Hybrid of Least Significant Bits and most Significant Bits for Improving Security and Quality of Digital Image Steganography

ABUBAKAR AMINU MU'AZU, KAUTHAR KABIR*
Department of Computer Science, Umaru Musa Yaradua University,
Katsina-Nigeria, Dutsin-ma Road, P.M.B 2218,
NIGERIA

**Corresponding Author*

Abstract: - The Security of confidential communication is protected using the most popular type of carrier to hold information known as Image steganography. The Least Significant Bit (LSB) algorithm and the Most Significant Bit (MSB) algorithm are steganography algorithms used for information hiding in digital images both have disadvantages of Low image quality, Security, vulnerability to any small modifications, and long encoding time during message compression. To overcome this limitation, the research proposes a Secured Hybrid algorithm called S-Hybrid to combine (LSB and MSB) bits based on checking Two bits (the least significant bit and the most significant bit) of the cover images and replace them with a secret message which was implemented in Netbeans IDE. However, the S-Hybrid algorithm produced the best stego-image quality. Large cover images made the hybrid algorithm's quality better. The proposed S-Hybrid had a lesser encoding time than the existing method having the highest compression ratio which reduces the transmission effort making the encoding time short which is correlated to the security and makes the proposed method perform better than the existing one. Therefore, a trade-off exists between the encoding time and the quality of stego-image as demonstrated in this work. Mean-squared error (MSE), Peak signal-to-noise ratio (PSNR), encoding time, and Compression ratio are used for performance evaluation between the proposed S-Hybrid algorithm and the existing Method after embedding messages in digital images.

Key-Words: - Cover images, Least Significant Bit (LSB), Most Significant Bit (MSB), Steganography, Mean-squared error (MSE), Peak signal-to-noise ratio (PSNR), S-Hybrid algorithm.

Received: July 19, 2023. Revised: October 9, 2023. Accepted: November 14, 2023. Published: December 12, 2023.

1 Introduction

Steganography is the skill and science of hiding delicate info in means that prevent revealing. The purpose of steganography is to deliver a message in such a way that not one person apart from the sender and projected recipient suspects the presence of the message. These messages are transported through cover objects such as text, audio, images, and protocols. The top-secret message could be plaintext, cipher text, or images. The embedding of the message into a cover object results in a stego-image. The study, [1], reported that the Most significant bit (MSB) is the highest bit in a series of numbers in binary. e.g. in the binary number: 11001100, the most significant bit is far left 1. In the MSB technique, the secret message is embedded in the most significant bit of the pixel of the image.mages are typically used as shield objects in steganography, [2], [3].

The method of Image steganography is classified into two categories based on the working domain: Spatial domain where the pixel value is directly modified for data hiding. Images in this domain are represented as a rectangular grid of pixels or points of color where the human perception does not observe the image as a grid. LSB and MSB known as Least significant bit and Most significant bit respectively -based hiding strategies are most commonly used in this approach. Frequency domain where the Images that are in the domain of transform space are more robust in terms of some image processing manipulation and lossy compression and less prone to attacks Discrete cosine transform-based steganography and Discrete wavelet transform-based steganography are most commonly used in this approach.

Parameters such as imperceptibility, robustness, and capacity can be used to measure the performance of a steganography technique. Imperceptibility is the capacity to avoid

recognition, i.e. the failure to define the presence of a concealed message. This makes it a significant prerequisite in steganography. Robustness is how fine a steganography method can battle the withdrawal of hidden data. It measures the capability of the steganography method to persist in the efforts of removing the hidden information. Such challenges include image manipulation (like cropping or rotating), data compression, and image filtering. Payload Capacity signifies the extreme amount of information that can be securely embedded and retrieved in a work without being statistically noticeable. When likened to watermarking which requires embedding only a minor amount of right information, Steganography requires adequate embedding capability.

Least Significant Bit (LSB) Replacement is an embedding method based on the fact that the least significant bits in an image can be thought of as random noise, and consequently, they become not responsive to any change in the image. The secret message is hidden by altering the least significant bit in a certain layer of the image file. This change is so slight that the human eye may not notice it.

The Hybrid LSB - MSB algorithm is a combination of the aforementioned algorithms. It works by combining the two techniques, LSB and MSB into a hybrid algorithm that embeds the top-secret message bits into the least significant bit of and the most significant bit of the cover image. This work aims to Enhance the combination of LSB-MSB algorithms into a secured hybrid approach for digital image quality steganography.

The objectives of this research are:

1. To develop a secured hybrid algorithm for encoding secret message bits into the least significant bit and most significant bit of the cover image based on checking two bits LSB and MSB and replacing them with the secret message bits.
2. To implement the secured hybrid algorithm having an encoding interface and a decoding interface for hiding and retrieving purposes respectively.
3. To evaluate the performance of the proposed algorithm and compare it with existing Methods using different image formats and the quality of the image with an increase in file size.

The continuing part of the paper is structured as follows. Subdivision 2 works on current image steganography methods and subdivision 3 presents the projected image embedding method. In Subdivision 4 the experimental outcomes & conversation are shown and conclusions in Subdivision 5.

2 Related Works

The security of information during transmission in the open network is crucial. While sharing digital data on the internet, it is essential to observe information security goals: confidentiality, integrity, authenticity, and accuracy, [1]. The study, [2], highlights the Issues due to limitations in color variations and the use of a color map in steganography utilizing the LSB technique to embed data in the 8-bit color image using Secret Key implementation and successfully embed data in the 8-bit color image because during its implementation, after the process of compression, a text message is hidden in the final, compressed image. It eases up the exchange of information in different forms, be it text, image, audio, video, or other formats; however, it becomes a challenge to secure the data during transmission in the open network, [3].The study, [4], works on insecurity in the transmission of confidential information using an Arithmetic coding algorithm in MATLAB to increase imperceptibility in stereo image PSNR MSE SSIM and HISTOGRAM for evaluation, needs improvement in PSNR and latch mechanism for selecting hidden bits' similar secret bits in RGB image.This hidden information can be retrieved only through proper decoding techniques. Unfortunately, it lacks features of support for file types other than bit maps. Authors of, [5], use an approach of the STC framework to implement an Algorithm of cost assignment according to the characteristics of GIF images and payload allocation algorithm for different frames. Use the motion difference of adjacent frames as an adjacent factor as a performance measure metric and Point out that Security is the major concern in Steganography.The study [6], implemented a Modified LSB Technique using a cryptography approach and tested the performance of the work with MSE and PSNR solving the issue of secrecy of data and cyber-crimes. The study, [7], proposed data hiding with 1 bpp, 2 bpp,3 bpp, and Variable embedding capacity, using three approaches K-bit LSB replacement, LSB matching revised and XOR-based data hiding method, and testing the work using Image analysis and Histogram analysis. Finally highlighted that the Security problem still needs to be solved.

Solve problems associated with effective and robust image security using a framework

particularly designed for the images using a hybrid image security approach implemented in MATLAB, the proposed algorithm is designed to fill that certain gap of stronger security mechanism for image sharing-based social media applications. Elapsed time, MSE, PSNR, and Compression ratio were the metrics used and the system does not work on different types of datasets of images or other types of digital media, [8]. The study, [9], solved Information hiding capacity in steganography using Novel LSB with the strength of Using coding to increase steganographic capacity method and weakness of no idea for hiding messages with a large number of bits, MSE, PSNR, capacity, and SSIM are used for evaluation. The study, [10], addressed the problem of data and information hiding in digital images using the Bitmap Steganography technique under the implementation called Any file can be hidden in an image, can take any type of image file without converting it to bitmap and using maximum memory space to hide files in pictures. Just an attempt to identify steganography techniques, [11]. The difficulty with confidentiality in symmetric cryptography is that, as we all know, a secret key is used to both convert and decode the communication. As a result, this key must be interchanged by both communication parties in some way, or they must depend on a third organization, such as a key allocation center, to allocate the key. However, depending on a third organization jeopardizes the secret key's confidentiality. In public key cryptography, each user must produce a pair of keys, one of which is kept hidden and is known as a private key, while the other is made public and is known as a public key.

The study, [12], presented the problem of data hiding in LSB thus utilizing the MSB for check, using the method of checking MSB values and replacing bits from LSB with secret messages, which was implemented in C visual studio. The proposed approach gives a better evaluation value and is more secure so that a hacker cannot estimate the pixel location and how to embed data by using LSB and MSB bits. MSE, PSNR, Payload, and Histogram were used as evaluation metrics, the security is weak because the information is hidden in only LSB abandoning the MSB part, and the encoding time issue is not addressed at all.

3 Proposed an S-Hybrid Algorithm

The S-hybrid algorithm is a combination of the MSB and the LSB algorithms. It pulls on the very best features of the earlier examined algorithms. It works by combining the LSB and the MSB techniques into a secured hybrid algorithm that embeds the secret message bits into the least significant bit and the most significant bit of the cover image. The goal of this method is to preserve the statistical and visual features of the cover image and obtain a better stego-image that solves the security issues which include the application of certain operations like cropping, and resizing by an unknown party to detect the hidden message not intended for them, image quality and long encoding time issues associated with information hiding in digital images. In the proposed system the secret message is used to hide in a cover jpg or png image. Firstly, the Cover image is broken into minor parts, say 8x8 pixels, working from left to right, top to bottom, the DWT is applied to each block and each block is compressed through quantization. Each character of the secret message and each pixel of the cover jpg or png image are converted to binary values. The user has to input the stego-key as the password (the stego-key is used to embed the secret message in a cover file). After embedding the secret message into to cover image file, the resulting end is the stego-image, while defining the starting point of embedding in LSB and MSB to enhance the security, the summation of the ASCII value of each character of the stego-key is calculated and then the average of those characters value is computed, substituting the secret message into the LSB and MSB of the cover image. The first LSB and MSB positions are chosen according to the calculated average value of the input stereo-key characters, the substitution processing will continue until the end of the secret message.

An illustration of message embedding and extraction using the proposed algorithm

The proposed S-Hybrid algorithm embeds the secret text in LSB and MSB. It takes two bits of secret text and hides the first bit in LSB and the second bit in the MSB. The research considers an RGB 24 jpg and PNG image.

Data to be inserted: character 'A': 01000001

Pixels are used to store one character of 8 bits.
Embedding 'A'

Cover Image:
00100111 11101001 11001000
00100111 11001000 11101001
11001000 00100111 11101001
S-Hybrid: 00100111 **0**1101100 **0**1001000

00100111 11001000 11101001
11001000 00100111 11101001
Extracting 'A'=> 0100000

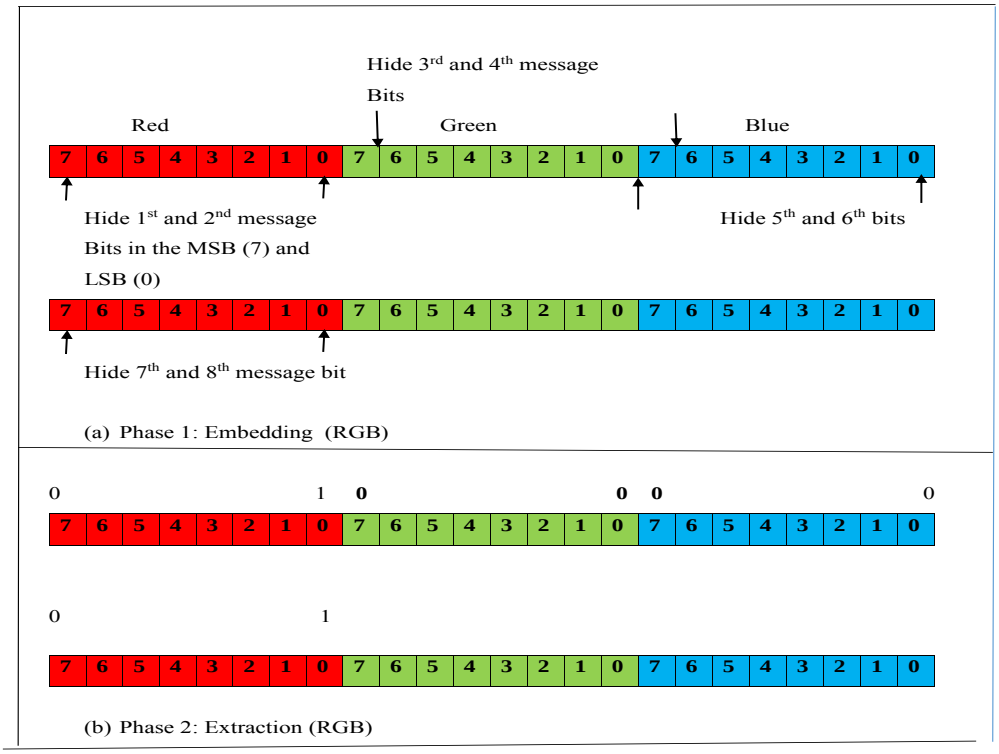

Fig. 1: LSB and MSB for embedding and extraction algorithm for three colors.

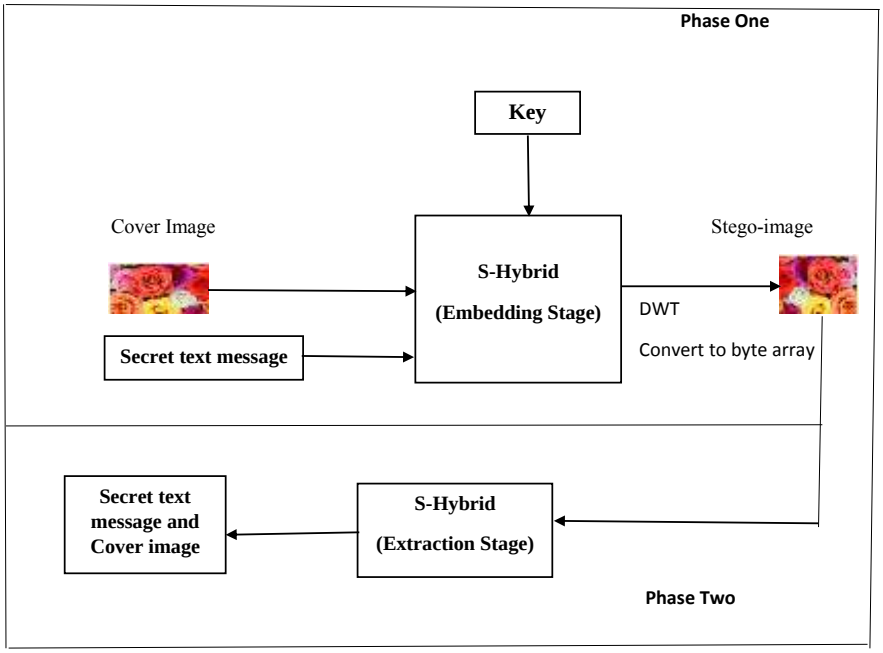

Fig. 2: Proposed Architectural Model

The Architectural Model designed for this research (Figure 2) is one of the key items of the research, From Figure 1, when the cover image and the secret text message have been carefully chosen, the embedding stage of the hybrid algorithm picks two bits of the secret message and embeds the first message bit in the least significant bit of the cover image byte and the second message bit in the most

significant bit of the cover image byte, the Key is the secret key utilized in the embedding stage increasing security. The retrieving stage is the opposite of the embedding stage.

3.1 Algorithm for the Proposed Secured Hybrid LSB-MSB

The Embedding algorithm is as follows;

Input: An M×N size cover image and message to be hidden.
Output: Stego image.
Step 1: Image img = get image
Step 2: Let n = width (img)
m = length (img)
Step 3: Let x be message to hide
Begin
Step 4: The image is broken into minor parts, say 8x8 pixels, working from left to right, top to bottom, the DWT is applied to each block and each block is compressed through quantization.
Step 5: Convert the cover image using the read() method of the image IO class into ByteArrayoutputstream
Step 6: Convert Message character text(x) string into Byte Array using string.getBytes()
Step 7: Accept the stegeo-key from the user and calculate their average value of them.
Step 8: Convert each character of the secret message and each LSB and MSB of the cover image from a position of an average of stegeo-key.
Step 9: If the image cannot contain the message exit with an error message
Else
for each bit in the message byte
Begin
Step 10: If using hybrid LSB-MSB (proposed algorithm), get two message(x) bits and hide the first message(x) bit in the MSB of the corresponding cover image byte and the second message(x) bit in the LSB of the corresponding cover image byte.
Step 11: End
End

The Extraction algorithm is as follows;

Input: Stego-image
Output: Cover image and message.
Step 1: Begin
Step 2: Input Stego-image
Step 3: Convert stego image using read() method of image IO class into ByteArrayoutputstream
Step 4: If the decoding type is LSB-MSB
Step 5: Begin
Step 6: for the first 32 bytes, copy the LSB and MSB into an array of 32
Step 7: Using the int attribute convert the array into an integer value
Step 8: Create an array of lengths of the integer value
Step 9: Starting from length 32+1 of the stego-image array
Step 10: Begin
Step 11: Copy the LSB and MSB of the equivalent stego array into an array of length 8.
Step 12: Convert the array into a byte value and save it in the corresponding index of the created array
Step 13: Convert the array value into a string or image
Step 14: Display msg and cover image
Step 15: End
End

3.2 Format of the File

Any image file design can be used equally as the cover image. However, the image was first transformed into PNG format before something could be done on it. After the entire procedure, the image was transformed back to its unique design. PNG format is chosen because it is sustained by the Java image IO library; it applies a lossless file density method and allows for easy exchange and observation of image data stored on local or isolated computer systems. Also, it appears to preserve a high point of image quality after the message has been embedded.

3.3 Performance Evaluation Metrics

Analyzing the image quality and security for proposed and existing work will be done using four parameters of analysis which include;

i. Mean-Squared Error
ii. Peak Signal-to-Noise ratio(PSNR)
iii. Encoding Time
iv. Compression Ratio

i. Mean Squared Error: This is defined to measure the distortion of the image which is the difference of error between the original and stego image. The less the Mean Squared Error, the better the image quality. To calculate the MSE between two images $I_1(M,N)$ and $I_2(M,N)$;

$$MSE = \sum \frac{[(I_1(M,N) - I_2(M,N))]2}{M * N} \quad (1)$$

Where M and N are the number of rows and columns in the input images respectively

ii. Peak Signal-to-Noise Ratio(PSNR): The Peak signal-to-noise ratio is used to compare the image compression quality of the original image and stego image. If PSNR is 40dB or greater, the original and reconstructed images are usually indistinguishable by human observers.

$$\text{PSNR} = 10\log_{10}\frac{(255)^2}{MSE} \quad (2)$$

Where the 255 here is the value as substituted for R

However, the lower the MSE value and the higher the PSNR value the better the quality of the image.

iii. Encoding time: Encoding time refers to the period it takes to embed a secret text message in an image. Processing image security mechanism had to be effective in terms of encoding time. If Time T is a variable and Data size D is another variable, then the rate of change of T with respect to D is given by

$$dT/dD. \quad (3)$$

iv. Compression ratio: represents the reduction in the size of the image after the compression process. The higher the compression ratio; the lower the transmission effort and disk space consumption.

Size of the original image
A = (Width * Height * Number of Color planes * bit depth)/8 bytes
B = Size of compression image = size_ in_bytes
Compression ratio = A: B

(4)

4 Simulated Results

A simple system was developed to implement the proposed Secured Hybrid LSB-MSB algorithm using JAVA programming language. There are two sides to the system, the embedding interface and the Extraction interface for hiding and extraction purposes respectively. We tested the system using two different images: rose.jpg, and giraffe.png as cover images. We have established that the encoding time is correlated to the security of the algorithm in question. A 30.4 kilo-byte document was also used as the message text.

To evaluate the performance of the proposed method, we use two images Rose.jpg and Giraffe.png for message embedding. Table 1 shows the results of the experiment using two jpeg and png images and their respective dimensions, file size, and the text size that had been added 'steganographically'.

I II

Fig. 3: (560 x 448 pixels rose.jpg):
(I) Original image (II) Stego-image using S-Hybrid

Using roses.jpg with dimensions 560 x 448 pixels as the cover image and a 30.4-kilo byte document as the message, it can be seen from image II of Figure 3 show noticeable differences when compared to the original cover image.

Increasing the dimension of roses.jpg to 5040 x 4032 pixels to improve the image quality of the proposed algorithm, the payload capacity increases for the proposed algorithm (Figure 3 (II)). Therefore, the larger the cover image the more data that can be stored.

I II

Fig. 4: (5040 x 4032 pixels rose.jpg):
(I) Original Image (II) Stego-image using S-hybrid

Figure 4 shows the 5040 x 4032 pixels rose.jpg hiding an image. Figure 5 shows the output of the newly created stego-images after hiding text with a file size of 30.4kb (31,160 bytes) in an image in

PNG format. The dimension of the cover image, giraffe.png is 750 x 1125 pixels. Figure 5 (II) showed a noticeable difference when compared to the original cover image after embedding text. The differences are noticeable in the top sections of Figure 5 (I) and (II).

I II

Fig. 5: (750 x 1125 pixels giraffe.png):
(I) Original image (II) Stego-image S-Hybrid

Increasing the dimension of the PNG file to 6750 x 10125 pixels for quality enhancement, produced a stego-image indistinguishable from the original cover image when viewed with the human eyes for the proposed algorithms (Figure 6 II).

I II

Fig. 6: (6750 x 10125 pixels giraffe.png hiding text): (I) Original Image (II) Stego-image using S-hybrid

Table 1 represents the Simulation results of PSNR and MSE for the proposed method by experimenting with Four images and different image formats and dimensions of the image and inserting a text message of 30.4 kilobytes.

Table 1. Simulation results of PSNR and MSE for an S-Hybrid

Cover Image	Size of the Image	PSNR	MSE
Rose.jpg	560 x 448	79.273	0.00010
Rose.jpg	5040 x 4032	80.256	0.00025
Giraffe.png	750 x 1125	81.390	0.00020
Giraffe.png	6770 x10125	50.31	0.061

- Here PSNR and MSE are calculated as follows:

$$\text{MSE} = \sum \frac{[(I_1(M,N) - I_2(M,N))]2}{M * N} \quad (5)$$

$$\text{PSNR} = \frac{10 \log_{10} (255)^2}{MSE} \quad (6)$$

Where the 255 here is the value as substituted for R

Table 2 represents the Simulation result of Encoding for the proposed method by experimenting with Four images and different image formats and the dimensions of the image and inserting a text message of 30.4 kilobytes.

Table 2. Simulation result of Encoding for an S-Hybrid

Cover Image	Size of the Image	Encoding Time(ms)
Rose.jpg	560 x 448	192
Rose.jpg	5040 x 4032	190
Giraffe.png	750 x 1125	198
Giraffe.png	6770 x10125	194

Here Encoding Time(ms) is calculated as follows:
If Time T is a variable and Data size D is another variable, then the rate of change of T with respect to D is given by:

$$dT/dD \quad (7)$$

Table 3 represents the Simulation result of the Compression ratio for the proposed method by experimenting with Four images and different image formats and dimensions of the image and inserting a text message of 30.4 kilobytes.

Table 3. Simulation result of the Compression ratio for an S-Hybrid

Cover Image	Size of the Image	Compression Ratio
Rose.jpg	560 x 448	38.96
Rose.jpg	5040 x 4032	43.43
Giraffe.png	750 x 1125	42.71
Giraffe.png	6770 x10125	43.46

Here Compression Ratio is calculated as follows:
Size of the original image
A = (Width * Height * Number of Color planes * bit depth)/8 bytes
B = Size of compression image = size_ in_bytes
Compression ratio = A: B (8)

Table 4. Values of MSEs, and PSNRs for the existing (Mahdi method) and S-hybrid (proposed) algorithm

S/N	Cover Image		Algorithm	Message Image (31,160 Bytes, 30.4KB)	
	Dimension	File Size		PSNR (db)	MSE (db)
1	Figure 3 560 x 448 pixels rose.jpg	96.3 KB	Proposed S-Hybrid	79.273	0.00010
			Mahdi method (Existing)	87.141	0.00012
	Figure 4 (5040 x 4032 pixels rose.jpg	2.14 MB	Proposed S-Hybrid	80.256	0.00025
			Mahdi method (Existing)	83.742	0.00027
2	Figure 5 (750 1125 pixels giraffe.png	1.2 MB	Proposed S-Hybrid	81.390	0.00020
			Mahdi method (Existing)	84.608	0.00022
	Figure 6 (6750 x 10125 pixels giraffe.png	37.0MB	Proposed S-Hybrid	89.23	0.0002
			Mahdi method (Existing)	87.35	0.0001

Table 4 shows the MSE and PSNR of the cover image text embedding. It can be seen that a lower MSE value and a higher PSNR value for the proposed S-Hybrid algorithms for text were obtained. This results in better image quality since the lower the MSE value and the higher the PSNR value, the better the quality of the image, and hence imperceptibility is improved. The last evaluation is a histogram showing the comparisons between the cover image and stego image using Rose.jpg and Giraffe.png of increasing dimensions as shown in Figure 7 which is the resulting stego image same as the histogram of the cover image.

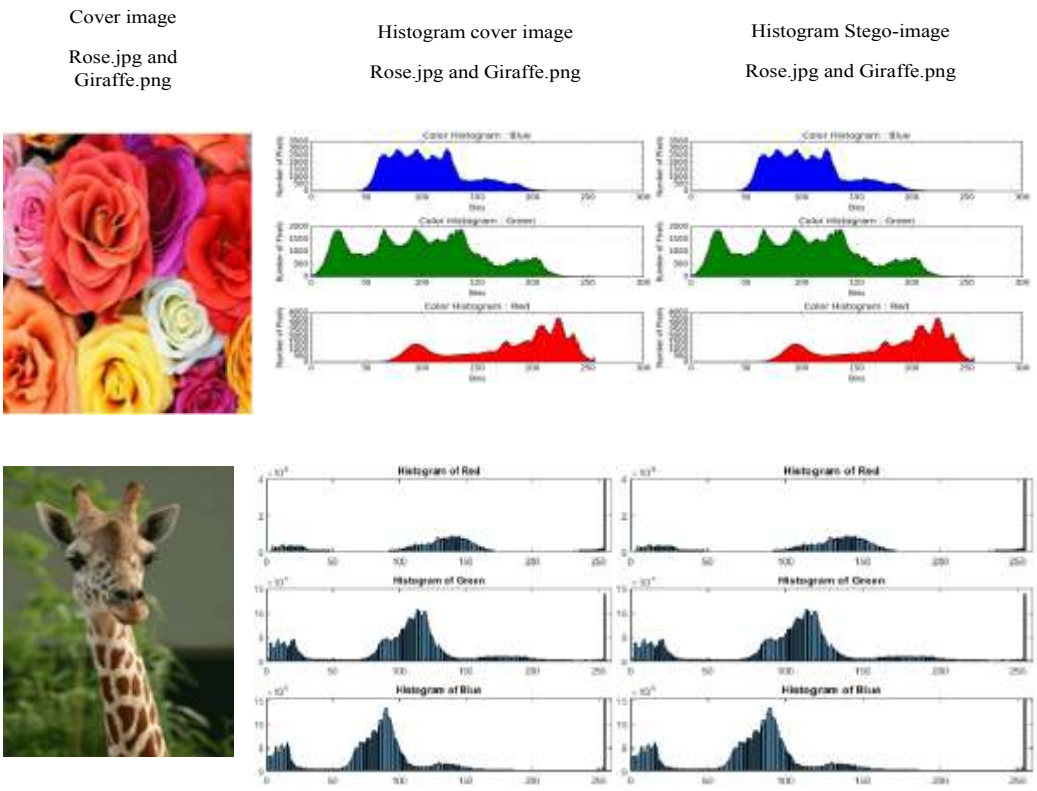

Fig. 7: Cover image and Stegeo image comparison Histogram

5 Conclusion and Future Work

The proposed method gives better performance in all the parameters than the existing one. The stego image generated after embedding the secret message in the cover image is almost identical to the original image. However, when the sizes of the cover images were increased, the image quality of the proposed algorithm increased, which means that the larger the cover image, the better the hiding capacity. Compression Ratio represents the reduction in the size of the image after the compression process. The higher the compression ratio; the lower the transmission effort and disk space consumption. In the case of the proposed algorithm, the compression is recorded way higher. The encoding times of the proposed Secured Hybrid algorithm for various sizes of the different images were lesser and the security is better because its complex coding is what makes the proposed algorithm better secured. The proposed scheme is developed to ensure more image security during transmission by facilitating quick image transfers. Also, the processing image security mechanism had to be effective in terms of encoding time. The results of the proposed algorithm have shown that the proposed algorithm has performed stronger and lossless compression on the images. The overall system performance has shown that the new system is robust, quick, and effective for image security.

5.1 Future Work

In the future, more work can be done to look into improving the Secured hybrid LSB - MSB steganography algorithm for increased efficiency without compromising data security or image quality. This can be achieved by working on the compression ratio for stronger embedding procedures and also finding a way to apply this technique on larger-sized gray-scale images. The proposed technique in the future will be extended to use on other steganographic cover objects such as video or audio.

Additionally, integrating machine learning into steganography presents a promising avenue to both detect and prevent steganographic activities while enhancing the overall security and quality of digital image steganography.

References:

[1] Marilou O. Espina, Arnel C. Fajardo, Bobby D. Gerardo, Ruji P. Medina (2019): Multiple Level Information Security Using Image Steganography and Authentication, *International Journal of Advanced Trends in Computer Science and Engineering*, vol.8(6), November - December 2019, pp.3297- 3303.

[2] Avni Aggarwal, Arpit Sangal, Aditya Varshney (2019): Image steganography using lsb algorithm, International Journal of Information Sciences and Application (IJISA). ISSN: 0974, 2255, Vol.11, No.1, 2019, (Special Issue) © *International Research Publication House*.

[3] M. Hussain, A. W. A. Wahab, Y. I. Bin Idris, A. T. S. Ho, and K. H. Jung, ―Image steganography in spatial domain: A survey, Signal Process. Image Commun., Vol. 65, pp. 46–66, 2018. https://doi.org/10.1016/j.image.2018.03.012.

[4] Khaled and Atta (2022): Developing algorithms for image steganography and increasing the capacity depending on choosing the best pixels. *International Journal of Computer Networks and Communications (IJCNC)*, Vol. 14, July 2022.

[5] Jingzhi Lin, Zhenxing Qian, Zichi Wang, Xinpeng Zhang,and Guorui Feng[1], (2020), A New Steganography Method for Dynamic GIF Images Based on Palette Sort, *Hindawi Wireless Communications and Mobile Computing*, Vol. 2020, 13 pages.

[6] Subhash Panwar, Mukesh Kumar, Sakshi Sharma, (2018), Digital Image Steganography Using Modified LSB and AES Cryptography, I*nternational Journal of Recent Engineering Research and Development*, Vol. 3, Issue 6, pp.18-27.

[7] Harakannanavar Sunil Ac, Ramachandra R, Pramodhini, (2019), Performance Analysis of MSB Based Iris Recognition Using Hybrid Features Extraction Technique, International *Journal of Engineering and Advanced Technology (IJEAT)*, Vol.8 Issue 6, August 2019, pp.230-239.

[8] Pooja Rani and Apoorva Arora (2015): Image Security System using Encryption and Steganography. *International Journal of Innovative Research in Science, Engineering and Technology* (An ISO 3297: 2007 Certified Organization), Vol. 4, Issue 6, June 2015.

[9] Mansoor Fateh, Mohsen Rezvani, and Yasser Irani (2021): A New Method of Coding for Steganography Based on LSB

Matching Revisited, *Security and Communication Networks*, Vol. 2021, Article ID 6610678, 15, https://doi.org/10.1155/2021/6610678.

[10] Satwinder Singh and Varinder Kaur Attri (2015): State-of-the-art Review on Steganographic Techniques. *International Journal of Signal Processing, Image Processing and Pattern Recognition,* Vol.8, No.7 (2015), pp.161-170.

[11] Vayadande (2022): Spell Checker Model for String Comparison in Automata. No. 7375. *Easy Chai* 2022.

[12] Sally A. Mahdi and Maisa A. Khodher (2021): An improved method for combining (LSB and MSB) Based on Color Image RGB. *Engineering and Technology Journal*, Vol. 39, part B (2021), No. 01, pp.231-242.

Contribution of Individual Authors to the Creation of a Scientific Article (Ghostwriting Policy)

The authors equally contributed in the present research, at all stages from the formulation of the problem to the final findings and solution.

Sources of Funding for Research Presented in a Scientific Article or Scientific Article Itself

No funding was received for conducting this study.

Conflict of Interest

The authors have no conflicts of interest to declare.