Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 11-2023
DOI: 10.5281/zenodo.10121619

NOVEL ENCRYPTED HEALTHCARE SYSTEMS BASED ON CHAOTIC MAPS

SALWA M. SERAGELDIN
Department of Computer Engineering, College of Computers and Information Technology, Taif University. Department of Electronics and Electrical Communications Engineering, Faculty of Engineering, Tanta University.

MOFREH A. HOGO
Electrical Engineering Department, Benha Faculty of Engineering, Banha University, Banha, Egypt.

SHADY EL GOHARY
Electrical Engineering Department, Air Defense College, Egypt.

AHMED KHAIRY MAHMOUD
Electrical Engineering Department, Air Defense College, Egypt.

WAGEDA I. AL SOBKY*
Basic Engineering Sciences Department, Benha Faculty of Engineering, Benha University, Banha, Egypt.
*Corresponding Author Email: wageda.alsobky@bhit.bu.edu.eg

HOSSAM E. AHMED
Electrical Engineering Department, Benha Faculty of Engineering, Banha University, Banha, Egypt.

Abstract

The conventional healthcare systems have recently undergone a radical transformation due to the incorporation of cutting-edge technologies such as compressive sensing, wireless networks, and cloud computing. Computer-aided diagnosis is one of the most active research topics, which shows a noticeable improvement in the medical field. As a result of the development of intelligent techniques, biomedical data processing has become simpler and less prone to errors. In addition, the internet of things (IoT) infrastructure makes it feasible to provide healthcare from a distance. However, the integration of technologies has led to a rise in security issues. Data security over remote healthcare systems is essential, and represents one of the most significant challenges. Consequently, e-health data security and privacy concerns must be thoroughly investigated. Typically, biomedical data are sensitive to external attacks, and even minor data manipulation can have a significant impact on the final result. In some cases, a wrong diagnosis can be fatal, and in most cases, it can be severe. In this paper, secured healthcare systems based on chaotic mapping techniques are reviewed. Future research in multimedia data security and biomedical image protection could greatly benefit from this work.

1. INTRODUCTION

Security and integrity of medical data, particularly medical images, have become significant issues in the e-healthcare environment as a result of the rapid expansion of the Internet of Things (IoT) field. To reduce risk and improve diagnosis results, healthcare must be modernized. Digital technologies make patient care delivery easier and more efficient, resulting in better outcomes. The advantages of technological innovation in healthcare are apparent. However, as digital technologies become more prevalent and healthcare systems become more interconnected, healthcare cybersecurity threats are increasing rapidly. Since medical images contain important sources of patient privacy

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 11-2023
DOI: 10.5281/zenodo.10121619

data, the development of efficient security mechanisms is necessary. More attention should be paid to provide secure services. Efficient encryption algorithms on the Internet of Healthcare Things (IoHT) systems need to be developed to avoid security breaches. Patient information must be transmitted and stored securely [1], [2].

With telemedicine technology, medical data/images are stored and transmitted over the internet for specified diagnostic purposes such as extracting discriminative features and hidden details, noise removal, segmentation, and feature reduction via efficient compression methodologies. Active medical research, remote wireless clinical diagnosis, prompt treatment of unforeseen incidents, and immediate access to patient data can all help improve communication among telemedicine systems. People are now able to communicate with one another from anywhere, thanks to the widespread use of computer networks, which are becoming increasingly popular for the transmission of digital medical images. When medical images are transmitted online, however, there may be serious issues with confidentiality, integrity, authentication, cropping, tampering, and destruction by attackers. As a result, the Society of Computer Applications in Radiology (SCAR) and the American College of Radiology (ACR) have published guidelines and suggestions to guarantee the safety of medical images [3].

Steganography and cryptography are two methods that are frequently used for securing image information. Encrypting images is very important for communication in networks because of the rapid growth of telemedicine, which makes it easy to send large amounts of medical image data [22]. As a result, encryption has become important for hiding private information of patients. The optimum way to provide medical data protection against threats is through encryption. For text data, the Data Encryption Standard (DES), Triple Data Encryption Standard (TDEA), Advanced Encryption Standard (AES), Rivest, Shamir, and Adleman (RSA), and Data Encryption Standard (DES) have been widely employed. However, due to their high pixel redundancy, these cryptographic techniques are not appropriate for large-size images. Recently, the dynamic properties of chaotic maps have been successfully exploited to construct chaotic-based cryptosystems [1, 2, 3].

2. SECURITY IN WIRELESS BODY AREA NETWORKS (WBANs)

By 2050, in the global population, there will be approximately 2.1 billion people who is beyond 60, according to a study done by World Health Organization (WHO) [4]. The growing number of the elderly will raise more and more healthy problems. Wireless Body Area Networks (WBANs) are genuinely capable of transforming the healthcare systems, as they provide sophisticated but easy-to-use diagnosis of diseases and real-life monitoring. WBANs are considered essential in detecting and treating dangerous cases such as diabetes and hypertension. Healthcare must be provided to all people, including citizens who live in small villages and rural regions. It is not often possible for most patients to stay long periods in hospitals, due to the economic constraints, work, and other personal reasons, although they must be continually supervised. Telemedicine provides the optimal solution. Telemedicine is defined as the benefit of wireless communications and information technology (IT) to offer clinical health services at a distance. It enables

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 11-2023
DOI: 10.5281/zenodo.10121619

eliminating distance obstacles and can facilitate accessing medical facilities not found in rural distant societies. Telemedicine is also important to rescue critical urgent cases and save life [5, 6]. Feasibility of telemedicine can be fulfilled by making use of the great recent advancement in microelectronics and telecommunications, and also the development in managing medical information through the internet. Telemedicine is classified according to transmission into two types:

1. Simultaneous diagnosis, where communication and interaction occur at the same time between patients on one side and the consultants on the other side.
2. Non-simultaneous diagnosis, where the supervisor of the patient provides the required reports on video or other tools, and receives the response from the consultant later [7].

Healthcare systems are divided according to severity of the patient case into [8]:

1. ***Primary Healthcare***: is a diagnosis of simple cases in urban or rural healthcare units. Medical examination is executed by a general practitioner or a family medicine specialist.
2. ***Secondary Healthcare***: applied in district hospitals mainly by specialists and consultants for mild or moderate cases, while severe cases are referred to tertiary healthcare.
3. ***Tertiary Healthcare*****:** applied in specialized hospitals, specialized health institutes and university hospital, benefiting from specialized lecturers or professors.

An IT-based telemedicine system is shown in Fig. 2.1 [9]. The system consists mainly of a number of tiny sensors and a gateway, which can be a smart phone or a personal digital assistant (PDA). The gateway forward sensor information to the destination when a communication link is available. Sensors are classified according to their position into wearable or implant. The wearable medical devices are attached to the skin or very near to the human body. Examples of wearable medical applications include telemonitoring of temperature, blood pressure, glucose levels, ECG, EEG, EMG, pulse oximetry, drugs supply, asthma and sleep surveillance. Many persons suffer from chronic diseases such as serious joint pains, diabetes and severe blood pressure. Implantable devices contain nodes that are implanted below the skin or in the blood stream. To support human life, they can be used for analyzing and sending warnings. In the human body, devices such as neuron stimulators, pacemakers, drug pumps, baclofen pumps and implanted cardiac defibrillators have been employed [8]. For efficient transmission of physiological signals, the system requires low latency and high reliability. Transmission should also be over suitable frequency bands that are immune to interference. Transmitter circuits should be with few components that have extremely low power consumption when designed with integrated circuit technologies. Moreover, security of wireless networking should be achieved such that a WBAN data cannot be collected by intruders [3].

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 11-2023
DOI: 10.5281/zenodo.10121619

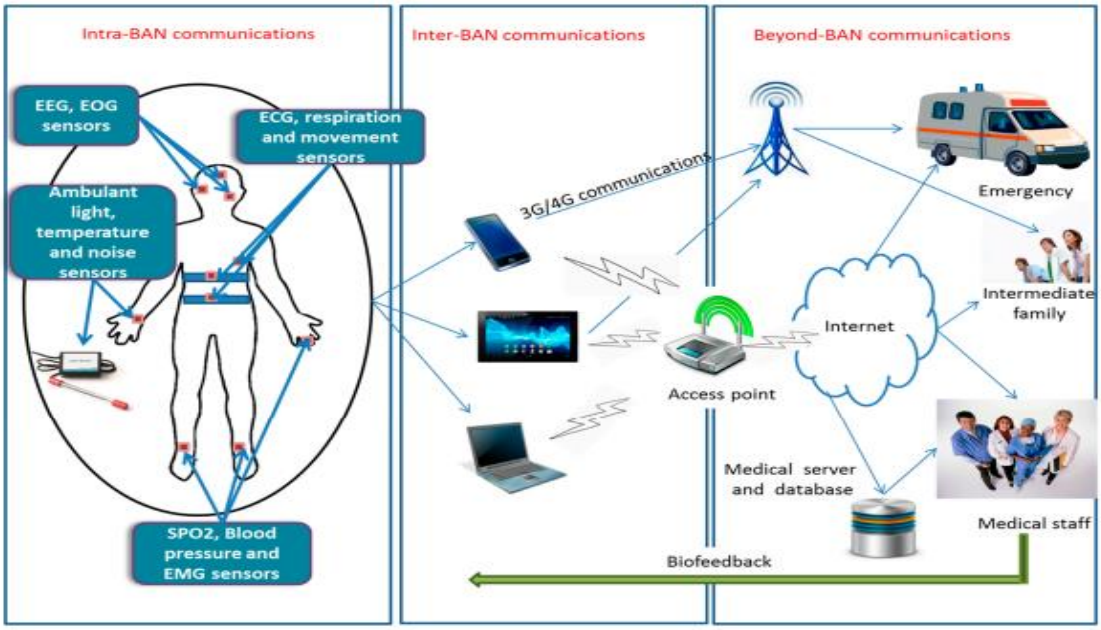


Figure 1: An IT-based telemedicine system

Four security requirements should be taken into consideration when communicating patient's information between sensors [8]:

1. **Data Confidentiality** Information privacy should be fulfilled by ensuring that only authorized persons can access the data. Data encryption using a private code helps in achieving this purpose.
2. **Data Authenticity** A criterion for ensuring that the data is transmitted by the claimed user should be provided. This can be done by calculating a message authentication code using a shared secret key.
3. **Data Integrity** This means ensuring that the received data is not tampered. This can be done by verifying the message authentication code.
4. **Data Freshness** It should be confirmed that the received information is recent and not an old previous message. A common method is to use a counter and increase it with every near sent message. The security techniques used in WSNs are not usually the optimum solutions for WBANs, since the latter have different characteristics that should be addressed when designing the system. The number of sensor nodes on the body, and the distance between them is limited. Optimized security solutions should be designed taking into consideration the available resources in this specific area. The privacy techniques use a part of these resources and thus should be lightweight and has small effect on energy consumption. One of the most attractive solutions for key management is employing biometrics. They can be used to ensure the security of the transmitted data between the personal device and all other nodes. One of the promising future research directions is developing efficient security algorithms for WBANs.

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 11-2023
DOI: 10.5281/zenodo.10121619

3. THE STATE-OF-THE-ART CHAOTIC MAP-BASED ENCRYPTION APPROACHES

Chaotic mapping is one of the most important encryption methods. Chaos-based encryption plays a larger and more important role than traditional algorithms in today's multimedia encryption. They are in many ways similar to using cryptography. Chaos-based cryptography has established itself as a fundamental part of cryptosystems in the field of cryptography. Ergodicity, structural complexity, and shuffling properties are just a few of the many properties of a chaotic map. For applications requiring secure communication, the maps fall into two categories: discrete maps and continuous maps. Chaotic maps are widely used because they offer enhanced security and high computational speed [10, 11].

Using the Bülban chaotic map, the authors in [11] developed method for fast encryption. In order to speed up the pixel-wise shuffling and substitution processes. They move and change pixels row by row, and then they do the same thing column by column. Modular operations and bitwise XOR operations are also used to mask the pixel value. This method is suitable for real-time applications because it has a fast computational speed and is extremely secure against differential attacks. The main problem, though, is applying this method with high-resolution images in real time.

An image encryption technique which relies on pixel permutation and chaotic mapping has been developed in [12] with the goal of increasing security. A normalized image is produced by employing pixel permutation. After that, a key is obtained from the normalized image, and a key is used to create and initialize a different matrix having the same size as the original. Finally, the image's encrypted version is identified by combining the normalized and newly created images.

The technique introduced by Ying and Zhang [13] takes into account pixel permutation and diffusion. In particular, the binary sequence is obtained from the original image using SHA-3. The input is then encrypted based on chaotic and diffusion processes. The simulation results indicate that the algorithm is robust against different types of attacks.

A secure and sensitive image encryption method that depends on beta chaotic maps is proposed in [14]. For the purpose of key construction and generation of random sequences, two maps with distinct initial values are randomly chosen. The technique shuffles plain image rows and columns using these random sequences to disrupt the relationship between the original and ciphered images. These outcomes amazingly increment the safety to assaults. Various block sizes are employed in each round during the diffusion stage, depending on the type of image; If any changes to these image blocks result in the plain image, they can be changed.

Li Xu et al. developed a firm and infallible bit-level image encryption scheme [15]. A piecewise linear chaotic map is used with only one round of encryption. The image is transformed in binary sequences of the same size that defuse one another. Following this, a chaotic map-controlled permutation operation is used to change binary elements from one bit plane to another. This approach is slower than other algorithms because it requires many steps such as swapping and constructing the chaotic sequences.

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 11-2023
DOI: 10.5281/zenodo.10121619

Memristive chaotic mapping and Latin square is introduced by Chai and Zhang [16] for effective image security. Applications in the medical field have greatly benefited from this method. Using the plain image with Latin square to mixing rows and columns reduces correlation between neighboring pixels. SHA-256 is used to calculate the original image's hash value, making this system resistant to well-known attacks [21].

An n effective algorithm has been developed in [17] to overcome the shortcomings of the existing image encryption algorithms. In the first step, logistic maps are utilized to scramble the original image. After that, the scrambled image is split into 22 sub blocks. The sub blocks are encrypted using hyper-chaotic maps in until the encryption of all boxes is complete. The suggested technique, which is more secure and robust, overcomes the problem of diffusion deficiency.

For effective medical image encryption, the researchers in [18] introduced a framework that employs chaotic-based encryption with dynamic S-boxes. S-boxes were set up before and after chaotic substitution in this plan, making the suggested method more resistant to attacks on chosen plaintext and cipher text. The results of additional tests showed that, the proposed framework passed all of the security tests. Hénon maps or the Classical Baker maps, which aid in achieving encryption throughput of approximately 90 mbps without requiring hardware modifications, are recommended by researchers for fast and effective processing.

Techniques including computed tomography, imaging based on magnetic resonance, and ultrasound are essential for medical diagnosis. Benefits of telemedicine include remote special clinical diagnosis, timely handling of unanticipated situations, instant access to patient information, and improved communication between stakeholders in healthcare systems. Based on these motivations, the authors in [3] suggested a visual encryption technique based on Chaos, and used them to provide protection for medical ultrasound images. An adaptive optimization technique based on adaptive Grey Wolf was presented. Various security threats such as histogram analysis. And correlation of image pixels was used to decide how resilient the suggested image encryption is. Additionally, the results of analysis were compared with Genetic algorithms and other optimization methods. Experimental findings demonstrate that the suggested technique is simpler and faster.

Because of the significance of medical information transmission and improved diagnosis, avoiding attacks over vulnerable networks via robust security algorithms is essential [19]. In [20], multiple chaotic maps were combined were combined with texture maps driven from Gabor filter for improved data security and interpretation. Pixel diffusion and large key length were guaranteed by the suggested method. Key sensitivity analysis, statistical analysis, and performance analysis were used to demonstrate the robustness of the proposed approach. Results proved that the method is efficient in addressing security issues of medical data when transmitted over communication networks.

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 11-2023
DOI: 10.5281/zenodo.10121619

4. BÜLBAN CHAOTIC MAP

The one dimensional Bülban map is a simple discrete map and is defined by the following equation:

$$x_{n+1} = x_n \sqrt{\frac{a}{x_n - b}} \tag{1}$$

where a and b are two real positive parameters of the Bülban. This map has two fixed points $x_1^* = 0$ and.$x_2^* = a + b$ In order to exclude complex values of x_n, the square root must be above zero for all iterations, which involves $x_0 > b > 0$ and $a > 0$. The Bifurcation and Lyapunov exponent analysis of the Bülban map when the parameter b = 2 is presented in the Figure 2.

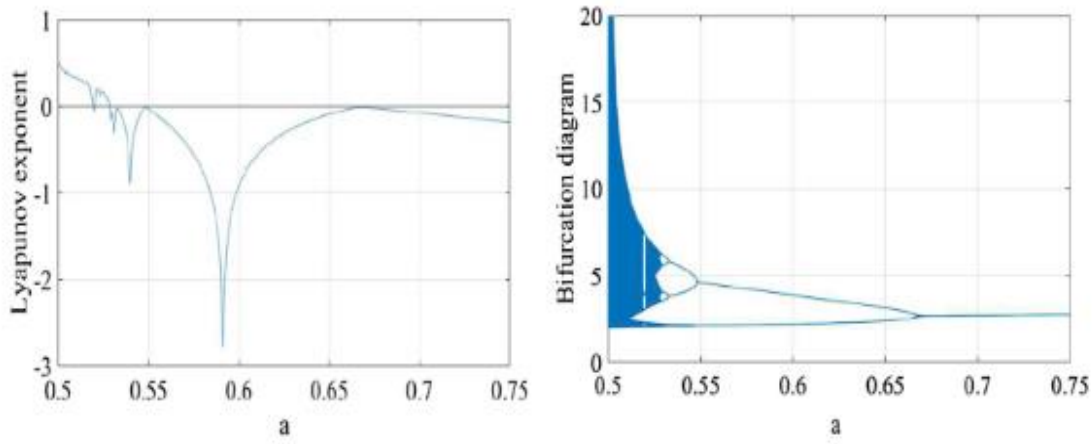


Figure 2: Bifurcation diagram and Lyapunov exponent of the Bülban map when b=2

5. PROPOSED ALGORITHM

The encryption algorithm consists from the following steps

1. Read the gray image
2. [M, N]=size(image)
3. Initialize the parameters of the map
4. L=M*N
5. For i=1 to L
6. Generate the chaotic sequence
7. Encrypt the pixel values of the image matrix based on the chaotic sequence generated
8. Repeat Step 7 until the ciphered image is reached

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 11-2023
DOI: 10.5281/zenodo.10121619

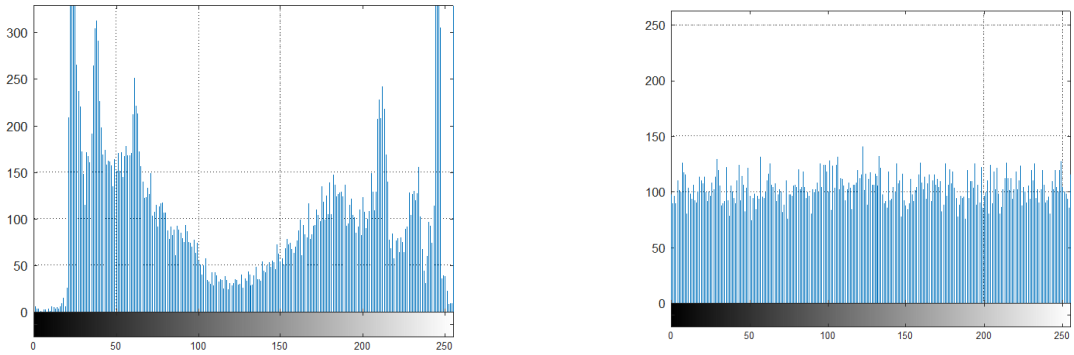
6. STATISTICAL ATTACK ANALYSIS

The statistical analysis of the original image and ciphered one can be tested by several methods as follows:

I. Histogram

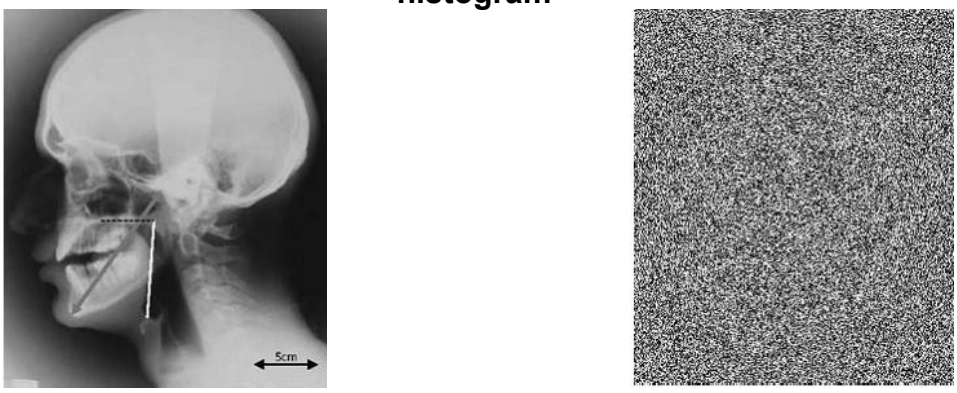
To protect the original data against the statistical attack, the histogram of the ciphered image must have uniform distribution as shown in the following figures

(a)



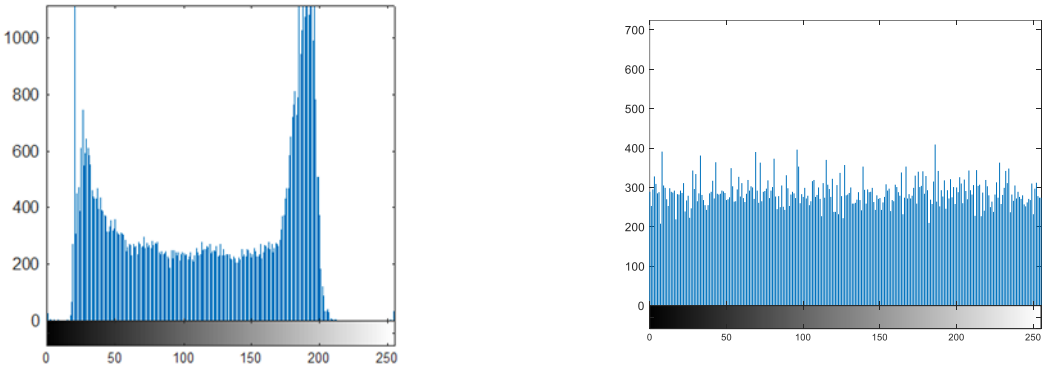
(b)

Figure 3: a) Test plain image1 and its histogram, b) Ciphered image and its histogram



(a)

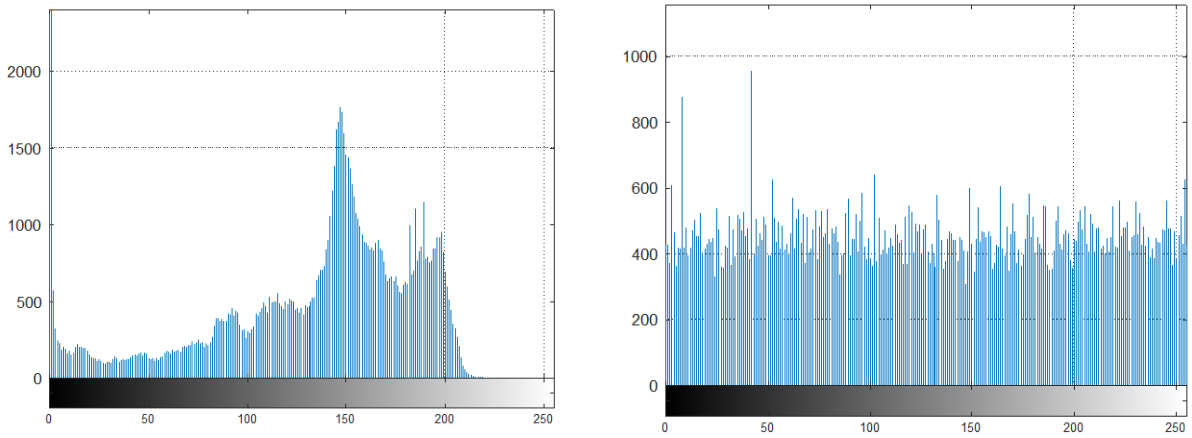
Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 11-2023
DOI: 10.5281/zenodo.10121619



(b)

Figure 4: a) Test plain image2 and its histogram, b) Ciphered image and its histogram

(a)



(b)

Figure 5: a) Test plain image3 and its histogram, b) Ciphered image and its histogram

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 11-2023
DOI: 10.5281/zenodo.10121619

II. Information entropy analysis

The entropy can be defined as follows

$$\eta = -\sum_{i} P(x_i)\, log_2 P(x_i) \tag{2}$$

The intensity of the pixel is x_i and the its probability is $P(x_i)$. The ideal value of the entropy is 8. So the entropy value is considered as a reflection for the encryption quality.

The entropy of the plain image and ciphered image is presented in the following table

Table 1: Entropy Analysis

	Plain	Cipher
Image 1	7.22779015808478	7.99020184173503
Image 2	7.60302869658637	7.98903599026046
Image 3	7.03948364839924	7.98310072200977

III. Adjacent pixels Correlations

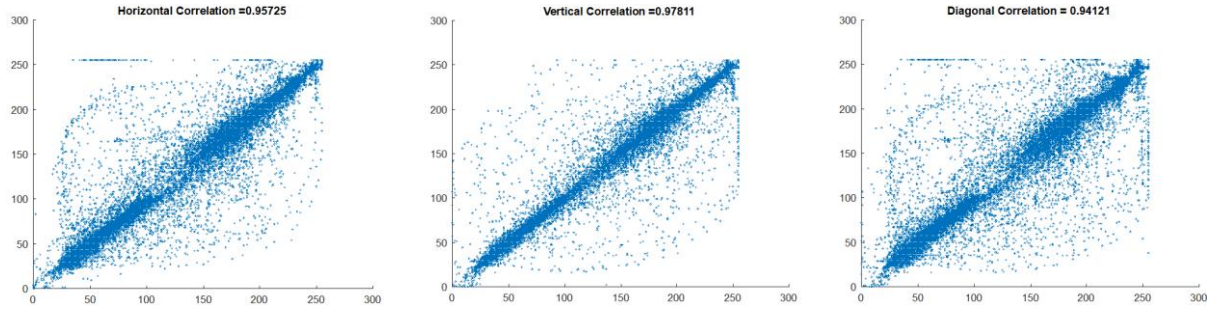
The correlation coefficient can be computed as follows

$$corr_{xy} = \frac{cov(x,y)}{\sqrt{D(x)D(Y)}} \tag{3}$$

$$cov(x,y) = \frac{1}{n}\sum_{i=1}^{n}\big(x_i - E(x)\big)\big(y_i - E(y)\big)$$

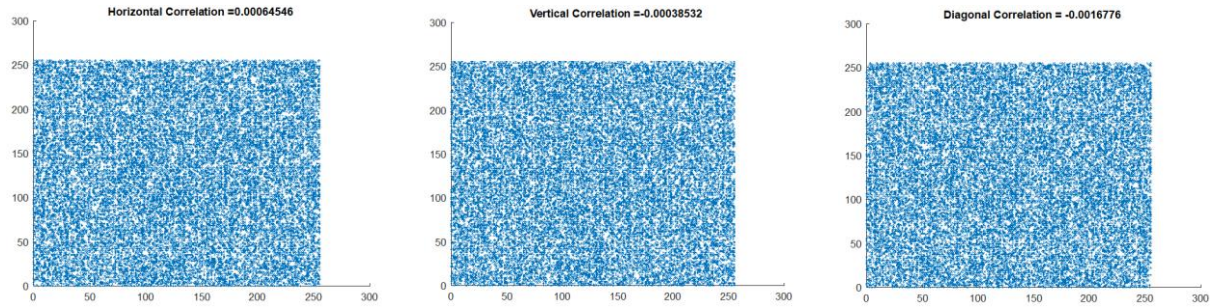
$$D(x) = \frac{1}{n}\sum_{i=1}^{n}\big(x_i - E(x)\big)^2$$

The following figures show the ability of the proposed encryption scheme to break the correlation of the plain image on an all directions



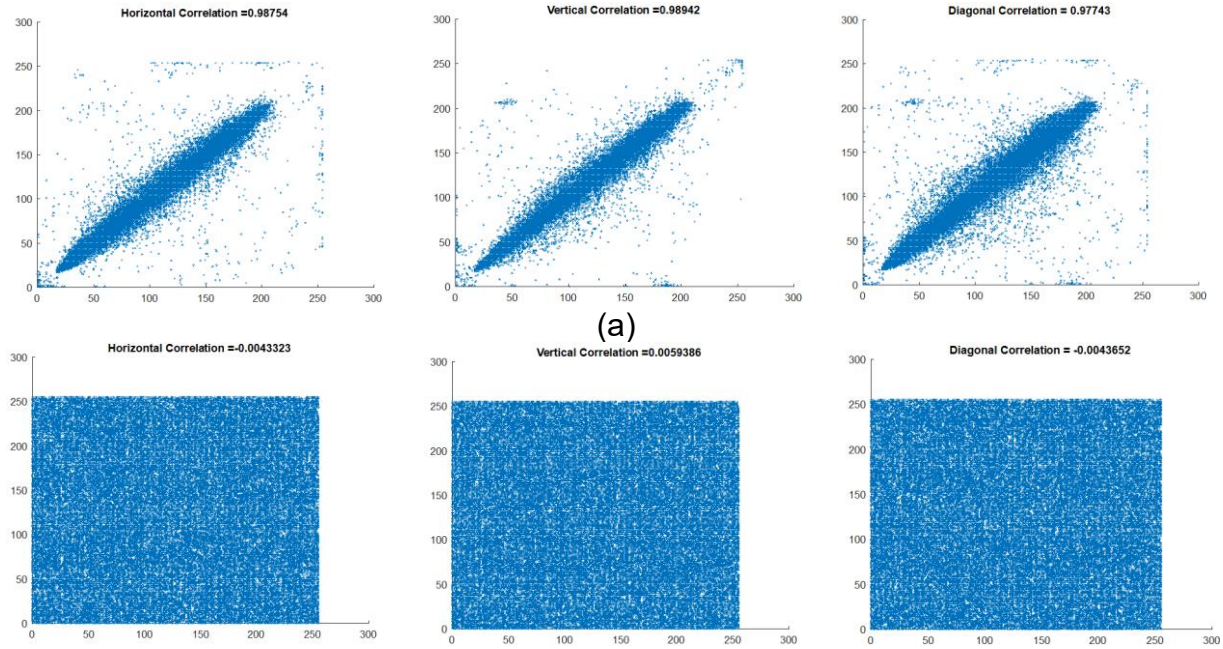
(a)

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 11-2023
DOI: 10.5281/zenodo.10121619



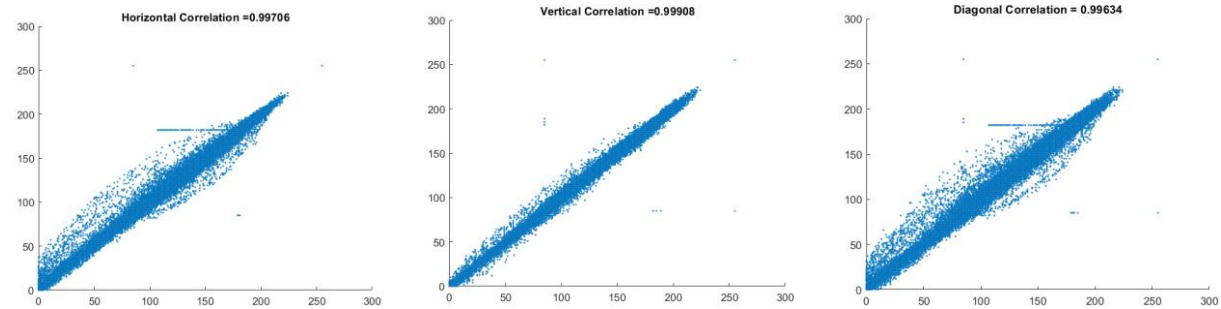
(b)

Figure 6: Correlation coefficients for a) plain image1 and b) Ciphered image.



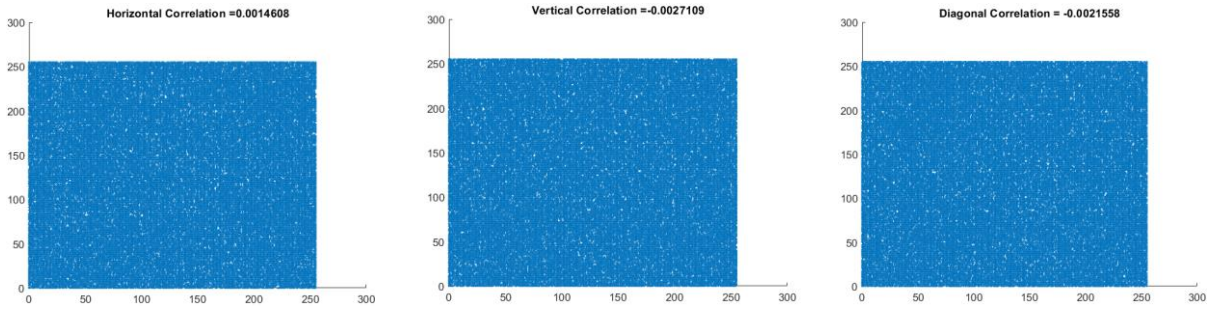
(a)

Figure 6: Correlation coefficients for a) plain image2 and b) Ciphered image.



(a)

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 11-2023
DOI: 10.5281/zenodo.10121619



(b)

Figure 7: Correlation coefficients for a) plain image3 and b) Ciphered image.

The correlation values are shown in Table 2 as shown below

Table 2: Correlation values

Image	Plain Image Correlation			Ciphered Image Correlation		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Image 1	0.9572469	0.9781144	0.9412053	0.00064546	-0.0003853	-0.0016776
Image 2	0.9875409	0.9894167	0.97743378	-0.0043323	0.00593855	-0.0043651
Image 3	0.9970602	0.9990799	0.99633571	0.00146077	-0.0027109	-0.0021558

IV. Signal to Noise Ratio

The quality of the proposed technique can define also based on the computed peak signal to noise ratio (PSNR) and signal to noise ratio (SNR) as follows:

$$PSNR = 10log\frac{m^2}{MSE} = 10log\frac{m^2}{\sum_{i=0}^{N}\sum_{j=0}^{M}[P(i,j)-C(i,j)]^2} \quad (4)$$

$$SNR = 10log\left(\frac{\sum_{i=0}^{N}\sum_{j=0}^{M}[P(i,j)]^2}{\sum_{i=0}^{N}\sum_{j=0}^{M}[P(i,j)-C(i,j)]^2}\right) \quad (5)$$

Where P is the plain image, C is the ciphered image and m is the plain image maximum value.

7. DIFFERENTIAL ATTACK ANALYSIS

The effect of changing one bit in the plain image and its effect on the ciphered image can be defined by two factors. The first one is the NPCR (number of pixels change rate) and the second is UACI (unified average changing intensity. These are computed as follows:

$$NPCR = \frac{\sum_{i=1}^{M}\sum_{j=}^{N}D(i,j)}{M\ X\ N}\ X\ 100\% \quad (4)$$

$$D(i,j) = C_1(i,j) \oplus C_2(i,j)$$

$$UACI = \frac{1}{M\ X\ N}\left(\sum_{i=1}^{M}\sum_{j=}^{N}\frac{|E_1(i,j)-E_2(i,j)|}{255}\right)X100\% \quad (5)$$

Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition)
ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 11-2023
DOI: 10.5281/zenodo.10121619

The values of the NPCR and UACI for the tested images are presented in the following table

Table 3: Differential Attack Analysis

Image	UACI	NPCR
Image 1	32.9945501792802	98.5336486192651
Image 2	32.9627556746402	97.763709919089
Image 3	30.7567018356325	97.5198179780855

8. CONCLUSION

Medical data/images are stored and distributed over the Internet for specific treatment purposes. Telemedicine has the following advantages: Supporting clinical research, removing exceptional clinical decisions, timely treatment of unanticipated episodes, patient data on immediate concern, and improved co-conspirator correspondence in health care benefits. However, medical and private information of patients are exposed to different types of attacks, and thus need to be encrypted. In this work, chaotic-mapping based encryption techniques for healthcare systems are surveyed. In addition to that, a chaotic encryption technique is used to encrypt some of the medical images. The analysis and the quality of the technique is tested against the differential and the statistical analysis. The technique proposed is fast and efficient for applying to encrypt the medical images.

References

1. H. Nasry, Chunlan Ye, Jianwei Gong, and Huiyan Chen, “Time-Delay Compensation in Environment Construction Using Laser Range Finder”, vol.5, pp. 707-711, Aug. 2013. DOI: 10.7763/IJCTE. 2013. V5.780.
2. Wang, Xingyuan; Zhao, Jianfeng (2012). "An improved key agreement protocol based on chaos". Commun. Nonlinear Sci. Numer. Simul. 15 (12): 4052–4057.
3. SeragEldin, S. M., El-Latif, A. A. A., Chelloug, S. A., Ahmad, M., Eldeeb, A. H., Diab, T. O., ... & Zaky, H. N. (2023). Design and Analysis of New Version of Cryptographic Hash Function Based on Improved Chaotic Maps with Induced DNA Sequences. IEEE Access
4. J. Scharinger, “Fast encryption of image data using chaotic Kolmogorov flows,” Journal of Electronic Imaging, vol. 7, no. 2, pp. 318–325, 1998.
5. D. Riadh and R. Shaker, "Implementation of gray image encryption using multi-level of permutation and substitution", Int. J. Appl. Inf. Syst., vol. 10, no. 1, pp. 25-30, Nov. 2015.
6. A. K. A. Hassan, "Proposed hyperchaotic system for image encryption", Int. J. Adv. Comput. Sci. Appl., vol. 7, no. 1, pp. 15-27, 2016.
7. S. Ibrahim and A. Alharbi, "Efficient image encryption scheme using Henon map dynamic S-boxes and elliptic curve cryptography", IEEE Access, vol. 8, pp. 194289-194302, 2020.
8. Nasry, Hany & Abdallah, Azhaar & Farhan, Alaa & Ahmed, Hossam & Alsobky, Wageda. (2022). MultiChaotic System to Generate Novel S-Box for Image Encryption. Journal of Physics: Conference Series. 2304. 012007. 10.1088/1742-6596/2304/1/012007.

ISSN: 1671-5497
E-Publication: Online Open Access
Vol: 42 Issue: 11-2023
DOI: 10.5281/zenodo.10121619

9. Kadir A, Aili M, Sattar M (2017) Color image encryption scheme using coupled hyper chaotic system with multiple impulse injections. Opt Int J Light Electron Opt 129:231–238.

10. Irani BY, Ayubi P, Jabalkandi FA, Valandar MY, Barani MJ (2019) Digital image scrambling based on a new one-dimensional coupled Sine map. Nonlinear Dyn 97(4):2693–2721.

11. El- Meligy, N. E., Diab, T. O., Mohra, A. S., Hassan, A. Y., & El-Sobky, W. I. (2022). A Novel Dynamic Mathematical Model Applied in Hash Function Based on DNA Algorithm and Chaotic Maps. Mathematics, 10(8), 1333

12. Liu H, Wen F, Kadir A (2019) Construction of a new 2D Chebyshev-Sine map and its application to color image encryption. Multimed Tools Appl 78(12):15997–16010.

13. Niyat AY, Moattar MH, Torshiz MN (2017) Color image encryption based on hybrid hyper-chaotic system and cellular automata. Opt Lasers Eng 90:225–237.

14. Pak C, Huang L (2017) A new color image encryption using combination of the 1D chaotic map. Signal Process 138:129–137.

15. Maolood, A. T., Farhan, A. K., El-Sobky, W. I., Zaky, H. N., Zayed, H. L., Ahmed, H. E., & Diab, T. O. (2023). Fast Novel Efficient S-Boxes with Expanded DNA Codes. Security and Communication Networks, 2023.

16. Z. A. Abduljabbar et al., "Provably secure and Fast Color Image Encryption Algorithm Based on S-Boxes and Hyperchaotic Map," in IEEE Access, vol. 10, pp. 26257-26270, 2022, doi: 10.1109/ACCESS.2022.3151174.

17. H. A. M. A. Basha, A. S. S. Mohra, T. O. M. Diab and W. I. E. Sobky, "Efficient Image Encryption Based on New Substitution Box Using DNA Coding and Bent Function," in IEEE Access, vol. 10, pp. 66409-66429, 2022, doi: 10.1109/ACCESS.2022.3183990.

18. R. Hamza and F. Titouna, "A novel sensitive image encryption algorithm based on the Zaslavsky chaotic map", Inf. Secur. J., vol. 25, no. 4, pp. 162-179, 2016.

19. Yassein, Hassan Rashed, Hany Nasry Zaky, Hadeel Hadi Abo-Alsoo, Ismail A Mageed, and Wageda I ElSobky. “QuiTRU: Design Secure Variant of Ntruencrypt Via a New Multi-Dimensional Algebra.” Appl. Math 17, no. 1 (2023): 49–53.

20. El-Meligy, N. E., El-Sobky, Mohra, A. S., Hassan, A. Y., & Diab, T. O., " New Hiding Technique in Digital Signature Based on Zigzag Transform and Chaotic Maps," Jilin Daxue Xuebao (Gongxueban)/Journal of Jilin University (Engineering and Technology Edition), Vol: 42 Issue: 09-2023.

21. T. O.Diab, W. I. A. Sobky, S. M. SeragEldin, A. K. Mahmoud, H. N. Zaky and M. A. Hogo, "Fast Simple Image Encryption Technique Based on Chaos Based System," 2023 International Telecommunications Conference (ITC-Egypt), Alexandria, Egypt, 2023, pp. 643-648, doi: 10.1109/ITC-Egypt58155.2023.10206390.

22. Alsobky, W., Saeed, H., & Elwakeil, A. N. (2020). Different Types of Attacks on Block Ciphers. Int. J. Recent Technol. Eng., 9(3), 28-31.

23. Hala Saeed, Hossam E.Ahmed, Tamer O.Diab, Hossam L.Zayed, Hany Nasry Zaky, and Wageda I.Elsobky, “Evaluation of the Most Suitable Hyperchaotic Map in S-Box Design Used in Image Encryption,” International Journal of Multidisciplinary Research and Publications (IJMRAP), Volume 5, Issue 4, pp. 176-182, 2022.