International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 5 | ISSN : 2456-3307

A Wavelet Domain Secured Digital Image Watermarking Using SVD Technique

[1]Prachi Mishra, [2]Pankaj Sahu
[1]Research Scholar, [2]Assistant Professor
Communication Systems, Dept. of ECE, GGITS, Jabalpur, Madhya Pradesh, India

ABSTRACT

In this work, a new wavelet based secured image to image watermarking based on singular value decomposition scheme is presented. This method uses the time domain signal & process it in frequency domain, while time domain features of the carrier remains same, so visually no one can identify the hidden data into it. The algorithm is based on DWT is used for this purpose, since wavelet decomposition of images gives better resolution results than other transforms. It generates a watermark signal using DWT & embeds it into the signal by measuring the subband threshold using DWT. The watermarks are embedded into non-overlapping DWT coefficients of the host signal which are randomly selected & very hard to detect even with the blind detection. The image watermarking is relatively new & has wide scope for research Proposed algorithm is based on DWT domain while considering the more active components of the signal. Comparison shows the PSNR is 51.95 dB & MSE is 0.78, also SSIM is 0.94 which is very good.

Keywords : Image watermarking, DWT, Security, Sub-band Coding, PSNR, MSE, SSIM.

I. INTRODUCTION

In modern world each and every form of information, like text, images, audio or video, has been digitized. [14] Widespread networks and internet has made it easier and far more convenient to store and access this data over large distances. Although advantageous, this property threatens the copyright protection purpose [14].

Media and information in digital form is easier to copy and modify, and distribute with the aid of widespread internet. Every year thousands of sound tracks are released and within a few days are readily available on the internet for download. Without any information on the track itself, it's easy for someone to make profit out of them by modifying the original and selling under a different name. As a measure against such practices and other intellectual property rights, digital watermarking techniques can be used as a proof of the authenticity of the data.

Digital Watermarking is the process of embedding or inserting a digital signal or pattern in the original data, which can be later used to identify the author's work, to authenticate the content and to trace illegal copies of the work [12].

II. DISCRETE WAVELET TRANSFORM (DWT)

The wavelet transform decomposes the image in four channels (LL, HL, LH and HH) with the same bandwidth thus creating a multi-resolution perspective. The advantage of wavelet transforms is to allow for dual analyses taking into account both frequency and spatial domains.

Wavelets are being widely studied due to their application in image compression, owing to which compression resistant watermarks may be achieved through their use. Another interesting feature of the DWT is the possibility to select among different types of filter banks, tuning for the desired bandwidth. The most commonly used filters are: Haar, Daubechies, Coiflets, Biorthogonal, Gaussian.

When the DWT is applied to an image, the resolution is reduced by a 2^K, where K is the number of times the transform was applied.

These algorithms are called the "Wavelet based Watermarking". The watermark is inserted by substituting the coefficients of the cover image for the watermark's data. This process improves mark robustness, but depends on the frequency. The low frequency (LL) channel houses image contents in which a coefficients change, however small, will damage the cover image, which in turn challenges the fidelity propriety [2]. However, when this region of the spectrum is watermarked, a robust mark against compressions like JPEG and JPEG2000 is attained. Furthermore, when the middle and high frequency channels are marked, some benefits against noise interference and several types of filtering show up. Therefore, these algorithms tend to be adapted for human visual system (HSV) to avoid small modification in the cover image being perceptible.

III. LITERATURE REVIEW

Copyright protection has now become a challenging domain in real life scenario. Digital watermarking scheme is an important tool for copyright protection technique. A good quality watermarking scheme should have high perceptual transparency, and should also be robust enough against possible attacks. A well-known (Lewis-Barni) Human Visual System (HVS) based watermarking model is fairly successful with respect to the first mentioned criterion, though its effectiveness in color images has not been claimed. Furthermore, it is true that although several watermarking schemes are available in literature for grayscale images, relatively few works have been done in color image watermarking, and the little that have been done, have mostly been tested in RGB, YUV, YIQ color spaces. Thus the question remains that, which is the optimal color space for color image watermarking and whether this HVS model is applicable for that color space. There are two main contributions of the present work with respect to the above. First, it claims that for color image watermarking, the YCbCr space can be used as the perceptually optimum color space, the Cb component being the optimal color channel here. Second, it also tests the effectiveness of the above-mentioned HVS model in that color space. These have been achieved by using the HVS model to propose a new non-blind (original image and the watermark logo image both are needed for extraction) image adaptive Discrete Wavelet transform and Singular Value Decomposition (DWT-SVD) based color image watermarking scheme in YCbCr color space. The multi-resolution property of DWT and stability of SVD additionally makes the scheme robust against attacks, while the Arnold scrambling, of the watermark, enhances the security of this method [1].

In spatial domain, watermarking is done in pixel domain. The main strengths of pixel domain methods are that they are conceptually simple and have very low computational complexities. Spatial domain technique is less time consuming as compare to wavelet or frequency domain. Embedding of the watermark into cover image is based on the operations like shifting or replacing of the bits. Most commonly used spatial domain watermarking technique is Least Significant Bit technique. In this technique, pixel values of cover image as well as watermark image are converted into binary form. The bits of cover image pixels are replaced by the bits of the watermark image pixels. Then the bits of watermark image replace the least significant bit of cover image and in this way, watermark can be embedded into cover image [2].

Watermarking using DCT is a very popular transform function used in signal processing. It transforms a signal from spatial domain to frequency domain. DCT is used to convert data into the summation of a series of cosine waves oscillating at different frequencies. Due to good performance, it has been used in JPEG standard for image compression. DCT has been applied in many fields such as data compression, pattern recognition, and image processing [2].

IV. PERFORMANCE EVALUATION OF WATERMARKING METHODS

Several Functions are used for quality assessment of the digital watermarking algorithms, examining tests on the resulted watermarked image.

MSE: Mean Squared Error (MSE) function is defined as:

$$MSE = \frac{1}{n}\sum_{i=1}^{n}\left(X_i - X_i^*\right)^2$$

PSNR: Peek Signal to Noise Ratio (PSNR) is defined as for SNR of an image:

$$PSNR = 10.\log_{10}\left(\frac{MAX_I^2}{MSE}\right)$$

SSIM: The Structural Similarity (SSIM) is a function defined as equation given below:

$$SSIM = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)}$$

Where: "μ", "σ", & "σxy" are mean, variance, and covariance of the images, and "c1, c2" are the stabilizing constants.

Robustness: Basically this term is related to the security and immunity to the attacks.

Noise: Gaussian, Poisson, Salt & Pepper, and Speckle etc. Also in extraction process the image from host has loss of some components which appears as noise.

V. PROPOSED METHODOLOGY

In this proposed work input image (original signal) is embedded into host image signal. We define this proposed algorithm as image to image wavelet based transform domain sub-band masking. In this proposed blind frequency masking algorithm entire unwatermarked signal isn't needed at the detector. Instead, a password is required (Co) usually a data reducing function, is used at the watermark detector to nullify "noise" effects included to the signal in the embedder. In a blind watermark detection, the un-watermarked signal is unknown, & cannot be removed before a watermark extraction. In this process the inserted watermark could be contaminated by the combination of impacts of the cover work & the noise signal. The received watermarked signal is now viewed as a corrupted type of the inserted pattern & the entire watermarked detector is viewed as the channel decoder.

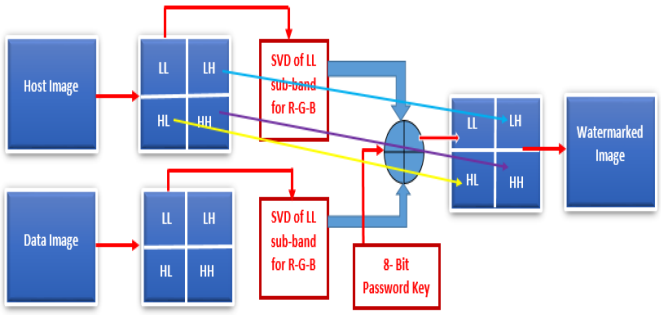

Figure 1: Proposed Watermarking System

5.1 Proposed Watermark Embedding Algorithm

- ✓ First take image i.e. information signal.
- ✓ Convert it in to frequency domain by taking its wavelet transform (DWT).
- ✓ Result in transformed/decomposed image.
- ✓ Similarly find transformed of host image i.e. carrier signal with any one of the wavelet filters.
- ✓ The image is decomposed by filter-banks into LL, LH, HL & HH sub-bands.
- ✓ Then LL sub-bands of both the images are gone through SVD for Red, Green & Blue components.
- ✓ Form embedded signal by adding transformed information after SVD of both LL sub-bands & taking LH, HL & HH same of the carrier signal i.e. selected watermarked sub –band(s).
- ✓ The take inverse wavelet transform (IDWT) i.e. convert it into time domain.
- ✓ Obtain watermarked image.
- ✓ Calculate performance parameters for watermarked & extracted images.

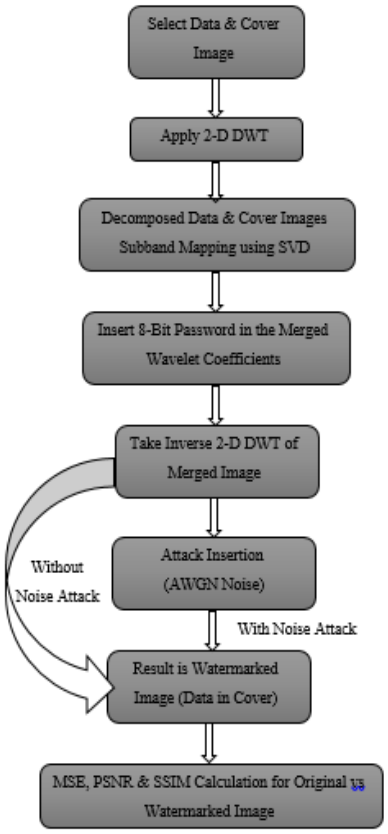

Figure 2 : Proposed Watermarking Embedding System

5.2 Proposed Watermark Extraction Algorithm

- ✓ First take watermarked image.
- ✓ Insert secret password key.
- ✓ Convert it in to frequency domain by taking its wavelet transform.
- ✓ Result in transformed/decomposed watermarked image.

- ✓ Removal of password from wavelet coefficients.
- ✓ Take transformed carrier signal.
- ✓ Extract image from watermarked image using owner's key & reverse decomposition from selected sub-band(s).
- ✓ The take inverse wavelet transform (IDWT) i.e. convert it into time domain.
- ✓ Obtain original image i.e. information signal.

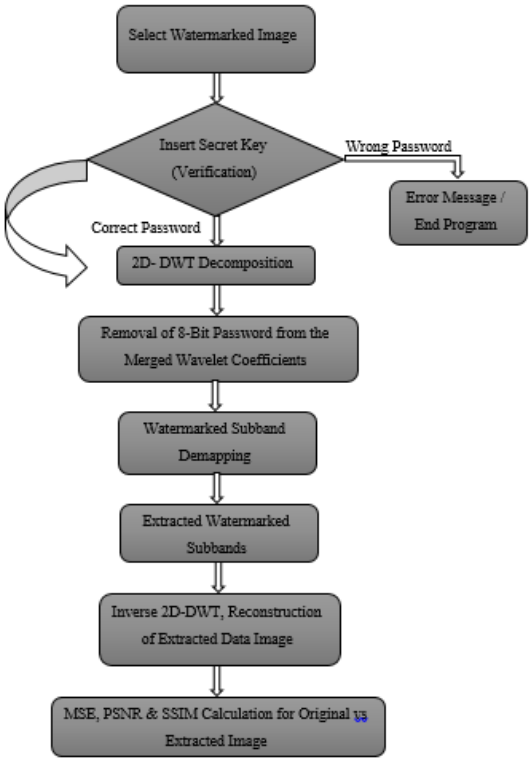

Figure 3 : Proposed Watermarking Extraction System

VI. SIMULATION RESULTS & DISCUSSIONS

6.1 Host / Cover Image for Embedding

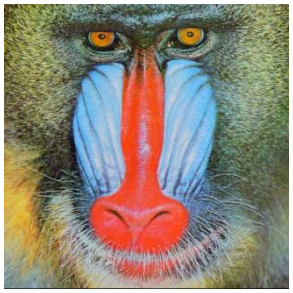

Figure 4 : Original Host (Cover) Image

6.2 Watermark Image to be Hidden

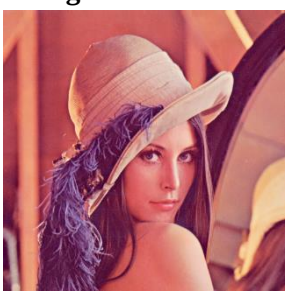

Figure 5: Original Watermark Image to be hidden

6.3 Watermarked image

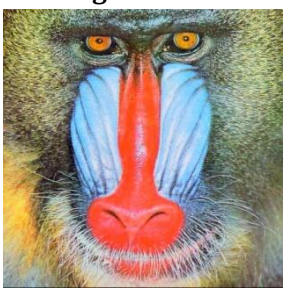

Figure 6: Watermarked Image after Embedding

6.4 Detected Image After Watermark Extraction

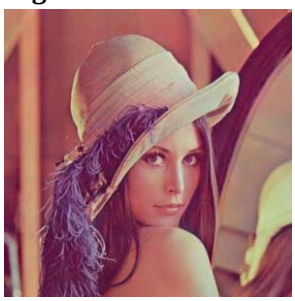

Figure 7: Extracted Watermark from Watermarked Image

The evaluation parameters & simulation results of images are given below.

Figure 8: SSIM between Host & Watermarked Image (0.9813)

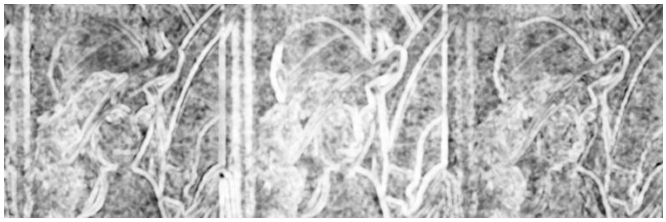

Figure 9: SSIM between Original & Extracted Watermark Image (0.9476)

6.5 Simulation Results Summary

In table 1 various parameters obtained after simulation between Host & Watermarked (after embedding) image are mentioned. After embedding we have corrupted the watermarked image with noise. The values of MSE & PSNR shown are for AWGN noise of different values in dB.

Parameters	Noise = 0 dB	Noise = 5 dB	Noise=10 dB	Noise=15 dB	Noise=20 dB
MSE	0.20	0.30	1.46	7.26	18.82
PSNR	57.54 dB	55.56 dB	47.67 dB	40.04 dB	35.63 dB
SSIM	0.9813	0.9765	0.9605	0.9345	0.9018
NCC	1.00	1.00	1.00	1.00	0.9994

Table 1: Host vs Watermarked Image Results

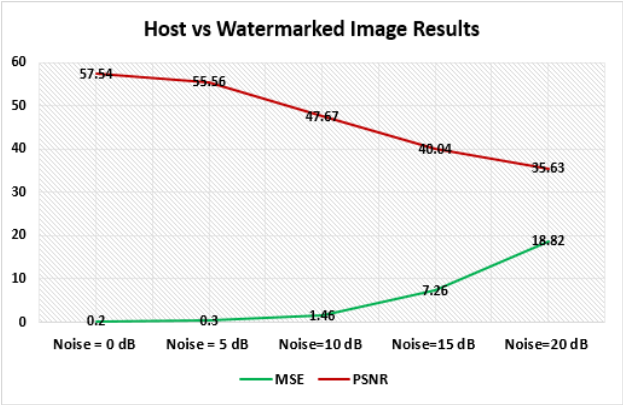

Figure 10 : Graph of PSNR & MSE for Host Vs Watermarked Image Results

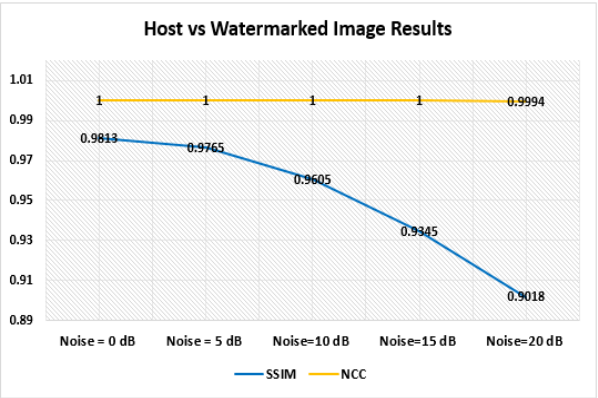

Figure 11 : Graph of PSNR & MSE for Host Vs Watermarked Image Results

Parameters	Noise = 0 dB	Noise = 5 dB	Noise=10 dB	Noise=15 dB	Noise=20 dB
MSE	84.28	84.33	93.16	112.07	127.99
PSNR	31.62 dB	31.55 dB	30.95 dB	29.40 dB	28.10 dB
SSIM	0.9476	0.9474	0.9368	0.8782	0.7541
NCC	1.00	1.00	0.9992	0.9984	0.9938

Table 2 : Original Watermark Vs Extracted Watermark

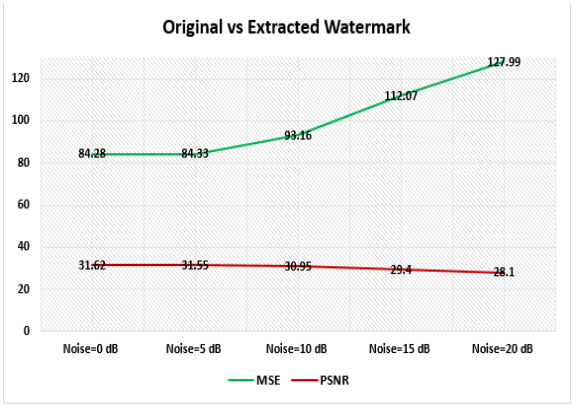

Figure 12 : PSNR & MSE Results for Original Vs Extracted Watermark

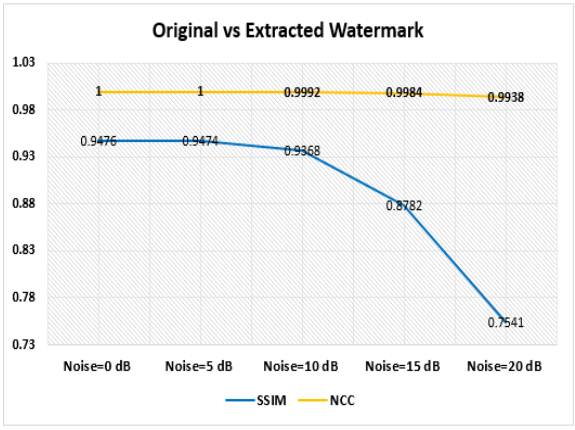

Figure 13 : SSIM & NCC Results for Original Vs Extracted Watermark

6.6 Results Comparison

In the [5] SSIM values for JPEG/ JPEG2000, in the presence of gaussian noise between original & extracted watermark is given. Comparison of SSIM with our proposed technique is shown in table 3.

SSIM	Noise = 0 dB	Noise = 5 dB	Noise=10 dB	Noise=15 dB	Noise=20 dB
Proposed Work	0.98	0.97	0.96	0.93	0.90
Base Paper [5]	0.80	0.60	0.45	0.25	0.20

Table 3 : SSIM Result Comparison for Watermark Vs Extracted Watermark

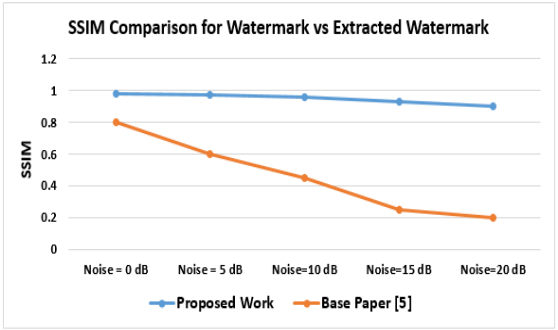

Figure 14 : Result Comparison for Watermark Vs Extracted Watermark

In table 4 comparison of PSNR for different techniques [2] is given for gaussian noise of 5 dB, with our proposed technique. From the table it can be summarized that the proposed algorithm out-performs in all the available techniques.

PSNR	LSB in 8th bit [2]	DCT [2]	DWT [2]	This Work
Gaussian Noise = 5 dB	46.3670 dB	46.2582 dB	44.0002 dB	55.56 dB

Table 4 : PSNR Comparison for Host Vs Watermarked Image Results

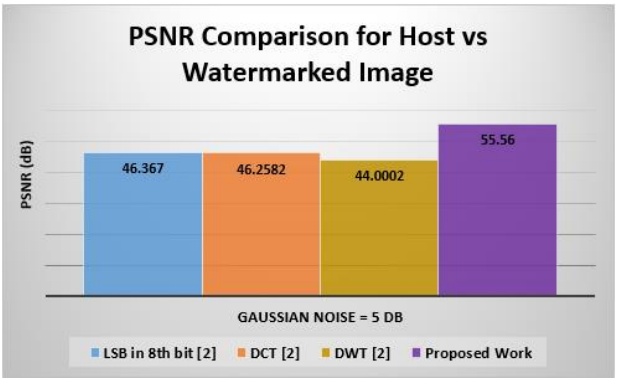

Figure 15 : Graph for PSNR Comparison for Host Vs Watermarked Image Results

In table 5 comparison of PSNR for mandrill image with a grey scale watermark object [1] is given without any attack, with our proposed technique with a color watermark object. From the table it can be summarized that the proposed algorithm out-performs technique mentioned in [1], even with color watermark object.

Watermarked image	YCbCr Watermarking [1]	This Work
Mandrill	51.9541 dB	55.56 dB

Table 5 : PSNR Comparison of Watermarked Image Results with [1]

VII. CONCLUSION

In this work, a new wavelet based secured image to image watermarking based on singular value decomposition scheme is presented. This method uses the time domain signal & process it in frequency domain, while time domain features of the carrier remains same, so visually no one can identify the hidden data into it. The algorithm is based on DWT is used for this purpose, since wavelet decomposition of images gives better resolution results than other transforms. It generates a watermark signal using DWT & embeds it into the signal by measuring the subband threshold using DWT. The watermarks are embedded into non-overlapping DWT coefficients of the host signal which are randomly selected & very hard to detect even with the blind detection. The image watermarking is relatively new & has wide scope for research Proposed algorithm is based on DWT domain while considering the more active components of the signal. Comparison shows the PSNR is 51.95 dB & MSE is 0.78, also SSIM is 0.94 which is very good.

VIII. REFERENCES

[1]. Aniket Roy et-al, "A perception based color image adaptive watermarking scheme in YCbCr space", 2nd IEEE International Conference on Signal Processing and Integrated Networks (SPIN), Pp- 537 - 543, Noida, 2015.

[2]. Neha Bansal et-al, "Comparative Analysis of LSB, DCT and DWT for Digital Watermarking", 2nd IEEE International Conference on Computing for Sustainable Global Development (INDIACom), Pp. 40 - 45, New Delhi, 2015.

[3]. Sudip Ghosh et-al, "A New Algorithm on Wavelet Based Robust Invisible Digital Image Watermarking for Multimedia Security", IEEE International Conference on Electronic Design, Computer Networks & Automated Verification (EDCAV), Pp- 72 - 77, Shillong, 2015.

[4]. S. Abolfazl Hosseini et-al, "A New Method for Color Image Watermarking Based on Combination of DCT and PCA", IEEE International Conference on Communications, Signal Processing, and their Applications (ICCSPA), Pp. 1-5, Sharjah, 2015.

[5]. Sha Wang et-al, "Adaptive Watermarking and Tree Structure Based Image Quality Estimation", IEEE Transactions on Multimedia, Volume 16, Number 2, February 2014.

[6]. Dhananjay Yadav et-al, "Reversible Data Hiding Techniques", International Journal of Electronics and Computer Science Engineering (IJECSE), Volume 1, Number 2, 2013.

[7]. Md. Iqbal Hasan Sarker et-al, "FFT-Based Audio Watermarking Method with a Gray Image for Copyright Protection", International Journal of Advanced Science and Technology, Volume 47, October, 2012.

[8]. I.J. Cox, M. L. Miller, J. A. Bloom, J. Fridrich, and T. Kalker, Digital Watermarking and Steganography. Morgan Kaufmann, 2008.

[9]. M. El-Gayyar and J. von zur Gathen, "Watermarking techniques spatial domain," University of Bonn Germany, Tech. Rep., 2006.
[10]. J. Liu and X. He, "A review study on digital watermarking," First International Conference on Information and Communication Technologies, pp. 337-341, 2005.
[11]. M. Arnold, M. Schmucker, and S. D. Wolthusen, Techniques and Applications of Digital Watermark and Content Protection. Artech House, 2003.
[12]. X. Wu, J. Hu, Z. Gu, and J. Huang, "A secure semi-fragile watermarking for image authentication based on integer wavelet transform with parameters," Australasian Information Security Workshop, vol. 44, 2005.
[13]. M. Antonini, M. Barlaud, P. Mathieu, and I. Daubechies, "Image coding using wavelet transform," IEEE Transaction on Image Processing, vol. 1, pp. 205-220, 1992.
[14]. Daubechies and W. Sweldens, "Factoring wavelet transforms into lifting steps," SIAM Journal on Mathematical Analysis, 1997.
[15]. V. M. Potdar, S. Han, and E. Chang, "A survey of digital image watermarking techniques," 3rd IEEE International Conference on Industrial Informatics, pp. 709-716, 2005.
[16]. Tefas, A. Nikolaidis, N. Nikolaidis, V. Solachidis, S. Tsekeridou, and I. Pitas, "Performance analysis of watermarking schemes based on skewtent chaotic sequences," NSIP'01, 2001.
[17]. S.Teskeridou, V. Solochidis, N. Nikolaidis, A. Tefas, and I. Pitas, "Bernoulli shift generated chaoticwatermarks: Theoretic investigation," SCIA2001, 2001.
[18]. W. Yan, Z. Shi-qiang, and W. Yan-chun, "Wavelet digital watermark based on chaotic sequence," ICICIC'08, 2008.
[19]. K. L. W. G. Natasa Terzija, Markus Repges, "Digital image watermarking using discrete wavelet transform: Performance comparison of error correction codes," Visualization, Imaging and Image Processing, 2002.
[20]. L. Haiyan, Z. Xuefeng, and W. Ying, "Analysis of the performance of error correcting coding in audio watermarking," 3rd IEEE Conference on Industrial Electronics and Applications, pp. 843-848, 2008.
[21]. P. Cika, "Watermarking scheme based on discrete wavelet transform and error-correction codes," 16th International Conference on Systems, Signals and Image Processing, pp. 1-4, 2009.
[22]. Bastug and B. Sankur, "Improving the payload of watermarking channels via ldpc coding," Signal Processing Letters, vol. 11, pp. 90-92, 2004.
[23]. Nafornita, A. Isar, and M. Kovaci, "Increasing watermarking robustness using turbo codes," International Symposium on Intelligent Signal Processing, pp. 113-118, 2009.
[24]. N. Pantuwong and N. Chotikakamthorn, "Line watermark embedding method for affine transformed images," ISSPA 2007, pp. 1-4, 2007