ISSN 2348-1218 (print)
International Journal of Interdisciplinary Research and Innovations ISSN 2348-1226 (online)
Vol. 7, Issue 2, pp: (262-267), Month: April - June 2019, Available at: www.researchpublish.com

# Analysis of Reversible Data Hiding and Data Scrambling-Embedding Technique

[1]Jaladi Vivek, [2]Dr Baswaraj Gadgay

[1]Assistant Professor & Research Scholar, Department of ECE. LAEC, Bidar, Karnataka
[2]Professor, Department of ECE.VTU, Kalaburagi, Karnataka

***Abstract:*** **The reversible data hiding (RDH) technique gains remarkable attention from research communities and academicians. A reversible data hiding as well as data scrambling methodology is proposed in this work. The RDH is also known as lossless or invertible data hiding. In this paper a novel hybrid method of data hiding, data scrambling and compression of image is proposed. Initially a color image is taken as input for data embedding and later converted into grayscale image. Discrete cosine transformation (DCT) for grayscale image compression and chaos encryption algorithm for scrambling the image are considered. Further, data has been embedded with the help of Least Significant Bit (LSB) insertion technique. This technique is one of the easiest ways to embed secret data in an image replacing the LSB of each sampling bit with binary information. The main advantage of this technique is that it allows for large secret information to be embedded. The whole methodology is implemented and tested in MATLAB. Different quality metrics such as PSNR, SSIM and MSE are computed for various test images. The obtained results are reasonable and acceptable.**

***Keywords*****: Steganography, reversible, data scrambling, data embedding.**

## I. INTRODUCTION

Day by day the usages of image and video applications are increasing tremendously. The safety and faster data transfer needed protection and compression of multimedia files. The problem of image protection can be resolved by only through encryption or data hiding or both. As we know that availability of bandwidth is limited, for proper utilization of bandwidth we apply data compression. Data hiding in the image or video file is becoming a significant technique for authentication of image. When transferring the image to the owner, encryption is needed for the secure transfer. Video files security has attracted more concentration among the users. Image or video files encryption techniques attempt to change an image or video files to decoded one that is difficult to understand.

The science and art of hiding information into image or other domains in such a manner that no-one could understand other than the sender and receiver is called steganography [1,2]. Ghoshal et al. [3,4] has stated that the steganography encompasses the concealment of embedded digital information inside the files of computer. Wang [1] inferred that the steganographic message resembles something like video, picture or image, sound file or radio communication. Such kind of messages is referred as cover-text. Wang [1] and Ghosal and Mandal [2] describes that the message will be hidden by using ink that is not visible between the innocuous documents' visible lines. The hidden content is referred as stego message. Security is considered as the big deal for the image transferring across the network. Security can be achieved only through data hiding within the picture, video and so on.

According to Benedett et al. [5], Liu et al. [6], Uhl and Pommer [7] and Norcen et al. [8] the binary information protection becomes compulsory in various fields. They refer that there are two security levels such as the full encryption assures the total obscurity of information and the partial encryption ensures a lower security level. Benedett et al. [5] and Uhl and Pommer [7] point out that several encryption procedures are used mainly for the encryption of the image.

Liang [9] and Lee [10] refer that digital watermarking is the best method for the authentication of image. The traditional methods related to authentication of digital signature have some issues. As soon as the signature is included in the digital image or other domains, it maximizes the size of the file and it can also be safely eliminated. It cannot be implemented for locating the tampered image area with high precision whereas digital watermarking (DW) resolves the above issues. Liang et al. [11] and Lee [10] point out that in DW, size of the file will not be changed after inserted in the watermark.

The paper is organized as follows: in section-1 brief introduction to different data embedding and scrambling techniques are discussed; in section-2 works related to the problem are discussed. The proposed methodology of data hiding and data scrambling embedding is discussed in section-3 and results are discussed in section-4. Finally, the paper is concluded in section-5.

## II. RELATED WORKS

Under this section various works related to the data hiding and scrambling are discussed.

Puech et al. [12] examined the novel reversible method for safe and fast image transfer. This study uses techniques that process partial encryption, information hiding and compression of images in a single step. Based on the size of the message to be embedded into image, partially image is encrypted without altering the content of the original image. Moreover, the rate of compression relies on the upper bound size of message to be embedded in the image. The purpose of the study is to divide the content of original image into two sub-images and applying different methods to each and every sub-image for gaining space, raising the information embedding capacity, minimizing the computational effort and time required for computation. After that these sub images are scrambled and partially encrypted. The most efficient feature of this study is to utilize the single procedure for performing the compression, the partial encryption and reversible data hiding (DH) rather than using three different techniques. Thus it was concluded that single processing steps were used to perform all the activities.

Devi and Venkatesan [13] proposed a study to determine the reversible authentication of image with tamper localization on the basis of watermarking in IWT (integer wavelet transforms). If the originality of image is checked, distortion based on watermark that is embedded can be fully eliminated from the watermarked image. Moreover, suppose the image is damaged and then positions of tampering will be localized. Double watermarking layers are adopted. The first layer of watermarking is embedded in SD (spatial domain) checks authenticity whereas second watermarking layer embedded in TD (transform domain) gives reversibility. The watermark is created and scrambled based on image size to be watermarked. To the WS (watermarking system) this gives more protection. IWT is implemented and the proposed WS localizes the tampering at level of pixel. It was also noted that if the image is found to be authentic, then the original image can be replaced. Thus it was concluded that the watermarking system gives more protection.

Shah and Saxena [14] studied and analysed the schemes related to image encryption. This study compares the frequency domain (FD) and spatial domain (SD) image encryption schemes. It was identified that schemes of SD are faster whereas security is very low. It was also seen that in SD scheme is good as compared to FD in terms of speed, security and compression. In the FD scheme it maintains good performance from viewpoint of security. Moreover, the scheme related to encryption is better as far as compression efficiency, speed and security is concerned.. Thus it was noted that encryption of the image is far better when compared with the speed, efficiency and security is taken into consideration.

## III. PROPOSED METHODOLOGY

The proposed study is designing an encryption scheme for maintaining good trade-off among reversible, tunable, speed, value of the image and so on. In the encoding process chaos encryption scheme is employed for scrambling the image and compression is carried out by discrete cosine transform (DCT) method. In the decoding process reverse process is employed for recovering back the original image and extracting the embedded information. .

Suppose an image J has G*H pixels and let J(g, h) denote the value of pixel at position (g,h) for $1 \leq g \leq G$ and $1 \leq h \leq H$. The neighboring pixels in the original image are highly correlated that is

$J(g, h) \sim J(g+\Delta g, h+\Delta h)$ ---------- (1)

For small $\Delta g$ and $\Delta h$ there is slight difference that occurs with the adjacent pixels. Such correlation is exploited as the basis for the information extraction and descrambling purposes.

ISSN 2348-1218 (print)
International Journal of Interdisciplinary Research and Innovations ISSN 2348-1226 (online)
Vol. 7, Issue 2, pp: (262-267), Month: April - June 2019, Available at: www.researchpublish.com

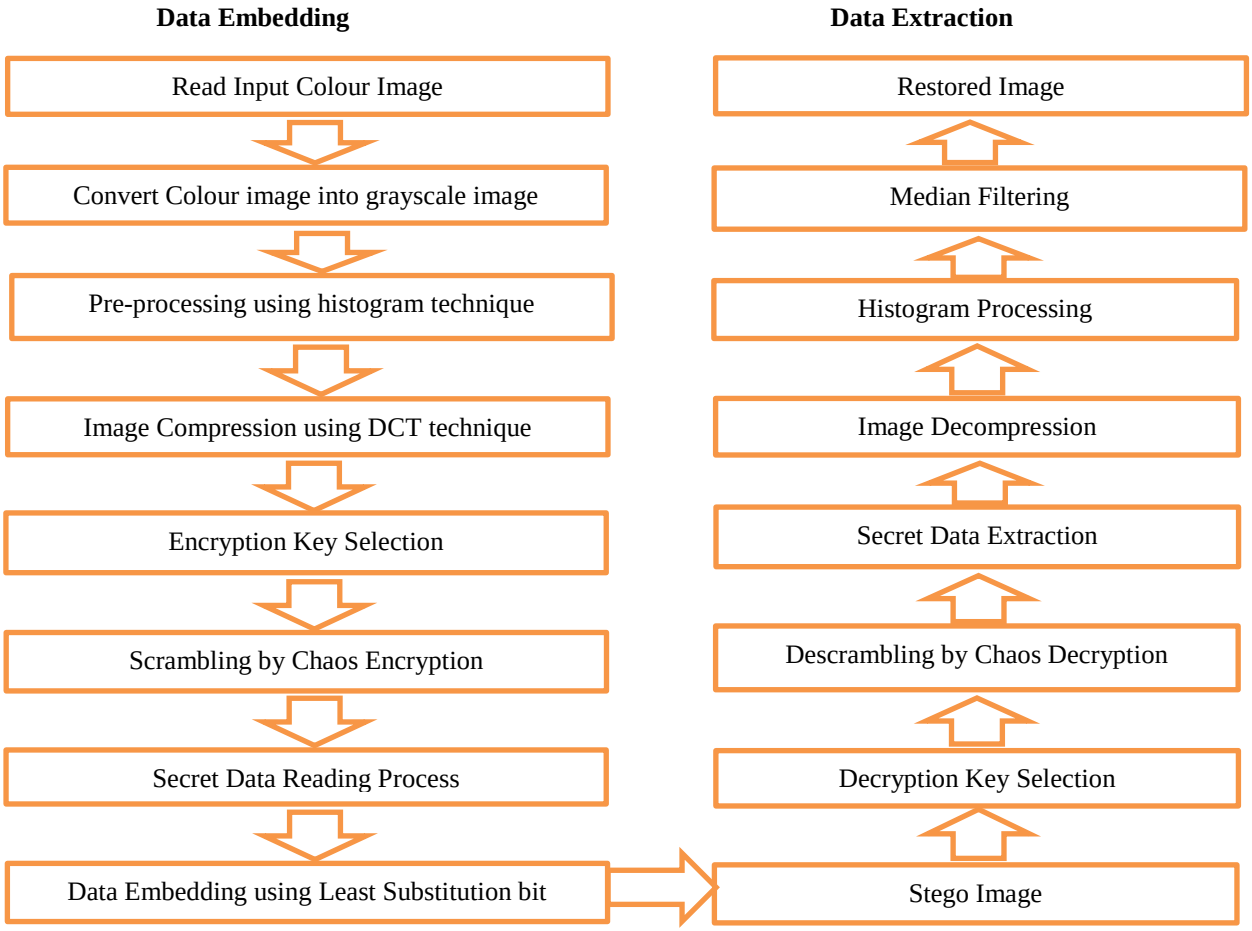


**Fig.1: Proposed Framework for Data Embedding and Data Extraction**

## IV. RESULTS AND DISCUSSION

Various standard test images are considered for our simulation and how these images are processed is discussed in this section. In the data embedding process six images are considered as input as shown in Fig.2. Further, step by step embedding process is clearly shown. Next input image is pre-processed and corresponding histogram of pre-processed image is shown in Fig.3. The Fig.4 shows the compressed image obtained with the help of Discrete Cosine Transform (DCT) .The Fig.5 shows the encryption key selection method used to perform on compressed image.


**Fig 2: Input Images**


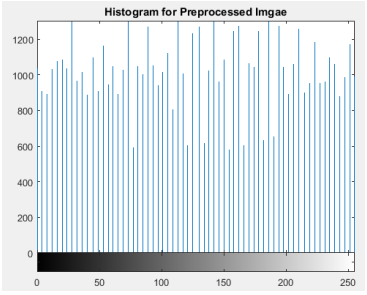


**Fig.3: Histogram of Pre-Processed image**


**Fig.4: Compressed image (DCT)**

ISSN 2348-1218 (print)
International Journal of Interdisciplinary Research and Innovations ISSN 2348-1226 (online)
Vol. 7, Issue 2, pp: (262-267), Month: April - June 2019, Available at: www.researchpublish.com

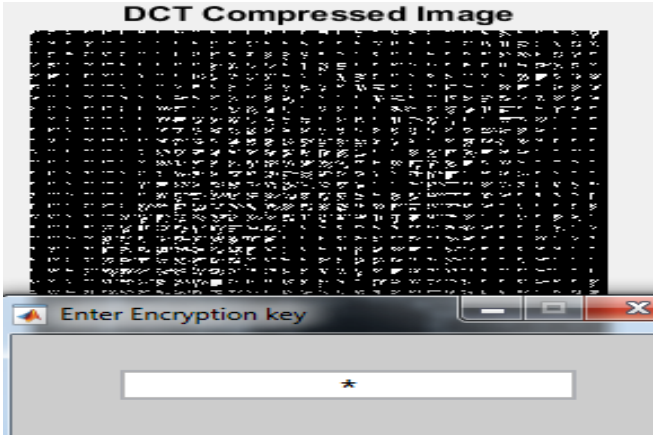


**Fig.5: Encryption key selection**

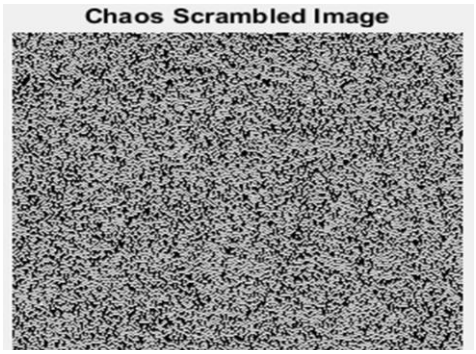


**Fig.6: Scrambling of Image by Chaos Encryption**

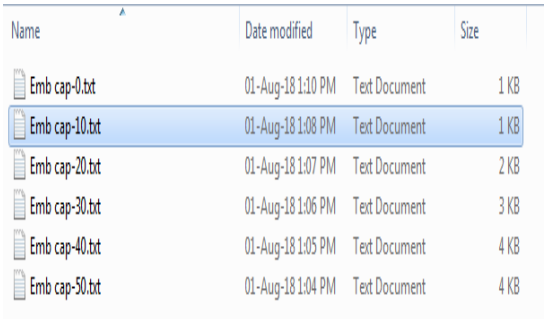


**Fig.7: Secret Data reading process**

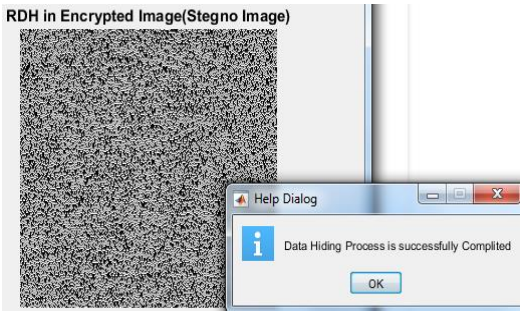


**Fig.8: Stegno image (Compressed-Scrambled-RDH image)**

Next scrambling of image is carried out with chaos encryption scheme. The logistic map equation is considered for scrambling the compressed image with Z output and input with the two initial conditions with V and U as follows in the Eq. (2),

$$Z_{n+1} = UV_n(1 - V_n) \text{ – – – – – – – – – – – – – – } \quad (2)$$

u < [1, 4] and v < [0, 1] in which the chaotic behaviour is achieved when u = 3.9999 and v = 0.4000. Here our model used logistic map equation to shuffle the pixel mapping tables (PMT) and to shift the pixel values. The Fig.6 shows the scrambling of image by using the chaos encryption algorithm. Fig.7 and Fig.8 shows respectively Secret Data reading process, Stegno image (Compressed-Scrambled-RDH image).


**Fig.9: Decryption of Image**

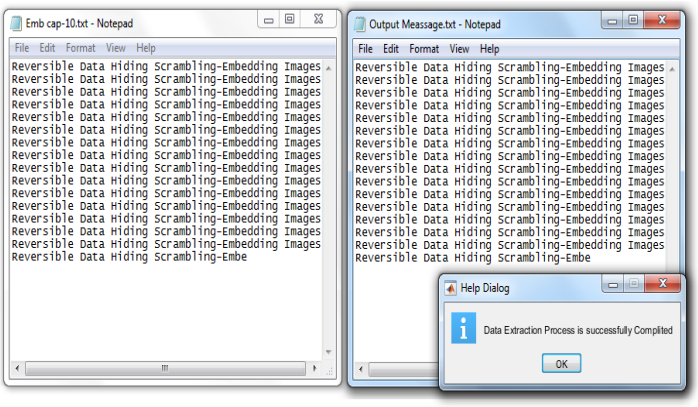


**Fig.10: Data Extraction Process**

ISSN 2348-1218 (print)
International Journal of Interdisciplinary Research and Innovations ISSN 2348-1226 (online)
Vol. 7, Issue 2, pp: (262-267), Month: April - June 2019, Available at: www.researchpublish.com



**Fig.11: Image decrypted using chaos algorithm** **Fig.12: Restored Image**

In the Data Extraction Process stegno image (Compressed-Scrambled-RDH image) is considered as input which is shown in Fig.9. After Decrypting the compressed–Scrambled–RDH image using decryption key data extraction is carried out this is shown in Fig.10. Fig.11 shows image decrypted using chaos algorithm. After Image decompression process the image has been restored as shown in Fig.12.

**Table 1: PSNR values of various images.**

| PSNR --> Result Analysis for Input and Stego Image | | | | | | |
|---|---|---|---|---|---|---|
| Image/Emb. Cap | 0 | 10 | 20 | 30 | 40 | 50 |
| Image1 | 27.4385 | 27.4385 | 27.4385 | 27.4383 | 27.4381 | 27.438 |
| Image2 | 27.5793 | 27.5791 | 27.5789 | 27.5788 | 27.5786 | 27.5787 |
| Image3 | 27.3814 | 27.3813 | 27.3812 | 27.3813 | 27.381 | 27.3807 |
| Image4 | 26.2208 | 26.2206 | 26.2204 | 26.2203 | 26.2205 | 26.2201 |
| Image5 | 27.5826 | 27.5824 | 27.5821 | 27.582 | 27.5822 | 27.5825 |
| Image6 | 26.9889 | 26.9886 | 26.9886 | 26.9886 | 26.9885 | 26.988 |

PSNR computation: Peak signal to noise ratio (PSNR) is used to measure the quality of reconstructed images that have been compressed. The PSNR is the ratio between a signal's maximum power and the power of the signal's noise. Signals have a wide dynamic range, and PSNR is calculated in decibels, which is a logarithmic scale. The PSNR of various images are shown in Table-1 and Fig.13.

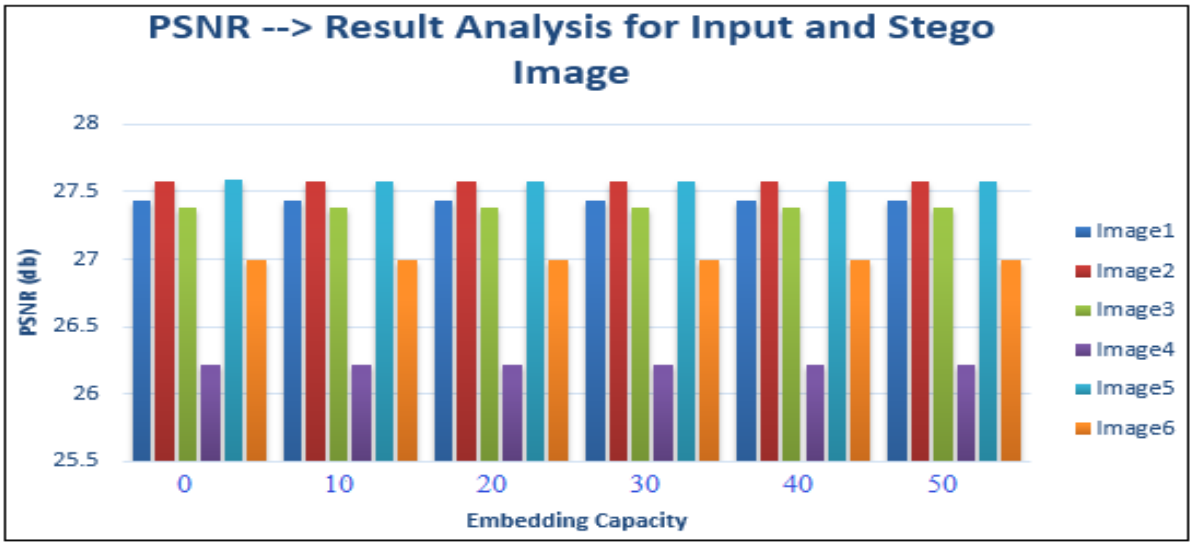


**Figure 13: PSNR values of various images vs embedding capacity**

## V. CONCLUSION AND FUTURE WORKS

Unified reversible data hiding technique as well as data scrambling technique is discussed in this paper. The performance of our algorithm is best suited for various images. The original image is first converted into the gray scale image, further compressed using discrete cosine transformation and chaos encryption algorithm is considered for scrambling the image.

Further, data has been embedded with the help of Least Significant Bit (LSB) insertion method. This we did for protection of image and data. Processing of data hiding, compression, scrambling of images in a single step results in stego-image. The reverse process we adhered for getting back the original image. PSNR, SSIM, MSE values for the various images are computed and obtained results are very reasonable and acceptable. Further, as the popularity of data hiding and scrambling is not confined to image files, in future this may be tested with various formats of videos files as well.

## REFERENCES

[1] R. Wang, C. Lib and J. Lin, Image hiding by optimal LSB substitution and Genetic algorithm, Pattern Recognition Society, Published by Elsevier Science Ltd, 2001.

[2] N. Ghoshal and J.K Mandal, A Bit Level Image Authentication /Secrete Message Transmission Technique (BLIA/SMTT) ,Association for the Advancement of Modelling & Simulation Technique in Enterprises (AMSE), AMSE journal of Signal Processing and Pattern Recognition, Vol. 51, No. 4, 2008, pp 1-13.

[3] N. Ghoshal, J.K. Mandal, et al., 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.

[4] N. Ghoshal, J.K. Mandal, et al., Image Authentication by Hiding Large Volume of Data and Secure Message Transmission Technique using Mask (IAHLVDSMTTM), Proceedings of IEEE international Advanced Computing Conference IACC, 2009.

[5] D. Benedetto, E. Caglioti, and V. Loreto, Language trees and zipping, Phys. Review Lett., 88(4),2002.

[6] H.T. Liu, B. Li, Z.L. Shang, X.Z. Li, R.L. Mu, D.Y. Sun and R.G. Zhou, Calmodulin is involved in heat shock signal transduction in wheat,Plant Physiol, Vol 132, 2003, pp 1186–1195.

[7] A. Uhl and A. Pommer, Image and Video Encryption:From Digital Rights Management to Secured Personal Communication, Springer, 2005.

[8] R. Norcen, M. Podesser, A. Pommer, H.P. Schmidt, and A. Uhl, Confidential Storage and Transmission of Med-ical Image Data. Computers in Biology and Medicine, Vol 33, 2003, pp 277–292.

[9] X. Liang, Reversible authentication watermark for image, Proceedings of the World Congress on Engineering and Computer Science 2008, San Francisco, USA, October 2008, pp 22 – 24.

[10] S. Lee, Reversible image watermarking based on integer-to-integer wavelet transform, Information Forensics and Security, Vol 2, No 3, 2007, pp 321-330.

[11] X. Liang, X. Wu and J. Huang Reversible data hiding for image based on histogram modification of wavelet coefficients, International Conference on Computational Intelligence and Security, Lecture notes on Artificial Intelligence, vol. 3802, 2005

[12] W. Puech, J.M. Rodrigues and J.E. Develay-Morice, A New Fast Reversible Method for Image Safe Transfer, Journal of Real-Time Image Processing Manuscript, 2007.

[13] P. Devi and M. Venkatesan, Reversible Image Authentication With Tamper Localization Based on Integer Wavelet Transform, International Journal of Computer Science and Information Security, Vol 6, No 2, 2009.

[14] J. Shah and V. Saxena, Performance Study on Image Encryption Schemes, International Journal of Computer Science Issues, Vol 8, 2011, pp 349-356.

[15] Q. Zhang, Y. Sun, Y. Yan, H. Liu and Q. Shang, Research on Algorithm of Image Reversible Watermarking Based on Compressed Sensing, Journal of Information and Computational Science, Vol 10, No 3, 2013, pp 701-709.

[16] S. Schmiedeke, P. Kelm and T. Sikora, Reversible Scrambling with Colour-Preservative Characteristic, 2013, Retrieved On:18th June 2014, Retrieved From: http://elvera.nue.tu-berlin.de/files/1432Schmiedeke2013.pdf.

[17] S. Ong, K. Wong and K. Tanaka, Reversible and Tunable Scrambling-Embedding Method,2013, Retrieved On:18th June 2014.

[18] S. Ong, K. Wong and K. Tanaka, A Scalable Reversible Data Embedding Method With Progressive Quality Degradation Functionality, Image Communication,2014.