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

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 Image Encryption

Image encryption involves transforming an image into a coded form, making it unreadable to anyone except the intended recipient. This is achieved through the use of encryption algorithms that employ various techniques such as substitution, permutation, diffusion, and confusion. The encrypted image can only be decrypted by the recipient who has the decryption key. Image encryption is used to protect the confidentiality and integrity of images in various applications such as secure image transmission, digital watermarking, and multimedia security. It ensures that images are protected from unauthorized access and tampering, making it a crucial aspect of digital communication.

1.3 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 shared passion for cryptography and fascination with chaos theory. We 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 us and we are 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 us to push the boundaries of what is currently possible. Successfully developing a new chaos-based image encryption technique would be a major accomplishment for us, both professionally and personally, and would be a source of pride and satisfaction in our careers as researchers.

3 Project Objectives

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

General

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.

Chaotic

1. Ensure confidentiality: The primary objective of image encryption is to ensure that the information contained within the image remains confidential and can only be accessed by authorized users. Encryption using chaotic maps helps achieve this objective by making it difficult for unauthorized users to access or read the encrypted data.

2. Provide integrity: Image encryption using chaotic maps also ensures the integrity of the image by detecting any unauthorized modification or tampering with the image. This objective is achieved by including error-detection and correction codes in the encryption process.

3. Increase resistance to attacks: Chaotic maps-based image encryption techniques are designed to increase resistance to attacks such as brute-force attacks, statistical attacks, and differential attacks, among others. The objective is to create an encryption scheme that is difficult to break even with advanced computing power.

4. Reduce computational complexity: Another objective of image encryption using chaotic maps is to reduce the computational complexity of the encryption algorithm. This is important for real-time applications where encryption and decryption need to be performed quickly.

5. Enhance robustness: Image encryption using chaotic maps also aims to enhance the robustness of the encryption scheme by ensuring that it is resistant to various types of noise, interference, and distortions that may occur during transmission or storage.

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.

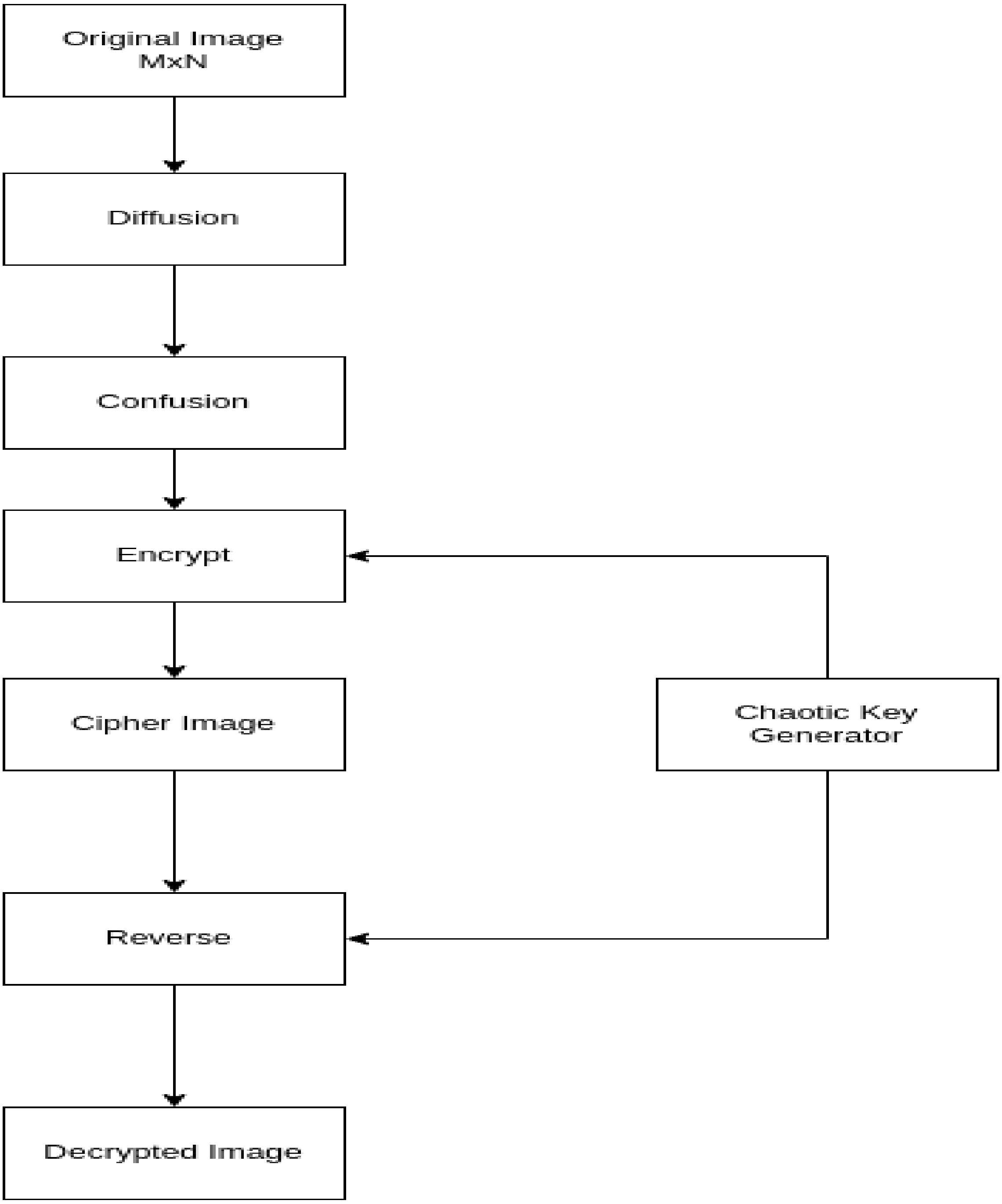
4. Divide the image into blocks: Divide the original image into smaller blocks of a fixed size. The size of the blocks should be selected to optimize the encryption process.

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.


Original Image
MxN
Diffusion
Confusion
Encrypt
Cipher Image
Chaotic Key
Generator
Reverse
Decrypted Image

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] 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.

[2] Michael Benedicks and Lennart Carleson. The dynamics of the hénon map. *Annals of Mathematics*, pages 73–169, 1991.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

[7] Eko Hariyanto and Robbi Rahim. Arnold's cat map algorithm in digital image encryption. *International Journal of Science and Research (IJSR)*, 5(10):1363–1365, 2016.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] Ping Ping, Feng Xu, Yingchi Mao, and Zhijian Wang. Designing permutation–substitution image encryption networks with henon map. *Neurocomputing*, 283:53–63, 2018.

[15] 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.

[16] 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.

[17] Priya R Sankpal and PA Vijaya. Image encryption using chaotic maps: a survey. In *2014 fifth international conference on signal and image processing*, pages 102–107. IEEE, 2014.

[18] SJ Sheela, KV Suresh, and Deepaknath Tandur. Image encryption based on modified henon map using hybrid chaotic shift transform. *Multimedia Tools and Applications*, 77:25223–25251, 2018.

[19] 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.

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