http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 8 (8): 1287-1291, 2009
ISSN 1812-5638

Blockwise Reversible Data Hiding by Contrast Mapping

[1]Wien Hong, [2]Jeanne Chen and [2]Tung-Shou Chen
[1]Department of Information Management, Yu Da University, Miaoli, Taiwan
[2]Graduate School of Computer Science and Information, National Taichung Institute of Technology, Taichung, Taiwan

Abstract: The insatiate demands for applications of imagery on the internet have further emphasized the importance of data hiding research. In this study, we proposed an improved reversible contrast mapping data hiding scheme that emphasized on the variance feature of the cover image. The cover image is partitioned into blocks where the variance of each block is calculated and sorted. Data was then embedded by reversible contrast mapping in these sorted blocks for which low variance blocks are embedded prior to those high variance blocks. In the proposed scheme, high payload is maintained and embedment can be selective to achieve high stego-image quality. In comparison to another similar work, the proposed scheme preserved significantly high quality in the stego-image especially for small payload.

Key words: Block variance, reversible, image contrast, data hiding, payload

INTRODUCTION

Rapid increase in image applications on the internet has attracted research in developing techniques on data hiding. Many data hiding techniques, reversible or non-reversible, have been proposed and many used digital images as carriers to embed secret message (Mielikainen, 2006; Zhang and Wang, 2006; Hong *et al*., 2009). During embedding, pixel values of the original image (or cover image) were modified and the resulting distorted image called a stego image. For non-reversible data hiding technique, the distorted stego image cannot be restored. On the other hand, a reversible data hiding technique has the capability to recover the stego image to its original state after extracting the embedded message. Reversible data hiding is widely emphasized for use in medical or military images because in many applications, images of these types often allowed no distortion (Lin *et al*., 2008).

Many of the reversible data hiding techniques proposed recently were based on the schemes of expansion embedding (Tian, 2003; Alattar, 2004; Kamstra and Heijmans, 2005), histogram-shifting embedding (Ni *et al*., 2006; Xuan *et al*., 2007) or a combination of these two (Thodi and Rodriguez, 2007; Hong *et al*., 2009). The expansion embedding scheme was first proposed by Tian (2003) and is considered as a high payload scheme with an upper bound at 0.5 bpp in that one data bit could concealed into two consecutive pixels. However, the scheme required a location map to record the locations of embeddable and non-embeddable pixels. The location map was compressed and embedded in the cover image and therefore, required considerably high overhead and computational costs. Others (Alattar, 2004; Kamstra and Heizmans, 2005; Thodi and Rodriguez, 2007) proposed improved versions of Tian's scheme but still require additional data compression. The histogram-shifting embedding scheme was proposed by Ni *et al*. (2006). Their method achieved a high stego image quality and required only a low overhead; however, the payload is limited by the peak of the image histogram. As a result, their scheme only allows low payload hiding. Some variant of Ni *et al*. (2006) scheme can be found (Hwang *et al*., 2006; Hong *et al*., 2008).

Coltuc and Chassery (2007) extended Tian's work and introduced a Reversible Contrast Mapping (RCM) scheme that achieved an upper bound payload at 0.5 bpp. The scheme did not require any additional data compression but analyze the parity of pixel pairs to avoid the overflow and underflow problems. The computational cost of the scheme was small but the embedding process did not take into consideration differences in image features; namely, the smooth and complex regions. Therefore, distortions were equally presented in both low and high payload hiding which should otherwise be less for low payload.

In this study, we proposed a Blockwise Contrast Mapping (BCM) scheme for reversible data hiding. The

Corresponding Author: Dr. Wien Hong, Department of Information Management, Yu Da University, Miaoli, 361, Taiwan
Tel: 886-37-651188/6129 Fax: 886-37-652143

cover image will be partitioned into *N* blocks and sorted in ascending order by their variance values. Secret bits would then be embedded by block order using the RCM scheme.

Coltuc *et al*. (2007) RCM SCHEME

Reversible Contrast Mapping (RCM), proposed by Coltuc *et al*. (2007), applies simple integer transform to pairs of pixels to conceal messages. The embedding procedure of their method is listed below:

Input: The cover image I, to-be-embedded message S and a threshold δ.

Output: A stego image I′ and the final embedding position L.

Step 1: Partition the cover image I into 2×1 non- overlapping pixel pairs, $\{P_i\}_{i=1}^{Np}$, where, $P_i = (p_{i,1}, p_{i,2})$ and Np denotes the number of pixel pairs

Step 2: Set i = 1

Step 3: Transform the pixel pairs P_i to $\hat{P}_i$ according to the following rule:

$$\hat{p}_{i,1} = 2p_{i,1} - p_{i,2},\ \hat{p}_{i,2} = 2p_{i,2} - p_{i,1}. \quad (1)$$

Step 4: If $\hat{p}_{i,1} < 0, \hat{p}_{i,2} < 0, \hat{p}_{i,1} > 255, \hat{p}_{i,2} > 255$ or $|p_{i,1}-p_{i,2}| \geq \delta$, pixel pair P_i is non-embeddable. Record the LSB of $p_{i,1}$ and then set it to 0

Step 5: If $0 \leq \bar{p}_{i,1}, \bar{p}_{i,2} \leq 255$, one message bit can be embedded according to the following rule:

- If the LSBs of $p_{i,1}$ and $p_{i,2}$ are both odd, then set the LSB of $p_{i,1}$ to 0 and replace the LSB of $p_{i,2}$ with one message bit
- If LSBs of $p_{i,1}$ and $p_{i,2}$ are not both odd, transform $(p_{i,1}, p_{i,2})$ to $(\bar{p}_{i,1}, \bar{p}_{i,2})$, then set the LSB of $\bar{p}_{i,1}$ to 1 and replace the LSB of $\bar{p}_{i,2}$ with one message bit

Step 6: Set i = i + 1 and repeat step 2 to step 5 until all bits of message S are embedded. The final embedding position L is recorded and served as a key for decoding

Once the recipient received the stego image and the key, the embedded message S can be extracted and the original image can be recovered by using the following procedure:

Input: A stego image I′, the final embedding position L and the threshold δ.

Output: The recovered original image I and extracted message S.

Step 1: Partition the stego image into 2×1 non-overlapping pixel pairs $\{P_i'\}_{i=1}^{Np}$, where, $P_i' = (p_{i,1}', p_{i,2}')$ and Np is the number of blocks, as in the embedding phase

Step 2: Set k = 1

Step 3: According the LSB of $p_{i,1}'$, perform the following extraction and recovery rule:

- If the LSB of $p_{i,1}'$ is 1, then one message bit can be extracted form the LSB of $p_{i,2}'$. To recover the original pixel value, set the LSBs of $p_{i,1}'$ and $p_{i,2}'$ to 0 first and then performs the following transformation rule to recover the original pixel values $p_{i,1}$ and $p_{i,2}$:

$$p_{i,1} = \left\lceil \frac{1}{3}(2\hat{p}_{i,1} + \hat{p}_{i,2}) \right\rceil, p_{i,2} = \left\lceil \frac{1}{3}(\hat{p}_{i,1} + 2\hat{p}_{i,2}) \right\rceil$$

- If the LSB of $p_{i,1}'$ is 0, temporally replace the LSB of $(p_{i,1}', p_{i,2}')$ with 1 and use Eq. 1 to check whether the overflow or underflow problem occurs and do the following step:

(a) If there is no overflow and underflow problem, then a message bit can be extracted form the LSB of $p_{i,2}'$. To recover the original pixel values, simply set the LSBs of $p_{i,1}'$ and $p_{i,2}'$ to 1

(b) If the overflow and underflow problem occurs, then there is no message bit embedded. The original pixel value $p_{i,1}$ can be recovered by replacing the LSB of $p_{i,1}'$ with previously recorded LSB of $p_{i,1}'$

Step 4: Set i = i+1 and repeat step 3 to step 4 until the end of embedding position L is met. Now the original image I is recovered and embedded message S is extracted

The RCM scheme requires no additional data compression and provides a comparable bit-rate to that of Tian's scheme and its extensions (Alattar, 2004; Thodi and Rodriguez, 2007). However, the RCM scheme does not take into consideration local variance of cover images. A high variance area in a cover image often embeds fewer messages but causes larger distortion. A better data hiding scheme should have a more sophisticate control to embed more while keeping the distortion low.

BLOCK VARIANCE CONTRAST MAPPING (BCM)

Here, we proposed a modified version based on RCM scheme. In the RCM scheme, every pixel pair embeds one message bit regardless the difference between these two pixels. However, pixel pairs with larger difference may cause larger distortion. Therefore, the proposed scheme modified the original RCM scheme by partitioning image into blocks and sorting them according to their variance in ascending order. Message is then embedded sequentially into the sorted blocks for which low variance blocks are embedded prior higher ones.

To calculate the block variance, an M×M grayscale image is partition into N blocks $\{B_i\}_{i=1}^{N}$. Each block is composed of n pixels $B_i = \{p_i^{(k)}\}_{k=1}^{n}$. The variance of each block is calculated by,

$$\text{var}(B_i) = \frac{1}{n}\sum_{k=1}^{n}(p_i^{(k)} - \bar{p}_i)^2 \quad (2)$$

where, $\bar{p}_i$ is the mean of pixel values of block B_i and n is the number of pixels in each block.

The blocks are sorted in ascending order by variance values. Secret bits are then embedded based on the RCM scheme starting from the smallest variance block. Data hidden in the lower variance blocks will cause less distortion as opposed to those in higher variance blocks. The flow for the embedding-extraction process is as shown in Fig.1. The location of blocks with embedded secret will be recorded and served as a key K. To extract the embedded secrets, the locations of hiding can be retracted from K. Note that K is accessible only to authorized users. The pixels of pairs will be decoded using the inverse RCM to extract the secret and to restore the cover image. Detailed embedding, extraction and restoration algorithm is as shown in Fig. 1.

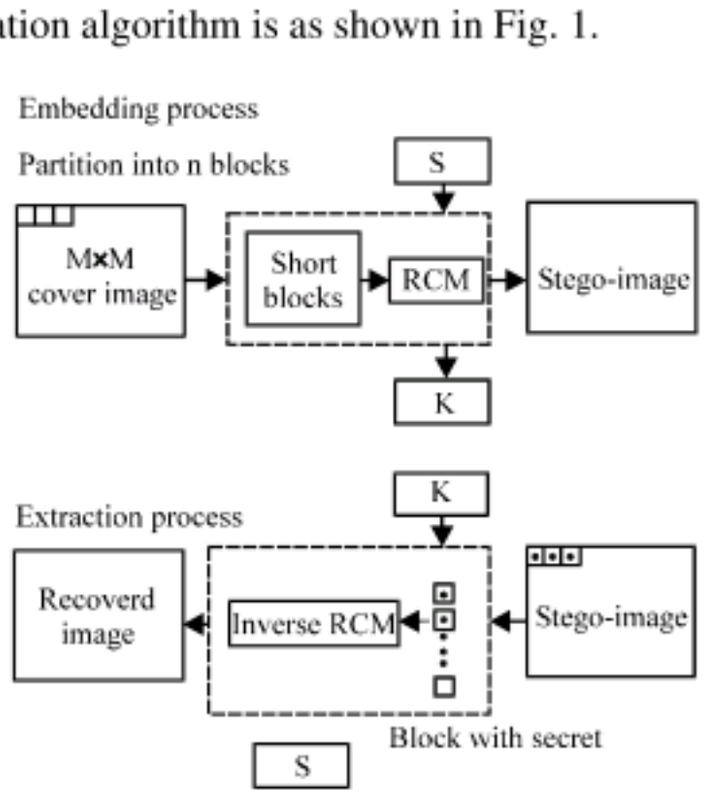

Fig. 1: Flow for the embedding and extraction processes

Embedding algorithm:

Input: M×M grayscale cover image, encrypted message bits S.

Output: Stego image, key K.

Step 1: Partition the cover image into N non-overlapping blocks $\{B_i\}_{i=1}^{N}$

Step 2: Sort $\{B_i\}_{i=1}^{N}$ according to their variance in ascending order, the results are $\{B_i'\}_{i=1}^{N}$

Step 3: Set k = 1

Step 4: Record the position of B_k' in K and embed message bits into B_k' by using the RCM technique. If the embeddable spaces in B_k' are depleted but some more message bits left to be hide, then set k = k+1

Step 5: Repeat step 4 until all secret bits are embedded and record the end of embedding position L in K

In the proposed scheme, The key size $|K|$ may be calculated using,

$$|K| = P\lceil \log_2 N \rceil + \left\lceil \log_2\left(\frac{M\times M}{N}\right)\right\rceil \quad (3)$$

where, P is the number of blocks that are embedded and $\lceil \bullet \rceil$ is the ceiling function. Note that $P\lceil \log_2 N \rceil$ is the size required to record the positions of blocks used for embedding and $\lceil \log_2 (M\times M/N \rceil$ denotes the size required to record the end of embedding position.

Extraction algorithm:

Input: Stego image, key K.

Output: Recovered cover image, encrypted message bits S.

Step 1: The key K contains the position of the blocks with embedded secret data. Using the inverse RCM, extract the embedded secret and restore the cover image by RCM

Step 2: Stop extracting once the end of embedding position L is located; otherwise repeat step 1

RESULTS AND DISCUSSION

Experimental tests were conducted with four 512×512 cover images as seen in Fig. 2a-d. The images were chosen with smoothness, complexity and well-distributed features; for example, Lena showed remarkable complexity in the hair areas and smoothness in the upper arm area; F-16 showed smoothness and both Barbara and Baboon are complex images. Each image was partitioned into 256 blocks. Different amount of payload, varying from

Fig. 2: Original 512×512 cover images. (a) Lena, (b) F-16, (c) Barbara and (d) Baboon

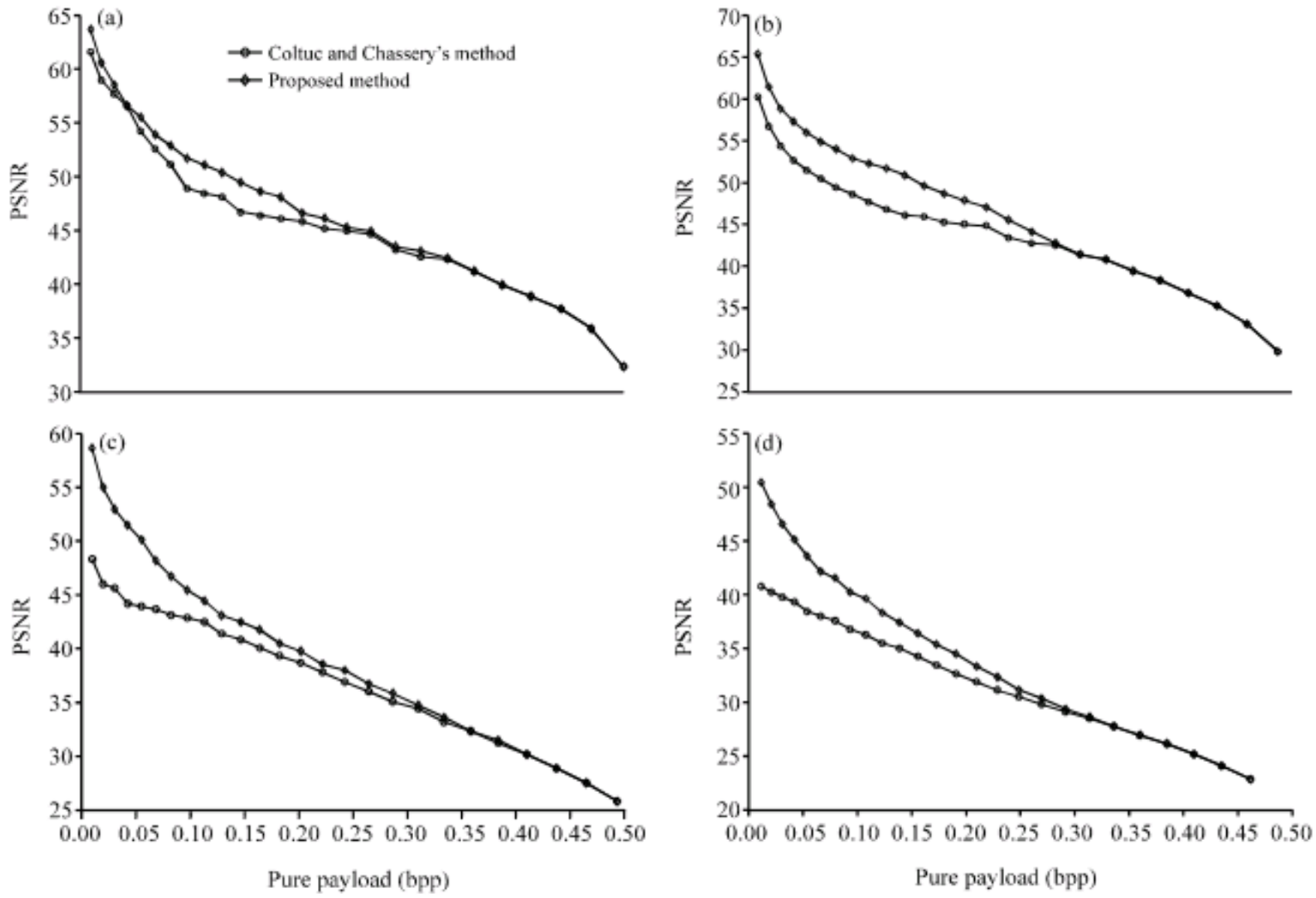

Fig. 3: Comparing the BCM and RCM methods. (a) Lena, (b) F-16, (c) Barbara and (d) Baboon

0.01 bpp to 0.5 bpp, was embedded to measure the performance of the proposed scheme.

Figure 3a-d show the comparison results of stego-image quality vs. payload for the proposed BCM and RCM methods. Measurement for the stego-images quality was based on peak signal to noise rate (psnr) values in dB.

As can be seen from Fig. 3, at 0.3 bpp and under, the psnr values were significantly higher for all four images using BCM. For example, for the test image Baboon at 0.1 bpp, the psnr for BCM is 40 dB, whereas for RCM method, only 36.5 dB can be obtained. That is, the gain in psnr is 3.5 dB at 0.1 bpp. The reason is that in BCM if payload does not require hiding in all blocks, then only

blocks with low variance were chosen for embedding data. Therefore, our method has a significant improvement over RCM when the cover image is partially embedded.

Comparison results also show that both methods have similar psnr values for hiding rates above 0.3 bpp. If the cover image is fully embedded, the psnr performance of BCM is equivalent to that of RCM method. This is due to the reason that all blocks were used for embedding; therefore both schemes had the same fair chance of embedding in the high variance blocks. This proved that hiding in the low variance regions can reduce distortion to the images.

Moreover, our method also provides a specially designed key to protect the embedded message. Without the correct key, the embedded message can not be exactly decoded. The key K used to record the locations of blocks with embedded secret data is small. Using Lena as an example, the key size is calculated as follows:

$$27\lceil \log_2 256 \rceil + \left\lceil \log_2 \left(\frac{512\times512}{256} \right) \right\rceil \simeq 29 \text{ bytes}$$

The total key size is only 29 bytes which is significantly small and can be easily delivered to the recipient via a secret channel.

The goal of data hiding is to transmit secret data via an innocent cover image to avoid the attention of someone who is interested in it (Hong *et al*., 2009). However, the distortion of an embedded stego image is inevitable. Generally, the more the distortion occurs in a stego image, the more detectable a data hiding algorithm will be (Zhang and Wang, 2006). Therefore, the distortion of the cover image should be as small as possible. In the proposed method, we significantly lower the distortion caused by data embedding at low embedding rate. Thus, the proposed method provides a more secure data hiding method than that of Coltuc and Chassery (2007) method.

CONCLUSION

The proposed BCM scheme took advantage of the characteristic of low variance in images by selecting to embed data in these regions. Experimental results showed that at the lower bound 0.3 bbp, BCM performed significantly better with high psnrs. The reason was that the blocks in BCM were sorted in ascending by variance values and at lower bound bpps not all blocks were used for embedding. As a result, all secret data were concentrated in the low variance region. BCM may be used to embed secret in selective regions as an added security for reversible data hiding.

REFERENCES

Alattar, A.M., 2004. Reversible watermark using the difference expansion of a generalized integer transform. IEEE Trans. Image Process., 13: 1147-1156.

Coltuc, D. and J.M. Chassery, 2007. Very fast watermarking by reversible contrast mapping. IEEE Signal Process. Lett., 14: 255-258.

Hong, W., T.S. Chen and C.W. Shiu, 2008. A high quality histogram shifting based embedding technique for reversible data hiding. Proceedings of the International Symposium on Intelligent Information Technology Application Workshops, Shanghai, Dec. 21-22, IEEE Computer Society, Washington, DC. USA., pp: 292-295.

Hong, W., T.S. Chen and C.W. Shiu, 2009. Reversible data hiding for high quality images using modification of prediction errors. The J. Syst. Software (In Press).

Hwang, J.H., J.W. Kim and J.U. Choi, 2006. A Reversible Watermarking Based on Histogram Shifting. In: Digital Watermarking, Shi, Y.Q. and B. Jeon (Eds.). LNCS., 4283, Springer-Verlag, Berlin, Heidelberg, ISBN: 978-3-540-48825-5, pp: 348-361.

Kamstra, L. and H.J.A.M. Heijmans, 2005. Reversible data embedding into images using wavelet techniques and sorting. I EEE Trans. Image Process., 14: 2082-2090.

Lin, C.C., W.L. Tai and C.C. Chang, 2008. Multilevel reversible data hiding based on histogram modification of difference images. Pattern Recogn., 41: 3582-3591.

Mielikainen, J., 2006. LSB matching revisited. IEEE Signal Process. Lett., 13: 285-287.

Ni, Z., Y.Q. Shi, N. Ansari and W. Su, 2006. Reversible data hiding. IEEE Trans. Circ. Syst. Video Technol., 16: 354-362.

Thodi, D.M. and J.J. Rodriguez, 2007. Expansion embedding techniques for reversible watermarking. IEEE Trans. Image Process., 16: 721-730.

Tian, J., 2003. Reversible data embedding using a difference expansion. IEEE Trans. Circ. Syst. Video Technol., 13: 890-896.

Xuan, G., Y.Q. Shi, P. Chai, X. Cui, Z. Ni and X. Tong, 2007. Optimum histogram pair based image lossless data embedding. Proceedings of the 6th International Workshop on Digital Watermarking, Guangzhou, China, LNCS., 5041, Dec. 3-5, Springer-Verlag Berlin, Heidelberg, pp: 264-278.

Zhang, X. and S. Wang, 2006. Efficient steganographic embedding by exploiting modification direction. IEEE Commun. Lett., 10: 781-783.