Intelligent Automation & Soft Computing

Tech Science Press

DOI: 10.32604/iasc.2024.057013

ARTICLE

Secure Digital Image Watermarking Technique Based on ResNet-50 Architecture

Satya Narayan Das[1,2,*] and Mrutyunjaya Panda[2,*]

[1]Department of Computer Science and Engineering, GIET University, Gunupur, Odisha, 765022, India

[2]Department of Computer Science and Applications, Utkal University, Bhubaneswar, Odisha, 751004, India

*Corresponding Authors: Satya Narayan Das. Email: sndas@giet.edu;
Mrutyunjaya Panda. Email: mrutyunjaya.cs@utkaluniversity.ac.in

Received: 05 August 2024 Accepted: 18 October 2024 Published: 30 December 2024

ABSTRACT

In today's world of massive data and interconnected networks, it's crucial to burgeon a secure and efficient digital watermarking method to protect the copyrights of digital content. Existing research primarily focuses on deep learning-based approaches to improve the quality of watermarked images, but they have some flaws. To overcome this, the deep learning digital image watermarking model with highly secure algorithms is proposed to secure the digital image. Recently, quantum logistic maps, which combine the concept of quantum computing with traditional techniques, have been considered a niche and promising area of research that has attracted researchers' attention to further research in digital watermarking. This research uses the chaotic behaviour of the quantum logistic map with Rivest–Shamir–Adleman (RSA) and Secure Hash (SHA-3) algorithms for a robust watermark embedding process, where a watermark is embedded into the host image. This way, the quantum chaos method not only helps limit the chance of tampering with the image content through reverse engineering but also assists in maintaining a high level of imperceptibility and strong robustness with efficient extraction or detection of watermark images. Lifting Wavelet Transformation (LWT) is a potential and computationally efficient version of traditional Discrete Wavelet Transform (DWT) where the host image is divided into four sub-bands to offer a multi-resolution view of an image with greater flexibility in watermarking methodologies. Furthermore, considering the robustness against attacks, a pre-trained Residual Neural Network (ResNet-50), a convolutional neural network with 50 layers deep, is used to better learn the complex features and efficiently extract the watermark from the image. By integrating RSA and SHA-3 algorithms, the proposed model demonstrates improved imperceptibility, robustness, and accuracy in watermark extraction compared to traditional methods. It achieves a Peak Signal-to-Noise Ratio (PSNR) of 49.83%, a Structural Similarity Index Measure (SSIM) of 0.98, and a Number of Pixels Change Rate (NPCR) of 99.79%, respectively. These results reflect the model's effectiveness in delivering superior quality and security. Consequently, our proposed approach offers accurate results, exceptional invisibility, and enhanced robustness compared to the existing digital image watermarking techniques.

KEYWORDS

Image watermarking; quantum logistics; Rivest–Shamir–Adleman (RSA); Secure Hash (SHA-3); Lifting Wavelet Transformation (LWT); ResNet-50; deep learning; secure communication

1 Introduction

Because of significant advancements in digital technology and broadband networks, digital works are duplicated and modified without sacrificing quality. The rise of unauthorized tampering, forgery, and theft underscores the immediate need to address information security and copyright protection as vital practical concerns. Watermarking digital images is a powerful method for taming copyright violations in digital content. It incorporates digital data or a watermark into the cover image [1,2]. Digital image watermarking alludes to the covert process of submerging and extricating information surrounded by a carrier image. In this process, data (known as the watermark) is invisible within a cover image to create a marked image that will be distributed over the Internet. Then the extraction of watermark information can only be accurately done by the authorized recipients. A general classification of watermarking schemes is presented in Fig. 1 to understand the several existing watermarking processes.

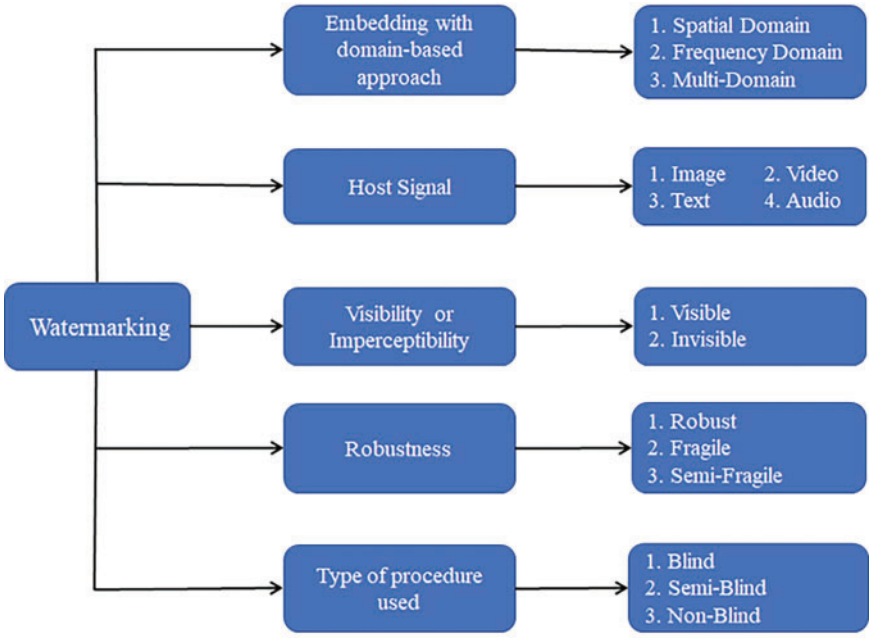

Figure 1: General classification of watermarking scheme

As evident from Fig. 1, the general watermarking scheme can be classified based on the following:

- The watermarking scheme is chosen based on the type of host signal, including Images, Videos, Text, and audio signals.
- The watermarking embedding process is carried out next to the input host signal with an original watermark. Sometimes, a secret key is applied at the input during the embedding process to add extra security to the watermarked signal. Watermark embedding of the data on the host signal may be done in the spatial domain, frequency domain or multi-domain. In the spatial domain, the watermark data is embedded in the host signal by spatially modifying the pixel value of the image content. In contrast, in the frequency domain, the use of frequency transformation methods such as Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) or Discrete Wavelet Transforms (DWT), etc., are used. The frequency

domain approach provides better imperceptibility and robustness at the cost of complexity. The combination of the domains makes it a multi-domain approach.

- The visibility or imperceptibility presents us with the image's visual quality by finding the similarity between the host signal or image and watermarked data. In an invisible watermark scheme called steganography or hidden watermarking, the data looks identical to the original ones, and the naked eye cannot recognize the embedded watermark. Examples of invisible watermarking include embedding a logo or image in the host image but keeping it transparent, making it difficult to acknowledge the watermark data. Those that fail can be classified as visible digital watermarks. This imperceptibility is not possible in the case of a text file, as there is hardly any spare space in it to hide anything. Still, it is likely in the case of images as there might be enough pixels to hide the watermark information and to confirm the copyright violation/protection.
- Robustness is an essential criterion for watermarking evaluations, as there are enough chances that the watermarked contents are altered by some means either during communication through transmission media or by adding some attacks based on content alteration. Robust watermarking enables us to protect digital content from such scenarios effectively. Based on these, a robust watermark process can be classified as fragile or semi-fragile. Where fragile watermarking ensures the security of the embedded watermark from unauthorized data tempering or data alterations, but can easily be attacked by minor modifications like lossy compression, which can destroy the digital content. On the other hand, robust watermarking secures digital content from data manipulation through signal processing operations, including compression, filtering, and cropping, to name a few. At the same time, the semi-fragile watermarking process deals with the integrity of content verification. It can distinguish between image processing operations causing lossy compression, bit error, salt and pepper noise, etc., from malicious yet intentional content modification.
- Finally, watermarking schemes are categorized based on the type of procedures used for the watermarking purpose. Blindness is an important characteristic used to illustrate the computational independence of the original information to retrieve the required information. Sometimes, blindness defines detecting and extracting the image watermarking process even though no clear-cut definition exists. In the case of a blind watermarking scheme, there is no such requirement for the source signal or image and the information extracted from the source signal, whereas, in the case of a semi-blind watermarking scheme, the source signal or image is needed even though the source signal or its derived information are not used in the detection and extraction process of the watermarking.

Depending on the user's requirements, the watermark can take various forms, such as (i) random bits or electronic signatures for image security and corroboration or (ii) concealed messages for covert communication [3]. Encoding the watermark serves multiple purposes, such as enhancing perceptible impermanence for heightened security through encryption techniques or restoring the watermark's integrity in the face of attacks by utilizing error correction codes [4,5]. A robust watermarking system requires three things: authenticity, which enables the watermark's integrity to be confirmed to verify the content's ownership or origin; robustness, which can withstand attacks like compression or cropping; and imperceptibility, which makes the watermark invisible or hidden to consumers. While the primary focus of an image steganography system is imperceptibility to the human eye and intangibility to machine analysis (i.e., struggling for machines to detect the existence of hidden information), an image watermarking methodology often prioritizes robustness. Consequently, the watermark should persist even if the marked image is deteriorated or deformed [6]. A watermarking scheme is robust if it

can resist non-malicious image processing operations like compression, filtering, geometric and non-geometric attacks or manipulations, etc. Ideally, a robust digital image watermarking system would maintain the watermark unspoiled despite certain distortions or manipulations without additional measures, except in some cases when it is under hostile attacks. Then, in such a hostile attack, several encoding techniques are proposed to restore the image [7,8].

Watermarks are placed on multiple picture domains using more complex watermarking methods. Digital Image Watermarking techniques based on the domain where the watermark is inserted are classified into two categories: spatial domain watermarking and frequency domain watermarking. In spatial domain watermarking, the watermark is directly inserted into the cover picture by changing the pixel values [9–11], which has minimal complexity and ease of implementation at the expense of not being resistant to geometric attacks. On the other hand, in frequency domain watermarking techniques, watermarks are embedded in the spectral coefficients of the cover image by using some frequency transformation tools, including Discrete Fourier Transform (DFT) [12], Discrete Cosine Transform (DCT) [13], Discrete Wavelet Transform (DWT) [14,15], and Lifting Wavelet Transform (LWT) [16] to name a few. Even though these transformation tools enable more information to be embedded with high resistance to assaults, they still often need more processing [17] to obtain adequate image content to reduce false-positive errors. Achieving optimal transform domain embedding with comprehensive performance remains a challenge, which can be tackled through Artificial intelligence approaches such as SVM (Support Vector Machine) in the LWT domain [18].

Watermarking in the learning and hybrid domains involves embedding watermarks using a unique identifier or watermark into digital content to protect it from unauthorized usage and thus ensure trustworthiness. In deep learning-based watermarking, neural network architecture embeds and detects the watermarks to ensure its robustness against several possible attacks [19]. On the other hand, hybrid domain watermarking combines multiple domains, such as spatial and frequency domain watermarking, to improve the watermarking scheme's stability, robustness and security. For example, while DWT, DCT or LWT is used for frequency domain watermark embedding to achieve enhanced robustness and security, when combined with the Singular Value Decomposition (SVD) method, the same watermarking scheme becomes more stable and able to withstand several attacks [20].

The SVM-based categorization with many features takes longer execution time and may not be suitable for use in real-time. To address this, Yang et al. [21] introduced a fuzzy support vector machine (FSVM) approach, which, performed effectively with a few host images, is robust to many attacks in terms of BER (bit error rate) but needs improvement in terms of computational time. Deep Neural Networks (DNNs) have recently gained popularity in digital image watermarking techniques for their inherent ability to automatically train the natural picture, resulting in increased imperceptibility and resilience [22]. Further, to reduce the computing time, several researchers have used the Joint Fingerprinting and Decryption (JFD) approach [23,24] by positioning the watermark embedding process at the recipient's end, irrespective of the watermark's vulnerability to various attacks during transmission over the network. Nonetheless, these JFD-based approaches are constrained by their limited data embedding capacity, so their security measures must be strengthened.

The JFD approach generates digital fingerprints by capitalizing on the discrepancy in information randomness between encryption and decryption keys. This leads to a scenario where a substantial amount of diverse information induces notable distortions in the host image. As a result, the implanted fingerprint is relatively modest. Moreover, their methods use symmetric encryption, where distinct keys are employed for encryption and decryption. The agent must possess each user's decryption key

to execute the copyright authentication [25]. Consequently, a security risk arises in managing and distributing secret keys.

Further, to enhance the security of watermarking schemes, several efficient encryption techniques, including hyper-chaotic mapping, may be used to protect highly sensitive digital content [20].

The hybrid watermarking process combines classical transform domain techniques with Convolutional Neural Network (CNN)-based methods to enhance robustness and imperceptibility. Classical methods embed watermarks in frequency coefficients for better attack resilience, while Convolutional Neural Networks (CNN) optimize feature learning and watermark extraction. This approach ensures improved security and reduced perceptual impact, leveraging the strengths of both techniques and watermarking advantages of deep learning techniques in a learning domain to automatically learn and extract robust features from images, significantly enhancing system performance. Using CNN, the watermarking process improved feature extraction and resilience, improving imperceptibility and robustness against attacks. This approach ensures more accurate watermark embedding and extraction, resulting in a more secure and efficient system.

Conventional watermarking systems frequently suffer from insufficient security measures and poor resilience against different types of attacks. Traditional approaches often do not achieve strong imperceptibility, leaving the watermark visible or easily discernible. Furthermore, the overall security of the watermark is compromised by the fact that traditional systems lack sophisticated encryption and scrambling mechanisms, making them open to tampering and illegal access.

Looking into these problems in the digital image watermarking process, we are motivated to develop efficient watermarking algorithms that can reduce the processing time and improve the watermark's security while providing high resilience. Thus, our research proposes a Deep Learning-Based Digital Image Watermarking Model with highly Secured Algorithms. Following are the highlights of our main contributions to this research.

1.1 Research Contributions

- In existing research, various watermarking algorithms have been used but are not sufficiently resilient against several attacks. Hence, our proposed study introduces a highly secure algorithm based on Quantum Logistics in which the RSA and SHA-3 algorithms are used for their robustness.
- Moreover, the key distribution and management process is a significant problem in the existing encryption algorithms. To overcome this, firstly, our research introduces RSA, which contains a random private and public key and gives a preprocessed image. Secondly, SHA-3 processes the preprocessed image to extract the plaintext message, which is then securely stored.
- Furthermore, the Residual Neural Network (ResNet-50), a deep-learning-based convolutional neural network with 50 layers deep, is used in this research to extract the watermark image, even though it requires more computation time and has degraded efficiency.
- Consequently, the proposed deep learning-based digital image watermarking algorithm, which combines ResNet-50 with quantum logistic-based watermark embedding and RSA and Secure Hash Algorithm-3 (SHA-3) based encryption algorithms, is found to be robust against various attacks and able to extract the original image very accurately.

The remaining part of this research work is organized as follows: Section 2 reviews the neural network-based image watermarking system. Section 3 discusses the principles of LWT, RSA, SHA, and Quantum Logistics. Section 4 describes the proposed Deep Learning-Based Digital Image

Watermarking Model with High-Secure Algorithms. Section 5 describes the experimental results with discussions and research case studies. Finally, Section 6 provides the conclusion.

2 Related Works

A novel frequency-domain chaos-based SVD picture watermarking system was proposed by Zainol et al. [26], where the secret key derived from both the host and watermark images is used to create a new chaotic matrix and multiple scaling factors (CMSF) to enhance the system's vulnerability. As the retrieved secret key and the watermark pictures are unique to the host, the frequency-domain chaos-based SVD picture watermarking system improves security with a low false positive rate. Sinhal et al. [27] developed a multiple LSB (Least Significant Bit) substitution method-based multifunctional digital picture watermarking technique, where a fragile watermark pattern is randomly inserted and due to this blind nature of watermark insertion, the multiple LSB bit substitution method enhances the security of the watermark image.

Zhong et al. [28] presented a deep neural network-based picture watermarking system that is both resilient and blind and aimed to promote flexible implementations without needing previous knowledge or adversarial instances of probable assaults. However, the research has not focused on security issues in digital image watermarking [28]. Pourhadi et al. [29] have introduced an enhanced digital image watermarking system that combines the Stationary Wavelet Transform (SWT) and Speed-Up Robust Feature (SURF) techniques for improved robustness. The proposed SWT+SURF approach within the Bat Optimization Algorithm framework leverages the host image's high-frequency coefficients of the SWT to optimize watermark strength parameters during the embedding process while also considering potential attacks. Various image processing techniques, including Gaussian filtering, scaling, rotation, salt and pepper noise, Poisson noise, speckle noise, and Gaussian noise, have been used as attacks [29] to assess the effectiveness of the proposed algorithm despite the increase in computation time.

Abdallah et al. [30] used Nonnegative Matrix Factorization (NMF) and FWHT (Fast Walsh-Hadamard Transform) to provide a durable and invisible safe picture watermarking technique. This is done by using four steps: First, the host image is divided into small blocks, on which NMF is being applied separately, followed by FWHT, which is used for the generation of the weight matrix, and then finally, the singular values of the watermark picture are properly distributed over the transformed blocks. Alam et al. [31] proposed a method for authenticating images at the receiver end utilizing information parameters and digital signatures. To enhance the security of the watermarking technique, DCT, DWT, hyperchaotic (HCM) map, and 2-level SVD (Singular Value Decomposition) features were effectively applied.

Jana et al. [32] introduced a novel Cellular Automata (CA) with a DCT-based picture watermarking system. In this system, a color cover image is divided into red, green, and blue channels, and then DCT is applied to 8×8 non-overlapping blocks of each channel, followed by Zigzag scanning. Encryption with CA rule-15 before embedding in a Digital Image watermark enhances security and resistance.

Helal et al. [33] presented a hybrid digital image watermarking system by combining Walsh Hadamard Transform (WHT) and SVD, which is effective in both imperceptibility and robustness criteria while maintaining transparency. Eltoukhy et al. [34] introduced a novel robust hybrid watermarking scheme for securing color medical images, where the proposed method relies on combining Slant, Singular Value Decomposition (SVD), and Quaternion Fourier-Transform (QFT).

The technique produces high invisibility and durability and is more resistant to several geometrical and hybrid attacks than the existing watermarking schemes.

Mellimi et al. [35] created a Deep Neural Network (DNN)-based resilient picture watermarking system that handled various geometric and noise assaults quite effectively. The suggested approach was evaluated for over three hundred untrained images and yielded a high PSNR (Peak Signal to Noise Ratio). Other assessment factors, including BER (Bit Error Rate), NCC (Normalized Cross-Correlation), and SSIM (Structural Similarity Index), have performed excellently. Among all potential sub-band combinations, LH (Low-High)/LH1/HL2 (High-Low) yielded the most promising results. The DNN enabled lightning-fast watermark extraction. Watermark image extracted with nearly minimal error for attacks such as Gaussian filter, JPEG (Joint Photographic Experts Group) compression, cropping, and scaling.

However, the existing digital image watermarking methods often have limitations such as insufficient security against various attacks, high computational demands, and suboptimal robustness. Deep learning-based methods, such as neural networks for watermark extraction, offer improved resilience but often lack a focus on security and can be computationally intensive. The proposed approach addresses these limitations by integrating RSA and SHA-3 algorithms for enhanced security and imperceptibility, using ResNet-50 for efficient feature extraction, and incorporating LWT to improve robustness against various attacks. This combination not only provides a high level of imperceptibility and robustness but also optimizes computational efficiency, surpassing many existing methods in both security and performance. Hence, new watermark approaches based on the deep-learning idea is proposed in our research to circumvent the restrictions, which are detailed in the subsequent sections.

3 Proposed Methodologies

This section contains the operational principles of LWT, SVD, Quantum Logistics, RSA, and SHA-3.

3.1 Lifting Wavelet Transform (LWT)

While the first generation filter process, including DWT, aims at separating the input signal into its corresponding low and high-frequency components and then performs the compression or down sampling on both signals at a later stage, the lifting-based wavelet transform (LWT) [36] considered as second generation of wavelets performs the compression in advance, resulting reduced computational complexity, has a better frequency localization characteristic, and eliminating the standard wavelet's flaws by effectively addressing the shift-invariance problem.

Lifting Wavelet Transform (LWT) is used to divide a targeted image into four categories of sub-bands: LL (Low-Low), HL (High-Low), LH (Low-High), and HH (High-High) in the LWT-based watermarking approach. The low-frequency component is represented as LL and has a low resolution. In this splitting process by LWT, the low-frequency part (LL) of the signal/image contains the essential information about the image; hence any alteration or adding watermark to it may result in image degradation but may present robustness, whereas most negligible image content is available in high-frequency part (HH) of the image/signal, hence may be used for watermarking purposes which may also provide high imperceptibility at the cost of elimination of the embedded watermark through some image processing operations. Therefore, it is advisable to use the mid-frequency part (HL, LH) with horizontal and vertical details for the image watermarking process with a trade-off between robustness and imperceptibility [37]. Better imperceptibility in embedded image watermarks is expected when the watermarking is done with the horizontal part of the image as the vertical part of

the image is considered more sensitive to human vision than its horizontal counterpart [37]. LWT offers several advantages over traditional wavelet transforms, such as better frequency localization, reduced computational complexity, and the ability to save time while preserving essential image features. These qualities make LWT more efficient in handling large-scale image data, making it ideal for digital watermarking. In this research, LWT is used because embedding watermarks in the low-frequency LL sub-band ensures higher robustness and imperceptibility, as the LL sub-band contains the most energy and is more resistant to standard image processing techniques, enhancing both security and quality.

The central concept behind the lifting wavelet is to create a new wavelet with improved features based on a simple wavelet. As discussed below, splitting, prediction, and updating are the three processes in signal decomposition using LWT [38].

- Split: Divide the original signal into non-overlapping even and odd samples, denoted as $x_{ze_z}[n_z]$ for even samples and $x_{zo_z}[n_z]$ for odd samples, respectively.

$$x_{ze_z}[n_z] = x_z[2n_z],\ x_{zo_z}[n_z] = x_z[2n_z + 1] \tag{1}$$

- Predict: If even and odd samples are connected, one can be used to predict the other. We use $x_{ze_z}[n_z]$ samples to estimate $x_{zo_z}[n_z]$, These are specified as:

$$d_z[n_z] = x_{zo_z}[n_z] - p_z[x_{ze_z}[n_z]] \tag{2}$$

  The predictor operator is denoted as $p_z()$, and $d_z[n_z]$ represents the difference between the actual sample and its predicted value, characterized as a high-frequency component.
- Update: update the even samples using the update operator $U_z()$ and the detail signal $d_z[n_z]$. The low-frequency components $l_z[n_z]$, Which describe the original signal's coarse structure, are then derived as:

$$l_z[n_z] = x_{ze_z}[n_z] + U_z[d_z[n_z]] \tag{3}$$

The watermark is embedded in the low-frequency sub-band (LL) because the signal's highest energy is concentrated in these low-frequency coefficients, which are more resistant to image processing techniques. In addition, incorporating the watermark in the LL sub-band makes it more visible to human vision. Let's consider the host image. $I_z = \{I_z(x_z, y_z) : 1 \le x_z \le M_z, 1 \le y_z \le N_z\}$ is a 512 × 512 8-bit grayscale image that has been decomposed into four sub-bands: LL, LH, HL, and HH using one level Lifting Wavelet Transform (LWT). Each sub-band has a size of $M_{zL_z} \times N_{zL_z}$, where

$$M_{zL_z} = \frac{M_z}{2^{k_z}}, N_{zL_z} = \frac{N_z}{2^{k_z}} \tag{4}$$

Here, k_z denotes the level of decomposition.

The LWT is significant in our work due to its computational efficiency, flexibility, and ability to address the shift-invariance problem commonly associated with traditional DWT. LWT provides a more straightforward and faster implementation by breaking down wavelet computations into simple prediction and update steps, reducing complexity without sacrificing accuracy. Additionally, LWT is highly adaptable for reversible integer-to-integer transformations, making it ideal for lossless processing. It is crucial for digital watermarking to preserve the integrity of the host image and watermark. Its consistency in signal alignment ensures greater robustness and imperceptibility in our watermarking approach, outperforming conventional DWT-based methods, particularly in scenarios involving attacks like compression or geometric transformations.

3.2 Singular Value Decomposition (SVD)

Singular Value Decomposition (SVD) is initially employed in linear algebra [39], but now, it has found extensive applications, including signal and image processing and digital watermarking. Typically, SVD operates directly or in several smaller blocks on the host image. These blocks are then subjected to SVD decomposition, resulting in the extraction of singular values, which are subsequently employed to embed watermark information. In digital watermarking, employing this decomposition method offers various advantages. These include the consistent size of the SVD coefficients, the ability of singular values to encapsulate essential algebraic characteristics of an image, and their resilience to significant alterations when the image undergoes slight disruptions. The decomposition formula is detailed as follows:

$$I_z = U_z.S_z.V_z^T \tag{5}$$

where I_z is the $m_z \times n_z$ matrix corresponding to an image, U_z is the $m_z \times m_z$ matrix, V_z is the $n_z \times n_z$ matrix, S_z is the diagonal matrix with the same size as I_z, and T is the matrix transformation coefficient.

3.3 Rivest-Shamir-Adleman (RSA) with Secure Hash Algorithm (SHA-3)

3.3.1 Rivest-Shamir-Adleman (RSA) Algorithm

The Rivest-Shamir-Adleman (RSA) algorithm, invented by three MIT (Massachusetts Institute of Technology) professors, Ronald Rivest, Adi Shamir, and Leonard Adleman, in the summer of 1977, was the first public-key cryptographic algorithm. It falls under the category of Asymmetric Encryption methods and is one of the most commonly used algorithms today because it is highly secure and fast in comparison to the many competing algorithms available [40].

Asymmetric encryption is used in the public critical encryption method, which protects encrypted data with a pair of keys. In this domain, RSA is a prominent approach. It is also a member of the block cipher domain. The following are the details of the essential generation process [41]:

Step 1: Choose two prime numbers at random, p_z and q_z.

Step 2: Utilize Euler's totient function (N_z) to calculate one secret key member $\varphi(N_z)$:

$$N_z = p_z \times q_z, \varphi(N_z) = (p_z - 1) \times (q_z - 1) \tag{6}$$

Step 3: Two requirements must be fulfilled when generating an encryption key at random:

$$\mathbf{1} < e_z < \varphi(N_z), \text{ great common divisor } (e_z, \varphi(N_z)) = 1 \tag{7}$$

where the logic equation shows that the greatest common divisor between e_z and $\varphi(N_z)$ is one, and that e_z and $\varphi(N_z)$ are co-primes.

Step 4: Calculate the decryption key d_z by using the formula below:

$$e_z \times d_z = 1 \,|\varphi(N_z)|\,, 0 \le d_z \le N_z \tag{8}$$

This public key system includes two types of secret keys: a public key and a private key. The public key is represented as (e_z, N_z), while the private key is represented as (d_z, N_z). The public key is widely disseminated, while the private key is kept confidential. The sender must first obtain the recipient's public key when sending data. The sender then encrypts the message using this public key and transmits the encrypted text to the recipient. The receiver then decrypts the encrypted text using their private key, resulting in a plain-text message. The security of the RSA encryption system is assured. Although attackers may have access to the public keys e_z and N_z, e_z is a random number and N_z is a large number.

Consequently, it is highly improbable that attackers can determine the values of p_z and q_z through large integer factorization, which is an NP-hard (Nondeterministic Polynomial-time hard) problem.

RSA key management can be simplified using centralized or decentralized critical management systems. Centralized Public Key Infrastructures (PKIs) use a trusted Certificate Authority to generate and distribute public and private keys, reducing tampering risks. Decentralized systems use blockchain technology to store public keys in an immutable ledger, facilitating safe key distribution. Hybrid critical management systems combine symmetric and asymmetric cryptography, such as RSA for key exchange and symmetric encryption for bulk data transfer, enhancing efficiency while maintaining security. These approaches reduce overhead and improve scalability in large-scale implementations.

3.3.2 SHA-3 (Secure Hash Algorithm 3)

SHA-3 (Secure Hash Algorithm 3) is a cryptographic hash function aimed at generating a unique, fixed-size hash value from an input image of any size, which found its main applications in data/image integrity and digital watermarking. This paper uses a novel reversible invisible watermarking scheme based on SHA-3 to protect the digital content or image from copyright violation and ensure the image's integrity. There are several versions of the SHA algorithm available, such as Secure Hash Algorithm 0 (SHA-0), Secure Hash Algorithm 1 (SHA-1), Secure Hash Algorithm 2 (SHA-2) and Secure Hash Algorithm 3 (SHA-3). Initially, the SHA-0 model was proposed by the National Institute of Standards and Technology (NIST) for the Secure Hash Standard (SHS), followed by SHA-1, both having a 160-bit hash value.

However, SHA-1 has been suspected of being insecure since 2005, and the use of SHA-1 has been phased out by the leading companies that use them in Secure Sockets Layer (SSL) certificates. Next, SHA-2 emerges as a successor to SHA-1 with SHA-224, SHA-256, SHA-384, and SHA-512 having 224-bit, 256-bit, 384-bit and 512-bit hash value respectively. At present, SHA-2 is still considered to be secure and is widely used in SSL certificates and cryptocurrency transactions. Recently, a new family member in the SHA family emerged as SHA-3 having a 512-bit length hash function found in applications for digital content authentication purposes, including watermarking scenarios [42].

3.3.3 Combining SHA-3 with RSA

This combination of SHA-3 and RSA combines the strengths of both algorithms: the robust hashing capabilities of SHA-3 and the secure key management of RSA. SHA-3 can be used to create a hash of an image/signal, which is then encrypted with the sender's private RSA key to create a watermarked image with the integrity and authenticity of the digital content.

Hence, from the above discussions, one can envisage that integrating the key management system using RSA keys and SHA-3 in digital watermarking applications can automate and streamline the watermarking process.

3.4 Quantum Logistic Map

A Quantum Logistic Map [43] extends a classical logistic map, incorporating quantum corrections to increase complexity and randomness. Introducing quantum fluctuations into chaotic behaviour increases the unpredictability and sensitivity to beginning conditions. In this research, it is used for secure digital image watermarking due to its ability to generate complex, non-periodic sequences with a vast key space, increasing security and robustness against attacks while ensuring the imperceptibility of the watermark. Its high randomness and sensitivity make it ideal for cryptographic solid properties applications.

The logistic map [43], described by the Eq. (9), is a widely used one-dimensional chaotic system [44].

$$x_{zn_z+1} = x_{zn_z} \times u_z \times (1 - x_{zn_z}) \tag{9}$$

The logistic map represents a crucial specific case of solid dissipation. A dissipative quantum logistic map is generated by coupling the quantum kick to a bath of harmonic oscillators. To examine the impact of quantum corrections, they write. $a_z = \langle a_z \rangle + \delta a_z$, where δa_z denotes a quantum fluctuation of a_z. The following equations regulate this chaotic map with lowest-order quantum corrections:

$$\begin{cases} x_{zn_z+1} = r_z \left(x_{zn_z} - \left| x_{zn_z} \right|^2 \right) - r_z y_{zn_z} \\ y_{zn_z+1} = -y_{zn_z} e^{-2\beta_z} + e^{-\beta_z} r_z \left[\left(2 - x_{zn_z} - x^*_{zn_z} \right) y_{zn_z} - x_{zn_z} z^*_{zn_z} - x^*_{zn_z} z_{zn_z} \right] \\ z_{zn_z+1} = -z_{zn_z} e^{-2\beta_z} + e^{-\beta_z} r_z [2 \left(1 - x^*_{zn_z} \right) z_{zn_z} - 2 x_{zn_z} y_{zn_z} - x_{zn_z} \end{cases} \tag{10}$$

where $x_z = \langle a_z \rangle$, $y_z = \langle \delta a_z \delta a_z \rangle$, $z_z = \langle \delta a_z \delta a_z \rangle$ and β_z is the dissipation parameter. In general, x_{zn_z}, y_{zn_z}, and z_{zn_z} are complex numbers with $x^*_{zn_z}$ being the complex conjugate of x_{zn_z} and z_{zn_z} being the same. If we set the initial values to real numbers, all subsequent values will also be accurate.

The logistic map with additive noise retains the same form as Eq. (10). It is important to note that the noise is generated continuously. In this context, the noise measures quantum correlation strength. When the quantum corrections y_{zn_z} and $z_{zn_z} \to 0$ Eq. (10) reduces to the classical, one-dimensional logistic map. The quantum logistic map's firm dissipation limit, $\beta_z \to \infty$ also yields the classical logistic map.

The initial conditions of a quantum logistic map are compassionate, so even slight changes can lead to vastly different sequences. The benefits of using the quantum logistic map include its high complexity and extensive key space. Additionally, it can effectively address the issues of fixed points and stable windows. The parameter variation range is broad and continuous, leading to a more uniform chaotic sequence output, increased non-periodicity, and enhanced randomness performance.

3.5 RESNET 50 Architecture

ResNet-50 [45] is a convolutional neural network (CNN) type that has revolutionized how we approach deep learning. It was first introduced in 2015 by He et al. at Microsoft Research Asia. Many papers will compare their results to a ResNet-50 baseline, which is valuable as a reference point, to quickly produce models to tackle new problems [46].

ResNet-50 consists of 50 layers divided into five residual blocks, using the concept of residual learning. The residual blocks safeguard information from earlier layers, helping the network learn with better descriptions of the input data and making it easier for very deep neural network training. This might be possible using skip connections or shortcuts, thus allowing the gradient to flow directly through the deep neural network.

The ResNet-50 architecture [47] consists of convolutional layers followed by batch normalization and rectified linear unit (ReLU) non-linear activation functions. The residual blocks, which contain the skip connections, enable the network to learn the identity mapping efficiently. The last layers typically use a global average pooling layer and a fully connected layer for classification.

4 Experimental Frameworks

In recent years, advancements in digital watermarking have significantly improved the precision and robustness of watermarked images against various attacks, including diverse sound alterations and random noise characteristics. Moreover, a decreased calculation time with remarkable resilience has become challenging in digital watermarking technology. Also, in existing research, ensuring that watermarked images are sufficiently resilient against such attacks is crucial. As a result, image encryption techniques and deep neural network principles are used to improve resilience. This paper proposes a Deep Learning-Based Digital Image Watermarking Model with High Secure Algorithms to ensure that watermarked images can withstand attacks.

In this research, we introduce a novel watermarking scheme, as depicted in Fig. 2, which consists of two primary processes: watermark embedding and watermark extraction. In the first step, scramble parameters have been chosen. A highly secure algorithm based on Quantum Logistics has been proposed to secure the digital image. The RSA and SHA-3 algorithms present Image encryption using quantum logistics techniques in the watermark image. Then, the watermark is embedded into the host image, which is called a watermarked image. Furthermore, several deep-learning neural networks have been developed to extract the watermark. The existing networks have taken more computation time, and efficiency degradation is also present in them.

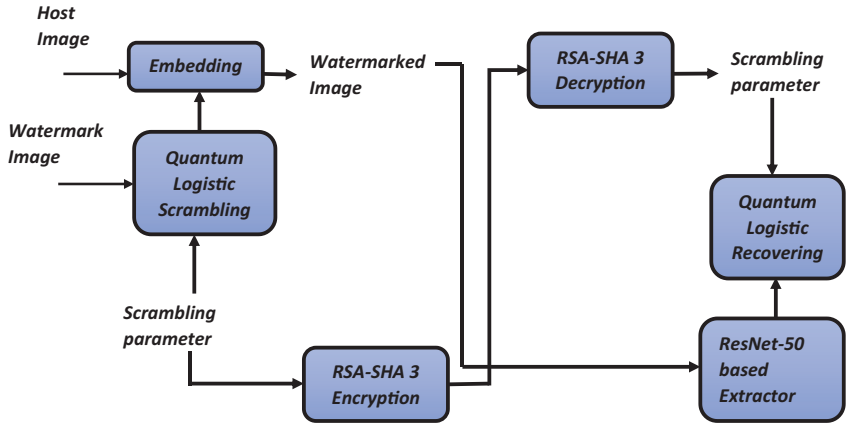

Figure 2: Experimental framework

To overcome the problems mentioned above, the ResNet-50 has been used to extract the features to obtain the original image from the watermarked image, in which the low-frequency sub-bands in the host image were used to create the feature set to train the given neural network with less time in a very accurate manner. The scrambled watermark image has been obtained, and the decryption is also done using the private key in the scrambled parameters. Ultimately, quantum logistics has been employed to retrieve the watermark image using specific scrambling parameters. As a result, the proposed deep learning-based image watermarking algorithm withstands various attacks, and the original image is extracted accurately.

4.1 Watermark Embedding

Consider the input plain image, and it has a size of $M_z \times N_z$. The plain image is first processed with a fixed matrix to produce a pre-treated image. The pre-treatment images are then computed using the SHA-3 hash function to get hash values, which are then used in the RSA algorithm to calculate the

quantum logistic map's initial values. Finally, the encrypted images could be obtained by confusing rows and columns in various directions, diffusion applied to odd rows and columns, confusion applied to rows and columns in different directions, and diffusion applied to even rows and columns. The following is a detailed description of our proposed Deep Learning-Based Digital Image Watermarking Model with a secure algorithm.

Within the watermark embedding technique, a Quantum Logistic algorithm was applied to scramble the watermark image before its insertion into the designated area of the host image. Construct a fixed matrix A_z of size $M_z \times N_z$, with a value that is a simple distribution from 1 to 255. Then, employ the following equation to perform the additive modular operation on the plaintext image P_z, resulting in the creation of the preprocessed image B_z.

$$B_z = P_z + A_z \tag{11}$$

where + signifies addition followed by a modulus operation under 256, and the generating process entails reversing the pixel values range from 255 to 1, starting from the first row to the last row. Moreover, to strengthen the security of the watermark, this research proposes RSA with SHA-3. Initially, the SHA-3 computes the preprocessed image to extract the plain message, which is then securely stored, applying SHA-3 to the image B_z to generate 32 hash values. As the initial data m'_{z1}, take the odd position numbers from these hash values and add them. Then, as the second data m'_{z2}, take the hash values at odd positions and add them together. The third data m'_{z3} is made up of the remaining hash values. The plain messages m'_{z1}, m'_{z2}, and m'_{z3} are then calculated using these data m_{z1}, m_{z2}, and m_{z3}.

$$m_{zi} = m'_{zi} \, mod \, 256 + 1, i = 1, 2, 3 \tag{12}$$

The encryption message corresponding to the plain message may be acquired using the RSA technique. Then, the RSA is used to produce key pairs containing a private key (d_z, N_z), and a public key (e_z, N_z) at random. Use the public key to encrypt the plain messages m_{z1}, m_{z2}, m_{z3} and get the public messages c_{z1}, c_{z2}, c_{z3} by the equation $c_{zi} = m_{zi}^{e_z} |n_z|$. Then, calculate the initial values using the following Eq. (13):

$$\begin{cases} x_{z0} = \dfrac{m_{z1}(m_{z1} + c_{z1} - 1)}{(m_{z1} + c_{z1})^2} \\ y_{z0} = \dfrac{m_{z2}(m_{z2} + c_{z2} - 1)}{(m_{z2} + c_{z2})^2} \\ z_{z0} = \dfrac{m_{z3}(m_{z3} + c_{z3} - 1)}{(m_{z3} + c_{z3})^2} \end{cases} \tag{13}$$

Afterwards, these initial values are substituted into the quantum logistic map to get the scrambled watermark; the quantum logistic technique scrambles the watermark image with the scrambled parameters. Iteratively discard the first 500 values to obtain the chaotic sequences x_z, y_z, z_z. Then, process the above sequence as follows:

$$\begin{cases} X_z = \left| floor\left(x_z\left(1 : M_z\right) \times 10^{14}\right), N_z + 1 \right| \\ Y_z = \left| floor\left(y_z\left(1 : N_z\right) \times 10^{14}\right), M_z + 1 \right| \\ Z_z = \left| floor\left(z_z \times 10^{14}\right), 256 \right| \end{cases} \tag{14}$$

To conduct cyclic confusion on the image B_z in both the row and column directions, use the above keystreams X_z and Y_z. To initiate each row in the image B_z is cyclically confused using X_z. As shown

below, odd rows rotate to the left, and even rows rotate to the right.

$$\begin{cases} C_z(i,j) = B_z(i,(j - X_{zi})\,|N_z + 1|), i = odd\ samples\ such\ as\ 1,3,5,\ldots,M_z \\ C_z(i,j) = B_z(i,(j + X_{zi})\,|N_z + 1|), i = even\ samples\ such\ as\ 2,4,6\ldots M_z \end{cases} \tag{15}$$

Consequently, for image C_z, the keystream Y_z is utilized to confuse the columns, with odd columns being circularly moved up and even columns being circularly shifted down as follows:

$$\begin{cases} D_z(i,j) = C_z\left(\left(i - Y_{zj}\right)|M_z + 1|, j\right), j = odd\ samples\ such\ as\ 1,3,5,\ldots,N_z \\ D_z(i,j) = C_z\left(\left(i + Y_{zj}\right)|M_z + 1|, j\right), j = even\ samples\ such\ as\ 2,4,6\ldots N_z \end{cases} \tag{16}$$

where $D_z(i,j)$ denotes a pixel in the image D_z row i and column j. Then, conduct XOR (Exclusive OR) diffusion and additive modular operation on the odd rows of the image D_z with Z_z using the equation below:

$$\begin{cases} E_{zi} = (D_{zi} \oplus Z_{zi}) + Z'_{zi} + (m_{z1} + m_{z2} + m_{z3}) \times Z_{zi}, i = 1,3,5\ldots M_z \\ E_{zi} = D_{zi}, i = 2,4,6\ldots M_z \end{cases} \tag{17}$$

where Z'_{zi} is the reverse order of Z_{zi}. The pixel value in the image E_z's odd columns are diffused again by:

$$\begin{cases} F_{zj} = \left(E_{zj} \oplus Z_{zj}\right) + Z'_{zj} + (c_{z1} + c_{z2} + c_{z3}) \times Z_{zj}, j = 1,3,5\ldots N_z \\ F_{zj} = E_{zj}, j = 2,4,6\ldots N_z \end{cases} \tag{18}$$

To get the image H_z, confuse image F_z iteratively with X_z and Y_z as the same process in Eqs. (15) and (16). To the even rows of image H_z, repeat the XOR and additive modular operations in Eqs. (17) and (18).

$$\begin{cases} I_{zi} = (H_{zi} + Z_{zi}) \oplus Z'_{zi}, i = 2,4,6\ldots M_z \\ I_{zi} = H_{zi}, i = 1,3,5\ldots M_z \end{cases} \tag{19}$$

The pixel values in the image I_z even columns are diffused.

$$\begin{cases} J_{zj} = \left(I_{zj} + Z_{zj}\right) \oplus Z'_{zj}, j = 2,4,6\ldots N_z \\ J_{zj} = J_{zj}, j = 1,3,5\ldots N_z \end{cases} \tag{20}$$

Hence, we can get the cipher image J_z. Finally, the watermark was embedded into the host image, yielding a watermarked image. The host image is divided into four sub-bands, LL, HH, LH, and HL, by Lifting Wavelet Transformation (LWT). Then, Singular Value Decomposition (SVD) was performed in the sub-band of LL and the SVD for the new singular values. Then, a new low-frequency approximate coefficient has to be reconstructed, and finally, a watermarked image is obtained by applying Inverse LWT. Furthermore, a feature vector is necessary to train any neural network. The neural network uses the LL, HH, LH, and HL bands as feature vectors. Watermarked images are subjected to various attacks to generate a feature vector. The proposed approach employs 11 multiple attacks, such as Gaussian low-pass filter, median filter, Gaussian noise, salt and pepper noise, speckle noise, JPEG compression, JPEG 2000 compression, sharpening attack, histogram equalization, average filter, and motion blur. As a result, the watermark embedding technique uses image encryption algorithms, which aid in maintaining a high level of imperceptibility and robustness.

Furthermore, several deep-learning neural networks have been developed to extract the watermark described in the forthcoming section.

Algorithm 1: High secure algorithm based on quantum logistics

Step 1: A number pair was chosen as scrambling parameters, and the ciphertext was obtained by encrypting it with the RSA technique using Eq. (14) and (e_z, N_z) as the public key.

Step 2: The Quantum Logistic has been used to scramble the grey-scale watermark image W using the scrambling parameters, giving scrambled watermark Wd.

Step 3: Then, LWT divided the gray-scale host image P_z into four sub-bands P_z^i, such as LL, HL, LH, and HH.

Step 4: SVD was carried out on LL, $U_{zP_z}.S_{zP_z}.{V_{zP_z}}^T = SVD(LL)$.

Step 5: A new single value has been calculated S_{new} by integrating S_{P_z} and scrambled watermark with a scale factor $\propto$, $S_{new} = S_{P_z} + \propto .W_d$

Step 6: Apply SVD to the new singular value, $U_{zw}.S_{zw}.{V_{zw}}^T = SVD(S_{new})$.

Step 7: A new low-frequency approximation coefficient has been reconstructed LL_{new}, and $LL_{new} = U_{zP_z}.S_{zw}.{V_{zP_z}}^T$

Step 8: Obtain the watermarked image P_{zw} by performing inverse LWT with the modified approximate coefficient.

The hybrid algorithm integrates multiple security techniques to enhance the watermarking process. By combining preprocessing, hashing, RSA encryption, quantum logistic scrambling, confusion and diffusion techniques, and advanced embedding methods with LWT and SVD, your model ensures high security, robustness, and imperceptibility. The deep learning component further strengthens the approach by enabling detailed analysis and evaluation of the watermarking effectiveness against various attacks. This comprehensive approach addresses potential vulnerabilities and ensures the watermarking process is secure and resilient.

4.2 Watermark Extraction

Multiple networks are employed to extract the watermarking image despite having more computation time and efficiency degradation. Thus, to overcome the problems mentioned above, the ResNet-50 has been used to extract the feature to obtain the original image from the watermarked image, and the low-frequency sub-bands of the host image were used to create the feature set. This feature set was then used to train the neural network, resulting in a highly accurate and time-efficient process. In the first step, we decompose the original host image and the watermarked image by using LWT. Then, SVD has been applied to low-frequency sub-bands, and the new low-frequency approximate coefficients must be reconstructed. Finally, the scrambled watermark image was obtained, and the decryption was also done in the scrambled parameters using the private key (d_z, N_z). The inverse operation of the encryption process is the decryption process. The following are phases associated with decryption:

To decrypt the public messages (c_{z1}, c_{z2}, c_{z3} by the equation $m_{zi} = c_{zi}^{dz} |n_z|$, i = 1,2,3), use the private key (d_z, N_z). Using Eq. (13), Calculate the initial values for the quantum logistic map. Iterate the map to generate the chaotic sequence, and then process this sequence to produce the keystreams X_z, Y_z and Z_z. In the cipher image J_z by Z_z, perform inverse diffusion on the even columns as follows:

$$\begin{cases} I'_{zj} = \left(J_{zj} \oplus Z'_{zj}\right) - Z_{zj}, j = 2, 4, 6 \ldots N_z \\ I'_{zj} = J_{zj}, j = 1, 3, 5 \ldots N_z \end{cases} \tag{21}$$

Do the inverse diffusion process on the even rows in the I'_z image as:

$$\begin{cases} H'_{zi} = \left(I'_{zi} \oplus Z'_{zi}\right) - Z_{zi}, i = 2, 4, 6 \ldots M_z \\ H'_{zi} = I'_{zi}, i = 1, 3, 5 \ldots M_z \end{cases} \tag{22}$$

where – denotes the 256-bit subtraction modular operation and Z'_{zi} denotes the reverse order of Z_{zi}. Using keystreams X_z, and Y_z, reverse the cyclic confusion procedure for image H'_z. The inverse confusion process of columns is performed using the keystream Y_z.

$$\begin{cases} G'_z\left(\left(i - Y_{zj}\right)|M_z + 1|, j\right) = H'_z(i,j), j = \textit{odd samples such as } 1, 3, 5, \ldots, N_z \\ G'_z\left(\left(i + Y_{zj}\right)|M_z + 1|, j\right) = H'_z(i,j), j = \textit{even samples such as } 2, 4, 6, \ldots, N_z \end{cases} \tag{23}$$

After that, the keystream X_z is utilized to conduct inverse cycle confusion on rows as follows:

$$\begin{cases} F'_z(i, (j - X_{zi})|N_z + 1|) = G'_z(i,j), i = \textit{odd samples such as } 1, 3, 5, \ldots, M_z \\ F'_z(i,j) = F'_z(i, (j + X_{zi})|N_z + 1|) = G'_z(i,j), i = \textit{even samples such as } 2, 4, 6 \ldots, M_z \end{cases} \tag{24}$$

For the image F'_z, use the keystream Z_z to perform inverse diffusion operations on the odd rows and odd columns to get the image D'_z. To get the image B'_z, apply the inverse cyclic confusion to the image D'_z. Recover the plain image P'_z by performing an inverse additive modular operation on the image B'_z with a fixed matrix A'_z. The following are the detailed steps:

Step 1: The original host image P_z and the watermarked image P_{zw} were decomposed into four sub-bands P^i_z and p^j_{zw} respectively, using LWT, where i = LL, HL, LH, HH and $j = LL_{zw}$, HL_{zw}, LH_{zw}, HH_{zw}.

Step 2: ResNet-50 constructing and training neural network converts and reorganizes the extracted LL_{zw} sub-band into a feature set of size 4×1024.

Step 3: The feature set obtained in the previous step is input into the trained network to generate the output for each 1×4 vectors.

Step 4: To construct the watermark, the 1024 values are anticipated for each attacked image and moulded into 32×32 matrices.

Step 5: SVD was performed on LL_{zw}, $U_{zP_zw}.S_{zP_zw}.{V_{zP_zw}}^T = SVD(LL_{zw})$.

Step 6: Reconstruct a new low-frequency approximate coefficient LL_{new1}, and $LL_{new1} = U_{zw}.S_{zP_zw}.{V_{zw}}^T$

Step 7: Obtain the scrambled watermark image by the formula of $W_{dnew} = (LL_{new1} - S_{zP_z})/\propto$.

Step 8: Decrypt the cipher image J_z to get the plain image of scrambling parameters by using the private key (d_z,N_z).

Step 9: Using the scrambling parameters, quantum logistics was used to extract the watermark image W.

As a result, the proposed deep learning-based image watermarking algorithm withstands various attacks, and the original image has been extracted very accurately. The proposed algorithm enhances watermark extraction accuracy and robustness by leveraging ResNet-50 for superior feature extraction and faster processing. It effectively withstands various attacks while preserving high imperceptibility compared to other models. The proposed ResNet-50 model attains higher performance than other CNN models, like DarkNet-53, in its unique design. It uses residual learning to solve the vanishing gradient issue and improves the model's ability to train deeper networks. ResNet-50's skip connections

retain essential features as the network deepens, ensuring no critical information is lost. This leads to better feature extraction, particularly important for tasks like digital watermarking, where preserving subtle details is crucial. Compared to models like DarkNet-53, which also offers strong performance, ResNet-50 is more optimized for tasks requiring accuracy and computational efficiency. Its ability to balance depth with reduced complexity makes it particularly suitable for watermark extraction since it offers faster training and inference times than other models and improves robustness while retaining high imperceptibility. Moreover, the following section describes the implementation and comparison results of the proposed approach.

5 Experimental Results and Discussions

This section outlines the implementation results and evaluates the performance of our proposed system by comparing it with existing methods. It also includes case studies for this proposed research. All the experiments were conducted in an Intel Core i5 machine with 1TB HDD and 8 GB RAM, operating in a Windows 10 operating system environment, using MATLAB 2018a software.

5.1 Dataset Description

A series of experiments were conducted to evaluate the effectiveness of the proposed watermarking strategy, and the results were compared with other approaches. As shown in Fig. 3, the grey-scale cameraman image of 256×256 is used in this article to implement the proposed deep learning-based high-secure watermarking algorithm. Fig. 4a,b illustrates the host image, and the RSA and SHA-3 embed watermarked images with quantum logistics algorithm. It is extracted by the deep learning process such as ResNet-50, illustrated in Fig. 4c. While Fig. 4a shows the original image, Fig. 4b shows the watermarked image, which was created using a combination of Lifting Wavelet Transformation (LWT) and Singular Value Decomposition (SVD), with a scaling factor of 0.1 with motion blur. The extracted watermark from the watermarked image is shown in Fig. 4c, and the obtained image is in a chaotic state.

Figure 3: Cameraman image. Reprinted from Reference [48]

Figure 4: Watermarked and Extracted watermark image

5.2 Performance Parameters

The proposed watermarking strategy's performance was evaluated using three widely used methods: PSNR, NCC, and SSIM.

5.2.1 Peak Signal-to-Noise Ratio (PSNR)

The Peak Signal to Noise Ratio (PSNR) calculates the peak error between the cover image and the image with embedded additional information. Its formula is as follows:

$$PSNR = 10\log 10\frac{255}{MSE};\ \text{MSE} = \frac{1}{m_z \times n_z}\sum_{i=1}^{m_z}\sum_{j}^{n_z}(P_z - P_{zw})^2 \tag{25}$$

MSE indicates for mean square error, the size of the image is represented as $m_z \times n_z$, P_z is the matrix of the original host image, and P_{zw} is the matrix of the watermarked image in this mathematical formula. PSNR is measured in decibels (dB).

Fig. 5 illustrates the PSNR value of the different scaling factors. The proposed high-secure algorithm RSA with SHA-3 indicates that a higher PSNR value corresponds to less image visibility distortion.

5.2.2 Normalized Cross-Correlation (NCC)

NCC is abbreviated for Normalized Cross-Correlation, which makes evaluating the quality of extracted data easier. The NCC formula can be used to determine the degree of similarity between the original watermark and the watermark extracted from the watermarked image:

$$NCC = \frac{\sum_{i=1}^{m_z}\sum_{j=1}^{n_z}(W_d.W)}{\sqrt{\sum_{i=1}^{m_z}\sum_{j=1}^{n_z}(W_d.W)}\sqrt{\sum_{i=1}^{m_z}\sum_{j=1}^{n_z}(W_d.W)}} \tag{26}$$

where W_d is the matrix of the original watermark, and W is the matrix of the extracted watermark in this formula. NCC values range from 0 to 1.

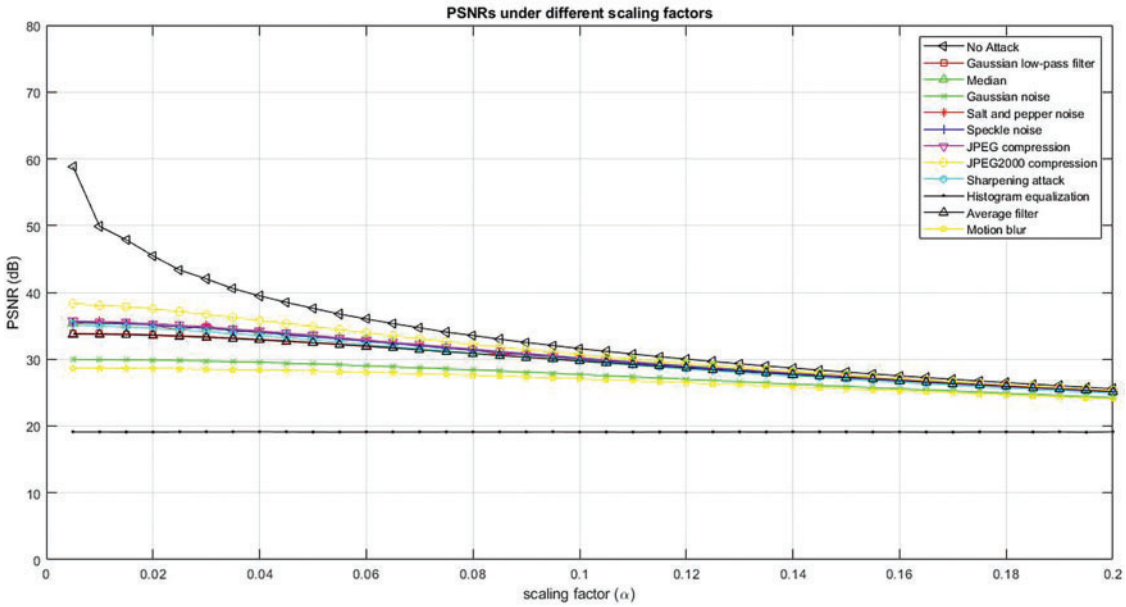

Figure 5: PSNR under different scaling factors

The proposed deep learning-based extraction, such as ResNet-50, extracts the watermark image from the original watermarked image. It is observed that the higher the value, the better the watermarking scheme's performance, as shown in Fig. 6.

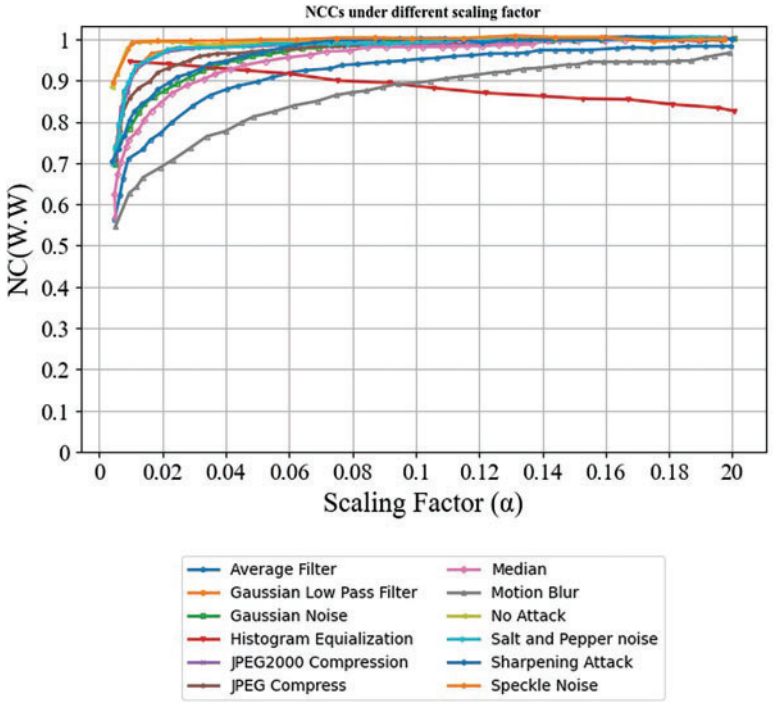

Figure 6: NCC under different scaling factors

5.2.3 Structural Similarity Index Measure (SSIM)

SSIM, derived as described in Eq. (27), is another evaluating measure used in this research.

$$SSIM = P(J,K)\, Q(J,K)\, , R(J,K) \tag{27}$$

$$P(J,K) = \frac{2\mu_J\mu_K + A_1}{\mu_J^2 + \mu_K^2 + A_1} \tag{28}$$

$$Q(J,K) = \frac{2\sigma_J\sigma_K + A_2}{\sigma_J^2 + \sigma_K^2 + A_2} \tag{29}$$

$$R(J,K) = \frac{\sigma_{JK} + A_3}{\sigma_J\sigma_K + A_3} \tag{30}$$

Eq. (28) compares the image's luminance. It assists in determining the degree of similarity between the mean luminance. μ_J and μ_K of images. When $\mu_J = \mu_K$, it means that the similarity factor is at its maximum and equals 1. Eq. (29) contains a function that is used to calculate contrast. It determines the closeness and contrasting characteristics of the two images; σ_J and σ_K are Standard deviation. When $\sigma_J = \sigma_K$, the factor is at its maximum and equal to one. When comparing image structures, the expression in Eq. (30) is employed to get the correlation coefficient between the images (J and K). σ_{JK} stands for covariance between images J and K. The positive constants A_1, A_2, and A_3 are utilized to avoid divide-by-zero errors.

Fig. 7 denotes the proposed method's SSIM. Our proposed method calculates the images' mean, standard deviation, and variance using SSIM. Thus, the DNN provides fast and accurate extraction.

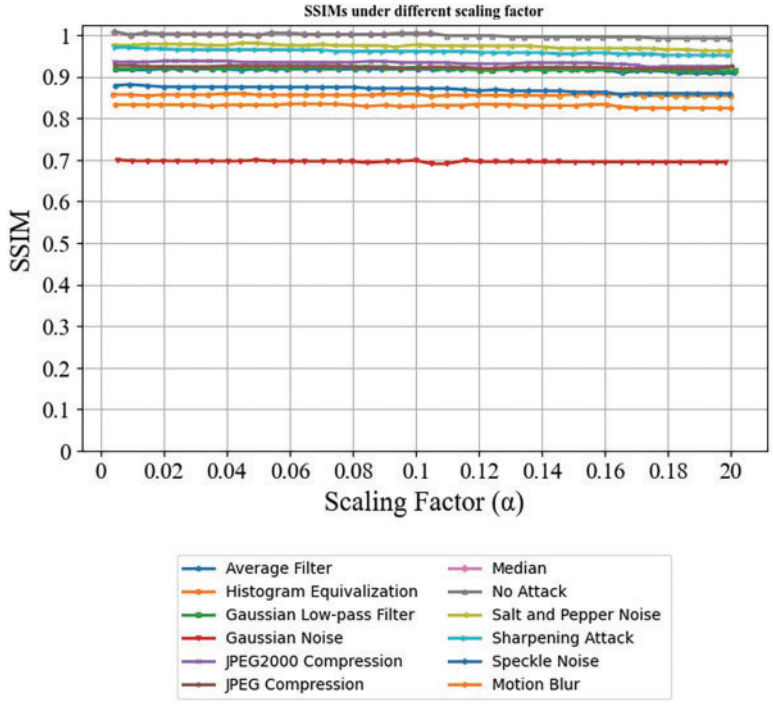

Figure 7: SSIM under the different scaling factors

5.2.4 Invisibility Performance

Fig. 8 illustrates the invisibility performance of the image with no attacks performed by the proposed deep learning-based high secure algorithm.

Figure 8: Invisibility performance

The watermark image varies with a scaling factor of 0.05. The PSNR value of the watermarked image size is 256 × 256, 128 × 128, and 64 × 64, such as 37.6179, 43.3941, and 49.2083, respectively. The SSIM values of the size of watermarked images 256 × 256, 128 × 128, and 64 × 64 are 0.99926, 0.99973, and 0.99992, respectively. The NCC values of the extracted watermark image are 0.99996, 0.99961, and 0.99741, respectively. The proposed algorithm's calculation time of 0.5 s is needed to process a 256 × 256 greyscale picture. The processing time rises to 1.2 s for a 512 × 512 greyscale picture. The calculation time for a 10-s movie at 30 frames per second is 15 s. A minute-long video takes 90 s to process.

5.2.5 Proposed NPCR and UACI

To measure the intensity of cipher pictures, two protocols can be used: a) the pixel number change rate (NPCR), and b) the uniform average change (UACI). The UACI and NPCR are calculated using the following formulas:

$$NPCR\left(J_z\right) = \sum_{i=1}^{M_z} \sum_{j=1}^{N_z} \frac{D_z\left(i,j\right)}{M_z \times N_z} \times 100\% \tag{31}$$

$$UACI\left(J_z\right) = \sum_{i=1}^{M_z} \sum_{j=1}^{N_z} \frac{C_{z1}\left(i,j\right) - C_{z2}\left(i,j\right)}{M_z \times N_z \times 225} \times 100\% \tag{32}$$

where $M_z \times N_z$ denotes the length and width of the image, $D_z\left(i,j\right)$ denotes a pixel in the image D_z row i and column j are calculated by Eq. (16).

Fig. 9 shows NPCR and UACI values for various pixel values at different locations in the image. The anticipated values of NPCR and UACI between two random 8-bit grayscale images are 99.79% and 38.62%, respectively. The test results show that the algorithm can withstand differential attacks.

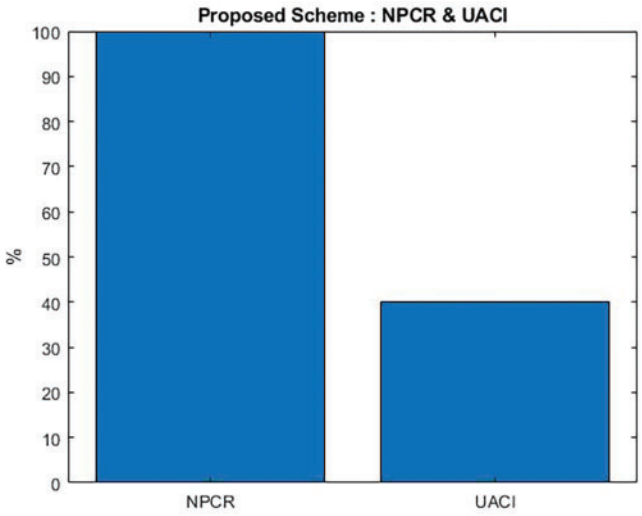

Figure 9: Proposed NPCR and UACI

5.3 Comparison Analysis

This section describes the proposed technique's results, comparing our novel technique with the baseline approach, such as the Blind Watermarking Algorithm [49], two-dimensional Discrete Cosine Transform (2D-DCT) [50], Clifford Algebra [44], Multidimensional Fourier Transforms [51], Non-Subsampled Contourlet Transform (NSCT) [52], and Color Image Watermarking Scheme [53].

Fig. 10 illustrates the overall comparison of the Peak Signal-to-Noise Ratio (PSNR). The PSNR of the proposed technique attains higher PSNR by using the Deep Learning-Based Digital Image Watermarking Model with High Secure Algorithms. Our proposed approach compared with the baseline Blind Watermarking Algorithm [49], two-dimensional Discrete Cosine Transform (2D-DCT) [50], and Clifford Algebra [44] such as 56.02%, 37.66%, and 56.7%. Thus, our novel technique obtained a PSNR of 49.83%, which is higher than the existing methods.

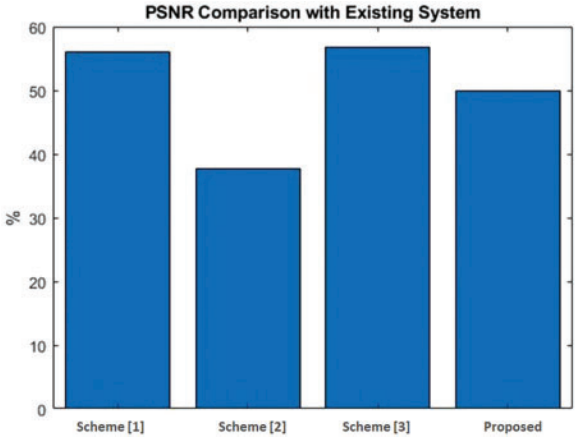

Figure 10: Comparison of Peak Signal-to-Noise Ratio (PSNR). Scheme [1]: Blind Watermarking Algorithm, Yuan et al., 2020 [49]; Scheme [2]: Two-dimensional Discrete Cosine Transform, Tsui et al., 2008 [50]; Scheme [3]: Clifford Algebra, Bhatti et al., 2020 [44]

Fig. 11 illustrates the overall comparison of the Structural Similarity Index Measure (SSIM). The SSIM of the proposed technique attains higher SSIM by using the Deep Learning-Based Digital Image Watermarking Model with High Secure Algorithms. Our proposed approach compared with the baseline Blind Watermarking Algorithm [49], two-dimensional Discrete Cosine Transform (2D-DCT) [50], and Clifford Algebra [44] such as 0.959%, 0.93%, and 0.97%. Thus, our novel technique has obtained an SSIM of 0.98%, which is higher than the existing techniques.

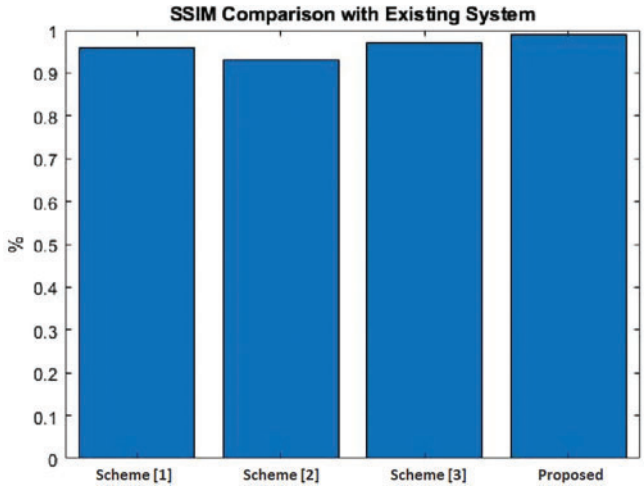

Figure 11: Comparison of structural similarity index measure (SSIM). Scheme [1]: Blind Watermarking Algorithm, Yuan et al., 2020 [49]; Scheme [2]: Two-dimensional Discrete Cosine Transform, Tsui et al., 2008 [50]; Scheme [3]: Clifford Algebra, Bhatti et al., 2020 [44]

Fig. 12 compares the overall Number of Pixel Change Rates (NPCR). The NPCR of the proposed technique attains higher NPCR by using the Deep Learning-Based Digital Image Watermarking Model with High Secure Algorithms. Our proposed approach compared with the baseline Multi-dimensional Fourier Transforms [51], Non-Subsampled Contourlet Transform (NSCT) [52], Color Image Watermarking Scheme [53], and Clifford Algebra [44] such as 99.16%, 99.56%, and 99.59%. Thus, our novel technique obtained an NPCR of 99.79%, higher than the existing techniques.

5.4 Discussion

The performance metrics for our proposed Deep Learning-Based Digital Image Watermarking Model with High Secure Algorithms reveal significant improvements over existing methods. Our technique's Peak Signal-to-Noise Ratio (PSNR) stands at 49.83%, demonstrating that while it is slightly lower than some baseline methods, it still effectively preserves image quality with minimal distortion. Regarding the Structural Similarity Index (SSIM), our approach achieves a value of 0.98%, surpassing the SSIM values of several baseline techniques. This indicates that our model maintains the watermarked image's structural integrity, ensuring it remains close to the original image. When evaluating the Number of Pixels Change Rate (NPCR), our method reaches a rate of 99.79%. This is higher than the rates of other methods, showing that our technique is highly effective in managing pixel changes and enhancing watermark robustness.

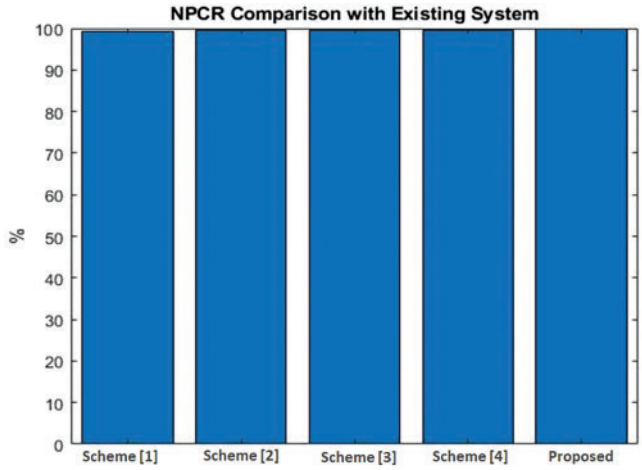

Figure 12: Comparison of number of pixels change rate (NPCR). Scheme [1]: Multidimensional Fourier Transforms, Tsui et al., 2008 [51]; Scheme [2]: Non-Subsampled Contourlet Transform, Niu et al., 2011 [52]; Scheme [3]: Color Image Watermarking Scheme, Chou et al., 2010 [53]; Scheme [4]: Clifford Algebra, Bhatti et al., 2020 [44]

Overall, these results highlight the strengths of our proposed model in delivering high-quality, structurally intact, and robust watermarking compared to traditional techniques. Our method begins by processing video inputs and extracting frames to break the video into manageable pieces. These frames are preprocessed to enhance quality, followed by feature extraction using a combination of Convolutional Neural Networks (CNN) and Temporal Convolutional Networks (TCN). This combination allows the model to capture spatial details and temporal patterns across frames. Once the features are extracted, the frames are grouped or clustered based on a certain threshold, which helps filter out less relevant information. The next step involves an attention-based transformer, which focuses on the most critical frames and summarizes them into a meaningful sequence, effectively reducing the complexity of the data while keeping the necessary information intact. This streamlined process helps handle extensive video data by focusing on essential aspects, leading to efficient and accurate analysis.

5.5 Case Study

This section includes several case studies showing how well the proposed deep learning-based digital watermarking model works against various image attacks. Every case study showcases the model's accuracy, imperceptibility, and robustness in maintaining watermark quality across different circumstances and offers performance metrics and comparisons to conventional approaches.

Case 1: Performance under JPEG Compression

Scenario: JPEG compression is a popular attack vector for digitally watermarked images. This attack may severely impact the watermark's detectability and quality.

Example: After applying JPEG compression with different quality factors (e.g., 50%, 70%, 90%), the proposed methodology attained a PSNR of 49.83% and an SSIM of 0.98 in research, comparing the performance of the proposed model with standard methods. However, under identical conditions, traditional approaches demonstrated a significant fall in PSNR and SSIM values, suggesting that the proposed model maintains stronger imperceptibility and robustness.

Case 2: Resistance to Gaussian Noise

Scenario: Gaussian noise is another prevalent attack that can cause image degradation and hinder the extraction of watermarks.

Example: The proposed model demonstrated resistance against noise by maintaining a high PSNR of 49.83% and SSIM of 0.98 in experiments where watermarked images were subjected to Gaussian noise with a mean of 0 and a standard deviation of 25. These measures were generally lower for traditional approaches, demonstrating the proposed model's greater resilience.

Case 3: Robustness to Rotation and Scaling Attacks

Scenario: Rotation and scaling attacks can change the position and size of the watermark, making precise extraction difficult.

Example: The proposed model showed consistent accuracy in watermark extraction with minimal performance reduction when applying rotation (up to 30 degrees) and scaling (up to 1.2x) adjustments. Similar conditions proved too difficult for traditional methods, demonstrating the robustness of the proposed methodology.

6 Conclusions

This research introduces a deep learning-based digital image watermarking model with advanced security algorithms aimed at achieving superior watermark quality and robustness. The proposed method excels in maintaining image imperceptibility and resilience against attacks, demonstrating improved performance over existing techniques. By incorporating the proposed RSA and SHA-3 algorithms, the model exhibits enhanced imperceptibility, robustness, and accuracy in watermark extraction compared to traditional PSNR, SSIM, and NPCR methods. It achieves a PSNR of 49.83%, an SSIM of 0.98%, and an NPCR of 99.79%, reflecting its effectiveness in delivering higher quality and security. The study finds that the proposed model significantly enhances watermark imperceptibility and robustness through advanced encryption and deep learning techniques. However, the reliance on complex algorithms may increase computational demands. Traditional watermarking systems often face limitations such as inadequate robustness against attacks and insufficient security measures, making them vulnerable to unauthorized access and tampering. Future work should explore integrating adaptive algorithms to enhance watermark resilience further and investigate real-time applications of the proposed model in dynamic environments.

Acknowledgement: This research is part of the Ph.D. work. The authors thank GIET University, Gunupur, and Utkal University, Bhubaneswar, for supporting necessary research.

Funding Statement: The authors received no specific funding for this study

Author Contributions: The authors confirm contributions to the paper as follows: study conception and design: Satya Narayan Das and Mrutyunjaya Panda; data collection: Satya Narayan Das; analysis and interpretation of results: Satya Narayan Das and Mrutyunjaya Panda; draft manuscript preparation: Satya Narayan Das; supervision: Mrutyunjaya Panda. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The authors declare that the image databases are publicly available in public repositories. The database details used are presented within the article, and references are given.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

References

[1] F. Cayre, C. Fontaine, and T. Furon, "Watermarking security: Theory and practice," *IEEE Trans. Signal Process.*, vol. 53, no. 10, pp. 3976–3987, 2005. doi: 10.1109/TSP.2005.855418.

[2] A. Tareef and A. Al-Ani, "A highly secure oblivious sparse coding-based watermarking system for ownership verification," *Expert Syst. Appl.*, vol. 42, no. 4, pp. 2224–2233, 2015. doi: 10.1016/j.eswa.2014.09.055.

[3] H. Berghel and L. O'Gorman, "Protecting ownership rights through digital watermarking," *Computer*, vol. 29, no. 7, pp. 101–103, 1996. doi: 10.1109/2.511977.

[4] R. Caldelli, F. Francesco, and R. Becarelli, "Reversible watermarking techniques: An overview and a classification," *EURASIP J. Inform. Security.*, vol. 2010, no. 1, 2010, Art. no. 134546. doi: 10.1155/2010/134546.

[5] B. Gunjal and R. R. Manthalkar, "An overview of transform domain robust digital image watermarking algorithms," *J. Emerg. Trends Comput. Inform. Sci.*, vol. 2, no. 1, pp. 37–42, 2010.

[6] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, *Digital Watermarking and Steganography*. Burlington, MA, USA: Morgan Kaufmann, 2008.

[7] F. Y. Shih, *Digital Watermarking and Steganography: Fundamentals and Techniques*, 2nd ed. Boca Raton, FL, USA: CRC Press, 2017.

[8] X. Kang, J. Huang, Y. Q. Shi, and Y. Lin, "A DWT-DFT composite watermarking scheme robust to both affine transform and JPEG compression," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 13, no. 8, pp. 776–786, 2003. doi: 10.1109/TCSVT.2003.815957.

[9] A. A. Tamimi, A. M. Abdalla, and O. Al-Allaf, "Hiding an image inside another image using variable-rate steganography," *Int. J. Adv. Comput. Sci. Appl.*, vol. 4, no. 10, pp. 18–21, 2013. doi: 10.14569/IJACSA.2013.041004.

[10] N. Nikolaidis and I. Pitas, "Robust image watermarking in the spatial domain," *Signal Process.*, vol. 66, no. 3, pp. 385–403, 1998. doi: 10.1016/S0165-1684(98)00017-6.

[11] J. -C. Liu and S. -Y. Chen, "Fast two-layer image watermarking without referring to the original image and watermark, image," *Vis Comput.*, vol. 19, no. 14, pp. 1083–1097, 2001. doi: 10.1016/S0262-8856(01)00068-3.

[12] M. Cedillo-Hernandez, F. Garcia-Ugalde, M. Nakano-Miyatake, and H. Perez-Meana, "Robust watermarking method in DFT domain for effective management of medical imaging," *Signal Image Video Process.*, vol. 9, no. 5, pp. 1163–1178, 2015. doi: 10.1007/s11760-013-0555-x.

[13] S. P. Singh and G. Bhatnagar, "A new robust watermarking system in integer DCT domain," *J. Vis. Commun. Image Represent.*, vol. 53, no. 5, pp. 86–101, 2018. doi: 10.1016/j.jvcir.2018.03.006.

[14] M. Ouhsain and A. B. Hamza, "Image watermarking scheme using non-negative matrix factorization and wavelet transform," *Expert Syst. Appl.*, vol. 36, no. 2, pp. 2123–2129, 2009. doi: 10.1016/j.eswa.2007.12.046.

[15] Y. -S. Lee, Y. -H. Seo, and D. -W. Kim, "Digital blind watermarking based on depth variation prediction map and DWT for DIBR free-viewpoint image," *Signal Process. Image Commun.*, vol. 70, no. 12, pp. 104–113, 2019. doi: 10.1016/j.image.2018.09.004.

[16] V. S. Verma, R. K. Jha, and A. Ojha, "Significant region based robust watermarking scheme in lifting wavelet transform domain," *Expert Syst. Appl.*, vol. 42, no. 21, pp. 8184–8197, 2015. doi: 10.1016/j.eswa.2015.06.041.

[17] B. E. Khoo, N. M. Makbol, and T. H. Rassem, "Block-based discrete wavelet transform-singular value decomposition image watermarking scheme using human visual system characteristics," *IET Image Process.*, vol. 10, no. 1, pp. 34–52, 2015. doi: 10.1049/iet-ipr.2014.0965.

[18] M. Islam, A. Roy, and R. H. Laskar, "SVM-based robust image watermarking technique in LWT domain using different sub-bands," *Neural Comput. Appl.*, vol. 32, no. 5, pp. 1379–1403, 2020. doi: 10.1007/s00521-018-3647-2.

[19] S. Boujerfaoui, R. Riad, H. Douzi, F. Ros, and R. Harba, "Image watermarking between conventional and learning-based techniques: A literature review," *Electronics*, vol. 12, no. 1, 74, pp. 1–39, 2023. doi: 10.3390/electronics12010074.
[20] Y. Dong, R. Yan, Q. Zhang, and X. Wu, "A hybrid domain color image watermarking scheme based on hyperchaotic mapping," *Mathematics*, vol. 12, no. 12, 2024, Art. no. 1859. doi: 10.3390/math12121859.
[21] H. -Y. Yang, X. -Y. Wang, and C. -P. Wang, "A robust digital watermarking algorithm in undecimated discrete wavelet transform domain," *Comput. Elect. Eng.*, vol. 39, no. 3, pp. 893–906, 2013. doi: 10.1016/j.compeleceng.2012.07.009.
[22] Y. Liu, M. Guo, J. Zhang, Y. Zhu, and X. Xie, "A novel two-stage separable deep learning framework for practical blind watermarking," in *Proc. 27th ACM Int. Conf. Multimedia*, 2019, pp. 1509–1517. doi: 10.1145/3343031.3351025.
[23] B. Czaplewski and R. Rykaczewski, "Matrix-based robust joint fingerprinting and decryption method for multicast distribution of multimedia," *Signal Process.*, vol. 111, no. 6, pp. 150–164, 2014. doi: 10.1016/j.sigpro.2014.12.026.
[24] L. Yang, S. Tang, R. Liu, L. Zhang, and Z. Ma, "Secure and robust digital image watermarking scheme using logistic and RSA encryption," *Expert. Syst. Appl.*, vol. 97, pp. 95–105, 2018. doi: 10.1016/j.eswa.2017.12.003.
[25] B. Czaplewski, "Joint fingerprinting and decryption method for color images based on quaternion rotation with cipher chaining," *J. Vis. Commun. Image Represent.*, vol. 40, no. 15, pp. 1–13, 2016. doi: 10.1016/j.jvcir.2016.06.006.
[26] W' H. Alshoura, Z. Zainol, J. S. Teh, and M. Alawida, "A new chaotic image watermarking scheme based on SVD and IWT," *IEEE Access*, vol. 8, pp. 43391–43406, 2020. doi: 10.1109/ACCESS.2020.2978186.
[27] R. Sinhal and I. A. Ansari, "A multipurpose image watermarking scheme for digital image protection," *Int. J. Syst. Assur. Eng. Manag.*, vol. 11, no. 2, pp. 274–286, 2020. doi: 10.1007/s13198-019-00855-0.
[28] X. Zhong, P. -C. Huang, S. Mastorakis, and F. Y. Shih, "An automated and robust image watermarking scheme based on deep neural networks," *IEEE Trans. Multimedia*, vol. 23, pp. 1951–1961, 2020. doi: 10.1109/TMM.2020.3006415.
[29] P. Ali and H. Mahdavi-Nasab, "A robust digital image watermarking scheme based on bat algorithm optimization and SURF detector in SWT domain," *Multimed. Tools Appl.*, vol. 79, no. 29, pp. 21653–21677, 2020. doi: 10.1007/s11042-020-08960-0.
[30] E. E. Abdallah, F. O. Ahmed, A. E. Abdallah, M. Bsoul, and S. Awwad, "A hybrid secure watermarking scheme using nonnegative matrix factorization and Fast Walsh-Hadamard transform," *J. Appl. Secur. Res.*, vol. 15, no. 2, pp. 185–198, 2020. doi: 10.1080/19361610.2019.1624100.
[31] S. Alam, T. Ahmad, and M. Doja, "A novel hybrid watermarking scheme with Image authentication based on frequency domain, 2-Level SVD using chaotic map," *EAI Endorsed Trans. Energy Web*, vol. 8, no. 31, 2020, Art. no. e7. doi: 10.4108/eai.13-7-2018.165512.
[32] M. Jana and B. Jana, "A new DCT based robust image watermarking scheme using cellular automata," *Inform. Secur. J.: A Global Perspect.*, vol. 31, no. 5, pp. 1–17, 2021. doi: 10.1080/19393555.2021.1956023.
[33] S. Helal and N. Salem, "A hybrid watermarking scheme using walsh hadamard transform and SVD," *Procedia Comput. Sci.*, vol. 194, no. 1, pp. 246–254, 2021. doi: 10.1016/j.procs.2021.10.080.
[34] M. M. Eltoukhy, A. E. Khedr, M. M. Abdel-Aziz, and K. M. Hosny, "Robust watermarking method for securing color medical images using Slant-SVD-QFT transforms and OTP encryption," *Alex. Eng. J.*, vol. 78, no. 2, pp. 517–529, 2023. doi: 10.1016/j.aej.2023.07.068.
[35] S. Mellimi, V. Rajput, I. A. Ansari, and C. W. Ahn, "A fast and efficient image watermarking scheme based on Deep Neural Network," *Pattern Recognit. Lett.*, vol. 151, no. 1, pp. 222–228, 2021. doi: 10.1016/j.patrec.2021.08.015.
[36] A. Guntoro and M. Glesner, "A lifting-based discrete wavelet transform and discrete wavelet packet processor with support for higher order wavelet filters," in *VLSI-SoC 2008, IFIP AICT 313*, C. Piguet, R. Reis, and D. Soudris, Eds. USA: IEEE, 2010, pp. 154–173.

[37] M. Khan, A. Kushwaha, and T. Verma, "Evaluating digital image watermarking based on image interlacing, DWT & DCT," *Int. J. Comput. Sci. Inform. Technol.*, vol. 7, no. 1, pp. 11–17, 2016. http://ijcsit.com/docs/Volume%207/vol7issue1/ijcsit2016070103.pdf.

[38] R. Mehta, N. Rajpal, and V. P. Vishwakarma, "A robust and efficient image watermarking scheme based on Lagrangian SVR and lifting wavelet transform," *Int. J. Mach. Learn. Cybern.*, vol. 8, no. 2, pp. 379–395, 2017. doi: 10.1007/s13042-015-0331-z.

[39] V. S. Verma and R. K. Jha, "An overview of robust digital image watermarking," *IETE Tech. Rev.*, vol. 32, no. 6, pp. 479–496, 2015. doi: 10.1080/02564602.2015.1042927.

[40] Ç. K. Koç, F. Özdemir, and Z. Ödemiş Özger, "Rivest-shamir-adleman algorithm," in *Partially Homomorphic Encryption*. Cham: Springer, 2021, pp. 37–41. doi: 10.1007/978-3-030-87629-6_3.

[41] A. Rojat, "Review of cryptanalysis of RSA and its variants by Jason Hinek," *ACM SIGACT News*, vol. 43, no. 1, pp. 16–18, 2012. doi: 10.1145/2160649.2160654.

[42] A. Kunhu, S. A. Mansoori, and H. Al-Ahmad, "A novel reversible watermarking scheme based on SHA3 for copyright protection and integrity of satellite imagery," *IJCSNS Int. J. Comput. Sci. Netw. Secur.*, vol. 19, no. 3, pp. 92–102, Mar. 2019.

[43] G. Ye, K. Jiao, and X. Huang, "Quantum logistic image encryption algorithm based on SHA-3 and RSA," *Nonlinear Dyn.*, vol. 104, no. 3, pp. 2807–2827, 2021. doi: 10.1007/s11071-021-06422-2.

[44] U. A. Bhatti *et al.*, "Hybrid watermarking algorithm using clifford algebra with arnold scrambling and chaotic encryption," *IEEE Access*, vol. 8, pp. 76386–76398, 2020. doi: 10.1109/ACCESS.2020.2988298.

[45] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," Technical Report, 2015. doi: 10.48550/arXiv.1512.03385.

[46] B. Koonce, "ResNet 50," in *Convolutional Neural Networks with Swift for Tensorflow*. Berkeley, CA, USA: Apress, 2021.

[47] L. Ali, F. Alnajjar, H. A. Jassmi, M. Goocho, W. Khan and M. A. Serhani, "Performance evaluation of deep CNN-based crack detection and localization techniques for concrete structures," *Sensors*, vol. 21, no. 5, 2021, Art. no. 1688. doi: 10.3390/s21051688.

[48] J. Bush, "C4L Image Dataset," *IEEE Dataport*. Accessed: Sep. 27, 2024. [Online]. Available: https://dx.doi.org/10.21227/bc9m-f507

[49] H. -T. Hu, L. -Y. Hsu, and H. -H. Chou, "An improved SVD based blind color image watermarking algorithm with mixed modulation incorporated," *Inform. Sci.*, vol. 519, pp. 161–182, 2020. doi: 10.1016/j.ins.2020.01.019.

[50] Z. Yuan, L. Decheng, Z. Xueting, and S. Qingtang, "New image blind watermarking method based on two-dimensional discrete cosine transform," *Optik*, vol. 204, no. 9, 2020, Art. no. 164152. doi: 10.1016/j.ijleo.2019.164152.

[51] T. K. Tsui, X. -P. Zhang, and D. Androutsos, "Color image watermarking using multidimensional Fourier transforms," *IEEE Trans. Inf. Forensics Secur.*, vol. 3, no. 1, pp. 16–28, 2008. doi: 10.1109/TIFS.2007.916275.

[52] P. -P. Niu, X. -Y. Wang, Y. -P. Yang, and M. -Y. Lu, "A novel color image watermarking scheme in nonsampled contourlet-domain," *Expert. Syst. Appl.*, vol. 38, no. 3, pp. 2081–2098, 2011. doi: 10.1016/j.eswa.2010.07.147.

[53] C. H. Chou and K. C. Liu, "A perceptually tuned watermarking scheme for color images," *IEEE Trans. Image Process.*, vol. 19, no. 11, pp. 2966–2982, 2010. doi: 10.1109/TIP.2010.2052261.