Int. J. Pure Appl. Sci. 9(1);1-6 (2023)

IJPAS
ijpas@munzur.edu.tr
ISSN: 2149-0910

Research article/Araştırma makalesi
DOI:10.29132/ijpas.1182404

Optimizasyon Algoritmaları ile Üretilen Kriptolojik Anahtarları Temel Alan Görüntü Şifreleme Algoritması

Eyüp Eroz*, Erkan Tanyıldız
Yazılım Mühendisliği, Teknoloji Fakültesi, Fırat Üniversitesi, Elâzığ, Türkiye
**eeroz@firat.edu.tr, etanyildizi@firat.edu.tr*
Makale gönderme tarihi:30.09.2022, Makale kabul tarihi:10.11.2022

Öz

Veri şifreleme ve sıkıştırma gereksinimlerini sağlayan bir görüntü şifreleme algoritması önerilmiştir. Şifreleme algoritmalarının en önemli aşaması güvenilir, tahmin edilemez ve rastgele anahtar üretme işlemidir. Önerdiğimiz yöntemde, verilerin şifreleme kısmında kullanılan anahtar üretim algoritması için optimizasyon temelli bir anahtar üreteci kullanılmıştır. Kullandığımız tek kullanımlık şerit prensibine dayanan rastgele sayı üreteci yöntem, her seferinde farklı rastgele anahtar üreterek koşulsuz güven sağlamaktadır. Optimizasyon temelli anahtar üretecinin elde ettiği istatistiksel başarılar görüntü şifreleme alanında da kendini göstermektedir. Değişken piksel hızı sayısı (NPCR), birleşik ortalama değişen yoğunluk (UACI) ve histogramı analizi gibi analiz yöntemleri ile görüntü şifreleme alanlarında başarısı incelenmiştir. Elde edilen başarılı sonuçlar, önerilen anahtar üretiminin görüntü şifreleme alanında da kullanılabilir güvenli bir anahtar üreteci olduğu ortaya koyulmuştur. Dolayısıyla kriptografik diğer pek çok alanda da optimizasyon temelli rastgele sayı üretecinin kullanılabileceği görülmüştür.

Anahtar Kelimeler: LFSR, görüntü şifreleme, bilgi güvenliği, optimizasyon, rastgele

Image Encryption Algorithm Based on Cryptological Keys Generated by Optimization Algorithms

Abstract

An image encryption algorithm has been proposed that satisfies the data encryption and compression requirements. The most important stage of encryption algorithms is reliable, unpredictable and random key generation. In our proposed method, an optimization-based key generator is used for the key generation algorithm used in the encryption part of the data. The random number generator method based on the disposable strip principle we use provides unconditional trust by generating different random keys each time. The statistical achievements of the optimization-based key generator also show themselves in the field of image encryption. Its success in image coding has been examined with analysis methods such as The number of changing pixel rate (NPCR), the unified averaged changed intensity (UACI) and histogram analysis. The successful results show that the proposed key generation is a secure key generator that can also be used in the field of image encryption. Therefore, it has been seen that optimization-based random number generator can be used in many other cryptographic fields.

Keywords: LFSR, image encryption, information security, optimization, randomness

GİRİŞ

Rastgelelik, tüm araştırma alanlarında pek çok araştırmacının çıktılarının başarısını etkileyen önemli bir özellik olmuştur. Rastgelelik kavramının temel gereksinimlerini karşılamak ise tek başına bir araştırma konusu haline gelmiştir. Bu doğrultuda, yıllarca pek çok rastgele sayı üreteci (RNG) geliştirilmiş ve önerilmiştir (Robshaw and Billet 2008;Garipcan ve Erdem, 2019). Rastgele sayı üreteçleri arasında en dikkat çekicisi ise Doğrusal Geri Beslemeli Kaydırmalı Yazmaç (LFSR) olmuştur (Garipcan ve Erdem, 2020). LFSR yapısı, rastgelelik gereksinimleri için temel kabul edilen istatistiksel gereksinimleri sağlayabildiği için birçok pratik uygulamada ilk tercih edilen üreteçlerden biri olmuştur. LFSR üreticinin en önemli sorunlarından biri uzun bit dizelerini üretmek için hangi

IJPAS
ijpas@munzur.edu.tr
ISSN: 2149-0910

Research article/Araştırma makalesi
DOI:10.29132/ijpas.1182404

konfigürasyonların kullanacağını belirlemektir. Çünkü bit dizisinin uzunluğu, konfigürasyonda kullanılan flip-flop sayısı ile ilgilidir. Flip-flop sayısı elde edilecek bit uzunluğu ile doğru orantılı olduğu için, flip-flop sayısı arttıkça hangi konfigürasyonun uygun olacağını belirlemenin karmaşıklığı da artacaktır (Sheveleva ve Balyaev, 2021; Asif ve Baig, 2009).

Büyük veri kavramı günlük yaşantımızın önemli bir parçası haline gelmektedir. Dolayısıyla bilgi güvenliği, dijital verilerimizi güvence altına almak gibi kavramlar ön plana çıkarılmaktadır. Bu bilgi güvenliğini sağlamak için kriptografik protokoller yani şifreleme algoritmaları kullanılmaktadır. Bu çalışmamızda bilgi güvenliği kavramının bir parçası olan görüntü şifreleme algoritmalarına odaklanılmıştır. Geçmiş çalışmalarımızda NP problemlerin çözümü için önerdiğimiz optimizasyona dayalı yaklaşımın başarısı istatistiksel olarak gösterilmiştir. Elde edilen istatistiksel sonuçlarının gerçek hayattaki kriptografik problemler üzerindeki etkisini görmek için görüntü şifreleme alanına uygulanmıştır (Eröz ve Tanyıldızı, 2021).

Çalışmamızın ikinci bölümünde önemli rastgele sayı üreteci olan LFSR tanıtılmış, üçüncü bölümünde rastgele sayı üretiminde kullandığımız optimizasyon algoritması olan ikili yarasa algoritmasına değinilmiştir, dördüncü bölümünde hibrit görüntü şifreleme algoritmamızın uygulanması anlatılmış, beşinci bölümde analiz sonuçlarına bakılarak altıncı bölümde genel sonuç değerlendirilmiştir.

Doğrusal Geri Beslemeli Kaydırmalı Yazmaç

Rastgele sayı üreteçleri içerisinde önemli yere sahip olan LFSR, flip-flop'lar ve geri besleme yolundan oluşur. 1-bit depolama alanı olan flip-flop sayısı LFSR derecesini vermektedir. Yani, m adet flip-flop'tan oluşan bir LFSR' nin derecesi de m olur (Schindler, 2009;Stipcevic 2014). Belirli flip-flop'ların XOR toplamının sonucu son flip-flop' un girişidir. Bu giriş de geri besleme yolu sayesinde tetiklenmektedir. Şekil 1'de 3 sıralı basit bir LFSR yapısı görülmektedir.

Şekil 1'deki konfigürasyon için 110 başlangıç tohum değerleri kullanılırsa, elde edilecek rastgele bit dizisinin çıkışı 01101101011011010111... olacaktır. Verilen örnekte başlangıç tohumu 3 bit olması 3 adet flip-flop kullanılacağı anlamına gelmektedir. Dolayısıyla, LFSR derecesi de 3 olduğundan elde edilen maksimum bit uzunluğu 2^3-1=7 olacaktır. 8. değerden sonra dizi kendini tekrar edecektir (Garipcan ve Erdem, 2020).

Belirtilen LFSR çalışma mantığını genel bir yapıda tanımlayacak olursak, Şekil 2'deki gibi m dereceli bir LFSR genel formu oluşturulabilmektedir. Bir geri besleme yolunun aktif olup olmadığı p geri besleme katsayısı ile tanımlanmaktadır. 1 olursa anahtar kapalı ve geri besleme yolu aktif anlamına gelirken, 0 olduğunda ise geri besleme yolu pasif anlamına gelmektedir.

İkili Yarasa Algoritması (BBA)

Yarasa algoritması literatürde önemli bir optimizasyon algoritmasıdır. Başarılı optimizasyon algoritması 0/1, Evet/Hayır vb. döndürmektedir. Problemlere uygun çözümler sunabilmek için ikili optimizasyon problemlerine uygun hale getirilmiştir. İkili arama uzayı bir hiperküp olarak düşünülebilir. İkili optimizasyon algoritmasının arama aracıları (parçacıkları), değişen sayıda biti çevirebilir ve bu bitleri yalnızca bu hiperküpün yakın ve uzak köşelerine kaydırabilmektedir (Kennedy ve Eberhart, 1997). Bu nedenle, İkili yarasa algoritmasındaki hız ve konum güncelleme denklemleri, ikili arama uzayına uyacak şekilde değiştirilmelidir. İkili arama uzayında konumları 0'dan 1'e veya tam tersi şekilde güncellemek için, hız ile konum güncelleme arasında bir bağlantı olacak şekilde tasarım yapılmalıdır. Ayrık ikili uzayda, konum güncelleme 0-1 değerleri arasında geçiş yapmak anlamına gelir ve bu, arama ajanlarının hızına göre yapılmalıdır. Konumları güncellemek için hız değerlerini olasılık değerlerine eşlemek için bir transfer fonksiyonu gerekmektedir. Bu transfer fonksiyonu, parçacıkların ikili uzayda hareket etmesine izin verir. Rashedi ve diğerleri, hız değerlerini olasılık değerleriyle eşleştirmek için bir transfer fonksiyonu seçerken aşağıdaki kavramlar dikkate alınmalıdır (Rashedi, 2009).

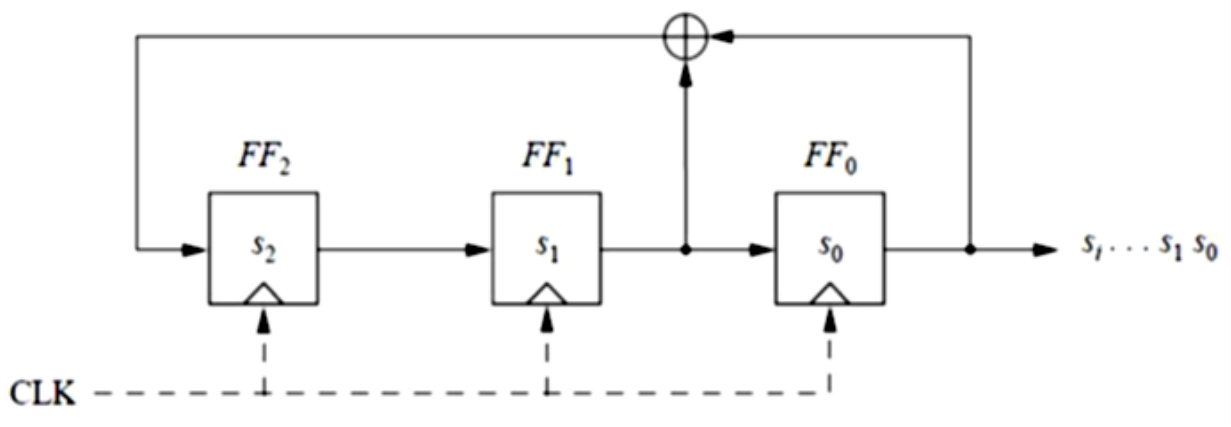
BBO için kullanılan transfer fonksiyonu Denklem 1 olarak verilmektedir (Kennedy ve Eberhart, 1997).

$$S\left(v_i^k(t)\right) = \frac{1}{1+e^{-v_i^k(t)}} \quad (1)$$

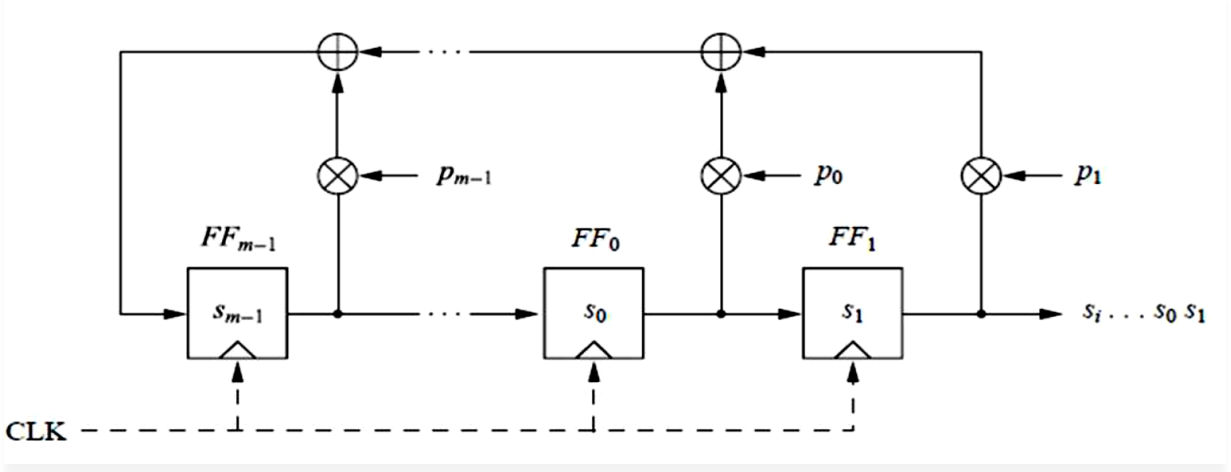
Transfer fonksiyonlarını kullanarak olasılıkları hesapladıktan sonra, Denklem 2'deki gibi parçacıkların konumunu güncellemek için yeni bir konum güncelleme denklemi gerekmektedir (Mirjalili, 2014).

IJPAS
ijpas@munzur.edu.tr
ISSN: 2149-0910

Research article/Araştırma makalesi
DOI:10.29132/ijpas.1182404



Şekil 1. LFSR temel yapısı



Şekil 2. LFSR genel yapısı

$$x_i^k(t+1) = \begin{cases} 0 \text{ eğer } rand < S(v_i^k(t)) \\ 1 \text{ eğer } rand \geq S(v_i^k(t)) \end{cases} \quad (2)$$

yöntemin bir dezavantajı parçacıkların 0 veya 1 değerlerini almaya zorlanmasıdır. Böylece hız değerleri arttığında parçacıklar konumlarında değişmeden kalırlar. Bununla birlikte, yukarıda bahsedilen kavramlara göre, bir transfer fonksiyonu tasarlamanın daha iyi bir yolu, yüksek hızlı parçacıkları konumlarını değiştirmeye zorlamaktır. Bu nedenle, v-şekilli bir transfer fonksiyonu ve konum güncelleme kuralı Denklem 3 ve 4'deki gibi uygulanmaktadır.

$$V\left(v_i^k(t)\right) = \left|\frac{2}{\pi}\arctan\left(\frac{\pi}{2}v_i^k(t)\right)\right| \quad (3)$$

$$x_i^k(t+1) = \begin{cases} x_i^k(t)^{-1} \text{ eğer } rand < V(v_i^k(t)) \\ x_i^k(t) \quad \text{eğer } rand \geq V(v_i^k(t)) \end{cases} \quad (4)$$

ÖNERİLEN ALGORİTMA

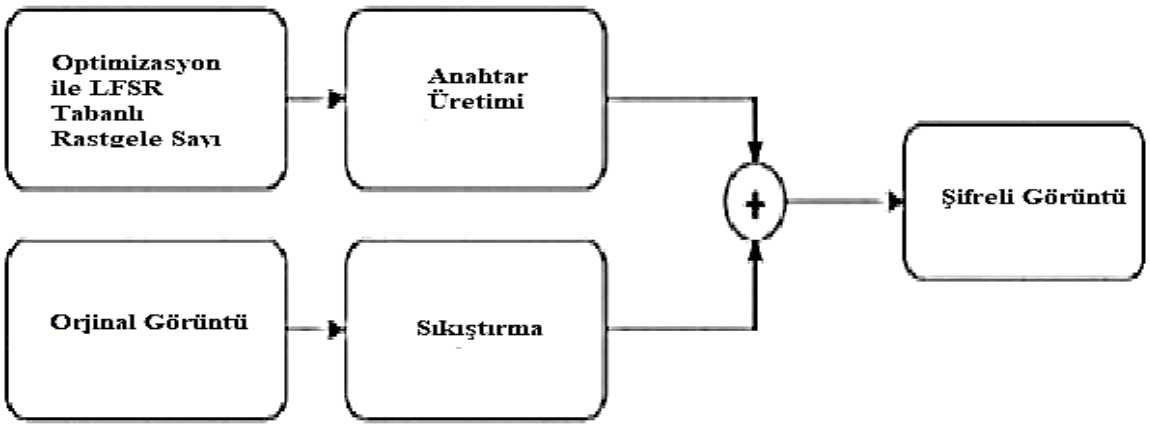
Önerilen görüntü şifreleme algoritmasına genel bakış şekilde gösterilmektedir. Algoritma kriptografik olarak tek kullanımlık şerit prensibine dayanmaktadır. Bu şifreleme protokolü ilk olarak Vernam tarafından önerilmiştir (Paar, 2010). Protokol XOR yöntemi ile uygulanmaktadır. XOR yöntemi çalışma prensibi; iki bit değerini girdi olarak alır ve bir bitlik çıktı üretir. Toplam 4 çıkış bulunmaktadır. Çıkışlarda sadece 1 veya 0 değeri üretilmektedir. Bu nedenle olasılık %50' dir (Burhan, Artuğer ve Ozkaynak 2019).

Daha spesifik olarak, şifrelenmiş görüntü bir bit dizisi olarak ifade edilir. Bu bit dizisi uzunluğunda bir anahtar dizisi oluşturulur. Ortaya çıkan iki bit dizisi,

IJPAS
ijpas@munzur.edu.tr
ISSN: 2149-0910

Research article/Araştırma makalesi
DOI:10.29132/ijpas.1182404

XOR işleneninin girişi olarak uygulanır ve şifreli bir diziyle sonuçlanır. Bu şifreleme protokolü, her bir anahtar dizisinin bir kez kullanılması durumunda koşulsuz olarak güvenlidir. Şifreleme protokolünün güvenli olmasının en önemli kısmı rastgele anahtar üretme aşamasıdır. Kriptografik işlemlerde rastgele anahtar üretecinin önemi büyüktür. Kriptografik anahtarlarda olması gereken en önemli özellikler rastgele ve tahmin edilemez olmasıdır. Dolayısıyla böyle bir kriptografik anahtarın üretilmesinde önerdiğimiz yöntem optimizasyon temelli doğrusal geri beslemeleri kaydırmalı yazmaç (LFSR) üretecidir.



Şekil 3. Önerilen görüntü şifreleme algoritmasının genel yapısı (Burhan, Artuğer ve Ozkaynak 2019)

Görüntü şifreleme algoritması için önerilen yöntemde gerekli olan anahtar üretimi kısmında optimizasyon temelli LFSR üreteci yöntemimiz ile güvenli bir algoritma elde edilmiştir.

Önerdiğimiz optimizasyon algoritmalarla üretilen kriptografik anahtarları temel alan görüntü şifreleme algoritmasının temel adımları şu şekilde olacaktır;

1) Orijinal görüntü, JPEG veya fraktal sıkıştırma algoritması kullanılarak sıkıştırılır. Bu adımla şifrelenecek piksel sayısı p azaltılır.

2) Optimizasyon algoritmasının başlangıç koşul ve parametreleri kontrol edilir.

3) LFSR tabanlı rastgele sayı üreteci istenilen flip-flop sayısında çalıştırılır

4) 0/1 lerden oluşan rastgele bit dizisi oluşturulur.

5) Elde edilen bitler 8 bitlik gruplara ayırılır ve gruplar 0-255 arasında tam sayı değerlere dönüştürülür. Bu değerler algoritmanın gizli anahtarıdır.

6) Piksel değerleri ve anahtar değerleri için XOR işlemi kullanılarak şifrelenmiş değerler elde edilir.

ANALİZ SONUÇLARI

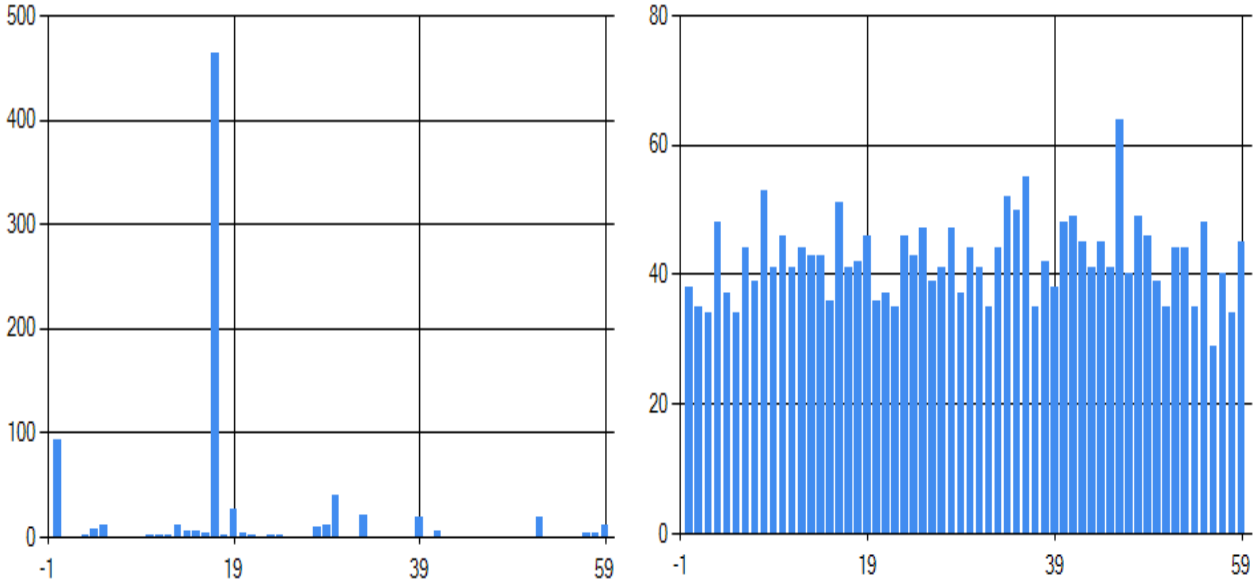
Önerilen görüntü şifreleme algoritmasının sonuçları analiz edilirken histogram, NPCR ve UACI ölçümleri kullanılmıştır. Analiz yapılırken düşük boyutlu görüntü kullanılmıştır. Orijinal görüntü boyutu ile şifrelenmiş görüntü boyutları birbirine eşittir. Dolayısıyla boyutsal anlamda kayıp oluşmamıştır. Elde edilen şifreleme algoritmasının küçük ölçekli görüntülerdeki başarısı gösterilmiştir. Analizde kullanılan orijinal görüntü Şekil 4' te verilmiştir.

Bu görüntülerin histogram analizi Şekil 5'te verilmiştir. Orijinal görüntülerin histogram dağılımında bir korelasyon vardır. Ancak, şifrelenmiş görüntülerin histogram dağılımından herhangi bir çıkarım yapılamaz. NPCR ve UACI ölçütlerinin ideal değerleri sırasıyla 1 ve 0.33' tür (Özkaynak, 2017). Bizim şifreleme algoritmamızın sonucunda NPCR değeri 0.9962 iken UACI değeri de 0.3362 olarak elde edilmiştir.

IJPAS
ijpas@munzur.edu.tr
ISSN: 2149-0910

Research article/Araştırma makalesi
DOI:10.29132/ijpas.1182404

Şekil 4. a) orijinal görüntü **b)** şifrelenmiş görüntü



Şekil 5. a) orijinal görüntü histogramı **b)** şifrelenmiş görüntü histogramı

SONUÇLAR

Çalışmamızda hibrit bir görüntü işleme algoritması önerilmiştir. Önerilen yöntemde şifrelenecek anahtar üretim kısmında optimizasyon tabanlı rastgele sayı üreteci kullanılmıştır. Geçmiş çalışmalarımızda oldukça iyi istatistik gösteren anahtar üretecimiz ile görüntü şifreleme işlemindeki güvenliği arttırma hedeflenmiştir. Elde edilen rastgele anahtar ile şifrelenen görüntünün histogramı, Değişken piksel hızı sayısı (NPCR) ve birleşik ortalama değişen yoğunluk (UACI) ölçütleri ile analizi gerçekleştirilmiştir. Analiz sonuçları incelendiğinde, rastgele ürettiğimiz anahtarın küçük ölçekli görüntüleri şifrelemede de oldukça başarılı olduğu gözlemlenmiştir. Gözlemler sonucunda, anahtar üretecinin daha büyük boyutlardaki görüntülerin şifrelenmesinde de başarılı olabileceği düşünülmektedir. Bilgi güvenliğinin bir parçası olan görüntü şifreleme üzerinde elde edilen bu başarı doğrultusunda, önerdiğimiz anahtar üreteci yönteminin diğer birçok alanda da etkili sonuçlar elde edebileceği ve gelecek çalışmalarda uygulanabilir ve kullanılabilir etkili bir anahtarlar üretebileceği sonucuna varılmıştır.

ÇIKAR ÇATIŞMASI BEYANI

Yazarlar bu makale ile ilgili herhangi bir çıkar çatışması bildirmemektedir.

ARAŞTIRMA VE YAYIN ETİĞİ BEYANI

Yazarlar bu çalışmanın araştırma ve yayın etiğine uygun olduğunu beyan eder.

IJPAS
ijpas@munzur.edu.tr
ISSN: 2149-0910

Research article/Araştırma makalesi
DOI:10.29132/ijpas.1182404

KAYNAKLAR

Asif, M. ve Baig, R., (2009). "Solving NP-complete problem using ACO algorithm," 2009 International Conference on Emerging Technologies, pp. 13-16, doi: 10.1109/ICET.2009.5353209.

Burhan, Y., Artuger, F. ve Ozkaynak, F., (2019). "A Novel Hybrid Image Encryption Algorithm Based on Data Compression and Chaotic Key Planning Algorithms," 2019 7th International Symposium on Digital Forensics and Security (ISDFS), pp. 1-5, doi: 10.1109/ISDFS.2019.8757530.

Eröz, E., Tanyıldızı, E. ve F. Özkaynak, (2021). "Determination of Suitable Configuration Parameters for Linear Feedback Shift Register using Binary Bat Optimization Algorithm," IEEE EUROCON 2021 - 19th International Conference on Smart Technologies, pp. 348-351, doi: 10.1109/EUROCON52738.2021.9535616.

Garipcan, A. M. ve Erdem, E., (2019). Implementation and Performance Analysis of True Random Number Generator on FPGA Environment by Using Non-periodic Chaotic Signals Obtained from Chaotic Maps. Arab J Sci Eng 44, 9427–9441. https://doi.org/10.1007/s13369-019-04027-x

Garipcan A. M. ve Erdem E., (2020). A TRNG using chaotic entropy pool as a post-processing technique: analysis, design and FPGA implementation. Analog Integr Circ Sig Process 103, 391–410. https://doi.org/10.1007/s10470-020-01605-0

Kennedy, J. ve Eberhart, R. C., (1997). A discrete binary version of the particle swarm algorithm. In: IEEE international conference on computational cybernetics and simulation, pp 4104–4108.

Mirjalili, S., Mirjalili, S.M. ve Yang, X.S., (2014). Binary bat algorithm, Neural Comput. Appl. 25, 663–681.

Özkaynak, F, (2017). Role of NPCR and UACI tests in security problems of chaos based image encryption algorithms and possible solution proposals, 2017 International Conference on Computer Science and Engineering.

Rashedi, E., Nezamabadi-pour H. ve Saryazdi S., (2009). BGSA: binary gravitational search algorithm. Nat Comput 9:727–745.

Robshaw, M. ve Billet, O., editors. (2008). New Stream Cipher Designs: The eSTREAM Finalists, volume 4986 of LNCS. Springer.

Schindler, W., (2009). "Random number generators for cryptographic applications", C.K. Koc (ed.): Cryptographic Engineering. Springer, Signals and Communication Theory, Berlin, DOI: 10.1007/978-0-387-71817-0_2.

Sheveleva, A. M. ve Belyaev, S. A., (2021). "Development of the Software for Solving the Knapsack Problem by Solving the Traveling Salesman Problem," 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus), pp. 652-656, doi: 10.1109/ElConRus51938.2021.9396448..

Stipčević, M. ve Koç, Ç. K., (2014). "True random number generators", in Koç Ç. K. (eds) Open Problems in Mathematics and Computational Science. Springer, Cham. DOI: 10.1007/978-3-319-106830_12.

Paar, C. ve Pelzl, J., (2010). Understanding Cryptography A Textbook for Student and Practitioners, Springer.