

Medical Image Cryptography Using Chaotic Methods: an study

Chin-Feng Lin *, *Member IEEE*, and Yan-Xuan Lin **

* Department of Electrical Engineering, National Taiwan Ocean University, Keelung 20224, Taiwan;

**School of Medicine, Chung Shan Medical University, Taichung 402307, Taiwan;

* lcf1024@mail.ntou.edu.tw; **1201106@live.csmu.edu.tw

Abstract—The expansion of medical encryption systems, and chaotic medical image cryptography (CRY) become an important research area in advanced encryption strategies. Chaotic medical image CRY technology can be used in cloud-based medical systems, health care systems, telemedicine, and telehealth. However, limited literature on chaotic medical image CRY is available at present. This study focuses on several basic frameworks for chaos-based medical image encryption. The major technical features and effectiveness of chaos-based encryption methods are investigated. The chaotic maps of chaos-based medical image CRY are illustrated, and security evaluation methods for chaos-based medical image CRY are explored. By revealing the basic principles of chaos-based medical image CRY, this study can inspire innovative design methods in this field.

Keywords—medical image, chaotic, cryptography, health care, telemedicine.

I. INTRODUCTION

Dachselt et al. [1] presented their opinion on the connection between chaos and cryptography (CRY), and many investigations have been conducted on the application of chaotic behavior to encryption. A chaotic masking encoder consists of a chaotic encryption module, whose output chaos-based signal is added to the information signal. This sum is transmitted over a security communication (SEC) or data encryption (DE) channel. A chaos shift keying encoder comprises two or more chaotic encryption modules with different parameters. The initial values and control parameters are used to iterate the chaotic maps to generate a real-number time series for the encryption. One of these whose output sum signal is transmitted over the SEC or DE channel is selected according to the discrete information signal. Chaotic entropy cryptanalysis properties have been highlighted in the design of new DE strategies [2]. Studying the chaos-based context of CRY requires basic knowledge regarding the dynamic properties of the adopted chaotic maps. Cryptanalysis methods can be applied to prove the inadequacy of chaotic encryption algorithms for SEC. Effective encryption technologies exhibit excellent diffusion (DIFF) and confusion (CONF) properties. The DIFF property indicates that a small change in the input of the chaos-based CRY translates into a very different output. The CONF property indicates that the temporal evolution of the output of the encryption technology is statistically independent of the input and key. Chaos-based CRY exhibits

ergodic behavior and CONF physical phenomena in terms of the chaotic initial conditions and control parameters. The problems and effectiveness of advanced sixth-generation mobile communication schemes, that are integrated into applications and the Internet of Medical Things (IoMT), for detecting, and mitigating the spread of COVID-19 and designing healthcare infrastructures for future pandemics have been introduced [3]. Chaotic EEG system of CRY has been implemented using Microsoft Visual Studio Development Kit and C# programming language, and it can run on computers with Microsoft Windows operating system [4]. The operations include logistic map (LM), discard, scramble (SCR), exclusive or (XOR), permutation (PER), percent root-mean-square difference (PRD), and time complexity analysis (TCA) parameters of the original and cipher electroencephalography (EEG) signals were explored for differential attack evaluation.

The remainder of this paper is organized as follows. Section II presents investigations into chaotic image encryption and medical image CRY. In Section III, the security evaluation analyses that used for chaos-based medical image CRY are outlined. Finally, Section IV, and V present discussions and conclusions of this study, respective.

II. STUDY ON CHAOTIC IMAGE ENCRYPTION

The aim of CRY design techniques is to provide SEC, as it protects information transmission from attackers, and is a significant aspect of data protection [5]. Chaos-based encryption mechanisms are suitable for the rapid encryption of large amounts of information content, such as images and videos in real time. Chaotic encryption technologies can be integrated into pseudorandom number generators (PNGs), CRY systems with symmetric keys (SKs), hash function (HF) CRY systems, and public key cryptosystems. Chaotic maps are sets of differential equations, whereas discrete chaos-based maps are recursive functions. Although chaos-based maps can have any number of dimensions, simple chaotic maps can only have one or two dimensions. Digital images are a major part of multimedia transmission in information communication technology [6]. The LM, sine map (SM), tent map (TM), piecewise linear map (PLM), two-dimension (2D) sine logistic modulation map (SLMM), Arnold cat map (ACM), Henon map (HM), and 2D TM, which are used in chaotic image encryption (IE), have been studied. The number of changing pixel rate (NPCR), and unified average changed intensity (UACI) parameters of the original and cipher images were

analyzed for differential attack evaluation, and correlation coefficient evaluations of the pixels of the original and cipher images have been performed. Fundamental problems relating to chaotic IE strategies have been demonstrated, and chaos-based IE has become a key concern [7]. Spatial-domain, and frequency-domain (TRAN) IE methodologies have been explored, and XOR, and PER operations that rely on Arnold cat map (ACM) have been used. Chaotic maps play an important role in chaos-based CRY, and the LM, HM, and PLM have been described [8]. Researchers need to evaluate vulnerabilities using the key space (KSP), key sensitivity (KSS), adjacent correlation coefficient (ACC), visual analysis (VA), histogram analysis (HA), NPCR, and UACI security measure parameters with respect to IE mechanisms.

III. STUDY ON CHAOTIC MEDICAL IMAGE CRY

Chaotic medical image CRY is a prime research focus worldwide. The medical cloud should be encrypted when the clinical information of patients is stored or transmitted between two medical institutions [9]. Medical imaging techniques include X-rays, magnetic resonance imaging (MRI), computed tomography (CT), ultrasound imaging, and brain imaging. Medical IE is challenging, and it is crucial to protect significant medical data using chaotic CRY. The LM has been used achieve chaotic medical data CRY. Statistical analysis can be applied to calculate changes in plaintext and ciphertext medical data [9]. The mean square error (MSE), global and local information entropy (GLIE), and TCA have been used to evaluate the encryption performance.

Medical images are widely used in modern clinical diagnosis and treatment. Medical images containing confidential information relating to patient's privacy are stored and transmitted using cloud-based networks [10]. SCR is performed on plain image, and a cipher image is generated. Chen et al. [10] developed an adaptive medical image CRY algorithm based on logistic sinusoidal map (LSM) chaotic mapping to increase the robustness of existing chaotic IE technology. Security evaluation methods using the HA, KSP, KSS, GLIE, NPCR, UACI, and normalized correlation coefficient (NCC) were employed, and the chaos-based medical IE schemes could effectively protect against attacks, with better security and robustness. A novel chaotic mapping encryption technology for medical images was developed [11]. The original medical images were divided into blocks and zigzag scanning was adopted. A chaos-based mapping procedure and SCR based on a cryptographic scheme were performed to encrypt the medical images. The LM and Bernoulli map (BERM) play vital roles in generating chaos-based encryption signals. The efficiency of medical image CRY technology has been evaluated in terms of statistical measures such as the HA, NCC, PSNR, NPCR, and UACI. Novel encryption/decryption technologies with perturbation (PERT), PER, and substitution (SUB) operations have been proposed to protect medical images [12]. Two novel 2D chaotic map based cipher approaches were proposed to enhance the robustness and reduce security breach risks for medical image CRY. The statistical and security analysis of

the medical image CRY were performed using the NPCR (99.814%), UACI (33.694%), PSNR (7.723 dB), and GLIE (7.998). The MSE, NCC, and TCA were also utilized.

The protection of patient privacy and clinical medical images has attracted considerable interest [13]. A large volume of medical images must be encrypted in real-time. A medical image CRY framework based on the baker map (BM), and HM was proposed. The encryption framework included the pseudorandom number generator (PNG), DIFF, CONF, S-box, masking (MAS), SUB, and XOR operations. A detailed security analysis was performed including statistical analyses of the HA, and pixel correlation (PC), differential analyses of the UACI and NPCR, KSS and KSP analyses, and TCA. A new medical image CRY scheme was presented, in which the linear feedback shift register (LFSR) was adopted as a PNG [14]. The medical images were randomized using the logistic-tent map (LTM), and SCR using the ACM. A cipher medical image can be generated using the XOR, PNG, randomized, and SCR operations. Medical image CRYs commonly apply SCR to remove the correlation between neighboring pixels of the medical images by shifting their positions. The ACM can be easily integrated, and exhibits superior ergodic properties.

IV. STUDY ON CHAOTIC MEDICAL IMAGE CRY

Table 1 displays the technical features and effectiveness of chaos-based medical image CRY. There are many technical features and effectiveness of operations commonly used in chaos-based medical image CRY, such as block ciphers (BC), CONF, DE, DIFF, Discard, HF, IE, MAS, medical image encryption (MIE), PER, perturbation (PERT), PNG, SBOX, stream cipher (SC), SCR, SEC, SUB, transform (TRAN), XOR, and so on. Table 2 shows the chaotic maps of medical image CRY. These chaotic maps are used in chaos-based medical image CRY, such as 2D cosine map (CM), 2D SLMM, 2D TM, ACM, BM, Bernoulli map (BERM), Chebyshev polynomials map (CPM), HM, LM,

TABLE 1. Technical features and effectiveness of chaos-based medical image CRY.

Technical Features and Effectiveness	References
BC	[6]
CONF	[2][13]
DE	[1][2][6]
DIFF	[2][13]
Discard	[4]
HF	[5]
IE	[5][6][7][8]
MAS	[13]
MIE	[9][10][11][12][13][14]
PER	[4][7][10][13]

PERT	[12]
PNG	[5][13][14]
SBoX	[13]
SC	[6]
SCR	[4][10][11][12][14]
SEC	[1][2][5][6]
SUB	[12][13]
TRAN	[7]
XOR	[4][6][7][11][13][14]

TABLE 2. BASIC CHAOTIC MAPS OF CHAOS-BASED MEDICAL IMAGE CRY.

Basic chaotic maps	References
2D CM	[12]
2D SLMM	[6]
2D TM	[6]
ACM	[6][7][14]
BM	[13]
BERM	[11]
CPM	[5]
HM	[6][8][13]
LM	[4][5][6][9]
LSM	[10]
PLM	[5][6][8]
SM	[6]
TM	[8][9]

TABLE 3. SECURITY EVALUATION METHODS FOR CHAOS-BASED MEDICAL IMAGE CRY.

Security evaluation methods	References
ACC	[8]
GLIE	[6][9][10][12]
HA	[6][8][10][11][13]
KSP	[8][10][13]
KSS	[8][10][13]
MSE	[9][12]
NCC	[10][11]
NPCR	[6][8][10][14]

PC	[6][13][14]
PRD	[4]
PSNR	[11][14]
SSIM	[14]
TCA	[4][9][12][13][14]
UACI	[4][10][11][12][13][14]
VA	[8]
VARH	[14]

LSM, PLM, SM, TM, and so on. Table 3 lists security evaluation methods for chaos-based medical image CRY. The basic security evaluation methods include ACC, GLIE, HA, KSP, KSS, MSE, NCC, NPCR, PC, PSNR, PRD, SSIM, TCA, UACI, VA, VARH, and so on. In this study, we have focused on chaos-based medical encryption, which is critical in clinical medical image CRY operations. All of the aforementioned technologies have been significant in the advancement of chaos-based medical image encryption. Relevant studies focusing on the following aspects are deemed significant:

- Chaos-based medical image encryption operations;
- Chaos-based maps;
- Chaos-based medical image cryptanalysis.

V. CONCLUSIONS

The main objective of this study was to present innovative approaches for the chaotic encryption of medical images. The fundamental knowledge outlined in this study plays a significant role in chaotic image CRY. We examined the basic concepts of modern CRY published in research between 2001 and 2024 concerning chaos-based image CRY. The principal categories of the chaos-based medical image CRY are shown in Figure 1. The surveyed literature relating to chaos and CRY included three papers [1][2] [5], the reviewed literature relating to chaos-based medical IE included three papers [6][7][8], the literature relating to chaos-based medical IE included one papers [9], and the literature relating to chaos-based EEG signal encryption included one papers [4]. The original literature relating to multiple chaotic maps included two papers [10][11] original literature relating to robust chaos-based technique included one papers [14] and the original literature relating to fast and simple chaotic system included one papers [13] for the chaos-based EEG signal encryption.

Chaotic image CRY was comprehensively demonstrated, to provide a better understanding, and several representative articles were investigated. In addition, the security concerns of chaotic image CRY were presented. Chaotic image CRY can effectively encrypt image information, and protect against attackers. Chaotic medical image CRY has been applied to telehealth, telemedicine, IoMT, and cloud-based medicine systems.

This is a conceptual article, and the article has guided beginners to understand the principles of the chaotic medical image encryption. The introductory article has been guided beginners in the field of chaotic medical image encryption. Beginners should also study the papers of the chaos and cryptography [1][5], that of chaos-based encryption image encryption [6][7][8] in detail.

ACKNOWLEDGMENT

The authors acknowledge the valuable comments of the reviewers

REFERENCES

- [1] F. Dachsel, and W. Schwarz, "Chaos and cryptography," *IEEE Transactions on Circuits and Systems—I: Fundamental Theory and Applications*, vol. 48, pp. 1498-1509, 2001.
- [2] D. Arroyo, G. Alvarez, and V. Fernandez, "A basic framework for the cryptanalysis of digital chaos-based cryptography," in *Proceedings of the IEEE 6th international multi-conference on systems, signals and devices*, Djerba, Tunisia, 2009.
- [3] C. F. Lin, and S. H. Chang, "Advanced mobile communication techniques in the fight against the COVID-19 pandemic era and beyond: an overview of 5G/B5G/6G," *Sensors*, vol. 23, pp. 1-16, 2023.
- [4] C. F. Lin, S. H. Shih, and J. D. Zhu, "Chaos based encryption system for encrypting electroencephalogram signals," *Journal of Medical Systems*, vol. 38, pp. 1-10, 2014.
- [5] P. Zhen, G. Zhao, L. Min, and X. Li, "A survey of chaos-based cryptography," in *Proceedings of the IEEE 9th international conference on P2P, parallel, grid, cloud and internet computing*, Guangdong, China, 2014.
- [6] K. Suneja, S. Dua, and M. Dua, "A review of chaos based image encryption," in *Proceedings of the IEEE 3rd international conference on computing methodologies and communication*, Erode, India, 2019.
- [7] G. Ghosh, D. Anand, K. S. Verma, N. Z. Jhanjhi, and M. N. Talib, "A review on chaotic scheme-based image encryption techniques," in *Intelligent Computing and Innovation on Data Science*, S. L. Peng et al., Ed., Springer Nature, Singapore, pp. 473-481, 2021.
- [8] M. Sharma, R. K. Ranjan, and V. Bharti, "Image encryption using chaotic maps: a survey," in *Soft Computing: Theories and Applications*, R. Kumar et al. Ed., Springer Nature, Singapore, pp. 835-844, 2022.
- [9] S. Sumathi, S. Gopika, S. Nivedha, and R. Kalaimathi, "Chaotic map based encryption algorithm for secured medical data analytics," in *Data Intelligence and Cognitive Informatics, Algorithms for Intelligent Systems*, J. Jacob et al. Ed., Springer Nature, Singapore, pp. 59-68, 2024.
- [10] X. Chen, and C. J. Hu, "Adaptive medical image encryption algorithm based on multiple chaotic mapping," *Saudi Journal of Biological Sciences*, vol. 24, pp. 1821-1827, 2017.
- [11] G. A. Sathishkumar, K. Bhoopathyagan, N. Sriraam, S. P. Venkatachalam, and R. Vignesh, "A novel image encryption algorithm using two chaotic maps for medical application," in *Proceedings of the CCSIT*, Meghanathan, N. et al. Ed., Springer-Verlag, Berlin, pp. 290-299, 2011.
- [12] I. Yasser, A. T. Khalil, M. A. Mohamed, A. S. Samra, and F. A. Khalifa, "A robust chaos-based technique for medical image encryption," *IEEE Access*, vol. 10, pp. 244-257, 2022.
- [13] S. Ibrahim, H. Alhumyani, M. Masud, S. S. Alshamrani, O. Cheikhrouhou, G. Muhammad, M. S. Hossain, and A. M. Abbas, "Framework for efficient medical image encryption using dynamic s-boxes and chaotic maps," *IEEE Access*, vol. 8, pp. 160433-160449, 2020.
- [14] S. Deb, and B. Bhuyan, "Chaos-based medical image encryption scheme using special nonlinear filtering function based LFSR," *Multimedia Tools and Applications*, vol. 80, pp. 19803-19826, 2021.

Dr. Chin-Feng Lin was born in Taiwan, in 1974. He received the Ph.D. degrees in Communication Engineering from National Chiao Tung University, Taiwan, in 2002. Afterwards, he served as an assistant professor and has been an associate professor since 2004 in the Department of Electrical Engineering at National Taiwan Ocean University, Taiwan. He has been published 30 SCI journal papers, one English online book, 6 English book chapters, 2 Chinese books, 9 Taiwan patents, and 92 conference papers. His research interests include mobile telemedicine, biomedical signal processing, and underwater multimedia communication.

Yan-Xuan Lin was born in Taiwan, in 2005. She is an undergrad since 2023 in the School of Medicine at Chung Shan University, Taiwan. Her research interests include biomedical signal processing, and mobile telemedicine.