. Önerilen algoritma kaotik haritalamaya dayalı diğer algoritmalara göre hem basit hem de verimli olması sebebiyle avantajlıdır. Makaledeki değerlendirme ise karıştırma derecesi ile karıştırma sayıları arasındaki ilişkiyi gösteren bir korelasyon algoritması kullanılarak yapılır.

W7 ve piksel karıştırma birlikte kullanılarak yeni bir görüntü şifreleme şeması önerilen makalede (Jolfaei ve Mirghadri, 2010), W7'nin gizli anahtar olarak kullanılmasının yanı sıra permütasyon işlemi için kaotik Henon haritası da kullanılır. Dikey ve yatay permütasyonlar aracılığı ile piksellerin karıştırılması işlemi yapılır. Piksel

korelasyonlarının karıştırma işlemi kullanılarak dağıtılması sağlanır. Önerilen şema uzun bir anahtar alana sahiptir; bu nedenle kaba kuvvet ve istatistiksel saldırılara karşı iyi direnç gösterir.

El-Alfy ve arkadaşları tarafından yapılan çalışmada genetik bir operatör ve bitişik piksellerin korelasyon katsayısını minimuma indirmek için kaotik harita kullanılan çalışmanın dört adımı vardır. İlk olarak, şifreleme işlemi için kullanılan anahtarların dört farklı kaotik dizi oluşturması için Lojistik kaotik harita metodu kullanılır. İkinci adım olarak oluşturulan dört diziyi anahtar akışlara eşlemek için kullanılması üzerine niceleme çalışması yapılır. Üçüncü adımda görüntüyü karıştırma işlemini satır ve sütun bazında yapmak için çaprazlama metodu kullanılır. Sonrasında ise mutasyon aşaması gerçekleştirilir ve çaprazlama sonucu oluşan görüntü ile rastgele görüntü arasında XOR işlemi uygulanarak şifreli görüntü elde edilir (El-Alfy ve Al-Utaibi, 2011).

Yapılan başka bir çalışmada (Zhao ve ark, 2014) kaotik haritaların avantajları göz önüne alınarak kaos tabanlı bir görüntü şifreleme sistemi önerilir. Önerilen sistemde kullanılan kaotik harita Arnold haritasıdır. Permütasyon ve yer değiştirme metotları kullanılırken birçok yenileme turu yerine bir kez permütasyon ve yer değiştirme prosedürlerine dayandırılır. Şifreleme hızında artırım yapmak için de piksel piksel çalışmak yerine satır ve sütun bazında yer değiştirme işlemi yapılır. Önerilen algoritmanın performansını analiz etmek için anahtar uzay analizi, histogram analizi, duyarlılık analizi vb. gibi metrikler kullanılır. Sonuç olarak algoritma etkili sonuçlar gösterir ve doğası gereği güvenlidir.

AES'in literatüre de bakıldığı zaman yüksek hesaplama maliyeti, düşük güvenliği, öngörülebilir modeller gibi birçok dezavantajları olması sebebiyle bu metodolojinin geliştirilmesi önerilir (Abdulgader ve ark., 2015). Önerilen algoritma, bu dezavantajları azaltmak için kaotik bir harita ve bir XOR operatörü kullanılması yönünde geliştirilir. Önerilen yöntemin testi için literatürde de bulunan birkaç görüntü kullanılarak elde edilen sonuçlara bakıldığında pikseller arasında çok küçük korelasyon katsayıları, şifreleme hızının artması ve güvenliğinin AES algoritmasına göre artığı gözlemlenir. Makaleden çıkarılan sonuca göre algoritma, görüntü şifreleme alanında uygulanacak AES algoritması için iyi bir adaptasyon gösterir.

Verma ve arkadaşları tarafından yapılan çalışmada kriptosistem, karıştırma ve yayılma olarak iki aşamadan oluşur. Dış saldırılara karşı güvenliği artırmak için algoritmanın karmaşıklığının artırılması gerekçesi ile karmaşık kaotik haritalar seçilir. Görüntü şifreleme yapılırken ilk olarak karıştırma aşamasında, piksel konum permütasyonu kaotik sistemler kullanılarak gerçekleştirilir. İkinci aşama olarak piksel değeri difüzyonu gerçekleştirilir. Başlangıç koşulları ile birlikte kullanılan kontrol parametreleri algoritmanın iki aşamasında da gizli anahtar görevindedir. Algoritmanın karmaşıklığını artırarak güvenliği sağlamak için iki aşamada da ayrı anahtarlar kullanılır. Şifreyi çözme işlemi ise görüntüyü şifrelerken yapılan işlemlerin tersinin yapılması ve aynı anahtarların kullanılması ile gerçekleşir (Verma ve Jain, 2016). Testler sonucu şemanın etkinliğine bakıldığında yüksek güvenlik sağladığı gözlemlenir.

Çok gizli görüntüler için güvenli bir Boole tabanlı paylaşım şeması ele alınan makalede (Mary ve ark., 2018) birden fazla gizli görüntü, XOR ve DNA'ya dayalı olarak kodlanır. İlk adım, XOR'u gizli görüntüler üzerinde sırayla yürüterek bunun sonucunda ön paylaşım matrisleri setini elde etmektir. Bu matrislerin değerleri DNA dizilerine kodlanır. Bir matristeki anahtarın oluşturulması için karşılık gelen DNA'nın ondalık değerini içeren DNA sözlüğü tutulur. Sonuç olarak görüntüler ve anahtar matris arasında bir XOR işlemi gerçekleştirilerek görüntü şifreleme işlemi tamamlanır.

Hiperkaotik haritaya ve permütasyon-difüzyon mimarisine dayanan yeni bir renkli görüntü şifreleme şeması önerilen makalede (Cheng ve ark., 2019) R, G, B bileşenlerinin karıştırılmasıyla gerçekleştirilen bir blok permütasyonu kullanılır. Hiperkaotik sistem tarafından üretilen anahtarlar pikselleri dağıtmak için kullanılır, bu sebeple üç renk bileşeni birbirini etkiler. Daha sonra difüzyon sürecinde, G bileşeni ters sırada dağıldığı için son piksel değiştirilse dahi tamamen farklı iki şifreli görüntü elde edilebilir. Elde edilen deneysel sonuçlara bakıldığında, algoritmanın diğer kaos tabanlı renkli görüntü şifreleme algoritmalarına kıyasla istatistiksel ve kaba kuvvet saldırılarına karşı daha dirençli olmasının yanı sıra, daha büyük anahtar alanına sahip olduğu gözlemlenir.

Multimedya teknolojisinde kullanılan görüntülerden ziyade tıbbi görüntüler için yeni bir kaos tabanlı şifreleme şeması önerilen makale (Belazi ve ark, 2019) kaos ve DNA hesaplanmasının birleşimine dayanır. Burada oluşturulan senaryo; kaos ve DNA hesaplamasının bir kombinasyonundan sonra permütasyon-yer değiştirme-difüzyon yapısını takip eder. Önerilen algoritmanın her bir turu, blok tabanlı permütasyon, piksel tabanlı yer değiştirme, DNA kodlaması, bit düzeyinde yer değiştirme, DNA kodunun çözülmesi ve bit düzeyinde difüzyon olmak üzere altı adımı içerir. Son şifrelenmiş görüntü, yeni gizli anahtarlar aracılığı ile önceki adımlar bir kez tekrarlanarak elde edilir. Yapılan güvenlik analizleri sonucu, önerilen şemanın her türlü saldırıya karşı yeterince

sağlam olduğu doğrulanır. Bunun yanı sıra düşük karmaşıklığı, gerçek zamanlı ve güvenli görüntü uygulamaları için yüksek potansiyel içerdiğini gösterir.

Tıbbi görüntülerin bilgi aktarımı yapılırken güvenliğini sağlamak için Hermite kaotik sinir ağına dayalı bir algoritma öneren makalede (Han ve ark, 2020), kaotik diziler oluşturulması için lojistik harita kullanılır. Oluşturulan kaotik diziler Hermite kaotik sinir ağının eğitilmesinde rol oynar. Sinir ağı iki anahtar akışı üreterek görüntülerin şifrelenmesini sağlar. Yapılan incelemeye göre bu algoritma çok etkilidir, saldırılara karşı dirençlidir, ayrıca güçlü anahtar duyarlılığına, geniş anahtar alanına sahiptir ve tıbbi görüntülerin güvenliğini büyük ölçüde artırır.
Ma ve arkadaşları tarafından, iki döngü şifreleme işlemi içeren, seriye dayalı, düz metinle ilgili ve yüksek hızlı kaotik bir görüntü şifreleme modeli önerilir. Blok parite kontrolü, şifrelemenin ilk döngüsü sırasında yapılırken, ikinci döngüde tekrarlı kodlama yapılır. Anahtar alanı, anahtar duyarlılığı, diferansiyel saldırı direnci yeteneği, korelasyon katsayısı ve bilgi entropisini içeren ayrıntılı performans değerlendirmeleri, önerilen şemanın iyi rastgelelik, geniş anahtar alanına sahip olduğunu gösterir (Ma ve ark., 2019).

2019 yılında Li ve arkadaşları, saçılma-karışıklık sistemlerini ve bellek hücresel otomata görüntü şifrelemesini entegre eden verimli bir şifreleme sistemi sunmaktadır (Li ve ark., 2019). Zhang ve ark. (2019)'da, hiper-kaotik yöntemin sözde rastgeleliği ile başlangıç değerlerinin duyarlılığını birleştiren yeni bir görüntü şifreleme tekniği önerilir. Liu ve ark. (2019)'da adaptif DNA ve 4-D bellek hiper-kaotik tabanlı bir renkli görüntü şifrelemesi önerilir. Huang ve ark. (2019)'da, klasik 2B Lojistik, Sinüs ve Kosinüs haritalarına dayanan 2B Lojistik-Sinüs-Kosinüs haritası sunulmaktadır.

Bu makale, fraktal setler ile kaosun birleşiminden oluşan algoritma önerdiği için literatürdeki şifreleme algoritmalarından farklıdır. Literatüre bakıldığında genel olarak farklı kaotik haritaların birleştirilerek kullanıldığı gözlemlenirken burada fraktal setlerin kullanılması ile bir algoritma oluşturulmuştur. Fraktal setler, görüntü şifrelemede kullanılacak anahtarların boyutu genişlerken dışarıdan gelecek olan kaba kuvvet ve istatistiksel saldırılara karşı daha dirençli olacaktır.

3. MATERYAL VE METOT

Bu bölüm, çalışmada kullanılan kaotik haritayı ve fraktal setleri kısaca gözden geçirmektedir.

3.1. Lojistik Kaotik Harita

Kaotik teori, yoldaki hava, iklim ve trafik gibi başlangıç koşullarına fazlası ile duyarlı doğal ve yapay sistemlerin dinamik davranışını dikkate alan bir matematik alanıdır (Patel ve ark, 2020). Kaotik matematiksel model kullanılarak analiz edilebilir veya yineleme grafikleri kullanılarak da yapılabilir. Kaos teorisi, nöroloji, kardiyoloji, kontrol ve devre teorisi, hava tahmini vb. gibi gelişen teknolojiler için kullanılır. Kaosta, başlangıç koşullarındaki küçük bir değişiklik bile tamamen ilişkisiz bir sıralamaya yol açabilir. Kaos fonksiyonunun şifreleme için kullanılabileceği ve iyi sonuçlar verdiği söylenmiş ve literatürde yapılan çalışmalarla kanıtlanmıştır.

Lojistik fonksiyon, başlangıç koşulları ile yüksek hassasiyetle değişen ve periyodik olmayan sahte rastgele dizili üretilen kaos fonksiyonlarından biridir ve eğer doğru çatallanma parametresi 'r' seçimi dikkate alınırsa, tamamen öngörülemez olacaktır. Kaotik teoriyi kullanarak görüntü şifreleme uygulamak basit, hesaplama açısından daha hızlıdır (Patel ve ark, 2020). Lojistik kaotik harita aşağıdaki denklem ile ifade edilebilir.

$$x_{n+1} = r\, x_n(1 - x_n), x_n \in [0, 1] \quad (1)$$

3.2. Mandelbrot Fraktal Setleri

Fraktallar (Pickover, 2001), tüm ölçeklerde aynı derecede düzensizliğe sahip olan düzgün olmayan geometrik şekillerdir. Benoit Mandelbrot, 1979'da Mandelbrot kümesi olarak bilinen çok karmaşık bir yapı üzerinde çalışmıştır (Mandelbrot, 1982). Mandelbrot kümesinin tanımı (Crownover, 1995)'de şu şekilde verilmiştir: "Mandelbrot kümesi, karmaşık ikinci dereceden polinom $z_{n+1} = z_n^2 + c$'nin yinelemesi altında 0 yörüngesinin sınırlı kaldığı karmaşık düzlemdeki c değerleri kümesidir."

Fraktal görüntüler, güvenilir bir şifreleme sistemi tasarlamaya uygun rastgelelik özelliğini sergiler. Fraktal tabanlı kriptosistem asal sayı yerine karmaşık bir sayı kullanılarak tasarlandığından, anahtar üretimleri, karmaşık sayılar kullanılarak aritmetik olarak gerçekleştirilir. Fraktalın kaotik doğası, anahtar değerin başlangıç değerine karşı hassasiyetine yol açar, yetkisiz kullanıcı tarafından doğru bir anahtar üretilmesini zorlaştırarak şifrenin

kırılmasını zorlaştırır. Anahtar olarak fraktal kullanmanın ek bir avantajı, genellikle bir saldırganın anahtarı bulmak için yapması gereken tahmin sayısını etkileyen anahtar boyutudur, örneğin kaba kuvvet saldırısı, yani bir çarpışma saldırısının uygulanabilirliğini belirler. (Negi, 2016).

4. ÖNERİLEN ŞİFRELEME METODOLOJİSİ

Bu çalışmada görüntü şifrelemede kullanılacak anahtarı oluşturmak için Mandelbrot fraktal seti ve bir Lojistik kaotik harita metodundan yararlanılmıştır. Görüntünün iki metodolojiden üretilen anahtarlarının XOR işlemine tabi tutulmasından sonra sütun bazında difüzyon işlemi gerçekleştirilmiştir. Bu işlemler belirlenen iterasyon sayısı kadar tekrarlanarak şifrelenmiş görüntü elde edilmiştir.
Şifre çözme, şifreleme işlemlerinin son adımından ilk adımına kadar ters sırada uygulandığı bir prosedürdür.

4.1. Şifreleme İşlemi

Şifreleme işlemi aşağıda anlatılan adımlardan oluşmaktadır. Görüntü şifreleme işlemi Algoritma 1'de verilmiştir.

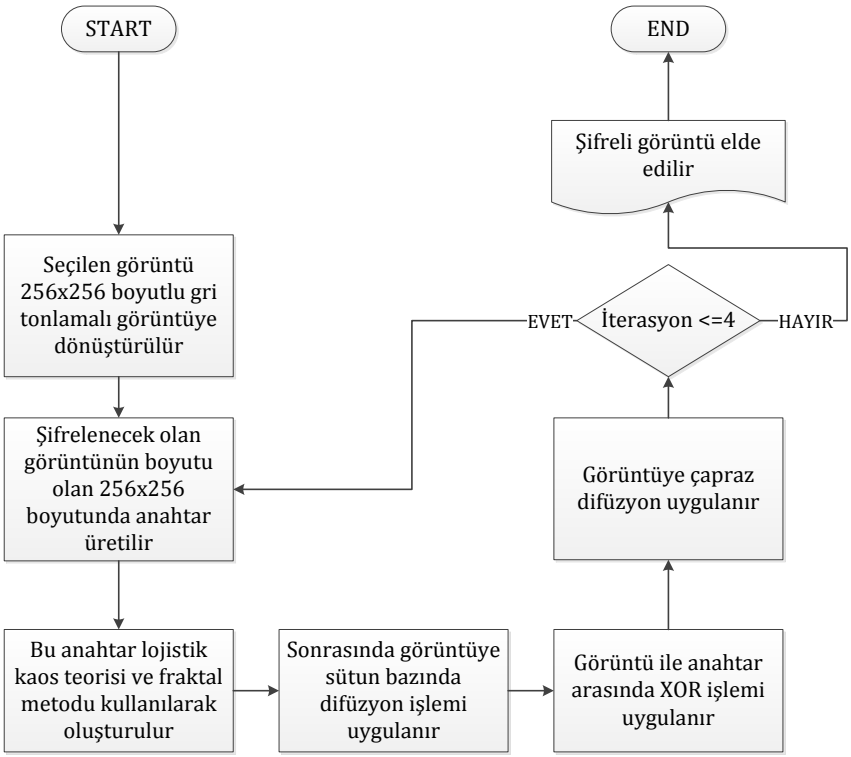
Algoritma 1 Şifreleme algoritması sözde kodu

Girdi: I_P WxH boyutunda bir görüntü
İterasyon sayısı (varsayılan 4)

Çıktı: I_C 256x256 boyutunda şifrelenmiş görüntü

```
IP = resize(IP, [256 256])
IP = rgb2gray(IP)

IC = IP
for j = 1: iterasyon sayısı
    IC = EncryptedVertical(IC, j);
    IC(1, 1) = bitxor(IC(1,1), IC(256,256));
    IC = EncryptedVertical(IC, j+1);
    xx = bitxor(IC(1,1), IC(256,256));
    IC = EncryptedCross(IC, j);
    IC(1, 1) = xx;
end for

function EncryptedVertical(image, keyParameter)
    EncryptedImage = image;
    finalKey = keyCreator(image, 3.991461146114611);

    for col = 1:1: sütun sayısı
        if(mod(col,2)~=0)
            f–or row = 1:1: satır sayısı
                EncryptedImage = bitxor(EncryptedImage(row, col), EncryptedImage(row-1, col));
             end for
        else
            for row2 = satır sayısı:-1:1
                EncryptedImage = bitxor(EncryptedImage(row2, col), EncryptedImage(row2-1, col));
            end for
        end if
    end for

   EncryptedImage = bitxor(EncryptedImage, finalKey);

function keyCreator(image, r)
    for col = 1:1: sütun sayısı
        for row = 1:1: satır sayısı
            X1(row,col)= r*x*(1-x);
            x=  X1(col,j);
           key(row,col)=mod(floor(x*10^15),256); %logistic map
        end for
```

```
    end for

    for row = 1:1: satır sayısı
        for col = 1:1: sütun sayısı
            finaloutput{row,col} = dec2bin(key(row,col), 8);
        end for
    end for

    mandel = mandelbrot(image);

    for row = 1:1: satır sayısı
        for col = 1:1: sütun sayısı
            finaloutput2{row,col} = dec2bin(mandel(row,col), 8);
        end for
    end for

    finalKey = bitxor(finaloutput, finaloutput2);

function EncryptedCross(image, keyParameter)
    EncryptedImage = image;

    for row = 1:1: sütun sayısı/ keyParameter
        for col = 1:1:satır sayısı
            EncryptedImage((sütun sayısı + 1)-row,(satır sayısı + 1)-col) = EncryptedImage(row,col);
            EncryptedImage(row,col) = EncryptedImage((sütun sayısı + 1)- row,(satır sayısı + 1)-col);
        end for
    end for
```

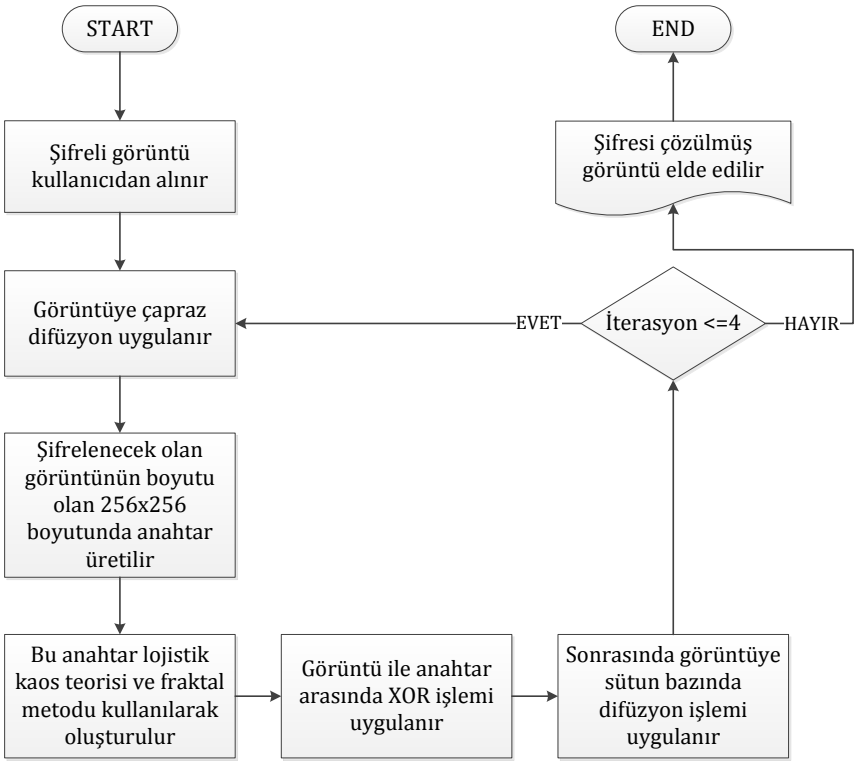


Şekil 1. Şifreleme algoritmasının akış şeması

Şekil 1'de önerilen şifreleme algoritmasının akış şeması görülmektedir.

4.2. Şifre Çözme İşlemi

Şifre çözme, şifreleme işlemlerinin son şifre adımından birinciye kadar ters sırada gerçekleştirildiği bir prosedürdür. Şifre çözme işlemi Algoritma 2'de verilmiştir.



Şekil 2. Şifre çözme algoritmasının akış şeması

Şekil 2'de önerilen şifre çözme algoritmasının akış şeması görülmektedir.

Algoritma 2 Şifre çözme algoritması sözde kodu

Girdi: I_C 256x256 boyutunda şifrelenmiş görüntü
İterasyon sayısı (varsayılan 4)

Çıktı: I_P 256x256 boyutunda şifresi çözülmüş görüntü

```
I_C = I_P
for j = 1: iterasyon sayısı
    I_C(1, 1) = xx;
    I_C= DecryptedCross(Ic, j);
    xx = bitxor(I_C(1,1), I_C(1,256));
    I_C= DecryptedVertical(Ic, j+1);
    I_C(1, 1) = bitxor(Ic(1,1), Ic(1,256));
    I_C= DecryptedVertical(Ic, j);
end for

function DecryptedVertical(image, keyParameter)
    DecryptedImage = image;
    finalKey = keyCreator(image, 3.991461146114611);
    DecryptedImage = bitxor(DecryptedImage, finalKey);

    for col = 1:1: sütun sayısı
        if(mod(col,2)~=0)
```

```
            for row = 1:1:satır sayısı
                DecryptedImage = bitxor(DecryptedImage(row, col), DecryptedImage(row-1, col));
             end for
        else

            for row2 = satır sayısı:-1:1
                DecryptedImage = bitxor(DecryptedImage(row2, col), DecryptedImage(row2-1, col));
            end for
        end if
    end for

function DecryptedCross(image, keyParameter)
    DecryptedImage = image;

    for row = 1:1: sütun sayısı / keyParameter
        for col = 1:1:satır sayısı
            DecryptedImage ((sütun sayısı + 1)-row,( satır sayısı + 1)-col) = DecryptedImage (row,col);
            DecryptedImage (row,col) = DecryptedImage ((sütun sayısı + 1)- row,( satır sayısı + 1)-col);
        end for
    end for
```

5. PERFORMANS ANALİZİ

Bu bölüm, önerilen şifreleme sisteminin güvenlik seviyesini ve hesaplama yükünü göstermek için gerçekleştirilen çeşitli güvenlik analizlerinin deneysel sonuçlarını sunar. İyi bilinen bir veri tabanından (https://sipi.usc.edu/database/) elde edilen bir dizi test görüntüsü üzerinde yürütülen ortak testler, aşağıdaki alt bölümlerde detaylandırılmış ve tartışılmıştır. Mevcut durumda, önerdiğimiz algoritma gri ölçekli görüntülerle sınırlıdır, ancak önerilen şifreleme sistemi renkli görüntüler üzerinde çalışmak üzere kolayca uyarlanabilir (Yavuz, 2021).

5.1. Anahtar Alan Analizi

Anahtar, belki de her şifreleme sisteminin en temel yönüdür. Şifreleme algoritmasının güvenilir olma ölçütü anahtarının büyüklüğü ile ölçülür. Anahtar alanının boyutu, şifreleme sisteminde mevcut olan şifreleme/şifre çözme anahtar çiftlerinin sayısıdır (Akhshani ve ark, 2012). Anahtar alanın boyutu ise literatürde yer alan çalışmalarla da ispatlandığı gibi $2^{128'}$den büyük olmalıdır. Günümüzün hesaplama gücü seviyelerini göz önünde bulundurduğumuzda, kapsamlı anahtar aramasına dayanmak için sistemin daha büyük bir anahtar alanına sahip olması daha iyidir (Yavuz, 2021). Yapılan hesaplamalara göre anahtar boyutu $2^{128'}$den büyük bir değer bulunmuştur.

5.2. Bilgi Entropi Analizi

Bilgi entropisi, diğer adıyla Shannon entropisi (Yavuz, 2021), sistemdeki belirsizliklerin derecesini ifade etmek için tanımlanır. Bunu görüntü bilgisinin belirsizliklerini ifade etmek için de kullanabiliriz (Soni A., Acharya A. K, 2012). Görüntü bilgisine gelince, entropi, gri tonlamalı görüntüde bulunan yoğunluk seviyelerinin dağılımını ölçer. Rastgele bir değişkenin Shannon entropisi (gri tonlamalı görüntü) aşağıdaki gibi tanımlanabilir (Yavuz, 2021).

$$H(X) = H(P_0, \dots, P_{n-1}) = -\sum_{i=0}^{L-1} P_i \, log_2 P_i \tag{2}$$

$$P_i = \Pr(X = x_i) \tag{3}$$

Burada L, gri tonlama düzeylerinin (yoğunluklarının) sayısıdır, P_i, $X = x_i$ olasılığını temsil eder ve x_i, L piksel değerlerinin i. olası X değerini temsil eder. 8 bitlik gri tonlamalı görüntü için 256 yoğunluk düzeyi olduğundan, L yoğunluk düzeylerinin gri tonlamalı görüntüsü için Shannon entropi puanının teorik maksimumu, her yoğunluk düzeyinin eşit olasılıkla dağıtılması koşuluyla $H(X)=\log_2 L = 8$'dir. Bu, görüntünün her bir yoğunluk seviyesinin aynı olasılığı paylaştığı tamamen tek tip bir dağılıma sahip olduğu ideal durumdur. Bu nedenle, daha yüksek entropi puanı, yoğunluk değerlerinin daha düzgün dağılımını gösterir, bu da bir görüntünün pikselleri arasında daha düzensiz durum anlamına gelir (Niyat ve ark, 2017).

Tablo 1. Düz/Şifreli/Şifresi çözülmüş görüntülerin global entropi sonuçları

	Orijinal Görüntü Global Entropisi	**Şifreli Görüntü Global Entropisi**	**Şifresi Çözülmüş Görüntünün Global Entropisi**
Baboon	7.247873802	7.997502631	7.248267696
House	6.496137130	7.997254276	6.496451250
Couple	6.420700137	7.997466783	6.421130147

Tablo 1, analizde kullanılan düz, şifreli ve şifresi çözülmüş görüntülerin global entropi sonuçlarını sunmaktadır. Tablodaki sonuçlar 256x256 boyutundaki test görüntülerini içerir. Elde edilen global entropi sonuçları incelendiğinde, önerilen şifreleme algoritmasının entropi değerleri teorik üst sınır olan 8'e yakın ve yüksek oranda rastgele şifreli görüntüler ürettiğini göstermektedir.

Global Shannon entropi ölçüsü, gerçek rastgeleliği kanıtlamak için yeterli değildir. Bazı durumlarda, üretilen şifreli görüntülerin rastgeleliğini doğrulamak için yalnızca bu metriği kullanmak yanıltıcı olabilir. Örnek verecek olursak, biri algılanabilir ve diğeri rastgele benzeri olan iki görüntü, aynı Global Shannon entropi değerlerine sahip olabilir (Yavuz, 2019). Bu sebeple, mutlaka gerçek rastgeleliğin kanıtı olarak kullanılamaz. Bunun yerine, şifreli görüntülerin gerçek rastgeleliğini kanıtlamak için Yerel Shannon entropi testi kullanılır. Rastgele seçilmiş bir dizi örtüşmeyen bloğun yerel entropi değerlerinin ortalamasının alınması, aşağıdaki gibi tanımlanan Yerel Shannon entropi metriğini (Wu ve ark, 2013) verir:

$$\overline{H_{k,T_B}}(S) = \sum_{i=1}^{k} \frac{H(S_i)}{k} \tag{4}$$

Burada T_B, yerel bloktaki piksel sayısını temsil eder ve k, S_i ile gösterilen rastgele seçilen blokların sayısını sembolize eder. T_B ve k parametreleri, önem düzeyi α ile birlikte ideal yerel entropi değerini belirler.

Tablo 2. Düz/Şifreli/Şifresi çözülmüş görüntülerin Yerel Shannon entropi sonuçları

	Orijinal Görüntü Yerel Entropisi		**Şifreli Görüntü Yerel Entropisi**		**Şifresi Çözülmüş Görüntünün Yerel Entropisi**	
	$\mathbf{h_{sol}}^*$	$\mathbf{h_{sağ}}^*$	$\mathbf{h_{sol}}^*$	$\mathbf{h_{sağ}}^*$	$\mathbf{h_{sol}}^*$	$\mathbf{h_{sağ}}^*$
Baboon	7.244806723	7.134224429	7.988449909	7.989494235	7.245369226	7.134775792
House	5.631226771	6.435040916	7.988781716	7.988180923	5.632015502	6.436073288
Couple	5.898468014	6.396219959	7.988281324	7.989133980	5.899108183	6.396411857

Tablo 2'de orijinal, şifreli ve şifresi çözülmüş görüntülerin yerel entropi değerleri sunulmuştur. Tüm yerel entropi sonuçları kritik değerler α = 0.001 anlamlılık düzeyi için önerilen algoritmanın testi başarıyla geçtiği ifade edilebilir.

5.3. Diferansiyel Saldırı Analizi (NPCR/UACI)

Diferansiyel saldırıya direnmek için, güvenli bir şifreleme sistemi, düz görüntüdeki herhangi bir küçük değişikliğin, şifreli görüntüler arasındaki fark üzerinde önemli etkilere neden olmasını sağlamalıdır (Yin Q, Wang C, 2018). Yayılma ve karışıklık özelliklerine sahip olmayan bir şifreleme algoritması, farklı saldırılara karşı savunmasız olacaktır (Akhshani ve ark, 2012). Şifreleme yeteneğini değerlendirmek için Piksel değişim hızı (NPCR) ve birleşik ortalama değişim yoğunluğu (UACI) kullanılır (Xu ve ark, 2019). Literatüre bakıldığı zaman NPCR değerinin %99, UACI değerinin ise %33 civarı olması şifreleme algoritmasının dışarıdan gelecek

saldırılara karşı dirençli olduğunu gösterir (Menezes ve ark, 1996). İki farklı şifreli görüntü arasındaki NPCR ve UACI aşağıdaki gibi tanımlanır:

$$Diffp\big(A(i,j),B(i,j)\big) = \begin{cases} 1, & A(i,j) \neq B(i,j) \\ 0, & A(i,j) = B(i,j) \end{cases} \quad (5)$$

$$Diff(A,B) = \sum_{i=0}^{W-1}\sum_{j=0}^{H-1} Diffp(A(i,j),B(i,j) \quad (6)$$

$$NPCR = \frac{Diff(C_1,C_2)}{W.H}.100\% \quad (7)$$

$$UACI = \frac{1}{W.H}\sum_{i=0}^{W-1}\sum_{j=0}^{H-1}\frac{|C_1(i,j) - C_2(i,j)|}{255}.100\% \quad (8)$$

Burada C_1 ve C_2 sırasıyla düz görüntüyü ve biraz değiştirilmiş versiyonunu temsil eder. W ve H, görüntünün genişliğini ve yüksekliğini simgelemektedir.

Tablo 3. Şifreli görüntünün diferansiyel saldırı sonuçları

	UACI	**NPCR**
Baboon	33.656622195	99.468994141
House	33.208534390	99.493408203
Couple	33.044128418	99.429321289

Tablo 3'te çeşitli test görüntülerinden elde edilen UACI ve NPCR değerleri sunulmuştur. Yukarıda da bahsedildiği gibi NPCR ve UACI değerlerinin teorik değerlere yakın olduğu gözlemlenir. Bu durum da dışarıdan gelebilecek saldırılara karşı algoritmanın dirençli olduğunu gösterir.

5.4. Gürültü Girişim Analizi (PSNR/MSE)

Görsel değerlendirme analizi, iki görüntü için bileşenin ortalama kare farkının, herhangi iki görüntü arasında bulunabilecek maksimum ortalama kare farkına oranıdır. Orijinal görüntüden ve şifreli görüntüden türetilen PSNR değeri karşılaştırıldığında, daha düşük PSNR değeri, aralarındaki daha büyük farkı gösterir ve bu da sonuçta daha güvenli bir görüntü şifrelemesi anlamına gelir. Ortalama Kare Hatası (MSE), piksellerin 0 ile 255 arasında ifade edildiği orijinal ve şifreli görüntü arasındaki farkı ölçmek için kullanılan bir parametredir. MSE şu şekilde tanımlanabilir:

$$PSNR = 10.log\frac{255^2}{MSE}(dB) \quad (9)$$

$$MSE = \frac{1}{W.H}\sum_{i=0}^{W-1}\sum_{j=0}^{H-1}(I_P(i,j) - I_D(i,j))^2 \quad (10)$$

Burada I_P ve I_D, sırasıyla (orijinal) düz görüntüyü ve şifresi çözülmüş görüntüyü belirtir. Daha yüksek PSNR değeri, orijinal görüntüye daha yüksek aslına uygunluk anlamına gelir. 30 dB'den büyük PSNR değerleri için görüntü kalitesindeki bozulmanın hissedilmediği bilinmektedir. Öte yandan, 20 dB'den düşük PSNR değerleri, kötü görüntü kalitesini gösterir (Yavuz, 2021).

Görüntü şifreleme durumunda MSE mümkün olduğunca yüksek olmalıdır. Orijinal ve şifreli görüntü arasında daha yüksek MSE değeri, saldırılara karşı daha fazla bağışıklığı temsil eder.

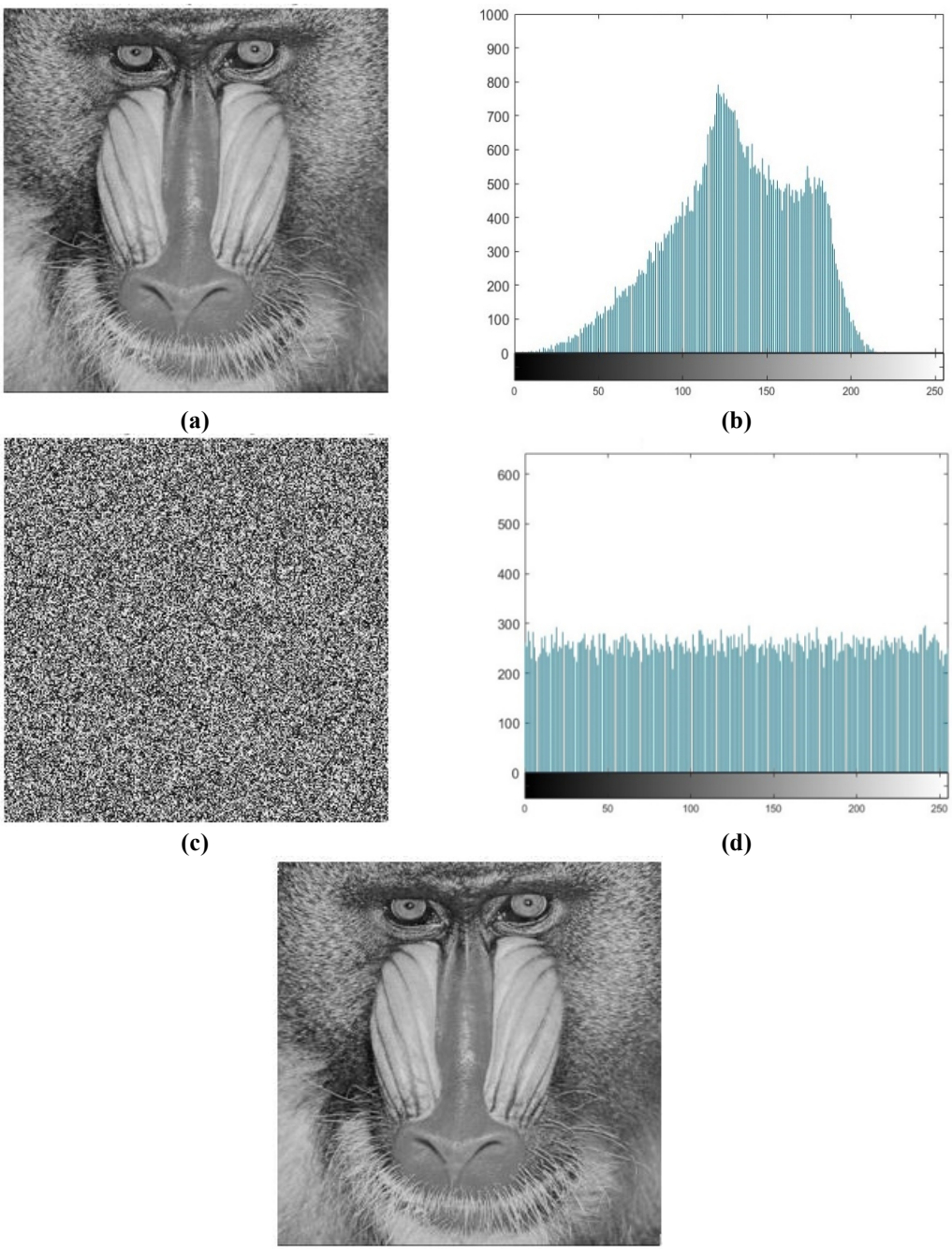
Tablo 4. Şifresi çözülmüş görüntünün gürültü girişim analizi sonuçları

	PSNR	**MSE**
Baboon	Inf	0.000000000
House	Inf	0.000000000
Couple	Inf	0.000000000

Tablo 4'te şifresi çözülmüş görüntülerin PSNR ve MSE değerleri sunulmaktadır. PSNR değerlerine bakıldığında değerlerin 30 dB'den büyük olması sebebiyle, görüntü kalitesinin bozulmadığı kanısına varılır.

5.5. Histogram Analizi

Histogram, dijital bir görüntüde her bir gri tonlamanın oluşma sıklığını temsil eden istatistiksel bir ilişkidir. Resmi gizlemek için bilgi iyi, şifreli görüntünün histogramı mümkün olduğunca düz olmalıdır. Açıktır ki, şifrelenmiş görüntünün her piksel değerinin sayıları [0, 255] aralığında neredeyse eşittir, bu da istatistiksel analiz yoluyla düz görüntü bilgisini elde etmenin zor olduğu anlamına gelir. Şifresi çözülen görüntünün histogramı, düz görüntü ile kabaca aynıdır; bu, önerilen algoritmanın görüntüyü iyi bir şekilde kurtardığı anlamına gelir (Xu ve ark, 2019).



Görsel 1: Deneysel Sonuçlar: (a) Orijinal görüntü
(b) Orijinal görüntü histogramı
(c) Şifreli görüntü

(d) Şifreli görüntü histogramı
(e) Şifresi çözülmüş görüntü

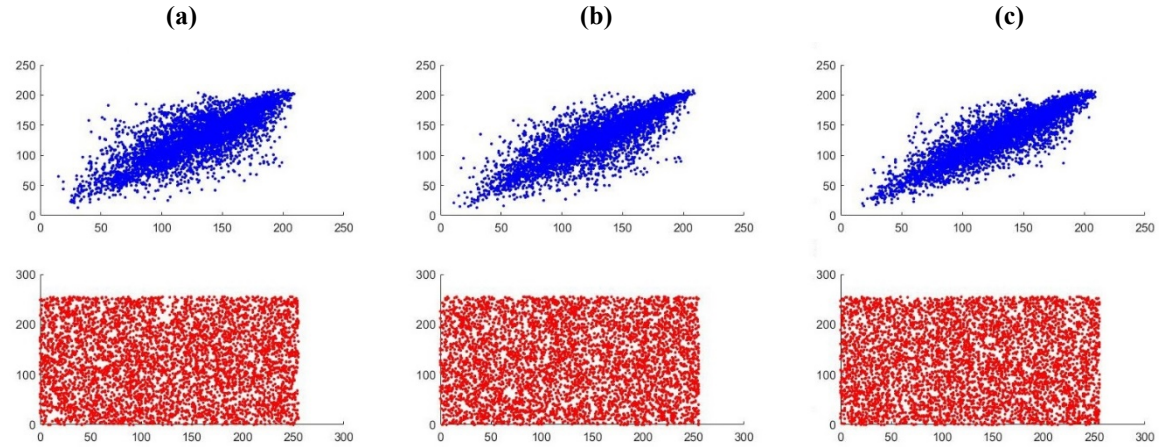
Görsel 1'de yukarıda da bahsedildiği gibi şifreli görüntünün histogramının mümkün olduğunca düz olduğu görülmektedir. Şifresi çözülmüş görüntü ile orijinal görüntünün de aynı olduğu gözlemlenebilir.

5.6. Korelasyon Analizi

Doğal görüntülerdeki komşu pikseller, yoğunluk değeri açısından birbirlerine yakın olma eğilimindedir. Bu, yatay, dikey ve diyagonal komşuluklardaki bitişik pikseller arasında yüksek korelasyonlar sağlar (Liu ve ark., 2018). Görüntü şifrelemenin amacı, saldırganların kırabileceği bir güvenlik açığı bırakmamak için komşu pikseller arasındaki güçlü olan korelasyonları bozmaktır (Xu ve ark, 2019). Bu nedenle, iyi bir şifreleme algoritması, pikseller arasındaki korelasyonu azaltmalıdır. Üstün karışıklık ve yayılma özellikleri olan bir şifreleme algoritması ile şifrelenen görüntüde korelasyon analizi yapıldığında piksellerin birbirleri arasındaki korelasyonun zayıfladığı gözlemlenir. Korelasyon katsayısı şu şekilde hesaplanabilir:

$$corr(x,y) = \frac{E[(x-\mu_x)(y-\mu_y)]}{\sigma_x \sigma_y} \tag{11}$$

Burada x ve y, bitişik piksellerin yoğunluk değerlerini içeren iki veri dizisidir ve E[.], beklenti fonksiyonudur. Burada, μx ve μy x ve y dizilerinin ortalama değerlerini gösterir ve σ_x ve σ_y standart sapmaları temsil eder. 1'e çok yakın korelasyon katsayısı, bitişik pikseller arasında güçlü bir korelasyon olduğunu gösterirken, sıfıra yakın korelasyon değeri aralarında korelasyon olmadığını gösterir (Lan R ve ark, 2018).



Görsel 2: Baboon görüntüsü ve şifre karşılığı için **(a)** diyagonal, **(b)** dikey ve **(c)** yatay yönlerde bitişik piksel korelasyonları

Yukarıda açıklanan amaca uygun olarak Baboon test örneğinde rastgele 5000 piksel seçildi; yatay, dikey ve diyagonal olarak hem orijinal hem de şifrelenmiş görüntünün korelasyonları Görsel 2'de grafik olarak açıkça gösterilmektedir. Grafiklere bakıldığında üç yönde orijinal görüntünün komşu pikselleri arasındaki güçlü korelasyonlar görülürken, önerilen şifreleme algoritması tarafından şifrelenen görüntünün bitişik pikseller arasındaki dağılmış yapı görsel olarak sunulur.

5.7. Yapısal Benzerlik İndeksi Ölçümü (SSIM)

Yapısal benzerlik (SSIM) indeksi, iki görüntü arasındaki benzerliği ölçmek için kullanılan bir yöntemdir. Yapısal bilgi, piksellerin özellikle uzamsal olarak yakın olduklarında güçlü karşılıklı bağımlılıkları olduğu fikridir. Bu bağımlılıklar, görsel olarak nesnelerin yapısı hakkında önemli bilgiler taşır. Ortaya çıkan SSIM indeksi, 0 ile 1 arasında bir ondalık değerdir ve 1 değerine yalnızca iki özdeş veri kümesi olması durumunda erişilebilir (Abdul ve Abbas, 2015).

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \tag{12}$$

Formülde;

- μ_x x'in ortalaması
- μ_y y'nin ortalaması
- σ_x^2 x'in varyansı
- σ_y^2 y'nin varyansı
- σ_{xy} x ve y arasındaki kovaryans
- $c_1 = (k_1L)^2$, $c_2 = (k_2L)^2$, zayıf payda ile bölmeyi stabilize etmek için iki değişken;
- L piksel değerlerinin dinamik aralığı (genellikle bu $2^{\text{her pikseldeki bit sayısı}}$ - 1 olarak hesaplanır)
- $k_1 = 0.01$ and $k_2 = 0.03$ olarak kullanılır.

Tablo 5. Şifresi çözülmüş görüntü ile orijinal görüntü arasındaki yapısal benzerlik indeksi

	SSIM
Baboon	1.0000
House	1.0000
Couple	1.0000

Tablo 5'te şifre çözme işlemi gerçekleştirildikten sonra elde edilen görüntüler ile orijinal görüntülerin yapısal benzerlik indeksi verilmiştir. Önerilen algoritmada, daha iyi sonuçlar için orijinal ve şifreli görüntüler arasındaki benzerlik değeri mümkün olduğunca küçük olmalı, orijinal ve şifresi çözülmüş görüntüler arasındaki benzerlik değeri ise mümkün olduğunca büyük ve 1'e yakın bir değer olmalıdır.

6. TARTIŞMA

Tablo 6. Literatürde yer alan çalışmalar ile karşılaştırma

İlgili Çalışma	**NPCR**	**UACI**	**PSNR**	**MSE(dB)**	**Şifreli Görüntü Entropisi**
(Anees ve ark, 2014)	0.0015	0.0010	8.7671	37.69	7.8026
(Zhou ve ark, 2018)	52.39	33.57	X	X	7.9993
(Liu ve ark, 2019)	50.57	25.19	8.3499	X	7.9969
(Krishnamoorthi ve Murali, 2014)	99.62	27.38	9.22	X	X
(Jain ve Rajpal, 2016)	99.62	33.06	27.7	X	7.9952
(Ahmad ve Hwang, 2015)	99.36	32.72	X	40.39	7.9801
(Huang ve Nien, 2009)	99.42	24.94	X	X	X
(Huang ve ark, 2013)	99.54	28.27	X	X	7.9967
(Loukhaoukha ve ark, 2012)	99.58	28.62	X	X	7.9968
(Hussain ve ark, 2020)	99.61	33.08	X	X	7.9353
Önerilen metodoloji	99.6658	33.6566	Inf	0.00	7.9975

Tablo 6'da şimdiye kadar gerçekleştirilen çalışmalar ile önerilen hibrit algoritmanın karşılaştırması yapılmıştır.

Tablodaki NPCR değerleri incelendiğinde, önerilen metodolojinin literatürdeki çalışmalara kıyasla daha iyi sonuçlar verdiği görülmüştür. Önceki bölümlerde bahsedildiği gibi NPCR değerinin %99 civarı olması dışarıdan gelecek saldırılara karşı algoritmanın diğer çalışmalara göre daha güvenli olduğunu göstermektedir. UACI değerinin %33 civarı çıkması orijinal görüntüde bir piksel dahi değişiklik olduğunda bu değişiklikten tüm görüntünün şifreli halinin etkilenmesi demektir ve bu değerin diğer algoritmalardan elde edilen sonuçlar kadar

iyi olduğu gözlemlenmiştir. PSNR değeri ise şifre çözme adımında çözülen görüntünün kalitesinin bozulmamış bir şekilde elde edildiğini gösteren bir metriktir. Diğer çalışmalara oranla daha yüksek sonuca ulaşılmıştır. MSE, şifresi çözülmüş görüntü ile orijinal görüntünün arasındaki farklılığı gösteren bir metriktir. Bu sebeple MSE değerinin minimum olması beklenir, önerilen yöntem bu koşulu da sağlamaktadır. Şifreli görüntü entropisinin yukarıda da bahsedildiği gibi 8 değerine yakın olması beklenir, algoritmanın da bu şarta uygun olduğu görülmüştür. Nihai sonuç olarak bu makaledeki hibrit metodolojinin performans metriklerine göre teorik değerlere ulaştığı görülmüştür.

7. SONUÇLAR VE GELECEKTEKİ ÇALIŞMALAR

Geleneksel görüntü şifreleme şemaları, yeterli rastgelelik sağlamada yetersizdir ve bu da bir güvenlik açığına yol açar. Bu nedenle, şifreli alanda yeterli rastgeleliğe ulaşma boşluğunu kapatmak amacıyla, bu makalede kaotik haritanın Mandelbrot fraktal setleri ile kullanıldığı hibrit bir çözüm sunulmaktadır. Kaotik haritaların seçimi, kaotik aralıkta periyodik pencerelerin varlığı gibi 1 boyutlu kaotik haritalarla ilgili sınırlamaları ortadan kaldıracak şekildedir. Kaosun kullanılması geleneksel algoritmalara kıyasla sadece anahtar alanı genişletmekle kalmaz, aynı zamanda önemli ölçüde başlangıç koşullarına bağlı olarak daha fazla rastgelelik ve hassasiyet sağlar. Şifreli alanda tek tip bir histogram elde edilir, böylece diğer şemalara göre gelişimini doğrulayan neredeyse optimal entropi elde edilir. Önerilen şemanın, farklı istatistiksel ve sayısal analizler yoluyla çeşitli güvenlik saldırılarına karşı oldukça sağlam olduğu kanıtlanmıştır.

Şifreleme metodolojisi literadürde de veri gizliliği sebebiyle tıbbi görüntülerin saklanması için kullanılan diğer algoritmalar gibi bu alanda kullanılabilir. Bu kapsamda hastaların tıbbi görüntülerinin bulut tabanlı bir yerde şifreli şekilde saklanarak buna erişmek isteyen personellere şifresi çözülmüş halde gönderilebilir.

Gelecekte, önerilen şema renkli görüntüler ve diğer görüntü formatlarına kolayca uyarlanabilir ve farklı kaotik haritalar ile fraktal setlerin birlikte olduğu bir şema üzerinde çalışılıp karşılaştırması yapılabilir. Ek olarak, önerilen şema esas olarak tek gri görüntü şifrelemesine odaklanmaktadır. Şifreleme verimliliğini artırmak için gelecekte makaledeki hibrit algoritmanın çoklu görüntü şifrelemede kullanılabilirliği araştırılacaktır.

REFERANSLAR

Abdul, N., Abbas, M., (2015). Image encryption based on Independent Component Analysis and Arnold's Cat Map. Egyptian Informatics Journal, 17, 139-146

Ahmad, J., Hwang, S., (2015). Chaos-based diffusion for highly autocorrelated data in encryption algorithms, Nonlinear Dynamics, 82(4), 1839–1850.

Abdulgader, A., Ismail, M., Zainal, N., Idbeaa, T., (2015) Enhancement of AES algorithm based on chaotic maps and shift operation for image encryption. Journal of Theoretical and Applied Information Technology, 71(1), 1-12

Akhshani, A., Akhavan, A., Lim, S., Hassan, Z., (2012). An image encryption scheme based on quantum logistic map. Communications in Nonlinear Science and Numerical Simulation, 17(12), 4653-4661

Anees, A., Siddiqui, A. M., Ahmed, F. (2014). Chaotic substitution for highly autocorrelated data in encryption algorithm. Communications in Nonlinear Science and Numerical Simulation, 19(9), 3106–3118

Belazi, A., Talha, M., Kharbech, S., Xiang, W., (2019). Novel Medical Image Encryption Scheme Based on Chaos and DNA Encoding, IEEE Access, 7, 36667–36681

Chen, G., Mao, Y., Chui C.K., (2004). A symmetric image encryption scheme based on 3D chaotic cat maps, Chaos, Solutions & Fractals, 21(3), 749-761

Cheng, G., Wang, C., Chen, H. (2019). A Novel Color Image Encryption Algorithm Based on Hyperchaotic System and Permutation-Diffusion Architecture, International Journal of Bifurcation and Chaos, 29(9), 1950115-1, 1950115-17

Crownover, R. M., (1995). Introduction to Fractals and Chaos; Jones and Bartlett: Burlington, MA, USA., ISBN 978-0-86720-464-3

Dong, Y., Liu, J., Zhu, C., Wang, Y., (2010). Image encryption algorithm based on chaotic mapping. (ICCSIT), 2010 3rd IEEE International Conference, 289-291.

El-Alfy, E., Al-Utaibi, K., (2011). An Encryption Scheme for Color Images Based on Chaotic Maps and Genetic Operators, The Seventh International Conference on Networking and Services, 92-97

Han, B., Jia, Y., Huang, G., Cai, L., (2020). A Medical Image Encryption Algorithm Based On Hermite Chaotic Neutral Network, 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), 1, 2644-2648

Huang, C. K., Liao, C. W., Hsu, S. L., Jeng, Y. C., (2013). Implementation of gray image encryption with pixel shuffling and gray-level encryption by single chaotic system, Telecommunication Systems, 52(2), 563-571

Huang, C. K., Nien, H. H (2009). Multi chaotic systems-based pixel shuffle for image encryption. Optics communications, 282(11), 2123-2127

Huang, H. (2019). Novel Scheme for Image Encryption Combining 2D Logistic-SineCosine Map and Double Random-Phase Encoding. IEEE Access, 7, 177988–177996

Hussain S., Jamal S. S., Shah T., Hussain I., (2020) A Power Associative Loop Structure For The Construction Of Non-Linear Components Of Block Cipher, IEEE Access, 8, 123492-123506

Jain, A., Rajpal, N., (2016). A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps, Multimedia Tools and Applications, 29(1), 5455–5472

Jolfaei, A., Mirghadri, A., (2010). An image encryption approach using chaos and stream cipher. Journal of Theoretical and Applied Information Technology, 19(2), 117-125.

Krishnamoorthi, R., Murali, P., (2014). Chaos based image encryption with orthogonal polynomials model and bit shuffling, Proceedings of the IEEE International Conference on Signal Processing and Integrated Networks, Noida India, 107–112.

Lan, R., He, J., Wang, S., Gu, T., Luo, X., (2018). Integrated chaotic systems for image encryption. Signal Processing, 147, 133–145

Li, A., Belazi, A., Kharbech, S., Talha, M., Xiang, W., (2019). Fourth Order MCA and Chaos-Based Image Encryption Scheme. IEEE Access, 7, 66395–66409

Liu, D., Zhang, W., Yu, H., Zhu, Z.L., (2018). An image encryption scheme using self-adaptive selective permutation and inter-intra-block feedback diffusion, Signal Processing, 151, 130–143

Liu, X., Xiao, D., Xiang, Y., (2019). Quantum image encryption using intra and inter bit permutation based on logistic map, IEEE Access, 7, 6937–6946.

Liu, Z., Wu, C., Wang, J., Hu, Y. (2019). A Color Image Encryption Using Dynamic DNA and 4-D Memristive Hyper-Chaos. IEEE Access, 7, 78367–78378.

Loukhaoukha, K., Chouinard, J. Y., Berdai, A., (2012). A secure image encryption algorithm based on Rubik's cube principle, Journal of Electrical and Computer Engineering, 2012

Ma, S., Zhang, Y., Yang, Z., Hu, J., Lei, X. (2019). A New Plaintext-Related Image Encryption Scheme Based on Chaotic Sequence. IEEE Access, 7, 30344–30360

Mandelbrot, B.B., (1982). The Fractal Geometry of Nature; Henry Holt and Company: New York, NY, USA; ISBN 978-0-7167-1186-5.

Mary, R., Eswaran, P., Shankar, K., (2018). Multi Secret Image Sharing Scheme Based on DNA Cryptography with XOR, Pure and Applied Mathematics, 118(7), 393-398

Menezes, A. J., Van Oorschot, P. C., Vanstone, S. A. (1996) Handbook of applied cryptography, CRC press, 810, Florida

Negi, D., Negi, A., Agarwal, S., (2016). The complex key cryptosystem. International Journal Application Eng. Res., 11, 681–684.

Niyat AY, Moattar MH, Torshiz MN (2017). Color image encryption based on hybrid hyper-chaotic system and cellular automata, Optics and Lasers in Engineering, 90, 225–237

Patel S, Bharath K P, Muthu R. (2020) Image Encryption Decryption Using Chaotic Logistic Mapping and DNA Encoding, Computer Science

Pickover, C.A. (2001) Computers, Pattern, Chaos, and Beauty: Graphics from an Unseen World; Courier Corporation: North Chelmsford, MA, USA; ISBN 978-0-486-41709-7.

Shubo, L., Sun, J., Xu, Z., (2009). An improved image encryption algorithm based on chaotic system. Journal of Computers, 4(11), 1091-1100.

Stallings, W. (2006). Cryptography and network security: principles and practices. Pearson Education India, 900, Hindistan

Soni, A., Acharya A. K., (2012). A Novel Image Encryption Approach using an Index based Chaos and DNA Encoding and its Performance Analysis, International Journal of Computer Applications, 47(123), 1-6

Verma, A., Jain, A., (2016). Pixel chaotic shuffling and Arnold map based Image Security Using Complex Wavelet Transform. Journal of Network Communications and Emerging Technologies (JNCET), 6(5): 8-11

Wu, Y., Zhou, Y., Saveriades, G., Agaian, S., Noonan, J.P., Natarajan, P., (2013). Local Shannon entropy measure with statistical tests for image randomness, Information Sciences, 222,323–342

Xua, Q., Sun, K., Cao, C., Zhu, C., (2019), A fast image encryption algorithm based on compressive sensing and hyperchaotic map, Optics and Lasers in Engineering, 121, 203-214

Yavuz, E., (2019). A novel chaotic image encryption algorithm based on content-sensitive dynamic function switching scheme. Optics Laser Technology,114:224–239

Yavuz, E., (2021). A new parallel processing architecture for accelerating image encryption based on chaos, Journal of Information Security and Applications, 63

Yin, Q., Wang, C., (2018). A New Chaotic Image Encryption Scheme Using Breadth-First Search and Dynamic Diffusion, International Journal of Bifurcation and Chaos, 28(4), 1850047-1, 1850047-13

Zhang, X., Wang, L., Zhou, Z., Niu, Y. (2019). A Chaos-Based Image Encryption Technique Utilizing Hilbert Curves and H-Fractals. IEEE Access, 7, 74734–74746.

Zhao, J., Guo, W., Ye, R., (2014). A chaos-based image encryption scheme using permutation-substitution architecture, International Journal Computer Trends and Technology, 15(4), 174- 185.

Zhou, N., Chen, W., Yan, X., Wang, Y., (2018). Bit-level quantum color image encryption scheme with quantum cross-exchange operation and hyper-chaotic system. Quantum Information Processing, 17(6):137

İNTERNET KAYNAKLARI

https://sipi.usc.edu/database/

Not: *Bu makale, İstanbul Ticaret Üniversitesi Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Tezli Yüksek Lisans Programı'nda, Doç.Dr. Mustafa Cem Kasapbaşı danışmanlığında, Gülseren Kibar tarafından yürütülecek olan, "Mandelbrot Fraktal Setleri Kullanarak Yeni Bir Şifreleme Yöntemi Önerilmesi ve Analizlerin Gerçekleştirilmesi" başlıklı yüksek lisans tezinin ön çalışmalarından yararlanılarak hazırlanmıştır.*