HCTL Open International Journal of Technology Innovations and Research (IJTIR)
http://ijtir.hctl.org
Volume 17, September 2015
e-ISSN: 2321-1814, ISBN (Print): 978-1-94416-926-8

Secure Digital Image Watermarking using DWT, SVD and Chaotic Encryption with Genetic Algorithm

Roshan Jahan[1], **Preetam Suman**[2]

roshan@iul.ac.in, preetam.suman@ieee.org

Abstract

Watermarking is very useful to secure multimedia and personal data. The protection of watermark image is an issue these days. There are various threats occurs which can change watermark image. This paper is proposing a security mechanism for watermark image using DWT-SVD and optimized chaotic based image encryption through genetic algorithm with high level of robustness and security. The proposed mechanism is implemented on MATLAB, and tested in presence of various attacks. The algorithm is very efficient with respect to other security mechanism. The results are discussed in the paper.

Keywords: Watermarking, Gaussian noise, salt and pepper noise, DWT.

Introduction

Digital multimedia data are not safer these days because possibility of duplication or manipulation of the data [1]. Reliable transmission of digital data needs a technique to preserve and secure the data. [2].

There are few approaches designed for protecting data and securing systems. One of them is data encryption (cryptography) [3]. The key distribution is one of the approaches. Encrypted data can be decrypt only using the key. But distribution of key is not secure [4]. The other technique is steganography. It was derived from Greek, literally means “covered writing” is the art of hiding information inside other data in ways that prevent the detection of hidden message. Watermarking is other reliable technique for security of digital data [5, 6]. It is a hidden method to protect digital data. There are various applications of watermarking like copyright protection, fingerprinting, copy protection, broadcast monitoring, data authentication, indexing, medical safety, and data hiding.

[1, 2] Assistant Professor, CSE Department, Integral University, Kursi Road, Lucknow, UP, India

There are various literatures available on security of watermark images. It provides right direction to perform research on various techniques.

Qing Liu et. al. [7] proposed a method to reduce effect of attack on watermark image. This method was based on superimposing digital watermarking principle and wavelet multi-resolution analysis, adaptive blind grayscale image watermarking algorithm. Author has implemented the method and tested it. The result shows that the proposed algorithm is able to defend the attacks on watermark images.

Chaofan Peng et. al. [8] described the preliminary study and exploration of dynamic watermarking scheme on the basis of software watermarking technology and analysis the process of dynamic graph watermarking. Author also proposed the IPPCT dynamic watermarking scheme based on Chinese remainder theorem. In the research paper author has described the stages of watermarking embedding, decomposition, encryption and identification. The experimental results show that the new scheme was efficient in protection of watermark image.

Moniruzzaman et. al. [9] proposed a technique to protect patient information in medical images. The technique was based on discrete wavelet transform (DWT) domain and chaotic system based medical image watermarking scheme. Author has also compared experimental results of the proposed method with existing algorithms. The proposed method was better than existing algorithms.

Umaamaheshvari et. al. [10] proposed a mechanism to improve the embedding phase based on convolution code to improve the robustness of the embedded watermark. The proposed watermarking technique is preferred in low frequency band of the Discrete Wavelet Transform (DWT) and as a result it can refuse to accept the destruction of image processing. The parameters for evaluation of proposed algorithm were PSNR, MSE, SSIM, Correlation, and Entropy. Experimental results show that this proposed watermarking technique is more robust than the existing method.

Dhole et. al. [11] introduced a modified fragile watermarking technique for image recovery to detect and recover the tampered image with its tampered region. The author has focused on provide resistance on various attacks like birthday attack, college attack and quantization attacks. In this modified technique author put a watermark information and information of recovery of image block into the image block. These blocks are linked with next randomly generated block of image. The results show that, the proposed technique can be used as an alternative approach to image recovery.

Moniruzzaman et. al. [12] has proposed a scheme based on fragile watermarking scheme based on chaotic system. Two dimensional Arnold's cat map has been used to improve the security of the proposed watermarking scheme. Arnold's cat map is used to obtain the scrambled image by shuffling the pixel positions of the image. From the experimental results it can be observed that the proposed watermarking scheme gives better results than other chaos based watermarking schemes.

Organization of paper: section II describes attacks on images, proposed methodology is described in section III, section IV presents results and then conclusion is discussed in section V.

Attacks on Images

There are various types of attacks performed by attackers [13, 14]. Few of them are following:

1) Active attacks: In this attack intruder remove all security watermarks or change it according to him.
2) Passive attacks: In this attack attacker is not trying to remove the watermark but simply attempting to determine if a given mark is present or not.
3) Collusion attacks: In this type of attacks, the goal of the hacker is to remove the watermark, using several copies of the same data, containing each different watermark, each signed with a key, to construct a new copy without any watermark
4) Forgery attacks: In this attack the hacker tries to embed a new, valid watermark rather than removing it.
5) Ambiguity attacks: These are attacks that attempt to embed one or several additional watermarks such that it is unclear which the first authoritative watermark was.
6) Protocol attacks: Protocol attacks aim at attacking the entire concept of the watermarking application.
7) Gaussian Noise Attack: In this attack original image becomes blur image.
8) Salt and pepper attack: An image containing salt-and-pepper noise will have dark pixels in bright regions and bright pixels in dark regions.
9) Multiplicative Noise: Multiplicative noise refers to an unwanted random signal that gets multiplied into some relevant signal during capture, transmission, or other processing.

Methodology

Discrete Wavelet Transform (DWT) is a multiresolution analytical approach of time-frequency and can describe partial characteristics of time and frequency domains. The basic thought is to decompose the image to sub images with different space and frequency, then the coefficient is processed.

The DWT can be implemented as a multistage transformation. An image is decomposed into four sub-bands denoted as LL, LH, HL, and HH in DWT domain, where LH, HL, and HH represent the finest scale wavelet coefficients and LL stands for the coarse-level coefficients.

Proposed model for watermark embedding:

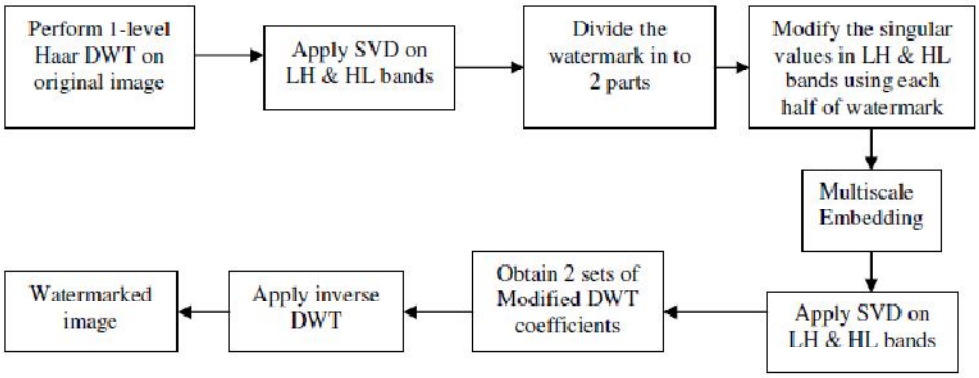

Figure 1: block diagram of proposed model for watermark embedding

Step 1: The first step of the model is to perform one-level Haar Discrete Wavelet Transform which is used to divide the cover image I into four non-overlapping multi-resolution sub-bands (i.e., LL, LH, HL, and HH).

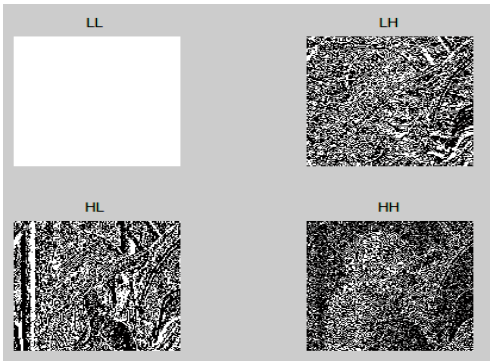

Figure 2: Input image and one level Haar DWT

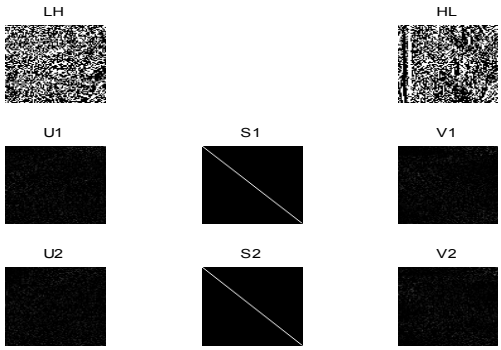

Figure 3: Result of step 2

Step 2: Now Perform Singular Value Decomposition to LH and HL subbands, i.e.,

$$In = Un\ Sn\ VnT, n = 1, 2 \quad (1)$$

Where, n represents sub-bands.

Step 3: Decompose the watermark image into two parts: W = W1 +W2,

Where, Wn denotes half of the watermark.

HCTL Open International Journal of Technology Innovations and Research (IJTIR)
http://ijtir.hctl.org
Volume 17, September 2015
e-ISSN: 2321-1814, ISBN (Print): 978-1-94416-926-8

Figure 4: decomposition of watermark image

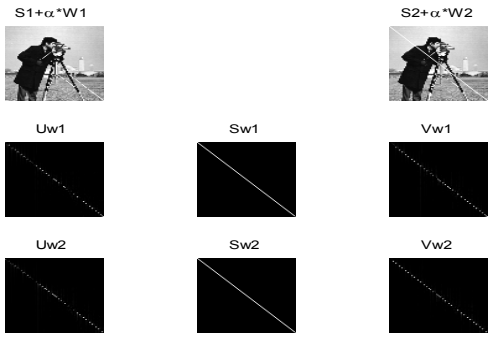

Figure 5: Result of step 4 on watermark images

Step 4: Modify the singular values in HL and LH subbands with half of the watermark image and then apply SVD to them,respectively, i.e.,

$$Sn + \alpha * Wn = Unw\ SnW\ \ VnTW \qquad (2)$$

Where, α denotes the scale factor. The scale factor is used to control the strength of the watermark to be inserted.

Step 5: Apply the given method to obtain the two sets of modified DWT coefficients, i.e.,

$$I*n = Un\ SnW\ VnT,\ \ n= 1, 2 \qquad (3)$$

Step 6: Now by performing the inverse DWT, obtain the watermarked image IW using two sets of modified DWT (i.e LH & HL) coefficients and two sets of unmodified DWT(LL & HH) coefficients.

Figure 6: DWT coefficients

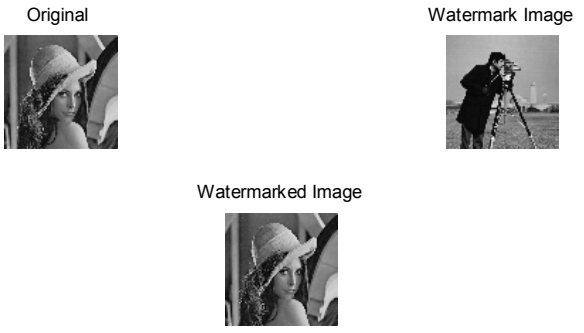

Figure 7: Result of inverse DWT

Proposed Model for Watermark Extraction:

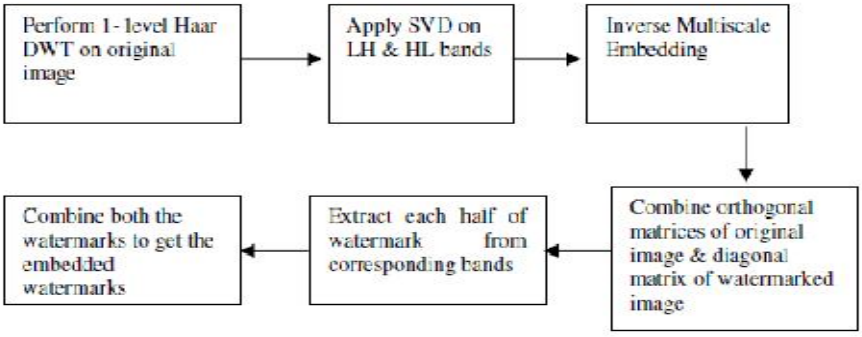

Figure 8: Block diagram of proposed model for watermark extraction

Step 1: Perform one-level Haar DWT to divide the watermarked (possibly distorted) image I□W into four sub bands (i.e. LL, LH, HL, and HH.)

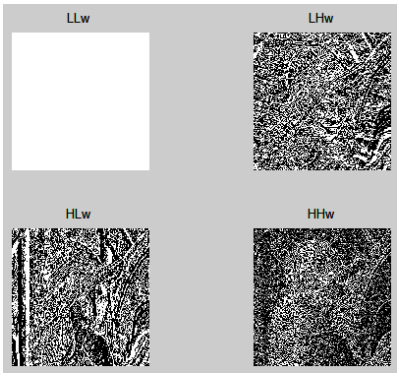

Figure 9: One level Haar output of image

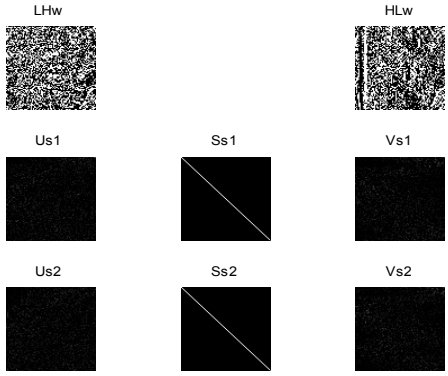

Figure 10: Singular Value Decomposition to LH and HL sub bands

Step 2: Perform Singular Value Decomposition to LH and HL sub bands, i.e.,

$$I^*nW = U^*n\ S^*nW\ V^*nT, \qquad n= 1, 2 \quad (4)$$

Where, n represents one of two sub-bands.

Step 3: Compute E*n = UnW S*nW V nTW , n = 1, 2

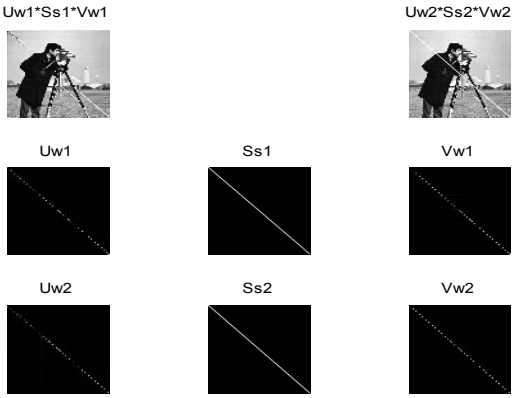

Figure 11: Result of step 3 on watermark image

Figure 12: Extraction of half watermark image

Step 4: Now Extract half of the watermark image from each sub-band, i.e.,

$$W^*n = (E^*n - Sn)/\alpha, \quad n = 1, 2 \qquad (5)$$

Step 5: Combine the results of Step 4 to obtain the embedded watermark:

$$W = W1 + W2$$

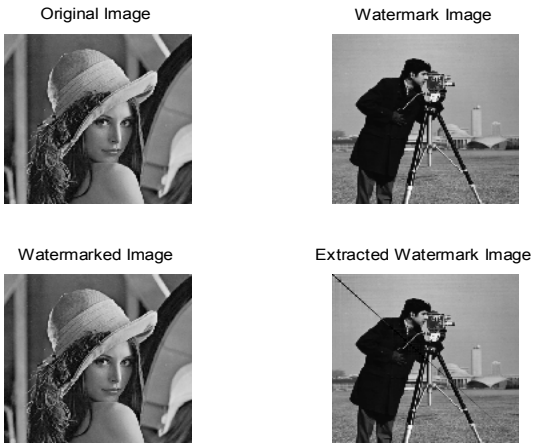

Figure 13: Final result of watermark image

Proposed model for secure watermark: The proposed model for secured watermark is the combined approach of image watermarking which have been used that satisfies two requirements i.e. imperceptibility and robustness.

The watermarking method consists of combination of discrete wavelet transform (DWT) and singular value decomposition.

The encryption method used for the watermark image is combination of a genetic algorithm and chaotic function. Every time an encrypted image with the highest entropy and the lowest correlation coefficient among adjacent pixels is produced.

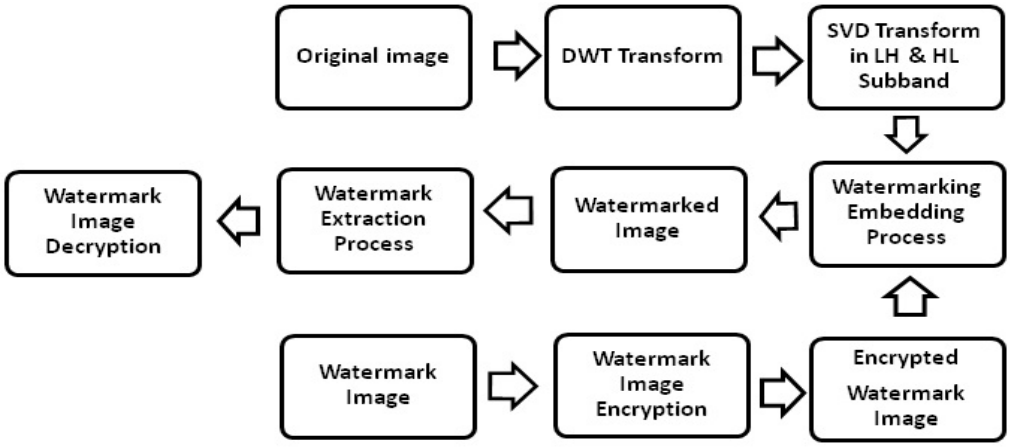

Figure 14: Proposed model for watermark image with security features

Results

Algorithm has been tested on standard image of Leena and Cameraman. In this paper image of 'Lena' was used as cover image and image of 'cameraman' was used as watermark image.

The following parameters were used for evaluation.

- Peak signal-to noise ratio (PSNR)
- Normalized Cross-Correlation (NC)
- Correlation coefficient (CC) and
- Histogram Deviation (HD)

The algorithm has been evaluated in presence of following attacks:

- Gaussian noise (GN)
- Salt & Pepper (SP)
- Multiplicative Noise(MN)

Figure 15 is showing images and effect of watermarking on original image.

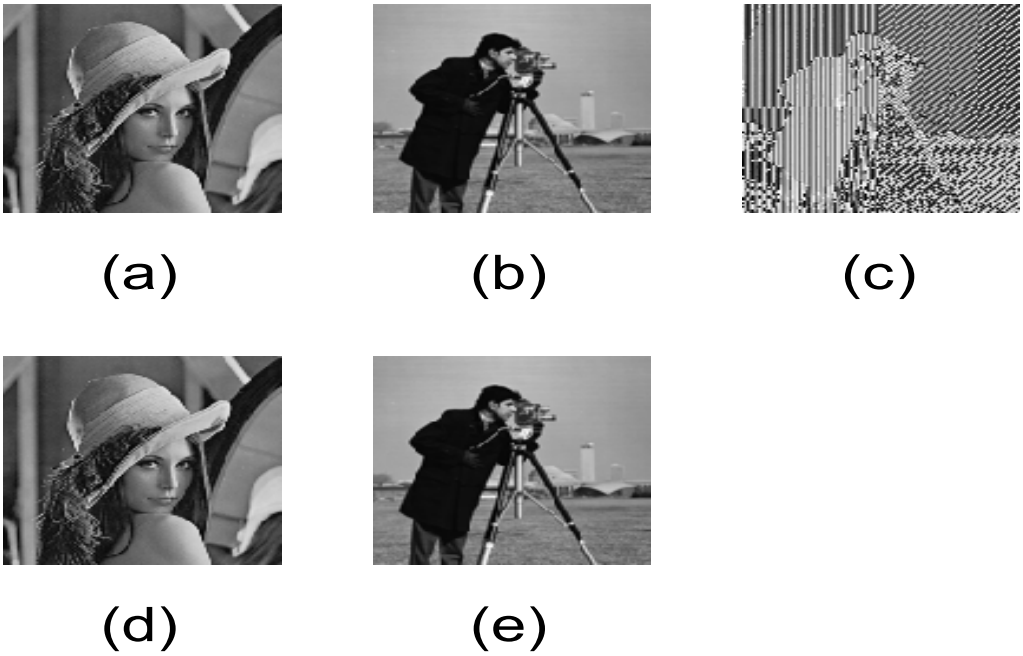

Figure 15: (a) Leena image (b) Photographer image as watermark, (c) Encrypted watermark image, (d) Watermarked image and (e) extracted and decrypted watermark image.

Results in absence of Attacks:

Without attack	
Parameter	Value
Psnr	39.3673
Psnr1	58.7429
NC	1
CRbest	-0.0741
HD	2.9999

Table 1: Results in absence of Attacks on Image

Results in presence of Attacks on Image

	Gaussian Noise Attack			Salt and pepper attack			Multiplicative Noise		
	G=0.001	G=0.01	G=0.1	S=0.005	S=0.05	S=0.1	Mn=0.004	Mn=0.04	Mn=0.1
Psnr	30.7182	30.6911	33.2083	50.0706	40.5358	32.6545	30.6702	29.4167	27.7171
Psnr1	33.3300	28.7810	27.6074	50.2596	39.9908	37.1599	34.3375	29.3894	28.5843
NC	0.8974	.8140	0.7928	0.9982	0.8110	0.8788	0.8147	0.8118	0.6159
Crbest	0.0682	0.0571	0.0566	0.0638	-0.0554	-0.0736	-0.0553	-0.0601	-0.0581

Table 2: Result of proposed mechanism in presence of noise

Conclusion

Security of multimedia data is very important. Watermarking is the one of the best method to provide security on images. A security mechanism for watermark image is discussed in this paper using DWT-SVD and optimized chaotic based image encryption through genetic algorithm with high level of robustness and security. The proposed mechanism was implemented on MATLAB, and tested in presence of various attacks. The mechanism is able to reduce effects of Gaussian noise (GN), Salt & Pepper (SP), and Multiplicative Noise (MN).

References:

1. Boopathy, D.; Sundaresan, M., "Data encryption framework model with watermark security for Data Storage in public cloud model," in *Computing for Sustainable Global Development (INDIACom), 2014 International Conference on* , vol., no., pp.903-907, 5-7 March 2014
2. Swanson, M.D.; Kobayashi, M.; Tewfik, A.H., "Multimedia data-embedding and watermarking technologies," in *Proceedings of the IEEE* , vol.86, no.6, pp.1064-1087, Jun 1998
3. Johannes Buchmann “Introduction to Cryptography” Springer Science & Business Media, 2004
4. Ingemar Cox, Matthew Miller, Jeffrey Bloom, Mathew Miller, “Digital Watermarking” Morgan Kaufmann, 2001.
5. Thangadurai, K.; Sudha Devi, G., "An analysis of LSB based image steganography techniques," in *Computer Communication and Informatics (ICCCI), 2014 International Conference on* , vol., no., pp.1-4, 3-5 Jan. 2014
6. Roshan Jahan, "Efficient and Secure Digital Image Watermarking Scheme using DWT-SVD and Optimized Genetic Algorithm based Chaotic Encryption" International Journal of Science, Engineering and Technology Research (IJSETR), Volume 2, Issue 10, 2013.
7. Qing Liu; Jun Ying, "Grayscale image digital watermarking technology based on wavelet analysis," in *Electrical & Electronics Engineering (EEESYM), 2012 IEEE Symposium on* , vol., no., pp.618-621, 24-27 June 2012

8. Chaofan Peng; Qinglei Zhou, "An IPPCT Dynamic Watermarking Scheme Based on Chinese Remainder Theorem," in Computational and Information Sciences (ICCIS), 2013 Fifth International Conference on , vol., no., pp.167-170, 21-23 June 2013.
9. Moniruzzaman, M.; Kayum Hawlader, M.A.; Hossain, M.F., "Wavelet based watermarking approach of hiding patient information in medical image for medical image authentication," in Computer and Information Technology (ICCIT), 2014 17th International Conference on , vol., no., pp.374-378, 22-23 Dec. 2014
10. Umaamaheshvari, A.; Thanushkodi, K., "Robust image watermarking based on block based error correction code," in Current Trends in Engineering and Technology (ICCTET), 2013 International Conference on , vol., no., pp.34-40, 3-3 July 2013
11. Dhole, V.S.; Patil, N.N., "Self Embedding Fragile Watermarking for Image Tampering Detection and Image Recovery Using Self Recovery Blocks," in Computing Communication Control and Automation (ICCUBEA), 2015 International Conference on , vol., no., pp.752-757, 26-27 Feb. 2015
12. Moniruzzaman, M.; Hawlader, M.A.K.; Hossain, M.F., "An image fragile watermarking scheme based on chaotic system for image tamper detection," in Informatics, Electronics & Vision (ICIEV), 2014 International Conference on , vol., no., pp.1-6, 23-24 May 2014
13. Ingemar J. Cox “Digital Watermarking and Steganography” Morgan Kaufmann Publishers, 2008.
14. Juergen Seitz “Digital Watermarking for Digital Media” Information Science Pub., 01-Jan-2005.
15. Manoj Prabhakar; Manoj Kumar, Impact of Image Processing in Saving the Human Life By Automating Traffic Signals, HCTL Open International Journal of Technology Innovations and Research, Volume 3, May 2013, Pages 42-57, ISSN: 2321-1814, ISBN: 978-1-62776-443-8.
16. Pooya Najafi; Vahid Ghods, Monitoring and Remote Sensing of the Street Lighting System using Computer Vision and Image Processing Techniques for the Purpose of Mechanized Blackouts (Development Phase), HCTL Open International Journal of Technology Innovations and Research, Volume 4, July 2013, Pages 24-35, ISSN: 2321-1814, ISBN: 978-1-62776-132-1.
17. Gaurav Mohan Singh, Mahipal Singh Kohli and Manoj Diwakar, A Review of Image Enhancement Techniques in Image Processing, HCTL Open International Journal of Technology Innovations and Research, Volume 5, Sept 2013, ISSN: 2321-1814, ISBN: 978-1-62840-986-4.
18. Shubhi Shrivastava, Towards Fast and Efficient Foreground Color Based Image Search Using Supervised Learning and Its Comparison with Unsupervised Learning, HCTL Open International Journal of Technology Innovations and Research, Volume 3, May 2013, Pages 108-118, ISSN: 2321-1814, ISBN: 978-1-62776-443-8.