Chaotic Medical Image Encryption Based on Arnold Transformation and Pseudorandomly Enhanced Logistic Map

Joshua C. Dagadu, Jianping Li, Emelia O. Aboagye, Xuedzi Ge
School of Computer Science and Engineering,
University of Electronic Science and Technology of China,
Chengdu, China
joscaldag@yahoo.com

***Abstract*— Transmission and storage of digital medical images for telemedicine facilitates healthcare delivery. However, this gives rise to security concerns such as confidentiality integrity and reliability. In this paper, an efficient chaotic encryption scheme is proposed for gray scale medical images using Arnold cat map and pseudorandomly enhanced chaotic map. The scheme achieves secure encryption by Arnold transformation followed by pixel value modification with chaotic key sequence. The robustness of the scheme is measured by various metrics such as histogram analysis, key sensitivity and information entropy. Furthermore, we compare the efficiency of the pseudorandomly enhanced logistic map with the logistic map. The initial experimental results show that the scheme promises stronger resistance against diverse forms of common attacks.**

Keywords—medical image; encryption; Arnold cat map; pseudorandomly enhanced logistic map

I. Introduction

Medical images obtained via diverse imaging technologies of computed tomography, X-ray radiology, magnetic resonance imaging, ultrasonography, etc. [1] form critical components of the medical diagnostic procedures and are at the core of electronic health systems. Aside of offering means of assessment and management of patients' diagnosis and effects of treatment, they also provide non-invasive approaches of viewing anatomical cross sections of internal organs and other features of patients. As such, modified medical images might result in irreversible wrong diagnostic consequences since such data do not give true reflections of patients' medical conditions [2]. Besides, modern remote medical systems interactively use radiological data stored in picture archiving and communication systems of various health organizations, enabling practitioners located across various geographical borders to work together. This obviously exposes these images to security vulnerabilities; hence the need for security measures such as steganography, watermarking and encryption.

Encrypting medical images in eHealth systems is very challenging owing to the fact that the encryption and decryption techniques must not modify relevant data contained in these images. Moreover, these security techniques must be robust enough to resist attacks of diverse forms while possessing high execution speed. Most existing security techniques that have been used in medical imaging systems are based on the conventional encryption techniques which are not ideal for practical image encryption [3]. When encrypting data with small sizes, the traditional cryptographic algorithms are efficient [1]. However, these traditional protocols are not ideal for image encryption due to certain intrinsic features of images such as bulk data capacity, high redundancy and strong correlation among adjacent pixels. They lack efficiency and good computational time due to the high redundancy and correlation of pixels with the low resolution [4]. In order to overcome the challenges associated with image encryption, many researchers have proposed chaos based methods for pixel shuffling and subsequent encryption. The use of chaos based techniques for information security has been extensively studied in recent years due to the properties of ergodicity, sensitivity to initial conditions and system parameters that are intrinsic in chaotic systems.

These properties in chaos systems have strong relations with cryptography properties that help to design encryption schemes with complexity in the source system together with excellent confusion and diffusion processes. The various chaotic maps such as Arnold cat map, Logistic map and Henon map have been used in isolation and in some cases, in combination with other techniques to achieve efficient image encryption. In [5], a chaos-based medical image security scheme with permutation-substitution architecture was proposed in which Arnold cat map and logistic map were used to get rid of strong correlation among adjacent pixels and to achieve confusion. A hybrid encryption model based on Tinkerbell chaotic map and deoxyribonucleic acid and cellular automata for images was proposed in [6]. Askar et al. [7] introduced the use of a chaotic economic map for image encryption. An image encryption technique based on permutation substitution network and chaotic logistics systems was posited by Akram et al. [8] where substitution was based on S-boxes followed by the logistic map based diffusion. A fast and robust chaos-based cryptosystem structure was proposed in [9] which uses a diffusion layer followed by a bit permutation (achieved by 2D cat map) layer to shuffle pixels. A chaotic image encryption algorithm was suggested by [10] which combines double chaotic maps, Secure Hash Algorithm-3 (SHA-3) and auto-updating system. Here, the 3D chaotic cat map was employed to enlarge key space in the diffusion process. In [11], a chaos-based color pathological image encryption scheme using SHA-2 to generate one time keys was proposed. Parvees et al. [1] proposed a cryptosystem for 16-bit DICOM images using enhanced chaotic economic map.

The efficiency of low-dimensional and high-dimensional nonlinear systems play a vital role in hardware implementations of cryptosystems [12]. The more attractive ones that have been widely employed to generate pseudorandom key stream for image encryption have been the low-dimensional chaotic systems, despite some associated disadvantages when used in encryption. Their simple structure, high output processing, discrete nature, less arithmetic operations and relatively easier implementations in digital systems among others make them more attractive for particularly image cryptosystems. Enhancing these systems to possess better statistical properties to improve their efficiency has been a focused research area in recent times.

In this paper, we leverage on the strengths of the pseudorandomly enhanced logistic map (PELM) as proposed in [12] to achieve high security for medical images. Arnold transformation is followed with the use of the PELM to generate random bits for key formulation and subsequent encryption. The rest of the paper is organized as follows: We give overviews of the theories of Arnold cat map and the PELM in section II and introduce our proposed scheme in section III. Our experimental setup is summarized in section IV, followed by the presentation of results and discussion in section V. We finally give our concluding remarks in section VI.

II. PRELIMINARIES

A. *Arnold Cat Map*

The Arnold cat map has been used extensively particularly in image cryptography due to its chaotic nature. It is a simple illustration of a chaotic principle of underlying order to an apparently random evolution of a system. When an image is transformed, its original pixel organization is randomized; however, the original pixel positions are restored after a number of iterations [13].

It is described as [14]

$$\begin{bmatrix}\acute{x}\\ \acute{y}\end{bmatrix} = A\begin{bmatrix}x\\ y\end{bmatrix}(mod\ N)$$

$$= \begin{bmatrix}1 & c\\ d & cd+1\end{bmatrix}\begin{bmatrix}x\\ y\end{bmatrix}(mod\ N) \qquad (1)$$

Where c and d are positive integers, $det(A) = 1$. $(\acute{x}, \acute{y})$ is the new position while (x, y) is the original position of a pixel. $N \times N$ is the dimension of the image matrix. Iterations of A on a pixel $r_0 \in S = \{(x,y)|x,y = 0,1,2,\dots,N-1\}$ form a dynamical system $r_{n+1} = Ar_n(mod\ N)$, where $n = \{0,1,2,\dots\}$ [13]. After iterating for n times, there exist positive integers T such that $r_n + T = r_n$. The period T depends on the parameters c, d and the size N of the original image. Thus ,c , d and the number of iterations M could be used as secret keys. It is very efficient to scramble the positions of pixels using the Arnold cat map since there only exists a linear transformation and modulo function [14][15]. The strong correlation among adjacent pixels is eventually eliminated or reduced significantly after a number of iterations. It is however possible for attackers to iterate the Arnold cat map until the original image is obtained. The pixel values must therefore be obscured in addition to the pixel position scrambling. To achieve the desired level of security, this paper adopts the pseudorandomly enhanced logistic map to change pixel values after Arnold shuffling.

B. *Pseudorandomly Enhanced Logistic Map Map*

The logistic map is a polynomial mapping of degree two. It is often cited as a typical example of how very simple non-linear dynamical equations can result in complex chaotic behaviours [16]. It is one of the simple systems that exhibits order to chaos transition and possesses many properties required of a pseudorandom-number generator (PRNG) [17]. The main criterion that distinguishes different PRNGs is usually the quality of randomness. Moreover, the quality of randomness, implementation cost and throughput are essential factors to evaluate the effectiveness of PRNGs in applications [18]. For the largest value of its control parameter, the logistic map has the ability to generate an infinite chaotic sequence of numbers. When compared to the usual congruential random generators which are periodic, the logistic random number generator is infinite, aperiodic and not correlated [19].

It is mathematically given as:

$$x_{n+1} = px_n(1 - x_n) \qquad (2)$$

Where $p \in (0,4)$ and $x \in (0,1)$ and n is the iteration. The logistic map is in a chaotic condition when the control parameter is [3.57, 4.0] as illustrated in Fig 1.

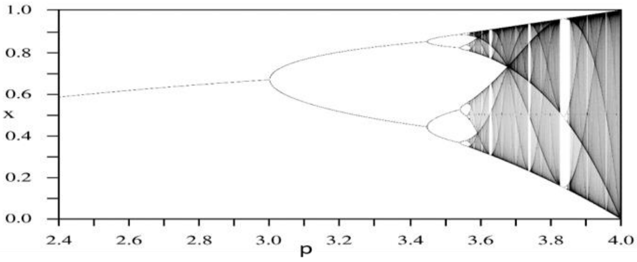

Fig 1. Logistic map

The PELM was proposed by [12] in which the properties of the chaotic logistic map were enhanced to generate better pseudorandom sequences by including one multiplication in each iteration and applying mod 1. The PELM is expressed mathematically as

$$X_{n+1} = mod\left(\left(\left(pX_n(1 - X_n)\right)(100000)\right), 1\right) \quad (3)$$

where mod is the modulo 1 operation. The PELM provides a higher and faster divergence between two chaotic orbits than the logistic map. In this paper, we leverage on the chaotic ability of the PELM to generate our encryption key stream.

III. PROPOSED SCHEME

Chaotic functions are sensitive to initial conditions. Slight changes in the initial conditions therefore result in massive alterations in the final outcome. Diverse chaotic maps have been used for image encryption in different schemes. In this proposed scheme, the Arnold cat map is combined with the PELM to encrypt medical images. The scheme first generates pseudorandom bits using PELM. The PELM bit sequence is formulated into a key image and subsequently used to change pixel values after shuffling with the Arnold cat map, eventually resulting in the cipher image. Fig 2 is a block diagram of the full encryption scheme.

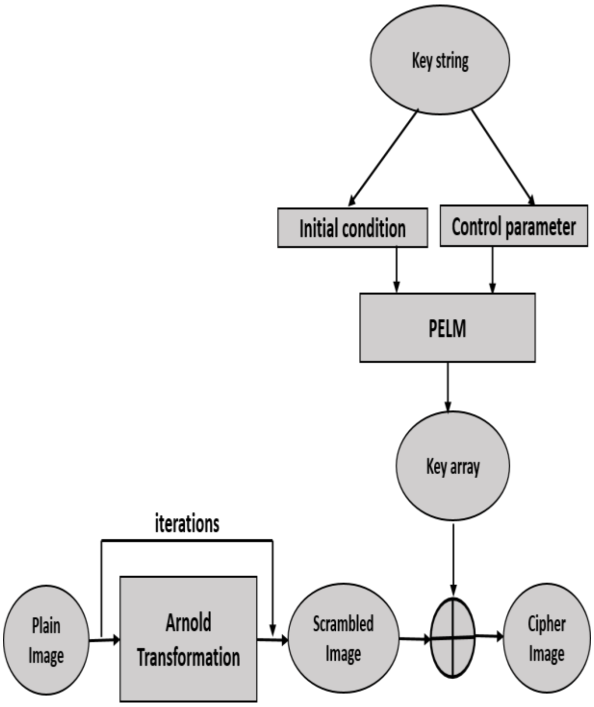

Fig 2. Block diagram of proposed scheme

A. *Key Generation (Algorithm 1)*

Step 1: A string of 16 ASCII characters made up of 128 bits are taken as input

$$K = K_1, K_2, \dots, K_{16} \quad (4)$$

where $K_i = b_1, b_2, \dots, b_8$ and $i = 1,2, \dots, 16$. This ASCII character string is used to generate the initial value x_0 and parameter p of the PELM.

Step 2: We transform each element of K into its binary form to get a stream of 128 bits:

$$\beta = b_1, b_2, \dots, b_{128} \quad (5)$$

Step 3: We put the bit stream β into four blocks of 32 bits each and perform the following operations:

$$\beta_1 = \frac{\sum_{i=1}^{32}(b_i \times 2^i)}{2^{32}+1} \quad (6)$$

$$\beta_2 = \frac{\sum_{i=33}^{64}(b_i \times 2^i)}{2^{32}+1} \quad (7)$$

$$\beta_3 = \frac{\sum_{i=65}^{96}(b_i \times 2^i)}{2^{32}+1} \quad (8)$$

$$\beta_4 = \frac{\sum_{i=97}^{128}(b_i \times 2^i)}{2^{32}+1} \quad (9)$$

Step 4: Using β_1, β_2, β_3 and β_4, we derive x_0 and p as

$$x_0 = (\beta_3 + \beta_4) mod\ 1 \quad (10)$$

$$p = 3.999 + \left(\left((\beta_1 + \beta_2) mod\ 1\right) \times 0.001\right) \quad (11)$$

Step 5: Using x_0 and p, we iterate equation (3) (i.e. PELM) MN times to generate the pseudorandom bit sequence X where M and N are the dimensions of the input medical image.

Step 6: The chaotic sequence $X = \{x_1, x_2, x_3, \dots, x_{MN}\}$ and we convert the elements $x_i \in X$, into integer sequence to produce the key image $P = \{P_1, P_2, P_3, \dots, P_{MN}\}$ as

$$P_i = floor(256 \times x_i) \quad (12)$$

The chaotic key image can now be used to encrypt the medical image using algorithm 2.

B. Encryption

Algorithm 2. Arnold Shuffling

```
Input: Plain image $I$
Output: Cipher image $Q$
Read image matrix $I$
Get matrix dimensions $r, c$ of $I$
Generate the key array $P$ of size $r * c$
For $l = 1:n$
  For $i = 1:r$
    For $j = 1:c$
      $row = i$
        $col = j$
        For $k = 1:l$
          $x = [1\ 1; 1\ 2] * [row\ col]$
          $row = x(1)$
          $col = x(2)$
          I(r, c)=(I(mod(row, r)+1), mod(col, c)+1)
          P(r, c)=(I(mod(row, r)+1), mod(col, c)+1)
          $Q = bitxor(I(r, c), P(r, c))$
        End for
    End for
  End for
End for
Return $Q$
```

The positions of the image are shuffled with algorithm 2 (Arnold transformation) for a number of iterations specified by the user, to provide confusion. This is followed by the engagement of the PELM generated key array in an *XOR* operation with the transformed medical image at the bit level to change the values of the pixels and to achieve diffusion; hence producing a well cipher image with the correlation between adjacent pixels adequately broken.

The decryption process is the reverse of the encryption process. In this process, the cipher image first goes through a reverse Arnold shuffling for a number of iterations calculated based on the periodicity of the Arnold cat map during encryption. Using the same seed key and logical sequence of steps as in algorithm 1, the decryption key is obtained. This key is again engaged in a XOR operation at the bit level with the unshuffled image to produce the plain image.

IV. EXPERIMENTATION

A number of gray scale medical images of diverse dimensions were selected for experimentation. Two of such are presented in this paper. The pixel scrambling phase with Arnold cat map without the introduction of encryption keys was carried out for different number of iterations to determine at which number of iterations could a compromise between the degree of pixel scrambling that is enough to obscure any identifiable pattern with the plain images and a good speed irrespective of image dimensions. However, to demonstrate the strength of our proposed scheme, we iterate the scrambling process for just three rounds for both test images herein presented; hence full scrambling with key is implemented as such.

The experiment is carried out on a personal computer with Intel core i5, 2.6GHz CPU, 4GB memory, windows10 and MATLAB 2016b. An encryption key 'AFBVX9859fa87bmy' was used for both images. Correlation analysis, number of pixel change rate (NPCR), unified average changing intensity (UACI), histogram analysis and key analysis are the evaluation metrics used to assess the strength of the proposed scheme.

V. RESULTS AND DISCUSSION

Various analyses such as statistical analysis, differential analysis and key analysis are used to analyze the robustness of our proposed scheme. Statistical analysis is done by histogram analysis and correlation coefficient calculation of both plain and cipher images. Shannon [20] indicated the possibility of security breaches on many kinds of encryption schemes through statistical analysis on the correlation of adjacent pixels and their histograms.

A. Histogram Analysis

An efficient encryption scheme should have a uniform histogram in order to make it impossible for an attacker to extract any meaningful information from the histogram since the histogram's distribution reveals the pixel value distribution within the image.

As shown in Fig. 3 and Fig. 4, it is evident that the proposed scheme uniformly distributes pixel values in the cipher image through the confusion and diffusion phase; hence has the capability to resist cipher only attacks.

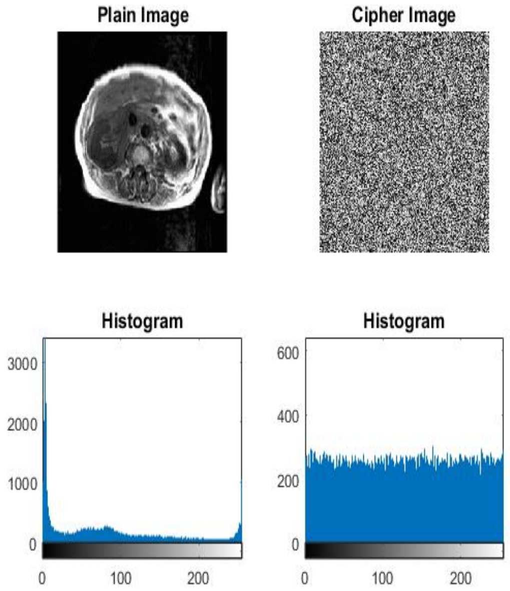

Fig 3. Histograms of plain and encrypted ultrasound images

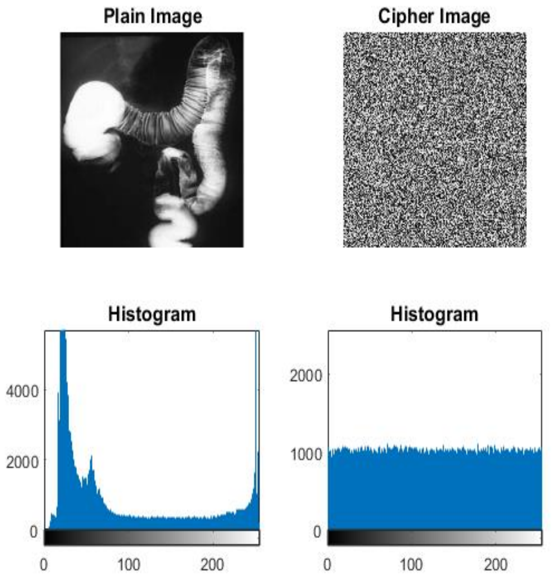

Fig 4. Histograms of plain and encrypted MRI images

B. *Correlation Coefficients*

The correlation coefficients of adjacent pixels of an image give information about the image. High correlation coefficients of adjacent pixels is evidence that, information can be extracted from the image. It is therefore necessary that correlation coefficients of adjacent pixels in cipher images are very low. In images, the horizontal, vertical and diagonal correlations between pixels are high. Cipher images must reduce these relationships among the adjacent pixels. The correlation coefficients among adjacent pixels is calculated with (13), (14), (15) and (16) [21]

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \qquad (13)$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)^2 \qquad (14)$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)\left(y_i - E(y)\right) \qquad (15)$$

$$r_{xy} = \frac{cov(x,y)}{\sqrt{D(x)\times\sqrt{D(y)}}} \qquad (16)$$

Where x and y are the gray scale values of two adjacent pixels of the image, $D(x)$ is the variance, $cov(x,y)$ is the covariance and $E(x)$ is the mean. We randomly selected 2000 pairs of adjacent pixels from both original and encrypted images and calculated their horizontal, vertical and diagonal correlation coefficients.

Table I is our test results of the correlation coefficient analysis. It is evident from the graphs (Fig. 5 and Fig. 6) and the table that the proposed scheme adequately breaks the correlation among adjacent pixels; hence is robust enough against statistical attacks.

TABLE I. CORRELATION COEFFICIENT

Test image	Form	Correlation Coefficients		
		Horizontal	Vertical	Diagonal
Ultrasound (256 X 256)	Original	0.9775	0.9836	0.9642
	Cipher	0.0009	0.0010	0.0033
MRI (512 X 512)	Original	0.9978	0.9969	0.9949
	Cipher	0.0000	-0.0046	-0.0009

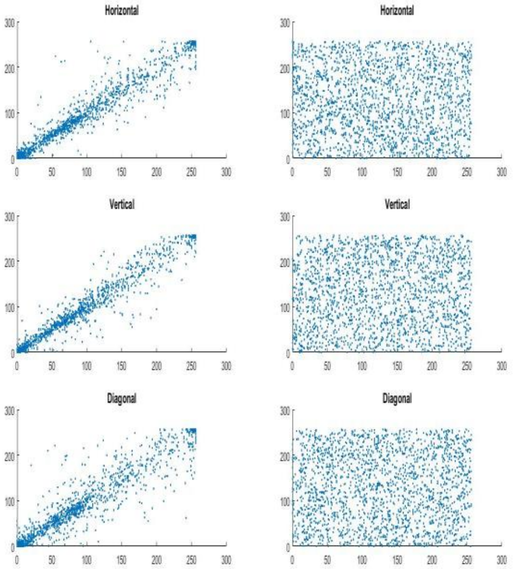

Fig 5. Correlation coefficients of plain and encrypted ultrasound images

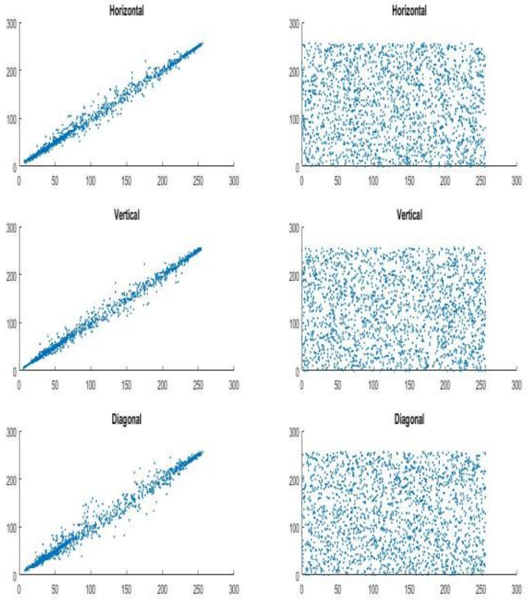

Fig 6. Correlation coefficients of plain and encrypted MRI images

C. Information Entropy

Another criterion for measuring the strength of an encryption algorithm is the information entropy which is given as

$$H(m) = \sum_{i=0}^{2^N-1} p(m_i) log_2 \frac{1}{p(m_i)} \qquad (17)$$

Where N is the total number of symbols $m_i \in m$, $p(m)$ denotes the probability of occurrence of symbol m_i and log represents the base 2 logarithm which measures the randomness of encryption. If there are 256 possible outcomes of the 8-bit message m with equal probability, the message source is said to be random in which case $H(m) = 8$; the ideal situation. As seen from Table II, the entropy values of all test images are very close to the ideal value, giving an indication of negligible information leakage during encryption; hence strong resistance against entropy attacks.

TABLE II. UACI, NPCR AND INFORMATION ENTROPY

Test Image	Information Entropy		UACI (%)	NPCR (%)
	Original Image	Cipher image		
Ultrasound (256 X 256)	5.9123	7.9975	32.48	93.12
MRI (512 X 512)	6.8620	7.9994	33.36	99.72

D. NPCR and UACI

Sensitivity of a cipher image to slight changes in plain image is one way to measure the resistance of image encryption algorithms to differential cryptanalysis. The two metrics used are the NPCR and UACI which are defined as

$$NPCR = \frac{1}{M \times N}\left(\sum_{i,j} D(i,j)\right) \times 100\% \qquad (18)$$

$$D(i,j) = \begin{cases} 0 & C_1(i,j) = C_2(i,j) \\ 1 & C_1(i,j) \neq C_2(i,j) \end{cases} \qquad (19)$$

$$UACI = \frac{1}{M \times N}\left(\sum_{i,j} \left|\frac{C_1(i,j) - C_2(i,j)}{255}\right|\right) \times 100\% \qquad (20)$$

Where C_1 and C_2 are two encrypted images which have one pixel difference in their corresponding plain images. $C_2(i,j)$ is their pixel values and M and N represent their dimensions. An attacker would inverse a pixel in the plain image and observe the corresponding change in the cipher image. If the changes in the plain image do not lead to non-uniform changes in the cipher image, the differential attack fails [6], [22], [23]. The results of our experiment are shown in Table II. It is obvious our scheme is resistant to differential attacks.

E. Key Analysis

The Key analysis metrics: key space analysis and key sensitivity test are used to measure the strength of encryption algorithms.

Key sensitivity ensures that partial guesses of the key aimed at decrypting the cipher image fail. With the incorrect keys, the guessed key should not provide any pattern of information in the wrongly decrypted image. This means that if two different keys are used to encrypt the same plain image, the resulting cipher images must be different. We made slight changes in the seed keys for decrypting the same cipher image. In Fig. 7, it is evident that if the wrong key is applied to decrypt the image, the resulting image still shows no pattern of the original image.

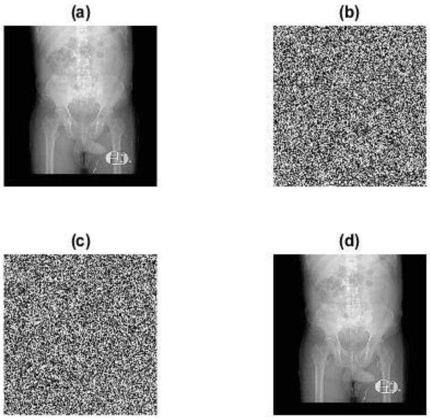

Fig 7. Key Sensitivity Test (a) original image, (b) encrypted image, (c) image decrypted with incorrect key, (d) image decrypted with correct key

We generated the initial condition and control parameter of PELM from an external input key of size 128 bits. The computational precision of the 64-bit double precision number is about 10^{-15} according to the IEEE floating-point standard [24]. For an effective encryption scheme, the key space size should not be smaller than 10^{100} in order to resist brute-force attacks [25]. The secret key space for our scheme is 10^{128} which is adequate to resist brute-force attacks.

F. Comparative Analysis with Logistic Map

We now compare the efficiency of the PELM-Arnold Transformation with the direct logistic map with Arnold transformation using the ultrasound image with dimension 256 X 256. We do this by using the same encryption key as already indicated. This provides the same initial conditions and control parameters for both the PELM and the logistic map (LP). Arnold shuffling for three rounds is used for both maps. It is obvious from Fig. 8 and Table III that the PELM uniformly distributes pixel values in the cipher image better than the LP and also breaks the correlation between adjacent pixels better.

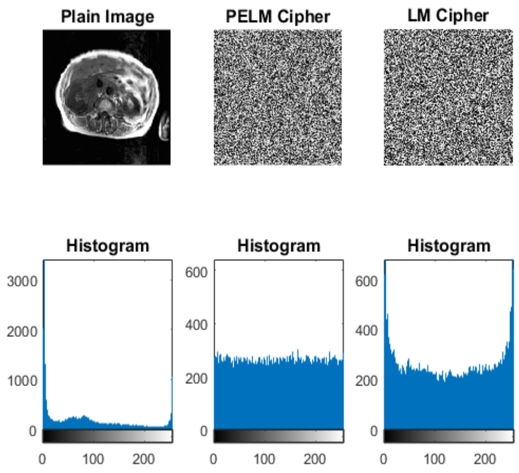

Fig 8. Histogram comparison

TABLE III. CORRELATION COMPARISON

Correlation Direction	Image Format	Scheme	
		PELM	LM
Horizontal	Original	0.9775	0.9775
	Cipher	0.0009	-0.0001
Vertical	Original	0.9836	0.9836
	Cipher	0.0010	-0.0214
Diagonal	Original	0.9642	0.9642
	Cipher	0.0033	0.0074

VI. CONCLUSION

We have proposed an encryption scheme for securing medical images based on Arnold transformation and PELM. Our experiments have demonstrated the scheme's potentials in terms of resistance against various forms of attacks and can be well integrated into eHealth applications. Furthermore, our experiment has confirmed that PELM produces better pseudorandom properties than the direct logistic map.

ACKNOWLEDGMENT

This paper was supported by the National Natural Science Foundation of China (Grant No. 61370073), the National High Technology Research and Development Program of China (Grant No. 2007AA01Z423), the project of Science and Technology Department of Sichuan Province.

REFERENCES

[1] M. Y. M. Parvees, J. A. Samath, and B. P. Bose, “Secured Medical Images-a Chaotic Pixel Scrambling Approach,” *J. Med. Syst.*, vol. 40, no. 11, p. 232, 2016.

[2] A. A. Omala, N. Robert, and F. Li, “A provably-secure transmission scheme for wireless body area networks,” *J. Med. Syst.*, vol. 40, no. 11, p. 247, 2016.

[3] M. A. F. Al-Husainy, “A novel encryption method for image security,” *Int. J. Secur. Its Appl.*, vol. 6, no. 1, 2012.

[4] D. Ravichandran, P. Praveenkumar, J. B. B. Rayappan, and R. Amirtharajan, “Chaos based crossover and mutation for securing DICOM image,” *Comput. Biol. Med.*, vol. 72, pp. 170–184, 2016.

[5] C. Fu *et al.*, “An efficient and secure medical image protection scheme based on chaotic maps,” *Comput. Biol. Med.*, vol. 43, no. 8, pp. 1000–1010, 2013.

[6] R. Enayatifar, H. J. Sadaei, A. H. Abdullah, M. Lee, and I. F. Isnin, “A novel chaotic based image encryption using a hybrid model of deoxyribonucleic acid and cellular automata,” *Opt. Lasers Eng.*, vol. 71, pp. 33–41, 2015.

[7] S. S. Askar, A. A. Karawia, and A. Alshamrani, “Image encryption algorithm based on chaotic economic model,” *Math. Probl. Eng.*, vol. 2015, 2015.

[8] A. Belazi, A. A. A. El-Latif, and S. Belghith, “A novel image encryption scheme based on substitution-permutation network and chaos,” *Signal Processing*, vol. 128, pp. 155–170, 2016.

[9] S. El Assad and M. Farajallah, “A new chaos-based image encryption system,” *Signal Process. Image Commun.*, vol. 41, pp. 144–157, 2016.

[10] G. Ye and X. Huang, “A secure image encryption algorithm based on chaotic maps and SHA-3,” *Secur. Commun. Networks*, 2016.

[11] G. Liu, J. Li, and H. Liu, “Chaos-based color pathological image encryption scheme using one-time keys,” *Comput. Biol. Med.*, vol. 45, pp. 111–117, 2014.

[12] M. A. Murillo-Escobar, C. Cruz-Hernández, L. Cardoza-Avendaño, and R. Méndez-Ram’\irez, “A novel pseudorandom number generator based on pseudorandomly enhanced logistic map,” *Nonlinear Dyn.*, vol. 87, no. 1, pp. 407–425, 2017.

[13] G. Peterson, “Arnold's cat map,” *Math45-Linear Algebr. http//online. redwoods. cc. ca. us/instruct/darnold/maw/c atmap. htm*, 1997.

[14] Z.-H. Guan, F. Huang, and W. Guan, “Chaos-based image encryption algorithm,” *Phys. Lett. A*, vol. 346, no. 1, pp. 153–157, 2005.

[15] C. Wei-Bin and Z. Xin, “Image encryption algorithm based on Henon chaotic system,” in *Image Analysis and Signal Processing, 2009. IASP 2009. International Conference on*, 2009, pp. 94–97.

[16] S. Chakraborty, A. Seal, M. Roy, and K. Mali, “A novel lossless image encryption method using DNA substitution and chaotic Logistic map,” *Int. J. Secur. Its Appl.*, vol. 10, no. 2, 2016.

[17] S. C. Phatak and S. S. Rao, “Logistic map: A possible random-number generator,” *Phys. Rev. E*, vol. 51, no. 4, p. 3670, 1995.

[18] S.-L. Chen, T. Hwang, and W.-W. Lin, “Randomness enhancement using digitalized modified logistic map,” *IEEE Trans. circuits Syst. II express briefs*, vol. 57, no. 12, pp. 996–1000, 2010.

[19] M. Andrecut, “Logistic map as a random number generator,” *Int. J. Mod. Phys. B*, vol. 12, no. 9, pp. 921–930, 1998.

[20] C. E. Shannon, “Communication theory of secrecy systems,” *Bell Labs Tech. J.*, vol. 28, no. 4, pp. 656–715, 1949.

[21] E.-S. M. El-Alfy, S. M. Thampi, H. Takagi, S. Piramuthu, and T. Hanne, *Advances in Intelligent Informatics*. Springer, 2015.

[22] R. Enayatifar, A. H. Abdullah, and I. F. Isnin, “Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence,” *Opt. Lasers Eng.*, vol. 56, pp. 83–93, 2014.

[23] R. Enayatifar, A. H. Abdullah, and M. Lee, “A weighted discrete imperialist competitive algorithm (WDICA) combined with chaotic map for image encryption,” *Opt. Lasers Eng.*, vol. 51, no. 9, pp. 1066–1077, 2013.

[24] F. W. Group and others, “IEEE Standard for Binary Floating-Point Arithmetic. ANSI,” *IEEE Std*, pp. 754–1985, 1985.

[25] G. Alvarez and S. Li, “Some basic cryptographic requirements for chaos-based cryptosystems,” Int. J. Bifurc. Chaos, vol. 16, no. 8, pp. 2129–2151, 2006.