

# Performance Analysis of Simple Hybrid and New Hybrid (NHB) for Hiding Secret Text in Digital Image

Yu Yu Wai <sup>[1]</sup>, Ei Ei Myat <sup>[2]</sup>

Department of Information Technology Engineering  
Technological University (Thanlyin)  
Myanmar.

## ABSTRACT

One of the most important factors of information technology and communication have been the security of information. This paper presents a performance analysis of simple hybrid (SHB) and new hybrid (NHB) for hiding secret text in digital image. The embedding and extracting procedure of simple hybrid (SHB) steganography is very simple. The new hybrid (NHB) steganography procedures are complex. The new hybrid (NHB) technique produced a stego image without distortion in image quality which is better than simple hybrid (SHB). By using this technique stego image quality is better than the simple hybrid (SHB) so attacker cannot easily extract the secret data from stego image. The simple hybrid (SHB) embeds the secret data in the alternative to LSB and MSB. The new hybrid (NHB) is not a direct method to hide the value of secret text in LSB and MSB. It depends on the value of secret text in LSB and MSB. Performance was based on MSE and PSNR between the simple hybrid (SHB) and the new hybrid (NHB). The security of NHB is better than that of the SHB.

**Keywords** :— Simple Hybrid (SHB), New Hybrid (NHB), MSE and PSNR.

## I. INTRODUCTION

Steganography is the art and science of invisible communication. The word steganography is derived from the Greek words “stegos” meaning “cover” and “grafia” meaning “writing” defining it as “covered writing” [5]. Both Steganography and cryptography are used to ensure data confidentiality. Cryptography protects the content of the message in such a way anybody can see that both parties are communication in secret. Steganography hides the existence of a secret message in such a way that nobody can see that both parties are communication in secret [2]. The rightmost bit is called the LSB because changing it has the least effect on the value of the number. The leftmost bit is called the MSB because changing it has the most effect on the value of the number. The hybrid is combined the least significant bit (LSB) and the most significant bit (MSB). Steganography is comprised of two phases, one for embedding and one for extracting. The embedding process is concerned with hiding a secret data within a cover image. The extracting process reveals the secret data. In this paper, the inserting secret text is done in simple hybrid or new hybrid of the image pixel.

## II. SIMPLE HYBRID (SHB) ALGORITHM

- Simple hybrid (Combined LSB & MSB) techniques embed secret image bits into the least significant bit and most significant bit of the cover image.
- The first data bit is inserted in the least significant bit of the cover image byte.
- The second data bit is inserted in the most significant bit of the cover image byte.
- The output of the process is a stego image.

- The retrieving stage is just the inverse of the embedding stage [7].

## III. NEW HYBRID (NHB) ALGORITHM

The new hybrid (NHB) that embeds secret text if the MSB value of cover image is the identical to the MSB value of secret text, the cover image of LSB was inserted the MSB value of each byte at cover image. If the MSB value of cover image is not identical the MSB value of secret text, it insert the last 2 bit of each byte at cover image ‘01’ or ‘10’. For example, let consider a 24 bit for jpg image:

Data to be inserted: character ‘A’: 01000001

3 pixels will be used to store one character of 8 bits.

Embedding ‘A’

Cover Image:	00100111	11101001	11001000
	00100111	11001000	11101001
	11001000	00100111	11101001
New Hybrid Method:	<u>0010011</u> <u>0</u>	<u>1110100</u> <u>1</u>	<u>110010</u> <u>10</u>
	<u>001001</u> <u>10</u>	<u>110010</u> <u>10</u>	<u>111010</u> <u>10</u>
	<u>110010</u> <u>10</u>	<u>001001</u> <u>01</u>	11101001

Extracting ‘A’=> 01000001

## III. COMPARISON METHODS

To compare the image quality of the two algorithm i.e the SHB and the NHB algorithms, two metrics were used, which are the Mean Square Error (MSE) and the Peak Signal to Noise Ratio (PSNR). The MSE represents error between the cover image and stego image. If the value of MSE is lower then the image quality is good [1]. The equation is as follow:

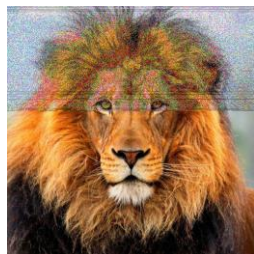
$$MSE = \frac{[I_1(M, N) - I_2(M, N)]^2}{M \times N}$$

The PSNR is used to compare the compression image quality of original image and stego image. If the value of PSNR is higher then the image quality is good [1]. The equation is as follow:

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

#### IV. EXPERIMENTAL RESULT

The secret texts are used for testing data. In the secret text, the text formats are docx, pdf, xlsx file. The two different sizes of different images are considered as cover image to analyze the performance of these two methods. Lion.jpg with dimension (512 x 512) pixels and file size of 272 kilo byte, Fruit.jpg with dimension (1024x682) pixels and file size of 630 kilo byte are used as cover image. Fig. 1(a), (b), (c) show the differences between the original image and stego image using simple hybrid (SHB) algorithm.



Original Image (512 x 512) Stego Image  
MSE = 1778.86, PSNR = 15.63 dB

Fig.1(a) Lion.jpg hiding docx file using SHB



Original Image (512 x 512) Stego Image  
MSE = 967.68, PSNR = 18.27 dB

Fig.1(b) Lion.jpg hiding pdf file using SHB



Original Image (512 x 512) Stego Image  
MSE = 2679.35, PSNR = 13.85 dB

Fig.1(c) Lion.jpg hiding xlsx file using SHB

Fig. 2(a), (b), (c) show unnoticeable differences when the original image is compared to the stego image embedding text file in Lion.jpg using NHB algorithm.



Original Image (512 x 512) Stego Image  
MSE = 0.43, PSNR = 51.84 dB

Fig. 2(a) Lion.jpg hiding docx file using NHB



Original Image (512 x 512) Stego Image  
MSE = 0.24, PSNR = 54.42 dB

Fig. 2(b) Lion.jpg hiding pdf file using NHB



Original Image (512 x 512) Stego Image  
MSE = 0.65, PSNR = 50.03 dB

Fig. 2(c) Lion.jpg hiding xlsx file using NHB

Fig. 3(a), (b), (c) show the differences between the SHB algorithm embedding the same text file in Fruit.jpg. Therefore, the larger the cover image, the more data can be stored.



Original Image (1024x682) Stego Image  
MSE = 624.23, PSNR = 20.18

Fig. 3(a) Fruit.jpg hiding docx file using SHB





Original Image (1024x682)  
Stego Image  
MSE = 356.27, PSNR = 22.61 dB

Fig. 3(b) Fruit.jpg hiding pdf file using SHB



Original Image (1024x682)  
Stego Image  
MSE = 962.46, PSNR = 18.30 dB

Fig. 3(c) Fruit.jpg hiding xlsx file using SHB

Fig. 4 (a), (b), (c) show the differences between the original image and stego image embedding the same text file in Fruit.jpg using NHB algorithm.



Original Image (1024x682)  
Stego Image  
MSE = 0.15, PSNR = 56.26 dB

Fig. 4(a) Fruit.jpg hiding docx file using NHB



Original Image (1024x682)  
Stego Image  
MSE = 0.09, PSNR = 58.75 dB

Fig. 4(b) Fruit.jpg hiding pdf file using NHB



Original Image (1024x682)  
Stego Image  
MSE = 0.24, PSNR = 54.43 dB

Fig. 4(c) Fruit.jpg hiding xlsx file using NHB

## V. HELPFUL HINTS

The experimental results using SHB and NHB are shown in Table I. The performance of these two methods is measured

with MSE and PSNR. The lower MSE and higher PSNR can cause the better performance. The MSE value of SHB is larger than that of NHB. Moreover, the PSNR values of SHB are significantly smaller than that of NHB. Based on these two factors, the performance of NHB is better than SHB.

The new hybrid (NHB) method producing stego image is almost identical to the original image. When the sizes of the cover image were increased, the image quality of the NHB algorithm increased the better image quality.

TABLE I

EXPERIMENTAL RESULTS USING SHB AND NHB

SN	Cover Image	Algo-rithm	Secret Data Type	File Size (KB)	Stego Image Result			
					MSE	PSNR (dB)	Image Qty	Security Level
1	Lion.jpg (512x512) 272 KB	SHB	docx	41	1778.86	15.63	bad	weak
			pdf	23	967.68	18.27		
			xlsx	62	2679.35	13.85		
		NHB	docx	41	0.43	51.84	good	strong
			pdf	23	0.24	54.42		
			xlsx	62	0.65	50.03		
2	Fruit.jpg (1024x682) 630 KB	SHB	docx	41	624.23	20.18	bad	weak
			pdf	23	356.27	22.61		
			xlsx	62	962.46	18.30		
		NHB	docx	41	0.15	56.26	good	strong
			pdf	23	0.09	58.75		
			xlsx	62	0.24	54.43		

## VI. CONCLUSION

In this paper, the performance of the simple hybrid (SHB) and the new hybrid (NHB) was presented. In the hybrid steganography, system-identified and stego key can be used to secure the secret data. The simple hybrid (SHB) algorithm is very simple because the secret bits are alternately inserted LSB bit and MSB bit. Unlike the simple hybrid (SHB), new hybrid (NHB) algorithm complicates. The security of NHB is better than SHB.

In future work, other data types will be able to embed into the cover image with this NHB algorithm. It is better to be upgraded the new hybrid (NHB) algorithm to get superior image quality and security. In the proposed research, embedding algorithm was operated on spatial domain. Moreover, a study can also be done in frequency domain.

## REFERENCES

- [1] Solomon O.Akinola and Adebanye A.Olatidoye, "On the Image Quality and Encoding Times of LSB, MSB and combined LSB-MSB Steganography algorithms using digital images", *International Journal of Computer Science & Information Technology (IJCSIT)* Vol 7, No 4, August 2015
- [2] Mr. Gaurav, "A New Method for Image Steganography Using LSB and MSB", *International Journal of Recent Research Aspects* ISSN: 2349-7688, Vol. 2, Issue 4, December 2015, pp. 169-174
- [3] Rohit Garg and Tarun Gulati, "Comparison of LSB& MSB Based Steganography in Gray-Scale Images",

*International Journal of Engineering Research & Technology (IJERT)*, Vol. 1, Issue8, 2012.

- [4] Kanika Anand, Rekha Sharma, “Data Security Using LSB & MSB Image Steganography”, *International Journal of Electrical & Electronics Engineering(IJEEE)*, Vol.1, Issue6 (December,2014)
- [5] Anil Khurana, B. Mohit Mehta, “Comparison of LSB and MSB based Image Steganography”, *International Journal of Computer Science And Technology (IJCT)* Vol. 3, Issue 3, July - Sept 2012
- [6] Yu Yu Wai, Ei Ei Myat, “Comparison of LSB, MSB and New Hybrid (NHB) of Steganography in Digital Image”, *International Journal of Engineering Trends and Applications (IJETA)* Volume 5 Issue 4, 2018
- [7] Mr. Nyi Nyi Tun, “Comparison of Simple Hybrid and Modified Hybrid of Audio in Image Steganography”, *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)* Volume 7, Issue 7, July 2018, ISSN: 2278 – 1323
- [8] Arun Kumar Singh, Juhi Singh, Dr. Harsh Vikram Singh, “Steganography in Images Using LSB Technique”, *International Journal of Latest Trends in Engineering and Technology (IJLTET)*, Vol. 5 Issue 1 January 2015, ISSN: 2278-621X
- [9] Deepika [1], Dr. Sanjay Kumar [2], “Image Based Steganography Using LSB Method and Java Based Encryption”, *International Journal of Engineering Trends and Applications (IJETA)* – Volume 2 Issue 5, Sep-Oct 2015
- [10] Mr. Falesh M. Shelke, Miss. Ashwini A. Dongre, Mr. Pravin D. Soni, “Comparison of different techniques for Steganography in images,” *International Journal of Application or Innovation in Engineering & Management (IIAEM)*, Volume 3, Issue 2, February 2014