A Minor Project Synopsis
on
Chaos Based Image Encryption for Medical Reports

Submitted to Manipal University Jaipur
towards the partial fulfillment for the award of the degree
of

Bachelor of Technology
In Information Technology

By
Ayush Jaipuriyar
209302167
Pratham Dhiman
209302249
Section E

Under the Guidance of
Dr. Anju Yadav

MANIPAL UNIVERSITY JAIPUR
INSPIRED BY LIFE

Department of Information Technology
School of Information Technology
Manipal University Jaipur
2022-2023

Contents

1 Introduction

Encryption of images is important in today's digital world as it helps to protect sensitive and confidential information contained in images from unauthorized access. With the increasing use of digital images for personal, business and government purposes, there is a growing need to ensure that this data is protected from hackers, cyber-criminals and other malicious actors who might use the information for their own purposes. Encryption provides a secure and effective means of protecting images by transforming them into an unreadable form, making it difficult for unauthorized individuals to access or view the original image. This helps to ensure the privacy and confidentiality of the information contained in the image and reduces the risk of data breaches and theft.

1.1 Encryption

Encryption is the process of converting plaintext into an unreadable form (ciphertext) to protect its confidentiality and prevent unauthorized access to its content. It uses mathematical algorithms (cipher) and a key to transform the data. Only those with the corresponding decryption key can reverse the process and access the original plaintext. Encryption helps to ensure the privacy and security of data transmitted over networks or stored on devices.

1.2 Chaos Theory

Chaos theory is a branch of mathematics that studies the behavior of dynamic systems that are highly sensitive to initial conditions, leading to seemingly random patterns and unpredictable behavior. It deals with how small differences in initial conditions can lead to vastly different outcomes over time, which is often referred to as the butterfly effect. Chaos theory has applications in various fields, such as physics, economics, and weather forecasting.

Chaos theory provides several important features to image encryption, including:

1. **Sensitivity to Initial Conditions**: The sensitivity to initial conditions in chaotic systems provides a high degree of security as small differences in the initial conditions can lead to vastly different results, making it difficult for an attacker to determine the encryption process.

2. **Unpredictability:** The unpredictable behavior of chaotic systems adds an extra layer of security as the encrypted image appears to be random noise, making it difficult for an attacker to determine the original image.

3. **High-dimensional Dynamics:** The high-dimensional dynamics of chaotic systems allow for the creation of complex encryption algorithms that can provide a high degree of security.

4. **Ease of Implementation:** The mathematical simplicity of some chaotic systems makes them easy to implement in software, providing a convenient means of encrypting images.

Overall, chaos theory provides a means of creating secure, efficient, and easy-to-implement image encryption algorithms that can help protect sensitive information transmitted over communication networks.

2 Motivation

Our motivation for developing a new chaos-based image encryption technique is a result of our passion for cryptography and our fascination with chaos theory. I believe that this research will not only advance the field of cryptography but also help to improve the security of sensitive information. The challenge of developing a new image encryption technique appeals to me and I am eager to explore the unique properties of chaos-based encryption and apply them to image encryption. This work presents a significant challenge and an opportunity for me to push the boundaries of what is currently possible. Successfully developing a new chaos-based image encryption technique would be a major accomplishment for me, both professionally and personally, and would be a source of pride and satisfaction in our career as a researcher.

3 Project Objectives

The objectives of the project are out lined as follows :-

1. To develop an efficient and secure image encryption system for medical images that meets the requirements of the hospital.

2. To ensure the privacy and security of medical images and information stored and transmitted within the hospital network.

3. To comply with relevant regulations and standards regarding the storage and transmission of medical information and images.

4. To provide authorized personnel with fast and secure access to encrypted medical images.

5. To improve the backup and recovery of medical images, ensuring that important information is not lost in case of data loss or corruption.

6. To reduce the risk of data breaches and unauthorized access to sensitive medical information.

7. To increase the efficiency and accuracy of medical diagnoses and treatment decisions by enabling fast and secure access to medical images.

8. To provide a user-friendly interface for encrypting and decrypting medical images, with a focus on simplicity and ease of use.

9. To ensure that the encryption system can scale to accommodate the growing needs of the hospital over time.

4   Methodology

1. Select a chaotic system: Choose a well-studied and well-understood chaotic system that can be used as the basis for the encryption algorithm. For example, the logistic map or the Lorenz system can be used.

2. Generate a chaotic sequence: Using the selected chaotic system, generate a chaotic sequence that will be used as the key for the encryption process. The length of the sequence should be equal to or greater than the number of pixels in the image.

3. Initialize encryption parameters: Select the encryption parameters such as the number of iterations, the number of encryption rounds, and the size of the encryption block. These parameters will determine the strength of the encryption.

4. Divide the image into blocks: Divide the original image into smaller blocks of a fixed size. The size of the blocks should be selected to optimize the encryption process.

5. Perform encryption: For each block of the image, perform the encryption process. The encryption process involves combining the block with the chaotic sequence using an appropriate encryption algorithm, such as XOR or addition. The encrypted block is then stored in a new image.

6. Repeat encryption: Repeat the encryption process for each block of the image for the specified number of encryption rounds.

7. Store the encrypted image: Store the encrypted image on a secure storage device, such as a hard drive or a secure cloud storage service. The original image and the encryption key should also be stored securely.

8. Decryption process: To decrypt the image, the same encryption process is performed in reverse using the encryption key.
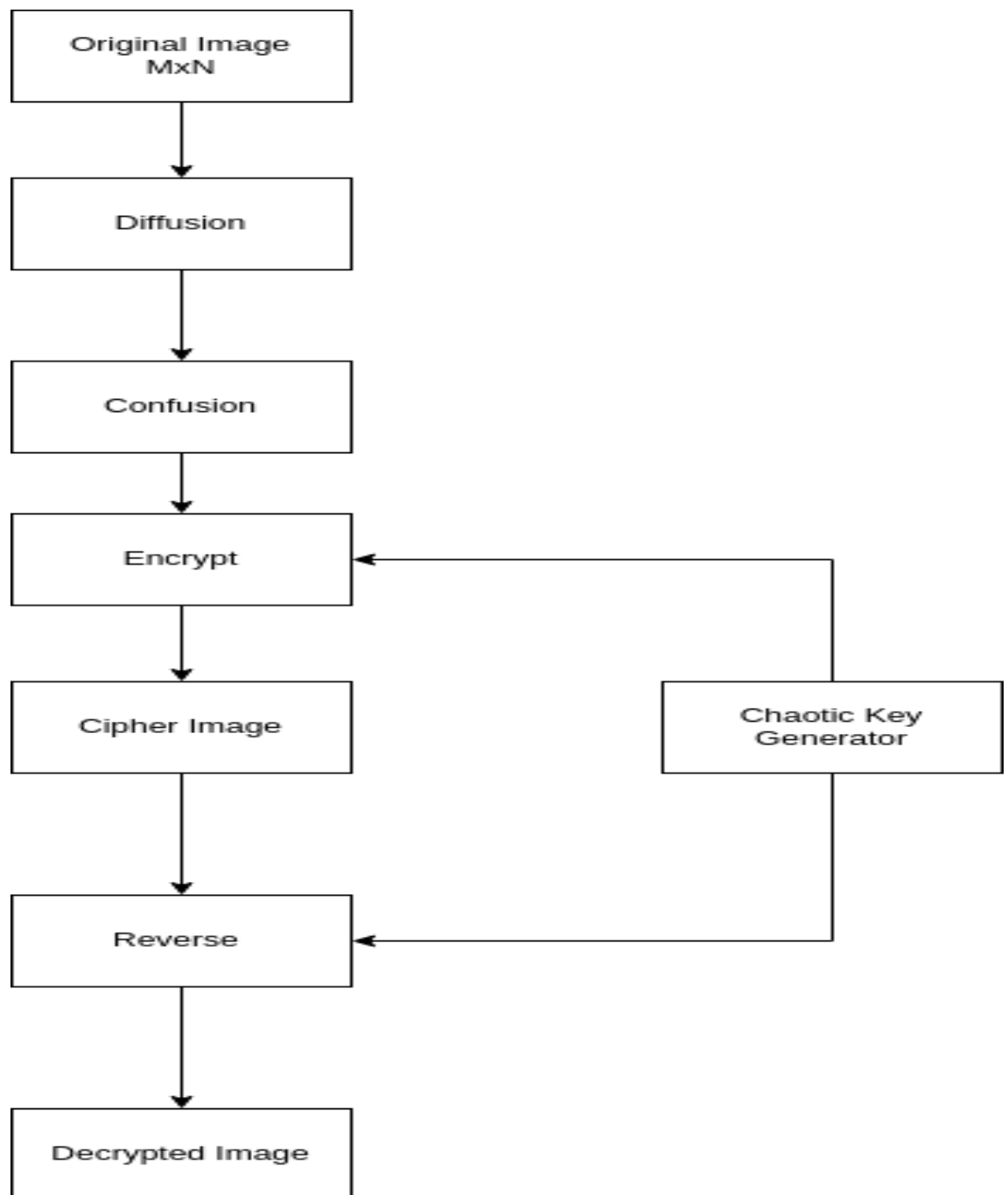
5 Facilties reqired for proposed work

5.1 Hardware Requirements

For an image encryption project that needs to be deployed in a hospital environment, the hardware requirements may need to be higher to ensure stability and performance. Here are some suggested hardware requirements:

1. **Processor:** A high-performance processor with multiple cores and a high clock speed is recommended for fast processing and encryption of medical images.

2. **RAM:** At least 16GB of RAM, but 32GB or more is recommended to ensure smooth processing of large medical images.But for now 4GB is also enough

3. **Storage:** A solid-state drive (SSD) with a large capacity for storing encrypted medical images and other data.

4. **Graphics Card:** A dedicated graphics card with a high amount of VRAM for rendering medical images in real-time.

5. **Network Connectivity:** Fast and reliable network connectivity is essential for transferring medical images and other data within the hospital network.

5.2 Software Requirements

A few of the basic software requirements are as follows:-

1. **Operating System:** Any modern operating system such as Windows, Linux, or macOS should suffice.

2. **Programming Language:** Python

3. **Image Processing Library:** An image processing library such as OpenCV, Pillow, or scikit-image for processing and manipulating images.

4. **Development Environment:** An integrated development environment (IDE) such as Visual Studio Code for writing and testing code.

5. **Version Control System:** A version control system such as Git for tracking changes and collaborating with others.

6 Bibliography

References

[1] Alaa M Abbas, Ayman A Alharbi, and Saleh Ibrahim. A novel parallelizable chaotic image encryption scheme based on elliptic curves. *IEEE Access*, 9:54978–54991, 2021.

[2] Salwa K Abd-El-Hafiz, Sherif H AbdElHaleem, and Ahmed G Radwan. Permutation techniques based on discrete chaos and their utilization in image encryption. In *2016 13th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)*, pages 1–6. IEEE, 2016.

[3] Meghdad Ashtiyani, Parmida Moradi Birgani, and Hesam M Hosseini. Chaos-based medical image encryption using symmetric cryptography. In *2008 3rd International Conference on Information and Communication Technologies: From Theory to Applications*, pages 1–5. IEEE, 2008.

[4] Binu Balakrishnan and D Muhammad Noorul Mubarak. An improved image encryption using 2d logistic adjusted sine chaotic map with shuffled index matrix. In *2021 International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT)*, pages 1–6. IEEE, 2021.

[5] Abhilash Ashok Bhadke, Surender Kannaiyan, and Vipin Kamble. Symmetric chaos-based image encryption technique on image bit-planes using sha-256. In *2018 Twenty Fourth National Conference on Communications (NCC)*, pages 1–6. IEEE, 2018.

[6] Ankita Bisht, Priyanka Jaroli, Mohit Dua, and Shelza Dua. Symmetric multiple image encryption using multiple new one-dimensional chaotic functions and two-dimensional cat man. In *2018 International Conference on Inventive Research in Computing Applications (ICIRCA)*, pages 676–682. IEEE, 2018.

[7] Sudeshna Bora, Pritam Sen, and Chittaranjan Pradhan. Novel color image encryption technique using blowfish and cross chaos map. In *2015 international conference on communications and signal processing (ICCSP)*, pages 0879–0883. IEEE, 2015.

[8] Santosh Chapaneri and Radhika Chapaneri. Chaos based image encryption using latin rectangle scrambling. In *2014 annual IEEE India conference (INDICON)*, pages 1–6. IEEE, 2014.

[9] Xuzhou Jiangsu China. An image encryption algorithm based on the combination of low-dimensional chaos and high-dimensional chaos. 2019.

[10] Un Sook Choi, Sung Jin Cho, and Sung Won Kang. Color image encryption algorithm for medical image by mixing chaotic maps. In *2020 12th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP)*, pages 1–5. IEEE, 2020.

[11] Aesha N Elghandour, Ahmed M Salah, Yasser A Elmasry, and Abdelrahman A Karawia. An image encryption algorithm based on bisection method and one-dimensional piecewise chaotic map. *IEEE Access*, 9:43411–43421, 2021.

[12] Osama S Faragallah, Ashraf Afifi, Walid El-Shafai, Hala S El-Sayed, Ensherah A Naeem, Mohammed A Alzain, Jehad F Al-Amri, Ben Soh, and Fathi E Abd El-Samie. Investigation of chaotic image encryption in spatial and frft domains for cybersecurity applications. *IEEE Access*, 8:42491–42503, 2020.

[13] Amnah Firdous, Aqeel Ur Rehman, and Malik Muhammad Saad Missen. A gray image encryption technique using the concept of water waves, chaos and hash function. *Ieee Access*, 9:11675–11693, 2021.

[14] Hao Gao and Xingyuan Wang. Chaotic image encryption algorithm based on zigzag transform with bidirectional crossover from random position. *Ieee Access*, 9:105627–105640, 2021.

[15] Víctor Manuel Silva García, Marlon David González Ramírez, Rolando Flores Carapia, Eduardo Vega-Alvarado, and Eduardo Rodríguez Escobar. A novel method for image encryption based on chaos and transcendental numbers. *IEEE Access*, 7:163729–163739, 2019.

[16] Djamal Eddine Goumidi and Fella Hachouf. Hybrid chaos-based image encryption approach using block and stream ciphers. In *2013 8th International Workshop on Systems, Signal Processing and their Applications (WoSSPA)*, pages 139–144. IEEE, 2013.

[17] Kamlesh Gupta, Ranu Gupta, Rohit Agrawal, and Saba Khan. An ethical approach of block based image encryption using chaotic map. *International Journal of Security and Its Applications*, 9(9):105–122, 2015.

[18] M Habibipour, R Maarefdoust, M Yaghobi, and S Rahati. An image encryption system by 2d memorized cellular automata and chaos mapping. In *6th International Conference on Digital Content, Multimedia Technology and its Applications*, pages 331–336. IEEE, 2010.

[19] J Mohaimen Hassan and F Alaa Kadhim. New s-box transformation based on chaotic system for image encryption. In *2020 3rd International Conference on Engineering Technology and its Applications (IICETA)*, pages 214–219. IEEE, 2020.

[20] Xiancheng Hu, Liansuo Wei, Wei Chen, Qiqi Chen, and Yuan Guo. Color image encryption algorithm based on dynamic chaos and matrix convolution. *IEEE Access*, 8:12452–12466, 2020.

[21] Yuanyuan Huang, Longwang Huang, Yinhe Wang, Yuxu Peng, and Fei Yu. Shape synchronization in driver-response of 4-d chaotic system and its application in image encryption. *IEEE Access*, 8:135308–135319, 2020.

[22] Aiping Jiang, Jia Yu, and Xiaoyu Cang. Image encryption algorithm based on chaos and contourlet transform. In *2010 First International Conference on Pervasive Computing, Signal Processing and Applications*, pages 707–710. IEEE, 2010.

[23] Hui-yan Jiang and Chong Fu. An image encryption scheme based on lorenz chaos system. In *2008 Fourth International Conference on Natural Computation*, volume 4, pages 600–604. IEEE, 2008.

[24] Jayashree Karmakar and Mrinal Kanti Mandal. Chaos-based image encryption using integer wavelet transform. In *2020 7th International Conference on Signal Processing and Integrated Networks (SPIN)*, pages 756–760. IEEE, 2020.

[25] G Kavinmozhi, R Premkumar, S Anand, and S Robinson. A hybrid chaos approach for image encryption using ctic map. In *2018 International Conference on Current Trends towards Converging Technologies (ICCTCT)*, pages 1–5. IEEE, 2018.

[26] Jan Sher Khan, Atique ur Rehman, Jawad Ahmad, and Zeeshan Habib. A new chaos-based secure image encryption scheme using multiple substitution boxes. In *2015 Conference on information assurance and cyber security (CIACS)*, pages 16–21. IEEE, 2015.

[27] Krishna Kumar, Satyabrata Roy, Umashankar Rawat, and Shashwat Malhotra. Iehc: An efficient image encryption technique using hybrid chaotic map. *Chaos, Solitons & Fractals*, 158:111994, 2022.

[28] Xiaofeng Li and Yinhui Zhang. Digital image encryption and decryption algorithm based on wavelet transform and chaos system. In *2016 IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC)*, pages 253–257. IEEE, 2016.

[29] Xue Mei Li and Lin Dai. Reality-preserving image encryption assosiated with the chaos and the lct. In *2010 3rd International Congress on Image and Signal Processing*, volume 6, pages 2624–2627. IEEE, 2010.

[30] Lei Li-Hong, Bai Feng-Ming, and Han Xue-Hui. New image encryption algorithm based on logistic map and hyper-chaos. In *2013 International Conference on Computational and Information Sciences*, pages 713–716. IEEE, 2013.

[31] Liu Lidong, Donghua Jiang, Xingyuan Wang, Linlin Zhang, and Xianwei Rong. A dynamic triple-image encryption scheme based on chaos, s-box and image compressing. *IEEE Access*, 8:210382–210399, 2020.

[32] Chih-Min Lin, Duc-Hung Pham, and Tuan-Tu Huynh. Encryption and decryption of audio signal and image secure communications using chaotic system synchronization control by tsk fuzzy brain emotional learning controllers. *IEEE Transactions on Cybernetics*, 52(12):13684–13698, 2021.

[33] Jinyuan Liu. A novel sensitive chaotic image encryption algorithm based on sha-3 and steganography. In *2020 IEEE 3rd International Conference of Safe Production and Informatization (IICSPI)*, pages 370–374. IEEE, 2020.

[34] Lidong Liu, Linlin Zhang, Donghua Jiang, Yifan Guan, and Zhaolun Zhang. A simultaneous scrambling and diffusion color image encryption algorithm based on hopfield chaotic neural network. *IEEE Access*, 7:185796–185810, 2019.

[35] Qing Lu, Congxu Zhu, and Xiaoheng Deng. An efficient image encryption scheme based on the lss chaotic map and single s-box. *IEEE Access*, 8:25664–25678, 2020.

[36] Yuling Luo, Minghui Du, and Dong Liu. Jpeg image encryption algorithm based on spatiotemporal chaos. In *2012 Fifth International Workshop on Chaos-fractals Theories and Applications*, pages 191–195. IEEE, 2012.

[37] Yuling Luo, Xue Ouyang, Junxiu Liu, and Lvchen Cao. An image encryption method based on elliptic curve elgamal encryption and chaotic systems. *IEEE Access*, 7:38507–38522, 2019.

[38] Corina Macovei, Mircea Răducanu, and Octaviana Datcu. Image encryption algorithm using wavelet packets and multiple chaotic maps. In *2020 International Symposium on Electronics and Telecommunications (ISETC)*, pages 1–4. IEEE, 2020.

[39] Zahir Muhammad Ziad Muhammad and Fatih Özkaynak. A cryptographic confusion primitive based on lotka–volterra chaotic system and its practical applications in image encryption. In *2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, pages 694–698. IEEE, 2020.

[40] Xiaoliang Qian, Qi Yang, Qingbo Li, Qian Liu, Yuanyuan Wu, and Wei Wang. A novel color image encryption algorithm based on three-dimensional chaotic maps and reconstruction techniques. *IEEE Access*, 9:61334–61345, 2021.

[41] Jubao Qu. Image encryption algorithm based on logistic chaotic scrambling system. In *2020 IEEE 3rd International Conference on Information Systems and Computer Aided Education (ICISCAE)*, pages 519–522. IEEE, 2020.

[42] Manju Rani and Sudesh Kumar. A novel and efficient approach to encrypt images using chaotic logistic map and stream cipher. In *2015 International conference on green computing and internet of things (ICG-CIoT)*, pages 1442–1447. IEEE, 2015.

[43] Mujeeb Ur Rehman, Arslan Shafique, Sohail Khalid, and Iqtadar Hussain. Dynamic substitution and confusion-diffusion-based noise-resistive image encryption using multiple chaotic maps. *IEEE Access*, 9:52277–52291, 2021.

[44] Malika Sharma and Anuja Bhargava. Chaos based image encryption using two step iterated logistic map. In *2016 International Conference on Recent Advances and Innovations in Engineering (ICRAIE)*, pages 1–5. IEEE, 2016.

[45] Nabil Ben Slimane, Kais Bouallegue, and Mohsen Machhout. A novel image encryption scheme using chaos, hyper-chaos systems and the secure hash algorithm sha-1. In *2017 International Conference on Control, Automation and Diagnosis (ICCAD)*, pages 141–145. IEEE, 2017.

[46] Jiayu Sun, Chunbiao Li, Tianai Lu, Akif Akgul, and Fuhong Min. A memristive chaotic system with hypermultistability and its application in image encryption. *IEEE Access*, 8:139289–139298, 2020.

[47] Harshvardhan Tiwari, Kumar N Satish, R Harshitha, N Shilpa, S Rakshatha, and KN Archana. Ensuring confidentiality in bsn with 1-d chaos based image encryption scheme. In *2018 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*, pages 331–334. IEEE, 2018.

[48] De Wang and Yuan-Biao Zhang. Image encryption algorithm based on s-boxes substitution and chaos random sequence. In *2009 International Conference on Computer Modeling and Simulation*, pages 110–113. IEEE, 2009.

[49] Xingyuan Wang and Pengbo Liu. A new image encryption scheme based on a novel one-dimensional chaotic system. *IEEE Access*, 8:174463–174479, 2020.

[50] Jingjin Wei, Miao Zhang, and Xiaojun Tong. Image encryption algorithm based on fractional order chaotic system. In *2021 IEEE 12th International Conference on Software Engineering and Service Science (ICSESS)*, pages 72–75. IEEE, 2021.

[51] Xiaolin Wu, Bin Zhu, Yutong Hu, and Yamei Ran. A novel color image encryption scheme using rectangular transform-enhanced chaotic tent maps. *IEEE Access*, 5:6429–6436, 2017.

[52] Zhengze Wu, Xiaohong Zhang, and Xiaoyong Zhong. Generalized chaos synchronization circuit simulation and asymmetric image encryption. *IEEE Access*, 7:37989–38008, 2019.

[53] Ge Xin, Liu Fen-lin, Lu Bin, Wang Wei, and Chen Juan. An image encryption algorithm based on spatiotemporal chaos in dct domain. In *2010 2nd IEEE international conference on information management and engineering*, pages 267–270. IEEE, 2010.

[54] Sen Yang and Xiaojun Tong. A block image encryption algorithm based on 2d chaotic system. In *2021 IEEE 12th International Conference on Software Engineering and Service Science (ICSESS)*, pages 61–64. IEEE, 2021.

[55] Ping Yin and Lequan Min. A color image encryption algorithm based generalized chaos synchronization for bidirectional discrete systems for audio signal communication. In *2010 International Conference on Intelligent Control and Information Processing*, pages 443–447. IEEE, 2010.

[56] Sura F Yousif, Ali J Abboud, and Hussein Y Radhi. Robust image encryption with scanning technology, the el-gamal algorithm and chaos theory. *IEEE Access*, 8:155184–155209, 2020.

[57] Haini Zeng and Deli Chen. Image encryption algorithm based on logistic-sine compound chaos. In *2020 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, pages 120–123. IEEE, 2020.

[58] Huacheng Zhang, Jinyu Zhu, Shuaijie Zhao, Qing He, XiaoXiong Zhong, and Jianming Liu. A new image encryption algorithm based on 2d-lsimm chaotic map. In *2020 12th International Conference on Advanced Computational Intelligence (ICACI)*, pages 326–333. IEEE, 2020.

[59] Peng Zhang, Mo Chen, and Jian-Guang Zhang. Image encryption algorithm of hyper-chaotic system based on spiral scrambling. In *2020 IEEE International Symposium on Product Compliance Engineering-Asia (ISPCE-CN)*, pages 1–5. IEEE, 2020.

[60] Xuncai Zhang, Lingfei Wang, Zheng Zhou, and Ying Niu. A chaos-based image encryption technique utilizing hilbert curves and h-fractals. *IEEE Access*, 7:74734–74746, 2019.

[61] Fangzheng Zhao, Chenghai Li, Chen Liu, and Jie Zhang. Image encryption algorithm based on sine-logistic cascade chaos. In *2019 5th International Conference on Control, Automation and Robotics (IC-CAR)*, pages 224–228. IEEE, 2019.

[62] Congxu Zhu and Kehui Sun. Cryptanalyzing and improving a novel color image encryption algorithm using rt-enhanced chaotic tent maps. *Ieee Access*, 6:18759–18770, 2018.

[63] Hegui Zhu, Yiran Zhao, and Yujia Song. 2d logistic-modulated-sine-coupling-logistic chaotic map for image encryption. *IEEE Access*, 7:14081–14098, 2019.