International Journal of Intelligent Communication and Computer Science
Vol. 1, No. 1, 2023, Pages 12-25.

Securing the Digital Flow: Exploring the Efficacy of Watermarking Techniques for Enhanced Online Transmission

Research Paper

Anubhav Bewerwal[1], Rahul Singh[1], Aviral Awasthi[1] and Devesh Pandey[1]

[1]Department of Computer Science & engineering, Graphic Era Hill University, Bhimtal Campus, Nainital Uttrakhand, INDIA
Email:bewarwalanu@gmail.com
Received: 20 April 2023, Revised: 30 Jun 2023, Accepted: 17 July 2023

Abstract:

In today's digital era, the increasing reliance on online applications has led to a growing concern regarding data security on the network. Safeguarding sensitive information is of paramount importance in various domains, including surveillance applications. To address these security challenges, this research focuses on the assessment of digital watermarking techniques under various quality measures to ensure secure online data transmission. The proposed approach incorporates a multi-layered security framework, with the initial layer utilizing Least Significant Bits (LSB) steganography. The recipient receives a decryption key beforehand to ensure secure communication. Subsequently, the actual data is transmitted as an encrypted image through digital watermarking, providing an additional layer of protection. This dual security mechanism ensures the safety and confidentiality of the data which is transmitted. Two widely adopted watermarking techniques, the discrete cosine transform (DCT) and the discrete wavelet transforms (DWT), are extensively explored in this study. Both techniques are evaluated in terms of their effectiveness in preserving data integrity and providing robust security. To assess the effectiveness of the watermarking methods, several quality measures are being used. These include the widely used Peak Signal to Noise Ratio (PSNR) and Structural Similarity (SSIM) metrics, which offer insights into the level of distortion introduced during the watermarking process. Additionally, the Universal Image Quality Index (UIQI) is utilized to gauge the visual quality of the watermarked images.

Keywords: Watermarking, DCT, DWT, PSNR, UIQI and SSIM

1. Introduction:

The concept of digital watermarking shares similarities with traditional watermarks, which are added to provide authenticity verification. In the case of digital watermarks, they are embedded into still photographs in a manner that remains visible to a computer but imperceptible to the human eye [1]. These digital watermarks serve the purpose of transmitting messages containing essential details about the creator, seller, or the image itself. The primary objective of using watermarks is to convey information about the image, specifically to combat copyright infringement. When a watermarked image is opened in an image-editing program that supports Digimarc, the copyright symbol (©) notifies the user that the image is protected by copyright [2]. The watermark further includes a link to the complete contact information of the image's copyright owners, facilitating a straightforward process for the viewer to obtain a license for the image. In this research, we propose a method of dual security, where genuine information is presented as a watermarked image, and a distinct password (key) is transmitted separately before utilizing text steganography. The critical data can only be accessed and retrieved using this unique key. By combining the benefits of digital watermarking and text steganography, this double security approach enhances the

protection of sensitive information within the image. The watermarked image ensures the authenticity and copyright protection, while the hidden text steganography fortifies the security by concealing the actual data in a manner that can only be decoded with the correct key. The dual security methodology is designed to address the increasing concern over data security in various applications, especially when sharing sensitive information over networks. With the integration of watermarked images and the utilization of a separate decryption key for text steganography, unauthorized access to the original data is significantly restricted. This two-step security process provides a robust and efficient means of safeguarding critical information from potential threats and unauthorized use.

2. Preliminary Concepts

In this section basic concept related to Steganography and digital watermarking are presented.

A. Steganography:

Steganography is a technique of covert communication that involves concealing secret information within innocuous-looking cover media, such as images, audio files, videos, or text, in a way that the presence of the hidden data remains undetectable to casual observers [3]. The primary goal of steganography is to ensure the secrecy of the transmitted message by making it appear as ordinary and inconspicuous as possible, effectively hiding it in plain sight. This ancient art has seen modern applications in digital contexts, leveraging the vast storage capacities of digital media to embed sensitive data within the least significant bits of the carrier, making it extremely challenging to detect without specific knowledge of the steganographic technique used. Steganography serves as a valuable tool in fields ranging from information security and cryptography to digital forensics and digital watermarking.

The steganography can be classified into five categories audio/video [4], text [5], protocol [6] and image based [7] on the cover medium as depicted in Figure 1.

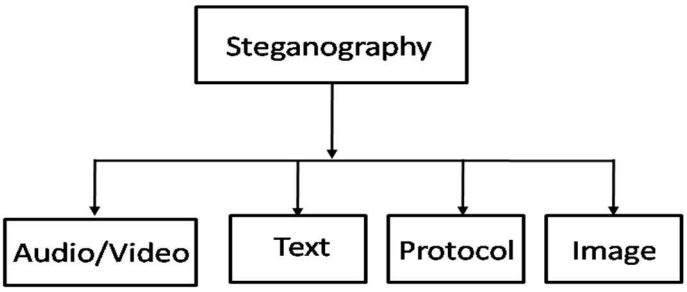


Figure 1: Types of Stenography

In the proposed method, text steganography is utilized, with images being the most common cover media. An embedding system is employed to insert information into a digital image, and this process is accomplished using a secret key. The receiver then decodes the resulting stego-image using the same key through an extraction algorithm. Unauthorized individuals can only observe the transmission of the stego-image but are unable to discern the location of the hidden message.

1. LSB Replacement Method

An image is commonly defined as a digital representation of a image, which can be captured, copied, and saved in digital form. This numerical representation is composed of small units called pixels, forming a grid-like structure. For grayscale graphics, 8 bits are used per pixel, allowing the display of 256 different shades of grey or colors. On the other hand, digital color photos typically utilize the RGB color model, also known as true color, and are stored in 24-bit files. The RGB model employs three primary colors: green, red, and blue, with each color variation in a pixel being defined by 8 bits. Consequently, a single pixel in a 24-bit image can represent 256 different levels of red, green, and blue. To incorporate hidden messages within images, the least significant bit (LSB), specifically the 8th bit, is utilized to carry the concealed information [8]. In the case of 24-bit images, three bits of information can be embedded, with each bit occupying the LSB position of the three eight-bit color values in a pixel. Importantly, altering the LSB does not significantly impact the overall

appearance of the image, ensuring that the resulting stego image appears almost identical to the original cover image. Additionally, in 8-bit graphics, one piece of information can be masked. Overall, digital images come in two primary forms: 24-bit and 8-bit images [8]. While 24-bit images allow for more hidden information due to their higher bit depth, 8-bit images are still capable of concealing a single piece of information [8].

The inverse method is used to remove the hidden image from the stego-image. In the case of the message bit "m" of the secret message to be embedded is comparable to the LSB of the cover image pixel value Q(i, j), then Q(i, j) does not change; otherwise, set the LSB of Q(i, j) to m. The steps for message embedding are as follows:

$T(i,j) = Q(i,j) - 1$, if $\text{LSB}(Q(i,j)) = 1$ and $m = 0$

$T(i,j) = Q(i,j)$, if $\text{LSB}(Q(i,j)) = m$

$T(i,j) = Q(i,j) + 1$, if $\text{LSB}(Q(i,j)) = 0$ and $m = 1$

where LSB $(Q(i, j))$ stands for the LSB of cover image $Q(i, j)$ and m is the next message bit to be embedded. $T(i,j)$ is the stego image.

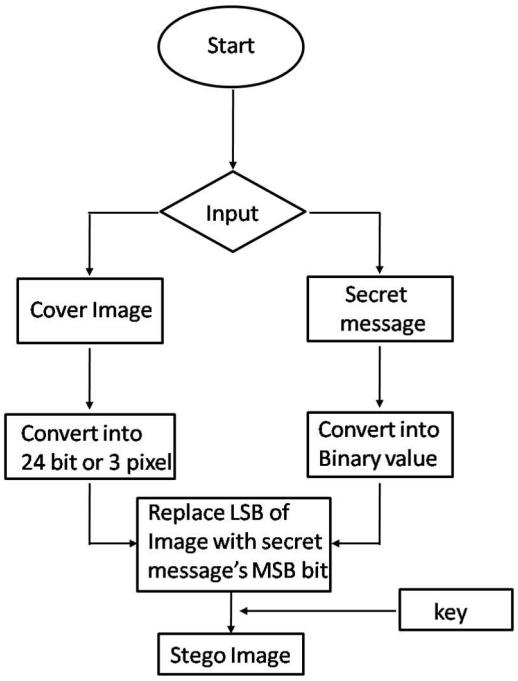


Figure: 2 Flow chart description of LSB Steganography

B. Digital Watermarking:

Digital watermarking is a technique used to embed imperceptible and unique information into digital media, such as images, audio files, videos, or documents, with the aim of verifying the authenticity or ownership of the content [9]. Similar to a physical watermark on a piece of paper, a digital watermark is a digital signature that remains hidden but can be extracted or detected with appropriate tools. The process involves altering the content slightly, typically by making modification in the least significant bits of the data, in a way that does not compromise the media's overall quality or appearance. Digital watermarking finds diverse applications, including copyright protection, content authentication, and tracking intellectual property rights [10]. It allows content creators to assert their ownership, discourage unauthorized distribution or reproduction, and provides a means of tracing the origin of leaked or pirated materials. The robustness and invisibility of digital watermarks make them an invaluable tool in safeguarding digital assets and preserving the integrity of digital content in today's vast and easily accessible digital landscape.

1. Transform Domain Technique

The message is encapsulated within modified coefficients of the image in the frequency domain, increasing both the message's ability to conceal information and its resistance to attacks. One category of embedding techniques is transform domain embedding [11]. Algorithms of several types have been proposed for

embedding methods. Strong steganographic and watermarking technologies now operate mostly in the transform domain.
The Transform domain approaches employed in the paper are listed is detailed as:
1. Discrete cosine transformation technique (DCT).
2. Discrete Wavelet transformation technique (DWT).

(a) Discrete Cosine Transform
After converting the colour coordinates, the three colour components of the image are divided into different 8x8 blocks [12].
Forward DCT

$$F(u,v) = \frac{2}{N} C(u)C(v) \sum_{x=0}^{N-1} \sum_{y=0}^{N-1} f(x,y) \cos\left[\frac{\pi(2x+1)u}{2N}\right] \cos\left[\frac{\pi(2y+1)v}{2N}\right]$$

$$\text{for } u = 0,\ldots,N-1 \text{ and } v = 0,\ldots,N-1 \qquad (1)$$

$$\text{where } N = 8 \text{ and } C(k) = \begin{cases} 1/\sqrt{2} & \text{for } k = 0 \\ 1 & \text{otherwise} \end{cases}$$

Inverse DCT

$$f(x,y) = \frac{2}{N} \sum_{u=0}^{N-1} \sum_{v=0}^{N-1} C(u)C(v)F(u,v) \cos\left[\frac{\pi(2x+1)u}{2N}\right] \cos\left[\frac{\pi(2y+1)v}{2N}\right] \qquad (2)$$

$$\text{for } x = 0,\ldots,N-1 \text{ and } y = 0,\ldots,N-1 \text{ where } N = 8$$

In the chosen 8×8 block, the individual pixel values are represented by f(x, y), while the resulting DCT coefficients after transformation are denoted by F (*u*, *v*). It's important to note that the transformation process converts the original 8×8 block into another 8×8 block composed of F (*u*, *v*) coefficients. Cox introduced the initial frequency-domain watermarking system. Following that, numerous frequency domain watermarking algorithms were presented [7]. The frequency-domain watermark should be incorporated into the host image's mid-band, which is now a widely acknowledged practice. Watermarks often have less of an influence on the original image's nature in the high frequency region than in the low frequency band, and the mid-bind approach strikes the correct balance between imperceptibility and durability [7].

(b) Discrete Wavelet Transform
DWT is a fundamental concept extensively used in image processing, aiming to decompose an image into sub-images, each with distinct spatial domains and frequency regions [12]. This transformation process begins by separating the image into different frequency components, which are then further analyzed and processed.
The image is transformed with the DWT on an input image, it undergoes a process of multi-level differentiation. The image is divided into smaller sub-images, typically in a hierarchical manner. At each level of decomposition, the sub-images are further split into four distinct frequency districts: one low-frequency district (LL) and three high-frequency districts (LH, HL, HH). When subjecting the low-frequency district (LL) information to the DWT, we acquire sub-level frequency district data. As depicted in Figure 3, the image has undergone a 3-level DWT decomposition, producing various frequency components. In this context, the letter "L" represents a low-pass filter operation, while "H" denotes a high-pass filter operation.
It is possible to separate an original image into its LL1, LH1, HL1, and HH1 frequency districts. The sub-level frequency district information of LL2, HL2, LH2, and HH2 can be further deconstructed from this low-frequency district data. This allows the procedure to proceed for an n-level wavelet transformation. Low frequency region information closely resembles the original image. This frequency band contains a sizable amount of the signal information of the original image. The level, upright and diagonal detail of the actual image is each represented by the frequency districts LH, HL, and HH.
As per the HVS character, it is possible for humans to observe any changes in smooth areas of an image but unable to figure changes in edge, profile, and streak. Thus, it is hard to fathom that adding a watermarking signal to the highly amplifiable high-frequency band of an image that has undergone DWT transformation. Now, it has a greater concealing effect and can transmit more watermarking signal.

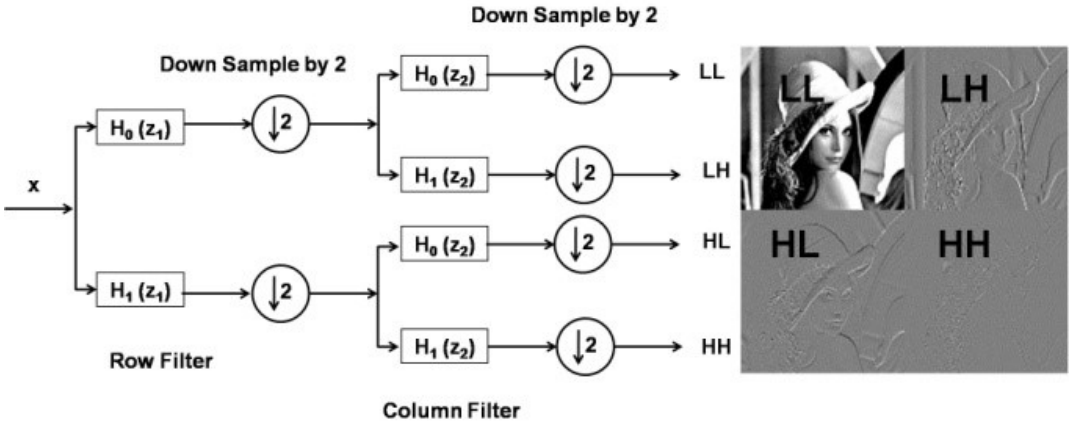


Figure 3: Image decomposition using DWT

3. Proposed Method

The proposed dual security system provides an enhanced level of protection for secure online data transmission by combining text steganography and digital watermarking techniques. The system operates in two main stages: the key exchange phase and the data transmission phase.

A. Key Exchange Phase: In the key exchange phase, a password or encryption key is securely transmitted to the intended recipient using text steganography. Text steganography is a method of hiding information within a text, and in this case, it is used to conceal the key within a seemingly innocent text message or document. The sender and the recipient must have a prearranged understanding of how the key is concealed within the text. This method ensures that the key is securely shared between the sender and the recipient without being intercepted by unauthorized individuals. In this work Elliptic Curve Cryptography is considered for key exchanges.

Elliptic Curve Cryptography (ECC) is a widely used public-key cryptographic technique that is based on the mathematics of elliptic curves [13]. It offers strong security with relatively smaller key sizes compared to traditional public-key algorithms like RSA. The security of ECC relies on the difficulty of solving certain mathematical problems associated with elliptic curves. Below, I will explain the key concepts of ECC with mathematical formulations:

1. **Elliptic Curves:** An elliptic curve is a mathematical curve defined by an equation of the form: $y^2 = x^3 + ax + b$ where a and b are constants that define the specific curve. The curve is defined over a finite field, denoted as F_p where p is a prime number. The points on the elliptic curve form a group with a special point called the "point at infinity" denoted as O.
2. **Point Addition:** Points on an elliptic curve can be added together using geometrically defined addition formulas. Given two points P and Qon the curve, their sum R =P+Q is calculated as follows:
   If P and Q are distinct points:

$$\lambda = \frac{y_Q - y_P}{x_Q - x_P} \tag{3}$$

$$x_R = \lambda^2 - x_P - x_Q \tag{4}$$

$$y_R = \lambda(x_P - x_R) - y_P \tag{5}$$

If P and Q are the same point (i.e., doubling a point):

$$\lambda = \frac{3x_P^2 + a}{2y_P} \tag{6}$$

$$x_R = \lambda^2 - 2x_P \tag{7}$$

$$y_R = \lambda(x_P - x_R) - y_P \tag{8}$$

3. **Scalar Multiplication:** Scalar multiplication involves adding a point to itself multiple times, and the result is another point on the curve. Mathematically, scalar multiplication is defined as: $n \cdot P = P+P+P+\ldots+P$ (n times)
4. **Public and Private Keys:** In ECC, each user has a public-private key pair. The public key is a point QQ on the curve, while the private key is an integer dd. The public key is obtained by scalar multiplication of a fixed base point G on the curve with the private key: $Q = d \cdot G$
5. **Key Exchange:** ECC is used for key exchange. For key exchange, two parties exchange their public keys and perform scalar multiplication with their private keys to obtain a shared secret that can be used for symmetric encryption.

ECC's security is based on the difficulty of the elliptic curve discrete logarithm problem, which involves finding d given $Q = d \cdot G$. The best-known algorithm to solve this problem is the generic "brute-force" approach, which is computationally infeasible for sufficiently large key sizes.

B. Data Transmission Phase: Once the key exchange phase is completed, the actual data transmission takes place. This phase involves the use of a watermarked image that contains an embedded message or another image. The watermarked image is created by embedding the data to be transmitted within the image using digital watermarking techniques.

Before sending the watermarked image over the network, an additional layer of security is applied. The watermarked image is encrypted to further protect the concealed data from unauthorized access or tampering. This encryption process converts the watermarked image into a ciphertext, which appears as random and meaningless data to anyone without the decryption key. Upon receiving the encrypted watermarked image, the recipient can proceed with the decryption process using the previously shared key. The decryption restores the original watermarked image. The recipient can then extract the concealed data from the image using the key that was received before the transmission. Since the decryption key is required to obtain the hidden information, unauthorized individuals who intercept the encrypted image during transmission will not be able to access the concealed data without the corresponding key. By employing this dual security system, the transmitted data benefits from two layers of protection: the steganographically concealed key and the encryption of the watermarked image. This approach significantly enhances the security of online data transmission, making it challenging for potential attackers to intercept, interpret, or tamper with the sensitive information being sent. The system's effectiveness lies in the combination of these two robust security measures, safeguarding the confidentiality and integrity of the transmitted data throughout the entire communication process.

Figure 4 shows the concept mentioned previously. Two strategies, DCT and DWT, are taken into consideration in the analysis for watermarks, and it is demonstrated that they both function very well. In the prior system (Figs. 4 and 5), PSNR is regarded as the primary criterion for evaluating image quality. The fundamental concept of both systems is the same; in this case, both the cover image and the secret image or messages are first transformed (DCT/DWT), after which a watermarked image is produced. At the receiver end, an inverse transform is carried out to produce the cover image and secret image or message. PSNR is calculated for cover, secret, and recovered images for the quality evaluation. As a result, the transforms employed in the aforementioned tow system will solely have an impact on PSNR. The next section demonstrates why PSNR is a poor-quality indicator and why other approaches should be employed to accurately assess the image quality.

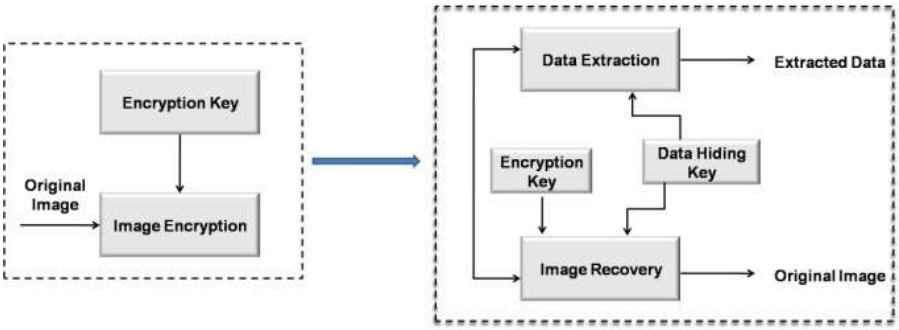


Figure 4: Schematic of proposed work

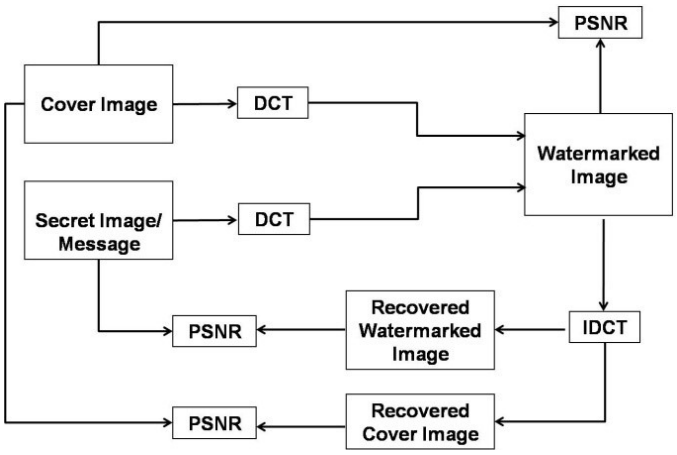


Figure 5: Flow chart description of DCT based watermark

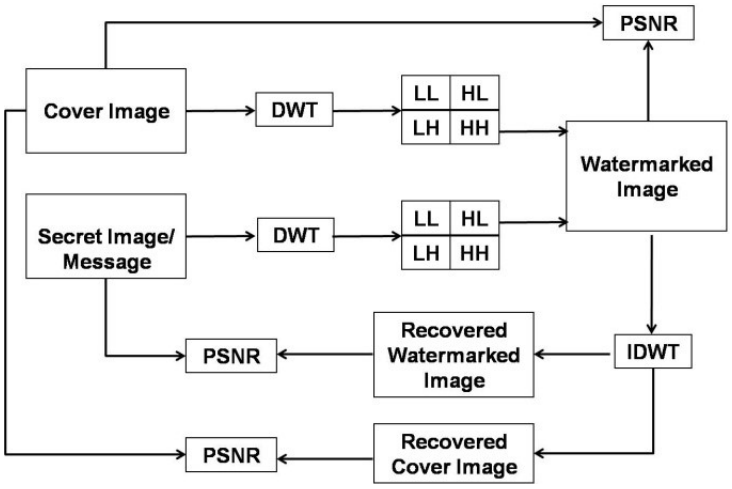


Figure 6: Flow chart description of DWT based watermark

4. Performance Measures

In this study, the assessment of digital watermarking techniques for secure online transmission involves the evaluation of four performance measures: Peak Signal to Noise Ratio (PSNR), Universal Image Quality Index (UIQI), SSIM, and Entropy.

A. Peak Signal to Noise Ratio (PSNR)

Famous PSNR can be used to stego images as a performance indicator for visual distortion caused by message concealing. It's outlined as [14]:

$$PSNR(dB) = 10\log\frac{\left(Q_{\max}\right)^2}{MSE} \tag{9}$$

MSE = mean square error;
which is given as:

$$MSE = \frac{\left(T-Q\right)^2}{MN} \tag{10}$$

With $Q_{\max} = 255$:

Where M and N are the dimensions of the image, T is the resultant stego-image, and Q is the cover image.

B. Universal Image Quality Index (UIQI)

The UIQI is a metric used to assess the quality of an image by comparing it to a reference or original image. It is a full-reference objective image quality assessment method that takes into account various aspects of image fidelity. UIQI measures the structural similarity between the two images by evaluating their luminance, contrast, and structural information. The index is designed to be robust and provide consistent results across different types of images, making it a versatile tool in image processing and compression applications. By computing the UIQI, one can quantitatively analyze the degradation or loss of image quality due to various image processing operations or transmission through lossy channels. With its ability to objectively measure image quality, the Universal Image Quality Index serves as a valuable resource in image and video processing, enabling researchers and practitioners to optimize and enhance image-related applications with a focus on preserving visual fidelity [15].

Let $x = \{x_i \mid i = 1, 2 \ldots N\}$ and $y = \{y_i \mid i = 1, 2 \ldots N\}$ be the original and test images signals respectively. The UIQI index is defined as

$$UIQI(x, y) = \frac{4\mu_x \mu_y \sigma_{xy}}{\left(\mu_x^2 + \mu_y^2\right)\left(\sigma_x^2 + \sigma_y^2\right)} \tag{11}$$

$$UIQI(x, y) = l(x, y), c(x, y), s(x, y) \tag{12}$$

UIQI index is composed of three components, luminance (*l*), contrast (*c*) and similarity measure (*s*) in terms of co-relation co-efficient and defined as

$l(x, y) = \frac{2\mu_x \mu_y}{\mu_x^2 + \mu_y^2}$, $c(x, y) = \frac{2\sigma_x \sigma_y}{\sigma_x^2 + \sigma_y^2}$ and

$s(x, y) = \frac{\sigma_{xy}}{\sigma_x \sigma_y}$.

Where, $\mu_x = \frac{1}{N}\sum_{i=1}^{N} x_i$, $\mu_y = \frac{1}{N}\sum_{i=1}^{N} y_i$, $\sigma_x^2 = \frac{1}{N-1}\sum_{i=1}^{N}(x_i - \mu_x)^2$, $\sigma_y^2 = \frac{1}{N-1}\sum_{i=1}^{N}(y_i - \mu_y)^2$ and

$$\sigma_{xy} = \frac{1}{N-1}\sum_{i=1}^{N}(x_i - \mu_x)(y_i - \mu_y). \tag{13}$$

C. Structure Similarity Image Metrics (SSIM)

The foundation of SSIM lies in the understanding that the human visual system is highly attuned to processing structural details in images. SSIM's underlying concept is to mimic this perceptual sensitivity by devising an algorithm that measures the alterations in structural information between a reference (original) and a distorted image. By doing so, SSIM aims to provide a more accurate assessment of the subjective quality of an image compared to traditional metrics such as Mean Squared Error (MSE) or PSNR [16].

At its core, SSIM attempts to gauge the changes in various important aspects of an image, namely, luminance, contrast, and structure. These fundamental elements play crucial roles in human visual perception and image quality assessment. SSIM's approach involves analyzing these components to quantitatively measure the similarity between a reference (original) image and a distorted image.

$$SSIM(x, y) = \frac{\left(2\mu_x \mu_y + c_1\right)(2\sigma_{xy} + c_2)}{\left(\mu_x^2 + \mu_y^2 + c_1\right)\left(\sigma_x^2 + \sigma_y^2 + c_2\right)} \tag{14}$$

$$MSSIM = \frac{1}{T}\sum_{j=1}^{T} SSIM_j \tag{15}$$

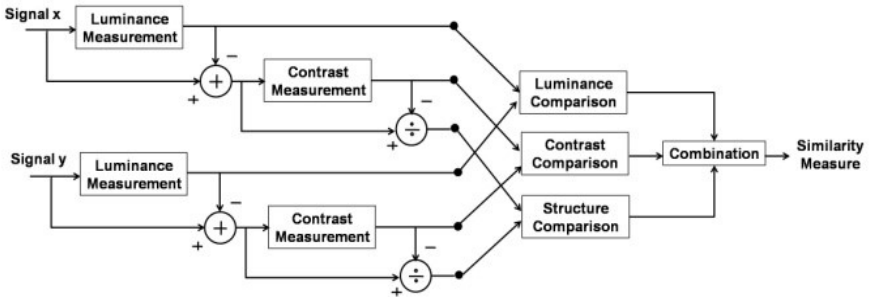


Figure 7: Flow chart description of DWT based watermark

D. Entropy

Entropy can be defined as a measure of randomness or uncertainty in a given set of data. In the context of an image, entropy is used to quantify the amount of information or randomness present in the pixel intensities. Higher entropy values indicate more complex and varied pixel patterns, while lower entropy values suggest a more uniform or predictable distribution of pixel intensities. Mathematically, the entropy of an image can be calculated using the given below formula [17]:

$$H = -\sum_{i=1}^{N} p(i) \log_2 p(i) \tag{16}$$

Where, H is the entropy of the image. is the number of possible pixel intensity levels (usually 256 for an 8-bit grayscale image) and $p(i)$ is the probability of occurrence of a pixel intensity i in the image.

5. Simulation Results

In the initial phase of the secure data transmission process, a random key with the value '3774' is sent from the sender to the receiver using text steganography. Text steganography involves concealing information within a seemingly innocuous text or document. In this case, the key '3774' is cleverly embedded within a text message to ensure secure transmission without raising suspicion. Upon receiving the transmitted text message, the receiver successfully decodes the hidden key '3774' using the prearranged understanding of how the key was concealed within the text. This key exchange phase establishes a secure communication channel between the sender and the receiver, allowing for the subsequent transmission of sensitive data. For the watermark embedding phase, a set of standard images, namely Lena, Baboon, Boat, Barbara, and Peppers, are considered. Each of these images is in the pgm (Portable Gray Map) format and has a resolution of 512x512 pixels. The digital watermarking technique employed for embedding the data into the standard images uses an embedding depth of 0.01. The embedding depth represents the strength of the watermarking process, determining how much the watermark is blended into the image without significantly altering its visual appearance.

A. DCT Results

The results obtained under the DCT for the digital watermarking process are presented in Table 1. The table showcases the performance metrics for each of the considered images, including Lena, Baboon, Boat, Barbara, and Peppers. To illustrate the results obtained, the paper displays the watermarked image of Baboon, showcasing the effectiveness of the watermarking technique for this specific image. The PSNR for the Lena image is 41.0595, with a UIQI value of 1, implying that the watermarked Lena image maintains its visual quality and closely resembles the original image. However, the SSIM value for the Lena image is 0.8807, indicating a slight decrease in structural similarity compared to the Baboon image.

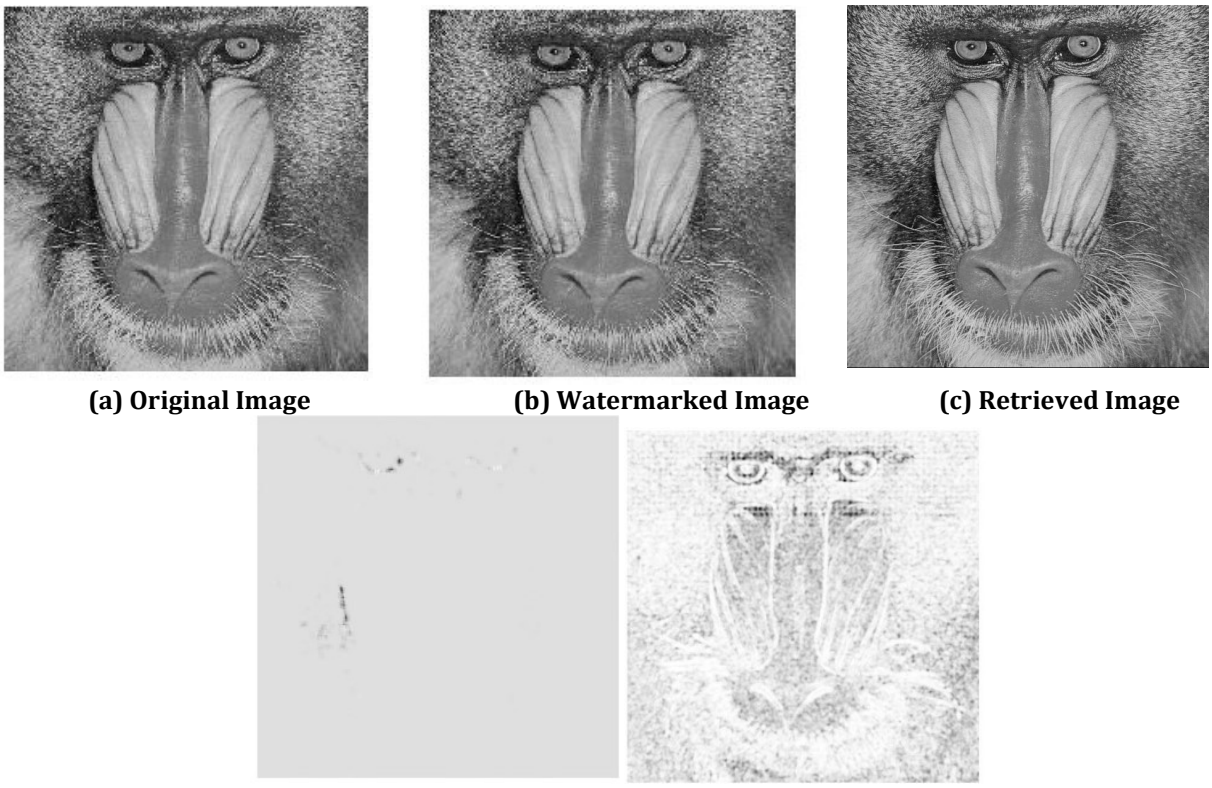
Table 1: DCT Results for various images

Image	PSNR	IQUI	SSIM
Lena	41.0595	1.0000	0.8807
Baboon	40.5107	1.0000	0.9239
Boat	40.8441	0.9999	0.8802
Barbara	41.0948	1.0000	0.9146
Peppers	40.4979	0.9918	0.8644

One of the key metrics used for the evaluation of the watermarked images quality is the PSNR. For the considered images, the PSNR values are nearly around 40 dB. A higher PSNR value indicates better image fidelity, signifying that the watermarked images closely resemble the original images, with minimal distortion.

The UIQI is another metric used to assess the overall visual quality and similarity between the original and watermarked images. For most of the images, the UIQI value is nearly one, which suggests that the watermarked images exhibit high visual similarity to their respective original images. A UIQI value close to one indicates a strong resemblance between the watermarked and original images, ensuring that the watermarking process preserves the visual integrity of the images.

On the other hand, the SSIM varies across the considered images. The minimum SSIM value is 0.8644 for the Peppers image, indicating some variation and loss of structural similarity between the original and watermarked versions. However, the maximum SSIM value is 0.9239 for the Baboon image, demonstrating a higher level of structural similarity between the two versions. A higher SSIM value indicates a closer match between the structural elements of the original and watermarked images.



(a) Original Image **(b) Watermarked Image** **(c) Retrieved Image**

(d) IQUI Index Map Image **(e) SSIM Index Map Image**

Figure 8: Results for DCT watermarks (Baboon Image)

In Figure 8 (a-e), the results obtained from the DCT for the digital watermarking process are visually demonstrated. The figures provide a comprehensive illustration of the effectiveness of the watermarking technique on the Baboon image.

In Figure (a), the original Baboon image is displayed, representing the unaltered and pristine version of the image. This serves as the baseline for comparison with the watermarked and retrieved images.

In Figure (b), the obtained watermarked image is presented. This image is the result of embedding the concealed data into the Baboon image using the DCT-based watermarking technique. Despite the watermarking process, the visual quality of the Baboon image is well-preserved, and the watermarked image appears very similar to the original Baboon image.

In Figure (c), the retrieved image is showcased. This image is the output of the watermark extraction process performed on the watermarked image. The retrieved image demonstrates the successful recovery of the

concealed data, and its high resemblance to both the original and watermarked images indicates the accuracy and effectiveness of the watermark retrieval process. To the human eye, it is challenging to detect any noticeable differences among these three images, confirming the seamless integration of the watermark into the Baboon image.

To quantitatively assess the quality of the retrieved image, the PSNR is obtained and presented in Table 1. PSNR provides a numerical value that represents the level of distortion introduced during the watermarking and retrieval processes. Higher PSNR values indicate a closer resemblance between the retrieved image and the original image, signifying higher image fidelity.

Additionally, Figure (d) displays the obtained UIQI map, and Figure (e) presents the SSIM map. These maps provide visual representations of the quality and similarity between the retrieved image and the original image at different regions. A higher UIQI value and SSIM value suggest a stronger similarity and better preservation of structural elements between the retrieved image and the original image, confirming the successful retrieval of the watermark without significant visual degradation.

Overall, the visual results and quantitative assessments presented in Figure 8 (a-e) and Table 2 demonstrate the effectiveness and robustness of the DCT-based digital watermarking technique in securing and preserving the integrity of the Baboon image during the transmission and retrieval process.

B. DWT Results

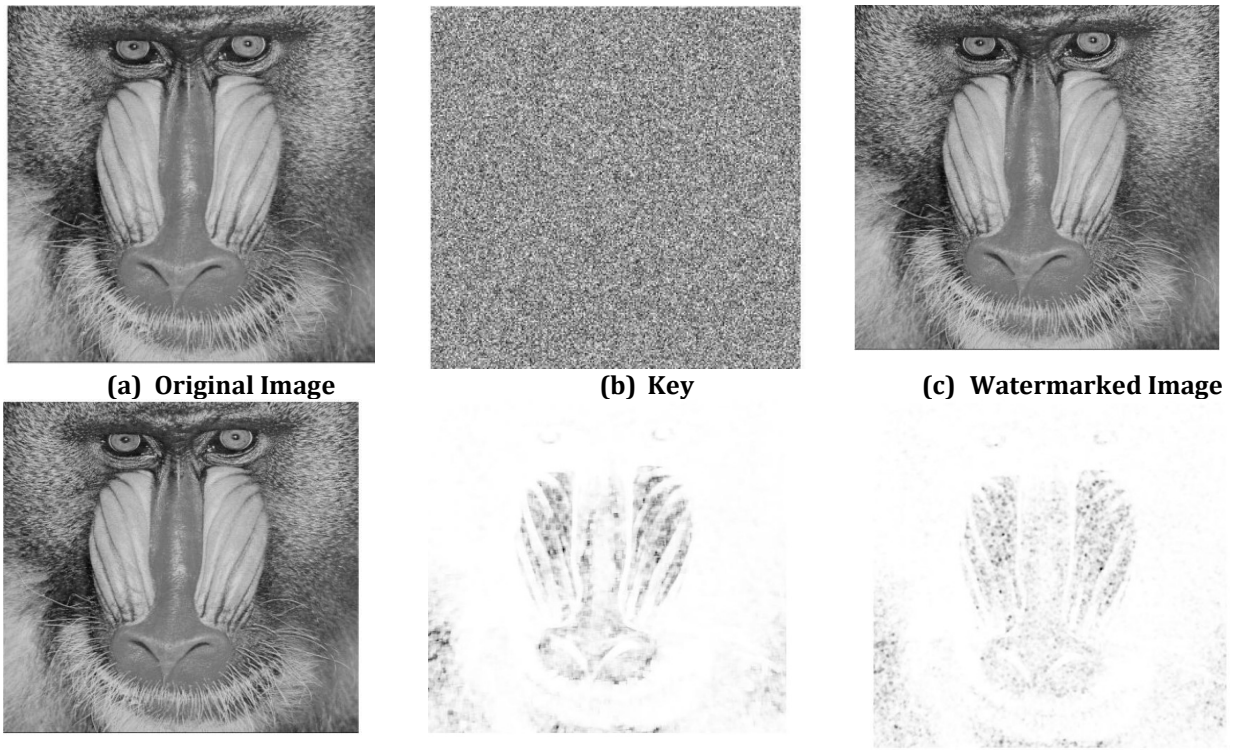
Table 2 presents the results obtained under the Discrete Wavelet Transform (DWT) for the digital watermarking process. This table showcases the performance metrics for the considered images, including Lena, Baboon, Boat, Barbara, and Peppers. Upon analyzing the results in Table 2, it is evident that the PSNR values for the considered images are approximately around 24 dB. The PSNR metric provides a measure of the image fidelity, indicating how well the watermarked images resemble the original images. A higher PSNR value suggests a closer match between the watermarked and original images, indicating better image quality and lower distortion. Similarly, for most of the images, the UIQI and SSIM values are nearly one. A UIQI and SSIM value close to one imply a high level of visual similarity and structural preservation between the original and watermarked images. These results indicate that the DWT-based watermarking process successfully preserves the visual quality and structural elements of the watermarked images, ensuring a high degree of image integrity. For the purpose of illustrating the obtained results, the paper showcases the watermarked image of Baboon, demonstrating the effectiveness of the DWT-based watermarking technique specifically for this image. By comparing Table 1 and Table 2, a significant difference is observed in the PSNR values between the DWT and DCT watermarking techniques. The PSNR values obtained with DWT are noticeably lower compared to those achieved with DCT. This difference in PSNR values suggests that the DWT-based watermarking process introduces more distortion or loss of information in the watermarked images compared to the DCT-based process. This may be attributed to the different mathematical properties and transformations used in DWT and DCT. However, it is noteworthy that despite the lower PSNR values, the DWT-based technique exhibits higher structural similarity between the watermarked and original images compared to DCT. The higher SSIM values for DWT indicate that the DWT-based process better preserves the structural elements of the images, leading to images that closely resemble the originals in terms of texture and patterns.

Table 2: DWT Results for various images

Image	PSNR	IQUI	SSIM
Lena	24.0654	0.9837	0.9961
Baboon	24.0702	0.9980	0.9986
Boat	24.0657	0.9737	0.9958
Barbara	24.0654	0.9925	0.9978
Peppers	24.3212	0.9926	0.9973

In Figure 9 (a-e), the results obtained using the DCT for digital watermarking are visually presented. These figures provide a comprehensive illustration of the effectiveness of the watermarking technique for the Baboon image. In Figure (a), the original Baboon image is displayed, representing the unaltered and pristine version of the image, which serves as the baseline for comparison. In Figure (b), the key used in the watermarking process is shown. The key '3774' was sent in advance using text steganography, as mentioned earlier. This key plays a crucial role in the watermarking process, ensuring secure and accurate data retrieval.

Figure (c) showcases the obtained watermarked image. This image is the result of embedding the concealed data into the Baboon image using the DCT-based watermarking technique. The watermarking process ensures that the sensitive data is seamlessly integrated into the image, without causing significant visual distortion or degradation. The watermarked image closely resembles the original Baboon image, making it difficult for the human eye to detect any visible differences. In Figure (d), the retrieved image is displayed. This image is the outcome of the watermark extraction process performed on the watermarked image using the key sent in advance. The successful retrieval of the concealed data is evident from the high resemblance between the retrieved image and both the original and watermarked images. This demonstrates the accuracy and effectiveness of the watermark retrieval process, where the data is recovered without any loss of information. To further assess the quality of the retrieved image, Figure (e) presents the obtained UIQI map, and Figure (f) showcases the SSIM map. These maps provide visual representations of the quality and similarity between the retrieved image and the original image at different regions. The high UIQI and SSIM values in these maps signify the strong similarity and preservation of structural elements between the retrieved image and the original image, confirming the successful retrieval of the watermark without significant visual degradation.



(a) Original Image **(b) Key** **(c) Watermarked Image**

(d) Retrieved Image **(e) IQUI Index Map Image** **(f) SSIM Index Map Image**

Figure 9: Results for DWT watermarks (Baboon Image)

Notably, both DCT and DWT methods have been used in this work, and in both cases, the concealed message is successfully retrieved using the key sent in advance. This verifies the effectiveness of the dual security system, where the combination of text steganography for secure key exchange and the chosen watermarking method ensures the secure transmission and retrieval of the concealed data. This robust approach enhances the confidentiality and integrity of the transmitted data, making it challenging for unauthorized individuals to intercept or tamper with the sensitive information being sent.

Upon comparing the results in Tables 1 and 2, it becomes evident that, except for the PSNR, the other performance metrics are very similar in both tables. The tables present the results obtained from the Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) methods for digital watermarking.

To investigate the differences in PSNR values further, the researchers explore the randomness of the images by measuring the entropy of the original and watermarked images. Entropy is a measure of randomness or

uncertainty in an image's pixel intensities. Higher entropy values indicate greater complexity and variation in pixel patterns.

C. Entropy

Table 3: Entropy Results for various images

Image	Original Image	Watermarked Image DCT	Watermarked Image DWT
Lena	7.4456	7.4655	7.4595
Baboon	7.3579	7.3763	7.3811
Boat	7.1238	7.1597	7.1419
Barbara	7.6321	7.6546	7.6462
Peppers	7.5715	7.6052	7.5923

The results of the entropy analysis are shown in Table 3. Surprisingly, it is observed that the entropy of the original images, as well as the watermarked images using both DCT and DWT, is nearly the same. This means that the level of randomness or complexity in the original and watermarked images is similar, regardless of the watermarking technique used. This suggests that the watermarking processes do not significantly alter the overall randomness or information content of the images.

Based on the discussions and the obtained results, it becomes clear that PSNR alone cannot be solely relied upon as an image quality assessment parameter. While PSNR values may vary significantly between DCT and DWT watermarking techniques, the other quality measures such as UIQI, SSIM, and entropy show minimal differences.

This observation highlights the importance of considering multiple quality metrics when evaluating the effectiveness and performance of digital watermarking techniques. While PSNR is a commonly used metric, it may not fully capture the visual quality and structural similarity of watermarked images. Other metrics like UIQI, SSIM, and entropy provide more comprehensive insights into image quality, preservation of visual features, and information content.

In conclusion, a holistic evaluation of digital watermarking techniques should involve analyzing a combination of different quality measures to make informed decisions regarding their suitability for specific applications. A single metric may not provide a complete image of image quality, and it is essential to consider a range of measures to ensure the effectiveness and security of the watermarking process.

5. Conclusions

This research article presents a comprehensive and in-depth examination of a novel two-fold secure online transmission system that seamlessly integrates fundamental steganography and watermarking methods. The primary focus of the study revolves around conducting a meticulous comparison between the efficiency and performance of two widely recognized watermarking methods: the DCT based scheme and the DWT based scheme. The obtained results were presented in terms of PSNR, UIQI, SSIM, and entropy as image quality assessment metrics. Through rigorous experimentation and evaluation, the paper demonstrates that both DCT and DWT-based schemes are equally efficient in securing online data transmission. The dual security system, which combines text steganography for key exchange and watermarking for data concealment, proves to be robust in preserving the confidentiality and integrity of transmitted data. The analysis of image quality metrics revealed interesting findings. While the PSNR results varied between the DCT and DWT methods, the other quality measures, including UIQI, SSIM, and entropy, remained consistently similar. This suggests that the watermarking techniques, irrespective of their differences in PSNR values, effectively preserve the visual quality and structural similarity of the watermarked images. A critical insight drawn from the research is that PSNR alone cannot be considered as a reliable quality measure for images. The paper highlights the importance of using a diverse set of quality metrics to gain a comprehensive understanding of image fidelity and preservation. Relying solely on PSNR may overlook critical nuances in the visual appearance and structural similarity of watermarked images.

References

1. Cox, Ingemar, Matthew Miller, Jeffrey Bloom, Jessica Fridrich, and Ton Kalker. *Digital watermarking and steganography*. Morgan kaufmann, 2007.

2. Seitz, Juergen. *Digital watermarking for digital media*. IGI Global, 2005.
3. Cheddad, Abbas, Joan Condell, Kevin Curran, and Paul Mc Kevitt. "Digital image steganography: Survey and analysis of current methods." *Signal processing* 90, no. 3 (2010): 727-752.
4. Kakde, Yugeshwari, Priyanka Gonnade, and Prashant Dahiwale. "Audio-video steganography." In *2015 International Conference on Innovations in Information, Embedded and Communication Systems (ICIIECS)*, pp. 1-6. IEEE, 2015.
5. Krishnan, R. Bala, Prasanth Kumar Thandra, and M. Sai Baba. "An overview of text steganography." In *2017 Fourth International Conference on Signal Processing, Communication and Networking (ICSCN)*, pp. 1-6. IEEE, 2017.
6. Jankowski, Bartosz, Wojciech Mazurczyk, and Krzysztof Szczypiorski. "PadSteg: Introducing inter-protocol steganography." *Telecommunication Systems* 52 (2013): 1101-1111.
7. Hussain, Mehdi, Ainuddin Wahid Abdul Wahab, Yamani Idna Bin Idris, Anthony TS Ho, and Ki-Hyun Jung. "Image steganography in spatial domain: A survey." *Signal Processing: Image Communication* 65 (2018): 46-66.
8. Al-Shaarani, Faiza, and Adnan Gutub. "Securing matrix counting-based secret-sharing involving crypto steganography." *Journal of King Saud University-Computer and Information Sciences* 34, no. 9 (2022): 6909-6924.
9. Nematollahi, Mohammad Ali, Chalee Vorakulpipat, and Hamurabi Gamboa Rosales. *Digital watermarking*. Springer Singapore:, 2017.
10. Tao, Hai, Li Chongmin, Jasni Mohamad Zain, and Ahmed N. Abdalla. "Robust image watermarking theories and techniques: A review." *Journal of applied research and technology* 12, no. 1 (2014): 122-138.
11. Kadian, Poonam, Shiafali M. Arora, and Nidhi Arora. "Robust digital watermarking techniques for copyright protection of digital data: A survey." *Wireless Personal Communications* 118 (2021): 3225-3249.
12. Mehto, Amit, and Neelesh Mehra. "Adaptive lossless medical image watermarking algorithm based on DCT & DWT." *Procedia Computer Science* 78 (2016): 88-94.
13. Koblitz, Neal, Alfred Menezes, and Scott Vanstone. "The state of elliptic curve cryptography." *Designs, codes and cryptography* 19 (2000): 173-193.
14. Korhonen, Jari, and Junyong You. "Peak signal-to-noise ratio revisited: Is simple beautiful?." In *2012 Fourth International Workshop on Quality of Multimedia Experience*, pp. 37-38. IEEE, 2012.
15. Medda, Alessio, and Victor DeBrunner. "Color image quality index based on the UIQI." In *2006 IEEE Southwest Symposium on Image Analysis and Interpretation*, pp. 213-217. IEEE, 2006.
16. Sara, Umme, Morium Akter, and Mohammad Shorif Uddin. "Image quality assessment through FSIM, SSIM, MSE and PSNR—a comparative study." *Journal of Computer and Communications* 7, no. 3 (2019): 8-18.
17. Tsai, Du-Yih, Yongbum Lee, and Eri Matsuyama. "Information entropy measure for evaluation of image quality." *Journal of digital imaging* 21 (2008): 338-347.