Received: November 9, 2016

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

2D Chaotic Map Based on 2D Adaptive Grey Wolf Algorithm for Ultra Sound Medical Image Security

Srinivas Koppu [1]* Madhu Viswanatham V[2]

[1]*School of Information Technology and Engineering,VIT University, Vellore, India.*
[2]*School of Computing Science and Engineering,VIT University, Vellore, India*
* Corresponding author's Email: srinukoppu@vit.ac.in

Abstract: In this paper, we have proposed a chaos-based visual encryption method that can be applied to Ultra Sound Medical Images. We used adaptive Grey Wolf Optimization (GWO) to archive Ultra Sound Medical Image encryption. The robustness of the proposed image encryption are measured by various security attacks such as key sensitivity, histogram analysis, adjacent pixel autocorrelation, chi-square test, etc. Moreover, analytical outcomes are compared with the conventional algorithms like Genetic Algorithm (GA) and GWO. The experimental result shows that the proposed method is faster with low complexity.

Keywords: Chaotic encryption, Chaotic decryption, 2DCM, GWO, Modified GWO.

1. Introduction

Medical diagnostics depend on modalitie such as, ultrasound, Computed Tomography (CT), Magnetic Resonance Imaging (MRI), Positron Emission Tomography (PET).The Medical images are stored and distributed over the internet or intranet for specific diagnostic purpose like feature extraction, image denoising, segmentation and compression in the arena of telemedicine [1].Telemedicine had benefits: restorative medical research, remote special clinical diagnosis, unexpected incidents handling in time, patient information on immediate demand, enhance the communication between partners in health care systems.

In recent days, people can communicate from anywhere to everywhere due to wide use of Computer Networks, and transmission of digital medical images over the internet has become more and more popular. However, the transmission of the medical images over the internet may suffer from the serious problems of confidentiality, integrity, Authentication, cropping, tampering and destroying from attackers. Therefore, recommendations and instructions for ensuring medical image protection have been issued by American College of Radiology (ACR) and Society of Computer Applications in Radiology (SCAR).In 1996, United States Congress, Health Insurance Portability and Accountability Act (HIPAA) and signed by President Bill Clinton, President Bill Clinton, obliges health care institutions to take legitimate measures to guarantee that patients' information is only accessible to people who have a specialized need [2].
Cryptography and steganography are the two techniques which are broadly utilized for the image security.

During the communication in the networks encrypting the images are very crucial through the rapid development of telemedicine large medical image data can be easily transmitted, thus the encryption has become a significant for patient data[3].The most classical cryptographic techniques can be classified into private and public encryption[4-6].

Encryption of medical image is a better solution to protect medical images from the various threats. Data Encryption Standard (DES) [7], Triple Data Encryption Standard (TDEA) [8], Advanced Encryption Standard (AES) [9], Rivest, Shamir and Adleman (RSA) [9,10] have been developed for text data. However, these cryptographic algorithms are not suitable for large size images because of high pixel redundancy and correlation.

Table 1. Comparison of Cryptographic Systems and Chaos systems.

Cryptographic Systems	Chaotic Systems
Private and Public keys	Parameters
No of Rounds	No of Iterations
Integers	Real Numbers
Diffusion	Depends on initial conditions
Finite field	Continuum

However, these are well developed for the security of textual data. Some researchers used selective based encryption techniques for medical images based on stream ciphers data [11]. But, these methods lead to loss of and misdiagnosis. The Visual image encryption methods can be applied to image encryption [12]. since, 1990s, chaotic frameworks have been drawn much importance as their fundamental characteristics such as ergodicity, randomness, and sensitivity [13]. Both have sensitive, randomness, confusion and diffusion.Cryptographic methods and chaotic maps have some similar characteristics show in table 1.

Chaos theory is the branch of mathematics that deals with design of dynamic nonlinear system, complex systems with random behavior called chaos". Chaos theory, applications such as signal processing, image security, Information Security, fluid mechanics, mathematics, biology, engineering, psychology, robotics, etc. [14-15]. A chaotic system has properties such as sensitivity to initial conditions, topologically mixing and mixing of the periodic orbits. It is a novel and interesting research subjects for real time encryption, such as audio and video signal [16-20].

Test results have shown that the 2D-AGWA medical image cryptosystem is much more efficient than the well-known Genetic algorithm, which leads to use in real-time environments transmission for medical image protection. This paper is organized as follows. Section 3 has two sub-sections. In 3.1 presents the Conventional GWO of the medical image cryptosystem. The 3.2 presents the proposed GWO. In Section 4, analysed the detail security and performance of the proposed medical image protection mechanism. Finally, Section 5 concludes the propose system work.

2. Literature Review

In[21] Jiri Fridrich, was introduced based on symmetric block cipher for digital image security by 2 dimensional map. Figure 1 shows permutation process and substitution process based on Permutation key (P) and Substitution key (S) which is used widely in security mechanisms. Input image

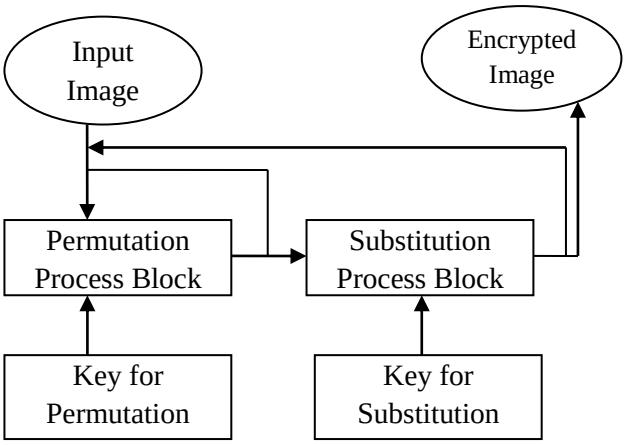

Figure 1. General architecture of chaotic crypto system.

(plain image) was shuffled using the Arnold cat map in bit-wise permutation. Logistic map was used in Substitution process which modifies the pixel values. However, the system is not efficient in the image scrambling process. Jiun-In Guo, Jui-Cheng Yen [22], have presented an efficient binary sequence based chaotic map which gives low computational complexity. But, it's lack of security threats. In [23] chaotic map was proposed by using logistic map and standard two dimensional chaotic maps. An XOR operator used to produce the encrypted text for intermediate data.However, it has small key size which leads to brute-force attack.

Figure 1 shows, Input Image is given to Permutation block for pixel position transformation with permutation key.substitution process takes shuffled image as input and do the pixel value transformation based on substitution key.[24] Two dimensional cat maps were applied for image blocks (8 X 8 block size) to shuffle the image pixels. The shuffled image was encrypted by one dimensional logistic map.

In [25] proposed hybrid image encryption method based on a Cyclic Elliptic Curve Points (CECP) and generalized logistic chaotic map systems. The chaotic system scheme generates an initial key and an external secret key of 256-bit in a feedback manner. Then, the generated keys are combined with a key sequences derived from the Cyclic Elliptic Curve Points (CECP).[26] Deoxyribonucleic Acid matrix sequence is learnt by encoding the host image, and then decomposes the DNA sequence into some equal matrix blocks and use the DNA sequence addition operation to comprise the matrix blocks. Image pixels are shambled by the DNA addition and complementary operation. It used two Logistic maps for performing the DNA complementary operation on comprise matrix blocks.

Table 2. shows the Review of chaotic systems.

References	Analysis
Gao, H., Zhang, Y., Liang, S. and Li, D [42]	**Method:** • Nonlinear Chaotic Map (NCM) based power function and tangent function. **Advantages:** • more secure than DES **Disadvantages:** • Less key space
Sun, F., Liu, S., Li, Z. and Lü, Z.,[43]	Method: • Spatial chaotic map based pixel by pixel. **Advantages:** • High degree security. **Disadvantages:** • Computation speed.
Pareek, N.K., Patidar, V. and Sud, K.K. [44]	**Method:** • Two chaotic logistic maps based 80-bit external secret key. **Advantages:** • Resistance to statistical analysis • Key sensitivity tests. **Disadvantages:** • Computation speed. • Less key space.
Chen, G., Mao, Y. and Chui, C.K [45]	**Method:** • symmetric encryption scheme based on 3D chaotic cat map **Advantages:** • Defends statistical • Differential attacks. • High speed encryption **Disadvantages:** • Key size small. • Input image must be square size.
Mao, Y., Chen, G. and Lian, S [46]	**Method:** • Three dimensional baker map based symmetric encryption **Advantages:** • High speed encryption **Disadvantages:** • Small key size. • Accepts only Input image with equal row-columns.
	Method: • Nonlinear dynamic chaos system for image confusion.
Song, Z., Hengjian, L. and Xu, Y. [47]	• Logistic map to Shuffle the positions of image pixels. **Advantages:** • It is efficient and secure for fingerprint images **Disadvantages:** • Consumes time
Gao, T. and Chen, Z [48]	**Method:** • Lorenz chaotic system • Chen's chaotic system. • Logistic map **Advantages:** • Low time complexity. • Large key space. • High security. **Disadvantages:** • Not efficient for color images.
Lai, J., Liang, S. and Cui, D [49]	**Method:** • Fractional Fourier Transform (FFT) **Advantages:** • Repel to brute force Attack **Disadvantages:** • Small key space
Fu, C., Meng, W.H., Zhan, Y.F., Zhu, Z.L., Lau, F.C., Chi, K.T. and Ma, H.F [50]	**Method:** • Arnold cat map • chaotic logistic map **Advantages:** • Statistical analysis • key space analysis • key sensitivity analysis **Disadvantages:** • Time consumes.

The Results were shown: good encryption, defending exhaustive attack, statistical attack and differential attack. Dimensinal logistics map, 3Dimensional Chebyshev map has been used for key generation, and 3D, 2D Arnold cat map for colour image encryption. Image pixels are scrambled by 2Diemensional chaotic map and diffusion was achieved for colour images by 3Deimensional Arnold cat map.In 2016,Srinivas Koppu and Madhu Viswanatham [39,40] adapted magic matrix increase the randomness and complexity which is efficient from the existing method.In 2016 Kuruva Lakshmanna and Neelu khare [41] have proposed Constraint-Based Measures for DNA Sequence Mining using Group Search Optimization Algorithm to optimize the DNA sequences.

In [27], Initial external key to chaotic map was derived by 80 bit key size with different weightage for bits. 1D chaotic map was to use to image pixel

shuffle. It causes small key space and lower security.The Proposed method was robust for statistical analysis and key sensitivity.[28] Host image has been shuffled with sequence generated by DNA. Later, image pixels are replaced. Three DNA sequence templates are used to reduce encryption time complexity. Analysed attacks: exhaustive attack, statistical analysis and brute-force attacks [29] Secret keys are generated by using DNA systems.Hao's fractal sequence was used for representation, image permutation process. Proposed system is simple and defending exhaustive attacks.

[30] Three two dimensional chaotic is used for image encryption to obtain higher security than one dimensional chaotic maps. The proposed scheme had classic bi-modular architecture in which the medical image pixels are shuffled via new propose algorithm and also in diffusion process image pixel values are modified by XOR operation.

[31-32] Conventional block based image encryption methods are not advised to use for medical image protection due to their large size and increasing demand of telemedicine. A bit level Arnold cat map was adapted for medical image shuffling. Image correlation has been eliminated by combining Arnold cat map with the logistic map.To improve the performance, the substitution process was applied to permutation phase by light weight bit level shuffling method. The performance of the proposed image encryption system was measured by the time complexity, statistical attack analysis, key space analysis, key sensitivity [33]. They had proposed symmetrical image encryption algorithm based on a skew tent map which can be applied on gray level and colour images. Further, it may be implemented in parallel way to improve the medical image encryption speed.[34] Permutation key was generated in both 'X' and 'Y' axes by Henon chaotic map. They sent the same medical image in two axes. Address attacks: brute-force and statistical attacks.[35] Medical image gray pixels are scrambled by DNA sequence addition and complementary operation. Duffing map was used for image encryption. Not addressed: image noise and image blurring. [36] Pixel correlation distributed among the entire image pixels. Pixel scrambling was done in horizontally and vertically with the help of 2 dimensional baker map.scrambelled image becomes pre-encrypted image. [37] ROI was compressed from an image by a lossless compression method where as NROI was compressed by lossy compression method. Key is generated by Henon map for shuffling and given as input for blowfish algorithm for image encryptiom. However it was slow and not reliable in real time communications and also not suitable for large size images [38].

Basic theory of chaotic systems

The chaotic system is a nonlinear deterministic system [51].The characteristics are: randomness in performance, more sensitivity to primary conditions and system attributes. Chaotic system dynamic system defined as the following Eq.1:

$$C_{(i+1)}=\alpha(C_i),C_\epsilon(0,1),i=0,1,2,3 \quad (1)$$

The initial output chaotic stream are distributed and speeded over the entire full space, in un-correlated sequence C_i: *i=1,2,3.*

Eq.2: defines the simple logistic map with the following initial condition

$$C_{(i+1)}=f(c) = \mu C_i\,(1-C_i\,);\ \mu\epsilon(0,4),C_i\in(0,1) \quad (2)$$

Chaotic state depends on $\mu\in(3.5699456,4)$
Two dimensional logistic map defined in the *Eq.3-4* [52]:

$$p_{i+1}=\mu_1\, p_i=(1-p_i\,)+\gamma_i\, y_i^2 \quad (3)$$

$$y_{i+1}=\mu_2\, y_i(1-y_i)+\gamma_2\,(p_i^2+(p_i y_i) \quad (4)$$

A 2D Adaptive Grey Wolf Approach is suggested in this paper for efficient and secure medical image protection[53,54]. To enhance the efficiency of the 2D chaotic system, we propose a permutation and substitution method based on standard chaotic system. Two dimensional Adaptive Grey Wolf Approach (2D-AGWA) has been used to encrypt the image which depends on the initial values of entropy.

3. Proposed Methodology

The proposed method intends to introduce an two dimensional (2D) chaotic mapping (2DCM) for medical image encryption. The block diagram of the proposed encryption process is shown in figure 2. Since the conventional chaotic mapping highly rely on the initial chaotic system parameters and the order of permutation, it is challenging to determine the optimal initial system parameters. The proposed security scheme introduces a enchancing grey wolf optimization algorithm for determining the optimal chaotic system parameters. Proposed optimized 2D chaotic mapping model requires a security model to represent the a priori ciphered image. Hence, we have adapted information entropy, for chaotic key generation system.The chaotic key generation system is nothing but the proposed grey wolf optimization algorithm that will attempt to maximize the information entropy model. As a result, optimal initial parameters for the chaotic system can be determined.Based on those parameters, the image encryption can be performed. The parameters are termed as which is estimated

using GWO. Further, this computed parameter is applied to 2DCM for encrypting the image.

3.1 Conventional GWO

This method describes the hunting activities of the grey wolves to get the appropriate prey[52]. Generally, the grey wolves are categorized into four levels such as α, β, δ and ω. The first level α is the leader of the grey wolves group. The decision regarding the activities of the wolves is done by the leader. The next levels β and δ is the subsidiary group that helps α to make the decisions where as the lower level ω is just the followers and they are the last wolves that are allowed to eat, and hence it plays less importance in the hunting activities.The general phases of GWO is described as 1) tracking, chasing and approaching the prey 2) Pursuing, encircling and harassing the prey until it stops moving 3) continually attacks towards the prey.

The pseudo code of the conventional GWO is depicted below.

Step 1: Start to initialize the grey wolves population $Z_m (m = 1,2.....N_{iter})$

Step 2: Initialize the values of $\vec{a}$, $\vec{A}$ and $\vec{H}$

Step 3: Compute the fitness function of wolves among the population

Step 4: Determine the positions Z_α, Z_β and Z_δ of α, β and δ

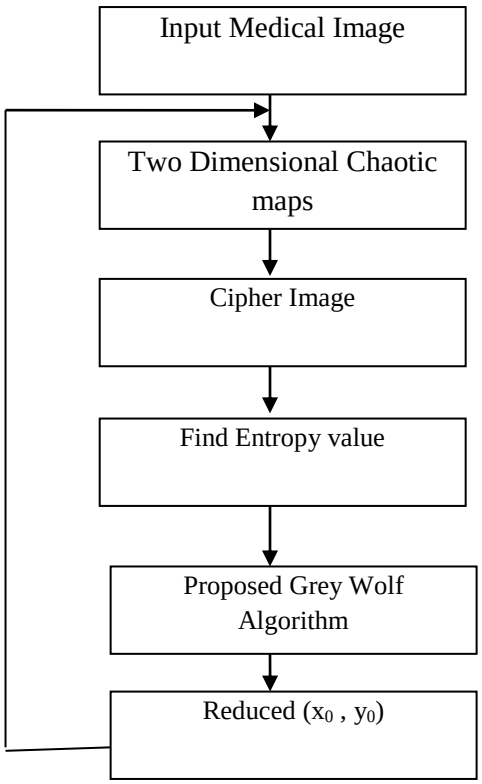

Figure 2. Block diagram of the proposed system.

Step 5: While ((i<n) // n number of Iterations

Step 5.1: Update the position of the grey wolves

Step 5.2: Update the value of $\vec{A}$ and $\vec{H}$ using $\vec{a} = 2 - 2 * \frac{i}{n}$ that linearly reduced from 2 to 0.

Step 5.3: Compute the fitness of the wolves.

Step 5.4 Update the positions Z_α, Z_β and Z_δ of α, β and δ

End

Step 6: Return Z_α

3.2 Proposed GWO

The mathematical formulation for encircling prey is represented in eq. (5) and eq. (6) where $\vec{A}$ and $\vec{H}$ represents the coefficient vectors, $\vec{Z}$ represents the position vector of the grey wolf and *t* represents the present iteration.

$$\vec{G} = \left| \vec{H} \cdot \vec{Z}_p(t) - \vec{Z}(t) \right| \tag{5}$$

$$\vec{Z}(t+1) = \vec{Z}_p(t) - \vec{A} \cdot \vec{G} \tag{6}$$

The vectors regarding $\vec{A}$ and $\vec{H}$ are expressed in eq. (7) and eq. (8) where r_1 and r_2 represents the random vectors in [0, 1].

$$\vec{A} = 2\vec{a} \cdot \vec{r}_1 - \vec{a} \tag{7}$$

$$\vec{H} = 2 \cdot \vec{r}_2 \tag{8}$$

Basically, the value of the constituent $\vec{a}$ is linearly reduced from 4 to 0. Instead, the proposed GWO is exponentially decreased from 4 to 1 and the corresponding formulation for the component $\vec{a}$ is represented in eq. (9) where $\alpha_{\max}$ is set as 2 and $\alpha_{\min}$ is set as 1 and B is a constant (0.1×10^{-5}). If the corresponding value of $\vec{a}$ is 0, then the golf is almost nearest to the prey.

$$\vec{a} = [(\alpha_{\max} - \alpha_{\min}) * \frac{2}{Maximum \quad iteration} + B] \tag{9}$$

The general formulation for the hunting behavior is described as in eq. (10).

$$\vec{Z}(t+1) = \frac{\vec{Z}_1 + \vec{Z}_2 + \vec{Z}_3}{3} \tag{10}$$

$$\vec{Z}_1 = \vec{Z}_\alpha - \vec{A}_1 \cdot (\vec{G}_\alpha) \tag{11}$$

$$\vec{Z}_2 = \vec{Z}_\beta - \vec{A}_2 \cdot (\vec{G}_\beta) \tag{12}$$

$$\vec{Z}_3 = \vec{Z}_\delta - \vec{A}_3 \cdot (\vec{G}_\delta) \tag{13}$$

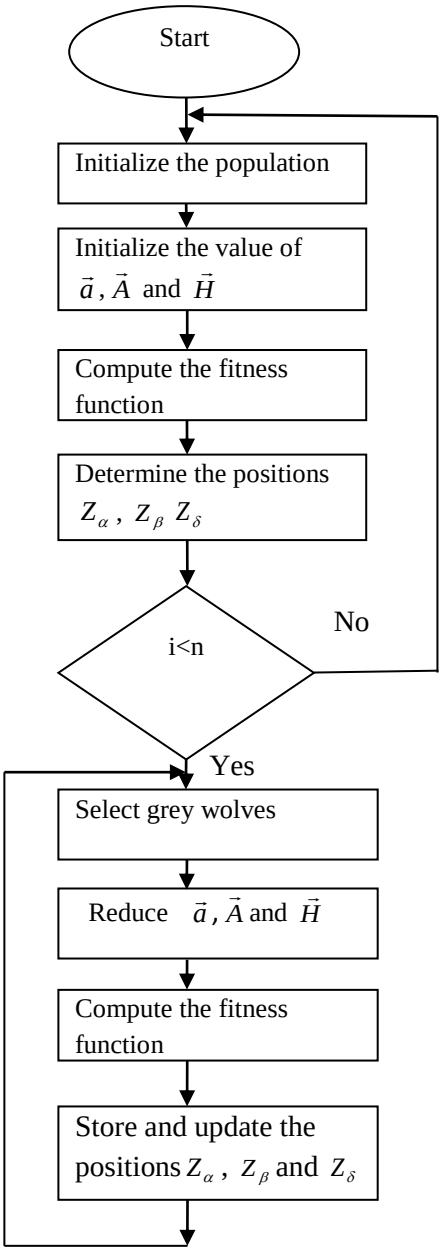

Figure 3. Flow chart of the proposed system.

$$\vec{G}_\alpha = \left|\vec{H}_1 \cdot \vec{Z}_\alpha - \vec{Z}\right| \tag{14}$$

$$\vec{G}_\delta = \left|\vec{H}_3 \cdot \vec{Z}_\delta - \vec{Z}\right| \tag{15}$$

The position of α, β and δ defines the final position of the prey. Thus the aforesaid wolves are responsible for identifying the position of the prey, whereas the other wolves randomly update their positions in the region of the prey. The flowchart of the proposed GWO is given below and the corresponding flowchart is shown in figure 3.

The Adaptive 2DCM was experimentally investigated on ultrasound medical images from, http://www.ultrasoundcases.info/case-list.aspx?cat=26) and the extensive performance study was carried out.

4.Results and Discussions

4.1 Key Space Analysis

The required parameter (x_0, y_0) for the encryption of image using 2DCM is selected as constant in the standard process. However, the proposed GWO methodology choose the range of the parameter within the limit of $(x^{\max}, y^{\max})$. When the (x_0, y_0) is constant, the key space analysis can be performed better. Here since, the parameter have high range, the key analysis seems to be critical as the key space is large.

4.2 Key sensitivity analysis

The key sensitivity depends the percentage deviation of the two cipher image obtained by using two keys to a single image. Initially, k_1 key is used to obtain the first cipher image C_1. Further, another k_2 key is used to obtain the second cipher image C_2.The percentage differences of the two keys are computed using eq. (16).

$$\%D = \frac{C_1 - C_2}{255 \times \ Number \ \ of \ \ pixels} \tag{16}$$

Demonstrated using Eq.(16) on Ultrasound images and obtained percentage difference between the two ciphers are shown in table 3.. accordingly, the tabulation shows the comparison of the standard encryption with the encryption using GA, GWO and proposed GWO. The key sensitivity corresponds to the ultrasound images of the proposed method is 1%, 2.29% and 2.07% better than the standard, GA and GWO. Similarly, the key sensitivity related with the Ultrasound images of the proposed method provides better performance of 0.17%, 1.34%, 1.83% and 0.72%, 1.29%, 0.75% from the GA and GW methodologies.

In this section, the histogram analysis of the original image with its corresponding cipher image is analysed. The uniform histogram gives that better performance.The histogram analysis of the Ultrasound images and their respective cipher images are shown in figure 4 and figure 5. From the analysis, it is noted that the histogram of the original images shows the difference among diverse images, but the histogram of the cipher images seem to be similar. (H), vertical (V) and diagonal (D) pixels are analyzed in table 4. less autocorrelation which is better than conventional methods like standard, GA and GWO.

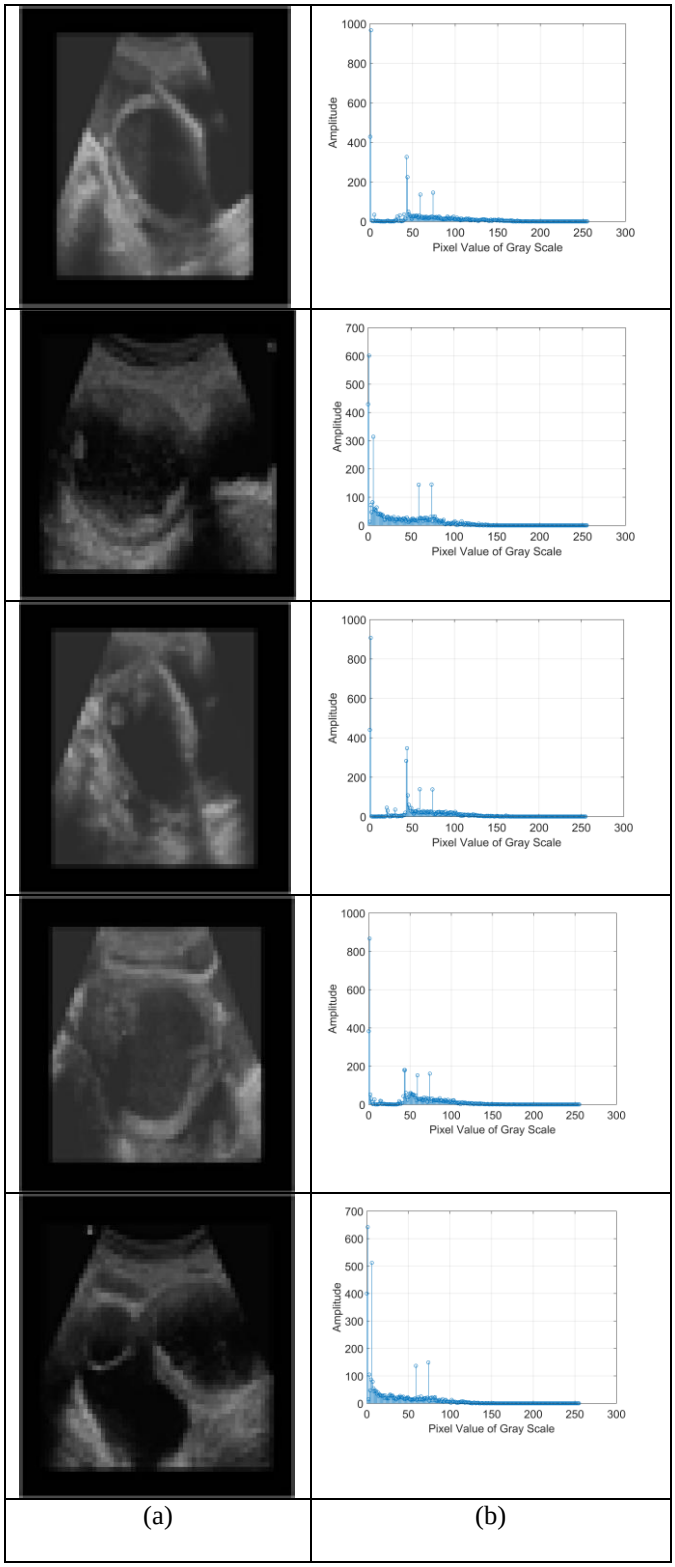

Figure 4. Histogram analysis of ultrasound images with its cipher images (a) Original images (b) Histogram of original images.

4.3 Auocorrelation of adjacent pixels

The autocorrelation of the adjacent pixel of ultrasound images, corresponding to the horizontal H is verified by computing the correlation among the pixels of the horizontal matrix of the image. Similarly, V is the correlation among the pixels of vertical matrix and D is the correlation among pixels of the diagonal matrix of the image. Here in most cases, the proposed GWO provides good results.

4.4 Estimation of ellaped time

The total time required for both encryption and decryption process is determined. The demonstration of the elapsed time is shown in table 5. Here the required elapsed time for the proposed GWO is less when compared with the conventional methods for different metrics.

4.5 Attacks

The attacks such as Known Plain Text Attacks (KPA) and Cipher Plain Text Attacks (CPA) are determined. KPA is analyzed by correlating one original image with all original images and one cipher images with all cipher images. Similarly, the CPA analysis is described by correlating each cipher image with its corresponding decrypted image.Further, the first row of the original image is changed and the cipher images are obtained. By following this process for all images, the correlation between each original image with the corresponding cipher images is analyzed which is referred as the chosen KPA. The KPA, CPA and chosen KPA analysis is shown in table 6. Thus the proposed GWO is in pass condition for all attacks when compared with the standard, GS and GWO. F indicates fail and P indicates Pass.

4.6 Chi-Square Test

Chi-Square is the statistical test determining the righteousness of the predicted and the observed values.The Chi- square analysis of ultrasound images are observed in results analysis. The comparison between the proposed and the existing methods have proved that the proposed GWO provides better performance by obtaining minimum ranking.

Table 3. Key Sensitivity of Ultrasound Images

Ultrasound	STANDARD	GWO	PROPOSED
Image 1	16.32	16.80	16.64
Image 2	16.63	16.58	16.79
Image 3	16.88	16.24	16.82
Image 4	16.91	16.54	17.23
Image 5	16.96	16.67	17.07

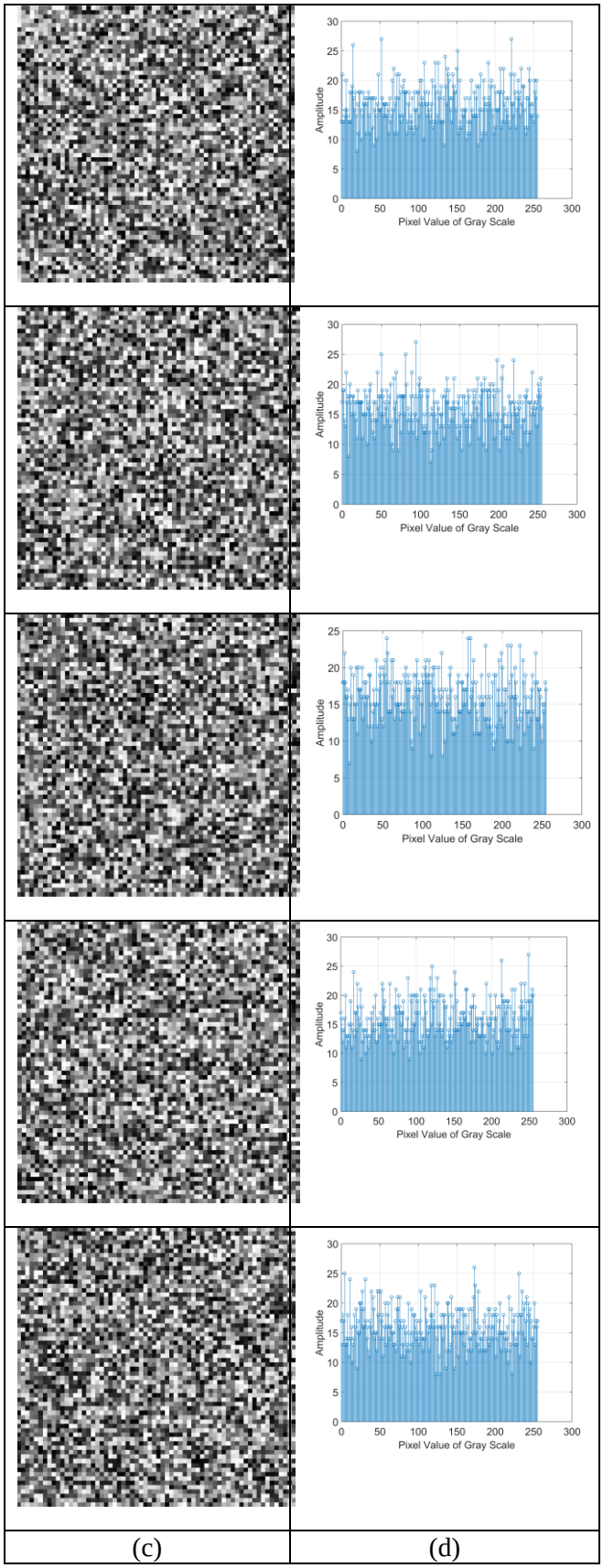

Figure 5. Histogram analyses of cipher ultrasound images

Table 4. Analysis of Proposed Autocorrelation of Adjacent Pixels with the Conventional Methods of Ultrasound Images

Images		Standard	GA	GWO	Proposed
Image 1	H	-0.008	0.022	0.019	0.007
	V	0.002	-0.019	-0.017	0.024
	D	0.032	-0.013	0.006	0.020
Image 2	H	-0.009	0.008	0.012	-0.030
	V	-0.014	0.007	0.011	0.014
	D	-0.003	0.026	-0.005	-0.003
Image 3	H	-0.025	-0.019	0.0051	0.006
	V	-0.003	0.011	-0.011	-0.004
	D	-0.014	-0.011	-0.007	-0.019
Image 4	H	-0.002	0.022	-0.012	0.020
	V	-0.005	0.027	0.008	-0.016
	D	0.016	-0.015	0.013	-0.002
Image 5	H	-0.009	-0.012	0.006	0.005
	V	-0.0131	-0.036	-0.015	0.012
	D	-0.018	0.029	0.001	-0.036

Table 5. Elasped Time Estimation of Proposed GWO with Conventional Methods

Metrics	Standard	Genetic	GWO	Proposed
32x32	1.4496	62.019	59.861	57.602
64x64	1.0774	339.94	268.35	264.78
128x128	4.7329	1237.9	1437.9	1437.9
256x256	22.14	5794.3	6729.4	6186.9

Table 6. Analysis of KPA, CPA and Chosen KPA

Methods	KPA	CPA	Chosen KPA
Standard	0.07635(F)	0.4815(F)	0.9736(P)
Genetic	0.2942 (F)	-0.3327(P)	0.9140(F)
GWO	0.1278(F)	0.4878(F)	0.9630(F)
Proposed	-0.1075(P)	-0.1016(P)	-0.4759(P)

5. Conclusion

Considering the popularity of E-hospitals and M-hospitals, it is necessary to encrypt clinical ultrasound medical images. In this study, we developed a chaos-based visual encryption based on adaptive 2DCM that applied to clinical ultrasound medical images.The interleaved image is thus transferred over noisy channels and stored the performance analysis has been done by determining the key sensitivity, histogram analysis, adjacent pixel autocorrelation, Chi-square test etc. Further, this system may be applied to other medical image modalities such MRI,CT-Scan,X-Ray etc. also may be applied to 3D medical image protection.

Reference

[1] S. Mitra,and B.U. Shankar,"Medical image analysis for cancer management in natural computing framework", *Information Sciences*,Vol. 306, pp.111-131,2015.

[2] United States Department of Health and Human Services. HIPPA: medical privacy—national *standards to protect the privacy of personal health information.* Available from http://www.hhs .gov/ocr/hippa

[3] X.Y. Wang,Y.Q. Zhang and L.T. Liu,"An enhanced sub-image encryption method", *Optics and Lasers in Engineering*, vol. 86, pp. 248-254, November, 2016.

[4] H. Hofbauer and A. Uhl, "Identifying deficits of visual security metrics for images", *Signal Processing: Image communication* , Vol. 46,pp.60-75,2016.

[5] X. Wu,D. Wang, J. Kurths, and H.Kan, "A novel lossless color image encryption scheme using 2D DWT and 6D hyperchaotic system", *Information Sciences* 349, pp. 137-153,2016.

[6] S.Mirjalilii,S.M and A.Lewis,"Grey wolf Optimizer," *Advances in Engineering Software* 69 (2014): 46-61.

[7] E. Biham and A. Shamir, "*Differential cryptanalysis of the data encryption standard*", Springer Science & Business Media, 2012.

[8] W.C Barker, and E.B Barker,"SP 800-67 Rev. 1. Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher", (2012).

[9] B. Nicholas, "News and views: RSA algorithm in the public domain; Woz joins the Inventors Hall of Fame; entangled photons mean faster, smaller ICs; BEHEMOTH mothballed; Advanced Encryption Standard selected; SGI releases SDK as open source; WSDL spec released", *Dr. Dobb's Journal of Software Tools*, Vol.25, No. 12, 2000.

[10] A.Das and A.Adhikari,"An Efficent Multi-use Multi-Secret Sharing Scheme based on Hash Function", Appliead Mathematics Letters",Vol. 23, pp.993-996,2000.

[11] K. Martin,R. Lukac and K.N. Plataniotis, "Efficient encryption of wavelet-based coded color images", *Pattern Recognition*,Vol. 38, No. 7, pp. 1111-1115,2005.

[12] M.Naor, and A. Shamir, "Visual Cryptography, ''Advances in Cryptology Eurocrypt 94,Lecture Notes in Computer Science 950: 1.

[13] J.X. Chen, Z.L. Zhu, C.Fu, H.Yu, and L.B.Zhang, "A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism ", *Communications in Nonlinear Science and Numerical Simulation*, Vol.20, No. 3,pp.846-860,2015.

[14] C.F.Lin,W.T. Chang and C.Y.Li,"A Chaos based Visual Encryption Mechanism in-JPEG Medical Images",*Journal of Medical and Biological Engineering*, Vol.27,No.3,pp.144-149, 2007.

[15] https://en.wikipedia.org/wiki/Chaos_theory.

[16] Y. Li, L.Liang, Z.Su, and J.Jiang,"A new video encryption algorithm for H. 264", In *2005 5th International Conference on Information Comm unications & Signal Processing*, pp. 1121-1124. IEEE, 2005.

[17] K.D. Rao,"A robust and secure scheme for image communication over wireless channels", In *2005 IEEE 7th CAS Symposium on Emerging Technologies: Circuits and Systems for 4G Mobile Wireless Communications*, pp. 88-91. IEEE, 2005.

[18] K.W. Tang and W.K. Tang,"A chaos-based secure voice communication system", *IEEE International Conference on Industrial Technology*, pp. 571-576. IEEE, 2005.

[19] C.K.Volos, I.M.Kyprianidis and I.N. Stouboulos, "Chaotic cryptosystem based on inverse duffing circuit." In *Proc. of the 5th International Conference on Non–linear Analysis, Non–linear Systems and Chaos (NOLASC 2006)*, pp. 92-97. 2006.

[20] V. Grigoras, and C. Grigoras,"Chaos Encryption Method Based on Large Signal Modulation in Additive Nonlinear Discrete-Time System",*Proc. of the 5th WSEAS Int. Conf. on Non-Linear Analysis, Non-Linear Systems and Chaos, Bacharest, Romania*, pp.16-18,2006.

[21] H.P.Xiao, and G.J Zhang,"Image encryption based on chaotic maps", *In Systems, Man, and Cybernetics,. Computational Cybernetics and Simulation, 1997 IEEE International Conference on*, Vol. 2, pp.1105-1110, IEEE, 1997.

[22] J.C.Yen,and J.I.Guo,"A New Mirroe-like image encryption algorithm and its VLSI architecture", *Department of Electronics Engineering National Lien-Ho College of Technology and Commerce*, Miaoli, Taiwan, Republic of China in 1999.

[23] F.Han,J.Hu,X.Yu, and Y.Wang,"Fngerprint images encryption via multi-scroll chaotic attractors" , *Applied Mathematics and Computation*, Vol.185, No. 2, ppp. 931-939,2007.

[24] S.S.Maung, and M.M. Sein," A fast encryption scheme based on chaotic maps",pp.1-16,2008.

[25] A.A.El-Latif, and X.Niu,"A hybrid chaotic system and cyclic elliptic curve for image encryption", *AEU-International Journal of Electronics and Communications*, Vol.67, No2, pp.136-143,2013.

[26] Q.Zhang, L.Guo and X.Wei,"Image encryption using DNA addition combining with chaotic maps", *Mathematical and Computer Modelling*, Vol.52, No.11, pp.2028-2035,2010.

[27] N.K.Pareek, V.Patidar,K.K.Sud, "Image encryption using chaotic logistic map", *Image and Vision Computing*, Vol.*24,No.*9, pp.926-934.

[28] S.R.Maniyath, and M. Supriya," An uncompressed image encryption algorithm based on DNA sequences", *Computer Science and Information Technology*, Vol.2, pp.258-270, 2011.

[29] Q.Zhang,S.Zhou, and X.Wei,"An efficient approach for DNA fractal-based image encryption", *Appl. Math. Inf. Sci*,Vol. 5, pp.445-459,2011.

[30] R.E.Boriga, A.C.Dăscălescu, and A.V.Diaconu, "A new fast image encryption scheme based on 2D chaotic maps", *IAENG Int. Journal of Computer Science*, Vol.41, No.4, pp.249-258, 2014.

[31] C.Fu, W.H. Meng, Y.F. Zhan, Z.L.Zhu, F.C.Lau, K.T.Chi, and H.F.Ma, "An efficient and secure medical image protection scheme based on chaotic maps", *Computers in biology and medicine*, Vol. 43, No.8, pp.1000-1010, 2013.

[32] J.Hu, and F.Han, "A pixel-based scrambling scheme for digital medical images protection", *Journal of Network and Computer Applications*, Vol.32, No.4, pp.788-794,2009.

[33] G.Zhou, D.Zhang, Y.Liu, Y.Yuan, and Q.Liu, "A novel image encryption algorithm based on chaos and Line map", *Neurocomputing*, No.169, pp.150-157, 2015.

[34] I.Bremnavas, B.Poorna, and I.R.Mohamed, "Secured medical image transmission using chaotic map", *Elixir Comp. Sci. Eng*, Vol.54, 2013.

[35] K.Singh, and K.Kaur, "Image Encryption using Chaotic Maps and DNA Addition Operation and Noise Effects on it", *International Journal of Computer Applications",* Vol, 23, pp. 0975-8887, 2011.

[36] L.Gupta,R.Gupta, and M.Sharma,"Low Complexity Efficient Image Encryption Technique Based on Chaotic Map", *International Journal of*, 2014.

[37] R.Kaur,"Comparative analysis and implementation of image encryption algorithms", *International Journal of Computer Science and Network Security (IJCSNS)*, Vol.13,No.12, 2013.

[38] P.N.Khade, and M.Narnaware,"3D chaotic functions for image encryption", *IJCSI International Journal of Computer Science Issues*, Vol.9,No.3, pp.323-328,2012.

[39] S.Koppu and V.,"A novel chaotic image encryption system for color images based Arnold cat map and efficient pixel shuffling," International Journal of Pharmacy & Technology, Vol.8, No.2, pp.13353-13361,2016

[40] S.Koppu and V., "A survey on security issues: digital images", International Journal of Pharmacy & Technology, Vol.8, No.2, pp.13420-13427, 2016.

[41] K. Lakshmanna and N. Khare, "Constraint-Based Measures for DNA Sequence Mining using Group Search Optimization Algorithm", The Intelligent Networks and Systems Society, Vol.9, No.3, pp.91-100, 2016.

[42] H.Gao, Y.Zhang, S.Liang and D.Li, D., "A new chaotic algorithm for image encryption," *Chaos Solitons & Fractals*, Vol.29, No. 2,pp.393-399, 2006.

[43] F.Sun, S.Liu, Z.Li, and Z. Lü, "A novel image encryption scheme based on spatial chaos map", *Chaos, Solitons & Fractals, Vol.*38, No.3, pp.631-640, 2008.

[44] N.K.Pareek, V.Patidar, and K.K.Sud, "Image encryption using chaotic logistic map", *Image and Vision Computing*, Vol.24, No. 9, pp.926-934,2006.

[45] G.Chen, Y. Mao, and C.K. Chui, "A symmetric image encryption scheme based on 3D chaotic cat maps", *Chaos, Solitons & Fractals Vol.*21, No.3, pp.749-761,2004.

[46] Y.Mao,G.Chen, and S.Lian,"A novel fast image encryption scheme based on 3D chaotic baker maps", *International Journal of Bifurcation and Chaos,Vol.*14, No.10, pp.3613-3624, 2004.

[47] Z.Song, L.Hengjian, and Y.Xu, "A secure and efficient fingerprint images encryption scheme", *In Young Computer Scientists, 2008, The 9th International Conference*, pp.2803-2808,IEEE, 2008.

[48] T.Gao, and Z.Chen,"Image encryption based on a new total shuffling algorithm",*Chaos, solitons & fractals*, Vol.38, No.1 pp.213-220,2008.

[49] J.Lai, S.Liang, S. and D. Cui, "A novel image encryption algorithm based on fractional Fourier transform and chaotic system", *In Multimedia Communications (Mediacom), International Conference on*, pp. 24-27. IEEE, 2010.

[50] C.Fu,W.H.Meng,Z.han, Y.F.,Zhu, Z.L.Lau, H.F.Ma and"An efficient and secure medical image protection scheme based on chaotic maps", *Computers in biology and medicine*, Vol.43, No. 8,pp.1000-1010,2013.

[51] Q.Zhang, L.Guo, and X.Wei,"Image encryption using DNA addition combining with chaotic maps", *Mathematical and Computer Modelling*, Vol.52, No.11,pp.2028-2035,2010.

[52] S.Mirjalili, S.M.Mirjalili, and A.Lewis,"Grey Wolf Optimizer", *Advances in Engineering Software*, Vol. 69, pp.46–61, 2014.

[53] R.Kaluri, C.H. Pradeep Reddy, "A Framework for Sign Gesture Recognition using Improved Genetic Algorithm and Adaptive Filter", Cogent Engineeri ng, Vol.3, No.1, pp.1-9, 2016.

[54] C.D. Naidu, S. Koppu, V. and S.L. Aarthy," Crystography Based Medical Image Security with LSB-Blowfish Algorithms", *ARPN Journal of Engineering and Applied Sciences*,Vol.9,No.8,2014.