Araştırma Makalesi / Research Article

İnsan Hareketleri Tabanlı Gerçek Rasgele Sayı Üretimi

Yeliz GENÇ, Seda Arslan TUNCER*

Fırat Üniversitesi, Mühendislik Fakültesi, Yazılım Mühendisliği, Elazığ

Öz
Gerçek rasgele sayı üreteci (GRSÜ) ile rasgele sayı üretmek için deterministik olmayan bir gürültü kaynağından yararlanılır. Rasgelelik derecesinin daha yüksek olması nedeniyle GRSÜ, Sözde rasgele sayı üreticisinden daha güvenli sayı üretir. Bu makalede, insan hareketleri ile rasgele sayı üreten bir GRSÜ öneriyoruz. Önerilen GRSÜ, hemen hemen tüm insanların kullandığı mobil telefonlardaki ivme ve GPS sensörlerini kullanmaktadır. İlk olarak, mobil telefonu taşıyan kişinin 3-D ortamdaki hareketleri sonucunda ivme ve konum değişimleri android tabanlı bir mobil cihazdan örneklenerek elde edilmiştir. Daha sonra, elde edilen bu işaretler, normalizasyon işlemi uygulanarak ham sayı dizilerine dönüştürülmüştür. Son olarak, sayı dizilerinin istatistiksel özelliklerini iyileştirmek için XOR son işlemi uygulanmış ve rasgele sayı üretimi gerçekleştirilmiştir. Kişi yürürken, koşarken ve stabil konumda iken sensörlerden elde edilen toplamda 15 veri seti oluşturulmuştur. Sayıların istatistiksel özellikleri NIST test süiti, Skala İndeks ve otokorelasyon ile incelenmiştir. Önerilen GRSÜ, cep telefonu platformu için uygun, evrensel ve düşük maliyetli olup kişiye özgü rasgele sayı üretmektedir.

Anahtar kelimeler: İvme Sensörü, GPS, İstatistiksel Testler, Son İşlem.

True Random Number Generation Based on Human Movements

Abstract
A non-deterministic noise source is used to generate the random number with the real random number generator (TRNG). Because the degree of randomness is higher, TRNG produces a more secure number than the PRNG number generator. In this article, we propose a TRNG that produces random numbers with human movements. The proposed TRNG uses the acceleration and GPS sensors in almost all people's mobile phones. First, the acceleration and position changes resulting from the movements of the person carrying the mobile phone in the 3-D environment are obtained by sampling from an android based mobile device. Then, these obtained marks are converted into raw number sequences by normalization process. Finally, to improve the statistical properties of the number sequences, XOR finishing was performed and random number generation was performed. A total of 15 data sets were generated from the sensors while walking, running and in stable position. The statistical properties of the numbers were examined by NIST test suite, Scale Index and autocorrelation. The proposed TRNG is suitable for mobile phone platform, universal and low cost, and it is possible to produce random number of the unique number.

Keywords: Acceleration Sensor, GPS, Statistical Test, Post-Processing.

1. Giriş

Bilgisayar biliminde oyun programlama ve şifreleme gibi alanlarda rasgele sayı üretimine ihtiyaç vardır. Üretilen sayılar tahmin edilemez, tekrar üretilememe ve iyi istatistiksel özelliklere sahip olmalıdır. Rasgele sayıların elde edilmesi amacıyla Gerçek Rasgele Sayı Üreteçleri (GRSÜ) ve Sözde Rasgele Sayı Üreteçleri (SRSÜ) olmak üzere iki üreteç vardır. Matematiksel bir fonksiyonun yardımıyla sayı üretiliyorsa, bu yolla üretilen rasgele sayılara sözde rasgele sayı adı verilir. Sözde rasgele sayılar üretmek için matematiksel fonksiyona bir başlangıç değer(tohum) verilir. Üretilecek sayılar tohuma bağlı olarak üretilir ve istendiğinde tohum değiştirilerek farklı rasgele sayılar üretilir. Her bir tohum

*Sorumlu yazar: satuncer@firat.edu.tr
Geliş Tarihi: 30.09.2018, Kabul Tarihi: 18.01.2019

değeri, ayrı bir rasgele sayı dizisi üretilmesine neden olur. GRSÜ'leri gürültü kaynağı(entropi kaynağı) olarak kontrol edilemeyen ve tahmin edilemeyen gerçek fiziksel süreçleri kullanarak sayı üretir. GRSÜ'ler tarafından üretilen sayıların rasgeleliği fiziksel sürecin rasgeleliğine bağlıdır.

Literatürde entropi kaynağı olarak elektronik devrelerde termal ve shot gürültüsü [1], jitter ve metastability [2-4], Brownian Motion [5], atmosferik gürültü ve nükleer bozulma [6] kullanılmıştır. Bunların yanı sıra ses, video, EEG, ECG, Mouse hareketleri gibi insan kaynaklı gürültü kaynaklarından SRSÜ ve GRSÜ tabanlı üreteçler gerçekleştirilmiştir. Mousavi ve arkadaşları ECG sinyallerinden sözde rasgele sayı ürettiler [7]. Üretilen rasgele sayıların kriptografik uygulamalar da anahtar olarak kullanılabilmesi için farklı iki yaklaşım sundular. Bu yaklaşımlar Advanced Encryption Standard (AES) Algorithm ve ECG'nin Interpulse Interval (IPI) özelliği tabanlıdır. Her iki yaklaşım ile elde edilen sayılar NIST test suiti ile analiz edilmiş başarılı sonuçlar elde edilmiştir. Chen ve arkadaşları kriptografik sistemler için ECG sinyallerini kullanarak SRSÜ tabanlı sayı üreteci geliştirdiler[8]. Geliştirilen sayı üreteci literatürde bilinen dokuz SRSÜ yapısı ile karşılaştırılmıştır. ECG tabanlı SRSÜ ile üretilen sayılar NIST istatistiksel testlerinden başarılı olmuş ve XOR (Exclusive OR Generator), CCG (Cubic Congruential Generator) gibi SRSÜ'lerden daha iyi sonuçlar elde edilmiştir. Dang ve arkadaşları EEG sinyalleri kullanarak SRSÜ tabanlı bir üreteç önerdiler[9]. EEG sinyallerinin 0-1 sayı dizilerine dönüştürülmesi için modüler aritmetik kullandılar. EEG veri seti alkolik kişilerden elde edilmiştir. Sayıların istatistiksel özellikleri NIST test suiti ile incelenmiş ancak bazı testlerden başarısız sonuçlar elde edilmiştir. Chen ve arkadaşları hem sağlıklı hemde hasta insanlardan alınan 5 farklı EEG işaretlerini analiz ettiler [10]. EEG işaretlerinin gausian dağılımına uyduğunu gösterdiler. Üretilen sayılar NIST testinin Non-periodic templates testinden başarısız olmuştur. Chen ve arkadaşları ses ve video görüntüler üzerindeki white noise sinyallerini entropi kaynağı olarak kullandılar [11]. GRSÜ ve SRSÜ tabanlı geliştirilen Ses and Video rasgele sayı üreteci NIST testlerinden başarılı olmuştur. Nikolic ve arkadaşları ses kartı ve mikrofon yardımıyla elde ettikleri çevresel gürültü sinyallerini kullanarak GRSÜ tabanlı sistem geliştirdiler [12]. Üretilen sayılar NIST, FIPS, otokorelasyon testlerinden başarılı olmuş mükemmel kalitede sayı üretmişlerdir. Zhou ve arkadaşları mouse hareketlerinden rasgele sayı üretmek için GRSÜ önerdiler [13]. Sayı üreteci, kişisel bilgisayar platform için uygun, düşük maliyetli ve evrensel uygulamadır. Aynı kullanıcıların alışkanlıklarından kaynaklanan hareketleri yok etmek için kaotik hash fonksiyonu kullandılar. x-y düzlemindeki mouse hareketleri 0-1 sayı dizilerine dönüştürülerek sayıların üretim hızı, düfüzyon ve rasgelelikleri test edilmiş başarılı sonuçlar elde edilmiştir [13]. Xingyuan ve arkadaşları tek boyutlu kaotik harita ve mouse hareketleri kullanarak yeni bir GRSÜ geliştirdiler. Üretilen sayılar NIST ve otokorelasyon testlerine tabi tutulmuş başarılı sonuçlar elde edilmiştir [14]. Hu ve arkadaşları mouse hareketlerinden 256 bitlik sayılar üretmek için yeni bir GRSÜ önerdiler [15]. Önerilen sistemde aynı kullanıcıların benzer hareketlerini elimine etmek için Ayrıklaştırılmış 2D Kaotik Harita değişimi, spatiotemporal kaos ve MASK algoritmalarını kullandılar. Her 3 algoritma ile üretilen sayılar istatistiksel testlerden başarılı olmuştur. Schulz ve arkadaşları kişiye özgü rasgele sayıların analizi için örüntü tabanlı analiz önerdiler [16]. 20 sağlıklı insan tarafından her birinde 300 sayı bulunan ikişer adet sayı dizileri oluşturdular. İnsana özgü rastgele sayı dizisi içinde kişiye özel bilgilerin var olabileceği gösterilmiştir. İnsan kaynaklı gürültü kaynakları kullanan rasgele sayı üreteçlerinin özeti Tablo 1'de verilmiştir.

Tablo.1 İnsan kaynaklı rasgele sayı üreteçleri ile ilgili çalışmalar

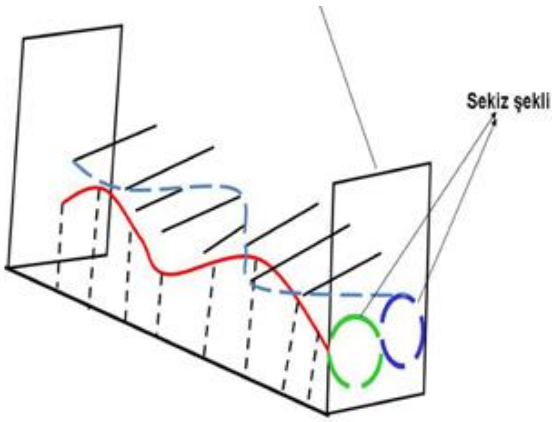
Kaynaklar	Gürültü Kaynağı	Tip	Test	Performans
[7]	ECG sinyali	SRSÜ	NIST	Başarılı
[8]	ECG sinyali	SRSÜ	NIST	Başarılı
[9]	EEG sinyali	SRSÜ	NIST	Kısmen
[10]	EEG sinyali	SRSÜ	NIST	Kısmen
[11]	Ses, Video	SRSÜ, GRSÜ	NIST	Başarılı
[12]	Ses	GRSÜ	NIST,FIPS,otokorelasyon	Başarılı
[13]	Mouse Hareketi	GRSÜ	Diffusion, NIST	Başarılı
[14]	Mouse Hareketi	GRSÜ	NIST, otokorelasyon	Başarılı
[15]	Mouse Hareketi	GRSÜ	NIST	Başarılı

Bilgisayar algoritmaları sadece rastlantısal olarak rastgele veya sahte sayılar üretebilirken, EEG, Mouse hareketleri gibi bazı doğal gürültü kaynakları gerçek rastgele sayılar üretmek için

kullanılmaktadır. Bu makalede, insanların hareketlerinin gözlemlenmesi ile gerçek rasgele sayı üretme kabiliyeti test edilmiştir. Hemem hemen tüm yetişkinlerin kullandıkları mobil telefonlardaki ivme sensörü ve GPS donanımları kullanılarak sayı üretimi gerçekleştirilmiştir. Sağlıklı bireylerin 3D ortamında hareketleri sonucunda android telefonlarından konum değişimleri ve ivme bilgileri örneklenerek elde elde edilmiştir. Elde edilen veriler normalize edilerek 0-1 sayı dizilerine dönüştürülmüştür. Sayıların istatistiksel özelliklerinin iyileştirilmesi için son işlem uygulanmış ve rasgele sayılar üretilmiştir. Öncelikle, üretilen sayı dizilerinin lineer değişime sahip olmadıklarını göstermek için Skala İndeksi testi uygulanmıştır. Daha sonra sayılar arasındaki ilişkinin belirlenmesi için otokorelasyon testi yapılmıştır. Son olarak sayıların istatistiksel özellikleri NIST test süiti ile incelenmiştir. Sonuçlar, insan hareketleri ile birbirlerinden bağımsız ve öngörülemeyen, eşit şekilde dağılmış rastgele sayılar üretebildiklerini göstermektedir.

2. Hareket Dinamiği, Konum Değişimi ve İvme

Yürümenin duruş (stance) ve salınım (swing) olmak üzere iki fazı vardır. Yürüme hızının artması sonucu oluşan koşma döngüsünde iki ayağın da yerle temas etmediği iki adet süzülme dönemi vardır. Hızlanma durumunda basma fazı kısalırken, salınım fazı uzar. Her iki eylemde amaç vücudu istenilen hız ve doğrultuda, farklı yönlerde hareket ettirmektir. Bu işlem sırasında ayak kol ve gövdedeki eklemler, kaslar, tendon ve bağlar belirgin bir şekilde kullanılır [17]. Hem yürüme hemde koşma sırasında vücut ağırlık merkezi, dikey düzlemde aşağı yukarı, yatay düzlemde ise sağa-sola hareket eder. Yatay ve düşeydeki hareketin birleştirilmesi ile hareket örüntüsü oluşur. Şekil.1 hareket esnasında ortaya çıkan örüntüyü göstermektedir. Buna bağlı olarak ta anlık x-y-z eksenindeki ivme ve konum sürekli değişiklik gösterir.



Şekil 1. İnsan hareketi esnasında ortaya çıkan örüntü

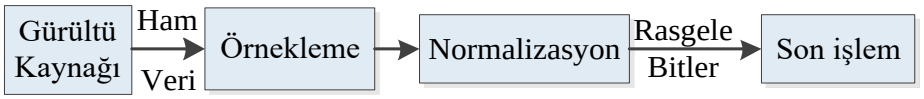
Harekete bağlı olarak küçük bir zaman içinde hızda oluşan değişimim zamana oranı ivme olarak adlandırılır. İvme, hız ve konum değişimi hakkında bilgi veren, hareketlerin takip edilmesi ve analizi için önemli bir özelliktir. Son yıllarda mobil telefonların yaygınlaşması ve donanımların ucuzlaması ile birlikte ivme sensörü tüm mobil telefonları için standart bir sensör olmuştur. Böylece ivme ölçer, kamera ve sağlıklı yaşam ile ilgili mobil uygulamalarda standart olmuştur. Bu sensörün yanı sıra tüm mobil telefonlarda bulunan bir diğer özellik GPS'lerdir. GPS, dünyanın neresinde olduğumuz konusunda bizleri bilgilendirmek adına sinyalleri uydudan alır. GPS sinyaliyle bulunulan konum x,y koordinatları mobil telefonlar ile kolaylıkla elde edilebilmektedir.

3. Önerilen GRSÜ Yapısı

Şekil 2'de GRSÜ'nin genel tasarım mimarisi gösterilmiştir. GRSÜ'lerin en önemli bileşeni gürültü kaynağıdır. Gürültü kaynağı tipik olarak elektronik devreler (gürültülü diyot veya serbest çalışan osilatör) veya fiziksel deneyler (radyoaktif bozulma veya ışığın kuantum etkisi) ile gerçekleştirilir. Gürültü kaynağı sürekli zamanlı analog sinyaller üretmekte ve aynı adımda bu değerler periyodik olarak

sayısallaştırılarak ikili (binary) değerlere dönüştürülmektedir. Sayısal değerler, sayısallaştırılmış analog sinyaller olarak adlandırılırlar. GRSÜ'lerin içerebileceği potansiyel zayıflıkları gidermek için sayılara çeşitli algoritmik son işlem yöntemleri uygulanabilir. Zayıflıkları indirgemek için XOR, von Neumann gibi basit son işlemler uygulanacağı gibi Hash tabanlı daha karmaşık son işlemler kullanılabilmektedir [18, 19]. Ancak son işlemin kullanımı durumunda GRSÜ'nin sayı üretim hızı düşmektedir.

Bu makalede önerilen GRSÜ yapısı Şekil 2'de gösterildiği gibi toplam üç bölümden oluşmaktadır. Bunlar örnekleme, normalizasyon ve son işlemdir.



Şekil 2. GRSÜ yapısı

3.1. Örnekleme

Bu makalede gürültü kaynağı olarak insan hareketleri ve buna bağlı olarak ivme ve konum değişimleri kullanılmıştır. Hareketi gerçekleştiren bireyin yürüme, koşma ve hatta durma konumunda tekrarlı hareketleri olabilir. Ancak tekrarlanan hareketlerde bile mobil telefonun ivme sensöründen ve GPS sisteminden elde edilen sayılar değişiklik gösterir. Elde edilen bu sayılar kayan noktalı sayı formatında olup örnekleme işlemi periyodik ve periyodik olmayan bir işaret ile gerçekleştirilebilmektedir. Bu makalede örnekleme işlemi periyodik olmayan kaotik davranış sergileyen tent map ile gerçekleştirilmiştir. Kaotik tent map denklem.1'eki gibi verilir.

$$f(x_i,\mu)=\begin{cases}\mu x_i & eğer\ x_i<0.5\\ \mu(1-x_i) & diğer\end{cases} \quad (1)$$

Burada, i≥0 için $x_i \in [0,1]$ aralığına sahiptir. μ , kontrol parametresi $\mu \in [0,2]$ aralığında olup x_0 sistemin başlangıç değeridir. Sonraki iterasyonlarda i≥1 için üretilecek sayılar x_1, x_2, …. olacaktır. r=1.997 ve x_0=0.32 için üretilen ilk 10 sayı S={ 0,1,1,1,1,0,0,1,0,0} olacaktır. Örneğin, x eksenindeki harekete bağlı olarak, ivme sensöründen elde edilen kayan noktalı formatındaki değerlerin a_x={ 6.18, 1.75, 1.83, 1.17, 3.05, 3.88, 2.41, 5.74, 3.39, 6.24} olması durumunda örnekleme işareti sonucunda üretilen sayı dizisi {1.75, 1.83, 1.17, 3.05, 5.74 } olacaktır. Tablo 2 örnekleme işlemi ile normalize işlemine tabi tutulacak işaretlerin elde edilmesini göstermektedir.

Tablo 2. Örnekleme işlemi ile normalize işlemine tabi tutulacak işaretlerin elde edilişi

A	6.18, 1.75, 1.83, 1.17, 3.05, 3.88, 2.41, 5.74, 3.39, 6.24
Tent map	0, 1, 1, 1, 1, 0, 0, 1, 0, 0
Örneklenmiş işaret	1.75, 1.83, 1.17, 3.05, 5.74,

3.2. Normalizasyon

Örneklenmiş işaret kayan noktalı sayı formatındadır. Bu sayılardan 0-1 sayı dizileri üretilmesi için modüler aritmetik tabanlı aşağıdaki süreç işletilmelidir. Örneklenmiş işaret $x=(x_1,x_2,\ldots x_n)^T$ olsun. Her bir örnek, tamsayı formatına dönüştürülmesi için 100 değeri ile çarpılmıştır. Elde edilen bu tam sayı dizisi modüler aritmetik kullanılarak 5 bit ile ifade edilir.

Örneğin 1.75 sayısı 175 tamsayısına dönüştürülmüştür. Bu sayının mod 32 'si alındığında, y_0 ikilik tabanda 01111 elde edilir. Elde edilen 5 bitlik y_i dizilerinden 0 ve 1 üretmek için XOR işlemi uygulanarak z_i dizisi elde edilir. Böylece y_0 için üretilen rasgele sayı z_0=0 olacaktır. Yukarıda verilen Normalizasyon süreci ile z_i rasgele sayı dizisinin elde edilişi Algoritma.1'de verilmiştir [10,20].

Algoritma 1. Normalizasyon Prosedürü

```
x=(x1,x2, ...xn)^T                    //örneklenmiş veri seti
for i=1 to n
    yi= yi*100
    yi=xi mod (32)                    // yi [0-31] aralığında
                                      //yi ikilik formata dönüştür
    for k=1 to 5
        zi= yi,0 XOR yi,1 XOR yi,2 XOR yi,3 XOR yi,4
    end
end
```

3.3. Son işlem

GRSÜ tarafından üretilen rasgele sayıların istatistiksel zayıflıklarını gidermek için son işlem uygulanır. En yaygın bilinen son işlem fonksiyonları XOR, von Neumann, BHC, hash ve kaotik haritalardır. Bu makalede elde edilen z_i dizisine uygulanan son işlem fonksiyonu XOR'dur. z_i dizisinin ardışık bitlerinin 0 ve 1 veya 1 ve 0 olması durumunda üretilen gerçek rasgele sayı 1 diğer durumlarda 0 olacaktır.

4. İstatistiksel Özellikler ve Test Sonuçları

Mobil telefon kullanıcısının 3D ortamdaki hareketleri ile hem ivme sensöründen hemde GPS ile konumlar geliştirilen android yazılım ile elde edilmiştir. Veriler kullanıcının koşma, yürüme ve durma esnasında alınmıştır. İvme sensöründen x, y, z eksenlerindeki değişimler yürüme, koşma ve sabit durumlar için elde edilmiş toplam dokuz veri setinden oluşmaktadır. GPS'in sadece x ve y eksenlerinde değer vermelerinden dolayı toplam altı veri seti oluşturulmuştur. Elde edilen sayı dizilerinin lineer değişim göstermediğini ispatlamak için öncelikle Skala İndeksi testi kullanılmıştır. Üretilen sayı dizilerindeki 0 ve 1'lerin değişimini belirlemek için otokorelasyon testi uygulanmıştır. Son olarak sayıların istatistiksel testleri NIST test süiti ile incelenmiştir.

4.1. Skala indeks

Sayıların istatistiksel analizi için uygulanan bir testtir. Benitez tarafından önerilen skala indeks üretilen rasgele sayıların periyodik olup olmadıklarını ve derecesini belirlemek için kullanılmaktadır [21]. Literatürde Gerçek ve sözde rasgele sayı üreteçlerinin periyodikliğini ölçmek için kullanılmaktadır [22, 23]. Skala indeks Sürekli Dalgacık Dönüşümü (Continuous Wavelet Transform) ve Dalgacık Çoklu Çözünürlük (Wavelet Multi Resolution) analizlerine dayanmaktadır [21]. Tablo 3 konum ve ivme için elde edilen skala indeks değerlerini göstermektedir.

Tablo 3. Konum ve ivme için Skala indeks değerleri

	$Ivme_x$	$Ivme_y$	$Ivme_z$	$Konum_x$	$Konum_y$
Koşma	0.893	0.937	0.891	0.753	0.834
Yürüme	0.945	0.879	0.847	0.955	0.894
Durma	0.882	0.870	0.765	0.881	0.851

Skala indeks değeri, i_{scale}, $0 \leq i_{scale} \leq 1$ aralığında olmalıdır. Eğer Skala değeri 0 veya 0'a çok yakın değer ise üretilen sayıların periyodik olduğunu, eğer 1 veya 1'e yakın bir değer ise üretilen sayıların periyodik olmadığını gösterir. Tablo 3 te gösterildiği gibi skala indeksi 0.7'den büyüktür. Bu sonuç, kullanıcı hareketlerinden elde edilen sayı dizilerinin lineer yapıda olmadığını göstermektedir.

4. 2. Otokorelasyon

Üretilen rasgele sayılardaki 0 ve 1'lerin değişimini gözlemlemek için otokorelasyon testi kullanılmaktadır [24,25]. Denklem.2 testin matematiksel tanımını vermektedir.

$$A(d) = \sum_{i=0}^{n-d-1} b_i \oplus b_{i+d} \tag{2}$$

Burada, $\oplus$ XOR operatörü, n üretilen sayı dizisinin uzunluğunu ve b_i, i. sayı dizisini temsil eder. d değeri [1,(n/2)] aralığında sabit bir tamsayıdır. Üretilen rasgele sayı dizisi için elde edilen *A(d)* değeri kullanılarak 0 ve 1'ler arasındaki ilişki denklem.3'deki gibi elde edilir. |X5| < 1.6449 şartının sağlanması durumunda test başarılıdır.

$$X5 = \frac{2[A(d) - (n-d)/2]}{\sqrt{n-d}} \tag{3}$$

İvme ve konum ile ilgili üretilen sayıların 0-1 değişimleri otokorelasyon ile incelendiğinde 0-1 sayı dizisinin birbirleriyle ilişkili olmadığı gözlemlenmiştir. Tablo 4, *d*=8, *d*=10 ve *d*=13 değeri için elde edilen otokorelasyon sonuçlarını göstermektedir.

Tablo 4. d=8, d=10 ve d=13 için otokorelasyon sonuçları

	d=8			d=10			d=13		
	Koşma	Yürüme	Durma	Koşma	Yürüme	Durma	Koşma	Yürüme	Durma
$İvme_x$	0.187	-0.091	0.547	-0.879	0.274	0.912	10.627	-0.547	0.347
$İvme_y$	-0.906	0.492	0.911	-0.533	0.347	1.131	-0.493	0.803	0.911
$İvme_z$	-0.479	0.331	0.298	-1.066	1.185	0.124	0.795	0.912	0.196
$Konum_x$	-1.019	0.304	0.565	0.712	0.028	-1.130	-1.425	-0.111	1.002
$Konum_y$	-0.647	0.738	0.400	-0.388	0.101	0.100	0.104	-0.386	0.225

4. 3. NIST testi

Gerçek rasgele sayıların bilgisayar biliminde kriptoğrafi, oyun teorisi ve simülasyon gibi alanlarda kullanılması için iyi istatistiksel özellikler göstermesi gerekmektedir. Literatürde rasgele sayıların istatistiksel özelliklerini belirlemek için NIST, Diehard ve FIPS gibi test süitleri vardır. Bu makalede sayıların istatistiksel özelliklerini belirlemek için NIST test süiti kullanılmıştır. NIST test suitinde toplam 15 test mevcuttur [26]. Üretilen rasgele sayılar bu testlerin tümünden başarılı olmak zorundadır. Sayıların testlerden başarılı olması için iki önemli parametre vardır. Bunlar önem seviyesi (α) ve P-value'dir. Önem seviyesinin 0.01olarak seçilmesi test edilecek sayıların rasgeleliğinin 99% güven değerine sahip olduğunu belirtir. Rasgelelik ölçüsü olarak hesaplanması gereken P-value 1'e eşit olursa sayılar mükemmel rasgeleliğe sahiptir denir. Aksi durumda sayıların rasgele olmadığı kabul edilir. Her bir test için P-value, α değerinden büyük ve eşit olursa test başarılıdır. Aksi durumda test sonucu başarısız kabul edilir. Tipik olarak önem seviyesi [0.001, 0.01] aralığında seçilir. Tablo 5, Tablo 6 ve Tablo 7 sırasıyla koşma, yürüme ve durma eylemleri için elde edilen NIST test sonuçlarını göstermektedir.

Tablo 5. Koşma esnasında elde edilen sayılar için NIST test sonuçları

	$Ivme_x$	$Ivme_y$	$Ivme_z$	$Konum_x$	$Konum_y$
The Frequency (Monobit) Test	0.894	0.462	0.035	0.052	0.423
Frequency Test within a Block	0.251	0.182	0.464	0.625	0.382
The Runs Test	0.066	0.018	0.995	0.823	0.100
Tests for the Longest-Run-of-Ones in a Block,	0.913	0.371	0.272	0.041	0.972
The Binary Matrix Rank Test	0.539	0.550	0.161	0.693	0.039
The Discrete Fourier Transform (Spectral) Test	0.271	0.363	0.463	0.596	0.481
The Non-overlapping Template Matching Test	0.532	0.156	0.814	0.607	0.686
The Overlapping Template Matching Test	0.841	0.627	0.340	0.886	0.887
Maurer's "Universal Statistical" Test	0.416	0.365	0.652	0.279	0.547
The Linear Complexity Test	0.300	0.165	0.567	0.985	0.915
The Serial Test	0.894	0.462	0.109	0.143	0.208
The Approximate Entropy Test	0.244	0.109	0.260	0.993	0.187
The Cumulative Sums (Cusums) Test	0.872	0.783	0.049	0.097	0.767

Tablo 6. Yürüme esnasında elde edilen sayılar için NIST test sonuçları

	$Ivme_x$	$Ivme_y$	$Ivme_z$	$Konum_x$	$Konum_y$
The Frequency (Monobit) Test	0.236	0.729	0.121	0.437	0.569
Frequency Test within a Block	0.665	0.265	0.906	0.558	0.751
The Runs Test	0.907	0.333	0.014	0.710	0.499
Tests for the Longest-Run-of-Ones in a Block,	0.231	0.943	0.965	0.505	0.582
The Binary Matrix Rank Test	0.741	0.481	0.741	0.291	0.793
The Discrete Fourier Transform (Spectral) Test	0.877	0.046	0.747	0.373	0.859
The Non-overlapping Template Matching Test	0.941	0.152	0.734	0.666	0.746
The Overlapping Template Matching Test	0.496	0.633	0.838	0.488	0.108
Maurer's "Universal Statistical" Test	0.125	0.429	0.580	0.568	0.351
The Linear Complexity Test	0.121	0.631	0.849	0.320	0.238
The Serial Test	0.956	0.612	0.175	0.437	0.569
The Approximate Entropy Test	0.163	0.881	0.235	0.386	0.241
The Cumulative Sums (Cusums) Test	0.472	0.678	0.218	0.580	0.624

Tablo 7. Durma esnasında elde edilen sayılar için NIST test sonuçları

	$Ivme_x$	$Ivme_y$	$Ivme_z$	$Konum_x$	$Konum_y$
The Frequency (Monobit) Test	0.512	0.970	Başarısız	0.028	0.331
Frequency Test within a Block	0.918	0.912	0.116	0.746	0.647
The Runs Test	0.682	0.662	Başarısız	Başarısız	0.019
Tests for the Longest-Run-of-Ones in a	0.342	0.891	Başarısız	0.027	0.180
The Binary Matrix Rank Test	0.176	0.271	0.196	0.693	0.693
The Discrete Fourier Transform (Spectral)	0.160	0.789	0.201	0.757	0.024
The Non-overlapping Template Matching	0.158	0.177	0.801	Başarısız	0.817
The Overlapping Template Matching Test	0.703	0.702	0.838	0.295	0.488
Maurer's "Universal Statistical" Test	0.296	0.659	Başarısız	Başarısız	Başarısız
The Linear Complexity Test	0.969	0.985	Başarısız	0.808	0.985
The Serial Test	0.754	0.908	Başarısız	0.028	0.039
The Approximate Entropy Test	0.951	0.915	Başarısız	Başarısız	Başarısız
The Cumulative Sums (Cusums) Test	0.516	0.973	Başarısız	0.027	0.631

5. Sonuçlar

Bilgisayar biliminin birçok alanında ihtiyaç duyulan rasgele sayıların üretimi için kullanıcı hareketleri tabanlı bir GRSÜ geliştirilmiştir. Mobil telefon kullanan kişilerin koşma yürüme ve durma anlarında ivme ve GPS sistemlerinden elde edilen konumlar yardımıyla rasgele sayılar üretilmiştir. Sayıların kalitesini belirlemek için NIST, Skala İndeks ve Otokorelasyon testleri kullanılmıştır. Elde edilen sonuçlara göre koşma ve yürüme esnasında üretilen sayılar testlerden başarılı olmuştur. Ancak kişinin durma anında çok küçük hareket (milimetre seviyelerindeki değişimler) etmesi GPS'den elde edilen konumunlar da herhangi bir değişiklik göstermediğinden testlerden başarısız olunmuştur. Bunun yanı sıra durma esnasındaki çok küçük konum değişikliği x ve y eksenlerinde ivme sensörü tarafından algılanmış ve üretilen sayılar testlerden başarılı olmuştur. Sonuç olarak önerilen GRSÜ cep telefonu

platformu için uygun, evrensel ve düşük maliyetli olup kişiye özgü rasgele sayı üretiminin mümkün olduğu gösterilmiştir.

Kaynaklar

[1] Tokunaga C,. Blaauw D,. Mudge T. 2008. True random number generator with a metastability-based quality control. IEEE Journal of Solid-state Circuits, 43 (1): 78-85.

[2] Tuncer S.A. 2018. Real-Time Random Number Generation With RO-Based Double PUF. J. Microelectron. Electron. Compon. Mater, 48 (2): 121-128.

[3] Tuncer T., Avaroğlu E., Türk M., Özer A.B. 2014. Implementation of non-periodic sampling true random number generator on FPGA. J. Microelectron. Electron. Compon. Mater, 4 (4): 296-302.

[4] Koyuncu I., Ozcerit A.T., Pehlivan I., Avaroglu E. 2014. Design and implementation of chaos based true random number generator on FPGA. In 22nd Signal Processing and Communications Applications Conference (SIU), pp. 236–239.

[5] Wei Z., Katoh Y. Ogasahara S,. Yoshimoto Y., Kawai K., Ikeda Y., Eriguchi K., Ohmori K., Yoneda S. 2016. True random number generator using current difference based on a fractional stochastic model in 40-nm embedded ReRAM. IEEE Electron. Dev. Meet., 4.8.1-4.8.4.

[6] Walker J. 2002. HotBits: Genuine Random Numbers Generated by Radioactive Decay. http://www.fourmilab.ch/hotbits (Erişim tarihi: 01.02.2019).

[7] Moosavi S.R., Nigussie E., Virtanen S., Isoaho J. 2017. Cryptographic Key Generation Using ECG Signal. 14th IEEE Annual Consumer Communications & Networking Conference (CCNC), pp.1024-1031.

[8] Chen X., Zhang Y., Zhang G., Zhang Y. 2012. Evaluation of ECG Random Number Generator for Wireless Body Sensor Networks Security. 5th International Conference on BioMedical Engineering and Informatics (BMEI 2012), pp. 1308-1311.

[9] Dang N., Tran D., Ma W., Nguyen K. 2017. EEG-Based Random Number Generators. Lecture Notes in Computer Science, 10394: 245-256.

[10] Chen G. 2014. Are electroencephalogram (EEG) signals pseudo-random number generators?. Journal of Computational and Applied Mathematics, 268: 1-4.

[11] Chen I.T. 2013. Random Numbers Generated from Audio and Video Sources. Mathematical Problems in Engineering, Vol.2013, Article ID 285373.

[12] Nikolic S. Veinovic M. 2016. Advancement of True Random Number Generators Based on Sound Cards Through Utilization of a New Post-processing Method. Wireless Pers Commun 91: 603.

[13] Zhou Q., Liao X., Wong K., Hu Y., Xiao D. 2009. True random number generator based on mouse movement and chaotic hash function. Information Sciences, 179 (19): 3442-3450.

[14] Xingyuan W., Xue Q., Lin T. 2012. A novel true random number generator based on mouse movement and a one-dimensional chaotic map,. Mathematical Problems in Engineering, vol. 2012, Article ID 931802.

[15] Hu Y., Liao X.F., Wong K., Zhou Q. 2009. A true random number generator based on mouse movement and chaotic cryptography. Chaos, Solitons & Fractals, 40 (3): 2286-2293.

[16] Marc-Andre´ S., Barbara S., Peter B., Karsten W. 2012. Analysing Humanly Generated Random Number Sequences: A Pattern-Based Approach. Plos ONE, 7 (7): e41531.

[17] Zajac F.E., Neptune R.R., Kautz S.A. 2002. Biomechanics and muscle coordination of human walking. Part I: introduction to concepts, power transfer, dynamics and simulations. Gait Posture 16 (3): 215-32.

[18] Avaroğlu E., Türk M. 2013. Son işlemin Gerçek Rasgele Sayı Üreteçleri Üzerindeki etkisinin İncelenmesi. 6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, Ankara-Türkiye, 291-294, 20-21 Eylül.

[19] Kwok S.-H., Ee Y.-L., Chew G., Zheng K., Khoo K., Tan C.-H. 2011. A comparison of post-processing techniques for biased random number generators. Proc. Inf. Security Theory Practice, 6633: 175-190.

[20] Tuncer S.A, Kaya T. 2018. True Random Number Generation from Bioelectrical and Physical Signals. Computational and mathematical methods in medicine, Vol. 2018, Article ID 3579275.

[21] Benìtez R., Bolos V.J., Ramìrez M.E. 2010. A wavelet-based tool for studying non-periodicity. Comput. Math. Appl., 60: 634.

[22] Yang Y.G., Zhao Q.Q. 2016. Novel pseudo-random number generator based on quantum random walks. Scientific Reports, 6: 20362.
[23] Karakaya B., Çelik V., Gülten A. 2017. Chaotic cellular neural network-based true random number generator. Int. J. Circ. Theor. Appl., 45: 1885-1897.
[24] Chan J.J.M., Thulasiraman P., Thomas G., Thulasiram R. 2016. Ensuring Quality of Random Numbers from TRNG: Design and Evaluation of Post-Processing Using Genetic Algorithm. Journal of Computer and Communications, 4: 73-92.
[25] Chen X.M., Wang L., Li B.X., Wang Y., Li X., Liu Y.P., Yang H.Z. 2016. Modeling Random Telegraph Noise as a Randomness Source and its Application in True Random Number Generation. IEEE Trans. Comput-Aided Des. Integr. Circuits Syst., 35: 1435-1448.
[26] NIST Special Publication 800-22, http://csrc.nist.gov/rng/rng2.html, 2001 (Erişim tarihi: 01.02.2019).