Sindh Univ. Res. Jour. (Sci. Ser.) Vol. 48 (2) 297-300 (2016)

SINDH UNIVERSITY RESEARCH JOURNAL (SCIENCE SERIES)

Increasing Hiding Efficiency of Image Steganography using Pre and Post Image Compression

S. KHAN[++], T. KHAN*, M. ISMAIL, H. ZAFAR, M. A. IRFAN, N. AHMAD

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

Received 12th August 2014 and Revised 8th September 2015

Abstract- Steganography is one of the important fied of information security. A steganography technique hides secret information in the least significant bits of cover image. Security of hidden information and hiding efficiency are two main objectives of a steganographic technique. High data hiding efficiency and good visual quality of stego image are always attempted to be achieves. The work presents a new image steganography technique to increase the hiding capacity and security of hidden information. It makes use of lossless image compression technique to enhance hiding capacity and applied compression before and after data hiding. In pre-compression,lossless compression is applied on secret message to reduce its size and in post-compression the stego image is subjected to lossless compression. The pre-compression increase the hiding efficiency of 4LSB steganography from 50% and a hiding efficiency of 89% has been achieved with LZW compression technique with a compression ratio of 0.56. The PSNR value greater than 30dB threshold is presented by the proposed method. A PSNR of up to 43dB has been achieved.

Keywords: Steganography, Lossless Compression, *Run-Length Encoding, Steganalysis, RLE*

1. INTRODUCTION

Steganography is the art of secret message exchange using a cover medium to keep its presence invisible (Xuan *et. al.* 2002). Thus is an old technique its traces were found back in Greek era (Johnson and Jajodia. 1998). Greek were the first whose use steganography for covert communication. They wrote secret message on the head of a herald, roofed with full-grown hairs (Khan *et. al*. 2016). But, the development of digital system set new direction for secure communication. Steganographer started the use digital media, i.e. Digital image, audio and videos, for hiding information (Kessler. 2004).

Any digital media like image, video, audio or text can be used as cover medium for data hiding. However, the medium with high density of redundant bits are more suitable for hiding information (Neeta *et. al.* 2006). Digital imaging has a high level of redundancy and is considered more suitable and widely used. That why the Digital image steganography, got a lot of fame and attracted the attention of researchers to develop new techniques to communicate secret information (Khan *et. al.* 2016).

Many steganography methods have been developed by researchers both in the spatial domain and transform domain. (Fridrich *et al*. 2001) proposed Steganography methods in the spatial domain by hiding secret information directly in image pixels (Swanson *et. al.* 1998, Fridrich *et. al.* 2001). VLSB Steganography was proposed by Sahib et al. and they also presented the algorithms for implementation of VLSB Steganography i.e. MDT and DDDBA (Khan and Yousaf. 2013).

The transform domain is also an active region for steganography. In discrete cosine transform (DCT), the coefficients are subjected to LSB substitution instead of pixels. Implemented his method for data hiding in transform domain (Irfan *et. al.* 2014). De Vleeschouwer *et al*. 2001 and Goljan *et al*. also developed invertible data hiding techniques. The proposed method was poor due to low hiding capacity, however, the image quality was in acceptable range and the quality of the stego image dropped severely when the capacity was increased (Goljan *et. al.* 2001, De Vleeschouwer *et. al*. 2001). proposed a variable data hiding method in DCT domain (Khan *et. al.* 2015). Xuan *et al.* method, achieved a quite large hiding efficiency by hiding data in cover media using wavelet transform (Xuan *et. al.* 2002); but, the image quality was affected significantly. To transmit images over Internet, the images size should be small enough to be. When the larger images with greater bit depth are transmitted over the Internet the size of the image has to be reduced by adopting a compression technique (Gopalan. 2007). Compression has an important impact on steganography. Lossy compression reduces the size of image, but the hidden information is lost. For e.g. in JPEG the secret information is lost in decreasing the size of U and V to their halves and then in the quantization process also affects the hidden information (Jokay and Moravcik. 2010). So it is neither feasible nor possible to hide information in an image that is subjected to lossy

[++]Corresponding Author email: S. Khan, sahibkhan@uetpeshawar.edu.pk
*Department of Mathematics, Abdul Wali Khan University, Mardan

compression for size reduction. However, to use the lossless JPEG compression may be used for reducing the size of image after data hiding.

This paper presents a pre-compression based 4LSB steganography technique. The proposed method compresses secret message using a lossless compression and hide the compressed message in a cover image using 4LSB steganography. The paper is further divided in four sections of proposed method, hiding efficiency, experimental results and conclusion.

2. IMPLEMENTATION

To increase the hiding efficiency of LSB steganography lossless compression are used. There are two options to increase the hiding efficiency. In fist case only pre-compression is used to compress the message size. The secret message is compressed by using lossless compression technique e.g. Huffman coding, Run length encoding, etc. The lossless compression reduced the size of secret message and doesn't affect the message contents. After compression the message is hidden in cover image using 4LSB steganography. The 4LSB steganography take cover image pixels one by one and replace the least significant bits of cover image elements with compressed message bits. At the end all the modified pixels are combined to get one stego image. The stego image is file having compressed secret message in its least significant bits. The process of hiding pre-compressed message is shown here in **(Fig) 1**.

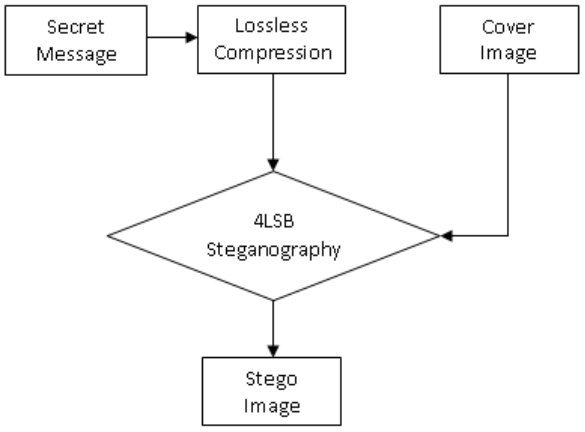


Fig.1. Pre-compressed 4LSB Steganography

At the receiver side, the stego image is received and hidden information are retrieved by accessing the least significant bits of stego image. After reading all the pixels of stego image only compressed encoded compressed message is retrieved. To get final message decompression process is applied on the retrieved secret message. The retrieval and decompression process is given in **(Fig 2).**

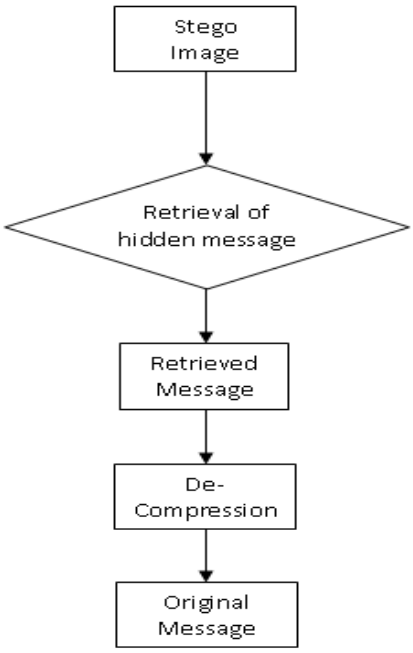


Fig. 2. Retrieval of Original Secret Message

3. HIDING EFFICIENCY

The compression process increases the overall hiding efficiency of steganography. If a message of size "m" is hidden using 4LSB steganography, it will need a cover image of double size i.e. "2xm"The ideal hiding efficiency of 4LSB steganography is equal to 50%.

$$HE_{4LSB} = \frac{m}{2\times m} \times 100 \quad (1)$$

$$HE_{4LSB} = 50\% \quad (2)$$

In the pre-compressed 4LSB steganography the message of size "m" is compressed, if the compression ratio of the lossless compression is "CR" the new size and the new size "m`" is given by Equation (3).

$$m' = m \times CR \quad (3)$$

Then a cover image of size "2xm`" is needed to hide the compressed message. So the hiding efficiency of pre-compressed 4LSB steganography is given here in Equation (6)

$$HE_{pre-comp\ 4LSB} = \frac{m}{2\times m'} \times 100 \quad (4)$$

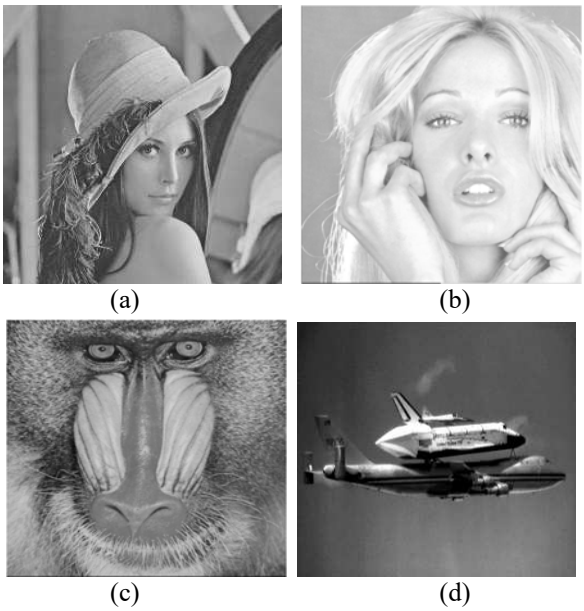
$$HE_{pre-comp\ 4LSB} = \frac{m}{2\times m\times CR} \times 100 \quad (5)$$

$$HE_{pre-comp\ 4LSB} = \frac{50}{CR}\% \quad (6)$$

As CR< 1, so the hiding efficiency will be larger than 50%. Let a compression method with compression ratio of 0.75 is used then, hiding efficiency will be 66.67%.

4. EXPEIMENTAL RESULTS

To implement the pre-compressed, 4 LSB steganography and get the experimental results four different lossless compression techniques are applied on secret message and the compressed messages are hidden using Lena, Tiffany, Mandrill and Shuttle as cover image as shown in **(Fig. 3).**



(a) (b) (c) (d)

Fig. 3. Cover Images (a) Lena (b) Mandrill (c) Tiffany (d) Shuttle

An image of size 240x320 is age is considered as message and it is compressed using run length encoding (RLE), Huffman encoding, Shannon Fano algorithm (SFA) and LZW compression techniques. The hiding efficiency, MSE and PSNR obtained for hiding compressed messages, using the mentioned lossless compression technique, in Lena image are listed in **(Table 1)**.

Table 1. MSE and PSNR for Lena as cover image

Compression Method	Message Size	Compression Ratio	Compressed Size	Hiding Efficiency	MSE (dB)
RLE	614400	0.88	540672	56.82	12.9389
Huffman Encoding	614400	0.67	411648	74.63	12.8208
SFA	614400	0.59	362496	84.74	10.5035
LZW	614400	0.56	344064	89.28	8.9458

The compressed messages by RLE, Huffman encoding, SFA and LZW are the hidden in Tiffany image and statistical values of hiding efficiency, MSE and PSNR are calculated after hiding. The resulted are given here in **(Table 2).**

Table 2. MSE and PSNR for Tiffany as cover image

Compression Method	Message Size	Compression Ratio	Compressed Size	Hiding Efficiency	MSE (dB)
RLE	614400	0.88	540672	56.82	30.2458
Huffman Encoding	614400	0.67	411648	74.63	27.5468
SFA	614400	0.59	362496	84.74	19.3278
LZW	614400	0.56	344064	89.28	11.8745

Similarly the compressed message of each compression techniques is hidden in Mandrill and Shuttle images and the results of hiding efficiency, MSE and PSNR are listed in **(Table 3** and **Table 4)**, respectively.

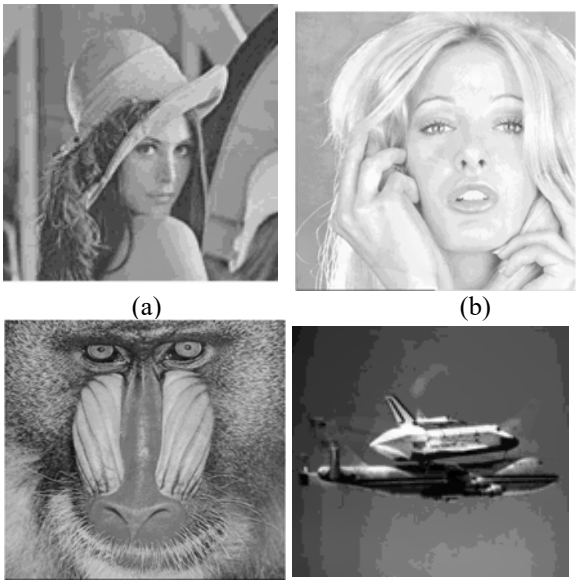
Table 3. MSE and PSNR for Mandrill as cover image

Compression Method	Message Size	Compression Ratio	Compressed Size	Hiding Efficiency	MSE (dB)
RLE	614400	0.88	540672	56.82	31.2421
Huffman Encoding	614400	0.67	411648	74.63	26.2890
SFA	614400	0.59	362496	84.74	10.2985
LZW	614400	0.56	344064	89.28	3.0911

Table 4. MSE and PSNR for Shuttle as cover image

Compression Method	Message Size	Compression Ratio	Compressed Size	Hiding Efficiency	MSE (dB)
RLE	614400	0.88	540672	56.82	25.4500
Huffman Encoding	614400	0.67	411648	74.63	22.5480
SFA	614400	0.59	362496	84.74	18.1588
LZW	614400	0.56	344064	89.28	9.9952

The stego images of hiding each compressed message in each of the cover image are obtained. However, the stego images obtained after hiding LZW compressed message only are shown here in **(Fig. 4).** The quality of the images shows that the hiding process doesn't generate any visually significant distortion and doesn't attract the attention of intruders.



(a) (b)

(c) (d)

Fig. 4. Stego Images (a) Lena (b) Tiffany (c) Mandrill (d) Shuttle

4. CONCLUSION

The pre-compressed 4LSB steganography is good technique to be used for low bandwidth channels. The statistical results shows that the proposed methods has significantly high data hiding efficiency and also result in a god quality stego image of PSNR value of 43dB which is much higher than the threshold of 30dB. The pre-compressed 4LSB steganography can be used efficiently with any lossless compression technique like run length encoding, Huffman encoding, Shannon Fano algorithm and LZW method. This technique make sure the recovery of message in full health and increases the overall security of hidden information because to retrieve information the same decompression method need to be used at the receiver as compression method at the sender side. If the compression and decompression technique used is not known to a person, original message can't be retrieved. Hence, in conclusion, the pre-compressed 4LSB steganography technique meets the needs of modern communication to a large extent.

REFERENCES:

Anderson, R. J., and F. A. Petitcolas. (1998) On the limits of steganography. IEEE Journal on Selected Areas in Communications. 16(4): 474-481.

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

Gopalan, K. (2007). An image steganography implementation for JPEG-compressed images. In International Symposium on Communications and Information Technologies, 2007. ISCIT'07:739-744, Sydney, New South Wales, Australia. DOI: 10.1109/ISCIT.2007.4392114

Goljan, M., J. J., Fridrich, and R. Du. (2001). Distortion-free data embedding for images. In Information Hiding: 27-41, Springer Berlin Heidelberg.

Irfan, M., N. Ahmad, and S. Khan. (2014). Analysis of Varying Least Significant Bits DCT and Spatial Domain Stegnography. Sindh University Research Journal (Science Series). 46(3):301-306.

Jókay, M., and T. Moravćík. (**2010**). Image-based JPEG steganography. Tatra Mountains Mathematical Publications. 45(1):65-74.

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.

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.

Khan, S., T. Khan, M. Naeem and N. Ahmad. (2015). Run-Length Encoding based Lossless Compressed Image Steganography. Sindh University Research Journal-SURJ (Science Series), 47(3): 541-544.

Kessler, G. C. (2004). An overview of steganography for the computer forensics examiner. Forensic Science Communications. 6(3):1-27.

Neeta, D., K. Snehal, and D. Jacobs. (2006). Implementation of LSB steganography and its evaluation for various bits. In 1st International Conference on Digital Information Management: 173-178. IEEE.

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.

Vleeschouwer, C. D., J. F. Delaigle, and B. Macq. (2001). Circular interpretation of histogram for reversible watermarking. In IEEE Fourth Workshop on Multimedia Signal Processing:345-350, Cannes, France. DOI: 10.1109/MMSP.2001.962758.

Xuan, G., J. Zhu, J. Chen,Y. Q. Shi, Z. Ni, and W. Su. (2002). Distortionless data hiding based on integer wavelet transform. Electronics Letters. 38(25): 1646-1648.