https://doi.org/10.26682/sjuod.2023.26.2.51

Journal of University of Duhok., Vol. 26, No.2 (Pure and Engineering Sciences), Pp 565 - 577, 2023 (Special Issue)

SECURE IMAGE STEGANOGRAPHY USING GHM: HIDING TEXT IN PLAIN SIGHT

SARAH FAEQ ABDULLAH and SHAHIR FLEYEH NAWAF
College of Engineering, University of Tikrit- Iraq

(Accepted for Publication: November 27, 2023)

ABSTRACT

Steganography is a method for concealing confidential information in digital images in a way that is imperceptible to humans. However, existing steganographic techniques are frequently vulnerable to assaults such as steganalysis, which can detect the presence of hidden data. The purpose of this work is to develop a method for securely embedding text data within images while minimizing the visual impact on the carrier image. This research paper introduces an efficient method for image steganography by leveraging the GHM GHM(Geronimo-Hardin-Massopust) multiwavelet transform and n-bit Least Significant Bit (LSB) techniques. The proposed algorithm consists of three stages and for six different cases according to the altering of n- bits of the Least Significant Bit (LSB) embedding algorithm. Quality and safety of the stego-images were evaluated by experimental evaluations using metrics like Peak signal-to-noise ratio(PSNR), Root Mean Square Error (RMSE), and Structural Similarity Index Measure(SSIM). The results consistently demonstrated advantages of the suggested algorithm in terms of Peak signal-to-noise ratio(PSNR) about 24% improvement over the Least Significant Bit (LSB) techniques and 17% improvement over the the DWT (Discrete Wavelet Transform),also in terms of the Root Mean Square Error (RMSE), about 78% improvement over the Least Significant Bit (LSB) techniques and 67% improvement over the the DWT (Discrete Wavelet Transform) in average. The proposed approach significantly enhanced image quality while maintaining a high level of resemblance to the original image, showcasing its efficacy in preserving the underlying structure of the cover image.

KEYWORDS: *Discrete wavelet transforms; Hiding Information; Least Significant Bit; GHM (Geronimo, Hardian,and Massopust) multiwavelet; Peak signal-to-noise ratio.*

1. INTRODUCTION

In ancient Greece, efforts to convey a message through the approved media consisted of driving it through hostile territory. Numerous techniques are employed to conceal information on any medium in modern digital communication and sophisticated exchanges. One of these strategies is the use of images to conceal data; data such as text, advanced images, video, or audio files can be used to transmit secret messages. The term " Steganography " is derived from two Greek words: "word" and "graphs," both of which mean "writing" and frequently refer to "secret writing" or "data hiding"(Rathika & Gayathri, 2023; Rustad et al., 2022). The anonymity of intelligence and military personnel who are subject to censorship is protected by steganography. The significance of steganography is to transmit sensitive information by concealing it within harmless conceal objects, such as digital images, audio, and video, so a third party cannot discover it. To accomplish this, you must meet the four

sara.f.abdullah44345@st.tu.edu.iq
shahir735@gmail.com

fundamental steganographic requirements: (The amount of information that can be hidden in a cover medium), security (how easy it is for an adversary to uncover the hidden information), imperceptibility (how difficult it is for an adversary to perceive the hidden information), and robustness (how many changes to the medium can occur without destroying the message). Digital images are susceptible to assaults such as tampering, duplication, and unauthorized distribution, which can compromise their authenticity and integrity. The cover object is referred to as a stego-object following the embedding procedure. If a sufficient amount of change occurs during the embedding procedure in the cover medium, embedded data may become visible (Rajendran & Doraipandian, 2017). To satisfy the requirement for robustness, the transform domain is frequently used as the principal embedding method. It has been determined that transform embedding methods are superior to spatial domain methods because they have the potential for greater embedding capacity and increased robustness. The transform, the rapid Fourier transform, the wavelet transforms, and the multiwavelet transform are examples of frequently employed transform domains (Awadh et al., 2022; Gulati et al., 2022). The image as a whole, or only selected areas, can undergo the change. Modifying coefficients selected based on the desired level of security constitutes the embedding process. If the message is needed to be incomprehensible, the high frequency is chosen, but if it needed to be robust, the low frequency spectrum range is chosen (Joseph & Rajan, 2020).

(Ren et al., 2022),Proposed a digital image Algorithm for Disguising Multi-Carrier Data to address single-carrier algorithm restrictions. The algorithm uses GHM(Geronimo-Hardin-Massopust) multiwavelet transform and selects information hiding areas based on energy characteristics. To improve camouflage and resistance to analysis, secret information is embedded with only minor adjustments to the carrier picture. In the face of intense composite assaults, the algorithm's resilience climbs to 39.3274dB while its invisibility PSNR value rises by 27.05% and 9.46%, respectively.(Ren et al., 2020) ,Proposed a new compression sensing-based algorithm is proposed to address security issues in secret information preprocessing and improve the capacity and robustness of single-carrier image information hiding algorithms. The algorithm uses angle structure descriptor feature vectors, GHM(Geronimo-Hardin-Massopust) multiwavelet transform, compressed sensing, and segmented secret information classification in order to streamline many carriers and raise embedding standards. Experimental results show that the algorithm significantly improves invisibility and robustness compared to image sharing and single-carrier information hiding algorithms. It is well suited for big volume secret communication and high-security applications due to its robust anti-analysis capabilities and resistance to most image processing assaults.(Alwan, 2014), proposed hiding an image in the cover image. In the suggested technique, the cover picture goes through a multiwavelet transformation. The modified image's (Stego image's) high-frequency subbands are where the secret image's bit stream is hidden. Scaling variables and the frequency domain are crucial in determining image quality. LSB steganography has a low embedding capacity and a high detection risk since data is concealed in the least significant bits of pixels. While DWT(Discrete Wavelet Transform) steganography's use of wavelet transformation allows for more embedding capacity, it is possible that its complexity will make it vulnerable to assaults.Some of these restrictions can be bypassed by using multilevel wavelet-based steganography. The approach uses various wavelet decomposition levels to increase embedding capacity and improve attack resistance. Spreading the secret information out

across many frequency ranges does two things: it makes artifacts less noticeable and it makes detection less likely.

The purpose of this study is to create a safe method of image steganography that employs the multiwavelet transform of Geronimo-Hardin-Massopust (GHM) to conceal text. The aim is to overcome the limitations of current methods by leveraging the unique properties of GHM(Geronimo-Hardin-Massopust) multiwavelet transform and integrating them into the text hiding process.The concealed information is resilient against picture compression and other manipulations when using multilayer wavelet steganography. Using wavelets, the hidden information may be dispersed more evenly, making the steganographic method more robust and safe.

The GHM(Geronimo-Hardin-Massopust) multiwavelet transform has several advantages over conventional transforms such as the DWT (Discrete Wavelet Transform), including the ability to localize frequencies at a lower frequency. This characteristic makes the GHM(Geronimo-Hardin-Massopust) multiwavelet transform appropriate for securely and robustly embedding information in images. This paper will also provide a numerical analysis of the proposed method using peak signal-to-noise ratio (PSNR), structural similarity index (SSIM) and Root mean square error (RMSE) to be compared with other techniques to demonstrate its superiority over existing steganographic techniques.

The structure of this paper is as follows: Methods, mathematical foundation, and assessment metrics are discussed in Section 2 of this study. In Section 3, the suggested algorithm is laid out in detail. The results of the experiments are presented in Section 4. The report finishes with some recommendations for further study in Section 5.

2. METHOD AND MATERIALS

Implementing the LSB (Least Significant Bit) method and the GHM(Geronimo-Hardin-Massopust) multiwavelet transform domain, this paper proposes a novel method for embedding text in digital images. Next, we will discuss the methodology, the procedure, and the analytical performance metrics.

2.1. Steganography-Based on LSB (Least Significant Bit):

The concept of LSB (Least Significant Bit) is to use the least significant bits as insignificant bits for information security. This LSB (Least Significant Bit) modification is intended to prevent data from being viewed by others. In this situation, bare vision suffices. LSB-based algorithms preserve the appearance of the cover image while replacing the LSBs of pixels with bits from the secret message. This conceals the encoded confidential information contained within the cover image. When text is embedded, the concluding bits of each pixel are modified, resulting in a change of up to three colour values per pixel. This distinction is invisible to humans. The embedding process minimizes the resulting hue variation. Due to this, the cover image has only undergone minute changes, which can only be detected by comparing the cover image and the stego image's histograms(Abuali et al., 2019). The user must eliminate the sections with the least weight. The quantity of colour variation caused by the embedding procedure is minimized. The cover image has endured only minor changes as a result, and these changes can only be observed by comparing the cover image and the stego's histograms. To recover the concealed images, the user must remove the least significant bits from the modified pixels. To recover each image's bits independently, it is necessary to divide each image's bits. Using this method, it is possible to retain and transfer digital photographs in a covert and secure manner. Figure 1. depicts a straightforward illustration of how to conceal the

number 300 in the first eight bytes by modifying only five bits of the encoded confidential information(Al-Aidroos & Bahamish, 2019).

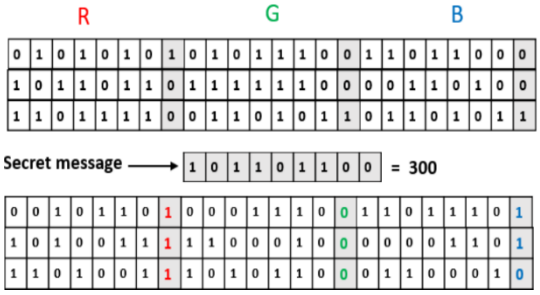

Fig.(1):-Pixel Value Changes That May Occur Due to LSB Substitution

The idea behind LSB(Least Significant Bit) substitution is to incorporate sensitive information in the rightmost bits, those with the smallest weighting, so that the embedding operation has less of an impact on the value of the original pixel. The LSB method is mathematically represented as follows(Mohamed et al., 2023):

$$x_i^{'} = x_i - x_i * \bmod 2^k + m_i \quad (1)$$

"x_i'" represents the stego n-th pixel value in Equation (1), "x_i" represents the original image, and "m_i" means the decimal value of the nth data to be hidden. k indicates the number of LSBs to be replaced. During extraction, the k-rightmost bits are copied immediately.

The extracted message is represented mathematically as Equation (2):

$$m_i = x_i^{'} * \bmod 2^k \quad (2)$$

Therefore, the original secret data can be obtained by conducting a simple permutation on the extracted m_i. This technique is simple and straightforward to implement.

2.2 Steganography-Based on DWT (Discrete wavelet transform)

A more efficient and reliable method may be developed by fusing the Discrete Wavelet Transform (DWT) with the Least Significant Bit (LSB) method .In the temporal and frequency domains, it is a potent instrument for multiresolution analysis. Time and frequency information are used in Discrete Wavelet Transform (DWT) to segment signals into several narrower bands. One level of breakdown and reconstruction is shown in Figure 2. using the two-dimensional DWT(Discrete wavelet transform)(Kunhoth et al., 2023).Figure 2. displays the components of the LL, LH, HL, and HH sub-bands produced by 2D-DWT. The LH sub-band represents an approximation of the image's horizontal frequencies; the HL sub-band represents an approximation of the vertical frequencies; and the HH sub-band represents an approximation of the diagonal value. High pass (H_P) and low pass (L_P) filters are used to separate the signal. Sub-bands HH adds distinctive details to the picture, whereas LH and HL are intermediate frequency sub-bands. The approximate picture is defined by the low frequency sub-band, often known as LL.In the LLsuband the embedding process can be done by using Least Significant Bit (LSB) to the frequency coefficient in this suband. To make sure that changes to a Discrete Wavelet Transform DWT(Discrete wavelet transform) coefficient only affect the associated region, this feature allows us to take use of the masking effect of the human visual system. Due to the high concentration of energy in these sub-bands,

picture quality may suffer if data is embedded there. On the other hand, they provide increased durability. Due to the human eye's decreased sensitivity to fluctuations in frequency band borders, these sub-bands are typically selected for steganography.

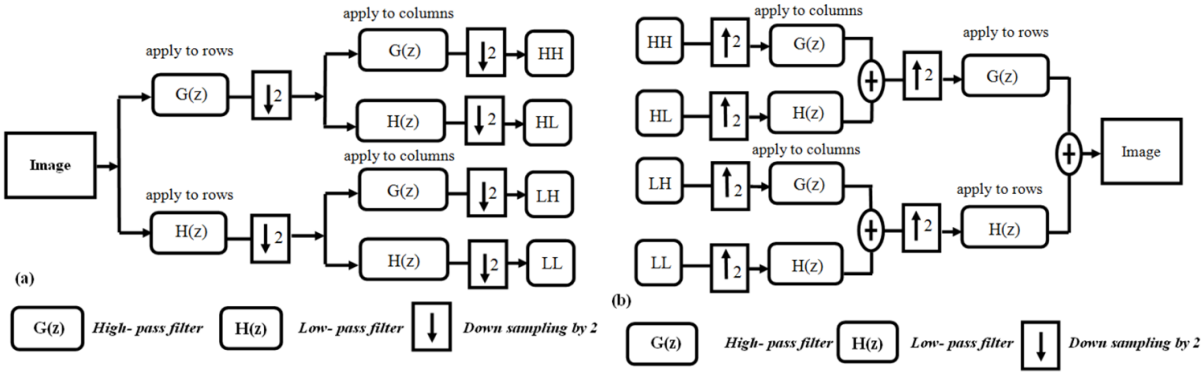

Fig.(5):- (a) Decomposition(b)Reconstruction of DWT transform

2.3 GHM(Geronimo-Hardin-Massopust) multiwavelet transform

Historically, Wavelets originated from the study of time-frequency signal analysis, wave propagation, and sampling theory. Introduction of wavelets for nonstationary signal analysis as many functions constructed by extension and translation of a mother wavelet(Hussein & Alhijaj, 2023).Multiwavelets have served as a wavelet generalization(Li et al., 2023),(Strela, 1996). Additional degrees of freedom are permitted, unlike in the scalar case,allowing the construction of functions with multiple desirable properties, such as, symmetry, transient support, orthogonality and vanishing moments(Deivalakshmi et al., 2019).

GHM(Geronimo-Hardin-Massopust) multiwavelet transform wavelet's function and scaling function are given by Equations (3) and (4). Equations (5),(6) provides the filter H_k and G_k , where k=2 is the number of scaling and wavelet functions (Agreste & Vocaturo, 2009):

$$\Phi(t)=\sqrt{2}\sum_{-\inf}^{\inf} H_k\Phi(2t-k) \tag{3}$$

$$\Psi(t)=\sqrt{2}\sum_{-\inf}^{\inf} G_k\Phi(2t-k) \tag{4}$$

$$H_k=\begin{pmatrix} h_1(2k) & h_1(2k+1) & h_1(2k+2) & h_1(2k+3) \\ h_2(2k) & h_2(2k+1) & h_2(2k+2) & h_2(2k+3) \end{pmatrix} \tag{5}$$

$$G_k=\begin{pmatrix} g_1(2k) & g_1(2k+1) & g_1(2k+2) & g_1(2k+3) \\ g_2(2k) & g_2(2k+1) & g_2(2k+2) & g_2(2k+3) \end{pmatrix} \tag{6}$$

In the multi wavelets scenario, a signal is represented using several scaling and wavelet functions. Similar to scalar wavelets, multi wavelet decomposition may be accomplished with filter banks, except in this instance the filter coefficients are matrices. Decomposition (a) and reconstruction (b) of a multiwavelet transform are shown in Figure 3.(Geronimo et al., 1994; Sun et al., 2014).

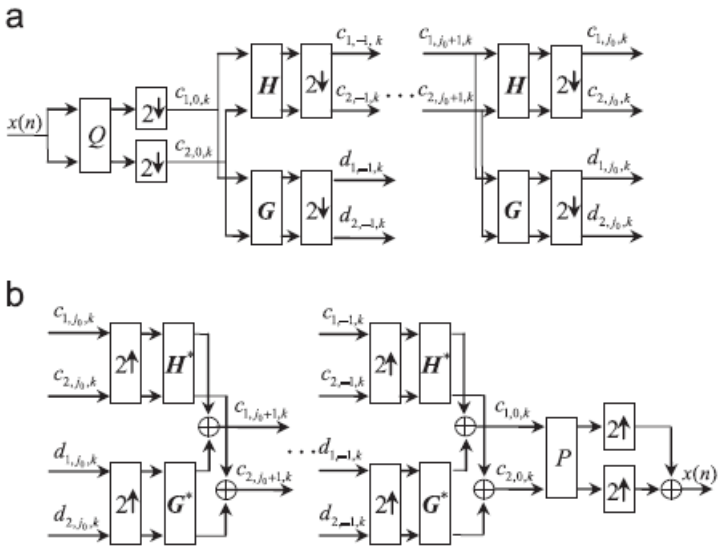

Fig.(3) (a) Decomposition(b)Reconstruction of GHM multiwavelet transform

2.3 Objective Measures of Error

This study employed three evaluation metrics to assess the efficacy of the proposed steganography technique: Root mean square error, peak signal-to-noise ratio, and structural similarity index Measure. RMSE (root mean square error)and PSNR(peak signal-to-noise ratio) measure the differences in pixel values between the cover and stego images, whereas SSIM(structural similarity index Measure) measures the structural similarity between the two. A higher PSNR(peak signal-to-noise ratio) or SSIM value as well as a lower RMSE value indicate a higher quality stego image. Embeddability and visual distortion are determined using the embedding procedure and evaluation metrics. Let's define the employed measures. PSNR(peak signal-to-noise ratio) is a well-known and reliable statistic that contrasts the mean squared error between the cover and stego images. The PSNR is computed as (Çataltaş & Tütüncü, 2017; Douglas et al., 2018):

$$PSNR = 20log_{10}(\frac{255}{MSE}) \quad (7)$$

The greater the PSNR(peak signal-to-noise ratio), the more accurate the reconstruction. The PSNR is greater when the MSE is lower

$$MSE = \frac{1}{M \times N}\sum_{m=0}^{m-1}\sum_{n=0}^{n-1}\left[(I - I')^2\right] \quad (8)$$

When (I) is the original image, (I') is the stego image, and (M), (N) are the dimensions of the image, The Mean Square Error (MSE) between the two images is calculated using Equation (8). The Mean Square Error(MSE) should be kept to a minimum. When the Mean Square Error (MSE) equals zero, the carrier and stego images are identical. Commonly used as a quality metric, the Root Mean Square Error (RMSE) can be calculated as follows Equation (9,10)(Maurya et al., 2023):

$$RMSE = \sqrt{MSE} \quad (9)$$

$$RMSE = \sqrt{\frac{1}{M \times N} \sum_{m=0}^{m-1} \sum_{n=0}^{n-1} \left[\left(I - I' \right)^2 \right]} \quad (10)$$

PSNR(peak signal-to-noise ratio) alone is insufficient to infer conclusions about image quality. The measure of structural similarity Measure(SSIM), which computes the average similarity between image regions. The computation appears as follows in Equation (11)(Zebari et al., 2020):

$$SSIM(C,S) = \frac{(2\mu_c\mu_s + c_1)(2\sigma_{c,s} + c_2)}{(\mu_c^2 + \mu_s^2 + c_1)(\sigma_c^2 + \sigma_s^2 + c_2)} \quad (11)$$

Here μ_C, μ_S refer to average intensity and $\sigma_{C,}\sigma_S$ is the difference between the cover and stego picture. σ_C, s represents covariance, while $c_{1=0.01}, c_2 = 0.03$, constants. Utilizing the SSIM(structural similarity index Measure) as a quality metric, the imperceptibility of the stego image can be demonstrated.

3. ALGORITHM PROPOSAL

To ensure both security and minimal visual degradation of the cover image, an effective steganography scheme must be employed. LSB(Least Significant Bit) substitution, a technique where sensitive information is embedded in the least significant bits of pixels, is commonly used. However, increasing the embedding capacity can lead to noticeable degradation of image quality, raising suspicion. The GHM(Geronimo-Hardin-Massopust) multiwavelet transform, specifically, is advantageous for effective embedding of secret messages in areas of the cover image. This takes advantage of the masking effect of the human visual system, modifying only the corresponding region when altering a GHM(Geronimo-Hardin-Massopust) multiwavelet transform's coefficients. While embedding in these low frequency sub-bands can degrade the image, they offer greater durability. Additionally, the frequency band boundaries within these sub-bands are less noticeable to the human eye, making them suitable for steganography. By combining the strengths of GHM(Geronimo-Hardin-Massopust) multiwavelet transform and LSB(Least Significant Bit), a more robust and efficient strategy can be devised, effectively utilizing their respective advantages in steganography.Below 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, 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.GHM(Geronimo-Hardin-Massopust) multiwavelet transform of the cover- image: Obtain the frequency coefficient of the cover image by applying the GHM(Geronimo-Hardin-Massopust) multiwavelet transform 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 GHM(Geronimo-Hardin-Massopust)
multiwavelet transform to the original image is iterated through. 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 process 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. By following this method, the secret message becomes seamlessly integrated into the image without significantly altering its overall appearance. This technique of Least Significant Bit (LSB) substitution within the LL component of GHM(Geronimo-Hardin-Massopust) multiwavelet transform of 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 Multiwavelet GHM (Geronimo-Hardin-Massopust) transform. During this step, the effects of the GHM(Geronimo-Hardin-Massopust) multiwavelet transform were reversed to restore the stego image from the wavelet components. The combined image was reconstructed using the inverse Multiwavelet GHM (Geronimo-Hardin-Massopust) transform, resulting in the retrieval of 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 stego- image while preserving the hidden information within it.

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 distance between the stego picture and the cover image was also measured using Mean Squared Error (MSE) and Root Mean Squared Error (RMSE). Insights into the efficacy of the picture concealment approach utilized during message embedding were gained by comparing the quality of the stego image to the original cover image using these measures. For different cases of using different bit in each case and perform comparison between them.

7. The procedure for extracting is the inverse of embedding. To recover the secret message, the user must first determine the correct order in which to extract the least significant bits from the modified pixels. Each image has to have its bits separated before it can be recovered separately. This method allows for the preservation and dependable transmission of digital images without raising suspicion among prying eyes.

Figure 4. Shows the flowchart of the proposed algorithm.

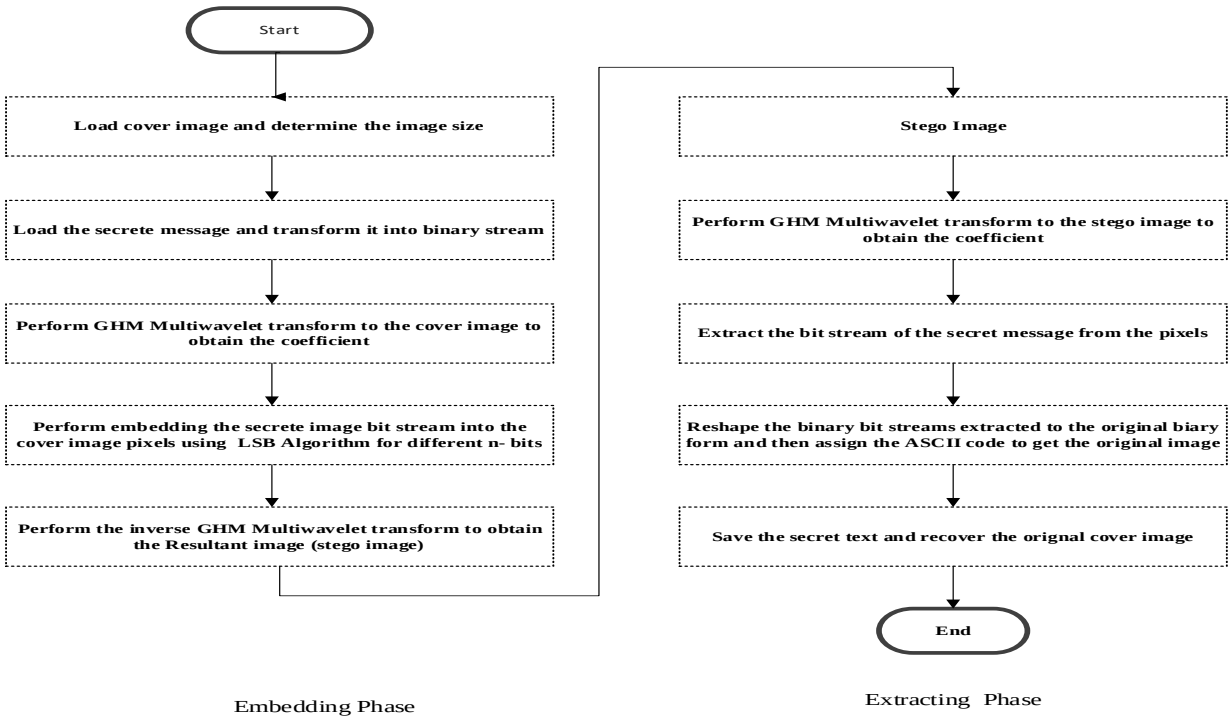

Fig.(4):- The Flow chart of the Proposed Algorithm .

4. FINDING AND ANALYSIS

This section describes the experimental work and analyses the resulting findings. The experiments were conducted on an Intel Core i7 using MATLAB R2020a. The images used in the experiments had dimensions of (512 by 512) pixels.

Three different methods of image steganography were compared to the proposed algorithm and contrasted: the conventional LSB(Least Significant Bit) approach, the Hybrid DWT (Discrete Wavelet Transform)-LSB(Least Significant Bit) approach, and the proposed method. The peak signal-to-noise ratio (PSNR), the root means square error (RMSE) and the measure of SSIM(structural similarity index Measure) was used for comparisons between various bit rates to demonstrate the Proposed Algorithm strength. Comparing distinct bit planes of the proposed algorithm reveals that as the, peak signal-to-noise ratio (PSNR), SSIM(structural similarity index Measure), increases the RMSE decreases, as shown in Table 1. In comparison to the conventional LSB(Least Significant Bit) approach and the Hybrid DWT (Discrete Wavelet Transform)-LSB(Least Significant Bit) approach, the PSNR(peak signal-to-noise ratio) value for the ((LSB(Least Significant Bit) and GHM(Geronimo-Hardin-Massopust) multiwavelet transform)) indicates a more accurate restoration. This demonstrates that the proposed method yielded a more accurate reproduction of the original image than other methods, which was affected by noise during the process. A PSNR(peak signal-to-noise ratio) of less than 30 dB indicates that the stego-image modifications may be visible to the naked eye(Gutub & Al-Shaarani, 2020).The proposed algorithm presents a value of (63.7898)dB Which is better than the other approaches.

sara.f.abdullah44345@st.tu.edu.iq
shahir735@gmail.com

Table (1):- The PSNR performance

n-bit LSB	PSNR(dB)		
	LSB	LSB& DWT	Proposed
1-bit	51.1359	54.1638	63.7898
2-bit	44.1362	49.3992	56.6092
3-bit	37.8935	43.7408	49.9911
4-bit	31.7786	36.4425	46.3105
5-bit	25.7318	29.6249	40.3639
6-bit	19.8716	23.2893	34.2221

Following the concealment of the secret message within the cover image, Root Mean Square Error (RMSE) values for the proposed method are also calculated. RMSE values that are minimal indicate that the procedure generated stego-images with minimal variation or error. For 1-bit, the Root Mean Square Error (RMSE) has a minimum value of (0.1648), and as multibit embedding is used, the RMSE increases, indicating a decrease in image quality. Table 2. illustrates Root Mean Square Error (RMSE) performance. The proposed hybrid scheme, which utilizes both LSB(Least Significant Bit) and GHM(Geronimo-Hardin-Massopust) multiwavelet transform techniques, achieves the lowest Root Mean Square Error (RMSE) values among all the tested methods. This indicates that the proposed method outperforms both the LSB(Least Significant Bit) and DWT (Discrete Wavelet Transform) schemes in terms of minimizing distortion and maintaining image fidelity.

Table (2):- The RMSE performance

n-bit LSB	RMSE		
	LSB	LSB& DWT	Proposed
1-bit	0.7075	0.4993	0.1648
2-bit	1.5839	0.8641	0.3768
3-bit	3.2498	1.6577	0.8072
4-bit	6.5706	3.8407	1.2331
5-bit	13.1811	8.4197	2.4454
6-bit	25.8797	17.4612	4.9595

Finally, the structural similarity index measure (SSIM) is applied to determine the degree of similarity between the genuine cover picture and the stego-images. The SSIM is a measure of the visual similarity between the original and the stego-image. When the structural similarity index measure (SSIM) value is high, there is a strong correlation between images. The SSIM(structural similarity index Measure)performance is displayed in Table 3. where it can be observed that the SSIM(structural similarity index Measure) for the proposed technique is constant (1) and near to (1), indicating less stego image deterioration than the other tested methods as bit plane utilization rises.

Table (3):- *The SSIM performance*

n-bit LSB	SSIM		
	LSB	LSB& DWT	Proposed
1-bit	0.9998	0.9997	1.0000
2-bit	0.9989	0.9997	0.9999
3-bit	0.9956	0.9992	0.9999
4-bit	0.9825	0.9973	0.9994
5-bit	0.9360	0.9894	0.9977
6-bit	0.8029	0.9598	0.9908

Figure 5. depicts the modified images (stego) for the various steganography used in this paper. The degradation is perceptible for higher embedding rates, but it is improved in the proposed algorithm, which demonstrates yet another positive result.

Fig.(5):- Different Stego Images for Various Bit Planes and Different Methods

4. CONCLUSION

Based on GHM(Geronimo-Hardin-Massopust) multiwavelet transform and n-bit LSB(Least Significant Bit) techniques, this study presents an efficient method for image steganography. The primary goal was to compare the performance of the proposed algorithm to that of conventional LSB(Least Significant Bit) and combined (Least Significant Bit) and (Discrete Wavelet Transform) methods. In terms of Peak signal-to-noise ratio(PSNR), Root Mean Square Error (RMSE), and Structural Similarity Index Measure (SSIM), experimental results demonstrated that the proposed algorithm outperforms both (Least Significant Bit) and (Discrete Wavelet Transform) techniques. The quality and security of stego-images were evaluated through exhaustive experimental evaluations employing metrics such as Peak

signal-to-noise ratio (PSNR), Root Mean Square Error (RMSE), and Structural Similarity Index Measure (SSIM). The results consistently demonstrated the superiority of the proposed algorithm in terms of Peak signal-to-noise ratio(PSNR) about 24% improvement over the Least Significant Bit techniques and 17% improvement over the the (Discrete Wavelet Transform),also in terms of the Root Mean Square Error (RMSE), about 78% improvement over the Least Significant Bit techniques and 67% improvement over the the (Discrete Wavelet Transform) in average. The proposed approach significantly enhanced image quality while maintaining a high level of resemblance to the original image, showcasing its efficacy in preserving the underlying structure of the cover image. The paper suggests investigating the use of encryption techniques in conjunction with GHM(Geronimo-Hardin-Massopust) multiwavelet transform -based steganography to further improve the algorithm's security in future research. Overall, the study offers valuable insights into the advancement of steganography techniques that prioritize image quality and security.Image steganography has several real-life practical applications, both in everyday scenarios and more specialized fields. Some of the practical applications of image steganography are:Confidential Communication ,Digital Watermarking, Covert Communication in Social Media ,Steganography in Journalism ,Digital Forensics ,Biomedical Applications and Military and Intelligence Communication.

REFERENCES

Abuali, M. S., Rashidi, C., Salih, M. H., Raof, R., & Hussein, S. S. (2019). Digital Image Steganography in Spatial Domain a Comprehensive Review. *Journal of Theoretical and Applied Information Technology*, *97*(19).

Agreste, S., & Vocaturo, A. (2009). Wavelet and multichannel wavelet based watermarking algorithms for digital color images. Communications to SIMAI Congress,

Al-Aidroos, N. M., & Bahamish, H. A. (2019). Image steganography based on LSB matching and image enlargement. 2019 First International Conference of Intelligent Computing and Engineering (ICOICE),

Alwan, I. M. (2014). Image steganography by using multiwavelet transform. *Baghdad Sci J*, *11*(2), 275-283.

Awadh, W. A., Alasady, A. S., & Hamoud, A. K. (2022). Hybrid information security system via combination of compression, cryptography, and image steganography. *International Journal of Electrical and Computer Engineering*, *12*(6), 6574.

Çataltaş, Ö., & Tütüncü, K. (2017). Comparison of LSB image steganography technique in different color spaces. 2017 international artificial intelligence and data processing symposium (IDAP),

Deivalakshmi, S., Palanisamy, P., & Gao, X. (2019). Balanced GHM Mutiwavelet Transform Based Contrast Enhancement Technique for Dark Images Using Dynamic Stochastic Resonance. *Intelligent Automation & Soft Computing*, *25*(3).

Douglas, M., Bailey, K., Leeney, M., & Curran, K. (2018). An overview of steganography techniques applied to the protection of biometric data. *Multimedia Tools and Applications*, *77*(13), 17333-17373.

Geronimo, J. S., Hardin, D. P., & Massopust, P. R. (1994). Fractal functions and wavelet expansions based on several scaling functions. *Journal of approximation theory*, *78*(3), 373-401.

Gulati, S., Bashir, A., & Mir, A. H. (2022). COMPARATIVE STUDY OF LSB AND DWT BASED STEGANOGRAPHY COMBINED WITH ARNOLD TRANSFORMATION FOR IMAGE SECURITY. *Journal of Information System Security*, *18*(1).

Gutub, A., & Al-Shaarani, F. (2020). Efficient implementation of multi-image secret hiding based on LSB and DWT steganography comparisons. *Arabian Journal for Science and Engineering*, *45*(4), 2631-2644.

Hussein, M. K., & Alhijaj, A. A. (2023). Protection of images by combination of vernam stream cipher, AES, and LSB steganography in a video clip. *Bulletin of Electrical Engineering and Informatics*, *12*(3), 1578-1585.

Joseph, H., & Rajan, B. K. (2020). Image security enhancement using DCT & DWT watermarking technique. 2020 International Conference on Communication and Signal Processing (ICCSP),

Kunhoth, J., Subramanian, N., Al-Maadeed, S., & Bouridane, A. (2023). Video steganography: recent advances and challenges. *Multimedia Tools and Applications*, 1-43.

Li, M., Ke, L., Wang, L., Deng, S., & Yu, X. (2023). A novel hybrid gene selection for tumor identification by combining multifilter integration and a recursive flower pollination search algorithm. *Knowledge-Based Systems*, *262*, 110250.

Maurya, S., Nandu, N., Patel, T., Reddy, V. D., Tiwari, S., & Morampudi, M. K. (2023). A discrete cosine transform-based intelligent image steganography scheme using quantum substitution box. *Quantum Information Processing*, *22*(5), 206.

Mohamed, M. H., Mofaddel, M. A., El-Naser, A., & Tarek, Y. (2023). Comparison Study Between Simple LSB and Optimal LSB Image Steganography. *Sohag Journal of Sciences*, *8*(1), 29-33.

Rajendran, S., & Doraipandian, M. (2017). Chaotic map based random image steganography using lsb technique. *Int. J. Netw. Secur.*, *19*(4), 593-598.

Rathika, S., & Gayathri, R. (2023). An ensemble of monarchy butterfly optimization based encryption techniques on image steganography for data hiding in thermal images. *Multimedia Tools and Applications*, 1-18.

Ren, S., Feng, Q., & Wang, M. (2022). Multi-Carrier Information Hiding Algorithm Based on GHM Multiwavelet Transform and Singular Value Decomposition. Proceedings of the 6th International Conference on Advances in Image Processing,

Ren, S., Zhang, T., Wang, M., & Shahzad, K. (2020). Identifiable tampering multi-carrier image information hiding algorithm based on compressed sensing. *IEEE Access*, *8*, 214992-215009.

Rustad, S., Syukur, A., & Andono, P. N. (2022). Inverted LSB image steganography using adaptive pattern to improve imperceptibility. *Journal of King Saud University-Computer and Information Sciences*, *34*(6), 3559-3568.

Strela, V. (1996). *Multiwavelets--theory and applications* Massachusetts Institute of Technology].

Sun, H., He, Z., Zi, Y., Yuan, J., Wang, X., Chen, J., & He, S. (2014). Multiwavelet transform and its applications in mechanical fault diagnosis–a review. *Mechanical Systems and Signal Processing*, *43*(1-2), 1-24.

Zebari, R., Abdulazeez, A., Zeebaree, D., Zebari, D., & Saeed, J. (2020). A comprehensive review of dimensionality reduction techniques for feature selection and feature extraction. *Journal of Applied Science and Technology Trends*, *1*(2), 56-70.