CHAPTER 1
INTRODUCTION

1.1 Background

The use of digital technology in healthcare has made it easier to deal with medical information, particularly in terms of the storage and transfer of medical imaging data. Medical imaging modalities such as magnetic resonance imaging, CT scans, X-rays, and endoscopy play a very important role in making diagnoses and decisions affecting patient follow-up in the clinic. However, this kind of advancement has meanwhile increased the secrecy and security hazards present in medical data. According to data from the World Health Organization (WHO), more than 35% of the occurrences of data breach events in the field of healthcare related to medical imaging information [1]. This emphasizes the need for strict procedures to protect visual data in medical information systems.

His clearly shows the need for strict measures to secure visual data within healthcare information systems. Concerning the security of visual data, it is common for digital image encryption to be the main means. Traditional encryption algorithms such as AES and RSA can neither exploit all the features of photographs nor readily cope with their relatively high redundancy and the typical distributions of pixel values. As a result, chaos-based encryption has been widely explored as one of the approaches. Chain systems like Lorenz have an inherent delicacy at the outset to produce extremely complex pseudorandom sequences and are thus suitable for pixel scrambling in images [2].

The main problem in visual data security lies in ensuring the confidentiality of the image information while keeping the image quality intact. Many encryption techniques give encrypted images that look like nothing more than noise or random patterns. Although such security utilizing encryption cannot be absolutely guaranteed, these types of encrypted images may instill suspicion at sites along the public network. The Visual Meaningful Image Encryption (VMEI) method has been proposed to solve this problem. It develops an encryption technology that can ensure the similarity between figures and encrypted images and thus reduce their likelihood of being recognized as signals [3].

Within the VMEI framework, Huang et al.(2023) combine the Lorenz system with a digital signature and wavelet transformation. The results show a

PSNR greater than 50 dB and a correlation value of decryption approaching 1, demonstrating the efficiency of this methodology in maintaining the visual quality and precision of decryption [3]. In addition, they included a digital signature to help authenticate the user, which strengthens the security aspect of the system.

Tao Li, Baoxiang Du, and Xiaowen Liang (2020) suggested a visually striking and notable image encryption technique based on cryptographic key scrambling and discrete wavelet modification [4]. The original picture divides into several blocks, each encrypted separately. The bits were then put together again to produce the encrypted picture. The results and the experimental analysis reveal that the proposed approach preserves the image information against exposure and displays good performance.

Using an encryption method, Hamza et al.(2017) [5] suggest protecting the main frames acquired from diagnostic hysteroscopy recordings. This method relies on a two-dimensional logistic map to generate cryptographic keys and improves confidentiality. It emphasizes the balance between security and computational economy, therefore offering resistance against many hazards and maintaining reasonable computational complexity. This approach is suitable for real-time medical imaging and telemedicine environments, since it can be added to mobile cloud ecosystems and expanded to secure cloud content and data transmission.

Li et al. (2020) on biometrics shows how realistically user identity might be included in the encryption process. To show improvements in the security aspects of data access, a system was developed using a biometric verification mechanism and a chaotic map [6]. Still, this approach has not yet been shown in relation to visually important photos.

PSNR readings ranging from 24 to 26 dB were obtained by Abd-Elazeem et al. (2020) from an encryption method using DCT and chaotic maps. This method has not yet addressed the application of a user authentication mechanism [7] or visually important encryption. The publications show a dearth of studies that combine VMEI, digital signatures, and role-based access control into a coherent system.

The choice of medical imagery in this study is deliberate. The high sensitivity of the data is compounded by the fact that medical images are directly linked to clinical decisions that affect patient safety. The risk of data leaks encompasses not only administrative concerns, but also potential legal infractions and reputational harm to healthcare organizations. Consequently, it is essential to establish a system that preserves data secrecy while also guaranteeing the integrity and authenticity of the data owner.

In addition, health information systems such as PACS and EHR frequently

involve data interchange between several organizations. This situation requires security solutions that operate interoperably, quickly, and effectively. The Lorenz algorithm, when integrated with the DWT transformation, achieves a balance between the complexity of randomness and the computational efficiency of encryption.

This study employs a digital signature for the verification of user identity, ensuring that the encryption-decryption process is restricted to authorized entities. The adoption of digital signature-based authentication improves the system both cryptographically and in terms of access management within a therapeutic setting.

This research introduces a role-based access control mechanism that distinguishes authorization levels between administrators and physicians. The administrator is tasked with entering patient and physician information while the physician authenticates patient data and executes encryption and decryption procedures. This methodology aims to synchronize technical security with operational protocols in the healthcare sector.

Using the VMEI approach, the developed system not only obscures information but also produces images that visually resemble the original photographs. This is critical in medicine, requiring that a visual representation remain identifiable, especially during system tests or field trials soon afterward.

This project aims to combine a Lorenz algorithm with wavelet transformation to develop an encryption and signature scheme for medical images. The program does not only maintain the visual significance of its results, but also possess a digital signature to authenticate such effort. The system was rigorously tested in multiple technical parameters, such as resolution, rotation, alpha value, and starting state, to determine its robustness under real-world uses.

1.2 Problem Formulation

The main problems to be solved in this study are how to develop a secure, efficient, and sound methodology to encrypt medical images (especially endoscopic images) by integrating online chaotic Lorenz systems, digital signatures, and steganographic techniques. This new type of development aims not only to protect the security and integrity of sensitive medical data but also to provide information addressing its provenance via digital authentication.

To address these problems, the study mainly involves three aspects: First, methods must be devised to ensure that the Lorenz chaotic encryption algorithm is strong enough to encrypt endoscopic pictures without compromising their clinical

value. At the same time, secondarily, the doctor's digital signatures must be integrated into the encrypted images. The system must be able to insert these authentication codes effectively without messing up a valuable data structure or disturbing the encryption process. Third, we applied steganographic techniques to hide additional data including digital signatures and secrets-and integrated the whole insertion process without destroying the integrity of the main data or compromising security during its transmission and storage.

And finally, system performance, including factors such as speed of data handling, efficiency in resource use, and adaptability in a clinical environment where demands for high reliability are stringent. For everyday medical applications to be successful in the real world, apart from comprehensive security assessments including resistance against attacks and how well decryption is accomplished via PSNR and BER metrics, it is also important to test the stability of the entire system.

1.3 Objectives and Benefits of the Research

This research aims to develop a medical image encryption system based on the Lorenz algorithm integrated with digital signatures and steganography techniques to maintain the security, integrity and authenticity of medical data in a comprehensive way. In general, the specific objectives of this research are as follows:

1. Design and implement an encryption method based on the Lorenz algorithm that can maintain the visual quality of endoscopic images and produce encrypted images that remain visually meaningful (Visually Meaningful Encrypted Image / VMEI).

2. Integrating the doctor's digital signature into the encryption system as a form of authentication to ensure the authenticity and integrity of medical data.

3. DWT-based steganography techniques and permutation have been applied to insert secret images and digital signatures into the carrier image efficiently and safely.

4. Developing a web-based system with two user roles (admin and doctor) that allows the integration of data input, validation, encryption, and decryption.

5. Conduct a quality evaluation of the encryption and decryption results using the PSNR (Peak Signal-to-Noise Ratio) and BER (Bit Error Rate) parameters to assess the effectiveness and resilience of the system against data disturbances.

6. Ensure that the system consistently achieves PSNR values greater than 30 dB for secret decrypted images with a resolution of 1024×1024, as a benchmark for preserving critical visual information essential for medical analysis and interpretation.

This research is expected to provide benefits both theoretically and practically, among others:

1. Theoretical Benefits
    a. Adding insight and scientific contribution in the field of information security, especially in the application of the Lorenz chaos system for medical image encryption.
    b. Providing a new approach in the integration of encryption and digital authentication through a combination of chaos algorithms, digital signatures, and steganography techniques.
2. Practical Benefits
    a. Providing a medical image security system solution that can be used in the clinical world to maintain the confidentiality and authenticity of patient information digitally.
    b. Providing a web-based system that facilitates doctors and admins in processing medical data securely, efficiently, and in a structured manner
    c. Providing a foundation for the development of similar systems for hospital needs, telemedicine, or other digital health services.

1.4 Problem Limitations

To make this research more focused and effective, some limitations are set as follows:

1. Type of medical images

    This research only uses endoscopic-type medical images as the secret image and patient images as the carrier image. The doctor's digital signature image is used as the signature image.

2. Encryption Algorithm

    The encryption algorithm used is limited to the Lorenz chaos algorithm, which is combined with permutation techniques and DWT (Discrete Wavelet Transform). Other algorithms outside the scope are not discussed.

3. The Steganography Method

   The embedding technique of secret images and digital signatures is limited to DWT-based embedding methods and permutation. In this research, no evaluation of other embedding methods is conducted.

4. Digital Authentication

   The doctor's digital signature in this research is represented in the form of an image (image-based signature) that is embedded in the encryption process. It does not include the use of digital signatures based on digital certificates or PKI.

5. System Evaluation

   The evaluation of image encryption and decryption quality is limited to two main parameters: PSNR (peak signal-to-noise ratio) and BER (bit error rate). Security aspects beyond these two parameters are not included in the scope of this study.

6. Web System Scope

   The developed application system is a web-based prototype with two main roles, namely admin and doctor, and only operates in a local environment (localhost). It does not include direct application on hospital networks or integration with electronic medical record (EMR) systems.

7. Image Size and Data Set

   This research uses a data set of medical images and digital signatures with resolution variations of 64x64, 128x128, 256x256, 512x512, 1024x1024, and 2048x2048 pixels. Size adjustment is done through a resizing process to ensure compatibility in the embedding, encryption, and evaluation processes.

1.5 Hypothesis

Based on the background and problem formulation that have been outlined, the hypothesis in this research is formulated as follows:

1. Main Hypothesis (Inductive Hypothesis):

   The use of the Lorenz algorithm combined with permutation techniques and DWT transformation and the integration of digital signatures in the medical image encryption process is able to produce visually meaningful

encrypted images (Visually Meaningful Encrypted Image/VMEI), safe from unauthorized modifications, and has good decryption quality based on PSNR and BER metrics.

2. Operational Hypothesis (Working Hypothesis)

    a. H1 : The Lorenz algorithm can produce effective chaotic patterns in the permutation process to enhance the security of medical images during encryption.

    b. H2 : The integration of digital signatures in image form (image-based signature) into the carrier image using steganography techniques does not significantly reduce the visual quality of the encryption results.

    c. H3 : DWT-based embedding and permutation techniques can securely and efficiently insert images of secrets and digital signatures into the carrier image.

    d. H4 : The VMEI decryption process can produce secret images and signatures that closely resemble the original, as indicated by PSNR values above 30 dB and BER close to 0.

    e. H5 : The developed encryption-decryption system can be implemented in web-based applications with stable performance and accurate authentication validation.

1.6 Research Methodology

This research uses a quantitative approach and applied experiments to develop and evaluate a medical image encryption system based on the Lorenz algorithm integrated with digital signatures. The stages in this methodology are explained as follows:

1. Preliminary Study and Literature Review

    Conducting a literature review on relevant topics, such as image encryption of medical images that are visually meaningful (VMEI), the Lorenz chaos algorithm, digital signatures, steganography techniques, and DWT transformation. The purpose of this stage is to understand the theoretical foundations and recent developments in the field of medical image security.

2. Problem Formulation and Hypothesis

Identify the main issues in current medical image encryption systems, particularly related to visual aspects, data integrity, and security. Based on this identification, a problem formulation and hypothesis are developed that explain the role of the Lorenz algorithm in enhancing encryption effectiveness.

3. Research Design

   Determining the type of research approach used (quantitative), as well as defining the research variables, namely:

   a. Independent variables: implementation of the Lorenz algorithm and integration of digital signatures.
   b. Dependent variables: Encryption effectiveness, visual quality of the encryption results, and data integrity (measured by PSNR and BER).

4. Data set Collection

   The data set used in this study consists of three types of images: endoscopy images, patient face photos, and doctor's digital signatures. The collection method for each type is as follows:

   a. Endoscopy images were obtained from publicly available datasets on Kaggle, which provide a variety of labeled and unlabeled medical images for academic and non-commercial research purposes.
   b. Patient photos were sourced from publicly accessible web-based image repositories such as Google Images by searching for synthetic or sample images that do not contain identifiable or sensitive data. The use of these images is strictly for testing the technical performance of the encryption system and does not involve any real patient identity.
   c. Digital signature images were created independently using a digital signature application. These signatures were collected by manually drawing or signing on a touchscreen device or stylus input, then saved in image format (PNG/JPEG) for integration into the encryption system.

   To ensure consistency in system processing, all images, regardless of source, underwent a resizing process to fit the required system dimensions, ranging from 64×64 up to 4096×4096 pixels. This resizing ensures compatibility for the embedding, encryption, and evaluation stages in the system.

5. Implementation of the Lorenz Algorithm and Digital Signature

Developing program code for the Lorenz algorithm used as the basis for permutation on images. Furthermore, it is integrated with the process of embedding the doctor's digital signature in image form. The embedding process is carried out using DWT-based methods and permutation.

6. Experimental System Testing

   Performing encryption on medical images using the system that has been built, as well as performing the decryption process to evaluate the results. Testing encompasses the dimensions of security, authenticity, and visual integrity of encryption and decryption outcomes.

7. Data Analysis

   Using quantitative measures such as:

   a. PSNR (Peak Signal-to-Noise Ratio) to evaluate the visual quality of the decryption output.

   b. BER (Bit Error Rate) to gauge data integrity and correctness. The effectiveness of the system is evaluated by a comparison between the encryption results and the original picture.

8. Evaluation and Validation of the System

   The visual quality and data integrity of the decrypted images help to evaluate the effectiveness of the system by comparison with the initial hypotheses. The consistency of PSNR and BER readings across several resolutions and parameter settings helps to validate.

9. Conclusions and Recommendations

   Formulating conclusions based on the results of analysis and evaluation, as well as providing recommendations for future system development. Recommendations also include potential development for implementation in clinical settings or other digital health systems.

10. Documentation and Reporting of Research Results

    Compiling the thesis document systematically covers the background, methodology, test results, discussion, and conclusions. Preparation of technical documents as well as scientific presentations that can be used for publication or academic seminars.

1.7 Research Method

This research develops a system for 'Meaningful Medical Image Encryption Visually Using a Digital Signature-Based Lorenz Algorithm,' with the main focus on two important aspects: the application of the Lorenz algorithm as a chaos-based encryption mechanism, as well as the integration of digital signatures as an authentication tool and medical image verification. Here is an explanation of the main methods used in this research as follows:

1. Application of the Lorenz Algorithm for Medical Image Encryption

   The Lorenz algorithm is a non-linear chaos system that was originally developed for weather modeling. Its main characteristic is high sensitivity to initial condition values, making it very suitable for use in encryption systems, as it can produce difficult-to-predict pseudorandom sequences. In the context of medical image encryption, this algorithm is utilized to perform permutations on pixel values to obscure the original information in the image.

2. Adaptation to Medical Images Several adaptation stages are carried out to ensure the compatibility of medical images with the encryption process using the Lorenz algorithm, namely:

   a. Modification of Chaos Parameters The default parameters of the Lorenz system are modified to suit the characteristics of medical images that require a balance between strength of encryption and preservation of visual meaning.

   b. Image Preprocessing Before the encryption process, medical images (endoscopy and patient photos) go through the resizing, normalization, and format conversion stages to ensure uniformity and compatibility with the Lorenz algorithm.

   c. Encryption Process The adjusted Lorenz algorithm will change the arrangement of pixels in the image, producing an encrypted image that can no longer be visually recognized by unauthorized parties, but still retains important diagnostic information that can be retrieved during decryption.

3. Integration of Digital Signatures for Authentication and Verification As part of securing data integrity, this system also integrates digital signatures into the encryption process through the following steps:

a. Integration in the Encryption Process The digital signature scheme is incorporated as part of the embedding process, where the doctor's signature in image form will be inserted together with the secret image (endoscopic image) into the carrier image. This signature is also generated based on the original image information and the key encryption, so it can only be verified with the correct image and key during the decryption process.

b. Security and Efficiency The addition of a digital signature provides an additional layer of security by ensuring authenticity and preventing unauthorized data modification. The system is designed to be efficient and practical for use in clinical settings so that the verification process can be performed simultaneously with the decryption process without requiring additional complex steps.

This study integrates the Lorenz chaos algorithm with digital signature verification and employs a visual steganography technique to ensure that encrypted images retain visual significance while remaining difficult to discern. The objective is to develop a system that is secure, efficient, and practical to manage sensitive medical data.