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 11 (8): 1109-1114, 2012
ISSN 1812-5638 / DOI: 10.3923/itj.2012.1109.1114

An Improved Reversible Data Hiding Method Using Alternative Location Map Embedment Strategy

[1]Yan-Wei Li and [2]Wien Hong
[1]Department of Information Engineering,
Chenggong College of Henan University of Economics and Law, Zhengzhou, China
[2]Department of Information Management, Yu Da University, Miaoli, Taiwan

Abstract: This study proposed an improved data embedding scheme based on the Local Variance Controlled Reversible data hiding method (LVCR) proposed by Hong and Chen in 2010. In LVCR, the location map has to be recorded in the LSBs of a set of cover pixels and the original LSBs of these cover pixels have to be embedded into the other set of cover pixels. As a result, the pure payload of the cover image may significantly be decreased when the location map is large. The proposed method adopts an alternative method to embed location map together with the secret data directly into the pre-processed cover pixels. Therefore, the number of cover pixels for carrying data bits is increased. The location map can be directly extracted from the stego image. Experimental results reveal that the proposed method offers better or equivalent stego image quality than that of LVCR under the same payload.

Key words: Location map, reversible data hiding, pure payload

INTRODUCTION

Data hiding is a technique that embeds secret data into a cover image for secret transmission of messages (Provos and Honeyman, 2003). It is an art to embed secret data into multimedia data (Al-Frajat *et al*., 2010). The secret data can be embedded in videos (Hmood *et al*., 2010), in audio (Ahmed, *et al*., 2010) and also can be in images. Because images are widely used over the internet (Salem *et al*., 2011) and also provide rich embedding spaces for data concealment, they have become one of the most used carriers for data hiding. An image used for carrying data is called a cover image and an image that carried data is called a stego image. Since most of the data hiding technique embeds data by altering pixel values, the distortion occurs after data concealment. It is often desirable to reduce the distortion to evade the detection of human eyes or statistical tools.

Many of the data hiding method distorts the cover image to obtain the stego images and the stego image can not be recovered to the original one (cover image) (Hong and Chen, 2010; Mohammad *et al*., 2011). However, some types of the digital images may not allow any distortion such as military or medical images. As a result, the reversible data hiding technique has draw attention to many researches to investigate the embedment of this type (Luo *et al*., 2011; Li *et al*., 2011; Zhao and Luo, 2012; Yang and Yin, 2012). The earliest reversible data hiding method is the pattern and several other reversible data hiding methods have been proposed over the past decade. Tian (2003) proposed a reversible data hiding method based on difference. His method expands the difference of pixel pairs and embeds a bit into the expanded difference. Although this method theoretically provides a high payload of 0.5 bpp, the distortion can be apparent because the pixel difference has to be doubled. Alattar (2004) generalized Tian's method by extending the maximum payload to (n-1)/n bits. However, Alattar's method also introduces a significant distortion and is not suitable for applications requiring high quality images.

Ni *et al*. (2006) proposed a histogram-shifting method to recover the original image from the stego image via the shifting of histogram. Ni *et al*. (2006)'s method shifts bins of histogram to vacate an empty bin for data embedding. Because every pixel is modified only a grayscale unit at most, this method achieves a very acceptable image quality. However, the distortions are almost the same for an image regardless of the payload, that is to say, there are will be cause unnecessary distortions for small payload. Hong *et al*. (2010) introduce a mechanism to control the capacity-distortion, which shift histogram only when embedding the secret data. No extra amount of pixels will be shifted when all the secret data have been

Corresponding Author: Yan-Wei Li, Department of Information Engineering, Chenggong College of Henan University of Economics and Law, Zhengzhou of Henan, China Tel: 86-371-64561717 Fax: 86-371-64561286

embedded. Thus, the image quality will be better. But the maximum payload of the method based on histogram-shifting is limited by the most frequent occurring pixel values. Tsai *et al.* (2009) proposed a reversible data hiding method based on prediction and shifting. Their method partitions the cover image into N blocks of m×m pixels and the center pixel is selected as the basic pixel. Each block is sequentially visited and uses the value of the basic pixel to predict the other pixels in the same block to obtain N×(m×m-1) prediction errors. Data are then embedded by shifting the prediction error histogram. Tsai *et al.* (2009)'s method achieves a higher payload over Ni *et al.*'s method while providing almost the same stego image quality. However, Tsai *et al.* (2009)'s method does not consider the local complexity of images and thus the image quality could be reduced, especially at low payload. Inspired by there another method (Hong *et al.*, 2009), Hong and Chen (2010) proposed a local variance-controlled reversible data hiding method (LCVR) based on shifting of prediction histogram. LCVR excludes those regions with larger variance from data embedment and provides a bi-linear prediction technique to better predict the pixel values. As a result, the image quality is higher than that of Tsai *et al.*'s method under the same payload.

Although, LCVR provides a better embedding performance, it requires a set of pixel in the cover image for storing the location map to deal with the underflow/overflow problem. As a result, the payload could be reduced as the size of location map is increased. To embed the location map, LCVR partitions the cover image I into two sub-images I_L and I_M. Then, the location map is compressed using the JBIG2 (Howard *et al.*, 1998) coder and embeds the compress location map L of size |L| into the LSB of I_L. The original LSB of I_L is embedded together with the secret data into I_M. Note that in order to embeds L, LCVR has to use |L| pixels in I_L to record L and the LSBs of I_L are still needed to be embedded with the secret data. When |L| is small, the embedding of location map adds a little impact on the pure payload. However, pure payload may significantly reduce as |L| is increased. This study proposed an improved method for location map embedment by pre-shifting those saturated pixels before embedding and embeds the compressed location map and the secret data directly into the pre-shifted cover image. The proposed method does not need require extra set of cover pixels to record the compressed location map and thus the pure payload can be increased.

Hong and Chen (2010) proposed a LCVR method by employing a new prediction method and considering the local pixel activity of the cover image to achieve a better embedding performance. The embedding, extraction and restoration procedures of LCVR method are briery summarized in the following sub-suctions.

EMBEDDING PROCEDURE

In the embedding phase, the cover image is scanned and records the positions of pixels valued 0 and 255 using a binary location map. The location map is then compressed using JBIG2 (Howard *et al.*, 1998) coder to obtain a compressed location map L of size |L|. According to |L|, cover image I is partitioned into I_L and I_M for carrying location map and secret data, respectively. To embed messages into I_M, I_M is partitioned into N blocks $\{B_i\}_{i=1}^{N}$ of size m×m. For each block B_i, the center pixel c_i is selected as the basic pixel and the other $\{b_{i,j}\}_{j=0}^{7}$ pixels are non-basic pixels. The basic pixels c_i^L, c_i^T, c_i^R, c_i^B of the four neighboring blocks of B_i is called satellite basic pixels, as shown in Fig. 1.

The local variance at c_i is calculated by:

$$V(c_i) = \frac{1}{5}((c_i - \bar{c})^2 + (c_i^L - \bar{c})^2 + (c_i^R - \bar{c})^2 + (c_i^T - \bar{c})^2 + (c_i^B - \bar{c})^2) \quad (1)$$

where, $\bar{c}$ is the average of c_i^L, c_i^T, c_i^R, c_i^B and c_i. If V (c_i) is smaller than a threshold value TH, the block B_i is considered as a smooth block. For every smooth block B_i, the prediction errors $e_{i,j}$ is calculate by:

$$\{e_{i,j}\}_{j=0}^{7} = \{b_{i,j}\}_{j=0}^{7} - \{p_{i,j}\}_{j=0}^{7} \quad (2)$$

where, $\{p_{i,j}\}_{j=0}^{7}$ is the prediction value of non-basic pixel $\{b_{i,j}\}_{j=0}^{7}$, which is calculated by:

$$p_{i,0} = \text{round}(\frac{1}{3}(c_i + c_i^L + c_i^T)) \quad (3)$$

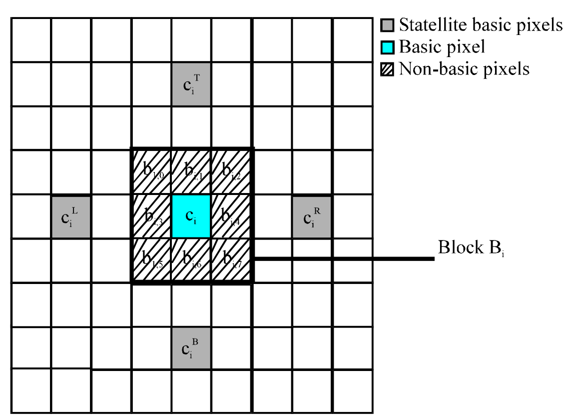

Fig. 1: Schematic diagram of basic pixel, non-basic pixels and satellite basic pixels

$$p_{i,1} = \text{round}(\frac{1}{3}(2c_i + c_i^T)) \quad (4)$$

$$p_{i,2} = \text{round}(\frac{1}{3}(c_i + c_i^T + c_i^R)) \quad (5)$$

$$p_{i,3} = \text{round}(\frac{1}{3}(2c_i + c_i^L)) \quad (6)$$

$$p_{i,4} = \text{round}(\frac{1}{3}(2c_i + c_i^R)) \quad (7)$$

$$p_{i,5} = \text{round}(\frac{1}{3}(c_i + c_i^L + c_i^B)) \quad (8)$$

$$p_{i,6} = \text{round}(\frac{1}{3}(2c_i + c_i^B)) \quad (9)$$

$$p_{i,7} = \text{round}(\frac{1}{3}(c_i + c_i^B + c_i^R)) \quad (10)$$

Once the prediction error histogram is obtained, two pair of peak and zero points are calculated. The LSBs of I_L and secret data *S* are embedded into I_M by modifying the prediction errors $\{e_{i,j}\}_{j=0}^{7}$ to $\{e'_{i,j}\}_{j=0}^{7}$ and obtain the stego block B'_i. Combining the stego blocks, the modified sub-image I'_M is obtained. In order to extract the embedded data, two pairs of peak and zero points, TH, |L|, |S| and L are concatenated to form a bit stream BS and BS is then embedded into the LSBs of I_L. We denote the embedded version of I_L by I'_L. Combining I'_M and I'_L, we obtain the stego image I'.

EXTRACTION AND IMAGE RECOVER PROCEDURES

According to the length of BS, the stego image I' is partitioned into I'_L and I'_M. Extract the LSBs of I'_L, we have two pair of peak and zero points, TH, |L|, |S| and L. This information is essential for data extraction.

To extract the embedded data in I'_M, I'_M is partition into blocks $\{B'_i\}_{i=1}^{N}$ of size m×m. For each block, the local variance is calculated using Eq. 1. For those blocks with variance smaller than TH, the modified prediction error $e'_{i,j}$ is calculated. Sequentially scan $e'_{i,j}$ and extract the embedded bits and recovered the $e'_{i,j}$ to $e_{i,j}$. The first |L| extracted bits are the LSBs of I_L and therefore, I_L can be recovered. Combining I_L and I_M and shifting those pixels recorded in the location map back to its original state, the original cover image I can be recovered.

PROPOSED METHOD

LVCR method provides a better embedding performance over Tsai *et al.* (2009)'s method; however, it is inefficient in dealing with the location map. To store

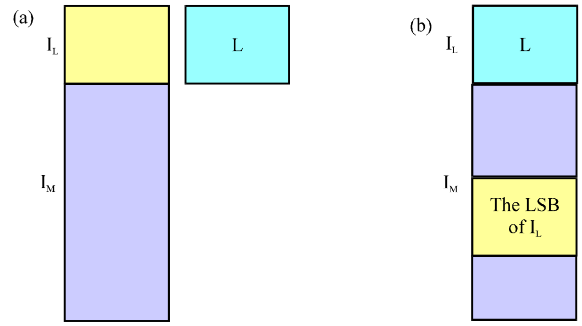

Fig. 2: Embed the L: (a)Before embed and (b) After embed

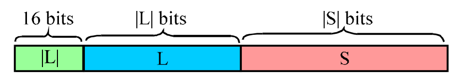

Fig. 3: The component and it's length of LS

the compressed location map L, LVCR has to use |L| pixels in I_L to record L and the LSBs of these pixels have to be embedded into I_M together with the secret data, as shown in Fig. 2. It can be seen that a large |L| might occupy the embeddable spaces significantly.

This study proposed an efficient method for storing the compressed location map. Instead of embedding L in the LSBs of pixels in I_L, we adopt the strategy used by Tsai *et al.* (2009) to concatenate L with the secret data, as show in Fig. 3 and the resultant bit stream BS are then embedded directly into the pre-shifted cover image. Because the embedment of L in the LSBs of I_L is no longer required, the proposed method improves the payload considerably, especially when the size of the location map is large. The detailed embedding and extraction procedures are given in the following sub-section.

The embedding procedure:

Input: A cover image Ic of size P×Q and secret data S

Output: A stego image I'.

Step 1: Construct a zero-initialized binary location map of size P×Q and scan the cover image Ic. If the scanned pixel is 0 or 255, set the pixel value in the corresponding position of the map to 1 and shift pixels valued 0 and 255 to 1 and 254, respectively. The location map is then compressed using a JBIG2 (Howard, *et al.*, 1998) coder. Denote the compressed result by L of size |L| and denote the shifted cover image by I

Step 2: Concatenate |L|, L and *S* of size |S| to form a bit stream BS. Let |BS| denote the length of BS.

Step 3: Partition I into N blocks $\{B_i\}_{i=0}^{N-1}$ of size 3×3. The variance of each block is calculated using Eq. 1. For those blocks with variance smaller than the threshold TH, use Eqs. 2-10 to predict the values of those non-basic pixels of each block and obtain a set of prediction errors $e_{i,j}$

Step 4: From the prediction error histogram, obtain two pairs of peak and zero points (P_L, Z_L) and (P_R, Z_R), where the subscript L and R represent the left hand side and right hand side peak and zero points, respectively.

Step 5: Scan the prediction errors $e_{i,j}$. If the scanned prediction error $e_{i,j} = P_R$ or $e_{i,j} = P_L$, extract a bit s from S and perform the following modification:

$$e'_{i,j} = \begin{cases} e_{i,j} & s = 0, \\ e_{i,j} + 1 & s = 1 \text{ and } e_{i,j} = P_R, \\ e_{i,j} - 1 & s = 1 \text{ and } e_{i,j} = P_L. \end{cases}$$

Otherwise, $e_{i,j}$ has to be shifted to $e'_{i,j}$ using the following equation:

$$e'_{i,j} = \begin{cases} e_{i,j} + 1 & P_R < e_{i,j} < Z_R, \\ e_{i,j} - 1 & Z_L < e_{i,j} < P_L, \\ e_{i,j} & \text{otherwise.} \end{cases}$$

Step 6: The stego block B'_i can be obtained by adding up $e'_{i,j}$ and $p_{i,j}$. Combine all the stego block, we obtain a stego image I'

Once the embedding procedure is complete, a stego image is embedded with secret data and the information required for data extraction.

DATA EXTRACTION AND IMAGE RECOVERY

Since the basic pixels remains unchanged after secret data embedded, the modified prediction errors can be reconstructed by referencing the same set of basic pixels. The embedded data and image recovery can be performed by shifting the modified prediction errors. The detailed procedure is listed:

Input: A stego image I' of size P×Q.
Output: A recovered original image I and secret data S
Step 1: Partition I' into blocks $\{B'_i\}_{i=0}^{N-1}$ of size 3×3.
Step 2: For those blocks with variance smaller than TH, obtain the prediction errors $e'_{i,j}$ of those non-basic pixels using Eqs. 2-10
Step 3: Scan the prediction errors $e'_{i,j}$ using the same order as in the embedding stage. A data bit can be extracted using the following equation:

$$s = \begin{cases} 0 & e'_{i,j} = P_R \quad \text{or} \quad e'_{i,j} = P_L, \\ 1 & e'_{i,j} = P_R + 1 \quad \text{or} \quad e'_{i,j} = P_L - 1. \end{cases}$$

The origin prediction error can be recovered by shifting $e'_{i,j}$ back to its original state $e_{i,j}$:

$$e_{i,j} = \begin{cases} e'_{i,j} - 1 & P_R < e'_{i,j} < Z_R, \\ e'_{i,j} + 1 & Z_L < e'_{i,j} < P_L, \\ e'_{i,j} & \text{otherwise.} \end{cases}$$

Step 4: Repeat Step 3 until all the embedded message bits LS are extracted. The first 16 bits records the length |L| and the compressed location map L and S can then be obtained
Step 5: Add $e_{i,j}$ to $p_{i,j}$, the original block B_i can be obtained. Combine the recovered blocks to obtain the shifted cover image I
Step 6: According to L, recover the shifted cover image I to the original cover image Ic

Note that the secret message can only be extracted when P_R, Z_R, P_L, Z_L, TH and |LS| are known. Therefore, these information can be used as a key and transmitted to the receiver side via a secret channel.

EXPERIMENTAL RESULTS

To demonstrate the improvement of the proposed method over LVCR method, four common images, Airplane, Parrots, Farmhouse and Hats were employed as the cover images, as shown in Fig. 4. These images are 8-bit of size 512×768. The secret bits were generated by using a Pseudo Random Number Generator (PRNG) and the Peak Signal to Noise Ratio (PSNR) was used to measure the image quality of the stego image. A higher PSNR indicates that the stego image offers a better image quality.

Because the proposed method is an improvement of the LVCR method, we compare the payload of the proposed method and PSNR with those of LVCR. In the experiments, TH is set to infinity to obtain the maximum payload. The results are shown in Table 1.

Table 1 reveals that as |L| increased, the performance of the proposed method is significantly better than that of LVCR. The reason is that the proposed method does not require preserving a special part for embedding the location map. We embed data directly into the cover image with the secret data. Therefore, the payload of the proposed method is considerably increased and the high quality stego image is generated.

The experiment results also demonstrate the proposed method provides better results for various payloads. Figure 5 shows the PSNR in dB versus payload

Table 1: Comparison of maximum payload and PSNR

	Maximum payload(bit)				PSNR		
Image (512×768)	Proposed method	|L|	LVCR	Gain	Proposed method	LVCR	Gain
Airplane	119906	42664	83193	36713	50.21	49.59	0.062
Parrots	111399	2424	110424	975	51.71	49.97	1.74
Farmhouse	52631	24728	45642	6989	49.96	49.72	0.24
Hats	118959	464	117942	1017	50.05	50	0.05

Fig. 4(a-d): Four common test images. (a) Airplane, (b) Parrots, (c) Farmhouse and (d) Hats

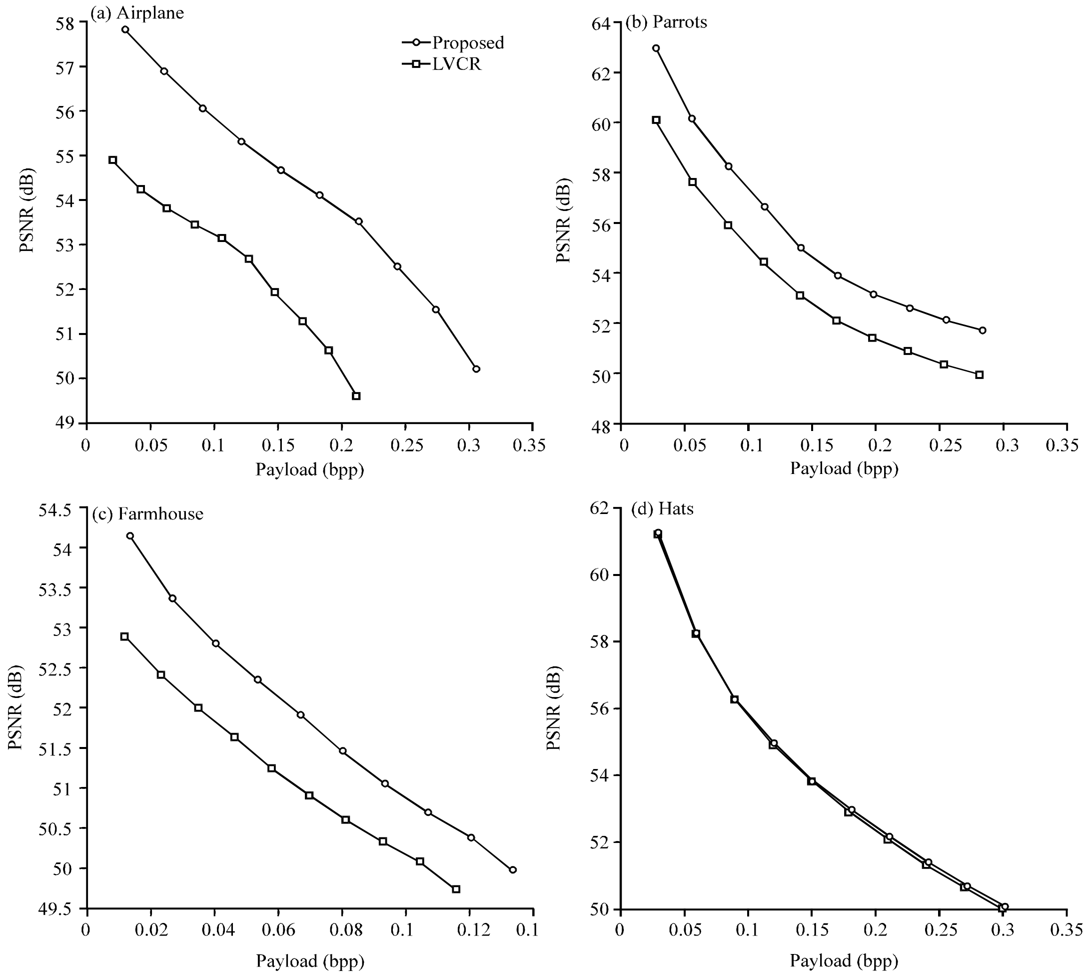

Fig. 5(a-d): Comparison of the pure payload and PSNR

in bpp. The results reveal that the proposed method offers higher PSNR under the same payload. For example, for the Airplane image, the PSNR of the proposed method is 55.8 dB at 0.1 bpp, whereas the PSNR of LVCR is only 53.2 dB. For those images requiring smaller location map such as Hats, the proposed method also provides a slightly better or equivalent image quality.

CONCLUSIONS

In this study, we proposed an alternative method for recording the location map to improve Hong and Chen's LVCR method proposed in 2010. In LVCR, the location map is recorded using the LSBs of a set of cover pixels, which may significantly reduce the payload when the location map is large. The proposed method adopts an alternative method to pre-shift the saturated pixels in the cover image and embed the compressed location map directly into the cover pixels. The experimental results reveal that the proposed method offers higher or equivalent PSNR than that of LVCR method under the same payload.

ACKNOWLEDGMENTS

This research was supported by the National Science Council of the Republic of China under the Grants NSC100-2622-E-412-003-CC3andNSC100-2221-E-412-003.

REFERENCES

Ahmed, M.A., M.L.M. Kiah, B.B. Zaidan and A.A. Zaidan, 2010. A novel embedding method to increase capacity and robustness of low-bit encoding audio steganography technique using noise gate software logic algorithm. J. Applied Sci., 10: 59-64.

Al-Frajat, A.K., H.A. Jalab, Z.M. Kasirun, A.A. Zaidan and B.B. Zaidan, 2010. Hiding data in video file: An overview. J. Applied Sci., 10: 1644-1649.

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

Hmood, A.K., B.B. Zaidan, A.A. Zaidan and H.A. Jalab, 2010. An overview on hiding information technique in images. J. Applied Sci., 10: 2094-2100.

Hong, W. and T.S. Chen, 2010. A local variance-controlled reversible data hiding method using prediction and histogram-shifting. J. Syst. Software, 83: 2653-2663.

Hong, W., J. Chen and T.S. Chen, 2009. Blockwise reversible data hiding by contrast mapping. Inform. Technol. J., 8: 1287-1291.

Hong, W., T.S. Chen, K. Y. Lin and W.C. Chiang, 2010. A modified histogram shifting based reversible data hiding scheme for high quality images. Inform. Technol. J., 9: 179-183.

Howard, P.G., F. Kossentini, B. Martins, S. Forchhammer and W.J. Rucklidge, 1998. The emerging JBIG2 standard. IEEE Trans. Circuits Syst. VideoTechnol., 8: 838-848.

Li, C.H. Z.M. Lu and Y.X. Su, 2011. Reversible data hiding for Btc-compressed Images based on bitplane flipping and histogram shifting of mean tables. Inform. Technol. J., 10: 1421-1426.

Luo, H., Z. Zhao and Z.M. Lu, 2011. Joint secret sharing and data hiding for block truncation coding compressed image transmission. Inform. Technol. J., 10: 681-685.

Mohammad, N., X. Sun and H. Yang, 2011. An excellent Image data hiding algorithm based on BTC. Inform. Technol. J., 10: 1415-1420.

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

Provos, N. and P. Honeyman, 2003. Hide and seek: An introduction to steganography. IEEE Secur. Privacy, 1: 32-44.

Salem, Y., M. Abomhara, O.O. Khalifa, A.A. Zaidan and B.B. Zaidan, 2011. A review on multimedia communications cryptography. Res. J. Inform. Technol., 3: 146-152.

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

Tsai, P.Y., Y.C. Hu and H.L. Yeh, 2009. Reversible image hiding scheme using predictive coding and histogram shifting. Signal. Process., 89: 1129-1143.

Yang, H. and J. Yin, 2012. An adaptive block truncation coding algorithm based on data hiding. Inf. Technol. J., 10: 1-4.

Zhao, Z. and H. Luo, 2012. Reversible data hiding based on Hilbert curve scan and histogram modification. Inform. Technol. J., 11: 209-216.