Pixel Mapping Method (PMM) Based Bit Plane Complexity Segmentation (BPCS) Steganography

Souvik Bhattacharyya[1], Aparajita Khan,Aunkita Nandi,Aveek Dasmalakar,Somdip Roy[2] and Gautam Sanyal[3]
[1]Department of Computer Science and Engineering, University Institute of Technology
The University of Burdwan, West Bengal, India, e-mail: (souvik.bha@gmail.com)
[2]Department of Computer Science and Engineering, University Institute of Technology
The University of Burdwan West Bengal,India
e-mail: (friendapara@gmail.com,n.aunkita@gmail.com, adasmalakar@live.in)
[3]Department of Computer Science and Engineering, National Institute of Technology
West Bengal,India, e-mail: (nitgsanyal@gmail.com)

Abstract

Steganography is the art and science of communicating in a way which hides the existence of the communication. Important information is firstly hidden in a host data, such as digital image, text, video or audio, etc, and then transmitted secretly to the receiver.In this work the authors propose a new image based steganographic method for hiding information within the spatial domain of the gray scale image. The proposed method is based on pixel mapping method(PMM) for image data and bit-plane complexity segmentation (BPCS) steganography.The proposed approach works by selecting the embedding bit planes using some mathematical function and then applies the pixel mapping method (PMM) in a 8x8 blocks of the each selected plane. The integrated approach of PMM and BPCS produces a robust image based steganography method which is independent of the nature of the data to be hidden and produces a stego image with minimum degradation.The experimental results shows this method is sperior to other existing methods in terms of robustness and embedding capacity tradeoffs.

Keywords

Cover Image, Pixel Mapping Method (PMM), Stego Image,BPCS Steganography.

1. Introduction

To protect secret message from being stolen during transmission, there are two ways to solve this problem in general. One way is encryption, which refers to the process of encoding secret information in such a way that only the right person with a right key can decode and recover the original information successfully. Another way is steganography and this is a technique which hides secret information into a cover media or carrier so that it becomes unnoticed and less attractive.Capacity and invisibility are the benchmarks needed for data hiding techniques of steganography.A famous illustration of steganography is **Simmons' Prisoners' Problem** [19]. An assumption can be made based on this model is that if both the sender and receiver share some common secret information then the corresponding steganography protocol is known as then the secret key steganography where as pure steganography means that there is none prior information shared by sender and receiver. If the public key of the receiver is known to the sender, the steganographic protocol is called public key steganography [1], [2] and [9].For a more thorough knowledge of steganography methodology the reader may see [17], [21].Some Steganographic model with high security features has been presented in [3], [4] and [5].Almost all digital file formats can be used for steganography, but the image and audio files are more suitable because of their high degree of redundancy [21]. Fig. 1 below shows the different categories of steganography techniques.

Fig. 1. Types of Steganography

A block diagram of a generic image steganographic system is given in Fig. 2.

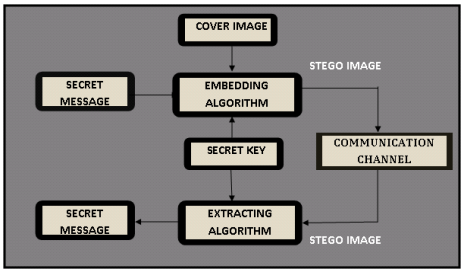

Fig. 2. Generic form of Image Steganography

A message is embedded in a digital image (cover image) through an embedding algorithm, with the help of a secret key.

The resulting stego image is transmitted over a channel to the receiver where it is processed by the extraction algorithm using the same key. During transmission the stego image, it can be monitored by unauthenticated viewers who will only notice the transmission of an image without discovering the existence of the hidden message. In this work a specific image based steganographic method for gray level image has proposed. In this method instead of embedding the secret message into the cover image a mapping technique has been incorporated to generate the stego image. This method is capable of extracting the secret message without the presence of the cover image.

This paper has been organized as following sections: Section II describes some related works, Section III deals with proposed method. Algorithms are discussed in Section IV and Experimental results are shown in Section V. Section VI contains the analysis of the results and Section VII draws the conclusion.

2. Related Works

2.1. Data Hiding by LSB

Various techniques about data hiding have been proposed in literatures. One of the common techniques is based on manipulating the least-significant-bit (LSB) [7], [8] and [15], [18]planes by directly replacing the LSBs of the cover-image with the message bits. LSB methods typically achieve high capacity but unfortunately LSB insertion is vulnerable to slight image manipulation such as cropping and compression.

2.2. Data Hiding by PVD

The pixel-value differencing (PVD) method proposed by Wu and Tsai [22] can successfully provide both high embedding capacity and outstanding imperceptibility for the stego-image. The pixel-value differencing (PVD) method segments the cover image into non overlapping blocks containing two connecting pixels and modifies the pixel difference in each block (pair) for data embedding. A larger difference in the original pixel values allows a greater modification. In the extraction phase, the original range table is necessary. It is used to partition the stego-image by the same method as used to the cover image. Based on PVD method, various approaches have also been proposed. Among them Chang et al. [14]. proposes a new method using tri-way pixel-value differencing which is better than original PVD method with respect to the embedding capacity and PSNR.

2.3. Data Hiding by GLM

In 2004, Potdar et al.[10] proposes GLM (Gray level modification) technique which is used to map data by modifying the gray level of the image pixels. Gray level modification Steganography is a technique to map data (not embed or hide it) by modifying the gray level values of the image pixels. GLM technique uses the concept of odd and even numbers to map data within an image. It is a one-to-one mapping between the binary data and the selected pixels in an image. From a given image a set of pixels are selected based on a mathematical function. The gray level values of those pixels are examined and compared with the bit stream that is to be mapped in the image.

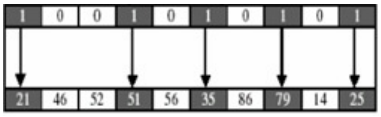

Fig. 3. Data Embedding Process in GLM

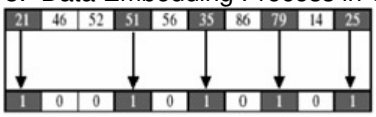

Fig. 4. Data Extraction Process in GLM

3. BPCS Steganography

BPCS (Bit-Plane Complexity Segmentation) steganography was introduced by Eiji Kawaguchi and Richard O. Eason [11] ,to overcome the short comings of traditional steganographic techniques like Least Significant Bit (LSB) technique, Transform domain embedding technique. The important aspect of BPCS-Steganography compared to those methodology is that the embedding capacity is very large.BPCS steganography makes use of important characteristic that of human vision. In BPCS, the vessel image is divided into informative region and noise-like region and the secret data is hidden in noise blocks of vessel image without degrading image quality [11], [16]. In LSB technique, data is hidden in last four bits i.e. only in the 4 LSB bits[13]. But in BPCS technique, data can also be hidden in MSB planes along with the LSB planes provided secret data is hidden in complex region [11].

3.1. Basic Principle of BPCS Steganography

In BPCS, a multi-valued image (P) consisting of n-bit pixels can be decomposed into set of n binary pictures. Example: P is an n-bit gray image say n=8. Therefore P = [P7 P6 P5 P4 P3 P2 P1 P0] where P7 is the MSB bit plane and P0 is the LSB bit plane. Each bit plane can be segmented into informative and noise region. An informative region consists of simple pattern while noise-like region consists of complex pattern. In BPCS, each noise-looking region is replaced with another noise-looking pattern without changing the overall image quality.Thus, BPCS steganography makes use of this nature of human vision system [16], [12].

4. Pixel Mapping Method(PMM)

Pixel Mapping Method [6], [20] is a method for information hiding within the spatial domain of any gray scale

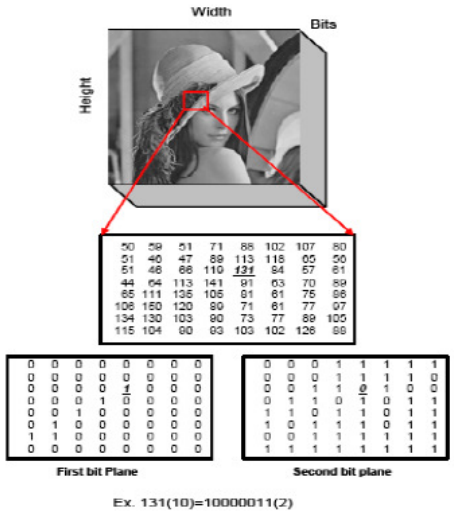

Fig. 5. Bit Plane Slicing concept considering pixel having value 131.

image.Embedding pixels are selected based on some mathematical function which depends on the pixel intensity value of the seed pixel and its 8 neighbors are selected in counter clockwise direction. Before embedding a checking has been done to find out whether the selected embedding pixels or its neighbors lies at the boundary of the image or not. Data embedding are done by mapping each two or four bits of the secret message in each of the neighbor pixel based on some features of that pixel. Figure 6 and Figure 7 shows the mapping information for embedding two bits or four bits respectively.

PAIR OF MSG BIT	PIXEL INTENSITY VALUE	NO OF ONES (BIN)
01	EVEN	ODD
10	ODD	EVEN
00	EVEN	EVEN
11	ODD	ODD

Fig. 6. PMM Mapping Technique for embedding of two bits

Extraction process starts again by selecting the same pixels required during embedding. At the receiver side other different reverse operations has been carried out to get back the original information.

5. Proposed Data Embedding Method

In this image based steganographic approach, the secret message is embedded though pixel mapping method into the highly complex bit planes or noisy bit planes of the cover image. The proposed approach works by selecting the embedding bit planes using some mathematical function and then applies the pixel mapping method (PMM) in a 8x8 blocks of the each

MSG BIT SEQ	2nd SET – RESET BIT	3rd SET – RESET BIT	PIXEL INTENSITY VALUE	NO OF ONES(BIN)
0000	EVEN	EVEN	EVEN	EVEN
0001	EVEN	EVEN	EVEN	ODD
0010	EVEN	EVEN	ODD	EVEN
0011	EVEN	EVEN	ODD	ODD
0100	EVEN	ODD	EVEN	EVEN
0101	EVEN	ODD	EVEN	ODD
0110	EVEN	ODD	ODD	EVEN
0111	EVEN	ODD	ODD	ODD
1000	ODD	EVEN	EVEN	EVEN
1001	ODD	EVEN	EVEN	ODD
1010	ODD	EVEN	ODD	EVEN
1011	ODD	EVEN	ODD	ODD
1100	ODD	ODD	EVEN	EVEN
1101	ODD	ODD	EVEN	ODD
1110	ODD	ODD	ODD	EVEN
1111	ODD	ODD	ODD	ODD

Fig. 7. PMM Mapping Technique for embedding of four bits

selected plane. The integrated approach of PMM and BPCS produces a robust image based steganography method which is independent of the nature of the data to be hidden and produces a stego image with minimum degradation.The experimental results shows this method is superior to other existing methods in terms of robustness and similarity measures between cover image and stego image.

6. Algorithms

In this section, algorithms for different processes used both in the sender side and receiver side are described.

6.1. Data Embedding Method

- Slice Cover Image into 8-bit planes of [b1,b2,b3,b4,b5,b6,b7,b8] where b1 represents the highest bit plane and b8 representing the lowest bit plane.
- Compute the complexity (alpha) of each bit plane from b1 to b8.
- Compute the threshold complexity for the planes.
- Fetch the higher complexity planes(that is bit planes with complexity greater than threshold complexity).
- Convert the entire secret text message into 8-bit binary form and divide the entire binary message into a sequence of 2-bit binary stream.
- Divide the a high complexity bit plane into 32X32 blocks which again partitioned into 8X8 binary blocks. Thus partitioning the entire image into 8X8 binary blocks.
- Each of the 2-bit binary bit stream is embedded into each 1X8 binary image data blocks of higher complex plane using 2-bit embedding method of Pixel Mapping Method(PMM).
- Merge all the 8X8 changed and unchanged binary blocks to get the modified bit plane.

- Repeat steps 7 - 9 until all the secret message characters have been embedded.
- Merge all the bit planes [b1,b2,b3,b4,b5,b6,b7,b8] to get the stego-image.

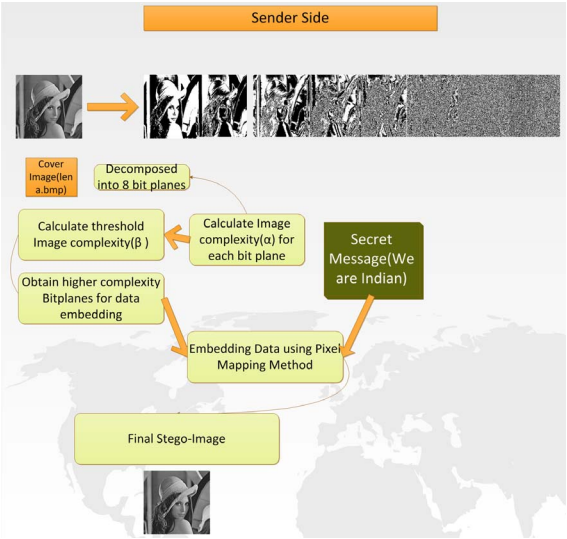

Fig. 8. Block Diagram of Sender Side System

6.2. Data Extraction Method

- Slice the stego image into 8-bit planes of [b1,b2,b3,b4,b5,b6,b7,b8] where b1 represents the highest bit plane and b8 representing the lowest bit plane.
- Find the embedded bit planes and divide them into 8X8 binary blocks.
- Access each 8X8 block and apply extraction method of PMM(2 Bit) to get back the embedded bits.
- Arrange the bits obtained in proper order to get back the secret message.

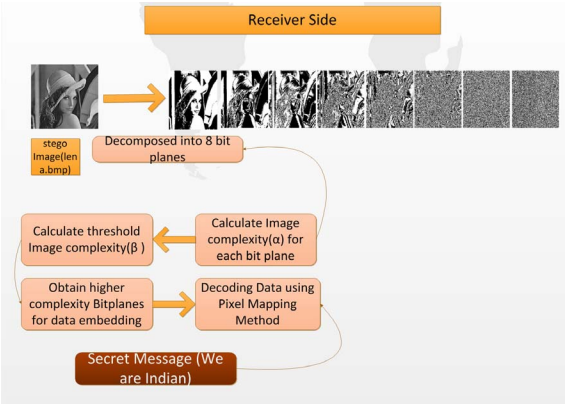

Fig. 9. Block Diagram of Receiver Side System

6.3. Embedding Plane Selection Method

- Consider 4-connectivity of pixels and compute the black-and- white border,defined as the sum of the color changes along the rows and columns in the image.
- Border length can be computed as : say,a single white pixel surrounded by 4 black pixels, i.e., having all its 4-connected neighbors as black pixels, will have a border length of 4 (2 color changes each along the rows and columns).
- For a square binary image of size $2^N * 2^N$, the minimum border length possible is 0, obtained for an all-white or all-black image, and the maximum border length possible is $2 * 2^N * (2^N - 1)$.
- Compute image complexity measure, a, is then defined as the normalized value of the total length of the black and white border in the image, i.e. ,$0 \leq k \leq 2*2^N*(2^N-1)$ here k is the actual length of the black and white border in the image. It is evident that α lies in [0, 1].
- β is the average complexity of all the 8 bit-planes.
- Select those bit planes whose complexities (α) are greater than average complexity (β).

7. Experimental Results

In this section the authors present the experimental results of the proposed method based on two benchmarks techniques to evaluate the hiding performance. First one is the capacity of hiding data and another one is the imperceptibility of the stego image, also called the quality of stego image. The quality of stego-image should be acceptable by human eyes. The authors also present a comparative study of the proposed methods with the existing methods like PVD,GLM and PMM(2 bit) by computing embedding capacity, mean square error (MSE) and peak signal-to noise ratio(PSNR).The authors also compute the normalized cross correlation coefficient for computing the similarity measure between the cover image and stego image.A comparison of the embedding capacity has been illustrated in figure 10.

IMAGE	IMAGE SIZE	PVD	GLM	PMM(2 bit)	PMM BPCS
LENA	128x128	**	2048	2393	2048
	256x256	**	8192	10012	8192
	512x512	50960	32768	45340	32768
PEPPER	128x128	**	2048	2860	2048
	256x256	**	8192	11694	8192
	512x512	50685	32768	46592	32768

Fig. 10. Comparision of embedding capacity(** For PVD method all the images used are of size 512x512.)

Fig. 11. A) Bit Plane 1 of Lena before embedding B) Bit Plane 1 of Lena after embedding C) Bit Plane 2 of Lena before embedding D) Bit Plane 2 of Lena after embedding.

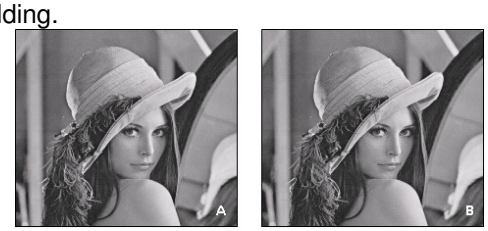

Fig. 12. A) Cover Image B) Stego Image of Lena after embedding 32678 character

7.1. Peak Signal to Noise Ratio (PSNR)

PSNR measures the quality of the image by comparing the original image or cover image with the stego-image, i.e. it measures the percentage of the stego data to the image percentage.The PSNR is used to evaluate the quality of the stego-image after embedding the secret message in the cover. Assume a cover image C(i,j) that contains N by N pixels and a stego image S(i,j) where S is generated by embedding / mapping the message bit stream. Mean squared error (MSE) of the stego image as follows:

$$MSE = \frac{1}{[N \times N]} \sum_{i=1}^{N} \sum_{j=1}^{N} [C(ij) - S(ij)]^2$$

The PSNR is computed using the following formulae:

$$PSNR = 10 \log_{10} 255^2 / \ MSE \ db.$$

A comparative study of PSNR of various methods has been illustrated in figure 13.

7.2. Similarity Measure

For comparing the similarity between cover image and the stego image, the normalized cross correlation coefficient (r) has been computed. In statistics, correlation indicates the strength and direction of a linear relationship between two random variables. The value of correlation is 1 in the case of an increasing linear relationship, -1 in the case of a decreasing linear relationship, and some value in between in all other cases, indicating the degree of linear dependence between the variables.

Image	GLM	PVD	PMM(2 bit)	PMMBPCS
Lena(128X128)	30.6	38.6	54.15	36.8707
Lena(256X256)	33.8	35	50.34	37.0794
Lena(512X512)	35.2	33.8	49.02	36.9760
Pepper(128X128)	39.1	39	54.15	36.5712
Pepper(256X256)	37.8	35	48.36	37.8785
Pepper(512X512)	34.6	32.7	47.94	36.1794

Fig. 13. Comparision of PSNR

Cross correlation is a standard method of estimating the degree to which two series are correlated. Consider two series x(i) and y(i) where i=0,1,2,. . . ,N-1. The cross correlation r at delay d is defined as

$$r = \frac{\sum_i [(x(i) - mx)(y(i-d) - my)]}{\sqrt{\sum_i (x(i) - mx)^2} \sqrt{\sum_i (y(i-d) - my)^2}}$$

where mx and my are the means of the corresponding series.

Similarity measure of two images can be done with the help of normalized cross correlation generated from the above concept using the following formula:

$$r = \frac{\sum_{(C(i,j)-m_1)(S(i,j)-m_2)}}{\sqrt{(\sum_{C(i,j)-m_1})^2} \sqrt{(\sum_{S(i,j)-m_2})^2}}$$

Here C is the cover image, S is the stego image,m_1 is the mean pixel value of the cover image and m_2 is the mean pixel value of stego image. It has been seen that the correlation coefficient computed here for all the images is almost one which indicates the both the cover image and stego image are of highly correlated i.e. both of these two images are same.

8. Analysis of the Results

In this article the authors proposes an efficient image based steganography approach for hiding information in a gray scale image through the integrated approach of PMM(2 bit) with BPCS. Comparison has been shown with some of the existing methods like PVD, GLM and also with PMM(2bit).From the experimental results in can be seen that although the embedding capacity of the proposed method is less compared to PVD and PMM(2bit) as all the bit planes of the cover image is not suitable for embedding.With the computation of cross-correlation coefficient for measuring the similarity between the cover image and stego image, this method gives an excellent result.Besides PSNR value of the proposed method for various size of the image this better in most cases compared to PVD and GLM technique.As the message bits are not

Images		100	500	1000	2000	5000	10000	20000
Lena 512X512	PSNR	76.2632	69.460	66.2954	61.51	59.30	53.82	45.034
	MSE	0.0015	0.0078	0.0153	0.046	0.076	0.269	2.04
	Correlation	1.00	1.00	0.99	0.99	0.99	0.998	0.998
Lena 256X256	PSNR	73.3406	64.55	60.3011	51.93	45.253	NA	NA
	MSE	0.0060	0.28	0.0607	0.4163	1.938	NA	NA
	Correlation	1.00	1.00	0.99	0.99	0.99	NA	NA
Lena 128X128	PSNR	64.3532	57.445	49.5831	36.34	NA	NA	NA
	MSE	0.0239	0.123	0.7158	15.09	NA	NA	NA
	Correlation	0.99	1.00	0.99	0.99	NA	NA	NA
Pepper 512X512	PSNR	76.1567	69.2605	66.1831	63.252	59.321	53.89	45.027
	MSE	0.0016	0.0077	0.0157	0.0308	0.0760	0.2650	2.043
	Correlation	1.00	1.00	1.00	1.00	1.00	1.00	0.99
Pepper 256X256	PSNR	70.318	63.355	60.353	57.30	45.340	NA	NA
	MSE	0.006	0.03	0.599	0.1210	1.9012	NA	NA
	Correlation	1.00	1.00	1.00	1.00	0.99	NA	NA
Pepper 128X128	PSNR	64.011	57.217	49.47	36.611	NA	NA	NA
	MSE	0.0258	0.123	0.7370	14.187	NA	NA	NA
	Correlation	1.00	1.00	0.99	0.99	NA	NA	NA

Fig. 14. Results of PMM(BPCS) at a glance

directly embedded/mapped at the pixels of the cover image like PMM(2 bit) PMM(BPCS) method can be considered as more robust technique compared to PMM(2 bit).

9. Conclusion

The work dealt with the techniques for steganography as related to gray scale image. A new and efficient steganographic method for embedding secret messages into images without producing any major changes has been proposed. Although in this method it has been shown that each two bit of the secret message has been mapped in each 8x8 sub planes of the cover image,but this method can be extended to map n no of bits in the selected bit planes in order to increase the embedding capacity.This method also capable of extracting the secret message without the cover image.

References

[1] RJ Anderson. Stretching the limits of steganography. *Information Hiding, Springer Lecture Notes in Computer Science*, 1174:39–48, 1996.

[2] Ross J. Anderson. and Fabien A.P.Petitcolas. On the limits of steganography. *IEEE Journal on Selected Areas in Communications (J-SAC), Special Issue on Copyright and Privacy Protection*, 16:474–481, 1998.

[3] Souvik Bhattacharyya. and Gautam Sanyal. Study of secure steganography model. In *Proceedings of International Conference on AdvancedComputing and Communication Technologies (ICACCT-2008)*, Panipath,India, 2008.

[4] Souvik Bhattacharyya. and Gautam Sanyal. An image based steganography model for promoting global cyber security. In *Proceedings of International Conference on Systemics, Cybernetics and Informatics*, Hyderabad,India, 2009.

[5] Souvik Bhattacharyya. and Gautam Sanyal. Implementation and design of an image based steganographic model. In *Proceedings of IEEE International Advance Computing Conference*, Patiala ,India, 2009.

[6] Souvik Bhattacharyya. and Gautam Sanyal. Hiding data in images using pixel mapping method (pmm). In *Proceedings of 9th annual Conference on Security and Management (SAM) under The 2010 World Congress in Computer Science,Computer Engineering, and Applied Computing(WorldComp 2010)*, LasVegas,USA, July 12-15,2010.

[7] J.Y. Hsiao. C.C. Chang. and C.-S. Chan. Finding optimal least-significant-bit substitution in image hiding by dynamic programming strategy. *Pattern Recognition*, 36:1583–1595, 2003.

[8] C.K. Chan. and L. M.Cheng. Hiding data in images by simple lsb substitution. *Pattern Recognition*, 37:469–474, 2004.

[9] Scott. Craver. On public-key steganography in the presence of an active warden. In *Proceedings of 2nd International Workshop on Information Hiding.*, pages 355–368, Portland,Oregon, USA, 1998.

[10] Potdar V.and Chang E. Gray level modification steganography for secret communication. In *IEEE International Conference on Industria lInformatics.*, pages 355–368, Berlin, Germany, 2004.

[11] Richard O. Eason. Eiji Kawaguchi. Principle and applications of bpcs-steganography. *Proc. of SPIE, 3528, pp.464-473*, 1998.

[12] Shrikant Khaire et. al. Review: Steganography bit plane complexity segmentation (bpcs)technique. *International Journal of Engineering Science and Technology,Vol. 2(9), 2010, 4860-4868*, 2010.

[13] A. Habes. 4 least significant bits information hiding implementation and analysis. *GVIP 05 Conference, CICC,Cairo, Egypt*, 2005.

[14] P Huang. K.C. Chang., C.P Chang. and T.M Tu. A novel image steganography method using tri-way pixel value differencing. *Journal of Multimedia*, 3, 2008.

[15] Y. K. Lee. and L. H.Chen. High capacity image steganographic model. *IEE Proc.-Vision, Image and Signal Processing*, 147:288–294, 2000.

[16] Hideki Noda Michiharu Niimi and Eiji Kawguchi. A steganography based on region segmentation by using complexity measure. *Trans. of IEICE, J81-D-II, pp.1132-1140*, 1998.

[17] N.F.Johnson. and S. Jajodia. Steganography: seeing the unseen. *IEEE Computer*, 16:26–34, 1998.

[18] C.F. Lin. R.Z. Wang. and J.C. Lin. Image hiding by optimal lsb substitution and genetic algorithm. *Pattern Recognition*, 34:671–683, 2001.

[19] Gustavus J. Simmons. The prisoners' problem and the subliminal channel. *Proceedings of CRYPTO.*, 83:51–67, 1984.

[20] Lalan Kumar Souvik Bhattacharyya and Gautam Sanyal. A novel approach of data hiding using pixel mapping method (pmm). *INTERNATIONAL JOURNAL OF COMPUTER SCIENCE AND INFORMATION SECURITY(IJCSIS)*, 8, 2010.

[21] JHP Eloff. T Mrkel. and MS Olivier. An overview of image steganography. In *Proceedings of the fifth annual Information Security South Africa Conference.*, 2005.

[22] D.C. Wu. and W.H. Tsai. A steganographic method for images by pixel-value differencing. *Pattern Recognition Letters*, 24:1613–1626, 2003.