CHAOS
Theory and Applications
in Applied Sciences and Engineering

e-ISSN: 2687-4539
RESEARCH ARTICLE
Vol.3 / No.1 / 2021 / pp.3-10
https://doi.org/10.51537/chaos.717432

A Chaos-Based Encryption Application for Wrist Vein Images

Ömer Faruk Boyraz [*,1], Murat Erhan Çimen [*,2], Emre Güleryüz [*,3] and Mustafa Zahid Yıldız [*,4]
[*]Department of Electrical & Electronics Engineering, Faculty of Technology, Sakarya University of Applied Sciences, 54187 Serdivan, Sakarya, Turkey.

ABSTRACT In this study, the images of the wrist vein taken from the individuals were subjected to various preprocessings and then encrypted with random numbers obtained from the chaotic system. Before encryption, random numbers were generated using a chaotic system. The random numbers produced have successfully passed the NIST 800-22 tests. Images encrypted with random numbers were subjected to security analysis such as correlation, NPCR, UACI and histogram analysis. With the study carried out, it has been shown that wrist vein patterns that can be used in authentication systems can be safely stored in the database.

KEYWORDS
Wrist vein image
Chaotic system
Random number generator
Encryption
Security analysis

INTRODUCTION

Biometrics allows individuals to classify individuals based on different physiological and behavioral characteristics, such as fingerprints, iris, manner of walking, and patterns of movement. While physiological features such as fingerprints, palm prints, iris are linked to the form of the body, behavioral features such as voice, handwriting signature, and walking are linked to the model of behavior of the person. (Lee *et al.* 2010). The near infrared wavelength is absorbed by the hemoglobin in the blood, and the region of vein near the skin are displayed darker with the infrared camera. Identification process from the vein pattern; It can be performed on various images such as dorsal hand vein pattern (Yildiz and Boyraz 2019), finger vein pattern (Cho *et al.* 2012), palm vein pattern (Raut *et al.* 2017) and wrist vein pattern (Niyaz *et al.* 2017).

Among the four different types of vascular patterns, the wrist vein pattern provides a clear view due to its close proximity to the outer skin and its intensive presence.

Wrist vascular biometry has not been studied much in the literature. In their study, Akhloufi and colleagues obtained the vascular network structures in the forearm wrist region through a CCD infrared camera. Anisotropic diffusion process was applied to improve the contrast of the images obtained, and then segmented the vascular network structures using morphological processes (Akhloufi and Bendada 2008).

Thanks to the lighting system and infrared camera platform designed by Pascual et al., they collected hand-wrist vein images and showed that these images are clear enough to be used for identification (Pascual *et al.* 2010).

Wrist vein are used in the process of personal identification. The advantage of performing touchless wrist vein recognition processes over other pattern recognition systems (touch based fingerprint, palm, finger vein, etc.) is the ability to conduct touchless identification and verification operations during image acquisition. In this way, in a more sterile setting, identification is achieved. Such advantages make touchless wrist vein recognition technology a more accurate and promising system that attracts increasing attention in security systems, hospitals, courthouses, banks, public institutions and industry.

Manuscript received: 9 April 2020,
Revised: 31 August 2020,
Accepted: 24 September 2020.

[1] oboyraz@subu.edu.tr (**Corresponding Author**)
[2] muratcimen@subu.edu.tr
[3] emre.guleryuz1@ogr.sakarya.edu.tr
[4] mustafayildiz@subu.edu.tr

Consequently, it is a crucial issue to secure fingerprint image transmission over the internet and its access in the open network environment. Therefore, it is very important to protect and store touchless wrist vein images by encrypting them.

Several technologies have been developed to secure and store various groups of images so far. Among these technologies, the chaos-based encryption method is the most intuitive and effective way to turn images into unrecognizable (Chai *et al.* 2017). Several image encryption algorithms have recently been proposed that can be used to preserve images at a high level of protection (Hua and Zhou 2017).

Dzwonkowski et al. presented an encryption scheme that uses quaternion to protect the image of DICOM (Digital Imaging and Communications in Medicine) (Dzwonkowski *et al.* 2015). Hsiao et al. Encrypted their contact fingerprint images using 2 different chaotic systems (Hsiao and Lee 2015). Random numbers produced using multiple chaotic system passed NIST SP 800-22a test. Zhang et al. proposed a medical image encryption and compression algorithm using the compression detection and pixel permutation approach. This algorithm will simultaneously encrypt and compress medical images. (Zhang *et al.* 2015).

Yildiz et al., In their study, encrypted the hand vein images that converted into 1 bit with a new encryption algorithm and stored them in the database (Yildiz *et al.* 2019).The SURF matching algorithm was used in the encrypted images.

In this study, wrist vein images taken from people with the help of infrared camera were subjected to various preprocesses on the microcomputer and it was aimed to store the vein images safely in the database since it is a personal data. After the wrist vein images were pretreated, they were encrypted by eXclusive OR (XOR) processing with random numbers obtained using the chaotic system.

MATERIAL AND METHOD

Material

Right and left hand wrist vein images obtained from a total of 50 volunteers from 20 females and 30 males used in the study were collected by the device shown in Figure 1. Volunteers were asked to place their wrists on the hand placement platform illuminated by infrared power leds with 850 nm wavelength and images were taken via an infrared camera.

The obtained images were transferred to the microcomputer environment and were subjected to image preprocessing and encryption algorithms, respectively. The encrypted images are securely stored in the database in the microcomputer environment.

Method

The block diagram of encryption of wrist vein images in microcomputer environment is shown in Figure 2. Hand-wrist vein images taken with the help of infrared camera were subjected to gray level conversion and contrast limited adaptive histogram equalizition processes, respectively. These images were then encrypted using random numbers obtained using the chaotic system.

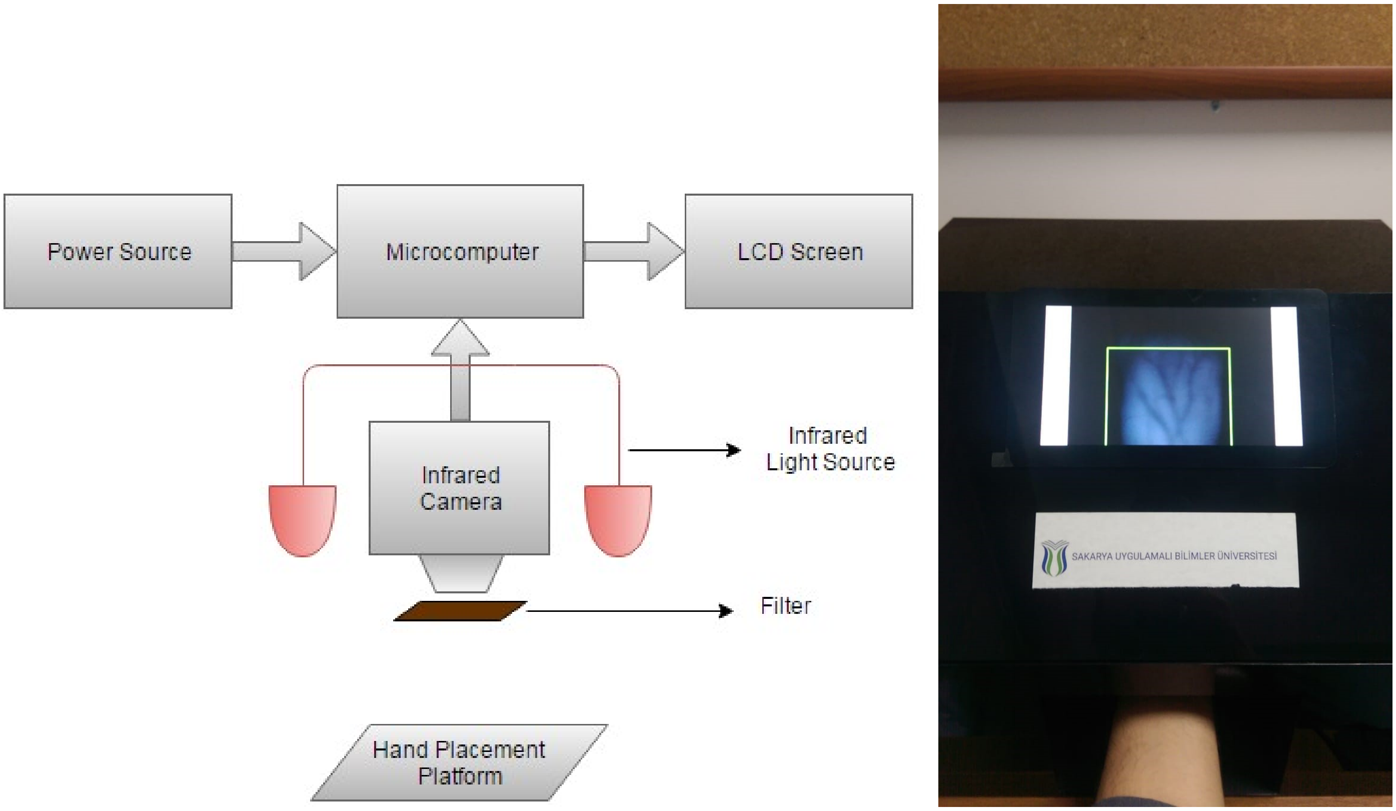
In this research, the chaotic system used is a continuous time, a chaotic 3-dimensional balance point system (Akgül *et al.* 2020). The system consists of 3 different differential equations as given in equation 1. There are three state variables in the system: x, y, z, and a total of four parameters: a, b, c, d. In order for the system to be chaotic, initial conditions are determined as x(0) = 0.4, y(0) = 0.1, z(0) = 0.

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

For the system given in Equation 1, the parameters show a chaotic feature when a = 1.9, b = 1.1, c = 11.5 and d = 0.7. In Equation 2, the parameters of the chaotic system are shown.

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

There are several techniques of research to understand whether or not a system is chaotic. The analysis of the system's behavior (time series), phase portraits, lyapunov exponentials, bifurcation diagrams over a certain period of time are some of these analysis methods. As a result of these analyzes, the system has been shown to exhibit chaotic behavior (Akgül *et al.* 2020).



(a)

(b)

Figure 1 a)Block diagram of system (Boyraz and Yildiz 2016) b)Collection of hand-wrist images from volunteers

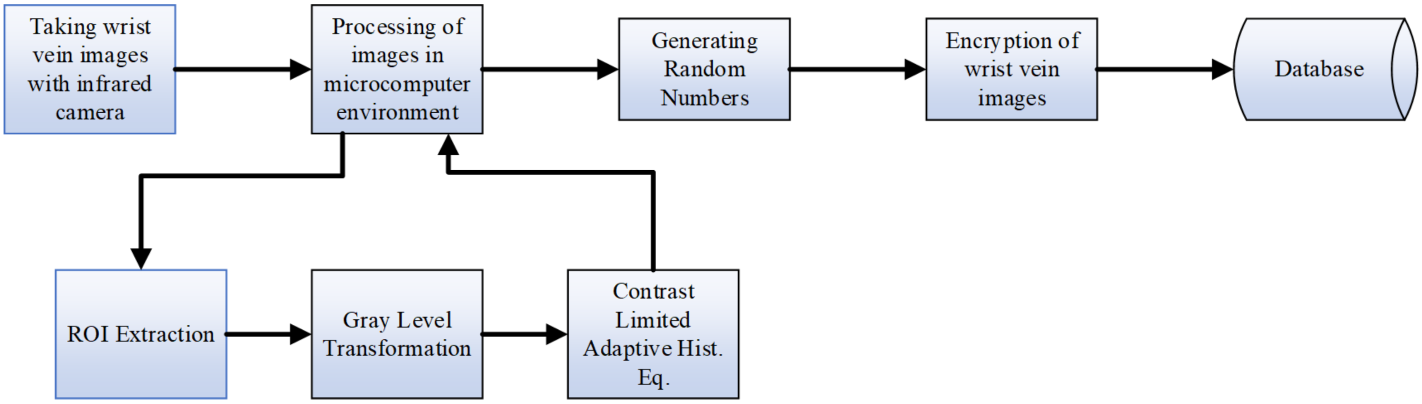

Taking wrist vein images with infrared camera
Processing of images in microcomputer environment
Generating Random Numbers
Encryption of wrist vein images
Database
ROI Extraction
Gray Level Transformation
Contrast Limited Adaptive Hist. Eq.

Figure 2 Block diagram of encryption of Hand-Wrist Vein images

PRE-PROCESSING OF WRIST IMAGES

Contrast improvement is aimed in the pre-processing process. The target area was removed from the wrist images taken with the help of the infrared camera, and then the contrast-limited adaptive histogram equalization was performed to make the vascular areas more visible.

The acquired images were first converted to gray level, and the areas of the vein were clarified by applying contrast-limited histogram equalization (CLAHE) method (Stimper *et al.* 2019). This method is used both on noise reduction and on medical images to eliminate the edge shadow effects in homogeneous areas. Figure 3 shows the vascular area, which has been converted to a gray level and the contrast has been improved with the CLAHE method. As a result of these processes, the stage before the 8-bit level encryption has been reached.

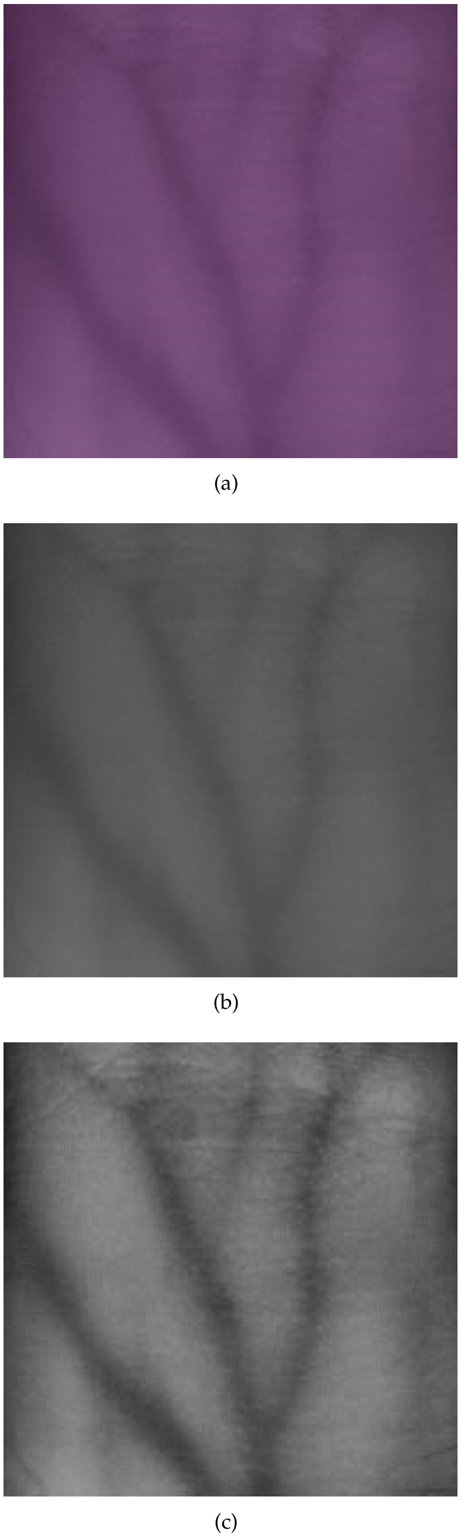
In Table 2 NPCR and UACI analyzes between the encrypted image and the 8-bit wrist image are given. According to the analysis, it is concluded that almost all the pixels of the 8-bit wrist image are changed and the image that is encrypted using random numbers produced from the chaotic 1system is formed. UACI results express the density of the changing pixels.

NIST 800-22 TESTS FOR RANDOMNESS

NIST-800-22 test was used to perform randomness tests of the produced numbers. The NIST-800-22 test bit sequence must pass all of these tests successfully to be considered successful. The NIST-800-22 test contains 16 different statistical tests which define the randomness of the bit sequences (Akgül *et al.* 2019). As all the numbers passed the test, it was concluded, according to Table 1. Randomness was obtained by random numbers created from the last 8 bits of the x, y and z values.

ENCRYPTION OF WRIST VEIN IMAGES

The flow chart showing the encryption of 8-bit vein images using random numbers produced is given in Figure 4. The wrist vein images taken are given to the system for encryption first. Then the dimensions of this image are calculated. Pixel values in each coordinate are converted to an 8-bit binary level. Number sequences converted into 8-bit binary level are subjected to XOR processing with random numbers generated from the chaotic system. After this process, the values formed are converted to decimal system and the pixel values of the encrypted image are obtained.



(a)

(b)

(c)

Figure 3 a) Raw image b) Gray Level c) CLAHE

Table 1 NIST-800-22 test results

Statistical Tests	P-value (X_8bit)	P-value (Y_8bit)	P-value (Z_8bit)	Results
The Frequency Test	0.3547	0.5425	0.4879	Successful
Frequency Test within a Block	0.4578	0.7421	0.6444	Successful
The Cumulative Sums Test	0.5412	0.3478	0.3789	Successful
The Runs Test	0.2879	0.3456	0.4785	Successful
Tests for the Longest-Run-of-Ones in a Block	0.6789	0.3127	0.1987	Successful
The Binary Matrix Rank Test	0.7214	0.4879	0.3414	Successful
The Discrete Fourier Transform Test	0.1754	0.1424	0.4232	Successful
The Non-overlapping Template Matching Test	0.7543	0.0425	0.1074	Successful
The Overlapping Template Matching Test	0.1987	0.7562	0.3412	Successful
Maurer’s Universal Statistical Test	0.7521	0.4017	0.3478	Successful
The Aproximate Entropy Test	0.1789	0.3485	0.6147	Successful
The Random Excursions Test (x = -4)	0.6755	0.3478	0.1977	Successful
The Random Excursions Variant Test (x = -9)	0.6478	0.3974	0.2476	Successful
The Serial Test-1	0.7213	0.3456	0.4102	Successful
The Serial Test-2	0.7620	0.4397	0.3157	Successful
The Linear Complexity Test	0.3024	0.3789	0.4987	Successful

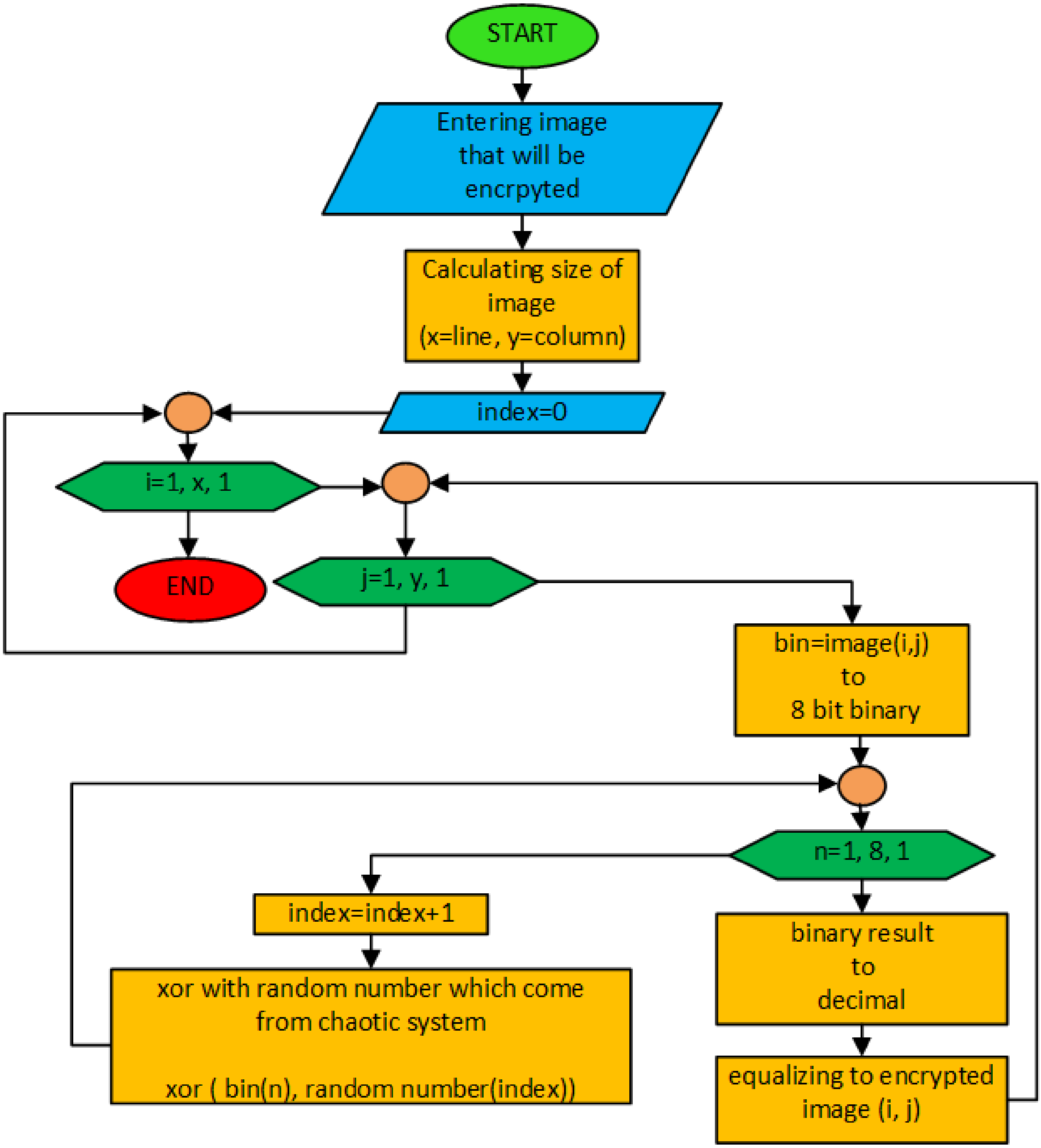


Figure 4 The Encryption Algorithm flowchart

SECURITY ANALYSIS

In this section, encryption operations are realized with random numbers produced from the chaotic system. The system's security analysis was performed using entropy, differential attack (NPCR, UACI), correlation and histogram methods after encryption. Figure 5 shows histogram analysis and correlation analysis of the encrypted wrist image. As a result of encryption, the correlation and histogram distributions of the images are homogeneous, indicating that the encryption is successful.

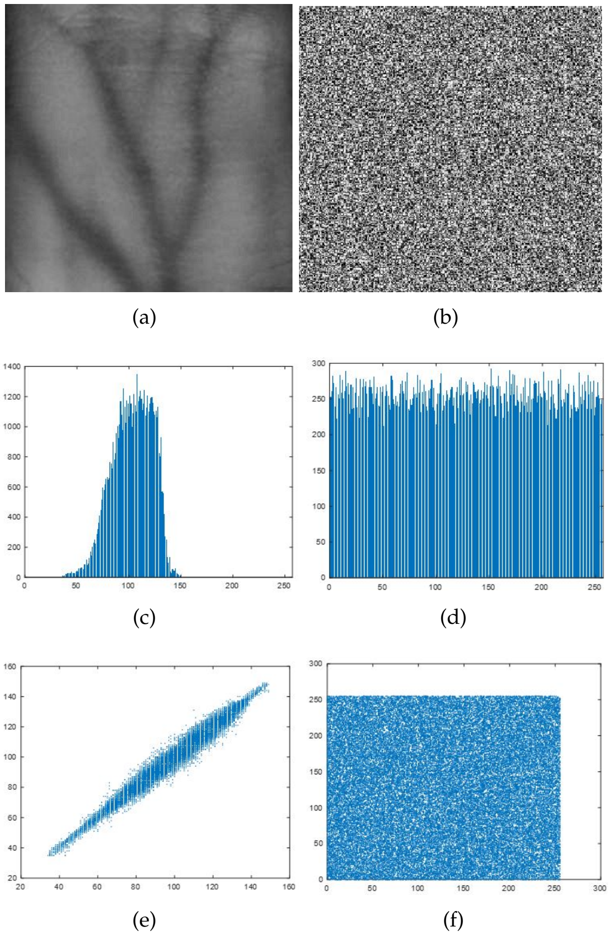


Figure 5 a) Wrist vein image b) Encrypted wrist image c) Histogram distributions of Wrist vein d) Encrypted histogram distributions of Wrist vein e) Correlation map of wrist vein image f) Correlation map of encrypted wrist image

Table 2 Security analysis for sample images

Sample Images	NPCR	UACI
1. Encrypted image	99.7894	29.4785
2. Encrypted image	100	28.9789
3. Encrypted image	99.8974	29.7454

CONCLUSION

In this article, the wrist vein images taken from people with the help of infrared camera are transferred to microcomputer, passed through various preprocesses, encrypted as chaos-based and security analysis are performed. Vein images vary from individual to individual, much like fingerprints. Hiding these data is therefore very necessary for the protection of the biometric recognition system. These images are encrypted and stored in the database to ensure the system's protection. Random numbers produced from the x, y and z phases of the chaotic system have successfully passed the internationally accepted NIST-800-22 tests Rukhin *et al.* (2001) and have been found to provide randomness in all 3 phases. In the encryption part, the encryption process was performed with random numbers generated. The images obtained after encryption and the pretreated vein images were analyzed by histogram, correlation, entropy, NPCR and UACI analysis and the encryption was successful.

Conflicts of interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

LITERATURE CITED

Akgül, A., C. Arslan, and B. Arıcıoğlu, 2019 Design of an interface for random number generators based on integer and fractional order chaotic systems. Chaos Theory and Applications **1**: 1–18.

Akgül, A., M. Z. Yıldız, Ö. F. Boyraz, E. Güleryüz, S. Kaçar, *et al.*, 2020 Doğrusal olmayan yeni bir sistem ile damar görüntülerinin mikrobilgisayar tabanlı olarak şifrelenmesi. Journal of the Faculty of Engineering & Architecture of Gazi University **35**.

Akhloufi, M. and A. Bendada, 2008 Hand and wrist physiological features extraction for near infrared biometrics. In *2008 Canadian Conference on Computer and Robot Vision*, pp. 341–344, IEEE.

Boyraz, Ö. F. and M. Z. Yildiz, 2016 Mobil damar görüntüleme cihazı tasarımı. In *4th International Symposium on Innovative Technologies in Engineering and Science (ISITES2016) 3-5 Nov 2016 Alanya/Antalya-Turkey*.

Chai, X., Z. Gan, Y. Chen, and Y. Zhang, 2017 A visually secure image encryption scheme based on compressive sensing. Signal Processing **134**: 35–51.

Cho, S. R., Y. H. Park, G. P. Nam, K. Y. Shin, H. C. Lee, *et al.*, 2012 Enhancement of finger-vein image by vein line tracking and adaptive gabor filtering for finger-vein recognition. In *Applied Mechanics and Materials*, volume 145, pp. 219–223, Trans Tech Publ.

Dzwonkowski, M., M. Papaj, and R. Rykaczewski, 2015 A new quaternion-based encryption method for dicom images. IEEE Transactions on Image Processing **24**: 4614–4622.

Hsiao, H.-I. and J. Lee, 2015 Fingerprint image cryptography based on multiple chaotic systems. Signal Processing **113**: 169–181.

Hua, Z. and Y. Zhou, 2017 Design of image cipher using block-based scrambling and image filtering. Information Sciences **396**: 97–113.

Lee, E., H. Jung, and D. Kim, 2010 Infrared imaging based finger recognition method. In *Proceedings of International Conference on Convergence and Hybrid Information Technology*, pp. 228–230.

Niyaz, O., Z. G. Cam, and T. Yildirim, 2017 Wrist vein recognition by ordinary camera using phase-based correspondence matching. In *Modelling, Identificat. Control*, pp. 89–93.

Pascual, J. E. S., J. Uriarte-Antonio, R. Sanchez-Reillo, and M. G. Lorenz, 2010 Capturing hand or wrist vein images for biometric authentication using low-cost devices. In *2010 Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pp. 318–322, IEEE.

Raut, S. D., V. Humbe, and A. V. Mane, 2017 Development of biometrie palm vein trait based person recognition system: Palm vein biometrics system. In *2017 1st International Conference on Intelligent Systems and Information Management (ICISIM)*, pp. 18–21, IEEE.

Rukhin, A., J. Soto, J. Nechvatal, M. Smid, and E. Barker, 2001 A statistical test suite for random and pseudorandom number generators for cryptographic applications. Technical report, Booz-allen and hamilton inc mclean va.

Stimper, V., S. Bauer, R. Ernstorfer, B. Schölkopf, and R. P. Xian, 2019 Multidimensional contrast limited adaptive histogram equalization. IEEE Access **7**: 165437–165447.

Yildiz, M. Z., O. Boyraz, E. Guleryuz, A. Akgul, and I. Hussain, 2019 A novel encryption method for dorsal hand vein images on a microcomputer. IEEE Access **7**: 60850–60867.

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

Zhang, L.-b., Z.-l. Zhu, B.-q. Yang, W.-y. Liu, H.-f. Zhu, *et al.*, 2015 Medical image encryption and compression scheme using compressive sensing and pixel swapping based permutation approach. Mathematical Problems in Engineering **2015**.

How to cite this article: Boyraz, O. F., Cimen, M. E., Guleryuz, E. and Yildiz, M. Z. A Chaos-Based Encryption Application for Wrist Vein Images. Chaos Theory and its Application, 3(1), 3-10, 2021.