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 12 (14): 2697-2702, 2013
ISSN 1812-5638 / DOI: 10.3923/itj.2013.2697.2702

An Secret Communication-oriented High Capacity Information Hiding Scheme Based on Cl Multi-wavelet and Combination Bit Plane

[1]Tao Zhang, [1]Yong-Feng Ju, [2]Shuai Ren and [2]Jing-Xiang Lei
[1]School of Electronic and Control Engineering, Chang'an University, Xi'an 710064, China
[2]School of Information Engineering, Chang'an University, Xi'an 710064, China

Abstract: Take advantage of the first-order transformation of CL multi-wavelet, carrier image is decomposed into four components of lowest resolution sub-image. Use the feather of image bit plane embedded strategy. Propose an Information hiding scheme based on CL and Combination Bit Plane (CBP). LL2 is embedded module of robust parameters. Embed hiding Information in LH2 and HL2 with RAID4 and fragile sign in HH2. The position carried with embedded information of every sub-image is Bit Plane 0. Bit Plane 3 and Bit Plane 7 are auxiliary embedded positions by XOR. Before embedding, improve the consistence of the embedded data bits' order and the character of the sub-image with the chaotic map and the genetic algorithm. The embedding sequence of each bit plane is traversal according to Knight-tour route. Experimental results indicate that the proposed scheme can increase imperceptibility by 20.89% averagely and robustness by 17.20% and have excellent sensitivity of image processing.

Key words: Information hiding, CL multi-wavelet transform, CBP (Combination Bit Plane), logistic chaotic map

INTRODUCTION

Attackers always destroy confidential communication by physical attacks without analysis. So, robustness of information hiding is of vital importance. Most of the literatures don't have good robustness against attacks such as solve rotation, cutting, mean and medium filtering and few resist against them at the same time (Abed and Mustafa, 2010; Lamgunde and Kale, 2011; Abdulfetah *et al*., 2010; Run *et al*., 2012). Multi-wavelet technologies have boosted in information hiding technical field and more and more researchers emphasis on its applications (Ghouti *et al*., 2006; Kumsawat *et al*., 2008; Liu *et al*., 2008). This paper focuses on information hiding algorithm based on CL multi-wavelet and CBP. Firstly, transform the cover image with first-order CL and use four LL_1 sub-images (LL_2, LH_2, HL_2 and HH_2) as host; Then draw the optimal embedded code; scramble pre-hiding information with chaotic map and search the optimal scrambled parameters with genetic algorithm in order to improve the consistence of pre-hiding information and the best embedded code; finally, embed hiding information with Knight-tour route and RAID4. The scheme is named as CL-CBP. Experiments illustrate that CL-CBP is better than traditional schemes as DCT-LSB and DWT-LSB in invisibility and robustness against image attacks such as JPEG2000, cutting, filter and noise. It also has excellent sensitivity to image attacks.

CL MULTI-WAVELET TRANSFORM

Compared with scalar wavelet, CL multi-wavelet transform (Chui and Lian, 1996), which is the earliest and most widely used in multi-wavelet transform field, has distinctive characteristics such as compact sup-port, second-order approximation, integer translation and orthogonality of scalar function. Figure 1 shows CL first-order transformation to Lena image. The research of Jun and Ma (2001) and Figure 1 illustrates that energy ratio LL_1: LL_1: HL_1: HH_1 of four sub-images is about 284:7:2:1.

COMBINATION BIT PLANE

In gray-scale image represented by several bits, each set of bits constitute a binary image, named as

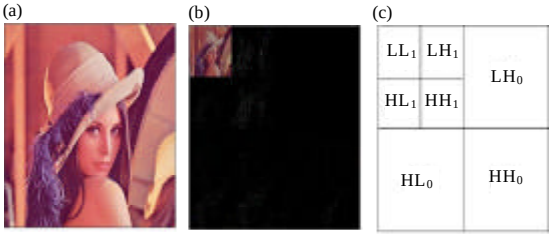

Fig. 1(a-c): First-order CL multi-wavelet transform, (a) Lena normal, (b) Lena CL first-order and (c) Hiding region

Corresponding Author: Tao Zhang, School of Electronic and Control Engineering, Chang'an University, 710064, Xi'an, China

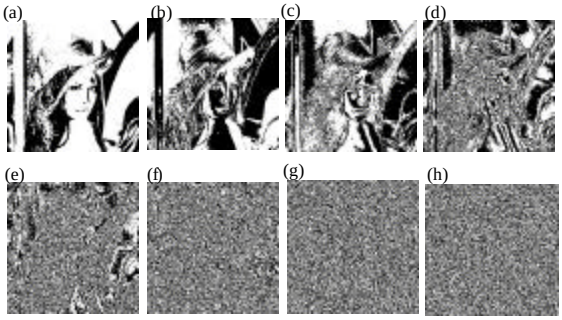

Fig. 2(a-g): Bit Plane decomposition of 256 gray-scale Image (a) Bit plan 7, (b) Bit plan 6, (c) Bit plan 5, (d) Bit plan 4, (e) Bit plan 3, (f) Bit plan 2, (g) Bit plan 1 and (g) Bit plan 0

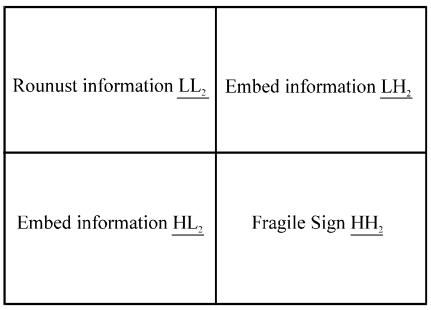

Fig. 3: Embedded region strategy

Bit Plane. Figure 2 shows a bit plane decomposition of normal Lena as a 256 gray-scale image.

Embedded region: Energy ratio of four First-order CL Multi-wavelet Transform sub-images is approximately 284:7:2:1. Based on this feature, Fig. 3 shows embedded region strategy of CL-CBP: LL_2 is robustness module, LH_2 and HL_2 are data embedded modules and HH_2 is a fragile sign module.

Embedded rules: Decompose bit plane from the four CL Multi-wavelet Transform sub-images. Expand the embedded rule to all bit planes overcome defect of the former Least Significant Bit (LSB). Propose the CBP embedding strategy. The embedded rules are as follows:

Rule 1: Bit Plane 0 of four LL_1 sub-images is information embedding plane. Embedded order follow Knight-tour route. Figure 4 shows the Knight-tour Matrix and route of 9×9 image. In the matrix T, "1" stands for the initial point of Knight-tour rout (Paris, 2004).

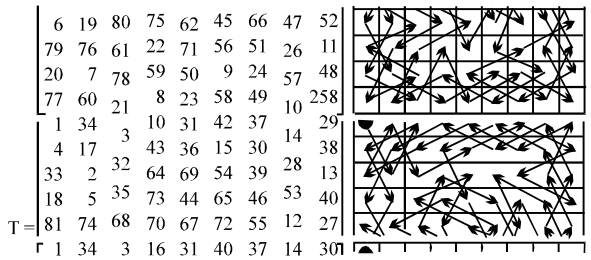

Fig. 4: Knight-tour matrix and route

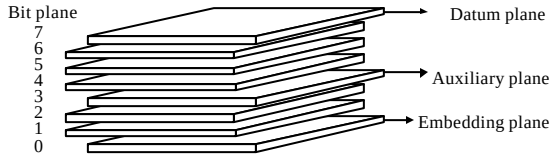

Fig. 5: Bit plane embedding strategies

Rule 2: Bit Plane 3 and Bit Plane 7 are respectively Datum Plane and Auxiliary Plane, as indicated in Fig. 5. C_7 and C_3 are, respectively binary data of Bit Plane 7 and Bit Plane 3. When C_1 is the embedding information, C_3 is modified data according to Eq. 1:

$$C_3 = C_7 \oplus C_1 \tag{1}$$

Embedded process: Information hiding scheme based on CL Multi-wavelet and CBP divided into seven steps. General process is showed in Fig. 6:

Step 1: Transform the cover image with first-order CL multi-wavelet to obtain four LL1 sub-images. Decompose each sub-image into Bit Plane 0, Bit Plane 3 and Bit Plane 7

Step 2: Traverse the Bit Plane 0, Bit Plane 3 and Bit Plane 7 of each sub-image by Knight-tour route. Extract information of Bit Plane 0, Bit Plane 3 and Bit Plane 7 respectively from these four sub-images. According to Eq. 1 in Rule 2, the code of Bit Plane 3 and 7 is , The final code in LH2 and HL2 is C

$$C_1^{3\oplus 7} = C_1^3 \oplus C_1^7 \tag{2}$$

$$C = C_2^{3\oplus 7} \oplus C_3^{3\oplus 7} = t_1, t_2, ..., t_n \quad , \quad n = 2k \tag{3}$$

Step 3: Chaotic map algorithm (Chen and Huang, 2004) of information hiding use Logistic mapping, as

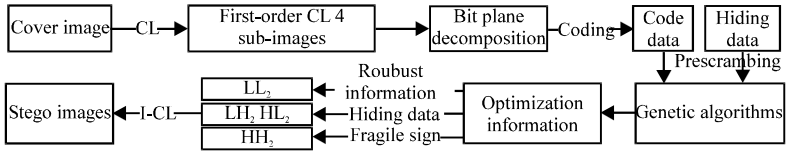

Fig.6 Process for CL-CBP scheme

defined in Eq. 4. Suppose the parameter ì and initial value x_k. The bit series after the logistic mapping is:

$$C_{IN}^{x}, C_{IN}^{x} = b_1^x, b_2^x, \ldots b_{n-1}^x, b_n^x$$

$$x_{k+1} = \mu x_k (1 - x_k), \quad x_k \in (0,1) \tag{4}$$

Step 4: In order to optimize the sequence of embedded bits with genetics algorithm, suppose F as the amount of the same bit value in matched positions of C_{IN}^{x} and C. Use genetic algorithm to change parameters x_k in order to maximize F. The optimization model based on CL-CBP is Eq. 5. Suppose y is the optimization solution. Bring y into C_{IN}^{x} to get optimization embedded bits:

$$C_{IN}^{x}, C_{IN}^{y} = b_1^y, b_2^y, \ldots b_{n-1}^y, b_n^y$$

$$F(y) = MaxF(x_k) = Max\sum(t_n \bar{\oplus} b_n^x) \tag{5}$$

Step 5: Embed C_{IN}^{y} into bit plane of LH_2 and HL_2 with RAID4. Eight bits is the basic data unit of RAID4. The embedding order in the LH_2 and HL_2 follows Knight-tour route

Step 6: LL_2 is the most robust region in four LL_1 sub-images. In order to judge and recover the imperfect information, The CL-CBP embed the Cyclic Redundancy Check (CRC) of RAID4 (recorded as R^L), the optimization scrambling parameters y and μ in LL_2. Therefore, the robustness is improved

Step 7: HH_2 is the most vulnerable region in four LL_1 sub-images. Embed the CRC of RAID4 (recorded as R^H) in HH_2. Information receiver can judge whether the stego image is attacked by comparing R^H and R^L

Embedded process: Information hiding scheme based on CL Multi-wavelet and CBP divided into seven steps. General process is showed in Fig. 6:

Step 1: Transform the cover image with first-order CL multi-wavelet and get four LL_1 sub-images

Step 2: Decompose Bit Plane of the four LL_1. Extract y, μ and R^L form LL_2 and R^H from HH_2

Step 3: It can be indicated that the stego image has not been attacked if $R^L = R^H$. The information receiver can extract Information from the Bit Plane of LH_2 and HL_2 by parameters y. It can be indicated that the stego image is attacked if $R^L \neq R^H$. The process continues

Step 4: Extracting information from bit plane 3 and bit plane 7 of LH_2 and HL_2 by using y and R^L. XOR is performed on Bit plane 3 and bit plane 7

SAFETY PERFORMANCE ANALYSIS

Concerning invisibility, reduce the change of cover image in order to improve invisibility by using chaotic map, genetic algorithm and the feature of Bit Plane 0. Concerning robustness, it can be improved by proposing a novel strategy based on features of CL Multi-wavelet energy distribution, especially embedding information in LH_2 and HL_2 with RAID4 and Knight-tour route, choosing Bit Plane 3 and Bit Plane 7 to be information redundancy embedding module. Concerning sensitivity, it makes the algorithm have excellent sensitivity of image processing using the feature of CL energy distribution, embedding fragile sign and CRC in HH_2.

SIMULATION EXPERIMENT

Simulation environment of the algorithm is Matlab7.0.0.19920. Cover image is Lena (256×256) as shown in Fig. 8a. Stego image is binary image baboon (64×64) as shown in Fig. 8b.

From the above discussion, it indicates that making mobile Ad Hoc Network so vulnerable and insecure is the wireless node authentication issue which was not fundamental resolved. It will introduce the trusted computing theory in the following article. The application of trusted computing is to achieve the purpose of high-security authentication under the low transmission costs in mobile Ad Hoc network.

Scheme performance analysis: Figure 8c shows stego image based on CL-CPB. PSNR value equals 35.9432. It shows that this method is of better invisibility.

Invisibility is determined by Information content. Embed information in 100 images randomly. 2^k is used to denote bit quantity ($0 = 2^k = 65536$). Figure 9 shows the PSNR of different embedding quantity. The experimental results indicated that when k = 12, it is of better invisibility (PSNR = 43.1014).

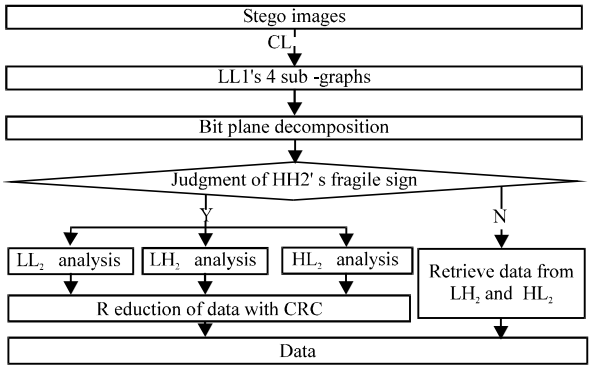

Fig .7: Process for Extracting Information

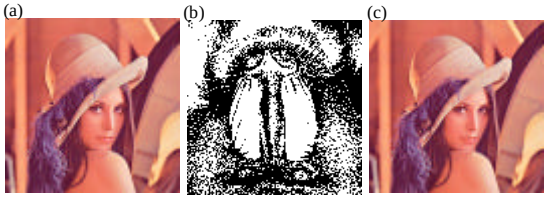

Fig.8(a-c): Invisibility experiment, (a) Cover image, (b) Hiding information and (c) Stego image

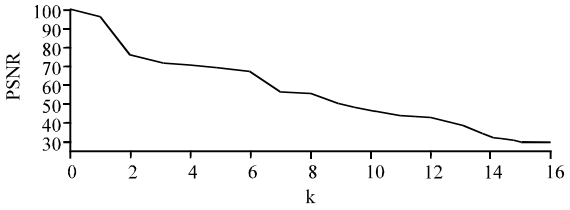

Fig. 9: PSNR of different embedding quantity

Definition of texture evaluation to binary image with n×n pixels is shown in Eq. 6. Where $n = N/2^d$, $d \in \{1,2, ..., \log_2 (N-1)\}$. F (I, j) is the pixel at (I, j) of normal image with n×n pixels. Define modification rate of binary image with n×n pixels in Eq. 7. Where f' (I, j) is the pixel at (I, j) of extraction image with n×n pixels:

$$w = \frac{n \times n}{\sum_{i=0}^{n-1}\sum_{j=0}^{n-1} f(i,j) \overline{\oplus} f(i \pm 1, j \pm 1)} \quad (6)$$

$$p = \frac{\sum_{i=0}^{n-1}\sum_{j=0}^{n-1} f(i,j) \overline{\oplus} f'(i,j)}{n \times n} \quad (7)$$

Robustness test algorithm is defined in Eq. 8. Q is robustness test value. Information extraction is the most preserved when Q = 100:

$$Q = w \times p \quad (8)$$

In the following experiments, the value of d is four. Where operated object is stego image Fig. 8c. Figure 10 shows the result of different attacks such as JPEG2000 compression, cutting, filtering and noise.

Images are vulnerable to compression and cutting attacks, Fig. 11 shows the robustness test value results corresponding to ratio of these attacks.

According to experiment data, embedded information can be identified when robustness test value reach about 30.

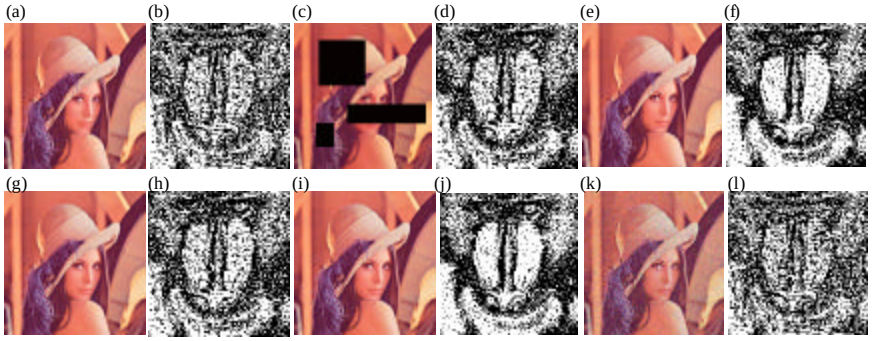

Fig. 10(a-f): Results of robustness experiment, (a) JPEG2000_58% Q=55.01, (b) cutting_25% Q=85.26, (c) mean filter_[3,3] Q = 59.68, (d) wiener2 filter_[3,3] Q = 54.24, (e) Gaussi_μ = 0,s2 = 0.003 Q = 70.24, and (f)'salt and pepper'_d = 0.15 Q = 30.64

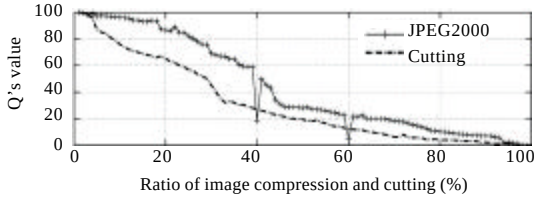

Fig. 11: JPEG2000 and cutting experiment

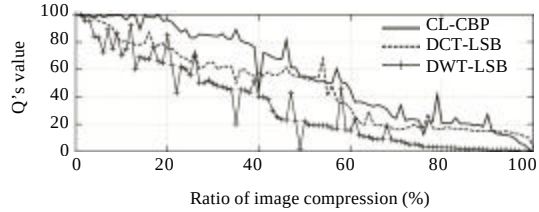

Fig. 12: Compression comparison

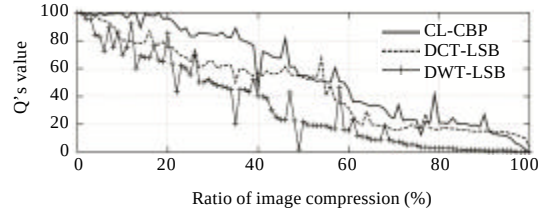

Fig. 13: Cutting comparison

Figure 10 and 11 show that this algorithm is robust against JPEG2000 compression below 51.23%, cutting below 37.90%, common filtering and adding noise.

Perception of tampering is the peculiar characteristic in CL-CBP. Comparing R^L with R^H indicates the algorithm have excellent sensitivity of image processing. Table 1 lists the detectable rate when JPEG2000 compression ratio is 5%, random cutting ratio is 5%, [3, 3] median filter, Gaussian ($\mu = 0$, $\sigma^2 = 0.003$) and 'salt and pepper' ($d = 0.15$). The average of detectable rate is 91.288%.

Comparison of algorithms: Compared with DCT-LSB and DWT-LSB, CL-CBP has advantage in invisibility and robustness. Experiment results are as follows:

According to PSNR, CL-CBP has advantages in invisibility by comparing with DCT-LSB and DWT-LSB. Table 2 shows that invisibility increases by 28.01% averagely when embedding rate is 25%.

Figure 12, 13 and Table 3 show robustness comparison results when the embedding rate is 25% based on Robustness test algorithm.

The experiment results show that robustness test value of CL-CBP increase by 40.25% compared with DCT-LSB and DWT-LSB in under attacks of JPEG2000 compression.

Table 1: Detectable rate of attacks

Image processing	JPEG2000 Compression (%)	Cutting (%)	Filtering (%)	Gaussian (%)	'Salt and Pepper' (%)
Detectable rate of attacks	93.47	84.32	90.23	93.20	95.22

Table 2: Invisibility comparison based on PSNR

Hiding algorithm	CL-CBP	DCT-LSB	DWT-LSB
PSNR	34.9482	25.4785	29.1246

Table 3: Robustness test values comparison of filtering and noise

	Information hiding algorithm		
Attacks	CL-CBP	DCT-LSB	DWT-LSB
[3,3] median filter	59.68	51.21	66.24
[3,3] wiener2 filter	54.24	44.26	56.32
Gaussian	70.24	60.27	65.22
'salt and pepper' d = 0.15	37.64	43.21	30.14

The experiment results show that robustness test value of CL-CBP increase by 29.90% compared with DCT-LSB and DWT-LSB under attacks of random cutting.

Robustness test value of CL-CBP increase by 1.63%, 7.85, 11.95 and 2.63% averagely compared with DCT-LSB and DWT-LSB in under attacks such as [3,3] median filter, [3,3] wiener 2 filter, Gaussian and 'salt and pepper' noise. To sum up, the results indicate that CL-CBP is advantageous in robustness.Perception of tampering is the peculiar characteristic in CL-CBP. The current algorithms don't have this characteristic.

ACKNOWLEDGMENTS

Our research was funded by many Projects and the names and numbers of these Projects are as follows: 1. Basic Research Project of Shaanxi Province Natural Science Foundation (Grant No. 2013JM8018). 2. The National Natural Science Foundation of China (Grant No. 61303041). 3. The Special Fund for Basic Scientific Research of Central Colleges of Chang'an University (Grant No. 2013G1241118 and 2013G2241020). 4. Xi'an Science and Technology Project (Grant No. CXY1318). 5. Jilin Province Association for International Exchange of Personnel Project (Grant No. 2012-7-102-2). 6. National IOT Project Major Demonstration Projects (Grant No. 2012-364-208-205 and 2012-364-812-105). 7. The State 863 Project (Grant No. 2012AA112312). 8. The Ministry of Transport of the People's Republic of China Project (Grant No. 2012-364-208-600, 2012-364-208-200 and 201231849A70). 9. The Fund from Xi'an Red Sun Company (Grant No. XARESUN2013090101).

CONCLUSION

Propose an information hiding scheme based on CL-CBP. Use energy distribution features of CL

Multi-wavelet Transform sub-images which are approximately 284:7:2:1 and bit plane theory to embed hiding information. Simulation results show that due to the combination CL multi-wavelet with bit plane and induction of chaotic map, genetic algorithm, Knight-tour and RAID4, this scheme satisfies information hiding and also meets the basic security needs of secret information transmission for communication system. Furthermore, CL-CBP is applicable to color images.

The future work is focus on alternating selection of bit plane, choosing embedded module and robustness parameters in LL_2 in order to improve invisibility, robustness and tampering perception. Especially research on applications in information hiding based on the theory of Image Multiscale Geometric Analysis (Jiao *et al*., 2008).

REFERENCES

Abdulfetah, A.A., X. Sun, H. Yang and N. Mohammad, 2010. Robust adaptive image watermarking using visual models in DWT and DCT domain. Inf. Technol. J., 9: 460-466.

Abed, F.S. and N.A. Mustafa, 2010. A proposed technique for information hiding based on DCT. Int. J. Adv. Comput. Technol., 2: 140-152.

Chen, Y.H. and X.Y. Huang, 2004. Digital image hiding technology based on chaos map and image blending. Acta Simulata Systematica Sinica, 16: 1648-1651.

Chui, C.K. and J.A. Lian, 1996. A study of orthonormal multi-wavelets. Applied Numer. Math., 20: 273-298.

Ghouti, L., A. Bouridane, M.K. Ibrahim and S. Boussakta, 2006. Digital image watermarking using balanced multiwavelets. IEEE Trans. Signal Process., 54: 1519-1536.

Jiao, L.C., B. Hou, S. Wang and F. Liu, 2008. Image Multiscale Geometric Analysis: Theory and Applications beyond Wavelets. Xidian University Press, China.

Jun, H.Z. and Z.M. Ma, 2001. Statistical analysis of multi-wavelet image transform. J. Image Graph., 6: 1198-1203.

Kunisawat, P., K. Attakitmongcol and A. Srikaew, 2008. Digital audio watermarking for copyright protection based on multiwavelet transform. Proceedings of the 1st European Conference on Intelligence and Security Informatics, December 3-5, 2008, Esbjerg, Denmark, pp: 155-164.

Lamgunde, A. and A. Kale, 2011. Palette based technique for image steganography. Proceedings of the International Conference on Advances in Computing, Communication and Control, January 28-29, 2011, Mumbai, India, pp: 364-371.

Liu, N.S., G.H. Yang, D.H. Guo and L.L. Cheng, 2008. A new wavelet watermark scheme of color image based on chaotic sequences. Proceedings of the International Conference on Intelligent Information Hiding and Multimedia Signal Processing, August 15-17, 2008, Harbin, China, pp: 994-998.

Paris, L., 2004. Heuristic strategies for the knight tour problem. Proceedings of the International Conference on Artificial Intelligence and Machine Learning: Models, Technologies and Applications, June 21-24, 2004, Las Vegas, USA., pp: 1121-1125.

Run, R.S., S.J. Horng, J.L. Lai, T.W. Kao and R.J. Chen, 2012. An improved SVD-based watermarking technique for copyright protection. Expert Syst. Appl., 39: 673-689.