College of Engineering

ISSN: 1813-162X (Print); 2312-7589 (Online)

Tikrit Journal of Engineering Sciences

available online at: http://www.tj-es.com

TJES Tikrit Journal of Engineering Sciences

Optimizing Data Security with Hybrid Scheme Based on LSB and DWT

Sarah Faeq Abdullah *[a], Shahir Fleyeh Nawaf [b]

a Electrical Department, Engineering College, Kirkuk University, Kirkuk, Iraq.
b Electrical Department, Engineering College, Tikrit University, Tikrit, Iraq.

Keywords:

Cryptography, Data hidings, PSNR, RMSE, Steganography.

ARTICLE INFO

Article history:

Received	04 May	2023
Received in revised form	31 July	2023
Accepted	07 Aug.	2023
Final Proofreading	17 Aug.	2023
Available online	15 Oct.	2023

Citation: Abdullah SF, Nawaf SF. **Optimizing Data Security with Hybrid Scheme Based on LSB and DWT**. *Tikrit Journal of Engineering Sciences* 2023; **30**(3): 190-199.
http://doi.org/10.25130/tjes.30.3.17

***Corresponding author:**

Sarah Faeq Abdullah

Electrical Department, Engineering College, Kirkuk University, Kirkuk, Iraq.

Abstract: One of the most popular techniques in image steganography is the Least Significant Bit (LSB) operation, which involves inserting secret data into the cover image's pixels' least significant bit. However, the amount of secret data that can be concealed in the cover image depends on the number of bits used for embedding. In this paper, a novel hybrid steganographic system based on Discrete Wavelet Transform (DWT) and Least Significant Bit (LSB) for image steganography is proposed. The proposed scheme aims to optimize data security by utilizing LSB and DWT techniques to embed secret data into an image robustly and efficiently. The present paper focuses on evaluating the algorithm performance by comparing the encrypted image quality using metrics such as PSNR, RMSE, and SSIM. The experimental results showed that the suggested method outperforms the existing LSB-based in terms of security performance. These results indicated that the proposed method consistently outperforms the conventional LSB-based method across all bit depths tested, with an overall improvement of 14.12% in PSNR, 41.87% in RMSE, and 4.02% in SSIM over the traditional LSB. The proposed method enhanced the PSNR values, reduced the RMSE values, and increased the SSIM values for all bit depths tested, indicating higher image fidelity, less distortion, and better preservation of structural similarity of the original image.

تحسين أمان البيانات باستخدام مخطط إخفاء المعلومات الهجين المستند إلى LSB وDWT

سارة فائق عبدالله [1]، شاهر فليح نواف [2]

[1] قسم الهندسة الكهربائية/ كلية الهندسة / جامعة كركوك / كركوك - العراق.

[2] قسم الهندسة الكهربائية/ كلية الهندسة / جامعة تكريت / تكريت - العراق.

الخلاصة

واحدة من أشهر تقنيات الاختباء في الصورة هي عملية البت الأقل (LSB)، والتي تتضمن إدراج البيانات السرية في البت الأقل لبكسلات الصورة الأصلية. ومع ذلك، فإن كمية البيانات السرية التي يمكن إخفاؤها في الصورة الأصلية تعتمد على عدد البت المستخدمة للتضمين. في هذا البحث، يتم اقتراح نظام هجين جديد للإخفاء في الصورة بناءً على تحويل الرقمية الموجي (DWT) والبت الأقل (LSB). يهدف النظام المقترح إلى تحسين أمان البيانات عن طريق استخدام تقنيتي LSB وDWT لتضمين البيانات السرية في الصورة بطريقة قوية وفعالة. يركز البحث على تقييم أداء الخوارزمية من خلال مقارنة جودة الصور المشفرة باستخدام مقاييس مثل PSNR وRMSE وSSIM. تشير النتائج التجريبية إلى أن الطريقة المقترحة تفوقت على طرق LSB التقليدية من حيث أداء الأمان. تشير هذه النتائج إلى أن الطريقة المقترحة تفوقت على الطريقة التقليدية المعتمدة على LSB في جميع عمق البت المجربة، مع تحسين إجمالي يبلغ 14.12% في PSNR و41.87% في RMSE و4.02% في SSIM على الـ LSB التقليدية. تعزز الطريقة المقترحة قيم PSNR، وتقلل من قيم RMSE، وتزيد من قيم SSIM لجميع عمق البت المجربة، مما يشير إلى وجود مزيد من الدقة في الصورة، وأقل تشويه، وحفظ أفضل لتشابه الهيكل للصورة الأصلية.

الكلمات الدالة: التشفير، اخفاء البيانات، نسبة ذروة الإشارة إلى الضوضاء، RSME, تقنية اخفاء المعلومات.

1.INTRODUCTION

In the digital era, data security has become a crucial concern for individuals, businesses, and governments. As more sensitive information is exchanged and stored online, the risk of data breaches and cyber-attacks has increased exponentially. Various security measures, such as encryption and firewalls, have been developed to counter these threats. However, these measures may not always be enough, and additional security measures, such as steganography, are required to ensure data security. Steganography involves concealing sensitive information behind a seemingly innocent cover medium, such as image, audio, or video files. It is an effective method that may be utilized to safely send sensitive information without raising any red flags [1]. The LSB (Least Significant Bit) algorithm is a popular steganographic technique that involves replacing the least significant bit of pixel values in an image. However, this method may not be secure enough against advanced steganography techniques. Therefore, using a multi-bit approach can enhance the security of the hidden data [2, 3]. Images are the most straightforward way to cloak spread covering when isolated from everything else [4, 5]. Imperceptibility, security, and concealed information capacity are the three key qualities to evaluate any steganography system. Another fourth characteristic is that robustness is considered [6]. LSB (Least Significant Bit) is used in the real world for things like steganography. Almost all disciplines make extensive use of secure and covert communication. Benefits include the use of covert communications for both interior and outdoor security in the medical, military, media, and industrial sectors. Some real-life applications of LSB steganography are as follows [7]:

- It is possible to conceal confidential information using LSB steganography in otherwise harmless files. For covert communication, for instance, digital photos can be modified to include hidden information and distributed openly [8].
- Copyright information in multimedia applications is frequently identified using steganography [9]. In this case, watermarking is used when the cover media is more important than the concealed data. Since insecure communication could cause catastrophic data loss, authenticity, and security are essential in industrial and business communication [10, 11].
- In healthcare, sensitive, protected information is concealed in medical records and sent using DNA sequences, which will help stop releasing confidential information to unauthorized parties [12].
- Covert Operations: LSB steganography may be used in intelligence and military operations to exchange communications or send information secretly. Agents can interact covertly by inserting data into seemingly innocuous files. The fundamental problem with military and defense communication is security. A danger to open channels makes authorized communication even more crucial. These steganographic systems use various double-layer encryption techniques before embedding [1].
- Digital Forensics: LSB steganography may be used to uncover concealed data or collect evidence in digital forensics. Investigators

looking for clues in a criminal case may look at seemingly inconsequential parts of a file. Compared to other spatial domain methods, LSB (Least Significant Bit) steganography has the following benefits [8]:

1. LSB is simple and uncomplicated, making it simple to apply. This straightforward and effective information-hiding method includes substituting the secret message for the carrier data's least significant bits.
2. LSB steganography's embedding capability is strong compared to other spatial domain methods. Since there are several bits per pixel, LSB increases the capability for concealing information inside the carrier data by allowing more bits to be substituted.
3. When implemented correctly, LSB steganography has a minor influence on the carrier data's perceived quality. The modifications introduced by LSB are less likely to be seen by human observers since they only affect the least significant bits, which have less influence on the total pixel value.
4. Detection is simple, which is both a strength and a weakness of LSB steganography compared to more sophisticated methods. Since LSB alterations may be detected using various statistical analysis techniques, they are useful when revealing the existence of concealed information is more important than fully concealing it.

The Discrete Wavelet Transform (DWT) can be useful in steganographic applications and much more useful when combined with LSB steganography. By applying LSB just to frequency subbands, embedding capacity is increased. Spreading changes over numerous subbands makes detection more difficult, which is how DWT offers security. This synergy makes the system more resistant to compression assaults and increases its invisibility to statistical analysis and visual examination [13]. Combining the Least Significant Bit (LSB) algorithm with the Discrete Wavelet Transform (DWT) technique, the purpose of this study is to develop a method for achieving strong information security and data concealment. The suggested technique uses varied quantities of LSB bits to embed hidden messages at various depths in the Discrete Wavelet Transform (DWT) domain, increasing the capacity and robustness of steganography systems. While the Least Significant Bit (LSB) technique permits effective data embedding and lowers the danger of image distortion, the Discrete Wavelet Transform (DWT) approach increases security and adds complexity for possible attackers. The main objectives of this research paper are:

1. To investigate the effectiveness of a combination of LSB and frequency transform (DWT) for image steganography.
2. To compare the proposed method with other image steganography techniques that use only LSB in terms of efficiency and robustness through the calculation of PSNR, RMSE, and SSIM.

By addressing these objectives, this research paper aims to contribute to the development of effective steganography techniques for protecting sensitive information. The rest of the paper is set up as follows: In Section 2, steganography techniques are discussed regarding related works. The methods and materials used in the proposed algorithm are covered in Section 3. Section 4 presents implementation outcomes and discussion. Section 5 provides conclusions.

2. RELATED WORKS

Adnan G. and Faiza S. posed a study proposal. The least significant bit (LSB) technique and the discrete wavelet transform (DWT) stego scheme was described. The latter, DWT, employed a wavelet transform to transfer the image from the spatial domain to the frequency domain, whereas the former, LSB, modified the image's least significant bit, i.e., the eighth bit, to conceal a portion of the covert message [8]. Both spatial domain methods, such as Least Significant Bit (LSB) and Patch Work Algorithm, and frequency domain methods, such as Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), and Discrete Fourier Transform (DFT), were discussed in the paper which presented by Hilkiya J. and Bindhu K. To digitally watermark an image, the suggested approach combined the discrete cosine transform (DCT) and discrete wavelet transform (DWT)[14]. In this study, Taha [15] proposed a strategy for image steganography incorporating steganographic and cryptographic techniques. The proposed method used LSBs as indicators for encrypting data within the dual-tree structure of DT-CWT. To encrypt the secret message, the cover image was first divided into three-by-three non-overlapping blocks, and then the key was generated by selecting the center pixel (pc) of each block. The DT-CWT output key was then used to determine the commencing concealing pixel in each block and the direction of hiding (clockwise or counterclockwise) relative to the cover image. The proposed method was evaluated using a variety of metrics, such as the Peak Signal-to-Noise Ratio (PSNR), Mean Square Error (MSE), Correlation Factor (CF), and Structural Similarity Index Measure (SSIM)[15]. To conceal their message in a picture, Imam [13] in this study employ two different encryption algorithms: the Improved AES-128 (Advanced Encryption Standard)

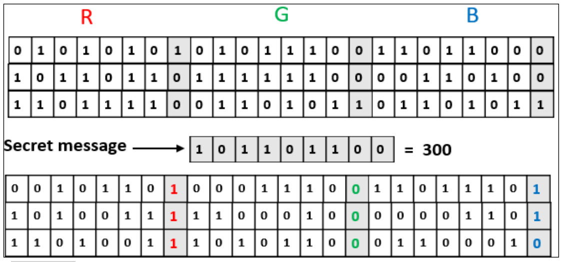
Algorithm and the LSB (Least Significant Bit) Algorithm. Messages can only be read on the original recipient's mobile by entering the right key, where the AES Algorithm Improvement was performed by adding a sending and receiving apps ID to adjust the Key Schedule procedure.

3. MATERIALS AND METHODS

The paper's proposed approach combines Discrete Wavelet Transform (DWT) image steganography with Least Significant Bit (LSB) embedding that will be covered next with the analytical performance metrics.

3.1.Steganography Based on LSB (Least Significant Bit):

The idea is to employ the (least significant bits) as inconsequential bits for information security. This LSB change is to conceal data from being seen by others [16]. In our case, a bare person's vision is sufficient. To be more precise, LSB-based algorithms keep the visual quality of the original image while altering the LSBs of pixels with bits from the secret message, which conceals the secret information encoded inside the cover picture. When text is embedded, the final bits of each pixel are updated, changing the color value each pixel represents by up to three values. Humans cannot see this distinction. The embedding procedure minimizes the color variance that results. Therefore, the cover image has undergone only tiny alterations that can only be seen and examined by inspection of the histograms concerning the stego and the cover images. The user must remove the least important sections. The amount of color variance brought on by the embedding procedure is kept to a minimum. Fig. 1 illustrates a straightforward example of how to conceal the number (300) in the first 8 bytes, requiring only a change to 5 bits of the encoded secret information [17, 18].



R								G								B							
0	1	0	1	0	1	0	1	0	1	0	1	1	1	0	0	1	1	0	1	1	0	0	0
1	0	1	1	0	1	1	0	1	1	1	1	1	1	0	0	0	0	1	1	0	1	0	0
1	1	0	1	1	1	1	0	0	1	1	0	1	0	1	1	0	1	1	0	1	0	1	1

Secret message →

1	0	1	1	0	1	1	0	0

= 300

0	0	1	0	1	1	0	1	0	0	0	1	1	1	0	0	1	1	0	1	1	1	0	1
1	0	1	0	0	1	1	1	1	1	0	0	0	1	0	0	0	0	0	0	1	1	0	1
1	1	0	1	0	0	1	1	1	0	1	0	1	1	0	0	0	1	1	0	0	0	1	0

Fig.1 Pixel Value Transitions that May Occur with LSB Substitution.

The fundamental idea behind LSB substitution is to embed sensitive information in the rightmost bits—those with the smallest weighting— to lessen how much the embedding operation affects the value of the original pixel. The LSB approach is mathematically represented as follows [18].

$$x_i' = x_i - x_i \text{ x } mod2^k + m_i \qquad (1)$$

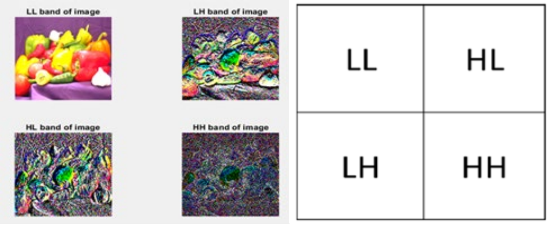
In Eq. (1), x_i' stands for the stego n-th pixel value, x_i for the cover _image, and m_i for the decimal value of the n-th block of secret data. The quantity of LSBs that must be substituted is denoted by the symbol k. The k-rightmost bits are copied immediately during the extraction procedure: The extracted message is represented mathematically in Eq. (2):

$$m_i = x_i' * mod2^k \qquad (2)$$

Therefore, the original secret data may be obtained by performing a straightforward permutation on the extracted m_i. This approach is simple and easy to follow.

3.2.Steganography Based on DWT (Discrete Wavelet Transform):

After Mallat suggested the multi-resolution representation of signals based on wavelet decomposition, the Discrete Wavelet Transform (DWT), developed by Daubechies and Mallat in the late 1980s, became a remarkably powerful signal processing tool. Since wavelets' energy is focused on time and still has wavelike (periodic) features, they really enable simultaneous time and frequency analysis of signals. The discrete wavelet transform (DWT) offers good picture coding performance. It is an extremely powerful tool for multi-resolution analysis in both the temporal and frequency domains. Using DWT, signals can be divided into numerous sub-bands with time and frequency information. This method allows more reliable coding efficiency and better image restoration quality than the traditional discrete cosine transformations [20]. Additionally, it offers a high compression ratio. Using the two-dimensional DWT [19], a one-level decomposition and reconstruction is demonstrated in Fig. 2.



(a) **(b)**

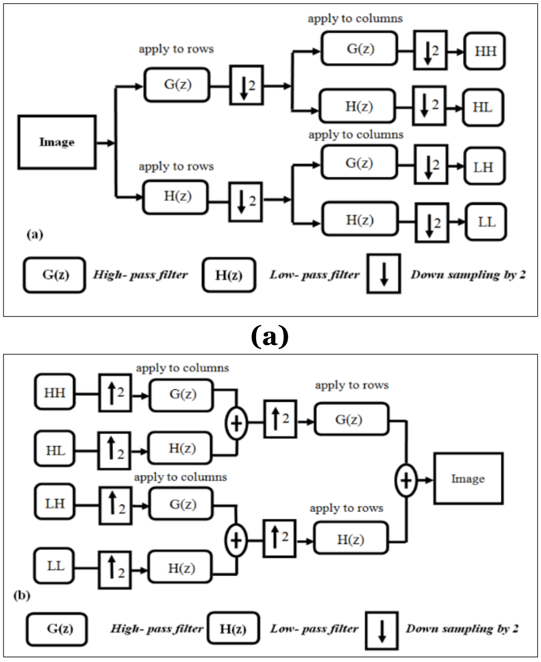
Fig. 2 DWT Pepper Image Decomposition (a) One level 2-D (b) Corresponding 'Wavelet' Sub-Bands of Pepper Image.

Fig. 3 shows how the LL, LH, HL, and HH sub-bands of the 2D-DWT level-1 decomposition can be used to dissect the original picture. The horizontal frequencies are indicated by LH, the vertical frequencies by HL, and the diagonal value by HH; the LL sub-band represents an image estimate. The signal is divided using high pass (H_P) and low pass (L_P) filters. LH and HL are the intermediate frequency sub-bands, and HH is the high frequency sub-band that gives the image unique information. The low-frequency sub-band, or LL, defines the approximate image. To lessen the impact of modifying the image's primary information or making a less obvious modification, the hidden message is embedded in the LL-sub band. The Discrete Wavelet Transform (DWT) for a signal x can be determined by subjecting it to separate low-pass and high-pass filters. The expressions are given in Eq. (3) and Eq. (4) [20]:

$$y_{\text{low}}[n] = (x * g)[n] = \sum_{k=-\infty}^{\infty} x[k] \cdot g[n-k] \qquad (3)$$

$$y_{\text{high}}[n] = (x * h)[n] = \sum_{k=-\infty}^{\infty} x[k] \cdot h[n-k] \qquad (4)$$

The approximate coefficients of the signal $y_{low}[n]$ can be obtained by convolution of the signal x with a low pass filter g. The detail coefficients of the signal$y_{high}[n]$ are produced by the convolution of the signal x with a high pass filter h. The term “quadrature mirror filter” refers to the relationship between these two filters. However, since half of the signal’s frequencies have been removed, half of the samples can now be discarded in accordance with Nyquist’s rule. The filter’s outputs will then undergo a factor (2) down sampling. This procedure involves twice transmitting the signal as a 1-dimensional signal for 2-dimensional signals, such as images. The image is filtered through low-pass and high-pass filters to obtain approximate and detailed sub-bands. Vertical, horizontal, and diagonal sub-bands comprise the detail sub-bands [19].



(a)

(b)

Fig.3 Two-Dimensional DWT One-Level Decomposition (a) The Decomposition Process (b) The Reconstruction Process.

3.3.The Proposed Algorithm

To keep a hidden message secure and maintain the visual quality of the cover image, a steganography scheme must meet certain criteria. When the capacity for message concealment is significantly increased, the image quality deteriorates noticeably, arousing suspicion that a stego-image is being employed. The Discrete Wavelet Transform (DWT) proved highly advantageous for identifying areas within a cover image that can effectively accommodate a secret message. This capability allows for leveraging the masking effect of the human visual system, ensuring that modifications to a DWT coefficient only impact the corresponding region. Since these sub-bands contain the majority of the image's energy, embedding data within them may cause some degradation in the image. However, they also offer greater resilience. Typically, these frequency sub-bands are preferred for steganography due to the human eye's reduced sensitivity to variations in frequency band boundaries. Combining the strengths of the Discrete Wavelet Transform (DWT) and the Least Significant Bit (LSB) technique, a more effective and robust strategy can be devised. Below are the procedures for the proposed algorithm:

1. Load the cover image: The first step in preparing to process (hiding the secret text within the cover image) is to determine the dimensions of the cover image (M×N) and the intensity of each pixel for each color channel (Red, Green, and Blue).
2. Load the secret message: The secret message is first decoded into its individual ASCII codes, and only then is the binary format applied. At this stage, the bitstream has been byte-shaped to obtain its LSB (least significant bit), and it may be inserted into the cover image in accordance with the n-bits (1-6) bits as required.
3. Discrete Wavelet Transform (DWT) of the cover- image: Obtain the frequency coefficient of the cover image by applying the Discrete Wavelet Transform (DWT) to each RGB channel of the original image. Divide the transformed image into four components: LL, LH, HL, and HH. Using the LL band to hide the secret text in each frequency coefficient of the cover image's pixels for each RGB color channel.
4. Secret text (hiding) Embedding: The message embedding process involves several steps. First, the binary message is reshaped into blocks of nth bits. Then, each pixel in the LL component of the transformed image obtained after applying the Discrete Wavelet Transform (DWT) to the original image is iterated.

For each pixel, the least significant bit (LSB) of its value is extracted. Subsequently, the LSB is replaced with bits 1 to 6 from the (message block), with the replacement depending on different cases. This procedure is repeated for the remaining bits in the message block. As the embedding continues, the pixel values are updated with the modified LSB values. Moving through each pixel in the LL component one by one, this embedding process is persisted until the entire message has been completely embedded into the image. Following this method, the secret message becomes seamlessly integrated into the image without significantly altering its overall appearance. This technique of LSB substitution within the LL component of the DWT-transformed image ensures that the hidden message is imperceptible to the human eye, making it suitable for secure and confidential communication purposes.

5. Image Reconstruction: In the image reconstruction process, the modified LL component was combined with the LH, HL, and HH components. Subsequently, the combined image underwent the inverse DWT transformation (IDWT). During this step, the effects of the Discrete Wavelet Transform were reversed to restore the original image from the wavelet components. The combined image was reconstructed using the IDWT technique, which retrieved the (stego image) with the embedded secret message. This method allowed for the seamless integration of the modified LL component with the other wavelet components, ensuring the accurate restoration of the cover- image while preserving the hidden information within the stego image.
6. The evaluation involved the calculation of the Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM) between the stego image and the original cover image. The Mean Squared Error (MSE) and Root Mean Squared Error (RMSE) were also calculated between the stego and the cover images. These metrics were used to assess the quality of the stego image compared to the original cover image, providing valuable insights into the effectiveness of the image-hiding technique employed during the message embedding process for different cases of using different bits in each case and comparing them.

The Flow Chart of the proposed Algorithm using a combination of LSB and DWT embedding is seen in Fig. 4.

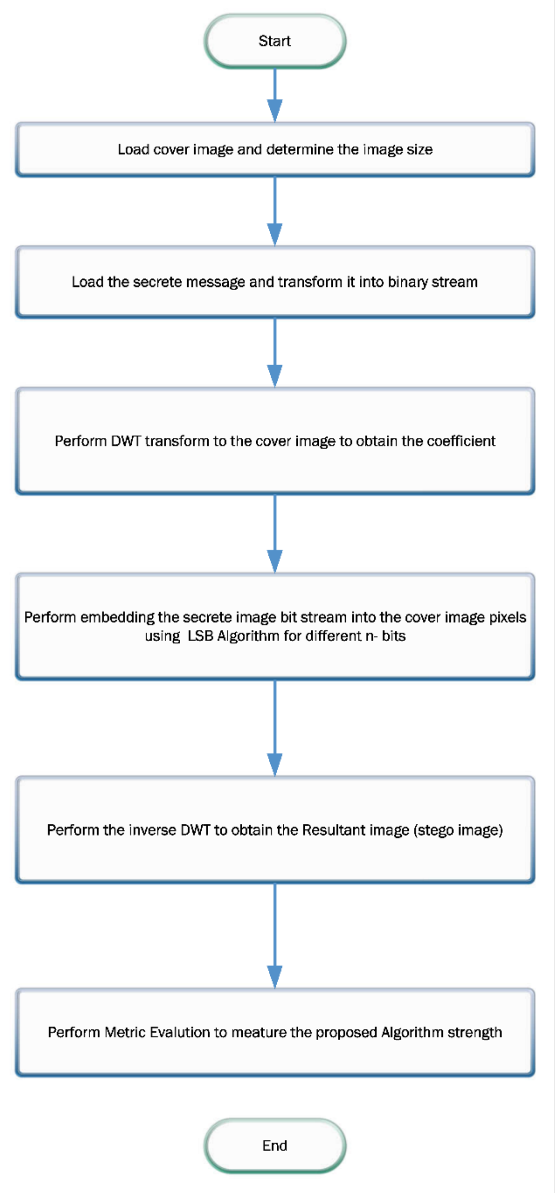

Start
Load cover image and determine the image size
Load the secrete message and transform it into binary stream
Perform DWT transform to the cover image to obtain the coefficient
Perform embedding the secrete image bit stream into the cover image pixels using LSB Algorithm for different n- bits
Perform the inverse DWT to obtain the Resultant image (stego image)
Perform Metric Evalution to meature the proposed Algorithm strength
End

Fig.4 The Proposed Algorithm Flow Chart.

3.4.Assessment Metrics

Three evaluation metrics were used in this work, i.e., the Root Mean Square Error (RMSE), Peak Signal to Noise Ratio (PSNR), and Structural similarity index measure(SSIM), to assess the effectiveness of the proposed steganography method [21-23]. PSNR and RMSE measure the pixel value differences between the cover image and the (stego) image, whereas SSIM measures the similarity of the images' structures. Better (stego) picture quality is indicated by greater PSNR or SSIM and lower RMSE values. The embedding process and evaluation metrics calculation for different n-bit LSB obtained a reliable estimate of the embedding capacity and visual distortion. The various measures employed are defined next.

3.4.1.Peak Signal-To-Noise Ratio (PSNR)

The pixel values change when the cover image is updated with the secret information. The changes must be considered because they directly affect the Stego output invisibly. The PSNR is a popular and high-quality statistic for assessing the quality of the Stego by comparing the mean squared error between the Cover and Stego images. PSNR is calculated using [21, 22]:

$$\mathbf{PSNR} = \mathbf{20\log 10}\left(\frac{\mathbf{255}}{\boldsymbol{MSE}}\right) \qquad \mathbf{(5)}$$

A higher PSNR indicates a more accurate reconstruction. The smaller the mean squared error (MSE), the higher the PSNR.

$$\mathbf{MSE} = \frac{\mathbf{1}}{\mathbf{MXN}}\sum_{m=0}^{m-1}\sum_{n=0}^{n-1}[(I - I')^2] \qquad \mathbf{(6)}$$

Where I is the original image, I' is the generated stego image, and M and N are the image's dimensions. Eq. (6) calculates the MSE between the two images. It is best to keep the MSE to a minimum. The carrier and the stego image are equivalent when the MSE equals 0. PSNR is quantified and displayed in decibels (dB). However, it has little relevance in comparing the restoration results on different photos. The PSNR is categorized in the following ways in various studies: 30 to 40 dB is OK, up to 40 dB is very good, and below 30 dB is unacceptable. Three bytes comprise a pixel in a color image, and each byte is represented by a pixel.

3.4.2 Root Mean Square Error (RMSE)

The RMSE (Root mean square error) is commonly used as a quality metric and may be calculated using Eq. (7) and Eq. (8) [21, 23]:

$$\mathbf{RMSE} = \sqrt{\boldsymbol{MSE}} \qquad \mathbf{(7)}$$

$$\mathbf{RMSE} = \sqrt{\frac{\mathbf{1}}{\mathbf{MXN}}\sum_{m=0}^{m-1}\sum_{n=0}^{n-1}[(I - I')^2]} \qquad \mathbf{(8)}$$

Where M and N are the image's dimensions, I is the created stego-image, and I' is the original image. It is best to keep the RMSE to a minimum. The carrier and the stego image are equivalent when the MSE equals 0.

3.4.3 Structural Similarity Index Measure (SSIM)

SSIM (Structural similarity index measure) is used to assess the similarity of two images. SSIM is determined using Eq. (9). Information is measured using the highly ordered nature of the natural landscape and the highly adaptable HVS "Human Visual System "perception. Image distortion is accurately estimated by the structural information shift between the carrier and stego images (SSIM); the computation looks like this [24]:

$$\mathbf{SSIM}(\boldsymbol{C},\boldsymbol{S}) = \frac{(2\mu_C\mu_S + c_1)(2\sigma_{C,S} + c_2)}{(\mu_C^2 + \mu_S^2 + c_1)(\sigma_C^2 + \sigma_S^2 + c_2)} \qquad \mathbf{(9)}$$

Where μ_C and μ_S refer to the mean intensity, and σ_C *and* σ_S indicate the original and stego frames variance, respectively. σ_C, s displays the covariance, and $c_1(= 0.01)$ and$c_2(= 0.03)$ are constants. The imperceptibility of the stego image has been demonstrated using the SSIM (Structural Similarity) Index as a quality metric [25].

4.ANALYSIS OF SIMULATION FINDINGS

This section discusses the experimental work and analyzes the findings. There are two key sections of the tests. First, a comparison between n-bits that have been varied for the conventional LSB. Second, a comparison of the proposed approach (n-bit LSB and DWT) for image steganography and the conventional LSB Algorithm. The tests were carried out on an Intel Core i7 using MATLAB R2020a. The tests were carried out on (512x512) pixel images.

4.1.Performance Evaluation for n-bit LSB

Comparing different bit planes of the LSB shows that as the number of bits used in embedding increased, the PSNR and SSIM decreased while the RMSE increased, indicating a loss in image quality, as seen in Table 1.

Table 1 Performance Comparisons between n-bit LSB Method.

n-bit LSB	PSNR	RMSE	SSIM
1-bit	51.1359	0.7075	0.9998
2-bit	44.1362	1.5839	0.9989
3-bit	37.8935	3.2498	0.9956
4-bit	31.7786	6.5706	0.9825
5-bit	25.7318	13.1811	0.9360
6-bit	19.8716	25.8797	0.8029

If the PSNR value exceeds 30 dB, it is typically difficult for simple human eyes to detect the visual quality aberration in a stego-image [8], which is the situation for all bits from (1-bit to 4-bit) embedding together. According to the high PSNR values, the image was correctly reconstructed, and there was very little influence of noise during the process, which can be confirmed using (1-bit to 4-bit) LSB. Fig.5 shows the PSNR performance.

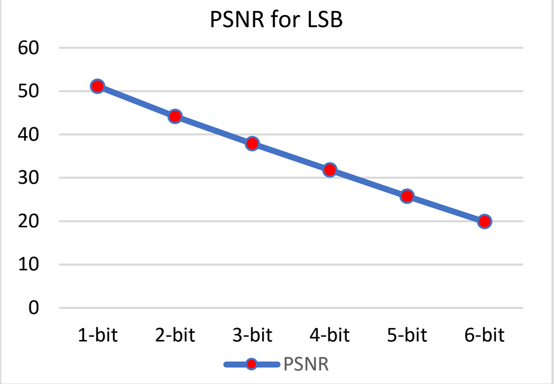


Fig.5 PSNR Comparison for LSB for Different bit Planes.

The RMSE (Root mean square error) values are also determined once the secret message is included in the cover picture. The approach yielded stego-images with a low error if the MSE value was small. For the 1-bit, the RMSE was at a minimum value of (0.7075), and as the embedding of multi-bit was used, the RMSE increased, indicating a loss in image quality. Fig.6 shows the RMSE performance.

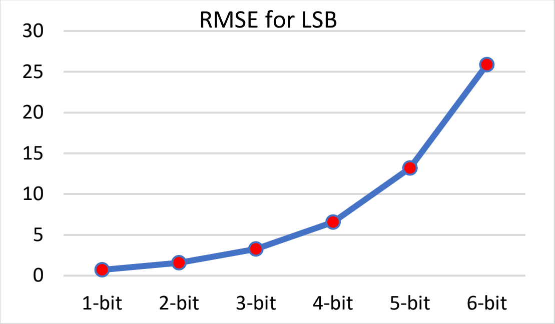


Fig.6 RMSE Comparison for LSB for Different bit Planes.

Finally, using SSIM (Structural similarity index measure), the degree of similarity between the actual cover image and the stego-images was determined. The SSIM measures the visual similarity between the original and the stego-image. The higher the SSIM, the more closely the images are connected. When the SSIM is 1, the compared images are identical in every way, so the more bits used to embed the secret message, the less SSIM. Fig.8 shows how well LSB preserved the original image's details. These results can help inform decisions on appropriate bit depths for image steganography applications.

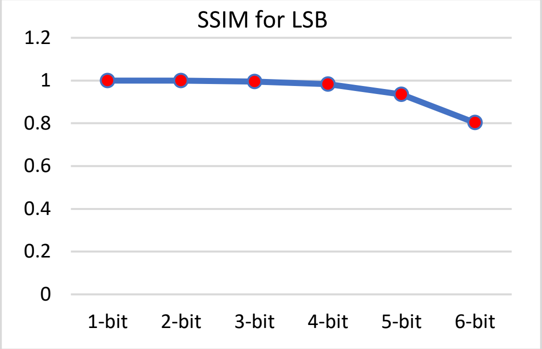


Fig.7 SSIM Comparison for LSB for Different bit Planes.

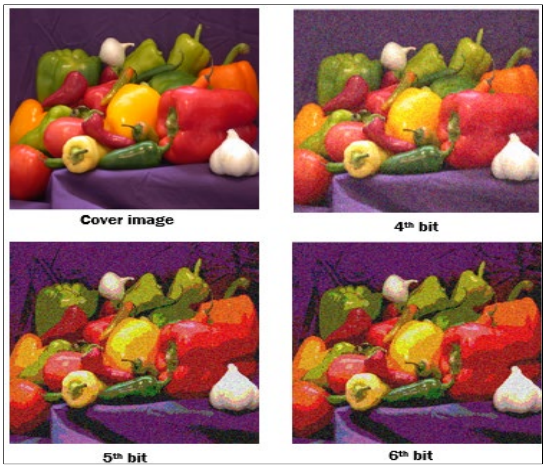


Fig.8 Comparison for LSB Stego Image for Different bit Planes.

4.2.Comparison of the Suggested Approach (n-bit LSB and DWT) for Image Steganography and LSB-based Steganography

Table 2 shows that the proposed method achieved significantly higher PSNR values and lower RMSE (Root mean square error) values than the conventional method for all bit depths tested. Specifically, for 1-bit LSB images, a PSNR of 54.1638 was observed for the proposed method compared to 51.1359 for the conventional method. Similarly, for 6-bit LSB images, it was found a PSNR of 23.2893 for our proposed method compared to 19.8716 for the conventional method. Comparing the proposed and the conventional LSB approaches, the PSNR value for the (LSB and DWT) demonstrates a more faithful restoration. This comparison indicates that the proposed approach returned a more accurate representation of the original picture, whereas LSB was impacted by noise during the process.

Table 2 Performance Comparisons between n-bit LSB and the Proposed Method for Different bit Planes.

n-bit LSB	**PSNR**		**RMSE**		**SSIM**	
	LSB	**Proposed**	**LSB**	**Proposed**	**LSB**	**Proposed**
1-bit	51.1359	54.1638	0.7075	0.4993	0.9998	0.9997
2-bit	44.1362	49.3992	1.5839	0.8641	0.9989	0.9997
3-bit	37.8935	43.7408	3.2498	1.6577	0.9956	0.9992
4-bit	31.7786	36.4425	6.5706	3.8407	0.9825	0.9973
5-bit	25.7318	29.6249	13.1811	8.4197	0.9360	0.9894
6-bit	19.8716	23.2893	25.8797	17.4612	0.8029	0.9598

A PSNR of less than 30 dB suggested that the alterations to the stego-image might be visible to the unaided eye [8], as shown in Fig.9. Following the concealment of the secret message within the cover image, the RMSE (Root mean square error) values were also calculated for the proposed method. Minimal MSE values indicated that the procedure generated stego-images with minimal variation or error. For the 1-bit, the RMSE was at a minimum value of 0.4993, and as the embedding of multi-bit was used, the RMSE increased, indicating a loss in image quality. Fig. 10 shows the RMSE performance. The proposed method also achieved higher SSIM values for all bit depths tested, indicating improved image quality. As shown in Fig.11, the SSIM for the proposed technique was consistent and near to (1), indicating less stego picture deterioration as bit plane utilization increased than with the LSB method. In contrast to the traditional LSB algorithm, the suggested technique exhibited encouraging results since the stego image started to degrade from the fifth bit and up, as seen in Fig. 12.

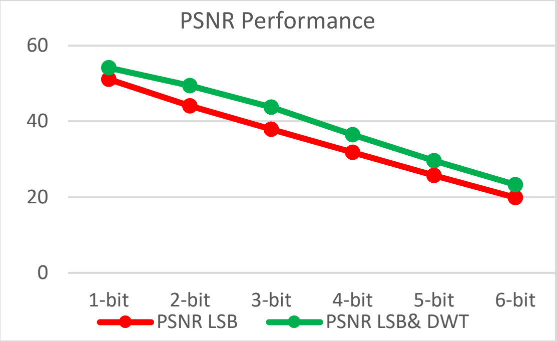


Fig.9 PSNR Comparison between the LSB and Proposed Methods for Different bit Planes.

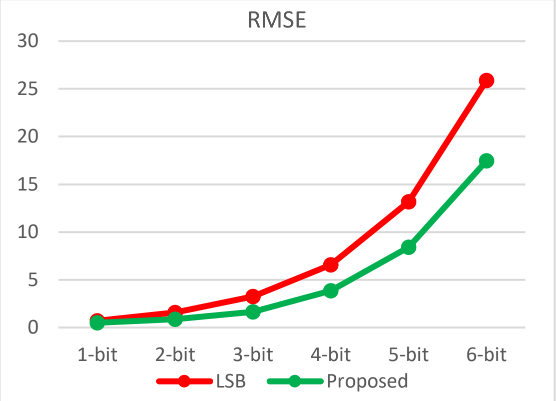


Fig.10 RMSE Comparison between the LSB and Proposed Methods for Different bit Planes.

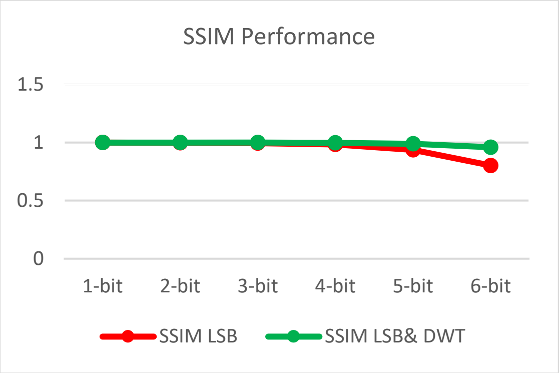
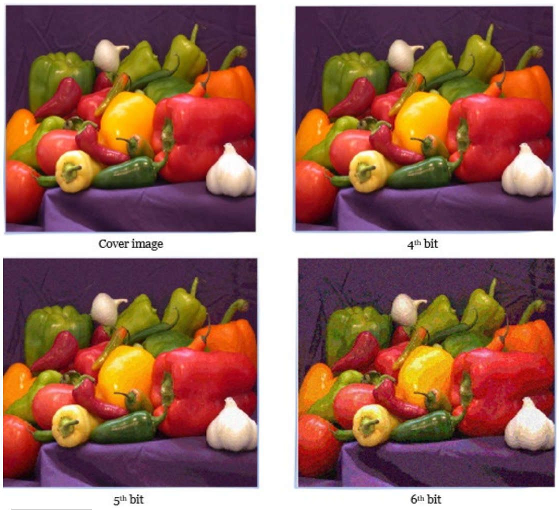


Fig.11 SSIM Comparison between the LSB and Proposed Methods for Different bit Planes.


Cover image

4th bit

5th bit

6th bit

Fig.12 Comparison for (LSB and DWT) Stego Image for Different bit Planes.

5. CONCLUSION

In the present study, steganography utilizing the LSB and DWT algorithms was described as a practical implementation. This study's objective was to compare and contrast the performance of the LSB method and the presented algorithms for concealing an n-bit secret message. The experimental results demonstrated that the proposed algorithm outperforms the LSB alone. Additionally, the results showed that the proposed algorithm outperforms the LSB algorithm in terms of PSNR, RMSE, and SSIM. These results indicated that the proposed method consistently outperformed the conventional LSB-based method across all bit depths tested, with an overall improvement of 14.12% in PSNR, 41.87% in RMSE, and 4.02% in SSIM. The proposed method enhanced the PSNR values, reduced the RMSE values, and increased the SSIM values for all bit depths tested, indicating higher image fidelity, less distortion, and better preservation of structural similarity of the original image. These findings can inform the development of more effective and efficient LSB, DWT-based steganography methods for hiding secret information within digital images while prioritizing image quality. Overall, the study presents a promising approach for enhancing the security and quality of LSB-based steganography methods. As a future work, the paper suggests changing the mechanism of embedding secret images and adding a layer of encryption to enhance security.

REFERENCES

[1] Gulati S, Bashir A, Mir AH. **Comparative Study of LSB and DWT Based Steganography Combined with Arnold Transformation for Image Security**. *Journal of Information System Security* 2022;**18**(1):63-80.

[2] Kadhim IJ, Premaratne P, Vial PJ, Halloran B. **Comprehensive Survey of Image Steganography: Techniques, Evaluations, and Trends in Future Research**. *Neurocomputing* 2019; **335** :299-326.

[3] Douglas M, Bailey K, Leeney M, Curran K. **An Overview of Steganography Techniques Applied to the Protection of Biometric Data**. *Multimedia Tools and Applications* 2018; 77(13):17333-17373.

[4] Rajendran S, Doraipandian M. **Chaotic Map Based Random Image Steganography Using LSB Technique**. *International Journal of Network Security* 2017;**19**(4):593-598.

[5] Hussain M, Wahab AWA, Idris YIB, Ho AT, Jung K-H. **Image Steganography in Spatial Domain: A Survey**. *Signal*

Processing: Image Communication 2018; **65**:46-66.

[6] Hameed AS. **High Capacity Audio Steganography Based on Contourlet Transform**. *Tikrit Journal of Engineering Sciences* 2018;**25**(1):1-7.

[7] Kini NG, Kini VG, Gautam. **A Secured Steganography Algorithm for Hiding an Image in an Image**. *Integrated Intelligent Computing, Communication and Security* 2019; **771** :539-546.

[8] Gutub A, Al-Shaarani F. **Efficient Implementation of Multi-Image Secret Hiding Based on LSB and DWT Steganography Comparisons.** *Arabian Journal for Science and Engineering* 2020;**45**(4):2631-2644.

[9] Alotaibi M, Al-hendi D, Alroithy B, AlGhamdi M, Gutub A. **Secure Mobile Computing Authentication Utilizing Hash, Cryptography and Steganography Combination**. *Journal of Information Security and Cybercrimes Research* 2019;**2**(1):73-82.

[10] Astuti YP, Rachmawanto EH, Sari CA. **Simple and Secure Image Steganography Using LSB and Triple XOR Operation on MSB**. *2018 International Conference on Information and Communications Technology (ICOIACT): IEEE*; 2018. pp. 191-195.

[11] Islam MR, Tanni T, Parvin S, Sultana M, Siddiqa A. **A Modified LSB Image Steganography Method Using Filtering Algorithm and Stream of Password**. *Information Security Journal: A Global Perspective* 2021; **30**(6):359-370.

[12] Salih AM, Mahmood AF. **Design and Implementation of Gray Scale JPEG CODEC on Spartan-3E**. *Tikrit Journal of Engineering Sciences* 2017;**24**(3):18-25.

[13] Pujiono IP, Rachmawanto EH, Nugroho DA. **The Implementation of Improved Advanced Encryption Standard and Least Significant Bit for Securing Messages in Images**. *Journal of Applied Intelligent System* 2023;**8**(1):69-80.

[14] Joseph H, Rajan BK. **Image Security Enhancement Using DCT & DWT Watermarking Technique**. *2020 International Conference on Communication and Signal Processing (ICCSP): IEEE*; 2020. pp. 0940-0945.

[15] Taha NA, Qasim Z, Al-Saffar A, Abdullatif AA. **Steganography Using Dual Tree Complex Wavelet Transform with LSB Indicator Technique**. *Periodicals of Engineering and Natural Sciences* 2021;**9**(2):1106-1114.

[16] Wang J, Cheng M, Wu P, Chen B. **A Survey on Digital Image Steganography**. *Journal of Information Hiding and Privacy Protection* 2019; **1**(2):87-93.

[17] Singh A, Singh H. **An Improved LSB Based Image Steganography Technique for RGB Images.** *2015 IEEE International Conference on electrical, computer and communication technologies (ICECCT): IEEE*; 2015. pp. 1-4.

[18] Al-Shaarani F, Gutub A. **Securing Matrix Counting-Based Secret-Sharing Involving Crypto Steganography**. *Journal of King Saud University-Computer and Information Sciences* 2022;**34**(9):6909-6924.

[19] Mistry D, Banerjee A. **Discrete Wavelet Transform Using Matlab**. *International Journal of Computer Engineering & Technology (IJCET)* 2013;**4**(2):252-259.

[20] Fadhil AF. **Formulation of Detection Strategies in Images**: Southern Illinois University at Carbondale; 2014.

[21] Hashim MM, Rahim MSM, Johi FA, Taha MS, Hamad HS. **Performance Evaluation Measurement of Image Steganography Techniques with Analysis of LSB Based on Variation Image Formats**. *International Journal of Engineering & Technology* 2018; **7**(4) :3505-3514.

[22] Wang Z, Bovik AC, Sheikh HR, Simoncelli EP. **Image Quality Assessment: From Error Visibility to Structural Similarity**. *IEEE Transactions on Image Processing* 2004;**13**(4):600-612.

[23] Hodson TO. **Root-Mean-Square Error (RMSE) or Mean Absolute Error (MAE): When to Use Them or Not**. *Geoscientific Model Development* 2022; **15**(14):5481-5487.

[24] Dalal M, Juneja M. **Evaluation of Orthogonal and Biorthogonal Wavelets for Video Steganography**. *Information Security Journal: A Global Perspective* 2020;**29**(1):40-50.

[25] Bakurov I, Buzzelli M, Schettini R, Castelli M, Vanneschi L. **Structural Similarity Index (SSIM) Revisited: A Data-Driven Approach**. *Expert Systems with Applications* 2022; **189**:116087.