




Integrating encryption and watermarking for enhanced information transmission security

Hadi Nazari , Mahmoud Mahlouji Bidgoli* , Hossein Ghasvari 

Department of Electrical and Telecommunication Engineering, Kashan Branch, Islamic Azad University, Kashan, Iran.

*Corresponding author: mmahlouji@yahoo.com

Original Research

Abstract:

Received:
22 February 2024
Revised:
10 March 2024
Accepted:
21 March 2024
Published online:
3 June 2024

© The Author(s) 2024

With the digital world booming, so too has the importance of information security. Ensuring safe transmission of data has become paramount, requiring robust mechanisms to navigate potential vulnerabilities. In this context, encryption and watermarking technologies emerge as key players. This article proposes a groundbreaking method that seamlessly integrates a lightweight encryption scheme with a dedicated watermarking approach for color images. Our proposed technique boasts two key advantages: efficient encryption and successful watermark concealment. The chosen encryption method is computationally light, meaning it requires minimal processing power, yet still effectively shields the embedded watermark. This watermarking process involves a clever two-step transformation. First, the color image is converted into a different color space using the Triangle Vertex Transform (TVT). This lays the groundwork for the second step, where the watermark itself is embedded. For this, we leverage a clever combination of the 2-level Discrete Wavelet Transform (DWT) and the Discrete Cosine Transform (DCT). To gauge the effectiveness of this innovative approach, we put it to the test using popular color images and evaluated it through various metrics. These include standard measures like histogram analysis, correlation, Peak Signal-to-Noise Ratio (PSNR), and Structural Similarity Index (SSIM). These metrics help us understand the success of both the encryption and watermarking aspects. The results speak for themselves: our proposed method achieves an impressive PSNR of 54.4798 dB and a near-perfect SSIM score of 1. This translates to a watermarked image with exceptional quality, practically indistinguishable from the original. Ultimately, this research presents a novel technique that shines in both robustness and imperceptibility, outperforming many existing state-of-the-art methods. This paves the way for safeguarding information with greater efficiency and accuracy, enhancing the reliability of our digital interactions in an increasingly interconnected world.

Keywords: Information security; Watermarking; Encryption; Triangle Vertex Transform (TVT); DWT; DCT

1. Introduction

Encryption and watermarking are essential components in ensuring the security of information during its transit. Encryption is a process that guarantees the secrecy of data by using cryptographic techniques to encode it. On the other hand, watermarking is a technique that involves embedding undetectable identifiers into the data to verify its validity and integrity. These strategies are particularly significant within the Internet of Things (IoT) field, where sensitive information is transmitted over IoT. The advent of the IoT has resulted in notable improvements and implementations

across different industries, transforming how we live and work, such as healthcare, environmental monitoring, industrial automation and manufacturing, and smart cities [1]. The IoT will affect many things, including the information process, social, commercial, and even industrial processes. The internet of things has yielded many advantages, such as heightened operational effectiveness, financial savings, excellent decision-making capabilities, and enhanced user experiences. As technology evolves, we can expect even more innovative solutions and advancements in various industries [2]. The IoT is experiencing widespread adoption and integration across multiple fields globally. Consequently,

specific industries are at the forefront of investing in this transformative technology, altering our daily lives and professional environments [3–5]. IoT has witnessed significant developments and applications in various industries, revolutionizing our lives and work.

The security, privacy, and authentication concerns at the presentation level are significant issues in the flow of information among IoT devices on a broad scale. In recent years, scholars have seen a substantial utilization of encryption and watermarking applications in content authentication and data security. Image encryption and watermarking have emerged as popular solutions for image protection in IoT applications, owing to their notable advantages over standard data-hiding methods at the presentation layer. In the given circumstance, a problem exists to develop a framework that can effectively provide a high level of resilience against a wide range of lawful and lawless data distortions. The researchers face a significant problem of maintaining a trade-off between imperceptibility and capacity while ensuring robustness [3, 6, 7].

Image encryption is a crucial technique to secure images by transforming them into an unreadable format using mathematical algorithms [8, 9]. This process ensures the confidentiality and integrity of sensitive visual data in various applications, including IoT systems. In IoT systems, which involve interconnected devices communicating and exchanging data, image encryption is vital in enhancing privacy and security. Encrypting images prevents unauthorized access and deciphering visual information, ensuring the confidentiality of sensitive content. Moreover, image encryption protects against cyberattacks and malicious activities, making it an essential component of the security infrastructure in IoT systems. With IoT devices constantly generating and transmitting large volumes of data, including images, encryption helps safeguard against unauthorized interception and manipulation of these visual assets. The main advantage of image encryption in IoT systems is the preservation of data confidentiality during transmission and storage [10–12].

Several methods of image encryption are suitable for IoT applications. One approach is to use lightweight block ciphers optimized for resource-constrained devices. These ciphers are designed to be efficient and require minimal processing power and memory. They can be implemented on microcontrollers and other low-power devices commonly used in IoT applications [1]. Another approach is to use chaotic maps to generate encryption keys. In chaotic maps, chaotic behavior is evident. They are deterministic, but their behavior is highly sensitive to initial conditions. This makes them suitable for generating encryption keys that are difficult to predict. Several studies have proposed using chaotic maps to encrypt images in real time for IoT applications [13–15].

Image watermarking involves embedding a watermark within an image to safeguard copyright, establish ownership, and enhance resistance against tampering. In the IoT context, image watermarking is essential to secure the images IoT devices capture [16, 17].

Several digital image watermarking techniques can be used

in IoT applications. These techniques include spatial, frequency, and hybrid domain watermarking. The first involves embedding the watermark directly into the image's pixel values. Frequency domain watermarking consists of embedding in the frequency domain using techniques such as discrete wavelet transform (DWT) and discrete cosine transform (DCT). Hybrid domain watermarking combines spatial and frequency domain watermarking techniques for better security [16, 18, 19].

In addition to watermarking techniques, several approaches to secure watermarking in IoT applications exist. These approaches include using robust watermarking algorithms that can withstand cropping, scaling, and compression attacks. Another method is to use multi-level watermarking, which involves embedding multiple watermarks into the same image to provide redundancy and increase the robustness of the watermarking system [20, 21].

Color image watermarking is a technique that embeds imperceptible watermarks or hidden messages in color images. It offers advantages such as improved robustness against attacks, enhanced capacity for larger or multiple watermarks, high visual quality of watermarked images, compatibility with multimedia applications, and flexibility in watermark design. It enables adequate copyright protection, authentication, and tamper detection in color-based media, making it suitable for various applications [22, 23].

Safe and fast data transfer is significant in IoT systems; therefore, using encryption and watermarking is common. The significant challenges of the image encryption techniques are security and privacy concerns, real-time processing requirements, and limited resources, i.e., The integrity of the watermark must be preserved, notwithstanding any modifications made to the image. On the other hand, robustness is a significant challenge among the main challenges of the digital watermarking algorithms. However, ensuring robustness enhancement should not compromise the image's quality nor significantly diminish the embedding capability. Accordingly, article presents a novel combination of lightweight encryption and DWT-DCT-based color image watermarking for information transmission. The key contributions are as follows: 1) Utilizing lightweight encryption and watermarking techniques to reduce resource requirements. 2) Introducing a hybrid encryption approach that combines Feistel and Substitution-Permutation networks, providing significant security while maintaining computational simplicity. 3) Applying a three-step frequency domain watermarking strategy using TVT, 2-level DWT, and DCT, resulting in strong robustness. The proposed technique achieves improved watermark invisibility and outperforms existing state-of-the-art methods, as evidenced by experimental findings.

The remaining parts of this article are divided as follows: In section 2, related works are discussed, and the proposed combination method is represented in section 3. The experimental results and the comparisons are given in section 4, and the conclusion is clarified in section 5.

2. Related works

As mentioned before, using various encryption and watermarking methods can significantly help increase the security of the information sent. On the other hand, in terms of the large amount of information transferred in the network, reducing the data size can increase the speed of information exchange.

2.1 Image encryption

The surge in digital image transmission over the internet and various digital platforms has necessitated secure methods to protect the privacy and integrity of these images. Image encryption methods play a key role in achieving this objective. Many image encryption approaches have been proposed for various applications. Traditional image encryption methods mainly include substitution, permutation, and transformation-based algorithms. These methods are successful to a certain extent but often compromise the quality of the image and require excessive computational resources, making them unsuitable for real-time applications [24]. This study presents a novel approach to encryption based on the principles of substitution and permutation that utilizes a single S-Box for the encryption process, which exhibits high sensitivity to plaintext attacks and is more resistant to statistical attacks than state-of-the-art encryption algorithms [25]. A new study presents a novel approach to encryption based on substitution principles [26]; researchers have introduced a novel image encryption technique that utilizes bit permutation, a three-dimensional puzzle, and chaos to enhance confusion and diffusion. The findings have shown that it provides security against statistical and differential attacks. Chaos-Based Image Encryption is another approach to image encryption. Chaos-based image encryption has garnered considerable attention due to its sensitivity to initial conditions and randomness in output. Chaos theory is inherently complex and unpredictable, making it an effective tool for encryption. New methods like hyperchaos have been used to address the limitations of conventional chaos-based encryption [27]. Another method of this category [28] via a bit-pair level process and pixel level XOR operator has shown superiority over four other methods regarding robustness to differential attack. Chaos-based encryption techniques offer effective security measures that can be utilized to ascertain the key and the image decryption; however, a novel approach has been introduced, which enhances security while preserving the identical level of pixel entropy as the preceding technique [29]. DNA sequence-based image encryption is a recent and effective approach. This approach is a bio-inspired scheme that uses the properties of DNA sequences for image encryption. These substitution and permutation methods use DNA sequence operations [30]. The DNA-based encryption techniques are known for their high security due to the complexity and variability of DNA sequences. A cryptosystem based on DNA chaos is proposed for medical image encryption, in which the cryptographic system exhibits resistance against many attacks, including known-plaintext and chosen-plaintext attacks. It has high security with an acceptable processing time [31]. This research introduces a novel image encryption technique that

utilizes a one-dimensional Logistic mapping, DNA coding sequence, and an arithmetic sequence scrambling model. The suggested approach effectively demonstrates the ability to withstand typical plaintext, noise, clipping attacks, and noise attacks and has a good encryption effect [32]. Quantum Image Encryption is a powerful encryption approach. Quantum image encryption methods are based on quantum mechanics, providing higher security and computational speed than traditional methods. Quantum image encryption utilizes the principles of superposition and entanglement in quantum bits (qubits) to encrypt images [33]. Content sent between places without encryption is vulnerable to attacks. Effective encryption should be highly sensitive to small key changes, drastically changing the cipher-text. Another study [34] proposed a highly sensitive image encryption algorithm. It designs a novel encryption for quantum images based on chaotic maps. The image is scrambled into a quantum state using circuits from the Quantum Hilbert Image Scrambling algorithm. The scrambled image is then encrypted using the quantum XOR gate and a chaotic maps algorithm. Numerical and simulation analyses show that the suggested technique is more efficient than its traditional equivalent. Another research introduces a novel quantum logistic image encryption algorithm, leveraging the RSA and SHA-3. This algorithm facilitates secure communication of network images within a public cryptosystem. It exhibits notable characteristics such as heightened sensitivity to plaintext and encryption keys and an improved capacity to withstand diverse attacks [35]. Deep learning-based image encryption methods use neural networks to encrypt and decrypt images. These methods have shown great potential in terms of accuracy and efficiency. The Convolutional Neural Network (CNN) and the Autoencoder are the most commonly used neural networks in these methods [36]. The article [37] presented a novel encryption approach inspired by HNN (Hierarchical Neural Network) models. This technique enhances the system's resilience against a wide range of attacks by continuously learning and updating. Another article introduced a novel network called DeepEDN, which utilizes deep learning techniques to encrypt and decrypt medical images. DeepEDN demonstrates a commendable degree of security and efficiency in its performance [38]. The final note is that recent advancements in image encryption methods have significantly improved the quality of secured image transmission. However, further research is still needed to balance the trade-off between the level of security, quality of images, and computational efficiency. Because IoT devices have low data rates and resources, lightweight image encryption will be a better selection, which encrypts image data using limited resources in a few rounds and low computational complexity. Accordingly, we use a lightweight encryption algorithm in the proposed method, which will be discussed in the following section.

2.2 Color image watermarking

Color image watermarking methods encompass many techniques developed in recent years. As technology and multimedia applications continue to advance, there is an in-

creased need for new watermarking methods that consider factors such as robustness, capacity, and security while maintaining the visual quality of watermarked images. In previous research, many color image watermarking approaches have been presented. Giri et al. [23] focused on the usage of watermarking in color data, particularly images. They noted that most research has concentrated on grayscale and monochrome media. Yet, with color images becoming increasingly prevalent in the everyday operations of many organizations, the need for color image watermarking methods cannot be overemphasized [23]. Going further, Mahto and Singh [39] extensively reviewed watermarking, its features, methods of embedding and recovery, evaluation metrics, and its applications. This work also surveys various algorithms used in watermarking, discussing their merits and limitations. In a more recent article [40], authors explored robust watermarking technologies, reviewing recent research on the topic. The article outlines the properties required for digital watermarking methods but does not delve into other applications, such as semi-fragile and fragile watermarking. A blind color image watermarking algorithm combining spatial domain and SVD is designed in [41]. It proposes a principle combining SVD and spatial domain. Watermarking directly embeds into the MSV in the spatial domain. Extracted watermarks are directly from watermarked MSV with correction. It has good imperceptibility, higher robustness, and shorter running time. In [42], a robust technique for watermarking color images within the spatial domain was proposed. The experimental findings demonstrate that the suggested watermarking method achieves enhanced imperceptibility of watermarks and increased resilience against typical attacks, such as noise addition, cropping, and JPEG compression. This study presents a unique and effective technique for color image watermarking that uses YCbCr color space, wavelet transforms, SVD, and QR codes to embed information, resulting in a novel and practical approach that is strong in contradiction of various attacks [43]. Discrete trunnion Fourier transform (DTFT) and quantization index modulation method [44] present a block-based color image watermarking method. In another study, Using the LWT, the researchers put forth a resilient and reliable technique for watermarking color images in the YCbCr color space. Watermarks are embedded and extracted using an alpha-blending strategy [45]. Another research presents a comprehensive rationale for choosing the Y component to embed watermarks. Additionally, it evaluates the effectiveness of the suggested methodology by comparing its performance to other contemporary methods [46]. A novel blind color image watermarking framework incorporating multilevel DHT has been developed to address the emerging issues posed by the 5G network in safeguarding the copyright protection of digital images. The whole watermarking scheme is implemented exclusively in the spatial domain, leveraging the spatial-domain computing property and the energy aggregation concept of the multilayer maximum energy coefficient. This approach significantly improves the real-time performance and the ability to withstand attacks of the watermarking technique. Multiple simulation results demonstrated the robustness,

security, and high efficiency, which is one effective measure for safeguarding digital copyright [47]. In [48], a revolutionary blind color image watermarking is introduced based on the Walsh Hadamard Transform. The experimental findings demonstrate that the suggested watermarking technique has a high level of resilience against various types of attacks. Accordingly, robustness is a significant one of the main challenges of digital watermarking algorithms. The robustness attribute is essential in image watermarking to ensure the integrity and persistence of the embedded watermark in the face of common image manipulations and attacks. However, Enhancing resilience should neither have a detrimental impact on image quality nor should it significantly decrease the embedding capacity. Accordingly, this article presents a combination of a TVT, DWT, and DCT for color image watermarking to ensure the watermarking robustness.

3. Proposed methods

Safely transmitting information in a way that requires the lowest cost of resources is one of the critical challenges in information transfer on the IoT. Encryption and watermarking operations are two main requirements to send information with high security. The use of encryption makes the original watermark undetectable. As a result of image encryption, a texture-like or noise-like unknown image format is produced, indicating the encrypted image includes hidden information. To address this problem, using watermarking, this encrypted information is hidden inside another image so that others do not notice the sending of the original information. As mentioned, we use a lightweight encryption algorithm with few resources and rounds for image encryption. For this reason, we use the lightweight algorithm for encryption. Despite being light, this algorithm can suitably encrypt the watermark image. TVT transform, besides 2-level DWT + DCT, is used for watermarking (Fig. 1a).

3.1 Lightweight encryption algorithm

The proposed method provides a light structure convenient for use in the IoT system. This is a block cipher for the symmetric key, which uses a 64-bit key. The encryption process of the symmetric key contains some encryption rounds, where each round is a mathematical function to make confusion and propagation [49]. The augmentation of the number of rounds results in enhanced security but, unfortunately, increases energy consumption. Thus, the encryption algorithm is limited to only five rounds to decrease energy consumption. Each round of encryption consists of mathematical operations. This algorithm uses the Feistel network of alternative diffusion functions to complicate the data and deal with the attacks. The two main parts of the algorithm are critical expansion and data encryption. Fig. 2 shows the flowchart of the encryption algorithm. The watermark image is a grayscale 8-bit image of size 64×64 . We divide the image into 64-bit blocks. In this case, each block will contain 8 pixels (see Fig. 2). Starting from the top-left corner of the image, the first block will have pixels (1,1) to (8,1), the second block will contain pixels (9,1) to (16,1), and so on. Then, each block is encrypted separately using the algorithm. The most fundamental part of cryp-

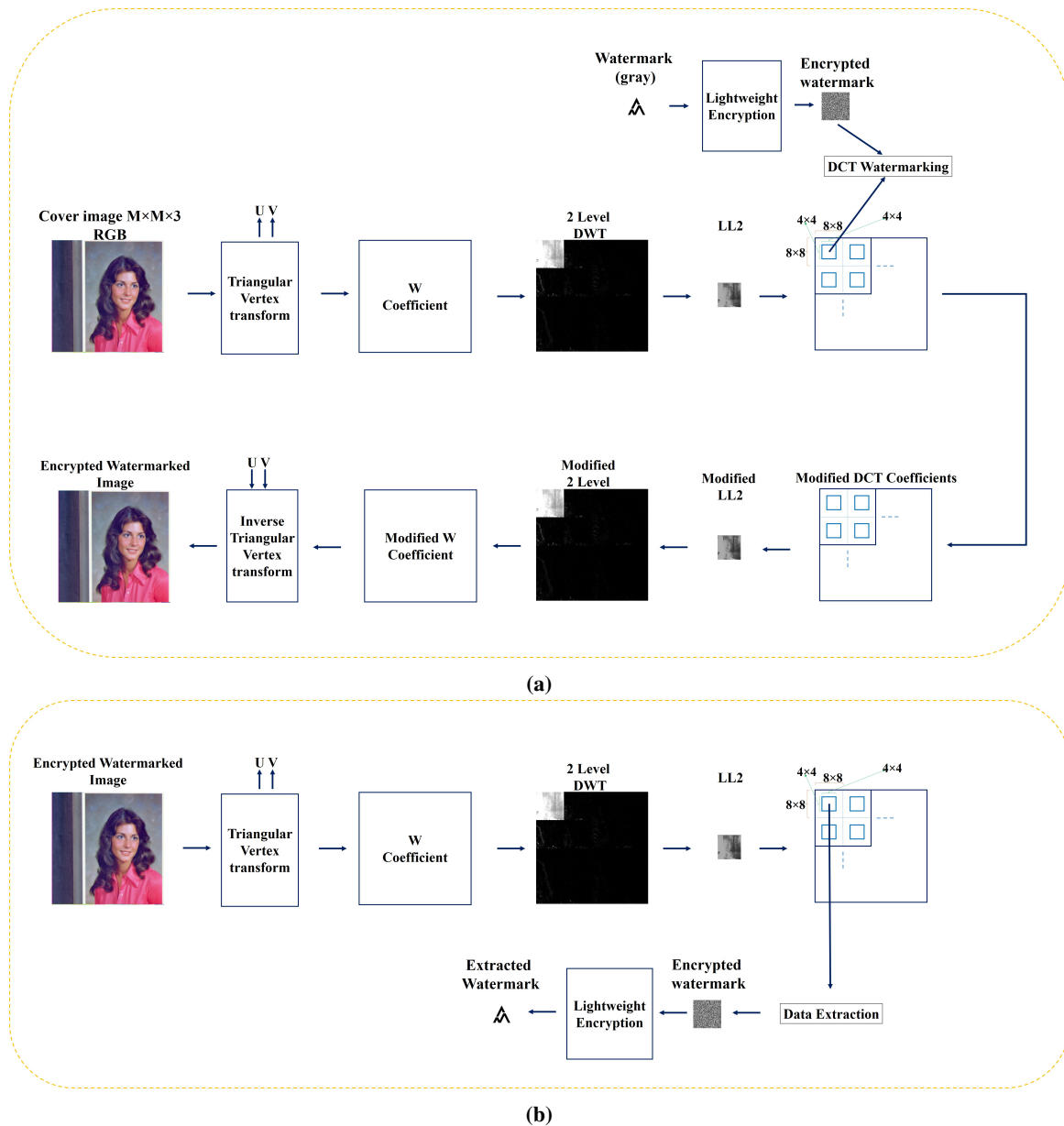


Figure 1. The flow chart of the proposed method. (a) encrypted watermarked image generation, (b) watermark extraction.

tography is the key. The whole security depends on the generated key. If the key is recognizable to the attacker, data confidentiality is lost. Therefore, producing the key requires caution. To make key disclosure as tricky as possible. The algorithm contains five rounds, so each round needs five unique keys. The algorithm is a 64-bit block cipher algorithm. It means that to encrypt 64 bits of data, 64 bits of key (i.e., four 16-bit keys) are needed. At first, an arbitrary 64-bit key is provided by the user. This key is the input of the critical expansion block. Then, the input key is divided into four 16-bit. After performing 16-bit-based relocation and map operations on the input key, the fundamental expansion block generates five unique keys (K1, K2, K3, K4, and K5). These keys are used in encryption and decryption and have high security against unknown attacks. Fig. 3 shows the flow chart of the key expansion. The critical expansion part uses the function provided, which is an optimized encoder. Our encryption method is an amalga-

mation of Feistel and Substitution-Permutation networks. Consequently, we use the qualities of both techniques to create a lightweight algorithm that provides considerable security in the IoT system while maintaining a reasonable degree of computational complexity.

3.2 Color image watermarking

The proposed article uses frequency domain watermarking techniques using TVT-DCT-DWT (Fig. 1a).

3.2.1 Watermark embedding

First, we transform the cover image from the RGB to the UVW space using the TVT. Then, using the W coefficients and DCT-DWT, the watermarking is performed. We use TVT and W coefficient for watermark embedding because it is less sensitive against different attacks. The cover image (RGB) is indicated by C, and EW indicates the encrypted watermark image. To get the EW, the watermark image is

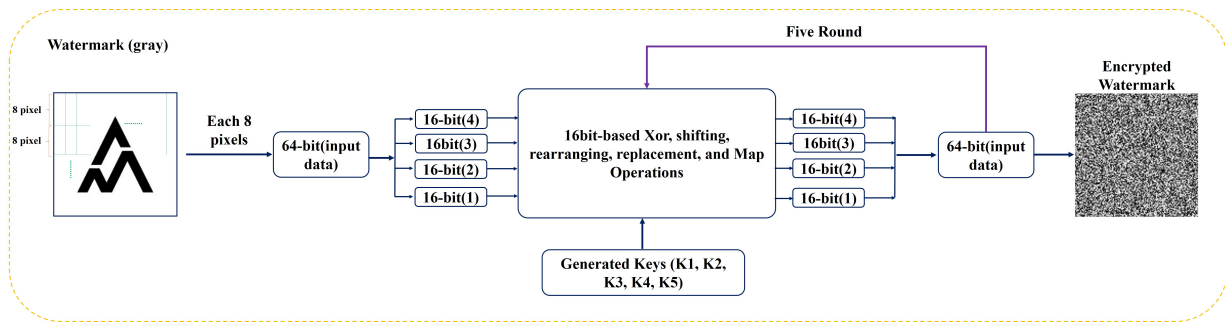


Figure 2. Lightweight watermark encryption.

encrypted using the lightweight encryption algorithm explained in subsection 3.1. Then, the EW is embedded into the C.

The proposed TVT transforms the cover image C. Thus, R, G, and B channels are converted into (U, V, W). U, V, and W are the same size as the size of R, G, and B. The encrypted watermark is used to embed the watermark. The W coefficient exhibits greater resilience against many types of attacks. To maintain the quality of the image, the watermark is not directly included in the W coefficient. The data is embedded via DWT + DCT.

A novel combination of the 2-level DWT+DCT inserts the EW in the W coefficients. DWT provides good resistance against attacks on watermarking images. DWT is used to decompose the W into several sub-bands. The watermark should be inserted appropriately to achieve maximum visual quality and resist potential attacks such as noise, low-pass filtering, JPEG compression, and geometric attacks. Such attacks tend to degrade the high-frequency component within the image while introducing a few disturbances to the low-frequency band. Therefore, we use the LL2 low-frequency spectrum to insert encrypted watermarks [50]. Using DWT on the W coefficient, it decomposes into four sub-bands: LH_{w1} , HL_{w1} , HH_{w1} , LL_{w1} . The high-frequency parts of the image, which contain information about the edges, are concentrated in LH_{w1} , HL_{w1} , HH_{w1} . On the other hand, most of the information is gathered in the LL_{w1} sub-band. When DWT is performed on the LL_{w1} band, the second level of decomposition (LH_{w2} , HL_{w2} , HH_{w2} , LL_{w2}) is obtained. Then, the calculated coefficients of LL2 are divided into non-overlapped 8×8 blocks, and we apply DCT decompo-

sition to each block. We use the values (DCT coefficients) obtained in the middle frequencies to add the watermark. After transformation, many AC and one DC coefficients make up each block. The transformed images contain most of their information in low-level frequency coefficients. We can see low-level frequency coefficients in the uppermost left corner of the image. AC coefficients include more information about the image on a smaller scale than DC coefficients. Three distinct frequency bands are generated by the block-based DCT algorithm: low-frequency, middle-frequency, and high-frequency. When the low-frequency band, which contains most of the image information, is altered, the visual quality of images is adversely affected. Conversely, the high-frequency band might be eliminated to aid compression. Because of its reduced perceptibility when modified [48], the DCT-based watermarking system is built on the middle band frequency. For this purpose, we specify a 4×4 block in the middle of each 8×8 block. On the other hand, the EW is divided into the non-overlapped 4×4 blocks. In this step, the 4×4 block in the middle of each 8×8 block and each 4×4 block of the EW are combined with a scaling weight α :

$$New\ DCT_{8 \times 8}\{4 \times 4\} = DCT_{8 \times 8}\{4 \times 4\} + \alpha Ew\{4 \times 4\} \tag{1}$$

Now, by applying inverse DCT, the modified LL2 is obtained. Then, the watermarked coefficient W^* is constructed using LH_{w1} , HL_{w1} , and HH_{w1} , LH_{w2} , HL_{w2} , HH_{w2} , LL_{w2} , and inverse 2-level DWT. In the final step, by using inverse TVT on U, V, and W^* , the watermarked color image C^* is constructed (Fig. 4a). Different steps for encrypted watermark embedding are given as Algorithm 1.

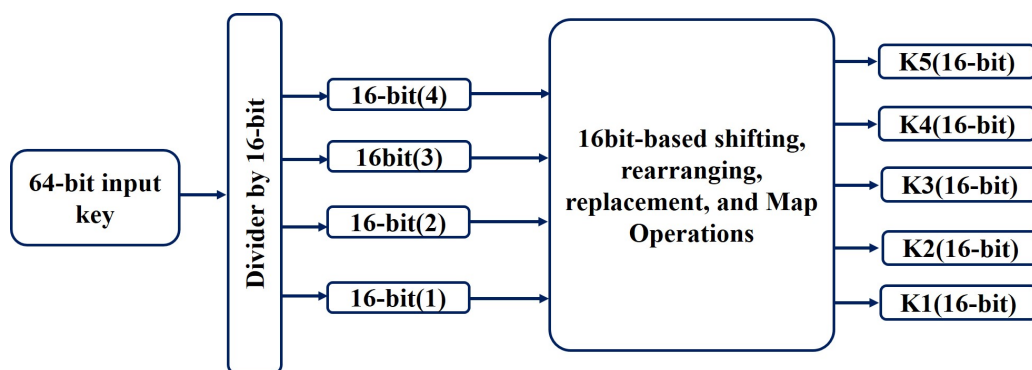


Figure 3. Five key generation based on the 64-bit input key.

3.2.2 Watermark extraction

The flowchart of the watermark extraction is shown in Fig. 4b. To extract the encrypted watermarked, C^* (the watermarked color image) is applied in the flowchart. The C^* is transformed by TVT, as discussed in the embedding section. Therefore, the R, G, and B channels are converted to the coefficients (U, V, and W^*) that the W^* contains the watermarked. Then, the matrix W^* is decomposed to the sub-bands LH_{w2} , HL_{w2} , HH_{w2} , LL_{w2} using 2-level DWT. Then, LL_{w2} coefficients are divided into 8×8 blocks. We applied the DCT transform in each block and specified a 4×4 block in the middle of each 8×8 block. Now, using the following equation, we can extract the encrypted watermark:

$$New\ DCT_{8 \times 8}\{4 \times 4\} = DCT_{8 \times 8}\{4 \times 4\} + \alpha E_w\{4 \times 4\} \tag{2}$$

By applying the lightweight decryption on the EW^* , the watermark can be extracted. Different steps for watermark extraction are given in Algorithm 2.

4. Experimental results and discussion

Here, our proposed method is looked at and compared to several new ways that are similar. All simulations are run in the Matlab 2020 on a computer system with 32 GB of RAM and a 1.8 GHz Intel Core i7 processor. We used several different images to evaluate the results of the proposed method and compare it with previous methods (Fig. 5).

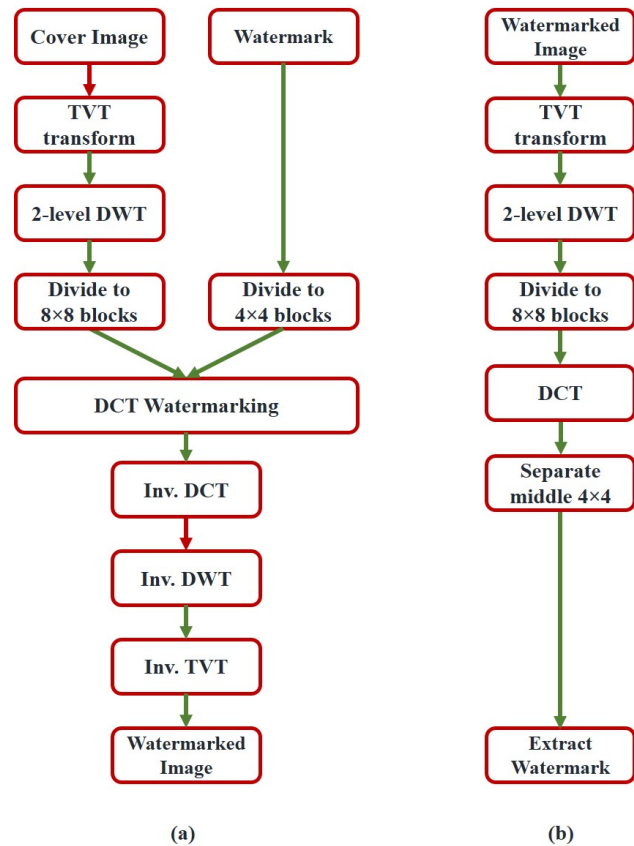


Figure 4. The flow chart of the watermark (a) embedding, (b) extraction.

Algorithm 1	Watermark Embedding
Inputs	Watermark ($M/8 \times N/8$) and Color Cover Image ($M \times M \times 3$)
Output	Watermarking Image ($M \times M$)
<p>do</p> <ol style="list-style-type: none"> 1. Apply a lightweight encryption algorithm to the watermark by the procedure outlined in subsection 3.1. 2. The color cover image is transformed to UVW using TVT: $CU.V.W = TVT(CR.G.B)$ 3. Select the W coefficient and apply 2-level DWT over it. 4. Apply 2-level DWT to approximation LL_{w2}: $LH_{w2}.HL_{w2}.HH_{w2}.LL_{w2} = DWT_2(W)$ LL_{w2} is selected for watermark embedding. 5. LL_{w2} is partitioned into the non-overlapped blocks of 8×8 and apply DCT on each block. Then, specify a block of size 4×4 in the middle of the block. 6. Partitioned EW into the non-overlapped blocks of size 4×4. 7. Embed the EW block by block using Eq. 1. 8. Apply an inverse DCT, a 2-level inverse DWT, and an inverse TVT to obtain the watermarked image. 	
return	Watermarked image

In addition to evaluating the proposed method from several

Algorithm 2	Watermark Embedding
Inputs	Watermark ($M \times M \times 3$)
Output	Watermarking Image ($M/8 \times M/8$)
<p>do</p> <ol style="list-style-type: none"> 1. The color Watermarked image C^* is transformed to UVW using TVT: $CU.V.W^* = TVT(C^* R.G.B)$ 3. Select the W^* coefficient and apply 2-level DWT over it. 4. Apply 2-level DWT to approximation LL_{w2}: $LH_{w^*2}.HL_{w^*2}.HH_{w^*2}.LL_{w^*2} = DWT_2(W^*)$ LL_{w^*2} is selected for watermark extraction. 5. Partitioned LL_{w2} into the non-overlapped blocks of size 8×8 and apply DCT on each block. Then, specify a block of size 4×4 in the middle of the block. 6. Extract the EW^* block by block using Eq. 2. 7. Extract the watermark image by applying lightweight decryption on the EW^*. 	
return	Watermarked image

angles and comparing it with other methods, some evaluation metrics are used in this article.

- Histogram analysis is another metric to evaluate the effects of the operation on the image. We use these metrics to study the encryption and watermarking operations.
- Corr.: The correlation between two variables is a statistical relation that shows how one variable is dependent on another. Data points that have a large dependence have a significant correlation value.

$$\text{Corr}(I_1, I_2) = \frac{\delta_{1,2}}{\sqrt{\delta_1 \delta_2}} \quad (3)$$

where $\delta_{1,2}$ is the covariance value between the images $I_1(i,j)$ and $I_2(i,j)$, and δ_1 , and δ_2 are the variances of the images.

- NCC shows the resilience of the watermarking method.

It computes as follows:

$$NCC = \frac{\sum_{i=1}^m \sum_{j=1}^m W(i,j) \times W_{\text{extracted}}(i,j)}{\sqrt{\sum_{i=1}^m \sum_{j=1}^m W(i,j)^2} \sqrt{\sum_{i=1}^m \sum_{j=1}^m W_{\text{extracted}}(i,j)^2}} \quad (4)$$

- MSE is the difference between two $M \times N$ images (the original and changed images):

$$MSE = \frac{1}{M \times N} \sum_{i=1}^M \sum_{j=1}^N [I_1(i,j) - I_2(i,j)]^2 \quad (5)$$

where $I_1(i,j)$ and $I_2(i,j)$ are original and changed images.

- PSNR is a quality metric frequently used to compare original and changed images. It is defined as follows:

$$PSNR = 10 \log_{10} \left(\frac{255 \times 255}{MSE} \right) \quad (6)$$

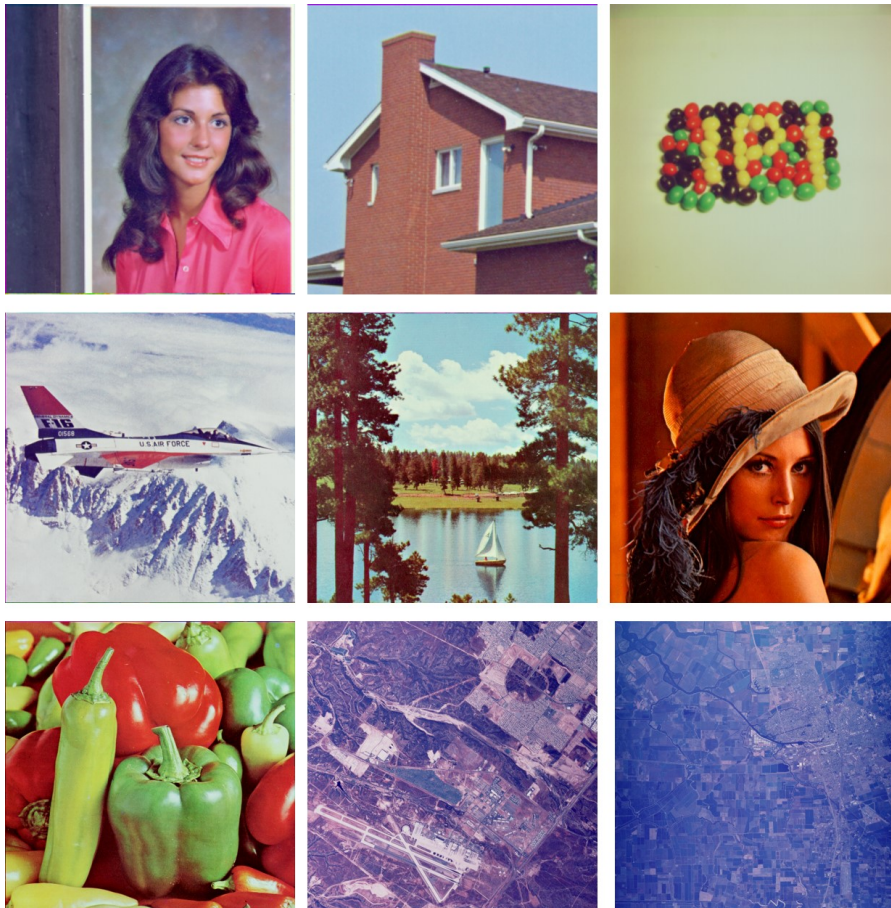


Figure 5. The test images, cover, and watermark image.

SSIM is a perceptual measure used to assess the degradation of the image resulting from various processing techniques, including data reconstruction or compression.

$$SSIM = \frac{(2\mu_1\mu_2 + C_1)(2\delta_{1,2} + C_2)}{(\mu_1^2 + \mu_2^2 + C_1)(\delta_1^2 + \delta_2^2 + C_2)} \quad (7)$$

where, μ_1 , μ_2 , δ_1 , and δ_2 are the means and variances of the images $I_1(i,j)$ and $I_2(i,j)$ respectively. $\delta_{1,2}$ is the covariance value between the images. C_1 and C_2 are two stabilizer variables in the division.

4.1 Lightweight encryption method

The encryption algorithm is a symmetric key block cipher that uses a 64-bit key and plain text. The algorithm is limited to only five rounds to decrease energy consumption. Each round of encryption consists of mathematical operations performed on 4-bit data. This algorithm uses the Feistel network of alternative diffusion functions to complicate the data to face the attacks. Fig. 6 shows the result of lightweight encryption and decryption for three images. An image of a logo is used as a watermark to evaluate the proposed integration method. Fig. 7 shows this watermark, its encryption, and its decryption using a lightweight algorithm.

On the other hand, we tested entropy and histogram on four 8-bit grayscale images. Moreover, the histograms in Fig. 8 for the original and encrypted images show uniform intensities after encryption, indicating the desired security. According to Table 1, all encrypted images have an entropy close to the maximum, demonstrating an algorithm property. The correlation values for the original images are higher than those for the encrypted images, indicating that the encryption process reduces the correlation between the pixels in the image. These results show that the proposed method effectively encrypts the watermark image.

4.2 Color image watermarking

This section encompasses a series of experiments to assess several factors, such as imperceptibility, resilience, and computing complexity.

4.2.1 Imperceptibility analysis

The characteristic of imperceptibility plays a significant role in the watermarking system. This subsection focuses on an examination of the imperceptibility of the proposed method. The imperceptibility of watermarking techniques is often evaluated using objective performance measurements like PSNR and SSIM. This study employs objective measures

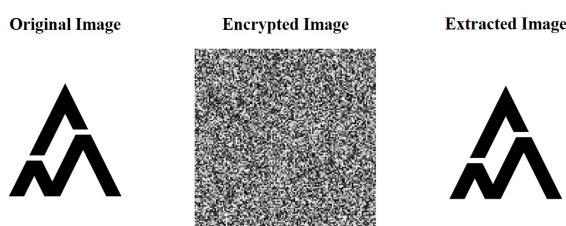


Figure 6. Lightweight encryption and extraction.

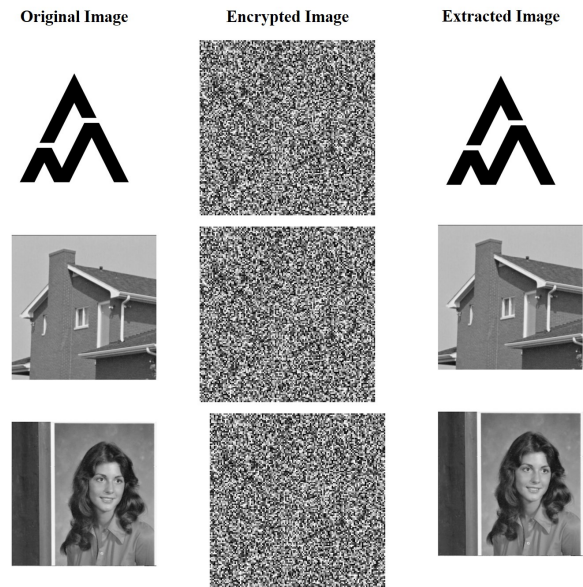


Figure 7. The watermark, its encryption and extraction.

such as PSNR, SSIM, MSE, and NCC to assess the perceptual transparency of the proposed method. Typically, when the PSNR value exceeds or equals 48 dB, the picture quality is exceptional, with no discernible variations perceptible to the human eye [51]. For $35 \text{ dB} < \text{PSNR} < 48 \text{ dB}$, the image has a favorable level of quality. The image has a suitable quality for $29 \text{ dB} < \text{PSNR} < 35 \text{ dB}$. When the PSNR ratio falls under 25 dB, it indicates that the image is detectable to the human visual system. The suggested system exhibits a range of PSNR values spanning from 53.8586 to 54.9250 dB, with an average PSNR value of 54.4798 dB. The proposed approach achieves an average SSIM value of one, the optimal value indicating minimal distortions in the watermarked photos.

The results of different imperceptibility metrics values of the suggested system are shown in Table 2. According to the findings shown in Table 2, it is evident that the Jelly image exhibits the highest PSNR value, while the San Diego image has the lowest PSNR value. Simultaneously, the SSIM value remains constant across all images. Table 2 presents the proposed method's PSNR, SSIM, MSE, and NCC values for both the cover and the watermarked image. The average PSNR is measured at 54.4798 dB, the SSIM is 1, the MSE is 0.4541, and the average NCC is 0.9995.

4.2.2 Robustness analysis

The efficacy of a watermarking technique is determined by its ability to withstand various forms of attack. To evaluate the resilience of our suggested method, a series of attacks are applied to the watermarked images. Some examples of image processing techniques include salt & pepper noise rotation, cropping, and JPEG. The Female image is used as an illustrative instance in this context. Fig. 9 illustrates the various attacks applied to the watermarked image, while Fig. 10 depicts the resulting extracted watermark. In this context, many image processing techniques are used, including Salt & Pepper noise with intensities of 0.02 and 0.05, rotation by 10 degrees, median filtering, Gaussian filtering,

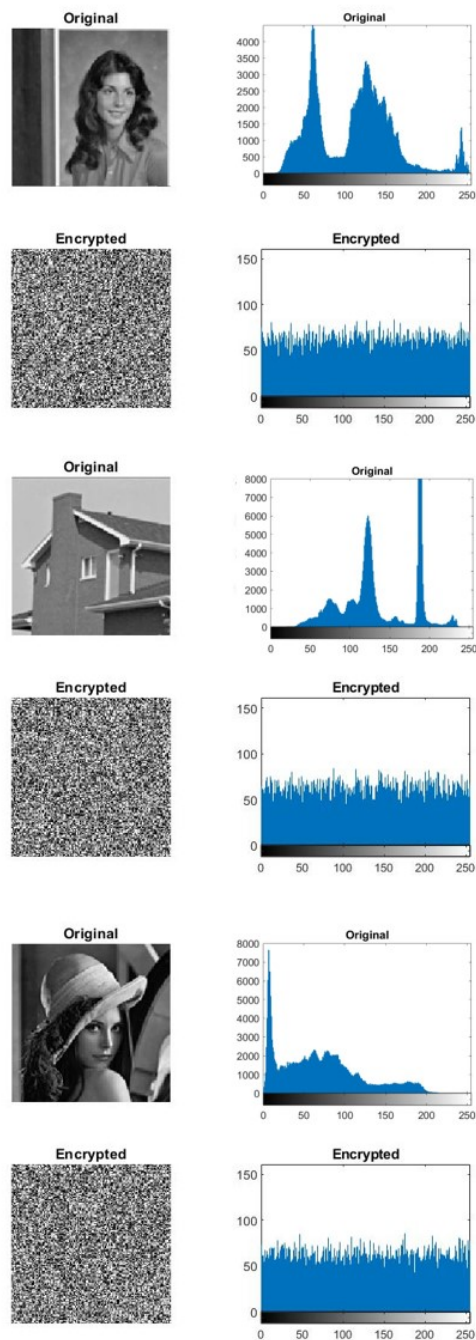


Figure 8. Histogram comparison between original and encrypted images.

histogram equalization, sharpening, Gaussian noise, speckle noise cropping by 10%, JPEG compression with a quality factor of 90%, contrast correction, and brightness modification by +40 and -30 units. The NCC metric is used as a quantitative measure to assess the resilience of a system's performance. Table 3 presents the PSNR values for the watermarked images under different attack scenarios. The suggested method exhibits an average PSNR of 54.4798 dB. The PSNR values decrease significantly under different attacks, with the lowest value of 11.7859 dB for rotation. Table 4 displays the NCC values for the original and ex-

tracted watermarks in the proposed approach. NCC is a measure of the robustness of a watermarking method when attacked. In the condition of no attacks, the average NCC is one. The experimental findings indicate that the suggested watermarking technique has a high level of resilience against various types of attacks. Table 5 presents the NCC and PSNR of the extracted watermark and the attacked images, respectively. The noise levels tested were 0.01, 0.02, 0.03, 0.04, and 0.05. As you see, The PSNR and NCC values decreased as the noise level increased. The Female image may be more resilient to salt and pepper noise than the other images tested. On the other hand, the House image may be more sensitive to salt and pepper noise. This table demonstrates the correlation between the imperceptibility and robustness of the attacked images, specifically in the Salt & Pepper attack context.

4.2.3 Computational complexity

This study conducted experiments using Matlab on a computer with an Intel i7 (1.8 GHz) and 32 GB of RAM. Based on the proposed scheme, the average computation time is 0.313867 seconds. Fig. 10 shows the computational time of the proposed scheme on various images. To calculate the computational time of the proposed scheme, we know that the proposed scheme involves several steps, comprising performing a level 2 DWT on a W coefficient of size $M \times M$, followed by applying a DCT on the LL2 coefficient, before using the DCT, the LL2 coefficient is separated into blocks of size 8×8 , and DCT is performed on each block. Finally, after inserting the watermark in the DCT coefficients, inverse DCT and inverse DWT are committed to achieve the original image. Combining these steps, the overall time complexity of the proposed method can be approximated as:

$$O(M^2 \log M^2) + O\left(\frac{M^2}{8}\right) + O(M^2 \log M^2) \quad (8)$$

4.2.4 Comparative analysis

This section compares the suggested method with recent state-of-the-art techniques [42, 43, 46, 48, 51–56]. Table 6 presents a comparative examination of the proposed method's imperceptibility compared to the other relative methods. In Table 6, PSNR and SSIM are used for comparison analysis. The use of NCC to conduct a comparative robustness study with several current schemes is shown in Table 7. The suggested approach exhibits an average PSNR of 54.4798 dB, while the SSIM is 1. The superiority of the proposed strategy over the alternative plan is evident based on the results shown in Table 6, as indicated by the higher values of SSIM and PSNR. This demonstrates the high level of perceptual quality achieved by the suggested approach. The outcomes of the experiments prove that the proposed system surpasses other techniques regarding PSNR and SSIM values.

The comparative analysis of the proposed scheme against various attacks is shown alongside other methods in Table 7. Under the no attack, NCC is 1 for all methods except in [48] is 0.9999. Under the Salt & Pepper attack, [43] represents the better result, one, than the proposed method,

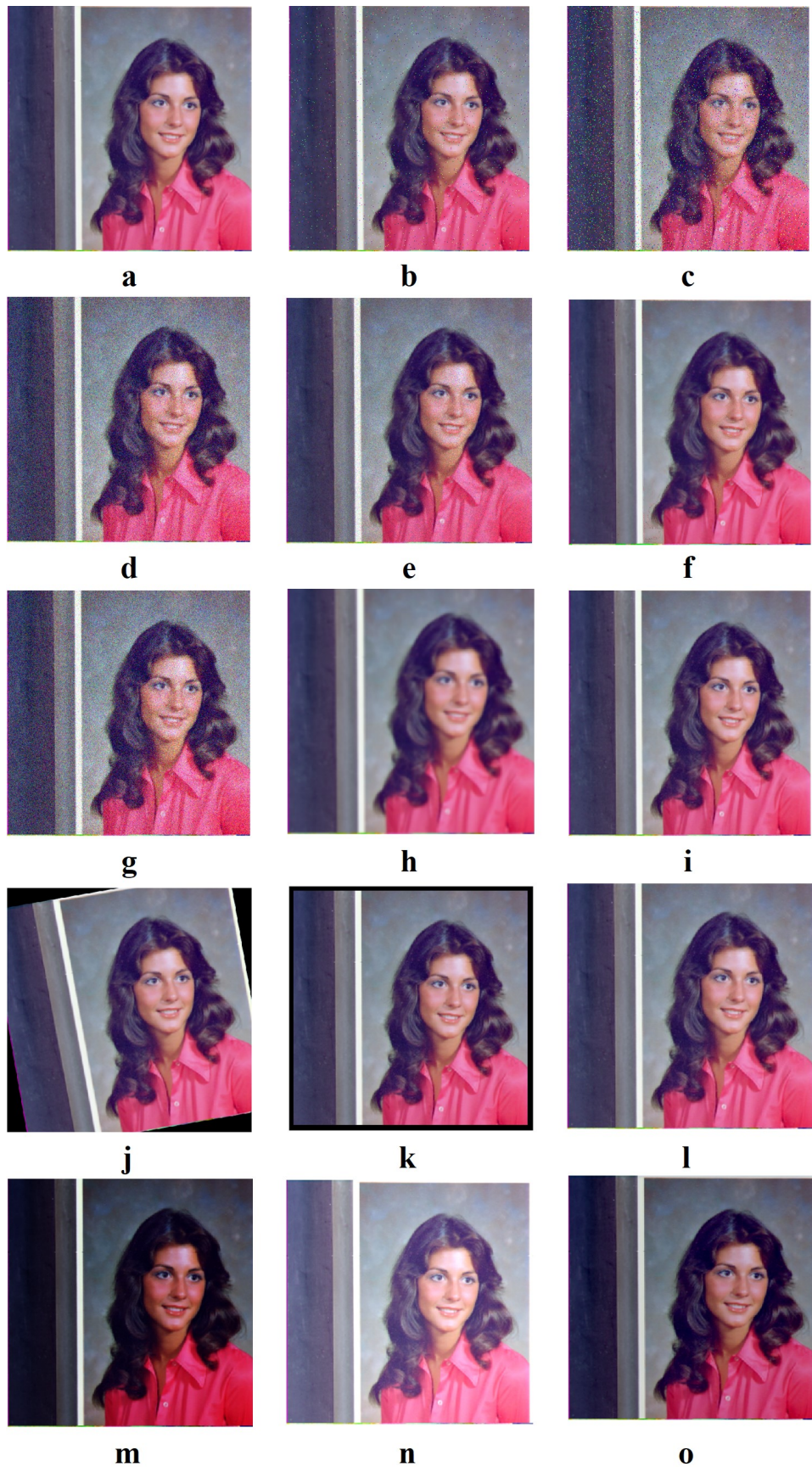


Figure 9. Various attacks on Female image with (a) no attacks, (b) Salt & Pepper (0.02), (c) Salt & Pepper (0.05), (d) Gaussian noise, (e) Speckle noise, (f) Sharpening, (g) Histogram equalization, (h) Gaussian filtering, (i) Median filtering, (j) Rotation(10°), (k) Cropping, (l) JPEG compression (QF = 90%), (e) Contrast adjustment, (e) Brightening by +40, (e) Darkening by -30.

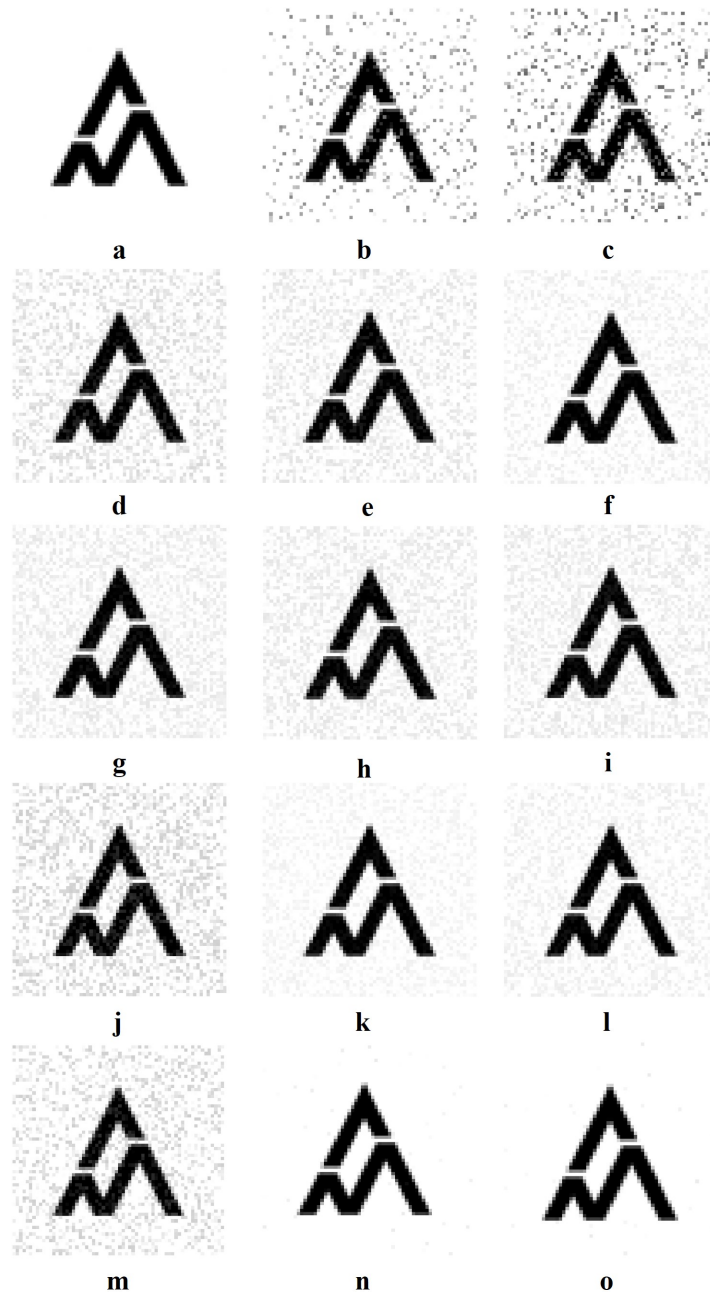


Figure 10. Extracted Watermark with (a) no attacks, (b) Salt & Pepper (0.02), (c) Salt & Pepper (0.05), (d) Gaussian noise, (e) Speckle noise, (f) Sharpening, (g) Histogram equalization, (h) Gaussian filtering, (i) Median filtering, (j) Rotation(10°), (k) Cropping, (l) JPEG compression (QF = 90%), (e) Contrast adjustment, (e) Brightening by +40, (e) Darkening by -30.

Table 1. Correlation and entropy comparison between original and encrypted images.

image	size	Entropy		Correlation					
		Original	Encrypted	original			Encrypted		
				Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Female	512×512	7.2682	7.9994	0.9924	0.9962	0.9887	0.0009	0.0001	0.0013
House	512×512	7.2430	7.9992	0.9932	0.9953	0.9894	0.0009	0.001	0.0016
Lena	512×512	7.3200	7.9994	0.9820	0.9884	0.9731	0.0009	0.0023	0.0008
Logo	64×64	1.1681	7.9971	0.8818	0.9358	0.8358	0.1346	0.0350	0.0581

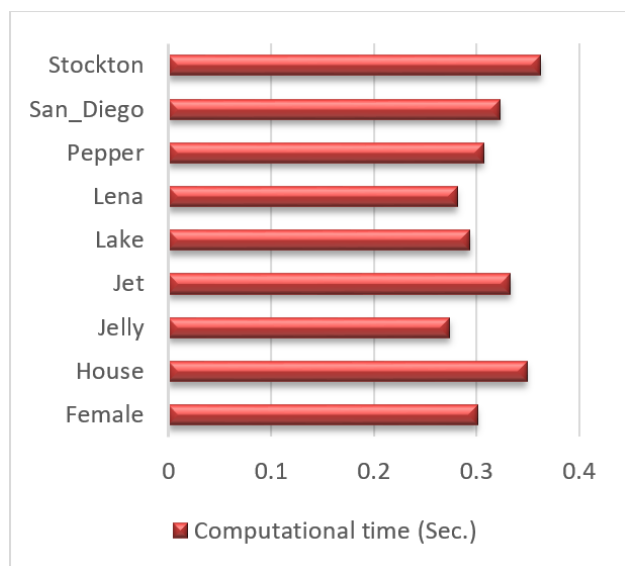


Figure 11. Computational time (Sec.) for different images.

0.9908. The proposed method outperforms all previous methods for both types of noise for Gaussian noise. On the other hand, the proposed method is the most effective at reducing speckle noise and sharpening the image. Method [46] and [52] have comparable results under speckle noise and sharpening, respectively. In addition, [46] has the best results under Histogram equalization and Gaussian filter. Under median filter, rotation, and cropping, the proposed method and [46] are the best methods. Finally, [53], [55], and the proposed method represent the desired result under the JPEG attack. Overall, Table 7 illustrates that the proposed method exhibits an acceptable NCC value than most of the comparative methods.

5. Conclusion

This article proposed an efficient method for transmitting images while ensuring robustness and security. The suggested approach combined simple encryption techniques and watermarking mechanisms to achieve the desired goals. The process involved a low-complexity encryption technique, color image conversion using the TVT transform, and watermark embedding using a combination of DWT and DCT. The simple encryption algorithm employed a symmetric key block cipher with five encryption rounds,

making it suitable for resource-limited systems. Watermarking was applied to the image’s LL2 coefficient using DCT, resulting in a modified coefficient to generate the watermarked image. The primary contributions of this research were using simple encryption and watermarking techniques to minimize resource requirements and enhance security. The proposed method demonstrated robustness through a three-step frequency domain watermarking strategy, incorporating TVT, 2-level DWT, and DCT. The effectiveness of the suggested methodology was evaluated using standard images and metrics such as histogram analysis, correlation, NCC, PSNR, and SSIM. The experimental results showed that the proposed technique outperformed alternative solutions, exhibiting significant improvements in PSNR, NCC, and robustness. Overall, the findings demonstrated the superiority of the suggested approach over existing leading methods.

Funding

No funding was received to assist with conducting this study and the preparation of this manuscript.

Authors Contributions

All authors have contributed equally to prepare the paper.

Availability of Data and Materials

The data that support the findings of this study are available from the corresponding author upon reasonable request.

Conflict of Interests

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Open Access

This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s)

Table 2. Evaluation of the cover and watermark image based on PSNR, SSIM, MSE, and NCC.

cover images	PSNR(cover)	SSIM(cover)	MSE(cover)	NCC(watermarked)
female	54.8756	1	0.0458	0.9998
house	54.8854	1	0.0452	0.9998
jelly	54.9250	1	0.0453	0.9995
jet	54.0875	1	0.0455	0.9992
lake	54.8756	1	0.0421	0.9996
lena	53.9369	1	0.0463	0.9994
San_Diego	53.8586	1	0.0445	0.9993
stockton	54.3939	1	0.0486	0.9995

and the source, provide a link to the Creative Commons license, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the OICC Press publisher. To view a copy of this license, visit <https://creativecommons.org/licenses/by/4.0>.

References

- [1] A. Mpatziakas, A. Drosou, S. Papadopoulos, and D. Tzouvaras. “**IoT threat mitigation engine empowered by artificial intelligence multi-objective optimization.**”. *Journal of Network and Computer Applications*, 203:pp. 103398, 2022.
- [2] K. Sorri, N. Mustafee, and M. Seppänen. “**Revisiting IoT definitions: A framework towards comprehensive use.**”. *Technological Forecasting and Social Change*, 179:pp. 121623, 2022.
- [3] E. Schiller, A. Aidoo, J. Fuhrer, J. Stahl, M. Zörjen, and B. Stillner. “**Landscape of IoT security.**”. *Computer Science Review*, 44:pp. 100467, 2022.
- [4] V. K. Quy. “**IoT-enabled smart agriculture: Architecture, applications, and challenges.**”. *Applied Sciences*, 12(7):pp. 3396, 2022.
- [5] A. Sreedevi, T. N. Harshitha, V. Sugumaran, and P. Shankar. “**Application of cognitive computing in healthcare, cybersecurity, big data and IoT: A literature review.**”. *Information Processing & Management*, 59(2):pp. 102888, 2022.
- [6] I. H. Sarker, A. I. Khan, Y. B. Abushark, and F. Alsolami. “**Internet of things (iot) security intelligence: A comprehensive overview, machine learning solutions and research directions.**”. *Mobile Networks and Applications*, 28(1):pp. 296–312, 2023.
- [7] P. K. Sadhu, V. P. Yanambaka, and A. Abdelgawad. “**Internet of things: Security and solutions survey.**”. *Sensors*, 22(19):pp. 7433, 2022.
- [8] K. N. Singh and A. K. Singh. “**Towards integrating image encryption with compression: A survey.**”. *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, 18(3):pp. 1–21, 2022.
- [9] U. Zia. “**Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains.**”. *International Journal of Information Security*, 21(4):pp. 917–935, 2022.
- [10] S. Roy, U. Rawat, H. A. Sareen, and S. K. Nayak. “**IECA: an efficient IoT friendly image encryption technique using programmable cellular automata.**”. *Journal of Ambient Intelligence and Humanized Computing*, 11:pp. 5083–5102, 2020.
- [11] H. Dweik and M. Abutaha. “**A survey of lightweight image encryption for IoT.**”. *Lightweight Cryptographic Techniques and Cybersecurity Approaches: IntechOpen*, , 2022.
- [12] S. Roy, M. Shrivastava, C. V. Pandey, S. K. Nayak, and U. Rawat. “**IEVCA: An efficient image encryption technique for IoT applications using 2-D Von-Neumann cellular automata.**”. *Multimedia Tools and Applications*, 80:pp. 31529–31567, 2021.
- [13] D. Trujillo-Toledo. “**Real-time medical image encryption for H-IoT applications using improved sequences from chaotic maps.**”. *Integration*, 90:pp. 131–145, 2023.
- [14] M. Devipriya and M. Brindha. “**Image encryption using modified perfect shuffle-based bit level permutation and learning with errors based diffusion for IoT devices.**”. *Computers and Electrical Engineering*, 100:pp. 107954, 2022.
- [15] T. A. Dhopavkar, S. K. Nayak, and S. Roy. “**IETD: A novel image encryption technique using Tinkerbell map and Duffing map for IoT applications.**”. *Multimedia Tools and Applications*, 81(30):pp. 43189–43228, 2022.
- [16] M. Begum and M. S. Uddin. “**igital image watermarking techniques: A review.**”. *Information*, 11(2):pp. 110, 2020.
- [17] R. Wazirali, R. Ahmad, A. Al-Amayreh, M. Al-Madi, and A. Khalifeh. “**Secure watermarking schemes and their approaches in the IoT technology: An overview.**”. *Electronics*, 10(14):pp. 1744, 2021.
- [18] O. P. Singh, A. Anand, A. K. Agrawal, and A. K. Singh. “**Electronic health data security in the internet of things through watermarking: An introduction.**”. *IEEE Internet of Things Magazine*, 5(2):pp. 55–58, 2022.
- [19] M. Begum and M. S. Uddin. “**Towards the development of an effective image watermarking system.**”. *Security and Privacy*, 5(2):pp. e196, 2022.
- [20] W. Wan, J. Wang, Y. Zhang, J. Li, H. Yu, and J. Sun. “**A comprehensive survey on robust image watermarking.**”. *Neurocomputing*, 488:pp. 226–247, 2022.
- [21] N. D. Pulgam and S. K. Shinde. “**Robust digital watermarking using pixel color correlation and chaotic encryption for medical image protection.**”. *International Journal of Intelligent Systems and Applications in Engineering*, 10(4):pp. 29–38, 2022.

- [22] D. K. Mahto and A. K. Singh. “A survey of color image watermarking: State-of-the-art and research directions.”. *Computers & Electrical Engineering*, 93:pp. 107255, 2021.
- [23] K. J. Giri, S. Quadri, R. Bashir, and J. I. Bhat. “DWT based color image watermarking: A review.”. *Multimedia Tools and Applications*, 79:pp. 32881–32895, 2020.
- [24] C. Tiken and R. Samli. “A comprehensive review about image encryption methods.”. *Harran Üniversitesi Mühendislik Dergisi*, 7(1):pp. 27–49, 2022.
- [25] J. Arif. “A novel chaotic permutation-substitution image encryption scheme based on logistic map and random substitution.”. *IEEE Access*, 10:pp. 12966–12982, 2022.
- [26] S. F. Raza and V. Satpute. “A novel bit permutation-based image encryption algorithm.”. *Nonlinear Dynamics*, 95:pp. 859–873, 2019.
- [27] M. Kumar, A. Saxena, and S. S. Vuppala. “A survey on chaos based image encryption techniques.”. *Multimedia Security Using Chaotic Maps: Principles and Methodologies*, :pp. 1–26, 2020.
- [28] R. Ge, G. Yang, J. Wu, Y. Chen, G. Coatrieux, and L. Luo. “A novel chaos-based symmetric image encryption using bit-pair level process.”. *IEEE Access*, 7:pp. 99470–99480, 2019.
- [29] S. Noshadian, A. Ebrahimzade, and S. J. Kazemitabar. “Breaking a chaotic image encryption algorithm.”. *Multimedia Tools and Applications*, 79:pp. 25635–25655, 2020.
- [30] M. Kaur and V. Kumar. “A comprehensive review on image encryption techniques.”. *Archives of Computational Methods in Engineering*, 27:pp. 15–43, 2020.
- [31] W. El-Shafai, F. Khallaf, E.-S. M. El-Rabaie, and F. E. A. El-Samie. “Robust medical image encryption based on DNA-chaos cryptosystem for secure telemedicine and healthcare applications.”. *Journal of Ambient Intelligence and Humanized Computing*, 12:pp. 9007–9035, 2021.
- [32] X. Yan, X. Wang, and Y. Xian. “Chaotic image encryption algorithm based on arithmetic sequence scrambling model and DNA encoding operation.”. *Multimedia Tools and Applications*, 80:pp. 10949–10983, 2021.
- [33] X. Liu and C. Liu. “Quantum image encryption scheme using independent bit-plane permutation and Baker map.”. *Quantum Information Processing*, 22(6):262, 2023.
- [34] C. Rajakumaran and R. Kavitha. “Chaos based encryption of quantum images.”. *Multimedia Tools and Applications*, 79:pp. 23849–23860, 2020.
- [35] G. Ye, K. Jiao, and X. Huang. “Quantum logistic image encryption algorithm based on SHA-3 and RSA.”. *Nonlinear Dynamics*, 104:pp. 2807–2827, 2021.
- [36] M. A. Wani and B. Sultan. “Deep learning based image steganography: A review.”. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 13(3):pp. e1481, 2023.
- [37] C. Lakshmi, K. Thenmozhi, J. B. B. Rayappan, S. Rajagopalan, R. Amirtharajan, and N. Chidambaram. “Neural-assisted image-dependent encryption scheme for medical image cloud storage.”. *Neural Computing and Applications*, 33:pp. 6671–6684, 2021.
- [38] Y. Ding. “DeepEDN: A deep-learning-based image encryption and decryption network for internet of medical things.”. *IEEE Internet of Things Journal*, 8(3):pp. 1504–1518, 2020.
- [39] M. Begum and M. S. Uddin. “Analysis of digital image watermarking techniques through hybrid methods.”. *Advances in Multimedia*, 2020:pp. 1–12, 2020.
- [40] S. B. B. Ahmadi, G. Zhang, and S. Wei. “Robust and hybrid SVD-based image watermarking schemes: A survey.”. *Multimedia tools and Applications*, 79:pp. 1075–1117, 2020.
- [41] Q. Su, X. Zhang, and H. Wang. “A blind color image watermarking algorithm combined spatial domain and SVD.”. *International Journal of Intelligent Systems*, 37(8):pp. 4747–4771, 2022.
- [42] Q. Su and B. Chen. “Robust color image watermarking technique in the spatial domain.”. *Soft Computing*, 22:pp. 91–106, 2018.
- [43] C. Patvardhan, P. Kumar, and C. Vasantha Lakshmi. “Effective color image watermarking scheme using YCbCr color space and QR code.”. *Multimedia Tools and Applications*, 77:pp. 12655–12677, 2018.
- [44] X. Liu, Y. Wu, Z. Shao, J. Wu, and H. Shu. “Color image watermarking using a discrete trinion Fourier transform.”. *Journal of Electronic Imaging*, 27(4):pp. 043046–043046, 2018.
- [45] S. Kumar and B. K. Singh. “An improved watermarking scheme for color image using alpha blending.”. *Multimedia Tools and Applications*, 80:pp. 13975–999, 2021.
- [46] S. Kumar and B. K. Singh. “DWT based color image watermarking using maximum entropy.”. *Multimedia Tools and Applications*, 80:pp. 15487–510, 2021.
- [47] X. Zhang and Q. Su. “A spatial domain-based color image blind watermarking scheme integrating multilevel discrete Hartley transform.”. *International Journal of Intelligent Systems*, 36(8):pp. 4321–4345, 2021.

- [48] K. Prabha and I. S. Sam. “**A novel blind color image watermarking based on Walsh Hadamard Transform.**”. *Multimedia Tools and Applications*, 79:pp. 6845–6869, 2020.
- [49] H. Nazari, M. M. Bidgoli, and H. Ghasvari. “**Integration of lightweight cryptography and watermarking with compression for high speed and reliable communication of digital images in IoT.**”. *IET Image Processing*, , 2023.
- [50] A. Benoraira, K. Benmahammed, and N. Boucenna. “**Blind image watermarking technique based on differential embedding in DWT and DCT domains.**”. *EURASIP Journal on Advances in Signal Processing*, 2015(1):pp. 1–11, 2015.
- [51] J. Abraham and V. Paul. “**An imperceptible spatial domain color image watermarking scheme.**”. *Journal of King Saud University-Computer and Information Sciences*, 31(1):pp. 125–133, 2019.
- [52] X.L. Liu, C.C. Lin, and S.M. Yuan. “**Blind dual watermarking for color images’ authentication and copyright protection.**”. *IEEE Transactions on Circuits and Systems for Video Technology*, 28(5):pp. 1047–1055, 2016.
- [53] N. A. Loan, N. N. Hurrah, S. A. Parah, J. W. Lee, J. A. Sheikh, and G. M. Bhat. “**Secure and robust digital image watermarking using coefficient differencing and chaotic encryption.**”. *IEEE Access*, 6:pp. 19876–19897, 2018.
- [54] M. Moosazadeh and G. Ekbatanifard. “**An improved robust image watermarking method using DCT and YCoCg-R color space.**”. *Optik*, 140:pp. 975–988, 2017.
- [55] M. K. Pandey, G. Parmar, R. Gupta, and A. Sikan-der. “**Non-blind Arnold scrambled hybrid image watermarking in YCbCr color space.**”. *Microsystem Technologies*, 25:pp. 3071–3081, 2019.
- [56] S. Roy and A. K. Pal. “**A blind DCT based color watermarking algorithm for embedding multiple watermarks.**”. *AEU-International Journal of Electronics and Communications*, 72:pp. 149–161, 2017.

Table 3. Evaluation of watermarked images under various attacks based on PSNR.

attack	female	house	jelly	jet	lake	lena	pepper	San_Diego	stockton
1 no attack	54.8756	54.8854	54.9250	54.2105	54.0875	54.8756	53.9369	53.8586	54.3959
2 salt & pepper (0.02)	24.3562	23.8163	24.8506	24.0256	23.3652	24.2352	24.1269	24.6527	24.8212
3 salt & pepper (0.05)	20.4927	20.5358	21.4500	20.1020	19.8578	20.1512	20.2254	20.7756	21.7207
4 Gaussian noise	22.2371	22.1805	23.1142	22.0251	21.9852	22.3121	20.3329	22.1315	23.1321
5 speckle noise	22.9843	22.9126	23.9112	21.8107	22.9113	22.1512	21.3208	22.5231	23.3621
6 sharpening	42.4113	40.9397	46.9211	33.7299	37.8952	41.2994	37.3265	28.5733	34.4908
7 histogram equalization	29.5569	28.6325	23.5485	23.1635	28.1254	24.2614	27.5214	27.0954	23.6961
8 Gaussian filtering	33.5239	40.2561	37.0548	26.7221	38.2491	35.2645	32.8621	23.6381	29.2355
9 median filtering	42.8890	42.9565	47.2459	24.3985	30.9854	33.2631	33.225	27.0186	32.9785
10 rotation (10°)	14.0738	13.6942	14.5368	11.9818	11.7859	12.3132	12.4431	14.1426	17.9979
11 cropping	18.7303	19.1729	18.1521	17.3396	21.0365	19.6382	20.1904	21.0965	22.3897
12 JPEG compression (QF = 90%)	43.7502	39.2676	42.4676	34.0762	43.1657	39.0562	43.8365	47.7563	34.5292
13 contrast adjustment	20.2803	22.1083	17.3266	22.0805	21.3298	20.3228	21.5642	17.5666	19.3759
14 brightening by +40	24.6512	24.6093	24.6090	24.6112	24.5892	24.1154	24.5862	24.3215	24.3156
15 darkening by -30	28.1379	28.1338	28.1308	28.1346	28.1232	28.3145	28.1421	28.1327	28.1309

Table 4. Evaluation of the extracted watermark under various attacks based on NCC.

	attack	female	house	jelly	jet	lake	lena	pepper	San_Diego	stockton
1	no attack	1	1	1	1	1	1	1	1	1
2	salt & pepper (0.02)	0.9934	0.9919	0.9958	0.9933	0.9924	0.9908	0.9917	0.9903	0.9952
3	salt & pepper (0.05)	0.9753	0.9818	0.9865	0.9760	0.9762	0.9825	0.9673	0.9818	0.9860
4	Gaussian noise	0.9848	0.9852	0.9809	0.9722	0.9702	0.9899	0.9735	0.9793	0.9838
5	speckle noise	0.9861	0.9998	0.9998	0.9995	0.9997	0.9978	0.9961	0.9996	0.9998
6	sharpening	0.9995	0.9995	0.9959	0.9996	0.9962	0.9996	0.9974	0.9936	0.9992
7	histogram equalization	0.9999	0.9997	0.9963	0.9998	0.9958	0.9979	0.9935	0.9946	0.9920
8	Gaussian filtering	0.9995	0.9999	0.9999	0.9921	0.9923	0.9993	0.9969	0.9968	0.9985
9	median filtering	0.9997	0.9998	0.9999	0.9935	0.9936	1	0.9974	0.9993	0.9997
10	rotation (10o)	0.9966	0.9938	0.9989	0.9969	0.9958	0.9978	0.9976	0.9915	0.9999
11	cropping	1	1	1	1	1	1	1	1	1
12	JPEG compression (QF = 90%)	0.9998	0.9999	0.9999	0.9998	0.9999	1	0.9997	0.9998	0.9999
13	contrast adjustment	0.9748	0.9825	0.9872	0.9766	0.9735	0.9823	0.9661	0.9829	0.9845
14	brightening by +40	0.9952	0.9989	0.9992	0.9991	0.9989	0.9992	0.9962	0.9992	0.9992
15	darkening by -30	0.9868	0.9995	0.9998	0.9994	0.9998	0.9996	0.9966	0.9994	0.9996

Table 5. The PSNR value of attacked images and NCC of the extracted watermark based on the Salt & Pepper attack.

salt & pepper	female		house		jelly		jet	
	PSNR	NCC	PSNR	NCC	PSNR	NCC	PSNR	NCC
0.01	25.5860	0.9951	26.0847	0.9929	27.0600	0.9931	26.7497	0.9951
0.02	24.3562	0.9934	23.8163	0.9919	24.8506	0.9958	24.0256	0.9933
0.03	23.8146	0.9859	24.4128	0.9829	25.3484	0.9916	25.0923	0.9855
0.04	21.0344	0.9811	21.4945	0.9830	22.2460	0.9792	22.2282	0.9715
0.05	20.4927	0.9753	20.5358	0.9818	21.4500	0.9865	20.1020	0.9760

Table 6. An analysis of the proposed method compared to other methods: Imperceptibility.

metrics	[48]	[52]	[53]	[54]	[55]	[56]	[43]	[?]	[42]	[46]	(Proposed method)
PSNR	47.4772	39.976	40.30	47.64	41.24	49.9898	37.87	37.87	40.85	51.8941	54.8756
SSIM	-	0.9874	-	0.9725	0.9979	-	0.9872	0.99	0.9814	0.9998	1

Table 7. An analysis of the proposed method compared to other methods: Robustness.

	attack	[48]	[52]	[53]	[54]	[55]	[56]	[43]	[56]	[42]	[46]	(proposed method)
1	no attack	0.9999	1	1	1	1	1	1	1	1	1	1
2	salt & pepper (0.02)	0.9874	0.8945	-	-	-	-	1	0.9981	0.9900	0.9895	0.9908
3	salt & pepper (0.05)	-	-	0.9488	0.9710	-	-	-	-	0.9500	0.9704	0.9825
4	Gaussian noise	0.9879	0.9363	0.9941	-	0.9924	0.8967	-	-	-	0.9878	0.9899
5	speckle noise	-	0.9194	0.8780	0.9129	-	0.8838	-	-	-	0.9945	0.9978
6	sharpening	-	1	1	0.9993	0.9248	1	-	-	0.9300	0.9998	0.9996
7	histogram equalization	0.9971	-	0.9961	0.9435	0.9324	0.9950	0.9977	-	0.9400	0.9991	0.9979
8	Gaussian filtering	0.9308	0.9186	1	-	0.9731	0.9313	-	-	0.8700	0.9995	0.9993
9	median filtering	-	0.9596	1	0.9455	0.9645	1	-	-	-	0.9995	1
10	rotation (10°)	0.9993	0.9569	-	-	0.9548	-	-	-	-	0.9979	0.9978
11	cropping	-	0.9438	-	-	-	-	-	0.9998	-	1	1
12	JPEG compression (QF = 90%)	0.9908	0.9979	1	-	1	-	0.931	0.9967	-	0.9999	1