Applied Computer Science, vol. 20, no. 1, pp. 28–55
doi: 10.35784/acs-2024-03

Submitted: 2023-05-25 | Revised: 2024-03-07 | Accepted: 2024-03-10

Keywords: watermarking, biometric system, chaotic systems, medical imaging, telemedicine

Ziadeddine MAKHLOUF [*], *Lakhdar LAIMECHE* [0000-0002-9473-2637]*, *Abdallah MERAOUMIA* [*], *Mohamed Yassine HAOUAM* [*]

ENHANCING MEDICAL DATA SECURITY IN E-HEALTH SYSTEMS USING BIOMETRIC-BASED WATERMARKING

Abstract

In the field of Electronic Health (e-Health), Electronic Health Records (EHR) are transmitted between health professionals using e-Health systems for cooperative medical practice, medical monitoring, telemedical expertise, and telemedical imaging. Medical images are a crucial component of EHR and are used in various aspects of telemedicine systems such as expertise, consultation, teaching, and research. However, protecting the authenticity and copyrights of medical images is essential to prevent duplication, modification, or unauthorized distribution. This paper proposes a robust medical image copyright protection method that uses patient palm-print template as watermark and Lorenz chaotic map for template concealing and selecting the appropriate embedding positions in medical images. The novelty of the method lies in optimizing the expected number of modifications per pixel of the medical images after being watermarked. Experimental results indicate that this approach has a high performance with a genuine accept rate of 99.86% and can withstand various image processing attacks, including Gaussian noise, compression, and image rotations, while ensuring personal data security during telemedicine data exchange.

1. INTRODUCTION

Electronic health records are an essential tool for healthcare providers, enabling them to capture and store patient data, medical histories, and treatment plans in a centralized digital format. This helps to ensure the continuity and quality of care for patients, as healthcare providers can easily access and share information across different specialties and care settings. With the advancement of technology, EHRs have become more sophisticated and user-friendly, enabling healthcare providers to collect and analyze data in real-time. This has led to improvements in patient outcomes, as providers can quickly and accurately identify trends and patterns in patient data, helping them to make more informed decisions about patient care (Bervell & Al-Samarraie, 2019).

[*] University of Echahid Cheikh Larbi Tebessi, LAboratory of Mathematics, Informatics and Systems (LAMIS), Algeria, ziadeddine.makhlouf@univ-tebessa.dz, lakhdar.laimeche@univ-tebessa.dz, ameraoumia@univ-tebessa.dz, mohamed-yassine.haouam@univ-tebessa.dz

Nowadays, e-Health systems have revolutionized the way healthcare providers share electronic health records and collaborate to provide patient care. E-Health is the implementation of Information and Communication Technologies (ICT) in the healthcare sector. E-Health systems enable healthcare providers to share patient information and medical records securely and efficiently, facilitating better coordination of care and improving patient outcomes. One of the key benefits of e-Health systems is the ability to provide remote care, such as teleconsultation, teleexpertise, telemonitoring, teleassistance, and medical regulation. These services enable healthcare providers to consult with patients remotely, reducing the need for in-person visits and allowing for more efficient use of healthcare resources. E-Health systems also facilitate the integration of prevention services, such as m-health applications, which allow patients to monitor and manage their health remotely. This can include tracking vital signs, managing chronic conditions, and receiving personalized health recommendations. By providing patients with these tools, e-Health systems can help improve patient outcomes and reduce the need for hospitalization (Tsou et al., 2021).

With the widespread use of e-Health applications and the transmission of patient EHR between different health actors, ensuring the protection of patient privacy and confidentiality has become a critical concern. It is essential that patient information is accessed only by authorized persons and that it is transmitted securely without any unauthorized modifications or disclosures. To address these concerns, various security measures are employed in e-Health systems to protect patient information. These security measures include authentication, authorization, and encryption (Idoga et al., 2016). Authentication ensures that the person accessing the EHR is authorized to do so by verifying their identity using various authentication methods such as passwords, biometrics, or smart cards. Authorization ensures that the person accessing the EHR is authorized to view only the specific information they need to carry out their job function. This is done by assigning different levels of access privileges to different users based on their roles and responsibilities. The application of encryption is aimed at maintaining the privacy and authenticity of patient data when it is being transmitted. This involves converting the EHR into a secure format that can only be accessed by authorized users using a decryption key. In overall, it is crucial to implement robust security measures in e-Health systems to protect patient privacy and confidentiality. By ensuring the confidentiality, integrity, and authenticity of patient information, healthcare providers can provide high-quality care and improve patient outcomes.

In literature, maintaining the privacy and confidentiality of patient's EHR have been assured by the advanced encryption techniques or by the cloud computing providers (Tertulino et al., 2022; Kang & Kim, 2022; Krishnan & Lalitha, 2020; Joshi et al., 2018). The former is the process of making data secure during transmission using a public key randomly generated by a key management center and a private key based on the public key used for decryption. Encryption techniques, on the other hand, are restricted due to its costly computation and to its inefficiency. This solution cannot guarantee the security of the HER in situations where there are insiders attacks carried out by the key manager, or when fraudulent login attempts, unauthorized login access, or deceptive phishing communications are involved in the exchange or response processes. While Cloud computing providers can also play a role in ensuring the security of patient EHRs, it is

important to carefully evaluate their security controls and protocols before entrusting them with sensitive data.

Biometric-based medical data watermarking in e-Health systems is a relatively new research area, and there is limited literature available on this topic (Pallaw et al., 2023; Vaidya, 2022; Ye & Chen, 2022; Jain et al., 2022; Fares et al., 2021; Mohan, 2020; Anand & Singh, 2020). It is regroups techniques that aim to secure the medical data, such as EHRs and medical images, by embedding biometric data into it. Biometric data, such as fingerprints, iris patterns, or palm-prints, are unique to each individual and can be used to confirm the identity of the person accessing the data. By embedding biometric data into medical data, the authenticity and integrity of the data can be ensured. It helps in protecting the privacy of patient information while ensuring that medical data can be accessed and shared securely among healthcare providers. These techniques have the potential to improve data management, reduce the risk of data breaches, identity theft, and improve patient privacy.

Despite the significant achievements of current methods, they have not adequately addressed the potential loss of essential information resulting from modifications in medical images. These methods primarily rely on basic watermarking techniques, which involve randomly selecting hiding locations and replacing them with encrypted data.

In addressing the critical concern of copyright protection for medical images, the authors introduce an innovative biometric watermarking system. This system places a strong emphasis on two key objectives: protecting patient privacy and ensuring the preservation of image quality. Given that medical images contain highly sensitive information, they are vulnerable to unauthorized access, alterations, or misuse, all of which can severely compromise patient confidentiality and the integrity of the medical data. Traditional methods for copyright protection often do not meet the specialized needs of medical imaging, such as securely embedding biometric data and ensuring the image's authenticity is upheld. However, the authors' novel approach to watermarking employs a patient's palm-print as a watermark securely concealed using the Lorenz chaotic map. This is coupled with the strategic use of the SM2LSB algorithm to determine the optimal locations for embedding within the medical images. As a result, this method offers a well-rounded and effective strategy for the protection of medical images. It safeguards against unauthorized exploitation while prioritizing the crucial aspects of patient privacy and the quality of the images. This technique is structured around three main phases: encoding, enrollment, and verification, providing a structured and secure framework for copyright protection in the medical imaging domain.

During the encoding stage, the authors employ the Lorenz chaotic map to generate cancelable biometric features from the palm-print modality. In the enrollment stage, the DCT was utilized to embed the palm-print features into the DCT coefficients of the medical images. Watermark insertion and extraction are performed by selecting middle frequency bands and using the Single Match Tow Least Significant Bits (SM2LSB) algorithm with the Lorenz chaotic map. Finally, the inverse DCT was applied to obtain the watermarked image.

By employing this comprehensive methodology, the authors aim to address the challenge of preserving crucial information in medical images while ensuring patient privacy and maintaining the visual integrity of the images.

The paper is structured as follows: Section 2 presents an overview of existing watermarking systems that aim to safeguard patient information privacy and confidentiality. Section 3 introduce the theoretical background and techniques used in the proposed method. Section 4 provides a detailed explanation of the proposed approach. The experimental results are discussed in Section 5 with a comparison study in Section 6. Finally, the article is summarized in Section 7.

2. EARLY WORKS

In this section, the authors aim to highlight recent advancements in the protection of patient EHR privacy and confidentiality through various techniques. Pallaw et al. (2023) introduced an innovative watermarking method utilizing natural optimization techniques within telemedicine applications to enhance watermark robustness. This method begins by decomposing the medical image with Discrete Wavelet Transform (DWT), followed by applying Singular Value Decomposition (SVD) to extract crucial image components. The watermark is embedded into these components through a mix of genetic algorithm (GA) and particle swarm optimization (PSO) to refine the embedding process. Evaluations across metrics like robustness, imperceptibility, and security demonstrated this technique's superiority over existing watermarking methods, suggesting its suitability for telemedicine applications requiring secure medical image transmission.

Vaidya (2022) developed a novel medical image watermarking technique by integrating the strengths of Lifting Wavelet Transform (LWT), DWT, and Local Binary (LBP) in a hybrid domain. This technique dynamically determines embedding factor values using LBP values as watermarking keys, enhancing robustness and imperceptibility against various attacks. It employs triple-layer security through the Arnold transform to protect against tampering and modifications. Experimental findings indicated its effectiveness in outperforming other techniques in metric evaluations, presenting an adaptive approach for securing e-Health care systems.

Ye & Chen (2022) proposed a secure medical image sharing technique in smart healthcare systems using a Conventional Neural Network (CNN). This method aims to safeguard medical images transmitted over insecure networks without compromising image quality. It incorporates a CNN-based encryption algorithm with a chaotic map for key generation, offering efficient encryption and decryption. The system includes a multi-factor authentication mechanism, ensuring access to encrypted medical images by authorized users only. The technique's efficiency, assessed through various metrics, confirmed its capability to maintain high-quality images while securing them against different attack types.

Jain et al. (2022) suggested a security enhancement for e-Health images by merging a robust zero-watermarking method with a hyper-chaotic system and Rivest, Shamir, Adleman (RSA) encryption technique. This approach inserts a resilient watermark into the medical image, designed to withstand diverse attacks and enhances watermark robustness using a hyper-chaotic system. The use of RSA encryption secures the watermark key, bolstering the watermark's confidentiality and integrity. The technique's efficiency, evidenced by metrics like Peak Signal to Noise Ratio (PSNR), Structural Similarity Index

Measure (SSIM), and NC, indicates its effectiveness in producing high-quality images resistant to various attacks.

Ghouzali et al. (2021) introduced an approach in their study focusing on preserving the privacy of biometric templates within a multimodal biometric system. The authors aimed to address both the cancelability issue of biometric templates and the efficiency of the authentication process. To achieve this, they introduced a transform based on chaotic maps to generate cancelable biometric features for face and fingerprint minutia points, utilizing the Logistic map and Torus Automorphism, respectively. These transformed features were concatenated and substituted for the original features in the system's database. During authentication, a weighted sum rule was utilized to calculate and combine the similarity scores of the transformed face and fingerprint templates.

Fares et al. (2021) proposed a watermarking technique for medical images that combines DCT and DWT techniques to enhance their security. The technique first applies DCT and DWT to the medical image to obtain the frequency coefficients. The watermark is then inserted into the selected coefficients using a technique that combines quantization and modulation. The proposed technique is analyzed on various metrics such as robustness, imperceptibility, and security. According to the experimental findings, the suggested methodology exhibits superior performance compared to existing watermarking techniques regarding robustness and security while maintaining high levels of imperceptibility. The proposed technique can be applied in various medical imaging applications such as telemedicine, Picture Archiving and Communication Systems (PACS), and medical data storage and transmission.

Wadood et al. (2020) introduced a novel approach to enhance security in biometric systems by integrating watermarking and encryption techniques. The proposed method integrates the mean quantization method with a block-based encryption algorithm using unique tokens for each user and a distinct key for each sample in a database generated through a hyper-chaotic map. These measures ensure the privacy and security of the biometric system. Importantly, the insertion procedure does not impact facial features, and the watermark extraction can be performed blindly without storing the initial fingerprint image in the database. Experimental outcomes indicated that the suggested watermarking technique was effective against various attack types.

Mohan (2020) proposed a technique to securely transmit medical data over insecure networks using a combination of genetic algorithm focusing on bit masks with encryption and steganography techniques. The technique aims to ensure data integrity, accuracy, and privacy during transmission. In this approach, a genetic algorithm utilizing bit masks is used to optimize the selection of secret bits for hiding within an image. The selected secret bits are encrypted using the Advanced Encryption Standard (AES) algorithm and then integrated into the cover image using the Least Significant Bit (LSB) steganography method. Various metrics such as PSNR, SSIM, and Mean Square Error (MSE) were employed to examine the efficiency of the proposed technique. The results demonstrate that the proposed approach can ensure high-quality image transmission and the robustness of the embedded data regarding various types of attacks such as noise, compression, and cropping.

An advanced watermarking technique for medical data protection in the DWT and Singular Value Decomposition (SVD) domain was suggested by Anand and Singh (2020). The proposed technique first applies DWT to the medical image to obtain the frequency

coefficients. Then, SVD is used to obtain the most significant singular values and vectors of the frequency coefficients. The watermark is embedded into the selected singular values using a technique that combines quantization and modulation. The proposed technique is assessed on various metrics such as robustness, imperceptibility, and security. According to the experimental results, the proposed method outperforms existing watermarking techniques in terms of robustness and security while maintaining high levels of imperceptibility. The proposed technique is applicable to a range of medical imaging applications, including telemedicine, picture archiving and communication systems, and medical data storage and transmission.

Cedillo-Hernandez et al. (2020) developed a dual watermarking method for medical images that enhances their management by providing robustness and security. The proposed technique embeds two watermarks into the medical image using discrete cosine transform and discrete wavelet transform. The first watermark is inserted into the high-frequency DCT coefficients, while the second watermark is inserted into the low-frequency DWT coefficients. The embedding process uses a technique that combines quantization and modulation. The proposed technique is evaluated on various metrics such as robustness, imperceptibility, and security. According to the experimental results, the proposed technique surpasses existing watermarking techniques in terms of robustness and security while maintaining high levels of imperceptibility. The proposed technique can be used in various medical applications such as telemedicine, teleradiology, and image archiving and communication systems to enhance their security and management.

In their work, Aparna and Kishore (2019) suggested a watermarking technique for medical images in e-Health applications, which employs the biometric characteristics of the user (e.g., fingerprint and iris pattern) as the encryption and decryption key for the watermark. The watermark is inserted into the DCT coefficients of the medical image using a technique that combines quantization and modulation. The proposed technique is evaluated on various metrics such as robustness, imperceptibility, and security. The results of the experiment indicate that the proposed technique outperforms existing watermarking techniques in terms of robustness and security while maintaining high levels of imperceptibility. The proposed technique can be used in e-Health applications such as telemedicine, remote consultation, and medical data storage and transmission.

Zulfiqar et al. (2018) introduced a zero-watermarking algorithm intended for safeguarding the privacy of biomedical signals. The technique aims to enhance the privacy and security of biomedical signals such as electroencephalogram (EEG) and electrocardiogram (ECG) by embedding a watermark into the signal without affecting the signal's integrity and accuracy. The proposed approach uses a discrete wavelet transform to decompose the biomedical signal into different frequency sub-bands. The algorithm then applies a binary mapping function to the DWT coefficients to produce the watermark, which is then integrated into the original signal using the LSB method. To ensure the robustness of the watermark against various attacks such as noise and signal processing, the proposed algorithm uses a scrambling technique that rearranges the watermark's bits in a pseudo-random order. The scrambling technique also enhances the imperceptibility of the watermark, ensuring that the watermark does not affect the signal's quality. The efficiency of the proposed algorithm was examined using various metrics such as mean square error, signal to noise ratio, and correlation coefficient. The results showed that the

suggested approach can provide a high-quality signal while maintaining the watermark's robustness against different types of attacks.

Murillo-Escobar et al. (2016) proposed a novel fingerprint authentication system utilizing a 32-bit microcontroller and chaotic encryption algorithms to protect biometric templates. The system employs feature transformation to preserve biometric templates and an embedded expert system for secure enrollment and authentication processes. The proposed scheme's security is evaluated through statistical and hardware analysis, demonstrating the system's suitability for critical real-world applications.

3. THEORETICAL PREREQUISITES

The Gabor filter and Lorenz chaotic system are both important theoretical concepts utilized in the proposed method. The Gabor filter, a mathematical function employed in signal processing for feature extraction, constitutes a complex sinusoidal signal modulated by a Gaussian envelope. These filters find extensive applications in various image processing tasks such as image analysis, feature extraction, and object recognition. In the proposed watermarking system, Gabor filters are utilized to extract pertinent features from the cover image, subsequently employed for embedding the watermark.

On the other hand, the Lorenz chaotic system serves as a mathematical model delineating the behavior of a dynamic system over time. Comprising a set of differential equations exhibiting chaotic behavior, small changes in initial conditions can result in significantly different outcomes. The widespread usage of the Lorenz system spans various domains including cryptography and data hiding. Within the proposed watermarking system, the Lorenz system operates as a key generator for watermark embedding. Leveraging the chaotic nature of the system, a sequence of random numbers is generated and subsequently utilized to embed the watermark into the cover image.

3.1. Gabor filter

The Gabor filter is a linear filter utilized in signal processing and image processing. It derives its name from physicist Dennis Gabor, who developed the concept of the filter in the 1940s (Roslan & Jamil, 2012). It represents a complex sinusoidal signal modulated by a Gaussian envelope, defined as the product of a Gaussian function and a complex sinusoidal wave. The Gaussian envelope controls the frequency and orientation of the filter, while the sinusoidal wave captures local details in the image. In image processing, the Gabor filter serves to extract features such as edges, textures, and contours from an image. Notably, the filter exhibits a strong response to features sharing similar frequency and orientation characteristics. The output of the filter manifests as a complex-valued signal, carrying information regarding the amplitude and phase of the filtered image.

An advantage of the Gabor filter lies in its capacity to capture local information within the image. This attribute stems from the filter's limited receptive field, responding solely to features within specific frequency and orientation ranges. This allows the filter to discern fine details in the image while remaining unaffected by the surrounding background. Specifically, a 2D Gabor filter $\psi\ (x, y;\ \sigma, \lambda, \theta_k\ )$ can be formulated as follows:

$$\psi\,(x,y;\,\sigma,\lambda,\theta_k) = g(x,y;\,\sigma)\exp\,(\frac{2\pi x_{\theta_k}}{\lambda}i) \tag{1}$$

In this formula, the Gaussian function is defined by:

$$g(x,y;\,\sigma)\,\exp\left(\frac{2\pi x_{\theta_k}}{\lambda}i\right) = g(x,y;\,\sigma)\exp\,\left(\frac{x_{\theta_k}^2+\gamma^2 y_{\theta_k}^2}{2\sigma^2}\right) \tag{2}$$

Where:

$$x_{\theta_k} = xcos(\theta_k) + ysin(\theta_k), \tag{3}$$

$$y_{\theta_k} = -xsin(\theta_k) + ycos(\theta_k), \tag{4}$$

and σ is the standard deviation of the Gaussian envelope along the x and y dimensions, and λ and θ_k are the wavelength and orientation, respectively. The parameter γ is usually equal to 0.5. Since the spatial aspect ratio γ is constant, we do not use it as a Gabor filter parameter.

Gabor Filter has a real and imaginary component representing the orthogonal directions defined as follows:

$$\psi_R\,(x,y;\,\sigma,\lambda,\theta_k) = g(x,y;\,\sigma)cos\left(\frac{2\pi x_{\theta_k}}{\lambda}\right) \tag{5}$$

$$\psi_I\,(x,y;\,\sigma,\lambda,\theta_k) = g(x,y;\,\sigma)sin\left(\frac{2\pi x_{\theta_k}}{\lambda}\right) \tag{6}$$

The two components can be formed into a complex number or used individually.

3.2. 2-D Discrete cosine transform basis

The 2-D DCT is a mathematical technique used to convert a 2-dimensional signal or image into a set of frequency components (Haouam et al., 2021). It is an extension of the 1-D DCT and is widely used in image and video compression, as well as other applications. The 2-D DCT is a linear transform that decomposes a 2-dimensional signal or image into a set of frequency components. The transform is defined by a set of basic functions that are the product of two cosine functions with different frequencies and amplitudes. The 2-D DCT of an N-by-M image F is given by:

$$F(u,v) = \left(\frac{2}{N}\right)^{\frac{1}{2}}\left(\frac{2}{M}\right)^{\frac{1}{2}}\sum_{i=0}^{N-1}\sum_{j=O}^{M-1}\Lambda(i)\,.\,\Lambda(j).\,cos\left[\frac{\pi.u}{2.N}(2i+1)\right]cos\left[\frac{\pi.u}{2.M}(2j+1)\right].f(i,j) \tag{7}$$

where $F(u,v)$ the 2-D DCT coefficient at the frequency is (u,v), $f(i,j)$ is the pixel value at position (i,j) in the input image, and $\Lambda(i)$ and $\Lambda(j)$ are scaling factors given by:

$$\Lambda(\xi) = \begin{cases} \frac{1}{\sqrt{2}} & for\ \xi = 0 \\ 1 & otherwise \end{cases} \tag{8}$$

The 2-D DCT has several properties that make it useful in image and video compression applications. One important property is the energy compaction property, which means that most of the energy of the input image is concentrated in a small number of low-frequency DCT coefficients. This allows the image to be compressed by discarding or quantizing the higher-frequency coefficients without significantly affecting the quality of the reconstructed image.

3.3. Lorenz chaotic system

The dynamic behavior of nonlinear systems has gained significant attention in various applications due to their simplicity and richness (Laimeche et al., 2021). Chaotic systems are considered to be one of the important nonlinear systems, which exhibit extreme sensitivity to initial conditions, periodicity, and pseudo-random behavior. The sensitivity to initial conditions is a key characteristic of chaotic behavior, where small differences in initial conditions can cause drastically different outcomes in the long run. Chaotic systems are defined by a set of equations, where a discrete-time chaotic system can be represented as follows:

$$x_{n+1} = \Gamma(x_n), \quad n = 0,1,2, \ldots \tag{9}$$

Where $x_n \in R^n$ called the chaotic system state, and Γ draws the next state x_{n+1}. From an initial state x_0 , the repeated application of this function (Γ) produces a sequence of N points ($\{x_n\}_{n=0}^{N}$) called the orbit of the discrete-time system.

The effectiveness of discrete-time chaotic systems in various information security applications, such as encryption, steganography, and watermarking, has been demonstrated in the literature. These systems have been utilized to generate secret keys due to their ability to exhibit extreme sensitivity to initial conditions, periodicity, and pseudo-random behavior (Laimeche et al., 2021).

Lorenz map is a commonly used chaotic system that is used to generate chaotic sequences. It is a simplified model of meteorological phenomena based on fluid mechanics, and is also known as the Lorenz dynamic system or Lorenz oscillator. The Lorenz map is a three-dimensional dynamic system that exhibits chaotic behavior under certain conditions. The system is described by the following equations:

$$\begin{pmatrix} \dot{x} \\ \dot{y} \\ \dot{z} \end{pmatrix} = \Gamma_S \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} \sigma(y - x) \\ \rho x - y - xz \\ xy - \beta z \end{pmatrix} \tag{10}$$

In this equation σ, ρ, and β are three strictly positive real parameters and the dynamic variables *x*, *y* and *z* represent the state of the system at any time. Lorenz map is a non-periodic system which shows how the different variables of the dynamic system grow over the time in a non-periodic trajectory. We often set σ = 10 and β = 8/3 and ρ remaining variable.

3.4. SM2LSB technique

Laimeche et al. (2016) presented a classification of insertion techniques utilized in watermarking systems that employ images, categorized by the method of insertion applied to the cover media. These techniques are classified into five categories: file structure, spatial domain, frequency domain, spread spectrum, and palette colors. The majority of these methods involve modifying the Least Significant Bits (LSBs) of the cover medium, except for the file structure technique.

One popular steganographic technique for embedding secret information in digital images is SM2LSB technique, which entails altering two LSBs of selected pixels in the image to convey the secret message. This technique is termed "Single Mismatch" because only one of the two LSBs is altered in pixels where both LSBs are initially the same, and "Two LSBs" because two LSBs are altered in pixels where both LSBs are initially different.

The SM2LSB technique functions by selecting specific pixels in the image to be modified to carry the secret message. The selection can be made randomly or using a predetermined pattern. The value of the selected pixels' LSBs is then altered according to the secret message to be incorporated. In pixels where both LSBs are initially the same, only one of the two LSBs is modified to carry the secret message. In pixels where both LSBs are initially different, both LSBs are modified to convey the secret message (Laimeche et al., 2016).

4. BIOMETRIC WATERMARKING SYSTEM

In this research, we introduce a robust method aimed at protecting the copyright of medical images. This method utilizes a patient's palm-print template as a watermark and employs the Lorenz chaotic map for concealing the template and selecting appropriate embedding positions within the medical images. The primary objective of this study is to capitalize on the synergy between biometric and watermarking systems to improve the effectiveness of watermarking mechanisms, especially for safeguarding copyrighted content. Biometric systems have evolved into dependable tools for user authentication, providing robust security measures rooted in distinctive physiological or behavioral traits. By incorporating biometric characteristics into watermarking schemes, an additional layer of security is introduced, enhancing protection against unauthorized access or alterations to the original content.

The contributions of this paper can be outlined as follows:

1. **Utilization of Palm-Print Modality-Based Biometric Identification**: The study focuses on leveraging palm-print modality-based biometric identification as the watermark, employing Gabor filters as the foundational framework. Gabor filters are well-suited for biometric identification tasks due to their ability to robustly capture unique features of palm prints, ensuring accurate and reliable user authentication. By employing Gabor filters, the study aims to extract distinctive palm-print features that can serve as the watermark for copyright protection purposes.

2. **Embedding of Extracted Watermark Using SM2LSB Technique:** The extracted watermark is seamlessly embedded into the content using the SM2LSB technique. This embedding process ensures the seamless integration of the watermark into the content while minimizing perceptual distortion and preserving the integrity of the original data. By incorporating the watermark using SM2LSB, the study guarantees that only authorized users possessing the corresponding palm-print characteristics can access or modify the content.
3. **Encoding of Biometric Template Using Lorenz Chaotic System:** To facilitate efficient embedding of the biometric template into the medical image, the template undergoes encoding using the Lorenz chaotic system. The Lorenz chaotic system offers a sophisticated encoding mechanism that generates a compact representation of the biometric template while retaining its essential characteristics. This encoding process ensures that the watermark can be embedded into the medical image without significantly compromising its quality or usability.
4. **Enhancement of Copyright Protection Measures**: By combining these advanced techniques, the proposed study aims to elevate copyright protection measures by integrating robust biometric authentication with state-of-the-art watermarking techniques. The incorporation of palm-print-based biometric identification, Gabor filters, SM2LSB embedding, and Lorenz chaotic encoding collectively strengthens the security of copyrighted content, ensuring that only authorized users can access or modify the data while preserving its integrity and authenticity.

4.1. Functional architecture

In Fig. 1, the proposed biometric watermarking system structure comprises two main phases: watermark embedding and watermark verification.

During the watermark embedding phase, the initial step involves extracting features from the user's biometric template. Subsequently, the biometric template is encoded to generate a compact representation that can be embedded into the medical image without significantly compromising its quality. Finally, the watermark is inserted into the medical image using an insertion algorithm, ensuring its imperceptibility and resilience against various attacks.

In the watermark verification phase, the process begins with extracting the embedded watermark from the watermarked image using an extraction algorithm. The extracted watermark is then decoded to retrieve the original biometric template. Finally, the decoded template is matched with the template extracted from the user's biometric characteristics using a matching algorithm.

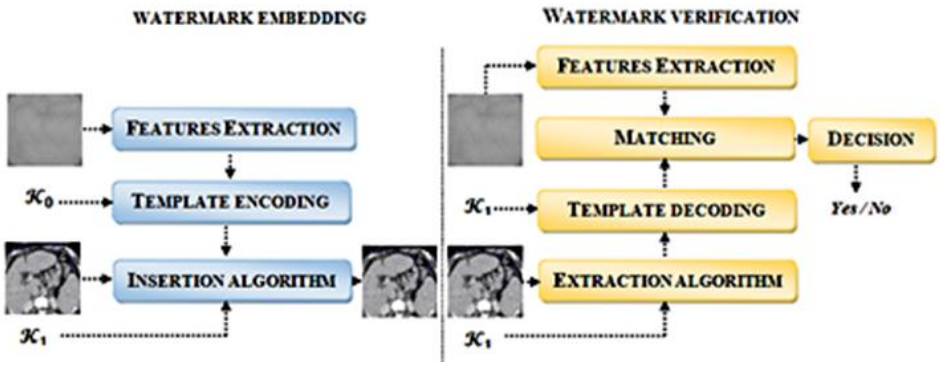

Fig. 1. Proposed biometric watermarking system

4.2. Watermark embedding phase

Fig. 1 depicts the watermark embedding phase which comprises three steps. Firstly, a binary biometric template is generated by applying the Gabor filter technique to extract discriminative binary features from the palm-print biometric modality and the amplitude of the filtered images. Secondly, to enhance the protection of the obtained binary template, the encoding step utilizes the Lorenz chaotic system to encode the biometric template. Lastly, the binary watermark is inserted into the DCT coefficients of the host image using the Lorenz chaotic system for position selection.

1. Feature extraction step

In the initial step of the watermarking phase, the palm-print modality undergoes several processing steps such as filtering, binarization, thresholding, and contour computation to extract its region of interest. After that, the Gabor filter technique is employed to filter the image with the most suitable parameters (the filter orientation, spatial frequency and standard deviation) for optimal feature extraction.

The application of 2D Gabor filter with a filter f_G to an image I is a convolution operation of this image with a Gabor filter defined by:

$$I_G(x,y) = f_G(x,y) * I(x,y) = \sum_{m=0}^{N-1} \sum_{n=0}^{N-1} f_G(m,n) \times I\,(x-m, y-m) \qquad (11)$$

Where, $*$ denotes the convolution operator and I_G is the convolution result of the image and the filter f_G. As the Gabor filter has a complex shape, and it is crucial to consider both the real and imaginary representations of the Gabor coefficients to extract meaningful information. Using both representations enables the creation of a unique feature vector (template) for each palm-print that can be used for recognition purposes. Previous studies have shown that using the real or imaginary representations separately as features does not result in good discrimination. However, combining these two representations, either in amplitude or phase, can significantly improve the performance of a recognition system.

The different steps to extract the discriminating characteristics of the palm-print are the following:

– A normalization operation is applied to increase the contrast of the image;

– Then, filter the image with the Gabor filter to obtain the template of the image in the form of two representations (real and imaginary). These two representations are used to calculate the amplitude (A_{IG}) as follows:

$$A_{IG}(x,y) = \sqrt{\psi_R\,(x,y;\,\sigma,\lambda,\theta_k)^2 + \psi_I\,(x,y;\,\sigma,\lambda,\theta_k)^2} \tag{12}$$

Finally, the amplitude representation is converted to a binary image using thresholding technique. Indeed, each point in the resulting representation is coded by a 0 or 1 bit as follows:

$$\Phi_{\mathrm{A_{IG}}}(x,y) = \begin{cases} 1 & if\ \ A_{IG}(x,y) \geq \tau_b \\ 0 & if\ \ A_{IG}(x,y) < \tau_b \end{cases} \tag{13}$$

Where, τ_b the threshold defined as follows:

$$k \times m$$

Where, m denotes the average of the amplitude image, and k is a positive number.

Finally, the binary image which represents the biometric template includes the black pixels that correspond to the background of the image and the white pixels that correspond to the features.

The process of feature extraction using Gabor filter is illustrated in Fig. 2. The filter is convolved with a palm-print image, producing two representations: real and imaginary. These representations are then used to create a unique features vector (template) for recognizing the palm-print of a person. The resulting binary image represents the features vector obtained from the amplitude representation, with black pixels representing the image background and white pixels representing the biometric image features.

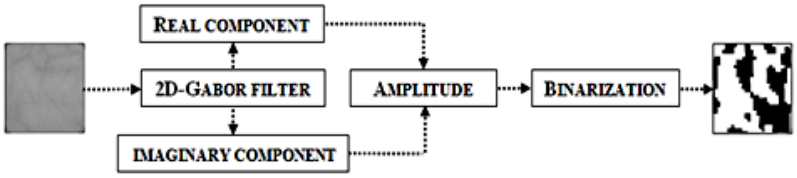

Fig. 2. Binary features extraction using Gabor filter

2. Template Encoding

While encryption is not always necessary in a watermarking system, we choose to use the Lorenz chaotic system to encode the biometric template in our work in order to enhance its protection before embedding it in the host image.

This encoding step is performed using the Lorenz chaotic system and is incorporated into the insertion algorithm, which is illustrated in Fig.3.

Fig. 3. Encoding and insertion chaotic systems

First, in this step, using the secret key $\{\mathcal{K}_0 = (x_{01}, y_{01}, z_{01},) \in [0 \dots 1]\}^3$ and the first principal chaotic system $(\mathcal{L}_1)$, to generate three sequences $(\mathcal{S}_x^1, \mathcal{S}_y^1, \mathcal{S}_z^1)$ which used: *i)* to rearrange the values of the biometric template, *ii)* to weight its values and iii) to determine the random values e_i for each values.

- Let a secret key $\mathcal{K}_0$ represented by*:*

$$\mathcal{K}_0 = \biguplus_{j=0}^{2} \widetilde{\mathcal{K}}_{0j} = \widetilde{\mathcal{K}}_{00} \widetilde{\mathcal{K}}_{01} \widetilde{\mathcal{K}}_{02} \tag{14}$$

Where $\widetilde{\mathcal{K}}_{0i}$ denotes a hexadecimal value encoded on $M\ bits$ (in our work $M = 16$) and $\biguplus$ is a concatenation function which allows a new value to join the hexadecimal string. Thus, the main system parameters $(\mathcal{L}_1)$ are defined as follows:

$$\mathcal{L}_1 = \begin{cases} x_{01} = \frac{\mathcal{K}_{00}}{2^{16}} \\ y_{01} = \frac{\mathcal{K}_{01}}{2^{16}} \\ z_{01} = \frac{\mathcal{K}_{02}}{2^{16}} \end{cases} \tag{15}$$

Where, $\mathcal{K}_{0i}|_{i=0,1,2}$ denotes the decimal representation of the hexadecimal value $\widetilde{\mathcal{K}_{Ci}}|_{i=0,1,2}$.

Before the encoding operation, the biometric template $(\mathcal{V}_0)$ is first reorganized by the sequence $\mathcal{S}_x^1$. Let $\mathcal{S}_x^{1b}$ be a sequence of integer components, produced from the sequence $\mathcal{S}_x^1$ as follows:

$$\mathcal{S}_x^{1b} = 1 + \left\lfloor 10^5 . \mathcal{S}_x^1 \right\rfloor (mod\ \eta_v) \quad \in \quad [1..\eta_v] \tag{16}$$

Where, η_v denotes the biometric template length. The sequence $\mathcal{S}_x^{1\mathrm{b}}$ is divided into two subsequences $\mathcal{S}_{x1}^{1\mathrm{b}}$and $\mathcal{S}_{x2}^{1\mathrm{b}}$ as folllows:

$$\begin{cases} \mathcal{S}_{x1}^{1\mathrm{b}} = \{\, C_i^1\}_{i=1,3,5,\dots,\eta_v} \\ \mathcal{S}_{x2}^{1\mathrm{b}} = \{\, C_i^2\}_{i=2,4,6,\dots,\eta_v} \end{cases} \tag{17}$$

Next, a straightforward permutation is carried out among the elements of $\mathcal{V}_0$:

$$\mathcal{V}_0 \left(\mathcal{S}_{x1}^{1\mathrm{b}}\,(i)\right) \leftrightarrows \mathcal{V}_0 \left(\mathcal{S}_{x2}^{1\mathrm{b}}\,(i)\right) \Leftrightarrow \mathcal{V}_0 \left(C_i^1\right) \leftrightarrows \mathcal{V}_0 \left(C_i^2\right) \tag{18}$$

Next, the rearranged template $\mathcal{V}_0^z$ is weighted by the sequence $\mathcal{S}_y^1$:

$$\mathcal{V}_0^p(i) = \mathcal{V}_0^z(i).\mathcal{S}_y^1,\ i = 1,2,3,\dots,,\eta_v \tag{19}$$

It should be noted that each value of sequence $\mathcal{S}_y^1$ which are zero are replaced by 1 in order to avoid losing the original value of

$$\mathcal{V}_0^p\ (\mathcal{V}_0^p(i)|_{i=1,2,3,\dots,}\eta_v) \tag{20}$$

Finally, using the sequence $\mathcal{S}_z^1$, we apply the sine transformation to the weighted model $\mathcal{V}_0^p$. As the amplitude of the sine function varies from -1 to 1, the values of the sequence $\mathcal{S}_z^1$ also belong to the interval [-1, 1]. These values are originally positive, for this a normalization operation is applied to $\mathcal{S}_z^1$ to produce a sequence that contains both positive and negative elements.

In fact, to normalize the sequence $\mathcal{S}_z^1$, all we have to do is remove their mean value:

$$\mathcal{S}_z^N = \mathcal{S}_z^1 - \rho_z \tag{21}$$

Where ρ_z is the average value of $\mathcal{S}_z^1$. The sequence $\mathcal{S}_z^1$ is then used as the random vector ε_0:

$$\varepsilon_0 = \mathcal{S}_z^N\ (i) \tag{22}$$

3. Insertion algorithm step

In a watermarking system, there are two main phases, namely the watermark insertion phase and the detection/extraction phase, and both require the use of a secret key $\mathcal{K}$. This key is utilized to determine the location in the host image where the data will be embedded or to be used in the extraction process. In this section, we will describe the method used for selecting the image location where the data will be embedded, as well as the algorithm used for inserting the data.

– **Image location selection**

To determine the location for embedding the binary biometric template in the host image, a secret key $\{\mathcal{K}_1 = (x_{11}, y_{11}, z_{11},) \in [0 \dots 1]\}^3$ and the second chaotic system $(\mathcal{L}_2)$ are utilized to generate three sequences $(\mathcal{S}_x^2, \mathcal{S}_y^2, \mathcal{S}_z^2)$. These sequences are then used to select the DCT coefficients where the binary template will be inserted in the host image.

Let a secret key $\mathcal{K}_1$ represented by*:*

$$\mathcal{K}_1 = \uplus_{i=1}^2 \widetilde{\mathcal{K}}_{1i} = \widetilde{\mathcal{K}}_{10}\widetilde{\mathcal{K}}_{11}\widetilde{\mathcal{K}}_{12} \tag{23}$$

Where $\widetilde{\mathcal{K}}_{1i}$ denotes a hexadecimal value encoded on $M\ bits$ (in our work $M = 16$). Additionally, the concatenation function $\uplus$ enables the incorporation of a new value into the existing hexadecimal string. Thus, the main system parameters $(\mathcal{L}_2)$ are defined as follows:

$$\mathcal{L}_2 = \begin{cases} x_{11} = \frac{\mathcal{K}_{10}}{2^{16}} \\ y_{11} = \frac{\mathcal{K}_{11}}{2^{16}} \\ z_{11} = \frac{\mathcal{K}_{12}}{2^{16}} \end{cases} \quad (24)$$

Where, $\mathcal{K}_{0i}|_{i=0,1,2}$ denotes the decimal representation of the hexadecimal value $\widetilde{\mathcal{K}_{Ci}}|_{i=0,1,2}$.

The coordinates (x_i, y_j) used to embedding the binary biometric template are then defined by:

$$x_i = 1 + \lfloor 10^5 . \mathcal{S}_x^2 \rfloor \ (mod\ H) \quad (25)$$

$$y_i = 1 + \lfloor 10^5 . \mathcal{S}_y^2 \rfloor \ (mod\ W) \quad (26)$$

Where, H and W denote the size of the host image.

– **Watermark insertion step**

The first step of this process involves transforming the host image into the frequency domain using discrete cosine transform, which is a more robust method than spatial domain watermarking and is compatible with popular image compression standards.

Next, using the $\mathcal{S}_x^1, \mathcal{S}_y^1$ sequences generated by Lorenz chaotic system $\mathcal{L}_2$, DCT blocks from the middle frequency bands are selected. Finally, based on the $\mathcal{S}_Z^1$ sequence, the coordinates of the selected DCT coefficients are determined and the watermark is inserted using the SM2LSB technique.

The process of using SM2LSB can be summarized as follows:

1. Encode the patient template as a bit stream.
2. Use the second chaotic system ($\mathcal{L}_2$) to generate a sequence of positions (quantized DCT coefficient) in the original image.
3. Select a cover quantized DCT coefficient from the original image at each position generated by the second chaotic system.
4. Compare the two least significant bits of the selected cover quantized DCT coefficient with the two bits of the patient template.
5. If there is a match between the two, leave the cover quantized DCT coefficient unchanged. Otherwise, modify the two least significant bits of the cover quantized DCT coefficient to match the corresponding two bits of the patient template.
6. Repeat steps 3-5 until all bits of the patient template have been embedded.

4. Watermarking verification

The biometric template is extracted from the test palm-print in this phase, using the same feature extraction technique as described in the watermark embedding section. To verify the image copyright, the embedded watermark or template is then extracted using the secret key $\mathcal{K}_1$, which indicates the location of the embedded template. Finally, a matching module is used to compare the two templates, and the comparison is done using the normalized Hamming distance.

Let the two templates $\mathcal{V}_p$ and $\mathcal{V}_Q$ of two individuals P and Q, and Hamming distance is defined as follows:

$$d_0 = \frac{\sum_{i=1}^{N}\sum_{j=1}^{N} \mathcal{V}_p(i,j) \otimes \mathcal{V}_Q(i,j)}{N \times N} \quad (27)$$

Where, $\mathcal{V}_p$ and $\mathcal{V}_Q$ are the templates of person P and Q, $\otimes$ is the or-exclusive, and N is the template length.

The final step in the verification phase of watermarking is the decision step, where the distance between the reference template and the test template is compared to the predefined security threshold $\mathcal{T}_b$. This step determines the final decision, which is as follows:

$$Decision = \begin{cases} d_0 \leq \mathcal{T}_b & \Longrightarrow Yes \\ d_0 > \mathcal{T}_b & \Longrightarrow No \end{cases} \quad (28)$$

If the obtained distance is less than $\mathcal{T}_b$, then the test template is considered genuine, otherwise, it is classified as an attacked template. The threshold $\mathcal{T}_b$ is usually chosen based on the system's security requirements and its false acceptance rate (FAR) and false rejection rate (FRR).

5. EXPERIMENTAL RESULTS AND DISCUSSIONS

This work involves carrying out multiple experiments, which can be categorized into two primary sections. The first section focuses on evaluating the imperceptibility and robustness of SM2LSB by assessing the performance of the watermarking system. In the second section, the security of the biometric system is evaluated based on the inserted and the extracted watermark. As well as in terms of the key space.

5.1. Watermarking system performance

Imperceptibility and robustness are two important properties of digital watermarking. Imperceptibility refers to the ability of a watermark to be embedded into the digital content without significantly degrading the quality of the content or being noticeable to the human eye or ear. While robustness, refers to the ability of a watermark to resist various types of attacks or modifications, such as compression, cropping, or noise addition, without being destroyed or significantly altered. This section presents a series of experiments conducted to evaluate the performance of the SM2LSB technique in terms of imperceptibility and robustness. The experiments were designed to measure the ability of the proposed method to embed the biometric template within a medical image without significantly affecting its visual quality, as well as its resistance to various attacks such as compression and filtering.

1. Watermarked images generation

First, to assess the efficiency of SM2LSB algorithm in terms of imperceptibility or robustness, the authors used 200 X-ray images and binary watermark (biometric template). For the purpose of this experiment, medical images with dimensions of 700 x 600 pixels were chosen from The National Library of Medicine's MedPix database. Some of medical images used in these experiments are showed in Fig.4 (a-h).

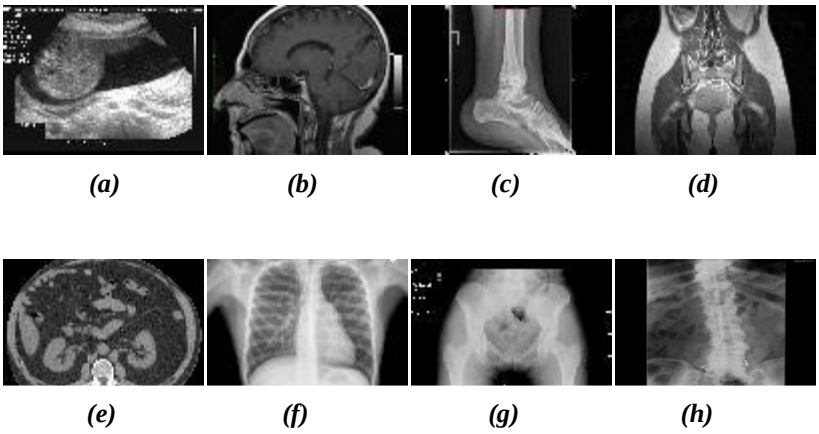

Fig. 4. Some of tested images of The National Library of Medicine's MedPix database

The SM2LSB was then used to embed the patient template, which involves comparing the two least significant bits of each cover quantized DCT coefficient with the two bits of the encoded patient template. This is achieved by generating a sequence of positions (quantized DCT coefficient) in the original image using the second chaotic system ($\mathcal{L}_2$). The patient template is then embedded based on the match and mismatch between these bits.

2. Distortion analysis

To assess the degree to which watermarked images are perceptible, two commonly used metrics are the Peak signal-to-noise Ratio (PSNR) and the Normalized Correlation (NC). These metrics are used to quantify the differences between two images, where one image is considered the original and the other is the watermarked version of the original. The PSNR measures the ratio of the maximum possible power of a signal to the power of the noise in the image, with a higher value indicating less distortion between the two images; it is computed using (29).

On the other hand, the NC serves as a metric for quantifying the similarity between a pair of images or image patches. It measures how much the pixel values of one image match the pixel values of another image, taking into account the brightness and contrast of the images. It ranges from 0 to 1, where a value of 1 indicates perfect correlation; it is computed using (31).

The use of these metrics helps to objectively evaluate the imperceptibility of watermarked images and determine the level of distortion that can be introduced while still maintaining an acceptable visual quality.

$$PSNR = 10 \times log_{10}\left(\frac{255^2}{MSE}\right) \tag{29}$$

where, C stands for the original image in its unaltered and unmodified form, and let CW be the altered image in its watermarked form.
and

$$MSE = \frac{1}{M \times N}\sum_{x=0}^{M-1}\sum_{y=0}^{N-1}(C(x,y) - CW(x,y))^2 \tag{30}$$

The NC metric is computed as follows:

$$NC = \frac{\sum_{x=1}^{M}\sum_{y=1}^{N} w(x,y)\times w'(x,y)}{\sum_{x=1}^{M}\sum_{y=1}^{N} w^2(x,y)} \quad (31)$$

where w stands for original watermark and w' stand for extracted watermark.

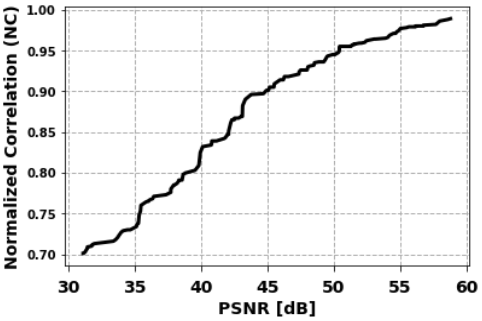

Fig. 5. Quality distortions of the watermarked image

Fig. 5 displays the evaluation of watermarked images and extracted watermarks using PSNR and NC, respectively. The PSNR values obtained range from **31.12 dB** to **58.77 dB**, which suggests that the watermarked images are very similar to the original ones. This can be attributed to the fact that SM2LSB considers the match and mismatch between the 2LSB of the original image and two bits of the binary template used for embedding. It assumes a single mismatch during the embedding process and, in some cases, modifies the third LSB of the cover image's pixel value to indicate the mismatch index. Additionally, the NC of the extracted watermark was computed, resulting in an average value of 0.86, which indicates a considerable quality of the extracted watermark.

3. Robustness Analysis

Watermarking systems are designed to embed a unique identifier into digital media to protect against unauthorized use or distribution. However, watermarking systems can be vulnerable to attacks that attempt to remove or modify the watermark. In this part, the authors tested the proposed watermarking system against popular attacks including Gaussian Noise attacks, Jpeg attacks, rotation attacks, and copping attacks.

- **Gaussian Noise Attacks**: The effectiveness of the proposed watermarking system was evaluated by testing it on watermarked images with varying degrees of Gaussian noise. Table 1 summarizes the findings of the experiments, including the mean NC and PSNR values for each level of noise intensity. The results indicate that the extracted watermarks are highly correlated with the original watermarks, with an average NC value of **0.92** when the noise intensity is below **6%**. As the noise intensity increases, the average NC value decreases, which is expected due to the interference caused by the noise. Despite this, the suggested watermarking system continues to exhibit a degree of resilience to Gaussian noise assaults, even in situations where the intensity of the noise reaches 8%, the average NC value of the extracted watermarks can still reach **0.77**. Thus, the proposed system shows promise for maintaining watermark integrity under severe distortion.

Tab. 1. Performance of the watermarking system under Gaussian noise attacks

Gaussian Noise [%]	2	4	6	8	10
PSNR	11.77	9.52	5.29	4.56	2.56
NC	0.957	0.930	0.890	0.822	0.721

- **Jpeg attacks**: In this section, the authors performed experiments on watermarked images compressed at different levels of quality to assess the impact of JPEG attacks on the proposed watermarking system. Table 2 illustrates that introducing distortions at compression levels exceeding **40%** resulted in an average NC value of **0.93**. Additionally, at compression levels below **30%**, a noticeable patch effect was observed, which further reduced the quality of the watermarked images. Despite these challenges, the watermark's average NC values remained reasonably high at **0.75**, indicating that it maintained a reasonable level of strength and integrity under these circumstances.

Tab. 2. Performance of the watermarking system under JPEG attacks

Compression Quality [%]	10	20	30	40	50
PSNR	19.78	20.62	22.19	24.52	29.84
NC	0.66	0.74	0.86	0.91	0.96

- **Rotation attacks**: To evaluate the watermarked image's resistance to rotation attacks, we performed experiments by gradually rotating the images by 5 degrees. According to Table 3, the extracted watermarks' NC mean value reaches **0.82** when the images are rotated up to **10%**. Nonetheless, if the rotation angle goes beyond **10%**, the average NC value decreases to **0.58**, indicating a decline in the watermark's robustness and integrity.

Tab. 3. Performance of the watermarking system under rotation attacks

Rotation (Clockwise)	5	10	15	20	25
PSNR	17.02	16.21	13.94	12.37	10.91
NC	0.89	0.75	0.67	0.57	0.51

5.2. Biometric system performance

To evaluate the effectiveness of the proposed system, the authors utilized a palm-print database provided by the Polytechnic University of Hong Kong (PolyU) (Bendib et al., 2022). This database was created by collecting multispectral palm-print images of 300 individuals using a multispectral palm-print capture device. The individuals included in the database are PolyU students and workers, with 195 males and a range of ages between 20 and 60 years. Two sessions were conducted to capture approximately 12 images of each individual, with an average interval of 9 days between the sessions. The images were taken under various lighting conditions and were acquired in four different spectral bands: Red (R), Green (G), Blue (B), and near infrared (N), resulting in a total of 14,400 images.

However, in our experiments, we only utilized the near infrared band, which represents the palm vein palm-print. All original images were 352x288 pixels with a resolution of 100 dpi.

This work consists of two main parts, each with a set of experiments. The first part focuses on the performance of the biometric system based on identification. The primary objective of this part is to determine the optimal parameters for the feature extraction method, namely the binarization threshold and orientation angle. Additionally, the performance of the biometric system is evaluated before and after the watermark embedding operation. The second part of the work assesses the security level of the biometric system against attacks.

- **Test protocol:** The proposed system, aimed at protecting the copyright of medical images, was implemented in a biometric identification system based on palm-veins. The database used for the experiments consisted of 2400 images of 200 individuals, with 12 images per person. Enrollment was conducted using three images per person (totaling 600 images), and the remaining 1800 images were used for testing. The performance of the system was evaluated based on imposter and client distributions generated by 179100 and 1800 comparisons, respectively. This database size is comparable to the number of employees in small and medium enterprises.
- **Preliminary tests:** To enhance the performance of the proposed system, the choice of binarization threshold ($\mathcal{T}_b$) plays a significant role as it affects the binary template. An empirical test was conducted to determine the optimal threshold that could improve the accuracy of the system. The test was conducted on the palm-print/palm vein biometric modality using the K-nearest neighbors (KNN) classifier. The tests aimed to choose the best threshold $\mathcal{T}_b$ based on the orientation angles of right angles, diagonal angles, and oblique angles.

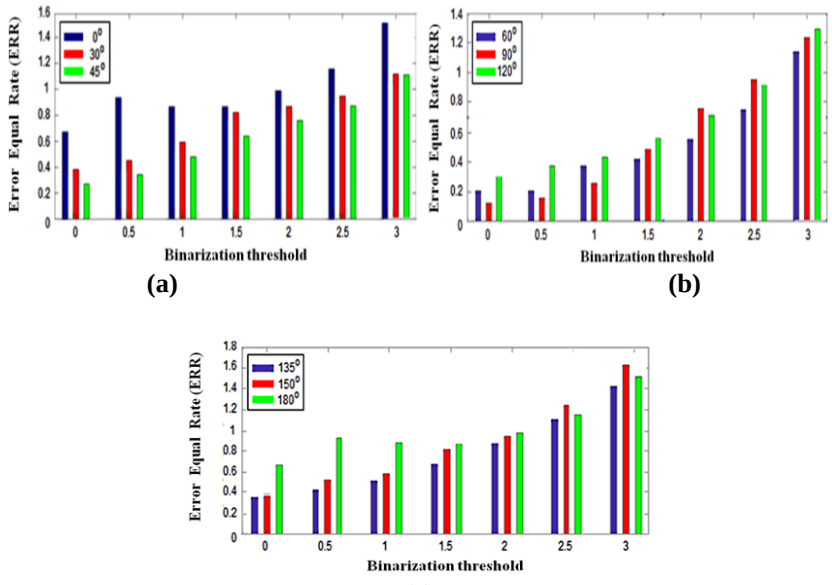

Fig. 5. System performance based on binarization threshold: (a) Right direction (0º, 30º, 45º), (b) Vertical direction (60º, 90º, 120º) and (c) Left direction (135º, 150º, 180º)

The findings presented in Fig. 5 highlight that an orientation angle of 90° yields the most favorable Equal Error Rate (EER) in comparison to other angles tested. Specifically, at a threshold $\mathcal{T}_b = 0$, the biometric system demonstrates an EER performance of **0.1324%**. This suggests that when the orientation angle is set to 90°, the system achieves its optimal balance between false acceptance and false rejection rates, resulting in the highest level of accuracy in biometric identification tasks.

- **Biometric system performance analysis:** In the watermarking embedding phase (Fig. 1), the binary template is embedded in the middle DCT coefficients of the host image after the application of the DCT transform. However, in the watermark extraction step, the embedded watermark can be modified. Therefore, it is crucial to evaluate the proposed system with the palm-print template before and after the embedding-extraction steps to ensure that the behavior of the biometric system remains consistent. The objective is to obtain two distributions that are nearly identical. To assess the biometric system's performance, we computed the normalized distance and the False Acceptance Rate (FAR) before and after the template insertion/extraction, as illustrated in Fig. 6-7.

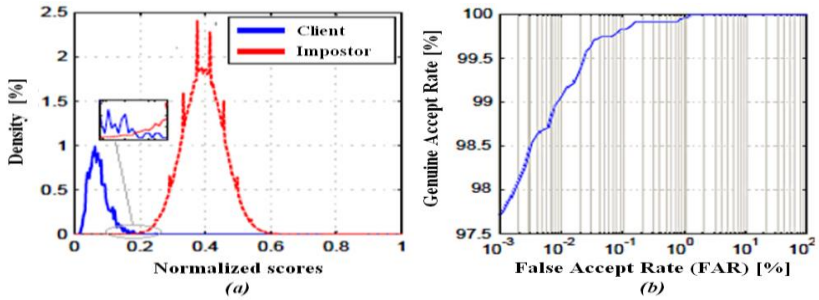

Fig. 6. Biometric system performance before embedding process: (a) Client-impostor distributions and (b) ROC curve of PLM biometric system based KNN

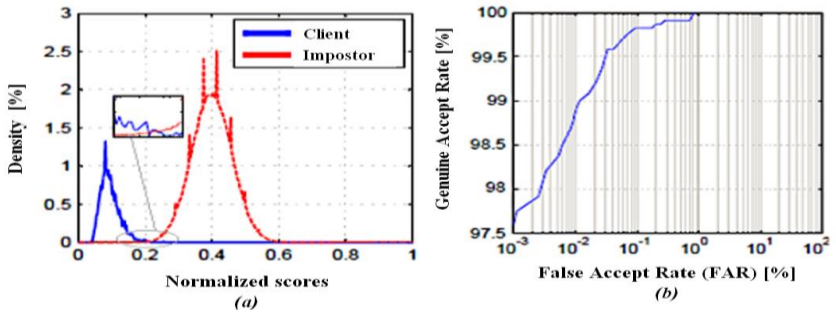

Fig. 7. Biometric system performance before embedding process: (a) Client-impostor distributions and (b) ROC curve of PLM biometric system based KNN

In Fig. 7, the data reveals that upon the extraction of the embedded template, the biometric system exhibits an Equal Error Rate (EER) of **0.1667%**, with a threshold value of **0.2274**, contrasting with the initial EER of **0.1324%** and a threshold of 0.2095, as depicted in Fig. 6 before the template embedding process. Despite this alteration, a closer examination of the results indicates that the efficacy of the biometric system undergoes

only a slight decline subsequent to the modification of the extracted biometric template. This suggests that while there is a noticeable change in performance metrics, the system remains largely resilient, maintaining a high level of accuracy even after the template manipulation.

- **Security Analysis:** The proposed system aims to protect the copyright of biometric templates, and to ensure its robustness against possible attacks, a security analysis is performed. Two important points are taken into consideration during the system design to ensure its safety. Firstly, to maintain the effectiveness of the biometric system, the secret-key space should be sufficiently large to generate a high number of templates for the same individual. Secondly, a small change in the secret-key should result in completely different templates.
- **Key space analysis*:*** The attack attempt space is determined by computing the mean absolute errors between two sequences produced by adjacent secret keys (Laimeche et al., 2020). The mean absolute error $\varepsilon_\ell|_{\ell=\{x,u\}}$ for the chaotic system is defined as follows:

$$\varepsilon_\ell\left(\mathcal{S},\tilde{\mathcal{S}}\right)=\frac{1}{\ell}\sum_{j=1}^{\ell}\left|\mathcal{S}(j)-\tilde{\mathcal{S}}(j)\right| \tag{32}$$

Two main chaotic systems ($\mathcal{L}_1$ for template encoding and $\mathcal{L}_2$ for watermark embedding) were used in this work. Therefore, the secret key space for each system was calculated separately. For both chaotic systems, the following conditions were applied: The sequences length ($S\varrho$) equal to 300 and the initial states of each parameter ($\varrho 0 \equiv \{x_0, y_0, z_0\}$) are initialized with 0, 1.

Following the simulation, the subsequent results were acquired:

$$\left(\mathbb{S}_x^i,\mathbb{S}_y^i,\mathbb{S}_z^i\right)|_{i=1}^2=(0.1750.10^{18},0.2230.10^{18},0.3110.10^{18})$$

The total space of secret-keys for both systems is then equal to:

$$\mathbb{T}_l(\mathcal{L}_1)=\mathbb{T}_l(\mathcal{L}_2)\simeq\mathbb{S}_x^i,\mathbb{S}_y^i,\mathbb{S}_z^i=0.129.10^{52}$$

We calculated the total system secret-key space under all possible configurations, and the results obtained are:

$$\mathbb{T}^{\mathcal{T}}=\prod\nolimits_{i=1}^{2}\mathbb{T}_l=0.258.10^{104}\approx 2^{340}$$

It is clear that the key-space is large enough which make it very secure.

- **Key Sensitivity analysis:** In this section, the authors performed several tests to examine the behavior of the proposed system under attacks. In these tests, the watermark (template) was inserted into the medical image using a secret key $\mathcal{K}_0$, and during the verification test, a wrong secret key ($\widetilde{\mathcal{K}_0}$) was used, which was closer to $\mathcal{K}_0$. The purpose of this test was to evaluate the performance of the verification system against this type of attack. The results of these tests are presented in Fig.8.

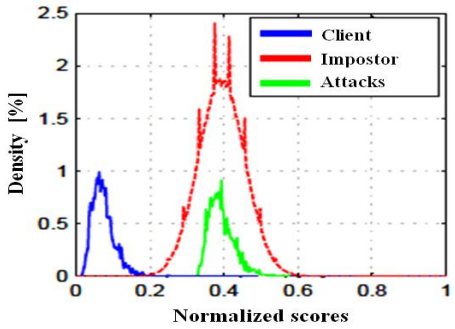

Fig. 8. Performance of biometric systems during an attack

Figure 8 provides a thorough examination of the score distributions resulting from both correct and incorrect secret keys, shedding light on their implications for the system's security in the face of potential attacks. Acting as a visual representation, the figure showcases how the system behaves across various scenarios. Noteworthy is the significant contrast observed between the distributions linked to correct and incorrect secret keys. This distinct separation suggests that the system's response varies notably depending on the authenticity of the keys utilized. This emphasis on differentiation underscores the system's adeptness at distinguishing between legitimate and unauthorized access attempts. Ultimately, the evident discrepancy in score distributions serves as compelling evidence of the proposed method's efficacy in enhancing system security. Through its robust discrimination of valid and invalid inputs, the method stands to fortify the system against possible attacks and uphold its resilience amidst security challenges.

6. COMPARISON STUDY

This section compares the performance of the proposed scheme with similar approaches presented in (Ghouzali et al., 2021; Wadood et al., 2020; Aparna & Kishore 2019; Murillo-Escobar et al., 2016). Table 4 summarises the biometric modalities used in these approaches. The effectiveness of the proposed system is evident from the table, as it outperforms all the systems listed in terms of:

- **Authentication Accuracy:** The proposed technique achieves an impressive Genuine Acceptance Rate (GAR) **of 99.86%**, which is crucial for biometric systems prioritizing security. This means that nearly all genuine users are accurately authenticated. In contrast, Ghouzali et al. achieves a GAR of **95.58%**, Wadood et al. (2020) **96.09%**, and Aparna & Kishore **97.62%**. Clearly, the proposed technique outperforms these methods in terms of authentication accuracy.
- **Key Space:** Key space plays a pivotal role in determining the security of a watermarking system. The proposed technique offers a substantial key space of $\mathbf{2^{340}}$, making it exceedingly challenging for attackers to guess or reverse-engineer the secret key, thereby enhancing the system's security. In comparison, Wadood et al. (2020) offers a key space of $\mathbf{2^{292}}$, while Ghouzali et al., Aparna and Kishore, and Murillo-Escobar et al. (2016) do not specify their key space. The larger key space of the proposed technique adds an extra layer of security.

- **Robustness:** The proposed technique demonstrates robustness against various attacks, including Gaussian noise, JPEG compression, and rotation, achieving high Normalized Correlation (NC) values for these attacks, indicating its resilience. For instance, it attains an NC of **0.92** for Gaussian noise, surpassing Wadood et al.'s (2020) NC of **0.86**. Similarly, its NC for JPEG (**0.96**) outperforms Wadood et al. (2020). In the case of rotation (**0.82**), the proposed technique maintains a reasonable level of robustness. Robustness is critical as it ensures the watermark remains intact under various real-world conditions and attacks.
- **Biometric Modalities:** The proposed technique is specifically tailored for palm-print features encryption, offering advantages for biometric systems relying on palm-print data. This optimization ensures that the technique aligns with the unique characteristics and requirements of palm-print biometrics. In contrast, other methods focus on different modalities, such as Ghouzali et al. utilizing face and fingerprint modalities, Aparna and Kishore fusing fingerprint features with medical images and health records, and Murillo-Escobar et al. (2016) concentrating on fingerprint features transformation. Each modality presents its own challenges and characteristics, with the proposed technique excelling in the context of palm-print biometrics.
- **Techniques Used:** The proposed technique leverages Lorenz chaotic maps for watermarking, known for their cryptographic strength and commonly employed in watermarking for security. In contrast, Ghouzali et al. uses chaos-based cancelable techniques, Wadood et al. (2020) employs mean quantization and hyper-chaotic maps, Aparna and Kishore utilize fusion methods, and Murillo-Escobar et al. (2016) rely on logistic map-based chaotic encryption. The choice of techniques significantly influences both the security and performance of the watermarking system, with chaotic maps, such as the Lorenz chaotic map, renowned for their cryptographic properties.

Tab. 4. Comparative Performance Analysis of Proposed Method with Existing Works in the Literature

Method	Technique	GAR [%]	Key space	Attacks [NC]
(Ghouzali et al., 2021)	Chaos-based cancelable Face and Fingerprint modalities	95.58%	2^{98}	-
(Wadood et al., 2020)	Mean Quantization and Hyper-chaotic Map	96.09%	2^{292}	Gaussian noise (NC=0.86) JPEG (NC=0.96)
(Aparna, & Kishore, 2019)	Fusion of Fingerprint features, encrypted medical images and Electric Health Record	97.62%	×	Gaussian noise (NC=0.95)
(Murillo-Escobar et al., 2015)	Fingerprint Features transform and Chaotic encryption based on logistic Map	-	2^{128}	-
Proposed technique	Palm-print Features encryption and embedding DCT selection Based Lorenz Chaotic Map	99.86%	2^{340}	Gaussian noise (NC=0.92) JPEG (NC=0.96) Rotation (NC=0.82)

7. CONCLUSION

The developed method addresses the critical challenge of safeguarding the copyright of medical images while also ensuring patient privacy and preserving visual integrity. Medical images contain sensitive data and are vulnerable to unauthorized access, tampering, or misuse, posing significant risks to patient confidentiality and data integrity. Conventional approaches to image copyright protection often fall short in addressing the unique complexities of medical imaging, including the secure embedding of biometric data and the preservation of image authenticity.

Hence, there is an urgent need for a comprehensive method that can effectively protect the copyrights of medical images while prioritizing patient privacy and maintaining the visual quality of the images. The proposed watermarking technique tackles this challenge by utilizing a patient's palm-print template as a watermark and the Lorenz chaotic map for template concealment, selecting appropriate embedding positions within the medical images based on the SM2LSB algorithm.

To validate the effectiveness of this approach, the authors conducted a series of assessment tests and compared the results against established standards to ensure the imperceptibility and robustness of the system. This research demonstrates that the suggested watermarking technique achieves lower distortion compared to state-of-the-art methods, generating high Normalized Correlation (NC) and Peak Signal-to-Noise Ratio (PSNR) values for watermarked images, making it particularly suitable for medical images. Furthermore, the NC value of the extracted watermark approaches 1, indicating excellent performance, even after subjecting the images to various processing attacks such as JPEG compression, Gaussian filtering, or rotation. Additionally, the authors evaluated the performance of the biometric system both before and after the template embedding and extraction stages to verify the consistency of its behavior. Finally, a comprehensive security analysis was conducted, assessing the key space and key sensitivity to evaluate the verification system's resilience against potential attacks. This rigorous testing and analysis demonstrate the effectiveness and reliability of the proposed method in protecting the copyright of medical images while maintaining patient privacy and image integrity.

Practical Uses of Our Method Include:

- **Enhanced Security for Medical Imaging:** By implementing this biometric watermarking technique, the security and authenticity of medical imaging data can be significantly improved, effectively protecting patient information and preventing unauthorized access or alterations.
- **Privacy Assurance for Patients:** The authors' method emphasizes the protection of patient privacy through the secure incorporation of biometric data into medical images. This approach guarantees the confidentiality and integrity of patient information, while also enabling safe data sharing and storage practices.
- **Reliable Authentication and Verification:** The proposed system facilitates the reliable authentication and verification of medical images. This is essential for forensic analysis, legal matters, and medical diagnostics, ensuring the precision and reliability of data.

Future Research Directions Highlighted by Our Findings:

- **Boosting System Robustness and Security:** Further research should explore ways to enhance the resilience and security of the biometric watermarking system. This

could involve investigating new encryption techniques or embedding methods that are more resistant to breaches and unauthorized interventions.

- **Incorporation of Additional Biometric Features:** Future studies should consider integrating other biometric features such as fingerprints, iris scans, or facial recognition. This would expand the method's usability and adaptability across different scenarios.
- **Improvements in Embedding and Extraction Techniques:** There is a need to focus on refining the processes of embedding and extracting watermarks. Efforts should aim at reducing any potential distortion and enhancing the invisibility of watermarks, possibly through the development of more sophisticated algorithms or the refinement of existing techniques.

Acknowledgments

This publication was supported by LAboratory of Mathematics, Informatics and Systems (LAMIS), under research project for e-government applications (TrustGov: 2022), Echahid Cheikh Larbi Tebessi University.

Conflicts of Interest

The authors declare that there are no conflicts of interest as applicable to this work.

REFERENCES

Anand, A., Singh, A. K. (2020). An improved DWT–SVD domain watermarking for medical information security. *Computer Communications*, *152*, 72–80. https://doi.org/10.1016/j.comcom.2020.01.038

Aparna, P., Kishore, P. V. V. (2019). Biometric-based efficient medical image watermarking in e-healthcare application. *IET Image Processing*, *13*(3), 409-548. https://doi.org/10.1049/iet-ipr.2018.5288

Bendib, I., Meraoumia, A., Haouam, M. Y., & Laimeche, L. (2022). A new cancelable deep biometric feature using chaotic maps. *Pattern Recognition and Image Analysis*, *32*(1), 109-128. https://doi:10.1134/S1054661821040052

Bervell, B., & Al-Samarraie, H. (2019). A comparative review of mobile health and electronic health utilization in sub-Saharan African countries. *Social Science and Medicine*, *232*, 1-16. https://doi.org/10.1016/j.socscimed.2019.04.024

Cedillo-Hernandez, M., Cedillo-Hernandez, A., Nakano-Miyatake, M., Perez-Meana, H. (2020). Improving the management of medical imaging by using robust and secure dual watermarking. *Biomedical Signal Processing Control*, *56*, 101695. https://doi.org/10.1016/j.bspc.2019.101695

Fares, K., Khaldi, A., Redouane, K., Salah, E. (2021). DCT & DWT based watermarking scheme for medical information security. *Biomedical Signal Processing Control*, *66*, 102403. https://doi.org/10.1016/j.micpro.2021.104134

Ghouzali, S., Nafea, O., Wadood, A., Hussain, M. (2021). Cancelable multimodal biometrics based on chaotic maps. *Applied Sciences*, *11*(18), 8573. https://doi.org/10.3390/app11188573

Haouam, M. Y., Meraoumia, A., Laimeche, L., Bendib, I. (2021). S-DCTNet: Security-oriented biometric feature extraction technique. *Multimedia Tools Applications*, *80*, 36059–36091, https://doi.org/10.1007/s11042-021-10936-7

Idoga, P. E., Agoyi, M. E., Coker-Farrell, Y., & Ekeoma, O. L. (2016). Review of security issues in e-healthcare and solutions. *International Symposium on High Capacity Optical Networks and Enabling Technologies (2016 HONET-ICT)* (pp. 118-121). IEEE. https://doi.org/10.1109/HONET.2016.7753433

Jain, J., Jain, A., Srivastava, S. K., Verma, C., Raboaca, M. S., & Illés, Z. (2022). Improved security of e-healthcare images using hybridized robust zero-watermarking and hyper-chaotic system along with RSA. *Mathematics*, *10*(7), 1071. https://doi.org/10.3390/math10071071

Joshi, M., Joshi, K. P., & Finin, T. (2018). Attribute based encryption for secure access to cloud based EHR systems. *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)* (pp. 932-935). IEEE. https://doi.org/10.1109/CLOUD.2018.00139

Kang, G., & Kim, Y. G. (2022). Secure collaborative platform for health care research in an open environment: perspective on accountability in access control. *Journal Medical Internet Research*, *24*(10), e37978. https://doi.org/10.2196/37978

Krishnan, C., & Lalitha, T. (2020). Securing healthcare data using attribute based encryption techniques in cloud environment. *European Journal of Molecular & Clinical Medicine*, *7*(11), 6271-6280.

Laimeche, L., Meraoumia, A., & Bendjenna, H. (2020). Enhancing LSB embedding schemes using chaotic maps systems. *Neural Computing & Applications*, *32*(21), 16605–16623. https://doi:10.1007/s00521-019-04523-z

Laimeche, L., Merouani, F. H., Smain, M. (2016). A new binary similarity metric for two LSB steganalysis. *2016 International Conference on Information Technology for Organizations Development (IT4OD)* (pp. 1-7). IEEE. https://doi.org/10.1109/IT4OD.2016.7479313

Mohan, P. H. (2020). Secure medical data transmission using a fusion of bit mask oriented genetic algorithm, encryption and steganography. *Future Generation Computer System*, *111*, 213–225. https://doi.org/10.1016/j.future.2020.04.034

Murillo-Escobar, M. A., Cruz-Hernández, C., Abundiz-Pérez, F., & López-Gutiérrez, R. M. (2016). Implementation of an improved chaotic encryption algorithm for real-time embedded systems by using a 32-bit microcontroller. *Microprocessors and Microsystems*, *45*, 297-309. https://doi.org/10.1016/j.micpro.2016.06.004

Pallaw, V. K., Singh, K. U., Kumar, A., Singh, T., Swarup, C., & Goswami, A. (2023). A robust medical image watermarking scheme based on nature-inspired optimization for telemedicine applications. *Electronics*, *12*(2), 334. https://doi.org/10.3390/electronics12020334

Roslan, R., & Jamil, N. (2012). Texture feature extraction using 2-D Gabor Filters. *International Symposium on Computer Applications and Industrial Electronics (ISCAIE)* (pp. 173-178). IEEE. https://doi.org/10.1109/ISCAIE.2012.6482091

Tertulino, R., Antunes, N., & Morais, H. (2022). Privacy in electronic health records: a systematic mapping study. *Journal of Public Health*, *32*, 435-454. https://doi.org/10.1007/s10389-022-01795-z

Tsou, C., Robinson, S., Boyd, J., Jamieson, A., Blakeman, R., Yeung, J., McDonnell, J., Waters, S., Bosich, K., & Hendrie, D. (2021). Effectiveness of telehealth in rural and remote emergency departments: systematic review. *Journal of Medical Internet Research*, *23*(11), e30632. https://doi: 10.2196/30632

Vaidya, S. P. (2022). Fingerprint-based robust medical image watermarking in hybrid transform. *The Visual Computer*, *39*, 2245-2260. https://doi.org/10.1007/s00371-022-02406-4

Wadood, A., Nafea, O., Ghouzali, S. (2020). Combining watermarking and hyper-chaotic map to enhance the security of stored biometric templates. *The Computer Journal*, *63*(3), 479-493. https://doi.org/10.1093/comjnl/bxz047

Ye, C., & Chen, C. (2022). Secure medical image sharing for smart healthcare system based on cellular neural network. *Complex Intelligent Systems*, *9*, 1653-1670. https://doi.org/10.1007/s40747-022-00881-9

Zulfiqar, A., Muhammad, I., Mansour, A., Tanveer, Z., Muhammad, S. (2018). A zero-watermarking algorithm for privacy protection in biomedical signals. *Future Generation Computer Systems*, *82*, 290-303. https://doi.org/10.1016/j.future.2017.12.007