Araştırma Makalesi
Adıyaman Üniversitesi
Mühendislik Bilimleri Dergisi
18 (2022) 571-580

KAYIPLI RESİM SIKIŞTIRMA ALGORİTMALARINI TEMEL ALAN RASTGELE SAYI ÜRETECİ

Selman YAKUT[1*]

[1]İnönü Üniversitesi, Mühendislik Fakültesi, Yazılım Mühendisliği Bölümü, Malataya, 02040, Türkiye
Geliş Tarihi/Received Date: 19.07.2022 Kabul Tarihi/Accepted Date: 11.10.2022 DOI: 10.54365/adyumbd.1145590

ÖZET

Dijitalleşen dünyada veri güvenliği önemli bir problemdir. Veri güvenliğini sağlamak için çeşitli kriptoğrafik sistemler ve uygulamalar kullanılır. Rastgele sayılar ise bu sistemlerin ve uygulamaların önemli bir parçasıdır. Bu makalede resim sıkıştırma algoritmalarının temeli olan ayrık kosinüs dönüşümünü kullanan bir rastgele sayı üreteci önerildi. Bu üreteçte öncelikle sıkıştırılacak olan resim, ayrık kosinüs dönüşümü ile frekans düzlemine aktarılır. Frekans düzleminde insan görme duyusu dikkate alınarak resmi ifade eden belirli katsayılar dikkate alınıp diğerleri ihmal edildiğinden veri kaybı olur. Daha sonar Frakans düzlemindeki veri ters ayrık kosinüs dönüşümü kullanılarak yeniden uzay düzlemine aktarılır. Bu dönüşüm esnasında hesaplanan küsuratlı değerler resmi ifade etmek için yuvarlanır. Yuvarlama esnasında bu veriler geriye döndürülemeyecek şekilde kaybedilir. Bu kayıplar bir entropi kaynağı olarak kullanıldı ve ham rastgele sayılar üretildi. Bu sayılardaki olası zayıflıklar kriptografik özet fonksiyonunun son işlem algoritması olarak kullanılmasıyla giderildi. Kriptografik özet fonksiyonu olarak SHA1 algoritması kullanıldı. Önerilen üreteç herhangi bir dijital veri kaynağını rastgele sayı üreteci olarak kullanabilir. Önerilen üretecin güvenliği yapılan testlerle ve analizlerle gösterildi.

Anahtar Kelimeler: *Ayrık kosinüs dönüşümü, Rastgele sayılar, Rastgele sayı üreteci, Son işlem algoritmaları*

RANDOM NUMBER GENERATOR BASED ON LOST PICTURE COMPRESSION ALGORITHMS

ABSTRACT

Data security is an important problem in the digitalized world. Various cryptographic systems and applications are used to ensure data security. Random numbers are an important part of these systems and applications. In this article, a random number generator using the discrete cosine transform, which is the basis of image compression algorithms, is proposed. In this generator, the picture to be compressed first is transferred to the frequency plane with the discrete cosine transform. Data loss occurs because certain coefficients expressing the picture are taken into account and others are neglected by considering human vision in the frequency plane. Then the data in the frequency plane is transferred back to the space plane using the inverse discrete cosine transform. The fractional values calculated during this conversion are rounded up to represent the picture. During rounding, this data is irreversibly lost. These losses were used as a source of entropy and raw random numbers were generated. Possible weaknesses in these numbers were addressed by using the cryptographic hash function as the post-processing algorithm. The SHA1 algorithm was used as the cryptographic hash function. The proposed generator can use any digital data source as a random number generator. The safety of the proposed generator has been demonstrated by tests and analysis.

Keywords: *Discrete cosine transform, random numbers, random number generator, post processing algorithms*

1. Giriş

Bilgi güvenliği günden güne daha fazla dijitalleşen dünyanın önemli bir problemidir. Akıllı telefon, tablet, bilgisayar, kamera gibi dijital veri kaynakları yaygın bir şekilde ve artarak

e-posta[1] : selman.yakut@inonu.edu.tr ORCID ID: https://orcid.org/0000-0002-0649-1993 (Sorumlu Yazar)

kullanılmaktadır [1]. Bu dijital kaynaklarının zayıf yönlerini kullanmaya yönelik birçok saldırı yapılmaktadır [1]. Bu saldırıların engellenmesi ve mağduriyetlere sebebiyet vermemek için çok sayıda kriptoğrafik sistem ve protokol kullanılmaktadır [3-5]. Bu sistemlerin ve protokollerin hem veri kaynaklarının güvenliğini hem de verilerin güvenliğini sağlaması amaçlanır. Bunların güvenliği ise temel olarak anahtar değeri, tohum değeri gibi gizli ve güvenli değerlere dayanır [3-4]. Bu değerlerin güvenliğinin garanti edilmesi için güvenli rastgele sayılar kullanılır.

Rastgele sayılar bilgi güvenliği üzerinde belirleyici olan önemli parametrelerden biridir [3-7]. Bu sayılar birçok kriptoğrafik uygulamanın ve sistemin önemli bir parçasıdır [6,7]. Özel-genel anahtar çifti, gizli anahtar, tohum değeri bunların başında gelmektedir. Bu değerin bütün sistem üzerinde kritik bir öneme sahip olduğundan bu sayıların üretilmesi önem arz etmektedir.

Rastgele sayı üretimi çeşitli yöntemler ve kaynaklar kullanılarak yapılabilir. Ancak temel olarak rastgele sayı üreteçleri gerçek rastgele sayı üreteçleri (GRSÜ), sözde rastgele sayı üreteçleri(SRSÜ) ve hibrit rastgele sayı üreteçleri(HRSÜ) olmak üzere üç sınıfa ayrılır. GRSÜ üreteçleri elektronik gürültü, radyoaktif bozulma gibi fiziksel ve tekrarlanmayan kaynakları kullanır [8, 9]. SRSÜ belirli bir algoritma ve tohum değeri kullanılarak hesaplamalara dayanan üreteçlerdir [10-12]. HRSÜ ise bu iki yaklaşımın beraber kullanımına dayanır.

Farklı rastgelelik kaynaklarından üretilen ham rastgele sayılardaki muhtemel zayıflıkların korelasyonun giderilmesi için son işlem algoritmaları kullanılır. Literatürde çok sayıda son işlem algoritması mevcuttur ve bu algoritmaların rastgele sayı üretiminde kullanımı yaygındır [6, 13-17]. Bunların önemli bir türü ise kriptografik özet algoritmalarıdır [14]. Bunun başlıca sebebi ise bu algoritmalar tek yönlü fonksiyonlardır ve giriş verisi özet değerinden üretilemez. Ayrıca bu algoritmaların çakışmaya karşı dayanıklı olması diğer bir önemli güvenlik parametresidir. Böylece bu algoritmalarla düzgün bir dağılıma sahip ve güçlü istatistiksel özelliklere sahip sayılar üretilir [17, 18].

Dijital verilerin iletim ve depolama işlemlerindeki yükünü azaltmak için bu veriler sıkıştırma işlemlerine tabi tutulur [19]. Sıkıştırma işlemi kayıplı ve kayıpsız sıkıştırma olmak üzere ikiye ayrılır [20-22]. Kayıpsız sıkıştırmada resim üzerinde herhangi bir kayıp olmadan orijinal resmin sıkıştırılır. Kayıplı sıkıştırmada ise orijinal resim bazı geri döndürülemeyen kayıplara uğrar ve orijinal resmin yeniden üretilemez. Kayıplı sıkıştırmada yaygın kullanılan yaklaşım orijinal resmin çeşitli dönüşümler yardımıyla frekans uzayına aktarılması ve aktarılan bu verinin frekans uzayındaki çeşitli işlemler yardımıyla sıkıştırılmasına dayanaır. JPEG gibi birçok algoritmanın kullanıldığı Ayrık Kosinüs Dönüşümü (AKD) ise bunların başında gelir.

AKD veri sıkıştırma için kullanılan yöntemlerin başında gelir [19, 24, 25]. AKD uygulanan veriler frekans düzlemine aktarılır. Frekans düzlemine insan görme duyusunu dikkate alınarak bazı katsayılar hesaplamada daha fazla dikkate alınırken bazı katsayılar ise göz ardı edilir [26]. Böylece insan gözü ile fark edilmeden veya az fark edilen veriler ihmal edilir ve kaybedilir. Daha sonra veri, Ters Ayrık Kosinüs Dönüşümü (TAKD) uygulanarak yeniden uzay düzlemine aktarılır. Bu aktarma sürecinde bir dizi matematiksel işlemler kullanılarak veri önemli oranda sıkıştırılır [23]. Sıkıştırılan veri uzay düzlemine aktarıldığında bazı kayıplara uğrar ve orijinal veri yani sıkıştırma işlemine uğramamış olan hali bu sıkıştırılmış veriden yeniden üretilmesi mümkün olmaz. [24-29].

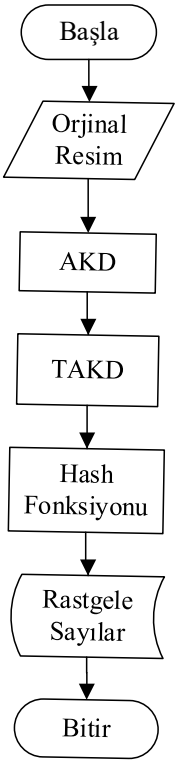
Önerilen yöntemde ayrık kosinüs dönüşümü kullanılarak sıkıştırılan resimdeki kayıplar kullanılarak ham rastgele sayılar üretildi. Herhangi bir işleme uğramamış olan orijinal resim sıkıştırma işleminden geçirilerek öncekle frekans uzayına aktarılır. Frekans uzayına aktarılan verilerin insan görme duyusu dikkate alınarak bazı katsayıları muhafaza edilirken bazı katsayıları ise göz ardı edilir. Daha sonra frakans uzayındaki veriler TAKD kullanılarak yeniden uzay düzlemine aktarılır. Yeniden aktarma işleminde veriler sıkıştırılmış resme dönüştürülürken yuvarlama işlemlerine tabi tutulur. Yuvarlanan bu verilerin küsuratlı kısmı geriye döndürülemez bir şekilde kaybedilir. önerilen bu yöntemde kayıp olarak ifade edilen bu veriler entropi kaynağı olarak kullanıldı ve bu entropi kaynağından ham rastgele sayılar üretildi. Üretilen bu sayılar son işlem olarak kriptografik özet algoritmalarından geçirildi. Böylece üretilen rastgele sayıların hem uniform bir dağılıma sahip olması hem de güvenli bir hale gelmesi

sağlandı. Önerilen yöntemle birçok dijital veri kaynağı rastgele sayı üreteci olarak kullanılabilir. Ayrıca bu yöntemle üretilen rastgele sayıların güvenli olduğu istatistiksel testlerle ve analizlerle gösterildi.

Bu çalışmanın devamı şu bölümler oluşur. İkinci bölümde önerilen yöntemin yapısı, kullanılan entropi kaynağı ve yapılan işlemler incelendi. Sonraki bölümde üretilen sayıların istatistiksel sonuçlarına yer verildi ve kullanılan yöntemin güvenlik değerlendirmesi yapıldı. Son bölüm de ise yapılan çalışmayla ilgili sonuçlara yer verildi.

2. Önerilen Yöntem

Önerilen yöntemle kriptografik uygulamalar başta olarak birçok uygulamanın önemli bir parçası olan güvenli rastgele sayılar üretildi. Bu yöntemin genel yapısı Şekil 1'de verildi. Bu yapıda öncelikle herhangi bir sıkıştırma ve benzeri işlemden geçirilmeyen resim, orijinal resim olarak ifade edilir ve AKD kullanılarak frekans düzlemine aktarılır. Bu düzleme aktarılan veri insan görme duyusunun hassas olduğu katsayılar korunurken diğerleri daha az muhafaza edilir. Daha sonra frekans düzlemindeki veri TAKD ile tekrar uzay düzlemine dönüştürülür. Bu ters dönüşüm işleminde hesaplanan değerlerin sıkıştırılmış resme dönüştürülmesi için hesaplanan değerler yuvarlanır. Yuvarlama işleminde küsurat verileri kaybedilir. Kaybedilecek bu verilerin ham rastgele sayı üretiminde kullanıldı. Böylece dijital resim bir entropi kaynağı olarak kullanıldı. Daha sonra bu ham veriler ise son işlem olarak kriptoğrafik hash algoritmasından geçirilerek güvenli gerçek rastgele sayılar üretildi.



Şekil 1. Önerilen metodun genel yapısı

AKD verilerin uzay düzleminden frekans düzlemine aktarılmasını sağlayan furier tabanlı bir dönüşümdür. İlk olarak orijinal veri AKD ile frekans düzlemine aktarılır. Bu düzleme aktarılan veriler katsayı matrisi ile ifade edilir. Bu katsayı matrisinin bazı değerleri korunurken bazı değerler ise ihmal edilir. Daha sonra frekans düzlemindeki veri TAKD dönüşümü kullanılarak uzay düzlemine aktarılır. Böylece orijinal veriden bazı kayıplar verilerek sıkıştırılmış veri oluşturulur. AKD dönüşümü için

kullanılan formül denklem1'de verildi. Öncelikle bu denklem kullanılarak uzay düzlemindeki resim frekans düzlemine aktarıldı. Bu matrisler kullanılarak ilgili düzlemler arasında dönüşümler yapıldı.

$$C(u,v) = \mathrm{a(u)a(v)} \sum_{x=0}^{N-1} \sum_{y=0}^{N\_1} f(x,y) \left(\cos \frac{(2x+1)\pi x}{2N} + \sin \frac{(2y+1)\pi x}{2N} \right) \tag{1}$$

Burada a(u) ve a(v) değerleri denklem 2'de gibi hazırlanır ve bu değerlerin ölçeklendirilmesi olarak ifade edilmaktedir.

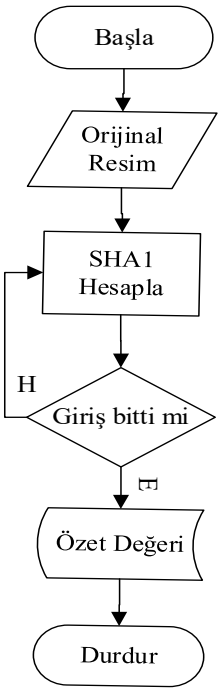
$$a(k) = \begin{cases} \sqrt{\frac{1}{N}} & k = 0 \; ise \\ \sqrt{\frac{2}{N}} & k \neq 0 \; ise \end{cases} \tag{2}$$

TAKD ise denklem3'te gösterildiği gibi gerçekleştirilir. Bu veriler kullanılarak frekans düzleminde bulunan veriler TAKD yeniden uzay düzlemine aktarılır.

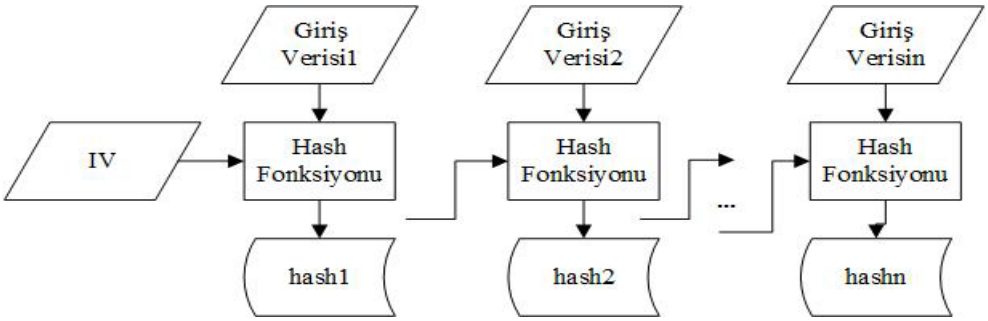
$$f(x,y) = \sum_{x=0}^{N-1} \sum_{y=1}^{N\_1} \mathrm{a(u)a(v)} C(u,v) \left(\cos \frac{(2x+1)\pi x}{2N} + \sin \frac{(2y+1)\pi x}{2N} \right) \tag{3}$$

Tasarlanan üreteçte son işlem algoritması olarak SHA1 kriptografik özet fonksiyonu kullanıldı. Bu fonksiyon birçok kriptografik protokolün ve sistemin temilinde yer alır. Bu fonksiyonları verilen bir mesaj için bu mesajın parmak izi olarak ifade edilebilen özetini oluşturur. Özet çıkarma işleminde giriş verisi bazı mantıksal veya cebirsel işlemlerden geçirilir ve sıkıştırılır. Böylece giriş verisindeki muhtemel zayıflıklar ve korelasyon giderilerek güvenli özet değerleri üretilir. Bu fonksiyonların genel yapısı Şekil 2'de verildi. Burada giriş mesajı bloklara ayrılarak SHA1 algoritmasından geçirilir. Son blok işlendikten sonra ise özet değeri üretilir.

Hash fonksiyonları tarafından üretilen özet değeri kullanılan fonksiyona bağlıdır. Farklı hash fonksiyonları kullanarak değişen uzunluklarda özet değeri üretilebilir. Bununla beraber kullanılan belirli bir fonksiyon için giriş mesajının uzunluğundan bağımsız olarak üretilen özet değeri sabit bir uzunluktadır. Bu problemin üstesinden gelmek ve istenilen uzunlukta çıkış verisi üretmek için Şekil 3'te verilenn yapı önerildi. Bu yapıda kriptografik hash fonksiyonları ardışık bağlanarak özet değerinin boyutundan daha büyük boyutta rastgele sayıların üretilmesi sağlandı. Her bir adımda alınan özet değeri hem rastgele sayı üretiminde ve hem de bir sonraki özet değerinin hesaplaması işleminde giriş olarak kullanılır.



Şekil 2. Kriptografik özet fonksiyonlarının yapısı



Şekil 3. Tasarlanan Son işlem algoritmasının yapısı

3. Önerilen Yöntemin Sonuç Analizi

Rastgele sayıların kullanıldığı uygulamaların güvenliği rastgele sayıların güvenliğine bağlıdır. Çünkü bu sayılar bu uygulamaların en temel ve önemli parçasını oluşturur. Dolayısıyla bu uygulamalarda kullanılan sayıların güvenli olması bir zorunluluktur. Bu sayıların güvenli kabul edilebilmesi için çeşitli güvenlik parametreleri sağlaması gerekir. Bu parametrelerden ilki rastgele sayıların üretildiği kaynağın ve kullanılan yöntemin güvenli olmasıdır. İkinci olarak üretilen rastgele sayılar herhangi bir istatistiksel zayıflık içermemelidir. Diğer bir önemli parametre ise bu sayılar kriptografik uygulamalar için gerekli güvenlik gereksinimlerini karşılamalıdır. Bununla beraber rastgele sayıların üretim maliyeti diğer önemli bir parametredir.

Önerilen yaklaşım kayıplı sıkıştırmada yaygın kullanılan AKD ve TAKD dönüşümlerine dayanır. Bu yaklaşımla orijinal veriden bazı kayıplar verilerek sıkıştırılmış veri üretilir. Burada kayıp miktarı

orijinal resimdeki sıkışma oranına göre değişir. Burada frekans uzayına aktarılan verinin bazı katsayıları göz ardı edildiği için orijinal resim yeniden üretilmez. Böylece sıkıştırılmış veri üretilirken oluşan bu kayıp entropi kaynağı olarak kullanılabilir. Bu çalışmada bu entropi kaynağı kullanılarak ham rastgele sayılar üretildi. Çizelge 1'de rasgele sayı üretiminde kullanılan orijinal resmin piksel değerleri verildi. Çizelge 2'de sıkıştırılma işleminin ilk adımı olan AKD uygulanan verileri göstermektedir. Çizelge 3'te TAKD uygulanarak frekans düzleminden uzay düzlemine yapılan dönüşümünde belirlenen katsayı değerlerini vermektedir. Çizelge 4'te ise rastgele sayı üretiminde kullanılan ham verilere ait değerlerden bir kısmını götermektedir.

Çizelge 1. Orijinal resmin piksel değerleri

	1	2	3	4	5	6	7	8	9	10	11	12
1	225	226	225	226	227	228	228	228	227	229	228	227
2	224	225	225	226	227	228	227	228	228	228	228	227
3	224	225	226	226	227	228	228	227	227	229	228	228
4	224	225	225	228	227	226	228	228	228	229	228	229
5	222	225	224	226	226	228	227	228	228	228	228	228
6	223	224	224	226	226	226	227	227	228	228	228	229
7	224	224	225	226	226	226	226	226	227	228	228	228
8	223	223	224	225	226	226	227	227	227	228	226	227
9	224	224	224	226	226	227	228	228	229	227	228	227
10	224	224	225	225	226	228	227	228	229	229	229	228

Çizelge 2. AKD uygulanan örnek veriler

	1	2	3	4	5
1	29785.2685489355	3603.60062826697	-1762.67385721419	1621.03676202521	-2092.81481009980
2	13557.3858786407	1558.12169270274	-619.011995007471	634.421290161716	-603.345430076651
3	10940.0939388269	779.343940800997	-521.386076234834	583.213324754933	-827.629459383619
4	85.4995012169370	-2757.807622913 28	-685.666724610639	-354.220359868185	974.357829024384
5	-100.698228203587	-2397.725642876 74	365.115993454813	-680.767764131329	702.706349828263

Çizelge 3. TAKD uygulanan örnek veriler

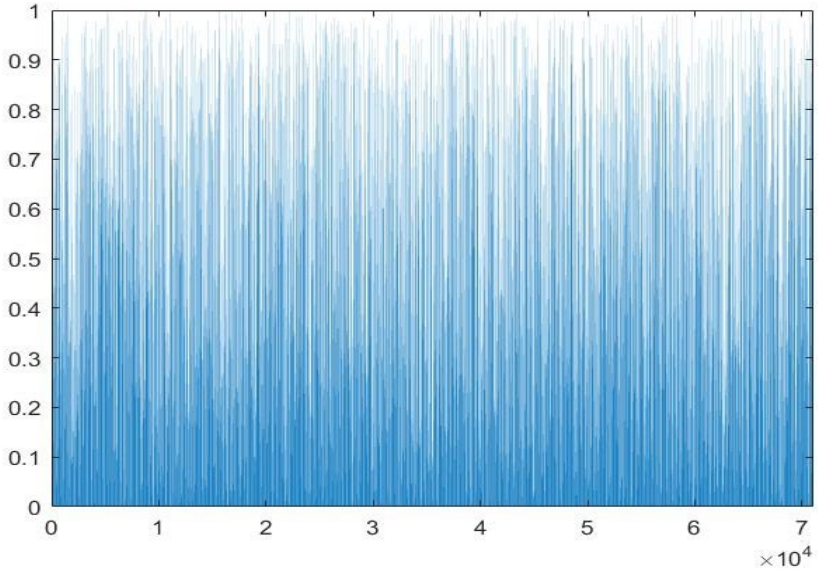
	1	2	3	4	5
1	0.901585108941195	0.916152200050551	0.917805901482007	0.939050886293754	0.937434486436737
2	0.904635680891901	0.926777479694500	0.919765978820472	0.922415043978554	0.927046446231555
3	0.904530628927833	0.932446129931800	0.927771885328633	0.931909201899830	0.928295933884807
4	0.938907631800396	0.934841224535532	0.914553095041629	0.918074397583235	0.913347187812485
5	0.916276058803425	0.916841528883139	0.911844743535691	0.911600911254935	0.913242539852693

Çizelge 4. Rastgele sayı üretiminde kullanılan ham veriler

	1	2	3	4	5
1	0.354107095182115	0.894186788153263	0.785651404172484	0.315792162514526	0.762536246987679
2	0.724289213617396	0.575984260591497	0.914030276460437	0.689567794389859	0.732456706155404
3	0.711202940039044	0.069927331086830 7	0.804946797249841	0.788761177295783	0.075541772366790 4
4	0.966947610207882	0.676723389703170	0.393939283765263	0.363382026595843	0.997473763301173
5	0.854141147551218	0.827035837561709	0.631685352548345	0.228520406866153	0.068712019918876 9

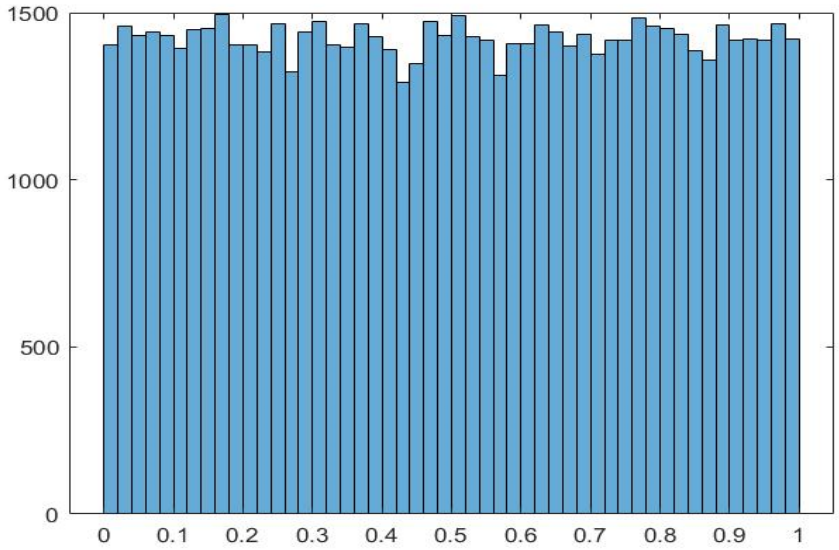
Önerilen üreteçteki muhtemel korelasyon ve zayıflıklar giderilmesi için SHA1 kriptoğrafik özet fonksiyonu kullanıldı. Bu fonksiyon kriptoğrafik uygulamalar için gerekli olan gereksinimleri karşıladığından üretilen sayıların güvenliğini garanti eder. R1-R4 olarak ifade edilen bu gereksinimler üretilen sayıların istatistiksel zayıflık içermemesi, yeniden üretilememesi, geriye döndürülememesi gibi parametrelerdir. İlk olarak SHA1 fonksiyonu, kriptografik özet fonksiyonlarında olduğu gibi tek yönlü olduğundan özet değerinden giriş mesajı hesaplanamz [30]. Ayrıca kriptografik özet fonksiyonları çakışmaya karşı dayanıklı olduğundan farklı giriş mesajları için aynı özet değerinini üretilemez. Bu gereksinimlerin karşılanması sağlanması güvenliği belirleyen iki önemli parametredir.

Güvenli rastgele sayı üreteçleri herhangi bir istatistiksel zayıflık içermemelidir. Bu zayıflıklar rastgele sayıları çeşitli saldırılara karşı açık hale getirir. SHA1 fonksiyonunun son işlem olarak kullanılması üreteçteki muhtemel istatistiksel zayıflıkların giderilmesini sağlar. Rastgele sayı üreteçlerini istatistiksel olarak değerlendirmek için histogram analizi yaygın bir şekilde kullanılan testlerden biridir. Ayrıca üretilen sayıların düzgün bir dağılıma sahip olması üretilen sayıların güvenliği için diğer bir önemli parametredir. Şekil 4'te verilen sonuçlar üretilen sayıların [0-1] aralığındaki dağılımını vermektedir. Şekilde dikey veriler [0-1] aralığında üretimini yatay eksende ise üretilen sayı adedini göstermektedir. Şekilde görüldüğü gibi üretilen sayıların bir düzgün dağılıma sahip olduğunu ve üretecin güvenli olduğunu gösterir.



Şekil 4. Kullanılan Ham verilerin üretim aralığı

Histogram analizi istatistiksel analizde yaygın kullanıldığından üretilen sayıların analizinde de kullanıldı. Böylece üretilen rastgele sayılar istatistiksel olarak analiz edilir ve üreteçteki muhtemel istatistiksel zayıflıklar tespit edilir [31]. Histogram analizinde elde edilen düzgün dağılım önerilen yöntemin güvenli olduğunu ve istatistiksel zayıflık içermediğini gösterir. Önerilen yöntemle ilgili test sonuçları Şekil 5'te verildi. Şekildeki yatay eksen verilen aralıktaki sayıları gösterir. Şekildeki dikey eksen rastgele sayıların üretim adedini gösterir. Burada üretilen adedinin bir birine yakın olduğunu ve düzgün bir dağılıma sahip olduğunu gösterir.



Şekil 5. Üretilen ham verilerin histogram dağılımları

4. Sonuçlar

Rastgele sayılar birçok uygulamanın önemli bir parçasını oluşturur. Bu sayılar atmosferik veri, elektriksel gürültü gibi farklı kaynaklardan üretilebilir. Bu çalışmada ayrık kosinüs dönüşümünü temel alan kayıplı sıkıştırma işlemleri kullanılarak rastgele sayılar üretildi. AKD uzay düzlemindeki verileri frekans düzlemine aktarılır. Frekans düzlemine aktarılan veriye ait katsayı matrisindeki bazı katsayılar, insan görme duyusu dikkate alınarak korunurken bazısı ise ihmal edilir. Böylece orijinal resim bazı kayıplar verilerek sıkıştırılır. Daha sonra frekans düzlemindeki veriler TAKD kullanılarak yeniden uzay düzlemine aktarılır. Bu sayıaları uzay düzleminde ifade etmek için veriler yuvarlanır ve kayıplar oluşur. Bu çalışmada bu kayıplar entropi kaynağı olarak kullanılıp rastgele sayılar üretildi. Üretilen saylardaki muhtemel zayıflıkların giderilmesi için son işlem algoritması olarak SHA1 kriptografik özet fonksiyonu kullanıldı. Bu fonksiyonun tek yönlü ve çakışmaya dayanıklı olması üretilen sayıların güvenli olmasını sağlar. Böylece başta kriptoğrafik uygulamalar olmak üzere birçok alanda gerekli olan güvenlik gereksinimleri karşılanır. Histogram analizi kullanılarak üretilen sayıların herhangi bir istatistiksel zayıflık içermediği gösterildi.

Kaynaklar

[1] Yadav H, Gautam, S, Rana, A, Bhardwaj, J, Tyagi, N. Various Types of Cybercrime and Its Affected Area. In: Tavares, J.M.R.S. Chakrabarti, S., Bhattacharya, A., Ghatak, S. (eds) Emerging Technologies in Data Mining and Information Security. Lecture Notes in Networks and Systems, 2021; vol 164. Springer, Singapore. https://doi.org/10.1007/978-981-15-9774-9_30

[2] Yakut S. Random Number Generator Based on Discrete Cosine Transform Based Lossy Picture Compression. NATURENGS, 2021; 2 (2): 76-85. DOI: 10.46572/naturengs.1009013
[3] Koç Ç. Cryptographic Engineering. Springer, New York 2009.
[4] Menezes AJ, van Oorschot PC, Vanstone SA. Handbook of Applied Cryptography, 1st edn. CRC Press, Boca Raton. 1996.
[5] Paar C, Pelzl J. Understanding cryptography: a textbook for students and practitioners, Universitat Bochum, Bochum, Germany, Springer Publishing Company, 2009.
[6] Garipcan AM. Gerçek rasgele sayı üreteçlerinin performansını iyileştirmek için yer değiştirme kutularını temel alan yeni bir yaklaşım, Doktora Tezi, Fırat Üniversitesi Fen Bilimleri Enstitüsü. 2021.
[7] Yakut S. Gerçek Rasgele Sayı Üreteçlerinin Tasarlanması ve Analizi, Doktora Tezi, Fırat Üniversitesi Fen Bilimleri Enstitüsü. 2019.
[8] Datcu O, Macovei C, Hobincu R. Chaos Based Cryptographic Pseudo-Random Number Generator Template with Dynamic State Change. Applied Sciences. 2020; 10, 451. https://doi.org/10.3390/app10020451
[9] Al-Roithy BO, Gutub A Remodeling randomness prioritization to boost-up security of RGB image encryption. Multimed Tools Applications. 2021; 80, 28521–28581. https://doi.org/10.1007/s11042-021-11051-3
[10] Aljohani M, Ahmad I, Basheri M, Alassafi MO. Performance Analysis of Cryptographic Pseudorandom Number Generators. IEEE Access. 2019; 7: 39794–39805.
[11] Kopparthi VR, Kali A, Sabat SL, Anumandla KK, Peesapati R, Fouda JAE. Hardware architecture of a digital piecewise linear chaotic map with perturbation for pseudorandom number generation. AEU-International Journal of Electronics and Communications, 2022; 147, 154138.
[12] Parisot A, Bento LMS, Machado RCS. Testing and selecting lightweight pseudo-random number generators for IoT devices. 2021 IEEE International Workshop on Metrology for Industry 4.0 & IoT (MetroInd4.0&IoT). 2021; pp. 715-720, doi: 10.1109/MetroInd4.0IoT51437.2021.9488454.
[13] Yakut S, Tuncer T, Özer AB. A New Secure and Efficient Approach for TRNG and Its Post-Processing Algorithms. Journal of Circuits, Systems and Computers. 2020.
[14] Avaroğlu E, Tuncer T. A novel S-box-based postprocessing method for true random number generation. Turkish Journual of Electrical Engineering and Compputer Sciences. 2020; 28: 288–301.
[15] Garipcan AM, Erdem E. A GRSÜ using chaotic entropy pool as a post-processing technique: analysis, design and FPGA implementation. Analog Integrated Circuits and Signal Processing. 2020; 103(3): 391-410.
[16] Łoza Sz, Matuszewski Ł, Jessa M, A Random Number Generator Using Ring Oscillators and SHA-256 as Post-Processing. International Journal of Electronics and Telecommunications. 2015; 61(2): 199-204.
[17] Garipcan AM, Erdem E. A gigabit TRNG with novel lightweight post-processing method for cryptographic applications. European Physical Journal Plus 137. 2022. 493: https://doi.org/10.1140/epjp/s13360-022-02679-7
[18] Patel R, Lad K, Patel M. A Robust Video Steganography Over DCT Components of Motion Region in Compressed Domain. Soft Computing and Signal Processing. Advances in Intelligent Systems and Computing. 2021; 1325. Springer, Singapore. https://doi.org/10.1007/978-981-33-6912-2_33
[19] Fuad M, Ernawan F. Video steganography based on DCT psychovisual and object motion. Bulletin of Electrical Engineering and Informatics. 2020; 9(3): 1015~1023, ISSN: 2302-9285, doi: 10.11591/eei.v9i3.1859
[20] Roman S. Hybrid Adaptive Lossless Image Compression Based on Discrete Wavelet Transform. Entropy (Basel, Switzerland). 2020; 22(7): 751, doi:10.3390/e22070751
[21] Patel R, Lad K, Patel M. Study and investigation of video steganography over uncompressed and compressed domain: a comprehensive review. Multimedia Systems 2021; 27: 985–1024. https://doi.org/10.1007/s00530-021-00763-z

[22] Hudson G, Yasuda H, Sebestyen I. The international standardization of a still picture compression technique. in IEEE Globecom Conf., Proc. of the Global Telecommunication Conf.. 1988; 1015 – 1021. https://doi.org/10.1109/GLOCOM.1988.25989
[23] Wedaj FT, Kim S, Kim H J, et al. Improved reversible data hiding in JPEG images based on new coefficient selection strategy[J]. Eurasip Journal on Image & Video Processing. 2017; 2017(1):63.
[24] Ajmera A, Divecha M, Ghosh SS, Raval I, Chaturvedi R. Video Steganography: Using Scrambling-AES Encryption and DCT, DST Steganography. 2019 IEEE Pune Section International Conference (PuneCon). 2019; 1-7, doi: 10.1109/PuneCon46936.2019.9105666.
[25] Mao BH, Wang ZC, Zhang XP. Asymmetric JPEG Steganography Based on Correlation in DCT Domain. Computer Science. 2019; 46(01): 203-207.
[26] Nasir A, Natarajan T, Rao KR. "Discrete Cosine Transform", IEEE Transactions on Computers, ; C-23 (1): 90–93, doi:10.1109/T-C.1974.223784
[27] Al-Roithy BO, Gutub A. Remodeling randomness prioritization to boost-up security of RGB image encryption. Multimed Tools Applications. 2021; 80: 28521–28581. https://doi.org/10.1007/s11042-021-11051-3
[28] Dang Q. Secure Hash Standard (SHS), Federal Inf. Process. Stds. (NIST FIPS), National Institute of Standards and Technology, Gaithersburg, MD 2012; [online], https://doi.org/10.6028/NIST.FIPS.180-4 (Accessed June 30, 2022)
[29] Sumagita M, Riadi I, Soepomo JP, Warungboto U. Analysis of secure hash algorithm (SHA) 512 for encryption process on web based application. Int J Cyber-Secur Digital for (IJCSDF). 2018; 7(4): 373–381
[30] FIPS PUB 180-4, Secure Hash Standard (SHS), Federal Informatıon Processıng Standards Publıcatıon, 2015.
[31] Rukhin A, Soto J, Nechvatal J, Smid M, Banks DA. statistical test suite for random and pseudorandom number generators for statistical applications. NIST Special Publication in Computer Security. 2001.