Fırat Üniv. Müh. Bil. Dergisi
30(2), 13-17, 2018

Science and Eng. J of Fırat Univ.
30(2), 13-17, 2018

Kaotik Fonksiyonlar Ile EKG Sinyalleri Kullanarak Kişisel Bilgi Şifrelemenin Matematiksel Kriptoanalizi

M.Tuncay GENÇOĞLU
Fırat Üniversitesi, Teknik Bilimler MYO, 23119 Elazığ, Türkiye
mt.gencoglu@firat.edu.tr

(Geliş/Received: 19/06/2017; Kabul/Accepted: 12.06.2018)

Özet

Kaotik sistem ve kriptografi bazı ortak özelliklere sahiptir. Kaotik sistem ve kripto sistem arasındaki yakın ilişkiden dolayı,araştırmacılar kaotik sistem ile kripto sistemi birleştirmeye çalışırlar. Bu çalışmada verilerin EKG sinyalleri ve kaotik fonksiyonlar ile veri şifrelemeyi amaçlayan bir şifreleme algoritmasının güvenlik analizi yapılmıştır. Önerilen algoritmada metin şifrelemede Lojistik harita ve resim şifreleme de ise Henon haritası kullanılarak metin ve resim verileri aynı anda şifrelenebilmektedir. Ayrıca şifreleme algoritmasının kişiselleştirilmesi amacıyla algoritmada kullanılan kaotik fonksiyonların başlangıç şartlarını ve kontrol parametrelerini belirlemek için EKG sinyalleri kullanılmıştır. Yapılan bu kriptanaliz çalışmasında bahsedilen işlemin yetersizliği ve önerilen yöntemin zayıf yönleri belirlenmiştir. Şifreleme algoritmasının anahtar alanının gerekli güvenlik seviyesini sağlamak için yeterli kapasiteye sahip olmadığı ve gizli anahtarın seçilen düz metin saldırısıyla yalnızca bir tane düz metin-şifreli metin çifti ile elde edilebileceği ortaya konulmuştur.

Anahtar Kelimeler: Kaos, Kriptografi, Kriptoanaliz.

Mathematical Cryptanalysis of Personalized Information Encryption Using ECG Signals with Chaotic Functions

Abstract

Chaotic system and cryptography have some common characteristics. Due to the close relationship between the chaotic system and the cryptosystem, researchers are trying to combine the chaotic system with the cryptosystem. In this study, Security analysis of an encryption algorithm aimed data encryption with ECG signals and chaotic functions has been performed. In the proposed algorithm for cryptoanalysed study; the logistic map in text encryption, Henon map in picture encryption using the text and image data can be encrypted at the same time. In addition, ECG signals have been used to determine the initial conditions and control parameters of the chaotic functions used in the algorithm with the aim of personalizing the encryption algorithm. In this cryptanalysis study, the inadequacy of the mentioned process and the weaknesses of the proposed method have been determined. It has been shown that the encryption field of the encryption algorithm does not have sufficient capacity to provide the required security level and that the secret key can be obtained with only one plaintext-encrypted text pair with the selected plaintext attack.

Keywords: Laplace Transform, Cryptography, Cryptanalysis.

1. Giriş

Kriptoloji biliminin asıl amacı,internet gibi kamusal iletişim kanallarında bulunan bir saldırganın tehditlerine karşı,gönderen ve alıcı arasındaki iletişimi güvenli olarak sağlamaktır. Kaotik sistemin özelliklerini kullanarak kripto sistem tasarımı son yirmi yılda bir çok araştırmacının ilgisini çekmiştir[1,2,5,15,20]. Fakat araştırmacıların çoğu yapılan tasarım çalışmalarının birkaçında tesadüfiliğin kaynağı olarak kaotik sistemlerle sunulan zengin dinamikler üzerine yoğunlaştıkları için bir kripto sistem tasarlanırken gözönünde bulundurulması gereken temel kriterlere dikkat etmemişlerdir [1-3,6,10,16,19-25,27]. Nihayetinde,kaos temelli kriptoloji, bir uygulama alanı olarak, temel kriptoloji literatürüne uzak kalır.

Bu çalışmada,EKG sinyalleri ve kaotik fonksiyonlarla veri şifrelemeyi amaçlayan bir şifreleme algoritmasının güvenlik analizi yapılmıştır[9]. Önerilen şifreleme algoritmasında metin ve resim verileri aynı anda

şifrelenebilmektedir. Metin şifreleme için Lojistik map ve resim şifreleme için Henon map kullanılmıştır. EKG sinyalleri,şifreleme algoritmasında kullanılan kaotik fonksiyonların başlangıç şartlarını ve kontrol parametrelerini belirlemek için kullanılmıştır. Bu işlemle şifreleme algoritmasının kişiselleştirilmesi amaçlanmıştır. Önerilen algoritmanın güvenlik analizi sadece histogram analizi ve deneysel sonuçlarla yapılmıştır.

Önceki araştırmalarda da olduğu gibi yazarlar[9], kaotik sistemlerin en belirgin özelliği olan başlangıç şartları ve kontrol parametrelerine aşırı bağımlılık gösteren tahmin edilemeyen tesadüfi yörüngelerle verinin şifrelemesini amaçlamışlardır. Önerilen algoritmayı daha karmaşık, sağlam ve güvenilir hale getirmek için şifreleme sistemine EKG sinyalleri ile kaotik fonksiyonların başlangıç şartlarının belirlendiği bir aşama eklenmiştir. Ancak,yapılan kriptoanaliz çalışmasında; şifreleme algoritmasının anahtar alanının gerekli güvenlik seviyesini sağlamak için yeterli kapasiteye sahip olmadığı gösterilmiştir. Ayrıca,algoritmanın gizli parametresi olan anahtarın seçilen düz metin saldırısıyla yalnızca bir düz metin-şifreli metin çifti ile elde edilebileceği gösterilmiştir.

Çalışmanın anahatları şu şekildedir;
Bir sonraki bölümde önerilen şifreleme algoritması detaylarıyla açıklanmıştır.3. Bölümde, kaos tabanlı şifreleme sisteminin güvenlik analizi yapılırken gözönüne alınması gereken şartlar kısaca açıklanmış ve önerilen şifreleme algoritması basit bir matematiksel modelle ifade edilmiştir. Ardından bu matematik model üzerinde uygulaması gösterilmiştir. Son bölümde, elde edilen sonuçlar tartışılmış ve bazı genel öneriler sunulmuştur.

2.Şifreleme Algoritmasının Açıklaması

Bu bölümde şifreleme algoritması[9] detayları ile açıklanmaktadır. Şifreleme algoritması iki temel kısımdan oluşur. 1. Kısımda, EKG sinyallerini toplamak için kullanıcılardan bir cihaz geliştirilmiş, bu cihaz yardımıyla kullanıcının kişisel özellikleri EKG sinyallerinden tahmin edilmiştir. Şifreleme algoritmasının 2. Kısmında,EKG sinyallerinden elde edilen bireysel özellikler kaotik fonksiyonların öngörülemeyen tesadüfi yörüngelerini üretmek için başlangıç şartları ve kontrol parametreleri olarak kullanılmıştır. Şifreleme işlemi üretilen kaotik öngörülemeyen tesadüfi yörüngeler yardımıyla veri karıştırılarak gerçekleştirilmiştir. Şifreleme adımları ise şu şekildedir;

1. Adım: Kullanıcının bireysel özelliklerinden oluşan ve Lojistik ve Henon haritaları için başlangıç anahtarı olarak kullanılan EKG sinyalleri, EKG çıkartma programı ile toplanır. Daha sonra kaotik fonksiyonlar kullanılarak bir öngörülemeyen tesadüfi yörünge üretilir.
2. Adım: Kaotik fonksiyonların kontrol parametreleri kullanılarak elde dilen kaotik yörünge çıktısındaki verilerle bir gizli şifreleme anahtar serisi üretim sistemi kurulur.
3. Adım: Şifrelenecek döküman hem metin hemde resim içeriyorsa,bunlar birbirinden ayrılır.
4. Adım: Henon map görüntü verilerinin şifrelemesi için kullanılır. Şifrelenecek verilerin koordinatlarının piksel değerleri yer değiştirilir. Yani iki boyutlu Henon haritasının yörüngeleri kullanılarak şifrelenecek verilerin yatay ve dikey karıştırılması yapılır.
5. Adım: Lojistik map metin verisinin şifrelemesi için kullanılır. Şifreli metin formatı metin dosyasına dönüştürülür. Satır sonlandırıcılarıyla dizi elde edilir ve dosyanın sonuna kadar karakterler ASCII kodlarına dönüştürülür. Şifreli metin, kaotik Lojistik harita kullanılarak her karekter ASCII kodları ile yer değiştirilir. Yani metin içindeki her karektere karşılık gelen ASCII kodlarının Lojistik harita yardımıyla karıştırılması ile şifreleme işlemi gerçekleşir.
6. Adım: Şifreli metin ve resim oluşturulur. Yani şifreli metin ve resim verileri birleştirilerek şifreleme işlemi tamamlanır.

3.Önerilen Algoritmanın Matematiksel Kriptoanalizi

Kaotik sistemlerin, kriptografik yapıların tasarımında temel unsur olarak kullanılması durumunda, yalnızca istatistiksel test yöntemlerini kullanarak şifreleme sisteminin güvenirliliğini değerlendirmek yetersiz bir analiz olacaktır.

Chen ve arkadaşları tarafından yapılan bu çalışmada şifreleme mimarisi

C=E (K, P) (1)

gibi basit bir matematiksel modelle ifade edilebilir. Bu modelde;

E: Şifreleme Algoritması

K: Kaotik öngörülemeyen tesadüfi yörüngeyle iletilen gizli anahtar

P: Orjinal veri

C: Şifrelenmiş veri

olarak tanımlanmıştır. Analizi yapılan algoritmada; kontrol parametreleri,başlangıç şartları ve kaotik fonksiyonların iterasyon sayısı gizli anahtar olarak kullanılmıştır. Ancak (1) denkleminde görüldüğü gibi aslında,EKG sinyalleri ile veya kaotik fonksiyonlarla şifreleme süreci arasında herhangi bir ilişki bulunmamaktadır. Şöyleki; K parametresine sahip olan herkes bir anahtarı şifreleyebilir yada herhangi bir veriyi deşifreleyebilir. Yani K parametresi şifreleme algoritmasının gizli anahtarı ile eşdeğerdir. [20] de Solak şöyle demektedir: "Kaos tabanlı şifrelere karşı belirli bir saldırı sınıfı,kripto sistemin kaotik kısmını bypass etmeyi amaçlar. Bu sınıfta,şifreleme algoritması,kaotik alt sistemlerin bir dizi gizli haritalar veya parametrelerle değiştirilmesine eşdeğer bir biçimde ifade edilir." Bu durumda,K'nın nasıl elde edileceği araştırılmalıdır.

Fiziksel bir sistemin davranışı onu nasıl tanımladığımıza bağlı değildir. Soyut bir dinamik sistemi tanımlayan denklemler,sadece onun durumlarının belirli bir parametrizasyonuna göre anlamlıdır. Eğer parametrizasyonu değiştirirsek,dinamik denklemler,benzer fiziksel durumların değişim kanunlarıyla ilişkilerine göre değiştirilmelidir[4,7].

Örneğin $x_{n+1} = f(x)$ için $f: X \to X$ ile verilen bir değişim kuralı(evrim yasası) na sahip $x \in X$ kordinatları tarafından parametrelendirilen fiziksel durumlara sahip olduğumuzu varsayalım; $y \in Y$ olmak üzere $y = C(x)$ ile belirtilen yeni bir koordinat sistemine geçersek,dinamik denklemler $y_{n+1} = g(y_n)$ olur,burada $g: Y \to Y$ bağıntısı sağlanır. Dolayısıyla;

$$C\big(f(x)\big) = g(C(x)) \quad (2)$$

elde edilir.

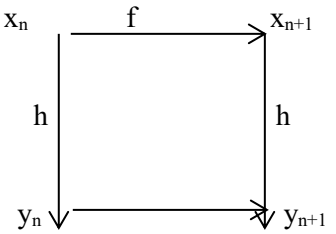
(2) denklemi basitçe bir taraftan

$$y_{n+1} = C(x_{n+1}) = C\big(f(x_n)\big)$$

diğer taraftan

$$y_{n+1} = C(y_n) = g\big(C(x_n)\big)$$

şeklinde ifade edilir. Bu şekil 1 de verilen komutatif diagram ile özetlenmiştir.



Şekil 1. Eşleniklik kavramı için Komutatif Diagram

Eşleniklik kavramı benzerliği açık bir şekilde göstermenin bir yoludur. Eğer açık resim-metin ve şifreli resim-metin arasındaki ilişki kaotik bağıntılarla belirlenirse, K parametresi (2)'den elde edilebilir. (2) denklemi x_n den y_{n+1} ' e giden iki yol karşılaştırılarak düzenlendiğinde;

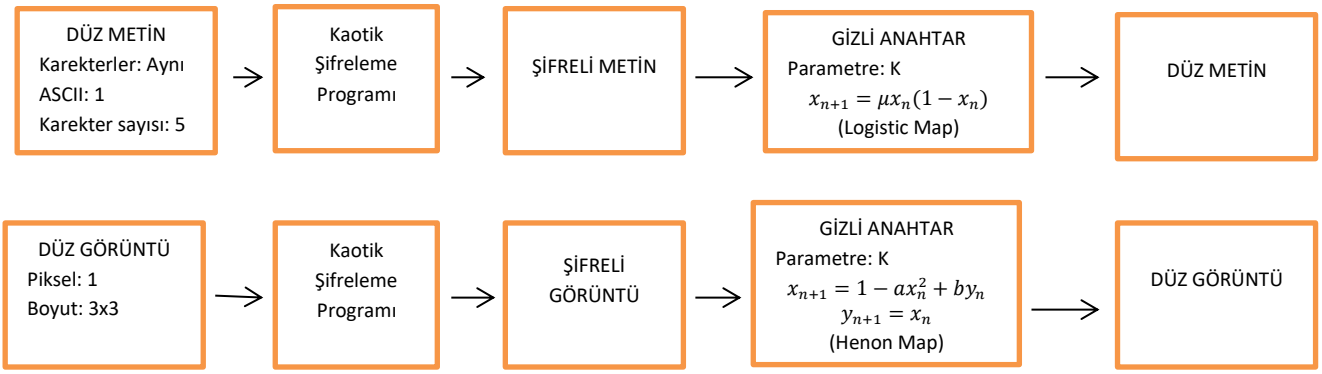
$$\begin{cases} x_{n+1} = 1 - ax_n^2 + by_n \\ y_{n+1} = x_n \end{cases} \quad (3)$$

$$x_{n+1} = \mu x_n(1 - x_n) \quad (4)$$

Denklemleri elde edilir.

K parametresi bilinen saldırı yöntemleri kullanılarak elde edilmeye çalışılır. Bu amaçla seçilen düz metin saldırısı kullanılabilir. Seçilen düz metin saldırısında, saldırgan bir düz resim-metin seçer ve bir şekilde karşılık gelen şifreli resim-metni elde eder. Düz-Şifreli resim-metin çifti analiz edilerek,gizli parametreleri ortaya çıkarmaya çalışır. Tüm sembolleri benzer karakterlerden oluşan bir metin verisi yada tüm pikselleri aynı değerlere sahip resim verisi için,şifreli veri elde edildiğinde K parametresi kolaylıkla elde edilebilir. Örneğin; tüm piksel değerleri 1 olan küçük bir 3x3 boyutlu görüntüsünü düz görüntü olarak seçelim ve bu görüntüye karşılık gelen şifreli görüntüyü önerilen yöntemle elde edelim. Düz görüntü ile şifreli görüntü Henon map ile belirlendiğinden K

parametresi (3)'den elde edilebilir. Benzer şekilde tüm karakterleri aynı ve ASCII kodu 1 olan 5 karakterli bir metin düz metin olarak seçilsin. Eğer bu veriye karşılık gelen şifreli metin elde edilirse,K parametresi (4) denklemi kullanılarak elde edilebilir. Sonuç olarak algoritmanın gizli anahtarı seçilen yalnız bir tane düz metin-şifreli metin çifti kullanılarak elde edilebilir. Sonuç olarak algoritmanın gizli anahtarı seçilen yalnız bir tane düz metin-şifreli metin çifti kullanılarak elde edilebilir. Bu işlem şekil 2. de özetlenmiştir.



Şekil 2. Düz Metin-Görüntü Kriptoanaliz Akış Şeması

Şifreleme algoritmasının diğer bir zayıf yönü ise; algoritmanın gizli anahtarları başlangıç şartları ve kontrol parametreleri EKG verisiyle belirlenen kaotik fonksiyonlarla üretilir. Lojistik harita ve Henon haritası kullanılarak şifreleme yapılır. Ancak hem Lojistik map hemde Henon map belirli paramete değerleri arasında kaotik davranış sergilerler. Algoritmanın konfizyon özelliğinin sağlanması kaotik iterasyonlara bağlı olduğundan,EKG verilerinden elde edilen parametre değerlerinin kaotik davranış sergilemediği durumda,şifreleme algoritmasının ana gereksinimi olan konfizyon özelliği sağlanamayacaktır. Sonuç olarak düz metin-şifreli metin çifti arasındaki ilişki kolaylıkla açığa çıkacaktır. Bu tür bir kriptoanaliz çalışması daha önceden Chee'nin kaotik şifrelemesi için [8] Arroyo ve arkadaşları tarafından yapılmıştır[6]. Ayrıntılı bir analiz için incelenebilir.

Analiz edilen algoritmanın önemli bir eksikliği ise; şifreleme mimarisinin difüzyon özelliğini sağlamamasıdır. Modern şifreleme algoritmalarının bir kaçı difüzyon özelliğini sağlamak için dairesel fonksiyonları defalarca tekrar ederek bunu gerçekleştirir. Önerilen algoritmada,şifreleme işlemi bir turda gerçekleştirilir.

4.Sonuç

Chen ve arkadaşları tarafından yeni bir görüntü şifreleme önerilmiştir[9]. Önerilen algoritmada,EKG sinyalleri ve kaotik fonksiyonlar gibi çeşitli yapılar kullanılarak şifreleme mimarisinin güçlendirilmesi amaçlanmıştır. Ancak, 3. Bölümde detaylı olarak ifade edildiği gibi;anahtar alanının boyutunun sadece istatistiksel testler ve kullanılan parametrelerin sayısına bağlı olarak ortaya konulması güvenlik analizi için yeterli değildir. Yalnızca daha karmaşık,öngörülemeyen,bireysel özellikli güvenilir yapılar kullanılarak güçlü kriptografik sistemler tasarlamak tek başına yeterli değildir. Aksi takdirde basit bir matematik bağıntı olan Lojistik map ve Henon map ele alındığında önerilen algoritmanın gizli anahtarları kolaylıkla elde edilebilecektir. Bu nedenle,mimaride kullanılacak olan unsurlar ve bu unsurların kullanılma şekline dikkat edilmelidir.

5. Kaynaklar

1. Alvarez G., Amigo J. M., Arroyo D., Li S., (2011). "Lessons Learnt from the Cryptanalysis of Chaos-Based Ciphers", in: L. Kocarev, S. Lian (Eds.), Chaos Based Cryptography Theory Algorithms and Applications, Springer-Verlag, 257-295.

2. Alvarez G., Li S., (2006) "Some basic cryptographic requirements for chaos-based cryptosystems". *International Journal of Bifurcation Chaos* **16/8:,**2129–2151.

3. Alvarez G., Li S., (2006). "Breaking an encryption scheme based on chaotic baker map". *Physics Letters A* **352**,78–82.

4. Alligood K., Sauer T., Yorke J., (, 1997). *Chaos an introduction to dynamical systems*, Springer-Verlag.

5. Amigo M., Kocarev L., Szczapanski J., (2007). "Theory and practice of chaotic cryptography". *Physics Letters A* **366**, 211-216.

6. Arroyo D., Alvarez G., Li S., Li C., Nunez J., (2008). "Cryptanalysis of a discrete-time synchronouschaotic encryption system". *Physics Letters A***, 372** ,1034–1039.

7. Katok A., Hasselblatt B., (1995). Introduction to the Modern Theory of Dynamical Systems. Cambridge University Press, Cambridge.

8. Chee C. Y., Xu D., (2006). "Chaotic encryption using dicrete-time synchronous chaos". *Physics Letters A* **348**, 284–292.

9. Chen C., Lin C., Chiang C., Lin S., (2012). "Personalized information encryption using ECG signals with chaotic functions". *Information Sciences* **19**, 125–140.

10. Çokal C., Solak E., (2009). "Cryptanalysis of a chaos-based image encryption algorithm".*Physics Letters A* **373**,1357–1360.

11. Fridrich J., (1998). "Symmetric ciphers based on two-dimensional chaotic maps". International *Journal of Bifurcation and Chaos* **8/6**,1259–1284.

12. Gao T., Chen Z., (2008). "Image encryption based on a new total shuffling algorithm". *Chaos, Solitons & Fractals* **38/1**, 213–220.

13. Guan Z.-H., Huang F., Guan W., (2005). "Chaos-based image encryption algorithm", *Physics Letters A*, **346**, 153 -157.

14. Huang C.K., Nien H.H., (2009). "Multi chaotic systems based pixel shuffle for image encryption". *Optics Communications*, **282/11**, 2123-2127.

15. Jakimoski G., Kocarev L., (2001). "Chaos and cryptography: block encryption ciphers". *IEEE Trans Circ Syst-I* **48/2,** 163–169.

16. Li C., Li S., Lo K., (2011). "Breaking a modified substitution–diffusion image cipher based on chaotic standard and logistic maps". *Communications in Nonlinear Science and Numerical Simulation* **16/2**, 837-843.

17. Pisarchik A.N., Flores-Carmona N.J., Carpio-Valadez M., (2006). "Encryption and decryption of images with chaotic map lattices". *Chaos* **16/3.**

18. Patidar V., Pareek N.K., Sud K.K., (2009). "A new substitution-diffusion based image cipher using chaotic standard and logistic maps". *Communications in Nonlinear Science and Numerical Simulation* **14/7**, 3056–3075.

19. Özkaynak F., Özer A. B., Yavuz S., (2012). Cryptanalysis of a novel image encryption scheme based on improved hyperchaotic sequences. *Optics Communications* **285/24**, 4946–4948.

20. Solak E., Cryptanalysis of Chaotic Ciphers, in: L. Kocarev, S. Lian (Eds.), (2011). *Chaos Based Cryptography Theory Algorithms and Applications*, Springer-Verlag, 227-256.

21. Ying-Qian Z., Xing-Yuan W., (2014). Analysis and improvement of a chaos-based symmetric image encryption scheme using a bit-level permutation. *Nonlinear Dynamics*, **77/3**, 687–698.

22. Solak E., Rhouma R., Belghith S., (2010). Cryptanalysis of a multi-chaotic systems based image cryptosystem. *Optics Communications* **283/2**, 232-236.

23. Chengqing L., Tao X., Qi L., Ge C., (2014). Cryptanalyzing image encryption using chaotic logistic map. *Nonlinear Dynamics*, **78/2**, 1545–1551.

24. Solak E., Çokal C., (2008). Cryptanalysis of a cryptosystem based on discretized two dimensional chaotic maps. *Physics Letters A* **372/46**, 6922–6924.

25. Özkaynak F., Yavuz S., (2014). Analysis and improvement of a novel image fusion encryption algorithm based on DNA sequence operarition and hyper-chaotic systems. *Nonlinear Dynamics*, **78/2**, 1311–1320.

26. Vrahatis M.N., Tsirogiannis G.A., Laskari E.C., (2010). Novel orbit based symmetric cryptosystems. *Mathematical and Computer Modelling*, Volume **51**, 239-246.

27. Wang X., He G., (2011). Cryptanalysis on a novel image encryption method based on total shuffling scheme. *Optics Communications*, **284/24**, 5804-5807.

28. Xiang T., Wong K.-W., Liao X. (2007). A novel symmetrical cryptosystem based on discretized two-dimensional chaotic map. *Physics Letters A* **364/3**, 252–258.

29. Zhu Z., Zhang W., Wong K, Yu H., (2011). A chaos-based symmetric image encryption scheme using a bit-level permutation. *Information Sciences*, **181/6**, 1171-1186.