iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 Issue: VI Month of publication: June 2015

DOI:

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

A Novel Semi-Blind Watermark Extraction Algorithm

Manoj Kumar. V. R.[1], C. Arun[2], S.Muthumanickam[3]
[1,2,3]*R.M.K.College of Engineering and Technology, Puduvoyal, Chennai, India.*

Abstract—in this paper, a novel algorithm for semi-blind watermark extraction is proposed. Though watermark embedding is done using a non-blind watermarking scheme, the detection method proposed extracts the watermark without the use of host image, i.e., semi-blind detection is done. A novel robust watermarking scheme using discrete wavelet transform (DWT) and singular value decomposition (SVD) for watermark embedding is also proposed. The levels of decomposition, the band in which SVD is performed and the color component used to embed the watermark, are all studied. Also, the effect of attacks on the robustness of the algorithm used is analyzed. Some of the attacks used are compression, resizing, cropping, histogram equalization, rotation, low pass filtering, high pass filtering, median filtering and various noise attacks such as Gaussian noise, salt and pepper noise and Poisson noise. The parameters used for the study are peak signal-to-noise ratio (PSNR) and correlation.
Keywords—2-level DWT, SVD in HH band, PSNR, Correlation, Robustness to attacks, Semi-blind detection.

I. INTRODUCTION

Currently, the primary concern in the cyberspace society is copyright protection, authentication of ownership of digital content and illegal copying. Digital watermarking served as the solution to the above problems and thus has drawn the interests of many research works. Watermarking can be done either in the spatial domain [1], [2] or in the frequency domains [3], [4]. The simplest watermarking in spatial domain is done by inserting the watermark image pixels in the least significant bits (LSB) of the host image. However, watermarking in spatial domain is not robust to most of common image processing attacks. Thus, watermarking in the frequency domain is preferred.

In watermarking, three broad detection schemes include: non-blind detection, semi-blind detection and blind detection. A non-blind scheme can use the original media, watermark sequence and secret key during extraction. However, a blind scheme can only use the secret key. In particular, a semi-blind scheme requires both the secret key and the watermark sequences [5], [6], [7], [8]. The classification of attacks in watermarking are: removal attack, geometric attack, cryptographic attack and protocol attack [9], [10]. Removal attack aims at complete removal of watermark data without breaking the security of the watermarking algorithm. Geometric attack is different in the sense that it intends to distort the watermark detector synchronization with the embedding information. Cryptographic attacks try to break the security of the watermarking schemes and thereby find a way to procedurally remove the embedded watermark or to embed misleading watermarks. Brute-force search method is one type of cryptographic attack that extensively attempts to identify the used watermark algorithm by using a large number of known possible measures. Protocol attack is a really different one that targets the actual concept of watermarking as a solution to copyright protection. For example, an attack that tries to attack the credibility of a watermark in claiming ownership. This paper is an extension of our previously published work on non-blind watermarking scheme [11], [12]. In this paper, we propose a completely novel method of watermark extraction which can be categorized as semi-blind detection scheme. Although we propose a non-blind watermark embedding algorithm that uses n-level discrete wavelet transform followed by performing SVD on the HH band, we extract the watermark in a semi-blind manner. Generally, it is suggested that watermarking is to be done to the blue component of the image in the papers [13], [14]. But in the proposed scheme the watermark is embedded in the green component of the RGB host image as it produces better PSNR values. Also, we do not use Fourier transform for watermarking, as the loss of time information in a signal by the transformation will lead to difficulty in processing [15]. The rest of the paper is organized as follows. Discrete wavelet transform is explained in section 2. Singular value decomposition is discussed in section 3. The proposed architecture for watermarking is presented in section 4. Experimental results are analyzed in section 5. Concluding remarks are given in section 6.

This work is a part of the funded project supported by the Indian Space Research Organization (ISRO) with approval number ISRO/RES/3/668/14-15

II. DISCRETE WAVELET TRANSFORM

The discrete wavelet transform is computed separately for different segments of the time-domain signal at different frequencies.

Multi-resolution analysis analyses the signal at different frequencies giving different resolutions. The multi-resolution successive approximation not only enhances the resolution of an image, but also enhances the resolution of watermark simultaneously. This is an advantage of the discrete wavelet transform. By using high energy watermarks in regions where the human visual system is known to be less sensitive, the robustness of the watermark to various attacks increases. The discrete wavelet transform converts an input series $X_0, X_1, \ldots X_m$, into one high-pass wavelet coefficient series and one low-pass wavelet coefficient series (of length n/2 each) given by:

$$Hi = \sum_{m=0}^{K-1} X2i - m.sm(z) \qquad (1)$$

$$Li = \sum_{m=0}^{K-1} X2i - m.tm(z) \qquad (2)$$

where sm (Z) and tm (Z) are called wavelet filters, K is the length of the filter, and i=0, ..., [n/2]-1. In practice, such transformation will be applied recursively on the low-pass series until the desired number of iterations is reached. When one-level 2-dimensional DWT is applied to an image, four transform coefficient sets are created. The four sets are LL, LH, HL and HH, where the first letter corresponds to applying either a low pass or high pass frequency operation to the rows and the second letter refers to the filter applied to the columns. The DWT decomposition of an image is shown in the following figure.

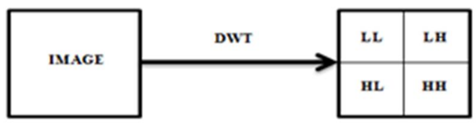


Fig. 1 DWT Decomposition of an image

That is, DWT divides the original image into an approximate image (LL) and three detail images LH, HL and HH. The approximate image holds most of the image data, while others contain details such as the edge and textures. The re-construction of the image is achieved by the inverse discrete wavelet transform (IDWT). Image watermarking algorithms using DWT [16], [17] are available in the literature. In this paper, we decompose the image up to two levels using DWT. The reason for the same is explained under the section of simulation results.

III. SINGULAR VALUE DECOMPOSITION

Let A be a general real (complex) matrix of order MxN. The singular value decomposition (SVD) of A is the factorization,

$$\begin{pmatrix} \\ \mathbf{A} \\ \\ \end{pmatrix} = \begin{pmatrix} \\ \mathbf{U} \\ \\ \end{pmatrix} \begin{pmatrix} s_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & s_n \end{pmatrix} \begin{pmatrix} \\ \mathbf{V} \\ \\ \end{pmatrix}^T \qquad (3)$$

where U and V are orthogonal(unitary) and S=diagonal($\lambda 1, \lambda 2, \ldots \lambda r$), where $\lambda i, I = 1{:}r$ are the singular values of matrix A with r=min(m,n) and satisfying

$$\lambda 1 \geq \lambda 2 \geq \lambda 3 \geq \cdots \geq \lambda r \qquad (4)$$

The first r columns of V are the right singular vectors and the first r columns of U are the left singular vectors of A. To calculate the SVD of A we need to compute the Eigen values and Eigen vectors of AA^T or A^TA. The eigenvectors of AA^T from the columns of U, while the Eigen vectors of A^TA from the columns of V. The singular values in S are the square roots of the Eigen values of AA^T or A^TA. Each singular value specifies the luminance of the image layer while the corresponding pair of singular value specifies the geometry of the image layer. Another important feature of SVD is the invariance of singular values to common image processing operations and geometric transforms like rotation, translation and scaling. Due to this property, SVD has been used and also combined with other techniques for developing watermarking algorithms particularly resistant to geometric attacks.

IV. PROPOSED ARCHITECTURE

In this paper, we propose a watermarking algorithm that uses 2-level DWT decomposition and SVD for embedding an imperceptible watermark. Let F be the host image of size MxN and W is the watermark of size mxn. Block diagram of the proposed scheme is shown in figure 2.

A. Watermark Embedding Algorithm

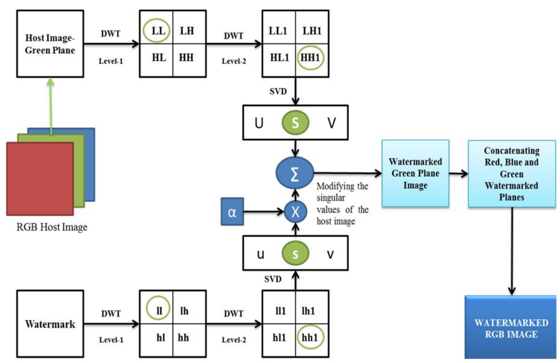


Fig. 2Proposed System Architecture-Watermark Embedding

Watermark is embedded as follows:

Separate the R, G and B components and perform 1-level DWT on the green plane of the host image.

Perform the second level of decomposition on the LL band of the first DWT decomposed image of both host and watermark images.

Perform SVD on the HH1 band of the resultant images of both the host and watermark images to obtain U, S and V matrices

$$I = Ui * Si * Vi' \qquad (5)$$

Embed the watermark into the host image by modifying the singular values of the host image

$$Swmi = Sh + (Sw * \alpha) \qquad (6)$$

The value of the scaling factor is chosen as 0.443 after a series of simulation results. Similarly, the level of decomposition chosen, performing SVD on the HH1 band are all justified with experimental results in the next section of the paper.

Now, perform the inverse of SVD to obtain the modified band HH2.

$$HH2 = Uh * Swmi * Vh' \qquad (7)$$

Perform inverse DWT on LL1; LH1; HL1; **HH2** sub-bands to obtain modified LL1' band.

Perform inverse DWT on **LL1'**; LH; HL; HH sub-bands to obtain the watermarked green plane image (G').

Concatenate the R, G' and B planes to obtain the watermarked RGB image.

B. Watermark Extraction Algorithm

Watermark extraction process is semi-blind in nature. The novel algorithm proposed for the same is given below:

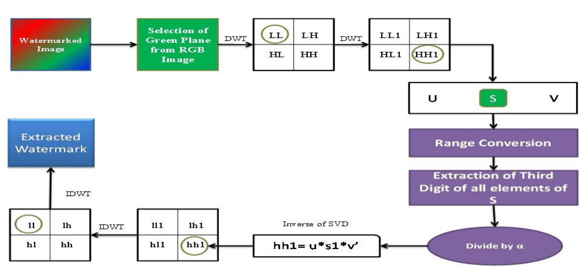


Fig. 3Proposed System Architecture: Semi-Blind Watermark Detection

Separate the R, G and B components and perform 1-level DWT on the green plane of the watermarked image.

Perform second level of decomposition on the LL band of the first DWT decomposed image.

Perform SVD on the HH1 band of the resultant image to obtain U, S and V matrices.

$$Iw = Uw * Sw * Vw' \qquad (8)$$

All the elements of 'Sw' matrix are converted to be within the range of 255 by dividing it by 255.

$$Src = \frac{Sw}{255} \qquad (9)$$

The third digit of all the elements of range converted matrix 'Src' is obtained, which is more or less equivalent to the singular values of the original watermark used during the embedded process. It can be obtained from the following equations:

$$Std = Src \bmod 100 \qquad (10)$$

Dividing 'Std' by α value, and then using it to perform the inverse of SVD to obtain the 'hh1' band corresponding to the watermark.

$$hh1 = Uhh * Std * Vhh' \qquad (11)$$

Perform inverse DWT on ll1; lh1; hl1; **hh1** sub-bands to obtain the 'll' band of extracted watermark.

Perform inverse DWT on **ll**; lh; hl; hh sub-bands to obtain the extracted watermark image.

When the third digit of all elements of 'Src' is taken, we obtain a matrix whose values are equivalent to the singular values of the watermark used during the embedding process. This can be justified by considering the following example:

Let one element of cover image be 100 and the corresponding watermark element be 200. Consider α value to be 0.01. Then by equation 6,

$$Swmi = 100 + (0.01) * 200 = 100 + 2 = 102 \qquad (12)$$

This is the singular matrix of the watermarked image at the detection side. Now, when we extract the third digit, we obtain value as 2.

When divided by alpha (here it is 0.01), we get 200 as the watermark element. In this way we obtain all the values of singular matrix of watermark embedded.

In cases when the watermark value is close to 1000 such as above 800, the probability of error is bound to increase, thereby reducing the PSNR of extracted watermark. It is important to note that range conversion is done to reduce the error probability in such cases. Thus, it is clear that we use only the value of α and watermark sequence to extract the watermark.

V. EXPERIMENTAL RESULTS

A. Experimental Setup

Matlab platform is used for the implementation and study of the proposed watermarking scheme. The Peppers image in Matlab of size 384*512 is used as the RGB cover image. A grayscale ISRO logo of size 500*500 is used as the watermark. After the embedding of the watermark, the watermarked image is tested various types of attacks to assess the performance of the proposed watermarking scheme. The cover image and the watermark are shown in figure 4. The visual quality of the watermarked image Ĝ in comparison with the original image G, is measured using PSNR (peak signal-to-noise ratio). PSNR is defined as

$$PSNR = 20\, log_{10}\left(\frac{255}{\sqrt{MSE}}\right) \quad dB \qquad (13)$$

where MSE is the mean squared error between the original image G and the watermarked image Ĝ,

given by

$$MSE = \left(\frac{1}{MN}\right)\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left[G(i,j) - \hat{G}(i,j)\right]^2 (14)$$

(a) (b)

Fig. 4 (a) Cover Image (b) Watermark Used

Watermarked Peppers image has a PSNR value of 52.0458 and a correlation of 0.9998. If we observe the watermarked and original cover image, we cannot find any perceptual degradation. For watermark embedding, 2-level DWT decomposition is performed and the HH band is used to perform SVD. This is justified by the data in tables 1 and 2 respectively. Table 1 consists of PSNR values for various levels of decomposition performed on the grayscale cover image. Figure 5 represents the data in graphical format. Table 2 consists of PSNR values for various chosen bands for performing SVD. In both the tables, the PSNR values of extracted watermark after JPEG compression is also given to get an idea of robustness to a very common attack which may even be an unintentional one.

TABLE I. CHOOSING THE LEVEL OF DECOMPOSITION

Levels	**PSNR- Watermarked image**	**PSNR- Extracted Watermark after JPEG compression**
Level I	44.0227	31.4917
Level II	44.0589	32.0931
Level III	44.1151	32.2509

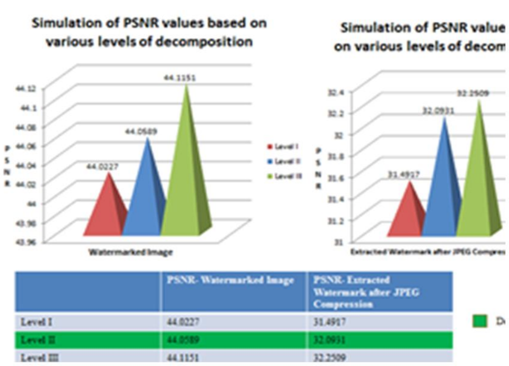


Fig. 5 Simulation results for choosing the level of decomposition

TABLE II. CHOOSING THE BAND FOR APPLYING SVD

Bands	PSNR- Watermarked image	PSNR- Extracted Watermark after JPEG compression
LL	12.3768	12.3464
LH	42.4209	38.4433
HL	43.2847	38.3391
HH	52.0458	42.2387

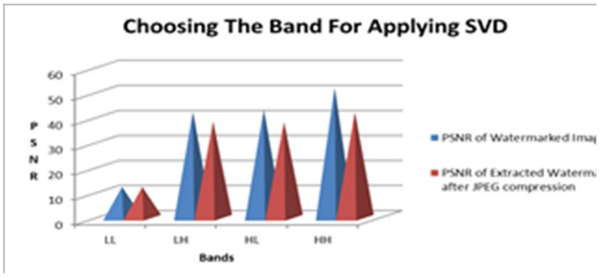


Fig. 6 Simulation results for choosing the band for applying SVD

A scaling factor of 0.443 is used and Haar wavelet is used for performing the DWT operation on the images. Similarly, the reason for choosing the green component of color image for watermarking is justified in table 3. Watermarking in green component produces a better PSNR value and is more robust to JPEG compression compared to watermarking in red and blue components.

TABLE III. CHOOSING THE GREEN COMPONENT FOR WATERMARKING

Levels	PSNR-Watermarked image	PSNR- Extracted Watermark after JPEG compression
R	70.9945	29.5423
G	70.9945	31.5329
B	70.9945	30.7754

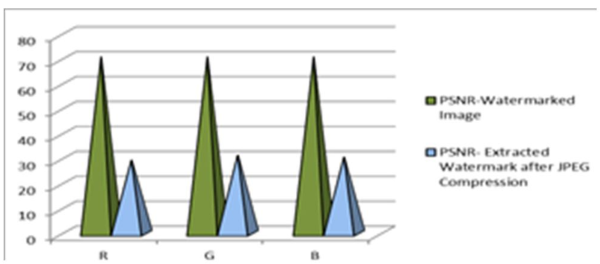
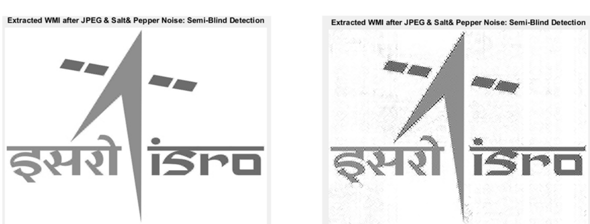


Fig. 7 Simulation results for choosing the green component for watermarking

Similarly, figure 8 shows the significance of range conversion in the proposed novel semi-blind detection scheme. When attacked by salt and pepper noise for example, the extracted watermark without range conversion suffers high error probability resulting in very low PSNR of 22.6777. On the other hand, when range conversion is done, the extraction is being robust returning a watermark with PSNR of 40.4664.



(a) PSNR=40.4464 (b)PSNR=22.6777

Fig. 8 Simulation results (a)with and (b)without Range Conversion

B. Results

The watermark is extracted from a watermarked image affected by various common attacks such as compression, resizing, cropping, histogram equalization, rotation, low pass filtering, high pass filtering, median filtering and various noise attacks such as Gaussian noise, salt and pepper noise and Poisson noise. The algorithm is tested for JPEG compression attack as the format is

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

used very commonly to store the images itself. We obtain the watermark with a PSNR of 40.2797 and correlation 0.9985 after JPEG. The algorithm is also tested for geometric attacks. In figure 9, after resizing the watermarked image to 250*250 from 384*512, we still get a watermark with a PSNR of 40.2527 and correlation 0.9984. In figure 10, a rotation attack for an angle of 30 degrees is applied and a watermark of 40.2655 PSNR and correlation 0.9985 is obtained. In figure 11, we get watermark with 40.2473 PSNR and correlation 0.9984 after cropping 50% of the watermarked image. In figure 12, histogram equalization attack is performed and watermark is still extracted with a PSNR of 40.3377 and correlation 0.9985. Our algorithm is also checked for its robustness to noise attacks. The algorithm is robust to Gaussian, salt and pepper noise and Poisson attacks as shown in figure 13, 15 and 16 respectively. The PSNR values of the extracted watermarks are 40.3449, 40.4464 and 40.2797 respectively. The correlations of the extracted watermarks are 0.9985, 0.9985 and 0.9985 respectively. The most common manipulation in digital image is filtering. Low, high and median filtering attacks are implemented on the watermarked image. Yet, the watermark is extracted with PSNR values of 40.2471, 40.2106 and 40.2620 respectively. The correlation values are 0.9984, 0.9984 and 0.9985 respectively. It is shown in figure 17, 18 and 14 respectively. Also, gamma and de-gamma attacks are used and a PSNR of 40.2771 and 40.2738 are obtained respectively with correlation of 0.9985 after both attacks. The above readings are tabulated in table 4, to provide better representation.

Fig. 9: Resizing attack

Attack	PSNR of Watermark	Correlation of Extracted Watermark to the Embedded Watermark
JPEG Compression	40.2797	0.9985
Resizing	40.2527	0.9984
Rotation of 30^{o}	40.2655	0.9985
Cropping of 50%	40.2473	0.9984
Histogram Equalization	40.3377	0.9985
Gaussian Noise	40.3449	0.9985
Salt & Pepper Noise	40.4464	0.9985
Poisson Noise	40.2797	0.9985
Median	40.2620	0.9985

Volume 3 Issue VI, June 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Filtering		
Low pass filtering	40.2471	0.9984
High pass filtering	40.2106	0.9984
Gamma Attack	40.2771	0.9985
De-Gamma Attack	40.2738	0.9985

TABLE IV. ROBUSTNESS OF THE ALGORITHM TO VARIOUS ATTACKS

FIG. 10: ROTATION ATTACK OF 30 DEGREES

Fig. 11: Attack by cropping of 50%

Fig. 12: Histogram Equalization attack

Fig. 13: Gaussian Noise attack

Fig. 14: Median Filter attack

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Fig. 15: Salt & Pepper Noise attack

Fig. 16: Poisson Noise attack

Fig. 17: Low Pass Filter attack

Fig. 18: High Pass Filter attack

Fig. 19: Gamma attack

Fig. 20: De-Gamma attack

VI. CONCLUSION

A novel algorithm is proposed for watermark embedding and it resembles that of a non-blind watermarking scheme. However, the watermark is extracted by using a novel semi-blind detection technique. The proposed embedding and detection algorithms are highly robust to various image processing attacks .The Indian Space Research Organization (ISRO) logo is used as watermark rather than noise type Gaussian sequences. The algorithm successfully extracts a visible watermark with good PSNR and correlation values after a variety of attacks. It is important to note that the watermark is removed only when the image quality is degraded to a great extent. That is, quality of extracted watermark is directly proportional to the image quality. Also, some of the planned future upgrades include either encryption of the image or implementation of neural networks to improve the robustness of the proposed algorithm.

VII. ACKNOWLEDGMENT

This work was possible because of Ritesh Kumar Sharma and Rahul Sharma, scientists at Indian Space Research Organization (ISRO). They provided us with the opportunity and constant support for the funded research project.

REFERENCES

[1] Liu JC, Chen SY, Fast two-layer image watermarking without referring to the original image and watermark. Image and Vision Computing 19(14) (2001) 1083-1097.

[2] Srdjan Stankovic, Igor Djurovic, Ioannis Pitas. "Watermarking in the space/spatial-frequency domain using two-dimensional radon-wigner distribution". IEEE Transactions on Image Processing. 2001, 10(4):650-658.

[3] Yong-Gang Fu, Rui-Min Shen, Colour image watermarking scheme based on linear discriminant analysis, Computer Standards and Interfaces 30(2008) 115-120.

[4] D.Kundur,D.Hatzinakos,"Towards robust logo watermarking using multi-resolution image fusion",IEEE Transactions on Multimedia 6,2004,pp.185-197.

[5] C.H.Lin, J.C.Liu and P.C.Han, "The security of the full-band image watermark for copyright protection", IEEE Int. Conf. on Sensor Networks, Ubiquitious, and Trustworthy Computing, Taichung, Taiwan, pp.74-79,2008.

[6] G.Bhatnagar and B.Raman, "A new robust reference watermarking scheme based on DWT-SVD", Computer Standards & Interfaces, vol.31, no.5, pp. 1002-1013, 2009.

[7] Habibollah Danyali, Morteza Makhloghi, Fardin Akhlagian Tab. "Robust blind DWT based Digital Image Watermarking using Singular Value Decomposition". Internation Journal of Innovative Computing, Information and Control, Vol.8, pp.4691-4703, July 2012.

[8] Kyung-Su Kim, Min-Jeong Lee, and Heung-Kyu Lee. " Blind Image Watermarking Scheme in DWT-SVD Domain". Intelligent Information Hiding and Multimedia Signal Processing(IIHMSP), Third International Conference, Vol. 2, pp. 477-480, 2007.

[9] R.Z.Wang,C.F.Lin and J.C.Lin,"Image hiding by optimal LSB substitution genetic algorithm",Pattern Recognition,vol.34671-683,2003.

[10] Chunlin Song, Sud Sudirman,Madjid Merabti. " A Spatial and Frequency Domain Analysis of the Effect of Removal Attacks on Digital Image Watermarks".ISBN: 978-1-902560-24-3 PGNet.

[11] Manoj Kumar.V.R.,C.Arun, S.Muthumanickam, R. Pravesh Anand, U.Manoranjan, K.Mohideen Abdhul Lathif. " Non-Blind watermarking of Colour Images in DWT-SVD Domain & Robustness to Various Attacks". International Journal of Advanced Information Science and Technology (IJAIST), Vol.35, No.35, March 2015. ISSN: 2319:2682.

[12] S.Muthumanickam, C.Arun, Manoj Kumar.V.R., Ritesh Kumar Sharma, Rahul Sharma. " Effects of Scaling factor for Non-Blind Watermarking of Colour Images in DWT-SVD Domain". International Journal of Applied Engineering Research, vol. 10, Number 31 (2015) Special Issues, pp.23174-23173.

[13] P.Ramana Reddy ,Munaga.V.N.K.Prasad,D.Sreenivasa Rao,"Robust Digital Watermarking of Color Images under noise attacks",International Journal of Recent Trends in Engineering,vol.1,No.1,May 2009.

[14] Peter Meerwald,"Digital image watermarking in the wavelet transform domain",Ph.D.Thesis

[15] P.Ramana Reddy, Munaga, V.N.K.Prasad, D.Sreenivasa Rao. "Robust Digital Watermarking of Color Images under Noise attacks". International Journal of Recent Trends in Engineering, Vol 1, No. 1, May 2009.

[16] M.Barni, M., Nartolini, F., V., Piva, A, "Improved wavelet based watermarking through pixel-wise masking," IEEE Trans Image Processing 10, 783-791, 2001.

[17] Y. Wang, J.F.Doherty and R.E.Van Dyck. "A wavelet based watermarking algorithm for ownership verification of digital images", IEEE Transactions on

Image Processing, 11, No.2, pp.77-88, February 2002.

AUTHOR'S PROFILE

Manoj Kumar. V. R. is currently pursuing his Bachelor of Engineering degree in Electronics and Communication Engineering at R.M.K. College of Engineering and Technology (Affiliated to Anna University), Puduvoyal, Chennai, Tamil Nadu India. Also he is serving as the Junior Research Fellow (JRF) for the funded project received by his project guide from Indian Space Research Organization (ISRO).

Dr. Arun Chokkalingam received his B.E degree in Electronics and Communication Engineering from Bharathidasan University, Trichy , India., He received his M.E and Ph.D. degree in VLSI design from Anna University, Chennai, India. He spent nearly 10 years as a teaching faculty in Electronics and Communication Engineering Department at Anna University Affiliated Colleges. His main research is on Channel Coding algorithms, VLSI Architecture, Mobile Communication and Signal Processing. He has published over 60 articles in reputed journals.

Mr.S.Muthumanickam has received his B.E degree in Electronics and Communication Engineering from Shanmugha College of Engineering Affiliated to Bharathidasan University, Trichirappalli in the year 2002, India. He pursued his M.E degree from College of Engineering Guindy, Anna University, Chennai, India in the year 2011. He is pursuing his research program in Anna University, Chennai, India. He has 13 years of teaching experience from Anna University Affiliated Colleges. His main area is on Image Processing, Wireless Communication, MIMO and MICs.