Securing Privacy in BSN with Chaos Based Image Encryption Scheme

[1]Harshvardhan Tiwari, [2]Shilpa N, [2]Harshitha R, [2]Rakshatha S, [2]Archana K N
[1]Centre for Incubation, Innovation, Research and Consultancy, Jyothy Institute of Technology, Tataguni, Bengaluru-560082
[2]Department of Information Science & Engineering, Jyothy Institute of Technology, Tataguni, Bengaluru-560082

Abstract

BSN play the vital role in the field of telemedicine. In BSN sensor nodes transmit different physiological information, thus privacy and security of these information become very important in these networks. In this paper we have presented a simple and secure scheme for image encryption using one-dimensional chaotic maps. This image encryption scheme first shuffles the position of pixel values using bit-level permutation method and then changes the gray values to make the complex relationship between original plain image and encrypted image. Image scrambling and diffusing, both operations are performed by logistic map and tent map. Various experiments have been conducted to test the robustness and security of proposed image cipher algorithm and the experimental results shows that the proposed scheme is resistant to different cryptanalytic attacks and provides adequate security.

Keywords: *BSN; Privacy, Encryption, Permutation, Logistic map, Tent map*

INTRODUCTION

Body Sensor Networks includes wearable and sensor nodes that collects biological information from the human body and transfers to a control device which is located on a reachable and accessible distance. These sensors senses vital body physiological signals such as electrocardiogram (ECG), photoplethysmogram (PPG), electroencephalography (EEG), pulse rate, respiration, oxygen saturation, pressure, and body temperature. Control device then transmits this medical information to remote networks for medical diagnosis purpose. The received important physiological signals at remote network can be stored and shared by different medical professionals. The servers at remote site should provide adequate privacy and confidentiality protection to patient's data. Therefore, these vital medical information need to be ciphered before sharing and storing at any other network site. There are two ways to provide the data encryption to protect the data confidentiality: first is between the sensor and the control device and the second is between the control device and remote network server site. The later is more important as it includes the patient information which is transmitted over the network.

Many encryption approaches have been applied to secure privacy of medical data. Identity-Based Encryption scheme (IBE) has been introduced by Shamir in 1985 [1]. IBE is different traditional encryption schemes as it uses any arbitrary string to encrypt the data in place of private-public key pair. In 2001 [2] Boneh and Franklin proposed the first secure and practical IBE scheme which is composed of four sub-schemes. This scheme encrypts the data with the help of master key and an arbitrary public key. In [3] Tan and team have studied Attribute-Based Encryption scheme. They analyzed the suitability of Key-Policy Attribute-Based Encryption scheme (KP-ABE) and Cipher text-Policy Attribute-Based Encryption scheme on BSN. They found KP-ABE is preferable for the body sensor network. In [4] different symmetric as well as asymmetric encryption algorithms have been proposed to provide secure transfer of data. In [5], a single secret key based approach is proposed to ensure security in data transfer for BSN, but this approach is vulnerable to attacks. All mentioned methods were weak due to small key space, low key sensitivity and poor randomness. Over the past two decades, the nonlinear chaotic systems have been widely used in image encryption as compared due to its characteristics such as high sensitivity to initial conditions and system parameters, pseudo-randomness, non-periodicity, and ergodicity. Fridrich in [6] has shown that dynamical chaotic maps possess good potential for symmetric image encryption scheme. In this paper, a novel image encryption algorithm based on 1-D maps is proposed. The proposed scheme combines the advantages of logistic map and tent map. There are many 1-D chaotic maps; selection of the chosen maps is based on values of Lyapunov exponent as higher exponent value represents more chaotic nature of the map. In the permutation process bit-level permutation is employed. In the diffusion stage the merits of logistic map and tent map are combined.

The rest of paper is organized as follows. In Section 2 the chaotic maps are discussed. In Section 3 image encryption algorithm is presented. Its performance and security is analysed in Section 4. Finally we concluded the paper in Section 5.

CHAOTIC MAP

Cryptographic encryption techniques provide the effective security to data by converting it into un-understandable form to attackers. Public key based cryptographic encryption algorithms are widely used in a large number of applications. One possible way of digital image protection is to use well-known and traditional cryptographic algorithms such as DES, Blowfish, AES, and IDEA to mask the digital image information. However the encryption of image is not similar to the encryption of text. Intrinsic features of images, such as large data capacity, high redundancy and high correlation among adjacent pixels make image encryption very complex.

Due to above mentioned features and high computation requirements these traditional text encryption algorithms are not suitable for the encryption of image. Chaotic theory has drawn wide attention among researchers so far, since it is very sensitive to system parameters and initial values. These distinct features make the chaos system more ergodic [7, 8]. Chaotic system strengthens various security applications by its unique chaotic characteristics and makes it different from traditional text encryption algorithms. Thus, chaotic encryption system has great importance in information security field because of its easy to control, deterministic and pseudo-random behavior [9, 10].

Logistic Map

The Logistic map presents a polynomial map of degree two. It is equivalent to the recurrence relation. It is a simple and one-dimensional discrete-time non-linear system. This widely used function exhibits quadratic non-linearity and is defined by following equation [1]:

Tent Map

Tent map is a simple one-dimensional chaotic map use in cryptographic applications. The tent map is known as its tent like shape in the graph of its bifurcation diagram. The bifurcation figure of one-dimensional Tent map has been shown in Figure 1(b). The can defined by the following equation[2]

$$x_n = \lambda x_{n-1}(1 - x_{n-1}) \quad (1)$$

$$x_{i+1} = f(x_i, \mu) \quad (2)$$

$$f(x_i, \mu) = \begin{cases} f_L(x_i, \mu) = \mu x_i, \text{ if } x_i < 0.5 \\ f_R(x_i, \mu) = \mu(1 - x_i), \text{ otherwise} \end{cases}$$

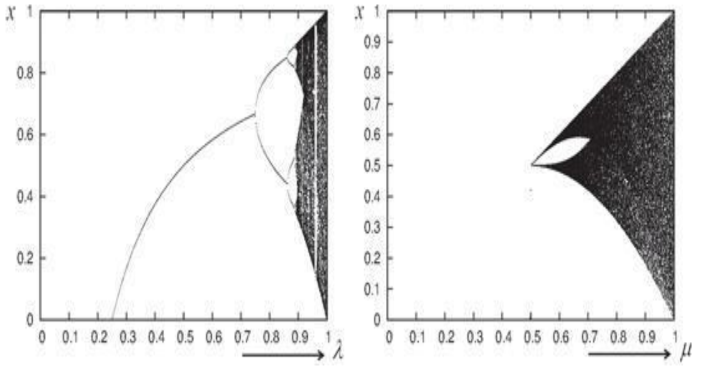

Fig 1. *Bifurcation diagram (a) Logistic Map (b)Tent Map*

Where λ is a control parameter and it lies between 0 and 4. The chaotic sequence is represented by x_n and it lies between 0 and 1. The logistic map becomes chaotic when the control parameter lies between 3.57 and 4. The bifurcation figure of one-dimensional logistic map has been shown in Figure 1(a). The diagram presents periodic windows in fixed intervals. The existence of periodic windows must be avoided; otherwise the ciphertext would not show random-like behaviour and resulting in an inefficient encryption procedure [5].

PROPOSED ENCRYPTION ALGORITHM

Encryption algorithm includes two procedures, permutation and diffusion. Permutation procedure is used to change the position of the pixels in the image whereas diffusion is used to change the values of pixels. There are two ways of performing the permutations: one is pixel permutation and other is bit-permutation. In pixel permutation the pixel is considered as a smallest unit of an image and its position is scrambled. In this procedure the distribution of gray-gray scales of image remains unchanged. In bit-level permutation pixel is converted to binary-bits and then these bits are scrambled [13]. Bit-level permutation performs shuffling as well as diffusion. In diffusion procedure a chaotic matrix is formed for changing the values of pixels in image.

Confusion Phase

A plain image of size $h \times w$ is converted to the matrix. Then each pixel value is converted to the corresponding binary values. We get a new binary matrix of $h \times 8w$ size. Bit-level permutation includes permutation in row direction then permutation in column direction. The permutation in row direction includes following steps:

a) An integer sequence is generated randomly $T = \{t_1, ,t_h\}$ where T is a permutation of integers.
b) Generate the two random sequences R_x, R_y with *8wh* elements by iterating Logistic map.
c) Sort the R_x, R_y random sequence in ascending order and get two index orders sequences.
d) Convert $h \times 8w$ matrix to 1-dimensional sequence with row order $T = \{t_1, ,t_h\}$ and reshape sequence to row permuted image. Row permutation

is over.

The permutation in column direction is similar to row permutation. Steps for column permutation are explained below:

a) An integer sequence is generated randomly $S = \{s_1 , , s_{8w}\}$ where S is a permutation of integers.
b) Extend the row-permutated image matrix to a 1-dimensional binary sequence with column order $S = \{s_1 , , s_{8w}\}$.
c) Reshape the binary sequence to a 2-dimensional matrix.
d) After the row and column permutation, we get the permutated binary matrix M_{rc}
e) Finally, convert all binary bit sequences to pixel values and form scrambled image matrix M'.

Diffusion Phase

Confusion phase generates a scrambled image with bit-level permutation. This scrambled image is still vulnerable to attacks as it can reveal some information to attacker through histogram analysis. In diffusion phase we change the values of scrambled image pixels obtained from confusion phase. Steps for diffusion phase are explained below:

a) Set the initial parameter values in Logistic map and build sub-chaotic matrix *SI* according to the generated one-dimensional chaotic sequence.
b) Set the initial parameter values in Tent map and build another sub-chaotic matrix *SJ* according to the generated one-dimensional chaotic sequence.
c) Combine sub-chaotic matrices *SI* and *SJ* to obtain the chaotic encrypted matrix *E*.
d) Perform XOR operation on the scrambled image matrix
e) M' and the chaotic encrypted matrix *E* to get the final encrypted image.

EXPERIMENTS

This section evaluates performance and security of given image encryption scheme. For experiments we have taken gray-scale images of different sizes. The experiments have been carried out on a 1.70 GHz Intel Core i3, 4 GB memory. Figure 2 shows the original images and corresponding cipher image respectively. Experiments results show that effect of encryption process is good, as the Logistic map and Tent map generate the random chaotic sequences. It shows high sensitivity to initial conditions and key. Any change in secret key generates a different encrypted or deciphered image. Different tests [14] have been conducted to test the security of scheme which is discussed below.

Analysis of Histogram

The image histogram is used to represent the distribution of pixels at different gray levels. Histogram of an image plots number of pixels at each gray intensity level. One can take out a great deal of statistical information about image from its histogram. The encrypted image histogram should have a meaningful information from uniform distribution of encrypted image. Figure 3 represents the original images and corresponding cipher images with histogram. The histograms of cipher images are representing uniform spikes. It shows that encrypted image does not reveal the statistical similarity structure of the original images to attacker. It becomes extremely difficult to implement any statistical attack on the scheme.

Analysis of Correlation Coefficients

In all kinds of images, usually there exists a strong correlation between two adjacent pixels. Any image encryption scheme should generate cipher image with a little correlations between two adjacent pixels. The correlation coefficient factor provides the difference measure between original image and its encrypted variant. This basic dissimilarity factor, correlation coefficient factor, between two images has been calculated by using the formulas

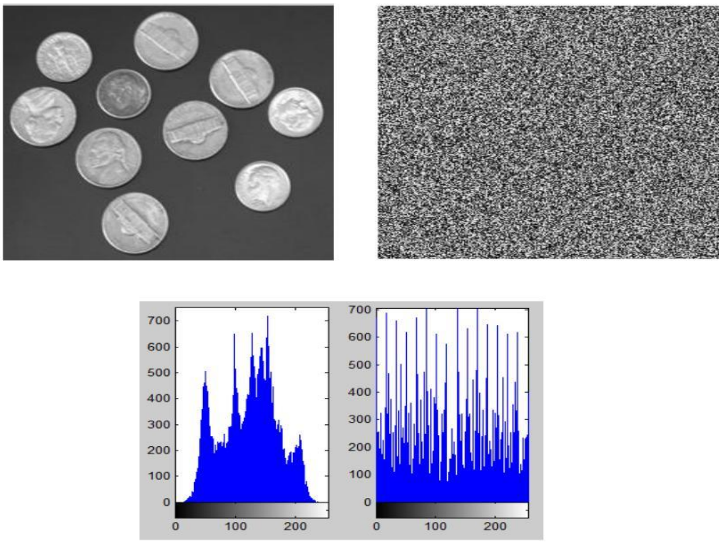

Fig 2. *Original images and corresponding cipher image*

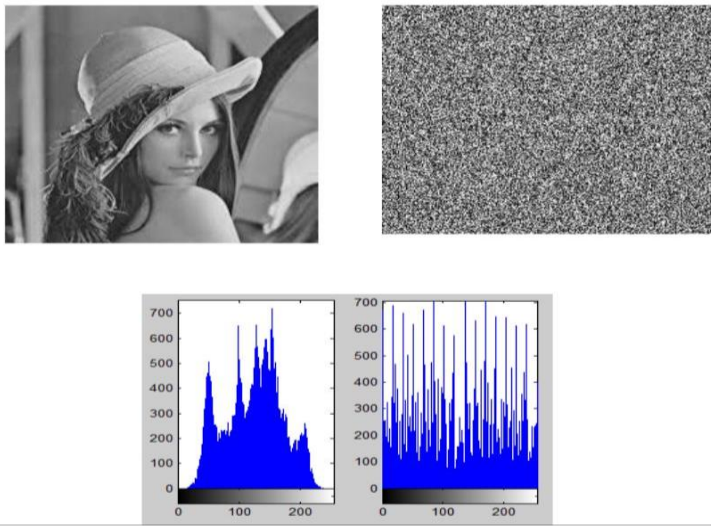

Fig 3. *Cipher images and corresponding histogram*

$$\zeta_{xy} = \frac{\text{cov}(x, y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad \ldots\ldots (3)$$

$$\text{cov}(x, y) = Exp(x - Exp(x))(y - Exp(y)) \quad \ldots\ldots (4)$$

$$Exp(x) = \frac{1}{n}\sum_{i=1}^{n} x_i, \; D(x) = \frac{1}{n}\sum_{i=1}^{N}[x_i - Exp(x)]^2 \quad \ldots\ldots (5)$$

The gray-scale values of two adjacent pixels in the image are represented by x and *y*. *Exp(x)* is the expectation of variable *x* and *D(x)* is a variance of variable *x*. The results of tests are given in the Table 1. From the result we draw the conclusion that the calculated values for correlation coefficients are very low i.e. near to zero and correlation coefficients of original image are almost close to 1. It indicates that the adjacent pixels in the encrypted image are not correlated.

Analysis of Entropy

The entropy is a statistical measure of uncertainty and randomness of information. One can also use this criterion to show the uncertainty present in image. It also expresses the distribution of gray levels in the image. In general entropy of image represents the total number of bits required for encoding the each pixel of the image. The ideal value for image entropy of the cipher image is 8. This measure of randomness and uncertainty of gray-scale values is described by following:

$$E = \sum_{i=0}^{n} p_i \log_2 p_i \qquad (6)$$

where n is the total number of gray levels. Total 256 gray levels are possible for an image. p_i is the probability of occurrence of intensity i in the given image. p_i is determined by dividing the number of pixels with intensity i with the total number of pixels present in the image. The $\log_2$ represents the base-2 logarithm which is used to calculate the image entropy in bits. The calculation of image entropy is performed for the cipher images, produced by the proposed encryption algorithm. Table 1 shows the calculated entropy values for encrypted images. Calculated experimental value for cipher image is very close to 8 that mean the encryption algorithm is not vulnerable to information entropy attack.

Table 1. *Correlation coefficients and entropy information of cipher image*

Image	Entropy	Correlation Coefficients	
		Original Image	Ciphered Image
Coins	7.942	0.9987	0.0276
Lena	7.942	0.9865	0.0053
Baboon	7.942	0.9934	0.0270
Peppers	7.942	0.9856	0.0091

Analysis of key sensitivity

We take original images of different sizes for the study of the sensitivity of our algorithm. The chaotic sequences are generated by taking for $x_0 = 0.0934$, $\lambda = 3.9138$ logistic map and for tent map $x_0 = 0.0001$, $\mu = 1.9999$ for encryption purpose. Now, if we decrypt it using $x_0 = 0.0934$, $\lambda = 3.9138$ and $x_0 = 0.0001$, $\mu = 1.9999$. From the Figure 4 it is noticed that with wrong key, we get completely different decrypted images

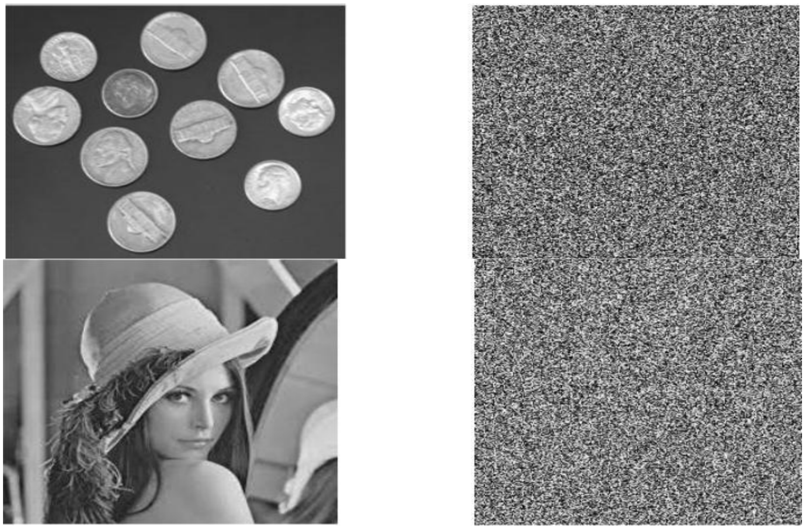

Fig 4. *Key sensitivity results*

CONCLUSION

This paper presented a simple image encryption scheme. It confuses an image matrix with bit-level permutation and then diffuses the pixels to generate the final cipher image. Confusing and shuffling are performed with the help of logistic map and tent map. Different experiments demonstrate that given scheme for image encryption is strong enough to statistical and other cryptanalytic attacks.

REFERENCES

1. Shamir, A. : (1985) "Identity-Based Cryptosystems and Signature Schemes" CRYPTO'85 , 196: 47–53.
2. Boneh, D.; Franklin, M.: (2001) "Identity-Based Encryption from the Weil Pairing" CRYPTO'01, 2139: 213–229.
3. A. Abd Manaf et al.: (2011) "A Study of Attribute-Based Encryption for Body Sensor Networks" ICIEIS,251: 238–247.
4. Jang, C.S.; Lee, D.G.; Han, J.-W.; Park, J.H.: (2011) "Hybrid security protocol for wireless body area networks", 11: 277–288.
5. Bao, S.D.; Shen, L.F.; Zhang, Y.T. : (2004) "A Novel Key Distribution of Body Area Networks for Telemedicine, In Proceedings of the 2004 IEEE International Workshop on Biomedical Circuits and Systems", 1-17.
6. Fridrich, J.: (1998) "Symmetric Ciphers Based on Two-Dimensional Chaotic Maps", 8: 1259–1284.
7. M. S. Baptista. : (1998) "Cryptography with chaos," 240: 50–54.
8. R. Matthews. : (1989) "On the derivation of a chaotic encryption algorithm" 13: 29-42.
9. S.Li et al.: (2004) "Baptista-type chaotic cryptosystems: problems and countermeasures" 332: 368-375.
10. R.M. May. : (1976) "Simple mathematical models with very complicated dynamics" 261: 459–467.
11. E. A. Jackson and A. H¨ubler. : (1990) "Periodic entrainment of chaotic logistic map dynamics" 44: 407–420.
12. T. Yoshida, H. Mori, and H. Shigematsu. : (1983) "Analytic study of chaos of the tent map: band structures, power spectra, and critical behaviors" 31: 279–308.
13. Hegui Zhu, Cheng Zhao, Xiangde Zhang, Lianping Yang.: (2014) "An image encryption scheme using generalized Arnold map and affinecipher", Optik-International Journal for Light and Electron Optics 125.22: 6672-6677.
14. A.L. Rukhin et al.: (2010) "A statistical test suite for random and pseudorandom number generators for cryptographic applications" 800-22.