Efficient Text Message Hidden Technique Using YIQ Model

Ali Nasser Hussain[a, #], Entidhar Mhawes Zghair[b, *]

[a]*College of Electrical Engineering Techniques, Middle Technical University, Baghdad, Iraq*
[b]*Technical Instructors Training Institute, Middle Technical University, Baghdad, Iraq*

[#]*E-mail: alinasser1974@yahoo.com,* [*]*E-mail: ent_mz2005@yahoo.com*

Abstract

This paper produces and investigates the steganography technique of information hiding in communication system by using other information to provide major security. Nowadays, the security in the information transferring plays a vital role due to data protection importance. Therefore, the traditional techniques by using invisible ink or hidden tattoos need to developed and compensate under digital processing. Hence, Red (R), Green (G) and Blue (B) plans (RGB) approach is activated to improve the proposed scheme. By this technique, the text message converted to binary code as first stage. Then, the binary code is arranged as an image and converted to (YIQ) model as second stage. The final stage is to save the picture and converted to color image to minimize the distortion. Results show high Peak Signal to Noise Ratio (PSNR) and minimum Mean Square Error (MSE) in the extracted picture. The suggested algorithm is a promising technique to enhance the current and future communication security and open new widow to develop this issue.

Keywords: Steganography, Data Hiding, Image Stages, YIQ**.**

فاعلية تقنية اخفاء رسالة نصية يستخدام بنموذج YIQ

الخلاصة:
تقدم هذه الدراسة، البحث في تقنية إخفاء المعلومات بواسطة معلومات أخرى في نظام الاتصالات لتوفير أمن كبير. في الوقت الحاضر،أمن نقل المعلومات يلعب دورا حيوياً بسبب أهمية حماية البيانات. لذلك، التقنيات التقليدية باستخدام حبر غير مرئي أو الوشوم المخفية تحتاج إلى تطويرها والاستعاضة عنها بالطرق الحديثة من المعالجات الرقمية. وبالتالي خطط، الأحمر (R)، الأخضر (G) والأزرق (B) او ما تدعى بطريقة (RGB) تفعل لتحسين المخطط المقترح. بواسطة هذه التقنية، الرسالة النصية تحول إلى شفرة ثنائية كمرحلة أولى. ثم، يتم ترتيب الشفرة الثنائية كصورة وتحويلها الى موديل (YIQ) كمرحلة ثانية. المرحلة الأخيرة هي لحفظ الصورة وتحويلها إلى صورة ملونة لتقليل التشوية. والنتائج أظهرت أشارة القمة العالية الى نسبة معدل الضوضاء (PSNR)مع نسبة خطأ طفيفة (MSE) في الصورة المستخرجة. الخوارزمية المقترحة هي تقنية واعدة لتعزيز أمن الاتصالات الحالية والمستقبلية وفتح نافذة جديدة لتطوير هذه المسألة.

1. Introduction

The digitalization of data transmission in the modern communication processing gave the researchers new open window to develop the security in the send information. Interfere information via internet suffer from unlawfully copy, tamper and intercept. Hence, fast growth in the data security technique was needed to overcome this phenomenon. One of the most important techniques is by using a steganography to hiding the data in the communication channels. The objective of this method is to increase the capacity and security enhancement for traditional message. The Steganography approach is typically containing a media conversion into secret data in term of such called storage media [1]. The cryptography, watermarking, and steganography is a different methods which is used to hidden the information via internet channels. Many researchers are contributing in this field as in [2-5]. This paper introduces and investigated a steganography technique only as a major goal. However, the hiding secret data is changed the Least Significant Bit (LSB) of each pixel in the image cover by the bits in the secret information resulting in low distortion. The idea contributed by [6] considers a simple and traditional compared with used demand in current communication complexity.

2. Bit Insertion Strategy

Today, the LSB insertion strategy is the most important method in the steganography data encryption way[7]. In the below message hidden example, one could hide the letter (A) in the first 8-bytes of three pixels in 24-bits image pixel.

(00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)

A:01000001

Result:

(00100110 11101001 11001000)
(00100110 11001000 11101000)
(11001000 00100111 11101001)

The transformed bits is show as three underlined bit which represent the half message bit in the LSB insertion bit were required. Insignificant difference in the suggested approach permit to insert the message in more LSB for each byte resulting in big information capacity as well. Due to slight change, one could avoid the pixel change too [8,9]. In the case of 24-bit image, every color bit of the red, green and blue components could be used. Subsequently, each color represented by a byte. In this case one could store 3 bits in each pixel. Thus, a 800×600 pixel image could store a

total amount of 1,440,000 bits or 180,000 bytes of fixed information as illustrated in the below example.
The 3 pixels of 24-bit image could be represented as:

(00101101 00011100 11011100)

(10100110 11000100 00001100)

(11010010 10101101 01100011)

The binary representation of (11001000) for the number 200 is embedded into LSB, then the resulting grid written as:

(00101101 00011101 11011100)

(10100110 11000101 00001100)

(11010010 10101100 01100011)

While the first 8 byte in the grid need to change only 3 underlined bits according to fixed message. Then, by using the maximum cover size one can use only half bits from the image for this duty. Subsequently, the 256 possible intensity of each color will change the LSB of pixel to introduce a small change in the colors intensity. Hence, the human eye can't distinguish this changes and the hidden process is successfully established [5].

3. YIQ Color

The National Television Systems Committee (NTSC) in United States used YIQ color space due to a great advantage of gray scale information could separate from color data; therefore it's used for both black/white and colors signals. The three components of NTSC color space include Luminance Y, hue I and saturation Q which represent gray and chrominance respectively. The approximation of given formulation between RGB and YIQ as in [11]:

$R, G, B, Y \in [0, 1][-0.5957, 0.5957]$

$I \in [-0.5957, 0.5957]$

$Q \in [-0.5226, 0.5226]$

$$\begin{bmatrix} R \\ G \\ B \end{bmatrix} = \begin{bmatrix} 1 & 0.9563 & 0.6210 \\ 1 & -0.2721 & -0.6474 \\ 1 & -1.1070 & 1.7046 \end{bmatrix} \begin{bmatrix} Y \\ I \\ Q \end{bmatrix}$$

$$\begin{bmatrix} Y \\ I \\ Q \end{bmatrix} = \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ 0.595716 & -0.274453 & -0.321263 \\ 0.211456 & -0.522591 & 0.311135 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix}$$

4. Suggested Model

The suggested technique depends on psycho visual redundancy and pixel dependency.
In general, the color image contains 3 different bands in its formed. This color like red, green and blue represent the color coordinate systems. The proposed flow chart of suggested algorithms for basing text message is illustrated in Figure 1.

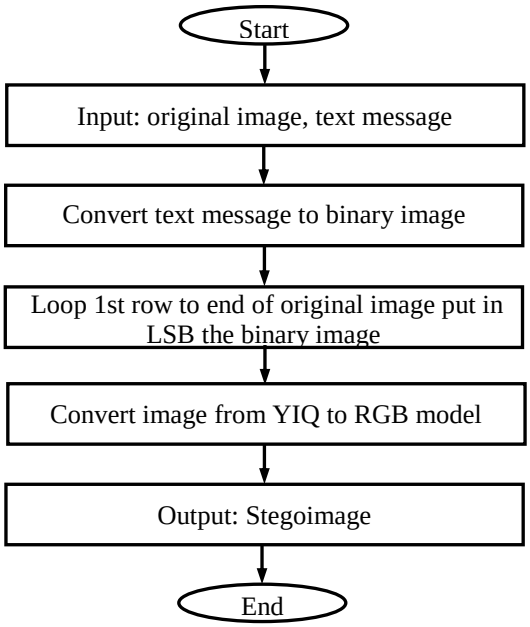

Figure 1: Suggest algorithms flowchart.

The information hiding process in suggested algorithms achieved in R, G and B band. Hence, the MATLAB program version (7.1) has been used to design the proposed algorithms. The first stage is to data hidden passing to Graphical User Interface(GUI) in MATLAB to implement the LSB algorithms. The second stage in this approach is to return back the reverse data in the cover RGB image cover by using GUI interface tool as illustrated below:

Input: RGB color cover image, text message to recover.

Output: Stego RGB color image.

Step 1: Decompose the color image into R, G, and B bands.

Step 2: Decompose each of the R, G, and B band data into binary bit planes.

Step 3: Transfer the covert information into the binary bit stream.

Step 4: Scan each binary bit in first binary image
1^{st}Red band of cover image bit = current pixel in the first binary image.

Step 5: Scan each binary bit in second binary image
1^{st}Green band of cover image bit = current pixel in second binary image.

Step 6: Scan each binary bit in third binary image
1^{st}Blue band of cover image bit = current pixel in third binary image.

Step 7: Save those information generated in steps 4, 5 and 6.

5. Hidden Data Extraction

The extraction of hidden data from original host image could be recreated without data losses as shown below:

Input: Embedded image.

Output: Original RGB color image, 3 Hidden Binary images.

Step 1: Decompose the Embedded image into R, G, and B bands.

Step 2: Decompose each of the R, G, and B band data into binary bit planes.

Step 3: Design temple zeroes matrix:
Temple (size) =original (size)
For each pixel in temple =1^{st} Red band bit of Embedded image.

Step 4: **S**ave temple matrix a first binary image.

Step 5: Implement step3 to step4 for Green band and Blue band.

Step 6: Save this information generated in steps 3, 4 and 5.

6. Results

Different image in size, application and field has been chosen to implement the suggested algorithms as illustrated in Table 1. Figures 2, 3 and Figure 4 show the different steps of implementation process in the suggested model.

Table 1: Groups original cover images size.

Class	Size
A	512×512
B	288×237
C	332×400

Figure 2: Class A covers images.

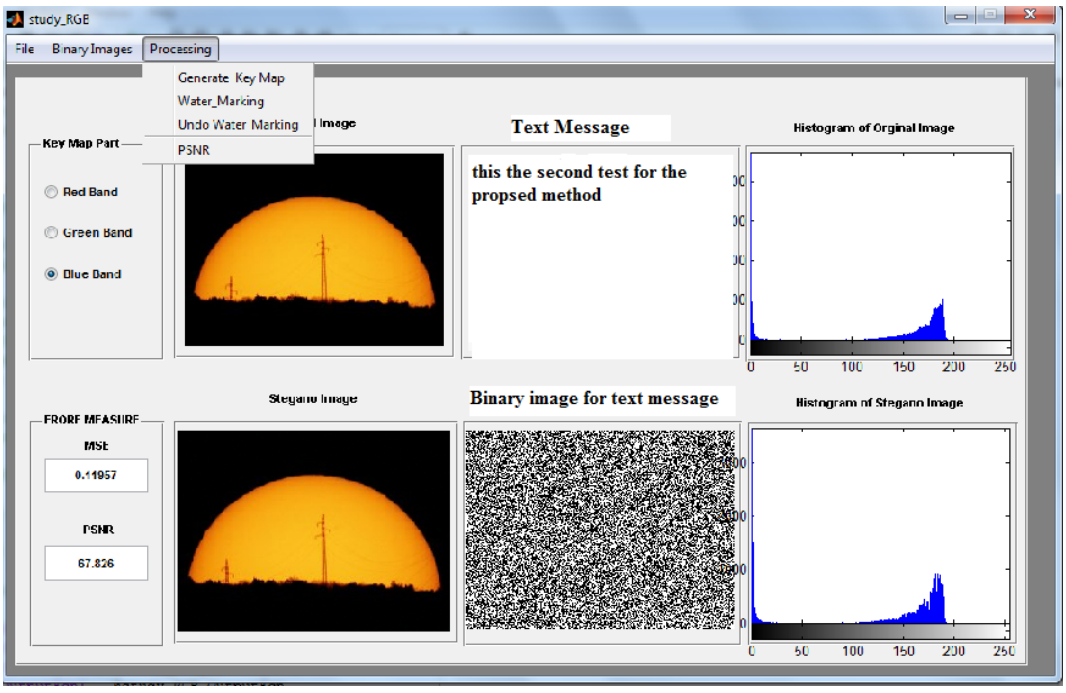

Figure 3: Class B covers images.

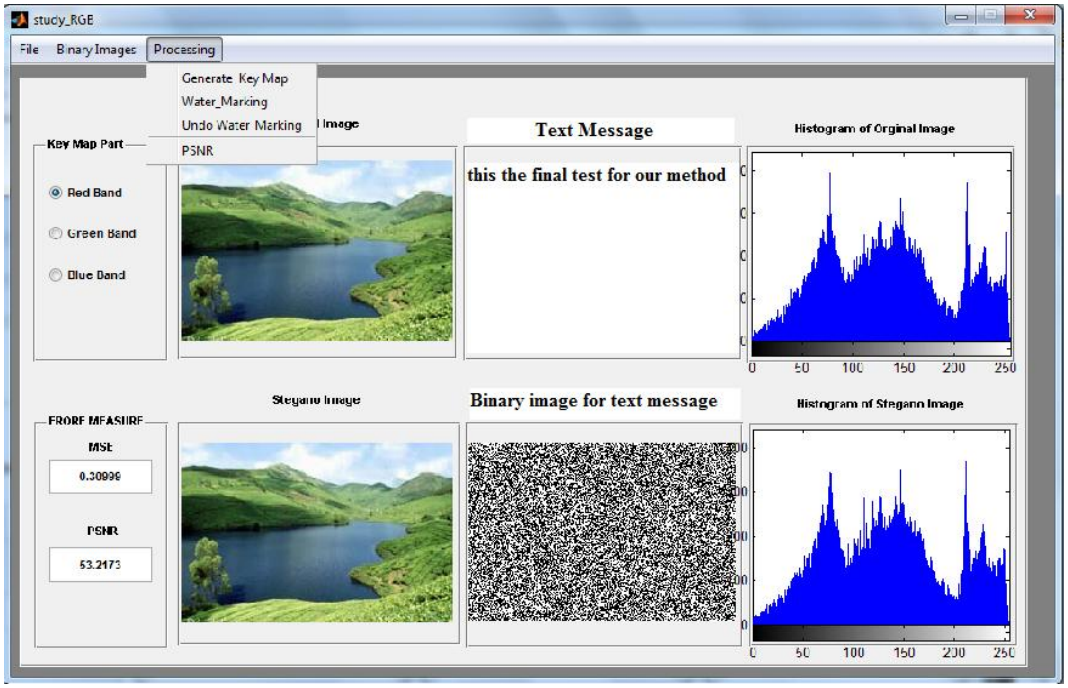

Figure 4: Class C covers images.

To create secret message, the MATLAB is used to implement the hidden image. The measurement of 3 stages image quality has been done using PSNR level. Hence, a large PSNR level represents small possibility of visual attack in human eyes. The three standard gray scale images in Figure 1, 2 and Figure 3 named Lena, Medical and Famous picture is illustrated as well. The exhibition of all images show the amount of smooth area and complicated area in the image effect which depend on the PSNR capacity inserting. The spreading in all images stage is highlight due to big secret message affected by use LSB in the RGB band techniques which is hidden for human eyes. As clear in all images, the medical image is more complicated than other image due to more edge area and frequent variation. Hence, the capacity is affected more than Lena image as shows in Figure 5, 6 and Figure 7.

The image imperceptibility is shown by PSNR values [3].

$$MSE = \frac{1}{MN}\sum_{i=0}^{M}\sum_{j=0}^{N}(X_{ij} - y_{ij}) \quad (1)$$

$$PSNR(dB) = 10\ log_{10}\left(\frac{1^2}{MSE}\right) \quad (2)$$

Where$X_{ij}$is the i^{th} rows and j^{th} columns of original imagewhiley_{ij} is the i^{th} row and j^{th} column of transformed image. Higher the PSNR value means more difficult to perceive that any hidden message is hidden. In our experimental work we have found that by increasing the payload, the PSNR value drops down. We have to make a compromise between payload and PSNR.

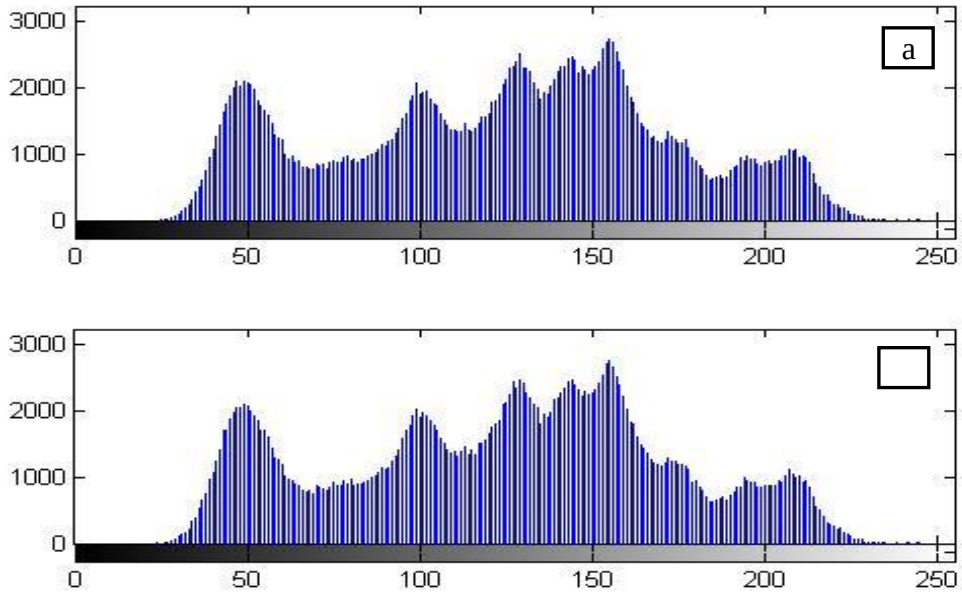

Figure 5: Histogram embedded image of original (a) and hidden (b) forclassA.

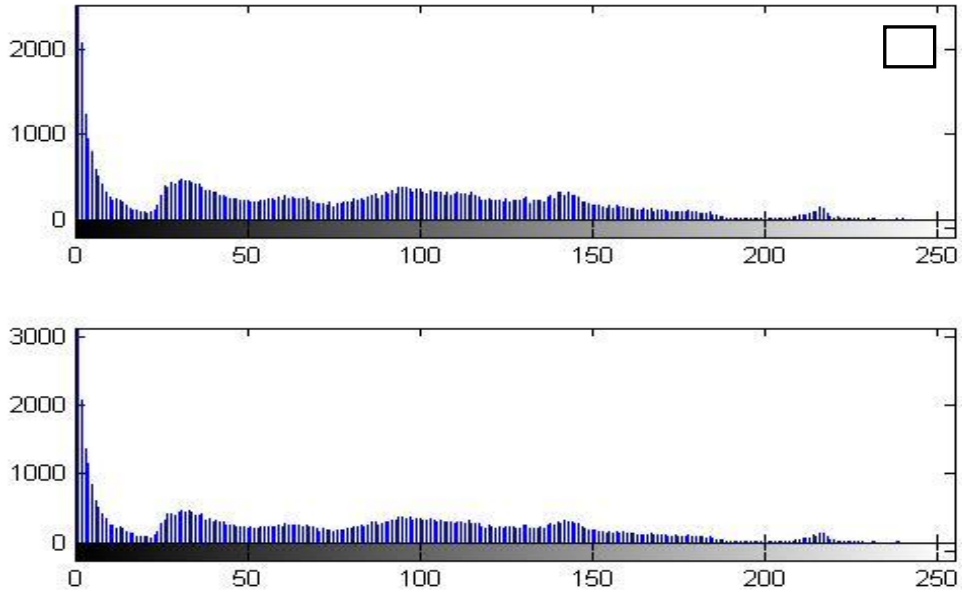

Figure 6: Histogram embedded image of original (a) and hidden (b) forclass B.

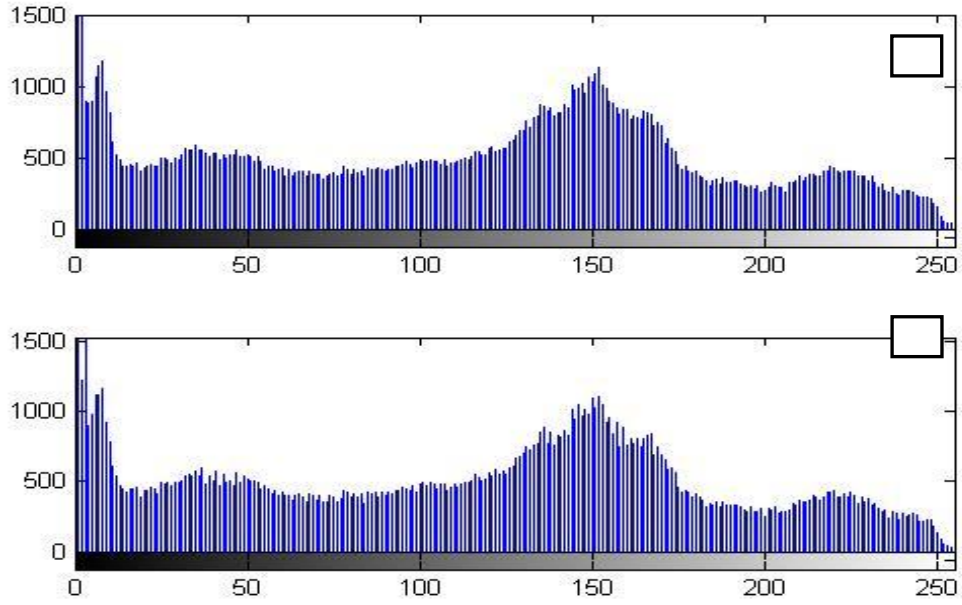

Figure 7: Histogram embedded image of original (a) and hidden (b) forclass C.

Table 2: The average results for each group of colored images.

Class	PSNR(dB)	Maximum Hiding Capacity in (bits)
A	41.1468	786432
B	36.5154	204768
C	41.0449	398400

Figures 5– 7show the results of each group for colored images in graph to help study the results more easily. Table 2shows the average results of each group for colored images. If we change our set of images, the results will change accordingly. The payload values can also be changed by using a different information or content to be Stephen by the proposed method**.**

7. Conclusions

The new technique of watermarking using RGB band for all images size is implemented in this paper. The suggested methods provide randomize key map hidden in single channel and two channels in binary and copyright image embedded into original image for more protection and improve the system security. The suggested technique is promising in attack the JPEG compression and noise. The more attractive feature for this proposed method is the ability to use either symmetric key or public key and the verification of original message could be done without hash. This work will support and accelerate the researcher developments in the communication security field.

8. References

1. Schaathun, H. G. (2012). Machine Learning in Image Steganalysis", *A John Wiley & Sons, Ltd., Publication*, pp. 279.
2. Provos and P. Honeyman, "Hide and Seek: an Introduction to Steganography", *IEEE Security Privacy Magazine*,Vol. 1, No. 3, 2003. pp. 32–42.
3. Rubab, S., Younus,M. (2012). Improved Image Steganography Technique for Colored Images Using Wavelet Transform. *Int. J. Computer Applic.* 39(14): 29–32.
4. Petitcolas, F.A.P., Anderson, R.J., Kuhn, M.G. (2004). Information Hiding a Survey, *Proceedings IEEE*. 87(7): 1062–1078.
5. Kumar, M., Kumar, S., Gupta, N. (2011). Image Steganography Tool Using Adaptive Encoding Approach to Maximize Image Hiding Capacity, *Int. J. Soft Computing Eng*, 1(2): 7–11.
6. Chan, C.K., Chen, L.M. (2004). Hiding Data in Images by Simple LSB Substitution, *Pattern Recognition*, 37(3): 469–474.
7. Juneja, M., Sandhu, P. (2009). Implementation of Improved Steganographic Technique for 24-bit Bitmap Images in Communication, *Marshland Press J. Am. Sci.*, 5(2): 36–42.
8. Al-Taani ,T. A. and AL-Issa, A. M. (200(). A Novel Steganographic Method for Gray-Level Images, *World Acad. Sci. Eng. Technol.* 27: 613– 618.
9. Johnson, N.F. and Katzenbeisser, S.C." A survey of Steganographic techniques", in S. Katzenbeisser and F. Peticolas (Eds.): Information Hiding, Artech House, Norwood, MA, pp.43–78.
10. Lou, D. C. and Liu, J. L. (2002). Steganography Method for Secure Communications, Elsevier Science on Computers & Security, 21 (5): 449–460.
11. Gonzalez, R.C., Woods, R.E. (2009). Digital Image Processing Using MATLAB", Second Edition.