Current Trends in
Clinical & Medical Imaging
ISSN: 2573-2609

Juniper Publishers
key to the Researchers

Clinical Image
Volume 3 Issue 2 - May 2019
DOI: 10.19080/CTCMI.2019.03.555609

Curr Trends Clin Med Imaging

Medical Image Security Based on Enhanced 1D Chaotic Map

Dhanalaxmi Banavath[1]*, Suryanarayana Lakavath[2] and Srinivasulu Tadisetty[1]

[1]*Department of Electronics and Communication Engineering, KU College of Engineering & Technology, Kakatiya University, University, (T.S), India*

[2]*University College of Pharmaceutical Sciences, Kakatiya University, (T.S), India*

Received date: April 24, 2019; **Published date:** May 28, 2019

***Corresponding author:** Dhanalaxmi Banavath, Department of Electronics and Communication Engineering, KU College of Engineering & Technology, Kakatiya University, University, (T.S), India

Abstract

Medical images are playing for an importance diagnosis of many diseases. However, the securities of medical images are inferior. Therefore, the importance of security of medical images is paramount to avoid mishandling moreover; the conventional cryptographic algorithms are unable to provide robust security. Hence, an innovative algorithm has been developed to provide robust security to medical images to avoid mishandling. In this paper introduces a new method for medical image of making a simple and more effective chaotic system by using two differences of the output sequence of same existing one-dimension (1D) chaotic maps. The medical images simulation and security evaluations show that the proposed system is able to produce a one-dimension (1D) chaotic system, which is better chaotic performance and wide chaotic ranges compared with the previous chaotic maps. To the investigate its applications in medical images security encryption, a novel encryption system of linear-nonlinear-linear structure based on total shuffling method is proposed. The experiment was demonstrated the accuracy of the medical image's encryption algorithm. The experiments and security analysis prove that the algorithm has an excellent performance in medical images encryption and various brute force attacks. As medical images contain noise, we should apply median filter as preprocessing step. And to get improved results we applied histogram equalization for encrypted image to get final encrypted image which is more robust than normal encryption.

Keywords: Medical images encryption; Chaotic algorithm; Histogram; PSNR; Image

Introduction

Traditionally, the pelvic treatment fields for gynaecological canNowadays information security is a vital key problem in information communication technology. With the advancements of information technology, plenty of digital contents are being stored and transmitted in various forms. As a result, the protection of digital contents data against non-uniform phenomena, such as illegal copying, and guarantee of their secure utility has become an important issue. Compared to text data, some intrinsic features of image data, such as big size, high diffusion of data and strong correlation among adjacent pixels are different with expected information. Furthermore, image data requires the strong real-time property in communication, therefore, an encryption method with fast speed and high security is needed. But the traditional algorithms block encryption being extensively used now is found to be inefficient for real-time communication system [1]. Therefore, too many image encryption methods using chaotic maps with more sensitivity to their initial conditions and system parameter values and simple structures are proposed. There are many algorithms used in image security encryption, such as fractional wavelet transform [2,3], p-Fibonacci transform [4], gray code [5], vector quantization [6] and chaos [10-29], have been proposed and among them the image security encryption based on the chaotic map is being more widely used. In some of the researches have been used, S-box using the chaotic sequence is in encryption and decryption system [30-32].

This encryption system can be divided into two parts:

i. One part is generating the security key.

ii. Other part is encryption by using the key.

In the chaotic maps used in creating the security key can be divided into two categories: one is one-dimension (1D) and other one is multi-dimension (MD). At present, the MD chaotic maps are being more widely applied to image security encryption systems. But, owing to their composite structures and multiple parameters, the difficulty of their hardware/software implementations and the estimation complexity ware increased. Here, the contrary, 1D chaotic map has an advantage that their structures are simple; they ware easiest to implement and have lowered the computation-cost.

Literature Survey

In this paper, some existing perceptual encryption algorithms of MPEG videos are reviewed and some problems, especially

security defects of two recently proposed MPEG video perceptual encryption schemes, are pointed out. Then, a simpler and more effective design is suggested, which selectively encrypts fixed-length code words (FLC) in MPEG-video bit streams under the control of three perceptibility factors. The proposed design is an encryption configuration that can work with any stream cipher or block cipher. Compared with the previously proposed schemes, the new design provides more useful features, such as strict size-preservation, on-the-fly encryption and multiple perceptibility, which make it possible to support more applications with different requirements. In addition, four different measures are suggested to provide better security against known/chosen-plaintext attacks.

Gaurav Bhatnagar proposed in this paper, the dual tree complex wavelet transform, which is an important tool and recent advancement in signal and image processing, has been generalized by coalescing dual tree complex wavelet transform and fractional Fourier transform. The new transform, i.e. the fractional dual tree complex wavelet transforms (FrDT-CWT) inherits the excellent mathematical properties of dual tree complex wavelet transform and fractional Fourier transform. Possible applications of the proposed transform are in biometrics, image compression, image transmission, transient signal processing etc. In this paper, biometric is chosen as the primary application and hence a new technique is proposed for securing biometrics during communication and transmission over insecure channel.

Proposed Method

In this section, a new image encryption algorithm is proposed and its application in information security is verified for medical images. The encryption algorithm uses five parameters of (X^0, u, k, N_0, l_p) as the security key. The diagrams of the proposed cryptosystem ware shown in (Figure 1).

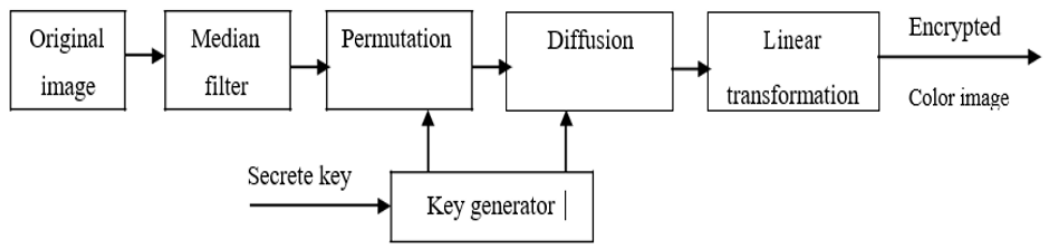

Figure 1: Block diagram of proposed cryptosystem.

Encryption Process

Step 1: The size of the color image of is $M \times N$ divided into 3 images with R, G and B channels respectively, and then the three images are linked to make a grayscale image with the size of $M \times 3N$ In this case of the Grayscale image with the size of $M \times N$, it will be used without conversion.

Step 2: medical images have more noise than we can use A median filter the median filter is used to remove noise from images.

Step 3: The image of grayscale is obtained above is converted into the 1D image pixel matrix $P = \{p1, p2, ...pM \times 3N\}$ with the size of $M \times 3N$.

Step 4: X is used in the chaotic system encryption is getting in the new chaotic system. The initial values are x0, u and k of the chaotic system and is used as the security keys. the new chaotic system is $(M \times 3N + N0)$ times and discard the former $N0$ elements to make a new sequence with $M \times 3N$ elements. Where N0 is a constant used as the security key.

Step 5: we can use and getting the permutation position matrix $X' = \{X'1, X'2....X'M \times 3N\}$ by sorting the chaotic sequence X in ascending order. The process is shown in below (Figure 2).

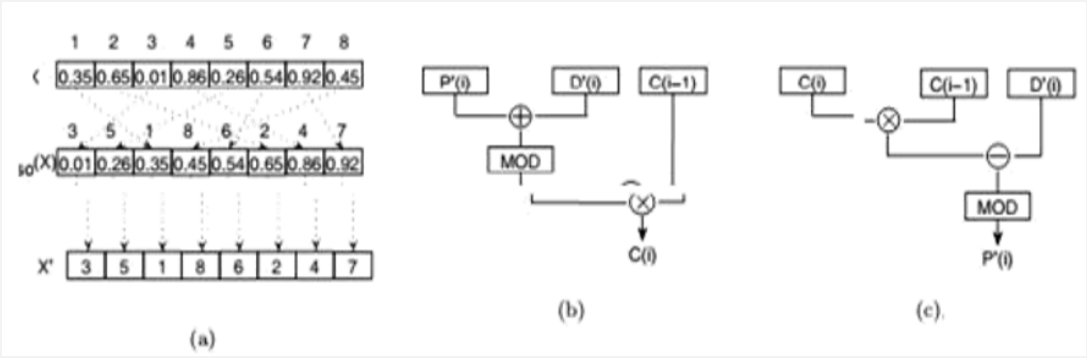

Figure 2: Diagram of A) Generating of permutation position matrix, B) Diffusion process encryption, C) Diffusion process in decryption.

How to cite this article: Dhanalaxmi Banavath, Suryanarayana Lakavath, Srinivasulu Tadisetty. Medical Image Security Based on Enhanced 1D Chaotic Map. Curr Trends Clin Med Imaging. 2019; 3(2): 555609.DOI: 10.19080/CTCMI.2019.03.555609

Step 6: The permuted image pixel matrix $P'=\{p'1,p'2,.....p'M\times 3N\}$ by using the permutation position matrix X' and the image pixel matrix P. Permutation equation can express as follows.

$$P'(i)=P(X'(i)); \quad (1)$$

Step 7: Diffusion matrix D $D'=\{d'1,d'2,....d'M\times 3N\}$ then the by the following equation.

$$D'(i)=\mathrm{mod}\left(floorX(i)\times 10^{14}\right),256; \quad (2)$$

Step 8: Obtain the encrypted image pixel matrix $C=\{C1,C2,....CM\times 3N\}$ from the diffusion matrix D' and the permuted image matrix P' by the following diffusion equation is.

$$C(i)=\mathrm{mod}\left(P'(i)\oplus D'(i),256\right)\oplus C(i-1); \quad (3)$$

Where $\oplus$ is the arithmetic plus operator, $\otimes$ bit-level XOR operator, and $C(i-1)$ the previous encrypted pixel. The process is shown in (Figure 3).

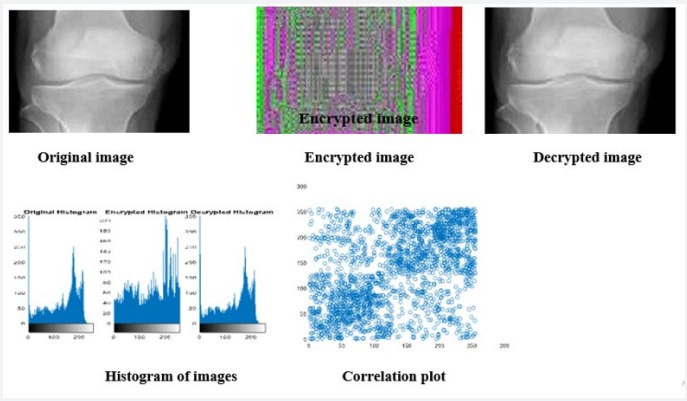

Figure 3: Previous work of MRI Image for knee joint of leg.

Step 9: A new encrypted image pixel matrix by $C'=\{C'1,C'2,....C'M\times 3N\}$ rotating the above obtained encrypted matrix C to the left by the amount of lp.

Where l_p is used as a security key and $1P\in[1,M\times 3N]$. The new image pixel matrix C' is obtained in the following equation.

$$\begin{cases} C''(i-lp)=C(i); & \text{i-lp}\geq 1 \\ C''(i-lp)+M\times N=C(i); & \text{i-lp}\geq 1 \end{cases} \quad (4)$$

The step 9 not only avoids the repetition of linear (permutation)-nonlinear (diffusion) conversion to shorten the encryption time, but also increases the strength of encryption.

Step 10: Apply Histogram equalization for encrypted image to get improved encrypted image.

Step 11: Convert them into the R, G and B color image with the size of $M\times N$

Decryption Process

The decryption is the inverse process of encryption. The permutation and diffusion equations used in decryption are as follows.

$$P(X_0(i))=P_0(i); \quad (5)$$

$$P_0(i)=\mathrm{mod}\left(C(i)\otimes C(i-1)D_0(i),256\right); \quad (6)$$

Where is the arithmetic minus operator. The process of the equation (6) is shown in (Figure 4). The encryption and decryption algorithms are simple, but they are enough to increase the strength of encryption. They can be applied not only to color image, but also to grayscale image (Table 1).

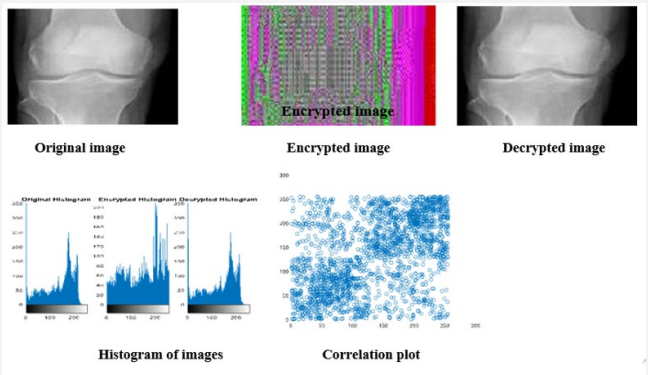

Figure 4: Present work of MRI Image for knee joint of leg.

How to cite this article: Dhanalaxmi Banavath, Suryanarayana Lakavath, Srinivasulu Tadisetty. Medical Image Security Based on Enhanced 1D Chaotic Map. Curr Trends Clin Med Imaging. 2019; 3(2): 555609.DOI: 10.19080/CTCMI.2019.03.555609

Table 1: MSE and PSNR results of proposed and extension methods.

Images	Proposed work		Extension work	
	MSE	PSNR	MSE	PSNR
1	44.42822	31.6542	21.08691	34.89067
2	20.26567	35.06319	2.049133	45.0151

Results

Differential Analysis of Medical Image

In the 1D chaotic algorithm is very specific for medical images, in order to test the effect of a pixel change on the entire cipher Image, present work is usually compared with existing work: The Number of Pixels Change Rate (NPCR) and the Unified Change Intensity (UACI). (Table 2): lists the medical image of NPCR and UACI values. As can be seen from (Table 2): different values of present and existing work encryption, the NCPR value very close to 1 and UACI value close to 0 [33-37].

Table 2: Correlation, NPCR and UPCI values of proposed and extension methods.

Images		Proposed work				Extension work				
	Time (sec)	Vertical correlation	Horizontal correlation	NPCR	UPCI	Time	Vertical correlation	Horizontal Correlation	NPCR	UPCI
1	2.71	-0.023	0.556957	0.99609	0.33463	0.42	-0.06056	0.533729	0.99609	0.33463
2	4.47	-0.4907	0.063144	0.996	0.33463	0.43	-0.56614	0.101228	0.99609	0.33463

Conclusion

As we saw, the security issues for Medical Images are the same as for any medical data. At the frontier between information security and trust during medical practice, we propose to express it in terms of Confidentiality, Availability Reliability, with output data integrity &authenticity this such a framework results modifying medical image accidental during communicating lossy image compressing cause unexpecting loss data image causing misdiagnose and responsibly physician shows interprets image not informed .

This paper, first, we proposed a method of making very simple and high effective chaotic system by using a difference of output sequences of the two same existing one-dimension 1D chaotic maps. Simulations, performance and evaluations showed that this proposed system is proficiency to produce a one-dimension (1D) chaotic system with better chaotic performances and wider chaotic ranges compared with the previous chaotic maps. Secondly, we proposed a novel encryption system of linear-nonlinear-linear structure based on total shuffling to confirm its applications in medical image encryption. Experiments and security analysis proved that the algorithm has an excellent performance in medical image encryption and various attacks. For extension we applied median filter to remove the noise from input medical image as well as at encryption stage we applied histogram equalization.

References

1. S Li, G Chen, A Cheung, B Bhargava, KT Lo (2007) On the Design of Perceptual MPEG-Video Encryption Algorithms. IEEE Transactions on Circuits & methods for Video technological know-how 17(2): 214-223.
2. G Bhatnagar, QMJ Wu, B Raman (2012) a brand new Fractional Random Wavelet develop into for Fingerprint safety. IEEE Trans. Syst. Man Cybern Part A: Syst Hum 42(1): 262-275.
3. G Bhatnagar, QMJ Wu, B Raman (2013) Discrete fractional wavelet develop into and its software to more than one encryption. expertise Sciences 223(2): 297-316.
4. Y Zhou, k Panetta, S Agaian, CLP Chen (2012) image encryption utilizing P-Fibonacci become and decomposition. Optics Communications 285(5): 594-608.
5. Y Zhou, okay Panetta, S Agaian, CL Chen (2012) (n, ok, p)-grey Code for photograph systems. IEEE Trans. Syst. Man Cybern. Phase A: Syst. Hum 43(2): 515-529.
6. TH Chen, CS Wu, (2010) Compression-unimpaired batch-image encryption combining vector quantization and index compression. Inf. Sci 180(9): 1690-1701.
7. Y Sangeetha, S Meenakshi, CS Sundaram (2014) A simple, touchy and cozy snapshot encryption algorithm headquartered on hyper-chaotic approach with only one round diffusion process. Multimedia tools and purposes 71(3): 1469-1497.
8. A Kassem, Hah Hassan, Y Harkouss, R Assaf (2014) effective neural chaotic generator for photo encryption. Digital signal Processing 25(2): 266-274.
9. D Arroyo, J Diaz, FB Rodriguez, (2013) Cryptanalysis of a one circular chaos-centered Substitution Permutation network signal Processing. Sixty-seven (2):1358-1364.
10. Aaa El-Latif, X Niu (2013) A hybrid chaotic process and cyclic elliptic curve for snapshot encryption AEU. Sixty-seven (2): 136-143.
11. Y Zhou, L Bao, CLP Chen (2014) a new 1D chaotic system for picture encryption. signal Processing 97(7): 172-182.
12. W Wen, Y Zhang, Z Fang, JX Chen (2015) Infrared target-centered selective encryption via chaotic maps. Optics Communications 341: 131-139.
13. Z Hua, Y Zhou, CM Pun, CLP Chen (2014) 2nd Sine Logistic modulation map for picture encryption, understanding Sciences. 297: 80-94.
14. CY Tune, YL Qiao, XZ Zhang (2013) An photograph encryption scheme established on new spatiotemporal chaos. Optik 124(18): 3329-3334.
15. C Lv-Chen, L Yu-Ling, Q Sen-Hui, L Jun-Xiu (2015) A perturbation procedure to the tent map founded on Lyapunov exponent and its software. chinese language Physics B 24(10): 78-85.

How to cite this article: Dhanalaxmi Banavath, Suryanarayana Lakavath, Srinivasulu Tadisetty. Medical Image Security Based on Enhanced 1D Chaotic Map. Curr Trends Clin Med Imaging. 2019; 3(2): 555609.DOI: 10.19080/CTCMI.2019.03.555609

16. Y Zhou, L Bao, CLP Chen (2013) photo encryption using a brand-new parametric switching chaotic method. signal Processing 93(11): 3039-3052.

17. RR Kumar, MB Kumar (2014) a brand-new chaotic snapshot encryption utilizing parametric switching centered permutation and diffusion. Ictact Journal on photo & Video Processing 4(4).

18. C Fu, BB Lin, YS Miao, X Liu, JJ Chen (2011) A novel chaos-based bit-level permutation scheme for digital photo encryption. Optics Communications 284(23): 5415-5423.

19. Z Eslami, A Bakhshandeh (2013) An development over an image encryption system headquartered on total shuffling. Optics Communications 286(1): 51-55.

20. G Zhou, D Zhang, Y Liu, Y Yuan, Q Liu (2015) A novel snapshot encryption algorithm centered on chaos and Line map. Neurocomputing 169: 150-157.

21. FG Jeng, WL Huang, TH Chen (2015) Cryptanalysis and development of two hyper-chaos-based photo encryption schemes. signal Processing photo conversation 34: 45-51.

22. FG Jeng, WL Huang, TH Chen (2015) Cryptanalysis of a development over an photograph encryption method based on complete shuffling. Optics Communications 350: 77-82.

23. R Liu (2015) New Algorithm for color photo Encryption using elevated 1D Logistic Chaotic Map. Open Cybernetics &Systemics Journal 9(1): 210-216.

24. L Xu, Z Li, J Li, W Hua (2016) A novel bit-stage photo encryption algorithm established on chaotic maps. Optics & Lasers in Engineering 78(21): 17-25.

25. B Stoyanov, k Kordov (2014) Novel picture encryption scheme established on Chebyshev polynomial and Duffing map, Scientific World Journal 283639.

26. B Stoyanov, ok Kordov (2015) picture Encryption utilising Chebyshev Map and Rotation. Equation Entropy 17(4): 2117-2139.

27. H liu, X Wang (2011) color photo encryption utilizing spatial bit-level permutation and high-dimension chaotic procedure. Optics Communications 284(1617): 3895-3903.

28. G Sun, M Wang, L Huang, L Shen (2011) generating Multi-Scroll Chaotic Attractors via Switched Fractional techniques. Circuits methods & signal Processing 30(6): 1183-1195.

29. Guang Hhui Sun, Mao Wang (2012) The Fractional Order Modified Chaotic n-SCROLL Chua Circuit and Fractional manage. worldwide Journal of cutting-edge Physics B 26(14): 1099-1113.

30. M Khan, T Shah (2015) An efficient chaotic snapshot encryption scheme. Neural Computing and applications 26(5): 1137-1148.

31. M Khan, T Shah, SI Batool (2016) construction of S-field headquartered on chaotic Boolean capabilities and its utility in photograph encryption. Neural Computing and applications 27(3): 677-685.

32. A Belazi, M Khan, Aaa El-Latif, S Belghith (2016) efficient cryptosystem approaches: S-boxes and permutation substitution-based encryption. Nonlinear Dynamics 1-25.

33. MT Rosenstein, JJ Collins, CJD Luca (1993) A practical system for calculating greatest Lyapunov exponents from small knowledge units. Physica D Nonlinear Phenomena 65(12): 117-134.

34. A Wolf, JB Swift, HL Swinney, JA Vastano, (1985) deciding upon Lyapunov exponents from a time sequence. Physica D Nonlinear Phenomena 16(3): 285-317.

35. MR Titchener, WB Ebeling (2001) Deterministic Chaos and information concept information. Compression convention 0520-0520.

36. CE Shannon (1974) A mathematical conception of verbal exchange. McGraw-Hill 27(3): 379-423.

37. KT Alligood, TD Sauer, JA Yorke (2008) CHAOS: An Introduction to Dynamical systems. Springer 50(11) 67-68.

DOI: 10.19080/CTCMI.2019.03.555609

How to cite this article: Dhanalaxmi Banavath, Suryanarayana Lakavath, Srinivasulu Tadisetty. Medical Image Security Based on Enhanced 1D Chaotic Map. Curr Trends Clin Med Imaging. 2019; 3(2): 555609.DOI: 10.19080/CTCMI.2019.03.555609