I.J. Information Engineering and Electronic Business, 2015, 3, 52-59
Published Online May 2015 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijieeb.2015.03.08

An Image Steganography-based Novel Approach to develop 8-Share Integrated Security Toolkit (ISTI-8)

Sabyasachi Samanta
Haldia Institute of Technology, Haldia, WB, INDIA
E-mail id: sabyasachi.smnt@gmail.com

Saurabh Dutta
Dr. B. C. Roy Engineering College, Durgapur, WB, INDIA
E-mail id: saurabh.dutta@bcrec.org

Gautam Sanyal
National Institute of Technology, Durgapur, WB, INDIA
E-mail id: nitgsanyal@gmail.com

Abstract—Encryption is a process or algorithm to make information hidden or secret and considered as a subset of cryptography. Using encryption data are being transformed into some another form that appears to be meaningless and incomprehensible. Here we have embedded encrypted data bits about the entire image to some suitable nonlinear pixel positions using key. After that we have formed several shares of image and key using R, G and B components and character or digits respectively. At the decryption end through appropriate arrangement of shares of image and key, make possible to retrieve hidden data bits from stego-image and reform into its original content.

Index Terms—Steganography, Nonlinear Pixel Position (NPP), Modulus Division based Encryption (MDE), Visual Cryptography, Component based Visual Cryptography for Image (CVCI), Integrated Security Toolkit for Image (ISTI).

I. Introduction

Encryption is the process for transforming plaintext into the cipher text. Where plaintext is the input and cipher text is the output of the encryption process. Decryption is the process of transforming cipher text into the plaintext. Where cipher text is the input and plaintext is the output of the decryption process. Visual cryptography is an emerging cryptography technology, uses the characteristics of human vision to decrypt encrypted images. It needs neither cryptography knowledge nor the complex computation [1][14]. In encryption procedure, it uses the technique for hiding a two-tone secret image into a set of binary transparencies which seem like random noise. The visual cryptography uses secret sharing scheme based on a $\{k, n\}$ threshold framework, where n means a secret image will be hidden in n transparencies, and k is that we can stack k or more than k transparencies to reconstruct the secret image in visual[1] [14].

In this paper, we have proposed a technique to embed the encrypted (using MDE method) message about the entire image at arbitrary pixel positions using NPP-2 bit method [3]. The text taken from the keyboard or special characters encoded into its ASCII-8 (American Standard Code for Information Interchange) binary equivalent. Here we also have taken a key (K) with 6-digit. Then the corresponding ASCII-8 value is taken for each character or digit and added each of it. The total key value is divided by eight and we get reminder. Depending on the reminder the encryption is being processed (Figure 2). At the time of encryption three bits are taken from the data array and replaced as per encryption wheel. Each three bit block is replaced by encryption circle. The encrypted data bits again divided into 8-bit blocks and n^{th} bit left or right shifted. If the reminder be odd then the left shift is performed. Otherwise the right shift is performed. If reminder is zero, then no shifting is being performed. At the time of embedding a pair off encrypted data bits are taken and rooted to carrier image at nonlinear pixel position (NPP) through the key and we get stego-image cascading unique methods i.e. through Integrated Security Toolkit for Image (ISTI). Finally, we have made different image and key shares using CVCI method as in Table1. In figure 1 the flow diagram for ISTI method has been depicted.

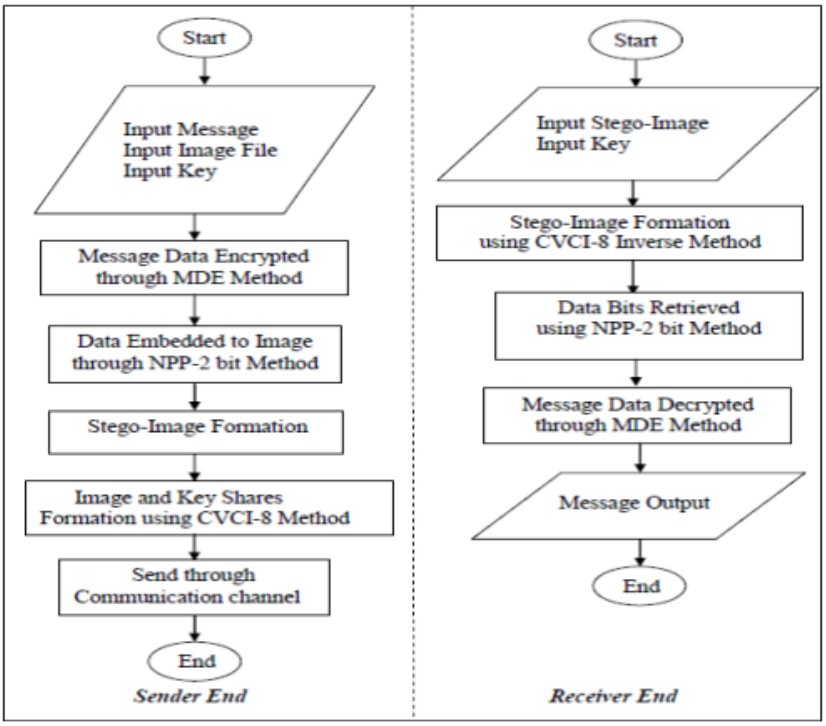

Fig.1. Flow Diagram for ISTI Method

In our work, we have targeted any two bit of last five significant bit of each R, G and B of any selected random pixel positions. The replacement of all the bits have done in nonlinear pixel and bit positions, in any one of five significant bit of R,G and B at selected pixels about the entire image using the private key cryptography technique taking the α value as 255 or as in the original image[2][3]. As, we have altered only any two bit of last five significant bits. If any bit generated from text become same to the targeted bit of image then there will be no change i.e. it will produce the same to original image [4] [5] [10].

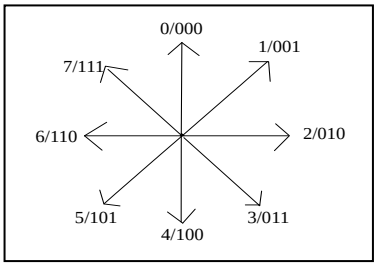

Fig.2. Encryption wheel

Here 8-image shares (IS_0-IS_7) are formed using presence (P) or absence (A) of Red (IM_R), Green (IM_G) and Blue (IM_B) color components respectively. Also the key shares (KS_0-KS_7) are formed with presence (P) or absence (A) of key shares (K_1, K_2 and K_3). At the decryption end suitable combination of image and key shares make possible to reform the stego-image (SI) and key (K). Formation of stego-image by using image shares (IM_R, IM_G and IM_B):

By using only one share: $SI_{11}=\{IS_7\}$

By using only two shares:

$SI_{21}=\{IS_0,IS_7\}$ $SI_{22}=\{IS_1,IS_6\}$
$SI_{23}=\{IS_2,IS_5\}$ $SI_{24}=\{IS_3,IS_4\}$
$SI_{25}=\{IS_3,IS_5\}$ $SI_{26}=\{IS_5,IS_6\}$
$SI_{27}=\{IS_3,IS_6\}$

Presence of shares IS_7 (similar to S_{21}} may produce more six combination like {{IS_1,IS_7}, {IS_2,IS_7}, {IS_3,IS_7}, {IS_4,IS_7}, {IS_5,IS_7}, {IS_6,IS_7}}. For the case of image, the shares S_0 forms a 100% black image and IS_7 form the stego-image. So the presence of IS_7 means the cent percent presence of stego-image.

Table 1. Formation of Image and Key Subset Using Shares

Image(IS)/ Key(KS) Subset	Image Shares			Key Shares		
	IM_R	IM_G	IM_B	K_1	K_2	K_3
S_0	A	A	A	A	A	A
S_1	A	A	P	A	A	P
S_2	A	P	A	A	P	A
S_3	A	P	P	A	P	P
S_4	P	A	A	P	A	A
S_5	P	A	P	P	A	P
S_6	P	P	A	P	P	A
S_7	P	P	P	P	P	P

For the key formation, by using (same as for stego-image) the key shares (KS_1, KS_2, KS_3) we may get back the original key (K). Also the presence of KS_7 means the cent percent presence of key (K).

Section 2 represents the scheme followed in the encryption technique. Section 3 represents an implementation of the technique. Section 4 gives you an

idea about the experimental results. Section 5 is an analytical discussion on the technique. Section 6 draws a conclusion.

II. Related Works

In this section we have discussed various encryption and steganographic data hiding methods.

A. Encryption methods

1. Encryption Algorithms are divided into 2 categories as follows:-
   a) *Symmetric Key Encryption* - In symmetric key encryption technique, single key is used in both encryption and decryption procedure. The key must be known to both the sender and receiver before encryption or decryption. So, the secret key plays important role and its strength depends on the length of key (in bits). Symmetric key encryption algorithms are- RC2, DES, 3DES, RC5, Blowfish, and AES et al [12].
   b) Asymmetric Key Encryption - Asymmetric key encryption algorithm uses two types of keys, Private keys and Public Keys. Public Key is used to encrypt the original data or plaintext and generate a cipher text [13]. This cipher text is decoded by the receiver when it receives, by using its own Private Key. Private Key is also known as secret key because it is unknown to all. Or it's known only to the person, who receives it or can say authorized person. Asymmetric key encryption algorithms are RSA, Digital Signatures et al.

2. Steganographic methods:

A. Spatial Domain Steganographic Method

a) *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)[4][8] and [9] planes by directly replacing the LSBs of the cover-image with the message bits.
b) *Data Hiding by PVD:* The pixel-value differencing (PVD) method proposed by Wu and Tsai [6] 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.
c) *Data Hiding by GLM:* In 2004, Potdar et al.[7] 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.

III. The Scheme

This section represents a description of the actual scheme used during "An Image Steganography-based Novel Approach to develop 8-Share Integrated Security Toolkit (ISTI-8)" technique. Section 3.1 describes the encryption technique using five algorithms 3.1.1, 3.1.2 & 3.1.3 while section 3.2 describes the decryption technique using algorithm 3.2.1 [3].

3.1. Encryption of data bits about the image and formation of image shares using ISTV-8 method

3.1.1. Create an encrypted array using MDE method

Step I: Take text input from keyboard or special characters and calculate the string length (chlen).

Step II: Convert the length (chlen) into its 8 bit binary equivalent. Store that data bits to earr[bit] as LSB (Least Significant Bit) to Arr[1] and MSB (Most Significant Bit) to Arr[8] respectively.

Step III: Convert each character of text into its ASCII-8 binary equivalent.

Step IV: Taking the key input, the corresponding ASCII-8 value of each character or digits is added.

Step V: Depending on the reminder through the modulus division by eight each three bit of Arr[] is encrypted.

Step VI: Again depending on the reminder the data bits are left or right shifted.

Step VII: Stop.

3.1.2 Stego-image formation using NPP-2 bit method

A. Selection of pixel positions of image

Step I: Take the value of bit from array Arr[bit] to calculate total number of required pixels(P). So, P= (ceil (bit /3)).

Step II: Take the key (K) and calculate the value of function: $F(x, y) = K^P$ [i.e. pow (K, P)].

Step III: Store the exponential long double values one by one.

Step IV: Repeat Step II to Step III for i= (1 to p) and go to Step V.

Step V: Read the values as character up to "e" of the every line of the file and store it to file.

Step VI: Take most three significant digits to $Arr_x[p]$, next three digits to array $Arr_y[p]$ and last significant digit to $Arr_z[p]$.

Step VII: Repeat Step V to Step VI up to end of the file.

Step VIII: Stop.

B. Replacement of array elements with R, G & B values of pixels

Step I: Calculate the width (w) and height (h) of the image.

Step II: Set $x=Arr_x[P]$ and $y=Arr_y[P]$.

Step III: To select the pixel position into image, compare the value of x and y with the value of w and h (where addressable pixel position is (0, 0) to (w-1, h-1)).

If (x >(w-1)) or (y >(h-1)) then

Set P (x, y) = P (0+(x %(w-1)), (0 +(y %(h-1)))

Otherwise Set P (x, y) = (x, y).

Step IV: To select the bit position (b) of selected pixel i.e. with which bit the array data will be replaced. Set z =Arr_z[p].

i) If (z%4=0) then b=1st LSB
ii) If (z%4=1) then b=2nd LSB
iii) If (z%4=2) then b=3rd LSB, Otherwise b=4th LSB of each R, G & B of a pixel.

Step V: A pair of data bits is replaced in corresponding and previous bit position and pixels are reformed**.**

Step VI: Repeat Step II to Step V for i=1 to P.

Step VII: Stop**.**

3.1.3 Creation of image and key shares using CVCV-8 Method

Step I: Create the image shares (IS_0- IS7) with presence (P) or absence (A) of Red (IM_R), Green (IM_G) and Blue (IM_B) elements respectively.

Step II: Also the key shares (KS_0-KS_7) are with presence (P) or absence (A) of key shares (K_1, K_2 and K_3).

Step III: Stop.

3.2 Decryption of the data bits from the image

3.2.1 Regain of replaced bits from the watermarked image and formation of original content

Step I: Take any two possible shares of image (IS_0-IS_7) to reform the stego-image.

Step II: Also Take any two possible shares of key (KS_0-KS_7) to reform the key (K).

Step III: To get the pixel and bit position in R, G & B of selected pixels go through Step I to Step VI of Algorithm 3.1.2.A and Step I to Step VI of Algorithm 3.1.2.B.

Step IV: Retrieving the encrypted bits from the selected bit positions of selected pixels store it to decrypted array from Darrlen[1] to Darrlen[bit] respectively.

Step V: To get the length repeat Step II to Step IV for i= 1 to 3 times (as every pixel contain three data bits) taking the key ($K_{[0]}$) and $ImgR_{[0]}$.

Step VI: Taking data bits of Darr[1] as LSB and Darr[8] as MSB calculate the length (chlen) of message.

Step VII: Repeat Step VIII for i=1 to 4.

Step VIII: Retrieving the encrypted bits, store it to decrypted character array from Darr[1] to Darr[bit] respectively (where bit is the array length from characters).

Step IX: Taking data values from the decrypted array Darr[ ], LSB as Darr[8*i+1] and MSB as Darr[8*(i+1))] respectively. Repeat Step V to Step VIII to decrypt the data bits and convert to its equivalent ASCII-8 character. Store the character to an array Msg[len].

Step X: Finally assemble the original message from the array Msg[len].

Step XI: Stop.

IV. Implementation And Result

Let the message to be encrypt is "MULTIMEDIA". So the length of the message =10 =00001010(8 Bit Binary equivalent).

First the bits from length and then from text are being stored to the array Arr[bit] respectively as,

Table 2. Characters with Binary Equivalent

Character	8Bbit Binary Equivalent
M	01001101
U	01010101
L	01001100
T	01010100
I	01001001
M	01001101
E	01000101
D	01000100
I	01001001
A	01000001

Let the key (K) =63A75C.

The image size= 128 X 128 (w x h).

Number of effected pixel required for character (p) = [ceil (90/3)] =30.

Calculate total (t) =54+51+65+55+53+67=345

Reminder (n) = 345%8= 1.

In the table below the process of encryption of text data depending on key is described.

Table 3. Encryption Using MDE Method

Bits after transposition	Bits after shifting
01110010	00111001
10100011	11010001
:	:
:	:
01110110	00111011

From the Table 2 to Table 3 how the data bits are encrypted and in Table 4 how the encrypted data bits are embedded is described.

Table 4. Positions of Array Elements about the Image

(Key, i)	Value	Pixel Position	Bit Position	Array Data
345,1	3450000E-04	(89,128)	LSB	Earr[1-2] Earr[3-4] Earr[5-6]
:	:	:	:	:
345,15	2533486E222	(125,92)	3rd LSB	Earr[85-86] Earr[87-88] Earr[89-90]

In figure 3 the original and image shares are presented. In figure 4 the histogram for the cover image and stego-image is given.

Fig.3. (a) is the first original image, (b) the watermarked image, (c) (d) (e) (f) (g) (f) (i) and (j) image shares corresponding to subsets (Table 1.1) from IS0 to IS8 respectively.

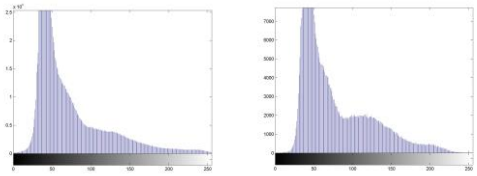

Fig.4. (a) and (b) the histogram of cover image, stego-image respectively

At the time of decryption let for SI_{24} ($\{IS_3, IS_4\}$), the union of subsets IS_3 and IS_4 make possible to produce the stego-image.

Fig.5. (a) (b) and (c) are the image subset IS4, IS5 and stego-image(SI)

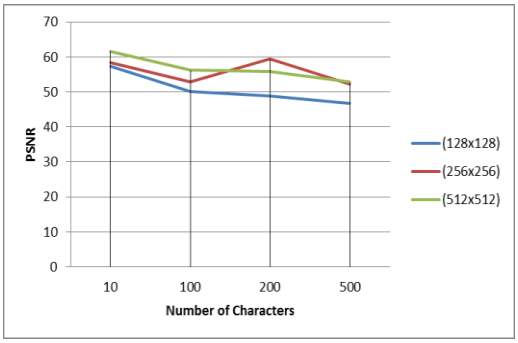

Fig. 6. Comparison of PSNR for image shares using NPP-2 bit method for LENA image

Table 5. PSNR of Image Shares using CVCI-8 Method

Characteristics	**CVCI-8**
1st image share PSNR	26.6274
2nd image share PSNR	27.1404
3rd image share PSNR	27.2427
4th image share PSNR	27.8866
5th image share PSNR	28.5859
6th image share PSNR	30.0579
7th image share PSNR	30.2734
8th image share PSNR	Infinity
No. of Shares Required for Decryption	Any Two as Per Algorithm
Reconstructed Image PSNR	Infinity
Quality and Clarity	High
Computational Complexity	Very High
Hardware Implementation	High

Table 6. Performance at a Glance for ISTI Method

Images	Image Similarity Matrices	Number of characters			
		10	100	200	500
LENA (128x128)	PSNR	57.2190	50.1686	48.8994	46.7911
	MSE	0.0152	0.3912	0.7019	1.8532
	RMSE	0.1233	0.6254	0.8337	1.3613
	SSIM	0.9999	0.9999	0.9998	0.9995
	Cross Correlation	1.0000	0.9999	0.9999	0.9999
	UIQI	0.9999	0.9999	0.9998	0.9995
	Entropy	7.2779	7.2786	7.2793	7.2803
	K-L Divergence	9.1256E-6	9.8666E-5	2.0388E-4	5.2539E-4

MONALISA (128x128)	PSNR	54.1677	50.2087	48.7557	46.6074
	MSE	0.0620	0.3840	0.7489	0.8029
	RMSE	0.2490	0.6197	0.8659	0.8960
	SSIM	0.9999	0.9998	0.9997	0.9997
	Cross Correlation	0.9999	1.0000	1.0000	0.9999
	UIQI	0.9999	0.9998	0.9997	0.9997
	Entropy	6.5800	6.5807	6.5801	6.5809
	K-L Divergence	1.6495E-5	1.1866E-4	2.5224E-4	2.9737E-4
LENA (256x256)	PSNR	58.3020	52.7810	59.3981	52.3215
	MSE	0.0092	0.1174	0.2220	0.0973
	RMSE	0.0961	0.3427	0.4712	0.3125
	SSIM	0.9999	0.9999	0.9999	0.9997
	Cross Correlation	0.9999	0.9999	1.0000	0.9999
	UIQI	0.9999	0.9999	0.9999	0.9997
	Entropy	7.2735	7.2737	7.2740	6.5608
	K-L Divergence	6.0120E-7	1.2022E-5	1.5636E-5	1.3971E-5
MONALISA (256x256)	PSNR	57.9877	53.4006	53.1847	51.6239
	MSE	0.0106	0.0883	0.0975	0.2001
	RMSE	0.1033	0.2971	0.3123	0.4473
	SSIM	0.9999	0.9999	0.9999	0.9999
	Cross Correlation	0.9999	0.9999	0.9999	0.9999
	UIQI	0.9999	0.9999	0.9999	0.9999
	Entropy	6.5407	6.5408	6.5408	6.5410
	K-L Divergence	1.0014E-6	8.9826E-6	1.8981E-5	2.6238E-5
LENA (512x512)	PSNR	61.6574	56.1612	55.9398	52.8098
	MSE	6.5697E-4	0.0247	0.2742	0.1159
	RMSE	0.0443	0.1573	0.1656	0.3404
	SSIM	0.9999	0.9999	0.9999	0.9999
	Cross Correlation	0.9999	0.9999	1.0000	0.9999
	UIQI	0.9999	0.9999	0.9999	0.9999
	Entropy	7.2881	7.2882	7.2881	7.2883
	K-L Divergence	4.1259E-8	4.6050E-7	3.6156E-7	2.1295E-6
MONALISA (512x512)	PSNR	61.1467	56.1969	54.7573	54.5438
	MSE	8.3118E-4	0.0243	0.0157	0.0521
	RMSE	0.0499	0.1560	0.2174	0.2283
	SSIM	0.9999	0.9999	0.9999	0.9999
	Cross Correlation	1.0000	0.9999	0.9999	0.9999
	UIQI	0.9999	0.9999	0.9999	0.9999
	Entropy	6.7464	6.7463	6.7464	6.7464
	K-L Divergence	6.2867E-7	4.6102E-7	1.0226E-6	1.3922E-6

Table 7. Comparative Analysis of Our Proposed Method with Other Method

Characteristics	**Wang et al.[7]**	**CVCI-8**
Types of Secret Sharing	(2,2)	(1,8)
Work on	Halftone (black & white)	Color Image
Size of Input Image	512x512	Any possible image size
Pixel Expansion	No	No
Intensity Division	No	No
Contrast Stretchment	No	No
Extra Information Needed	Yes	No
Codebook Needed	Yes	No
Shares Generated on the Basis of	Blocks	Pixel (RGB value)

V. Analysis

Here we have created a stego-image and then the image subsets using color components. We have used encryption technique but not any compression before the creation of array. Anybody may employ the compression at the time of creation of array. In that case, the length of array will be less and the strength of encryption will be higher than present. In addition the number of affected pixel will also be fewer. Here we have generated pixel positions depending on key value. Also key subsets have generated using key digits or characters. Here we have used six alphanumeric characters. Anybody may use only numerical digits and also with more digits or characters with variable length. As well may generate more subset of key. A pair of data bits are placed any five LSB position. Anybody may place less or more number of bits in any pixel position to each of R, G and B color components. The number of targeted pixels proportionally varies to size of text. If the image size becomes large and size of text becomes less then it will be quite harder to differentiate the encrypted image from the original image.

VI. Conclusion

Here we have used private key cryptographic technique to place the data bits (from both text and size of text) in arbitrary pixel positions about the entire image. Also we have generated random pixel positions depending on key. After that we generated image and key subsets from stego- image and key. Moreover, it produces the similar image using this method to see in naked eye. At the time of decryption only a proper combination of image and key subsets may produce the original stego -mage and key from which data can be extracted. After all, it will be quite impossible to find out the information from the stego-image.

References

[1] Feng Liu, Chuankun Wu,*"* Embedded Extended Visual Cryptography Schemes*"* , IEEE Transactions On Information Forensics And Security, Vol. 6, No. 2, June 2011, pp.307-322.

[2] Souvik Bhattacharyya, Goutam Sanyal "A Data Hiding Model with High Security Features Combining Finite State Machines and PMM method", International Journal of Electrical and Computer Engineering 5:2 2010, pp. 78-85.

[3] Sabyasachi Samanta, Saurabh Dutta, Goutam Sanyal, "An Enhancement of Security on Image Applying Asymmetric Key Algorithm", International Journal of Computer Applications (0975 – 8887), Volume 25– No.5, July 2011, pp. 19-23.

[4] Shan-Chun Liu, Wen-Hsiang Tsai, *"*Line-Based Cubism-Like Image—A New Type of Art Image and its Application to Lossless Data Hiding "IEEE Transactions On Information Forensics And Security, Vol. 7, No. 5, October 2012, pp. 1148-1458.

[5] Chung-Ming Wang , Nan-I Wu , Chwei-Shyong Tsai , Min-Shiang Hwang, "A high quality steganographic method with pixel-value differencing and modulus function", The Journal of Systems and Software (2007), pp. 1-9.

[6] J. K. Mandal, Debashis Das, "Steganography Using Adaptive Pixel Value Differencing (APVD) of Gray Images through Exclusion of Overflow/Underflow", CS & IT-CSCP 2012, pp. 93-102.

[7] Pradeep Kumar Sharma, Hari Mohan Singh" Visual Cryptography Scheme for Gray Scale Images based on Intensity Division" International Journal of Current Engineering and Technology, Vol.4, No.1 (Feb 2014) P-ISSN 2347 – 5161 pp.211-215.

[8] Dr. Ekta Walia, Payal Jain, An Analysis of LSB & DCT based Steganography", Global Journal of Computer Science and Technology, Vol. 10, Issue 1 (Ver 1.0), April 2010, pp. 4-8.

[9] M. Abolghasemi, H. Aghaeinia, K. Faez, "Data Hiding Detection Based on DWT and Zernike Moments" 4th International Conference: Sciences of Electronic, Technologies of Information and Telecommunications, March 25-29, 2007 – TUNISIA.

[10] Linfeng Guo, Yan Meng,"PSNR-Based Optimization of JPEG Baseline Compression on Color Images", ICIP 2006, pp. 1145-1148.

[11] Atallah M. Al-Shatnawi, "A New Method in Image Steganography with Improved Image Quality", Applied Mathematical Sciences, Vol. 6, 2012, pp. 3907 – 3915.

[12] Himanshu Gupta, Vinod Kumar Sharma, "Role of Multiple Encryption in Secure Electronic Transaction", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011, pp. 89-96.

[13] Pranam Paul, Saurabh Dutta, A K Bhattacharjee, "An Approach to ensure Security through Bit-level Encryption with Possible Lossless Compression", IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.2, February 2008, pp. 291-299.

[14] InKoo Kang, Gonzalo R. Arce, Heung-Kyu Lee, "Color Extended Visual Cryptography Using Error Diffusion", IEEE Transactions on Image Processing, Vol. 20, No. 1, January 2011, pp. 132-145.

[15] Shunquan Tan, Bin Li, *"*Targeted Steganalysis of Edge Adaptive Image Steganography Based on LSB Matching Revisited Using B-Spline Fitting *",* IEEE Signal Processing Letters, Vol. 19, No. 6, June 2012, pp. 336-339.

Authors' Profiles

Sabyasachi Samanta is working as Assistant Professor at Dept. of IT, Haldia Institute of Technology Haldia, WB, and India. He has received M. Tech Degree in IT and currently pursuing Ph. D at National Institute of Technology, Durgapur, WB, India. His main research interest includes watermarking, steganography and cryptography.

Saurabh Dutta is a professor in Dr. B. C. Roy Engineering College. He holds a Ph. D Degree in Coputer Science. His research domain is information security and cryptology.

Gautam Sanyal is a member of the IEEE. He has received his B.E and M. Tech degree from National Institute of Technology (NIT), Durgapur, India. He has received Ph.D. (Engg.) from Jadavpur University, Kolkata, India, in the area of Robot Vision.

He possesses an experience of more than 25 years in the field of teaching and research. He has published nearly 68 papers in International and National Journals / Conferences. Three Ph. Ds (Engg.) have already been awarded under his guidance. At present he is guiding six Ph. Ds scholars in the field of steganography, Cellular Network, High Performance Computing and Computer Vision. He has guided over 10 PG and 100 UG thesis. His research interests include Natural Language Processing, Stochastic modeling of network traffic, High Performance Computing, Computer Vision. He is presently working as a Professor in the department of Computer Science and Engineering and also holding the post of Dean (Students' Welfare) at National Institute of Technology, Durgapur, India.

How to cite this paper: Sabyasachi Samanta, Saurabh Dutta, Gautam Sanyal,"An Image Steganography-based Novel Approach to develop 8-Share Integrated Security Toolkit (ISTI-8)", IJIEEB, vol.7, no.3, pp.52-59, 2015. DOI: 10.5815/ijieeb.2015.03.08

