World Engineering & Applied Sciences Journal 6 (3): 157-163, 2015
ISSN 2079-2204

DOI: 10.5829/idosi.weasj.2015.6.3.22213

Formation and Transmission of Mosaic Image Based on IGM and DCT

S. Merlin

II ME CSE, Regional Centre of Anna University, Tirunelveli, Tamil Nadu, India

Abstract: Information hiding in images is an effective way to transmit images in a secure steganographic manner. In addition to keeping the content of the image secret, steganography has the added advantage of not raising suspicion in a hostile observer. Traditionally image hiding algorithms suffer from a lack of balance of capacity, invisibility and robustness. This paper presents two methods for steganographic transmission of images: one in spatial domain using reversible color transmission and another in discrete cosine transform domain using grey prediction based compression and embedding. The former exhibits higher embedding capacity since a secret image can be hidden onto a cover image of the same size providing a capacity of 8 bits per pixel. The latter exhibits higher robustness to various common image processing modifications. A comparative analysis is provided to evaluate the two methods. The methods exhibit good invisibility as measured by the peak signal to noise ratio and normalized correlation between the original cover and marked cover images. Experiments conducted using a test database made of images available in the public domain including UCSD database confirm the performance of the presented methods.

Key words: Data Hiding · Attacks · Discrete Cosine Transform · Steganography

INTRODUCTION

Information hiding model, put forward by Simmons in 1984, was derived from prisoner's problem. Along with the development of network communication, information security has become an ever-increasing concern. At the same time, enhancement of hacking techniques has caused the great threats to information communication. In order to deliver the information secretly, traditional cryptography mainly use replacing or scrambling the technologies to disrupt the original features of the secret information because the cipher-texts resemble a stream of meaningless codes, they are easily attract the attacker to try either recover them or simply destroy them, which is seriously affect the security information communication. So it has been difficult to meet the requirements of nowadays' secure communication. To this problem, information hiding technology it mainly focus on how to hide the code information into another host media, makes it hard for attackers to find out if the attacker is lucky enough to detect the carried secrets, they cannot extract the secret information from the carrier without the embedded key. These characteristics make it widely accepted in information security fields.

Information Hiding Algorithms: The first kinds are based on the spatial domain the second kinds are in transform domain. The third kinds are based on the covert channel, and the fourth kinds are based on quantization and compression.

- The first kinds of algorithms have large capacity, but the robustness is unsatisfactory.
- The second kinds of algorithms have good robustness and invisibility; however, the data-hiding capacity is low.
- The third kinds of algorithms have excellent concealment (imperceptibility), but the capacity is also very low and influenced by channel conditions greatly.

The defects lie in extracted secret information, which may have the slight distortion in the last kinds of algorithms. Information hiding should be viewed as a tradeoff among invisibility, capacity and robustness, which has grabbed the attention of researchers. In this project first compress the secret information by JPEG and then embed it into the transform domain of the cover image, which both have large capacity and reserve the

Corresponding Author: S. Merlin, II ME CSE, Regional Centre of Anna University, Tirunelveli, Tamil Nadu, India.

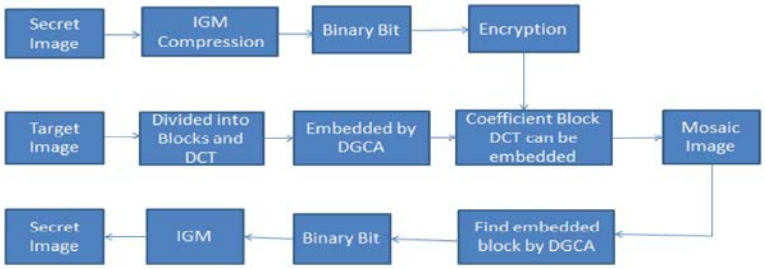

Fig. 1:

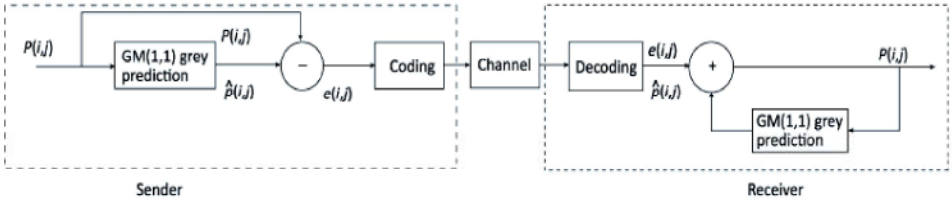

Fig. 2

satisfactory robustness in transform domain .In this project a blind color image information hiding algorithm based on grey prediction and grey relational analysis in Discrete Cosine Transform.(DCT)is proposed. Compressing the secret image lossless based on the improved GM (1, 1) prediction model is described in IGM compression.

Advantage: The advantage of this method is that can balance among invisibility, capacity and robustness.

Review of Related Methods: The methods are

- Image compression based on IGM
- Block section using DGRA
- Information embedding
- Information extracting

Data is embedded by performing de-clustering of pixels. To find similar pixels reversible data hiding scheme for embedding secret data in VQ compressed code based on de-clustering property of adjacent areas in natural image [1].

Digital water making is a technique which allows an individual to add hidden copy right notice or other verification messages to digital audio, video or image signals and documents. Water making is done using Discrete Cosine Transform (DCT) and Discrete Wavelet Transform techniques (DWT) are used to compare with peak signal to noise ratio (PSNR) with different threshold values.DCT give better image than (DWT) [2].

Proposed Method: The overall process for secure image transmission is explained in this Figure 1.

Image Compression Based on IGM: The image compression technology main contains lossless compression and lossy compression.

To deal with the general image information, lossy compression such as JPEG, MPEG is often used information such as satellite remote sensing image; geographical image, medical image and military secret image need to completely reflect the original information.

So these applications still use lossless compression to reduce the redundant data. It adopts IGM prediction model to compress the secret image. And the process of compression and decompression is shown in the Figure.

Suppose the original sequence is $P^{(0)} = (P^{(0)}(1), P^{(0)}(2), \ldots P^{(0)}(n))$, its generating sequence after accumulated one time is $P^{(1)} = (P^{(1)}(1), P^{(1)}(2), \ldots P^{(1)}(n))$, and $P^{(1)}(k) = \sum_{i=1}^{k} P^{(0)}(i) (k = 1,2,..n)$.

The nearest neighbor α-weighted generating sequence of $X^{(1)}$ which can be described by $Z^{(1)}(k) = \alpha p^{(1)}(k) + (1-\alpha) p^{(1)}(k-1), k = 2,3, \ldots n;$ $\alpha \in (0,1)$. So predicted value is $P^{(0)}(k+1) = P^{(1)}(k+1) - P^{(1)}(k), k = 1,2,..n-1$ and the prediction error is $e(k) = P^{(0)}(k) - P^{(0)}(k), k = 1,2.., n$.

The determination of weight α, first it sets α value close to zero, and figures out the sum of squares due to prediction errors (SSE), and then it sets $\alpha = \alpha + \Delta\alpha$.

Table 1: Paragraphs code

Paragraph Identification Code	Paragraphs Range	Digits of Segment Code
0	0	0
1	-1,+1	0
10	-2,+2	0
11	[-4,-3],[3,4]	1
100	[-8,-5],[5,8]	2
101	[-16,-9],[9,16]	3
110	[-32,-17],[17,32]	4
111	[-Max,-33],[33,Max]	8

Table 2: Segment code corresponding to paragraphs code 110

Quantization Error	Sign bit C_4	Segment Code C_5 C_6
-8	1	11
-7	1	10
-6	1	01
-5	1	00
5	0	00
6	0	01
7	0	10
8	0	11

Table 3: Compression ratio of several image lossless compression methods

Image	Huffman Coding	LZW Coding	DPCM Prediction+ Huffman Coding	JPEG-LS	GM(1,1)+Variable Length Coding
Lena	1.07	1.2	1.69	1.7	1.61
Peppers	1.04	1.08	1.53	1.81	1.85
Baboon	1.02	1.13	1.63	1.62	1.48
Barbara	1.13	1.17	1.57	1.78	1.76
Goldhill	1.05	1.11	1.54	1.79	1.78
Boat	1.08	1.15	1.61	1.65	1.49

Table 4: Time-consuming of several image lossless compression methods (units: ms)

Image	Huffman Coding	LZW Coding	DPCM Prediction+ Huffman Coding	JPEG-LS	GM(1,1)+Variable Length Coding
Lena	4880	5221	4520	4498	4474
Peppers	4907	5145	4285	4793	4605
Baboon	4977	5303	4583	4693	4306
Barbara	4753	5474	4253	4625	4522
Goldhill	5022	5401	4477	4630	4552
Boat	4940	5276	4208	4410	4384

Considering that IGM model has more accurate prediction results for those pixels whose values are changed slowly, it takes the place where pixel values vary greatly as a block of the partition line. In that way, it can get a smaller Prediction error and higher compression efficiency.

Combining them after the predictive coding for every block can make it more difficult for the attacker to interpret the secret information. Suppose the grey image is $P(i, j)$ i= 1, 2,…,MP ,j= 1, 2,….,NP, and we first divide the secret information into N pieces. All of the N pieces of secret information can be embedded into a carrier image.

It encodes $e(k)$ by the combination of PCM coding and variable length coding, where $c1c2c3$ are paragraph identity codes, and $c4$ is the sign bit. The specific mapping relation of error codes is provided in Table 1.

The max in paragraph identification code 111 should be determined by the actual maximum of absolute value of the prediction error.

Table 2 shows the segment code corresponding to paragraph identification code 110, and segment codes corresponding to other paragraph identification codes are similar to the Table 2. Suppose the prediction error after quantification is x, we can find out paragraph identification codes $c1c2c3$ and sign bit $c4$ from Table 1 according to x value.

Tables 3 and 4 show compression ratio and time consumed of several image lossless compression methods respectively. Compression ratio (Cr) in Table 3 is defined as:

$$Cr = \frac{Size\ before\ Compression}{Size\ after\ Compression}.$$

Block Section Using DGRA: Grey Relational analysis has been widely applied in data sequence relevance, image matching, image texture analysis. When it comes to color image, because of the high data redundancy, through DGRA to find out the blocks with rich texture and similar pixel value of corresponding position at R/G/B components. The visual quality of carrier image will not be changed after embedding.

The texture characteristic of color image are the same as that of its components of R, G, B. First choose the R component of the color image, every block will be executed DGRA with standard block to get DGCD(R). Then pick out those blocks with rich texture in terms of their respective DGCD(R).

According to direction sensitivity to image texture of human eyes, define double-dimensional weighted grey relational degree as

$$\mathrm{DGCD}= a\mathrm{GCD}H + b\mathrm{GCD}V + c\mathrm{GCD}D$$

$$X=(X_1,X_2,X_3,X_4,X_5,X_6,X_7,X_8)=\begin{bmatrix} x_{11} & x_{12} & x_{13} & x_{14} & x_{15} & x_{16} & x_{17} & x_{18} \\ x_{21} & x_{22} & x_{23} & x_{24} & x_{25} & x_{26} & x_{27} & x_{28} \\ x_{31} & x_{32} & x_{33} & x_{34} & x_{35} & x_{36} & x_{37} & x_{38} \\ x_{41} & x_{42} & x_{43} & x_{44} & x_{45} & x_{46} & x_{47} & x_{48} \\ x_{51} & x_{52} & x_{53} & x_{54} & x_{55} & x_{56} & x_{57} & x_{58} \\ x_{61} & x_{62} & x_{63} & x_{64} & x_{65} & x_{66} & x_{67} & x_{68} \\ x_{71} & x_{72} & x_{73} & x_{74} & x_{75} & x_{76} & x_{77} & x_{78} \\ x_{81} & x_{82} & x_{83} & x_{84} & x_{85} & x_{86} & x_{87} & x_{88} \end{bmatrix}$$

As one block of R component, so

$$DX=\mathrm{dct2}(X)=\begin{bmatrix} dx_{11} & dx_{12} & dx_{13} & dx_{14} & dx_{15} & dx_{16} & dx_{17} & dx_{18} \\ dx_{21} & dx_{22} & dx_{23} & dx_{24} & dx_{25} & dx_{26} & dx_{27} & dx_{28} \\ dx_{31} & dx_{32} & dx_{33} & dx_{34} & dx_{35} & dx_{36} & dx_{37} & dx_{38} \\ dx_{41} & dx_{42} & dx_{43} & dx_{44} & dx_{45} & dx_{46} & dx_{47} & dx_{48} \\ dx_{51} & dx_{52} & dx_{53} & dx_{54} & dx_{55} & dx_{56} & dx_{57} & dx_{58} \\ dx_{61} & dx_{62} & dx_{63} & dx_{64} & dx_{65} & dx_{66} & dx_{67} & dx_{68} \\ dx_{71} & dx_{72} & dx_{73} & dx_{74} & dx_{75} & dx_{76} & dx_{77} & dx_{78} \\ dx_{81} & dx_{82} & dx_{83} & dx_{84} & dx_{85} & dx_{86} & dx_{87} & dx_{88} \end{bmatrix}$$

Encryption: In Encryption part randperm function is used to shuffle the values before embedding the information.

Random shuffling perform by A(:,randperm(size(A,2))), using this function we can suffle the value in matlab.

Information Embedding:

Step 1: Compress the secret image by methods in IGM; determine the secret information bit stream.

Step 2: Encrypt the binary bit stream.

Step 3: Divide R, G, and B components of cover image into 8×8blocks.

Step 4: Select blocks which can embed secret information by methods in Section DGRA, denoted by Embed Block.

Step 5: Find out the embedding mid frequency coefficients in every block from Embed-Block according to the size of DGCD and the features of block DCT.

Step 6: Embed the secret information bit stream.

When Star(r) =0, the coefficient values are embedding in ascending order.

When Star(r) =1, here the coefficient values are embedding in descending order.

Step 7: Anti-Zigzag-Sag scanning and Inverse-DCT (IDCT) are applied in these blocks and recover the embedding secret information.

RESULT

Database Used, Size and Nature of the Images Used: The common database images like UCSD, standard test image database, medpix database, and USGS database are taken for result analysis the proposed system has been applied in these database and the obtain results have been analyzed. The size of each image in this database is 512*512; they are color images in JPEG format.

In the first phase the size the secret and target image of same size have been taken, therefore each pixel in the secret image can be embedded exactly on 1 pixel in the

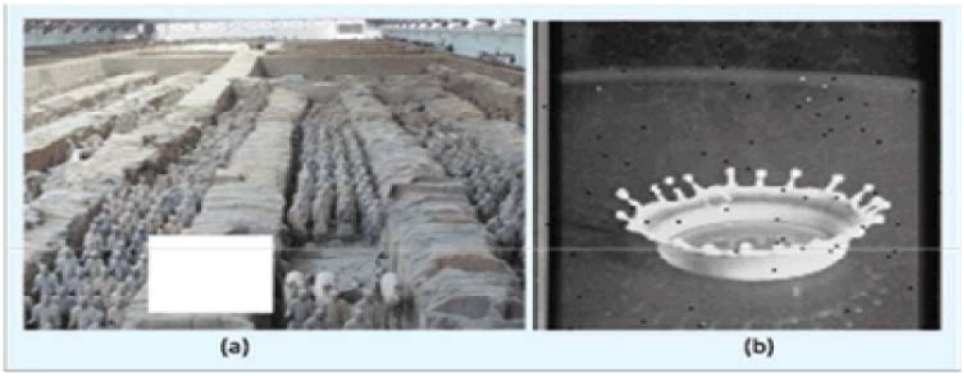

Fig. 3:

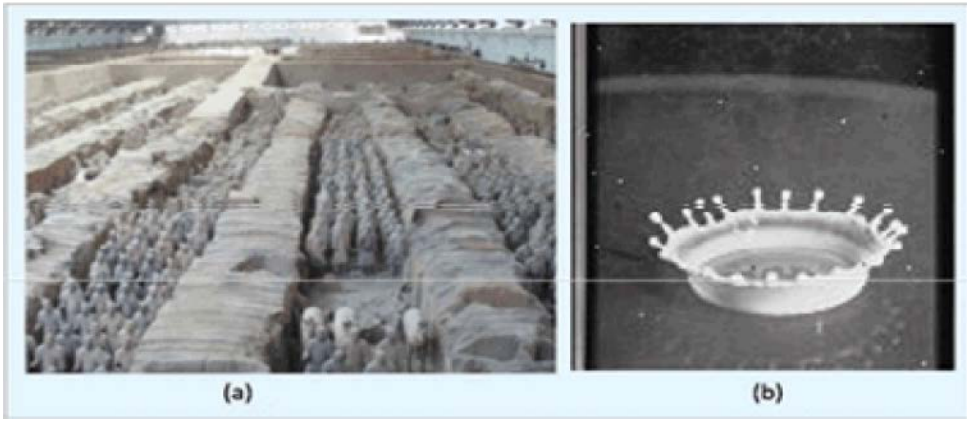

Fig. 4:

target image (Capacity=1 pixel), whereas in the proposed image the size of the target image will be fixed and the size of secret image may vary, here the capacity will be calculated using PSNR. The PSNR of the secret image has been compared with the PSNR of the recovered secret image thus the performance of the system can be analyzed.

Performance Measures: PSNR: The Peak Signal to Noise Ratio (PSNR) has been used as a benchmark to evaluate new objective perceptual video quality metrics .there is not currently an international Recommendation specifying exactly how to perform this critical measurement.

Since the calculation of PSNR is highly dependent upon proper calculation of spatial alignment, temporal alignment, gain, and level offset between the processed video sequence and the original video sequence, one must also specify the method of performing these calibration procedures.

Since the calculation of PSNR is highly dependent upon proper estimation of spatial alignment, temporal alignment, gain, and level offset between the processed video sequence and the original video sequence.

The method of measurement for PSNR should ideally include a method for performing these calibration procedures.

This PSNR calculation method in this Recommendation has the advantage of automatically determining the highest possible PSNR value for a given video sequence over the range of spatial and temporal shifts.

Only one temporal shift is allowed for all frames in the entire processed video sequence

Nature of Attacks

Cutting Attack: Cutting attack is the embedded image after cutting 1/16, and Figure 3(b) is the extracted secret information from Figure 3(a).

Low-Pass Filter (LPF) Attack: LPF is the carrier image after low- pass filtering with 3×3, and Figure 4(b) is the extracted secret information from Figure 4(a)

Gauss Noise: Figure 5(a) is the carrier image after Gauss noise with zero mean and 0.005 variance, and Figure 5(b) is the extracted secret information from Figure 5(a).

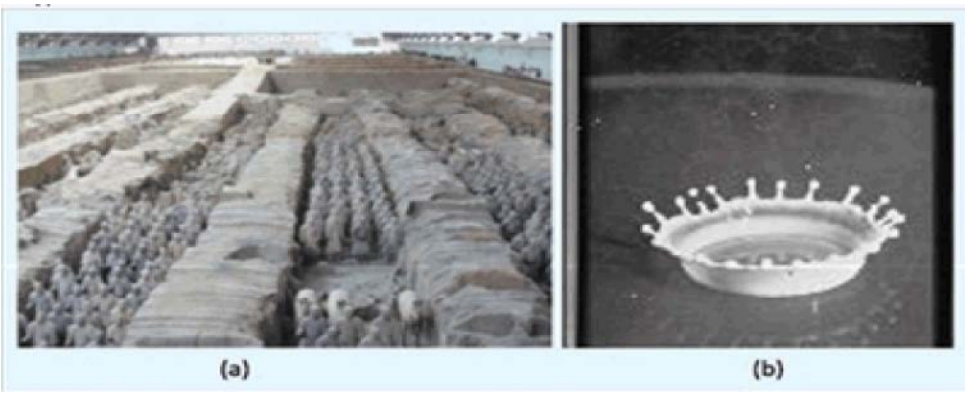

Fig. 5:

Fig. 6:

Fig. 7:

JPEG Attack: Figure 6(a) is the carrier image after 95% JPEG compression, and Figure 6(b) is the extracted secret information from Figure 6 (a).

S&P Attack: Figure 7(a) is the carrier image after adding S&P noise whose density is 0.01, and Figure 7(b) is the extracted secret information from Figure 7 (a).

Compare Embedding Capacity with Phase 1: The quality of the mosaic image is measured using PSNR value for both phases. In the first phase PSNR value was calculated for mosaic image. If it is below 20 in value , the quality of the mosaic is referred as average. In the second phase , PSNR value is calculated as done in phase one. When comparing phase one the PSNR value 35 and above is referred as good in phase two.

Images	PSNR value for phase 1	PSNR value for phase 2
Lena	16.264	40.340
Peppers	10.256	39.481
Baboon	15.936	45.531
Barbara	20.003	32.314
Gold hill	12.037	37.455
Boat	18.000	42.002

CONCLUSION

In this project a blind color image information hiding algorithm based on grey prediction and grey relational analysis in DCT domain. The DCT domain based blind information hiding occupies the main stream position . Various attacks in this project resilience of the process is used to confuse the blind information hiding to embedded the compress bit stream to incorporate the HVS properties. The proposed scheme is simulated and the result is compared with traditional algorithms. In future work focus on how to use the properties of HVS to further improve the quality of information hiding algorithm and develop robust information hiding scheme against geometric distortions.

REFERENCES

1. Chang, C.C., Y.P. Hsieh and C.Y. Lin, 2007. Lossless DataEmbedding With High Embedding CapacityBased on De-Clustering for VQ-CompressedCodes, IEEE Transactions on InformationForensics and Security, 2(3): 341-349.
2. Xinge, Y.O.U., D.U. Liang and CHEUNG Yiuming, 2010. A Blind Watermarking Scheme Using NewNon-Tensor Product Wavelet Filter Banks[J].IEEE Transactions on Image Processing, 19(12): 3271-3284.
3. JIAO Jianquan, 2008. Research on Information Hid-ing Technology on DCT Domain Based on Grey System Theory[D]. Zhengzhou, China:The PLA Information Engineering University.(in Chinese).
4. Kekre, H.B., A. Athawale and P.N. Halarnkar, 2010. Performance Comparison of DCT andWalsh Transform for Steganography[C]//Proceedings of International Conference andWorkshop on Emerging Trends in Technol-ogy (ICWET 2010): Mumbai, Maharashtra, India. ACM Press, pp: 81-88.
5. Coltuc, D. and J.M. Chassery, 2007. Very fast watermarking by reversible contrast mapping,? IEEE Signal Process. Lett., 14(4): 255-258.
6. Reinhard, E., M. Ashikhmin, B. Gooch and P. Shirley, 2001. Color transfer between images,? IEEE Comput. Graph. Appl., 21(5): 34-41.
7. Chen, G., Y. Mao and C.K. Chui, 2004. A symmetric image encryption scheme based on 3D chaotic cat maps,? Chaos Solit. Fract, 21(3): 749-761.
8. Kwok, H.S. and W.K.S. Tang, 2007. A fast image encryption system based on chaotic maps with finite precision representation, Chaos Solit. Fract., 32(4): 1518-1529.
I. Lai J. and W.H. Tsai, 2011. Secret-fragment-visible mosaic image—A new computer art and its application to information hiding, IEEE Trans. Inf. Forens. Secur, 6(3): 936-945.
9. Fridrich, J., 1998. Symmetric ciphers based on two-dimensional chaotic maps, Int. J. Bifurcat. Chaos, 8(6): 1259-1284.
10. Tian, J., 2003. Reversible data embedding using a difference expansion, IEEE Trans. Circuits Syst. Video Technol., 13(8): 890-896.
11. Fridrich, J., M. Goljan, and R. Du, 2001. Invertible authentication, Proc. SPIE, 3971: 197-208.
12. Zhang, L.H., X.F. Liao and X.B. Wang, 2005. An image encryption approach based on chaotic maps, Chaos Solit. Fract., 24(3): 759-765.
13. Wang, R.Z., C.F. Lin and J.C. Lin, Image hiding by optimal LSB substitution and genetic algorithm, Pattern Recog., 34(3): 671-683.
14. Lee, S., C.D. Yoo and T. Kalker, 2007. Reversible image watermarking based on integer-to-integer wavelet transform, IEEE Trans. Inf. Forens. Secur., 2(3): 321-330.
15. Patidar, V., N.K. Pareek, G. Purohit and K.K. Sud, 2011. A robust and secure chaotic standard map based pseudorandom permutationsubstitution scheme for image encryption, Opt. Commun., 284(19): 4331-4339.
16. Sachnev, V., H.J. Kim, J. Nam, S. Suresh and Y.Q. Shi, 2009. Reversible watermarking algorithm using sorting and prediction, IEEE Trans.Circuits Syst. Video Technol., 19(7): 989-999.
17. Lin, W.H., S.J. Horng, T.W. Kao, P. Fan, C.L. Lee and Y. Pan, 2008. An efficient watermarking method based on significant difference of wavelet coefficient quantization,IEEE Trans. Multimedia, 10(5): 746-757.
18. Zhang, W., X. Hu, X. Li and N. Yu, XXXX. Recursive histogram modification: Establishing equivalency between reversible data hiding and lossless data compression, IEEE Trans. Image Process., 22(7): 2775-2785.
19. Hu, X., W. Zhang, X. Hu, N. Yu, X. Zhao and F. Li, 2013. Fast estimation of optimal marked-signal distribution for reversible data hiding, IEEE Trans. Inf. Forens. Secur., 8(5): 187-193.
20. Li, X., B. Yang and T. Zeng, 2011. Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection, IEEE Trans. Image Process., 20(12): 3524-3533.
21. Ni, Z., Y.Q. Shi, N. Ansari and W. Su, 2006. Reversible data hiding, IEEE Trans. Circuits Syst. Video Technol., 16(3): 354-362.