Sindh Univ. Res. Jour. (Sci. Ser.) Vol.47 (3) 541-544 (2015)

SINDH UNIVERSITY RESEARCH JOURNAL (SCIENCE SERIES)

Run-Length Encoding Based Lossless Compressed Image Steganography

S. KHAN, T. KHAN*, M. NAEEM**, N. AHMAD++

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

Received 18th November 2014 and Revised 12th September 2015

Abstract- Secure communication with the least possible utilization of communication link is the need of modern communication systems. The treats and limited bandwidth of the Internet requires high security and size reduction of data. The technique proposed in this paper basically hides secret data in images and also reduce the size of images to meet the need of bandwidth limited communication systems. Least significant bits substitution method has been adopted for data hiding in the image and then RLE scheme has been used to reduce the size of stego image. A hiding capacity of 50% has been achieved with a reasonable high PSNR (i.e. greater than 30dB limit) and a compression ratio of greater than 1 has been achieved. The proposed method insures the 100% recovery of the secret message at the receiver side.

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

1. INTRODUCTION

Steganography is the art of covert communication (Xuan *et. al.* 2002). Data hiding is an old technique of hiding data in other data hiding the existence of secret information (Johnson and Jajodia. 1998). It was adopted by ancient people for communicating secret messages. They adopted various ways for the secret information exchange by writing secret message on the head of a messenger covered with grown hairs, later started to write a message using invisible ink. With the development of the digital systems the digital era gave a new direction to cover communication and secret information were hidden in digital cover files, i.e. digital images, audio and videos (Kessler. 2004).

Although any digital file can be used as cover for data hiding, but the file format having high redundancy is more suitable. The redundant bits are used to alter with secret messages and the changes remain invisible. Digital imaging has a high level of redundancy and is considered more suitable and widely used. Digital image steganography, due to its high level of redundancy, got a lot of fame and the researcher started to develop new techniques to communicate secret information using digital image as cover media (Honsinger, *et. al.* 2001).

Several data hiding methods have been reported both in the spatial domain and transform domain. Honsinger *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). In the transform domain DCT coefficients are subjected to data hiding instead of pixels. Macq et al. implemented his method for data hiding in transform domain (Irfan *et. al.* 2014). De Vleeschouwer et al. and Goljan et al. also developed invertible data hiding techniques, but the data hiding efficiency was very low for the acceptable image quality and the quality of the stego image dropped severely when the capacity was increased (Goljan *et. al.* 2001, De Vleeschouwer *et. al*. 2001). Sahib et al. proposed a variable data hiding method in DCT domain (Goljan *et. al.* 2001). Xuan et al.'s method, achieved a quite large hiding efficiency by hiding data in cover media using wavelet transform (Xuan *et. al.* 2002); however, 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 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 an RLE based compression image steganography technique. The RLE BASED hiding technique compresses the stego image without the loss of secret information. The proposed method

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

*Department of Mathematics, Abdul Wali Khan University, Mardan

**Department of Computer Science, University of Peshawar

insures the retrieval of secret information in it full health.

2. IMPLEMENTATION

To achieve compression without affecting the hidden data the secret information is first embedded in the cover image. The secret message is hidden in the least significant bits of the cover image pixels. The resulted stego image after the data hiding process is called stego image and is compressed by using a lossless compression technique. The stego image is encoded by using RLE scheme. The RLE scheme takes the advantage of redundancy in the Stego image and represents the most repeated value/strength with less number of bits. **(Fig.1)**

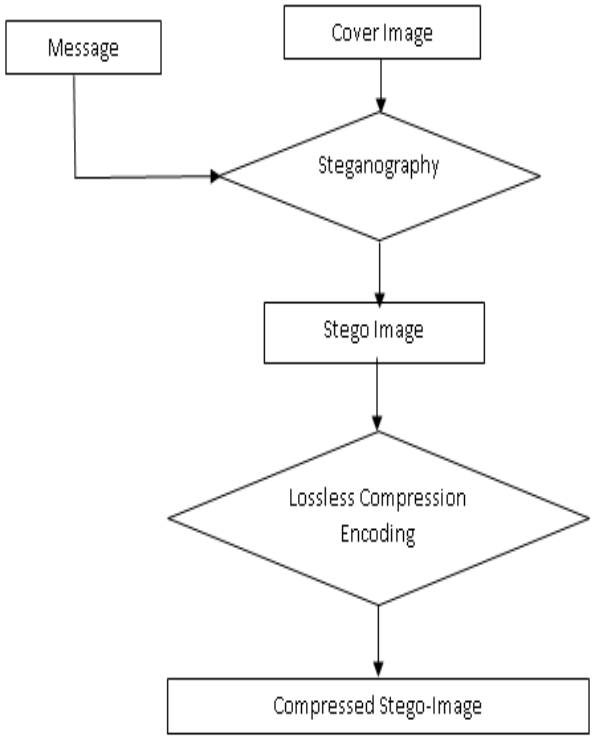


Fig.1. Implementation of Lossless compressed Image Steganography

The most occurring value is replaced with less number of bits actually reduce the size of data to be transmitted over a communication system. The compression process makes sure the best use of the communication link and save the bandwidth of the channel used for communication and the secret information is also convey to the receiver without any loss. The whole process of data hiding and compression is explained here in the block diagram shown in **(Fig. 1)**.

In run-length coding the stego image is transformed into identical symbols' segments. Each segment is represented in the form of a pair of symbol and its number of occurrences i.e. its probability of occurrence. For example, a portion of stego image pixels "8, 8, 10, 250, 250, 8, 255, 8, 10, 10" is coded as (8, 4), (10, 3), (250, 2), (255, 1) (Gopalan. 2007). The RLE scheme work very well on large files. Different stego images with the same message hidden in it are used for experimental results.

When the compressed file with secret information is received at the receiver side a reversible process is applied to recover the hidden message. The compressed stego image is decoded to get an uncompressed stego image and the least significant bits of stego image are searched for hidden information and the secret message is retrieved by reading the least significant bits of each pixel of the uncompressed stego image. The retrieval process is explained here with the help of a block diagram shown in **(Fig. 2)**.

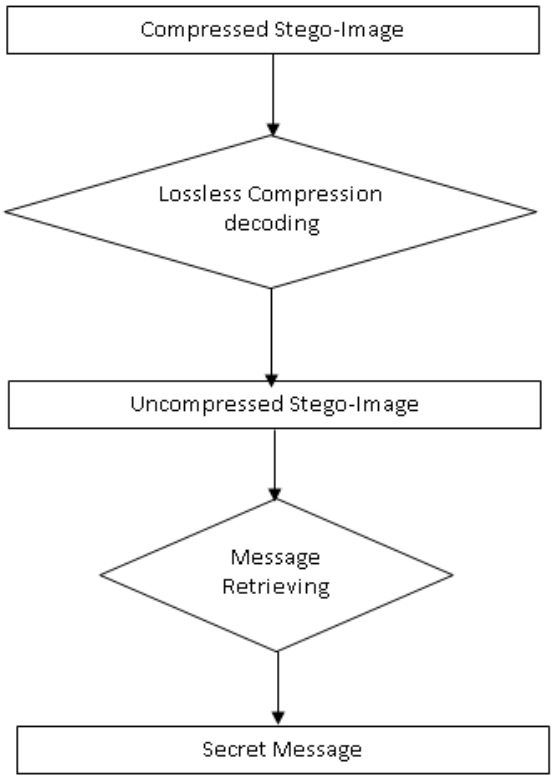
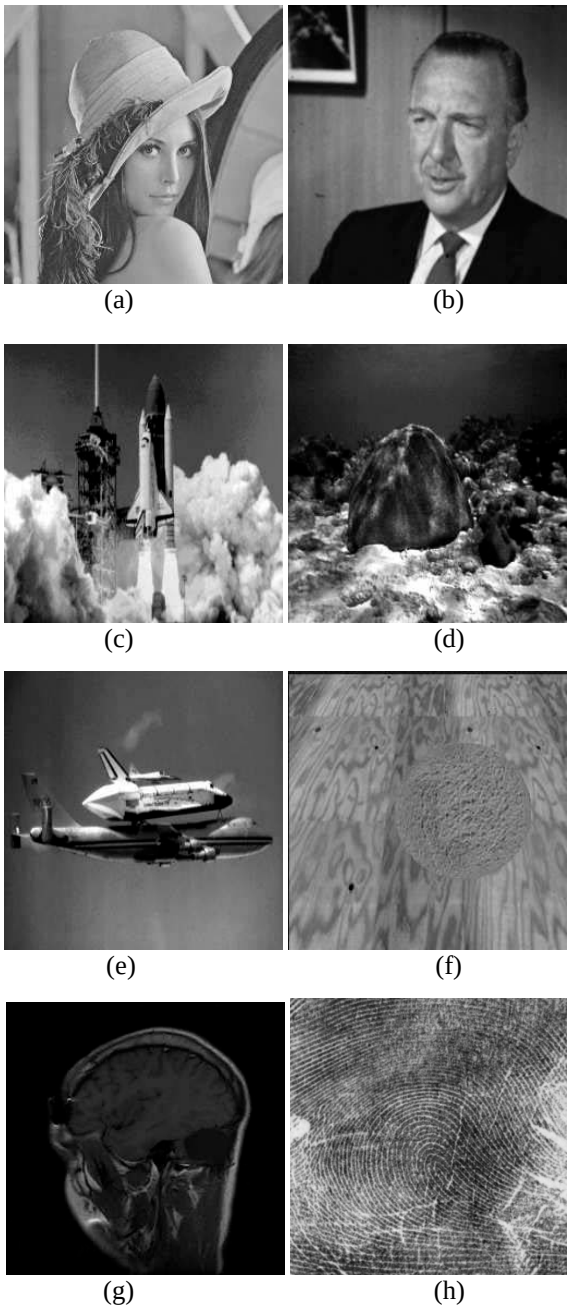


Fig. 2. Retrieval of secret information

3. EXPEIMENTAL RESULTS

The method explained in the implementation section is implemented by using Lena, Man, Space craft, Coral, Shuttle, Sphere, MRI and Fingerprint images as cover for hiding the same secret message. The cover images used are shown in **(Fig. 3)**. Each of the cover images is processed one by one for data hiding. The resulted stego images are shown here in **(Fig. 4)**.



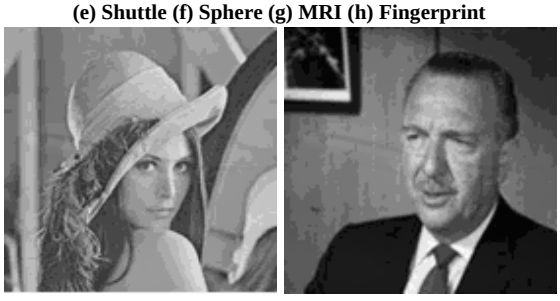
(a) (b)

(c) (d)

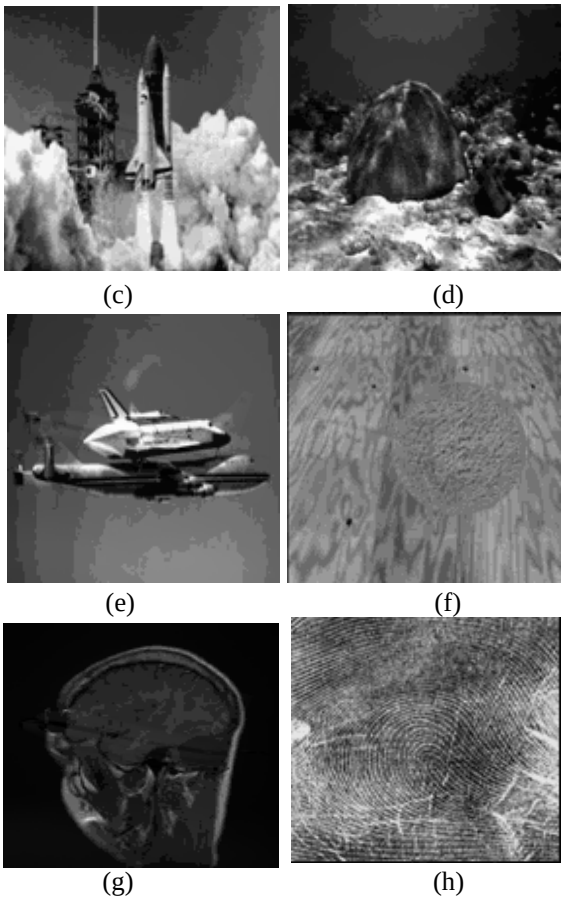
(e) (f)

(g) (h)

Fig. 3. Cover Images (a) Lena (b) Man (c) Space Craft (d) Coral (e) Shuttle (f) Sphere (g) MRI (h) Fingerprint



(a) (b)



(c) (d)

(e) (f)

(g) (h)

Fig. 4. Stego Images (a) Lena (b)Man (c) Space Craft (d) Coral Shuttle (f) Sphere (g) MRI (h) Fingerprint

The effect of Steganography on the quality of the image is measured quantitatively by calculating MSE and PSNR for each stego image by keeping hiding capacity fixed at 50% level. The resulted MSE and PSNR are listed here in **(Table 1).**

After data hiding each of the stego image is processed by using RLE. The effect of RLE is measured in the term of compression ratio. The compression ratios before and after data hiding is also calculated for each image and are listed in **(Table 2).**

Table 1. MSE and PSNR of lossless compressed image Steganography

Image	MSE	MSE (dB)	PNSR (dB)
Lena	19.6739	12.9389	35.1919
Man	19.1416	12.8208	35.3100
Space Craft	19.1950	12.8319	35.2983
Coral	17.0644	12.3209	35.8099
Shuttle	15.1566	11.8060	36.3248
Sphere	19.0287	12.7941	35.3367
MRI	7.8447	8.9458	39.1850
Fingerprint	18.9161	12.7683	35.3625

Table 2. Compression ratios with and without hidden information

Image	CR of Cover Image	CR of Stego Image
Lena	1.03	1.06
Man	1.07	1.10
Space Craft	1.15	1.21
Coral	1.13	1.15
Shuttle	1.17	1.16
Sphere	1.23	1.18
MRI	1.25	1.17
Fingerprint	1.26	1.28

4. CONCLUSION

The results show that the proposed methods hide a data of almost half of the cover image in size and assure the efficient recovery of a message in its full health. The quality of stego image is not affected significantly and the PSNR of the resultant stego images remains above the 30dB threshold for data hiding capacity of 50%. A reasonable compression ratio of greater than 1bpp has been achieved. The result also shows that the data hiding data affect the redundancy level of an image and that's why the compression ratio of compression the cover is different from that of the stego image. As the communication over an internet requires both security and reduce size, both of these issues are addressed by the proposed method. Hence, in conclusion, the lossless compressed image steganography technique meets the needs of modern communication to a large extent by reducing the size of an image and communicating information securely.

REFERENCES:

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

Fridrich, J., M. Goljan, and 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, 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.

Honsinger, C. W., P. W. Jones, M. Rabbani, and J. C. Stoffel, (2001). U.S. Patent. Washington, DC: U.S. Patent and Trademark Office. No. 6, 278,791

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.

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

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

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., M. N. Khan, S Iqbal, S. Y. Shah, and N. Ahmad, (2013). Implementation of Variable Tone Variable Bits Gray-Scale Image Stegnography Using Discrete Cosine Transform. Journal of Signal and Information Processing, 4(04), 343-350.

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

Macq, B., and F. Dewey, (1999). Trusted headers for medical images. In DFG VIII-D II Watermarking Workshop (Vol. 10). Germany: Erlangen.

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

Xuan, G., 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.

.