Sindh Univ. Res. Jour. (Sci. Ser.) Vol.48 (1) 151-154 (2016)

SINDH UNIVERSITY RESEARCH JOURNAL (SCIENCE SERIES)

Stego Block Chaining: A Secure 4LSB Steganography Technique

M. ISMAIL, S. KHAN, M. NAEEM*, N. AHMAD[++]

Department of Computer Systems Engineering, University of Engineering and Technology, Peshawar

Received 8th May 2014 and Revised 25th March 2015

Abstract-Least significant steganography is the most adopted technique for data hiding in digital images. This results in quality stego image, but the retrieval of hidden information is very easy. The intruder only need to read the least significant bits of the cover image, if the presence of secret information is suspected. To make the retrieval of information difficult a new mechanism is presented in this paper. The proposed stego block chaining technique composed of multiple stages to enhance the security of hidden information. The stego block chaining is implemented using 4LSB steganography. The security of the stego block chaining increase with the increasing number of stages but the hiding capacity deceases. The stego block chaining results in the peak signal to noise ratio of more than 40dB.

Keywords: Steganography, Chipper Block Chaining, Stego Block Chaining, Steganalysis

1. INTRODUCTION

Steganography is the science of hiding secret information in other information. The word steganography is actually the combination of two Greek words, “Stegos” meaning hidden or covered and “Graphia” meaning writing (Krenn.2004, Khan *et. al.* 2015). It is used for secure transmission information in an unpredictable manner. Various methods have been proposed in the spatial and transform domain to carry out steganography (Swanson *et. al.* 1998, Fridrich *et. al.* 2001). In spatial domain data is hidden in the least significant bits of cover image pixels e.g. in 4LSB steganography is the 4 least significant bits of the cover image pixels are substituted with secret information bits. This technique is very effective and creates high quality stego images (Johnson *et. al.* 1998). But once the existence of the secret information is suspected by an intruder the recovery of information is very easy (Khan *et. al.* 2013). To make the recovery of information, if detected, difficult for the intruder a new data hiding technique, called variable least significant bits (VLSB) steganography was proposed by Khan *et. al.* (Khan *et. al.* 2013). In transform domain data is hidden in the transform coefficient. In discrete cosine transform is mostly used for this purpose and data hidden in the least significant bits of DCT coefficients (Khan *et. al.* 2013).

While Cryptography means secret writing, in data transmission over un-trusted medium such as the internet, cryptography is necessary (Katz *et. al.* 2014, Menezes *et. al.* 1996). Various types of cryptography, i.e. symmetric cryptography, asymmetric cryptography and hash function (Akkar *et. al.* 2001). The text to be hidden is said as a plain text while an encrypted text is said as a cipher text. In symmetric cryptography, both sender and receivers use the same key for encryption and decryption respectively and in asymmetric cryptography different keys are used by sender and receiver for their respective purposes while in hash function, no key is used as cipher text cannot be recovered (Akkar *et. al.* 2001).

There are two categories in secret key cryptography, i.e. stream cipher and block cipher. A single bit or computer word is encrypted in stream cipher and a feedback mechanism change the secret key for operating on the next bit or computer word while in block cipher every time same key is applied to a block of information (Feistel *et. al.* 1982). The main purpose of the cipher block is to provide confidentiality and authentication (Bellare *et. al.* 2000). This method is important in encryption and decryption of a fixed length of data bits called block. To secure whole data the method is repeated for all the blocks of given data. Cipher Block has different types of implementation i.e. Electronic Codebook mode, Cipher Block Chaining mode, Cipher Feedback mode and Output Feedback mode (William. 2006).

This paper present a new block chaining technique of data hiding called stego block chaining in the inspiration from chipper block chaining.

2. PROPOSED METHOD

Inspired from “Cipher Block Chaining” a new technique will be developed as “Stego Block Chaining” for enhancing security. In Cipher Block Chaining (CBC) data is divided in blocks and encryption is applied on each individual block having different encryption key for each block. The main purpose of CBC is security confidentiality of the message signal. Stego Block Chaining (SBC) would be implemented in a slight different way from CBC. The Block diagram of SBC is given in **(Fig. 1),** bellow:

[++]Corresponding Author email: N. Ahmad, n.ahmad@nwfpuet.edu.pk, Ph. No +92-91-9216590

*Department of Computer Science, University of Peshawar

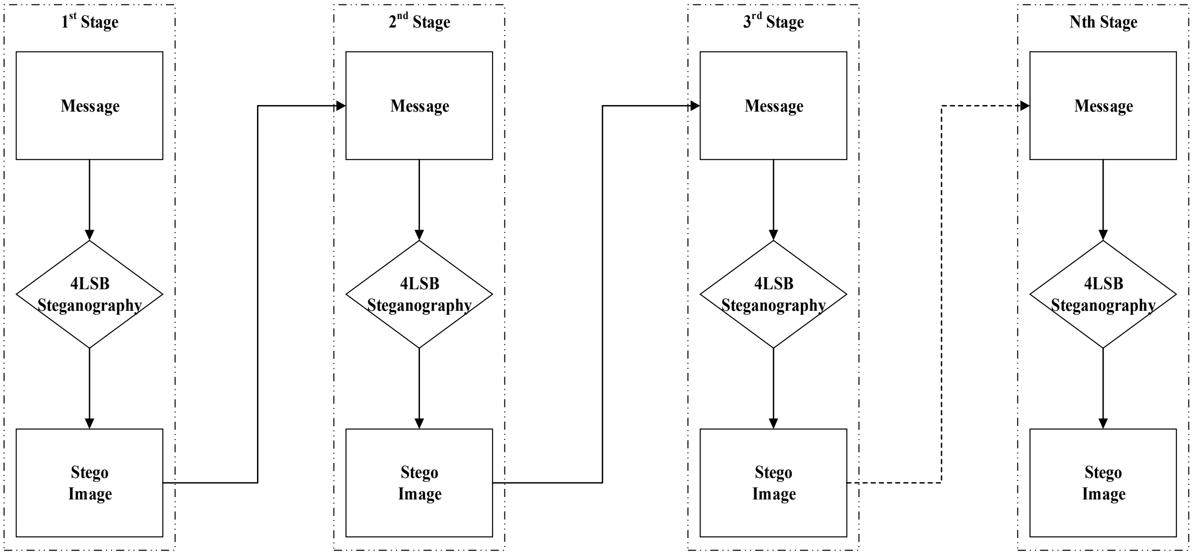

Fig. 1: Block diagram of SBC

This technique is proposed to have "N" number of stages where *N>2* depending on the required data hiding capacity.

In the proposed technique message will be hidden in 4-Least significant Bits (4LSB) of cover image. Each stage is having 50% data hiding capacity so in each stage, the cover image should be double in size as that of the corresponding secret message. In the 1st stage secret message will be hide using 4LSB steganographic technique and the resultant stego image of the 1st stage will act as the secret message for 2nd stage. This process will continue up to "N" number of stages and at each stage the message will be the stego image of the previous stage except 1st which will be the original message to hide. As the number of stages increases it becomes hard to detect or retrieve the message.

3. SECURITY OF SBC

By adding addition stages in the above process has the primary objective of enhancing security of the hidden information. As the process shows that after the first stage, the hidden information retrieval probability is 50% because of the fact that if information is suspected the reverse process of 4LSB steganalysis can recover the data. At the second stage probability of hidden information retrieval becomes 25% as two reverse iterations will be used to recover information. As the stages are increased the probability of retrieval of the hidden message is decreasing as in eq. (1).

$$P_N = 1/2^N \qquad (1)$$

Where P_N is the probability of retrieval by an intruder at stage N.

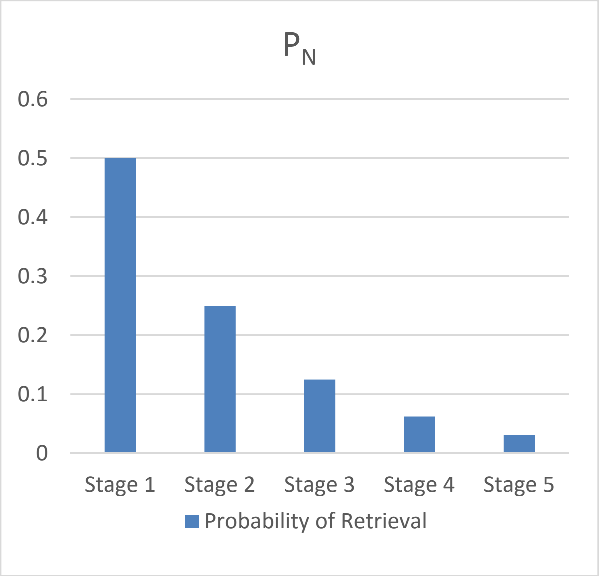

Fig. 2: The Probability of Retrieval

Graph in **(Fig. 2,3)** show that by decreasing the probability of retrieval, security of information is increasing.

4. THE HIDING CAPACITY OF SBC

Hiding capacity of the proposed method is decreasing at each addition stage to be added by half. As it is evident from the previous discussion that at each stage cover image should be double in size as that of the message so the hiding capacity become 50%. As the stages increases hiding capacity will decrease by half of that previous stage. The given equation shows it mathematically

$$C_N = 1/2^N \qquad (2)$$

Where C_N is hiding capacity at stage N.

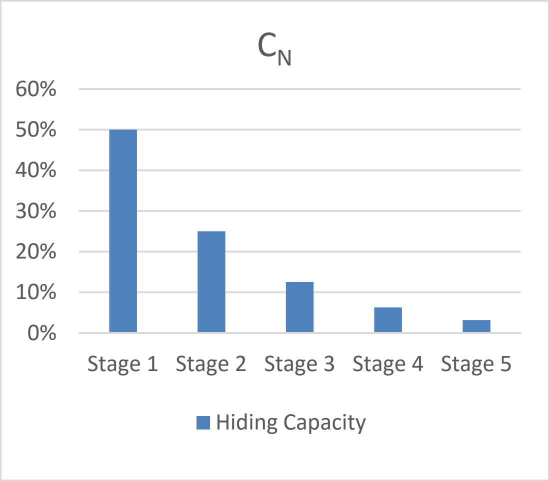

Fig. 3: Hiding Capacity

5. EXPERIMENTAL RESULTS

As the process was repeated to get the desired result in such a manner that the secret message was hidden in the cover image in the first iteration. The secret message is given in **(Fig. 4)** having size of 400x200. This secret message had to be hidden in the cover image of the double of its size. **(Fig, 5(a))** shows cover image of size 400x400 for the first stage of the SBC. **(Fig. 6(a)** shows stego of the first stage. For the second stage Fig. 6(a) is the secret message and Fig. 5(b) is cover image and the resultant stego image is Fig. 6(b). Size of the image in Fig. 6(a) is 400x400 and cover image size should be double of it i.e.800x400.The resultant stego image in Fig. 6(b) is also having the size of 800x400. For the third stage cover image of the double size of the stego image of the second stage would be used. Fig. 5(c) will be cover image for stego image Fig. 6(b) that will act as the secret message for the third stage and the resultant stego image will be Fig. 6(c). This process will continue to "N" number of stages. Fig. 6(e) show the final stego image in the below given five stages of SBC process.

Fig. 4: The secret message (400x200)

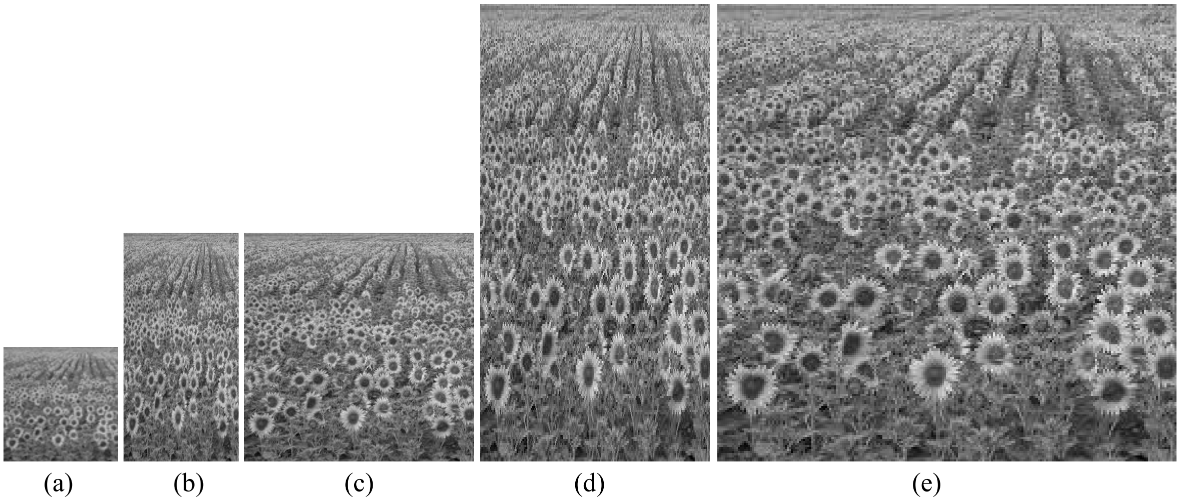

Fig. 5: Cover images a) cover image (400x400) b) cover image (800x400) c) cover image (800x800) d) cover image (1600x800) e) cover image (1600x1600)

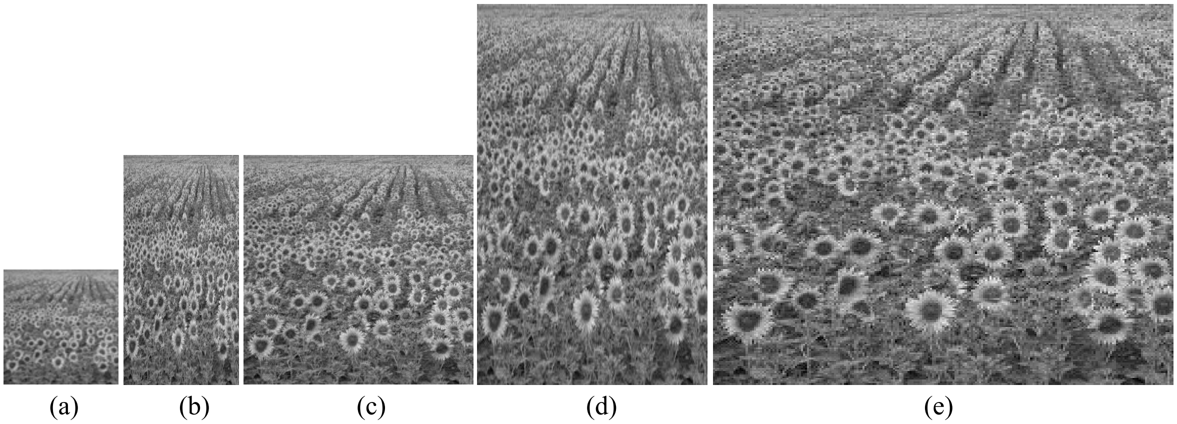

Fig. 6: Stegoimages a) Stego image (400x400) b) Stego image (800x400) c) Stego image (800x800) d) Stego image (1600x800) e) Stego image (1600x1600)

PSNR was calculated of each stage in SBC and the tabulated in the **(Table. 1).** Resultant stego image PSNR is above 40dB which is in the acceptable range.

Table 1: PSNR at different stages

Stage No	Size Cover	PSNR (dB)
1	400x400	42.56
2	800x400	41.52
3	800x800	41.71
4	1600x800	42.01
5	1600x1600	41.2645

6. CONCLUSION

As 4LSB steganography has limited security and data can be recovered by the intruder if suspected. In SBC, the primary focus is to increase security by a chain process and to make it hard for the intruder to recover secret data. Security level depends upon the number of stage applied in SBC. Higher the number of stages higher will be the security of the secret data. The actual key to recover the data in SBC is to find the number of iterations. The number of iteration should always be kept secret. On the other hand increasing the number of iteration decreases hiding capacity so higher the number of iteration in SBC increases security while decreasing hiding capacity. The stego image quality in each stage is above 40dB.

REFERENCES:

Akkar, M. L., and C. Giraud, (2001) An implementation of DES and AES, secure against some attacks. In Cryptographic Hardware and Embedded Systems—CHES. 309-318. Springer Berlin Heidelberg.

Bellare, M., J. Kilian, and P. Rogaway, (2000) The security of the cipher block chaining message authentication code. Journal of Computer and System Sciences. 61(3): 362-399.

Feistel, H., (1982) Stream/block cipher crytographic system. U.S. Patent 4,316,055, February 16, 1982.

Fridrich, J., M. Goljan, and R. Du, (2001) Invertible authentication. In Photonics West 2001-Electronic Imaging, International Society for Optics and Photonics. 197-208.

Johnson, N. F., (1998) Exploring steganography: Seeing the unseen. Computer. 31(2): 26-34.

Khan, S., and M. H. Yousaf, (2013) Implementation of VLSB Stegnography Using Modular Distance Technique. In Innovations and Advances in Computer, Information, Systems Sciences, and Engineering. 511-525. Springer New York.

Katz, J., and Y. Lindell, (2014) Introduction to modern cryptography. CRC Press.

Khan, S., N. Ahmad, and M. Wahid, (2016) Varying index varying bits substitution algorithm for the implementation of VLSB steganography. Journal of the Chinese Institute of Engineers. 39(1): 101-109.

Krenn, R., (2004) Steganography: Implementation and Detection. Available online on found online at< http://www. krenn. nl/univ/cry/steg/presentation/2004-01-21-presentation-steganography. pdf.

Menezes, A. J., C. P. C. VanOorschot, and S. A. Vanstone, (1996) Handbook of applied cryptography. CRC press.

Swanson, M. D., M. Kobayashi, and A. H. Tewfik, (1998). Multimedia data-embedding and watermarking technologies. Proceedings of the IEEE, 86(6): 1064-1087. DOI: 10.1109/5.687830.

William, S., and W. Stallings, (2006) Cryptography and Network Security, 4/E. Pearson Education India.