International Journal of Security and Its Application
Vol.11, No.1 (2017), pp.257-270
http://dx.doi.org/10.14257/ijsia.2017.11.1.21

A Robust and Secure Block-SVD based Embedding of Encrypted Watermark in Digital Images using RDWT

Sachin Gaur and Vinay Kumar Srivastava

Department of Electronics and Communication Engineering, Motilal Nehru National Institute of Technology Allahabad, INDIA
sachingaur1234@gmail.com, vinay@mnnit.ac.in

Abstract

Digital image watermarking has been proposed for treatment of the problem of copyright protection, authentication of digital data and ownership identification. In this paper a robust and secure digital image watermarking method based on Redundant Discrete Wavelet Transform (RDWT) and block-by-block SVD (Singular Value Decomposition) is presented. The watermark image is encrypted (scramble watermark) by using Cipher block chaining (CBC) to enhance its privacy and robustness. In the proposed scheme the gray scale host image is transformed by RDWT and is also segmented into non-overlapping blocks of each sub-band, and then a scramble watermark image is embedded in the singular values of these blocks in each sub-band. This scheme provides security by embedding encrypted watermark in block-by-block manner and has large capacity due to redundancy in RDWT domain and also preserves high imperceptibility due to SVD properties. The advantage of the given scheme is that it is much more robust to attacks such as cropping, compression, Gaussian noise. Experimental results show that this method performs better in terms of capacity, security and robustness than other block-based methods presented before.

Keywords*: Digital image watermarking; Redundant Discrete wavelet transform; Singular value decomposition, Cipher Block Chaining, NCC and PSNR.*

1. Introduction

Due to rapid growth of computer technology, multimedia and activity on the internet, digital data (Audio, Video, and Image) are widely spread and these data are not safe and the information hiding also becomes an important issue, so the problem of multimedia digital data security such as ownership identification, copyright protection, content authentication and tamper detection comes. Digital image watermarking is one the best solution to remove these problems. Watermarking means to hide the digital information into multimedia digital content (Audio, Video and Image) such that it is imperceptible to the human eye, only a real person can extract the information. The basic requirements of watermarking are robustness, imperceptibility, security [4]. Robustness means that the watermark should be resisted against various image processing attacks such as a noise addition, histogram manipulation, geometric attacks, filtering *etc*. Imperceptibility means that there is no difference between the original image and watermarked image. Security means the resistance against malicious attacks. As the capacity of the embedded data increase, performs of the system, improve but its effect on imperceptibility and robustness that is there is tradeoff between imperceptibility and robustness, as imperceptibility increases, the robustness decreases. This tradeoff is maintained by a factor is called scaling factor that is strength of embedding watermark. Digital image watermarking can be classified in two domains, one is spatial domain and other is transform domain. Spatial domain techniques advantages are simple to implement, low complexity and the capacity of data hiding is very high and disadvantage is less robust against various attacks [5].The

ISSN: 1738-9976 IJSIA
Copyright ⓒ 2017 SERSC

transform domain techniques Discrete Cosine Transform (DCT), Singular Value decomposition (SVD), Discrete Wavelet Transform (DWT), Discrete Fourier Transform (DFT) *etc*. are highly robust and imperceptible as compared to spatial domain techniques[6,8,12].The process of digital image scrambling by changing the pixel position of meaningful image through matrix transform in to meaningless disorder image is called image scrambling. There are several techniques for scrambling the image such as based on permutation substitution are enhanced blowfish algorithm, chaotic standard map and image encryption based algorithms are chaos random sequence, AES encryption algorithm [17,18], hash algorithm and block cipher. In our proposed scheme we use Cipher Block Chaining for encryption of the watermark image [16,19]. In SVD watermarking modified the singular values of the host image by watermark [3, 14, 15]. For tradeoff between imperceptibility and robustness we take scaling factor 0.02 for LL band and 0.002 for other band. RDWT has spatio-frequecy localization property and shift invariant and also overcome the DWT problem [10,11,12].Some researcher use block SVD- based watermarking techniques[6,7,8,9,12] for improving the robustness and imperceptibility also reduce the computational complexity.

The rest of the paper is organized as fallows In section 2 literature survey and brief background about SVD , RDWT and Cipher block chaining(CBC) then in section 3 embedding and extracting steps of proposed scheme are explained. The results and comparative analysis are in section 4 and finally conclusion are drown in section 5

2. Literature Survey

Liu *et al*. [3] Proposed SVD- based watermarking method that performs the embedding process to the singular values of the whole image. The Drawback of this scheme is watermark degradation due to some image processing attacks. Ganic et al. [2] Proposed DCT-SVD based watermarking scheme and suffers from the lack of robustness for some attacks. Kang et al. [1] used discrete Fourier transforms.it is more robust, but lack of imperceptible. Wang et al. [8] Using discrete Cosine transforms for transforming the block of pixel and improve the robustness. Navas et al. [7] Present a block based scheme using discrete wavelet transform and improve the imperceptibility as well as robustness. Mahammad et al. [12] proposed a DCT block based algorithm with human visual system (HSV) to get a higher detection rate as well as better fidelity, but the compression result is not good. Chin-Chen et al. [20] a block-based new watermarking technique using exclusive or operation to construct a secret key, this method is resist various attacks. Yixin Yan *et al*. [13] use just noticeable distance (JND) for an adaptive block based watermarking and quality factor above 40 this scheme is more robust. In Liu *et al*. [3] a single watermark embedded in singular values of the whole image and it is destroyed due to attacks. This is the main drawback of Liu *et al*. To avoid this drawback Ghazy *et al*.[9] proposed a block- by block SVD based techniques and removes this disadvantage and find out better results, but in Ghazy *et al*. [9] Scheme the size of watermark is very small as compared to the host image and has very low embedding capacity. Our presented block-by block RDWT –SVD based method has the high embedding capacity more robust against JPEG compression, cropping, rotation, blurring, Gaussian noise, resizing and rotation and also have high security and imperceptibility.

2.1. SVD

SVD is a numerical method for resolving the matrix for numerical analysis. It uses for extracting the algebraic feature of the image. The main properties of SVD are the singular values of an image matrix have good stability and when a small permutation is added to an image, its singular values do not change significantly [22]. In SVD transform, any $n \times n$ matrix A can be decomposed as $A = UDV^T$ where U and V are orthogonal matrix and $D = diag(\alpha_i)$ is a diagonal matrix, where α_i , $i = 1,2,3 \dots n$ are the singular values.

 Copyright ⓒ 2017 SERSC

The column U is the left singular and V is the right singular matrix of the image matrix A. It can be written as

$$A = UDV^T \quad (1)$$

$$= [u_1, u_2, \dots u_n] \times \begin{pmatrix} \alpha_1 & 0 & \cdots & 0 \\ 0 & \alpha_2 & \cdots & 0 \\ \vdots & 0 & \ddots & 0 \\ 0 & 0 & \cdots & \alpha_n \end{pmatrix} \times [v_1, v_2, \dots v_n]$$

$$= \sum_{i=1}^{r} \alpha_i u_i v_i$$

Where r is the rank of the matrix A. The singular values define the luminance of the image and the similar pair of singular matrix defines the geometry of the image.

2.2. RDWT

Watermarking in frequency domain, DWT is one of the mostly using techniques because it has spatio- frequency localization property. Due to shift variance a major change occur in the wavelet coefficients of the image even for minor shifts in the input image. As a result, there is an inaccurate extraction of watermark image and cover image data. [11, 21] RDWT solve this problem because it is shift invariant. 1D DWT and 1D RDWT can be described by Figure 1, Figure 2.Where$f(n)$ and $f^{`}(n)$ represents the 1D input and reconstruct the signal. h[-k] and g[-k] are analysis filters and h[k] and g[k] are synthesis low pass and high pass filters respectively. cj and dj are the low-band and high-band output coefficients at level j. The analysis and synthesis equation of RDWT are shown in equation (2), (3), (4).

Analysis

$$c_j[k] = (c_{j+1}[k] * h_j[-k] \quad (2)$$

$$d_j[k] = (c_{j+1}[k] * g_j[-k] \quad (3)$$

Synthesis

$$c_{j+1}[k] = \frac{1}{2}\left(c_j[k] * h_k[k] + d_j[k] * g_i[k]\right) \quad (4)$$

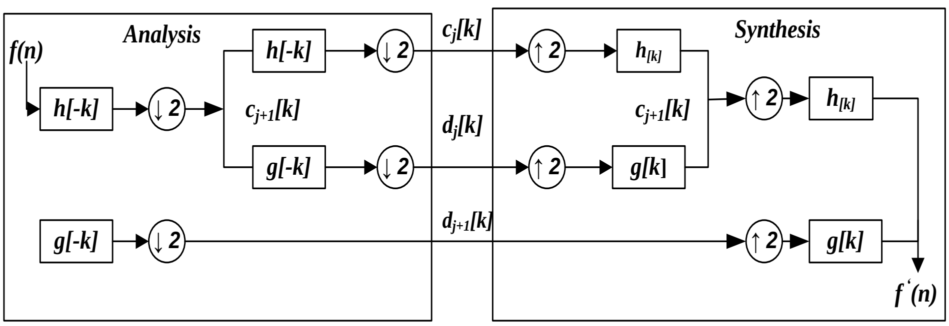


Figure 1. Analysis and Synthesis Filter Banks of I D DWT

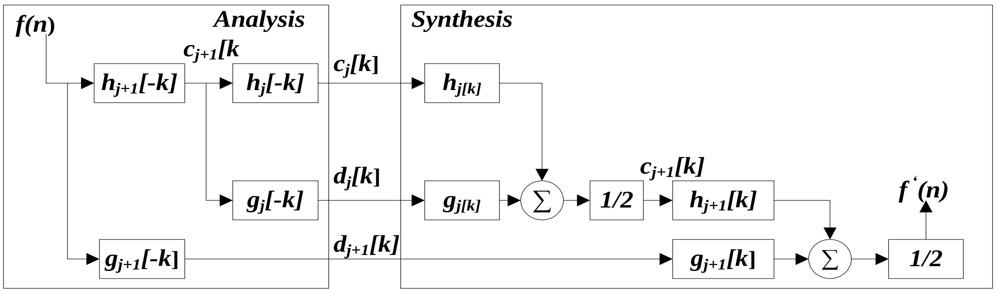


Figure 2. Analysis and Synthesis Filter Banks of I D RDWT

Where * means convolution and ↓2 means down sampling and ↑2 means up sampling at each level of iteration in DWT. Size of each sub band decrease due to down sampling and increase in levels of decomposition. RDWT discard down sampling and up sampling of coefficients. At each level the number of output coefficient doubles that of the input. RDWT based signal processing is more robust than DWT based techniques.

2.3. Cipher Block Chaining

Cipher Block Chaining (CBC) encrypts the sequence of bit as a single or block by block and changes the original image into encoded image.[16,19] It uses a vector of same length of plaintext with first block is called an initialization vector (IV).

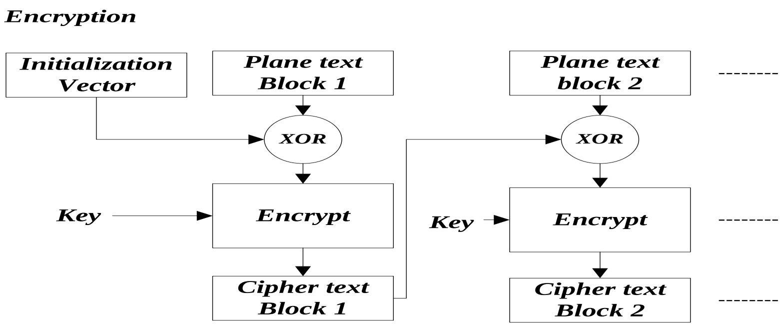


Figure 3. Encryption by Cipher Block Chaining

Initialization vector (IV) is not secret but unpredictable. Each plaintext block is XORed with the previous cipher block and then encrypted. Original image can be recovered by applying decryption process with the correct key. P_i, E_i, C_i, D_k, C_0 are plaintext, encrypted text, cipher text, decrypted text, and initialization vector respectively. The block diagram and the equation of encryption and decryption are shown in Figure 3, Figure 4 and equation (5), (6), and (7).

$$C_i = E_i(P_i \oplus C_{i-1}) \quad (5)$$

$$C_0 = IV \quad (6)$$

$$P_i = D_k(C_i) \oplus C_{i-1} \quad (7)$$

Copyright ⓒ 2017 SERSC

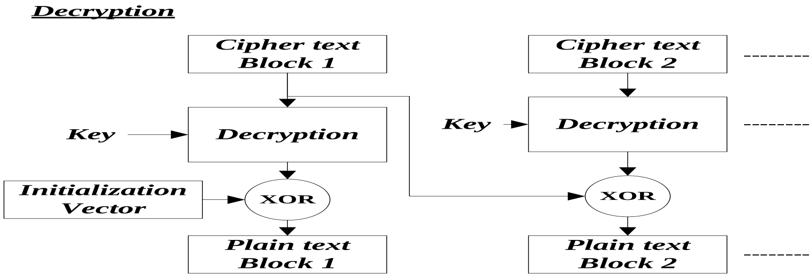


Figure 4. Decryption by Cipher Block Chaining

3. The Proposed Scheme

The proposed watermark embedding and extracting steps are given below.

3.1. Watermark Embedding steps:

1. The host image is transformed by RDWT and then divides all sub-bands in to non-overlapping blocks, here we show partition of LL bands in embedding block diagram in Figure 5.

2.An SVD process is apply on each block of LL sub band and get a matrix of singular values P_i , where i=1,2,3…….*N,N* is no of blocks

$$S_{bi} = K_i P_i L_i^T \quad (8)$$

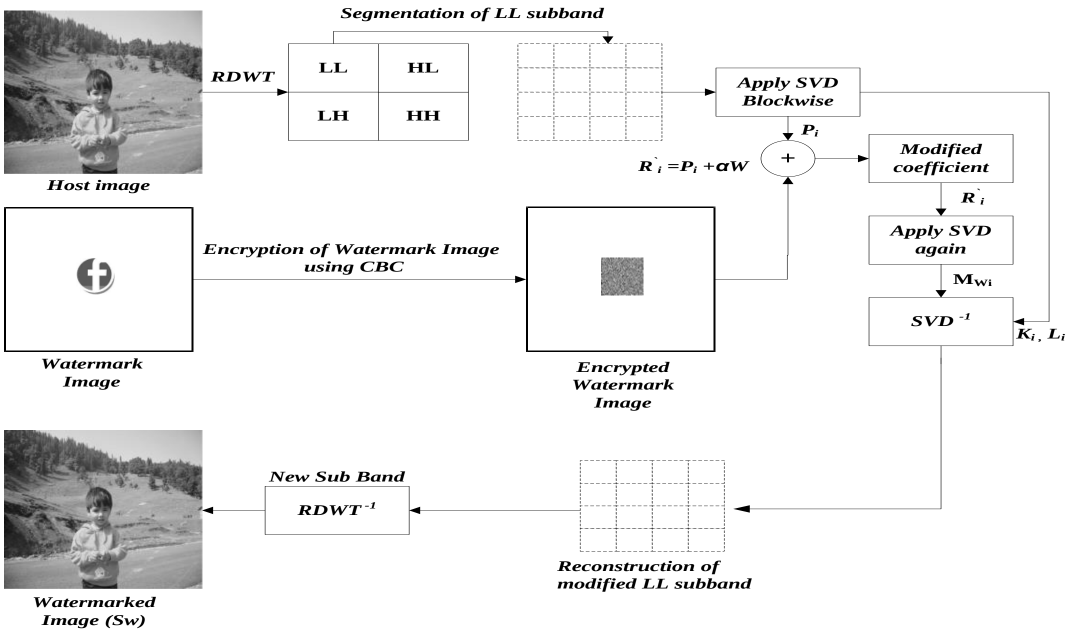


Figure 5. Watermark Embedding Process

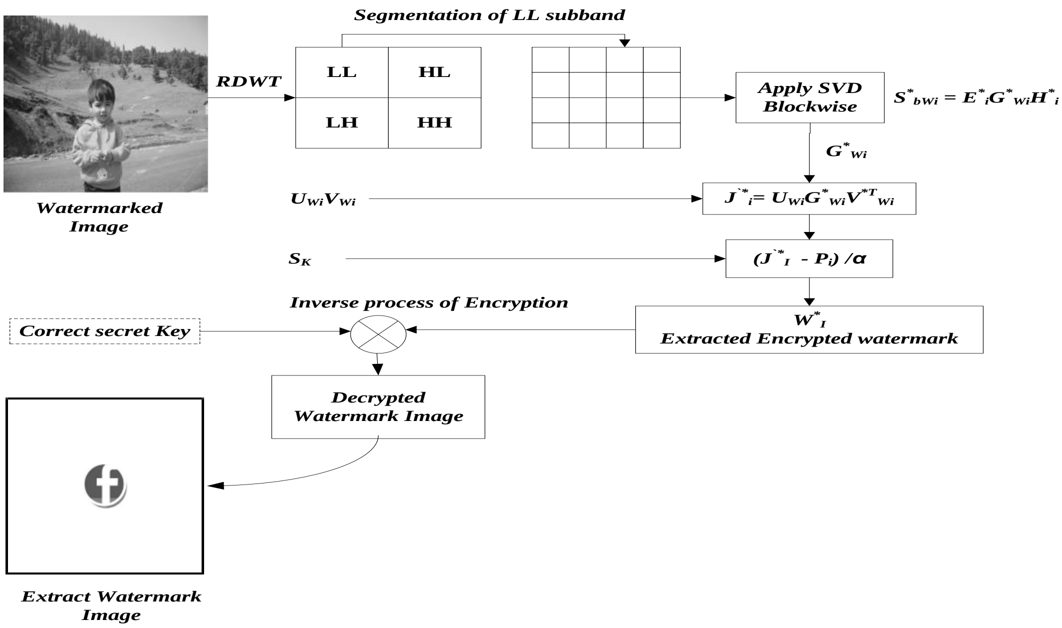


Figure 6. Watermark Extraction Process

3. Taking f logo as a watermark image and scrambled by using Cipher Block Chaining algorithm, now this scrambled watermark image is embedded.

- Watermark image f is divided into non-overlapping blocks and considers 8 successive pixels of the image as a single block for generation of key process.
- Now taking XOR operation with each block to obtain the encrypt image by using key.
- Encrypted image is called scrambling image.

4. This scrambled watermark directly adds to singular values of each block of LL sub band.

$$R_i^{`} = P_i + \alpha W \quad (9)$$

5. Again SVD process apply to modify the matrix $R_i^{`}$

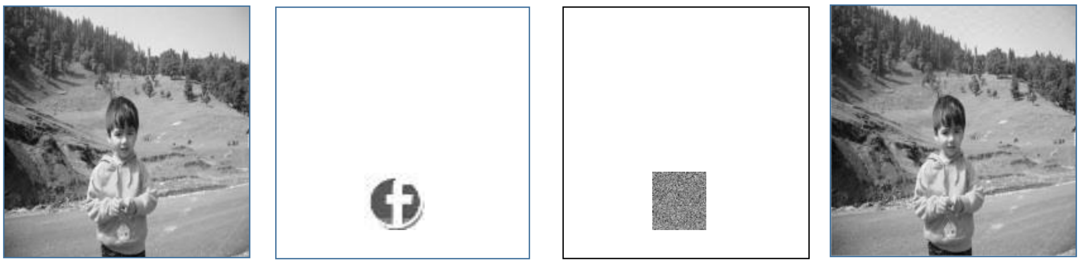
$$R_i^{`} = U_{Wi} M_{Wi} V_{Wi}^T \quad (10)$$

6. Perform new operation to modify the coefficient for each block of LL sub band

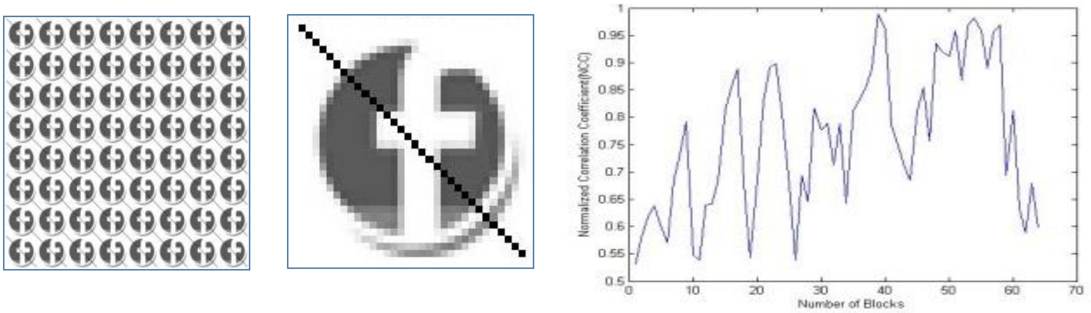
$$S_{bWi} = K_i M_{Wi} L_i^T \quad (11)$$

7. Apply inverse RDWT and rearrange all watermarks in each block and get watermarked image S_W

 Copyright ⓒ 2017 SERSC



(a) (b) (c)



(e) (f) (g)

Figure 7. Host Images: (a) Rudra, (b) Watermark Image f Logo, (c) Encrypted Watermark Image, (d) Watermarked Image Rudra, (*PSNR* 53.785dB.)(e) Extracted Watermark Images f Logo, (f) Magnified Watermark Maximum Correlation, (g) Watermark Normalized Correlation Coefficients

3.2. Watermarking Extracting Steps:

1. By applying RDWT on distorted image S_W^* and decompose it into four sub-bands
2. SVD is applied to all sub bands as fallows

$$S_{bWi}^* = E_i^* G_{Wi}^* H_i^{*T} \quad (12)$$

(a) (b) (c)

Figure 8. Watermarked Images after Applying Attacks (a) Gaussian Noise (0.01) (b) Blurring (3×3) (c) Cropping, All Images Size are 512×512

Copyright ⓒ 2017 SERSC

(d) (e) (f)

Figure 9. Watermarked Images after Applying Attacks (d) Resizing (512-256-512) (e) Rotation (150) (f) Compression All Images Size are 512×512

3. Now abstain $\grave{J}_i^*$ by applying operation

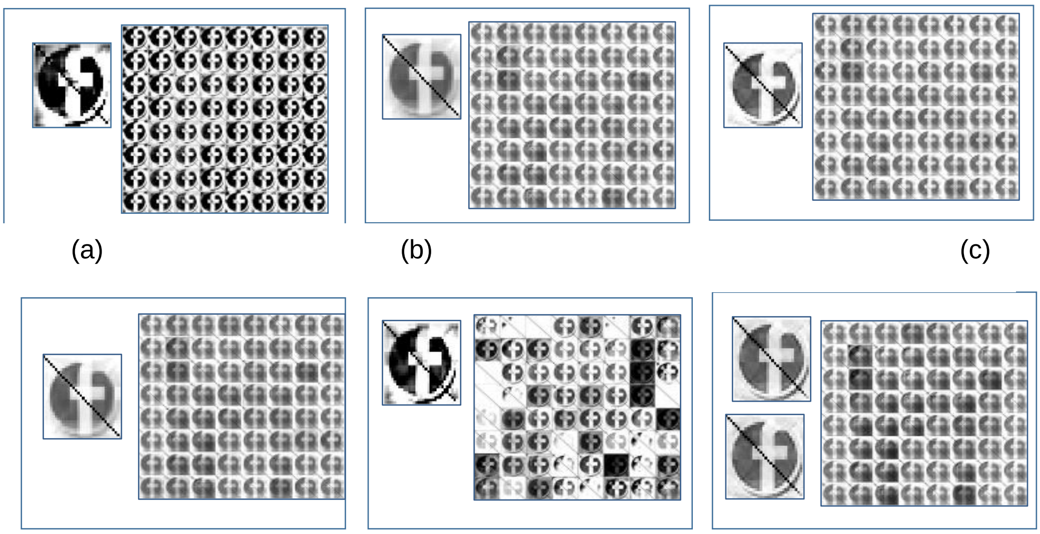
$$\grave{J}_i^* = U_{Wi} G_{Wi}^* V_{Wi}^{*T} \tag{13}$$

4. Now find extracted scrambled watermark

$$W_i^* = \frac{\grave{J}_i^* - P_i}{\alpha} \tag{14}$$

5. Now applying inverse encryption method to extract the watermark W_{Ei}^*

6. Now rearrange all extract watermark images in each block of each sub band and get combine image.



(a) (b) (c)

(e) (f) (g)

Figure 10. Extracted Watermark Images Image and Reconstructed Image of LL Sub-Band after Applying Attacks (a) Gaussian Noise(0.01), (b) Blurring(3×3), (c) Cropping, (d) Resizing 512-256-512), (e) Rotation, (150) (f) Compression

 Copyright ⓒ 2017 SERSC

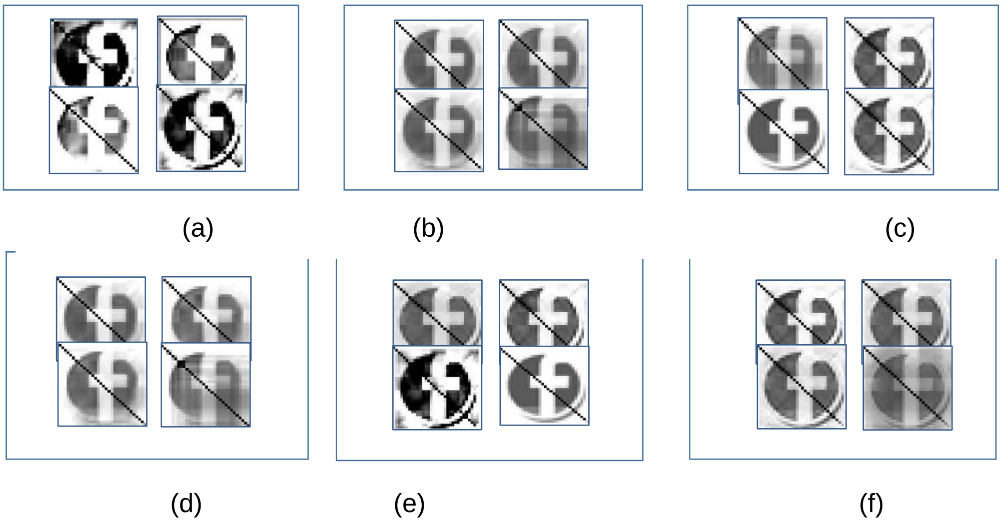


Figure 11. Extracted Watermark Images of Sub-Band (LL,LH,HL,HH) After Applying Attacks (a) Gaussian Noise(0.01), (b) Blurring(3×3),(c) Cropping, (d) Resizing(512-256-512), (e) Rotation, (150) (f) Compression

Table 1. Correlation Coefficient Value after Applying Attacks (a) Gaussian Noise (0.01), (b) Blurring (3×3), (c) Cropping, (d) Resizing (512-256-512), (e) Rotation, (15^0) (f) Compression in All Sub Band (LL,LH,HL,HH)

Attacks	Proposed Scheme(RDWT+Block based SVD and using CBC			
	LL	LH	HL	HH
Gaussian noise(0.01)	0.5152	0.5644	0.5648	0.5731
Blurring(3×3)	0.7839	0.7748	0.6981	0.5251
Cropping	0.5381	0.8938	0.9197	0.9979
Rotation(15^0)	0.5448	0.9114	0.8933	0.9393
Resizing512-256-512	0.5445	0.6459	0.6118	0.5773
Compression	0.6791	0.6551	0.6489	0.6187

Table 2. Imperceptibility (dB.) Compression Table in Proposed Scheme, Liu *et al*. [3], and Ghazy *et al*. [9] with Watermarked Image Rudra in Different Domain

Domain	Proposed Scheme	Liu *et al*.[3]	Ghazy *et al*. [9]
Spatial	51.8412	60.5250	45.8749
RDWT	53.7851	-	-
DWT	47.2581	61.1391	46.3865
DCT	48.9857	60.5284	49.7598

4. Experimental Results

In this section some experiments are executed by using the MATLAB 13a and find out the results and also checked the performance of the proposed scheme. In our experiments two gray scale standard images (Lena, Rudra) of size (515×512) and each block size is 64×64. Different block size can be use but this size has less complexity. Figure 7 (i) shows that the correlation coefficient is more than 0.5 for all extracted watermarks. This ensures that in the absence of attacks, the watermark can extract perfectly. In this paper results are given by taking Rudra as host image and f logo as a watermark image. For tradeoff between imperceptibility and robustness, we have taken two scaling factor for embedding the watermark into the host image are 0.02 for LL sub band and 0.002 for other sub bands are taken in this scheme. The imperceptibility analysis can be measured by calculating the PSNR (peak signal to noise ratio) value. The acceptable value of PSNR is 30 db.

The PSNR can be calculated by the given formula as.

$$PSNR = 10\, log_{10}\left[\frac{max\big(x(i,j)\big)^2}{MSE}\right] \qquad (15)$$

MSE (Mean square error between host image x and watermarked image y can be calculated as

$$MSE = \frac{1}{m \times n}\sum_{i=1}^{M}\sum_{j=1}^{N}[x(i,j) - y(i,j)]^2 \qquad (16)$$

For robustness we can calculate the normalize correlation coefficient (NCC) by given formula.

$$NC(w,\overline{w}) = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}[w(i,j) - \mu_w][\overline{w}(i,j) - \mu_{\overline{w}}]}{\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}[w(i,j) - \mu_w]^2}\sqrt{\sum_{i=1}^{M}\sum_{j=1}^{N}[\overline{w}(i,j) - \mu_{\overline{w}}]^2}} \qquad (17)$$

Where N and M present the no of pixel in watermark. $w, \overline{w}$ are original watermark and extracted watermark and are mean of original watermark and extracted watermark. Here we apply six attacks Gaussian noise with zero mean and 0.01varience, blurring using an average filtering, cropping, resizing(512-256-512), rotation(150) and compression, on watermarked image, whose results have been shown in the Table.1 and also these results, compared with the other previous scheme in Table.3 and get the better results. In our proposed scheme (Rudra) has been taken as host image and their corresponding watermarked image which is shown in Figure 7, The PSNR value of watermarked image Rudra is(53.7851dB.) and for Lena is 53.164dB.) It shows a big similarity between the host images and their corresponding watermarked images. The robustness can be calculated by finding the Normalized Cross-Correlation (NCC) from equation (17). The value of NCC should be in the range between −1 and 1. If the value of NCC closes to +1 then the extracted watermark is strongly correlated. If it is close to −1, the extracted watermark is also strongly correlated, but it seems to be a negative images. And if it is near 0, the extracted watermark is completely uncorrelated generally the NC acceptable value is 0.75 or above. The highest correlation coefficient between extracted watermark and original watermark is 0.9989 with no attack, values are given in Table.3. From Figure 7 and experimental values of PSNR in Table.2, it shows that our proposed scheme is highly imperceptible.

 Copyright ⓒ 2017 SERSC

Table 3.Compression of Highest Correlation Coefficient between Extracted Watermarks and Original Watermark with or without Attack in Proposed Scheme, Liu *et al*. [3] and Ghazy *et al*. [9]

Attacks	Domain		
	DWT		RDWT
	Liu *et al*. [3]	Ghazy *et al*. [9]	Proposed scheme
(a) Without Attack	0.8524	0.9985	0.9989
(b) Gaussian noise(0.01)	0.1332	0.5736	0.8193
(c) Blurring(3×3)	0.0916	0.7953	0.8033
(d) Cropping	0.0089	0.9984	0.9987
(e) Rotation(15^0)	0.0743	0.9312	0.9543
(f) Resizing(512-256-512)	0.1425	0.6572	0.9330
(g) Compression	0.0617	0.6811	0.7051

The extracted watermark image and reconstructed image of LL sub bands after applying attacks Gaussian noise, blurring, cropping, resizing, rotation and compression are shown in Figure 10, whose highest correlation coefficient values are also given in Table.3 and by seeing these values, We can say that the presented scheme is rich in terms of robustness and imperceptibility in comparison to previously proposed methods.

Comparative Study

In this section, we compare the results of the proposed scheme with Liu *et al*. [3]. Ghazy *et al*. [9] scheme is shown in Table 3. Liu *et al*. [3] Proposed SVD- based watermarking method that performs the embedding process to the singular values of the whole image. The main fragility in their systems is watermark degrade due to some image processing attacks. Ghazy *et al*. [9] proposed a block- by block SVD based techniques and solves this shortcoming and get better results, but the size of watermark is very small as compared to the host image. Comparative char is shown in Figure 12. Here (a) is without attack (b) is Gaussian noise with zero mean and 0.01 variance (c) is blurring using an average filtering(d) is cropping,(e) is resizing(512-256-512) (f) is rotation(150) and(g) is compression attacks.

Comparative Chart

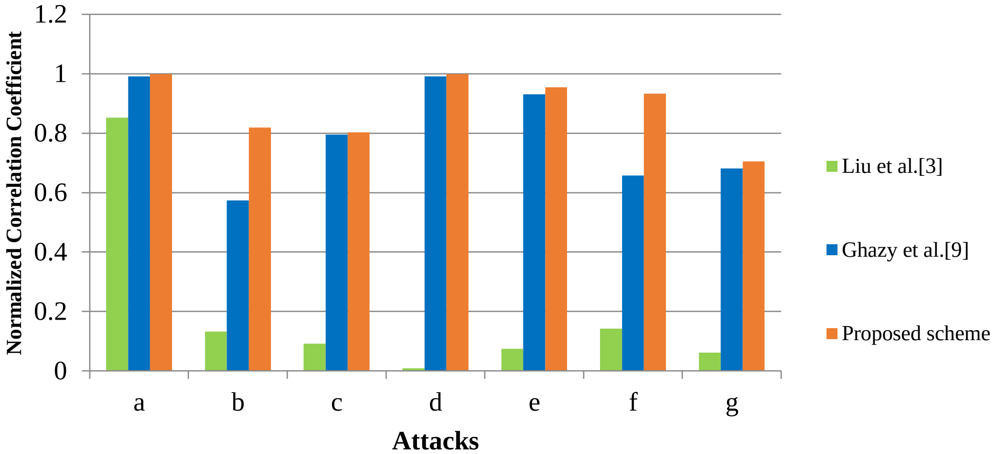


Figure 12. Compretive Chart where a, b, c ,d, e, f, g are Attacks

In our proposed scheme we use RDWT and encrypted watermark to enhance its privacy and robustness. This presented block-by block RDWT –SVD based method more robust against compression, cropping, rotation, blurring, Gaussian noise, resizing and rotation. After seeing the NCC values in Table 3, comparative chart, Figure 8, 9, 10, we can say that our proposed method is more robust than previously proposed techniques.

5. Conclusion

In this paper, we present a digital image watermarking scheme based on RDWT and block-SVD, to embed an encrypted (scramble) watermark image in the singular values of each block with all RDWT sub bands of the gray scale host image. The advantage of block based method is, to attend the each block independently, so each block with a distinct key can be used to increase the security. Also the size of the payload of each block depends on its characteristics may vary from one block to another, which enhance the visual quality and robustness by comparing the size of payload with these characteristics. This scheme has the high embedding capacity and a little degradation in the image due to the RDWT-SVD properties. Encrypted watermark inserted in the LL sub band is resist to some attacks and for other sub bands (LH, HL, HH) is resisted to other attacks to enhance the robustness of this scheme. So it is difficult to remove or destroy the watermark from all sub bands. The experimental results show that it is more robust against JPEG compression, cropping, rotation, blurring, Gaussian noise, resizing attacks and also improve the performance in terms of imperceptibility, capacity, and security. The future scope of this presented scheme is, by using a multilevel decomposition of RWDT with optimization techniques for different images to make it adaptive and get the better results.

References

[1] X. Kang, J. Huang, Y. Q., and Y. Lin, "A DWT-DFT Composite Watermarking Scheme Robust to Both Affine Transform and JPEG Compression," IEEE Transactions on Circuits and Systems for Video Technology, vol. 13, no. 8, pp. 776–786, 2003.

[2] E.Ganic, and A. M. Eskicioglu, "Robust DWT-SVD Domain Image Watermarking : Embedding Data in All Frequencies," Proceedings of MM&SEC, pp. 166–174.2004.

[3] R. Liu, T. Tan, and S. Member, "An SVD-Based Watermarking Scheme for Protecting rightful ownership," IEEE Transactions on Multimedia, vol. 4, no. 1, pp. 121–128, 2002.

[4] V. M. Potdar, S. Han, and E. Chang, "A Survey of Digital Image Watermarking Techniques," 3rd IEEE International Conference on Industrial Informatics (INDIN), pp. 709–716, 2005.

[5] C. Way, H. Fung, A. Gortan, and W.G.Junior "A Review Study on Image Digital Watermarking," 10th International Conference on Networks, pp. 24–28, 2011.

[6] R. A. Ghazy, M. M. Hadhoud, M. I. Dessouky, F. E. A. El-samie, and S. Elkom, "AN EFFICIENT BLOCK-BY-BLOCK SVD-BASED IMAGE WATERMARKING SCHEME," Proceedings of Radio Science Conference pp. 1–9.2007.

[7] K. A. Navas, A. Mathews, M. Lekshmi, A. T. S, and M. Sasikumar, "DWT-DCT-SVD Based Watermarking." IEEE Proceedings of COMSWARE pp. 271–274).2008

[8] Y. Wang and A. Pearmain, "Blind MPEG-2 video watermarking in DCT domain robust against scaling," IEEE Proc.-Vis. Image Signal Process., Vol. 153, No. 5, 2006.

[9] R. A. Ghazy, A. M. Abbas, N. Al-zubi, E. S. Hassan, N. A. El, M. M. Hadhoud, M. I. Dessouky, S. A. Alshebeili, F. E. A. El-samie, "Block-based SVD image watermarking in spatial and transform domains, International Journal of Electronics " vol. 7217, no 20. September, 2015.

[10] J. Guo and H. Prasetyo, "International Journal of Electronics and Communications (AEÜ) Security analyses of the watermarking scheme based on redundant discrete wavelet transform and singular value decomposition," AEUE - Int. J. Electron. Commun, vol. 68, no. 9, pp. 816–834, 2014.

[11] S. Lagzian, M. Soryani, and M. Fathy, "Robust watermarking scheme based on RDWT-SVD: Embedding data in all subbands," 2011 Int. Symp. Artif. Intell. Signal Process. AISP 2011, pp. 43–47, 2011.

[12] M. Keyvanpour and F. Merrikh-bayat, "Robust Dynamic Block-Based Image Watermarking in DWT Domain," Procedia Comput. Sci., vol. 3, pp. 238–242, 2011.

[13] Y. Yan, W. Cao, and S. Li, "Block-based Adaptive Image Watermarking Scheme Using Just Noticeable Difference," International Workshop on Imaging Systems and Techniques Shenzhen, no. 1, 2009.

 Copyright ⓒ 2017 SERSC

[14] R. Run, S. Horng, J. Lai, T. Kao, and R. Chen, "An improved SVD-based watermarking technique for copyright protection" Expert Systems with Applications vol. 39, pp. 673–689, 2012.
[15] C.C. Lai, "An improved SVD-based watermarking scheme using human visual characteristics," Opt. Commun., vol. 284, no. 4, pp. 938–944, 2011.
[16] Yong-Cong Chen and Long-Wen Chang, "A Secure and robust Digital Watermarking Technique By the block cipher RC6 and Secure Hash Algorithm", IEEE, pp 518-121, 2001.
[17] Lian Xiaoqin, Li Wei, Chen Xiuxin ,Zhang Xiaoli ,Duan Zhengang , "Application of the Advanced Encryption Standard and DM642 in the Image Transmission System",IEEE The 7th International Conference on Computer science & Education , pp 444-447, 2012.
[18] Vinod Patidar G. Purohit, K. K. Sud , N .K. Pareek , "Image Encryption Through a novel Permutation – Substitution Scheme Based on Chaotic Standard Map", IEEE International Workshop on Chaos –Fractal Theory and its Application, pp 164-169, 2010.
[19] Singh, S. Sharma, and S. Singh, "Image Encryption Using Block Scrambling Technique," vol. 5, no. June, pp. 963–966, 2014.
[20] C.C. Lai and C.C. Tsai, "Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition," IEEE Trans. Instrum. Meas., vol. 59, no. 11, pp. 3060–3063, 2010.
[21] T. Duy, Z. Nakao, and Y. Chen, "Robust multi-logo watermarking by RDWT and ICA," vol. 86, pp. 2981–2993, 2006.
[22] C.C. Chang, C.C. Lin, and Y.S. Hu, "An SVD oriented watermark embedding scheme with high qualities for the restored images," International Journal of Innovative computing, Information and Control (ICIC), vol. 3, no. 3, pp. 609-620

Authors

Sachin Gaur received his B.Tech degree in computer science and engineering from College of Engineering Roorkee, India in 2003, M.Tech in Digital signal processing from G.B.Pant Engineering College Pauri Garhwal, India in 2008. He is presently a Ph.D student of MNNIT, Allahabad, India in the department of ECE. His areas of interest are digital signal processing, digital image processing, information hiding and watermarking techniques.

Vinay Kumar Srivastava received his B.Tech degree in Electronics and Telecommunication engineering from GEC, Rewa, MP, India in 1989, M.Tech in Communication from IIT-BHU, India in 1991 and Ph.D in Electrical engineering from IIT Kanpur, India in 2001. Presently he is Professor and head of the department (ECE), MNNIT Allahabad, India. He has about 24 year of teaching and research experience in the area of signal and image processing. He has chaired many session in conferences. He has authored and coauthored around 30 publications. His current research interest includes image compression, digital watermarking, stability 2D PSV system, DSP methods for identification of protein-coding regions, design and analysis of IDMA systems.

Copyright ⓒ 2017 SERSC

 Copyright ⓒ 2017 SERSC