SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks (2017)
Published online in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.1769

RESEARCH ARTICLE

Enhanced stego block chaining (ESBC) for low bandwidth channels

Sahib Khan[1]*, Muhammad Ismail[2], Tawab Khan[3] and Nasir Ahmad[2]

[1] Department of Electronics and Telecommunication, Politecnico Di Torino, 10129 Torino, Italy
[2] Department of Computer Systems Engineering, University of Engineering and Technology Peshawar, 25120 Peshawar, Pakistan
[3] Department of Mathematics, Abdul Wali Khan University Mardan, 23200 Mardan, Mardan, Pakistan

ABSTRACT

This paper presents a new enhanced stego block chaining (ESBC) technique for data hiding to address the bandwidth and transmission time issues of simple stego block chaining (SBC). In simple SBC data hiding method, the security of the hidden information is increased by increasing the number of stages, but the addition of each stage decreases the hiding capacity. This increases the size of the data needed to transmit the secret message and thus results in an increase in the required bandwidth and transmission time. The proposed ESBC technique addresses the bandwidth and transmission time issues of the simple SBC method. The output of the ESBC is a high quality stego image with peak signal-to-noise ratio above 40 dB and provides the same additional security as simple SBC but reduces the requirements of the bandwidth and transmission time by one half of that of the simple SBC and, thus, solves the hiding capacity issues of SBC for low bandwidth channels. Copyright © 2017 John Wiley & Sons, Ltd.

KEYWORDS
stego block chaining; steganography; cryptography; steganalysis; payload

***Correspondence**
Sahib Khan, Department of Electronics and Telecommunication, Politecnico Di Torino, 10129 Torino, Italy
E-mail: engrsahib_khn@yahoo.com

1. INTRODUCTION

Steganography is the art of embedding secret information in other innocent information. The existence of information is not exposed to the eavesdroppers, and only the authorized or an intended person knows about the presence of secret information [1]. The word steganography is composed of two words from Greek language, “Stegos” and “Graphia” meaning covered writing [2]. Steganography keeps the secret information away from detection and even from suspicion of intruders.

Steganographers developed various methods to embed secret messages in cover file both in spatial and transform domain [2–4]. In spatial domain, steganographers make use of the least significant bits of cover image pixels. The LSB steganography, 4LSB steganography, VLSB steganography, data hiding in edge pixels, pixels value difference-based steganography and many more such techniques are part of this spatial domain data hiding family [5–10]. The transform domain data hiding methods uses the transform coefficient for the same purpose. Discrete cosine transform (DCT) is the most practiced transformation for steganography, and some of the DCT steganographic techniques are mentioned in [11–13]. Besides DCT, wavelet transform has been used for securing secret information too in [14].

However, the modification in pixel values and transformation coefficients creates some distortion, and if this distortion becomes visibly significant to attract the attention of eavesdropper, then the retrieval of hidden information is always attempted [10]. The integrity of data becomes at risk. So there is a need to make information more and more. To do so, cryptographic techniques are combined with steganographic techniques. The different types of cryptographic chippers can be the right choice to select, e.g. AES, DES, Hash functions etc. [15,16]. The use of cryptographic techniques combined with steganographic techniques ensures two-fold security. But, this increases the computation cost and processing time.

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 changes the secret key for operating on next bit or computer word while in block cipher every time same key is applied to a block of information [17]. The main purpose of cipher block is to provide confidentiality and authentication [18]. This method is important in encryption and decryption of 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 [17. 18].

This paper presents a new block chaining technique of data hiding called stego block chaining (SBC) in the inspiration from chipper block chaining.

1. STEGO BLOCK CHAINING

The SBC is an inspiration from a well-known cryptographic technique called cipher block chaining (CBC). CBC mode of encryption increases the security of encryption algorithms by arranging encryption techniques in cascade form. While SBC arranges steganographic technique, e.g. 4LSB in cascade form to increase the security of hidden information and make the steganographic technique more immune to steganalysis.

In 1976, IBM invented the CBC mode of encryption. It adds XOR a block of plaintext block to a ciphertext block previously produced, except the first block which is XOR plaintext block with an initialization vector. The result is then encrypted using the cipher algorithm, e.g. AES, DES etc. In CBC, each succeeding ciphertext block depends on the earlier one. The CBC implementation is shown in Figure 1.

SBC is a steganographic method that uses and connects 4LSB steganography blocks in a concatenated manner just like CBC that arranges ciphers in series concatenation. In CBC, data is divided in blocks, and encryption is applied on each individual block having different encryption key for each block. In SBC, whole secret message is dealt as one block, and the in place of encryption LSB substitution is applied to hide the secret message in the cover image. The stego image of previous steganographic block is fed as secret message to the next steganographic block to be embedded in the cover image, except the first one, in which original secret message is hidden in cover image. The SBC hides secret data by processing the secret message through a series of steganographic method, i.e. 4LSB steganography. On the other hand, SBC has no concept of initialization vector and encryption key as in CBC.

The CBC feed the cipher text of 1st stage as initialization vector to the 2nd stage and the cipher text of the 2nd stage is feed to the 3rd stage. Each stage of CBC converts the plain text to a cipher text. The cascade arrangement of CBC increases the security of secret information. In the same manner, the SBC is a series connected arrangement of steganographic methods [19]. The SBC implementation is shown here in Figure 2.

The SBC steganographic method uses steganographic technique of different stages. A number of stages "N" should be greater than or equal to 2 but not less than 2, i.e. $N > 2$. However, the SBC increases the size of data with increasing of stages. Each stage increases the size of cover image, indeed the stego image, by 2. This in turn increases the bandwidth and transmission time requirement for the original secret message to be transmitted completely over a communication channel.

In the SBC technique using 4LSB steganography, a message is hidden in the four 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. So, the 1st stage increases the size of transmittable data twice. The stage 2nd further increases the size and makes it 4 times of the original size and so on. The size of transmittable data becomes double with the addition of each new stage to SBC. This as a result increases the bandwidth and transmission time required for transmission of secret message over a communication link. The required bandwidth and transmission time versus number of stages "N" of SBC are discussed in the coming section.

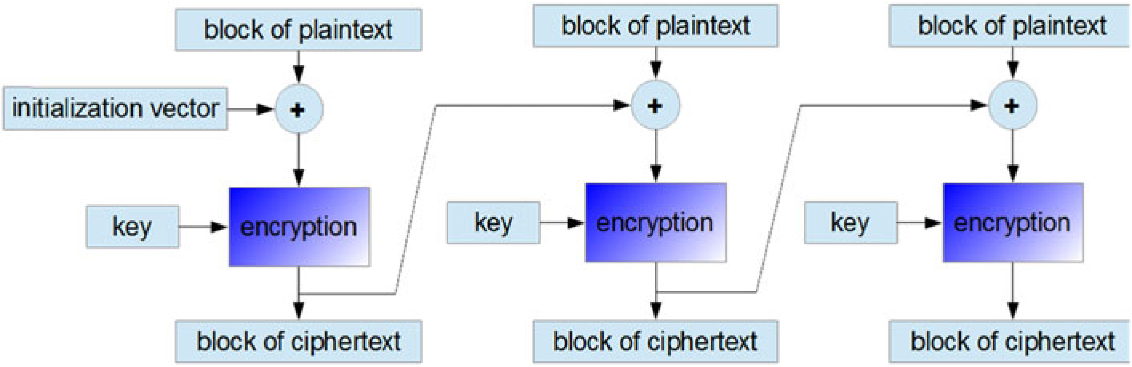


Figure 1. CBC encryption mode.

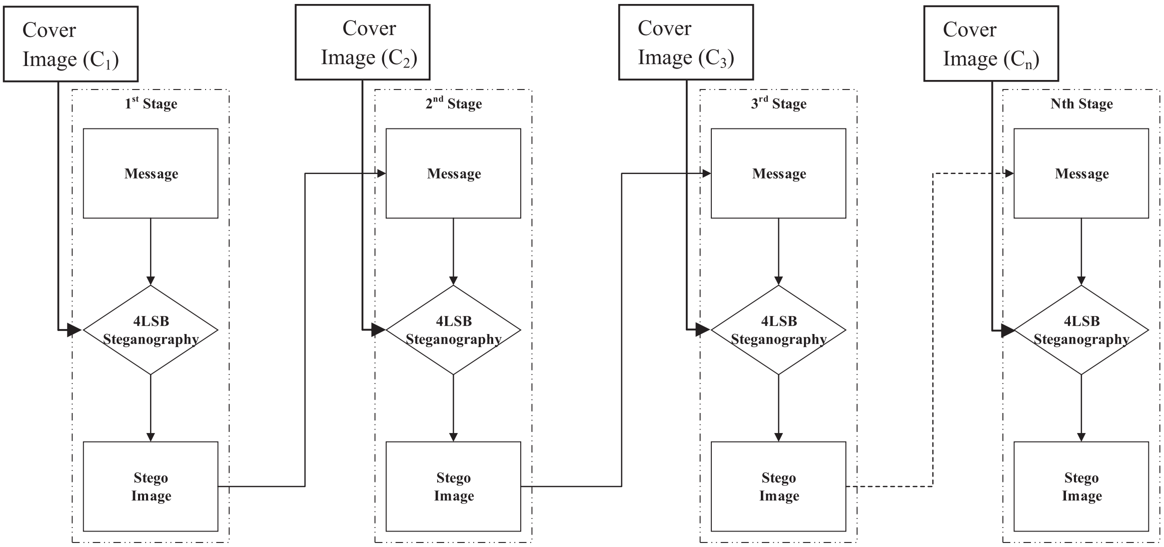


Figure 2. Stego block chaining.

2. BANDWIDTH AND TRANSMISSION TIME REQUIREMENT OF SBC

The main aim of a communication system is to transmit a given amount of data efficiently without any significant delay To use steganography for hiding secret information in cover medium increases the amount of transmittable data. For example, using 4LSB steganography makes the size of transmittable data double.

The SBC-based data hiding increases the size of data to a large extent. If SBC consisting of "*N*" number of stages is used to secure a message of "*m*" bits, the size of final cover image is "*m*'" bits, then "*m*'" is given by the equation as given:

$$m' = 2^N \times m$$

So, to send message "*m*" bits from sender to receiver, a data of "$2^N \times m$" bits has to be transmitted. Now, if transmission time is taken into consideration and the original message of "*m*" bits is transmitted over a communication channel of bandwidth "*D*", the message will take a time of "*t*" seconds from sender to receiver. The time "*t*" of transmission is given as in the equation below:

$$t = \frac{m}{D}$$

But using SBC of "*N*" stages, a cover image of "*m*'" bits has to be transmitted to send message of "*m*" bits securely, instead of message of "*m*" bits. Now, the time "*t*'" seconds are needed to transmit the final cover image with hidden information, over the channel of bandwidth "*D*" bps. The time "*t*'" is given by the equation below:

$$t' = \frac{m'}{D} = \frac{2^N \times m}{D}$$

$$t' = 2^N \times t$$

i.e. 2^N times larger than the transmission time of original message without using SBC.

Now, assume SBC is analyzed in terms of bandwidth requirement. If a data rate of "*D*" bps is sufficient to transmit a secret message "*m*", then using SBC of "*N*" stages to hide the message, it will need a data rate "D_{SBC}" to transmit cover image of "*m*'" bits having the hidden message of "*m*" bits inside it as:

$$D_{SBC} = 2^N \times D$$

This shows that it needs 2^N times more bandwidth to transmit the message of "*m*" bits after hiding using SBC.

The whole discussion and mathematical equations show that SBC increases the size of transmittable data significantly, which in turn increases the bandwidth requirements and increases the transmission time. The increase in data rate requirement also results in delay over a low bandwidth channel. To address these issues and to reach to an appropriate solution are the main aims of this work.

3. PROPOSED TECHNIQUE

In today's world of modern communication, only exchange of information is not sufficient. It requires high security measure to be adapted to exchanges of information between sender and receiver and ensure its security and integrity. The SBC is one such a method used to ensure the security of secret information, but this method increases the size of transmittable information. To send a secret message of "*m*" bits, secured with SBC technique of "*N*" stages, the sender has to transmit a net amount of "*C*" bits as given by the equation below:

$$C = 2^N \times m$$

The increased amount of data will require more bandwidth to transmit data completely, without any delay. Most of the channels are band limited and cannot provide data rate greater than a specific limited value. The only solution lift is to reduce the size of data, i.e. message.

In the proposed method, the message is preprocessed. In preprocessing, the size of message is reduced by half. This is achieved by combining the two message elements and converting to one element. The least significant bits of the two elements are discarded, and both are combined by replacing the 4LSB of the first element with the four most significant bits (4MSBs) second element, and hence one single message element is obtained by combining two elements as shown in Figure 3. Similarly, all the message elements considered two at a time are combined to generate one element. This process converts a message of “*m*” bits to a modified message of “m''” bits.

The preprocessed message of “m''” bits is a hidden cover medium by passing through “*N*” number steganography stages using SBC. The complete process of hiding reduce sized secret message in cover image using “*N*” stages of SBC is shown here in Figure 4.

On the receiver side, a reverse process is applied to retrieve the hidden message. However, the recover message of “*m* ’ ”” bits is not the original message of “*m*” bits. The recovered message of “*m* ’ ”” bits is further processed and expanded to get final message. Each element of the recovered massage of “*m* ’ ”” bits is divided into two elements by making 4MSBs of the recovered message as the 4MSBs of 1st element of final message and 4LSBs of the same recovered message of “*m* ’ ”” as 4MSBs of the 2nd element of the final message. Similarly, other elements of recovered message are expanded into two elements of final message. The expansion processed is shown here in Figure 5.

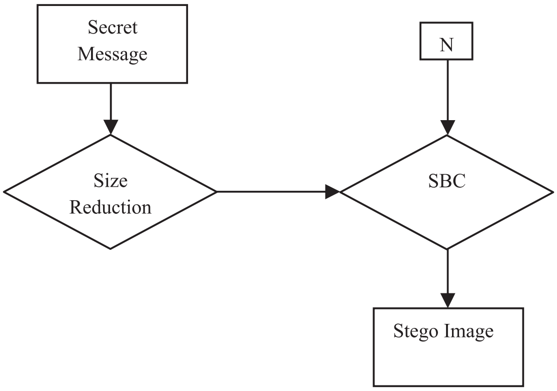


Figure 4. Implementation of proposed method.

4. BANDWIDTH REQUIREMENT OF ENHANCED SBC

To address the bandwidth limitation, the secret message size is reduced by ignoring the LSB of each message elements, and two consecutive message elements are combined to form one element as explained in Figure 2. This process reduces the message of “*m*” bits to a modified message of “m''” bits, which is half in size as that of the original secret message. The modified message of “*m* ’ ”” bits is secured by passing through a series steganography stages, and finally a stego image “S_n” is obtained. The size “*C*” of the final stego image “S_n” in terms of bits is given by the equation below:

$$C = 2^N \times m''$$

Now as:

$$m^{''} = \frac{m}{2}$$

So

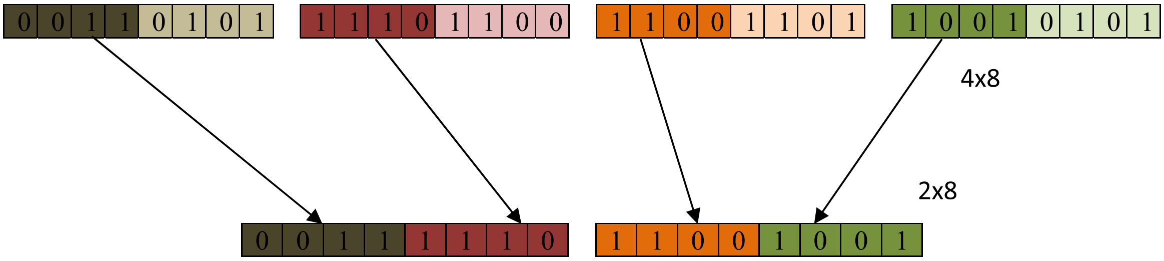
$$C = 2^{N-1} \times m$$

Now, to send the secret message of “*m*” bits from sender to receiver, a total of “$2^{N-1} \times m$” has to be transmitted. If a channel of bandwidth “*D*” bps is used to transmit the “$2^{N-1} \times m$” bits, it will take time “*t* ’ ”” as given by equation: $t^{''} = \frac{2^{N-1} \times m}{D}$Now as $t^{'} = \frac{2^N \times m}{D}$ so

$$t'' = \frac{t'}{2}$$

The equation above shows that the enhanced stego block chaining (ESBC) technique reduces the time “t''” required for transmitting the message from sender to receiver to half as compared to that of SBC, i.e. “t'”.

Now to analyze the bandwidth requirements of ESBC and compare with SBC, let us consider that a data rate of “*D*” bps is sufficient to transmit an original secret message of “*m*” bits, then using ESBC of “*N*” stages, to hide message, will need a data rate “D_{ESBC}” bps to transmit cover


0 0 1 1 0 1 0 1 | 1 1 1 0 1 1 0 0 | 1 1 0 0 1 1 0 1 | 1 0 0 1 0 1 0 1

0 0 1 1 1 1 1 0 | 1 1 0 0 1 0 0 1

Figure 3. Preprocessing of message to reduce size.

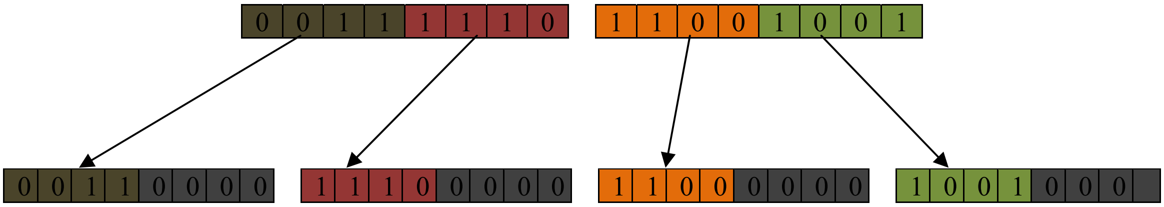


Figure 5. Expansion of retrieved message.

image of " S_n " of “$2^{N-1}\times m$” bits, having the hidden message of “m” bits inside it. The bandwidth “D_{ESBC}” bps required by ESBC is given by equation:

$$D_{ESBC} = 2^{N-1}\times D$$

As $D_{sbc} = 2^N \times D$ so,

$$D_{ESBC} = \frac{D_{SBC}}{2}$$

The above equation shows that ESBC technique is much efficient than SBC. The ESBC requires a bandwidth “D_{ESBC}” bps which is half of that required by SBC.

Figure 7. Cover image (Lena).

5. EXPERIMENTAL RESULTS

The proposed method is implemented using MATLAB and applied to hide a message in the different cover images of image database [21]. The image in Figure 6(a) is used as secret message. The size of secret message is reduced from 256 × 256 to 256 × 128 by neglecting the 4LSB of each pixels and combining the MSBs of two consecutive pixels to a single pixel. The reduce message is shown in Figure 6 (b).The process reduces the size to half. Then reduced message is hidden in cover image. The Lena image given in Figure 7 is used as cover for hiding the reduced message using SBC. In this work, three stages of SBC are used, and the stego image of stage 1st is used as message for 2nd, and similarly the stego image of stage 2nd is used as message for stage 3rd. The stego image of stage 3rd is the final stego image. As each stage uses 4LSB steganography, each stage required a cover image of double size than message of that stage. The stego images of stage 1st, 2nd and 3rd are given in Figure 8(a, b and c). The quality of stego image at each stage is measured using peak signal-to-noise ratio (PSNR) and mean squared error (MSE). The PSNR and MSE calculated after each stage are listed in Table I.

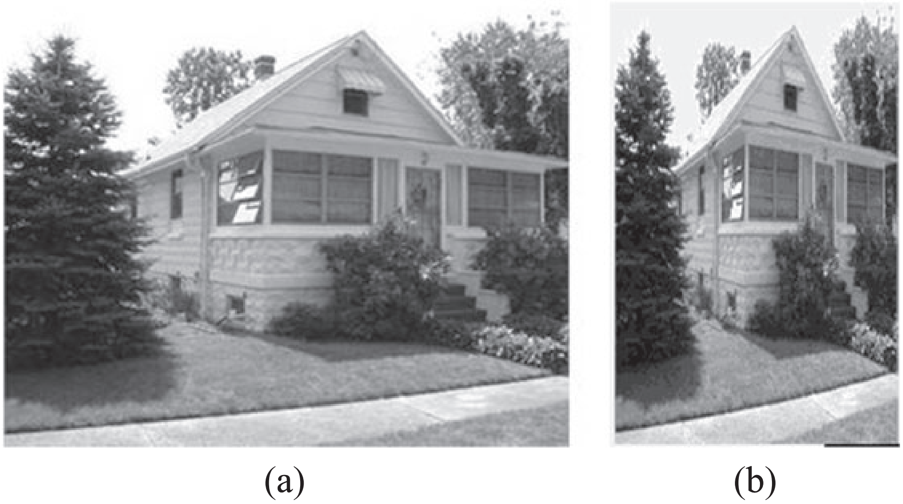


Figure 6. Message. (a) Original message. (b) Reduced message.

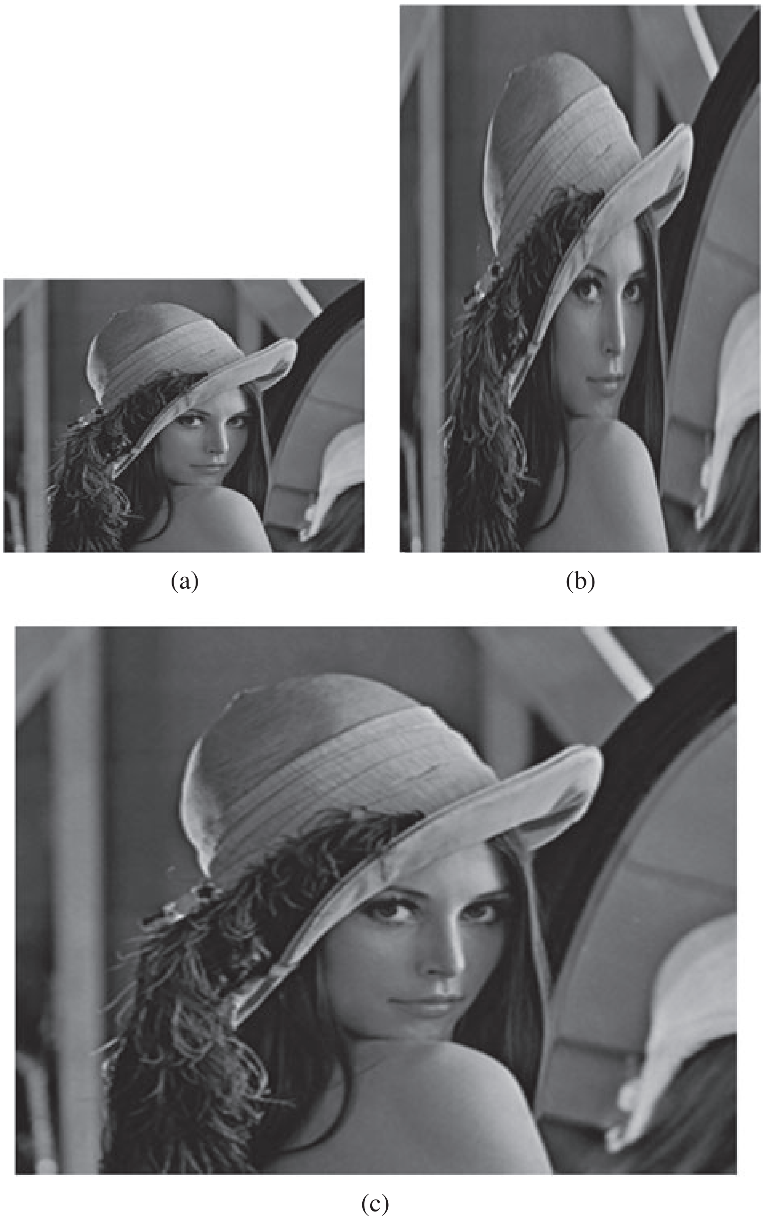


Figure 8. Stego images. (a) Stego image of stage 1st. (b) Stego image of stage 2nd. (c) Stego image of stage 3rd (final stage).

The secret message is also hidden in Couple, House, Tree, Child, Jellybeans, Chilly, Tiffany and other images from USC-SIPI image database [21], using ESBC, and the PSNR and MSE for stego images at each stage are calculated using the mentioned cover images. The PSNR and MSE calculated for the cover images are also listed in Table I.

The secret information is transmitted in hidden form by sending the final stego image to receiver. On the receiver side, the reverse process is applied, and after three stages of retrieval, the reduced message, hidden on the sender side, is recovered as shown in Figure 9(a). The recovered message image is expanded by converting one pixel in to two pixels. The final message obtained is shown in Figure 9(b). As the 4LSBs of the message are lost at the size reduction stage on the sender end and cannot be recovered, this causes some insignificant loss. However, the loss is not significant enough to distort the message. The quality of final recovered message is determined by calculating PSNR and MSE. The size, PSNR and MSE are listed here in Table II, using House, Girl, Jellybean and Flag image as message.

The results given Table II show that the recovered message image has a good quality with PSNR value 30 dB and higher.

Now, if the message information is very important and losses in message content cannot be afforded, then lossless compression tech techniques like run length encoding,

Table I. Quality of stego image of 1st, 2nd and final stage of SBC.

		Stage 1st		Stage 2nd		Stage 3rd (final stage)	
S. no.	Cover image	PSNR	MSE	PSNR	MSE	PSNR	MSE
1	Lena	44.67	2.22	44.68	2.21	44.66	2.23
2	Couple	42.9933	3.26	42.9853	3.27	42.9474	3.2987
3	House	45.58	1.8	45.70	1.75	45.61	1.78
4	Tree	43.39	2.98	43.15	3.15	43.2297	3.0911
5	Child	44.1168	2.52	47.8370	1.07	44.2214	2.46
6	Jellybeans	45.3662	1.89	43.0658	3.21	43.3451	3.01
7	Chilly	43.3741	2.99	42.4021	3.74	43.6592	2.80
8	Tiffany	42.3559	3.78	42.0030	4.10	43.8983	2.65
9	Moon Surface	44.8880	2.11	46.0896	1.6	45.5301	1.82
10	Mandrill	45.1861	1.97	43.7533	2.74	44.3650	2.38

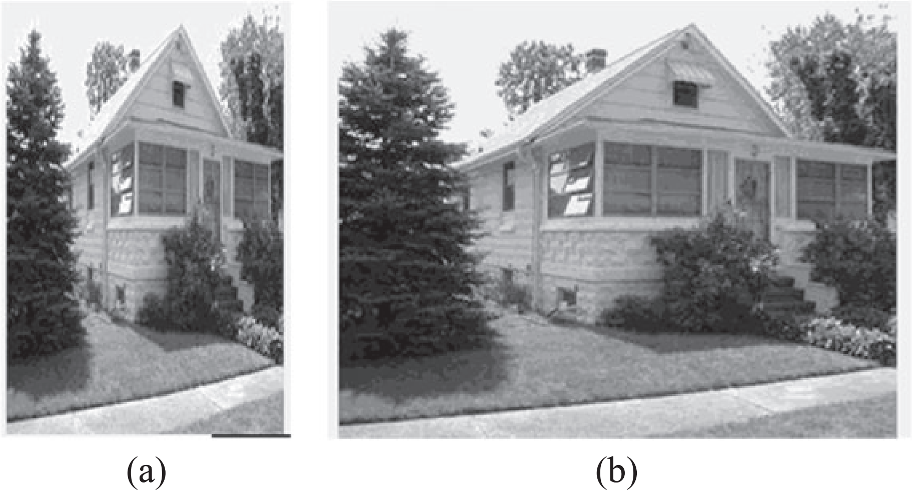


Figure 9. Received message. (a) Retrieved message from stego image. (b) Final message after expansion.

Table II. Size reduction of message and quality of recovered message.

S.	Message	Size		Received message	
no.	image	Before	After	PSNR (dB)	MSE
1	House	240 × 320	240 × 160	39.89	6.67
2	Girl	256 × 256	256 × 128	40.36	5.98
3	Jellybean	256 × 256	256 × 128	30.0484	64.30
4	Flag	500 × 500	500 × 250	38.47	9.24

Huffman coding and others can be deployed. This will reduce the amount hiding data and will make sure of the efficient recovery of original message at the receiver side. However, the lossless compression techniques have a low size reduction capability, which will increase the bandwidth requirement of ESBC as compared to the lossy size reduction mechanism.

6. COMPARISON

The main aim of all steganographic methods is to hide secret information in cover file in innocent manner, keep its presence invisible and undetectable and make retrieval of secret message difficult for any unauthorized user. Steganographers have proposed different steganographic techniques, and each of the steganography technique has their own strengths and limitations.

The well-known 4LSB [10,20] steganography technique has hiding capacity of 50% and results in a stego image quality of greater than 30-dB measure in terms of PSNR. The 4LSB needs a cover image double in size than the secret message so it doubles the size of transmittable data and hence doubles the bandwidth/data rate requirements. But it has low security because if an intruder suspects the presence of hidden information, it is much easier to retrieve secret message and intruder will just need to read the 4LSB of the cover image.

Table III. Comparison of ESBC with 4LSB and SBC.

Sr. no.	Hiding efficiency	Security	PSNR of stego image	Data rate
4LSB [4]	50% or $2^{-1} \times 100\%$	Less	>30 dB	2 × *Data rate of Message*
SBC [19]	$2^{-N} \times 100\%$	High	>30 dB	2^N × *Data rate of Message*
ESBC	$2^{-(N-1)} \times 100\%$	Very high	>30 dB	2^{N-1} × *Data rate of Message*

SBC technique makes use of 4LSB substitution mechanism for data hiding, and it implements 4LSB in "*N*" number of stages, arranged in cascade form. The hiding efficiency of SBC is quite less than 4LSB, and it increases the size of transmittable data significantly. The increase in size is proportional to the number of stages "*N*". That is why it required large bandwidth, i.e. 2^N times of the bandwidth required for 4LSB. However, SBC results in high quality stego images of PSNR value higher than 30 dB, and it provides high security than 4LSB [19].

The ESBC technique has advantages over both of the above mentioned techniques. It provides a hiding efficiency of 50%, equal to hiding efficiency of 4LSB if implemented with two numbers of stages. For large number of stages the hiding efficiency becomes less than 50%. Compared to SBC, ESBC provides double hiding efficiency for any but same number of stages. The ESBC provides high level of security than 4LSB and SBC, due to the block arrangement and preprocessing. The stego image quality is the same as the other two methods, and PSNR of stego image is greater than 30 dB. In terms of bandwidth, the ESBC is highly efficient than SBC, and it requires almost half bandwidth than SBC to transmit the secret message after hiding in cover media. As compared with 4LSB, it requires equal bandwidth to 4LSB, when two stages are used; however, the bandwidth requirement increases with increase in number of stages.

The ESBC is much better than 4LSB and SBC techniques in terms of security and needs less bandwidth than SBC and equal or less bandwidth than 4LSB. It provides high hiding efficiency than SBC, while hiding efficiency of ESBC is equal to or less than 4LSB. Hence, ESBC is better than SBC in terms of hiding efficiency, bandwidth and security, which makes it suitable to be used on low bandwidth channels than SBC. Table III presents a comparison ESBC with 4LSB and SBC.

8. CONCLUSION

The proposed ESBC technique provides equal amount of security as that of simple SBC method. Both, ESBC and SBC hide secret information in the least significant bits of cover images and provide significantly high visual quality stego images. However, the proposed method reduces the size of secret message by half which as a result produces final stego image, half in size than that of SBC with equal number of stages. The secret information hidden in cover using ESBC technique needs 50% less bandwidth/data rate as compared to SBC technique, which makes ESBC technique more suitable for low bandwidth channels than SBC. Moreover, the message is recovered in a good quality using the reverse process of ESBC. In short, the ESBC generates less payload than SBC and requires less bandwidth and transmission time as compared to SBC, making ESBC more favorable than SBC to be used for low data rate channels. This method can be extended to audio, video and text steganography in future.

REFERENCES

1. Provos N, Honeyman P. Hide and seek: an introduction to steganography. *IEEE Security and Privacy* 2003; **1**(3):32–44.
2. Fridrich J, Goljan M, Soukal D 2004, June. Searching for the stego-key. In *Electronic Imaging*. International Society for Optics and Photonics, 2004; 70–82.
3. Fridrich J, Goljan M, Du R. Reliable detection of LSB steganography in color and grayscale images. In *Proceedings of the 2001 Workshop on Multimedia and Security: New Challenges*. ACM, 2001, October; 27–30.
4. Zhang T, Ping X. A new approach to reliable detection of LSB steganography in natural images. *Signal Processing* 2003; **83**(10):2085–2093.
5. Chang CC *et al.* Reversible hiding in DCT based compressed images. *Science Direct, Information Sciences* 2007, July; **177**(13):2768–2786.
6. Khamrui A et al., 2011, December. A Data-Hiding Scheme for Digital Images using Pixel Value Differencing (DHPVD). *International Symposium on Electronic System Design*(*ISED*), 19–21 December, Kochi, India, **2011**.
7. Tsai CT, Liaw C, Liao CY, Ko CH. Concealing information in image mosaics based on tile image features. *Journal of the Chinese Institute of Engineers* 2011; **34**(3):429–440. doi:10.1080/02533839.2011.565618.
8. Wang CM, Wang PC. Data hiding on point-sampled geometry. *Journal of the Chinese Institute of Engineers* 2006; **29**(3):539–542. doi:10.1080/02533839.2006.9671149.
9. Khan S, Yousaf MH. Implementation of VLSB stegnography using modular distance technique. In *Innovations and Advances in Computer, Information, Systems Sciences, and Engineering*. 2013; 511–525. doi:10.1007/978-1-4614-3535-8_43.

10. Khan S, Ahmad N, Wahid M. Varying index varying bits substitution algorithm for the implementation of VLSB steganography. *Journal of the Chinese Institute of Engineers* 2016; **39**(1):101–109.
11. Raja KB, Chowdary CR, Venugopal KR, Patnaik LM 2005, December. A secure image steganography using LSB, DCT and compression techniques on raw images. In *Third International Conference on Intelligent Sensing and Information Processing, 2005*ICISIP. IEEE, 2005; 170–176.
12. Khan S *et al.* Implementation of variable tone variable bits gray-scale image stegnography using discrete cosine transform. *Journal of Signal and Information Processing* 2013; **4**(4):343–350. doi:10.4236/JSIP.2013.44043.
13. Walia E, Jain P, Navdeep N. An analysis of LSB & DCT based steganography. *Global Journal of Computer Science and Technology* 2010; **10**(1).
14. Xuan G, Zhu J, Chen J, Shi YQ, Ni Z, Su W. Distortionless data hiding based on integer wavelet transform. *Electronics Letters* 2002; **38**(25): 1646–1648.
15. Sarmah DK, Bajpai N. Proposed system for data hiding using cryptography and steganography. *International Journal of Computer Applications* 2010; **8**(9):7–10.
16. Usha S, Kumar G, Boopathybagan K 2011, December. A secure triple level encryption method using cryptography and steganography. In *International Conference on Computer Science and Network Technology (ICCSNT)*, Vol. **2**. IEEE, 2011; 1017–1020.
17. Stallings W. *Cryptography and Network Security: Principles and Practice* (5th edn). Prentice Hall Press, 2010.
18. Schneier B. *Applied Cryptography Protocols, Algorithm and Source Code* (2nd edn). Wiley: Indian, 2007.
19. Ismail M *et. al.* Stego block chaining: a secure 4LSB steganography technique. *Sindh University Research Journal (Science Series)* 2016; **48**(1):151–154.
20. Cheddad A *et. al.* Digital image steganography: survey and analysis of current methods. *Signal Processing* 2010; **90**:727–752.
21. Weber G. *USC-SIPI Image Database: Version 4. Dept. Elect. Eng. Syst*. Tech. Rep: Univ. Southern California, Loa Angeles, CA, USA, 1993; 244.