High Capacity data hiding using LSB Steganography and Encryption

Shamim Ahmed Laskar[1] and Kattamanchi Hemachandran[2]

Department of Computer Science
Assam University, Silchar, Assam, India
[1]shamim.aus@rediffmail.com, [2]khchandran@rediffmail.com

ABSTRACT

The network provides a method of communication to distribute information to the masses. With the growth of data communication over computer network, the security of information has become a major issue. Steganography and cryptography are two different data hiding techniques. Steganography hides messages inside some other digital media. Cryptography, on the other hand obscures the content of the message. We propose a high capacity data embedding approach by the combination of Steganography and cryptography. In the process a message is first encrypted using transposition cipher method and then the encrypted message is embedded inside an image using LSB insertion method. The combination of these two methods will enhance the security of the data embedded. This combinational methodology will satisfy the requirements such as capacity, security and robustness for secure data transmission over an open channel. A comparative analysis is made to demonstrate the effectiveness of the proposed method by computing Mean square error (MSE) and Peak Signal to Noise Ratio (PSNR). We analyzed the data hiding technique using the image performance parameters like Entropy, Mean and Standard Deviation. The stego images are tested by transmitting them and the embedded data are successfully extracted by the receiver. The main objective in this paper is to provide resistance against visual and statistical attacks as well as high capacity.

KEYWORDS

Steganography, Cryptography, plain text, encryption, decryption, transposition cipher, Least Significant Bit, Human Visual System, Mean square error and Peak Signal to Noise Ratio.

1. INTRODUCTION

With the growth of computer network, security of data has become a major concern and thus data hiding technique has attracted people around the globe. Steganography techniques are used to address digital copyrights management, protect information, and conceal secrets [1]. Data hiding techniques provide an interesting challenge for digital forensic investigators. Data is the backbone of today's communication. To ensure that data is secured and does not go to unintended destination, the concept of data hiding came up to protect a piece of information [2]. Digital data can be delivered over computer networks with little errors and often without interference. The Internet provides a communication method to distribute information to the masses. Therefore, the confidentiality and data integrity are required to protect against unauthorized access and use. Steganography and cryptography are two different information hiding techniques, where we

DOI: 10.5121/ijdms.2012.4605

transform the message so as to make it meaning obscure to a malicious people who intercept it [6].

Steganography relies on hiding message in unsuspected multimedia data and is generally used in secret communication between acknowledged parties [19]. The technique replaces unused or insignificant bits of the digital media with the secret data. The concept is to embed the hidden object into a significantly larger object so that the change is undetectable by the human eye [23]. All digital file formats can be used for steganography, but the formats those are with a high degree of redundancy are more suitable [6]. The redundant bits of an object are those bits that can be altered without the alteration being detected easily. The most popular cover objects used for steganography are digital images. Digital images often have a large amount of redundant data, and this is what steganography uses to hide the message [26]. Cryptography merely obscures the integrity of the information so that it does not make sense to anyone except the creator and the recipient [4]. Steganography could be considered as the dark cousin of cryptography. Cryptography assures privacy whereas Steganography assures secrecy [2]. Steganography and cryptography are both used to ensure data confidentiality. However, steganography differs from cryptography in the sense that the cryptography focuses on keeping the contents of a message secret, steganography focuses on keeping the existence of a message secret [4]. Thus, with cryptography anybody can see that both parties are communicating in secret. Steganography hides the existence of a secret message in such a way that nobody can see that both parties are communicating in secret.

The basics of embedding data rely on three different facts i.e. capacity, security, and robustness. Capacity means the media on which the data is to be hidden should hold the data, so that the complexity of the medium should not be disturbed [6]. Security means the embedding algorithm is said to be secure if the embedded information cannot be removed beyond reliable detection by targeted attacks [28]. Finally, robustness means the amount of manipulation a cover image (original image) can handle without drawing any attention that a change has taken place. Steganography and cryptography have to guarantee any of the requirements.

Steganography and Cryptography are parallel data security techniques and the techniques can be implemented side by side, in fact steganographic system can implement cryptographic data security. With cryptography we can protect the message but not hide its existence [7]. Steganography pay attention to the degree of invisibility while cryptography pays attention to the security of the message [35]. Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated [27]. The strength of steganography can thus be increased by combining it with cryptography.

2. LSB BASED IMAGE STEGANOGRAPHY

An image is the most common type of digital media used for steganography [1]. Digital images often have a large amount of redundant data and for this reason it is possible to hide message inside image file [12]. To a computer, an image is a collection of numbers that constitute different light intensities in different areas of the image. This numeric representation forms a grid and the individual points are referred to as pixels. These pixels make up the image's raster data. Image steganography is about exploiting the limited power of the human visual system (HVS) [23]. If any specific colour is viewed closely it has been observed that single digit modifications to the contribution level are imperceptible to the human eye (i.e. a pixel with a value of (255, 255, 0) is indistinguishable from (254, 255, 0)) in RGB colour representation.

The digital data related to images seem to be too large to be transmitted through the Internet. So, some techniques are used to reduce the data to a suitable size in order to display it in a reasonable amount of time across the Internet. This technique called compression makes use of some mathematical concepts to reduce the image data, resulting in smaller file sizes and plays a vital role in image based steganography methods. Image formats can mainly be divided into two categories based on compression, lossy and lossless. Both methods save storage space but have different results. Lossy compression (e.g. JPEG format) attains a high level of compression and thus saves more space but in doing so, the bits may be altered largely and the originality of the image may be affected [3]. The JPEG compression algorithm uses floating point calculations for converting image and it results in rounding errors which may eliminate portions of the image which are not visible to the naked eye. Although this rarely causes a noticeable change to the image it can significantly alter or destroy any information that was hidden in the image.

Lossless compression maintains the original image data exactly and the lossless compression images are preferred for steganography as image media. Spatial domain steganographic techniques, also known as substitution techniques, consists of simple techniques that create a covert channel in the parts of the cover image in which changes are likely to be imperceptible to the human visual system (HVS).One of the methods to do so is to hide information in the least significant bit (LSB) of the image data [32]. This embedding method is based on the fact that the least significant bits in an image can be thought of as random noise, and consequently they become not responsive to any change on the image [33]. Least significant bit (LSB) is the most commonly used type of insertion scheme used currently in digital steganography [15]. This method is probably the easiest way of hiding information in an image and yet it is surprisingly effective [18, 20]. The secret message is hidden by altering least significant bit in a certain layer of the image file.

The embedding procedure of LSB based steganography is described by the following equation:

$$yi = 2\left|\frac{x_i}{2}\right| + m_i \qquad (1)$$

where m_i , x_i , and y_i are the i-th message bit, and the i-th selected pixel value before and after embedding, respectively.

Let $\{P_m(x=0),\ P(x=1)\}$ denote the distribution of the least significant bits of the cover image, and $\{P_m(m=0), P(m=1)\}$ denote the distribution of the secret binary message bits.

The message is to be compressed or encrypted before being embedded just to protect its secrecy. According to this, the distribution of the message may be assumed to equal an averaged distribution, such that $\{P_m(m=0) \approx P_m(m=1) \approx \frac{1}{2}\}$

In addition, the cover image and the message may also be assumed to be independent. Therefore, the noise introduced into the image may be modeled as:

$$P_{+1} = \frac{P}{2}P_x(x=0),\ P_0 = 1-\frac{P}{2}\ ,\ P_{-1} = \frac{P}{2}P_x(x=1)$$

where P is the embedding rate, measured in bits per pixel (bpp). The embedding process described above, makes it clear to what extent it is possible to extract the secret message bits directly from the LSBs of these pixels already selected during this process [34].

In an image if we change the MSBs, it will have a noticeable impact on the colour, however, changing the LSBs will not be noticeable to the human eye [3]. The image formats typically used in the LSB substitution are lossless and the data can be directly manipulated and recovered [20]. Lossless data compression makes use of data compression algorithms that allows the exact original data to be reconstructed from the compressed data [22]. One of the most important features of lossless compression is to maximize the embedding capacity [25]. The use of digital images for steganography makes use of the weaknesses in the human visual system, which has a low sensitivity in pattern changes and luminance. Employing the LSB technique for data hiding achieves both invisibility and reasonably high storage payload [14].

The advantages of LSB based data hiding method is that it is simple to embed the bits of the message directly into the LSB plane of image and many techniques use these methods [12]. The LSB modification does not result in image distortion and thus the resulting stego-image will look identical to the cover-image [21]. Several variations of the basic LSB based steganographic techniques were described by Johnson, and Katzenbeisser [14]. They also describe a substitution technique for embedding message into the LSB bits of the palette of GIF or BMP image format. Bailey and Curran provide an evaluation of various techniques concerning spatial steganographic that principally applies to GIF images [21]. They discussed different strengths in terms of resistance to different types of steganalysis or their ability to maximize the size of the message that could be stored.

The LSB based data embedding differ in the way of information hiding process. Some of them embed the data inside an image file sequentially other randomly. In sequential LSB, the message is laid out across the image data sequentially. In the random embedding, the message bits are randomly scattered throughout the whole image using a random sequence to control the embedding sequence. Some modify pixels not in the whole image but in selected areas of it, and still others increase or decrease the pixel value of the LSB, rather than change the value.

In [20] the authors emphasize strongly on image Steganography providing a strong focus on the LSB techniques in image Steganography. This paper explained the LSB embedding technique and presents the evaluation results for 2, 4, 6 least significant bits for a PNG and BMP file. By applying an optimal pixel adjustment process to the stego-image obtained by the simple LSB substitution method, the image quality of the stego-image can be greatly improved with low extra computational complexity [24].

Gutte and Chincholkar proposed a text Steganography method along with cryptography for secret communication [5]. They used the LSB based method of steganography and also compared the data hiding at one LSB and two LSB positions and evaluated the performance parameters like Standard Deviation, MSE and Entropy etc. The data is encrypted using Extended Square Substitution Algorithm.

3. PROPOSED METHOD

To enhance the embedding capacity of image steganography and provide an imperceptible stego-image for human vision, we propose a framework for hiding large volumes of data in images by combining cryptography and steganography while incurring minimal perceptual degradation and to solve the problem of unauthorized data access. Steganography also can be implemented to cryptographic data so that it increases the security of this data [4]. In this method we first encrypt

a message using transposition cipher method and then embed the encrypted message inside an image using LSB embedding method. Hiding data using LSB modification alone is not highly secure. The combination of these two methods will enhance the security of the data embedded. This combinational methodology will satisfy the requirements such as capacity, security and robustness for secure data transmission over an open channel. The resulting stego-image can be transmitted without revealing that secret information is being exchanged. Furthermore, even if an attacker were to defeat the steganographic technique to detect the message from the stego-object, he would still require the cryptographic decoding method to decipher the encrypted message. One of the most important features of lossless compression is to maximize the embedding capacity.

3.1 Transposition Cipher

The proposed method depicts a typical cryptographic system based on classical encryption techniques i.e. substitutions and transpositions and they are regarded as building blocks for encryption [36]. Transposition technique changes the order of the letters in a message [13]. Instead of replacing characters with other characters as in the case of substitution technique, this cipher just changes the order of the characters [10]. Transposition does not alter any of the bits in the plaintext, but instant moves the position around within it [30]. Letter frequencies are preserved in the ciphertext. The ciphertext is the disguised form of the information. Such cipher text could be transmitted across a network or stored within a file system with the objective of providing confidentiality [7]. Here the text to be encrypted is arranged in a number of columns. The message is broken in to NXN matrix.

Often the transposition method is of a geometrical nature. In this transposition cipher method, the plaintext is written row wise in a matrix of given size, but is read out column wise in a specific order depending on a key [36]. Key is something the sender and the recipient agree on beforehand. Key tells the size of the matrix. To encrypt plaintext the transposition cipher writes the message in a rectangle, row by row, and reads the message off, column by column, but permutes the order of the columns based on the key. Both the length of the rows and the subsequent arrangement of the columns are defined by either a keyword or numerical key. In a regular columnar transposition cipher, any extra spaces are filled with nulls and in an irregular columnar transposition cipher, the spaces are left blank.

For an example, if we try to encrypt using transposition cipher the following plaintext “BY COMBINING STEGANOGRAPHY AND CRYPTOGRAPHY WE CAN ACHIEVE BETTER SECURITY OF DATA AND INFORMATION" with a 7X7 matrix, then the plain text will first be filled in row wise as depicted below:

Table 1. Plain Text entered into the matrix in row-wise

B	Y		C	O	M	B
I	N	I	N	G		S
T	E	G	A	N	O	G
R	A	P	H	Y		A
N	D		C	R	Y	P
T	O	G	R	A	P	H
Y		W	E		C	A

N		A	C	H	I	E
V	E		B	E	T	T
E	R		S	E	C	U
R	I	T	Y		O	F
	D	A	T	A		A
N	D		I	N	F	O
R	M	A	T	I	O	N

Now, we take the columns, and re-arrange them, according to some pattern and then we read across (columnwise in the indicated order). Thus, we have the ciphertext as "BITRNTYYNEADO IGP GWCNAHCREOGNYRA M O YPCBSGAPHANVER NR ERIDDMA TA ACBSYTITHEE ANIITCO FOETUFAON".

3.2 Data Embedding Procedure

The encrypted message to be hidden is converted into its ASCII equivalent character and subsequently into binary digit. For an example if the character "t" is an encrypted character of the message then as ASCII value for "t" is 116 and binary value for it is 1110100. As image comprises of pixel contribution from red, green and blue components and each pixel has numbers from the colour components (for 24-bit bitmap image each of red, green and blue pixel has 8 bit). At 8 bit of the colour number, if we change least significant bits, our visual system cannot detect changes in pixel and thus it is possible to replace message bits with image pixel bit. For example if we consider the pixel value 10111011, and we want to store the information in the least significant bit, at the worst situation the pixel changes to 10111010, examinations shows that HVS cannot distinguish this alteration [24]. So we embed the encrypted data into least significant bits of colour. If we change the LSB in a byte of an image, we either add or subtract one from the value it represents [29].

In order to hide the encrypted message, data is first converted into byte format and stored in a byte array. The message is embedded into the LSB position of each pixel. Suppose our original pixel has bits:

(r7 r6 r5 r4 r3 r2 r1 r0, g7 g6 g5 g4 g3 g2 g1 g0, b7 b6 b5 b4 b3 b2 b1 b0)
In addition, our encrypted character (bytes) has some bits: (c7 c6 c5 c4 c3 c2 c1 c0).

Then we can place the character bits in the least significant of selected pixel, next character bits in the next lowest pixel, and so on. (r7 r6 r5 r4 r3 r2 r1 c2, g7 g6 g5 g4 g3 g2 g1 c1, b7 b6 b5 b4 b3 b2 b1 c0).

If we take an example of pixel (225,107,100) represented in binary form (11100001, 01101011, 01100100) into which to embed message character "a" having bit 01100001(ASCII value 97), then we can obtain New pixel as (224, 106,101) represented in binary form (11100000, 01101010, 01100101).

Here we can notice that a pixel value of (225,107,100) is changed to a new pixel value of (224, 106,101). And this change is not visible to human vision [29]. The embedding process operates over the image, and embeds the message character into cover-image pixel by pixel at a time. Once all the message characters are embedded into the cover-image, the target character (*) represented in bit by 101010, is inserted in the pixel of the cover-image immediately next to the one containing the last input character of the message. The target character is a special symbol and is known as Terminator Character. Because it is the last character that is embedded and after embedding the target character (101010), insertion process stops from next row onwards. This helps the decoding process to stop extracting of data from stego-image by informing that the target character (*) signifies the end of the message.

3.3 Message Extraction Process

In the image based steganography the secret message is extracted from the stego-image. The recipient inputs the stego-image to the extraction algorithm, which outputs the secret message. The method of retrieval of message from the stego-image is called steganalysis [11]. The data extraction algorithm is the inverse of the embedding algorithm, although the embedding and extraction algorithm is created such that the extraction algorithm is not actually the mathematical inverse of the embedding algorithm. In extracting encrypted message, the process opens the stego-image file and read the RGB colour of each pixel. The LSBs of each pixel of stego-image is extracted. As in the embedding process a Terminator (Target) Character is placed in the message which is the last character to signify the end of embedding of data. When the binary representation of the Terminator character is found the extraction process stops. The purpose of putting this character is that in the process of retrieving the message, the extraction algorithm may take extra bits. Thus the terminator character helps the extracting algorithm by informing it to stop reading the bits of the stego-image from next pixel onwards as no more data is embedded in further pixels. The bits of the LSB are retrieved and placed in the array. Then content of the array converts into decimal value that is actually ASCII value of encrypted message. Each 8 bit from the array is converted into character. Thus the message that is retrieved from the image is actually encrypted form of the original message. The message retrieved is then decrypted using the same transposition method that is used in encrypting. In decrypting the message using transposition cipher method, the ciphertext is written row wise in a matrix of same size as in encrypting method, but will be read out column wise in a specific order depending on a key. Key tells the size of the matrix. If the key that is used in the encryption method doesn't match the ciphertext will not be retrieved. Thus the key plays a vital role in message extraction. The plaintext is then read off by column, as it was originally entered in the order specified by the key.

4. EXPERIMENTAL ANALYSIS

Figure 1. Clover (a) cover image (b) stego image

Figure 2. Flower (a) cover image (b) stego image

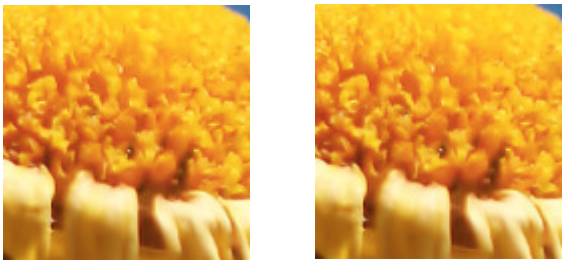

Figure 3. Bud (a) cover image (b) stego image

The proposed scheme ensures high embedding rates and also maintaining high levels of security. The experimental work was done using Matlab and in the experiment we observed that the messages were successfully embedded into the cover images. The complexity of the image is not disturbed as shown in figure 1. (a) and (b), figure 2. (c) and (d), figure3. (e) and (f). The difference of the stego-image can hardly be distinguished after using the LSB method insertion. The images that are taken for embedding message range from 35 KB to 47 KB. Thus, the modification of the cover-image is not perceptible on the stego-image at all and the process arouses no suspicion to third parties. The size of the stego-image is same as the original image and most importantly the messages were also extracted successfully. The proposed algorithm is analyzed in the light of the statistical framework 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) [16, 31]. If the distortion occurs after the detection program is implemented then it is detected that the images may containing the hidden data otherwise not. And thus it gives a clear idea of the security.

Usually, the invisibility of the hidden message is measured in terms of the Peak Signal-to-Noise Ratio [17]. To analyze the quality of the embedded texture image, with respect to the original, the measure of PSNR has been employed [16]:

$$\text{PSNR} = 10 \log_{10} \frac{255^2}{\text{MSE}} \qquad (2)$$

where mean square error (MSE) is a measure used to quantify the difference between the cover image I and the stego (distorted) image I' [17]. If the image has a size of M * N then

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} . \sum_{j=1}^{N} [I(i,j) - I`(i,j)]^2 \qquad (3)$$

TABLE 2. MSE and PSNR values for the Original and Stego images

Cover image	Stego Image	Amount of data embedded	MSE %	PSNR (dB)	Amount of data extracted
clover (35 KB)	stegclover (35 KB)	4267 bytes	0.48	51.28	4267 bytes
flower (43 KB)	stegflower (43 KB)	4513 bytes	0.41	51.93	4513 bytes
bud (47 KB)	stegbud (47 KB)	5075 bytes	0.43	51.69	5075 bytes

Generally speaking, when the payload increases, the MSE will increase, and this will affect the PSNR inversely [16]. So, from trade-off 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 [16]. Our results indicate that embedding process introduces less perceptual distortion and higher PSNR [17]. To measure the distortion introduced by the embedding in the cover-image, the Peak Signal to Noise Ratio (PSNR) after embedding was observed for some images. It was found that the PSNR is constantly above 51 dB as seen in table 2 which means that the quality degradations could hardly be perceived by a human eye.

The proposed method is also evaluated based on image parameters like Entropy, Mean and Standard deviation to check the impact on image in case of replacement of bits [31]. Here, we conduct an analysis between cover-image and the stego-image based on statistical distortion. The result of the performance parameters before and after the embedding process are calculated and summarized in Table 3. The image parameters are measurement of the security for the stego-system [31]. Minimizing parameters difference is one of the main objectives in order to get rid of statistical attacks.

TABLE 3. Image Parameters for Original image and Stego image

Before Embedding				After Embedding			
Cover Image	Standard Deviation	Mean	Entropy	Stego Image	Standard Deviation	Mean	Entropy
clover	71.8141	173.9736	7.6364	stegclover	71.8142	173.9313	7.6336
flower	75.3645	138.8579	7.8267	stegflower	75.3578	138.8248	7.8311
bud	82.9257	144.9935	7.5051	stegbud	82.9337	144.9475	7.5033

From the Table 3 it is seen that there is no significant difference between the entropy, mean and standard deviation between the cover-image and the stego-image. This study shows that the magnitude of change in stego-image based on image parameters is small from a cover file.

The method of steganography proposed by Gutte and Chincholkar that embeds encrypted message into the cover image [5]. The length of the plain text that was embedded contained 90 characters for this reason the result of the statistical image parameters were same. As in our method we tested the images ranging from 35 KB to 47 KB to embed 4000 to 5100 characters. In comparing with Gutte and Chincholkar method it is seen the embedding capacity of our proposed method is much high and also the quality of the image is retained. Experimental results show that the values entropy, mean and standard deviation of the image before the insertion are closely similar to the values after the insertion. Since the image parameters have not changed much, the method offers a good concealment of data and reduces the chance of the secret data being detected. Thus, it indicates a perfectly secure steganographic system. Furthermore, the secret information can be retrieved without encountering any loss of data. The major advantage is that the proposed method is quick and easy and it works well colour images.

5. CONCLUSION

The proposed method has been employed for applications that require high-volume embedding with robustness against certain statistical attacks. The present method is an attempt to identify the requirements of a good data hiding algorithm. And it is not intended to replace steganography or cryptography but rather to supplement it. Steganography is the data hiding technique which comes under the assumption that if the feature is visible, the point of attack is evident, thus the goal here is always to conceal the very existence of the embedded data. Steganography is not a good solution to secrecy, but neither is encryption. But if these methods are combined, we will have two layers of protection. If a message is encrypted and hidden with a LSB steganographic method the embedding capacity increases and thus we can hide large volume of data. And the method satisfies the requirements such as capacity, security and robustness which are intended for data hiding. The resulting stego-image can be transmitted without revealing that secret information is being exchanged. Furthermore, even if an attacker were to defeat the steganographic technique to detect the message from the stego-object, he would still require the cryptographic decoding key to decipher the encrypted message. The proposed algorithm is analyzed in the light of the statistical framework in order to prove its efficiency and also to show its level of security. The main focus of the paper is to develop a system with extra security features where a meaningful piece of text message can be hidden by combining two basic data hiding techniques. The method can further be extended with taking into account other data hiding and encryption techniques. Every technique leaves some space for further improvement. The method can further be extended with taking into account other data hiding and encryption techniques. We will try to develop some new techniques to yield higher steganographic capacities and also maintaining the level of resistance to visual and statistical attacks.

ACKNOWLEDGEMENTS

One of the authors (Shamim Ahmed Laskar) gratefully acknowledges UGC for granting Research fellowship (Maulana Azad National Fellowship).

REFERENCES

[1] Anderson , R. J. and Petitcolas, F. A.P. (1998) “On The Limits of Steganography”, *IEEE Journal of Selected Areas in Communications*, Vol.16 No.4, pp.474-481, ISSN 0733-8716.

[2] Petitcolas, F.A.P., Anderson, R. J. and Kuhn, M.G. (1999) “Information Hiding -A Survey”, *Proceedings of the IEEE*, Special issue on Protection of Multimedia Content, vol. 87, no. 7, pp.1062-1078.

[3] Johnson, N.F. and Jajodia, S. (1998) "Exploring Steganography: Seeing the Unseen", *IEEE, Computer*, vol. 31, no. 2, pp. 26-34.

[4] Raphael, A. J. and Sundaram, V. "*Cryptography and Steganography – A Survey*", Int. J. Comp. Tech. Appl., Vol 2 (3), pp. 626-630 , ISSN:2229-6093.

[5] Gutte, R. S. and Chincholkar, Y. D. (2012) "Comparison of Steganography at One LSB and Two LSB Positions", *International Journal of Computer Applications*, Vol.49,no.11, pp.1-7.

[6] Laskar, S.A. and Hemachandran, K. (2012), "An Analysis of Steganography and Steganalysis Techniques", *Assam University Journal of Sscience and Technology*, Vol.9, No.II, pp.83-103, ISSN: 0975-2773.

[7] Younes, M.A.B. and Jantan, A. (2008), "Image Encryption Using Block-Based Transformation Algorithm," *International Journal of Computer Science*, Vol. 35, Issue.1, pp.15-23.

[8] Walia, E., Jain, P. and Navdeep. (2010), " An Analysis of LSB & DCT based Steganography", *Global Journal of Computer Science and Technology*, Vol. 10 Issue 1 , pp 4-8.

[9] Khare, P., Singh, J. and Tiwari, M. (2011), "Digital Image Steganography", *Journal of Engineering Research and Studies*, Vol. II, Issue III, pp. 101-104, ISSN:0976-7916.

[10] Sokouti, M., Sokouti, B. and Pashazadeh, S. (2009), "An approach in improving transposition cipher system", *Indian Journal of Science and Technology*, Vol.2 No. 8, pp. 9-15, ISSN: 0974- 6846.

[11] Kharrazi, M., Sencar, H. T. and Memon, N. (2006), "Performance study of common image steganography and steganalysis techniques", *Journal of Electronic Imaging,* SPIE Proceedings Vol. 5681.15(4), 041104 pp.1-16.

[12] R., Chandramouli, and Nasir Memon.(2001), "Analysis of LSB based image steganography techniques." In *Image Processing, 2001. Proceedings. 2001 International Conference on*, IEEE, vol. 3, pp. 1019-1022.

[13] Giddy, J.P. and Safavi- Naini, R. (1994), " Automated Cryptanalysis of Transposition Ciphers", *The Computer Journal*, Vol.37, No.5, pp. 429-436.

[14] Johnson, N. F. and Katzenbeisser, S. (2000), "A survey of steganographic techniques", *In Information Hiding, Artech House, Norwood, MA,* pp. 43-78.

[15] Chandramouli, R. and Menon, N. (2001), "Analysis of LSB based image steganography techniques", *IEEE Proceedings on Image Processing*, Vol.3, pp.1019-1022.

[16] Carvajal-Gamez , B.E., Gallegos-Funes, F. J. and Lopez-Bonilla, J. L. (2009), " Scaling Factor for RGB Images to Steganography Applications", *Journal of Vectorial Relativity*, Vol. 4, no. 3, pp.55-65.

[17] Ulutas, G., Ulutas, M. and Nabiyev,V. (2011), "Distortion free geometry based secret image sharing", *Elsevier Inc*, Procedia Computer Science 3, pp.721–726.

[18] Tiwari, N. and Shandilya, M. (2010), "Evaluation of Various LSB based Methods of Image Steganography on GIF File Format", *International Journal of Computer Applications* (0975 – 8887) Vol. 6, no.2, pp.1-4.

[19] Rabah, K. (2004), "Steganography – The Art of Hiding Data", *Information Technology Journal*, Vol.3, no.3, pp. 245-269.

[20] Deshpande, N., Kamalapur, S. and Daisy, J. (2006), "Implementation of LSB steganography and Its Evaluation for Various Bits", *1st International Conference on Digital Information Management*, pp.173-178.

[21] Karen, Bailey, and Kevin Curran.(2006) "An evaluation of image based steganography methods" *Multimedia Tools and Applications, Springer* Vol.30, no. 1, pp. 55-88.

[22] Celik, M. U., Sharma, G., Tekalp, A.M. and Saber, E. (2005), "Lossless Generalized-LSB Data Embedding", *IEEE Transaction on Image Processing*, Vol. 14, No. 2, pp. 253-266.

[23] Huang, Y. S., Huang, Y. P., Huang, K.N. and Young, M. S. (2005), "The Assessment System of Human Visual Spectral Sensitivity Curve by Frequency Modulated Light", *Proceedings of the 2005 IEEE Engineering in Medicine and Biology 27th Annual Conference*, pp. 263-265.

[24] Chan, Chi-Kwong, and L. M. Cheng. (2004), "Hiding data in images by simple LSB substitution." *Pattern Recognition* Vol. 37, no. 3, pp. 469-474.

[25] Brisbane, G., Safavi-Naini, R. and Ogunbona, P. 2005. "High-capacity steganography using a shared colour palette", *IEEE Proceedings on Vision, Image and Signal Processing*, Vol.152, No.6, pp.787-792.

[26] Curran, K. and Bailey, K. (2003), "An Evaluation of Image Based Steganography Methods", *International Journal of Digital Evidence Fall 2003*, Volume 2, Issue 2, www.ijde.org.

[27] Dickman, S.D. (2007), "An Overview of Steganography", *JMU-INFOSEC-TR-2007-002*, http:// citeseerx.ist.psu.edu/viewdoc/summary? doi=10.1.1.137.5129.

[28] Dunbar, B. (2002). "A detailed look at Steganographic Techniques and their use in an Open-Systems Environment", *SANS Institute 2002*, pp.1-9, http://www.sans.org.

[29] Lee, Y-K. ; Bell, G., Huang, S-Y., Wang, R-Z. and Shyu, S-J. (2009), "An Advanced Least-Significant-Bit Embedding Scheme for Steganographic Encoding",*PSIVT 2009, LNCS 5414*, Springer, pp. 349–360.

[30] Smith, C. (2001), "Basic Cryptanalysis Techniques", *SANS Institute 2001*, GSEC Version 1.2f, http://www.sans.org.

[31] Kaur, R., Singh, B. and Singh, I. (2012), "A Comparative Study of Combination of Different Bit Positions In Image Steganography", *International Journal of Modern Engineering Research*, Vol.2, Issue.5, pp-3835-3840.

[32] Kruus, P., Caroline, S., Michael, H. and Mathew, M. (2002), "A Survey of Steganographic Techniques for Image Files", *Advanced Security Research Journal, Network Associates Laboratories*, pp.41-51.

[33] Kharrazi, M., Sencar, H. T. and Memon, N. (2004), "Image Steganography: Concepts and Practice", *WSPC/Lecture Notes Series: 9in x 6in*, pp.1-31.

[34] B, Li., J, He. and J, Huang. (2011), "A Survey on Image Steganography and Steganalysis", *Journal of Information Hiding and Multimedia Signal Processing*, Vol. 2, No. 2, pp. 142-172.

[35] Friedman, W.F. (1967), "*Cryptology*", *Encyclopedia Britannica*, Vol. 6, pp. 844-851, 1967.

[36] Kahate, A. (2008), "*Cryptography and Network Security*", 2nd Edition, Tata McGraw-Hill.

[37] Gonzalez, R. C. and Woods, R. E. (2002), "*Digital Image Processing*", 2nd edition, Prentice Hall, Inc.

Authors

Shamim Ahmed Laskar received his B.Sc. and M.Sc. degrees in Computer Science in 2006 and 2008 respectively from Assam University, Silchar, where he is currently doing his Ph.D. His research interest includes Image Processing, Steganography, Information Retrieval and Data Security.

Prof. Kattamanchi Hemachandran obtained his M.Sc. Degree from Sri Venkateswara University, Tirupati and M.Tech and Ph.D Degrees from Indian School of Mines, Dhanbad. Presently, he is serving as Head, Department of Computer Science, Assam University, Silchar. He is associated with this department since 1998. He is supervising many research scholars. His areas of research interest are Image Processing, Software Engineering and Distributed Computing.