IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received April 10, 2019, accepted April 28, 2019, date of publication May 3, 2019, date of current version May 21, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2914721

A Novel Encryption Method for Dorsal Hand Vein Images on a Microcomputer

M. Z. YILDIZ[1], O. F. BOYRAZ[1], E. GULERYUZ[1], A. AKGUL[1], AND I. HUSSAIN[2]
[1]Department of Electrical & Electronics Engineering, Faculty of Technology, Sakarya University of Applied Sciences, 54187 Sakarya, Turkey
[2]Department of Mathematics, Statistics and Physics, Qatar University, Doha 2713, Qatar

Corresponding author: I. Hussain (iqtadarqau@qu.edu.qa)

This work was supported by the Qatar National-Library.

ABSTRACT In this paper, a Lorenz-like chaotic system was developed to encrypt the dorsal hand patterns on a microcomputer. First, the dorsal hand vein images were taken from the subjects via an infrared camera. These were subjected to two different processes called contrast enhancement and segmentation of vein regions. Second, the pre- and post-processed images were encrypted with a new encryption algorithm in the microcomputer environment. For the encryption process, random numbers were generated by the chaotic system. These random numbers were subjected to NIST-800-22 test which is the most widely accepted statistical test suite. The speeded up robust feature (SURF) matching algorithm was utilized in the initial condition sensitivity analysis of the encrypted images. The results of the analysis have shown that the proposed encryption algorithm can be used in identification and verification systems. The encrypted images were analyzed with histogram, correlation, entropy, pixel change rate (NPCR), initial condition sensitivity, data loss, and noise attacks which are frequently used for security analyses in the literature. In addition, the images were analyzed after noise attacks by means of peak signal-to-noise ratio (PSNR), mean square error (MSE), and the structural similarity index (SSIM) tests. It has been shown that the dorsal hand vein images can be used in identification systems safely with the help of the proposed method on microcomputers.

INDEX TERMS Chaotic Encryption, random number generator, near-infrared imaging, SURF, hand vein imaging, microcomputer, raspberry pi.

I. INTRODUCTION

Biometry allows people to be differentiated between individuals according to their various physiological and behavioral characteristics such as iris, fingerprint, face shape and movement patterns. Physiological features such as fingerprints, facial shapes are related to the shape of the body, whereas behavioral characteristics such as signature, tone of voice, and forms of movement are related to the behavior model of the person [1].

Biometry technology is unique in terms of physiological or behavioral characteristics, and much safer compared to traditional knowledge-based descriptors, such as passwords, pin codes, because it is difficult to be lost or reproduced. In recent years, there has been a significant increase in the use of copied fingerprints, fake iris scales or sophisticated face masks [2].

Surgically changing the vein pattern under the skin is extremely difficult [3], [4]. Therefore, a biometric system using the dorsal hand vein pattern which differs from person to person is extremely safe. Since it is difficult to obtained dorsal hand vein patterns under visible light, the use of vein patterns in authentication applications is appropriate.

In comparison with pattern recognition systems such as fingerprints, palm print, and finger vein, the main advantage of identification and verification from the dorsal vein patterns is the ability to perform non-contact operations without touching any apparatus during the acquisition of the images [5]–[8]. Therefore the proposed system is more steril than any other authentication system when it is compared.

To date, many technologies have been developed and implemented to store and protect different groups of images. Among these technologies, chaotic encryption is one of the most effective way to make images indistinguishable [9]–[14].

The associate editor coordinating the review of this manuscript and approving it for publication was Kathiravan Srinivasan.

Recently, many image encryption algorithms have been proposed that can be used in high-secure encryption of medical images [15]–[18]. Cao *et al.* presented an encryption algorithm for medical images using edge maps derived from a source image [19]. Dai *et al.* proposed an encryption algorithm for medical images based on confusion and diffusion processes which are realized by Arnold's transformation and the use of two chaotic systems [20]. Laiphrakpam and Khumanthem developed an encryption scheme on medical images using the improved ElGamal encryption technique [21]. In their study, Hua et al. provide a new encryption scheme for the protection of medical images [22] and it was shown that the encryption performance was high and the data loss was minimized. In a study by Zhu *et al.* proposed a computational ghost imaging encryption method based on a fingerprint phase mask [23].

Since Lorenz modeled the forecast of weather events in 1963, chaotic systems have been involved in many engineering fields. Chaotic systems have been used in many different areas [24]–[29]. The most commonly used fields are engineering, population distribution, finance and encryption [30]. There are many analysis methods to check whether a system is chaotic or not. Lyapunov exponents, time series, phase portraits, equilibrium point analysis, bifurcation analysis are the main analysis methods used in the literature [31]. In recent years, different and novel chaotic systems have been presented to be used in practical applications [32]–[38].

Since random number generators have some crucial roles in cryptological applications, they have been used in various fields such as statistics, simulation, cryptography, modeling, numerical analysis [39]. Cicek et al. presented an electronic circuit design by performing dynamic analysis and numerical simulation of a 3-dimensional continuous time chaotic system and performed secure communication applications [40]. In another study, Çiçek *et al.* developed a discrete-time chaos-based random number generator using skew tent map with optimum parameter values that ensure maximum randomness [41]. Park *et al.* produced a real random number generator from the CMOS Boolean chaotic oscillator [42]. Koyuncu and Özcerit designed an FPGA based real random number generator using a 3-D chaotic system [43].

In this study, a new encryption method was developed to store dorsal hand vein images in a database safely on the Raspberry Pi microcomputer. In this new encryption method, both the random number generator algorithm and the encryption algorithm were based on the chaotic system. The chaotic system was used to encrypt the 1-bit and 8-bit vein images. The random numbers generated in the Raspberry Pi were successfully passed through NIST tests to ensure randomness. In order to prove the robustness of presented encryption method, SURF matching algorithm was used in the initial condition sensitivity analysis. In the decryption process the decrypted image did not match the original one when there was a very small change (10^(−18)) in the state variable of the chaotic system. However, in a simple chaotic based encryption methods present in the literature, SURF algorithm could match with approximately ∼100% when there was a little change in the state variable (one in a million). This shows that the proposed new encryption algorithm provides high security in mobile hand vein recognition systems.

II. VEIN IMAGING AND IMAGE PROCESSING

In this section, vein imaging system and image processing steps are mentioned. In the vein imaging system, the near-infrared light were passed over the diffusers and reflected onto the skin in a homogenous manner. Infrared rays (850 nm) can penetrate the skin to less than 3-4 mm and the hemoglobin in the blood absorbs the infrared radiation more than the surrounding tissues. Therefore, vein patterns appear darker with respect to the surrounding tissue on the captured images. In order to record the reflected lights from the subject, an RGB-Near-Infrared camera module of the Raspberry Pi 3 (Galler, Raspberry Pi Foundation) was used. The acquired images were digitized in the microcomputer (Raspberry Pi 3) system and various image processing steps were processed in Pyhton language using the OpenCV (open source computer vision) library.

There are two types of image processing processes before encryption steps. The first process involves contrast enhancement, encryption and saving the vein images into the database as 8 bit. Secondly, the images were converted to double level (1 bit) for faster processing and encryption. Then, before the encryption, various morphological operations were applied. In addition, the images were analyzed after noise attacks by means of peak signal-to-noise ratio (PSNR), mean square error (MSE), and the structural similarity index (SSIM) tests. It has been shown that dorsal hand vein images (1-bit and 8-bit) can be used in identification systems safely with the help of proposed method on microcomputers.

A. PRE-PROCESSING

In the first preprocessing step, contrast enhancement was aimed. The region of interest (ROI) was cropped from the images of the dorsal-hand vein by using an infrared camera. Then, the vein regions contrast were enhanced by adaptive histogram equalization. Figure 1 shows the preprocessing stages applied to the dorsal hand vein images. Firstly the images were converted to gray and then the contrast limited histogram equalization method was applied. Thus, the vein regions were clarified. This method is used in medical images to eliminate the effects of edge shading in both noise reduction and homogeneous areas [44]. The gray scale ROI region was shown in Figure 2.a. The contrast enhanced vein image

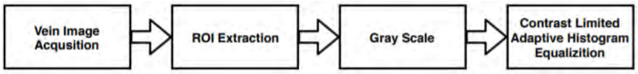

FIGURE 1. (a) Block diagram vein imaging setup. (b) Data acquisition of the vein-pattern imaging system.

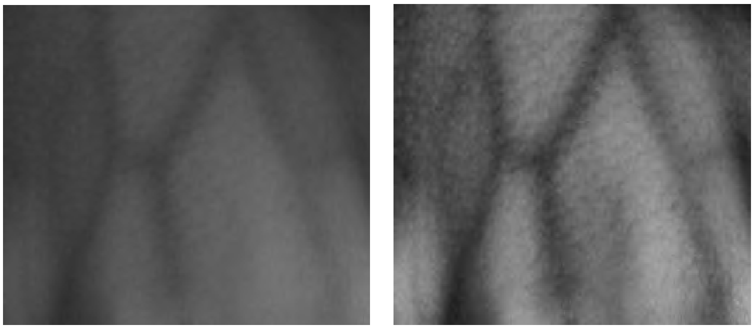

FIGURE 2. (a) Gray scale image. (b) Contrast enhanced vein image (8bit).

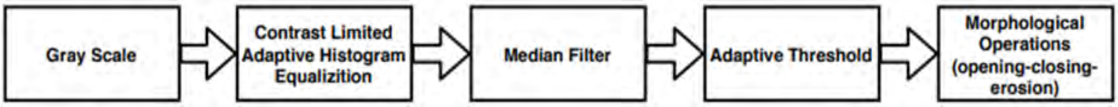
Gray Scale
Contrast Limited Adaptive Histogram Equalizition
Median Filter
Adaptive Threshold
Morphological Operations (opening-closing-erosion)

FIGURE 3. Hand vein image post processing (1 bit).

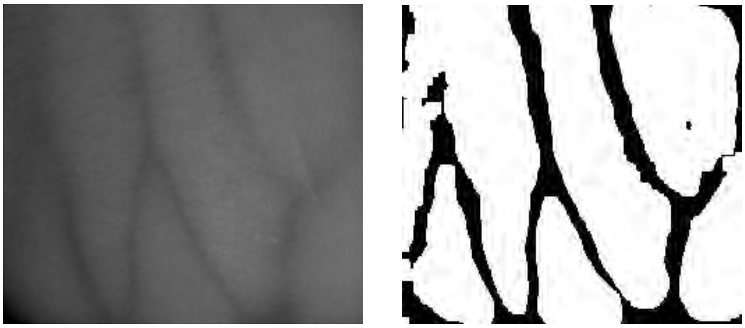

FIGURE 4. (a) Gray scale image. (b) Adaptive threshold and morphological operations.

was shown in Figure 2.b. As a result of this process, 8 bit vein images were prepared before encryption stage.

B. POST-PROCESSING

The second process was slightly more extensive. In Figure 3, the block diagram of the second process was shown. After image acquisition; gray level conversion, contrast-limited adaptive histogram equalization, median filtering, adaptive thresholding and various morphological processes were applied. During the advanced process, the contrast enhancement of the vein images was accomplished by median filtering to eliminate the noises caused by hairy areas and the external environment. After being processed with a median filter, the vein images were converted to 1 bit by adaptive thresholding. Afterwards, various morphological procedures (noise removal and thinning) were applied. Figure 4.a shows the gray level of the image, and Figure 4.b shows the region of the vein converted to 1 bit.

III. LORENZ-LIKE CHAOTİC SYSTEM AND DYNAMİC ANALYSİS

In this study, a simple 3-dimensional chaotic system similar to Lorenz [45] was used. The system shown in Equation (1) consists of 3 separate differential equations. The system has three status variables x, y and z and three parameters including a, b and c. In addition, the system contains seven terms which two of them were non-linear (xz, x^2). The initial conditions of the system were $x_0 = 1, y_0 = -1, z_0 = 1$

$$\begin{aligned} \dot{x} &= -x + ay \\ \dot{y} &= -y + bx - xz \\ \dot{z} &= -z + cx^2 \end{aligned} \tag{1}$$

The parameters for the system given in Equation (1) were chaotic, where a = 3, b = 3 and c = 1. Equation 2 shows the chaotic system in terms of the parameters a, b and c.

$$\begin{aligned} \dot{x} &= -x + 3.y \\ \dot{y} &= -y + 3.x - xz \\ \dot{z} &= -z + 1.x^2 \end{aligned} \tag{2}$$

A. DYNAMIC ANALYSIS OF CHAOTIC SYSTEM

In order to determine whether the system used was chaotic, analysis methods such as phase portraits, lyapunov exponents, kaplan-yorke, bifurcation diagrams and time series were used.

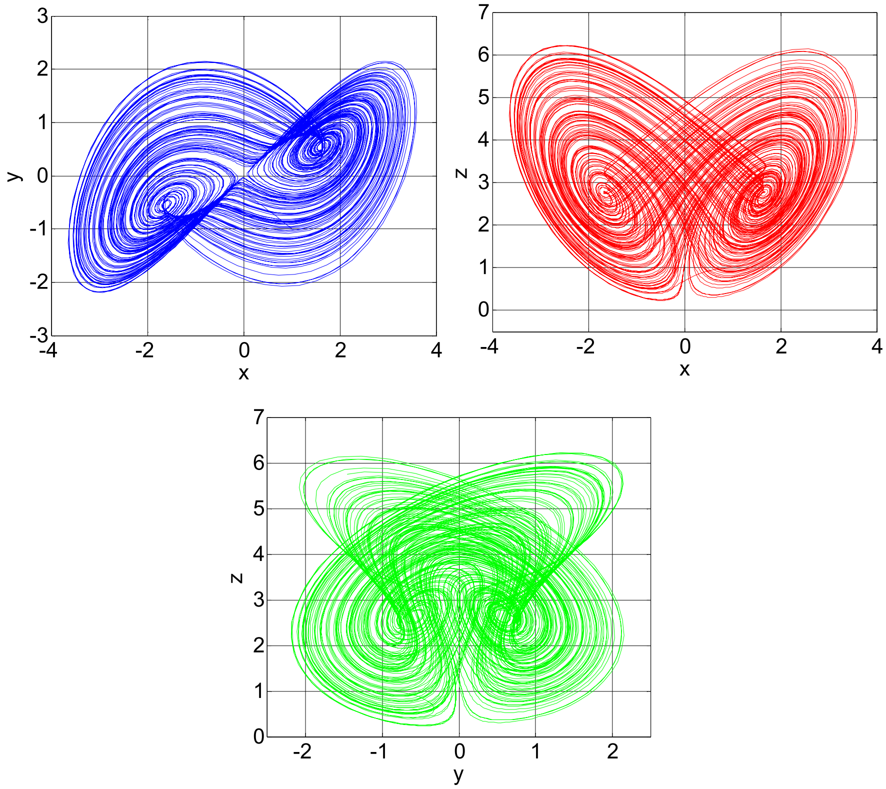

FIGURE 5. x-y, x-z, and y-z phase portraits of the chaotic system.

1) PHASE PORTRAITS

A three-dimensional system of $x - y$, $x - z$ and $y - z$ in three different ways to examine the phase portraits were given in Figure 5. As can be seen from phase portraits, it is understood that the system exhibits chaotic behavior.

2) LYAPUNOV EXPONENTS

Lyapunov exponents, which provide information on the characteristics of a dynamic system, are also measure of chaotic behavior. Whether the dynamic system is sensitive to the initial conditions can be analyzed by Lyapunov exponents [46].

Chaotic systems are very dependent on initial conditions. A small difference in initial conditions causes a huge difference in the future time behavior of the system. Lyapunov expansions allow the orbits to move away from each other with very small changes in initial conditions [47], [48]. If there is at least one positive Lyapunov exponent within the exponents, then the system is expressed as chaotic [49]. If all of the exponents are negative, the system is periodic [50]. In short, Lyapunov exponents help to characterize the types of state variables in the system [51].

In Figure 6, the Lyapunov exponents of the chaotic system, parameter ‘a’ between 0-3 were examined. Since the parameter ‘a’ is not positive for any Lyapunov exponent in the range 0-1.65, there is no chaotic behaviour. However, since a Lyapunov base of 1.65-3 has a positive value, the parameter ‘a’ leads to chaos in these ranges.

3) LYAPUNOV DIMENSION (KAPLAN-YORKE)

The analysis of the Lyapunov dimension of the system, namely the Kaplan-Yorke dimension, can be used to analyze whether the dynamic system is chaotic [52]. According to Equation 3, ‘j’ represents the number of variables in the system, while ‘λ_i’ refers to the Lyapunov exponents. In a dynamic system with three state variables, the result of the equation is expected to be 2 to 3. In other words, for the system to be chaotic, the process performed with the Lyapunov exponents must be between 0 and 1.

$$D = (j-1) + \frac{\sum_{i=1}^{j-1} \lambda_i}{|\lambda_j|} = 2 + \frac{\lambda_1 + \lambda_2}{|\lambda_j|} \tag{3}$$

According to Figure 7, the system’s parameter ‘a’ is in the range of 1.65-3, the parameter ‘b’ is between 1.67-3 and the parameter ‘c’ is in the range of 1-3, since the Lyapunov dimension is positive, the system is chaotic.

4) BIFURCATION

One of the analyses for the characteristics of dynamic systems is bifurcation. The graph, which is obtained by plotting different values of a parameter in the system according to the values taken by the state variable, is called as bifurcation.

In Figure 8, while the parameter ‘a’ in the system is in the range of 0.5-3, the values taken by the state variable ‘x’ are shown. Accordingly, since parameter ‘a’ is between

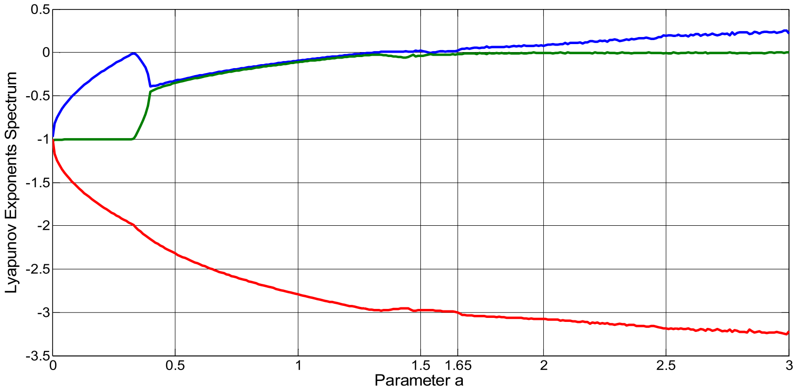

FIGURE 6. The parameter 'a' of the system used is Lyapunov exponents in the range of 0-3.

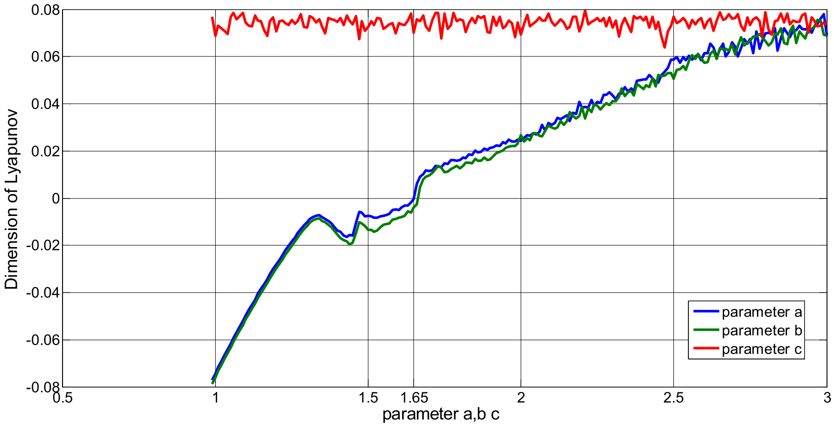

FIGURE 7. Lyapunov dimension according to the parameters a, b, and c of the system.

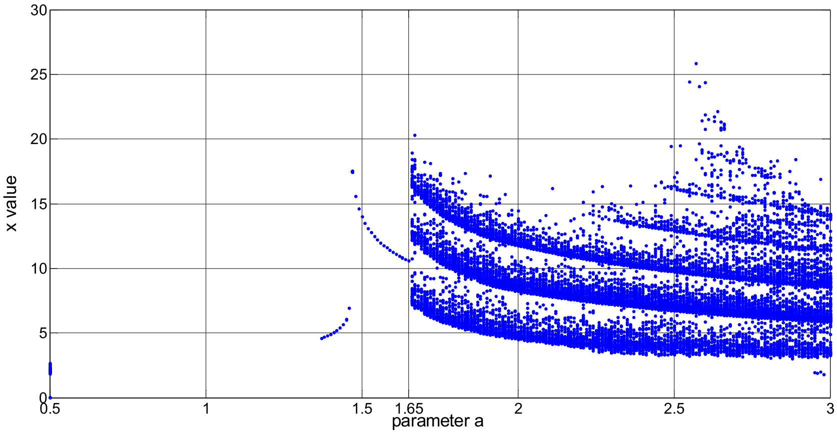

FIGURE 8. The bifurcation graph of the system for parameter "a" in the range of 0 – 3.

1.65 and 3, the system is chaotic, so the data in this analysis corresponds to the data from the Lyapunov exponents.

5) TIME SERIES AND INITIAL CONDITION SENSITIVITY

The time-dependent values of all state variables of chaotic systems should not include periodicity. Figure 9 shows the time-dependent analysis of the three state variables x, y and z of the chaotic system.

Chaotic systems should be sensitive to the initial conditions of all state variables. Figure 10 shows the time series of the 'x' state variable versus two different initial conditions, 1 and 1.000000001.

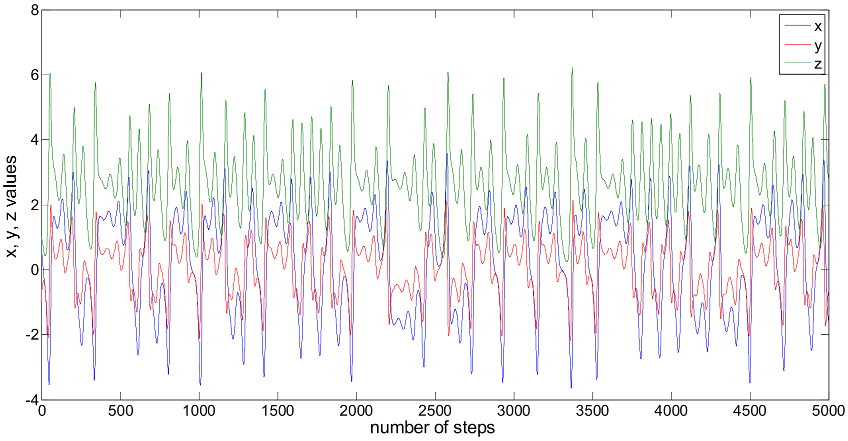

FIGURE 9. Time series of state variables of the system.

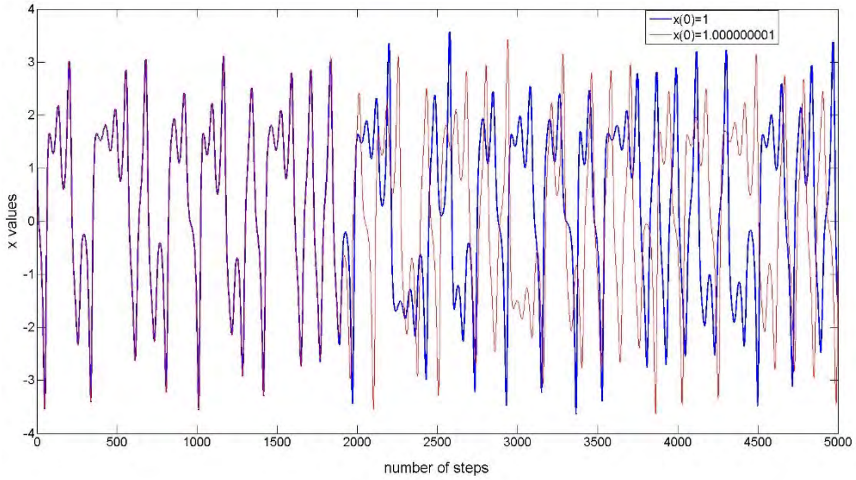

FIGURE 10. Initial condition sensitivity of the x value in the system.

IV. CHAOTIC ENCRYPTION

A. CHAOTIC-BASED RANDOM NUMBER GENERATOR

A chaotic random number generator was designed for encryption using Raspberry Pi 3 microcomputer system. In Algorithm 1, the pseudo-code algorithm of the random number generator was given. aSince the received images were 256 × 256 pixels in size, 3 × 525000 random numbers were generated for use in encryption.

In the algorithm, random numbers were used according to the pixel coordinates of rows and columns of the image. A more complex random number generator was designed using random numbers from the three state variable. With the random numbers produced, 1 bit and 8 bit vein images were encrypted.

B. ENCRYPTION

Encryption process was performed on the vein images with the random numbers. The main difference of this study from the studies in the literature, in this new encryption method, both the random number generator algorithm and the encryption algorithm were based on the chaotic system. Algorithm 2 shows the pseudo-code of the encryption algorithm.

In Algorithm 2, the pseudo-code of the determination of the coordinates to be made for XOR in order to execute encryption of the vein images are provided. In other words, the code that determines how XOR process shall be executed with which pixels and with which coordinates for the images by the random numbers that are generated in the chaotic system is indicated in the algorithm. For example, the dimensions of the vein images to be encrypted is 256 × 256. A series that increases one by one from 1 to 65536 shall be created. The initial value on the x state variable used on the chaotic system is 1. In accordance with the algorithm 2, the result of the mode (1, (0.000001*65536))*1000000 operation is 3852. The outcome result shall be deleted from the sequence so it does not appear again. Thus, there will be 65535 elements remain in the sequence. The second value of the X state variable is 0.8153. Then again in accordance with the Algorithm 2,

Algorithm 1 Random Number Generator Algorithm Pseudo Code

```
Start
Entering system parameters → (a = 3, b = 3, c = 1)
Entering initial condition → (x0 = 1, y0 = -1,
 z0 = 1)
Determination of the appropriate value of $\Delta$h (0.05)
Solving the chaotic system using RK-4 algorithm and
 obtaining time series
for i = 1 : 256*256
   x_rng ( 16*(i − 1) + 1 : 16*(i − 1) + 16 ) =decimal
 to binary ( round (mod (( x(i)*10^5),
 (10^(−7)*65535)*10$^{1}$2), 16 )
   y_rng ( 16*(i − 1) + 1 : 16*(i − 1) + 16 ) =decimal
 to binary ( round (mod (( y(i)*10^5),
 (10^(−7)*65535)*10^12 ),16 )
   z_rng ( 16*(i − 1) + 1 : 16*(i − 1) + 16 ) =decimal
 to binary ( round (mod (( x(i)*10$^{5}$),
 (10^(−7)*65535 ) *10^12),16 )
 end for
 Ready to use 3*525000 random number
 End
```

Algorithm 2 Sequence of xor operation algorithm pseudo code

```
Start
[row column]=size(image)
series=1:row*column
for i=1:row*column
   number=mod(x(i), (0.0000001*(row*column
 +1-i)))*1000000
   xor_sequence(i)=series(number)
   series(number)=[]
end for
End
```

Algorithm 3 Image Encryption Algorithm Pseudo Code

```
Start
[row column]=size(image)
Index=0 a=0
for i=1:row
 for j=1:column
   a= a+1 row2=ceil(xor_ sequence (a)/column)
  column2=mod(xor_ sequence(a),column)
   bin = decimal to binary (image (row2, column2), 8)
   if ( mod ( i+j, 3 ) == 1 )
     rng=x_rng
   elseif ( mod ( i+j,3 ) == 2 )
     rng=y_rng
   else
     rng=z_rng
   end if
   for n=1:bit_number   (bit_number = 1 or 8)
      index=index+1
      number(n)=(bitxor( rng (index),bin(n) )
   end for
     image_encryption ( i,j ) = binary to decimal
    (number)
    end for
 end for
 End
```

Algorithm 4 Random Number Generator Algorithm Pseudo Code for Initial Condition Sensitivity

```
Start
Entering system parameters → (a = 3, b = 3, c = 1)
Entering initial condition → (x0 = 1, y0 = -1,
 z0 = 1)
Determination of the appropriate value of $\Delta$h(0.05)
Solving the chaotic system using RK-4 algorithm
 and obtaining time series
for i=1: 65536 /32
  x_rng= x(i)*100000

  Rng ((i-1)*32+1: (i-1)*32+32) =decimal to binary
  32 bit (x_rng)
end for
Ready to use 65536 random number
End
```

the result of the mode (1, (0.000001*65536))*1000000 operation is 2691. This result is removed from the sequence and 65534 elements shall remain in the sequence. Because the vein images is in dimension of 256 × 256, this process shall repeat in 65536 times and the coordinates to be executed in XOR shall be determined.

In Algorithm 3, the pseudo-code is provided for the encryption for the vein images are provided. According to the algorithm the variable "a" is a type of counter. First, the order of the rows and columns in which the XOR operation shall be conducted will be determined. The xor_sequence variable obtained as a result from algorithm 2 shall be divided by the total number of columns of the image to provide the line coordinate as a result of rounding operation. When the mode operation of xor_sequence value is applied according to the total number of columns of the image, the coordinate of the column shall be obtained. For example, the first value of xor_sequence variable was found as 3852 as a result of Algorithm 2. Since the column value of the image is 256, the result of the first line value of the result ceil(xor_ sequence (a) / column) is 16, and the first column value is 12 according to the operation of mode (xor_ sequence (a), column). Therefore, the first random number arising from the chaotic system is subjected to XOR operation with the pixel value as found in the 16th line and 12th column of the image. The second value of xor_sequence is 2691. In accordance with the algorithm 3, 2nd line and 2nd column value is 11th line and 131th column. In the XOR process, 3 different random number sequences that are obtained from algorithm 1 are being used. Y was used in the first XOR. In the next cycle Z is used and in the next one after that random numbers obtained from the x state variable have been used. Thus, the pixel value in line 16 column 12 shall be subject to xor operation with a random number obtained from the y phase. The 11th line and 131th column pixel value of the vein image shall be subject to XOR operation with a random number obtained from z phase. These operations shall continue until the number of rows * column is completed.

C. NIST-800-22 TEST

The NIST-800-22 test [53] is used to measure the complexity of the generated random numbers. It is a security testing tool performed by the National Institute of Standarts and Technology [54], [55]. The NIST-800-22 test includes 16 tests. The random numbers generated must pass through all 16 tests to pass the NIST-800-22 test successfully.

The p-value, which is the most important parameter in this test, is accepted as the criterion of the complexity of the random number sequence entering the test. If the p-value is really a complex array, it will be 1, else it is close to 0. In order for the tests to be considered successful, these p values should be greater than 0.01 [56].

TABLE 1. NIST-800-22 Results for random arrays from chaotic system.

Statistical Tests	P Value	Result
Frequency Monobit Test	0.6859	Successful
Block-Frequency Test	0.7284	Successful
Run Test	0.0295	Successful
Longest-Run Test	0.7627	Successful
Binary Matrix Rank Test	0.8447	Successful
Discreate Fourier Transform Test	0.7213	Successful
Non overlopping Templates Test	0.3767	Successful
Overlapping Temp Templates Test	0.1531	Successful
Maurier's Universal Statistical Test	0.7151	Successful
Linear Complexity Test	0.6219	Successful
Serial Test -1	0.6471	Successful
Serial Test -2	0.8722	Successful
Approximate Entropy Test	0.3520	Successful
Cumulative Sums(Forward) Test	0.6149	Successful
Random Excursion Test (x=-4)	0.3032	Successful
Random Excursion Variant est(x=-9)	0.9393	Successful

In Table 1, the random numbers generated from the state variables of the chaotic system were subjected to the NIST-800-22 test to measure their randomness. According to the results, p-values from each of the 16 tests found in the NIST-800-22 test were greater than 0.01. Thus, the random number sequence produced through all of the 16 tests was found to be really random according to the NIST-800-22 test.

V. KEY POINT DETECTION WITH SURF METHOD

The Speed Up Robust Feature (SURF) algorithm was developed by Herbert Bay in 2006 to determine local feature points independent of rotation, scaling, and offset in an image [57]. The SURF algorithm is based on convolutional images and a convolution process combined with the Hessian matrix. While the use of integral images reduces the calculation time considerably, the use of the determinant of the Hessian matrix also enables the detection of feature points.

$$H(X,\sigma) = \begin{pmatrix} L_{xx}(X,\sigma) & L_{xy}(X,\sigma) \\ L_{yx}(X,\sigma) & L_{yy}(X,\sigma) \end{pmatrix} \tag{4}$$

In Equation 4, 'L_{xx}' is the second derivative of the original image X in the x-axis, in which 'L_{xy}' is the second derivative of the original image X in the x-axis and then in the y-axis in terms of 'σ'. The places where the determinant of this matrix is maximum are considered as image regions. This determinant is used to find the maxima and minima in the images with the help of the second order derivative of the image. In addition, the scale and position are also found using the determinant of the Hessian matrix.

The SURF identifier determines how points of interest determined by the Fast-Hessian detector are distributed. In addition, descriptive images are used with filters known as Haar wavelet to accelerate the process. Haar filters are simple filters used to find x and y gradients. In Figure 11, SURF algorithm was applied on 1 bit and 8 bit sample vein images and key points were determined. While 422 key points were detected in 1 bit vein image, 58 key points were found in 8 bit vein images. Identity recognition procedures were carried out with key points, respectively in initial condition analysis and loss-noise attack analysis.

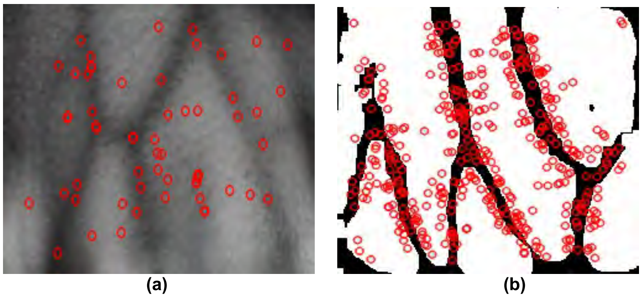

FIGURE 11. Examples of SURF features (keypoints) (a) 8 bit vein image, (b) 1 bit vein image.

The SURF algorithm is not used for encryption operations. In the analysis section, SURF method was used to state success rate of the developed encryption algorithm. Also, data loss and noise attack analyses were conducted under Section VI, sub-heading (F). It has been seen that the decrypted images following the various attacks on the encrypted images did match with their original images in the database (In the pairing process SURF algorithm was used).

VI. ANALYSIS OF EXPERIMENTAL RESULTS

A. HISTOGRAM ANALYSIS

For a good encryption process, pixel values must be evenly distributed [58]. In order for the images to be resistant to statistical attacks, they must have a smooth histogram. The histogram of the encrypted image indicates an equal number of gray pixel values, which the gray level is uniformly distributed and that randomness is ensured. Processed 8-bit vein image (Figure 12.a), encrypted vein image (Figure 12.b), and histogram analyses were given below. For the 8 bit image, only certain pixel values are weighted (Figure 12.c), whereas the encrypted image has a homogeneous distribution (Figure 12.d).

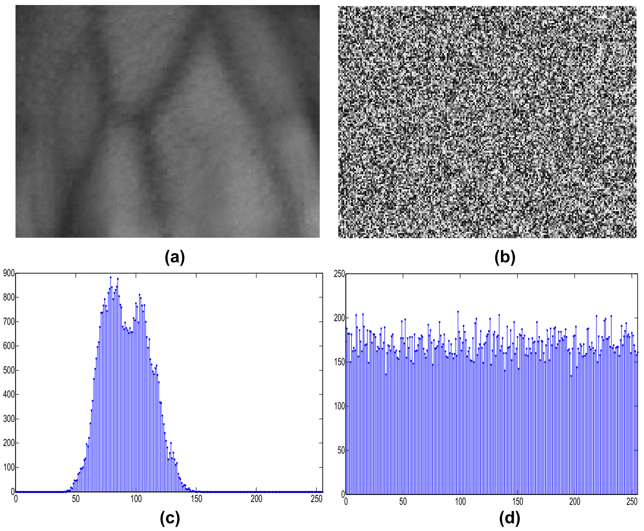

FIGURE 12. **(a) 8-bit vein image; (b) 8-bit encrypted vein image; (c) histogram of the 8 bit image; (d) histogram of the encrypted image.**

The vein image transformed into 1 bit (Figure 13.a), encrypted state (Figure 13.b), and histogram analysis were given. In the 1-bit vein image, there is a disproportion between the 0 and 1 pixel distributions (Figure 13.c), while the 0 and 1 pixel values in the encrypted image are distributed almost equally (Figure 13.d).

B. CORRELATION

In unencrypted images, there are strong correlations of pixels in vertical, horizontal and diagonal directions. Correlation results in a well-encrypted image should be scattered. The low correlation between adjacent pixels is an important step in image encryption. The correlation coefficient is between −1 and 1. The fact that it is close to 1 and −1, there is a high correlation. When it is close to 0, it means low correlation [59]. The correlation coefficient calculation is given in Equation 5.

$$C_r = \frac{\sum_{i=1}^{N}(x_i - \frac{1}{N}\sum_{j=1}^{N}x_j).(\sum_{i=1}^{N}(y_i - \frac{1}{N}\sum_{j=1}^{N}y_j)}{\sqrt{\sum_{i=1}^{N}(x_i - \frac{1}{N}\sum_{j=1}^{N}x_j)^2.(\sum_{i=1}^{N}(y_i - \frac{1}{N}\sum_{j=1}^{N}y_j)^2}} \tag{5}$$

The correlation coefficient is calculated horizontally, vertically and diagonally. In equation 5, if the vertical correlation is calculated, N is the total number of rows in the image, x_i is the value of a pixel in the image, y_i and is calculated as the pixel value under a row.

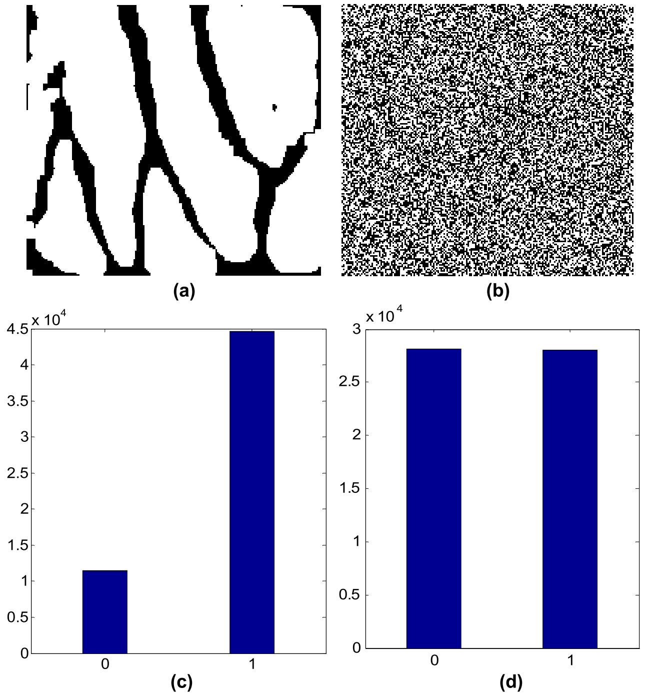

FIGURE 13. **(a) 1 bit vein image, and (b) 1 bit encrypted vein image, (c) Histogram of the unencrypted image, and (d) histogram of the encrypted image.**

TABLE 2. **Correlation coefficients of 8 Bit and 1 Bit images and encrypted images.**

	Horizontal	Vertical	Diagonal
Unencrypted image (8 bit)	0.9861	0.9749	0.9854
Encrypted image (8 bit)	-0.00048	0.00277	0.00096
Unencrypted image (1 bit)	0.95709	0.88897	0.91564
Encrypted image (1 bit)	0.000742	0.000745	0.00074

If the horizontal correlation is calculated, N represents the total number of columns in the image, the pixel value in the x_i image, the pixel value next to a column. In Table 2, the results of the horizontal, vertical and diagonal correlations of 8 bit and 1 bit vein images were high. In the encrypted images, this result was close to 0 and the correlation was low. Table 3 shows the correlation coefficients obtained in some recent studies. Correlation coefficients obtained from encrypted vein images were found to be better than most studies in the literature. In addition, all of the correlation coefficients of the encrypted image were less than 0.01 in the proposed algorithm; this showed a very insignificant correlation between adjacent pixels. In Fig. 14, the correlation maps of the 8-bit vein image showed a vertical (Figure 14.a), horizontal (Figure 14.b) and diagonal (Figure 14.c) high correlation. However, in encrypted vein images, the correlation was low (Figure 14.d-e-f) and dispersion was homogeneous.

C. ENTROPY

Entropy is a mathematical theory derived from Shannon [60], [61]. It is a feature that defines the level of randomness

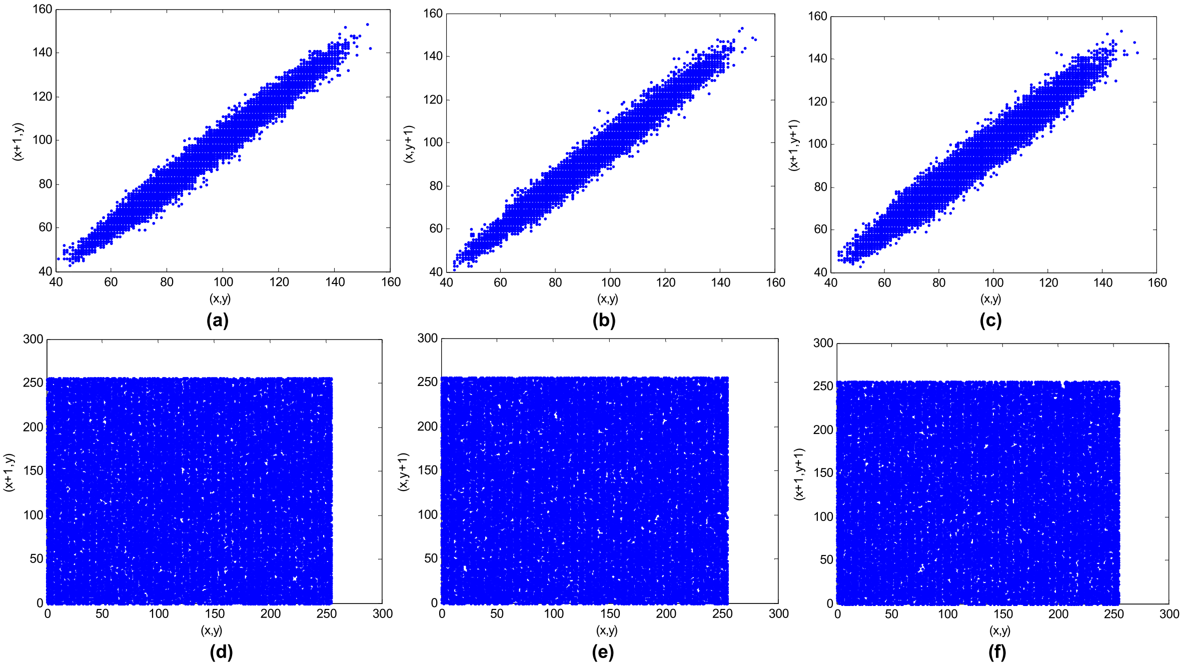

FIGURE 14. (a) Horizontal, (b) vertical, (c) diagonal correlation analysis of the 8-bit unencrypted vein images, (d) horizontal, (e) vertical, and (f) diagonal correlation analysis of the encrypted vein image.

and uncertainty in an image and is used to measure the uniform distribution of the gray pixel level in the image. The entropy value is calculated using Equation 6 [62].

$$H(s) = \sum_{i=0}^{2^N-1} P(s_i)\log(\frac{1}{P(s_i)}) \quad (6)$$

In Equation 6, M indicates the number of bit, and P indicates the probability of the pixel in the image and expresses the histogram distribution. In a well-encrypted image, the entropy value should be very close to the M.

In Table 4, the entropy value in the 1-bit vein image is 0.73 while in the encrypted image this value is equal to the number of bit. The entropy value was found as 6,238 in 8-bit vein images and this value was very close to 8 in the encrypted image. As a result, it is understood that the 1 and 8 bit encryption processes were very successful based on the entropy values.

Table 5 shows some of the entropy values from the literature reached in recent years. When the proposed encryption algorithm was compared with the other studies, all the entropy values of the encrypted images were very close to 8. This result shows that the encryption system can effectively resist malicious attacks and results were in congruent with the literature.

D. DIFFERENTIAL ANALYSIS

It is an important metric to compare the degree of similarities between two different images. The differential analysis method is used to measure this value in image encryption. According to Kerckhoffs scenario [63], the key used for a good encryption must be sensitive to mismatches. Because, a small change in the key causes very serious differences in the encrypted image. In order to measure and evaluate these sensitivities, two differential analysis was performed: NPCR (in Equation 7 and Equation 8) and UACI (in Equation 9) [64].

$$NPCR = \frac{1}{MN}\sum_{\text{i}=1}^{M}\sum_{J=1}^{N} Dif(i,j) \times 100\% \quad (7)$$

$$Dif(i,j) = \left\{ \begin{array}{ll} 1, & when\ C_1(i,j) \neq C_2(i,j) \\ 0, & when\ C_1(i,j) = C_2(i,j) \end{array} \right\} \quad (8)$$

$$UACI = \frac{1}{MN}\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}|C_1(i,j) - C_2(i,j)|}{255} \times 100\% \quad (9)$$

In the Equations 7 and Equation 9, M is the total number of rows in the image, N is the total number of columns, 'C_1' is the pixel value of the unencrypted image and 'C_2' is the pixel value of the encrypted image. The NPCR shows the number of the replaced pixels and the UACI indicates the average value of the changed pixels [65]. In previous studies, the NPCR was considered to be a good encryption, with a value greater than 99.6% and a UACI greater than or equal to 30% [66]. NPCR and UACI analyzes of 1-bit and 8-bit encrypted images were given in Table 6. In the encrypted 1-bit vein images, NPCR and UACI are equal because the total number of pixels and the changing pixel values are equal. There is a difference of 50% between the encrypted and unencrypted images because the pixel values in the 1-bit image have two different values, only 0 and 1. Thus, the

TABLE 3. The comparison of correlation coefficients with the literature.

Algorithm	Horizontal	Vertical	Diagonal
Proposed	-0,00048	0,00277	0,00096
Chen et al.(2017) [67]	-0,0028	0,0171	-0,0022
Pareek et al.(2006) [68]	0,0041	-0,0337	N/A
Zhang et al.(2016) [69]	0.00773	-0.01103	0.01454
Zhou et al.(2014) [70]	0.0102	-0.0053	-0,0161
Cao et al.(2017)	-0.0074	0.0019	-0.0017
Wang et al.(2015) [71]	0.0020	-0,0007	-0,0014
Wang et al.(2015) [72]	-0.0098	-0.0050	-0.0013
Xu et al.(2016) [73]	0.0019	0.0263	0.0196
Kaur et al. (2018) [74]	0.012	-0.0063	0.0058
Ullah et al. (2017) [75]	$2.754\text{x}10^{-6}$	$-5.9051\text{x}10^{-5}$	$2.9142\text{x}10^{-5}$
Li et al. (2018) [76]	0.0013	0.0008	0.0066
Cavusoglu et al. (2018) [77]	-0.00197	N/A	N/A
Sahari et al. (2018) [78]	−0.000736	0.000187	0.000592

TABLE 4. Entropy values of 1-Bit and 8-Bit unencrypted and encrypted vein images.

1 bit	**Unencrypted image**	0.73
	Encrypted image	1
8 bit	**Unencrypted image**	6.238
	Encrypted image	7.9973

results showed that the encrypted 1 and 8 bit vein images passed through the NPCR and UACI encryption analysis successfully. Table 7 shows the NPCR and UACI values obtained from the nine different studies. As can be seen from the table, NPCR and UACI values of the proposed encryption algorithm were obtained as 99.72% and 33.16%, respectively. In terms of its ability to prevent differential attack attacks, the proposed encryption algorithm was found to be superior to many algorithms developed in recent years.

E. INITIAL CONDITION SENSITIVITY

One of the most important reasons for the use of chaotic systems in encryption is that they are very sensitive to their initial conditions. That is, in the chaotic system used, very small changes of state variables (x, y and z) and parameters (a, b and c) cause the encrypted data to be incorrectly decrypted. For this reason, it is not enough to use only the chaotic system. In this respect, chaotic system based random number generator and encryption algorithm should be used together. In this study, a random number generator was designed with use of the chaotic system.

TABLE 5. The comparison of information entropy with the literature.

Algorithm	Information Entropy
Proposed	7.9973
Chen et al.(2017)	7.9891
Wang et al.(2015)	7.9972
Wang et al.(2015)	7.9974
Xu et al.(2016)	7.9974
Kaur et al. (2018)	7.9989
Ullah et al. (2017)	7.9798
Li et al. (2018)	7.9992
Cavusoglu et al. (2018)	7.9637
Sahari et al. (2018)	7.9982

TABLE 6. NPCR and UACI Analysis of 1-Bit and 8-Bit encrypted vein images.

	NPCR	UACI
1 Bit	%50.03	%50.03
8 Bit	%99.72	%33.16

In this system, the importance of strong algorithm by changing the initial value of x state variable was shown. In the Algorithm 4, the chaotic system was solved with Runge-Kutta 4. 65536 bit of random numbers are required for a vein image with dimensions of 256 × 256. For this purpose, 65536/32 steps were solved. The state variable ‘x’ was multiplied by 10000 and converted to 32 bit binary. As a result, 65536 random numbers were obtained.

The random numbers obtained from the chaotic system were subjected to XOR with 65536 pixels starting from the first pixel in the vein image. The encryption result was given in Figure 15.

The vein image was decrypted (Figure 16) by making an initial value of x state variable of 1.000001 (one in a millon).

The image that was decrypted by changing the initial condition was matched with the SURF algorithm in 160 different 1 bit vein images. Figure 17 shows an example correct match after decryption. In other words, it was observed that there was no significant information loss in the decrypted image by a small change in the initial condition.

TABLE 7. NPCR and UACI Comparison with the literature.

Algorithms	NPCR(%)	UACI(%)
Proposed	99.72	33.16
Chen et al.(2017)	99.59	33.42
Pareek et al.(2006)	99.70	28.29
Zhang et al.(2016)	88.99	30.21
Zhou et al.(2014)	96.46	33.10
Cao et al.(2017)	99.60	33.48
Wang et al.(2015)	98.64	27.97
Wang et al.(2015)	93.21	32.48
Xu et al.(2016)	99.62	33.51
Kaur et al. (2018)	99.67	33.58
Ullah et al. (2017)	99.60	33.85
Li et al. (2018)	99.60	33.43
Cavusoglu et al. (2018)	99.63	31.63
Sahari et al. (2018)	99.61	33.45

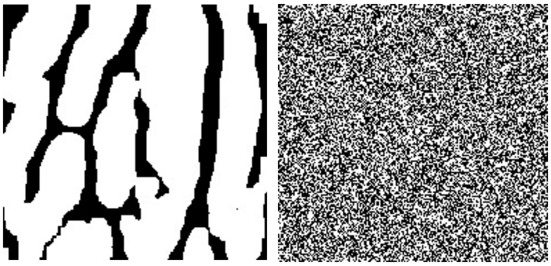

FIGURE 15. **(a) 1 bit vein image, (b) image encrypted with Algorithm 3.**

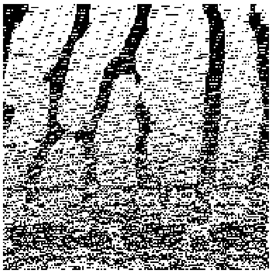

FIGURE 16. **Image is decrypted by changing the initial condition of 'X' by one in a million change.**

With this result, it was not enough to have a random number generator algorithm and encryption algorithm based on chaotic system alone. In addition, ''how this algorithm was designed'' was also very important.

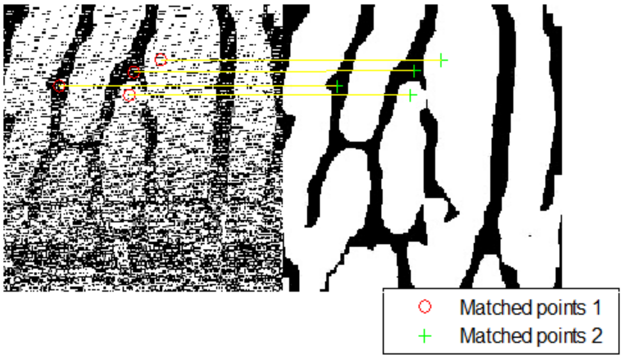

FIGURE 17. **Matching result by SURF algorithm of the decrypted image with the original image by changing the initial condition.**

In the new encryption algorithm, it was shown that 1-bit encrypted vein images by Algorithm 2 were resistant to slight change of initial condition. Because, in the new algorithm, the random numbers were generated by Algorithm 1. Figure 18 and Figure 19 show the decrypted image with suggested design by making change (10^{-18}) in the initial condition of state variable 'x'.

F. DATA LOSS AND NOISE ATTACK ANALYSIS

Data loss and noise attack analyzes are intended to control the robustness of the encryption algorithm against cropping of the encrypted image. A reliable encryption algorithm should recover the image without losing any significant information in the original image when the encrypted image loses some data. Data loss attack is a significant attack on the encrypted image by changing the values by selecting a certain section in the encrypted image. In addition, the noise attack is an attack by adding certain noises to the encrypted image. Since digital data may cause such distortions during transmission, it is necessary to analyze the encrypted image with these tests. In this study, 5%, 15% and 30% data loss attacks were performed and analyzed for these attacks for the encrypted vein images. As seen in Figure 20, there was data loss in the encrypted images, but there was no significant data loss in the decrypted image.

In Figure 21, encrypted images were given after 5%, 10%, 20% and 30% salt-pepper noise addition. It was observed that the encoded images were not subject to significant loss of information. Figure 22 shows 8-bit encrypted images, respectively 5%, 15% and 30% data loss attacks, and decrypted images after the attack. In Figure 23, 10%, 20% and 30% salt pepper noise attacks were performed to 8 bit encrypted images and decrypted images were shown after the attack.

1) IMAGE QUALITY ANALYSIS

The MSE and PSNR analyzes after data loss and noise attack are shown in Table 8. MSE (Mean Squared Error) analysis of a good decrypted image should be very low. PSNR shows the noise and quality level of the image. The PSNR is inversely proportional to the MSE and is close to 0, resulting in a

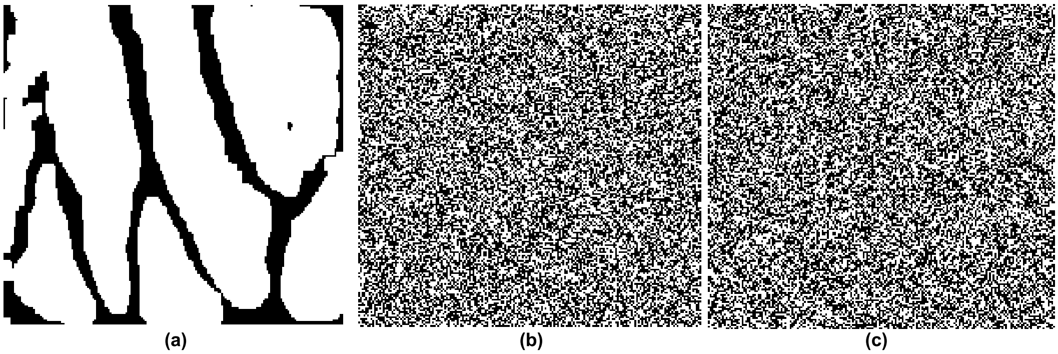

FIGURE 18. (a) 1-bit vein image, (b) Image encrypted using Algorithm 1 and Algorithm 2, and (c) Decrypted image by changing the initial condition of the state variable 'x' (10^{-18}).

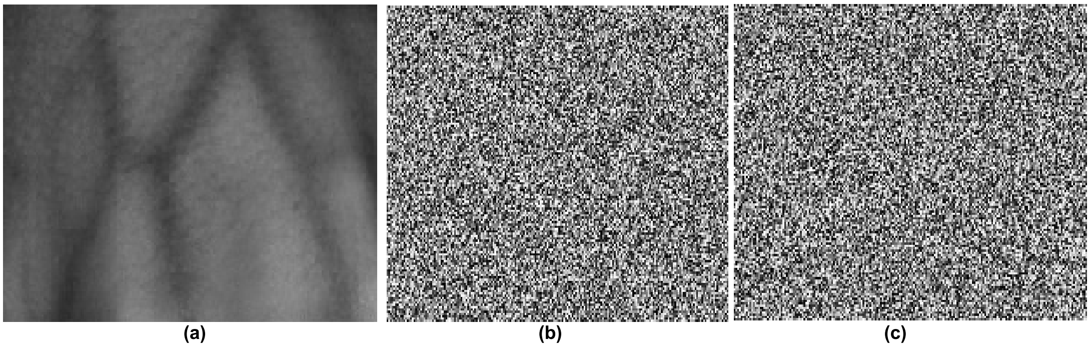

FIGURE 19. (a) 8-bit vein image, (b) Image encrypted using Algorithm 1 and Algorithm 2, and (c) Decrypted image by changing the initial condition of the state variable 'x' (10^{-18}).

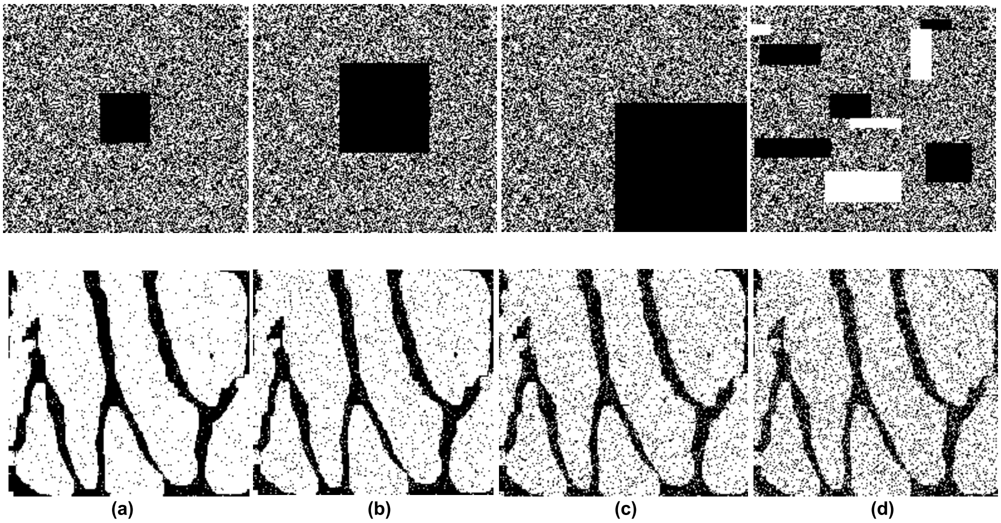

FIGURE 20. Encrypted and decrypted images (a) 5%, (b) 15%, (c) 30%, and (d) random data loss attacks.

noisy image. The values in Table 8 were calculated using Equation 10 and Equation 11.

$$MSE(I, I_0) = \frac{1}{MN}\sum_{y=1}^{M}\sum_{x=1}^{N}[I - I_0]^2 \tag{10}$$

$$PSNR = 20 \times \log_{10}(\frac{255}{\sqrt{MSE(I, I_0)}}) \tag{11}$$

In Equation 10, M represents the total number of rows in the image, N represents the total number of columns, I represents the pixel value of the image to be encrypted, and I_0 represents the pixel value of the encrypted image. In Table 9, the structural similarity between the images formed after data loss and noise attacks and the original images was tested by SSIM analysis. SSIM is an analysis method that measures

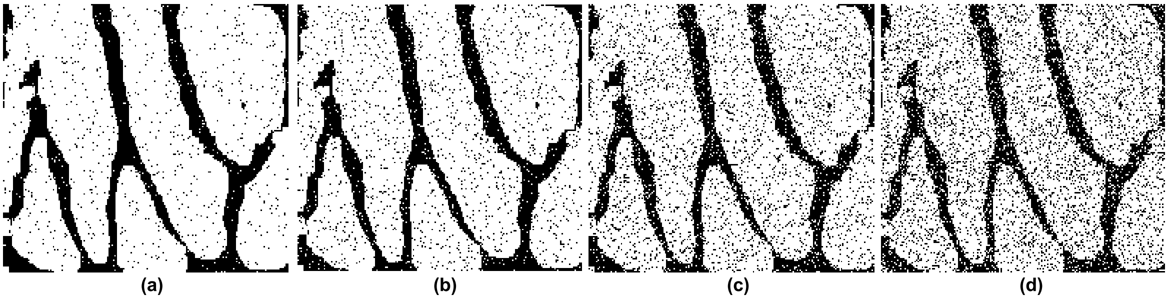

FIGURE 21. Decrypted images of (a) %5, (b) %10, (c) %20, and (d)%30 salt-pepper noises addition to encrypted images.

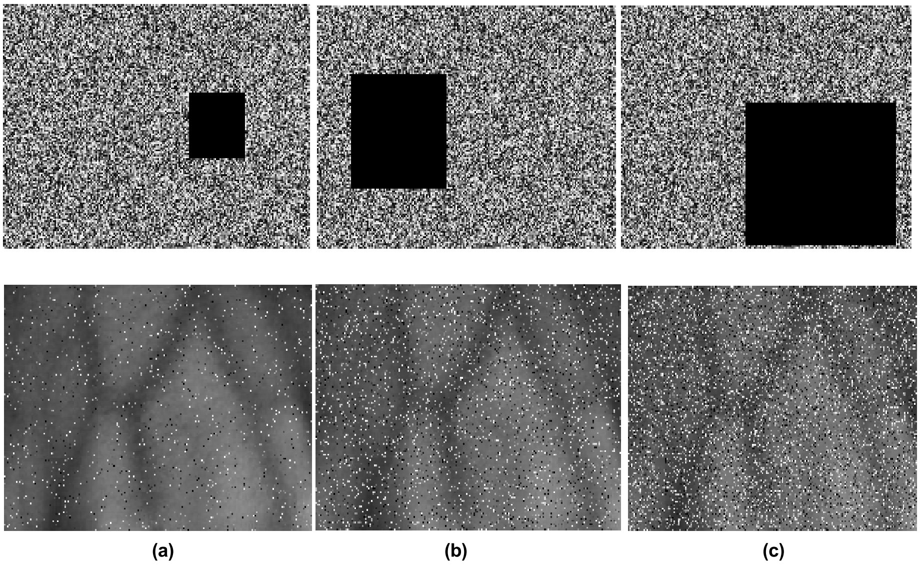

FIGURE 22. 8 bit decrypted images of (a) 5%, (b) 15%, and (c) 30% data loss attacks to encrypted images.

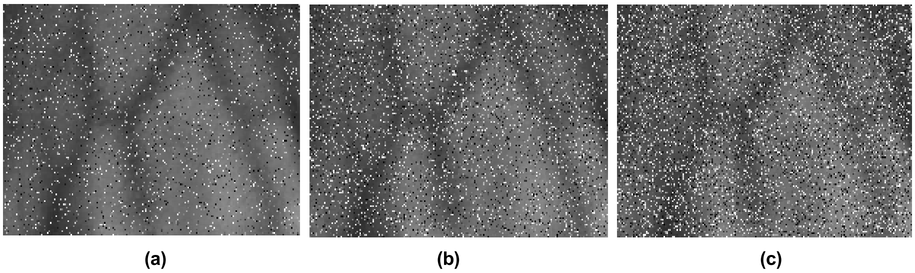

FIGURE 23. (a) 10%, (b) 20%, and (c) decrypted images of 8 bit encrypted images with 30% salt-pepper noises.

structural similarity between two images. The fact that SSIM is close to '1' indicates that the decrypted image is very similar to the unencrypted image. The values in Table 9 were calculated using Equation 12.

$$SSIM(n) = \frac{[2\mu_{I_R}(n)\mu_{I_D}(n) + C_1][2\sigma_{I_R I_D}(n) + C_2]}{[\mu^2_{I_R}(n)\mu^2_{I_D}(n) + C_1][\sigma^2_{I_R}(n)\sigma^2_{I_D}(n) + C_2]} \quad (12)$$

In Equation 12, $\mu_{I_R}(n)$ is the pixel value of the image to be encrypted, $\mu_{I_D}(n)$ the pixel value of the encoded image, $\sigma_{I_R}(n)$ the standard deviation of the image to be encrypted, $\sigma_{I_D}(n)$ standard deviation of the encrypted image. Figure 24 illustrates the success of the matching algorithm for decrypted images after data loss at different rates with the SURF algorithm. The number of key points were 88, 21, 7 and 14 with respect to 5% (Figure 24.a), 15% (Figure 24.b), 30% (Figure 24.c) and random (Figure 24.d) data loss by the SURF algorithm. Among the 160 vein images, the matching accuracy was 100% in spite of data loss. In Figure 25, after the addition of salt and pepper noises, the images were matched with the SURF algorithm and it was shown that

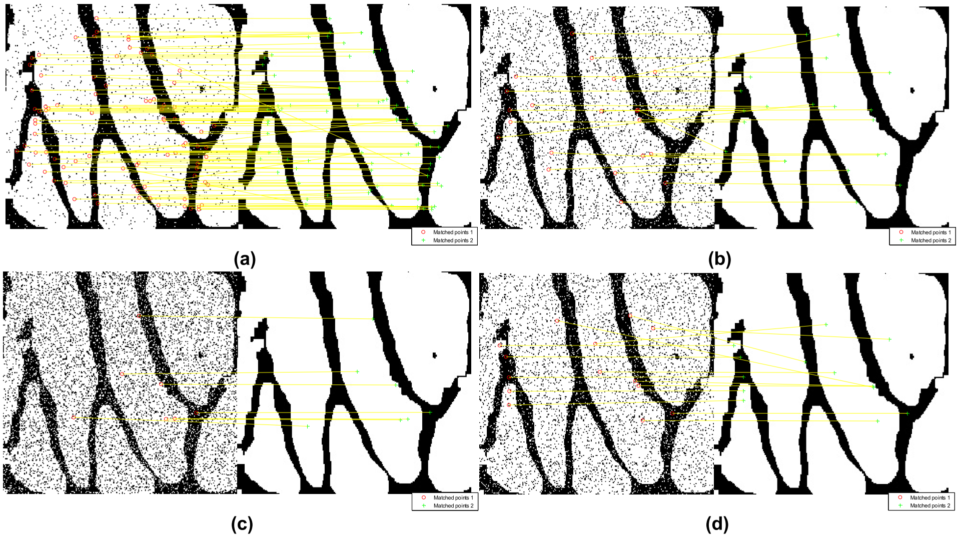

FIGURE 24. Image mathing by SURF algorithm after (a) 5%, (b) 15%, (c) 30%, and (d) random data losses.

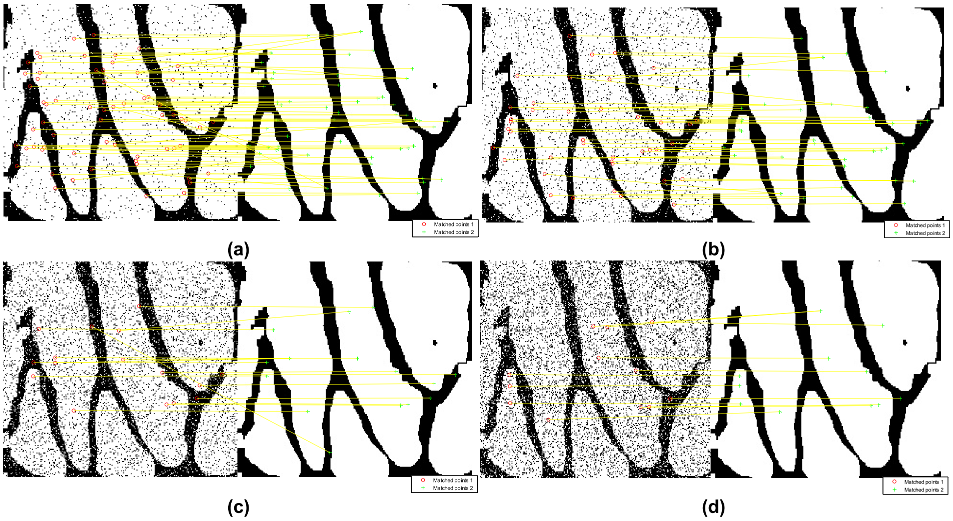

FIGURE 25. Image matching by SURF algorithm after (a) %5, (b) %10, (c) %20, and (d) %30 salt-pepper addition.

TABLE 8. MSE and PSNR analysis after data loss and noise attacks.

	MSE						PSNR					
	LOSS ATTACK			NOISE ATTACK			LOSS ATTACK			NOISE ATTACK		
	0.05	0.15	0.3	0.1	0.2	0.3	0.05	0.15	0.3	0.1	0.2	0.3
1 bit	0.0225	0.0723	0.1531	0.0503	0.1001	0.148	0.346	0.2401	0.174	0.2734	0.21	0.174
8 bit	0.0051	0.016	0.0327	0.0115	0.0215	0.0325	0.242	0.1883	0.156	0.2049	0.176	0.157

all the decrypted images matched with the original pictures. The number of key points found by the SURF algorithm were 63, 44, 16 and 12 with respect to 5% (Figure 25.a), 10% (Figure 25.b), 20% (Figure 25.c) and 30% (Figure 25.d) salt-pepper noise addition. Among the 160 vein images, the matching accuracy was 100% in spite of data loss.

G. PERFORMANCE ANALYSIS AND COMPARISONS

The proposed scheme is implemented in Python 3.4.4. Our tests were worked on a Raspberry Pi 3 (Model B+) with ARM Cortex-A53, CPU 1.4 GHz, and 1 GB memory, and the software running system is Raspbian. Simulation results show that for 8-bit gray level vein image of 256 × 256 pixels, the average encryption time is 0.31 s and the average decryption time is 0.29s. For 1-bit vein image of 256 × 256 pixels, the average encryption time is 0.07s and the avarage decryption time is 0.06s. Furthermore, Table 10 shows the time comparison with four similar works in the literature. The comparison result shows that our proposed image cryptosystem is faster than the other systems.

TABLE 9. SSIM analysis after data loss and noise attacks.

	SSIM					
	LOSS ATTACK			NOISE ATTACK		
	0.05	0.15	0.3	0.1	0.2	0.3
1 bit	0.929	0.787	0.595	0.8477	0.716	0.6066
8 bit	0.80	0.543	0.32	0.631	0.4495	0.329

TABLE 10. Algorithms with their encryption time (s).

Size of Image	Ullah et al. (2017)	Li et al. (2018)	Cavusoglu et al. (2018)	Sahari et al. (2018)	Proposed
256x256	0.8142	N/A	8.672	0.7	0.6
512x512	3.1238	2.007	N/A	1.1	N/A

VII. CONCLUSION

In this article, the images of the dorsal hand vein were collected from the people via the Raspberry Pi near-infrared camera. These images were transferred to the microcomputer and converted to 8 bit and 1 bit images by various pre- and post-processings. These were then processed separately and were encrypted with chaos-based algorithm and security analysis were performed. Vein images differ from each individual just like fingerprints. Therefore, hiding of these data is very important for the security of biometric recognition systems. In order to ensure the security of the system, these images are stored in the database using a new encryption algorithm.

In this study, a new encryption algorithm has been proposed for the protection of the hand vein images which can be used in biometric systems. In addition to the security analyzes used in the literature, the SURF algorithm has applied to these images. Therefore, the robustness of the proposed method were measured to the use of the system for biometric purposes. Futhermore, the images that were decrypted after the differential attacks were also utilized in the SURF algorithm. It has been seen that the images subjected to attacks have passed the identification process without any problem.

In the encryption method used in the study, both random number generator algorithm and encryption algorithm were chaotic system based. The chaotic system based algorithm was utilized to encrypt the 1-bit and 8-bit vein images. The random numbers generated in the Raspberry Pi were also successfully passed through the NIST-800-22 tests to ensure its randomness.

In order to show the strength of the proposed method, a simple chaotic based random number generator and encryption algorithm were used. The SURF matching algorithm was used for initial condition sensitivity analysis of encrypted vein images. It has been shown that the encrypted vein images, which were decrypted with a little change of the state variable in the chaotic system, were matched with unencrypted images. Thus, it has been shown that it cannot provide data security. Whereas, in the proposed system, the images encrypted with little change of state variable did not match any unencrypted images.

With the proposed study, it has been shown that the dorsal hand vein images may be used in mobile identification systems in a secure manner. In addition, the design may be used for various medical images in mobile systems when information security is required.

REFERENCES

[1] S. M. E. Hossain and G. Chetty, "Human identity verification by using physiological and behavioural biometric traits," *Int. J. Biosci., Biochemistry Bioinformat.*, vol. 1, no. 3, pp. 199–205, 2011.

[2] L. Wang, G. Leedham, and D. Siu, "Minutiae feature analysis for infrared hand vein pattern biometrics," *Pattern Recognit.*, vol. 41, no. 3, pp. 920–929, 2008.

[3] S. K. Im *et al.*, "An biometric identification system by extracting hand vein patterns," *J. Korean Phys. Soc.*, vol. 38, no. 3, pp. 268–272, 2001.

[4] M. V. N. K. Prasad and I. Kavati, "Biometric authentication based on hand vein pattern," in *Research Developments in Biometrics and Video Processing Techniques, Advances in Information Security, Privacy, and Ethics*. Hyderabad, India: IDRBT, 2014, pp. 52–64. [Online]. Available: https://www.igi-global.com/chapter/biometric-authentication-based-on-hand-vein-pattern/85985

[5] L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication," *Proc. IEEE*, vol. 91, no. 12, pp. 2019–2020, Dec. 2003.

[6] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 14, no. 1, pp. 4–20, Jan. 2004.

[7] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: Security and privacy concerns," *IEEE Security Privacy*, vol. 1, no. 2, pp. 33–42, Mar. 2003.

[8] Z. H. Liu, J. Yin, and Z. Jin, "An adaptive feature and weight selection method based on gabor image for face recognition," *Acta Photonica Sinica*, vol. 40, no. 4, pp. 636–641, 2011.

[9] X. W. Li and I. K. Lee, "Modified computational integral imaging-based double image encryption using fractional Fourier transform," *Opt. Lasers Eng.*, vol. 66, pp. 112–121, Mar. 2015.

[10] H. Liu, X. Wang, and A. Kadir, "Image encryption using DNA complementary rule and chaotic maps," *Appl. Soft. Comput.*, vol. 12, no. 5, pp. 1457–1466, 2012.

[11] X. Chai, Y. Chen, and L. Broyde, "A novel chaos-based image encryption algorithm using dna sequence operations," *Opt. Lasers Eng.*, vol. 88, pp. 197–213, Jan. 2017.

[12] P. Ping, F. Xu, and Z. J. Wang, "Image encryption based on non-affine and balanced cellular automata," *Signal Process.*, vol. 105, pp. 419–429, Dec. 2014.

[13] H. Wang, D. Xiao, M. Li, Y. Xiang, and X. Li, "A visually secure image encryption scheme based on parallel compressive sensing," *Signal Process.*, vol. 155, pp. 218–232, Feb. 2019.

[14] Y.-Q. Zhang and X.-Y. Wang, "A new image encryption algorithm based on non-adjacent coupled map lattices," *Appl. Soft. Comput.*, vol. 26, pp. 10–20, Jan. 2015.

[15] Z. Hua and Y. Zhou, "Design of image cipher using block-based scrambling and image filtering," *Inf. Sci.*, vol. 396, pp. 97–113, Aug. 2017.

[16] M. Prakash, P. Balasubramaniam, and S. Lakshmanan, "Synchronization of Markovian jumping inertial neural networks and its applications in image encryption," *Neural Netw.*, vol. 83, pp. 86–93, Nov. 2016.

[17] A. Belazi, A. A. A. El-Latif, and S. Belghith, "A novel image encryption scheme based on substitution-permutation network and chaos," *Signal Process.*, vol. 128, pp. 155–170, Nov. 2016.

[18] M. Zanin and A. N. Pisarchik, "Gray code permutation algorithm for high-dimensional data encryption," *Inf. Sci.*, vol. 270, no. 20, pp. 288–297, 2014.

[19] W. Cao, Y. Zhou, C. L. P. Chen, and L. Xia, "Medical image encryption using edge maps," *Signal Process.*, vol. 132, pp. 96–109, Mar. 2017.

[20] Y. Dai, H. Wang, and Y. Wang, "Chaotic medical image encryption algorithm based on bit-plane decomposition," *Int. J. Pattern Recognit. Artif. Intell.*, vol. 30, no. 4, p. 1657001, 2016.

[21] L. D. Singh and K. M. Singh, "Medical image encryption based on improved ElGamal encryption technique," *Optik*, vol. 147, pp. 88–102, Oct. 2017.

[22] Z. Hua, S. Yi, and Y. Zhou, "Medical image encryption using high-speed scrambling and pixel adaptive diffusion," *Signal Process.*, vol. 144, pp. 134–144, Mar. 2018.

[23] J. Zhu *et al.*, "Computational ghost imaging encryption based on fingerprint phase mask," *Opt. Commun.*, vol. 420, pp. 34–39, Aug. 2018.

[24] İ. Pehlivan, O. Kalaycı, E. Kurt, and M. Varan, "LabVIEW veArduinoUnoile Bir Kaotik Karıştırıcının Kontrolü," in *Proc. 5th Int. Symp. Innov. Technol. Eng. Sci.*, 2017, pp. 868–876.

[25] S. Vaidyanathan, A. Sambas, M. Mamat, and W. M. Sanjaya, "A new three-dimensional chaotic system with a hidden attractor, circuit design and application in wireless mobile robot," *Arch. Control Sci.*, vol. 27, no. 4, pp. 541–554, 2017.

[26] W. Zhang, J. Cao, A. Alsaedi, and F. E. S. Alsaadi, "Synchronization of time delayed fractional order chaotic financial system," *Discrete Dyn. Nature Soc.*, vol. 2017, pp. 1–5, Oct. 2017. [Online]. Available: https://www.hindawi.com/journals/ddns/2017/1230396/

[27] Y. Zhang, "A fast image encryption algorithm based on convolution operation," *IETE J. Res.*, vol. 65, no. 1, pp. 4–18, 2017.

[28] Y. Zhang, "The image encryption algorithm with plaintext-related shuffling," *IETE Tech. Rev.*, vol. 33, no. 3, pp. 310–322, 2015.

[29] G. A. Al-Suhail, F. R. Tahir, M. H. Abd, V.-T. Pham, and L. Fortuna, "Modelling of long-wave chaotic radar system for anti-stealth applications," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 57, pp. 80–96, Apr. 2018.

[30] A. Akgul, S. Hussain, and İ. Pehlivan, "A new three-dimensional chaotic system, its dynamical analysis and electronic circuit applications," *Optik*, vol. 127, no. 18, pp. 7062–7071, 2016.

[31] A. Ozdemir, İ. Pehlivan, A. Akgul, and E. Guleryuz, "A strange novel chaotic system with fully golden proportion equilibria and its mobile microcomputer-based RNG application," *Chin. J. Phys.*, vol. 56, no. 6, pp. 2852–2864, 2018.

[32] V. Sundarapandian and İ. Pehlivan, "Analysis, control, synchronization, and circuit design of a novel chaotic system," *Math. Comput. Model.*, vol. 55, nos. 7–8, pp. 1904–1915, 2012.

[33] İ. Pehlivan and Y. Uyaroğlu, "Simplified chaotic diffusionless Lorentz attractor and its application to secure communication systems," *IET Commun.*, vol. 1, no. 5, pp. 1015–1022, Oct. 2007.

[34] S. Çiçek, Y. Uyaroğlu, and İ. Pehlivan, "Simulation and circuit implementation of Sprott case H chaotic system and its synchronization application for secure communication systems," *J. Circuits, Syst. Comput.*, vol. 22, no. 4, p. 1350022, 2013.

[35] Y. Uyaroğlu and İ. Pehlivan, "Nonlinear Sprott94 case A chaotic equation: Synchronization and masking communication applications," *Comput., Electr. Eng.*, vol. 36, no. 6, pp. 1093–1100, 2010.

[36] İ. Pehlivan and Y. Uyaroğlu, "A new 3D chaotic system with golden proportion equilibria: Analysis and electronic circuit realization," *Comput., Electr. Eng.*, vol. 38, no. 6, pp. 1777–1784, 2012.

[37] A. Akgul and İ. Pehlivan, "A new three-dimensional chaotic system without equilibrium points, its dynamical analyses and electronic circuit application," *Tehnicki Vjesnik Tech. Gazette*, vol. 23, no. 1, pp. 209–215 2016.

[38] G. Q. Si, H. Cao, and Y. B. Zhang, "A new four-dimensional hyperchaotic Lorenz system and its adaptive control," *Chin. Phys. B*, vol. 20, no. 1, p. 010509, 2011.

[39] E. Fatemi-Behbahani, E. Farshidi, and K. Ansari-Asl, "Analysis of chaotic behavior in pipelined analog to digital converters," *AEU–Int. J. Electron. Commun.*, vol. 70, no. 3, pp. 301–310, 2016.

[40] S. Çiçek, A. Ferikoğlu, and İ. Pehlivan, "A new 3D chaotic system: Dynamical analysis, electronic circuit design, active control synchronization and chaotic masking communication application," *Optik*, vol. 127, no. 8, pp. 4024–4030, 2016.

[41] I. Çiçek, A. E. Pusane, and G. Dundar, "A novel design method for discrete time chaos based true random number generators," *Integr.*, vol. 47, no. 1, pp. 38–47, 2014.

[42] M. Park, J. C. Rodgers, and D. P. Lathrop, "True random number generation using CMOS Boolean chaotic oscillator," *Microelectron. J.*, vol. 46, no. 12, pp. 1364–1370, 2015.

[43] İ. Koyuncu and A. T. Özcerit, "The design and realization of a new high speed FPGA-based chaotic true random number generator," *Comput., Electr. Eng.*, vol. 58, pp. 203–214, Feb. 2017.

[44] P. Amorim, T. Moraes, J. Silva, and H. Pedrini, "3D adaptive histogram equalization method for medical volumes," in *Proc. 13th Int. Joint Conf. Comput. Vis., Imag. Comput. Graph. Theory Appl.*, 2018, pp. 363–370.

[45] E. N. Lorenz, "Deterministic nonperiodic flow," *J. Atmos. Sci.*, vol. 20, no. 2, pp. 130–141, 1963.

[46] K. Yonemoto and T. Yanagawa, "Estimating the Lyapunov exponent from chaotic time series with dynamic noise," *Stat. Methodol.*, vol. 4, no. 4, pp. 461–480, 2007.

[47] P. Stavroulakis, *Chaos Applications in Telecommunications*. Boca Raton, FL, USA: CRC Press, 2006, pp. 125–169.

[48] K. T. Chau and Z. Wang, *Chaos in Electric Drive Systems*. 2011, pp. 3–44. [Online]. Available: https://onlinelibrary.wiley.com/doi/book/10.1002/9780470826355 and https://ieeexplore.ieee.org/book/6016258

[49] M. Sandri, "Numerical calculation of Lyapunov exponents," *Math. J.*, vol. 6, pp. 78–84, 1996.

[50] A. Wolf, J. B. Swift, H. L. Swinney, and J. A. Vastano, "Determining Lyapunov exponents from a time series," *Phys. D, Nonlinear Phenomena*, vol. 16, no. 3, pp. 285–317, 1985.

[51] F. E. Yardim and E. Afacan, "Lorenz-Tabanli Diferansiyel Kaos Kaydirmali Anahtarlama (DCSK) Modeli Kullanilarak Kaotik Bir Haberleşme Sisteminin simülasyonu," *Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi*, vol. 25, no. 1, pp. 101–110, 2010.

[52] J. L. Kaplan and J. A. Yorke, "Numerical solution of a generalized eigenvalue problem for even mappings," in *Functional Differential Equations and Approximation of Fixed Points*. Berlin, Germany: Springer, 1979, pp. 228–237.

[53] A. Rukhin *et al.*, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Dept. Comput. Secur. Division, Inf. Technol. Lab., Nat. Inst. Standards Technol.–U.S. Dept. Commerce, Washington, DC, USA, Tech. Rep., 2000. [Online]. Available: https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=151231

[54] S. L. Hong and C. Liu, "Sensor-based random number generator seeding," *IEEE Access*, vol. 3, pp. 562–568, 2015.

[55] G. L. Re, F. Milazzo, and M. Ortolani, "Secure random number generation in wireless sensor networks," in *Proc. 4th Int. Conf. Secur. Inf. Netw. (SIN)*, 2011, pp. 175–182.

[56] L. E. Bassham *et al.*, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," Nat. Inst. Standards Technol.–U.S. Dept. Commerce, Washington, DC, USA, Tech. Rep., 2010. [Online]. Available: https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=906762

[57] H. Bay, A. Ess, T. Tuytelaars, and L. Van Gool, "Speeded-up robust features (SURF)," *Comput. Vis. Image Understand.*, vol. 110, no. 3, pp. 346–359, 2008.

[58] A. Gupta, R. Thawait, K. A. K. Patro, and, B. Acharya, "A novel image encryption based on bit-shuffled improved tent map," *Int. J. Control Theory Appl.*, vol. 9, no. 34, pp. 1–16, 2016.

[59] S. Behnia, A. Akhshani, H. Mahmodi, and A. Akhavan, "A novel algorithm for image encryption based on mixture of chaotic maps," *Chaos, Solitons, Fractals*, vol. 35, no. 2, pp. 408–419, 2008.

[60] A. Akhshani, A. Akhavan, S. C. Lim, and Z. Hassan, "An image encryption scheme based on quantum logistic map," *Commun. Nonlinear Sci. Numer. Simul.*, vol. 17, no. 12, pp. 4653–4661, 2012.

[61] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, 1949.

[62] A. H. Abdullah, R. Enayatifa, and M. Lee, "A hybrid genetic algorithm and chaotic function model for image encryption," *AEU–Int. J. Electron. Commun.*, vol. 66, no. 10, pp. 806–816, 2012.

[63] A. Kerckhoffs, "La cryptographie militaire," *J. Des. Sci. Militaires*, vol. 9, pp. 5–83, 1883.

[64] Y. Mao, G. Chen, and S. Lian, "A novel fast image encryption scheme based on 3D chaotic baker maps," *Int. J. Bifurcation Chaos*, vol. 14, no. 10, pp. 3613–3624, Oct. 2004.

[65] C. Fu, J. J. Chen, H. Zou, W. H. Meng, Y.-F. Zhan, and Y.-W. Yu, "A chaos-based digital image encryption scheme with an improved diffusion strategy," *Opt. Express*, vol. 20, no. 3, p. 2363, 2012.

[66] P. Praveenkumar, R. Amirtharajan, K. Thenmozhi, and J. B. B. Rayappan, "Pixel scattering matrix formalism for image encryption—A key scheduled substitution and diffusion approach," *AEU–Int. J. Electron. Commun.*, vol. 69, no. 2, pp. 562–572, 2015.

[67] X. Chen and C. J. Hu, "Adaptive medical image encryption algorithm based on multiple chaotic mapping," *Saudi J. Biol. Sci.*, vol. 24, no. 8, pp. 1821–1827, 2017.

[68] N. K. Pareek, V. Patidar, and K. K. Sud, "Image encryption using chaotic logistic map," *Image Vis. Comput.*, vol. 24, no. 9, pp. 926–934, 2006.

[69] J. Zhang, D. Hou, and H. Ren, "Image encryption algorithm based on dynamic DNA coding and Chen's hyperchaotic system," *Math. Problems Eng.*, vol. 2016, pp. 1–11, Aug. 2016.

[70] Y. Zhou, W. Cao, and C. P. Chen, "Image encryption using binary bitplane," *Signal Process.*, vol. 100, pp. 197–207, Jul. 2014.

[71] X.-Y. Wang, Y.-Q. Zhang, and X.-M. Bao, "A novel chaotic image encryption scheme using DNA sequence operations," *Opt. Lasers Eng.*, vol. 73, pp. 53–61, Oct. 2015.

[72] X. Wang and H.-L. Zhang, "A color image encryption with heterogeneous bit-permutation and correlated chaos," *Opt. Commun.*, vol. 342, pp. 51–60, May 2015.

[73] L. Xu, Z. Li, J. Li, and W. Hua, "A novel bit-level image encryption algorithm based on chaotic maps," *Opt. Lasers Eng.*, vol. 78, pp. 17–25, Mar. 2016.

[74] M. Kaur and V. Kumar, "Efficient image encryption method based on improved Lorenz chaotic system," *Electron. Lett.*, vol. 54, no. 9, pp. 562–564, 2018.

[75] A. Ullah, S. S. Jamal, and T. Shah, "A novel scheme for image encryption using substitution box and chaotic system," *Nonlinear Dyn.*, vol. 91, no. 1, pp. 359–370, 2018.

[76] Z. Li, C. Peng, L. Li, and X. Zhu, "A novel plaintext-related image encryption scheme using hyper-chaotic system," *Nonlinear Dyn.*, vol. 94, no. 2, pp. 1319–1333, 2018.

[77] Ü. Çavuşoğlu, S. Kaçar, A. Zengin, and İ. Pehlivan, "A novel hybrid encryption algorithm based on chaos and S-AES algorithm," *Nonlinear Dyn.*, vol. 92, no. 4, pp. 1745–1759, 2018.

[78] M. L. Sahari and I. Boukemara, "A pseudo-random numbers generator based on a novel 3D chaotic map with an application to color image encryption," *Nonlinear Dyn.*, vol. 94, no. 1, pp. 723–744, 2018.

M. Z. YILDIZ received the Ph.D. degree in biomedical engineering from Boğaziçi University, Istanbul, Turkey, in 2013. He is currently a Faculty Member with the Electrical and Electronics Engineering, Sakarya University of Applied Sciences, Sakarya, Turkey, and also the Director of the Biomedical Laboratory, Sakarya University of Applied Sciences. His research interests include biomedical instrumentation, biomedical signal processing, and bio-optics.

O. F. BOYRAZ received the M.S. degree in electrical and electronics engineering from Sakarya University, Sakarya, Turkey, in 2015, where he is currently pursuing the Ph.D. degree. He is also the Research Assistant with the Biomedical Laboratory, Sakarya University of Applied Sciences. His research interests include biomedical instrumentation, image processing, pattern recognition, data encryption, and medical electronics.

E. GULERYUZ graduated in electrical and electronics engineering from Sakarya University, Sakarya, Turkey, in 2016. He is currently pursuing the M.S. degree in electronics engineering with the Sakarya University of Applied Sciences. His research interests include chaos, data encryption, data security, nonlinear systems, image processing and digital, and analog signal processing.

A. AKGUL received the B.Sc. degree in electronics-computer education from Kocaeli University, in 2009 and in electrical- electronics engineering from Sakarya University, in 2013, and the M.S. degree in electronics computer education and the Ph.D. degree in electrical-electronics engineering from Sakarya University, in 2011 and 2015, respectively. He has joined the Institute of Electronics, Communications and Information Technology (ECIT), Queen's University Belfast, U.K., in 2015, as a Visiting Researcher. He is currently a Faculty Member with the Department of Electrical and Electronics Engineering, Sakarya University of Applied Sciences, Sakarya, Turkey. His current interest includes analog electronics, chaos theory, chaotic systems, chaos-based engineering applications (cryptography, steganography, pseudo, and true random number generators), experimental chaotic synchronization, analysis and design of analog circuits, and microcomputer-based applications.

I. HUSSAIN received the Ph.D. degree in mathematics from Quaid-i-Azam University, Pakistan, in 2014. He is currently an Assistant Professor with Qatar University. His h-index score is 23 and i-10 index score is 34. His research interests include the applications of mathematical concepts in secure communication and cybersecurity. He has published 67 papers in well-known journals in these areas.