International Journal of Engineering Science Invention
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org ||Volume 4 Issue 11|| November 2015 || PP.01-07

A Robust Technique to Encrypt and Decrypt Confidential Data within Image

Md. Shamimul Islam[1], Mahbuba Begum[2], Kanija Muntarina[3], and Md. Golam Moazzam[1]

[1]*Department of CSE, Jahangirnagar University, Savar, Dhaka-1342. Bangladesh.*
[2]*Department of CSE, Mawlana Bhashani Science and Technology University, Tangail, Bangladesh*
[3]*Department of CSE, Dhaka City College, Dhaka, Bangladesh.*

ABSTRACT *:* *The rapid development of data transfer through the Internet made it easier to send the data accurate and faster to the destination. There are many transmission media to transfer the data to destination like e-mails; at the same time it may be easier to modify and misuse the valuable information through hacking. So, in order to transfer the data securely to the destination without any modifications, there are many approaches like cryptography and steganography. This paper deals with a new technique steganography to hide encrypted confidential data within images. Steganography is the art of hiding the fact that communication is taking place, by hiding information in other information. Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the internet. For hiding secret information in images, there exist a large variety of steganography techniques. Some are more complex than others and all of them have respective strong and weak points. Different applications may require absolute invisibility of the secret information, while others require a large secret message to be hidden. This paper intends to give a brief idea about the new image steganographic approach that makes use of Least Significant Bit (LSB) algorithm for embedding the data into the bit map image.*

KEYWORDS - *Cryptography, Embedding technique, LSB, Steganography, Stegoimage.*

I. INTRODUCTION

With the rapid growth of computer networks, data security 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]. It is the art and science of hiding information into picture or other media in such a way that no-one apart from the sender and intended recipient even realizes there is a hidden information [2], [3]. This includes the concealment of digital information within computer files. Generally, a steganographic message will appear to be something else, may be picture, video, sound file, even the radio communication. This apparent message is the covertext. For instance, a message may be hidden by using invisible ink between the visible lines of innocuous documents. The hidden information is called stego message which may be open message, but may be encrypted one as well. Data hiding [4] in the image has become an important technique for image authentication. Ownership verification and authentication is the major task for military people, research institute and scientist. It refers to the nearly invisible embedding of information within a host data set as message, image, and video. In steganographic [5], [6] applications, the hidden data may be secrete message or secrete hologram or secrete video whose mere presence within the host data set should be undetectable; The goal of steganography is to hide the message in the source image by some key techniques and cryptography is a process to hide the message content. To hide a message inside an image without changing its visible properties [7] the source image may be altered. The most common methods to make these alteration involves the usage of the least-significant bit (LSB) developed by masking, filtering and transformations on the source image [8].

This paper focuses on the technique to secure data or message with authenticity and integrity. The entire work has been done in MATLAB. In this work, the secret message is encrypted before the actual embedding process starts. It uses a simple encryption technique and a secret key and hence it will almost be impossible for the intruder to unhide the actual secret message from the embedded cover file without knowing secret key. Only receiver and sender know the secret key. N-bit LSB substitution technique is used as embedding and extraction method.

II. LITERATURE REVIEW

Information security and image authentication has become very important to protect digital image document from unauthorized access. 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 [9]. 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 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 [10]. Steganography pay attention to the degree of invisibility while cryptography pays attention to the security of the message. Once the presence of hidden information is revealed or even suspected, the purpose of steganography is partly defeated. The strength of steganography can thus be increased by combining it with cryptography.

Steganography relies on hiding message in unsuspected multimedia data and is generally used in secret communication between acknowledged parties [11]. The technique replaces 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 [12]. All digital file formats can be used for steganography, but the formats those are with a high degree of redundancy are more suitable. 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 [13]. Cryptography merely obscures the integrity of the information so that it does not make sense to anyone except the creator and the recipient. Steganography could be considered as the dark cousin of cryptography. Cryptography assures privacy whereas Steganography assures secrecy. 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 [14]. 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 [15]. Security means the embedding algorithm is said to be secure if the embedded information cannot be removed beyond reliable detection by targeted attacks [16]. 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.

III. PROPOSED METHOD

Ensuring data security is a big challenge for all computer users. To enhance the embedding capacity of image steganography and provide an imperceptible stegoimage for human vision, it proposes 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 can also be implemented to cryptographic data so that it increases the security of this data. The method first encrypts a message using transposition cipher technique and then embeds the encrypted message inside an image using LSB embedding technique. The block diagram of proposed system is as shown in Fig. 1.

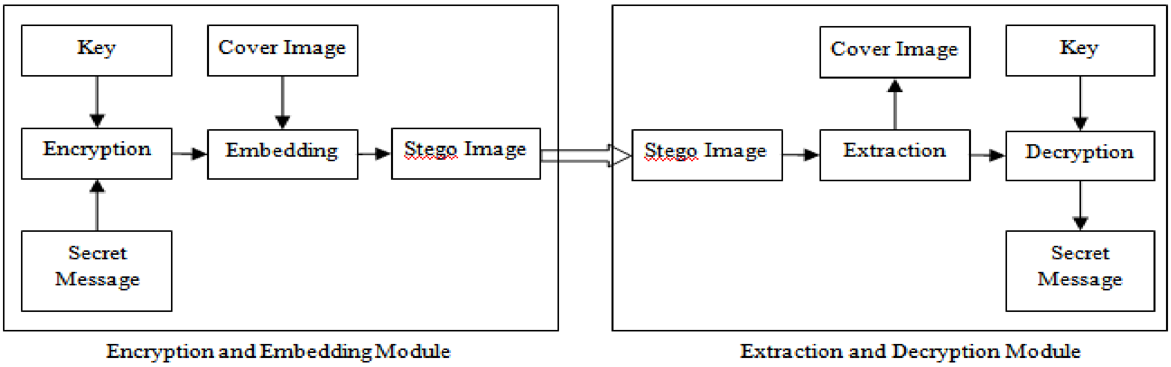


Fig. 1: Block Diagram of the Proposed System

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-image, he/she would still require the cryptographic decoding method to decipher the encrypted message.

3.1 Encryption Procedure

This encryptiom procedure is simple and efficient and is of symmetric type where only receiver and sender know the secret key. The secret key length is variable and is of range double precision. At the receiver side during extraction process the decryption, that is the reverse process of encryption is carried out using the same key to obtain the secret message from the stego-image. In 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 [17]. The 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. 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.

3.2 Data Embedding Procedure

Least Significant Bit substitution method is a very simple approach for embedding information in a cover image. The basic idea is to insert the secret message in the least significant bits of the images. The algorithm has to take the first *N* cover pixels, where *N* is the total length of the secret message that is to be embedded in bits. After that every pixel's last bit will be replaced by one of the message bits. To explain how the data embedding procedure works, let us consider the following cover image.

Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7	Byte 8
10101101	01011100	10011100	00101101	11000100	01101100	11010010	10110111

Suppose a secret number 183 is to embed. The binary equivalent of the number is 10110111. At least 8 bytes in cover image are needed to embed the secret number 183. Now modify the LSB of each byte of the cover image by each of the bit of the secret number 10110111. Table-1 shows the data embedding procedure for this secret number 183.

Table 1: Data Embedding Procedure using LSB Method

Before Embedding	After Embedding	Bit Inserted	Consequences
10101101	10101101	1	No change in bit pattern
01011100	01011100	0	No change in bit pattern
10011100	10011101	1	Change in bit Pattern
00101101	00101101	1	No change in bit pattern
11000100	11000100	0	No change in bit pattern
01101100	01101101	1	Change in bit Pattern
11010010	11010011	1	Change in bit Pattern
10110111	10110111	1	No change in bit pattern

3.3 Data Extraction Procedure

The data extraction procedure is the inverse of the data embedding procedure. In this procedure the secret message is extracted from the stego-image. The receiver inputs the stego-image to the data extraction algorithm. The LSBs of each pixel of stego-image is extracted and placed in an array. Each 8 bit from the array is then converted into characters. This output is actually encrypted form of the original message. Then the message is decrypted using the same transposition method that is used in encrypting. In decrypting, the ciphertext is written row wise in a matrix of same size as in encrypting method. To get the plaintext, the matrix will be read out column wise in a specific order depending on the key.

IV. IMPLEMENTATION AND EXPERIMENTAL RESULTS

Fig. 2 shows the steganography process of the cover image being passed into the embedding function with the message to encode resulting in a stego-image containing the hidden message. A key is used to protect the hidden message. The key is usually a password also used to encrypt and decrypt the message before and after embedding. Secret message can be hidden inside all sorts of cover information: text, images, audio, video and more. However, there are tools available to store secrets inside almost any type of cover source. The most important property of a cover source is the amount of data that can be stored inside it, without changing the noticeable properties of the cover image.

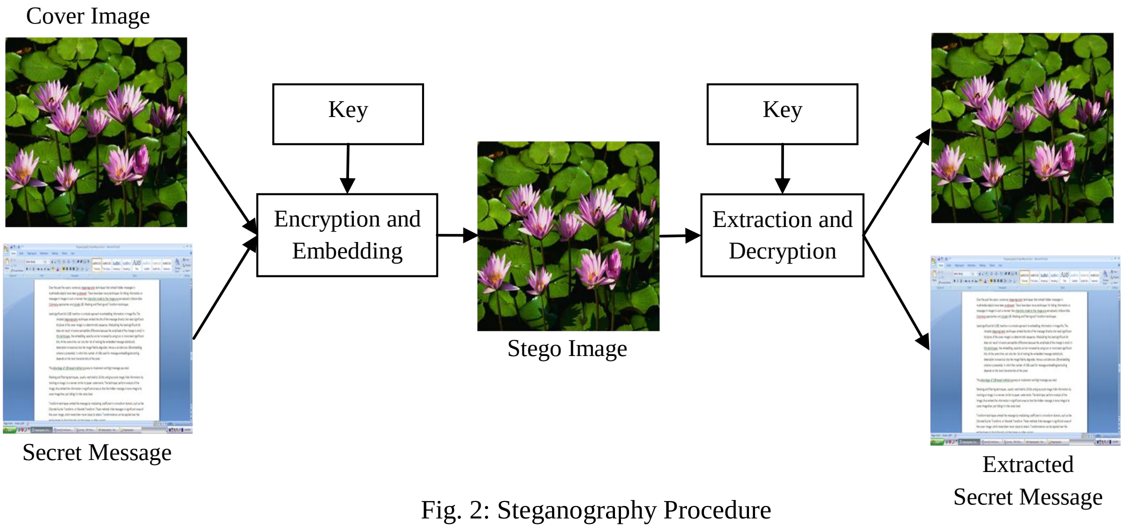


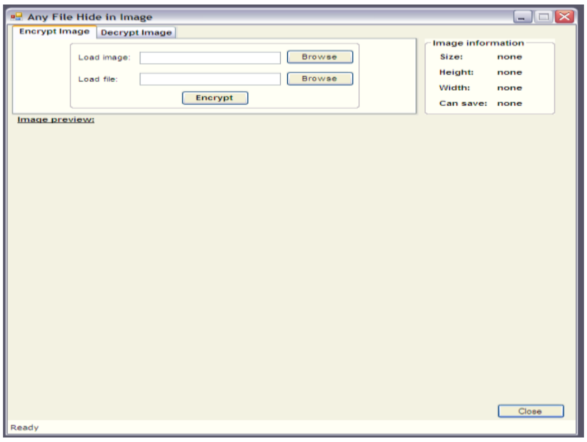
Fig. 2: Steganography Procedure

It has basically two modules: i) Encryption and Embedding Module, and ii) Extraction and Decryption Module. First module is used to hide encrypted information into the image; no one can see that information. This module requires any type of image and message and gives the only one image file in the destination.

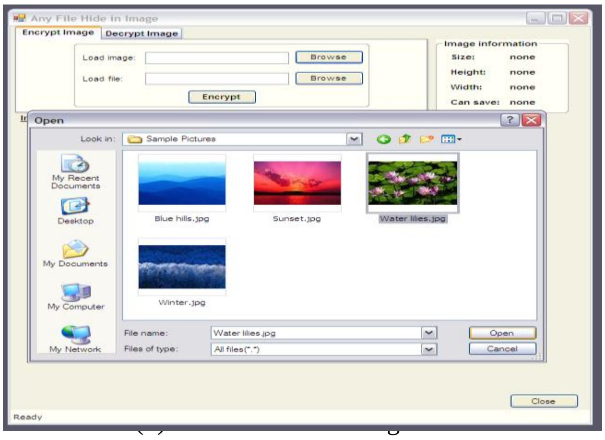
Second module is used to get the hidden information in an image file. It takes the image file as an output, and gives two files at the destination folder, one is the same image file and another is the original message file.

The graphical representation of the system is as follows:

1. Encryption and Embedding Module. Select two files: Image file and Message file as input.

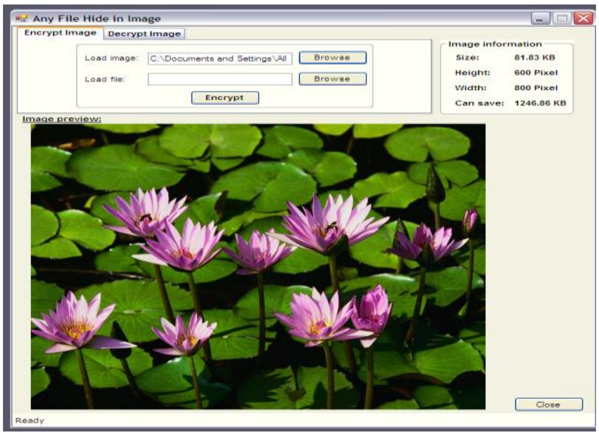


Size: none
Height: none
Width: none
Can save: none

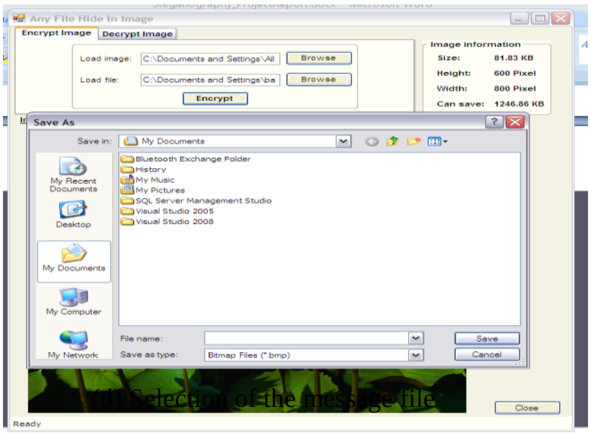


Size: none
Height: none
Width: none
Can save: none

Look in: Sample Pictures
File name: Water lilies.jpg
Files of type: All files(*.*)



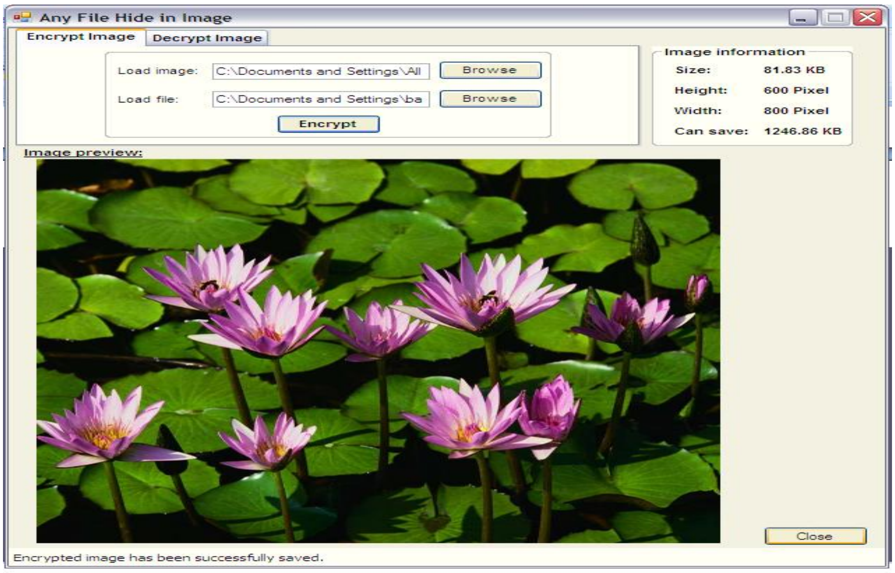
Load image: C:\Documents and Settings\All
Size: 81.83 KB
Height: 600 Pixel
Width: 800 Pixel
Can save: 1246.86 KB



Load image: C:\Documents and Settings\All
Load file: C:\Documents and Settings\ba
Size: 81.83 KB
Height: 600 Pixel
Width: 800 Pixel
Can save: 1246.86 KB

Save in: My Documents
File name:
Save as type: Bitmap Files (*.bmp)

(d) Selection of the message file



Load image: C:\Documents and Settings\All

Load file: C:\Documents and Settings\ba

Image information

Size: 81.83 KB

Height: 600 Pixel

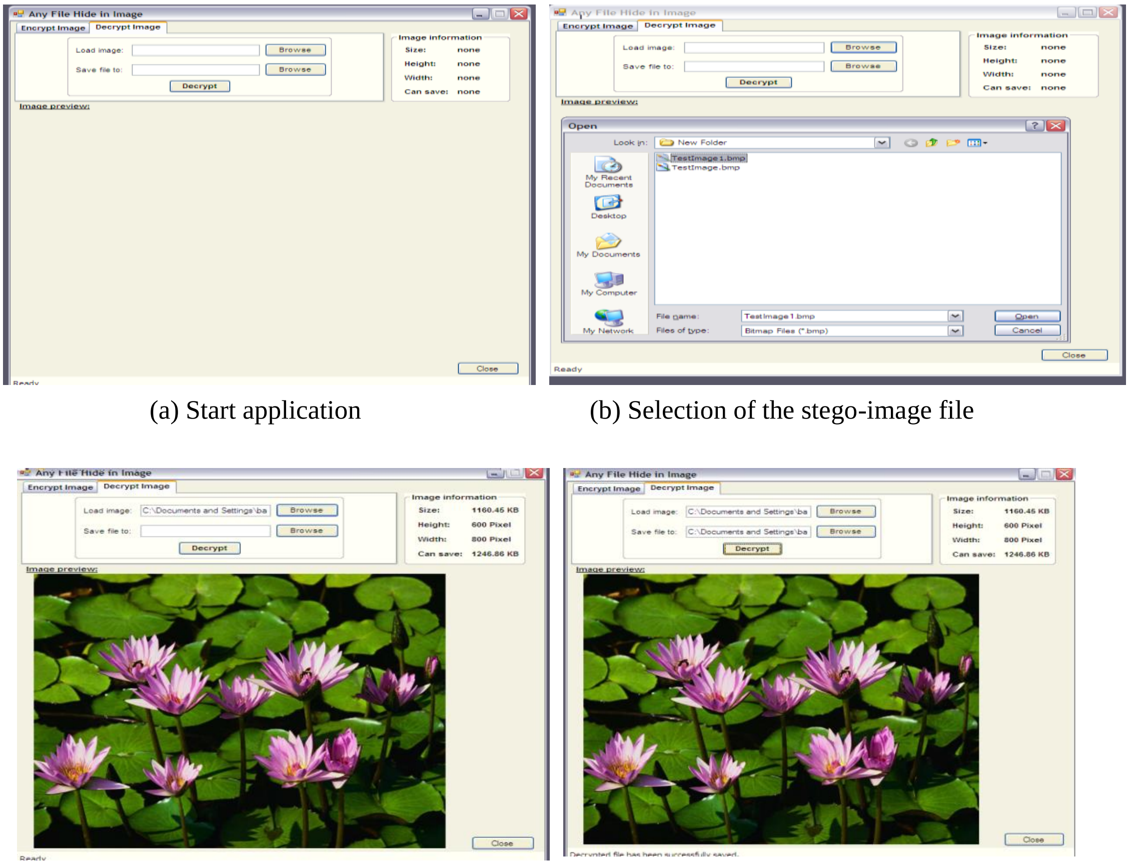
Width: 800 Pixel

Can save: 1246.86 KB

Encrypted image has been successfully saved.

Fig. 3: Encryption and Embedding Module

2. Extraction and Decryption Module. Select Stego-image file as input.



Load image:

Save file to:

Image information: Size: none; Height: none; Width: none; Can save: none

Ready

(a) Start application

Look in: New Folder

TestImage1.bmp

TestImage.bmp

File name: TestImage1.bmp

Files of type: Bitmap Files (*.bmp)

(b) Selection of the stego-image file

Load image: C:\Documents and Settings\ba

Save file to:

Image information: Size: 1160.45 KB; Height: 600 Pixel; Width: 800 Pixel; Can save: 1246.86 KB

Ready

(c) Preview of the stego-image

Load image: C:\Documents and Settings\ba

Save file to: C:\Documents and Settings\ba

Image information: Size: 1160.45 KB; Height: 600 Pixel; Width: 800 Pixel; Can save: 1246.86 KB

Decrypted file has been successfully saved.

(d) After extraction generated message file

Fig. 4: Extraction and Decryption Module

V. CONCLUSION

Data security is the most important issue in any communication. Lots of data security and data hiding algorithms have been developed in the last decade. Steganography has its place in security. It is the art of hiding information and an effort to conceal the existence of the embedded information. This work is a combination of steganography and cryptography, which provides a strong backbone for its security. Original message is being hidden within a carrier such that the changes so occurred in the carrier are not observable. In this paper we have discussed how digital images can be used as a carrier to hide messages. Steganography is a useful tool that allows covert transmission of information over communication channel. Combining secret image with the carrier image gives the hidden image. The hidden image is difficult to detect without retrieval. The entire work has done in MATLAB. The hidden message is encrypted using a simple encryption algorithm using secret key and hence it will be almost impossible for the intruder to unhide the actual secret message from the embedded cover file without knowing secret key.

Steganography has numerous useful applications. However, it can be misused like other technologies. For instance terrorists may use this technique for their secret secure communication.

REFERENCES

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

[2] Ghoshal N., Mandal, J. K., "Masking based Data Hiding and Image Authentication Technique (MDHIAT*)", Proceedings of 16th International Conference of IEEE on Advanced Computing and Communications ADCOM-2008, ISBN: 978-1-4244-2962-2, December 14-17th, Anna University.*

[3] S. Pavan, S. Gangadharpalli and V. Sridhar, "Multivariate entropy detector based hybrid image registration algorithm", IEEE Int. Conf. on Acoustics, Speech and Signal Processing, Philadelphia, Pennsylvania, USA, pp. 18-23, March 2005.

[4] P. Moulin and J. A. O'Sullivan, "Information-theoretic analysis of information Hiding", IEEE Trans. On Info. Theory, Vol. 49, No. 3, pp. 563-593, March 2003.

[5] C. Rechberger, V. Rijman and N. Sklavos, "The NIST cryptographic Workshop on Hash Functions", IEEE Security & Privacy, Vol. 4, pp. 54-56, Austria, Jan-Feb 2006.

[6] C.Y. Lin and S. F. Chang, "A robust image authentication method surviving JPEG lossy compression", Proc. SPIE, Vol. 3312, San Jose, pp. 296-307, Jan. 1998.

[7] S. Dumitrescu, W. Xiaolin and Z. Wang, "Detection of LSB steganography via sample pair analysis", *IEEE Trans. on Signal processing, Vol. 51, No. 7, pp. 1995-2007, 2003*

[8] R., Chandramouli, and Nasir Memon., "Analysis of LSB based image steganography techniques." *International Conference on Image Processing, 2001, IEEE, Vol. 3, pp. 1019-1022.*

[9] Petitcolas, F.A.P., Anderson, R. J. and Kuhn, M.G. "Information Hiding -A Survey*", Proceedings of the IEEE, Special issue on Protection of Multimedia Content, Vol. 87, No. 7, 1999, pp.1062-1078.*

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

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

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

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

[14] 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.*

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

[16] Soumyendu Das, Subhendu Das, Bijoy Bandyopadhyay, Sugata Sanyal, "Steganography and Steganalysis: Different Approaches", *International Journal of Computers, Information Technology and Engineering (IJCITAE), Vol. 2, No 1, June, 2008, Serial Publications, pp. 1-11.*

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

AUTHOR'S PROFILE

Md. Shamimul Islam completed his B.Sc (Hons) and M.S. in Computer Science and Engineering from Jahangirnagar University in 2011 and 2012 respectively. His research interests include Image Processing, Mobile Applications Development, Software Engineering and so on.

Mahbuba Begum received her B.Sc. and M.S. degree in Computer Science and Engineering from Jahangirnagar University, Bangladesh, in the year 2007 and 2009, respectively. Currently, She is serving in the Department of Computer Science and Engineering, Mawlana Bhashani Science and Technology University, Tangail, Bangladesh as a Lecturer. Her research interest is image processing, pattern recognition, face recognition & trademarks recognition

Kanija Muntarina completed her B.Sc (Hons) in Computer Science and Engineering from Jahangirnagar University in 2003 and M.S. in Computer Science and Engineering from the same University in 2005 respectively. Currently, She is an Assistant Professor in the Dept. of Computer Science and Engineering, Dhaka City College, Dhaka, Bangladesh. Her research interests include Artificial Intelligence, Neural Networks, Computer Vision, Image Processing and so on.

Md. Golam Moazzam completed his B.Sc (Hons) in Electronics and Computer Science and M.S. in Computer Science and Engineering from Jahangirnagar University in 1997 and 2001 respectively. His research interests include Digital Image Processing, Artificial Intelligence, Computer Graphics, Neural Networks, Computer Vision and so on.