IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

An Information Hiding System Based on Image Steganography for Color Images

Phyu Hnin Lwin[1], May Htet[2]

Department of Computer Engineering and Information Technology, Mandalay Technological University,
The Republic of the Union of Myanmar[1,2]

Abstract: Information Hiding is one of the challenging issues in the field of security. Steganography is one of the most important fields in information hiding system. Steganography is used to hide the existence of secret message by embedding the message inside any cover object like image, text, audio and video files. This paper proposes a new method based on modified PVD method in order to obtain larger embedding capacity and produce acceptable stego image quality. To prove the better performance of the proposed method, the comparison analysis is performed according to Peak Signal to Noise Ratio (PSNR) values and embedding capacity. Experimental results show that the proposed method provides an average hiding capacity gain of 1.85 times over the existing method while maintaining acceptable of stego image quality.

Keywords: Information Hiding; Image Steganography; Proposed Method; modified PVD method; Secret Message.

I. INTRODUCTION

With the exponential growth of the Internet usage, the demand for effective information security techniques is increasing day by day. Steganography is one the most common platforms used to maintain secrecy to the data in transit. Digital image steganography is one of those techniques that are used for effective secret communications. In this technique, secret communication is achieved by embedding a message into a cover image and generating a stego image that carries a hidden text message [1].

There are different methods for data hiding in image steganography such as least significant bit method, pixel-value difference method, histogram modification and pixel mapping method that use spatial domain. Many works have been done in this area and many methods have been developed because they are employed in various useful applications such as commercial, medical imaging and military communication systems and so on where the information security is essential [2, 3].

Wu and Tsai proposed a Pixel Value Differencing (PVD) method with outstanding quality of stego image and also hide more data. Thereafter, various PVD based approaches have been proposed [4].

C.S. Tsai, and M.S. Hwang [5] proposed Image steganographic scheme based on pixel-value differencing and LSB replacement methods. In this paper, the original PVD method is used for embedding data by applying Optimal Pixel Adjustment Process (OPAP) using target pixel with three surrounding pixels. The capacity of embedding data in target pixel is determine by calculating the largest pixel value differencing between three other pixels close to target pixel. To enhance image qualities of stego image, OPAP is used. The embedding error can be reduced by OPAP method.

Hsien-Wen Tseng [6] proposed a steganographic method based on Pixel-Value Differencing and the perfect square number. In this paper, new range table is designed by modifying original range width and embedding bit length. Range width is modified using Perfect Square Number. Embedding process is same as original PVD (embedding is done by calculating the difference values of two pixels). This method provides high embedding capacity than original method.

Nagaraj V, Vijayalakshmi V, Zayaraz G [7] proposed color image steganography based on Pixel-Value Differencing method. This modified PVD method uses color cover image with non-overlapping concept.

In order to obtain better embedding capacity with acceptable image quality, this work proposes a new embedding method based on modified PVD method [7]. To do the comparative study, the analysis of the proposed embedding method and modified PVD method is performed in term of embedding capacity and PSNR values.

The rest of the paper is organized as follows: Research Method is described in Section II. Design of the proposed system is presented in Section III. Section IV represent the implementation results. The performance analysis of this system is shown in Section V. Finally, Section VI draws the conclusion.

II. RESEARCH METHOD

In the proposed system, secret messages are hidden in the cover image using the proposed method. As the idea of proposed method is based on the concept of existing modified PVD method , this section first review on existing method.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

A. Review on the existing modified PVD method

The Existing Method [7] is one of the various PVD based approaches. This method divides color cover image into three color planes (Red, Green and Blue). Every pixel contains 24 bits (for 8-bit representation) each one as 8 bit components in pixel. In the existing embedding method, all the three components have been used for data embedding. First, each color component from a pixel is separated and three separate M*N matrix is obtained.
Data hiding in each plane is performed in a sequencing manner. The color image is separated into three component color matrix and apply sequentially on 1st pixel value of Red matrix, then 1st pixel value of Green matrix and finally on Blue matrix and continue the same procedure for 2nd pixel value of each plane and so on. Secret data (d) are converted into base 3 values of (0, 1, 2).

These secret values are embedded into three planes. Pixel values of the image matrix are grouped into $g_1, g_2, \ldots, g_n$. Decimal value of Red pixel is represented by g_{ri} , similarly decimal value of Green and Blue are represented as g_{gi} and g_{bi}. The function f (three components mod 3) has three cases.
Case 1: If $f = d$, then modification is not needed, directly g_{ri} is taken as new pixel value g_r'.
Case 2: If $f < d$, then increase the value of g_{ri} by 1, $g_{ri}' = (g_{ri} + 1)$ then new modified pixel value is obtained.
Case 3: If $f > d$, then the value of g_{ri} is decreased by 1, $g_{ri}' = (g_{ri} - 1)$ then new modified pixel value is obtained.

B. Disadvantages of the existing modified PVD method

First, existing embedding method embeds one secret digit on one component of cover image and therefore this method has to use all three components for embedding secret message because of using non-overlapping concept.
As existing embedding method embeds one secret digit on one component of color cover image, either some components have large embedding space to embed secret message or other components have small embedding space to embed secret message.

Second, pixels from cover image are selected in a sequencing manner thus every pixels of cover image cannot embed secret messages.

Third, the existing method needs to refer to the original image when extracting the embedded data from a stego image.

C. Example Calculation of the Data Embedding and Extraction Procesess for existing modified PVD method

For data embedding process, three components values of a color pixel are assumed to be $R_1 = 226$, $G_1 = 137$, and $B_1 = 126$. Secret data in ternary form (base 3) = d = 10212…For Red component, embedded secret message (base 3 value): d is 1. Modulus 3 Function = $f = R_1 \bmod 3 = 226 \bmod 3 = 1$. If $f = d$, then modification is not necessary, R_1 is directly taken as new pixel value $R_1' = 226$.

For Green component, embedded secret message (base 3 value): d is 0. Modulus 3 Function= $f = G1 \bmod 3 = 137 \bmod 3 = 2$. If $f > d$, then the value of G1 is decreased by 1, G1'= (G1 – 1) then new modified component value (136) is obtained. For Blue component, embedded secret message (base 3 value): d is 2. Modulus 3 Function = $f = B_1 \bmod 3 = 126 \bmod 3 = 0$.If $f < d$, then increase the value of B_1 by 1, $B_1' = (B_1 + 1)$ then new modified pixel value (127) is obtained. In Extraction Process, resulting three final stego components are 226, 136 and 127.

For Red component, stego component value = $R' = 226$ and cover component value = $R = 226$.
Modulus 3 Function = $f = R' \bmod 3 = 226 \bmod 3 = 1$. If f = 1, $R' = 226$ and $R = 226$ then embedded secret message (base 3 value): $d = 1$. For Green component, stego component value = $G' = 136$ and cover component value = $G = 137$.
Modulus 3 Function = $f = G' \bmod 3 = 136 \bmod 3 = 1$. If $f = 1$, $G' = 136$ and $G = 137$ then embedded secret message (base 3 value): $d = 0$.

D. The Proposed Method

To overcome the disadvantage of existing embedding method [7], the proposed method is developed in this paper.

First, the proposed method uses three consecutive components of a color pixel for embedding secret message bits in color cover image, therefore this method has four components for embedding secret message bits because of using overlapping concept.

Second, the three consecutive pixels from cover image are selected in a serial manner thus every pixels of cover image can hold the secret messages.

Third, the proposed method does not need to refer to the original image when extracting the embedded data from a stego image.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

E. The Example Calculation of the Data Embedding and Extraction Processes for Proposed Method

It is assumed that three consecutive overlapping components a color pixel: R_1= 102, G_1= 120 and B_1= 130 are selected from cover image to embed secret messages and partitioned into two component pairs.
In addition, it is assumed that the secret message to be embedded is 'Hello' and its binary form is (01001000 01100101 01101100 01101100 01101111)$_2$. First, the two component: R_1= 102 and G_1= 120 are taken as a first component pair. For the first component pair, the difference value is 18 (d = 120 – 102 = 18).The number of bits which can be embedded is 4 bits [(u_k– l_k + 1)] = 4). The first foure bits of binary secret message is (0100)$_2$ and its decimal value is 4. It is added to the lower bound range width of 16 to get the new difference value 20 (d' = 16 + 4 = 20). The temporary value is 2 [mj = dj'– dj , 20–18 = 2].

And then, two intermediate stego components are 101 and 121 [(R_1*, G_1*) = (102 – 1), (120 + 1) = (101, 121)].
Second, overlapping components: G_1= 120 and B_1= 130 are taken as a second component pair. For the second component pair, the difference value is 10 (d = 130 – 120 = 10) which is in the range width between 8 and 15.
The number of bits which can be embedded is 3 bits [(u_k–l_k+ 1) = 3]. The three bits binary secret message is (100)$_2$ and its decimal value is 4. It is added to the lower bound range width of 8 to get the new difference value 12(d'= 8 + 4 = 12). The temporary value is 2 [mj = dj'– dj , m = 12– 10 = 2] And then, two intermediate stego components are 119 and 131 [(G_1*, B_1*) = (120 – 1), (130 + 1) = (119, 131).

Finally, four intermediate stego components value: 101, 121, 119, 131 are modified by using adjustment process to get three final stego components: R_1' = 104, G_1' = 116 and B_1' = 136 [G_1' = 116 = (131+101)/2, R_1' = 119 – (131 – 116) = 104, B_1' = 121 – (101 – 116) = 136].

In Extraction Process, resulting three final stego pixels are 104, 116 and 136 and these stego components are partitioned into two components pairs: (104, 116) (116 , 136).

For the first stego components pair, the difference value is 12 (dj ' =116 – 104 = 12). Lower bound of this range width is 8. And then, embedded secret message is 4 (sj =dj ' – lk = 12 – 8 = 4) that is in decimal and this embedded secret values is converted in decimal to binary form = (0100)$_2$.

For the second stego component pair, the difference value is 20 (dj' = 136 – 116 = 20). which is between 16 and 31 range width. Lower bound of this range width is 16.
And then, embedded secret message is 4 (sj =dj ' – lk = 20 – 16 = 4) that is in decimal and this embedded secret values is converted in decimal to binary form = (100)$_2$.

III. DESIGN OF THE PROPOSED SYSTEM

The design of the proposed system is composed of two portions: secret message embedding process for sender site and secret message extracting process for receiver site and are illustrated in Fig 1.

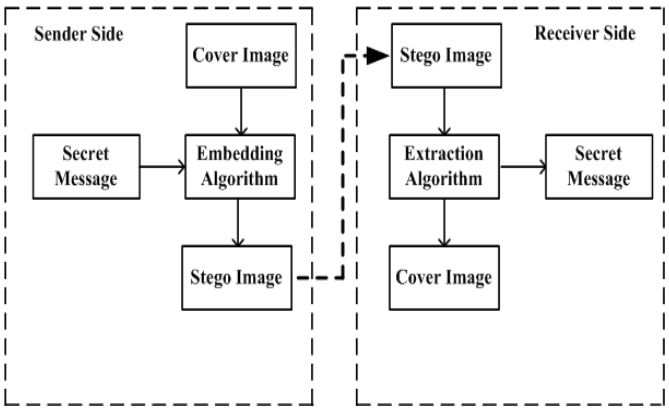


Fig 1. Design of the proposed system

In the embedding process, the cover image is used to embed secret message. Secret message is embedded in the cover image by using the proposed method to form the stego image. Resulting stego image is transmitted to receiver via a public channel.
In the extracting process, the receiver extracts the embedded message using the proposed method from received stego image. In the proposed system, embedded data can extract from the stego image without using the original cover image.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

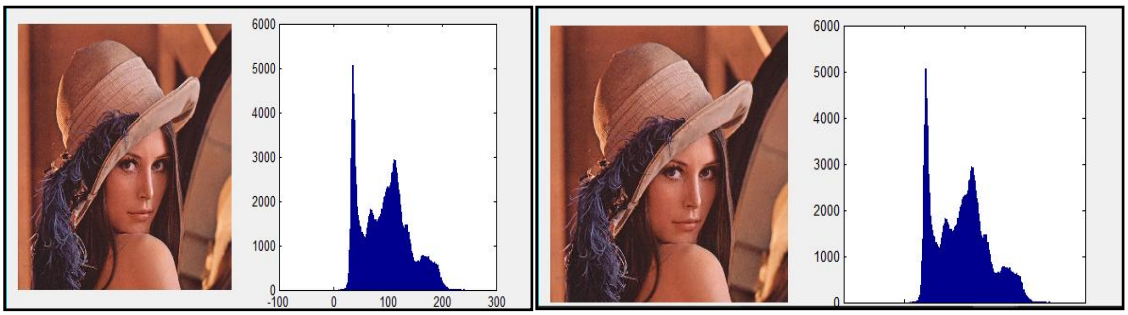
IV. IMPLEMENTATION RESULTS

The implementation result of the proposed system is implemented by using Matlab2014a. Five standard images: 'Lena', 'Boat', 'Babbon','Peppers', and 'Airplane', each with size 512×512 pixels, are used as cover images as depicted in Fig 2.

(a) (b) (c) (d) (e)

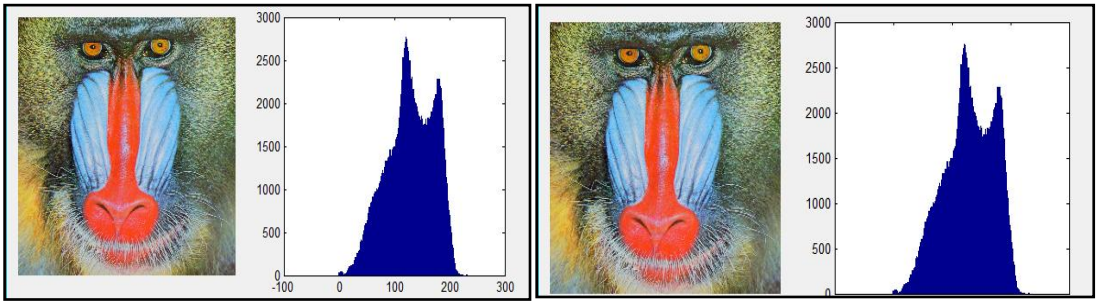
Fig 2. Five Cover Images (a) Peppers (b) Lena (c) Airplane (d) Babbon (e) Boat

Using Matlab2014a, the stego image and its histogram are created after embedding the secret message into cover image with the help of the proposed method. The histograms of five standard images and their corresponding stego images and shown in Fig 3, 4, 5, 6 and 7 respectively.



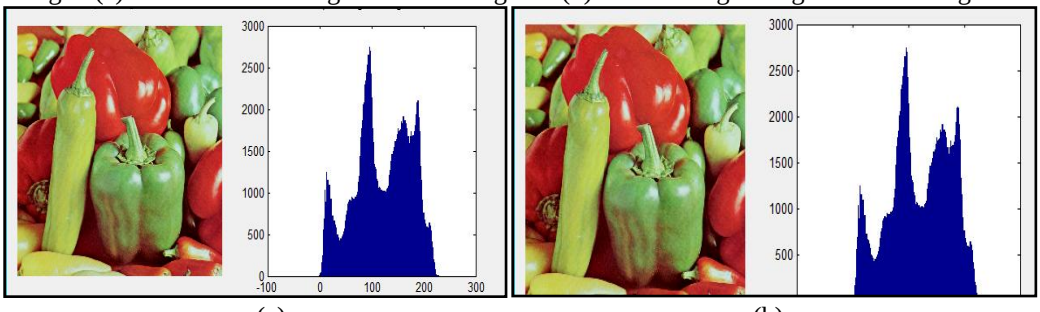
(a) (b)

Fig 3. (a) Lena Cover Image and its Histogram (b) Lena Stego Image and its Histogram



(a) (b)

Fig 4. (a) BaboonCover Image and its Histogram (b)Baboon Stego Image and its Histogram



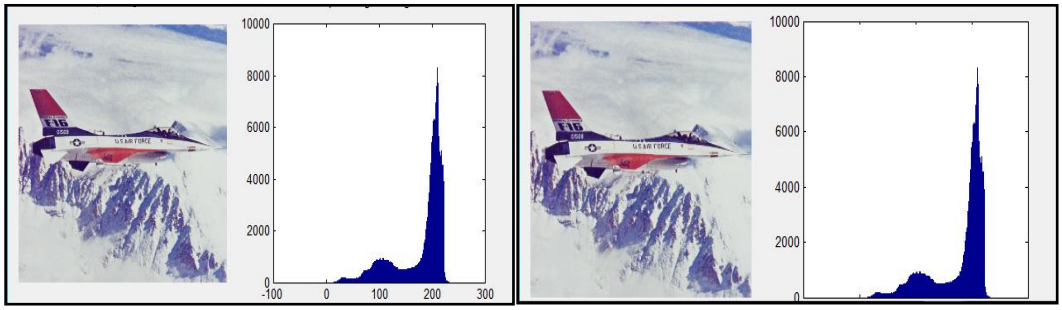
(a) (b)

Fig 5. (a) Peppers Cover Image and its Histogram (b) Peppers Stego Image and its Histogram

IJARCCE

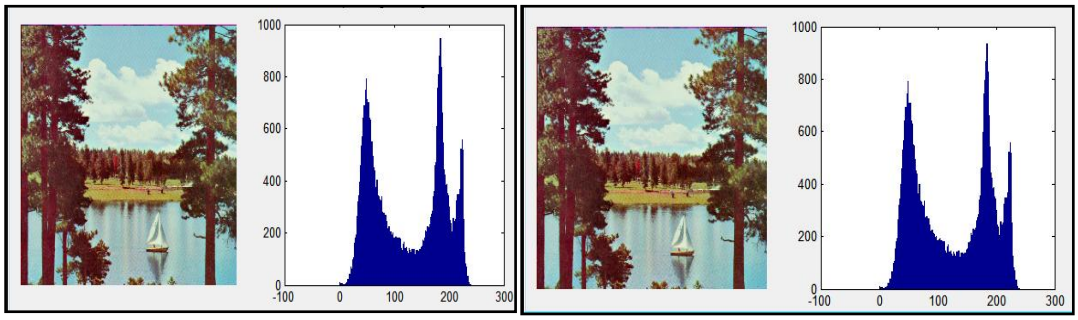
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018



(a) (b)

Fig 6. (a) Airplane Cover Image and its Histogram (b) Airplane Stego Image and its Histogram



(a) (b)

Fig 7. (a) Boat Cover Image and its Histogram (b) Boat Stego Image and its Histogram

The plotted histograms reveal similarity between original and stego images. Fig 3–7 suggest that, in the proposed embedding method, the disparities occurring due to embedding of secret message bitstreams are not noticeable in the stego image.
In addition, the differences occurring in histogram levels are reasonably insignificant, as shown in Fig 3 – 7. Hence, in the proposed scheme, the PSNR values as well as the visual appearance of the stego image and histogram suggestthat the distortion appearing after embedding of the secret message into the cover image is reasonablyless and imperceptible to human visual perception.

V. PERFORMANCE ANALYSIS

In this section, the experimental results are analyzed by two portions: embedding capacity and the PSNR values for stego image.

A. Embedding Capacity

The proposed method's embedding capacity can be considered depending on the number of components pairs

Embedding capacity of the proposed method is evaluated as follows:

$$\text{Capacity}_{\text{the proposed method}} = \sum_{i=1}^{n} p_i \qquad (1)$$

where,
p_i = the number of secret bits which can be embedded in a components pair
n = the number of components pairs

To compare the performance of the improved method and the existing method in terms of embedding capacity, the experiment is done on five test images: 'Lena', 'Babbon','Peppers', 'Boat' and 'Airplane'. According to the experimental results, the embedding capacity values of the improved method are higher than that of the the existing method as shown in Table 1.

In addition, the improvement of embedding capacity for the proposed embedding method over the existing method is also calculated as depicted in Table 1.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

TABLE I
IMPROVEMENT FOR EMBEDDING CAPACITY OF THE PROPOSED METHOD

Cover Image	Image Type	Image Size	Embedding Capacity (bytes)		Improvement for Embedding Capacity
			Existing Method [7]	Proposed Method	
Lena	JPEG	512 × 512	83654	239164	1.85
Boat	JPEG	512 × 512	84279	239789	1.84
Baboon	JPEG	512 × 512	91286	243588	1.66
Peppers	JPEG	512 × 512	78612	241636	2.07
Airplane	JPEG	512 × 512	81851	231881	1.83

According to the results in Table 1, the proposed method meets the higher embedding capacity requirement.

B. Peak Signal to Noise Ratio (PSNR)

Distortion analysis of stego images is carried out by studying distortion / similarity statistically. Distortion between two different images is measured by considering Mean Square Error (MSE), and PSNR (peak signal to noise ratio).

Usually, the invisibility of the hidden message is measured in terms of the Peak Signal-to-Noise Ratio. To analyze the quality of the embedded texture image, with respect to the original, the measure of PSNR has been employed.

$$PSNR = 10\log_{10}\frac{C_{\max}^{2}}{MSE} \quad (2)$$

where,
C_{max} = maximum pixels' value (255)
MSE = mean-squared-error

Note that PSNR ranging from 40 dB to 45 dB means that the quality degradations could hardly be perceived by a human eye.
Mean Square Error (MSE) is a measure used to quantify the difference between the cover image and the stego (distorted) image. If the image has a size of m × n then:

$$MSE = \left(\frac{1}{m \times n}\right)\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}(S_{ij} - C_{ij})^2 \quad (3)$$

where,
S_{ij} = The intensity value of the pixel in the stego-image.
C_{ij} = The intensity value of the pixel in the cover image.
$m \times n$ = Size of an Image.

When the payload increases, the MSE will increase, and this will affect the PSNR inversely. So, it was found that MSE decrease causes PSNR increase and vice-versa. PSNR is often expressed on a logarithmic scale in decibels (dB). PSNR values falling below 30 dB indicate a fairly low quality, i.e., distortion caused by embedding can be obvious; however, a high quality stego-image should strive for 40 dB and above.

The comparison result of the PSNR values of the proposed method and the existing method is shown in Table 2.

TABLE II
COMPARISON RESULT OF THE PSNR VALUES

Cover Image	Image Type	Image Size	PSNR (dB)	
			Existing method	Proposed Method
Lena	JPEG	512 × 512	45	56
Boat	JPEG	512 × 512	41	54
Baboon	JPEG	512 × 512	39	41
Peppers	JPEG	512 × 512	43	41
Airplane	JPEG	512 × 512	42	39

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 7, Issue 3, March 2018

IV. CONCLUSION

The proposed technique has its place in secured information hiding. The confidential message is embedded into an image file in such a manner that the degradation in quality of the carrier image is not noticeable. Thus, the proposed method allows users to send data through the network in a secured fashion. It can enhance confidentiality of information and provide a mean of communicating privately. The proposed method will provide acceptable image quality with very little distortion in the image. Experimental results show that the proposed method provides an average hiding capacity gain of 1.85 times over the existing method while maintaining acceptable stego image quality. This system can only embed the text files (.txt) which consists of alphanumeric characters. Among the image file formats, only JPEG image file format and PNG image file format are considered as a cover image in this paper. The proposed system can be effectively applied in various security awareness areas such as commercial, medical imaging and military communication systems and so on. As a further extension, the concept of proposed method can be extended for hiding other file format in any other cover image with various file formats and sizes.

ACKNOWLEDGMENT

I would like to express my deepest thanks to all my teachers and colleagues who lend a hand directly or indirectly during the arduous process of completing this work successfully. I also show admiration to my parents for their mental supporting.

REFERENCES

[1] K. Sullivan, Z. Bi, U. Madhow, S. Chandrasekaran and B. S. Manjunath, "Steganalysis of quantization index modulation data hiding," in Proc. IEEE, , p. 1165 - 1168,2004.
[2] Al-Qahtani A, Tabakh A, Gutub A. Triple-A: "secure RGB image steganography based on randomization," 7th ACS/IEEE Int. Conf. on Computer Systems and Applications (AICCSA-2009), Rabat, Morocco, pp. 400–403, 2009.
[3] V. Kumar and S. K. Muttoo, "A graph theoretic approach to sustainable steganography," MIS Review: An Int. Journal, vol. 17, pp. 19–37, 2010.
[4] Liao X,Wen Q-Y, Zhang J, "A steganographic method for digital images with four-pixel differencing and modified LSB substitution," pp.1–8. 2011. file
[5] Hsien-Wen Tseng "A Steganographic Method Based on Pixel-Value Differencing and the Perfect Square Number" Proceedings, Department of Information Management, Chaoyang University of Technology, No.168, JifengE. Road,Wufeng District, Taichung 41349,Taiwan, 2012.
[6] Hsien-Wen Tseng "A Steganographic Method Based on Pixel-Value Differencing and the Perfect Square Number" Proceedings, Department of Information Management, Chaoyang University of Technology, No.168, JifengE. Road,Wufeng District, Taichung 41349,Taiwan, 2012
[7] Nagaraj V, Vijayalakshmi V, Zayaraz G, "Color image steganography based on pixel value modification method using modulus function", Science Direct, Elsevier, Vol. 4, pp. 17–24, 2013. "PDCA12-70 data sheet," Opto Speed SA, Mezzovico, Switzerland.
[8] JagrutiSalunkhe, SumedhaSirsikarand MarathwadaMitraMandals, "Pixel Value Differencing a Steganographic method: A Survey," International Journal of Computer Applications, vol. 5, pp. 1711–1717, 2013.J. Padhye, V. Firoiu, and D. Towsley, "A stochastic model of TCP Reno congestion avoidance and control," Univ. of Massachusetts, Amherst, MA, CMPSCI Tech. Rep. 99-02, 1999.
[9] Chetna Mehto, RachanaKamble and Dr. BhupeshGour, "Investigation of digital image steganography: a survey," Int. J. Computer Technology and Applications, vol. 5, pp. 1711–1717, Sept- Oct. 2014.