Journal of the Faculty of Engineering and Architecture of Gazi University 35:3 (2020) 1369-1385

Mühendislik Mimarlık Fakültesi Dergisi
Journal of The Faculty of Engineering and Architecture of Gazi University

Elektronik / Online ISSN : 1304 - 4915
Basılı / Printed ISSN : 1300 - 1884

Microcomputer-based encryption of vein images with a non-linear novel system

Akif Akgül[1], Mustafa Zahid Yıldız*[1], Ömer Faruk Boyraz[1], Emre Güleryüz[1], Sezgin Kaçar[1], Bilal Gürevin[2]

[1]Sakarya University of Applied Sciences, Faculty of Technology, Department of Electrical & Electronics Engineering, 54055, Sakarya, Turkey
[2]Sakarya University of Applied Sciences, Faculty of Technology, Department of Mechatronics Engineering, 54055, Sakarya, Turkey

Highlights:

- Acquisition of dorsal hand vein images via infrared camera and pre-processing
- Designing a new chaotic-based random number generator on a microcomputer
- Encryption of vein images on a microcomputer with a new chaotic-based random number generator and securely stored in the database

Keywords:

- Vein imaging
- Vein image encryption
- Chaotic system
- Raspberry Pi
- Random Number Generator

Article Info:

Research Article
Received: 26.04.2019
Accepted: 01.02.2020

DOI:

10.17341/gazimmfd.558379

Acknowledgement:

This work is supported by the Scientific and the Research Council of Turkey (TUBITAK) under Grant No. 117E284.

Correspondence:

Author: Mustafa Zahid Yıldız
e-mail: mustafayildiz@subu.edu.tr
phone: +90 535 744 4130

Graphical/Tabular Abstract

In this study, dorsal hand vein images are encrypted with a new chaotic-based random number generator on a microcomputer and stored securely in the database. In the scope of the study, the images of the dorsal hand vein taken by an infrared camera from the subjects were enhanced through pre-processing methods. A new chaotic-based random number generator has been designed to securely store the hand vein images that can be used in identification systems. The random numbers generated prior to the encryption process were subjected to the most widely accepted NIST-800-22 and ENT tests, and successful results from all tests were obtained. The random numbers obtained from the new chaotic system were subjected to XOR with 65536 pixels starting from the first pixel in the dorsal hand vein image. Chaos-based encryption system performance was evaluated with security analyzes as commonly used in literature such as histogram, correlation, entropy, NPCR, and UACI. It has been shown that hand vein images can be used in mobile identification systems with the help of this proposed encryption modality.

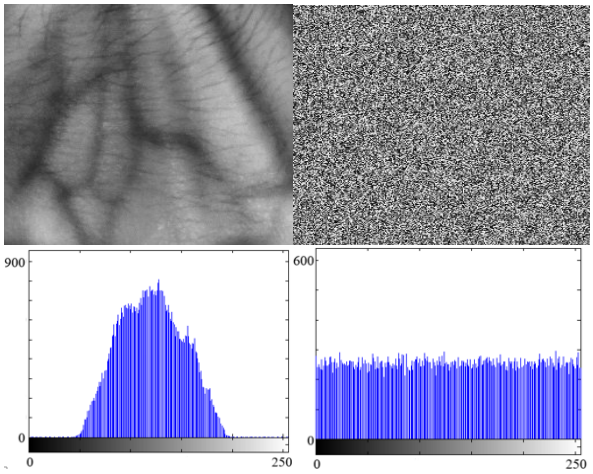


Figure A. Histogram analysis of the 8-bit vein image and encrypted vein image.

Purpose: The aim of this study is to encrypt hand vein images that vary from person to person on a microcomputer and store them securely in the database.

Theory and Methods:
The images of the dorsal hand vein taken by an infrared camera from the subjects were enhanced through pre-processing methods A unique random number generator was designed using a new 3D chaotic system in the Raspberry Pi microcomputer. The random numbers obtained from the new chaotic system were subjected to XOR with 65536 pixels starting from the first pixel in the dorsal hand vein image.

Results:
The vein images were encrypted with the newly designed random number generator and have been successfully passed through various security analyzes.

Conclusion:
It has been shown that hand vein images can be used in mobile identification systems with the help of this proposed encryption modality.

Journal of the Faculty of Engineering and Architecture of Gazi University 35:3 (2020) 1369-1385

Mühendislik Mimarlık Fakültesi Dergisi
Journal of The Faculty of Engineering and Architecture of Gazi University

Elektronik / Online ISSN : 1304 - 4915
Basılı / Printed ISSN : 1300 - 1884

Doğrusal olmayan yeni bir sistem ile damar görüntülerinin mikrobilgisayar tabanlı olarak şifrelenmesi

Akif Akgül[1], Mustafa Zahid Yıldız*[1], Ömer Faruk Boyraz[1], Emre Güleryüz[1], Sezgin Kaçar[1], Bilal Gürevin[2]
[1]Sakarya Uygulamalı Bilimler Üniversitesi, Teknoloji Fakültesi, Elektrik-Elektronik Mühendisliği Bölümü, 54055, Sakarya, Türkiye
[2]Sakarya Uygulamalı Bilimler Üniversitesi, Teknoloji Fakültesi, Mekatronik Mühendisliği Bölümü, 54055, Sakarya, Türkiye

ÖNEÇIKANLAR

- El üstü damar görüntülerinin kızılötesi kamera aracılığıyla elde edilmesi ve önişlemlerden geçirilmesi
- Mikrobilgisayar ortamında yeni bir kaotik tabanlı rastgele sayı üretecinin tasarlanması
- Damar görüntülerinin mikrobilgisayar ortamında yeni kaotik tabanlı rasgele sayı üreteci ile şifrelenip güvenli bir şekilde veri tabanında saklanması

Makale Bilgileri
Araştırma Makalesi
Geliş: 26.04.2019
Kabul: 01.02.2020

DOI:
10.17341/gazimmfd.558379

Anahtar Kelimeler:
Damar görüntüleme,
damar görüntüsü şifreleme,
kaotik sistem,
raspberry pi,
rasgele sayı üreteci.

ÖZET

Bu çalışmada yeni bir kaotik sistem ile mikrobilgisayar tabanlı olarak el üstü damar görüntülerinin şifrelenerek, güvenli bir şekilde veri tabanında saklanması ve kullanılması amaçlanmıştır. Çalışma kapsamında öncelikle kızılötesi kamera yardımıyla kişilerden alınan el üstü damar görüntüleri ön işleme ile iyileştirilmiştir. Daha sonra ön işlemeden geçirilmiş damar görüntüleri mikrobilgisayar ortamında şifrelenmiştir. Şifreleme işlemi için yeni tasarlanan ve analizleri gerçekleştirilen kaotik sistem ile üretilen rasgele sayılar kullanılmıştır. Şifreleme işlemi öncesi elde edilen rasgele sayılar, uluslararası alanda en çok kabul gören NIST-800-22 ve ENT testlerine tabi tutularak, tüm testlerden başarılı sonuçlar alınmıştır. Kaos tabanlı şifreleme sonucunda elde edilen görüntülerin histogram, korelasyon, entropi, NPCR ve UACI gibi literatürde sıklıkla kullanılan güvenlik analizleri ile başarımları ölçülmüştür. Gerçekleştirilen çalışma ile kimlik tanıma sistemlerinde de kullanılabilen el üstü damar görüntülerinin mobil olarak güvenli bir şekilde kullanılabileceği gösterilmiştir.

Microcomputer-based encryption of vein images with a non-linear novel system

HIGHLIGHTS

- Acquisition of dorsal hand vein images via infrared camera and pre-processing
- Designing a new chaotic-based random number generator on a microcomputer
- Encryption of vein images on a microcomputer with a new chaotic-based random number generator and securely stored in the database

Article Info
Research Article
Received: 26.04.2019
Accepted: 01.02.2020

DOI:
10.17341/gazimmfd.558379

Keywords:
Vein imaging,
vein image encryption,
chaotic system,
raspberry pi,
random number generator

ABSTRACT

In this study, it is aimed to store and use hand vein images which were microcomputer based encrypted with a novel chaotic system in a secure database. In the scope of the study, the images of the dorsal hand vein taken from the subjects by an infrared camera were improved by pre-processing methods. The pre-processed vein images were then encrypted in the microcomputer environment. For the encryption process, the newly designed and analyzed random numbers produced by the chaotic system were used. The random numbers generated before the encryption process were subjected to the most widely accepted NIST-800-22 and ENT tests in the international arena and successful results were obtained from all tests. The performance of chaos-based encryption system was tested with the security analyzes as frequently used in literature such as histogram, correlation, entropy, NPCR and UACI. It has been shown that hand vein images can be used in mobile identification systems with the help of this proposed encryption modality.

*Sorumlu Yazar/Corresponding Author: aakgul@subu.edu.tr, mustafayildiz@subu.edu.tr, oboyraz@subu.edu.tr, emreguleryuz61@gmail.com, skacar@subu.edu.tr, bilalsau@gmail.com / Tel: +90 535 744 4130

1. GİRİŞ (INTRODUCTION)

Biyometri; insanların parmak izi, iris, yürüyüş şekli, hareket biçimleri gibi çeşitli insan fizyolojik ve davranışsal özelliklerine göre kişileri tanımlamayı sağlar. Parmak izi, avuç içi izi, iris, gibi fizyolojik özellikler vücudun şekli ile ilgiliyken ses, el yazısı imzası ve yürüyüş gibi davranışsal özelliklerse bireyin davranış modeliyle ilgilidir. [1]

Biyometri geleneksel bilgi tabanlı tanımlayıcılarla (parola, pin kodu vs) kıyaslandığında bu teknolojiler daha güvenli ve güvenilirdir, çünkü fizyolojik ya da davranışsal özellikler benzersizdir ve kaybedilmesi ya da üretilmesi kolay değildir [2]. Özellikle sağlık ve finans gibi alanlarda güvenlik amaçlı çok yoğun bir şekilde kullanılmaktadır. Son on yılda cerrahi olarak değiştirilmiş parmak izlerinin, sahte iris pullarının ya da sofistike yüz maskelerinin kullanımında önemli bir artış olmuştur [3]. Deri altında bulunan vasküler deseni cerrahi olarak değiştirmek son derece zordur [4]. Bu yüzden kişiden kişiye benzersiz olan el üstü damar desenlerini kullanarak oluşturulan bir biyometrik sistem güvenlik açısından son derece güvenilirdir [5]. Vasküler modellerin büyük ölçüde gizlendiği ve görünür ışık altında çalınması ya da görüntülenmesi zor olduğu için, kimlik doğrulama uygulamalarında kullanılması yerindedir.

El üstü damar desenlerinden kimlik doğrulama ve tanıma işlemlerinin yapılması diğer örüntü tanıma sistemlerine (parmak izi, avuç içi, parmak damarı gibi) göre bir avantajı görüntülerin elde edilmesi esnasında herhangi bir düzeneğe dokunmadan temassız bir şekilde kimlik tanıma ve doğrulama işlemlerinin yapılabilmesidir [6]. Bu sayede kimlik tanıma işlemi daha steril bir ortamda yapılmış olur. Bu gibi avantajlar el üstü damar tanıma teknolojisini, güvenlik sistemlerinde, hastanelerde, adliyelerde, bankalarda, kamu kurum kuruluşlarında ve endüstride giderek artan ilgiyi çeken daha doğru ve umut verici bir sistem kılmaktadır.

Birçok güvenlik sisteminde ve hastanelerde kullanılabilen el üstü damar görüntüleri, kişilerin kimlik bilgilerini içerdiğinden çok önemlidir ve bu yüzden gizli olmalıdır. Bu özel görüntüler çalındığında, izlendiğinde veya yetkisiz erişimler tarafından kullanıldığında, çok ciddi sonuçlar doğurabilir. Örneğin, bir bilgisayar korsanı veya kötü niyetli bir veri tabanı yöneticisi, görüntüleri izinsiz elde edip kişisel çıkarları için kullanabilir. Bu nedenle el üstü damar görüntülerini korumak ve saklamak oldukça önemlidir.

Şimdiye kadar farklı görüntü gruplarını korumak ve saklamak amaçlı için birçok teknoloji geliştirilmiştir. Bu teknolojiler arasında kaotik şifreleme yöntemi, görüntüleri tanınmayacak hale dönüştüren en sezgisel ve etkili yoldur [7]. Son zamanlarda, tıbbi görüntüleri yüksek güvenlik seviyesinde tutmak için kullanılabilecek birçok görüntü şifreleme algoritması önerilmiştir [8]. Dzwonkowski vd. DICOM (Digital Imaging and Communications in Medicine) imajını korumak için kuaterniyonu kullanan bir şifreleme şeması sunmuşlardır [9]. Burada DICOM, tıbbi görüntülerin farklı medikal görüntüleme ekipmanı arasında güvenli ve güvenilir iletişimini kolaylaştırmak için geliştirilmiş bir standarttır [10]. Zhang vd. rotasyon matrisi bit seviyesi permütasyonu ve blok difüzyonunu kullanarak yeni bir görüntü şifreleme şeması tasarlamışlardır [11]. Zhang vd. sıkıştırma algılama ve piksel permütasyon yaklaşımını kullanarak bir tıbbi görüntü şifreleme ve sıkıştırma algoritması önermiştir. Aynı zamanda bu algoritma tıbbi görüntüleri aynı anda şifreleyip sıkıştırabilmektedir [12].

Kaos bilimi, dinamik sistemlerin en karmaşık hal davranışı olmakla birlikte doğrusal olmayan olayları açıklamada kullanılan bir bilim dalıdır [13]. Zaman boyutundaki düzensizlik, başlangıç şartlarına hassas bağımlılık, sınırsız sayıdaki farklı periyodik salınımlar, genlik ve frekansının tespit edilememesi ve sınırlı bir alan içerisinde değişen işaretler kaotik sistemlerin başlıca özelliklerindendir [14]. Günümüzde kaotik sistemlerin kullanıldığı birçok farklı alan mevcuttur [15]. Nüfus dağılımı, finans, mühendislik ve şifreleme kaotiğin en sık kullanıldığı alanlardan bazılarıdır [16].

Son yıllarda birçok alanda kullanılmak üzere ilginç özellikli ve pratik uygulamalarda kullanım potansiyeline sahip yeni ve farklı kaotik sistemler literatüre sunulmuştur. Bazı sistemler var olan sistemlerde değişiklikler yapılarak, bazıları ise tamamen yeni sistemler olarak geliştirilmiştir. Akgül ve Pehlivan yeni bir kaotik sistem oluşturarak onun özelliklerinin incelenmesini gerçekleştirmiştir [17]. Lü ve Chen ise, Lorenz ve Chen sisteminden yeni kaotik sistem tasarlamışlardır [18]. Sprott, kapsamlı araştırmalar sonucu 19 farklı yeni kaotik sistem bulmuştur [19].

Rasgele sayı üreteçleri kriptolojik uygulamalar için sistemlerin güvenliğini etkilediğinden önemli bir yere sahiptirler. Günümüzde kriptografi, istatistik, nümerik analiz, simülasyon, modelleme gibi çeşitli alanlarda kullanılmaktadır [20]. Bu çalışmada kızılötesi kamera yardımıyla kişilerden alınan el üstü damar görüntüleri mikrobilgisayarda (Raspberry Pi 3) çeşitli önişlemlerden geçirilmiş ve damar görüntülerinin kişiye ait özel bir veri olmasından dolayı veri tabanında güvenli bir şekilde saklanması amaçlanmıştır. Bu verilerin saklanması aşamasında Raspberry Pi 3 tabanlı yeni bir kaotik sistem kullanılarak üretilen rasgele sayılarla damar görüntüleri şifrelenmiş ve bu görüntülerin güvenli bir şekilde veri tabanında depolanması sağlanmıştır.

Literatürde bulunan çalışmalardan farklı olarak el-üstü damar görüntülerinin kızılötesi kamera ile alınması, alınan görüntülerin görüntü işleme teknikleri kullanılarak damar bölgelerinin görünürlüğünün arttırılması, yeni bir kaotik sistem tabanlı rasgele sayı üretecinin tasarımı ve rasgele sayıların elde edilmesi, üretilen rasgele sayılar ile biyometride kullanılan damar görüntülerinin şifrelenmesi ve şifre çözme işlemleri ile tüm analizler mikrobilgisayar tabanlı bir sistemde yapılmıştır. İlave olarak sistemin mobil

bir ortamda geliştirilmesi, tanımlama alanında (biyometri) taşınabilirlik ve kullanılabilirlik sağlaması öngörülmektedir. Bu makale çalışmasında giriş bölümünün ardından, ikinci bölümde damar görüntüleme sistemi ve alınan görüntüler üzerinde yapılan görüntü işleme adımlarından bahsedilmiştir. Üçüncü bölümde kullanılan yeni bir doğrusal olmayan sistem tanıtılarak, çatallaşma, lyapunov gibi dinamik analizleri gerçekleştirilmiş ve kaotik yapıya sahip olduğu gösterilmiştir. Dördüncü bölümde ise mikrobilgisayar tabanlı rasgele sayı üretim işlemi gerçekleştirilerek, elde edilen rasgele sayılar NIST-800-22 ve ENT testlerine tabi tutulmuştur. Testleri başarıyla geçen rasgele sayılar ile damar görüntüleri şifrelenmiştir. Beşinci bölümde şifrelenen damar görüntülerinin güvenlik analizleri yapılarak başarımları ölçülmüştür. Son bölümde ise sonuç ve değerlendirmeler yapılmıştır.

2. DAMAR GÖRÜNTÜLEME VE GÖRÜNTÜ İŞLEME
(VEIN IMAGING AND IMAGE PROCESSING

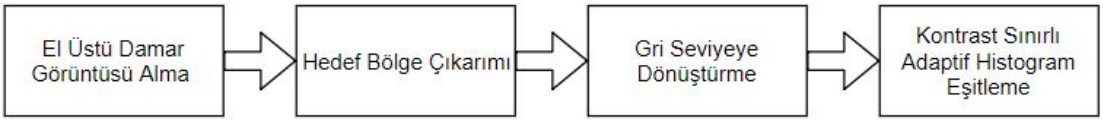
Bu bölümde damar görüntüleme sistemi ve alınan görüntüler üzerinde yapılan görüntü işleme adımlarından bahsedilmiştir. Damar görüntüleme sisteminde ilk olarak, yakın-kızılötesi ışık kaynağından yollanan ışınlar difüzörler üzerinden geçirilerek homojen bir şekilde deri üzerine yansıtılmıştır. Kızılötesi ışınların derinin 3-4 mm altına kadar nüfuz edebilmesi ve kanda bulunan hemoglobinin kızılötesi radyasyonu çevre dokulara göre daha fazla absorbe etmesi özelliklerinden yararlanarak, 850 nm dalga boyuna sahip kızılötesi led aydınlatma kullanılmış ve damar bölgelerinin diğer dokulardan daha koyu bir şekilde görüntülenmesi sağlanmıştır. Toplamda 72 kişiden alınmış (40 erkek, 32 kadın) el-üstü damar görüntüleri mikrobilgisayar (Raspberry Pi 3) sisteminde sayısal ortama aktarılmış ve OpenCV açık kaynak kodlu kütüphanesi kullanılarak Pyhton dilinde çeşitli görüntü işleme adımları uygulanmıştır. Şifreleme öncesi görüntü işleme süreci bulunmaktadır. Burada kontrast iyileştirme ile el üstü damar örüntülerinin belirgin bir hale getirilmiştir.

2.1. Ön İşleme (Pre-processing)

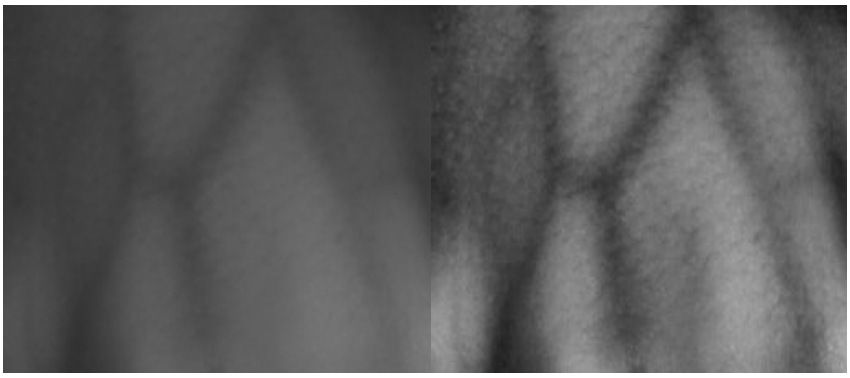
Yapılan ön işleme sürecinde kontrast iyileştirme amaçlanmıştır. Kızılötesi kamera yardımıyla alınan el üstü damar görüntülerinden hedef bölge çıkarılmış ve ardından kontrast sınırlı adaptif histogram eşitleme yapılarak damar bölgeleri daha belirgin hale getirilmiştir. Şekil 1'de el üstü damar görüntülerine uygulanan önişlem aşamaları gösterilmektedir. Alınan görüntüler önce gri seviyeye dönüştürülmüş ardından kontrast sınırlı histogram eşitleme (KSAHE) yöntemi uygulanarak damar bölgeleri netleştirilmiştir [21]. Bu yöntem hem gürültü azaltma işleminde hem de homojen alanlardaki kenar gölge etkilerini ortadan kaldırmak için medikal görüntüler üzerinde kullanılmaktadır. Şekil 2'de gri seviyeye dönüştürülmüş hedef bölgesi ve KSAHE yöntemi ile kontrastı iyileştirilmiş damar bölgesi görülmektedir. Bu işlemler sonucunda 8 bit seviyede şifreleme yapılmadan önceki aşamaya gelinmiştir.

3. YENİ KAOTİK SİSTEM VE DİNAMİK ANALİZLERİ
(NEW CHAOTIC SYSTEM AND DYNAMIC ANALYSIS)

Yeni ortaya konan kaotik sistem sürekli zamanlı, 3 boyutlu denge noktasız bir kaotik sistemdir. Sistem Eş. 1'de verildiği gibi 3 ayrı diferansiyel denklemden oluşmaktadır. Sistemde x, y, z olmak üzere üç adet durum değişkeni ve a, b, c, d olmak üzere toplam dört adet parametre bulunmaktadır. Sistemin kaotik özellik göstermesi için başlangıç şartları $x_0 = 0{,}4$, $y_0 = 0{,}1$, $z_0 = 0$ olarak belirlenmiştir.



Şekil 1. El damar görüntüsü önişleme adımları (Hand vein image preprocessing steps)



a) b)

Şekil 2. a) Gri seviyeli görüntü b) Kontrast sınırlı adaptif histogram eşitleme
(a) Gray level image b) Contrast limited adaptive histogram equalization)

$$\begin{aligned}\dot{x} &= ay \\ \dot{y} &= -x + byz \\ \dot{z} &= -x - cxy - dxz\end{aligned} \quad (1)$$

Eş. 1'de verilen sistem için parametreler a=1,9, b=1,1, c=11,5 ve d=0,7 olduğu durumda kaotik özellik göstermektedir. Eş. 2'de kaotik sistemin parametreleri yazılmış hali gösterilmektedir.

$$\begin{aligned}\dot{x} &= 1.9y \\ \dot{y} &= -x + 1.1yz \\ \dot{z} &= -x - 11.5xy - 0.7xz\end{aligned} \quad (2)$$

Bir sistemin kaotik olup olmadığını anlamak için yapılan birçok analiz yöntemi vardır. Sistemin belirli bir zaman içerisindeki davranışları (zaman serileri), faz portreleri, lyapunov üstelleri, çatallaşma diyagramlarının incelenmesi bu analiz yöntemlerinden bazılarıdır. Bu yöntemler sayesinde sistemin kaotik olup olmadığına karar verilebilmektedir.

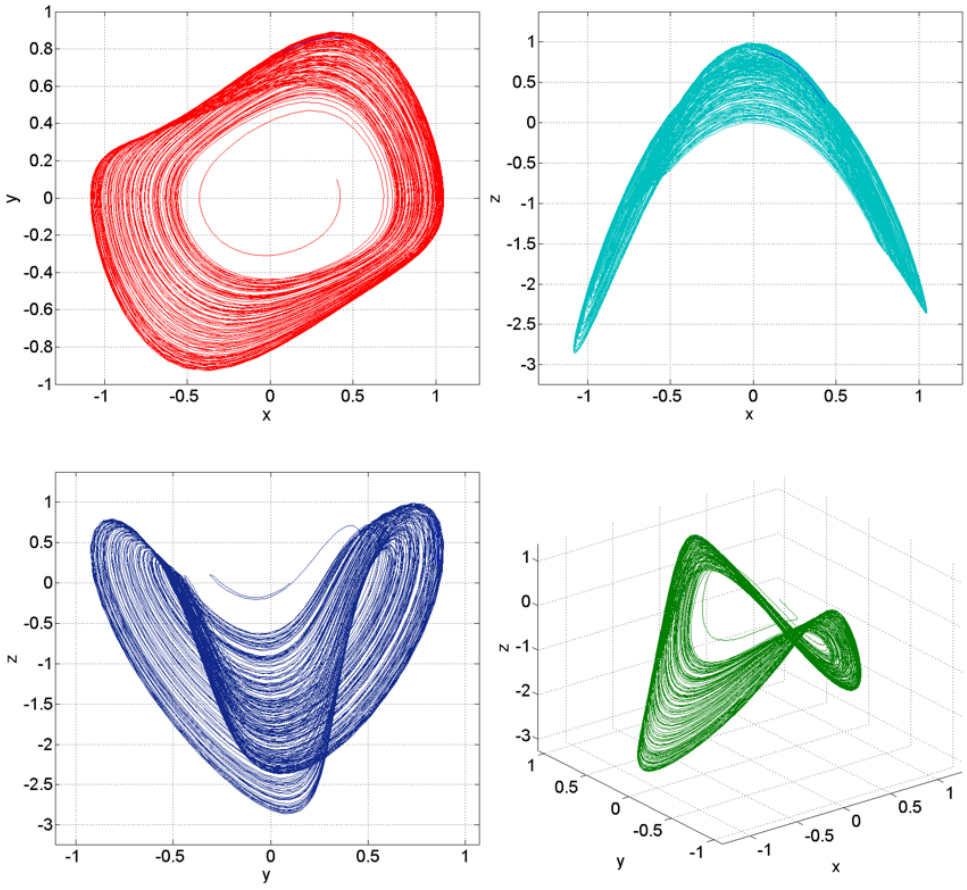
3.1. Faz Portreleri (Phase Portraits)

Üç boyutlu bir sistemin x-y, x-z, y-z, x-y-z olmak üzere dört farklı şekilde faz portrelerinin incelenmesi yapılabilir. Şekil 3'te de faz portrelerinden görüldüğü üzere yeni kaotik sistemimizin kararsız yani kaotik bir davranış sergilediği görülmektedir.

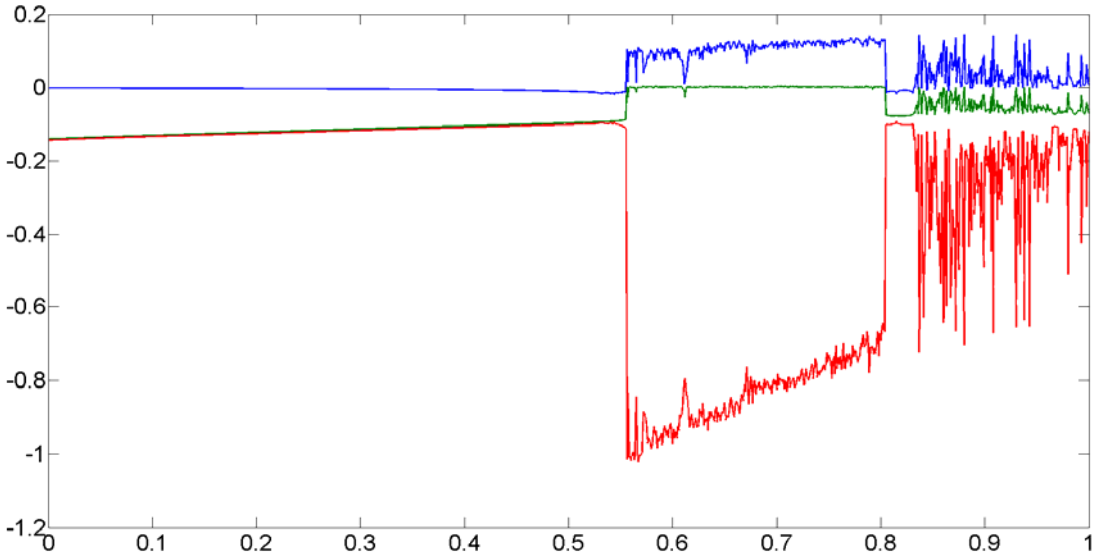
3.2. Lyapunov Üstelleri (Lyapunov Exponents)

Bir zaman serisinin kaotik bileşenler içerip içermediğini anlamamıza sağlayan bu yöntem ilk olarak Aleksandr Mikhailovich Lyapunov (1857-1918) tarafından tanımlanmıştır [22]. Bu yöntem ile zaman serisi içerisinde kaotik bileşenlerin varlığı incelenebilir. Yani Lyapunov üsteli ile başlangıçta birbirine yakın komşu olan iki rasgele noktanın ayrılma derecelerini ve başlangıç şartlarına olan hassas bağımlılıkları sayısal olarak ifade edilebilmektedir [23].

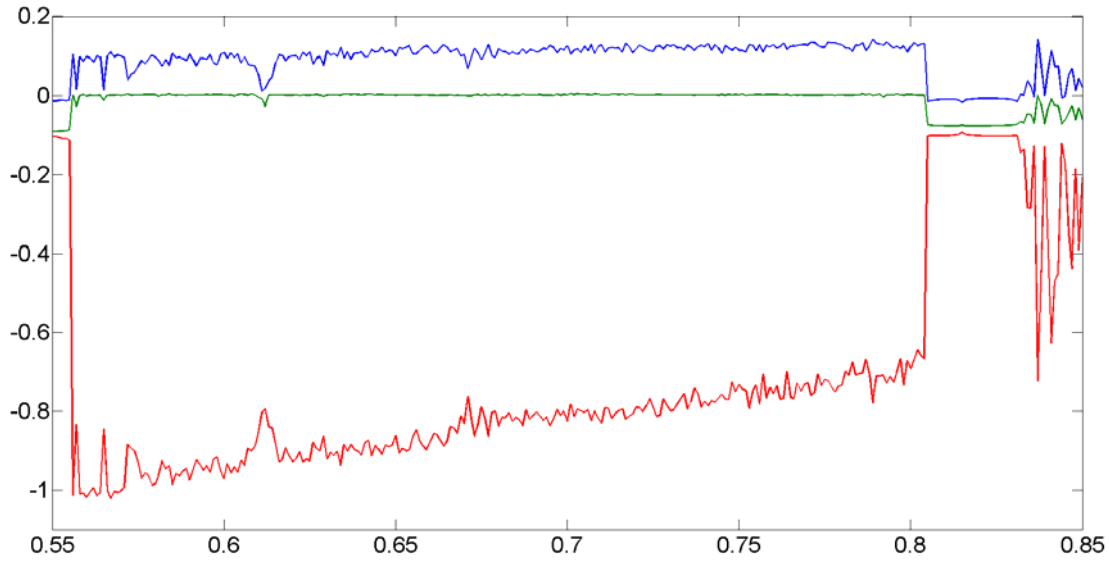
Bir sistemin kaotik olabilmesi için en az bir pozitif lyapunov üsteli λ içermesi gerekmektedir. Lyapunov üstelinin λ, negatif olması farklı başlangıç şartlarına karşılık aynı çıkışların üretileceğini yani sistemin kaotik olmadığını ifade eder. Diğer yandan lyapunov üstelinin λ, pozitif olması da tam tersi bir şekilde farklı başlangıç şartlarına karşılık farklı çıkışların üretileceğini, dolayısıyla da sistemin kararsızlığını yani kaotik olduğunu ifade eder. Şekil 4'te "d" parametresine göre lyapunov üstel spektrumu çizdirildiğinde sistemin 0,55 – 0,8 aralığında kaosa girdiğini görebiliriz. Şekil 5'te de bu aralığın büyütülmüş hali gösterilmektedir.



Şekil 3. Yeni kaotik sistemin x-y, x-z, y-z, x-y-z faz portreleri (x-y, x-z, y-z, x-y-z phase portraits of the new chaotic system)



Şekil 4. Yeni kaotik sistemin d parametresine göre Lyapunov Üsteli incelenmesi (0 – 1 aralığı)
(Lyapunov exponential analysis of the new chaotic system according to the d parameter (0-1 range))



Şekil 5. Yeni kaotik sistemin d parametresine göre Lyapunov Üsteli incelenmesi (0,55 – 0,85 aralığı)
(Analysis of the new chaotic system according to the d parameter Lyapunov (0.55-0.85 range)

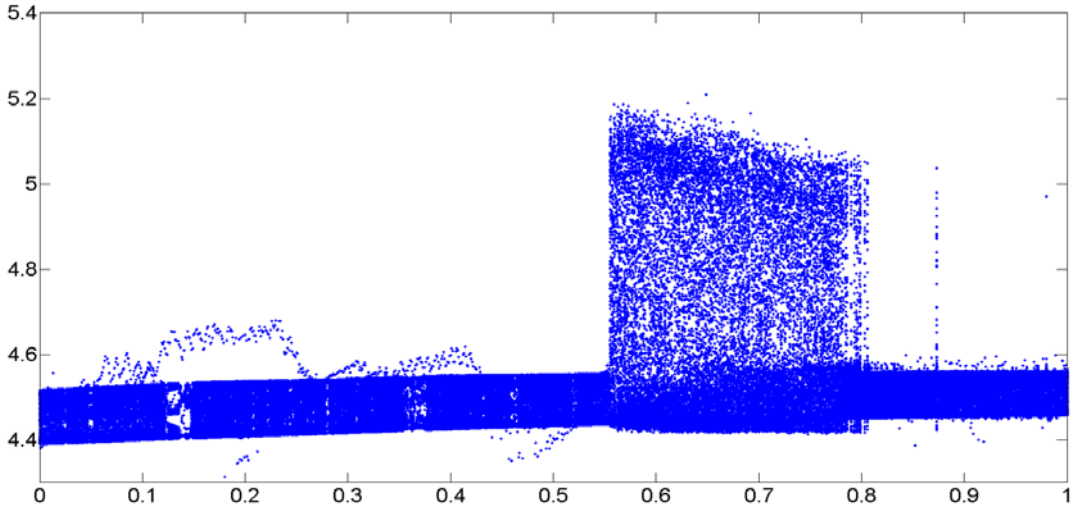
3.3. Çatallaşma Diyagramı (Bifurcation Diagram)

Bir sistemin kaotik olup olmadığını anlamak için yapılan analiz yöntemlerinden biri de çatallaşma diyagramlarının incelenmesidir. Sistem parametreleri değiştiğinde meydana gelen çatallaşmalar ile çizdirilen bu yöntem sayesinde sistemin kaotikliğine bakılabileceği gibi aynı zamanda hangi noktalarda kaotik olduğu ve hangi noktalarda kaotik olmadığı da incelenebilir.

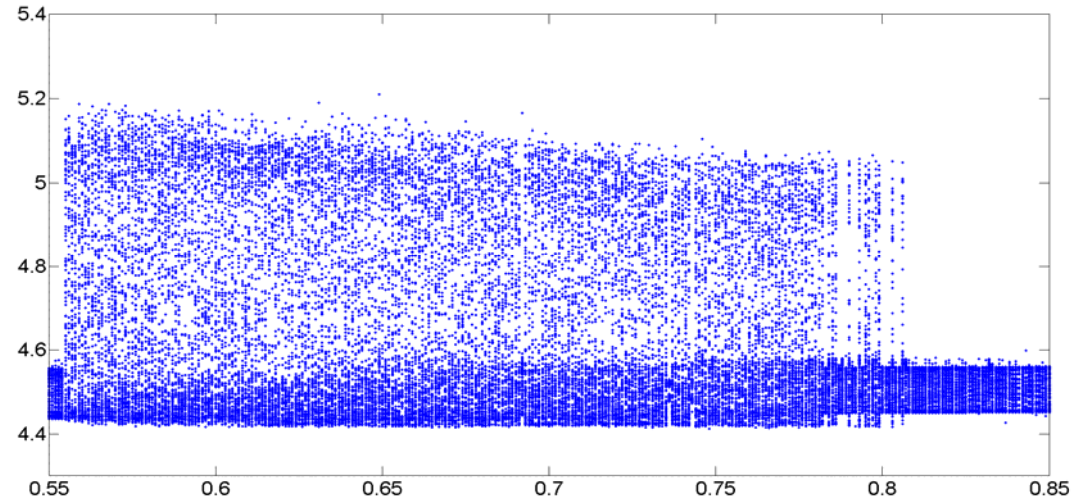
Yeni oluşturulan üç boyutlu sistemimizin çatallaşma diyagramına bakıldığında zaman (Şekil 6) yaklaşık olarak 0,55 – 0,8 aralığında kaosa girdiğini görebiliriz. Bu değer aralığı aynı zamanda Lyapunov üstel spektrumu ile de örtüşmektedir. Şekil 7'de ise kaosa girilen 0,55 – 0,8 aralığının büyütülmüş hali gösterilmektedir.

3.4. Zaman Serileri (Time Series)

Bir sistemin parametrelerinin zamanla değişimini ve zaman içerisinde nasıl bir davranış sergilediğini gösteren veriler grafiğine zaman serileri denir [23]. Eğer bir sistemin kaotikliğinden bahsedecek olursak zaman serilerinde başlangıç şartlarına hassas bir şekilde bağımsız olması beklenmektedir. Bu da sisteme verilen farklı başlangıç değerlerinin zamanla farklı kaotik işaretler üretmesi anlamına gelmektedir. Şekil 8'e bakıldığında sistemin kararsız bir yapıda olduğu ve Şekil 9'a bakıldığında ise



Şekil 6. Yeni kaotik sistemin d parametresine göre çatallaşma analizi (0 – 1 aralığı)
(Bifurcation analysis of the new chaotic system according to the d parameter(0-1 range))



Şekil 7. Yeni kaotik sistemin d parametresine göre çatallaşma analizi (0,55 – 0,85 aralığı)
(Bifurcation analysis of the new chaotic system according to the d parameter (0.55-0.85 range))

sistemin başlangıç şartlarına duyarlı olduğu gözlemlenebilmektedir.

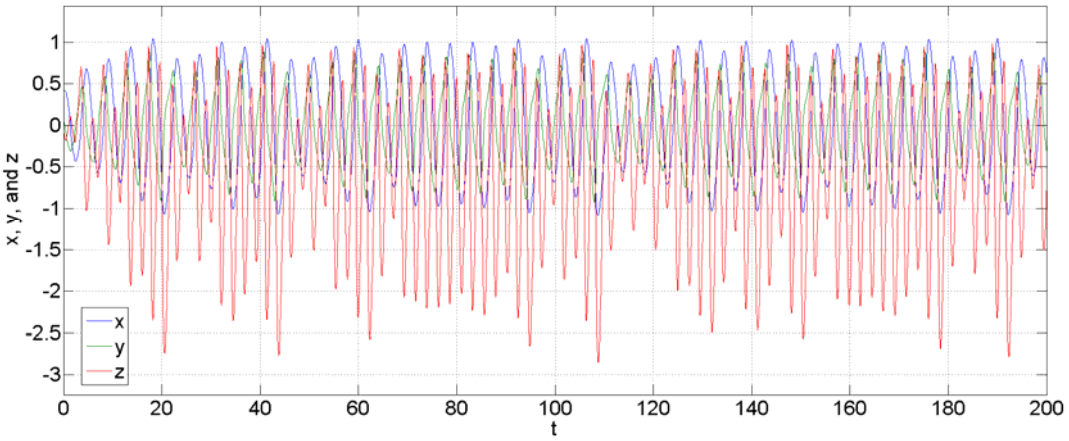
3.5. Hızlı Fourier Dönüşüm Analizi
(Fast Fourier Transform (FFT) Analysis)

Fourier dönüşüm yöntemi sinyalin içindeki bilgilerin elde edilebilmesi için, sinyallerin işlenmesinde kullanılan çok önemli bir yöntemdir. Bunun nedeni doğrusal olmayan sinyallerin frekans boyutunda analizleri daha verimli ve daha kullanışlı olmasıdır. Fourier dönüşümüyle bir sinyal, farklı genlik, frekans ve fazlarda kosinüs ve sinüs temel bileşenlerinin toplamı olarak ifade edilir. Her bileşenin frekans ve genliği ile birlikte gösterilmesi, bilgisayarla verilerin işlenmesi sırasında kolaylık sağlar. Kısaca zaman boyutunda olan bir sinyalin, frekans bileşenlerini öğrenmek için yapılan bir işlemdir. Kaotik sinyaller rastgeleliği sağladığı için periyodik bir sinyal ya da dar frekans bandına sahip olması beklenmez. Frekans bileşen sayısı arttıkça sinyalin karmaşıklığı daha da artar. Bu çalışmada kullanılan yeni 3 boyutlu kaotik sistemin x, y ve z durum değişkenlerinin FFT analizleri Şekil 10'da verilmiştir. Bu analize göre 3 durum değişkeninin de frekans bant genişliği geniş olduğundan rastgeleliği ve karmaşıklığı yüksek bir sistem sonucu çıkmaktadır.

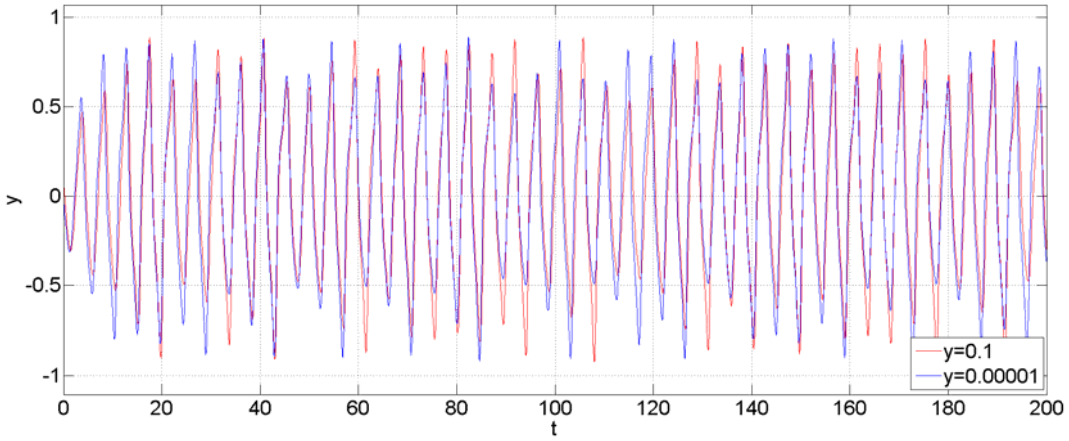
4. RASPBERRY Pİ 3 İLE RSÜ TASARIMI, RASTGELELİK TESTLERİ VE ŞİFRELEME
(RANDOM NUMBER GENERATOR (RNG) DESIGN, RANDOMNESS TESTS AND ENCRYPTION WITH RASPBERRY PI 3)

4.1. RSÜ Tasarımı (RNG Desing)

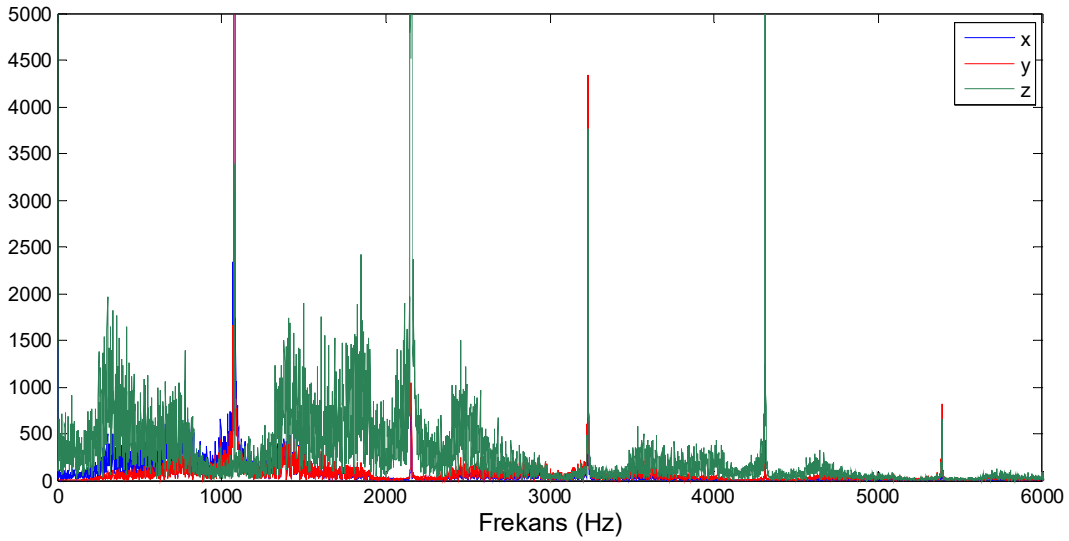
Raspberry Pi 3 üzerinde üretilen rastgele sayıların akış diyagramı Şekil 11'de gösterilmiştir. Öncelikle kullanılan kaotik sistemin parametreleri ve başlangıç şartları sisteme



Şekil 8. Yeni kaotik sistemin x-y-z zaman serilerinin incelenmesi (Examination of x-y-z time series of new chaotic system)

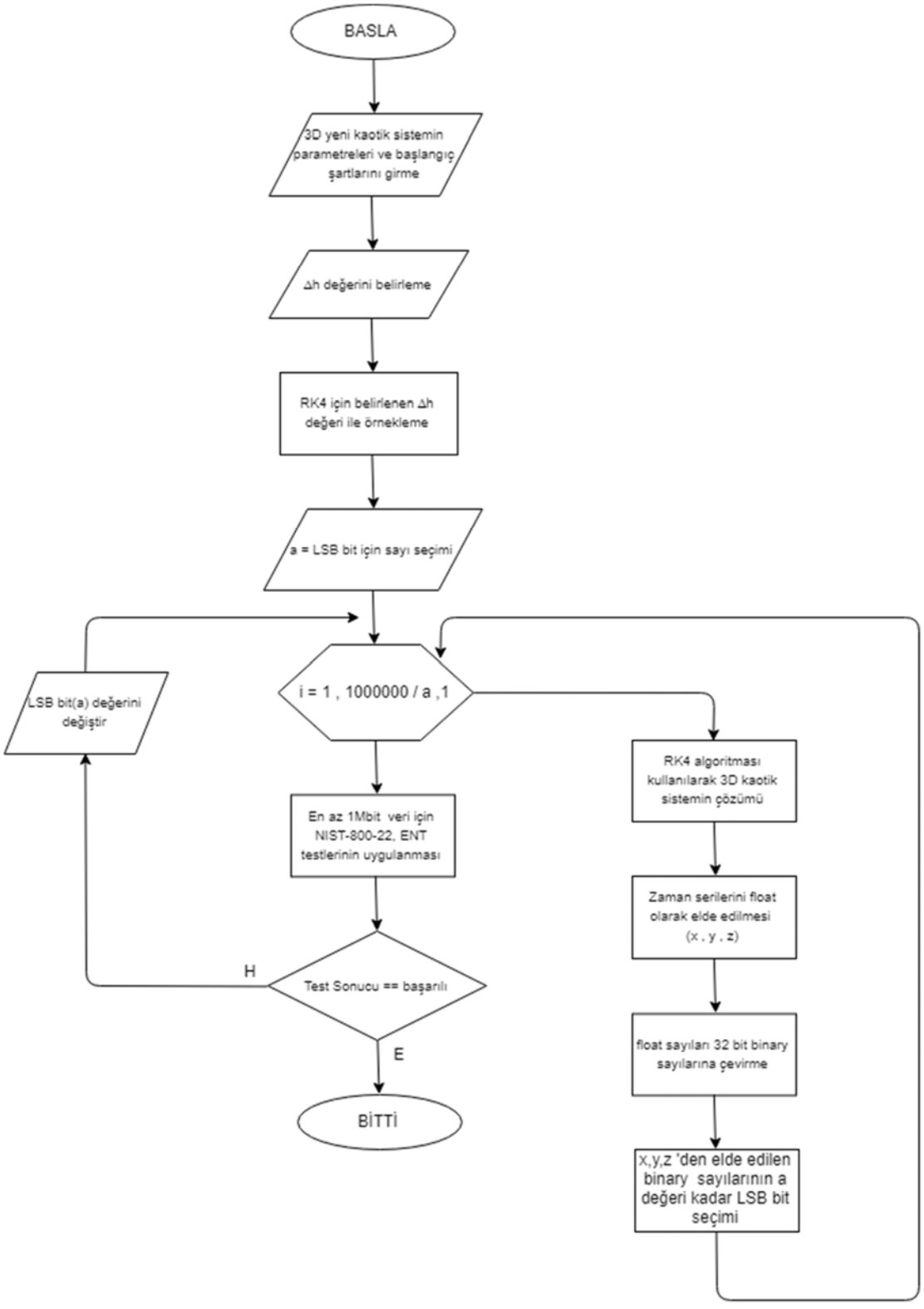


Şekil 9. Yeni kaotik sistemin y değişkeninin başlangıç şartlarına duyarlılığı
(Sensitivity of the new chaotic system to the initial conditions of the y variable)



Şekil 10. Yeni kaotik sistemin x, y, z değişkenlerinin FFT analizi (FFT analysis of x, y, z variables in new chaotic system)

girilir. Diferansiyel denklem çözüm yöntemi Runge Kutta 4 (RK4) için gereken Δh (adım aralığı) değeri belirlenir. Sonrasında belirlenen Δh değerinde örnekleme yapılarak seçilecek olan LSB bitinin sayısı (a) dışardan girilir. 1 milyon bit üretmek için RK4 çözümü için iterasyon hesabı yapılarak her iterasyonda elde edilen durum değişkenleri 32



Şekil 11. RSÜ algoritmasının akış diyagramı (Flowchart of the RNG algorithm)

bit ikilik sisteme (binary) dönüştürülür. 32 bit ikilik sisteme dönüştürülen sayı dizisinin belirlenen 'a' miktarında LSB biti elde edilerek 1 milyon adet rastgele sayı üretilmiş olur. Üretilen rastgele sayılar NIST-800-22 ve ENT testlerine tabi tutularak rastgelelilik analizleri yapılmıştır. Yapılan bu analizler sonucunda üretilen rastgele sayılar, NIST-800-22 ve ENT testinden başarıyla geçerse algoritma sonlanmış olur. Test sonucunda rasgelelik sağlanmadığı taktirde ise

a'nın değeri değiştirilir. Girilen bu a değeri sonrası tekrardan 1milyon adet rastgele sayı üretilir ve bu sayılar NIST-800-22 ve ENT testlerinden geçirilir. Üretilen sayıların rastgeleliği sağlanana kadar bu adımlar tekrar eder. Yapılan işlemler Şekil 11'de gösterilmiştir.

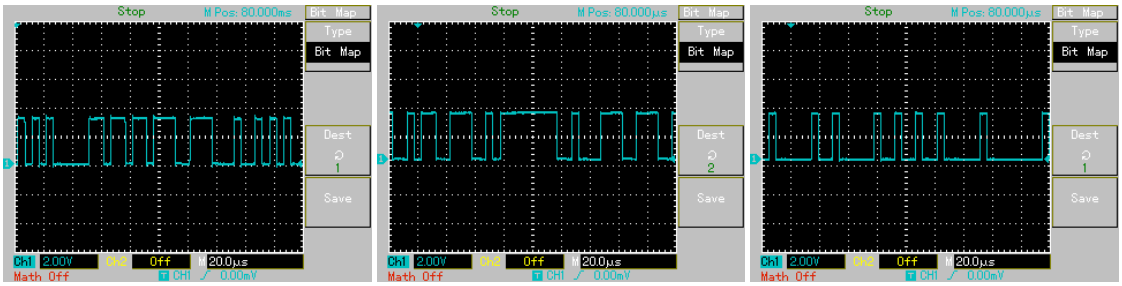
Kullanılan kaotik sistemden üretilen rastgele sayılar için hesaplanan x, y ve z durum değişkenlerinin osiloskop ekran görüntüleri Raspberry Pi 3'de çıktıları alınarak Şekil 12'de gösterilmiştir.

4.2. Rastgelelik Testleri (Tests For Randomness)

Raspberry Pi 3 mikrobilgisayarı üzerinde üretilen sayıların rastgelelik analizlerinin yapılması için NIST-800-22 ve ENT olmak üzere iki farklı test kullanılmıştır. Ulusal düzeyde kabul görmüş ve 1.000.000'luk sayı dizisine ihtiyaç duyan NIST-800-22 testi içeresinde 16 farklı testten oluşmaktadır. NIST-800-22 testine tabi tutulan bit dizisinin başarılı sayılabilmesi için bu testlerin hepsinden başarıyla geçmesi gerekmektedir. NIST-800-22 testinde, çıkan sonuçlar değiştirilebilen P-değerine göre değerlendirilmektedir. Eğer koşul olarak P-değeri 0,001 kabul edilmişse, bit testin başarılı olabilmesi için P-değerinin, 0,001'den büyük olması gerekmektedir. NIST-800-22 testinde bulunan ve bit dizilerinin rasgeleliğini tanımlayan 16 farklı istatistiksel test bulunmaktadır [24].

x, y ve z den elde edilen rasgele sayıların başarılı bir şekilde geçen NIST-800-22 test sonuçları Tablo 1'de gösterilmektedir. Tablo 1'e göre hepsi testten geçtiği için x, y ve z'nin son 8 bitler değerlerinden üretilen rasgele sayıların rasgeleliği sağlamış olduğu sonucuna varılmıştır.

ENT testi, sözde-rastgele sayı üreteci uygulamaları tarafından üretilen bayt dizilerine çeşitli testler uygulayan John Walker tarafından geliştirilen bir test uygulamasıdır [25]. ENT testinde bulunan ve bit dizilerinin rastgeleliğini tanımlayan 5 farklı istatistiksel test bulunmaktadır. x, y ve z den elde edilen rasgele sayıların ENT test sonuçları ortalama değerleri Tablo 2'de gösterilmektedir. Tablo 2'ye göre tüm testlerden geçen x, y ve z'nin son 8 bit değerlerinden üretilen rasgele sayıların rastgeleliği sağlamış olduğu sonucuna varılmıştır.



a) b) c)

Şekil 12. a) x b) y c) z fazlarından elde edilen rasgele sayıların osiloskop görüntüleri
(Oscilloscope images of random numbers obtained from a) x b) y c) z phases)

Tablo 1. x, y ve z'den elde edile rasgele sayıların NIST-800-22 test sonuçları
(NIST-800-22 test results of random numbers obtained from x, y and z)

İstatiksel Testler	P-değeri (X_8bit)	P-değeri (Y_8bit)	P-değeri (Z_8bit)	Sonuç
Frekans Testi	0,1835	0,5619	0,9028	Başarılı
Blok Frekans Testi	0,9886	0,4733	0,5049	Başarılı
Kümülatif toplamlar testi	0,1415	0,7570	0,7477	Başarılı
Yinelemeler Testi	0,7370	0,0596	0,1096	Başarılı
Blok İçinde En Uzun Bir Yinelemesi Testi	0,6039	0,7461	0,3937	Başarılı
İkili Matris Rankı Testi	0,3413	0,3521	0,7038	Başarılı
Aylık Fourier Dönüşümü Testi	0,2513	0,0454	0,4246	Başarılı
Örtüşmeyen Şablon Eşleştirme Testi	1,0103	0,0051	0,0506	Başarılı
Örtüşen Şablon Eşleştirme Testi	0,4714	0,6056	0,8564	Başarılı
Maurer's Universal Statistical Test	0,9012	0,4438	0,5287	Başarılı
Yaklaşan Entropi Testi	0,6074	0,2596	0,5061	Başarılı
Rastgele Gezinimler Testi (x = -4)	0,5684	0,1659	0,2135	Başarılı
Rastgele Gezinimler Değişken Testi (x = -9)	0,6490	0,4958	0,1828	Başarılı
Seri Testi-1	0,7416	0,5162	0,5991	Başarılı
Seri Testi-2	0,9123	0,2447	0,9363	Başarılı
Doğrusal Karmaşıklık Testi	0,1100	0,3270	0,3663	Başarılı

Tablo 2. x, y ve z'den elde edile rastgele sayıların ENT test sonuçları
(ENT test results of random numbers obtained from x, y and z)

Test Adı	Ortalama (Önerilen Yöntem(Ö.Y))	Sonuç
Aritmetik Ortalama	127,4990	Başarılı
Entropi	7,9995	Başarılı
Korelasyon	0,0031804	Başarılı
Ki Kare	259,041	Başarılı
Monte Carlo	3,1444(error = 0,0009)	Başarılı

Tablo 3'te önerilen kaotik yöntem sonucunda mikrobilgisayar vasıtasıyla elde edilen rastgele sayıların ENT test sonuçlarının literatürde bulunan bazı çalışmalarla kıyaslanması görülmektedir. Tablodaki sonuçlara bakıldığında elde edilen sayıların rastgeleliği sağladığı görülmektedir. Önerilen yöntemin, literatürdeki çalışmalara kıyasla ideal sonuçlara daha yakın bir sistem olduğu görülmektedir.

4.3. Damar Görüntülerinin Şifrelenmesi (Encryption of Vein Images)

Şifreleme işlemlerinde karıştırma (confusion) ve yayılma (diffusion) iki ana temel ihtiyaçtır. Kaotik sistemlerdeki, başlangıç koşulları ve kontrol parametreleri yayılmayı (hassasiyet) sağlarken kaotik sistemlerdeki karmaşıklık ise rastgeliliği yani karıştırmayı sağlamaktadır. Kaos tabanlı olmayan şifreleme algoritmalarında, şifrelemenin temel özellikleri olan karıştırma ve yayılmanın yeterince sağlanabilmesi için oldukça fazla işlem yükü oluşabilmektedir. Düşük işlem kapasitesine sahip platformlarda bu işlem yükü problem oluşturabilmektedir. Bu nedenle kaos tabanlı şifreleme yöntemleri düşük kapasiteli platformlar için tercih edilebilir.

Kaotik sistemlerde anahtar uzunluğu ve uzayı oldukça büyük olduğundan dolayı şifreleme işlemlerinde diğer kriptografik sistemlere göre daha güvenlidir. AES ve RSA gibi bilinen şifreleme yöntemlerine göre kıyas yapıldığında önerilen kaos tabanlı şifreleme yöntemi basit XOR işlemi içerdiğinden çok daha az işlem yüküne sahiptir ve mikrobilgisayar ortamında önerilen yöntemin uygulanması daha uygundur. Üretilen rastgele sayılar kullanılarak 8-bit damar görüntülerinin şifrelenmesi işlemlerini gösteren akış diyagramı Şekil 13'te verilmiştir. Alınan el üstü damar görüntüleri ilk olarak şifrelenmesi için sisteme verilir. Ardından bu görüntünün boyutları hesaplanır. Her koordinattaki piksel değerleri 8 bitlik ikili seviyeye dönüştürülür. 8 bitlik ikili seviyeye dönüştürülen sayı dizileri, kaotik sistemden üretilen rastgele sayılarla XOR işlemine tabi tutulur. Bu işlemin ardından oluşan değerler onluk (decimal) sayı sistemine dönüştürülerek şifreli görüntünün piksel değerleri elde edilmiş olur.

5. GÜVENLİK ANALİZLERİ (SECURITY ANALYSIS)

5.1. İstatistiksel Analizler (Statistical Analysis)

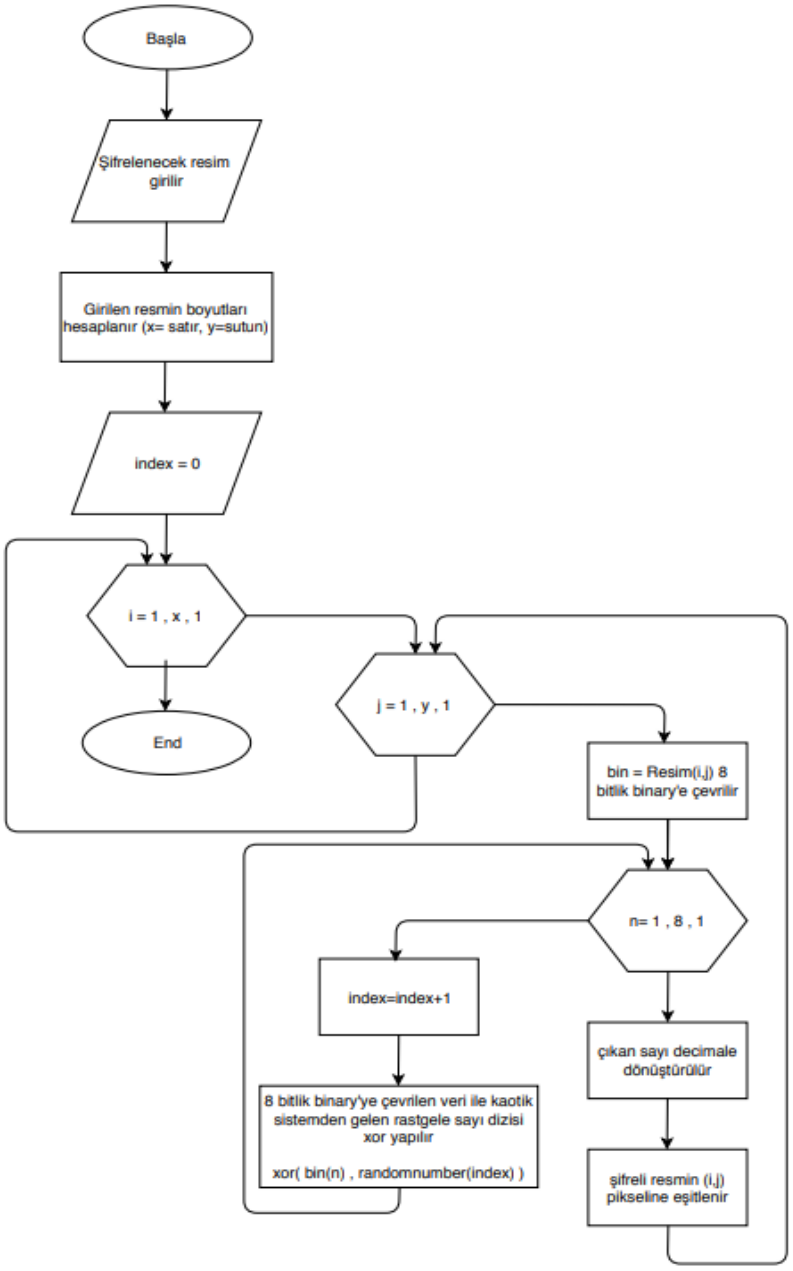
Kaos temelli şifreleme işlemi sonucunda ortaya çıkan şifrelenmiş görüntünün görsel olarak orijinal görüntüden tamamen farklı olması iyi bir şifreleme yapıldığını göstermekle birlikte tam bir güvenlik sağlandığını göstermez. Bunun için bazı istatistiksel güvenlik analizleri kullanılarak, gerçekleştirilen şifrelemenin performansı ortaya konmalıdır. Bu bölümde, şifrelemenin güvenlik analizi, 256x256 piksellik üç farklı görüntü için entropi, korelasyon, diferansiyel atak (NPCR, UACI) ve histogram yöntemleri kullanılarak, kaotik sistemin her fazına yönelik olarak gerçekleştirilmiştir.

Şekil 14'te kaotik sistemin x, y ve z fazları ile elde edilmiş sonuçlar incelendiğinde orijinal görüntülere ait analiz sonuçları ile Şekil 15'te gösterilen şifrelenmiş görüntülere ait sonuçların birbirinden tamamen farklı olduğu görülmektedir. Şekil 14'te orijinal görüntülerin histogram grafiklerinde yoğunluk belirli bir bölgede iken, Şekil 15'te şifreli görüntülerde ise histogram grafikleri homojen olarak dağılmıştır. Histogram dağılımlarının homojen olması şifrelemenin başarılı olduğunu göstermektedir.

8 bit damar resimlerine ait korelasyon katsayıları 1'e yakın bir sonuç verirken şifreli görüntülerde korelasyon katsayıları 0,0036, 0,0018, 0,0009 gibi sıfıra çok yakın sonuçlar elde

Tablo 3. Önerilen yöntemin ENT test sonuçlarının farklı modellerle kıyaslanması
(Comparison of the proposed method's ENT test results with different models)

	Aritmetik Ortalama	Entropi	Korelasyon	Ki Kare	Monte Carlo
Ö.Y	127,4990	7,9995	0,0001004	259,04 (%71,13)	3,1444 (hata: 0,0009)
Stoyanov vd. [26]	127,5013	7,9975	-0,000147	-	3,140569 (hata: 0,03)
Seetharam vd. [27]	122,885	7,7133	-0,058927	-	3,088126 (hata: 1,70)
Akhshani vd. [28]	127,7714	7,9999	0,000108	255,19	3,14062 (hata: 0,031)
İdeal Sonuçlar	127,5	8	0,0	%10 - %90 arası	3,14159 (Pi Sayısı)

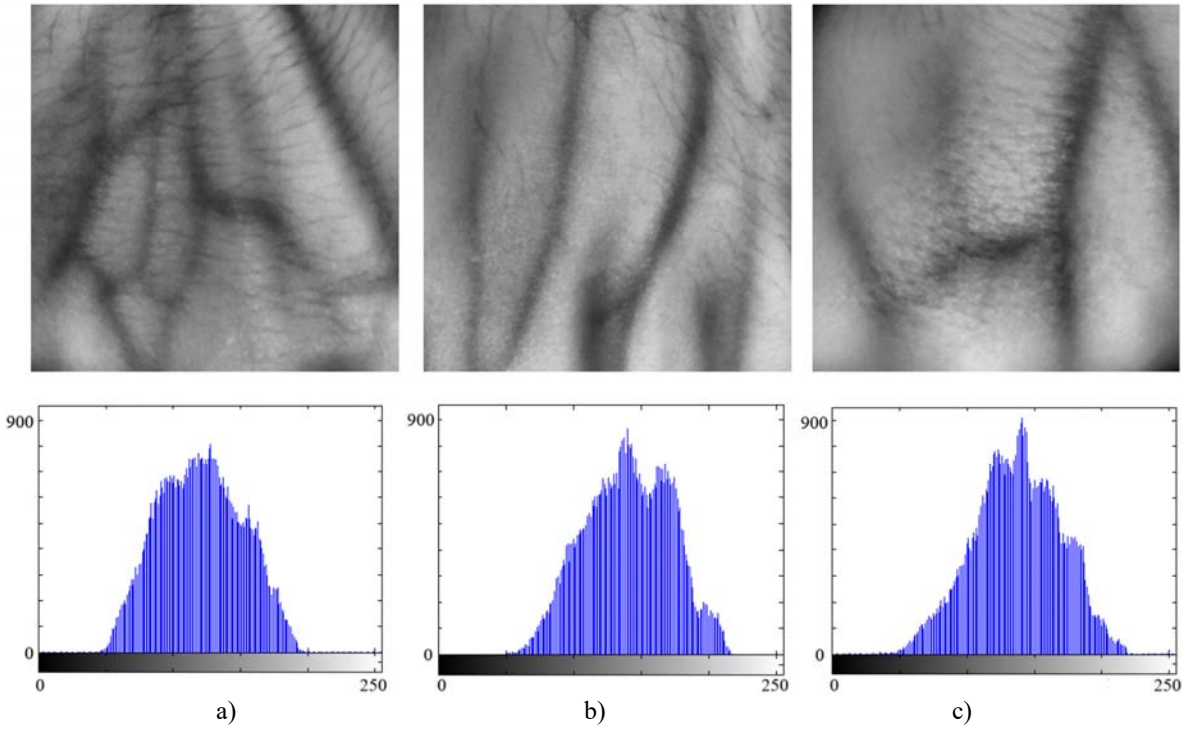


Şekil 13. Şifreleme Algoritmasının Akış Diyagramı (Flowchart of Encryption Algorithm)

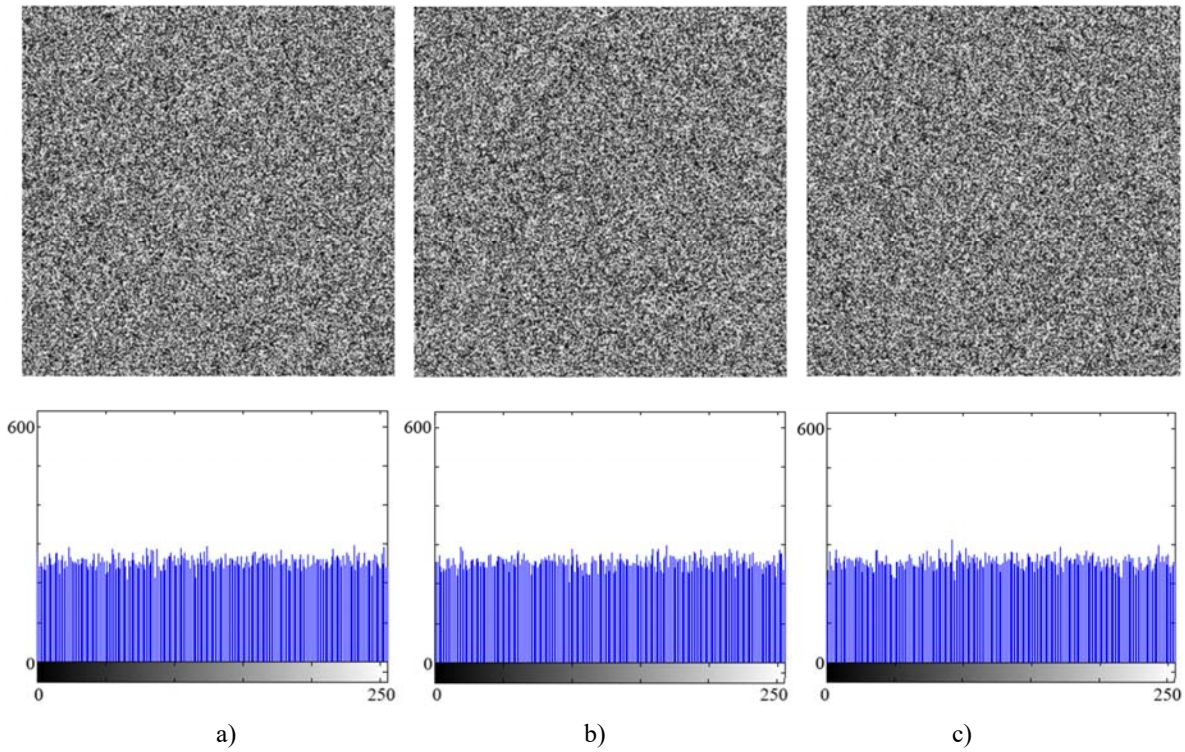
Tablo 4. 3 farklı 8 bit damar görüntüleri ile şifrelenmiş görüntülerinin korelasyon ve entropi katsayıları (Correlation and entropy coefficients of 3 different 8-bit images)

Örnek Görüntüler	Korelasyon Katsayısı	Entropi
1. 8 bit damar görüntüsü	0,9885	6,9489
X fazındaki şifreli görüntü	0,0036	7,9970
2. 8 bit damar görüntüsü	0,9883	6,9914
Y fazındaki şifreli görüntü	0,0018	7,9971
3. 8 bit damar görüntüsü	0,9886	7,0444
Z fazındaki şifreli görüntü		7,9973

edildiği Tablo 4'te gösterilmiştir. Bu değerler sonucunda şifrelemenin oldukça başarılı olduğu gösterilmiştir. Entropi değerleri incelendiğinde şifreli görüntülere ait değerin, 256x256 piksellik bir görüntü için olabilecek en yüksek



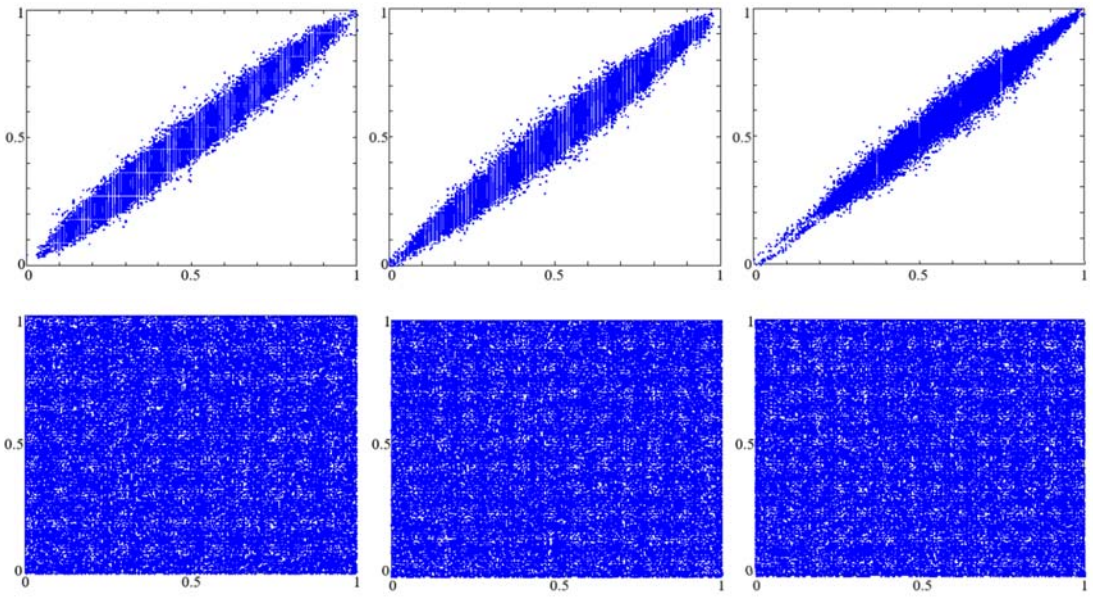
Şekil 14. a) b) c) 8 bitlik damar görüntüleri ve histogram dağılımları (a) b) c) 8-bit wein images and histogram distributions)



Şekil 15. a) x fazından b) y fazından c) z fazından elde edilen rastgele sayılar kullanılarak 8 bitlik şifrelenmiş damar görüntüleri ve histogram dağılımları
(8-bit encrypted vein images and histogram distributions using random numbers obtained from a) x b) y c) z phases)

değer olan 8 değerine çok yakın olduğu görülmektedir. Bu değer şifrelemedeki rasgele dağılımın istatistiksel olarak çok iyi olduğunu göstermektedir.

Şekil 16'da gösterilen korelasyon grafikleri incelendiğinde orijinal görüntülerde dağılım diagonal biçimde iken, şifreli görüntülerde dağılım yine homojen bir şekildedir.



Şekil 16. 3 farklı 8 bit damar görüntülerinin ve şifrelenmiş görüntülerin korelasyon haritaları
(Correlation maps of 3 different 8-bit wein images and encrypted images)

Korelasyon dağılımlarının homojen olması şifrelemenin iyi olduğunu göstermektedir.

Diferansiyel atak sonucu elde edilen NPCR ve UACI sonuçları da yine şifrelemenin başarılı olduğunu ve ataklara karşı dayanıklılığını göstermektedir. Tüm bu sonuçlar bir arada düşünüldüğünde şifrelemenin başarılı olduğu ve yüksek bir güvenlik sağladığı söylenebilir. Tablo 5'te 3 farklı şifreli görüntü ile 8 bit damar görüntüsü arasındaki NPCR, UACI analizleri verilmiştir. Analizlere göre birinci 8 bit damar görüntüsünün tüm piksel değerleri değişerek x fazından üretilen rasgele sayılar kullanılarak şifrelenen görüntünün oluştuğu, ikinci 8 bit görüntüsünün %99,9969'u değişerek y fazından üretilen rasgele sayılar kullanılarak şifrelenen görüntünün oluştuğu sonucuna varılmaktadır. UACI sonuçları ise değişen piksellerin yoğunluklarını ifade etmektedir.

Tablo 5. x, y ve z fazlarından üretilen rasgele sayılarla şifrelenen görüntülerin NPCR ve UACI analizleri
(NPCR and UACI analysis of images encryption with random numbers generated from x, y and z phases)

Örnek Görüntüler	NPCR	UACI
X fazındaki şifreli görüntü	100	28,7872
Y fazındaki şifreli görüntü	99,9969	28,5221
Z fazındaki şifreli görüntü	99,9969	28,2239

Yapılan analizler sonucunda X, Y ve Z fazları ile gerçekleştirilen şifreleme işlemlerinin de oldukça başarılı ve güvenli olduğu anlaşılmaktadır. Böylece, şifreleme için kaotik sistemin her fazının rahatlıkla kullanılabileceği ortaya konmuştur. Bununla birlikte, kaotik sistemin tüm fazları ile farklı görüntüler için elde edilen sonuçların iyi olması, kaotik sistemin dinamik özelliklerinin damar görüntülerinin şifrelenmesi için uygun olduğunu göstermektedir.

5.2. Uygulama Atakları (Implementation Attacks)

Bu çalışmadaki gibi donanımsal olarak gerçeklenen şifreleme yapılarında teorik atakların yanı sıra uygulama atakları olarak isimlendirilen ataklar da yapılabilmekte ve güvenlik seviyeleri tespit edilebilmektedir. Bu makalede Raspberry Pi gömülü bilgisayar kullanılarak bir şifreleme uygulaması gerçekleştirildiğinden bu cihazın baz alındığı uygulama ataklarına literatürde az sayıda da olsa rastlanmaktadır. Bu çalışmalarda Raspberry Pi üzerinde gerçeklenmiş RSA (Rivest–Shamir–Adleman) algoritmasına yan kanal saldırılarından olan SEMA (Simple Electromagnetic Analysis) ve DEMA (Differential Electromagnetic Analysis) saldırıları yapılmıştır [29]. Çalışmada SEMA saldırısına dayanıklı algoritma gerçeklenerek üretilen anahtarın SEMA saldırısı ile elde edilemediği görülmüştür. Diğer bir çalışmada Raspberry Pi üzerinde çalışan AES (Advanced Encrption Standart) algoritmasına karşı farksal yank anal analizi yöntemlerinden birisi olan DEMA saldırısı uygulanmıştır [30]. Saldırı sonrası platformun mini bir bilgisayar olması, monitor etme, haberleşme yeteneği ve çalıştırdığı servisler incelendiğinde bir şifreleme algoritmasının Raspberry Pi üzerinde çalıştığı tespit edilmiştir.

Buna karşın yapılan bir diğer çalışmada Sanada vd. Raspberry pi mikrobilgisayarın yan kanal ataklarına karşı ne kadar güvenli olduğunu test etmişlerdir. Çalışmalar neticesinde iki farklı şifreleme algoritmasına karşı yapılan yan kanal atakları sonucunda Raspberry Pi işlemcisinin güç tüketiminin benzer olduğu ve yan kanal sızıntısı vermediği gözlemlenmiştir. Raspberry pi mikrobilgisayarının sıradan bilgisayarlara göre güç tüketiminin çok düşük olması yan kanal saldırılarına karşı direncini arttırdığı belirtilmiştir [31]. Kaos tabanlı çalışmalar incelendiğinde ise Pareschi vd.

Tablo 6. Şifreleme & Şifre Çözme sürelerinin literatür ile kıyaslanması (sn)
(Comparison of encryption-decryption time with literature (sec))

Görüntünün Boyutu	Li ve vd. (2018)	Sahari vd. (2018)	Ullah vd. (2017)	Cavusoglu vd. (2018)	Geliştirilen Sistem
256x256		0,34 & 0,36	0,4071 & -	4,438 & 4,234	0,23 & 0,20
512x512	0,926 & 1,081	0,52 & 0,58	1,5619 & -	-	-

yaptıkları çalışmada kaos tabanlı rasgele sayılar ile yapılan şifrelemenin kullanılan kaotik yöntemin rassal sayılar üretmesinden dolayı güç analizine dayalı bir yan kanal saldırısından bilgi elde etmenin mümkün olmadığını göstermişlerdir. Yapılan çalışmaya göre Rastgele sayı üretecinden elde edilen sayılarla yapılan şifreleme uygulamasının yüksek güvenlikli olduğu sonucu elde edilmiştir. [32].

Bu makalede gerçekleştirilen şifreleme uygulamasında mikrobilgisayar üzerinde kaos tabanlı RSÜ tasarımı ile şifreleme işlemi yapılmaktadır. Yukarıda açıklandığı üzere literatürdeki çalışmalar göz önüne alındığında mikrobilgisayar üzerinde gerçeklenen kaos tabanlı üretilen rastgele sayıların kullanıldığı bir şifreleme uygulamasının sırasında uygulama ataklarına karşı yeterince güvenli olduğu söylenebilir.

6. SİSTEMİN PERFORMANS ANALİZİ
(PERFORMANCE ANALYSIS)

Yapılan tüm işlemler ve analizler Linux tabanlı Raspbian işletim sistemi üzerinde ARM Cortex-A53, CPU 1,4 GHz ve 1 GB belleğe sahip bir Raspberry Pi 3 (Model B +) üzerinde yapıldı. Damar görüntülerinin görüntü işleme teknikleri ile iyileştirilmesi, önerilen yeni kaotik sistem kullanılarak rastgele sayıların elde edilmesi, üretilen rasgele sayılar ile biyometride kullanılan damar görüntülerinin şifrelenmesi ve şifre çözme işlemleri ile tüm analizler açık kaynak kodlu Python 3.4.4 ve OpenCV 3.4.1 görüntü işleme kütüphaneleri kullanılarak gerçekleştirilmiştir. Simülasyon sonuçlarına göre 256 × 256 piksel 8 bit gri seviye damar görüntüsü için, ortalama şifreleme süresinin 0,23 s ve ortalama şifre çözme süresinin 0,20 s olduğu tespit edilmiştir. Ayrıca Tablo 6, literatürde bulunan benzer dört eserle süre kıyaslamalarını göstermektedir. Karşılaştırma sonucunda, önerilen yeni kaotik sistem ile gerçekleştirilen şifreleme-şifre çözme işlemlerinin Tablo 6'da gösterilen diğer kripto sistemlerden çok daha hızlı olduğu görülmüştür. Li vd. yaptıkları çalışmada yeni bir hiperkaotik lorenz sistemi kullanarak görüntüleri şifrelemişlerdir [33]. Sahari vd. ise yaptıkları çalışmada, parçalı ve lojistik haritaları birleştirerek elde ettikleri yeni bir 3 boyutlu kaotik sistem ile görüntü şifreleme işlemini yapmışlardır. Ürettikleri rasgele sayılar NIST 800-22 rasgelelik testlerinden başarıyla geçmiştir [34]. Yapılan diğer bir çalışmada S-Box ile kaotik sistem kullanılarak görüntü şifreleme işlemi gerçekleştirilmiştir. Veri aktarma güvenliğinin arttırılması amacıyla kaotik sistem ile beraber S-Box yöntemi kullanılmıştır. Bu yöntem sayesinde gürültü ve veri kaybı saldırılarına karşı dayanıklı bir sistem elde edilmiştir [35]. Çavuşoğlu vd. ise yaptıkları çalışmada güvenli ve etkili görüntü şifreleme için yeni bir kaos tabanlı hibrit şifreleme algoritması tasarımı sunmuşlardır. Algoritmayı tasarlamak için, Zhongtang kaotik sistemi zengin dinamik özellikleri nedeniyle seçilmiş ve dinamik analizleri yapılmıştır. Kaotik sistemden üretilen rasgele sayılar rastgelelik testlerinden başarıyla geçmiştir. Tasarlanan rastgele sayı üreteci ve S-Box üretim algoritmalarını kullanarak yeni bir hibrit görüntü şifreleme algortiması geliştirilmiştir [36].

7. SONUÇLAR VE TARTIŞMALAR
(RESULTS AND DISCUSSIONS)

Bu makale çalışmasında kızılötesi kamera yardımıyla kişilerden alınan el üstü damar görüntüleri mikrobilgisayara aktarılıp çeşitli önişlemlerden geçirilerek [37] kaos tabanlı olarak şifrelenmiş ve güvenlik analizleri yapılmıştır. Damar görüntüleri tıpkı parmak izi gibi kişiden kişiye farklılık göstermektedir. Bu nedenle bu verilerin gizlenmesi biyometrik tanıma sisteminin güvenliği açısından çok önemlidir. Çalışma kapsamında sistemin güvenliğini sağlamak için bu görüntüler şifreli bir şekilde veri tabanında saklanmıştır. Görüntülerin güvenliği için yeni bir kaos tabanlı rasgele sayı üreteci tasarlanmıştır. Raspberry Pi 3 platformunda geliştirilen yeni kaotik sistemin x, y ve z fazlarından üretilen rasgele sayılar, uluslararası düzeyde kabul gören NIST-800-22 ve ENT testlerinden başarıyla geçmiş olup 3 fazda da rasgeleliği sağladığı görülmüştür. Şifreleme kısmında ise üretilen rastgele sayılar ile şifreleme işlemi gerçekleştirilmiştir. Şifreleme sonrası elde edilen görüntüler ile ön işlemden geçirilmiş damar görüntüleri histogram, korelasyon, entropi, NPCR ve UACI analizlerinden geçirilmiş ve yapılan şifrelemenin başarılı olduğu görülmüştür. Literatürdeki çalışmalar göz önüne alındığında mikrobilgisayar üzerinde gerçeklenen kaos tabanlı üretilen rastgele sayıların kullanıldığı bir şifreleme uygulamasının uygulama ataklarına karşı da yeterince güvenli olduğu söylenebilir. Gerçekleştirilen çalışma ile kimlik tanıma sistemlerinde de kullanılabilen el üstü damar görüntülerinin mobil olarak güvenli bir şekilde kullanılabileceği gösterilmiştir. Ayrıca gerçekleştirilen tasarım, çeşitli medikal görüntülerde ve diğer bilgi güvenliğinin gerektiği yerlerde de mobil olarak kullanılabilir.

TEŞEKKÜR (ACKNOWLEDGEMENT)

Bu çalışma Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) tarafından, "3001- Başlangıç Ar-Ge Projeleri Destekleme Programı" kapsamında, 117E284 numaralı proje ile desteklenmiştir. Bu çalışma ayrıca Sakarya Üniversitesi Girişimsel Olmayan Araştırmalar Etik Kurulu tarafından kabul edilmiştir (no.71522473 /050.01.04 /341).

KAYNAKLAR (REFERENCES)

1. Lee E.C., Jung H., Kim D., Infrared Imaging Based Finger Recognition Method. In Proceedings of International Conference on Convergence and Hybrid Information Technology, Korea, 228-230, August, 2010.
2. Yang W. Wang S., Hu J., Zheng G., Valli C., A fingerprint and finger-vein based cancelable multi-biometric system, Pattern Recognition, 78, 242-251, 2018.
3. Wang L., Leedham G., Cho D.S.Y., Minutiae feature analysis for infrared hand vein pattern biometrics, In: Pattern Recognition. Part Special Issues in The Journal of the Pattern Recognition Society, 41 (3), 920–929, 2008.
4. Tanaka T., Kubo N., Biometric authentication by hand vein patterns, SICE, Annual Conference in Sapporo, 249-253, August, 2004.
5. Wang J., Wang G., Li M., Du W., Hand vein recognition based on PCET, Optik-International Journal for Light and Electron Optics, 127(19), 7663-7669, 2016.
6. Liu Z.H., Yin J., Jin Z., An adaptive feature and weight selection method based on gabor image for face recognition, Acta Photonica Sin, 40 (4), 636–641, 2011.
7. Chai X., Gan Z., Chen Y., Zhang Y., A visually secure image encryption scheme based on compressive sensing, Signal Processing, 134, 35–51, 2017.
8. Hua Z., Zhou Y., Design of image cipher using block-based scrambling and image filtering, Informations Sciences, 396, 97–113, 2017.
9. Dzwonkowski M., Papaj M., Rykaczewski R., A new quaternion-based encryp- tion method for DICOM images, IEEE Trans., Image Process., 24 (11), 4614–4622, 2015.
10. Mildenberger P., Eichelberg M., Martin E., Introduction to the DICOM standard, Eur. Radiol., 12 (4), 920–927, 2002.
11. Zhang Y., Xiao D., An image encryption scheme based on rotation matrix bit-level permutation and block diffusion, Communications in Nonlinear Science and Numerical Simulation, 19 (1), 74–82, 2014.
12. Zhang L.B., Zhu Z.L., Yang B.Q., Liu W.Y., Zhu H.F., Zou M.Y., Medical image encryption and compression scheme using compressive sensing and pixel swapping based permutation approach, Mathematical Problems in Engineering, 2015.
13. Akkaya S., Pehlivan I., Akgul A., Varan M., The design and application of bank authenticator device with a novel chaos based random number generator. Journal of the Faculty of Engineering and Architecture of Gazi University, 33 (3), 1172-1182, 2018.
14. Pehlivan I., Kurt E., Lai Q., Basaran A., Kutlu M., A Multiscroll Chaotic Attractor and its Electronic Circuit Implementation, Chaos Theory and Applications, (1), 29-37, 2019.
15. Ozdemir A., Pehlivan I., Akgul A., Guleryuz E., A strange novel chaotic system with fully golden proportion equilibria and its mobile microcomputer-based RNG application, Chinese Journal of Physics, 2018.
16. Çavuşoğlu Ü., Uyaroğlu Y., Pehlivan İ., Design of a continuous-time autonomous chaotic circuit and application of signal masking. Journal of the Faculty of Engineering and Architecture of Gazi University, 29 (1), 79-87, 2014.
17. Akgul A., Pehlivan I., A New Three-Dimensional Chaotic System Without Equilibrium Points, İts Dynamical Analyses And Electronic Circuit Application, Tehnicki Vjesnik-Technical Gazette, 209-214, 1330-3651, 2016.
18. Lu J., Chen G., Zhang S., Dynamical analysis of a new chaotic attractor, International Journal of Bifurcation and Chaos, 12(5), 1001-1015, 2002.
19. Sprott J.C., A new class of chaotic circuit, Physics Letters A, 266(1), 19-23, 2000.
20. Tuna M., Fidan C. B., A Study on the importance of chaotic oscillators based on FPGA for true random number generating (TRNG) and chaotic systems. Journal of the Faculty of Engineering and Architecture of Gazi University, 33 (2), 473-491, 2018.
21. Boyraz Ö. F., Yildiz M. Z., Mobil Damar Görüntüleme Cihazı Tasarımı, In 4th International Symposium on Innovative Technologies in Engineering and Science (ISITES2016), 3-5, November, 2016.
22. Sato S., Sano M., Sawada 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.
23. Tuna M., Fidan C., A Study on the importance of chaotic oscillators based on FPGA for true random number generating (TRNG) and chaotic systems, Journal of the Faculty of Engineering and Architecture of Gazi University, 33 (2), 473-492, 2018.
24. Koyuncu İ., Kriptolojik Uygulamalar İçin Fpga Tabanlı Yeni Kaotik Osilatörlerin Ve Gerçek Rasgele Sayı Üreteçlerinin Tasarımı Ve Gerçeklenmesi, Doktora Tezi, Sakarya Üniversitesi, Fen Bilimleri Enstitüsü, 2014.
25. http://www.fourmilab.ch/random/, Yayın tarihi Ocak 28, 2008. Erişim Tarihi Temmuz 18, 2018.
26. Stoyanov B., Kordov K., A novel pseudorandom bit generator based on chirikov standard map filtered with shrinking rule, Mathematical Problems in Engineering, 1-4, 2014.
27. Seetharam D., Rhee S., An efficient pseudo random number generator for low-power sensor networks wireless networks, In Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks, 2004.
28. Akhshani A,. Akhavan A., Mobaraki A., Lim S., Hassan Z., Pseudo random number generator based on quantum chaotic map, Communications in Nonlinear Science and Numerical Simulation, 19 (1), 101-111, 2014.
29. E. Hatun, E. Buyukkaya, and S. B. O. Yalcin, Electromagnetic radiation analysis of implementation of RSA algorithm on a Raspberry Pi, 2018 26th Signal

Processing and Communications Applications Conference (SIU), 2018.

30. E. Hatun, E. Buyukkaya, and M. A. Evci, Side Channel Analysis of Raspberry Pi with AES Algorithm and Measurement Improvement, 2019 27th Signal Processing and Communications Applications Conference (SIU), 2019.

31. F. Pareschi, G. Scotti, L. Giancane, R. Rovatti, G. Setti, and A. Trifiletti, Power analysis of a chaos-based Random Number Generator for cryptographic security, 2009 IEEE International Symposium on Circuits and Systems, 2009.

32. A. Sanada, Y. Nogami, K. Iokibe, and M. A.-A. Khandaker, Security analysis of Raspberry Pi against Side-channel attack with RSA cryptography, 2017 IEEE International Conference on Consumer Electronics - Taiwan (ICCE-TW), 2017.

33. Li Z., Peng C., Li L., Zhu X., A novel plaintext-related image encryption scheme using hyper-chaotic system, Nonlinear Dynamics, 94 (2), 1319-1333, 2018.

34. Sahari M.L., Boukemara I., A pseudo-random numbers generator based on a novel 3D chaotic map with an application to color image encryption, Nonlinear Dynamics, 94 (1), 723-744, 2018.

35. Ullah A., Jamal S.S., Shah T., A novel scheme for image encryption using substitution box and chaotic system, Nonlinear Dynamics, 91 (1), 359-370, 2018.

36. Çavuşoğlu Ü, S. Kaçar, A. Zengin, İ. Pehlivan, A novel hybrid encryption algorithm based on chaos and S-AES algorithm, Nonlinear Dynamics, 92 (4), 1745-1759, 2018.

37. Yildiz M.Z., Boyraz Ö.F., Development of a low-cost microcomputer based vein imaging system, Infrared Physics & Technology, 98, 27-35, 2019.