International Journal of Computer Applications (0975 - 8887)
National Conference on Electronics, Signals and Communication - 2017

Auto-Blocking based Image Encryption using ECG Signal

Kiran
Assistant Professor
Dept. of Electronics and communication Engineering
GMIT, Mandya
Karnataka

Parameshachari B. D., PhD
Professor and Head
Dept. of Telecommunication Engineering
GSSIETW, Mysuru
Karnataka

Sahana V. S.
UG student
Dept. of Electronics and communication Engineering
GMIT, Mandya
Karnataka

Apoorva C.
UG student
Dept. of Electronics and communication Engineering
GMIT, Mandya
Karnataka

Thanuja B. S.
UG student
Dept. of Electronics and communication Engineering
GMIT, Mandya
Karnataka

ABSTRACT

A novel image encryption algorithm is designed based on auto-blocking and a medical ECG signal. The chaotic logistic map and generalized Arnold map will be employed. ECG signal and wolf algorithm are used to generate initial conditions for the chaotic maps. Auto-blocking diffusion operation is performed only in the encryption process. The keystream is generated by a control parameter produced from the plain-image, which is proven to be secure against chosen-plaintext and known-plaintext attacks. Experimental results show that the proposed algorithm can achieve high security with good performance.

General Terms

Image encryption,auto-blocking,ECG signal.

Keywords

Diffusion,chatioc maps

1. INTRODUCTION

Digital image information can be widely accessed through internet and via wireless networks. Image is known to be different from text due to its bulky data capacity, redundancy and strong co-relation between adjacent pixels. Protection of image is inherently different from text. With the rapid advancement of network technologies, highly secure algorithms are needed for safeguarding digital images and protecting private and unauthorized images from being illegally visited, copied or modified. A novel chaotic based image encryption algorithm is proposed in this paper in which ECG signal is used to generate the initial keys. The encryption algorithm can implement auto-blocking for image matrix. The way to perform encryption is to perform permutation operation followed by diffusion operation. If two stages of permutation and diffusion are separated in an algorithm, then the security of the algorithm will depend on diffusion only. Here ECG signal can be directly acquired from a live human body was not considered in this work. The objectives are Encrypted algorithm may resist all kinds of differential attacks. High security to the image/data. It may resist sufficiently Brute force attack. A novel image encryption algorithm uses electrocardiography to generate initial keys and an auto-blocking method to remove the need for manual assignment. It has proven complex, strong, and flexible enough for practical applications.

1.1 Chaotic Map

Chaotic maps show excellent results towards encryption of video files. Programmers who work on cryptography and cryptosystems relevant to video, are very much interested towards chaotic maps due to the interesting bondage between cryptography and chaos. Chaotic properties like sensitive to system parameters/initial conditions, ergodicity, etc are equivalent to diffusion, confusion of cryptography. Chaotic systems exhibit non linearity and behave randomly for few ranges of system parameters. Such systems are spontaneous and will be applicable to security procedures directly.

$$X(i+1) = \mu X(i)(1 - X(i)) \tag{1}$$

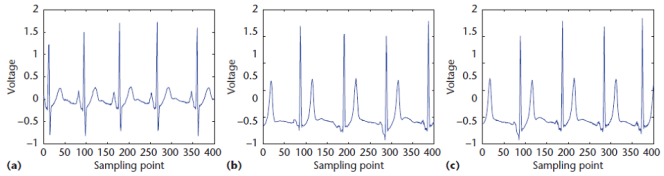


Fig. 1. ECG signal for a) Person A b) Person B c) Person B at different time

where μ is the cotrol parameter and the ogistic system is in chaos when $\mu \in [0, 4]$.

2. ECG SIGNAL

ECG is typically defined as a simple, noninvasive procedure that cyclically reports the successive a trial depolarization/repolarization and ventricular depolarization/repolarization that occur in each heartbeat (see Figure 3a).14 No precise mathematical model exists for cardiac electrical activity due to the complexity of the human bodys biological system. Moreover, ECG signals are significantly varied for different persons and even for the same person at different times. Figures 3b and 3c show the ECG signals for the same person at two different times. So, ECG signals cannot be copied or simulated precisely.

3. WOLF ALGORITHM FOR INITIAL CONDITIONS

Ching-Kun Chen and his colleagues have proposed a method for generating a secret key from an ECG signal. They calculate the largest Lyapunov exponent to extract ECG features using the Wolf algorithm. The algorithm first calculates the distance of two nearby points in the phase space of the signal, denoting it as . Then it computes again the new distance when these two points are moved a short distance in the phase space. If is too large, one of these two points will be kept and the other will be replaced by a new one in the same orbit. Finally, the largest Lyapunov exponent is obtained using the following equation after q iterations:

$$\lambda = \frac{1}{tq - t0} \sum_{k-1}^{q} log \frac{s1(k)}{s0(tk-1)} \tag{2}$$

The mathematical model described by Equation (4)generates three initial conditions for the generalized Arnoldmap and the logistic map:

$$\begin{aligned} x0 &= abs(\lambda) \\ y0 &= abs(\lambda) * 10^5 - floor(abs(\lambda) * 10^5) \\ x0bar &= abs(\lambda) * 10^8 - floor(abs(\lambda) * 10^5) \end{aligned} \tag{3}$$

4. AUTOBLOCKING METHOD

Suppose that a plain-image has size M*N, and the block numbers size is p1*p2.Here, p1 and p2 should not be too big or too small, since too big a size will result in a small block and too small will increase computation. Table 2 shows nine cases of block sizes for a 256_256 plain-image. Here, we consider only images of size 256_256 without loss of generality; other cases can be discussed similarly.

For example, if =2 and =1, then the corresponding block number will be (32,16)=(p1, p2), as shown in Table 2, with block size 8 16. Clearly, the autoblocking method depends on the outputs of the logistic map and the initial conditions from the ECG signals.

Table 1. Blocking size for 256*256

	0	1	2
0	(8,8)	(8,16)	(8,32)
1	(16,8)	(16,16)	(16,32)
2	(32,8)	(32,16)	(32,32)

5. PROPOSED METHOD

With initial conditions and given by Equation(4), we can get iterated values from the system in Equation (2).Assuming that the size of a sub-block is and using a starting control parameter r, we can collect a set of values of length MN: d= ,which is then converted into a pseudorandom matrix D of size M N. Like the division of the plain-image, we divide matrix D into r1 r2 blocks,with each block size being p1p2.

We consider and implement only the diffusion operation, as follows:

$$\begin{aligned} C1 &= A1 + vD1 + C0 \\ C2 &= A2 + vD2 + C1 \\ &\ldots\ldots\ldots\ldots \\ &\ldots\ldots\ldots\ldots \\ &\ldots\ldots\ldots\ldots \\ Cr1, r2 &= Ar1, r2 + Cr1, r2 - 1 \end{aligned} \tag{4}$$

Here, and denote the current and former cipher-image blocks, respectively; is a constant block; v is a new control parameter; and and are the ith blocks of the plain-image and the pseudorandom matrix, respectively. Notice that, before performing diffusion, the classical encryption architecture should include a permutation operation in the first stage. On the other hand, the two processes of permutation and diffusion will become independent when the plain-image is a homogeneous one with identical pixels.1 As a result, the security of the whole algorithm will rely only on diffusion. Based on these analyses, the proposed method considers only the diffusion process.

6. EXPERIMENTAL RESULTS AND PERFORMANCE ANALYSIS

6.0.1 Information entropy analysis. In information theory, entropy is the most significant feature of disorder, or more precisely unpredictability. To calculate the entropy H(X) of a source x, we have:

$$H(X) = \sum_{i=1}^{n} Pr(x_i) \log_2 \frac{1}{Pr(x_i)} \tag{5}$$

where X denotes the test image, x_i denotes the i^th possible value in X, and Pr(x_i) is the probability of X =x_i, that is, the probability of pulling a random pixel in X and its value is xi. For a truly random source emitting 2N symbols, the entropy is H(X)=N. therefore, for a ciphered image with 256 gray levels, the entropy should ideally be H(X)=8. If the output of a cipher emits symbols with entropy less than 8, there exists certain degree of predictability, which threatens its security. The entropies for plain image and ciphered images using various images are calculated in Table 2. Apparently, the proposed algorithm is much closer to the ideal situation. This means that information leakage in the encryption process is negligible and the cryptosystem is secure against entropy attack.

Table 2. Input and Encrypted Video frames

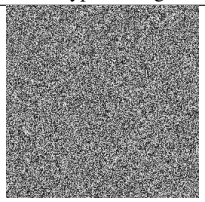
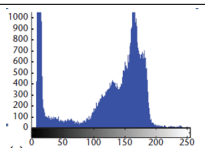
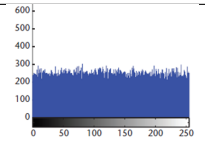
Input image	Encrypted image
	
	

Table 3. Performance analysis parameters

	2rounds	3rounds	4rounds	5rounds
NPCR	9.41	99.57	99.63	99.64
UACI	32.25	33.45	33.50	33.54

6.0.2 Analysis of differential attack. A well-designed encryption algorithm should be highly sensitive to plain-image and keys, so a slight change in plain-image or keys will make the cipher-image quite different. If an encryption scheme contains no confusion or diffusion stage, it would easily be destroyed by differential attacks. In order to confirm whether the proposed encryption algorithm is sensitive to plain image and keys, this paper brings out two tests: Number of pixels change rate (NPCR) and Unified average changing intensity (UACI) [8]. The equation to calculate UACI is Eq. 6

$$UACI = \frac{1}{M * N} \sum_{i,j} \frac{| C1(i,j) - C2(i,j) |}{255} \times 100\% \quad (6)$$

Where, M stands for images width, N stands for images height, c1(i,j) means the gray-scale value of cipher-image in position (i,j), and c2(i,j) means the gray-scale value of the new cipher-image which is the encryption result of modified plain image that has just one different pixel to the original plain-image. NPCR can be calculated by Eq. 7

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M \times N} \times 100\% \quad (7)$$

Where, M stands for images width, N stands for images height and where D(i,j) defined as follows

$$D(i,j) = \begin{cases} 1 & \text{if C1(i,j)} \neq \text{C2(i,j);} \\ 0 & \text{if C1(i,j)} = \text{C2(i,j).} \end{cases}$$

When one bit of a pixels gray-scale value in the plain image is changed, then a new plain image is generated from the original one. Encrypt the two images with the same secret keys, then take cipher images into Eqs. 6 and 7 and results are shown in Table 3.

7. CONCLUSION

Proposed algorithms includes ECG signal for key generation and auto blocking for segmentation process. The chaotic logistic map and generalized Arnold map will be employed. ECG signal and wolf algorithm are used to generate initial conditions for the chaotic maps. Auto-blocking diffusion operation is performed only in the encryption process. The keystream is generated by a control parameter produced from the plain-image. This method can be enhanced by using other medical information like EEG signals for key generation.

8. REFERENCES

[1] W. Zhang et al., *An Image Encryption Scheme Using Reverse 2-Dimensional Chaotic Map and Dependent Diffusion*, Comm. Nonlinear Science and Numerical Simulation, vol. 18, 2013, pp. 20662080.

[2] J. Fridrich, *Symmetric Ciphers Based on Two Dimensional Chaotic Maps*, Intl J. Bifurcation and Chaos, vol. 8, no. 6, 1998, pp. 12591284.

[3] A. Kumar and M.K. Ghose, *Extended Substitution-Diffusion Based Image Cipher Using Chaotic Standard Map*, Comm. Nonlinear Science and Numerical Simulation, vol. 16, no. 1, 2011, pp. 372382.

[4] H.J. Liu and X.Y.Wang, *Color Image Encryption Using Spatial Bit-Level Permutation and High- Dimension Chaotic System*, Optics Comm., vol. 284, 2011, pp. 38953903.

[5] Y. Tang, Z.D.Wang, and J.A. Fang, *Image Encryption Using Chaotic Coupled Map Lattices with Time-Varying Delays*,Comm. Nonlinear Science and Numerical Simulation, vol. 15, no. 9, 2010, pp. 24562468.

[6] Y.S. Zhang and D. Xiao, *An Image Encryption Scheme Based on Rotation Matrix Bit-Level Permutation and Block Diffusion*, Comm. Nonlinear Science and Numerical Simulation, vol. 19, no. 1, 2014, pp. 7482.

[7] Yue Wu, Joseph P. Noonan, *Shannon Entropy based Randomness Measurement and Test for Image Encryption* Information Sciences 00 (2011) 123

[8] Yue Wu, Joseph P. Noonan, and Sos Agaian, *NPCR and UACI Randomness Tests for Image Encryption* Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Telecommunications (JSAT), April Edition, 2011.