DOI:10.25092/baunfbed. 1018746 *J. BAUN Inst. Sci. Technol., 24(2), 608-622, (2022)*

Damar görüntülerinin şifrelenmesi için kullanılan kaos tabanlı bir rastgele sayı üretecinin kriptanalizi

Kaya DEMİR*

TÜBİTAK, Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi, Gebze, Kocaeli

Geliş Tarihi (Received Date): 03.11.2021
Kabul Tarihi (Accepted Date): 26.04.2022

Öz

Bu çalışmada, damar görüntülerinin mikrobilgisayar ile şifrelenmesinde kullanılan kaos tabanlı rastgele sayı üretecinin(RSÜ) kriptanalizi sunulmuştur. Doğrusal olmayan bir sistem tabanlı bu rastgele sayı üreteci, kızılötesi kamera ile elde edilen el üstü damar görüntülerinin şifrelenme ve depolanmasını sağlayan bir kriptografik sistemde kullanılmıştır. Bu çalışmada, kaos tabanlı rassal sayı üretecinin zayıflıkları kullanılarak kriptografik sisteme atak metodu önerilmiştir. Kaotik sisteme ait bir durum değişkeninin izlenmesi ve rassal sayı üretecinin yapısının bilinmesi ile, hedef rassal sayı üretecinin çıkışı ana köle senkronizasyon yöntemi kullanılarak klon bir rassal sayı üreteci tarafından üretilebilmiştir. Atak metodunun uygulanabilirliği nümerik benzetim sonuçları ile gösterilmiştir. Bu atak yöntemi ile damar görüntülerinin şifrelenmesinde kullanılmış olan anahtar değerleri elde edilmiştir ve şifrelenmiş görüntülerin çözülmesinin mümkün olduğu gösterilmiştir. Bu çalışmada, uygulama olarak özel bir kaotik tabanlı rassal sayı üreteci ve ilgili kriptografik sistem hedef alınmıştır. Ancak, bu çalışmada önerilen kriptanaliz yöntemi, genel olarak hem sürekli zamanlı hem de ayrık zamanlı kaotik rassal sayı üreteçlerinin güvenlik analizinde kullanılabilir. Bu nedenle, bu çalışma kaotik tabanlı rassal sayı üreteçlerinin güvenlik açıklarına ışık tutmaktadır ve deterministik kaosun salt entropi kaynağı olarak değerlendirilmemesi gerektiğini vurgulamaktadır.

Anahtar kelimeler: *Rastgele(rassal) sayı üreteçleri, kriptanaliz, kaotik sistemler, doğrusal olmayan sistemler, senkronizasyon*

*Kaya DEMİR, kaya.demir@tubitak.gov.tr, http://orcid.org/0000-0002-4915-6386

Cryptanalysis of a chaos based random number generator used for encryption of vein images

Abstract

In this study, the cryptanalysis of a chaos based random number generator(RNG) which is used for encryption of vein images is presented. This RNG based on a nonlinear system is deployed in a cryptographic system which is used for encryption and secure storage of dorsal hand images taken by an infrared camera. In this study, an attack method which exploits the security weaknesses of the chaos based RNG is propose. Assuming that one of the chaotic state variables of the RNG is observable and the structure of the target RNG is known, identical output bit stream of the target RNG is generated by a clone RNG used in master–slave synchronization scheme. The performance of the attack method is demonstrated using numerical simulation results. Using the attack method described in this study, it is demonstrated that it is possible to obtain the key values used for encryption of the vain images and use these key values to decrypt the images. In this study, a specific continuous-time chaos-based RNG is subjected to a cryptanalysis study to reveal the security weaknesses. However, the cryptanalysis method explained in this study can be used in the cryptanalysis of any continuous-time or discrete-time chaos-based RNGs. Therefore, this study brings light to the security weaknesses associated with chaos based RNGs and underlines the fact that chaos should not be treated as the sole entropy source in a RNG application as chaos is a deterministic phenomenon.

Keywords: *Random number generators, cryptanalysis, chaotic systems, nonlinear systems, synchronization*

1. Giriş

Elektronik finans, dijital imza ve şifreli mesajlaşma uygulamalarının kullanımının giderek yaygınlaşması sonucu bilgi güvenliği çok daha kritik hale gelmiştir. Bu sebeple, bilginin gizliliği, bütünlüğü ve özgünlüğünün korunmasından sorumlu kriptografik sistemler pek çok alanda yer bulmaktadır. Yaklaşık olarak tüm kriptografik sistemlerde şifreleme algoritmalarında kullanılan anahtar değerlerini üretmek için rastgele sayı üreteçleri (RSÜ) kullanılmaktadır [1]. Kriptografik sisteme konulan bir RSÜ şu kıstasları karşılamak zorundadır: (i) RSÜ'nün üreteceği sonraki bit tahmin edilemez olmalıdır, (ii) RSÜ ile ilgili olarak yapısı veya rastgele bit oluşturma yöntemi gibi tüm ayrıntılar bilinse dahi RSÜ çıkışındaki bit dizini tekrar üretilemez olmalıdır [2], iii) RSÜ çıkışındaki bit dizini istatistiksel rastgelelik testlerinden geçebilmelidir [3,4]. Bu sebeple, bir RSÜ'nün kriptografik sisteme yerleştirilmeden önce güvenlik zayıflıklarını ve çeşitli saldırılara karşı dayanıklılığını test etmek için kriptanaliz çalışması yapılması çok önemlidir.

Temel olarak, RNG'ler üç kısımdan oluşur [4]: (1) Bir direncin termal gürültüsü veya titrek osilatör gibi bir fiziksel entropi kaynağı, (2) Karşılaştırıcı veya D flip-flop gibi bir örnekleyici, (3) RNG çıkışındaki *1/0* dengesi gibi istatiksel kusurları düzeltmek için Von Neumann veya XOR gibi işlemler. RSÜ tasarımında sıklıkla dört temel yöntem kullanılır: (i) Bir gürültü kaynağının amplifikasyonu [5], (ii) Titrek osilatör tabanlı çift osilatör mimarisi [6], (iii) ayrık zamanlı kaotik haritalar [7] ve (iv) sürekli-zamanlı kaotik osilatörler [8,9]. Diğer yöntemlerle karşılaştırıldığında, sürekli zamanlı kaotik

osilatörlerin amplifikasyon veya istatiksel son işleme ihtiyaç duymadan daha yüksek hızda veri ürettiği gösterilmiştir [10]. Bu nedenle, sürekli zamanlı kaotik sistemlere dayalı RSÜ uygulamaları ilgi çekmektedir.

Bir şifreleme sistemi, RSÜ tarafından üretilen anahtar değerler bir saldırgan tarafından tahmin edilemez olduğu sürece güvenlidir [2,11]. Ancak, kaotik sistemler deterministik denklemlerle tanımlanır ve rasgele sayıların üretilmesi için tamamen deterministik kaos kullanılıyorsa, RSÜ'nün çıktısı kaotik osilatörlerin senkronizasyonu metoduyla tahmin edilebilir, ve dolayısıyla bilgi güvenliği tehlikeye düşer [12]. Bu sebeple [13, 14]'te anlatılan kaos tabanlı RSÜ'lerde, bu güvenlik sorununu çözmek için devre üzerindeki elektriksel gürültünün etkisi analiz edilir ve RSÜ'nün esas entropi kaynağının bu fiziksel gürültü olduğu belirtilmiştir. Aksine, [15]'te önerilen RSÜ'de ise rastgeleliğin kaynağı olarak yalnızca deterministik kaos öngörülmüştür. Akgül vd. [15]'te önerilen kaotik sistemi tanımlayan denklem seti Raspberry Pi 3 mikrobilgisayarı üzerinde çözülmüş ve kaotik durum değişkenlerinin değerleri ikilik sayı sistemine çevrilerek RNG bit çıktısı ve dolayısıyla şifrelemede kullanılacak olan anahtar değerleri elde edilmiştir. Sonrasında ise [16]'da açıklanan yöntemle kızıl ötesi kamera ile elde edilen el üstü damar görüntüleri, [15]'te anlatılan RSÜ tarafından üretilen anahtar değerleri ile XOR işlemine sokularak şifrelenmiştir.

Bu makalede, yukarıda bahsedilen [15]'te anlatılan kaos tabanlı bir RSÜ ve ilgili kriptografik sistemin kriptanalizi sunulmuştur. Bu RSÜ, rastgele sayı üretiminde entropi kaynağı olarak sadece deterministik kaosun kullanılmasının yol açtığı güvenlik açıklarını göstermek için hedef alınmıştır. RSÜ çıktısını doğru bir şekilde tahmin edebilmek için ana-köle senkronizasyon yöntemine dayalı bir saldırı sistemi önerilmiştir. Hedef (ana) ve atak (köle) RSÜ sistemlerinin eşzamanlı olarak çalışmasına dayalı kriptanaliz yöntemi matematiksel olarak analiz edilmiştir. Bu makalede, önerilen kriptanaliz metodunun uygulama gösterimi olarak [15]'te açıklanan kaos temelli RSÜ hedef olarak seçilmiştir. Ancak bu çalışmada detaylı biçimde sunulan kriptanaliz yöntemi herhangi bir kaos tabanlı RSÜ'ye de uygulanabilir. Dolayısıyla bu makalede, genel olarak bir kriptografik sistemde yer alan RSÜ'nün bilgi güvenliği için kritik önemi vurgulanmıştır. Bu makalenin organizasyonu şu şekildedir: Bölüm 2'de, hedef RSÜ sistemi ayrıntılı olarak açıklanmıştır. Bölüm 3'te, hedef RSÜ sistemindeki her kaotik durum değişkenine karşılık gelen atak sistemleri aracılığıyla yapılan kriptanaliz çalışması ve matematiksel teorisi açıklanmıştır. Bölüm 4'te, hedef ve atak sistemlerinin senkronize oluşunu gösteren nümerik benzetim sonuçları gösterilmiştir. Bölüm 5'te ise sonuç ve değerlendirmeler verilmiştir.

2. Hedef sistem

Kaotik sistemler deterministik denklemlerle tanımlanır. Ancak, kaotik sistemler doğrusal olmamaları ve pozitif Lyapunov üstelleri sebebiyle başlangıç koşullarına aşırı duyarlı ve farklı periyodik olmayan sinyaller üretirler [17]. Uzun vadede bu kaotik sinyaller tahmin edilemez hale gelir ve rastgele görünen bir davranış sergilerler. Bu sebeple RSÜ uygulamalarında kaotik sinyallerin kullanımı ilgi çekici hale gelmiştir.

Kaotik sistemler, zamanla değişimlerine göre ayrık zamanlı ve sürekli zamanlı olarak ikiye ayrılır. Ayrık zamanlı kaotik sistemlerin tasarımında, anahtarlamalı kapasitörler, çarpma ve işlemsel yükselteçler içeren karmaşık devreler gerekmektedir. Aksine, sürekli

zamanlı kaotik sistemler ise çarpma ve örnekle-ve-tut gibi bloklar gerektirmediğinden daha basit elektronik devreler kullanılarak gerçekleştirilebilir. Bu nedenle, uygulama kolaylığı açısından sürekli zamanlı kaotik sistemler, ayrık zamanlı kaotik sistemlere göre avantajlıdır.

Bu makalede [15]'te anlatılan kaos tabanlı RSÜ kriptanaliz çalışması için hedef olarak seçilmiştir ancak makalede önerilen kriptanalizi yöntemi diğer sürekli zamanlı veya ayrık zamanlı kaos tabanlı RSÜ sistemlerine de uygulanabilir. Bu makaledeki amaç deterministik kaosun entropi kaynağı olarak kulanılmasının yol açabileceği sonuçların bir örnek RSÜ üzerinde nümerik olarak gösterilmesidir. Akgül vd. [15]'te, üç boyutlu denge noktasız yeni bir sürekli zamanlı kaotik sistem önerilmiştir. Bu sistemi tanımlayan denklemler (1)'de verilmiştir. Sistemde x_1, y_1, z_1 olmak üzere üç adet kaotik durum değişkeni ve a, b, c, d dört adet kaos kontrol eden parametre bulunmaktadır.

$$\begin{aligned} \dot{x}_1 &= a y_1 \\ \dot{y}_1 &= -x_1 + b y_1 z_1 \\ \dot{z}_1 &= -x_1 - c x_1 y_1 - d x_1 z_1 \end{aligned} \tag{1}$$

Denklem (1) ile ifade edilen sistem için başlangıç koşulları ve parametrelerin değerleri [15]:

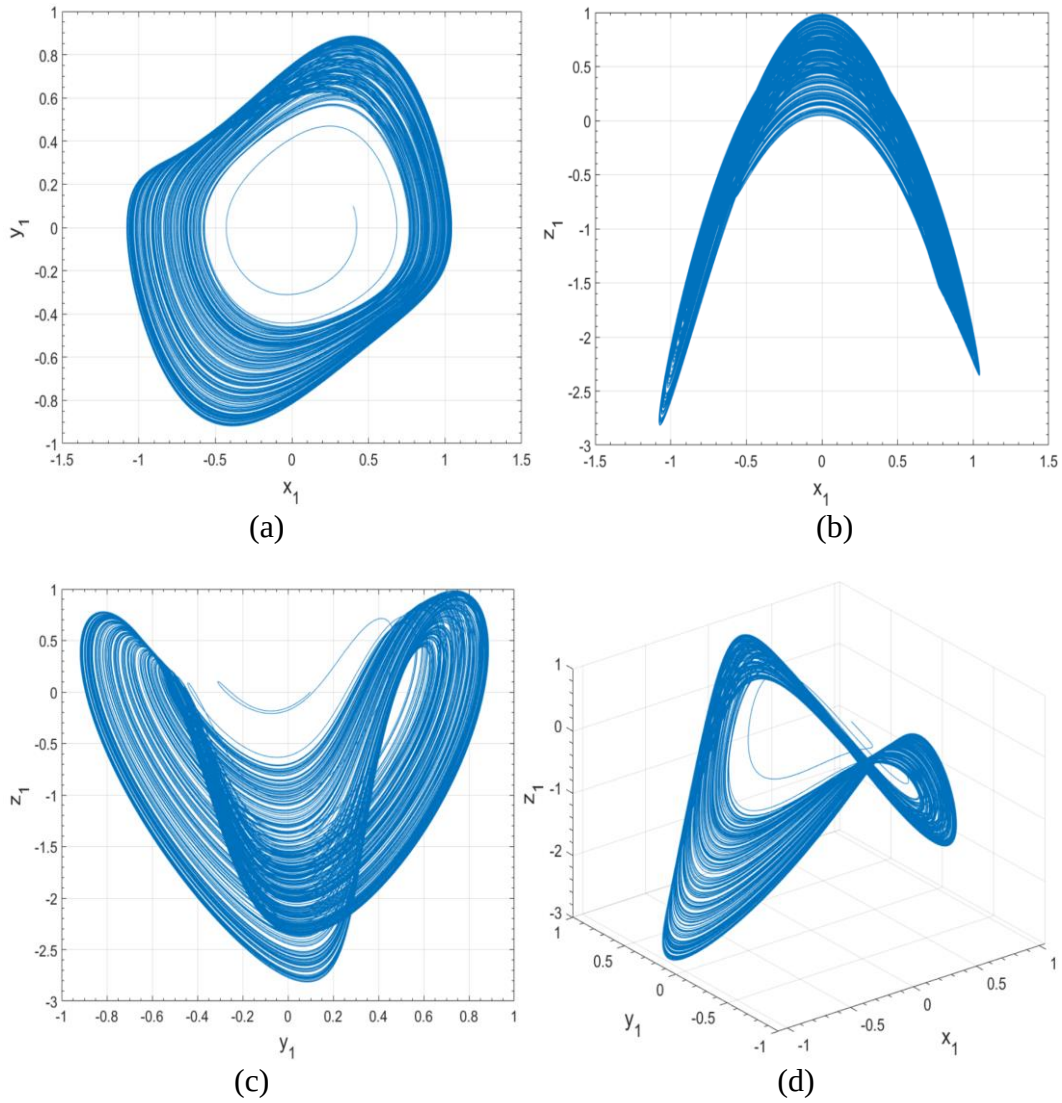
$$\begin{aligned} &\dot{x}_{1,0} = 0, \quad y_{1,0} = 0, \quad z_{1,0} = 0 \\ &a = 1, \quad b = 1, \quad c = 1, \quad d = 1 \end{aligned} \tag{2}$$

(2)'de verilen parametreler (1) denkleminde yerine konularak , [15]'te açıklanan kaotik sistem ifade edilir:

$$\begin{aligned} \dot{x}_1 &= 1.9 y_1 \\ \dot{y}_1 &= -x_1 + 1.1 y_1 z_1 \\ \dot{z}_1 &= -x_1 - 11.5 x_1 y_1 - 0.7 x_1 z_1 \end{aligned} \tag{3}$$

(3)'te verilen sistem, (2)'de verilen başlangıç koşulları için, dördüncü dereceden Runge-Kutta algoritması ve sabit adım boyutu h=0.001 kullanılarak nümerik olarak çözülebilir. Sistemin nümerik çözüm MATLAB kullanılarak elde edilmiş ve x_1, y_1, z_1 kaotik durum değişkenlerinin zamanla değişimini gösteren faz portreleri Şekil 1'de [15]'teki şekillere benzer olarak gösterilmektedir.

Denklem (3) ile tanımlanan sistemin kaosa girip girmediği Lyapunov üstelleri hesaplanarak anlaşılır [17, 18]. Bu sistemin üç adet kaotik durum değişkeni olduğu için, üç adet Lyapunov üsteli bulunmaktadır. Bu üç Lyapunov üstelinden en az birinin pozitif olması durumunda sistem kaostadır [17]. Bu kaotik sistemin d parametresine göre Lyapunov üsteli (λ) analizi [15]'te yapılmış ve $0.55 \le d \le 0.85$ aralığı için sistemin kaosta olduğu gözlenmiştir. Bu sebeple denklem (3)'te görüldüğü üzere aralığın orta değeri olarak $d = 0.7$ seçilmiştir.



Şekil 1. Kaotik sistemin nümerik benzetimi sonucu elde edilen faz portreleri:
a) x_1- y_1, b) x_1- z_1, c) y_1- z_1, d) x_1- y_1- z_1.

Referans [15]'te (3) ile tanımlanan sistemin nümerik çözümü kullanılarak bit üretilmiştir. Raspberry Pi mikrodenetleyici üzerinde dördüncü dereceden Runge-Kutta algoritması sabit bir adım boyutu kullanılarak, (3)'te verilen diferansiyel denklem (2)'de belirtilen başlangıç koşulları için çözülmüştür. Böylece kaotik durum değişkenlerinin (x_1, y_1, z_1) zamana göre değerleri hesaplamıştır ve 32-bitlik kayan noktalı sayılar olarak ifade edilmiştir. Sonrasında bu 32bitlik sayılardan belirlenen bir a miktarında LSB (Least significant bit - en az önemli bit) seçilip birleştirilmiş ve her kaotik durum değişkeni için 1 milyon bitlik seriler elde edilmiştir. Bu 1 Mbitlik seriler NIST 800-22 istatiksel rastgelelik testlerine sokulmuştur. Eğer bu seriler testi geçerse, anahtar değerleri elde edilmiş olur, testi geçemez ise a değeri değiştirilir ve aşamalar 1 Mbitlik seriler testi geçene kadar tekrarlanır. [15]'te bu yöntem detaylı olarak anlatılmış ve her kaotik durum değişkeni x_1, y_1, z_1 için 1 Mbitlik seriler elde edilmiş ve NIST 800-22 testini sağladığı gösterilmiştir. Böylece Akgül vd. [15]'te şifrelemede kullanılacak anahtar değerlerini oluşturmak için bu serilerin kullanılmasını önermiştir. Sonrasında ise, [15]'te kriptografik sistem uygulaması olarak, Yıldız vd. tarafından [16]'da anlatılan kızıl ötesi kamera ile alınan el damarı görüntülerine ait piksel değerleri, [15]'te anlatılan yöntemle oluşturulan

anahtar değerleri ile XOR işleminden geçirilerek şifrelenmiştir. Referans [15]'te el üstü damar görüntülerinin kimlik doğrulama ve tanıma işlemlerinde kullanılabilmesi sebebiyle güvenli olarak saklanmasının önemi belirtilmiştir. RSÜ tarafından üretilen bit dizilerinin istatiksel rastgelelik testlerini geçmesi ve şifrelenmiş görüntülerin piksel değerlerine ait histogram dağılımlarının homojenliği gösterilerek sistemin görüntüleri güvenli kaydetme imkânı sunduğu belirtilmiştir [15].

3. Atak sistemi

Sürekli zamanlı bir kaotik sinyal, gürültüye benzer şekilde öngörülemeyen bir düzensizlik sergiler ve geniş bant frekans spektrumuna sahiptir. Bu sebeple, kaotik sinyaller doğrudan rastgele bit üretimi için elverişli gözükür. Ancak kaotik sistemlerin kısa vadeli tahmin edilebilirliği güvenlikle ilgili endişeler ortaya çıkarmaktadır [18,19]. Kaotik sistemlerin kriptanalizi ve güvenliği ile ilgili tahmin atakları [20], senkronizasyon saldırıları [21] ve parametre tanımlama saldırıları [22] gibi yöntemler bildirilmiştir. Bu makale çalışmasında atak yöntemi, kaotik sistemlerin eşzamanı çalışır hale getirilmesine dayalıdır. Pecora vd. öncü çalışmasında açıkladığı gibi, ana-köle senkronizasyonu ve sürekli zamanlı geri bildirim yöntemi ile hedef ve atak kaotik sistemlerinin birbirine yakınsaması ve eş zamanlı çalışması sağlanabilir [23]. Bu çalışmada, hedef RSÜ'nün kriptanalizi için, her kaotik durum değişkenine karşılık olarak, üç farklı klon (atak) sistem önerilmiştir. Klon ve hedef sistemleri arasındaki kuplaj değerini ayarlanarak ve sürekli zamanlı geri besleme uygulanarak, klon ve hedef sistemlerinin eşzamanlı çalışmalarının sağlanabildiği gösterilmiştir. Bu makalede, saldırı yönteminin nümerik benzetimler yolu ile gösterimi amacıyla [15]'te detayları ile açıklanan hedef rassal sayı üreteci sistemine , hedef sistemin her bir kaotik değişkenine karşılık gelecek şekilde üç farklı klon sistem kullanılarak saldırı düzenlenmiş ve böylece kriptanaliz çalışması gerçekleştirilmiştir. Hedef kaotik sistemin yapısının bilindiği ve bu üç kaotik durum değişkeninden en az birinin belirli bir süre için gözlemlenebilir olduğu varsayılmıştır. Bu varsayım, Kerckhoff vd. tarafından [2]'de ileri sürülen prensip ile de uyumludur. Kerckhoff ilkesine göre bir kripto sistemin güvenilir kabul edilebilmesi için, kripto sistemin çalışma prensibi ve şifreleme algoritması gibi detayları bilinse dahi, anahtar değerinin tahmin edilemez olması gereklidir. Makalede anlatılan yöntem diğer kaos tabanlı RSÜ sistemlerinin de kriptanalizi için kullanılabilir.

3.1. Gözlemlenebilir x_1 için klon sistem

Hedef RSÜ'ye ait üç kaotik durum değişkeninden yalnızca x_1'in gözlemlenebilir olduğunu varsayılırsa hedef RSÜ'nün kriptanalizi için tanımlanan klon RSÜ sistemi tanımlanır. Hedef RSÜ'nün kopyası olan bu RSÜ sisteminin de kaotik durum değişkenleri x_2, y_2, z_2 ve parametreleri a, b, c, d olarak kabul edilir. Hedef RSÜ'ye ait olan gözlemlenebilir x_1 değişkeni kullanılarak atak RSÜ'ye doğrusal geri besleme uygulanırsa, atak RSÜ sistemi şöyle ifade edilebilir:

$$\begin{aligned} \dot{x}_2 &= a y_2 + k(x_1 - x_2) \\ \dot{y}_2 &= -x_2 + b y_2 z_2 \\ \dot{z}_2 &= -x_2 - c x_2 y_2 - d x_2 z_2 \end{aligned} \tag{4}$$

Burada k ana-köle senkronizasyon şeması içerisinde hedef (ana) RSÜ ile atak (köle) RSÜ arasındaki sürekli doğrusal geri besleme için kuplaj değeridir. Bu çalışmada, klon RSÜ sisteminin parametrelerinin hedef RSÜ'nün parametrelerine eşit olduğu varsayılmıştır. Bu durumda hedef ve atak RSÜ'leri arasında farkı gösteren hata sinyalleri $e_x = x_1 - x_2, e_y = y_1 - y_2, e_z = z_1 - z_2$ olarak ifade edilir. Hedef ve klon RSÜ'ler arasında senkronizasyonu sağlamak için k değeri, $t \to \infty$, $e_x(t), e_y(t), e_z(t) \to 0$ sağlayacak şekilde ayarlanmalıdır. Hedef ve atak sistemleri arasındaki kararlı senkronizasyonu sağlayacak k değerini bulmak için, fark sisteminin *CLE* (Conditional Lyapunov Exponent-Koşullu Lyapunov Üsteli) değerleri hesaplanır, ve maksimum *CLE* değerinin negatif olması durumunda senkronizasyon mümkündür. *CLE* değerlerinin bulunması için fark sistemine ait Jacobi matrisi yazılır ve bu matrisin aygen (öz) değerleri QR ayrışım metodu, Wolf algoritması [24] ve dördüncü dereceden Runge-Kutta algoritması kullanılarak hesaplanabilir. Hedef ve atak RSÜ'leri arasındaki farkı gösteren fark sistemi (4)'ü (1)'den çıkararak elde edilir:

$$\begin{aligned} \dot{e}_x &= \dot{x}_1 - \dot{x}_2 = a(y_1 - y_2) - k(x_1 - x_2) \\ \dot{e}_y &= \dot{y}_1 - \dot{y}_2 = -(x_1 - x_2) + b(y_1 z_1 - y_2 z_2) \\ \dot{e}_z &= \dot{z}_1 - \dot{z}_2 = -(x_1 - x_2) - c(x_1 y_1 - x_2 y_2) - d(x_1 z_1 - x_2 z_2) \end{aligned} \tag{5}$$

$\dot{e}_x$ 'in, e_x, e_y, e_z 'ye göre türevleri aşağıdaki gibi yazılabilir:

$$\frac{\partial \dot{e}_x}{\partial e_x} = -k, \quad \frac{\partial \dot{e}_x}{\partial e_y} = a, \quad \frac{\partial \dot{e}_x}{\partial e_z} = 0 \tag{6}$$

$\dot{e}_y$ 'in, e_x, e_y, e_z 'ye göre türevleri şöyle ifade edilebilir:

$$\frac{\partial \dot{e}_y}{\partial e_x} = -1, \quad \frac{\partial \dot{e}_y}{\partial e_y} = bz_1, \quad \frac{\partial \dot{e}_y}{\partial e_z} = by_1 \tag{7}$$

Aguirre vd. tarafından [25]'te anlatıldığı gibi $\frac{\partial \dot{e}_y}{\partial e_y}$ hesaplanırken $z_1 = z_2$ olarak, $\frac{\partial \dot{e}_y}{\partial e_z}$ hesaplanırken de $y_1 = y_2$ olarak varsayılmıştır.

Son olarak, $\dot{e}_z$ 'nin e_x, e_y, e_z 'ye göre türevleri benzer şekilde türetilebilir:

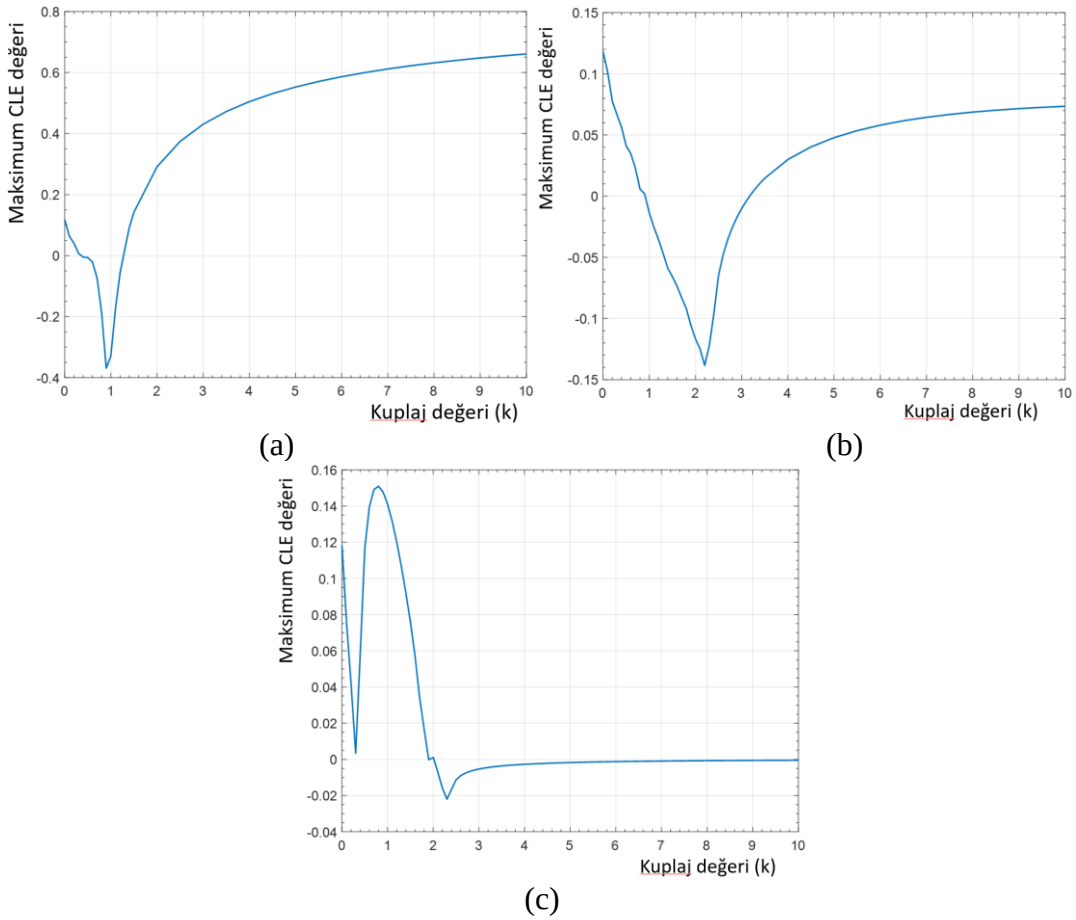
$$\frac{\partial \dot{e}_z}{\partial e_x} = -1 - cy_1 - dz_1, \quad \frac{\partial \dot{e}_z}{\partial e_y} = -cx_1, \quad \frac{\partial \dot{e}_z}{\partial e_z} = -dx_1 \tag{8}$$

Yine [25]'te anlatıldığı yöntemi uygulayarak $\frac{\partial \dot{e}_z}{\partial e_x}$ hesaplanırken $y_1 = y_2$, $z_1 = z_2$ olarak, $\frac{\partial \dot{e}_z}{\partial e_y}$ ve $\frac{\partial \dot{e}_z}{\partial e_z}$ hesaplanırken $x_1 = x_2$ olarak varsayılmıştır.

Böylece denklem (4) ile ifade edilen fark sistemin Jacobi matrisi, şöyle elde edilir:

$$J_X = \begin{bmatrix} \frac{\partial \dot{e}_x}{\partial e_x} & \frac{\partial \dot{e}_x}{\partial e_y} & \frac{\partial \dot{e}_x}{\partial e_z} \\ \frac{\partial \dot{e}_y}{\partial e_x} & \frac{\partial \dot{e}_y}{\partial e_y} & \frac{\partial \dot{e}_y}{\partial e_z} \\ \frac{\partial \dot{e}_z}{\partial e_x} & \frac{\partial \dot{e}_z}{\partial e_y} & \frac{\partial \dot{e}_z}{\partial e_z} \end{bmatrix} = \begin{bmatrix} -k & a & 0 \\ -1 & bz_1 & by_1 \\ -1-cy_1-dz_1 & -cx_1 & -dx_1 \end{bmatrix} \tag{9}$$

CLE değerleri, denklem (5) ile ifade edilen fark sisteminin Lyapunov üstelleridir ve (9) ile ifade edilen Jacobi matrisin öz değerlerine karşılık gelmektedir. Üç farklı kaotik durum değişkeni olduğu için, *CLE* spektrumu da üç bileşenden oluşur ve eğer en büyük *CLE* bileşeni negatifse, o zaman senkronizasyon elde edilir ve kararlıdır. Şekil 2'de, maksimum *CLE* değerinin, hedef ve atak sistemleri arasındaki kuplaj(k) değerine göre değişimi verilmiştir. Şekil 2. a'da görüldüğü üzere $0.5 \le k \le 1.3$ için maksimum *CLE* negatiftir, dolayısıyla hedef ve klon RSÜ sistemlerin senkronizasyonu mümkündür.



Şekil 2. Maksimum *CLE* değerinin farklı gözlemlenebilir kaotik durum değişkenine göre kuplaj değeri ile değişimi a) x1 b) y_1 c) z_1

3.2. Gözlemlenebilir y_1 için klon sistem

Gözlemlenebilir skaler zaman serisinin y_1 olduğunu varsayarsak, hedef RNG'nin kriptanalizi için klon sistemi makalenin 3.1 kısmına benzer şekilde aşağıdaki gibi ifade edilebilir:

$$\begin{aligned}\dot{x}_2 &= ay_2 \\ \dot{y}_2 &= -x_2 + by_2z_2 + k(y_1 - y_2) \\ \dot{z}_2 &= -x_2 - cx_2y_2 - dx_2z_2\end{aligned} \tag{10}$$

Yine makalenin 3.1 kısmında anlatılan yöntem takip edilerek, hedef ve atak sistemi arasındaki fark sisteminin Jacobi matrisi şöyle yazılabilir:

$$J_Y = \begin{bmatrix} \frac{\partial \dot{e}_x}{\partial e_x} & \frac{\partial \dot{e}_x}{\partial e_y} & \frac{\partial \dot{e}_x}{\partial e_z} \\ \frac{\partial \dot{e}_y}{\partial e_x} & \frac{\partial \dot{e}_y}{\partial e_y} & \frac{\partial \dot{e}_y}{\partial e_z} \\ \frac{\partial \dot{e}_z}{\partial e_x} & \frac{\partial \dot{e}_z}{\partial e_y} & \frac{\partial \dot{e}_z}{\partial e_z} \end{bmatrix} = \begin{bmatrix} 0 & a & 0 \\ -1 & bz_1 - k & by_1 \\ -1 - cy_1 - dz_1 & -cx_1 & -dx_1 \end{bmatrix} \tag{11}$$

CLE değerleri (11) ile ifade edilen Jacobi matrisi kullanılarak hesaplanır. Şekil 2.b'de y_1 gözlemlenebilir iken, maksimum *CLE* değerinin hedef ve klon RSÜ sistemleri arasındaki kuplaj değerine göre değişimi verilmiştir. Şekil 2.b'de görüldüğü üzere, $0.9 \le k \le 3.2$ için maksimum *CLE* değeri negatiftir ve dolayısıyla senkronizasyon mümkündür.

3.3. Gözlemlenebilir z_1 için klon sistem

Eğer hedef sisteme dair gözlemlenebilir durum değişkeni z_1 ise, hedef RSÜ'nün kriptanalizi için kullanılan klon sistem makalenin 3.1 kısmına benzer şekilde şöyle yazılabilir:

$$\begin{aligned}\dot{x}_2 &= ay_2 \\ \dot{y}_2 &= -x_2 + by_2z_2 \\ \dot{z}_2 &= -x_2 - cx_2y_2 - dx_2z_2 + k(z_1 - z_2)\end{aligned} \tag{12}$$

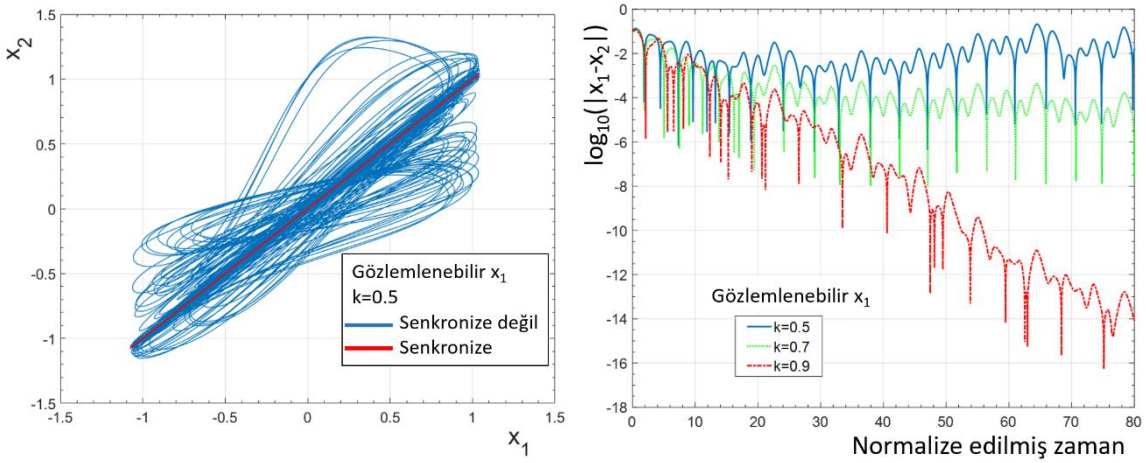
Hedef ve klon RNG sistemleri arasındaki fark sistemine ait Jacobi matrisi makalenin 3.1 bölümünde anlatılan yöntem kullanılarak şu şekilde türetilebilir:

$$J_Z = \begin{bmatrix} \frac{\partial \dot{e}_x}{\partial e_x} & \frac{\partial \dot{e}_x}{\partial e_y} & \frac{\partial \dot{e}_x}{\partial e_z} \\ \frac{\partial \dot{e}_y}{\partial e_x} & \frac{\partial \dot{e}_y}{\partial e_y} & \frac{\partial \dot{e}_y}{\partial e_z} \\ \frac{\partial \dot{e}_z}{\partial e_x} & \frac{\partial \dot{e}_z}{\partial e_y} & \frac{\partial \dot{e}_z}{\partial e_z} \end{bmatrix} = \begin{bmatrix} 0 & a & 0 \\ -1 & bz_1 & by_1 \\ -1 - cy_1 - dz_1 & -cx_1 & -dx_1 - k \end{bmatrix} \tag{13}$$

Şekil 2.c'de, en büyük *CLE* değerinin *k* kuplaj değerine göre değişimi verilmiştir. Şekil 2.c'de görüldüğü üzere $2 \le k \le 10$ aralığında, maksimum *CLE* değeri negatif hale gelmektedir, dolayısıyla hedef ve klon istemlerin senkronizasyonu mümkündür. Böylece, Şekil 2. a,2. b ve 2. c'ye göre kuplaj değeri gözlemlenebilir kaotik durum değişkenine bağlı olarak ayarlanırsa, hedef ve klon RSÜ'ler arası senkronizasyon elde edilebilir. Bu sayede, hedef RSÜ'nün bir sonraki bitini tahmin etmek ve aynı anda hedef RSÜ'nün bit akışını üretmek mümkün olur.

4. Nümerik analiz

Bu bölümde, bir önceki bölümde önerilen atak yöntemi kullanılarak sırasıyla (5), (10) ve (12) denklemleri ile ifade edilen klon istemler nümerik olarak modellenmiştir. Hedef ve klon RSÜ sistemleri arasındaki k kuplaj değeri, sırasıyla Şekil 2. a, Şekil 2. b ve Şekil 2. c'de gösterilen maksimum *CLE*-k grafiklerine göre ayarlanmıştır. Şekil 3. a'da gözlemlenebilir kaotik durum değişkeni x_1 ve kuplaj değeri $k = 0.5$ iken, hedef ve klon sistemlerin farklı başlangıç koşullarından başlayıp senkron hale gelişi gösterilmiştir. Şekil 2. a'ya göre $k = 0.5$ iken maksimum *CLE* değeri negatiftir, dolayısıyla hedef ve klon sistemler Şekil 3. a'da başlangıçta maviyle gösterildiği şekilde senkronize değil iken, kırmızı ile gösterildiği gibi belirli bir zaman içerisinde senkronize hale gelmişlerdir.

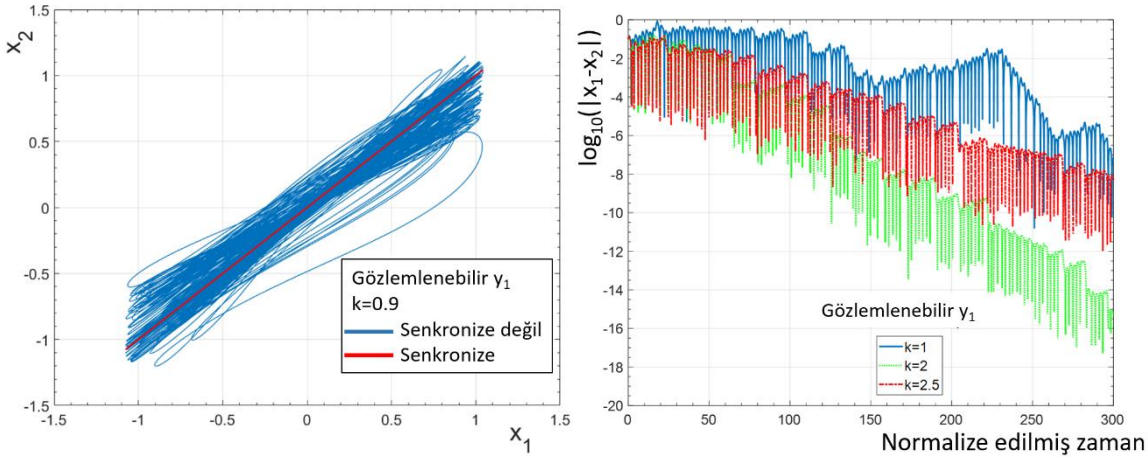


(a) (b)

Şekil 3. a) Kuplaj değeri $k = 0.5$ ve x_1 gözlemlenebilir iken, x_1 ve x_2 sinyallerinin farklı başlangıç değerlerinden başlayıp senkronize hale gelişi, b) Gözlemlenebilir x_1 ve farklı kuplaj değerleri için $\log_{10}(|x_1 - x_2|)$ 'in normalize edilmiş zamana göre değişimi.

Şekil 3. b'de x_1 gözlemlenebilirken farklı k kuplaj değerleri için, hedef ve klon RSÜ arasındaki hata sinyalinin zamanla değişimi karşılaştırma amacıyla verilmiştir. Şekil 3. b'de görüldüğü üzere, $k = 0.9$ iken, x_1 ve x_2 arasındaki senkronizasyona $k = 0.5$ ve $k = 0.7$ 'ye göre daha çabuk ulaşılmıştır. Bunun sebebi ise Şekil 2. a'da gösterildiği gibi negatif olan maksimum *CLE* değerinin mutlak değerinin, $k = 0.9$ için daha yüksek olmasıdır. Bu sebeple hedef ve klon sistemlerin yakınsaması için gereken zaman $k = 0.9$ iken daha kısadır.

Şekil 4. a'da gözlemlenebilir kaotik durum değişkeni y_1 ve hedef ve klon sistemi arasındaki kuplaj değeri $k = 0.9$ olarak ayarlanmıştır. Hedef ve saldırı sistemlerine ait kaotik durum değişkeni x_1 ve x_2 sinyallerinin farklı başlangıç koşullarından başlayıp senkronize değil durumundan senkronize durumuna geçişi Şekil 4. a'da gösterilmiştir.



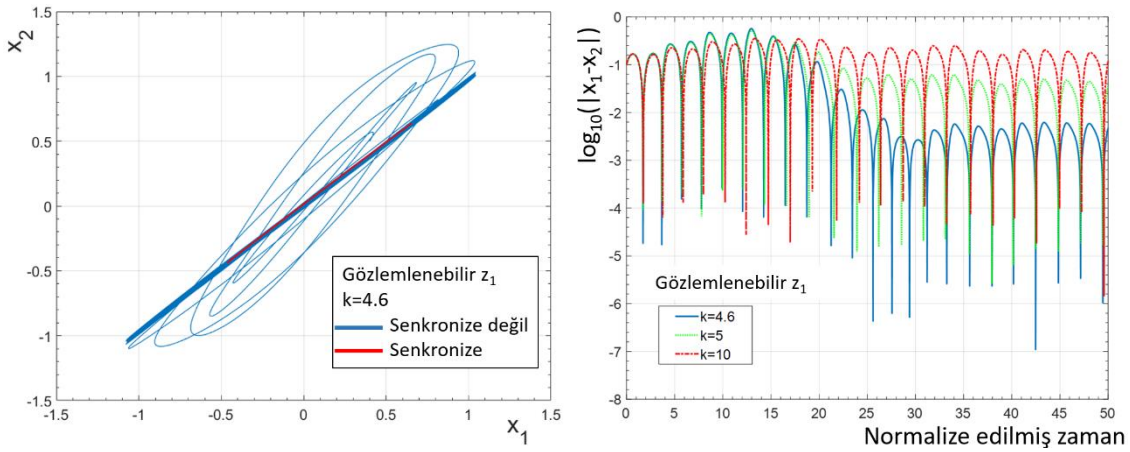
(a) (b)

Şekil 4. a) Kuplaj değeri $k = 0.9$ ve y_1 gözlemlenebilir iken, x_1 ve x_2 sinyallerinin farklı başlangıç değerlerinden başlayıp senkronize hale gelişi, b) Gözlemlenebilir y_1 ve farklı kuplaj değerleri için $\log_{10}(|x_1 - x_2|)$ 'in normalize edilmiş zamana göre değişimi.

Şekil 4. b'de ise gözlemlenebilir kaotik durum değişkeni y_1 iken hedef ve atak RSÜ'leri arasındaki kuplaj değerinin, $\log_{10}(|x_1 - x_2|)$ fark sinyalinin zamana göre değişimine etkisi gösterilmiştir. Şekil 4. b'de görüldüğü gibi kuplaj değeri $k = 2$ iken, hedef ve atak sistemleri arasındaki senkronizasyon $k = 1$ ve $k = 2.5$ durumlarına göre daha hızlı gerçekleşmiştir. Bunu sebebi ise, Şekil 2. b'de görüldüğü gibi $k = 2$ için maksimum *CLE* değerinin mutlak değeri diğer iki duruma kıyasla daha büyüktür.

Son olarak Şekil 5. a'da hedef sisteme ait gözlemlenebilir kaotik durum değişkeni z_1 ve $k = 4.6$ iken, farklı başlangıç noktalarından başlayan x_1 ve x_2 sinyallerinin kırmızı ile gösterildiği şekilde eşzamanlı hale gelişi ve $x_1 = x_2$ doğrusuna yakınsaması gösterilmiştir.

Şekil 5. b'de ise üç farklı kuplaj değeri ($k = 4.6, 5, 10$) için, hedef ve atak sistemleri arasındaki farkın zamanla değişimi gösterilmiştir. Şekil 5. b'de görüldüğü gibi x_1 ve x_2 arasındaki farkın azalma hızının $k = 10$ için en yavaş, $k = 4.6$ için ise en hızlı olduğu görülmüştür. Bu durumda Şekil 2. c'de görüldüğü gibi, maksimum *CLE* değerinin mutlak değerinin, $k = 4.6$ için en yüksek, $k = 10$ için ise en düşük olması ile açıklanır.



(a) (b)

Şekil 5. a) Kuplaj değeri $k = 4.6$ ve z_1 gözlemlenebilir iken, x_1 ve x_2 sinyallerinin farklı başlangıç değerlerinden başlayıp senkronize hale gelişi, b) Gözlemlenebilir z_1 ve farklı kuplaj değerleri için $\log_{10}(|x_1 - x_2|)$ 'in normalize edilmiş zamana göre değişimi.

Nümerik analiz sonucunda, farklı başlangıç koşullarından başlamasına rağmen, hedef RSÜ'ye ait bir kaotik durum değişkeninin sonlu bir süre boyunca gözlemlenmesi ve k kuplaj değerinin ayarlanması ile hedef ve klon RSÜ arasında senkronizasyonun mümkün olduğu gösterilmiştir. Kaotik sistemlerin başlangıç değerlerine aşırı hassaslığına rağmen, hedef ve atak sistemlerinin birbirine yakınsaması sağlanabilmektedir. Hedef ve atak sistemleri arasındaki kuplaj değeri, en büyük *CLE* değeri negatif olacak şekilde ayarlanabilirse, kararlı senkronizasyon elde etmek mümkündür. Böylece hedef RSÜ'nün bir sonraki biti kesin olarak tahmin edilebilir ve aynı bit akışı yeniden üretilebilir. Ancak, Akgül vd. tarafından [15]'te detaylı şekilde anlatılan hedef RSÜ'nün ürettiği bit dizileri NIST 800-22 istatiksel rastgelelik testlerini geçmesine rağmen, hedef RSÜ güvenli değildir. Çünkü bu makalenin giriş bölümünde bahsedilen güvenli bir RSÜ'nün sağlaması gereken üç kriterden ilk ikisini sağlayamamaktadır, sadece üçüncü kriteri sağlamaktadır. İlk iki kritere göre, RSÜ'nün yapısı, bit üretim şekli gibi RSÜ ile ilgili tüm detayların bilinmesi halinde dahi, kriptografik olarak güvenli bir RSÜ'nün bir sonraki bitini tahmin etmek ve ürettiği bit dizininin yeniden oluşturulabilmesi imkânsız olmalıdır [2].

RSÜ çıkışı tahmin edilebilir hale gelince, herhangi bir şifreleme sisteminin güvenliği, şifreleme algoritması ne kadar karmaşık olursa olsun tehlikeye girer. Referansta [15]'te uygulama gösterimi olarak, kaos tabanlı RSÜ'nün çıktıları anahtar değeri olarak kullanarak el damar görüntüleri şifrelenmiştir. Şifreleme işlemi için öncelikle Yıldız vs. tarafından [16]'da anlatılan sistem kullanılarak kızıl ötesi kamera ile elde edilen görüntülerin her pikseli 8 bitlik ikili seviyeye dönüştürülmüştür [15]. Sonrasında kaotik RSÜ'nün çıkışında üretilen bit dizini ile XOR'lanmıştır. Sonrasında [15]'te detaylı olarak anlatıldığı ve şeması verildiği şekilde, her piksel için elde edilen sekiz bitlik sayı, tekrar onlu sisteme dönüştürülerek şifrelenmiş görüntünün piksel değerleri elde edilmiş olur. Referans [15]'te bu işlemde kaotik sistem tabanlı RSÜ'nün rastgeleliği sağladığı ve güvenli olduğu ileri sürülmüştür. Ancak, XOR işleminde kullanılan anahtar değeri bu makalede gösterildiği gibi klon RSÜ'nün hedef RSÜ'ye senkronizasyonu sonucu ele

geçirilebilir. Böylece şifrelenmiş görüntünün her pikseli aynı anahtar değerleriyle XOR'lanarak çözülebilir ve görüntü ele geçirilebilir.

Gerçekleştirilen şifreleme sonrası [15]'te şifreleme yönteminin güvenlik analizleri sunulmuş ve şifrelenen görüntülerin piksel değerlerinin istatiksel dağılımları incelenerek kriptografik sistemin güvenli olduğu sonucuna varılmıştır. Ancak, Kerckhoff prensibine göre herhangi bir şifreleme yönteminin gücü, algoritmada kullanılan anahtar değerlerinin tahmin edilme zorluğuna bağlıdır [2]. Çünkü şifreleme algoritmasında kullanılan adımlar deterministik adımlardır ve [15]'te de detaylarıyla sunulmuştur. Dolayısıyla, bir şifreleme sisteminin gücü, şifreleme algoritmasının karmaşıklığına değil, RSÜ tarafından üretilen anahtar değerlerinin gizliliğine bağlıdır [2]. Bu çalışmada, [15]'te tasarımı anlatılan kaos tabanlı RSÜ'nün çıktılarının NIST 800-22 istatistiksel rastgelelik testlerinden geçmesine rağmen, RSÜ çıkışı tahmin edilebilir olması sebebiyle güvenli olmadığı gösterilmiştir. Bu makalede anlatılan kriptanalizi yöntemi [15]'te anlatılan RSÜ üzerinde gösterilmiştir, ancak bu kriptanalizi metodu diğer sürekli zamanlı veya ayrık zamanlı kaos tabanlı RSÜ'lere de uygulanabilir. Bu makalede amaçlanan, RSÜ sistemlerinde tek rastgelelik kaynağı olarak deterministik kaos kullanılırsa RSÜ çıkışının tahmin edilebileceğinin gösterilmesidir. Böylece, RSÜ çıkışındaki bit dizininin NIST 800-22 istatiksel rastgelelik testlerini geçmesinin, RSÜ çıkışının rastgele olmasını garantilemediğini ve güvenlik açıklarının oluşabileceği vurgulanmıştır.

5. Sonuçlar ve tartışma

Bu çalışmada, el üstü damar görüntülerinin şifrelenmesinde kullanılan bir kriptografik sistemde yer alan sürekli zamanlı kaotik bir RSÜ'nün kriptanalizi sunulmuştur. Kaos fiziksel bir gürültüye benzemesine rağmen, deterministik bir olgudur. Bu sebeple, bir RSÜ sistemindeki tek entropi kaynağı olarak kabul edilmemelidir. Kaotik bir RSÜ'de gerçek rastgelelik kaynağı, kaotik sistemin başlangıç koşullarındaki fiziksel gürültüye bağlı ortaya çıkan ve deterministik olmayan dalgalanmalardır. Deterministik kaotik sistem ise, başlangıç koşullarındaki bu dalgalanmanın çıkış üzerindeki etkisini yükseltme görevi görmektedir. Bu çalışmada, el üstü damar görüntülerinin şifrelenmesinde kullanılan kaos tabanlı spesifik bir RSÜ'nün güvenlik analizi yapılmıştır. Ancak bu makalede açıklanan yöntem, herhangi bir sürekli zamanlı veya ayrık zamanlı kaos tabanlı RSÜ'nün kriptanalizi için de kullanılabilir. Akgül vd. tarafından [15]'de anlatılan hedef RSÜ, hatalı bir şekilde deterministik kaosu tek entropi kaynağı olarak kullandığı için, bu kriptanaliz çalışmasına tabi tutulmuştur. Kaos tabanlı bu RSÜ'nün güvenlik açıklarını ortaya çıkarmak için bir kaotik sistemlerin senkronizasyonuna dayalı bir atak yöntemi önerilmiştir. Kaotik sistemlerin eş zamanlı çalışır hale getirilişi matematiksel olarak incelenmiştir. Ana-köle senkronizasyon şeması kullanılarak, hedef ve atak RSÜ'leri arasında kararlı senkronizasyon nümerik benzetimler yoluyla gösterilmiştir. Hedef RSÜ'nün bir kaotik durum değişkenini sonlu zamanlı gözlemleyerek ve hedef ve klon RSÜ'lerin arasındaki kuplaj değerini ayarlayarak, hedef ve klon RSÜ'lerin çıktısı senkron hale getirilmiştir. Böylece, hedef RSÜ çıktısı ile üretilen ve el üstü damar görüntülerinin şifrelenmesinde kullanılan anahtar değerlerinin elde edilebileceği ve şifrelenmiş görüntülerin çözülebileceği gösterilmiştir. Bu makalede, herhangi bir şifreleme sisteminin gücünün, şifreleme algoritmasının karmaşıklığına değil, RSÜ tarafından üretilen anahtar değerlerinin tahmin edilemezliğine bağlı olduğuna dikkat çekilmiştir. Böylece, bu çalışma ile kaos tabanlı RSÜ'lerin güvenlik açıklarının belirlenmesine yönelik kriptanaliz çalışmalarının önemi vurgulanmıştır.

Kaynaklar

[1] Shannon, C. E., Communication theory of secrecy systems, **The Bell System Technical Journall**, 28, 4, 656-715, (1949).

[2] Kerckhoffs, A., La cryptographie mlitaire, **Journal des sciences militaires**, 5-83, (1883).

[3] Schneier, B., **Foundations-applied cryptography**, 2, John Wiley & Sons Inc., (2015).

[4] Menezes, A., van Oorschot, P., Vanstone, S.A., **Handbook of applied cryptography**, 1, CRC Press, (1996).

[5] Petrie, C. S., Connely, J. A., A noise-based ic random number generator for applications in cryptography, **IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications**, 47,5,615-621, (2000).

[6] Bucci, M., Germani, L., Luzzi, R., et al, A high-speed ic random-number source for smartcard microcontrollers, **IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications,** 50,11,1373-1380, (2003).

[7] Callegari, S., Rovatti, R., Setti, G., Embeddable ADC-based true random number generator for cryptographic applications exploiting nonlinear signal processing and chaos, **IEEE Transactions on Signal Processing**,53,2,793-805, (2005).

[8] Ergün, S., Özoğuz, S., Truly random number generators based on nonautonomous continuous time chaos**, International Journal of Circuit Theory and Applications** ,38,1,1-24, (2010).

[9] Özoğuz, S., Elwakil, A.S., Ergün, S., Cross-coupled chaotic oscillators and application to random bit generation, **IEE Proceedings-Circuits, Devices and Systems**,153, 5, 506-510, (2006).

[10] Ergün, S., A chaos-modulated dual oscillator-based truly random number generator, **2007 IEEE International Symposium on Circuits and Systems(ISCAS)**, 2482-2485, (2007).

[11] Al-Vahed, A., Sahhavi, H., An overview of modern cryptography, **World Applied Programming**,1,1, 55-61, (2011).

[12] Ergün, S., On the security of chaos based true random number generators, **IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences**, 99,1,363-369,2016.

[13] Ergün, S., Güler, Ü., Asada, K., IC truly random number generators based on regular & chaotic sampling of chaotic waveforms, **IEICE Nonlinear Theory and Its Applications**, 2, 2,246-261, (2011).

[14] Ergün, S., Güler, Ü., Asada, K., A high speed ic truly random number generator based on chaotic sampling of regular waveform**, IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences**, 94,1,180-190, (2011).

[15] Akgül, S., Yıldız, M.Z., Boyraz, Ö. F., Güleryüz, E., Kaçar, S., Gürevin, B., Microcomputer-based encryption of vein images with a nonlinear novel system, **Journal of the Faculty of Engineering and Architecture of Gazi University**, 35,3,1369-1385, (2020).

[16] Yıldız, M. Z., Boyraz, Ö. F.,Development of a low-cost microcomputer based vein imaging system, **Infrared Physics & Technology**, 98,27-35, (2019).

[17] Sato, S., Sano, M., Swada, Y., Practical methods of measuring the generalized dimension and the largest lyapunov exponent in high dimensional chaotic systems, **Progress of Theoretical Physics**, 77,1, (1987).

[18] Ergün, S., Revealing the unknown parameters of a microcomputer-based random number generator, **2019 IEEE Asia Pacific Conference on Circuits and Systems (APCCAS)**, Bangkok, 237-240, (2019).

[19] Demir, K., Ergün, S., Cryptanalysis of a random number generator based on continuous-time chaos, **IET Circuits, Devices & Systems**, 14,5, 569-575, (2020).

[20] Zhou, C., Lai, C. H., **Extracting messages masked by chaotic signals of time-delay systems**, Physical Review E, 60,1,320, (1999).

[21] Alvarez, G., Montoya, F., Romera, M.,et al, Breaking two secure communication systems based on chaotic masking, **IEEE Transactions on Circuits and Systems II: Express Briefs**, 51,10,505-506, (2004).

[22] Alvarez, G., Li, S., Montoya, F., et al, Breaking projective chaos synchronization secure communication using filtering and generalized synchronization, **Chaos, Solitons & Fractals**, 24, 3, 775-783, (2005).

[23] Carrol, T.L., Pecora, L. M., Synchronizing chaotic circuits, **IEEE Transactions on Circuits and Systems**, 38,4,453-456, (1991).

[24] Wolf, A., Swift, J.B., Swinney, H.L., et.al., Determining lyapunov exponents from a time series, **Physica D: Nonlinear Phenomena**,16, 3, 285-317, (1985).

[25] Aguirre, L.A., Letellier, C., Controllability and synchronizability: are they related?, **Chaos, Solitons & Fractals**, 83, 242-251, (2016).