International Journal of Intelligent Communication and Computer Science
Vol. 3, No. 1, 2025, Pages 72-86.

An Encrypted Watermarking For Secure Medical Image Sharing: An Overview

Vidisha Vishwakarma[1], Sunil Kumar Vishwakarma[1], Anshul Atre[1]

[1]Department of Computer Science & Engineering, Pranveer Singh Institute of Technology, Kanpur, (U.P.) India.

Review Paper

Email: vidvishwakarma2707@gmail.com

Received: 30 Apr 2025, Revised: 15 Jun. 2025 Accepted: 21 Jun. 2025

Abstract:
The investigation of various medical image datasets in order to arrive at a successful diagnosis for the afflicted patients is known as medical image processing. Patients' medical records are digitally saved as Electronic Patient Records (EPRs), which require the highest level of security and confidentiality because the patient's data will be connected to open, external platforms for future diagnosis. In order to successfully secure patient picture data, medical image watermarking and encryption approaches help to achieve the aforementioned standards. The goals of image encryption and compression are to simultaneously boost security and use less bandwidth. Patients' privacy must be secured due to the constantly increasing volume of medical digital images as well as the necessity of sharing them across hospitals and experts for improved and more precise diagnosis. This means that medical image watermarking (MIW) is required. Furthermore, in past few years, it was effectively utilized for medical image watermarking. The current study is to attempt a thorough brief to summarize articles on MIW evaluation with deep learning released in 2020–2023, since the majority of review works on the subject were completed prior to 2020. In addition to providing insights into the developments and potential avenues for upcoming research on deep learning for the analysis of MIW, this study contrasts deep learning with conventional machine learning.

Keywords: Medical image watermarking, encryption, Electronic Patient Records (EPRs), etc.

1. Introduction

With the advancement of digital healthcare systems and telemedicine, medical image processing has become an essential component in modern diagnostic workflows. The primary necessity of medical image processing techniques lies in their ability to enhance and analyse collected medical images efficiently, enabling accurate interpretation and diagnosis by automated systems or healthcare professionals [1]. However, as these images are increasingly transmitted across networks, especially in cloud-based or distributed healthcare environments, the challenge of securing sensitive medical data has become a major concern. The security of medical images must address not only confidentiality, but also integrity and authenticity, while simultaneously preventing unauthorized access and data manipulation during transmission between medical institutions [2]. A critical issue arises when manipulated or tampered medical data is sent to specialists for clinical evaluation. Such alterations, whether accidental or malicious can lead to misinterpretation, resulting in incorrect diagnoses and potentially life-threatening treatments. For example, Electronic Patient Records (EPRs) facilitate the transmission of medical images over public networks such as the Internet, which are inherently vulnerable to interception, tampering, or unauthorized access [3]. Therefore, achieving robust security during medical image transmission is imperative, and it requires a combination of multiple protective mechanisms. The three core security requirements for this purpose include confidentiality, data integrity, and authentication, as illustrated in Figure 1.

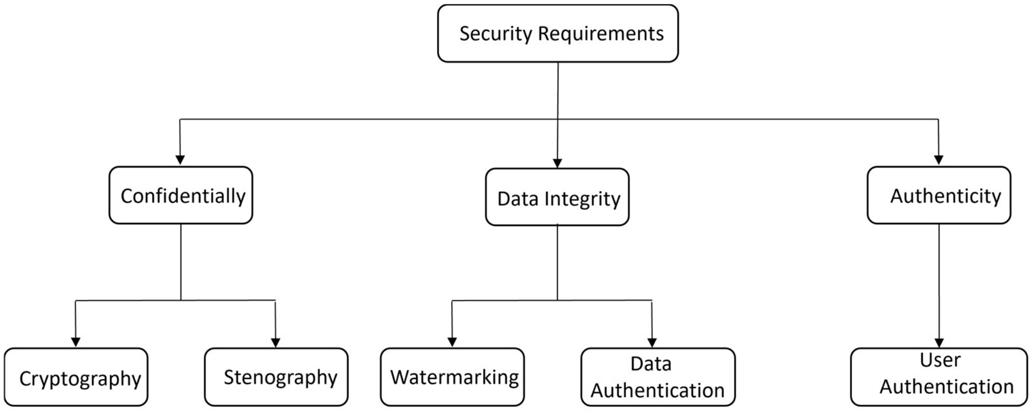

Figure 1: Security Requirements in transmission of medical images [4]

Confidentiality ensures that transmitted medical images remain inaccessible to unauthorized entities, including hackers and malicious users [4]. A commonly used approach to maintaining confidentiality is cryptography, which converts image data into an encrypted form that cannot be interpreted without the appropriate decryption key [5]. Cryptographic algorithms protect image content from eavesdropping or data leaks during network transmission.

Data integrity, on the other hand, ensures that the medical image received is exactly the same as the one sent, without any alteration or corruption during the communication process. One effective method for ensuring integrity is digital watermarking, which involves embedding imperceptible but verifiable information within the medical image [6]. These watermarks can serve as a checksum or proof of authenticity, enabling the detection of even the slightest modification. Advanced watermarking methods can also include authentication data, such as message authentication codes (MACs), which confirm that the image has not been tampered with.

Authentication plays a crucial role in verifying the identity of both the sender and the receiver during image transmission. It ensures that medical images originate from a trusted source and are delivered to the intended recipient without interception or impersonation. As discussed by Roseline and Oluwakemi [7], digital signatures are one of the most widely used techniques for authentication in secure communication. When integrated with watermarking and encryption, authentication forms a robust security framework that can withstand various cyber threats.

In this context, encrypted watermarking has emerged as a powerful hybrid approach for securing medical image sharing. It combines the strengths of cryptography and watermarking offering dual-layer protection where encryption ensures confidentiality and watermarking guarantees integrity and authenticity. This paper provides an overview of encrypted watermarking techniques, explores their roles in secure medical image transmission, and highlights current trends, challenges, and opportunities in this evolving field.

2. Encryption of Medical Images

In general, most attacks that occur during the transmission of medical images can be categorized into four types: interruption, interception, modification, and fabrication. Interruption attacks aim to damage or disrupt medical data, often through the use of malicious software or small viruses. Interception attacks focus on capturing sensitive medical information during transmission, typically through hidden malicious code embedded in certain free or pirated software. Modification attacks involve the intentional alteration of the contents of transmitted medical images, which can lead to incorrect diagnoses or treatments. Fabrication attacks result in the insertion of false or harmful data into the network, potentially misleading healthcare systems or professionals. Due to the critical implications of such attacks, there is a pressing need to develop advanced techniques that ensure the secure transmission of medical images [8–10].

To maintain high confidentiality, the transmitted medical data must be protected from unauthorized access. One of the most effective methods for achieving this is encryption, which ensures that the data remains unreadable to intruders. Consequently, the implementation of enhanced encryption algorithms is essential to fulfil the fundamental security requirements of confidentiality, integrity, and authenticity. Encryption techniques can generally be divided into two categories: symmetric key encryption and asymmetric (or public key) encryption. In symmetric encryption, the same key is used for both encrypting and decrypting the data. This method is known for its speed and efficiency, making it particularly suitable for large data types such as images. In contrast, asymmetric encryption uses a pair of keys one public and one private. While the public key is openly distributed for encryption, only the intended recipient holds the private key required for decryption. Although asymmetric encryption offers strong security, it is often less efficient for large-scale image data.

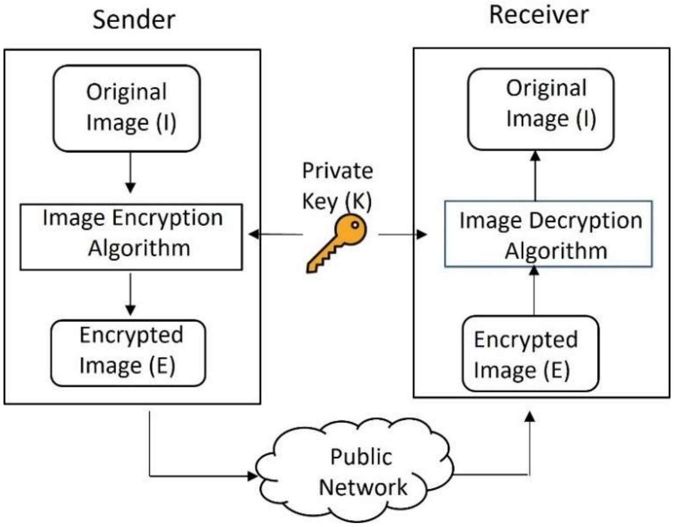

Figure 2: Image Encryption & Decryption Procedure [4]

Despite the availability of several symmetric and asymmetric encryption methods for securing digital content and textual data, symmetric encryption remains more suitable for image encryption due to its reliance on a single private key and lower computational complexity [11]. The process of encrypting and decrypting medical images can be understood through the following sequence: at the sender's end, the original image (denoted as I) is encrypted using a private key (K), resulting in an encrypted image (E). This encrypted image is then transmitted over public networks. At the receiver's end, the encrypted image (E) is decrypted using the same private key (K), allowing for the retrieval of the original image (I) through a corresponding decryption algorithm (Figure 2). This process ensures that the medical data remains protected and accessible only to authorized parties throughout its transmission.

3. Digital Image Watermarking

In recent years, the proliferation of digital media such as text, videos, images, and audio files on the internet has grown exponentially, transforming the world into a globally connected digital community. However, as digital processing systems increasingly integrate with the internet, multimedia content becomes highly vulnerable to security threats. Transmitted information can be altered, intercepted, or disseminated without prior authorization, posing serious challenges to data privacy and ownership. Common security threats include copyright infringement, unauthorized access, data theft, and illegal redistribution. According to the Institute for Policy Innovation (IPI), annual breaches involving movies, texts, audio, and software have resulted in significant copyright violations, financial losses, and job displacement.

To address these issues, digital image watermarking has emerged as an effective solution, offering a wide range of benefits in securing multimedia content. One of its key advantages lies in its ability to embed hidden data within digital images without compromising their semantic integrity. As such, digital watermarking plays a crucial role in enhancing multimedia security by ensuring content authenticity and ownership verification [12–13].

Typically, the digital image watermarking process involves three main phases: watermark generation, watermark embedding, and watermark detection. First, a watermark generator creates a unique watermark tailored to a specific application, often based on predefined keys. Next, the embedding phase incorporates this watermark into a cover image using embedding keys. Finally, in the detection phase, a decoder is used to extract and verify the watermark from the potentially altered image. By comparing the extracted watermark with the original, any tampering or unauthorized modification can be effectively identified.

The major benefits of digital image watermarking include improved data security and privacy, non-repudiation, controlled access, prevention of unauthorized duplication, and efficient usage of memory and bandwidth. Watermarking techniques are generally classified into three categories: robust, fragile, and semi-fragile watermarking. Each category serves different security and authentication needs, depending on the sensitivity and application of the media.

In the context of medical imaging, digital watermarking is especially important for preventing unauthorized access, ensuring diagnostic integrity, and protecting patient confidentiality. Contemporary digital watermarking approaches often employ domain transformation techniques such as the Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), and Discrete Wavelet Transform (DWT) for embedding and extracting watermarks with high precision and robustness [14].

Figure 3 presents a schematic block diagram of the medical image watermarking process. At the sender's end, an encoder embeds the watermark into the medical image to enhance both security and authentication. At the receiver's end, a decoder extracts the watermark from the received image. By comparing the extracted watermark with the original, it becomes possible to detect any tampering or unauthorized alterations to the image. To ensure both reliability and high image quality, the performance of the watermarking system is commonly evaluated based on perceptibility, which refers to the visual invisibility of the watermark in the image [15].

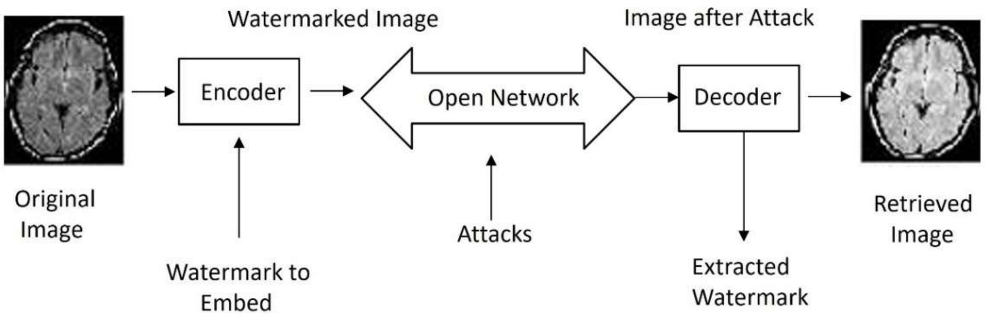

Figure 3: Digital Image Watermarking Procedure

4. Types of Watermarking

Watermarking can be broadly classified based on various criteria such as visibility, detection method, embedding domain, and the type of media being protected. The main types include visible and invisible watermarking, spatial domain and frequency domain watermarking, as well as detection-based types like blind, semi-blind, and non-blind watermarking. Additionally, watermarking techniques vary according to the type of content, including image, video, audio, and text watermarking (Figure 4). These classifications help select the most suitable approach depending on the application's needs for security, robustness, and imperceptibility, as detailed below.

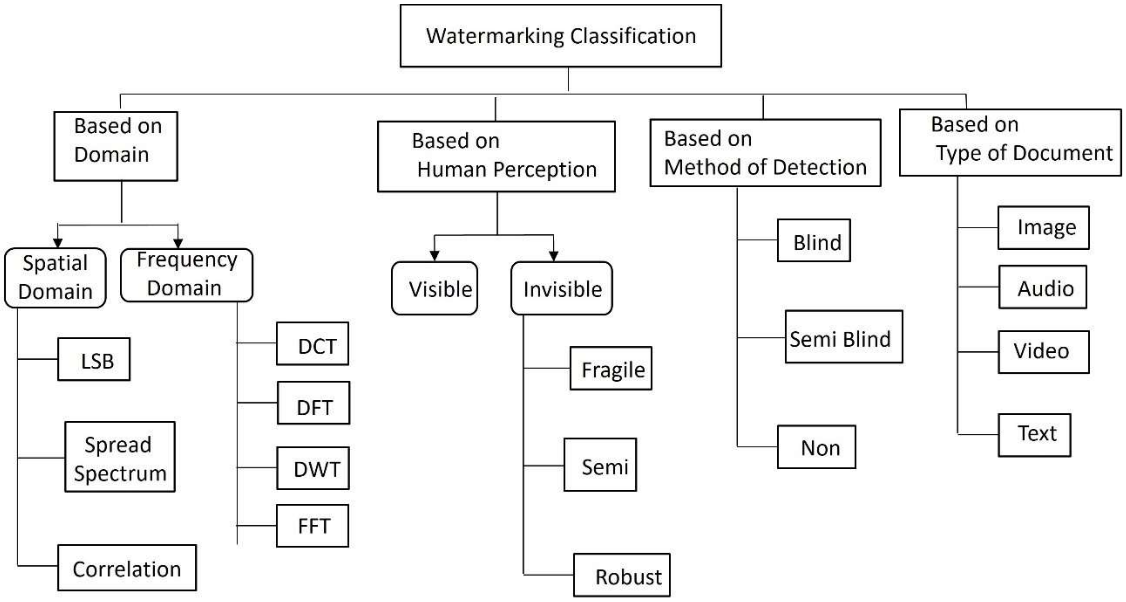

Figure 4: Classification of Watermarking Methods

4.1 Spatial Domain Watermarking

4.1.1 Least Significant Bit (LSB) Method

The Least Significant Bit (LSB) watermarking technique is one of the most basic spatial domain methods. It embeds watermark information by altering the least significant bits of selected pixels in the original image. This approach maintains high visual fidelity, as changes to LSBs are generally imperceptible to the human eye [16]. However, LSB watermarking is highly vulnerable to image compression, noise, filtering, and geometric transformations, which can easily destroy or remove the embedded watermark. Thus, it is typically used in applications where robustness is not the primary concern [17].

4.1.2 Correlation-Based Watermarking

Correlation-based watermarking techniques embed the watermark into the image such that it can later be detected using a correlation detector. In this method, the watermark signal is typically a pseudo-random sequence which is added directly to the image pixels in a predefined manner [18]. During detection, the presence of the watermark is confirmed by correlating the received image with the original watermark pattern. If the correlation exceeds a certain threshold, the watermark is deemed present. This method provides moderate robustness and security compared to LSB, as it is less sensitive to small distortions. However, its success depends on the correlation strength and the correct threshold selection [19].

4.1.3 Spread Spectrum (SS) Watermarking

Spread Spectrum watermarking improves robustness and security by spreading the watermark information across a wide range of spatial pixels using a pseudo-random noise pattern [20]. This technique is inspired by communication systems where the signal is spread over a broader bandwidth. In image watermarking, it ensures that even if parts of the image are altered or removed, the watermark can still be detected. Spread spectrum methods are more resilient to common image processing attacks and are difficult to detect or remove without the appropriate key, making them suitable for higher-security applications [21].

4.2 Frequency (Transform) Domain Watermarking

4.2.1 Discrete Cosine Transform (DCT)

The DCT is a popular frequency domain method that converts spatial pixel values into frequency components. It is typically applied block-wise (e.g., 8×8) to the image [22]. Watermarks are embedded in the mid-frequency coefficients, balancing imperceptibility and robustness. Modifying low-frequency components can significantly degrade image quality, while high-frequency components are prone to loss during compression [23]. DCT-based watermarking is widely used in compressed image formats such as JPEG and is effective against lossy compression and minor manipulations.

4.2.2 Discrete Fourier Transform (DFT)

The DFT represents an image in terms of its global frequency characteristics. Watermarking with DFT typically involves modifying the magnitude or phase components of the transform domain. It offers strong resilience against geometric attacks like rotation, scaling, and translation, as such transformations affect the spatial domain more than the frequency magnitude [24]. Though DFT is computationally intensive, its robustness makes it suitable for high-security applications, including document authentication and copyright protection [25].

4.2.3 Discrete Wavelet Transform (DWT)

The DWT provides a multi-resolution representation of an image, dividing it into various sub-bands (LL, LH, HL, HH) corresponding to different frequency ranges [26]. Watermarks are often embedded into the higher-frequency sub-bands to maintain imperceptibility, or in lower-frequency bands for improved robustness. DWT is particularly useful in medical imaging applications due to its ability to preserve critical diagnostic information while ensuring secure watermark embedding [27]. Its layered decomposition also makes it highly adaptable for hierarchical and scalable watermarking.

4.2.4 Fast Fourier Transform (FFT)

The FFT is a computationally efficient algorithm for performing the DFT. It retains the core benefits of DFTs robustness to geometric and signal-based attacks, while significantly reducing processing time. FFT is suitable for real-time watermarking and high-resolution image scenarios where performance and scalability are essential [28]. Like DFT, FFT-based watermarking embeds data in the frequency domain, making it harder for attackers to detect or tamper with the watermark without altering the image noticeably [29].

4.3 Watermarking Based on Human Perception

Digital watermarking techniques that leverage human perception are broadly classified into two categories: visible and invisible watermarking. These classifications are based on the perceptibility of the watermark to the Human Visual System (HVS).

4.3.1 Visible Watermarking

Visible watermarking refers to the deliberate embedding of logos, text, or patterns onto the visible part of an image. These watermarks are clearly perceptible to human viewers and are typically placed in a prominent location within the image, such as a corner or center, to declare ownership or assert copyright. Commonly used in digital photography, broadcasting, and online image sharing, visible watermarks serve as a deterrent against unauthorized use or reproduction. Although they are easily noticed, visible watermarks must still be carefully designed to avoid obstructing critical content in the image, especially in sensitive domains like medical imaging. The challenge lies in achieving an optimal balance between visibility, aesthetic quality, and tamper resistance.

4.3.2 Invisible Watermarking

Invisible watermarking involves embedding watermark data into the image in a manner that is imperceptible to the human eye but can be detected or extracted through computational methods. These watermarks are typically used for copyright protection, authentication, and data integrity verification. Invisible watermarking techniques take advantage of the HVS by embedding data in areas where visual sensitivity is low, such as high-frequency regions or textured areas of the image. Advanced algorithms also incorporate perceptual models that consider luminance masking, contrast sensitivity, and texture masking to maintain the image's visual fidelity. Invisible watermarking is widely applied in scenarios where preserving the image quality is critical, such as in medical imaging, legal evidence, or confidential document exchange, while still maintaining a hidden layer of security.

Both visible and invisible watermarking methods play crucial roles in digital rights management and secure multimedia distribution. While visible watermarking emphasizes public attribution and deterrence, invisible watermarking focuses on covert protection and forensic tracking without altering the visual experience. The choice between the two depends on the application context and the required trade-off between perceptibility, robustness, and security [30].

4.4 Watermarking Based on the Method of Detection

Digital watermarking techniques can also be classified based on the method used to detect or extract the watermark from the watermarked image. This classification affects the system's complexity, security, and practicality in real-world applications. The three main categories under this approach are: Blind, Semi-Blind, and Non-Blind watermarking.

4.4.1 Blind Watermarking (Oblivious Detection)

Blind watermarking refers to techniques in which the watermark can be detected or extracted without requiring access to the original (unwatermarked) image. This method is highly practical, especially in real-time or large-scale applications, since storing or accessing the original image during detection is not necessary [31]. Blind detection is ideal for applications like copyright enforcement, content tracking, and authentication in decentralized systems. However, designing blind watermarking schemes that are both robust (resistant to attacks) and imperceptible (not visible) is more challenging, as the extraction must rely solely on the information present in the watermarked image.

4.4.2 Semi-Blind Watermarking

Semi-blind watermarking requires partial information about the original content for watermark detection. This may include a secret key, watermark sequence, or some feature of the original image, but not the complete image itself [32]. It offers a compromise between robustness and practicality, less complex than non-blind methods and more accurate than blind methods. Semi-blind detection methods are useful in authentication systems where the watermark needs to be validated using reference data (like a hash or template) but storing the entire original image is impractical due to memory or bandwidth limitations.

4.4.3 Non-Blind Watermarking (Informed Detection)

Non-blind watermarking, also known as informed detection, requires full access to the original image during the watermark extraction process. This approach allows for more accurate and reliable watermark detection, especially in the presence of distortions, as the detector can directly compare the watermarked image with the original [33]. Non-blind watermarking is commonly used in controlled environments such as medical imaging, secure digital archiving, and legal evidence management, where the original data is available and verification accuracy is critical. However, its dependence on the original image makes it less suitable for scenarios involving large-scale distribution or remote verification.

4.5 Watermarking Based on the Type of Document

Digital watermarking techniques are tailored according to the nature of the content being protected. The type of media, whether it is an image, video, audio, or text—significantly influences the choice of embedding strategy, robustness requirements, and perceptual constraints. The following are the common classifications based on the type of document:

4.5.1 Image Watermarking

Image watermarking involves embedding watermark data into still images. This is one of the most researched areas in digital watermarking due to the widespread use of digital images across the internet, especially in medical imaging, digital photography, and media [34]. Watermarks can be embedded in the spatial domain (e.g., LSB, correlation-based) or frequency domain (e.g., DCT, DWT, DFT). Image watermarking must ensure high imperceptibility and robustness against operations like compression, cropping, resizing, and filtering. Applications include copyright protection, medical image security, and image authentication.

4.5.2 Video Watermarking

Video watermarking extends image watermarking techniques to temporal data. A video is essentially a sequence of image frames, often accompanied by audio [35]. Watermarking in video can be done frame-by-frame or by using temporal characteristics like motion vectors or scene changes. Frequency-domain techniques (like DWT-DCT hybrids) are frequently used for robustness. Video watermarking must meet stricter requirements for real-time processing, synchronization, and resilience to compression (e.g., MPEG), frame dropping, temporal scaling, and re-encoding. It is commonly applied in broadcast monitoring, digital cinema, surveillance, and streaming media protection.

4.5.3 Audio Watermarking

Audio watermarking focuses on embedding data into digital audio signals such as speech, music, or sound recordings. The watermark must be inaudible to human listeners while remaining robust against common audio transformations like compression (e.g., MP3), filtering, and noise addition. Techniques typically use time domain (e.g., echo hiding, phase coding) or frequency domain (e.g., FFT, DCT, wavelet transforms) [36]. Psychoacoustic models are often employed to exploit the limitations of the Human Auditory System (HAS) for perceptual transparency. Applications include music rights management, audio fingerprinting, and broadcast tracking.

4.5.4 Text Watermarking

Text watermarking is more challenging due to the discrete and limited redundancy in text documents. Unlike images or audio, where small changes can be imperceptible, even minor alterations in text can be easily noticeable or disrupt semantics. Text watermarking techniques include formatting-based methods (e.g., altering spacing, font, or punctuation), syntactic methods (rephrasing sentences), and semantic methods (replacing synonyms without changing meaning) [37]. The goal is to embed information without affecting readability or content integrity. Applications include document authentication, plagiarism detection, and copyright protection of digital manuscripts or e-books.

Each type of document presents unique challenges for watermarking, and the techniques must be adapted accordingly to ensure imperceptibility, robustness, security, and efficiency. The choice of approach is highly dependent on the media's perceptual characteristics and the intended application domain.

5. Digital Image Watermarking System Requirements

For particular objectives, like in medical applications, few other characteristics like imperceptibility and reversibility should be included and it is completely explained in medical segment.

Fidelity: This metric decides similarity amongst the watermarked and non-watermarked image. Otherwise said, fidelity refers to the degree of invisibility of the watermark present in the watermarked image.

Robustness: In contrary to fragile watermarking, robustness indicates the resilience against different nondeliberate and unauthorized attacks. Cropping, resizing, and compression are instances of unintentional attacks, which may occur generally during the processing of a digital image. Noise inclusion and geometrical distortion constitute the two examples of intrusive attacks, which may be utilized by attackers for removing the watermark.

Data Payload (Capacity): it his aspect depicts maximum amount of data, which can be inserted into an image with no significant reduction in the image quality. The effect of capacity on robustness and perceptibility of watermarked image is very important; for example, when the data payload is increased, the robustness will reduce and the perceptibility will improve. The dimensions of the host image must also take into consideration, due to the fact that the more the image resolution, the higher the degree of watermark is suitable in terms of bits [38].

Security: This metric is associated with the usage of various types of keys, like public or private, such that unauthenticated individuals cannot compromise the watermark.

Computational Complexity (Speed): This measure is associated with the computation time taken to embed and extract the watermark, which directly decides the computational complexity. For instance, real-time application needs rapid techniques. But, for higher-security applications, time consumption of embedding as well as extracting techniques are generally high.

Perceptibility: This metric is associated with the degree of distortion appearing on watermarked image once a watermark is inserted. In the case of imperceptible watermarks, this metric must be a minimal value.

6. Applications of Digital Watermarking System

Watermarking approaches are application based. Various techniques show diverse constraints and criteria. Below is a list of a few uses:

Copyright Protection: This application claims that the digital image clearly incorporates the owner's copyright information, and it may be extracted to demonstrate ownership in the event of an infringement. To do this, the watermark has to be resistant to both approved and illegal assaults. It is not appropriate to apply this kind of watermark to prevent users from duplicating the digital image.

Fingerprinting: The creator of this program should add various watermarks according to each user's identification. It implies that the data, which are utilized in the form of a watermark, will be selected as per the information of the client. This method makes it easier for the proprietor to identify the origin of illicit copies and quickly apprehend users who break licensing agreements. Additionally, this watermark ought to be trustworthy and undetectable.

Authentication as well as Integrity Verification:

This application's goal is to determine whether or not the digital picture has been altered, and if so, to identify the location of the alteration. Fragile or semi-fragile watermarking methods, which are unreliable against content changes, must be utilized in this application. Digital picture watermarking may also be used for clandestine communication, content description, even broadcast monitoring.

7. Issues In Encryption, and Digital Watermarking of Medical Images

All the existing image encryption techniques do not ensure complete robustness towards digital watermarks in encryption domains. In case of few of these image encryption approaches, the extraction of watermarks could be carried out after embedding the watermarks. However, owing to the presence of numerous interferences like Gaussian noise, median filtering, rotations, etc., the quality of the watermarks become poorer, therefore the robustness of the watermarks could not be assured [39, 40]. Considering plaintext domains, even though numerous effective digital image watermarking approaches were formulated, owing to the restrictions in the encryption techniques, transplanting these effective digital image watermarking approaches directly to the encryption domains become little tedious task especially when processing medical images as these medical image security applications need specific requirements. Imperceptibility is considered as one of the major concerns while processing medical images using digital image watermarking techniques. In many applications, altering the medical images after embedding watermarks is not permitted. Imperceptibility could be attained by picking the Region of non-interest (RNOI) watermarking, where the watermarks are inserted in the medical images' RNOI region. Moreover, imperceptibility could be attained with the help of reversible watermarking approaches that assist in recovering the original medical images by performing the reverse operation of watermark embedding mechanism at receiver end. At receiver end, it must be able to easily extract the original medical images as well as embedded watermarks. This property which is commonly referred as reversibility of medical image watermarking has to be seriously encountered. Moreover, for enabling e-treatment, most of the medical images were transmitted via internet so as to accomplish remote diagnosis. In these cases, transmission speed has a serious impact, therefore the chosen algorithm must be of reduced complexity for minimizing the execution time.

8. Recent Notable Works

E-healthcare applications are increasingly vulnerable to various cyberattacks, which may lead to severe consequences including unauthorized data access, manipulation, or loss of sensitive medical information. These threats undermine the security, confidentiality, and integrity of electronic health records and transmitted medical images.

Hosny et al. (2024) presented an in-depth survey on digital image watermarking using deep learning techniques, outlining recent advancements and applications in securing visual data [41]. The study categorized various deep learning-based watermarking approaches into supervised, unsupervised, and generative models, highlighting their effectiveness in terms of robustness, imperceptibility, and capacity. The authors noted that deep neural networks (DNNs), especially convolutional neural networks (CNNs) and autoencoders**,** have shown promising results in embedding and extracting watermarks under a variety of attacks. Their work emphasized the growing potential of AI-powered watermarking in adapting to increasingly complex threats in multimedia security.

Sharma et al. (2024) conducted a comprehensive review on the use of image watermarking for identity protection and verification**,** particularly in the context of biometric and personal data [42]. Their study focused on how watermarking techniques are integrated into identity authentication systems to prevent spoofing, tampering, and identity theft. The paper examined domain-specific methods such as DWT-SVD and hybrid transform-based watermarking, and assessed their performance in terms of fidelity, security, and real-time processing capabilities. This work reinforces the critical role of watermarking in safeguarding identity within secure access systems and digital identification platforms.

Yang et al. (2025) explored a novel frontier in watermarking its application in large language models (LLMs)**.** Their survey discussed the design and implementation of watermarking strategies for protecting and tracing outputs generated by LLMs, such as GPT-style models [43]. Key methods reviewed include prompt-level watermarking, output perturbation, and probabilistic watermarking for text generation. The study highlighted the importance of such techniques in intellectual property protection, content authenticity, and misinformation control, especially in an era where AI-generated content is widely disseminated.

Ye et al. (2025) proposed a periodic watermarking scheme for copyright protection of LLMs within cloud computing environments [44]. Their approach embeds periodic watermarks directly into the output patterns of language models, allowing for efficient tracking of model usage and protection against unauthorized distribution. The study also introduced a detection framework that uses periodic signature analysis for watermark verification, even under adversarial transformations. This method enhances cloud security by enabling copyright holders to prove ownership and monitor model misuse without compromising performance.

Ye et al. (2025) also introduced a hybrid security framework for social image protection**,** combining encryption and watermarking across multiple domains [45]. Their method employs multi-domain watermarking**,** embedding data in both spatial and transform domains while concurrently encrypting the image to ensure end-to-end confidentiality. This dual-layer approach enhances protection against unauthorized sharing, tampering, and reverse engineering in social media contexts. Their research demonstrates how combining cryptographic encryption with robust watermarking significantly strengthens data security in publicly shared digital content.

Wandile et al. (2025) developed a compact and secure image encryption model tailored for IoT-based medical systems**,** combining Elliptic Curve Cryptography (ECC) with Advanced Encryption Standard (AES) [46]. Their hybrid cryptographic approach ensures a strong balance between lightweight processing and robust encryption, which is critical for resource-constrained environments like IoT healthcare devices. The proposed scheme showed notable improvements in execution speed and energy efficiency while maintaining high levels of image confidentiality and integrity. The model is particularly useful in e-health applications where real-time encryption of sensitive medical images is required.

Pandey and Sharma (2025) introduced a novel encryption-validation mechanism based on ECC for medical images, enhanced with genetic algorithms for embedding watermark data in the low-frequency region of the image spectrum [47]. This method not only secures the image through strong encryption but also integrates a validation process to verify authenticity. By targeting low-frequency regions, the embedded watermark remains resilient against common image processing operations such as compression and filtering. Their approach provides a dual-layer defense system that ensures both security and **v**alidation of transmitted medical content.

El-Rahman et al. (2025) proposed C-HIDE, a steganographic and encryption framework that introduces a coverless hybrid image encryption scheme using ECC and AES to ensure enhanced data hiding and confidentiality [48]. Unlike conventional watermarking, C-HIDE focuses on robust steganography**,** eliminating the need for a visible or detectable cover medium. The system supports high payload capacity and security through an advanced hybrid cryptographic model, making it ideal for embedding sensitive patient information within medical images in telemedicine and cloud-based healthcare systems.

Chaouch et al. (2025) addressed image security in cloud computing environments by developing a hybrid encryption technique that combines ECC with spatiotemporal cryptography [49]. Their model introduces dynamic temporal encryption parameters, increasing resistance to known-plaintext and chosen-ciphertext attacks. The approach enhances data protection during storage and transmission of medical images in distributed cloud networks. The use of ECC ensures computational efficiency, while spatiotemporal scrambling adds an additional layer of unpredictability and resilience, making this method highly applicable to modern e-health infrastructures.

9. Performance Metrics Analysis

Peak Signal to Noise Ratio (PSNR): It is the highest power to noise distortion image representation ratio, or peak signal to noise ratio (PSNR). Typically, PSNR is presented using a decibel scale. A common metric for assessing image quality is PSNR. The original data in this case is the signal, while the error is the noise. Higher PSNR displays higher image quality. PSNR is most easily defined via the mean squared error is provided in equation (1).

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left[I\left(i,j\right)-K\left(i,j\right)\right]^2 \quad (1)$$

The PSNR (in dB) shall be defined using equation (2).

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

The original, watermarked images are I and K respectively.

Compression Ratio (CR): The compression ratio refers to the proportion between the size of the original image and the size of the compressed image. It indicates how effectively an image compression algorithm reduces data. A higher compression ratio means more data reduction, resulting in smaller file sizes, which is especially important for storing and transmitting large medical images. However, care must be taken to maintain image quality, especially in medical applications where diagnostic accuracy is critical.

CR= Original Image in bytes/ Compressed Image in bytes (3)

Normalized Correlation (NC): is a metric used to evaluate the similarity between the extracted watermark from a compromised or distorted image and the original watermark. It measures how closely the retrieved watermark matches the original, with values typically ranging from 0 to 1. A value closer to 1 indicates high similarity, implying that the watermarking technique is robust against attacks or distortions. This makes NC a crucial parameter in assessing the reliability and effectiveness of digital watermarking systems.

$$NC = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}\left(I\left(i,j\right)*K\left(i,j\right)\right)}{\sum_{i=1}^{m}\sum_{j=1}^{n}I\left(i,j\right)^2} \quad (4)$$

Embedding Capacity (EC): Embedding Capacity refers to the amount of data that can be embedded within an image without significantly degrading its quality. It is commonly measured in bits per pixel (bpp), indicating how many bits of watermark or hidden data are stored in each pixel of the host image. A higher embedding capacity allows for more information to be embedded, but it must be balanced with imperceptibility and robustness to ensure that the watermark remains invisible and resistant to attacks.

$$Capacity = \frac{|m|}{|A|} \quad (5)$$

Where, m is the message that is embedded in cover image.

Structural Similarity Index Measure (SSIM): The calculation of the structural similarity index tests the similarity to structures and compares normal luminance and contrast patterns in local pixel intensities. The concept behind this quality assessment is that the visual system is good for the collection of structural details. Structural awareness is the concept of strong interdependence in the pixels, particularly when near the space. These dependencies provide valuable information on the organization of the visual scene components. Several windows of an image are used to compute the structural similarity (SSIM) measure. The range of its value is [0, 1]. Equation (6) is used to represent the measure across two windows of common size N×N.

$$SSIM\left(x,y\right)=\frac{\left(2*\mu_x*\mu_y+C_1\right)\left(2*\sigma_{xy}+C_2\right)}{\left(\mu_x^2+\mu_y^2+C_1\right)\left(\sigma_x^2+\sigma_y^2+C_2\right)} \tag{6}$$

where, μ_x - An average of x, μ_y - An average of y , σ_x^2 - A variance of x, σ_y^2 - A variance of y and σ_{xy} - A covariance of x as well as y. $C_1=\left(k_1 L\right)^2, C_2=\left(k_2 L\right)^2$ represents the two variables that maintain the weak denominator division. L is the pixel-values' dynamic range and K_1 =0.010 and k_2 =0.030, the standard value.

10. Conclusion

With the increasing use of digital communication in healthcare, especially through telemedicine, teleradiology, remote diagnosis, and virtual consultations, ensuring the security, authenticity, and integrity of medical images has become more important than ever. To meet these growing demands, researchers have proposed various medical image watermarking techniques, each offering certain advantages while also facing specific limitations. In this study, we presented a detailed overview of medical image watermarking methods, emphasizing their fundamental concepts, practical challenges, and real-world applications. We discussed the basic structure of watermarking systems, explained where digital watermarks are typically embedded within medical images, and outlined key requirements such as robustness, invisibility, and embedding capacity. Additionally, we explored common threats and evaluated how different techniques can protect against them. This review aims to guide future research and development in building secure and reliable systems for medical image protection in modern healthcare environments.

References

1. Li, Xiang, Yuchen Jiang, Juan J. Rodriguez-Andina, Hao Luo, Shen Yin, and Okyay Kaynak. "When medical images meet generative adversarial network: recent development and research opportunities." *Discover Artificial Intelligence* 1 (2021): 1-20.
2. Chen, Yung-Yao, Yu-Chen Hu, Hsiang-Yun Kao, and Yu-Hsiu Lin. "Security for eHealth system: data hiding in AMBTC compressed images via gradient-based coding." *Complex & Intelligent Systems* 9, no. 3 (2023): 2699-2711.
3. Kruse, Clemens Scott, Brenna Smith, Hannah Vanderlinden, and Alexandra Nealand. "Security techniques for the electronic health records." *Journal of medical systems* 41 (2017): 1-9.
4. Masood, Fawad, Maha Driss, Wadii Boulila, Jawad Ahmad, Sadaqat Ur Rehman, Sana Ullah Jan, Abdullah Qayyum, and William J. Buchanan. "A lightweight chaos-based medical image encryption scheme using random shuffling and XOR operations." *Wireless personal communications* 127, no. 2 (2022): 1405-1432.
5. Elamir, Mona M., Walid I. Al-atabany, and Mai S. Mabrouk. "Hybrid image encryption scheme for secure E-health systems." *Network Modeling Analysis in Health Informatics and Bioinformatics* 10, no. 1 (2021): 35.
6. Gao, Hang, and Tiegang Gao. "A secure lossless recovery for medical images based on image encoding and data self-embedding." *Cluster Computing* 25, no. 1 (2022): 707-725.

7. Ogundokun, Roseline Oluwaseun, and Oluwakemi Christiana Abikoye. "A safe and secured medical textual information using an improved LSB image steganography." *International Journal of Digital Multimedia Broadcasting* 2021, no. 1 (2021): 8827055.
8. Thanki, Rohit, and Ashish Kothari. "Multi-level security of medical images based on encryption and watermarking for telemedicine applications." *Multimedia tools and applications* 80, no. 3 (2021): 4307-4325.
9. Priya, S., and B. Santhi. "A novel visual medical image encryption for secure transmission of authenticated watermarked medical images." *Mobile networks and applications* 26, no. 6 (2021): 2501-2508.
10. Kumar, Manish, and Prateek Gupta. "A new medical image encryption algorithm based on the 1D logistic map associated with pseudo-random numbers." *Multimedia Tools and Applications* 80, no. 12 (2021): 18941-18967.
11. Li, Jian, Zelin Zhang, Shengyu Li, Ryan Benton, Yulong Huang, Mohan Vamsi Kasukurthi, Dongqi Li et al. "A partial encryption algorithm for medical images based on quick response code and reversible data hiding technology." *BMC Medical Informatics and Decision Making* 20 (2020): 1-16.
12. Vaidya, S. Prasanth, and V. Ravi Kishore. "Adaptive medical image watermarking system for e-health care applications." *SN Computer Science* 3, no. 2 (2022): 107.
13. Zermi, Narima, Amine Khaldi, Med Redouane Kafi, Fares Kahlessenane, and Salah Euschi. "A lossless DWT-SVD domain watermarking for medical information security." *Multimedia Tools and Applications* 80 (2021): 24823-24841.
14. Soualmi, Abdallah, Adel Alti, and Lamri Laouamer. "A new blind medical image watermarking based on weber descriptors and Arnold chaotic map." *Arabian Journal for Science and Engineering* 43, no. 12 (2018): 7893-7905.
15. Wee, Tan Chi, Mohd Shafry Mohd Rahim, Gloria Jennis Tan, Ghazali Sulong, and Chaw Jun Kit. "High imperceptibility medical image watermarking scheme based on Slantlet transform by using dynamic visibility threshold." In *2020 6th International Conference on Interactive Digital Media (ICIDM)*, pp. 1-5. IEEE, 2020.
16. Bansal, Kriti, Aman Agrawal, and Nency Bansal. "A survey on steganography using least significant bit (lsb) embedding approach." In *2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184)*, pp. 64-69. IEEE, 2020.
17. Tseng, Hsien-Wen, and Hui-Shih Leng. "A reversible modified least significant bit (LSB) matching revisited method." *Signal Processing: Image Communication* 101 (2022): 116556.
18. Ahmed, Farid, and Ira S. Moskowitz. "Correlation-based watermarking method for image authentication applications." *Optical Engineering* 43, no. 8 (2004): 1833-1838.
19. Ejima, Masataka, and Akio Miyazaki. "An analysis of correlation-based watermarking systems." *Electronics and Communications in Japan (Part III: Fundamental Electronic Science)* 86, no. 11 (2003): 1-12.
20. Xiang, Yong, Iynkaran Natgunanathan, Yue Rong, and Song Guo. "Spread spectrum-based high embedding capacity watermarking method for audio signals." *IEEE/ACM transactions on audio, speech, and language processing* 23, no. 12 (2015): 2228-2237.
21. Maity, Santi P., and Malay K. Kundu. "Performance improvement in spread spectrum image watermarking using wavelets." *International Journal of Wavelets, Multiresolution and Information Processing* 9, no. 01 (2011): 1-33.
22. Alotaibi, Reem A., and Lamiaa A. Elrefaei. "Text-image watermarking based on integer wavelet transform (IWT) and discrete cosine transform (DCT)." *Applied Computing and Informatics* 15, no. 2 (2019): 191-202.
23. Alomoush, Waleed, Osama A. Khashan, Ayat Alrosan, Hani H. Attar, Ammar Almomani, Fuad Alhosban, and Sharif Naser Makhadmeh. "Digital image watermarking using discrete cosine transformation based linear modulation." *Journal of Cloud Computing* 12, no. 1 (2023): 96.
24. Zhang, Xueting, Qingtang Su, Zihan Yuan, and Decheng Liu. "An efficient blind color image watermarking algorithm in spatial domain combining discrete Fourier transform." *Optik* 219 (2020): 165272.
25. Solikhin, Mukhammad, Yohanssen Pratama, Purnama Pasaribu, Josua Rumahorbo, and Bona Simanullang. "Analisis Watermarking Menggunakan Metode Discrete Cosine Transform (DCT) dan Discrete Fourier Transform (DFT)." *Jurnal Sistem Cerdas* 5, no. 3 (2022): 155-170.

26. Kashyap, Nikita, and G. R. Sinha. "Image watermarking using 3-level discrete wavelet transform (DWT)." *International Journal of Modern Education and Computer Science* 4, no. 3 (2012): 50.
27. Barnouti, Nawaf Hazim, Zaid Saeb Sabri, and Khaldoun L. Hameed. "Digital watermarking based on DWT (discrete wavelet transform) and DCT (discrete cosine transform)." *International Journal of Engineering & Technology* 7, no. 4 (2018): 4825-4829.
28. Dhar, Pranab Kumar, and Jong-Myon Kim. "Digital watermarking scheme based on fast Fourier transformation for audio copyright protection." *International Journal of Security and Its Applications* 5, no. 2 (2011): 33-48.
29. Pourhashemi, Seyed Mostafa, Mohammad Mosleh, and Yousof Erfani. "Audio watermarking based on synergy between Lucas regular sequence and Fast Fourier Transform." *Multimedia Tools and Applications* 78, no. 16 (2019): 22883-22908.
30. Wang, Qingzhu, Xiaoming Chen, Mengying Wei, and Zhuang Miao. "Simultaneous encryption and compression of medical images based on optimized tensor compressed sensing with 3D Lorenz." *Biomedical engineering online* 15 (2016): 1-20.
31. Eggers, Joachim J., and Bernd Girod. "Blind watermarking applied to image authentication." In *2001 IEEE International Conference on Acoustics, Speech, and Signal Processing. Proceedings (Cat. No. 01CH37221)*, vol. 3, pp. 1977-1980. IEEE, 2001.
32. PVSSR, Chandra Mouli. "A robust semi-blind watermarking for color images based on multiple decompositions." *Multimedia Tools and Applications* 76, no. 24 (2017): 25623-25656.
33. Houmansadr, Amir, Negar Kiyavash, and Nikita Borisov. "Non-blind watermarking of network flows." *IEEE/ACM Transactions on Networking* 22, no. 4 (2013): 1232-1244.
34. Begum, Mahbuba, and Mohammad Shorif Uddin. "Digital image watermarking techniques: a review." *Information* 11, no. 2 (2020): 110.
35. Asikuzzaman, Md, and Mark R. Pickering. "An overview of digital video watermarking." *IEEE Transactions on Circuits and Systems for Video Technology* 28, no. 9 (2017): 2131-2153.
36. Hua, Guang, Jiwu Huang, Yun Q. Shi, Jonathan Goh, and Vrizlynn LL Thing. "Twenty years of digital audio watermarking—a comprehensive review." *Signal processing* 128 (2016): 222-242.
37. Kamaruddin, Nurul Shamimi, Amirrudin Kamsin, Lip Yee Por, and Hameedur Rahman. "A review of text watermarking: theory, methods, and applications." *IEEE Access* 6 (2018): 8011-8028.
38. Jabade, Vaishali S., and Sachin R. Gengaje. "Literature review of wavelet based digital image watermarking techniques." *International Journal of Computer Applications* 31, no. 7 (2011): 28-35.
39. Bhardwaj, Rupali, and Ashutosh Aggarwal. "Hiding clinical information in medical images: an enhanced encrypted reversible data hiding algorithm grounded on hierarchical absolute moment block truncation coding." *Multidimensional Systems and Signal Processing* 31, no. 3 (2020): 1051-1074.
40. Ahmed, Saja Theab, Dalal Abdulmohsin Hammood, Raad Farhood Chisab, Ali Al-Naji, and Javaan Chahl. "Medical image encryption: a comprehensive review." *Computers* 12, no. 8 (2023): 160.
41. Hosny, Khalid M., Amal Magdi, Osama ElKomy, and Hanaa M. Hamza. "Digital image watermarking using deep learning: A survey." *Computer Science Review* 53 (2024): 100662.
42. Sharma, Sunpreet, Ju Jia Zou, Gu Fang, Pancham Shukla, and Weidong Cai. "A review of image watermarking for identity protection and verification." *Multimedia Tools and Applications* 83, no. 11 (2024): 31829-31891.
43. Yang, Zhiguang, Gejian Zhao, and Hanzhou Wu. "Watermarking for large language models: A survey." *Mathematics* 13, no. 9 (2025): 1420.
44. Ye, Pei-Gen, Zhengdao Li, Zuopeng Yang, Pengyu Chen, Zhenxin Zhang, Ning Li, and Jun Zheng. "Periodic watermarking for copyright protection of large language models in cloud computing security." *Computer Standards & Interfaces* 94 (2025): 103983.
45. Ye, Conghuan, Shenglong Tan, Jun Wang, Li Shi, Qiankun Zuo, and Wei Feng. "Social image security with encryption and watermarking in hybrid domains." *Entropy* 27, no. 3 (2025): 276.
46. Wandile, Piyush S., Bhupendra Singh Kirar, Saurabh Jain, and Yatendra Sahu. "Compact and Secure Image Encryption for IoT Systems Employing ECC and AES Hybrid Cryptography." In *2025 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS)*, pp. 1-6. IEEE, 2025.
47. Pandey, Kartikey, and Deepmala Sharma. "Digital image encryption with validation by ECC and embedding at low frequency region using the genetic approach." *International Journal of Electronics and Telecommunications* (2025): 87-93.

48. El-Rahman, Sahar A., Ahmed E. Mansour, Leila Jamel, Manal Abdullah Alohali, Mohamed Seifeldin, and Yasmin Alkady. "C-HIDE: A Steganographic Framework for Robust Data Hiding and Advanced Security Using Coverless Hybrid Image Encryption With AES and ECC." *IEEE Access* 13 (2025): 41367-41381.
49. Chaouch, Ismehene, Anis Naanaa, and Sadok El Asmi. "Enhanced Image Security in Cloud Computing Using Hybrid Encryption with ECC and Spatiotemporal Cryptography." In *International Conference on Advanced Information Networking and Applications*, pp. 175-187. Cham: Springer Nature Switzerland, 2025.