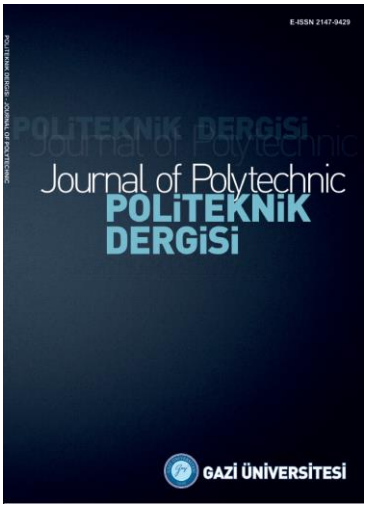


POLİTEKNİK DERGİSİ

JOURNAL of POLYTECHNIC

ISSN: 1302-0900 (PRINT), ISSN: 2147-9429 (ONLINE)
URL: http://dergipark.org.tr/politeknik

Tarama modeli kullanan karma bir görüntü şifreleme yöntemi

A hybrid color image encryption method using a scan pattern

***Yazar(lar) (Author(s))**: Nurettin DOĞAN[1] , Hidayet ÇELİK[2]*

ORCID[1]: 0000-0002-8267-8469

ORCID[2]: 0000-0002-9898-6925

Bu makaleye şu şekilde atıfta bulunabilirsiniz(To cite to this article): Doğan N. ve Çelik H., "Tarama modeli kullanan karma bir görüntü şifreleme yöntemi", ***Politeknik Dergisi***, 25(4): 1475-1485, (2022).

Erişim linki (To link to this article): http://dergipark.org.tr/politeknik/archive

DOI: **10.2339/politeknik.902661**

Tarama Modeli Kullanan Karma Bir Görüntü Şifreleme Yöntemi

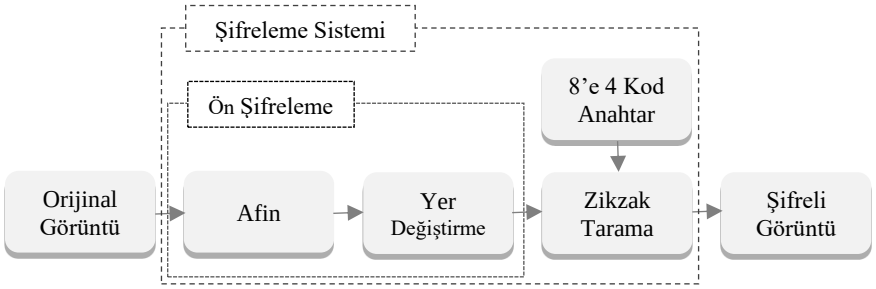
A Hybrid Color Image Encryption Method Using A Scan Pattern

Önemli noktalar (Highlights)

- *Renkli görüntü şifreleme / Color image encryption*
- *Afin şifreleme / Affine cipher*
- *Zikzak tarama modeli / Zigzag scan pattern*

Grafik Özet (Graphical Abstract)

Bu çalışmada, görüntü şifrelenmesi için kullanılabilecek geleneksel kripto sistemlerinden oluşan karma bir şifreleme yöntemi önerilmiş ve bu yöntem uygulama ile anlatılmıştır. / In this study, a hybrid encryption method consisting of traditional crypto systems that can be used for image encryption has been proposed and this method has been described by application.



Şekil. Şifreleme sisteminin blok diyagramı **/ Figure.** Block diagram of the encryption system

Amaç (Aim)

Görüntü şifreleme için kullanılabilecek geleneksel kripto sistemlerinden oluşan karma bir şifreleme yöntemin kullanılabilirliği amaçlanmaktadır. / It is aimed at the usability of a hybrid encryption method consisting of traditional crypto systems that can be used for image encryption

Tasarım ve Yöntem (Design & Methodology)

Geleneksel kripto sistemlerinden Sezar, Afin, Yer değiştirme ve Vigenere yöntemleri görüntü üzerindeki piksel renk değerleri ve piksel konumlarına ayrı ayrı uygulanarak şifreleme performansları incelenmiştir. / The traditional crypto systems such as Caesar, Affine, Substitution and Vigenere methods have been applied separately to pixel color values and pixel positions on the image, and encryption performance has been studied.

Özgünlük (Originality)

Afin ve yer değiştirme kripto sisteminin beraber kullanılarak yapıldığı bir şifreleme yöntemi önerilmiştir. Şifrelenen görüntü daha sonra 8'e 4 kod ve zikzak tarama modeli kullanılarak kuvvetlendirilmiştir. / A method of encryption has been proposed, in which Affine and Substitution cipher systems are performed together. Then the encrypted image has been strengthened using by 4 out of-8 codes and a zigzag scan pattern.

Bulgular (Findings)

Önerilen şifreleme algoritması ile işlem sonucunda hiçbir veri kaybı ya da değişikliği olmadan orijinal görüntünün tekrar elde edildiği gözlemlendi. / It was observed that the original image was recovered without any loss or change of data as a result of the operation with the proposed encryption algorithm.

Sonuç (Conclusion)

Elde edilen test sonuçları doğrultusunda önerilen algoritmanın görüntü şifreleme işlemlerinde kullanılabileceği uygun görülmektedir. / According to test results, it seems appropriate that the proposed algorithm can be used in image encryption operations.

Etik Standartların Beyanı (*Declaration of Ethical Standards*)

Bu makalenin yazar(lar)ı çalışmalarında kullandıkları materyal ve yöntemlerin etik kurul izni ve/veya yasal-özel bir izin gerektirmediğini beyan ederler. / The author(s) of this article declare that the materials and methods used in this study do not require ethical committee permission and/or legal-special permission.

Tarama Modeli Kullanan Karma Bir Görüntü Şifreleme Yöntemi

Araştırma Makalesi / Research Article

Nurettin DOĞAN*, Hidayet ÇELİK,

Teknoloji Fakültesi, Bilgisayar Mühendisliği Bölümü, Selçuk Üniversitesi, Türkiye

(Geliş/Received : 24.03.2021 ; Kabul/Accepted : 06.04.2021 ; Erken Görünüm/Early View : 10.06.2021)

ÖZ

Bu çalışmada, görüntü şifrelenmesi için kullanılabilecek geleneksel kripto sistemlerinden oluşan karma bir şifreleme yöntemi önerilmiş ve bu yöntem uygulama ile anlatılmıştır. İnternetin yaygın olarak kullanılması ve paylaşılanlara 3. Şahısların erişebiliyor olma durumu ve düşüncesi metin ve görsellerin şifrelenerek dijital ortamda gönderilmesi zorunluluğunu doğurmuştur. Geleneksel kripto sistemler metin şifrelemede kullanılmasına rağmen, görüntü şifrelenmesinde yüksek korelasyon ve veri miktarından dolayı tercih edilmediği görülmüştür. Kriptoloji ile ilgili genel bilgi verildikten sonra bazı güncel görüntü şifreleme algoritmalarına ve bu algoritmaların özelliklerine değinilmiştir. Geleneksel kripto sistemlerinden Sezar, Afin, Vigenere ve Yer değiştirme yöntemleri görüntü üzerindeki piksel renk değerleri ve piksel konumlarına ayrı ayrı uygulanarak şifreleme performansları incelenmiştir. Afin ve yer değiştirme kripto sisteminin beraber kullanılarak yapıldığı bir şifreleme yöntemi önerilmiştir. Şifrelenen görüntü daha sonra 8'e 4 kod ve zikzak tarama modeli kullanılarak kuvvetlendirilmiştir. Performans analizleriyle önerilen yöntem değerlendirilmiştir.

Anahtar Kelimeler: Şifreleme, renkli görüntü şifreleme, afin şifreleme, zikzak tarama modeli, veri güvenliği.

A Hybrid Color Image Encryption Method Using A Scan Pattern

ABSTRACT

In this study, a hybrid encryption method consisting of traditional crypto systems that can be used for image encryption has been proposed and this method has been described by application. The fact that the internet is widely used and third parties can access what is shared has led to the need for text and images to be encrypted and sent digitally. Although traditional crypto systems are used in text encryption, it has been found that image encryption is not preferred due to high correlation and the amount of data. After giving general information about cryptology, some current image encryption algorithms and the properties of these algorithms have been mentioned. The traditional crypto systems such as Caesar, Affine, Vigenere and Substitution methods have been applied separately to pixel color values and pixel positions on the image, and encryption performance has been studied. A method of encryption has been proposed, in which Affine and Substitution cipher systems are performed together. Then the encrypted image has been strengthened using by 4 out of-8 codes and a zigzag scan pattern. The proposed method has been evaluated with performance analyses.

Keywords: Encryption, color image encryption, affine cipher, zigzag scan pattern, data security.

1. GİRİŞ (INTRODUCTION)

İnsanoğlunun var olduğundan beri bilgi hayatımızda değerli bir yere sahip olmuştur. Bilginin aktarılırken güvenli ve gizli bir şekilde yapılması da hayatımızda büyük önem taşımıştır. Aktarılmak istenen bilgilerin ilgisiz kişiler tarafından kolayca ulaşılmaması ve anlaşılmaması için çeşitli şifreleme yöntemleri kullanılmıştır. M.Ö. 400 yıllarında Antik Yunanlıların kullandığı Scytale yöntemi ve daha sonra M.Ö. 50 yıllarında Sezar'ın kullandığı şifreleme yöntemi en temel yöntemlerdir [1].

Şifreleme gizleme bilimi anlamına gelen, cruptos ve logos kelimelerinin birleşiminden oluşan kriptoloji olarak da bilinmektedir [2]. Kriptolojide orijinal metin, düz metin (plaintext), şifrelenmiş metin ise şifreli metin (ciphertext) olarak isimlendirilir [3]. Düz metin bir anahtar kullanılarak şifreli metin haline getirilirse şifreleme işlemi (encryption) gerçekleştirilmiş olur. Bu işlem ile bilgi başkasının anlayamayacağı şekle dönüştürülmüş olur. Düz metni şifrelerken kullanılan anahtara sahip kişiler bu anahtar sayesinde, şifreli metni şifre çözme (decryption) işlemi yaparak tekrar orijinal haline geri çevirebilirler [4]. Şekil 1'de şifreleme ve şifre çözme adımları gösterilmiştir [5].

Şekil 1. Şifreleme ve Şifre Çözme İşlemleri (The encryption and decryption steps)

Burada şifreleme ve şifre çözmede kullanılan temel mantık şekillendirilmiştir. En basitinden bir kelime şifrelenecekse bu bir anahtar ve bir algoritma ile gerçekleştirilir. Çözme işlemi için ise şifreli kelimeyi

*Sorumlu Yazar (Corresponding Author)
e-posta : ndogan@ymail.com

alan kişinin, şifrelemede kullanılan anahtar ve algoritmayı bilmesi gerekir. Görüntü şifreleme işlemlerini bu mantıkta düşünebiliriz. Orijinal görüntü anahtar veya anahtarlar kullanılarak çeşitli algoritmalarla piksel konum veya değer bilgileri karıştırılarak şifrelenebilir. Şifreleme kaotik yapılarla daha karmaşık ve çözülmesi zor duruma getirilebilir. Şifreli görüntüyü alan kişilerin çözme işlemi için başlangıçta kullanılan bu anahtarları ve kullanılan şifreleme algoritmalarını bilmesi gerekir.

21. yüzyıl ile beraber bilgi ve iletişim teknolojileri önemli ölçüde gelişmiştir. Dijital dönüşümle beraber kişisel bilgilerimizin yanı sıra devletlerin ya da kurumların askeri, ticari vb. stratejik bilgileri dijital ortamda bulunabiliyor ve bu önemli büyük veriler bulut teknolojilerinde işlenip saklanabiliyor [6]. Veriye hızlı bir şekilde ulaşıp işlem yapmak bürokrasi açısından kişi, kurum veya devletlere çok büyük bir zaman avantajı sağlasa da, değerli bilgilerin ağ ortamında bulunması ilgisiz 3. şahısların, dijital korsanların ya da teröristlerin her zaman iştahını kabartacaktır. Bu yüzden bilgi gizliliği ve güvenliği son derece önemlidir. Kriptoloji ise bu aşamada bir çözüm yolu olarak kullanılmaktadır. Metin mesajların yanı sıra değerli bilgi içeren görüntülerin de şifrelenerek ağ ortamından aktarılması gerekebilir. Klasik şifreleme yöntemleri metin mesajları üzerinde etkili sonuçlar göstermektedir. Görüntü şifreleme de ise genellikle kaotik şifreleme yöntemleri tercih edilmektedir. Görüntü şifrelemede kaotik sistemlerin tercih edilmesinin en büyük nedeni, şifrelemede kullanılan anahtardaki çok küçük değişikliğin bile orijinal görüntü hakkında bilgi veremeyecek durumda olmasıdır. Oysa klasik yöntemler kullanılarak yapılan şifrelemede, piksellerdeki renk değişikliği ya da piksel konumlarındaki küçük değişiklikler orijinal görüntü ya da görüntü içindeki bilgi hakkında çıkarım yapma imkanı sunacaktır.

Bu çalışmada metin şifreleme için kullanılan afin ve yer değiştirme şifreleme yöntemleri ile bir karma şifreleme yöntemi üzerinde durulacaktır. Bu iki algoritmayla renk ve konum değerleri değiştirilen görüntü üzerine, 4 biti '1', 4 biti '0' olan 8'e 4 kod ile oluşturulan şifreleyici kelime ile şifrelenmek istenen görüntü boyutunda zikzak tarama modeli kullanılarak elde edilen şifreleyici görüntünün eklenmesiyle şifreli görüntü oluşturulacaktır. Önerilen şifreleme yöntemi kaotik sistem kullanan şifreleme yöntemi değildir, bu yüzden kaotik sistemler kadar karmaşık değildir ve uygulanabilirliği daha kolaydır. Performans analizleri yapıldıktan sonra literatürde kullanılan şifreleme yöntemleriyle kıyaslamaları yapılacaktır.

2. İLGİLİ ÇALIŞMALAR (RELATED WORKS)

Bu bölümde, bazı güncel görüntü şifreleme algoritmalarına ve bu algoritmaların özelliklerine değinilmiştir.

Atalay vd., çalışmalarında şifreleme yöntemlerini permütasyon, yer değiştirme, permütasyon ve yer değiştirme olarak kategorilendirip yaygın kullanılan görüntü şifreleme algoritmalarının performanslarını karşılaştırmışlardır. Çalışmaları sonucunda Vigenere algoritmasının frekans analizi saldırılarına karşı, DES (Data Encryption Standard - Veri Şifreleme Standardı) algoritmasının ise diferansiyel ataklara karşı zayıf olduğunu göstermişlerdir. AES (Advanced Encryption Standard - Gelişmiş Şifreleme Standardı) algoritmasının en büyük dezavantajının yüksek maliyetinin olduğunu, RC4 algoritmasının ise hızlı ve istatistiksel olarak iyi özelliği sahip olduğunu belirtmişlerdir. BZ [7] algoritması yüksek gürültü oranına sahip olması yanında kaotik yapılarla beraber steganografi kullanarak güvenli sistem oluşturabileceği sonucu elde edilmiştir [8].

BZ algoritması ön şifreleme yöntemiyle görüntü şifreleme gerçekleştiren bir yöntemdir. Permütasyon ve yer değiştirmeyle şifrelenen görüntüye daha sonra bir referans görüntü ayrık dalgacık dönüşüm kullanılarak eklenmesiyle nihai şifreleme sonucu elde edilmektedir. Bu yöntemde şifreli görüntü normal bir görüntüye benzediği için saldırganların ayırt etmesi zorlaşmaktadır [7].

Farklı sistemlerle piksel değerlerini veya konumlarını değiştirerek görüntü şifreleme algoritması öneren çalışmalar olmuştur. Bhatnagar vd., güvenli olmayan kanallar üzerinden iletişimde görüntü güvenliğini sağlamak için bir şifreleme algoritması önermişlerdir. Bu çalışmada kesirli dalgacık dönüşümü ve kaotik haritaları kullanmışlardır [9]. Hua vd., iki boyutlu sinüs-lojistik modülasyon haritası üzerinde çalışmışlardır. Görüntüdeki piksel konumlarını etkin bir şekilde değiştirmek için kaotik dönüşüm önermişlerdir. Mevcut kaotik haritalarla karşılaştırıldığında, daha geniş kaotik menzile, hiper kaotik özelliğe ve düşük uygulama maliyetine sahip olduğunu söylemişlerdir [10].

Kumari vd., çalışmalarında 10 tane geleneksel ve 5 tane kaotik şifreleme tekniğini karşılaştırmıştır. İnceledikleri kaotik şifreleme teknikleriyle, yüksek görsel olarak karıştırılmış tek tip histogramlara sahip şifreli görüntüler elde edildiği görülmüştür. Ayrıca bu tekniklerdeki yatay, dikey ve diagonal korelasyon katsayılarının çok düşük olduğu, bu sayede şifreli görüntülerin istatistiksel saldırılara karşı yüksek direnç göstereceği sonucuna varmışlardır. Kaotik şifreleme tekniklerindeki anahtar hassasiyetinin yüksek olması diferansiyel saldırılara karşı dirençli olacağını da göstermektedir. İnceledikleri geleneksel şifreleme teknikleri ise özellikle görüntüler için tasarlanmamıştır. Bu yüzden zayıf piksel değişim hassasiyeti gösterdikleri ve diferansiyel saldıra karşı zayıf olacakları sonucuna varmışlardır. Performans değerlendirmek için en önemli kriterlerden birinin zaman olduğu, zamanın sınırlı olduğu durumlarda kaotik sistemlerle birlikte geleneksel şifreleme tekniklerinden AES ve RC4 şifreleme tekniklerinin etkili olabileceği sonucuna varılmıştır [11].

Nag vd., çalışmalarında konum dönüştürme tabanlı şifreleme tekniği önermişlerdir. Dört adet 8 bitlik anahtarla afin dönüşüm tekniğini kullanarak piksel

değerlerini farklı konumlarla değiştirmişlerdir. Dönüştürülen görüntü daha sonra 2x2 piksel bloklara bölünerek ve her blok XOR işlemi ile 8 bitlik 4 anahtarla şifrelenmiştir. Afin dönüşümden sonra piksel değerleri arasındaki korelasyonun önemsiz olduğunu kanıtlanmıştır [12].

Zhu vd., bit düzeyinde permütasyon ve piksel düzeyinde difüzyon işlemi ile yapılan bir görüntü şifreleme üzerinde çalışmışlarıdır. Bit düzeyinde permütasyonu, her pikseli 8 bite dönüştürdükten sonra konumlarını Arnold map ile tekrar düzenlemişlerdir. Piksel düzeyindeki difüzyon işleminde, permütasyonlu görüntünün gri değerini ve histogram dağılımını değiştirmek için afin şifre uygunlanmıştır. Çalışmaları sonucunda önerilen algoritmanın sıradan permütasyon-difüzyon tipi görüntü şifrelemeyle rekabet edebileceğini ve pratik görüntü şifreleme için uygun olabileceğini göstermişlerdir [13].

Ke vd., şifreleme anahtar güvenliğini artırmak ve şifrelenmiş görüntünün daha iyi difüzyon etkisini elde etmek için afin şifreleme kullanan görüntü şifreleme algoritması çalışmışlardır. Önce Lorenz kaos dizisini kullanarak piksellerin konumu karıştırılmış sonra piksel değerlerini dağıtmak ve karıştırmak için afin şifresi kullanılmıştır. Çalışma sonucunda algoritmanın XOR şifrelemeye kıyasla daha iyi bir difüzyon etkisine sahip olduğu ve daha iyi şifreleme güvenliği sağladığı gösterilmiştir [14].

Rad vd., görüntü şifreleme için çalışmalarında üç bağımsız adımda tarama modellerini ve XOR işlevini kullanmışlardır. Önerilen algoritmayı kullanarak, şifreleme ve şifre çözme işlemi için bilgi kaybı olmadan orijinal görüntünün yeniden üretilmesi sağlamışlardır. Algoritmanın, diğer yaklaşımlarla karşılaştırılabilecek kadar hızlı olduğunu ve tüm güvenlik gereksinimlerini karşıladığını söylemişlerdir [15].

Panduranga ve Kumar, tarama modelleri tarafından oluşturulan taşıyıcı görüntü ile görüntü şifreleme tekniği önermişlerdir. Çalışmalarında taşıyıcı görüntüyü alfanümerik anahtar kelime yardımıyla oluşturmuşlardır. Oluşturulan bu taşıyıcı görüntü, şifreli görüntü elde etmek için orijinal görüntü ile eklenmiştir [16].

Literatürdeki araştırmalardan da görüldüğü üzere, görüntü şifreleme üzerinde farklı yöntemler kullanılmıştır. Çoğunlukla permütasyon ve difüzyon işlemleriyle pikseller üzerinde değişikliklere gidilmiştir. Şifreleme işlemlerinde kaotik yapılarla anahtarlara müdahale edilmiş, anahtar uzayları genişletilerek anahtar hassasiyeti artırılmıştır. Farklı tarama modelleriyle görüntü üzerindeki piksellere işlemler yapılmış ya da bu tarama modelleriyle oluşturulan görüntüler orijinal görüntülere eklenerek pikseller arası korelasyon katsayısının azaltılması hedeflenmiştir. Hızlı bir iletişim için açık ağların kullanılmasına devam edildiği sürece önemli bilgi içeren görüntülerin şifrelenmesine her zaman ihtiyaç duyulacaktır. Burada şifreleme ve çözme işlemlerinde hızlı ve/veya saldırılara karşı kuvvetli algoritmaya sahip yöntemlerin tercih edilebilir.

Bu çalışmamızda öncelikle metin şifreleme için kullanılan algoritmaların görüntü şifrelemede kullanılabilirliği gösterilecektir. Şifreleme işlemi 256X256 boyutlarındaki renkli Lena fotoğrafı üzerinde piksel değerleri ve piksel konumları değiştirilerek gösterilecektir. Daha sonra literatürdeki bazı çalışmalarda da kullanılan afin şifreleme işlemine yer değiştirme şifrelemesinin ve 8'e 4 kod ve zikzak tarama modeli kullanılarak oluşturulan taşıyıcı görüntünün eklenmesiyle gerçekleştirilen şifreleme yönteminden bahsedilecektir.

Önerilen yöntemin sonuçları 4. bölümde detaylı bir şekilde incelenecektir. Bu bölümde de görülebileceği üzere yöntem kaotik bir sistem olmasa bile, kullanılan farklı anahtarlar sayesinde şifrelenmiş görüntüdeki karmaşıklık daha basit bir uygulamayla elde edilebilecektir. Afin ve yer değiştirme gibi metin şifrelemede kullanılan yöntemlerin görüntü şifrelemede de başarılı sonuç verebileceği gösterilecektir. Önerilen yöntemin literatürdeki aynı resmi kullanarak kaotik şifreleme yapan bazı farklı çalışmaların sonuçlarından başarılı sonuçlar elde ettiği gösterilecektir.

3. ÖN HAZIRLIKLAR VE ÖNERİLEN YÖNTEM (PRELIMINARIES AND PROPOSED METHOD)

Makalenin bu bölümünde, öncelikle ön bilgi verilecek ve ardından önerilen yöntem anlatılacaktır.

3.1. Ön Hazırlıklar (Preliminaries)

Bu alt bölümde makale için gerekli bazı ön bilgiler uygulamalarla birlikte verilecektir.

3.1.1. Sezar şifreleme (Caesar cipher)

Modüler aritmetik kullanılarak yapılan şifreleme işlemidir. Şifreleme için İngiliz alfabesinin kullanıldığı düşünülürse 26 harf, 0-25 arasındaki tam sayılarla ifade edilir.

$$e_k(x) = x + k \ (mod\ 26) \quad (1)$$

$$d_k(y) = y - k \ (mod\ 26) \quad (2)$$

Denklem (1) şifreleme için kullanılırken, Denklem (2) şifre çözme için kullanılır. Burada k, şifreleme ve şifre çözme işleminde kullanılan anahtardır.

Dijital görüntülerde rengi oluşturan bir pikselin değeri 0-255 arasındaki sayılarla ifade edildiğinden, Sezar şifrelemeyi görüntü şifreleme ve çözme işlemlerinde kullanmak istersek Denklem (1) ve Denklem (2)'deki mod işlemi 256'ya göre yapmamız gerekir. K anahtar bilgisini '150' olarak seçersek Sezar şifreleme ile elde edeceğimiz görüntü Şekil 2 (b)'deki gibi olacaktır.

Piksel konumları değiştirilerek şifreleme yapıldığında, bir pikseli aynı satırda kaydıracağımızı düşünürsek mod işlemi resmin genişliği baz alınarak yapılmalıdır. K anahtar bilgisini '150' olarak seçersek Sezar şifreleme ile elde edeceğimiz görüntü Şekil 2 (c)'deki gibi olacaktır.

Şekil 2 (b) ve (c)'den görüldüğü üzere, Sezar şifrelemenin tek başına görüntü şifreleme yetersiz olacağı kesindir.

3.1.2. Afin şifreleme (Affine cipher)

$$e_k(x) = ax + k \ (mod\ 26) \quad (3)$$

$$d_k(y) = a^{-1}(y - b) \ (mod\ 26) \quad (4)$$

Denklem (3) bir metni şifrelemek için kullanılacak fonksiyondur. Denklem (4) ise şifreli metni çözmek için kullanılır. Burada a ve b, şifreleme ve şifre çözme işleminde kullanılan iki anahtardır. Şifre çözme işleminin düzgün yapılabilmesi için, EBOB(a,26) =1 olmalıdır. Yani a anahtarı 26 ile ortak böleni olmayacak şekilde seçilmelidir, b anahtarı ise 0-25 arasında herhangi bir değer olabilir.

Afin şifrelemeyi dijital görüntülerde piksel değerine uygulanacak şekilde kullanmak istersek, a anahtarını 256 ile ortak böleni olmayacak şekilde seçmemiz gerekir. a anahtar değerini '13', b anahtar değerini '100' olarak seçersek afin şifreleme ile elde edeceğimiz görüntü Şekil 2 (d)'deki gibi olacaktır.

Piksel konumları değiştirmek için seçeceğimiz a anahtarı resmin genişlik değerine göre ortak böleni olmayacak şekilde seçilmelidir. a anahtar değerini '13', b anahtar değerini '100' olarak seçersek afin şifreleme ile elde edeceğimiz görüntü Şekil 2 (e)'deki gibi olacaktır.

Şifreli görüntüler incelendiğinde piksel değerlerinin resmin tamamına homojen bir şekilde dağılmadığını görebiliyoruz. Birtakım saldırılarla görüntü bilgisine ulaşılabileceği açıktır.

3.1.3. Vigenere şifreleme (Vigenere cipher)

Vigenere şifrelemede şifrelenecek metin m uzunluğundaki anahtar kelime ile şifrelenir. Anahtar kelimedeki her bir harf k anahtarını temsil eder. Şifrelenecek metin m uzunluğundaki blok bölünür, bloklardaki aynı harfler anahtar metinden dolayı farklı değerlere sahip olarak şifrelenebilir.

$$e_k(x_1, x_2, .., x_m) = (x_1 + k_1, x_2 + k_2, .., x_m + x_m) \quad (5)$$

$$d_k(y_1, y_2, .., y_m) = (y_1 - k_1, y_2 - k_2, .., y_m - y_m) \quad (6)$$

Denklem (5) şifreleme için, Denklem (6) şifre çözme için kullanılacak fonksiyondur. Buradaki işlemler mod 26'ya göre yapılır.

Dijital görüntülerde Vigenere yöntemi kullanılarak piksel değerleri üzerinde bir şifreleme işlemi yapılacaksa fonksiyonlardaki işlemleri 256'ya göre mod alarak yapmak gerekir. Şekil 6'daki şifrelemede m uzunluğundaki anahtar, orijinal görüntü üzerindeki piksel değerleri kullanılarak seçildi. Orijinal resmin 100. satır 100. sütundan başlayarak alınan 100 pikselin değerinden oluşan anahtar ile şifreleme yapıldığında şifreli görüntü Şekil 2 (f)'deki gibi olacaktır.

Piksel konumlarını değiştirerek şifrelemede seçilen m uzunluğundaki blok için değerler rastgele sıralanır. Pikselin yeni konumu bloktaki ile yer değiştirir. Satır boyunca blok kaydırılarak işlemler tekrar edilir. Örneğin şifreleme için blok uzunluğu 128 seçildiğinde Şekil 2 (g)'deki şifreli görüntü elde edilmiştir.

Vigenere şifreleme yöntemiyle piksel değeri ve konumu değiştirilerek yapılan her iki işlemde de şifreleme sonuçlarının tatmin etmeyeceği görülmektedir.

3.1.4. Yer değiştirme şifrelemesi (Substitution cipher)

Yer değiştirme şifreleme anahtar sadece 26 harfin permütasyonudur. Olabilecek permütasyonların sayısı ise 26!'dir. Sezar şifreleme bunlardan bir tanesine örnek olarak verilebilir.

$$e_k(x) = \pi(x) \quad (7)$$

$$d_k(y) = \pi^{-1}(y) \quad (8)$$

Şifreleme için Denklem (7), şifre çözme için Denklem (8) kullanılır. Burada π mümkün olan permütasyonlardan bir tanesidir.

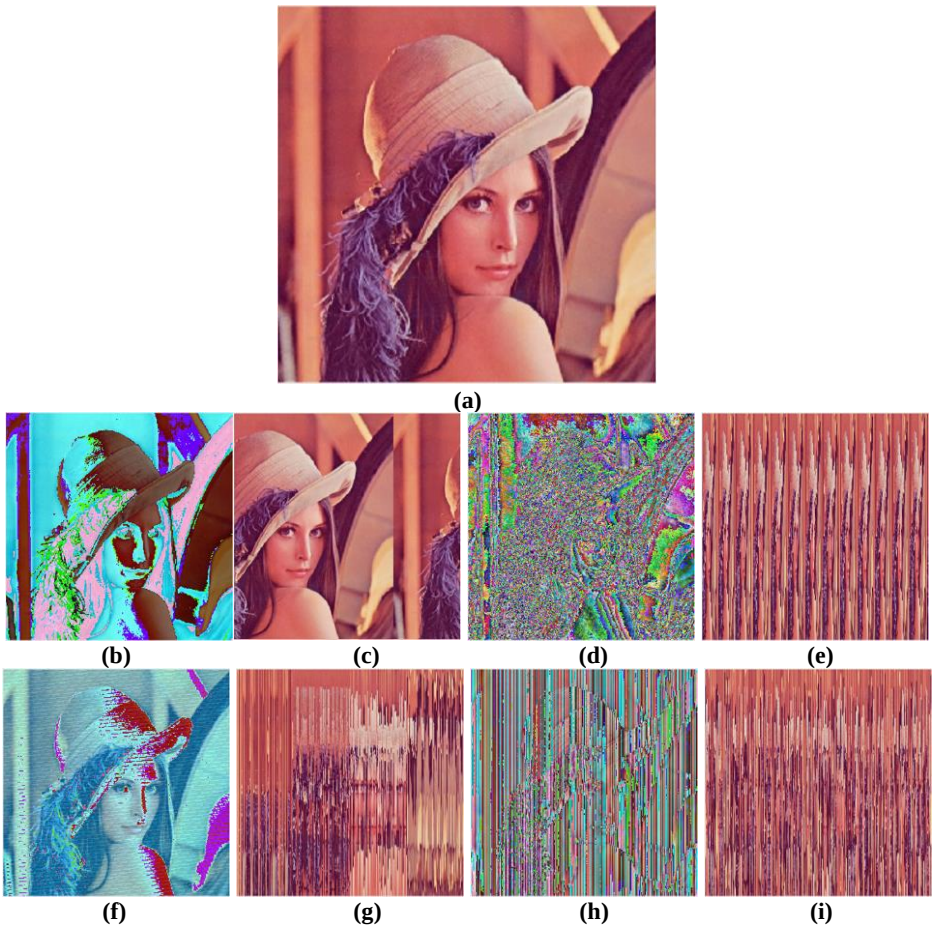
Dijital görüntülerde yer değiştirme yöntemi kullanılarak piksel değerleri üzerinde bir şifreleme işlemi yapılacaksa piksel değerini temsil edecek 0-255 arasındaki değerler rastgele dağıtılıp bir dizi değişkende tutulabilir. Bu dağıtımla 256! durumdan sadece bir tanesi oluşturulmuş olur. Şekil 2 (h)'de bu şekilde rastgele oluşturulmuş anahtar dizisinin orijinal resmin piksellerine eklenmesiyle oluşturulan şifreli görüntü mevcuttur.

Piksel konumları değiştirilerek yapılan şifreleme işleminde önce resmin genişliği baz alındığında 1-256 arasında rastgele değer tutan bir dizi değişken oluşturulmalıdır. Sonra orijinal görüntüdeki renk bilgisi dizi değişkende aynı indiste bulunan değere taşınarak yer değiştirme işlemi tamamlanmış olur. Bu şekilde yapılan bir şifrelemenin sonucu Şekil 2 (i)'de görülmektedir.

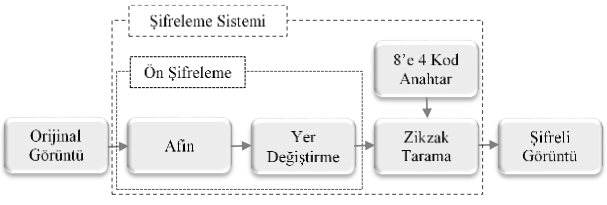
Bu iki sonucu da incelediğimizde şifrelenmiş görüntülerin yeterince kuvvetli olmadığı ve orijinal görüntü hakkında bilgiler içerdiğini söyleyebiliriz.

3.2. Önerilen Yöntem (Proposed Method)

Yukarıdaki şifreleme sonuçlarına tekrar bakıldığında görsel olarak karmaşıklığı veren iki şifreleme yöntemi olan afin ve yer değiştirme şifrelemesi kullanılarak bir algoritma tasarlandı. Bu algoritmayla öncelikle orijinal resmin hem piksel değerleri hem de konumları değiştirilerek bir ön şifreleme yapıldı. Daha sonra 8'e 4 kod kullanılarak zikzak tarama modeliyle oluşturulan taşıyıcı resmin ön şifreleme görüntüsüne eklenmesiyle şifreleme algoritması tamamlandı. Bu sisteme ait blok diyagram Şekil 3'te gösterilmektedir.



Şekil 2. (a) Orijinal resim (Original image) (b) Sezar piksel değeri şifreleme (Pixel value encryption with Caesar cipher) (c) Sezar piksel konumu şifreleme (Pixel position encryption with Caesar cipher) (d) Afin piksel değeri şifreleme (Pixel value encryption with Affine cipher) (e) Afin piksel konumu şifreleme (Pixel position encryption with Affine cipher) (f) Vigenere piksel değeri şifreleme (Pixel value encryption with Vigenere cipher) (g) Vigenere piksel konumu şifreleme (Pixel position encryption with Vigenere cipher) (h) Yer değiştirme piksel değeri şifreleme (Pixel value encryption with Substitution cipher) (i) Yer değiştirme piksel konumu şifreleme (Pixel position encryption with Substitution cipher)



Şekil 3. Şifreleme sisteminin blok diyagramı (Block diagram of the encryption system)

Şifreleme sisteminin birinci aşamasında afin şifreleme iki şekilde kullanıldı. Önce orijinal renkli görüntüdeki RGB piksel değerleri ikişer anahtarla değiştirildi. Daha sonra elde edilen yeni görüntüdeki piksel konumları değiştirilmek üzere 2 yeni anahtarla piksel değerleri değiştirilen görüntüye tekrar afin şifreleme uygulandı. Böylelikle afin şifreleme ile hem piksel renk değerleri hem de piksel konumları değiştirilmiş oldu.

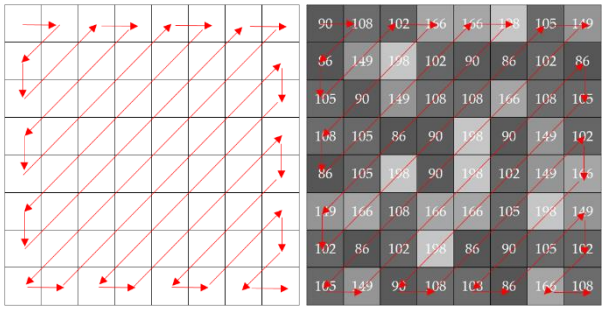
Şifreleme sisteminin ikinci aşamasında afin şifrelemeden dönen renk değeri ve konumu değişen görüntüye yer değiştirme şifrelemesi uygulandı. Burada yer değiştirme şifrelemesi görüntünün piksel değerlerini tekrar değiştirmek için kullanıldı. 3 adet 0-255 arasında rastgele yerleştirilen 256 değere sahip anahtarlarla, görüntüdeki RGB piksel değerleri tekrar değiştirildi. Birinci ve ikinci aşama aynı anahtarla 2 tur tekrar ettirildi.

Şifrelemenin üçüncü aşamasında 8'e 4 kod ile üretilen anahtar kelimeyle zikzak tarama modeli kullanılarak bir taşıyıcı görüntü oluşturuldu. 8'e 4 kod, dördü lojik '0', dördü lojik '1' den oluşan 8 bitlik binary koddur. İngiliz alfabesindeki 26 harf ve 0-9 arasındaki rakamlar için kullanılan kodlar Çizelge 1'de gösterilmiştir [17].

Girilen anahtar kelimeye karşılık gelen decimal değerler ile Şekil 4 (a)'daki zikzak tarama modeli kullanılarak bir taşıyıcı görüntü elde edildi. Örneğin anahtar kelime 'kripto06' seçildiğinde bu anahtara karşılık gelen decimal değerler '90-108-86-105-149-102-166-198' şeklinde olacaktır. Bu değerler kullanılarak zikzak taramayla oluşan taşıyıcı görüntünün bir kısmı Şekil 4 (b)'de gösterilmiştir.

Çizelge 1. Alfanümerik karakterlerin 8'e 4 binary kodları ve decimal karşılıkları (4 out of 8 binary codes and decimal equivalents of alphanumeric characters)

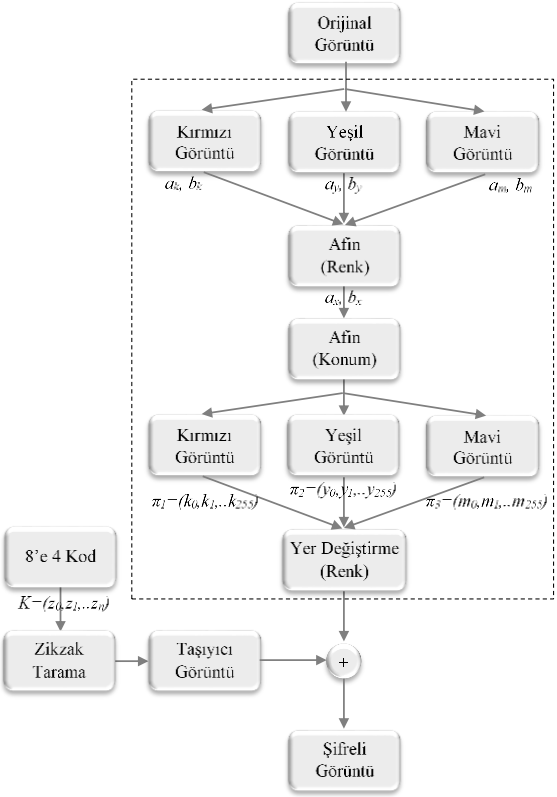
Sıra No	Alfanümerik Karakter	Binary Kod	Decimal Değeri
1	A, a	0011 0011	51
2	B, b	0011 0101	53
3	C, c	0011 0110	54
4	D, d	0011 1001	57
5	E, e	0011 1010	58
6	F, f	0011 1100	60
7	G, g	0101 0011	83
8	H, h	0101 0101	85
9	I, i	0101 0110	86
10	J, j	0101 1001	89
11	K, k	0101 1010	90
12	L, l	0101 1100	92
13	M, m	0110 0011	99
14	N, n	0110 0101	101
15	O, o	0110 0110	102
16	P, p	0110 1001	105
17	Q, q	0110 1010	106
18	R, r	0110 1100	108
19	S, s	1001 0011	147
20	T, t	1001 0101	149
21	U, u	1001 0110	150
22	V, v	1001 1001	153
23	W, w	1001 1010	154
24	X, x	1001 1100	156
25	Y, y	1010 0011	163
26	Z, z	1010 0101	165
27	0	1010 0110	166
28	1	1010 1001	169
29	2	1010 1010	170
30	3	1010 1100	172
31	4	1100 0011	195
32	5	1100 0101	197
33	6	1100 0110	198



(a) **(b)**

Şekil 4. (a) Zikzak tarama modeli (Zigzag scan pattern) (b) Anahtar kelimeyle taşıyıcı görüntü oluşturulması (Creating a carrier image with a keyword)

Şifrelemenin son aşamasında elde edilen bu taşıyıcı görüntü, yer değiştirme sonucu elde edilen şifreli görüntüye eklenerek şifreleme işlemi sonlandırılmış oldu. Şekil 5'te önerilen şifreleme sisteminin genel blok diyagramı verilmiştir.



Şekil 5. Önerilen şifreleme sisteminin blok diyagramı (Block diagram of the proposed encryption system)

Önerilen şifreleme sistemi Çizelge 2'deki değerlerle çalıştırıldığında elde edilen sonuç Şekil 6'da gösterilmiştir.

Çizelge 2. Şifreleme sistemi anahtar değerleri (Encryption system key values)

Afin Renk Anahtarları					
a_k	13	a_y	17	a_m	19
b_k	133	b_y	177	b_m	199
Afin Konum Anahtarları					
a_x	177				
b_x	177				
Yer Değiştirme Renk Anahtarları					
π_1	Rastgele 256 değer	π_2	Rastgele 256 değer	π_3	Rastgele 256 değer
8'e 4 Anahtar					
K	hidayet208173001007celik				

(a) **(b)**

Şekil 6. (a) Zikzak tarama modeli (Zigzag scan pattern) (b) Anahtar kelimeyle taşıyıcı görüntü oluşturulması (Creating a carrier image with a keyword)

4. DENEYSEL SONUÇLAR VE PERFORMANS ÖLÇÜTLERİ (EXPERIMENTAL RESULTS AND PERFORMANCE METRICS)

Önerilen yöntemin etkinliğini değerlendirmek için farklı ölçütler kullanılabilir. Bu makalede önerilen algoritmanın fizibilitesi MATLAB yazılımı kullanılarak test edilmiştir. Kullanılan renkli Lena fotoğrafının boyutu 256X256'dır. Bu bölümdeki çizelgelerde sunulan test sonuçlarının literatür karşılaştırmasında aynı boyutlara sahip renkli Lena fotoğrafını kullanan çalışmalar seçilmiştir.

4.1. Histogram Analizleri (Histogram Analysis)

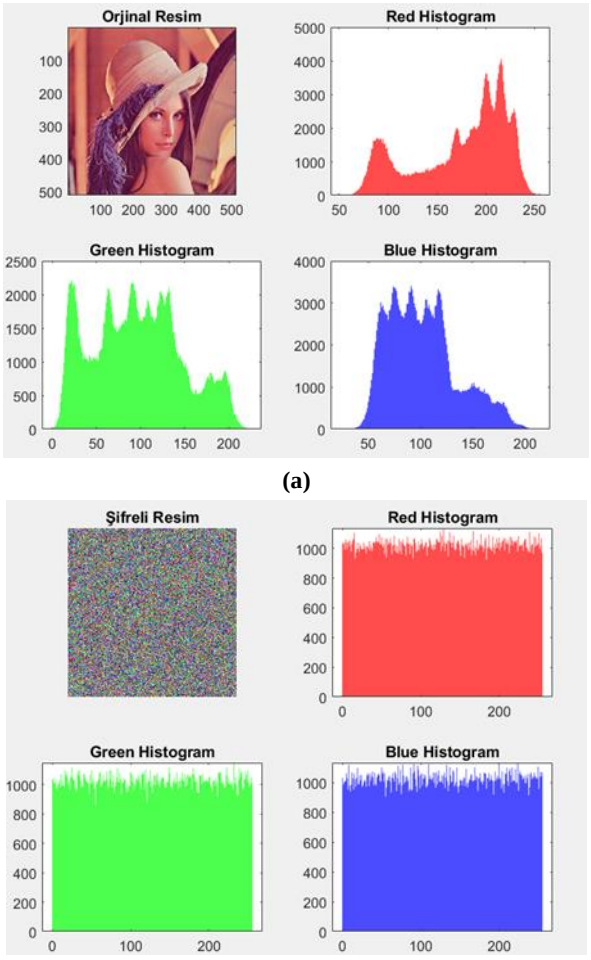
Histogram görüntüdeki piksel yoğunluk dağılımını gösterir. Saldırganlar şifreli görüntüler üzerinde istatistiksel saldırıları gerçekleştirmek için histogramları kullanıp frekans analizleri yapabilmektedirler. İstatistiksel saldırıların engellenmesi orijinal görüntünün ve şifreli görüntünün histogramlarının benzersiz olması gerekir. Özellikle şifreli görüntü histogramının homojen dağılımı görüntü şifrelemede kullanılan algoritmanın kalitesini gösterir. Şifreli görüntüdeki tek tip dağılım gösteren histogramlar istatistiksel saldırı kullanmak için herhangi bir ipucu sağlamayacaktır [18]. Şekil 7'de orijinal görüntünü ve önerilen şifreleme algoritma sonucu elde edilen şifreli görüntünün histogram grafikleri verilmiştir.

Şifreli görüntünün histogramına bakıldığında homojen dağılımın gerçekleştiği ve orijinal görüntüden çok farklı olduğu görülmektedir. Önerilen şifreleme algoritmasının bu durumda güvenli olduğu ve istatiksel saldırılara karşı dayanıklı olduğu söylenebilir.

4.2. Korelasyon Analizi (Correlation Analysis)

Korelasyon katsayısı, değişkenler arasındaki ilişkinin yönünü ve derecesini belirtir. -1 ile +1 arasında değer alır. Değişkenler arasında bir ilişkinin var olduğunu söyleyebilmek için korelasyon katsayısının -1'e veya +1'e yakın değere sahip olması gerekir. 0'a yakın korelasyon katsayı değeri değişkenler arasında bir ilişki olmadığını gösterir [19].

Bu çalışmada şifreli görüntü üzerindeki korelasyon analizi yapabilmek için yatay, dikey ve çapraz komşu pikseller dikkate alınmıştır. Renkli görüntülerdeki korelasyon katsayılı Çizelge 3'te gösterilmiştir.



(a)

(b)

Şekil 7. (a) Orijinal görüntü (Original image) (b) Şifreli görüntü, histogramları (Encrypted image, histograms)

Çizelge 3. Orijinal ve Şifreli görüntüdeki korelasyon katsayıları (Correlation coefficients in original and encrypted image)

		Kırmızı	Yeşil	Mavi
	**Yatay**	0.94874	0.97421	0.92307
	Dikey	0.94824	0.97437	0.92418
	Çapraz	0.91251	0.95134	0.87534
	**Yatay**	-0.00864	0.01177	0.00616
	Dikey	-0.00248	0.02560	0.00562
	Çapraz	0.00315	0.00672	-0.0034

4.3. Yapısal Benzerlik Testi (Structural Similarity Test)

Yapısal benzerlik katsayısı (SSIM), orijinal ve değiştirilmiş iki görüntü arasındaki kalite farkını ölçerek benzerliklerini gösteren bir yöntemdir. Denklem (9) kullanılarak benzerlik katsayısı hesaplanabilir [20].

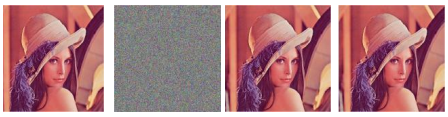
$$S(x,y) = \frac{(2\mu_x\mu_y+C_1)(2\sigma_{xy}+C_2)}{(\mu_x^2+\mu_y^2+C_1)(\sigma_x^2+\sigma_y^2+C_2)} \quad (9)$$

Burada, yapısal benzerlik testi yapılacak iki görüntü x ve y olarak temsil edilir. Görüntülerin ortalamaları $\mu_x$ve μ_y, varyansları σ_x^2 ve σ_y^2, kovaryansları σ_{xy} ile gösterilir. C_1 ve C_2 ise, görüntüleri dengelemek için kullanılan sabit değişkenlerdir.

Yapısal benzerlik katsayının 0'a yakın olması, iki görüntü arasında benzerliğin olmadığı, 1'e eşit olması, iki görüntü arasında tam benzerliğin olduğu anlamına gelir.

Çizelge 4'te orijinal görüntü ile önerilen sistem kullanılarak şifrelenen görüntünün ve şifreli görüntüden elde edilen çözülmüş görüntünün aralarındaki yapısal benzerlik katsayıları verilmiştir.

Çizelge 4. Yapısal benzerlik testi (SIMM) sonuçları (Structural similarity test (SIMM) results)



	Orijinal – Şifreli Görüntü	Orijinal – Çözülmüş Görüntü
Yapısal Benzerlik (SIMM)	**0.0095**	**1.0**

Test sonuçlarına bakıldığında, orijinal ve şifreli görüntü arasındaki yapısal benzerlik sonucunun 0'a çok yakın çıkması şifreleme işlemenin çok kuvvetli olduğunu, çözülmüş görüntünün de orijinal görüntü ile bire bir aynı olması işlem sonucunda her hangi bir piksel kaybı olmadan görüntünün tekrar elde edildiğini göstermiştir.

4.4. Entropi Testi (Entropy Testing)

Entropi bir sistemdeki belirsizlik derecesini belirtir. Denklem (10) kullanılarak hesaplanabilir.

$$H(m) = \sum_{i=0}^{2^M-1} P(m_i) log_{\,2} \frac{1}{P(m_i)} \quad (10)$$

Burada $P(m_i)$ mesajdaki sembollerinin olasılık durumlarını temsil eder. İdeal entropi değeri rastgele mesajlarda 8'e eşit olmalıdır. Şifreli görüntüler de rastgele piksel değerlerinden oluştuğu için entropi test sonucunun 8 çıkması beklenir. 8'den daha düşük entropi değerleri mesajlardaki rastgelelik oranının daha az olduğu durumlarda görülür. Eğer entropi değeri 8'den çok düşükse güvenlik tehdidi olabileceği düşünülmelidir [21].

Orijinal, şifreli ve çözülmüş renkli görüntülerde, RGB kanallarının her biri için ayrı ayrı hesaplanan entropi değerleri Çizelge 5'te verilmiştir.

Çizelge 5. Entropi test sonuçları (Entropy test results)

Orijinal Görüntü		Şifreli Görüntü		Çözülmüş Görüntü	
Kırmızı	7.2286	**Kırmızı**	7.9962	**Kırmızı**	7.2286
Yeşil	7.5498	**Yeşil**	7.9965	**Yeşil**	7.5498
Mavi	6.9675	**Mavi**	7.9966	**Mavi**	6.9675

Test sonuçlarına bakıldığında şifreli görüntüdeki entropi değerlerinin 8'e çok yakın olduğu görülmektedir. Bu sonuç önerilen şifreleme algoritmasının saldırılara karşı dayanıklı olacağının göstergesidir. Ayrıca orijinal ve çözülmüş görüntülerdeki değerlerin aynı olması işlemler sonucunda bir veri kaybı olmadığını göstermiştir. Çizelge 6'da önerilen yöntem literatürdeki bazı çalışmalarla karşılaştırılmıştır.

Çizelge 6. Entropi test sonuçlarının karşılaştırılması (Comparison of entropy test results)

	Kırmızı	Yeşil	Mavi
Önerilen Yöntem	**7.9962**	**7.9965**	**7.9966**
(Rhouma, 2009) [22]	7.9732	7.9750	7.9715
(Wei, 2012) [23]	7.9901	7.9898	7.9899
(Dong, 2014) [24]	7.9901	7.9912	7.9921
(Wu, 2015) [25]	7.9893	7.9896	7.9903
(Liu, 2015) [26]	7.9896	7.9893	7.9896
(Ur Rehman, 2018) [27]	7.9892	7.9898	7.9899

4.5. Diferansiyel Saldırı Analizi (Differential Attack Analysis)

Saldırganlar şifreli görüntülerde küçük değişiklikler yaparak orijinal görüntü hakkında anlamlı bir ilişki kurabilirler. Orijinal görüntüdeki küçük bir değişikliğin şifreli görüntüde kafa karıştıracak kadar önemli bir değişikliğe neden olması bu tür saldırıları verimsiz ve işe yaramaz duruma getirebilir.

Diferansiyel saldırı analizinde orijinal görüntüdeki bir piksel değişikliğin şifreli görüntüye etkisini araştırmak için genellikle iki test yapılır; NPCR (Number of Pixel Change Rate – Piksel Değişim Oranı) ve UACI (Unified Average Change Intensity – Birleşik Ortalama Değişim Yoğunluğu). Bu iki testin sonucu 8 bitlik bir görüntü için sırasıyla %100 ve %33'lük değerlere yaklaşıksa, bu

durumda görüntünün diferansiyel saldırılara karşı sağlam olduğu söylenebilir [28].

İki renkli şifreli görüntü için NPCR ve UACI oranları Denklem (11) ve Denklem (12) ile hesaplanabilir.

$$NPCR = \sum_{i,j} \frac{d(i,j)}{h*w} \quad d(i,j) = \begin{cases} 1 & c_1(i,j) \neq c_2(i,j) \\ 0 & d.d. \end{cases} \quad (11)$$

$$UACI = \frac{1}{h*w} \sum_{i,j} \frac{|c_1(i,j) - c_2(i,j)|}{255} \quad (12)$$

Orijinal görüntüde bir piksel değiştirilip önerilen şifreleme algoritmasıyla tekrar bir şifreleme yapıldı. İki şifreli görüntü arasındaki test sonuçları Çizelge 7'de verilmiştir.

Çizelge 7. UACI ve NPCR test sonuçları (UACI and NPCR test results)

	UACI	**NPCR**
Kırmızı (K)	33.65	99.629
Yeşil (Y)	33.60	99.623
Mavi (M)	33.50	99.592

Çizelgeye bakıldığında, NPCR sonuçlarının %99, UACI sonuçlarının %33 olması görüntünün diferansiyel saldırılara karşı sağlam olduğu sonucunu göstermiştir. Çizelge 8'de önerilen yöntem literatürdeki bazı çalışmalarla karşılaştırılmıştır.

Çizelge 8. UACI ve NPCR test sonuçlarının karşılaştırılması (Comparison of UACI and NPCR test results)

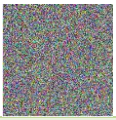
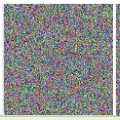
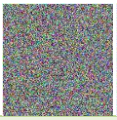
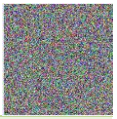
	UACI			**NPCR**		
	K	**Y**	**M**	**K**	**Y**	**M**
Önerilen Yöntem	**33.657**	**33.604**	**33.500**	**99.629**	**99.623**	**99.592**
(Wu, 2015) [25]	33.463	33.504	33.477	99.610	99.609	99.609
(ur Rehman, 2018) [27]	33.429	33.425	33.422	99.607	99.608	99.608
(Lone, 2020) [28]	33.548	33.622	33.409	99.618	99.624	99.623
(Zhu, 2006) [29]	21.41	23.42	15.08	99.26	99.45	99.13
(Huang, 2009) [30]	27.78	27.66	24.94	99.42	99.60	99.54
(Parvaz, 2018) [31]	33.445	33.558	33.524	99.607	99.614	99.603

5. SONUÇ (CONCLUSION)

Bu çalışmada, geleneksel metin şifreleme algoritmalarının görüntü şifrelemede kullanılabilirliği tartışıldı ve bu algoritmalardan ikisiyle oluşan karma bir şifreleme algoritması önerildi. Önerdiğimiz şifreleme yönteminde afin şifreleme görüntünün hem piksel değerlerini değiştirmek hem de konumlarını değiştirmek için kullanıldı. Renk değerlerini değiştirirken her renk kanalı için ikişer anahtar kullanıldı. Afin şifreleme ile yapılan işlemden sonra yer değiştirme şifrelemesi ile piksel değerleri tekrar değiştirildi. Yer değiştirme şifrelemesi de her renk kanalı için üretilen anahtarlarla gerçekleştirildi. Bu iki işlem ile bir şifreleme işlemi zaten gerçekleştirilmiş oldu fakat şifreleme işlemini daha da kuvvetlendirmek için anahtar kelime kullanılarak zikzak tarama yöntemiyle oluşturulan taşıyıcı görüntü şifrelenmiş görüntünün üzerine eklendi. Şifrelemenin her aşaması farklı anahtarlar kullanılarak gerçekleştiği için geniş anahtar uzayına sahiptir.

Farklı anahtarlar kullanılarak yapılan şifreleme işleminde elde edilen entropi ve yapısal benzerlik test sonuçları Çizelge 9'da gösterilmiştir.

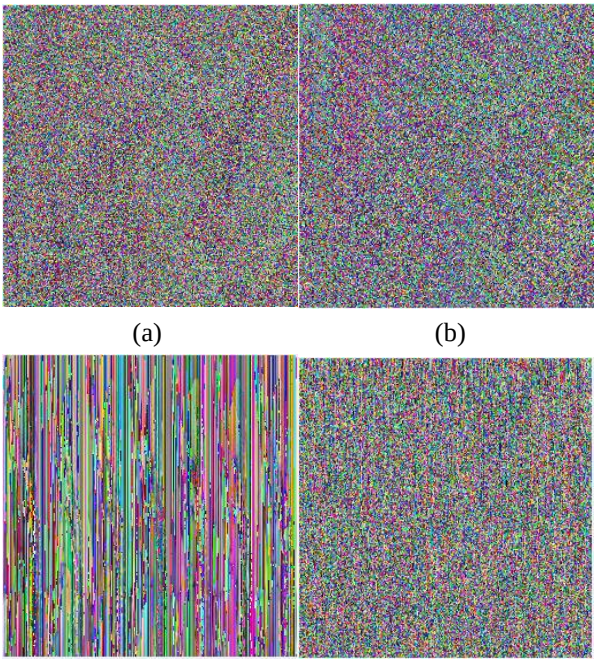
Çizelge 9. Farklı anahtarlar kullanılarak elde edilen test sonuçları (Test results obtained using different keys)

Şifreli Görüntü				
8'e 4 (K) Anahtarı	hidayet208173001007celik	selcuk	selcukuniversitesi	selcukuniversitesifenbilimlerienstitusubilgisayarmuhendisligi
Kırmızı Entropi	7.9962	7.9956	7.9958	7.9961
Yeşil Entropi	7.9965	7.9947	7.9965	7.9964
Mavi Entropi	7.9966	7.9952	7.9961	7.9970
Yapısal Benzerlik	0.0095	0.0098	0.0102	0.0095

Çizelge 2'de şifreleme sisteminin kullandığı anahtarlar ve değerleri gösterilmişti. Piksel konumlarını ve değerlerini değiştirmek için farklı, taşıyıcı görüntüyü oluşturmak için farklı anahtarın kullanıldığı bilinmektedir. Şifrelemede her anahtardaki değişiklik sonuca etki edecektir. Sadece 8'e 4 (K) anahtarı değiştirilip diğer bütün anahtarların aynı kalması ile sistem performansı tekrar test edildiğinde Çizelge 9'daki sonuçlar elde edildi. Buna göre sistem farklı anahtarlarla da başarılı sonuca ulaşmıştır.

Önerilen şifreleme yöntemi kaotik sistem kullanan şifreleme yöntemi değildir, bu yüzden kaotik sistemler kadar karmaşık değildir ve uygulanabilirliği daha kolaydır. Bu çalışmayla geleneksel metin şifreleme yöntemlerinin görüntü şifrelemede de iyi performans sunabileceği gösterildi. Tek başlarına kullanıldıklarında yeterli şifreleme yapılamadığı, farklı yöntemlerle birleştirilerek kullanıldıklarında görüntü şifrelemenin istenen düzeyde olabileceği gösterildi. Önerilen yöntemde, piksel renk ve konum değerlerini değiştirmek için birden fazla anahtar kullanıldı. Görüntü üzerindeki karmaşıklık kullanılan bu farklı anahtarlar sayesindedir. Literatürdeki aynı ortak resmi kullanarak gerçekleştirilen bazı çalışmalardan başarılı sonuçlar elde ettiği gösterilmiştir.

Şifreleme işleminde doğru anahtarlarla orijinal görüntüyü yeniden elde edilebilmek gerekir. Farklı anahtarlarla elde edilen şifre çözme sonuçları Şekil 8'de gösterilmiştir.



(a) (b)

(c) (d)

Şekil 8. (a) Tek karakteri eksik 8'e 4 anahtar (Missing one karakter at 4 out of 8 key) (b) Farklı 8'e 4 anahtar (Different 4 out of 8 key) (c) Farklı afin konum anahtarı (Different affine position key) (d) Farklı afin renk ve konum anahtarları (Different affine position and value keys)

Şekil 8 (a), afin renk anahtarları (a_k, b_k, a_y, b_y, a_m, b_m) ve afin konum anahtarları (a_x, b_x) şifreleme işleminde kullanılan anahtarlarla aynı, 8'e 4 anahtarı (K="hidayet208173001007celi") son karakteri eksik girildiğinde elde edilen sonuçtur. Şekil 8 (b), afin renk ve konum anahtarları şifreleme işleminde kullanılan anahtarlarla aynı, 8'e 4 anahtarı (K) farklı girildiğinde (K="selcukuniversitesi") elde edilen sonuçtur. Şekil 8 (c), afin konum anahtarlarının farklı (a_x=13, b_x=13), diğer anahtarların şifreleme işleminde kullanılan anahtarlarla aynı girildiğinde elde edilen sonuçtur. Şekil 8 (d), 8'e 4 anahtarın şifreleme işleminde kullanılan anahtarla aynı, afin renk ve konum anahtarlarının farklı girildiğinde (a_k=133, b_k=13, a_y=177, b_y=17, a_m=199, b_m=19, a_x=155, b_x=155) elde edilen sonuçtur. Buradan şifreleme aşamasındaki bir anahtarın bilinmesi orijinal görüntünün tamamen geri elde edilemeyeceği sonucuna varılabilir. Orijinal görüntü, tüm anahtarlar doğru girildiğinde elde edilebilecektir.

Yaptığımız testlerin sonuçlarına tekrar bakıldığında önerilen şifreleme algoritması ile işlem sonucunda hiçbir veri kaybı ya da değişikliği olmadan orijinal görüntünün tekrar elde edildiği gözlemlendi. Elde ettiğimiz bu test sonuçları doğrultusunda önerdiğimiz algoritmanın görüntü şifreleme işlemlerinde kullanılabileceği uygun görülmektedir.

ETİK STANDARTLARIN BEYANI (DECLARATION OF ETHICAL STANDARDS)

Bu makalenin yazar(lar)ı çalışmalarında kullandıkları materyal ve yöntemlerin etik kurul izni ve/veya yasal-özel bir izin gerektirmediğini beyan ederler.

YAZARLARIN KATKILARI (AUTHORS' CONTRIBUTIONS)

Nurettin DOĞAN: Makalede kullanılacak yöntemleri belirlemiş ve makalede kullanılan algoritmayı kurmuştur.

Hidayet ÇELİK: Deneyleri yapmış ve sonuçlarını analiz etmiştir. Makalenin yazım işlemini gerçekleştirmiştir.

ÇIKAR ÇATIŞMASI (CONFLICT OF INTEREST)

Bu çalışmada herhangi bir çıkar çatışması yoktur.

KAYNAKLAR (REFERENCES)

[1] Reinke, E. C., "Classical cryptography". ***The Classical Journal***, *58*(3), 113-121, (1962).

[2] Zaidan, B. B., Zaidan, A. A., & Mwafak, H., "New Comprehensive Study to Assess Comparatively the QKD, XKMS, KDM in the PKI encryption algorithms." ***Int. J. Comput. Sci. Eng,*** *1*(3), 263-268, (2009).

[3] Kodaz, H., & Botsali, F. M., "Simetrik ve Asimetrik Şifreleme Algoritmalarının Karşılaştırılması." ***Selçuk Teknik Dergisi,*** 9(1), 10-23, (2010).

[4] Özdemir, A., & Katrancı, Y., "Strengthening the Subject of Modular Arithmetic With the Help of RSA Encryption." ***Kalem International Journal of Education and Human Sciences.*** 3. 149-185. (2013).

[5] Beşkirli, A., Özdemir, D. & Beşkirli, M., "Şifreleme Yöntemleri ve RSA Algoritması Üzerine Bir İnceleme." ***European Journal of Science and Technology, (Special Issue),*** 284-291, (2019).

[6] Karabey, I , Yelkuvan, A , Akal, F., "Bulut Bilişim Ve Genomik Verilerin Gizliliği", ***Uluslararası Bilgi*** Güvenliği Mühendisliği Dergisi, 6 (2) , 72-88, (2020).

[7] Bao, L., & Zhou, Y., "Image encryption: Generating visually meaningful encrypted images". ***Information Sciences***, 324, 197-207, (2015).

[8] Atalay, N. S., Doğan, Ş., Tuncer, T., & Akbal, E., "İmge Şifreleme Yöntem ve Algoritmaları." ***Dicle Üniversitesi Mühendislik Fakültesi Mühendislik Dergisi***, 10(3), 815-831, (2019).

[9] Bhatnagar, G., Wu, Q. J., & Raman, B., "Discrete fractional wavelet transform and its application to multiple encryption.", ***Information Sciences***, 223, 297-316, (2013).

[10] Hua, Z., Zhou, Y., Pun, C. M., & Chen, C. P., "2D Sine Logistic modulation map for image encryption.", ***Information Sciences,*** 297, 80-94, (2015).

[11] Kumari, M., Gupta, S., & Sardana, P., "A Survey of Image Encryption Algorithms.", ***3D Research,*** 8(4),8-35, (2017).

[12] Nag, A., Singh, J. P., Khan, S., Ghosh, S., Biswas, S., Sarkar, D., & Sarkar, P. P., "Image Encryption Using Affine Transform And XOR Operation.", ***International Conference on Signal Processing, Communication, Computing and Networking Technologies.*** 309-312, (2011).

[13] Zhu, H., Zhao, C., Zhang, X., & Yang, L., "An Image Encryption Scheme Using Generalized Arnold Map And Affine Cipher.", ***Optik - International Journal For Light And Electron Optics,*** 125(22), 6672–6677, (2014).

[14] Ke, Q., Liao, Q.-N., Li, A.-Q., & Gao, R., "Digital Image Encryption Algorithm Based on Affine Cipher.", ***International Conference on Applications and Techniques in Cyber Security and Intelligence ATCI 2018***, 578–585, (2018).

[15] Rad, R. M., Attar, A., & Atani, R. E., "A New Fast And Simple Image Encryption Algorithm Using Scan Patterns And XOR.", ***International Journal Of Signal Processing, Image Processing And Pattern Recognition,*** 6(5), 275-290, (2013).

[16] Panduranga, H. T., & Kumar, S. N., "Hybrid Approach For Image Encryption Using SCAN Patterns And Carrier Images.", ***International Journal On Computer Science And Engineering,*** 2(02), 297-300, (2010).

[17] Sunil K. M., Kiran K., Anand U. H., "Image Encryption Using Modified 4 Out Of 8 Code And Chaotic Map", ***International Journal Of Computer Applications***, 74(11), 1-6, (2013).

[18] Naveenkumar, S.K., Panduranga, H.T., "Triple Image Encryption Based On Integer Transform And Chaotic Map", ***International Conference On Optical Imaging Sensor And Security (ICOSS)***, 1-6, (2013).

[19] Güvenoğlu, E., "Resim şifreleme amacıyla dinamik S kutusu tasarımı için bir yöntem.", ***El-Cezeri Journal of Science and Engineering,*** 3(2), (2016).

[20] Wang, Z., Bovik, A. C., Sheikh, H. R., Simoncelli, E. P., "Image Quality Assessment: From Error Visibility To Structural Similarity", ***IEEE Transactions On Image Processing***, 13(4), 600-612, (2004).

[21] Munir, R. "Security Analysis Of Selective Image Encryption Algorithm Based On Chaos And CBC-Like Mode.", ***2012 7th International Conference On Telecommunication Systems, Services, and Applications (TSSA)***, 142-146, (2012).

[22] Rhouma, R., Meherzi, S., & Belghith, S., "OCML-based colour image encryption.", **Chaos, Solitons & Fractals,** 40(1), 309-318, (2009).

[23] Wei, X., Guo, L., Zhang, Q., Zhang, J., & Lian, S., "A novel color image encryption algorithm based on DNA sequence operation and hyper-chaotic system.", ***Journal of Systems and Software,*** 85(2), 290-299, (2012).

[24] Dong, C., "Color Image Encryption Using One-Time Keys And Coupled Chaotic Systems.", ***Signal Processing: Image Communication,*** 29, 628–640, (2014).

[25] Wu, X. J., Kan, H. B., & Kurths, J., "A New Color Image Encryption Scheme Based On DNA Sequences And Multiple Improved 1D Chaotic Maps.", ***Applied Soft Computing***, 37, 24–39, (2015).

[26] Liu, H. J., & Kadir, A., "Asymmetric Color Image Encryption Scheme Using 2D Discrete-Timemap.", ***Signal Processing***, 113, 104–112, (2015).

[27] ur Rehman, A., Liao, X. F., Ashraf, R., Ullah, S., & Wang, H. W., "A Color Image Encryption Technique Using Exclusive-OR With DNA Complementary Rules Based On Chaos Theory And SHA-2.", ***Optik***, 159, 348–367, (2018).

[28] Lone, P. N., & Singh, D., "Application Of Algebra And Chaos Theory In Security Of Color Images.", ***Optik***, 218, 165155, (2020).

[29] Zhu, C. X., "A new image encryption algorithm based on general Chen's chaotic system.", ***Journal of Central South University (Science and Technology)***, 37, 1142, (2006).

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

[31] Parvaz, R., & Zarebnia, M., "A Combination Chaotic System And Application In Color Image Encryption.", ***Optics & Laser Technology***, 101, 30-41, (2018).