Volume 3, No. 9, September 2012

Journal of Global Research in Computer Science

ISSN-2229-371X

RESEARCH PAPER

Available Online at www.jgrcs.info

HIGHLY SECURED AND RANDOMIZED IMAGE STEGANOGRAPHIC ALGORITHM

Dr. R.Sridevi
Associate Professor Department of Computer Science and Engineering
JNTUH College of Engineering, JNTUH, Hyderabad
sridevirangu@yahoo.com

Abstract: In today's internet scenario, secured data transfer is very difficult if not impossible due to the technology and computing power availability to the attackers. Hence more robust methods are required to provide a secured data transfer. Though steganographic algorithms are existing, no algorithm is fool proof for long time, as hackers gain more knowledge over time [1]. In this proposed work, a new technique to improve the security of steganographic algorithm by using the high level of randomization is proposed and implemented. It has the high embedding capacity and more robustness in the stego key.

In proposed algorithm, message to be transmitted is encrypted. The encrypted message is embedded on image in randomized pixels. The randomness of the position of pixels on which the encrypted message to be embedded will be decided by the stego key. The stego key itself is encrypted and transmitted to other party in a secured form. Hence it is more robust and secured algorithm. The algorithms used for steganography process is Pixel Value Differencing with Modulus (PVDM) [6] and Least Significant Bit(LSB) algorithms[5] with randomization.

Keywords: LSB, AES, RSA

INTRODUCTION

Here we are using the following two algorithms:

LSB Algorithm:

A simple and well known approach is to directly hide secret data into the least-significant bit (LSB) of each pixel in an image. Many modifications have been proposed to this LSB algorithm [11].

The proposed method uses a stego key to determine the pixels to embed the data bits (contrary to LSB of each pixel), thus provides more random spread of data.

Pixel Value Differencing with Modulus Function Algorithm:

In 2008 C.-M. Wang et al. proposed a refined version of Wu and Tsai scheme, Pixel Value Differencing with Modulus function [6]. In this method the modulus of two consecutive pixels is modified to embed the secret data instead of the difference of the pixel values.

The given image is scanned in a zigzag manner to obtain the pixels. Blocks of two consecutive pixels are obtained. Given a sub-block F_i composed of two continuous pixels $P_{(i,x)}$ and $P_{(i,y)}$ from the cover image, obtain the difference value d_i, the sub-range R_i such that R_i belongs to $[l_i,u_i]$, the width $w_i = u_i – l_i + 1$, the hiding capacity t_i bits, and the decimal value v of t_i for each $F_{i.}$ Where l_i is lower limit and u_i is upper limit of the Range R_i.

The remainder values $P_{rem(i,x)}$, $P_{rem(i,y)}$ and $F_{rem(i)}$ of $P_{(i,x)}$, $P_{(i,y)}$ of sub-block F_i are computed respectively by using the following equations:

$$P_{rem(i,x)} = P_{(i,x)} \bmod w_i$$

$$P_{rem(i,y)} = P_{(i,y)} \bmod w_i$$

$$F_{rem(i)} = (P_{(i,x)} + P_{(i,y)}) \bmod w_i$$

Where w_i is the width of the suitable range.

t_i bits of secret data are embedded into sub block F_i by altering $P_{(i,x)}$ and $P_{(i,y)}$ such that $F_{rem(i)} = v$. The optimal approach to alter the $P_{(i,x)}$ and $P_{(i,y)}$ to achieve the minimum distortion is as follows:

case 1: $F_{rem(i)} > v$ and $m \le (2^{t_i}/2)$ and $P_{(i,x)} \ge P_{(i,y)}$

$$P'_{(i,x)}= P_{(i,x)} – \text{ceil}\ (m/2)$$
$$P'_{(i,y)}= P_{(i,y)} – \text{floor}\ (m/2)$$

case 2: $F_{rem(i)} > v$ and $m \le (2^{t_i} / 2)$ and $P_{(i,x)} < P_{(i,y)}$

$$P'_{(i,x)}= P_{(i,x)} – \text{floor}\ (m/2)$$
$$P'_{(i,y)}= P_{(i,y)} – \text{ceil}\ (m/2)$$

case 3: $F_{rem(i)} > v$ and $m > (2^{t_i} / 2)$ and $P_{(i,x)} \ge P_{(i,y)}$

$$P'_{(i,x)}= P_{(i,x)} + \text{floor}\ (m_1/2)$$
$$P'_{(i,y)}= P_{(i,y)} + \text{ceil}\ (m_1/2)$$

case 4: $F_{rem(i)} > v$ and $m > (2^{t_i} / 2)$ and $P_{(i,x)} < P_{(i,y)}$

$$P'_{(i,x)}= P_{(i,x)} + \text{ceil}\ (m_1/2)$$
$$P'_{(i,y)}= P_{(i,y)} + \text{floor}\ (m_1/2)$$

case 5: $F_{rem(i)} \le v$ and $m \le (2^{t_i} / 2)$ and $P_{(i,x)} \ge P_{(i,y)}$

$$P'_{(i,x)}= P_{(i,x)} + \text{floor}\ (m/2)$$
$$P'_{(i,y)}= P_{(i,y)} + \text{ceil}\ (m/2)$$

case 6: $F_{rem(i)} \le v$ and $m \le (2^{t_i} / 2)$ and $P_{(i,x)} < P_{(i,y)}$

$$P'_{(i,x)}= P_{(i,x)} + \text{ceil}\ (m/2)$$
$$P'_{(i,y)}= P_{(i,y)} + \text{floor}\ (m/2)$$

case 7: $F_{rem(i)} \le v$ and $m > (2^{t_i} / 2)$ and $P_{(i,x)} \ge P_{(i,y)}$

$$P'_{(i,x)}= P_{(i,x)} – \text{ceil}\ (m_1/2)$$
$$P'_{(i,y)}= P_{(i,y)} – \text{floor}\ (m_1/2)$$

case 8: $F_{rem(i)} \le v$ and $m > (2^{t}_{i} / 2)$ and $P_{(i,x)} < P_{(i,y)}$
$P'_{(i,x)} = P_{(i,x)} - \text{floor}\ (m_1/2)$
$P'_{(i,y)} = P_{(i,y)} - \text{ceil}\ (m_1/2)$

Here $m = |F_{rem(i)} - v|$ and $m_1 = 2^{t}_{i} - |F_{rem(i)} - v|$

Falling – off - Boundary Problem:

Whenever the modified pixel values fall beyond the boundaries 0-255, consider that situation as Falling-Off-Boundary problem. The following two situations are considered for the Falling-Off-Boundary problem.

case 1:

If $P_{(i,x)} \approx 0$, $P_{(i,y)} \approx 0$ and $P'_{(i,x)} < 0$ or $P'_{(i,y)} < 0$
then $P'_{(i,x)} = P'_{(i,x)} + 2^{ti}/2$
and $P'_{(i,y)} = P'_{(i,y)} + 2^{ti}/2$

case 2:

If $P_{(i,x)} \approx 255, P_{(i,y)} \approx 255$ and $P'_{(i,x)} > 255$ or $P'_{(i,y)} > 255$
then $P'_{(i,x)} = P'_{(i,x)} - 2^{ti}/2$
and $P'_{(i,y)} = P'_{(i,y)} - 2^{ti}/2$

Extraction Scheme:

In recovery process, the secret data can be extracted without using the original image. Nevertheless, it is essential to use the original range table R designed in the embedding phase inorder to figure out the embedding capacity for each sub-block F_i. Given a sub-block F_i with two consecutive pixels from the stego-image with their pixel values being $P_{(i,x)}$ and $P_{(i,y)}$ respectively, the difference value d_i of $P_{(i,x)}$ and $P_{(i,y)}$ is computed. Each F_i can be related to its optimal sub-range R_i from the original table R according to the difference value d_i. Hence, the width of the sub-range can be calculated as $w_i = u_i - l_i$, and the number of bits t_i of the secret data can be extracted from F_i by equation

$$t_i = \text{floor}\ (\log_2 |w_i|)$$

Eventually, compute the remainder value of Fi by using Equation

$$F_{rem(i)} = (P_{(i,x)} + P_{(i,y)}) \bmod w_i$$

And transform the remainder value $F_{rem(i)}$ into a binary string with the length t_i. $F_{rem(i)}$ is nothing but decimal value to be extracted.

PROPOSED SYSTEM

Though many steganographic algorithms are available, none of them is completely randomized. Since all steganographic algorithms are public, once if an attacker suspects message bits on the stego image, the attacker can try all the possible methods of deciphering existing algorithms (brute force) to extract message bits.

Sender's side Process:

In proposed method, the pixels of the carrier file, in which original message bits are stuffed is completely random and is decided by the stego key. The stego key inturn is transmitted to the other party after encrypting with the public key algorithm like RSA.

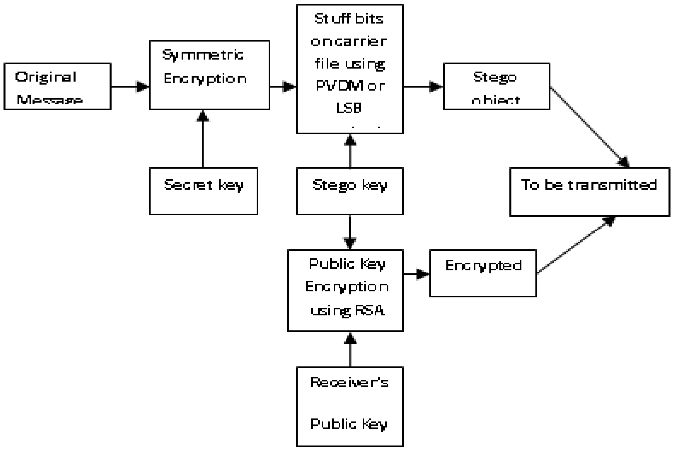


Figure 1: Proposed system – Sender's side

Figure 1 explains the proposed algorithm from sender's side as follows:

a. Original message to be transmitted is encrypted using the symmetric encryption algorithm like AES.
b. Secret key used for encrypting the message is one of the fields in stego key.
c. Depending on the stego key shown in Table 1, find which pixels of the cover image or carrier image are used to stuff the encrypted data bits.
d. Find the pixel value difference between the two pixels in carrier image and this difference is compared with threshold value.
e. Depending on this comparison, it considers either the LSB algorithm or the PVDM algorithm for the steganography process.
f. The stego key provides high level of randomness. Now stuffed image or stego image is transmitted on the channel along with the encrypted stego key.
g. The stego key is encrypted using any public key algorithm like RSA.

Stego Key:

Table 1: Structure of Stego key

Total number of parts of an image	At which part of the pixel stuffing starts	Position of the start pixel	Inter pixel distance	Secret key

Receiver's side Process:

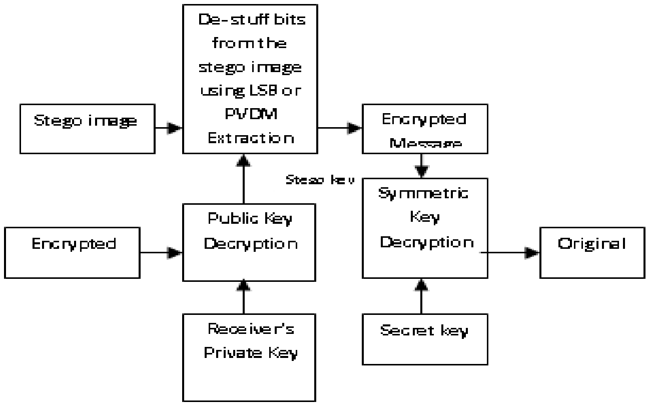


Figure 2: Proposed system – Receiver's Side

Figure 2 presents the block diagram of the proposed system on receiver's side. Encrypted Stego key and the stego object are received by the receiver. Stego key must be decrypted and retrieved with the receiver's private key. De-stuff the encrypted form of message bits using the parameter values in the stego key.

These bits can be decrypted using the secret key (which is one of the parameter in stego key) inorder to get the original message bits at the receiver's end.

Below are the steps for the proposed algorithm to improve the security by randomization given by stego key:

a. Initially cover image having a resolution of 512 x 512 is taken and array of pixels with dimension 500 x 500 is considered for computational simplicity to divide an image as equal size of parts. The total number of parts an image is divided into is the first field of the stego key.
b. The part of the cover image at which the encrypted bits are to be stuffed is decided by second field of stego key.
c. Pixel position, at which stuffing of secure data bits starts in that corresponding image part, is given in third field of stego key.
d. The inter pixel distance between the pixels is fourth field of stego key.

Considering all these random variables, the position of the bits to be stuffed in the cover image is decided. Exchange of key can be achieved through various methods not just limited to network.

Table 2: Range Table

Ranges	Range (R)	Width (W)	No. of bits that can be embedded (t)
R0	0-7	8	3
R1	8-15	8	3
R2	16-31	16	4
R3	32-63	32	5
R4	64-127	64	6
R5	128-255	128	7

Once after deciding, instead of using the simple steganographic techniques, the proposed method uses the combination of methods, either the PVDM or 3-bit LSB method depending on the inter pixel value difference.

The proposed algorithm provides improvement of stuffing capacity. In PVDM method, the pixel pairs are classified as smooth area pixels, where the pixel value difference is small and edge area pixels, where the pixel value difference is large. It can be realized that the number of pixel pairs in smooth areas is considerable in amount.

Inorder to improve the capacity of the technique, these smooth area pixels can be used for embedding secret data using LSB replacement method, which accommodates more number of bits. PVDM method is used for the pixel pairs in edge areas.

PVDM method:

Consider a pixel pair in smooth area with values 32, 34.
The difference is 2.
The range suitable is [0, 7] from the range table is given in table (3.2).
Width of range [0, 7] is 8 = 2^3.
Number of original data bits that can be stuffed are 3.

If 3-bit LSB method is used in smooth area, a total of 6 bits can be embedded in those two pixels with acceptable distortion.

A threshold value is determined for the pixel value difference to decide whether to use LSB or PVDM method i.e., if difference in value less than the threshold, they are considered to be in smooth area, other wise they are considered to be in edge area. When the difference between the pair of pixels is more than the threshold, PVDM is used.

Illustration:

Consider another pair 246, 100.
d_i= |246-100| =146 > threshold so PVDM method should be applied
Select the appropriate range from the range table (3.2) which is chosen by user.
i.e. [128,255]
The width of the range W_i = 128= 2^7
Hence the number of data bits can be stuffed are 7,
Let the 7 secret data bits are 1011100
The decimal value of the secret data v= 92
Calculate $F_{rem(i)}$ with the following formula.

$F_{rem(i)}$ = ($P_{(i,x)}$ + $P_{(i,y)}$) mod W_i = 246+100 mod 128 =90

m =|F_{rem} - v| =|90-92|=2
From the above given criterion in case 5
The new values are 247 and 101.

LSB replacement method:

This method is one of the best known and simple steganographic algorithms. When the pixel value difference of a pair is less than the assumed threshold, LSB method is used which is described in the following steps.

Step 1: Read six bits from the secret data stream.

S= [m1 m_2 m_3 m_4 m_5 m_6].

Step 2: Convert the decimal pixel values $P_{(i,x)}$ and $P_{(i,y)}$ into binary values.
Step 3: Replace 3-LSB of $P_{(i,x)}$ with m_1 m_2 m_3.
Step 4: Replace 3-LSB of $P_{(i,y)}$ with m_4 m_5 m_6.
Step 5: Convert the binary values $P_{(i,x)}$ and $P_{(i,y)}$ into decimal values.
Step 6: Calculate the pixel value difference d_i=| $P_{(i,x)}$ - $P_{(i,y)}$ |.
Step 7: If di > threshold value, then re-modify $P_{(i,x)}$ and $P_{(i,y)}$ as per the following criterion.

$P_{(i,x)} = P_{(i,x)} - 8$ and $P_{(i,y)} = P_{(i,y)} + 8$ if $P_{(i,x)} \geq P_{(i,y)}$

$P_{(i,x)} = P_{(i,x)} + 8$ and $P_{(i,y)} = P_{(i,y)} - 8$ if $P_{(i,x)} < P_{(i,y)}$

Step 8: If di ≤ threshold value, the final values are $P_{(i,x)}$ and $P_{(i,y)}$.

Illustration:

Let the pixel pair be 32 and 34, and threshold value 15

d_i= |32-34| =2 < threshold so LSB should be applied
Let the 6 bits of secret data be 110011
The binary value of 32 = 00100000
The binary value of 34= 00100010
3-bit LSB replacement of first pixel 00100***110*** (the substituted bits are emphasized).
3-bit LSB replacement of Second pixel is 00100***011.***
The decimal value of first pixel is 00100***110 =*** 38.
The decimal value of first pixel is 00100***011 =*** 35.
The new difference is |38-35|=3< threshold value.
So the new values are 38 & 35.

The original Pixel values of cover image are considered are (246,100).The stego pixel values of the cover image after stuffing 7bits of secret bits are (247,101). Hence without much difference in pixel values, 7 secret data bits can be embedded which shows an improvement in data stuffing capacity.

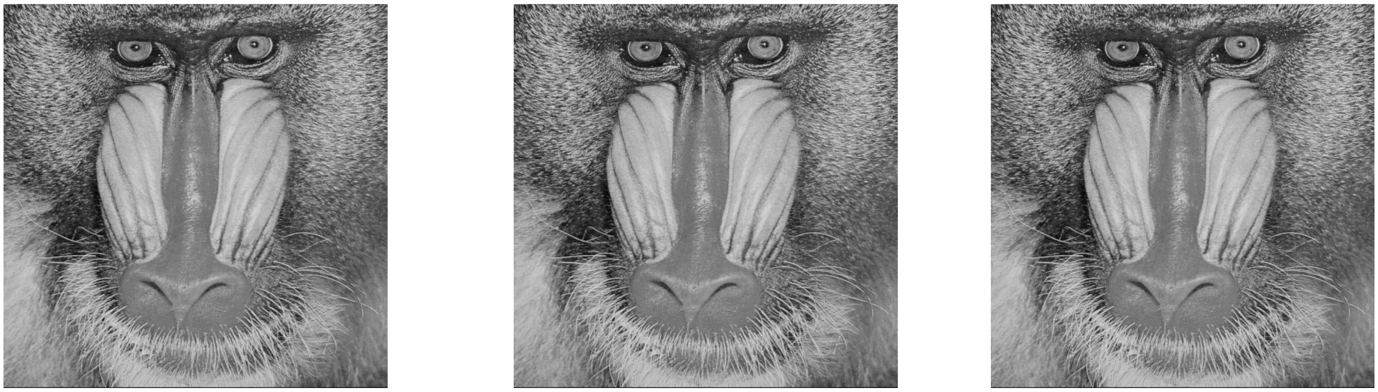
RESULTS ANDANALYSIS

(a) Cover Image
500 x500

(b) PVDM method
PSNR=43.9284 dB
Capacity=391145 bits

(c) Proposed method-1
PSNR= 37.6490 dB
Capacity= 730079 bits

Figure 3 : TEST IMAGE 1-Lena



(a) Cover Image
500 x500

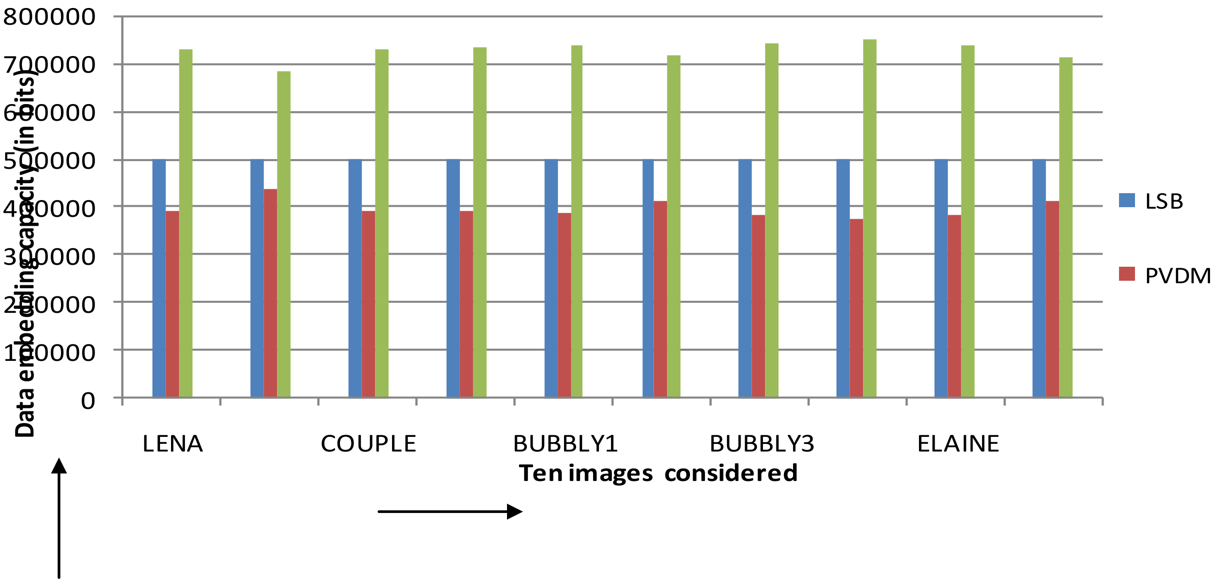
(b) PVDM method
PSNR = 40.1038 dB
Capacity=436930 bits

(c) Proposed method-1
PSNR= 36.8794 dB
Capacity=684088bits

Figure 4 : TEST IMAGE 2-Baboon

Table 3: Increase in Hiding Capacity comparing with PVDM

Image	**size**	**CAPACITY IN BITS**		
		PVDM	**Proposed method**	**% increase**
Lena	500 x 500	391145	730079	86.65
Baboon	500 x 500	436930	684088	**56.57**
Couple	500 x 500	393111	727770	85.13
Jet	500 x 500	391555	733438	87.31
Bubbly1	500 x 500	386537	738191	90.97
Bubbly2	500 x 500	414486	718251	73.29
Bubbly3	500 x 500	381887	743573	94.71
Bubbly4	500 x 500	375316	749497	**99.70**
Elaine	500 x 500	382809	738048	92.80
Man	500 x 500	412542	710994	72.34



Graph 1 : Comparision of LSB, PVDM and Proposed Methods

From Table 3, it can be observed that the hiding capacity of data bits is increased in the range of **56.57%** to **99.70%** for various images, by comparing the capacity of Pixel Value Differencing with Modulus function method.

The increase in data stuffing capacity for LSB, PVDM and proposed methods are shown in Graph 1. It is evident that the proposed method offers the accepted image qualities with the images having a PSNR value more than **36**.

CONCLUSION

The proposed method is a randomized method using robust key for embedding encrypted data bits with higher capacity maintaining acceptable image quality. The stego key chosen by the user gives randomization property which can withstand steganalysis process. The stego key has good level of robustness, because it is encrypted using RSA algorithm while transmitting on the channel.

Finally this method gives a good quality because the PSNR values are greater than **36** and high embedding capacity (increase in hiding capacity ranges from **56.57%** to the **99.70%** for various images considered). The average increase in hiding capacity of the proposed method is **84.05%**.

This proposed method is highly secured and has high embedding capacity with randomization properties to provide better data security while transmitting data bits on the channel compared to other existing algorithms.

BIBLIOGRAPHY

[1] Adem Orsdemir, H. Oktay Altun, Gaurav Sharma and Mark F. Bocko, "steganalysis aware steganography: statistical indistinguishability despite high distortion", SPIE-IS&T, Vol.6819, 2008, pp.1 - 9.

[2] Ahmad T. Al-Taani and Abdullah M. AL-Issa, "A Novel Steganographic Method for Gray-Level Images", International Journal of Computer, Information, Systems Science and Engineering 3:1 2009.

[3] Alvaro Martín, Guillermo Sapiro and Gadiel Seroussi, "Is Image Steganography Natural?", IEEE Transactions on Image Processing, Vol.14, 2005, pp.2040-2050.

[4] C.-C. Chang and H.-W. Tseng, "A steganographic method for digital images using side match", Pattern Recognition Letters, Vol.25, 2004, pp.1431–1437.

[5] C.-K. Chan and L.M. Cheng, "Hiding data in images by simple LSB substitution", Pattern Recognition, Vol.37, 2004, pp.469 – 474.

[6] Chung-Ming Wang, Nan-I Wu, Chwei-Shyong Tsai and Min-Shiang Hwang, "A high quality steganographic method with pixel-value differencing and modulus function", The Journal of Systems and Software, Vol.81, 2008, pp.150–158.

[7] Da-Chun Wu and Wen-Hsiang Tsai, "A steganographic method for images by pixel-value differencing", Pattern Recognition Letters, Vol.24, 2003, pp.613–1626.

[8] H.B.Kekre, Archana Athawale and Pallavi N.Halarnkarg, "Increased Capacity of Information Hiding in LSB's Method for Text and Image", International Journal of Electrical, Computer and Systems Engineering, 2008, pp.246-249.

[9] Hong–juan zhang and Hong-jun tang," A Novel Image Steganography Algorithm against Statistical Analysis", in proceedings of ICMLC, 2007, pp.3884-3888.

[10] Huaiqing Wang and Shuozhong Wang,"Cyber Warfare: Steganography vs. Steganalysis", Communications of the ACM, Vol.47, No.10, 2004, pp.76-82.

[11] Johnson N. and Jajodia.S, "Exploring steganography: Seeing the unseen", IEEE Computer, Vol.31, 1998, pp.26–34.

[12] Sorina Dumitrescu, Xiaolin Wu and Zhe Wang, "Detection of LSB Steganography via Sample Pair Analysis", IEEE Transactions on Signal Processing, Vol.51, 2003, pp.1995-2007.

[13] Tse-Hua Lan and Ahmed H. Tewfik, "A Novel High-Capacity Data-Embedding System" IEEE Transactions on Image Processing, Vol.15, 2006, pp.2431-2440.

[14] Tseng Y.C, ChenY.Y and Pan H.K, "A secure data hiding scheme for binary images", IEEE Transactions on Communications, Vol.50, 2002, pp.1227–1231.

[15] Tseng Y.C and Pan H.K," Data hiding in 2-color images", IEEE Transactions on Computers, Vol.51, 2002, pp.873–878.

[16] Behrouz A.Forouzan, "Cryptography & Network Security ", Special Indian Edition, 2007.

[17] William Stallings, "Cryptography & Network Security Principles &Practices", 3rd Edition, 2003.