Araştırma Makalesi

JULİA SETLERİ VE LOJİSTİK HARİTA KULLANILARAK GÖRÜNTÜ ŞİFRELEME

Bahar ARITÜRK[†], 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

bahar_ariturk@hotmail.com, mckasapbasi@ticaret.edu.tr

0000-0001-5972-401X, 0000-0001-6444-6659

Atıf/Citation: ARITÜRK, B., KASAPBAŞI, M. C., (2022). Julia Setleri ve Lojistik Harita Kullanılarak Görüntü Şifreleme, Journal of Technology and Applied Sciences 5(2), s. 65-78, DOI: 10.56809/icujtas.1150308

ÖZ

Açık ağlar ve internet üzerinden veri alışverişi hızla büyüdüğü için, verilerin güvenlik açığı incelenecek büyük bir sorun haline gelmektedir. Bu soruna olası bir çözüm olarak ise metin, görüntü, ses, video gibi verilerin şifrelenmesi yöntemi önerilir. Bu işlem yapılacağı zaman Gelişmiş Şifreleme Standardı (AES) gibi klasik şifreleme algoritmaları her zaman birincil seçimdir, ancak görüntü veya video şifreleme söz konusu olduğunda, literatürdeki birçok araştırmaya bakıldığı zaman hesaplama verimliliği nedeniyle yazarların kaos tabanlı şifreleme tekniklerini önerdiği sıkça görülmektedir. Kaos şifrelemenin ana özelliklerine bakıldığında anahtarların rastgeleliği, başlangıç koşullarına duyarlılığı ve daha büyük anahtarlarla çalışıldığında daha verimli sonuçlar elde edildiği göze çarpar. Bu araştırma makalesinde görüntü işleme konusunda kriptografik yeni bir yaklaşım önerilmiştir. Bu yaklaşımda kaotik haritalardan birisi olan lojistik harita ile julia fraktal setlerinin birlikte kullanılarak bir şifreleme algoritması sunulmaktadır. Yaklaşımda fraktal tabanlı setin kullanılmasının sebebi anahtarın gücünün arttırılarak şifrelemenin daha başarılı olmasını sağlamasıdır. Bu algoritma iki anahtarın işlemden geçirilmesiyle oluşturulan yeni anahtarın görüntü şifrelemede kullanılması ile ortaya çıkmıştır. Buna ilave olarak da algoritmanın başarı oranının arttırılması için çalışmalar yapılmıştır. Sunulan yeni yaklaşımla birlikte oluşan şifreli görüntülerin asıl görüntüler ile birlikte analizinin çıkarılması ve yapılan analiz sonucu elde edilen nicel değerler mevcuttur. Bu değerlerin iyileştirilmesi için de algoritmada çeşitli değişiklikler yapılarak testler yapılmıştır. Bu testler sonucunda şifreli görüntü ile asıl görüntünün karşılaştırılarak yöntemin başarısı ölçülmüştür. Bu başarıyı ölçmek için Piksel Sayısı Değişim Hızı (NPCR), Tepe Sinyal Gürültü Oranı (PSNR), Sinyal Gürültü Oranı (SNR), Korelasyon Katsayısı, Birleşik Ortalama Değişen Yoğunluk (UACI), Yapısal Benzerlik İndeks Ölçüsü (SSIM), Entropi ve Yerel Shannon Entropisi, Ortalama Karesel Hata (MSE), Histogram Analizi metrikleri kullanılmıştır.

Anahtar Kelimeler: Julia Set, Kaos Teorisi, Kaotik Görüntü Şifreleme, Kaotik Harita, Kripto Analizi

IMAGE ENCRYPTION USING JULIA SETS AND LOGISTIC MAP

ABSTRACT

As data exchange over open networks and the internet is growing rapidly, data vulnerability is becoming a major issue to examine. As a possible solution to this problem, the method of encrypting data such as text, images, audio, and video is recommended. When doing this, classical encryption algorithms such as Advanced Encryption Standard (AES) are always the primary choice, but when it comes to image or video encryption, when looking at many studies in the literature, it is often seen that the authors recommend chaos-based encryption techniques due to computational efficiency. Looking at the main features of chaos encryption, the randomness of the keys, sensitivity to initial conditions and more efficient results are obtained when working with larger keys. A new cryptographic approach to image processing is proposed in this research paper. In this approach, an encryption algorithm is presented by using the logistic map, which is one of the chaotic maps, and the julia fractal sets together. The reason for using the fractal-based set in the approach is to increase the strength of the key and ensure that the encryption is more successful. This algorithm has emerged with the use of the new key, which is created by processing two keys, in image encryption. In addition, studies have been carried out to increase the success rate of the algorithm. With the new approach presented, there are quantitative values obtained as a result of the analysis and analysis of the encrypted images together with the original images. In order to improve these values, various changes were made in the algorithm and tests were carried out. As a result of these tests, the success of the method was measured by comparing the encrypted image with the original image. To measure this success, Pixel Count Rate of Change (NPCR), Peak Signal to Noise Ratio (PSNR), Signal to Noise Ratio (SNR), Correlation Coefficient, Combined Average Variable Intensity (UACI), Structural

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

Similarity Index Measure (SSIM), Entropy, and Local Shannon Entropy, Mean Squared Error (MSE), Histogram Analysis metrics were used.
Keywords: Chaos Theory, Chaotic Image Encryption, Chaotic Map, Crypto Analysis, Julia Set

1. GİRİŞ

Son yıllarda, dinamik sistemler ve kaos teorisinden gelen farklı yöntemler, iletişim ve özellikle kriptografi uygulamalarında araştırmacılar tarafından büyük ilgi gördü. Kaotik sistemlerin başlangıç koşullarına ve parametrelere yüksek duyarlılığı, kaotik şifreleme sistemlerinin, onları herhangi bir istatistiksel saldırıya karşı sağlam kılan güçlü kriptografik özellikleri anlamına gelir. Şifreler için rastgele benzeri davranış ve uzun periyotlara sahip kararsız periyodik yörüngeler olması oldukça avantajlı olmasıdır.

Kaos ve kriptografi arasındaki yakın ilişki, kaos tabanlı kriptografik algoritmaları güvenli iletişim için doğal bir aday haline getirir. Kaos tabanlı şifreler, güvenlik, karmaşıklık, hız, bilgi işlem gücü vb. ile ilgili birçok açıdan bazı olağanüstü iyi özellikler göstermiştir. Toplu veri kapasitesi ve pikseller arasındaki yüksek korelasyon gibi görüntünün bazı içsel özellikleri nedeniyle, görüntülerin şifrelenmesi, metin şifrelemesinden farklıdır. Bu nedenle, şifrelemede kullanmak için bazı yüksek boyutlu kaos sistemlerine veya ayrıntılı yapılara ihtiyaç vardır.

Şimdiye kadar, internet üzerinden ve kablosuz ağlar aracılığıyla güvenli görüntü aktarımı gerçekleştirmek için çok çeşitli kaos tabanlı şifreler önerildi. Bu çalışmada, mevcut kaotik harita şemalarına katkıda bulunmak için Fraktal-Kaos akış şifrelemesi sunulmaktadır. Sunulan çalışmanın literatürde yer alan verilerin kullanılarak performans analizleri yapıldığında başarılı sonuçlar 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 algoritmasının çalışması ayrıntılı olarak açıklanmıştır. Bölüm 5'te algoritmanın literatürde de yer alan güvenlik analizleri ve performans değerlendirmeleri sonuçları ile birlikte detaylandırılmıştır. Sonuçlar ve tartışmalarda, literatürde önerilen kaotik şemalarla elde edilen sonuçların önerilen algoritma sonuçlarıyla karşılaştırması verilmektedir. Sonuç açıklamaları son bölümde verilmiştir.

2. LİTERATÜR TARAMASI

Alsafasfeh ve Arfoa (2011) tarafından önerilen görüntü şifreleme algoritması için hem Rössler kaotik sistemi hem de Lorenz kaotik sistemi birlikte kullanılır. Bir algoritmada iki veya daha fazla kaotik haritanın kullanılması algoritma karmaşıklığını artırarak daha güvenli hale gelinmesini sağlar. Uzun vadeli kaotik davranışa bakıldığında periyodik ve başlangıç değişkenlerine bağlı olduğu gözlemlenir (Wang ve ark., 2008), Rössler ve Lorenz kaotik haritalarının her ikisi de üç değişkene bağlıdır, toplam parametre sayısı altı değişkene bağlı olduğundan önerilen kaotik sistemin güvenliğini artırır ve bu da onu dışarıdan olabilecek saldırılara karşı daha güvenli kılar. Önerilen algoritma, rastgele görüntü verilerini orijinal görüntüyle aynı boyutta bir kaotik matriste depolamadan önce görüntünün piksellerini kendi içinde karıştırır ve belirli sayıda yineleme yaparak gri tonlama değerlerini değiştirme işlemini gerçekleştirir. XOR işlemleri hem şifreleme hem de şifre çözme için kullanılır.

Khanzadi ve ark (2014) tarafından kaotik haritalara dayalı rastgele bit dizileri üretmek için bir algoritma önerilir. Bu algoritma, çadır haritası ve lojistik haritalardan oluşturulan rastgele bit dizisini kullanır. Düz görüntü piksellerinin permütasyonu bu kaotik fonksiyonlarla yapılır ve ardından görüntü sekiz bitlik harita düzlemlerine bölünür. Bitler, kaotik bir matrise göre başka bir bit değeriyle değiştirilerek şifreleme işleminin yapılması sağlanır. Yapılan incelemelere göre önerilen algoritmanın performansı, hem anahtar duyarlılığı hem de anahtar alanı açısından iyi olması sebebiyle kaba kuvvet saldırılarına ve istatistiksel saldırılara karşı oldukça dirençlidir.

Liu ve ark (2019) tarafından DNA kriptografisi ve İki Boyutlu Lojistik Haritaya dayalı gri tonlamalı görüntüler için bir şifreleme metodolojisi önerilir. Sisteme genel olarak bakıldığında, DNA ve sözde rastgele sayı güvenliği ilkelerine göre çalıştığı gözlemlenir. Kaotik kriptografi için bir karıştırma ve difüzyon yapısı kullanılır. DNA yapıları ve sözde rastgele sayılar daha büyük bir kaos düzeyine ulaşmak için birlikte karıştırılır. Rastgele sayılar lojistik harita tarafından iki boyutlu olarak üretilir. Görüntü şifreleme algoritmasında DNA kodlaması ve lojistik harita tarafından rastgele sayıların oluşturulmasından sonra piksel düzeyinde ve DNA'nın baz düzeyinde yeniden düzenlenmesi kullanılır. Oldukça düzgün bir dağılım elde edilirken, dışarıdan oluşabilecek saldırılara karşı daha güvenlikli olmasının yanı sıra yüksek şifreleme hızına sahiptir ve diğer DNA tabanlı görüntü şifreleme şemalarından üstündür.

Al-Maadeed ve ark. (2012) tarafından hazırlanan bu makalede, yeni görüntü şifreleme şeması piksel karıştırma ve bir akış şifreleme birimlerinden oluşur. Piksel karıştırma birimi, bitişik piksel korelasyonunu azaltmak için dikey ve yatay olmak üzere iki yönde uygulanabilen bir permütasyon haritasından oluşur. Piksel permütasyonundan sonra W7 algoritması uygulanır. W7 algoritması, uzunluğu karıştırılmış görüntü ikili dizisine eşit olan anahtar akışı adı verilen bir sözde rastgele şifre bit akışı üretir. Şifreli görüntü, karıştırılmış görüntü ikili dizisinin anahtar akışıyla XOR işlemine tabi tutularak elde edilir. Şifre çözme için, alınan şifreli görüntü anahtar akışı ile XOR işlemine tabi tutulur ve ters permütasyon aracılığıyla orijinal görüntü elde edilir.

Al-Najjar ve ark. (2011) makalesinde, lojistik harita kaotik işlevine dayalı bir görüntü şifreleme tartışılır. Şifreleme sistemi incelendiği zaman, piksel değiştirme yaklaşımı ve piksel karıştırma yaklaşımı olarak iki yaklaşıma ayrıldığı görülür. Piksel değiştirme yaklaşımında, piksel değerleri değiştirilirken, piksel karıştırmada

ise piksel konumları değiştirilir. Bu algoritma, görüntünün kendisini karıştırmadan pikselin değerini değiştirmek için lojistik harita yardımı ile oluşturulan iki piksel haritalama tablosu kullanılır. Piksel eşleme tablosu (PMT), 256x1 boyutunda karıştırılmış sırada 0 ile 255 arasındaki piksel değerlerini içerir. Algoritma, görüntüyü şifrelemek için yalnızca değiştirme yaklaşımlarını kullanır. İki farklı değiştirme yaklaşımı şunlardır: ilk yaklaşımda, pikseller, rastgele bir değer talep edilerek ve PMT kullanılarak eşlenerek kaydırılır. İkinci yaklaşımda, lojistik harita kullanılarak oluşturulan belirli rastgele vektör ile XOR işlemine tabi tutularak değiştirme yapılır. Şifre çözme işlemi ise ters sırada yapılır .

El-Latif ve ark. (2018) hasta güvenliği ve veri gizliliği sebebiyle tıbbi görüntüler için kaos tabanlı bir kuantum şifreleme önerir. Bu çerçevede şifreli görüntüler bulutta saklanarak buna erişmek isteyen sağlık personeline şifresi çözülmüş halde buluttan gönderilir. Önerilen çalışma, tıbbi verileri korumak için gri kod ve kaotik haritadan yararlanır. Burada kuantum gri kod görüntüyü karıştırır. Ardından, karıştırılmış görüntüyü şifrelemek için anahtar oluşturucuya dayalı olarak kuantum XOR işlemi gerçekleştirilir. Önerilen yaklaşım sağlam, gerçekleştirilebilir ve oldukça verimlidir.

Wade ve ark. (2019) günümüzde multimedya teknolojisinin ilerlemesi ile dijital veri iletişim alanındaki en büyük problem olan görüntü verilerine yetkisiz erişimi engellemek için bir çalışma önerir. Bu çalışmada verileri şifrelemek için kriptografik algoritmalar ile biyolojik diziler de kullanılır. Çalışmada, görüntüleri korumak için iki aşamalı bir yöntem önerilmiştir. Görüntüleri yetkisiz erişimden korumak için DNA şifrelemesi ve Polimeraz Zincir Reaksiyonu (PCR) Amplifikasyonu kullanılır. Algoritmanın, farklı standart parametreler kullanılarak test edildiğinde verimlilik sergilediği gözlemlenir.

Askar ve ark.(2017), iki boyutlu kaotik ekonomik harita ve lojistik haritaya dayalı bir şifreleme algoritması önerir. İlk önce renkli olan orijinal görüntüyü okur ve gri görüntüye dönüştürür, ardından karıştırma dizisi oluşturmak için satır ve sütun karıştırma işlemini gerçekleştirir, iki boyutlu kaotik ekonomik haritayı kullanarak pikselleri ondalık sayıdan ikiliye dönüştürür ve elde edilen değerler arasında bit düzeyinde XOR işlemini gerçekleştirir, ardından şifre pikseli alınarak her bir bitin yeniden şekillendirilmesi ile şifreli görüntü elde edilir. Önerilen algoritmanın geniş anahtar güvenlik alanı ve ayrıca entropi bilgisi ile ilişkili olduğu ve gürültü, kaba kuvvet, istatistiksel saldırılar gibi çeşitli diğer saldırılara karşı verimli bir şekilde direnebileceği sonuçlardan çıkarılabilir.

Roy ve ark. (2017) hiperkaos permütasyon sistemine dayalı bir renkli görüntü şifreleme sistemi önerir. Yazarlar ayrıca Dikey boşluklu Yüzey yayan Lazer (VCSEL) kavramına dayalı şifreleme ve şifre çözme sürecini de inceler. Önerilen sistemde renkli bir görüntü ele alınır ve esas lazer anahtar vektörü kullanılarak üretilir. Piksel permütasyonundan sonra bit düzeyinde permütasyon yapılır ve bit düzeyinde XOR işlemi yapıldıktan sonra karşılık gelen şifreli görüntü elde edilir. Önerilen sistem, diğer kaos tabanlı sistemlere göre daha basit ve hızlı olması ile ön plana çıkmıştır.

Li ve ark. (2020)'de, iki boyutlu Lorenz ve Lojistik'e odaklanan yeni bir görüntü şifreleme şeması önerir. Şifreleme sisteminde, görüntüyü kodlamak için iki çift kaotik dizi verisi üretmek için klasik kaotik yöntem kullanılır. Lu ve ark. (2020)'da Lojistik-Sinüs sistemini kullanan ayrı bir kaotik haritaya ve S-Box'a odaklanan yeni bir görüntü şifreleme yöntemi önerir. Liu ve ark. (2020)'de, eşzamanlı permütasyon-difüzyon işlemi ile güvenli ve hızlı kaotik bir görüntü şifreleme algoritması önerir. Bu algoritma permütasyon ve difüzyon prosedürlerini birleştirir. Wang ve ark.(2020)'de, kaotik bir sisteme dayalı yeni bir şifreli görüntü yöntemi anlatılır. Önerilen yöntem, kaotik sistemin N ortogonal matrislerini ve belirli temel dinamik özelliklerini elde etmek için Schur ayrıştırma yöntemini kullanır. Liu ve ark. (2020)'de (5-D) hiper-kaotik haritayı DNA yöntemiyle bütünleştiren yeni bir görüntü kriptografik algoritma sunar. Bu sistem dört bölüm için tasarlanmıştır: piksel seviyesinde difüzyon, piksel seviyesinde permütasyon, DNA seviyesinde difüzyon ve ikinci permütasyon. Wang ve Liu (2020)'de karma tablo karıştırma ve DNA değiştirme çerçevesine bağlı bir görüntü şifreleme tekniğini önerir. Algoritma, klasik 'karıştırma-yayılma' sürecini ve hiper-kaotik Chen'i kullanır. Sistem, her faz için kullanılan sözde rastgele serileri üreterek görüntü şifreleme işlemini yapar.

3. MATERYAL VE METOT

Bu bölüm, çalışmada kullanılan kaos teorisi, lojistik kaotik harita ve fraktal setleri anlatmaktadır.

3.1. Kaos teorisi ve Lojistik Harita

Kaos teorisi, doğadaki doğrusal olmayan dinamik sistemlerle ilgilenen bir matematik dalıdır. Bir sistem, daha büyük bir bütün oluşturan etkileşimli bileşenler kümesidir. Doğrusal olmayan, bileşenler arasındaki geri besleme veya çarpımsal etkiler nedeniyle bütünün tek tek parçaları toplamaktan daha büyük bir şey olduğu anlamına gelir. Son olarak dinamik, sistemin mevcut durumuna göre zaman içinde değiştiği anlamına gelir. (https://geoffboeing.com/2015/03/chaos-theory-logistic-map/)

Kaotik sistemler ise, doğrusal olmayan dinamik sistemlerin basit bir alt türüne girer. Çok az etkileşimli parça içerebilirler ve bunlar çok basit kuralları takip edebilir, ancak bu sistemlerin tümü başlangıç koşullarına çok hassas bir şekilde bağımlıdır. Belirleyici basitliklerine rağmen, zamanla bu sistemler tamamen öngörülemeyen

ve farklı (kaotik) davranışlar üretebilir. Kaos teorisinin babası Edward Lorenz, kaosu "şimdinin geleceği belirlediği, ancak yaklaşık şimdinin geleceği yaklaşık olarak belirlemediği" olarak tanımlamıştır.
İlk olarak 19. yüzyılın ortalarında bir çevrede nüfus gelişimini modellemek için kullanılan lojistik harita (Baker ve Gollub, 1996), artık rastgele benzeri davranış dizileri oluşturmak için kullanılan en pratik işlevlerden biridir. Bu basit harita aşağıdaki fark denklemi ile ifade edilir. (Yavuz,2021)

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

3.2. Julia Fraktal Setleri

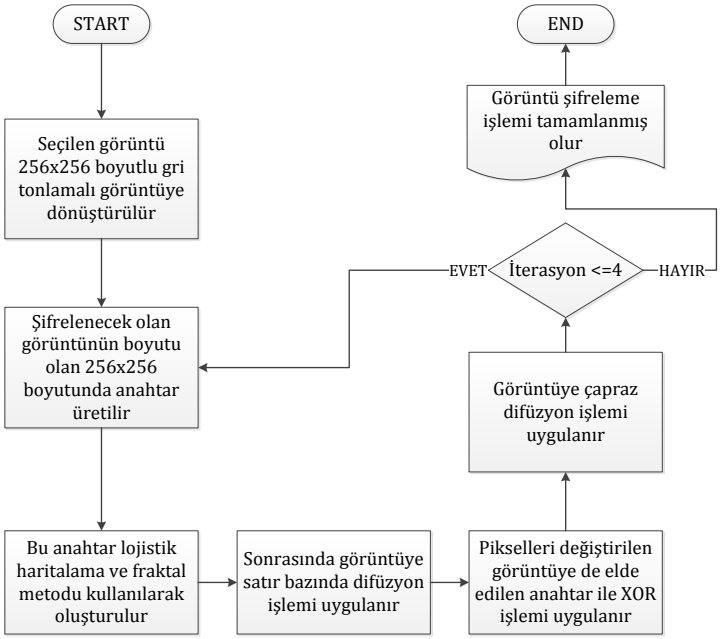
Matematikte, fraktal, genellikle topolojik boyutu kesinlikle aşan bir fraktal boyuta sahip, keyfi olarak küçük ölçeklerde ayrıntılı yapı içeren düzgün olmayan geometrik şekilleri tanımlamak için kullanılan bir terimdir (Liu ve ark. 2003). Fraktal geometri, ölçü teorisinin matematiksel dalı içinde yer alır.
17. yüzyılda özyineleme kavramlarıyla başlayarak, fraktallar giderek daha titiz matematiksel işlemlerden geçerek 19. yüzyılda Bernard Bolzano, Bernhard Riemann ve Karl Weierstrass'ın ufuk açıcı çalışmalarıyla sürekli fakat türevlenemeyen fonksiyonların incelenmesine doğru ilerledi (Segal , 1978) ve 20. yüzyılda fraktal kelimesinin ortaya çıkışına, ardından bilgisayar tabanlı modellemeye olan ilginin artması üzerine fraktalların çok büyük önem gördüğü gözlemlenmiştir. (Edgar, 2004),(Trochet, 2009)
Yinelenen fonksiyon sistemleri, klasik Cantor kümeleri, Sierpinski, Julia kümeleri ve çok daha fazlasını içeren geniş bir fraktal sınıfını oluşturmanın birleşik bir yolu olarak tanıtıldı. Bu kümelerin çoğu, geleneksel olarak, sınıra kadar götürülen ardışık mikroskobik iyileştirme süreciyle üretiliyor olarak görülür (Barnsley ve Demko, 1985). Klasik Julia kümesi, $f(z) = z^2 + c$ eşleme fonksiyonu ile birkaç yinelemenin bir ürünüdür. Karmaşık sayı $z = x + iy$, reel sayı uzayında (x, y)'ye benzersiz olarak eşlenebildiğinden, karmaşık sayı uzayı ile gerçek sayı uzayı arasında bire bir ilişki kurulabilir.

4. ŞİFRELEME İÇİN ÖNERİLEN ALGORİTMA

Bu makalede görüntü şifreleme işleminde kullanılacak anahtarı oluşturmak için julia seti ve bir lojistik harita kaotik setinden yararlanılarak hibrit bir algoritma önerilmiştir. Elde edilen anahtarlar ile görüntünün XOR işlemine tabi tutulmasından sonra satır bazında difüzyon işlemi ile görüntünün karıştırılması sağlanmıştır. Bu işlemler başlangıçta belirlenen tur sayısı kadar tekrarlanarak şifreleme işlemi tamamlanır.
Şifreli görüntü elde edilirken yapılan işlemlerin ters sırayla uygulanması sonucu orijinal görüntüye ulaşılır.

4.1. Şifreleme İşlemi

Şifreleme işlemi aşağıda anlatılan adımlardan oluşmaktadır.
Adım 1. Kullanıcıdan alınan şifrelenecek renkli görüntü gri tonlamalı resme 256x256 boyutlu olarak dönüştürülür.
Adım 2. Üretilecek anahtarlar için lojistik harita ve Julia fraktal setleri kullanılarak iki ayrı anahtar oluşturulur ve bu anahtarlar arasında XOR işlemi yapılarak şifrelemede kullanılacak asıl anahtar elde edilir.
Adım 3. Görüntüye satır bazında difüzyon işlemi uygulanır.
Adım 4. Görüntü ile anahtar arasında piksel bazında XOR işlemi uygulanır. (Anahtarlar da satır ve sütun bazında iki boyutlu oluşturulur)
Adım 5. Görüntüye çapraz difüzyon işlemi uygulanır.
Adım 6. Başlangıçta belirlenen tur sayısı kadar Adım 2'den Adım 5'e kadar işlemler gerçekleştirilir.
Adım 7. Belirlenen tur sayısına ulaşınca işlemler sonlandırılarak şifreli görüntü elde edilmiş olur.



Şekil 1. Önerilen şifreleme metodolojisinin 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.

Adım 1. Kullanıcıdan şifresi çözülecek 256x256 boyutlu şifreli görüntü alınır.

Adım 2. Görüntüye çapraz difüzyon işlemi uygulanır.

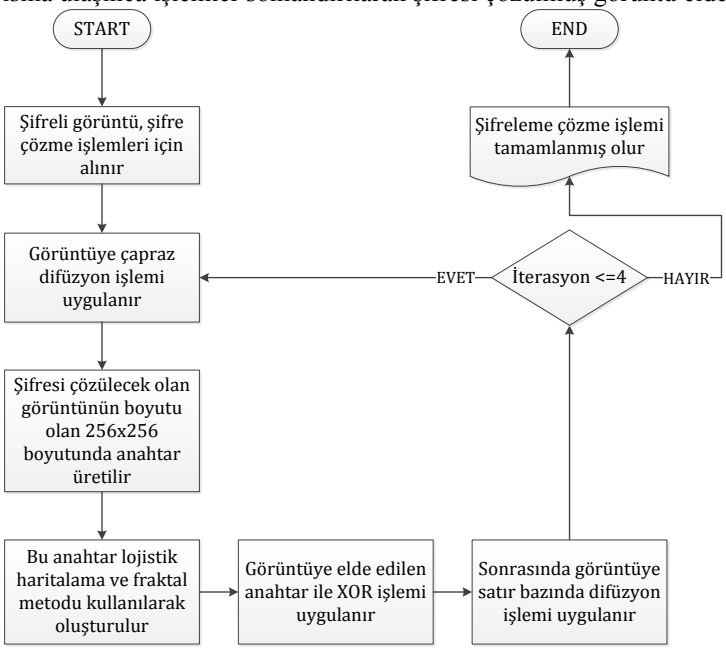
Adım 3. Lojistik kaotik harita kullanılarak üretilen anahtar ile Julia fraktal setleri ile oluşturulan anahtar birlikte XOR işlemine tabi tutularak şifre çözme işlemi için yeni bir anahtar elde edilir.

Adım 4. Şifreli görüntü ile anahtar arasında XOR işlemi uygulanır.

Adım 5. Şifreli görüntüye satır bazında ters difüzyon işlemi uygulanır.

Adım 6. Belirlenen tur sayısı kadar Adım 2'den Adım 5'e kadar işlemler gerçekleştirilir.

Adım 7. İterasyon sayısına ulaşınca işlemler sonlandırılarak şifresi çözülmüş görüntü elde edilmiş olur.



Şekil 2. Önerilen şifre çözme metodolojisinin şeması

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

5. PERFORMANS ANALİZİ

Bu bölüm, önerilen şifreleme algoritmasının güvenlik seviyesini ve hesaplama yükünü göstermek için literatürde yer alan çeşitli güvenlik analizlerinin deneysel sonuçlarını sunar. Literatürde fazlaca bilinen bir veri tabanından (https://sipi.usc.edu/database/) elde edilen test görüntüleri üzerinde gerçekleştirilen testler, aşağıdaki alt bölümlerde detaylandırılmıştır.

5.1. Anahtar Alan Analizi

Anahtar uzay analizi, görüntü şifreleme algoritmasının performans analizinin önemli kriterlerinden biridir. İyi bir şifreleme algoritması, geniş bir anahtar alanına sahip olmalı (Soni ve Acharya ,2012),ayrıca anahtar değerine duyarlı ve kaba kuvvet saldırılarına direnecek kadar büyük olmalıdır. Kriptografik açıdan,yüksek düzeyde güvenlik sağlamak için anahtar alanın boyutu 2^{128}' den küçük olmamalıdır (Akhshani ve ark., 2012). Yapılan hesaplamalara göre anahtar boyutu 2^{128}'den büyük bir değer bulunmuştur.

5.2. Bilgi Entropi Analizi

Bilgi teorisi, 1949'da depolama teorisi ve veri iletişiminin matematiksel olarak Shannon tarafından ifade edilmiştir (Agarwal, 2018). Modern bilgi teorisi, hata düzeltme, veri sıkıştırma, kriptografi, iletişim sistemleri ve ilgili konularla ilgilidir. Bu entropiyi hesaplamak için iyi bilinen bir formül vardır: (Akhshani ve ark., 2012)

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

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

Sonuç, şifrelenmiş görüntünün entropisinin ideal entropi değerine çok yakın olduğunu, yani 8 olan ve diğer mevcut algoritmaların çoğundan daha yüksek olduğunu göstermektedir. Bu, önerilen görüntü şifreleme algoritmasından bilgi sızıntısı oranının sıfıra yakın olduğunu gösterir. (Akhshani ve ark., 2012)

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

	Orijinal Görüntünün Global Entropisi	Şifreli Görüntünün Global Entropisi	Şifresi Çözülmüş Görüntünün Global Entropisi
Lena	7.431372405	7.997237194	7.431372405
House	7.229802394	7.997295383	7.229802394
Female	7.052497571	7.997135415	7.052497571

Tablo 1, 256x256 boyutundaki düz, şifreli ve şifresi çözülmüş görüntülerin global entropi sonuçlarını göstermektedir. Global Shannon entropi değerine bakıldığı zaman teorik üst sınır olan 8 değerine oldukça yakın sonuçlar elde edildiği görülür.

Global Shannon entropi ölçüsü, gerçek rastgeleliği kanıtlamak için yeterli değildir. Biri algılanabilir ve diğeri rastgele benzeri olan iki görüntü, aynı Global Shannon entropi değerlerine sahip olabilir. Bu yüzden şifreli görüntülerin rastgeleliğini doğrulamak için yalnızca bu testi kullanmak yanıltıcı olabilir (Yavuz, 2019). Bunun yerine, şifreli görüntülerin gerçek rastgeleliğini kanıtlamak için Yerel Shannon entropi testi kullanılır. Denklem 4'te yer aldığı gibi rastgele seçilmiş bir dizi örtüşmeyen bloğun yerel entropi değerlerinin ortalamasının alınması, aşağıdaki gibi tanımlanan Yerel Shannon entropi ölçümünü (Wu vd., 2013) verir.

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

Tablo 2'de görüntülerin yerel entropi değerlerine yer verilmiştir. Tüm yerel entropi sonuçları kritik değerler α=0.001 anlamlılık düzeyi için önerilen algoritmanın testi başarıyla geçtiği ifade edilebilir.

Orijinal görüntü ile şifresi çözülmüş entropi değerlerinin aynı olması şifreli ve şifresi çözülmüş görüntünün aynı olduğunu, orijinal görüntüde bir kayıp olmadığını gösterir.

Tablo 2. Düz/Şifreli/Şifresi çözünmüş görüntülerin Yerel entropi sonuçları

	Orijinal Görüntünün Yerel Entropisi	Şifreli Görüntünün Yerel Entropisi	Şifresi Çözülmüş Görüntünün Yerel Entropisi

	h_{sol}^*	$h_{sağ}^*$	h_{sol}^*	$h_{sağ}^*$	h_{sol}^*	$h_{sağ}^*$
Lena	7.0708509045	7.206199362	7.9882965855	7.9893367525	7.0708509045	7.206199362
House	7.1648415605	6.9701047055	7.9894099425	7.9896091405	7.1648415605	6.9701047055
Female	6.0881721995	7.2656222995	7.989107779	7.988304178	6.0881721995	7.2656222995

5.3. Diferansiyel Saldırı Analizi (NPCR/UACI)

Saldırganlar genellikle orijinal görüntü için küçük bir değişiklik yapar, orijinal görüntüyü değiştirmeden önce ve sonra şifrelemek için önerilen algoritmayı kullanır ve orijinal görüntü ile şifreli görüntü arasındaki ilişkiyi bulmak için iki şifreli görüntüyü karşılaştırır. Bu, diferansiyel saldırı olarak bilinir. Bir piksel değişikliğinin şifrelenmiş görüntünün tamamı üzerindeki etkisini test etmek için, araştırmacılar genellikle iki ölçü kullanır: iki görüntü arasındaki farklı piksel sayılarının yüzdesini ölçen piksel değişim hızı (NPCR); ve iki görüntü arasındaki ortalama fark yoğunluğunu ölçen birleşik ortalama değişim yoğunluğu (UACI). (Soni ve Acharya ,2012),
NPCR ve UACI metrikleri aşağıdaki gibi hesaplanabilir:

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

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

$$NPCR = \frac{Diff(D_1,D_2)}{W.H}\,.100\% \quad (7)$$

$$UACI = \frac{1}{W.H}\sum_{i=0}^{W-1}\sum_{j=0}^{H-1}\frac{|D_1(i,j) - D_2(i,j)|}{255}.100\% \quad (8)$$

Literatürde bir şifreleme algoritmasının başarılı sayılabilmesi için NPCR değerinin %99, UACI değerinin ise %33 civarı olması gereklidir (Menezes ve ark, 1996). Burada D_1 ve D_2 sırasıyla düz görüntüyü ve biraz değiştirilmiş versiyonunu temsil eder. W ve H ise şifrelenecek görüntünün genişliğini ve yüksekliğini simgelemektedir.

Tablo 3. Şifreli görüntünün diferansiyel saldırı sonuçları

	UACI	**NPCR**
Lena	33.465019675	99.629211426
House	33.140109193	99.440002441
Female	33.296837900	99.589538574

Tablo 3'te yer alan değerlere bakıldığında, yukarıda da bahsedildiği gibi NPCR ve UACI değerlerinin teorik değerlere yakın olduğu görülmektedir. Bu da algoritmanın, dışarıdan gelebilecek istatistiksel ve kaba kuvvet saldırılarına karşı dirençli olduğunu gösterir.

5.4. Gürültü Girişim Analizi (PSNR/MSE)

PSNR, görüntü işlemeden sonra şifresi çözülen görüntünün kalitesini değerlendirmek için önemli bir indekstir. PSNR ne kadar büyükse, bozulma o kadar küçüktür. Ek olarak, farklı görüntülerin PSNR'leri benzerdir, bu da önerilen algoritmanın sıkıştırma performansının kararlı olduğu anlamına gelir (Xua ve ark.,2019). İdeal olarak benzer görüntüler için PSNR sonsuzdur ve tamamen birbirinden farklı görüntüler için ise değeri sıfırdır.
Diğer bir hata ölçütü ise, PSNR ile yakından ilişkili olan MSE'dir. Bu hata metrikleri, karesi alınmış hataların ortalaması açısından iki görüntü arasındaki farklılığı ölçer. MSE'nin değeri daha yüksek, daha yüksek farklılığı gösterir. Tam olarak benzer görüntülerde MSE için ideal değer sıfırdır. (Kaur ve ark., 2020) Matematiksel olarak şu şekilde tanımlanır:

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

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

Burada I_R orijinal görüntüyü belirtirken I_E şifresi çözülmüş görüntüyü belirtir. PSNR değerinin yüksek olması, orijinal görüntüye daha yakın olduğu 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).

Tablo 4. Şifresi çözülmüş görüntünün gürültü girişim analizi sonuçları

	PSNR	**MSE**
Lena	Inf	0.000000000
House	Inf	0.000000000
Female	Inf	0.000000000

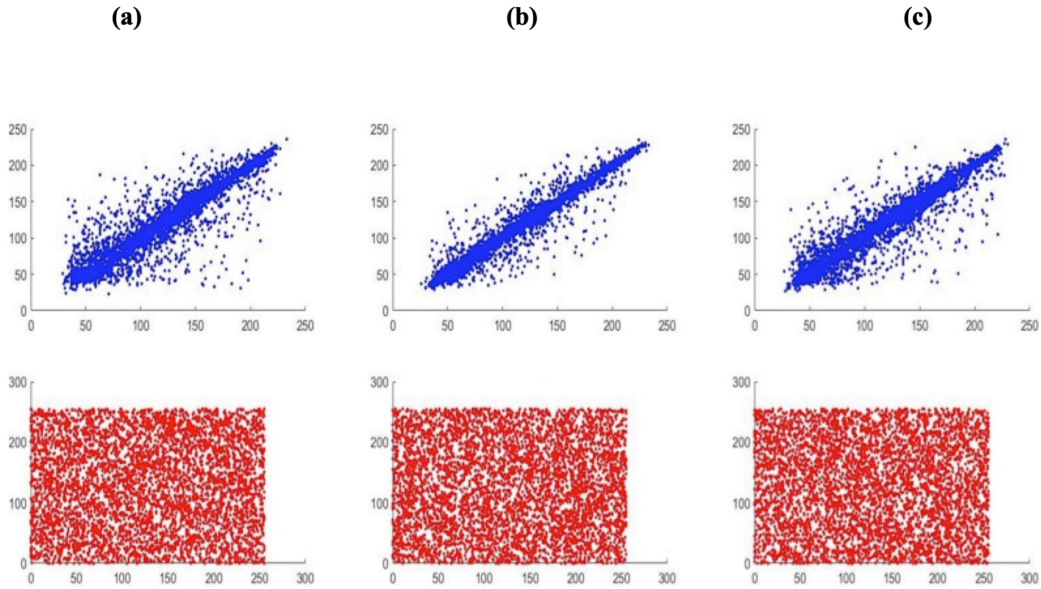
Tablo 4'te şifresi çözülmüş görüntünün gürültü girişim analizi sonuçları yer almaktadır. PSNR değerleri incelendiği zaman şifresi çözülmüş görüntünün kalitesinin bozulmadığı sonucuna ulaşılır. MSE değerinin 0 olması algoritmanın şifre çözme yöntemi ile tam olarak ilk görüntüye ulaşıldığını gösterir . PSNR sonuçlarında Inf değerinin elde edilme nedeni PSNR formülünde paydada MSE değerinin yer almasıdır ve MSE değerinin 0(sıfır) olması PSNR değerinin de Inf olarak hesaplanmasına neden olur. Bu da bizi şifresi çözülmüş görüntünün kalitesinin bozulmadığı sonucuna ulaştırır.

5.5. Korelasyon Analizi

Korelasyon katsayısı, bir görüntüdeki iki bitişik piksel arasındaki korelasyonu değerlendirir (Kumar ve Chahal, 2014). Genel olarak korelasyon, iki piksel arasındaki benzerlik derecesini ölçer. Orijinal görüntünün bitişik pikselleri, yatay, dikey ve çapraz yönlerde yüksek bir korelasyona sahiptir (Yin ve Wang, 2018). Şifreleme algoritmasının başarılı olabilmesi ve istatistiksel saldırılara direnmesi için şifrelenmiş görüntüdeki piksellerin korelasyon katsayılarını yeterince düşük yapması gerekir. Korelasyon katsayıları -1 ile +1 arasında değer alır. Korelasyon katsayısı şu şekilde hesaplanabilir:

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

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 1: Lena görüntüsü ve şifre karşılığı için (a) diyagonal , (b) dikey ve (c) yatay yönlerde bitişik piksel korelasyonları.

Korelasyon analizi testi yapılırken Lena test örneğinde 5000 piksel rastgele olarak seçildi. Diyagonal, dikey ve yatay olarak hem orijinal(üstte) hem de şifrelenmiş(altta) görüntünün korelasyonları grafik olarak Görsel 1'de verilmiştir. Şifrelemenin amacı komşu piksellerin arasındaki korelasyonları kırmak olduğu için görsele bakıldığında şifreli görüntünün pikselleri arasında dağınıklığın sağlandığı görülmüştür.

5.6. Histogram Analizi

Görüntü histogramı bir görüntüdeki piksel yoğunluğu değerlerinin dağılımını temsil eder. İyi bir güvenli şifreleme sisteminin histogramı mümkün olduğunca düz olmalıdır. Şifreli görüntünün her bir gri tonlama değerinin sayısının neredeyse eşit olduğunu gösterir, bu da şifreleme sisteminin istatistiksel saldırılara direnebileceği anlamına gelir (Yin ve Wang, 2018).

Görsel 2'de yukarıda da bahsedildiği gibi şifreli görüntünün histogramının beklenildiği gibi düz olduğu görülmektedir. Bu da görüntünün her bir piksel değerinin neredeyse eşit olduğunu gösterir.

5.7. Yapısal Benzerlik İndeksi Ölçümü (SSIM)

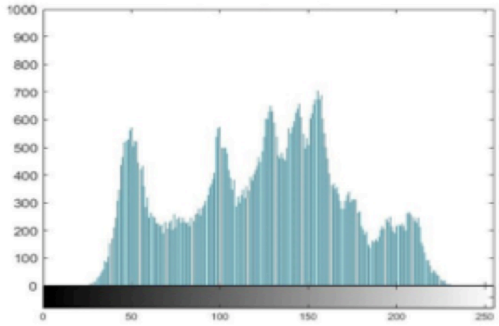
SSIM, parlaklık, kontrast ve yapının üç yönünü baz alarak orijinal görüntü ile şifresi çözülmüş görüntü arasındaki benzerliği ölçer. SSIM'in değeri 0 ile 1 arasındadır. SSIM değerinin 1'e yakın olması şifresi çözülen resmin orijinal görüntüye çok fazla benzemesi anlamına gelir.1 değerine ise yalnızca iki aynı görüntünün olması durumunda erişilebildiği gözlemlenir. (Brahim ve ark., 2020) .

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

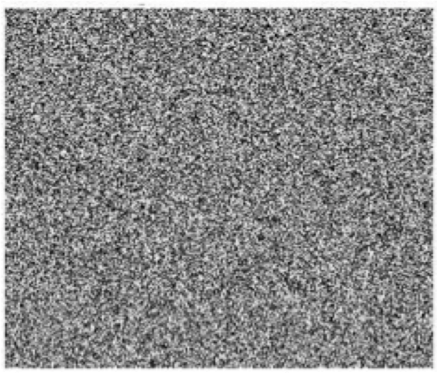
Formülde;

- 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 $2^{\text{pikseldeki bit sayısı}}$ - 1 olarak hesaplanır)
- $k_1 = 0.01$ and $k_2 = 0.03$ olarak kullanılır.

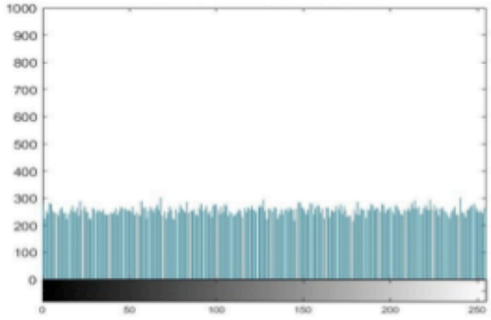
(a)



(b)



(c)



(d)

(e)

Görsel 2: Deneysel Sonuçlar: **(a)** Orijinal görüntü
(b) Orijinal görüntü histogramı
(c) Şifreli görüntü
(d) Şifreli görüntü histogramı
(e) Şifresi çözülmüş görüntü

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

	SSIM
Lena	1.000000000
House	1.000000000
Female	1.000000000

Tablo 5'te şifre çözme işlemi gerçekleştirildikten sonra elde edilen görüntü ile orijinal görüntünün yapısal benzerlik indeksi verilmiştir. Buradaki beklentimiz orijinal ve şifresi çözülmüş görüntüler arasındaki benzerlik

değerinin mümkün olduğunca büyük ve 1'e yakın bir değer olmasıdır. Tablodan da görüldüğü üzere SSIM değerinin 1 olması şifresi çözülmüş görüntü ile orijinal görüntünün birebir aynı olduğu sonucunu verir.

6. TARTIŞMA

Tablo 6'da literatürde yapılan çalışmalar ile önerilen metodolojinin karşılaştırması yapılmıştır. Yapılan güvenlik analizlerine göre önerilen algoritmada teorik değerlerin elde edildiği görülmüştür.

Tablo 6. Literatürde yer alan çalışmalar ile karşılaştırma

İlgili Çalışma	NPCR	UACI	PSNR	MSE(dB)	Şifreli Görüntü Entropisi
(Wang ve ark, 2015)	99.6094	33.4690	X	X	7.9024
(Hua ve ark, 2019)	99.6088	33.4501	X	X	X
(Diab, 2018)	55.5385	1.1776	X	X	7.9017
(Wang ve ark, 2018)	X	X	X	X	7.9022
(Wang ve ark, 2021)	99.6088	33.46	X	X	7.9023
(Krishnamoorthi ve Murali, 2014)	99.62	27.38	9.22	X	X
(Anchal ve Ravin, 2016)	99.62	33.06	X	X	X
(Harjo ve Setiadi, 2020)	99.63	28.7772	7.9758	X	7.9992
(Anees ve ark, 2014)	0.0015	0.0010	8.7671	37.69	7.8026
Önerilen metodoloji	99.6292	33.4650	Inf	0.0000	7.9972

Tablodaki değerlere bakıldığında NPCR değerlerinin literatürdeki çalışmalarla karşılaştırılması sonucu önerilen algoritmanın diğer çalışmalardan daha iyi sonuç verdiği görülmüştür. Literatürde bir şifreleme algoritmasının başarılı sayılabilmesi için NPCR değerinin %99, UACI değerinin ise %33 civarı olmasının gerekli olduğundan bahsetmiştik . Yani NPCR değerlerinin %99 civarları olması dışarıdan gelebilecek saldırılara karşı diğer çalışmalara göre daha dirençli olduğunu gösterir. UACI değerinin %33 civarı çıkması ise orijinal görüntüde yapılan küçük bir değişiklikten şifreli görüntünün tamamının etkilenmesi demektir. Her iki değer de diğer çalışmalardan daha yüksektir, ayrıca başarılı olarak kabul gören değerlere de ulaşılmıştır. Şifrelenmiş görüntünün şifresinin çözümünde bazen görüntü kalitesinde orijinal görüntüye nazaran bozulmalar yaşanabilir. Bu durumu ölçen metrik ise PSNR'dır. Önerilen algoritmada şifre çözüldüğü zaman elde edilen görüntünün kalitesinde bozulma yaşanmadığı görülmüştür. Orijinal görüntü ile şifresi çözülmüş görüntünün arasındaki fark ise MSE değerlerinden anlaşılır. Bu değerin mümkün olduğunca sıfıra yakın olması beklenir. Tezde kullanılan yöntem ile sıfır sonucu elde edilmiştir. Yani orijinal görüntü kayıpsız bir şekilde elde edilmiştir. Şifreli görüntüde bilgi sızıntısı oranının sıfıra yakın/sıfır olması, entropi değerinin 8'e yakın olmasını gerektirir. Algoritmanın bu şartı da sağladığı gözlemlenmiştir. Sonuç olarak bu tezde önerilen hibrit algoritmada elde edilen performans ve güvenlik sonuçlarına göre algoritma sonuçlarının teorik değerlere ulaştığı ve bu nedenle de kullanıma uygun ve gelişmeye açık olduğu söylenebilir.

7. SONUÇLAR VE GELECEKTEKİ ÇALIŞMALAR

Kriptografinin amacı, ister görüntü isterse başka bir veri biçimi olsun, verileri güvenli bir şekilde göndermektir. Fakat geleneksel görüntü şifreleme algoritmaları, gereken rastgelelik sağlama işleminde yetersiz kalmıştır. Bu durum kriptografinin amacı olan güvenli veri iletimine ters düşmektedir. Bu nedenle bu tez kapsamında, şifreli görüntüde yeterli rastgeleliğe ulaşarak kriptografi amacını gerçekleştirebilmek için, kaotik haritanın Julia fraktal setleri ile kullanıldığı hibrit bir çözüm sunulmaktadır. Önerilen mimari şifrelemedeki kalite, güvenilirlik ve karmaşıklığın artırılması için kullanılan Lojistik kaotik harita, rastgeleliğini arttırmak için Julia fraktal set, satır bazında difüzyon ve çapraz difüzyon olmak üzere 4 ana bileşen altında listelenebilir. Bir satır şifrelenmeden önce difüzyon işlemi yapılmıştır, sonrasında üretilen anahtarlar ile piksel bazında şifreleme yapılmıştır. Anahtarlar ise Lojistik kaotik harita ve Julia fraktal setleri ile görüntünün genişliği ve yüksekliği kadar oluşturulmaktadır. Önerilen algoritmanın daha dirençli olmasını, Julia fraktal setlerinin rastgeleliğinin katılması sağlamıştır. Önerilen algoritma, yaygın olarak kullanılan tek boyutlu kaotik sistemdeki küçük anahtar uzayı ve zayıf güvenlik dezavantajlarının üstesinden gelmektedir. Kaotik haritanın yanı sıra Julia fraktallarının kullanımı da algoritmanın yapılan performans testlerinde daha başarılı olmasını sağlamıştır.

Veri gizliğinin önemi gün geçtikçe arttığı için hastaların tıbbi görüntülerinin gizliliği de önemli bir konu haline gelmiştir. Tez kapsamında kullanılan metodoloji ile bu görüntülerin şifrelenmesi ve de veri gizliliğinin sağlanması gerçekleştirilebilir. Böylece bu görüntüler sadece veri erişimine izin verilen kişiler tarafından görüntülenerek hastanın gizliliği sağlanmış olur.
Önerilen sistemin daha yüksek bir karmaşıklık sunduğu sonuçlardan görülebilir. Bu tür kaotik dinamik sistemin yüksek karmaşıklığı, gelişmiş güvenlik ile kaotik kriptografik tekniklerde avantajlı bir şekilde kullanılabileceğini gösterir. Deneysel sonuçlar ve performans metrikleri, şifreleme algoritmasının etkili ve oldukça güvenli olduğunu göstermektedir.
Önerilen hibrit sistem görüntü şifrelemeyi amaçlasa da, sadece bu alanla sınırlı kalmayıp ve gelecekte hologramlar gibi 3 boyutlu görüntülerin şifrelenmesinde de kullanılabilirliği araştırılacaktır.

REFERANSLAR

Agarwal S.(2018) Secure Image Transmission Using Fractal and 2D-Chaotic Map. Journal of Imaging, 4, 17.

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 Volume 17, Issue 12, Pages 4653-4661

Al-Maadeed S, Al-Ali A, Abdalla T (2012) A New Chaos-Based Image-Encryption and Compression Algorithm",Hindawi Publishing Corporation, Journal of Electrical and Computer Engineering, Article ID 179693.

Al-Najjar H., AL-Najjar A.,(2011) "Image Encryption Algorithm Based on Logistic Map and Pixel Mapping Table"

Alsafasfeh Q, Arfoa A(2011). Image encryption based on the general approach for multiple chaotic systems. Journal of Intelligent Learning Systems and Applications.; 3(3): 238-244.

Anchal J, Navin R (2016), "A robust image encryption algorithm resistant to attacks using DNA and chaotic logistic maps," Multimed. Tools. Appl., Vol. 75, no. 10, pp. 5455–72.

Anees A., Siddiqui A. M., Ahmed F. (2014) ''Chaotic substitution for highly autocorrelated data in encryption algorithm,'' Commun. Nonlinear Sci. Numer. Simul., vol. 19, no. 9, pp. 3106–3118.

Askar S.; Karawia A.; Al-Khedhairi A.; Al-Ammar F.(2018) "An Algorithm Of Image Encryption Using Logistic and Two-Dimensional Chaotic Economic Maps", Entropy, MDPI,Vol.20, Issue 1.

Baker G, Gollub J .(1996) Chaotic dynamics: an introduction. Cambridge University Press; second ed.

Barnsley, M.F., Demko S.(1985) 'Iterated function systems and the global construction of fractals', Proc. R. Soc. Lond. A, Math. Phys. Sci., 399, pp. 243–275

Brahim A., Pacha A., Said H. (2020) Image encryption based on compressive sensing and chaos systems, Optics & Laser Technology Volume 132, 106489

Diab H. (2018) An efficient chaotic image cryptosystem based on simultaneous permutation and diffusion operations. IEEE Access;6:42227–44.

Edgar G.(2004). Classics on Fractals. Boulder, CO: Westview Press. ISBN 978-0-8133-4153-8.

El-Latif A., El-Atty B., Talha M,(2018) "Robust Encryption of Quantum Medical Images", IEEE Access, vol. 6, pp. 1073 – 1081

Hua Z, Zhou Y, Huang H. (2019)Cosine-transform-based chaotic system for image encryption. Inform Sci;480:403–19.

Kaur G, Agarwal R, Patidar V. (2020) Chaos based multiple order optical transform for 2D image encryption, Engineering Science and Technology, an International Journal 23, 998–1014

Khanzadi H, Eshghi M, Borujeni S (2014). Image encryption using random bit sequence based on chaotic maps. Arabian Journal for Science and engineering; 39(2): 1039-1047.

Krishnamoorthi R, Murali P (2014) "Chaos based image encryption with orthogonal polynomials model and bit shuffling," in Proceedings of the IEEE International Conference on Signal Processing and Integrated Networks, Noida India, pp. 107–12.

Kumar M., Chahal A.(2014) Effect of Encryption Technique and Size of Image on Correlation Coefficient in Encrypted Image, International Journal of Computer Applications (0975 – 8887), Volume 97– No.12

Li T., Du B., Liang X. (2020). Image Encryption Algorithm Based on Logistic and Two-Dimensional Lorenz. IEEE Access, 8, 13792–13805.

Liu H, Zhao B, Huang L,(2019) "A RemoteSensing Image Encryption Scheme Using DNA Bases Probability and Two-Dimensional Logistic Map", IEEE Access, vol. 7, pp. 65450–65459.

Liu J, Zhang L,Yue G (2003). "Fractal Dimension in Human Cerebellum Measured by Magnetic Resonance Imaging". Biophysical Journal. 85 (6): 4041–4046

Liu L., Lei Y., Wang D. (2020). A Fast Chaotic Image Encryption Scheme with Simultaneous Permutation-Diffusion Operation. IEEE Access, 8, 27361–27374.

Liu L., Wang D., Lei Y. (2020). An Image Encryption Scheme Based on Hyper Chaotic System and DNA with Fixed Secret Keys. IEEE Access, 8, 46400–46416.

Lu Q., Zhu C., Deng X. (2020). An Efficient Image Encryption Scheme Based on the LSS Chaotic Map and Single S-Box. IEEE Access, 8, 25664–2567

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

Roy A., Misra A. P., Banerjee S.(2017) "Chaos-based image encryption using vertical-cavity surface-emitting lasers", arXiv preprint arXiv: 1705.00975

Segal S. (1978). "Riemann's example of a continuous 'nondifferentiable' function continued". The Mathematical Intelligencer. 1 (2): 81–82

Soni A, Acharya A,(2012) A Novel Image Encryption Approach using an Index based Chaos and DNA Encoding and its Performance; International Journal of Computer Applications 47(23):1-6

Trochet H. (2009). "A History of Fractal Geometry". MacTutor History of Mathematics

Wade M., Chouikha M., Gill T.; Patterson W., Washington T,(2019) "A Dual Layer Image Encryption using Polymerase Chain Reaction Amplification and DNA Encryption", IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON).

Wang L, Ye Q, Xiao Y, Zou Y, Zhang B. (2008), An image encryption scheme based on cross chaotic map. Congress onImage and Signal Processing; 3: 22-26.

Wang T., Song L., Wang M., Zhuang, Z. (2020). A novel image encryption algorithm based on parameter-control scroll chaotic attractors. IEEE Access, 8, 36281–36292.

Wang W, Si M, Pang Y, Ran P, Wang H, Jiang X, Liu Y, Wu J, Wu W, Chilamkurti N, et al(2018). An encryption algorithm based on combined chaos in body area networks. Comput Electr Eng;65:282–91.

Wang X, Wang Q, Zhang Y (2015). A fast image algorithm based on rows and columns switch. Nonlinear Dynam;79(2):1141–9

Wang X., Liu L. (2020). Image Encryption Based on Hash Table Scrambling and DNA Substitution. IEEE Access, 8, 68533–68547.

Xua Q, Suna K., Caoa C., Zhub C.(2019) A fast image encryption algorithm based on compressive sensing and hyperchaotic map. Optics and Lasers in Engineering (121) 203–214

Yin Q, Wang C. (2018) A New Chaotic Image Encryption Scheme Using Breadth-First Search and Dynamic Diffusion, International Journal of Bifurcation and Chaos, Vol. 28, No. 4

İNTERNET KAYNAKLARI

https://geoffboeing.com/2015/03/chaos-theory-logistic-map/

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, Bahar Arıtürk tarafından yürütülecek olan, "Yeni Julia Fraktal Setleri Kullanarak Yeni Bir Şifreleme Yöntemi Önerilmesi ve Analizlerin Gerçekleştirilmesi" başlıklı yüksek lisans tezinin ön çalışmalarından yararlanılarak hazırlanmıştır.*