International Journal of Electrical and Electronics Engineers
Vol. No. 9, Issue No. 01, January-June 2017
ISSN (O) 2321-2055
ISSN (P) 2321-2045

DWT-SVD BASED DIGITAL WATERMARKING SCHEME

Alifa D'Silva[1] , Nayana Shenvi[2]

[1,2]*Dept. of Electronics and Telecommunication Engineering, Goa College of Engineering (India)*

ABSTRACT

Digital watermarking aims at copyright protection. Any digital information can be carried in the form of audio, video or image. The copyright used can be a series of digits, company logo or signature. This is called a watermark which can be visible or invisible. There is a constant risk of copyright misuse and integrity violation of digital object. In case of any violation, ownership can be proved by recovering the watermark. In this paper, a DWT-SVD based hybrid scheme is developed. Firstly the original image is decomposed to DWT components and then the watermark is embedded in singular values obtained by applying SVD (Singular Value Decomposition). The performances of the proposed techniques after subjecting it to several attacks such as noise, compression, rotation, crop, shear, etc. has been carried out and its PSNR and correlation values are evaluated. MATLAB is used for simulation.

Keywords:watermark; security; authentication; singular value decomposition; discrete wavelet transform.

I. INTRODUCTION

With the advancement in technology digital data can be stored and transmitted by means of data communication networks with greater efficiency and quality. Two main concerns about illegal duplication and manipulation of data are copyright protection and integrity of the contents. Watermarking emerges as a solution for preventing misuse of digital multimedia. Watermark embedding is a process wherein a watermark is inserted into the original digital content. Watermark extraction is the reverse process which is used to extract the watermark from the original digital content.

Transform domain based techniques are mostly preferred over spatial domain based techniques due to higher robustness property of the transform based techniques. DWT provides better spatial localization, frequency spread and gives multiresolution characteristics of an image. There are three fundamental factors which determine the quality of the watermarking scheme.

- Imperceptibility: A good watermarking scheme will ensure that the host image is not distorted when watermark is embedded into it. High PSNR means better imperceptibility.
- Robustness: This property determines whether the watermarking technique is resilient to attacks such as cropping, noise attacks, filtering, compression, etc. The watermark should be recoverable even after the watermarked image is attacked. Correlation factor determines the robustness property.

International Journal of Electrical and Electronics Engineers
Vol. No. 9, Issue No. 01, January-June 2017
ISSN (O) 2321-2055
ISSN (P) 2321-2045

- Security: Use of keys or signature for authentication provides a sense of security to the watermarking scheme. Hence only the authorized party will be able to detect the watermark.

SVD is an important tool in linear algebra and is used due to its attractive mathematical properties which helps in preserving superior image quality. The cover image's singular values (SV's) are found and these SV's are used for embedding. Some important properties of SV'S are as follows: (i) Singular values are stable (ii) They represent intrinsic algebraic properties (iii) SV's can be applied to rectangular matrices (iv) They can survive various noise attacks (iv) SVD preserves both one-way and non-symmetric properties of an image (v) large portion of signal energy can be represented by just a few SV's.

Consider an image represented by a matrix Am×n, where m is the number of rows and n is the number of columns. The result of applying SVD on matrix Am×n is

SVD(Amxn) = [Umxn Smxn Vnxn]

where, U and V are the orthogonal matrices and S is the diagonal matrix. The elements of S represent the singular values (SVs).

Image assessment is done to find the quality of the watermarking technique. This is achieved by finding the PSNR value using the formula given below:

$$PSNR(db) = 10log_{10}\frac{(Max\ \imath)^2}{MSE}$$

Where ɪ is the maximum pixel value of the image. MSE is the mean square error given by:

$$MSE = \frac{[\Sigma_{i=1}^{M}\Sigma_{j=1}^{N}[f(i,j) - f'(i,j)]^2]}{M \times N}$$

f(i,j) and f'(i,j) are the original and watermarked image respectively of size M×N.

In order to find the robustness we calculate the correlation factor given by:

$$NC = \frac{\Sigma_{j=1}^{N} W\,W'}{\sqrt{\Sigma_{j=1}^{N} W}\sqrt{\Sigma_{j=1}^{N} W'}}$$

Where W and W' are the original watermark logo and extracted watermark logo respectively.

II. REVIEW OF PAPERS REFERRED

Farhan Alenizi, Fadi Kurdahi, Ahmed Eltawil, Abdullah Aljumah [1] proposed a DWT based scheme for video authentication. The DWT process is implemented using orthonormal filters. The watermark is inserted in one of the subbands. The Y- components of the video frames are decomposed and filters used for the DWT decompositions are randomly generated. This is to increase the security of the algorithm. High efficiency video coding (HEVC) technique is integrated with this method to examine the whole performance. This scheme is computationally faster, robust and provides multiresolution in images.

In this process a tradeoff between Transparency and robustness is observed. Also it produces blurring & ringing noise. Football video gives less performance in terms of correlation due to fast camera panning process. So the hiding process is not optimal in this case.

Md. Abul Kayum Hawlader, Md. Moniruzzaman, Md. Foisal Hossain [2] presented a scheme which uses singular value decomposition (SVD) technique. 2D Arnold's cat map is used to scramble the cover image. A

International Journal of Electrical and Electronics Engineers
Vol. No. 9, Issue No. 01, January-June 2017
ISSN (O) 2321-2055
ISSN (P) 2321-2045

secret key obtained from the ratio of modified SV's of secondary watermark and SV's of cover image is used during watermark extraction phase. High PSNR and Correlation values can be obtained in this method.

However, this method is computationally expensive and is not adaptive.

Haohao Song, Jian Gu [3] proposed a curvelet based adaptive watermarking scheme for images (CvAWI). In this method, the 3rd MF subbands of the zero coefficients image is obtained by embedding the matrices with pseudorandom binary values {-100, 100} into them. This scheme shows Robustness against common attacks such as low-pass filtering, noise & rotation.

The embedded watermark is susceptible to attacks that destroy the subbands of the image.

Jagdesh Prasad, Mahendra Kumar, Garima Mathur, R P Yadev, Rajesh Kumar [4] proposed a robust Image Watermarking using DCT based Pyramid Transform which involves Image Compression. Each level of the Laplacian pyramid is recursively constructed from its lower level by applying blurring (low-pass filtering); sub-sampling (reduce size); interpolation (expand); and differencing (to subtract two images pixel by pixel). This method provides high compression rates & low complexity encoder.

However, it shows less robustness to rotation and translation operation and there is information loss.

Maryam Karimi, Majid Mohrekesh, Shekoofeh Azizi, Shadrokh Samavi [5] have designed a Multi-Layer Perceptron(MLP) neural network which can predict blocks in the images that will not make major changes in quality of image after watermarking. The number of pixels in each watermarked block that intolerably changed on the basis of Weber ratio forms the target. Output obtained as a result of this network is a set of corrected biases and weights.

Although this method is adaptive it is computationally slower.

Myasar Mundher, Dzulkifli Muhamad, Amjad Rehman, Tanzila Saba, Firdous Kausar [6] proposed a scheme which uses Discrete Slantlet Transform (DST) to find the best frequency sub-band for embedding. Pre-processing is done to find the best RGB channel and quadrant of RGB host image in which the watermark will be introduced. This method provides good security and robustness against noise attacks.

It shows less robustness against sharpening, rotation, contrasting and histogram equalization. Also it degrades the image quality to some extent.

III. PROPOSED ALGORITHM

The objective of this project is to develop a watermarking scheme which is based on cascading DWT with SVD. DWT decomposes the image into four frequency bands: LL band which represents low frequency, HL and LH representing middle frequency and HH represents high frequency band. LL band gives approximate details. In this proposal, we select LL band to embed the watermark because it contributes significantly to the robustness of an image. Thus it can survive certain image processing operations like noise addition, intensity manipulation, etc. [15]. In this SVD based watermarking scheme, instead of embedding the watermark directly on the wavelet coefficients SVD transformation is applied to the whole image and then the singular values of the host image are modified to embed the watermark.

A. Watermark Embedding

- Watermark W is decomposed using SVD

$$W = U_W \times S_W \times V_W^T$$

International Journal of Electrical and Electronics Engineers
Vol. No. 9, Issue No. 01, January-June 2017
ISSN (O) 2321-2055
ISSN (P) 2321-2045

- Using Haar wavelet perform first level decomposition of the cover image: LL, HL, LH, and HH. SVD is then applied to LL band.

$$L = U_L \times S_W \times V_L^T$$

- The singular values of the LL band are replaced with the singular values of the watermark. After applying inverse SVD we obtain modified LL band.

$$L' = U_L \times S_L \times V_L^T$$

- Inverse DWT is applied to produce the watermarked cover image.

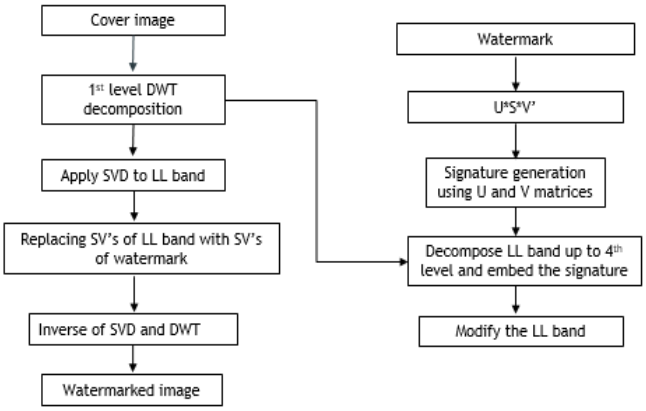

Fig 1.a Watermark embedding block diagram

B. Watermark Extraction

- Using Haar wavelet, the noisy watermarked image is decomposed.
- SVD is applied to LL band

$$L = U_L \times S_L \times V_L^T$$

- Then extract the singular values from LL band.
- The watermark is constructed using singular values and orthogonal matrices U_W and V_W obtained using SVD of original watermark.

$$W_E = U_W \times S_L \times V_W^T$$

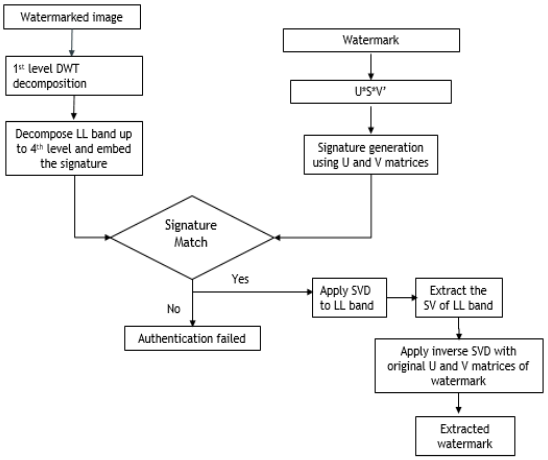

Fig 1.b Watermark extraction block diagram

International Journal of Electrical and Electronics Engineers
Vol. No. 9, Issue No. 01, January-June 2017
ISSN (O) 2321-2055
ISSN (P) 2321-2045

C. Signature based Authentication

The U and V orthogonal matrices needs to be authenticated before extracting the watermark. A unique signature is generated using the U and V matrices and it is embedded into the cover image along with the watermark. There is one to one correspondence between the SV's and orthogonal matrices.

Digital signature for the U and V matrices is generated as follows:

- Create an array by summing the column of the U and V orthogonal matrices.
- Map the values of the array obtained with the corresponding binary digits based on threshold.
- XOR the binary digits to obtain the signature.

For embedding the signature we generate the signature of N bits for the U and V matrices of watermark. Using Haar wavelet, we perform fourth level decomposition of the cover image's LL band. N random coefficient are selected from LL4 and HH4 band with the help of secret key. Then we convert the integer part into L bits binary code. For signature extraction, perform the inverse procedure. To generate the signature use the U and V matrices of the original watermark at the receiver and compare it with the extracted signature. If they match, U and V matrices are authenticated and hence we can use them in the extraction of the watermark.

IV. EXPERIMENTAL RESULTS

In this experiment 512 × 512 8 bit gray 'Cameraman' image is used as shown in fig 2.a–b.

Fig 2.a Original Cameraman image (512×512)

Fig 2.b Watermark logo

The simulation result for the attack free case is shown in fig 3.a-b.

Fig 3.a Watermarked Cameraman image signed with secret key

Fig 3.b Watermark logo extracted from Cameraman image

Table I shows the PSNR and correlation values obtained for the attack free case.

TABLE I. Attack free case

Test Image	*PSNR(db)*	*Correlation factor*
Cameraman	41.6513	0.9994

International Journal of Electrical and Electronics Engineers
Vol. No. 9, Issue No. 01, January-June 2017
ISSN (O) 2321-2055
ISSN (P) 2321-2045

Fig 4.a-g shows the result of attacks on the cameraman image.


Fig 4.a Mean attacked image and extracted watermark


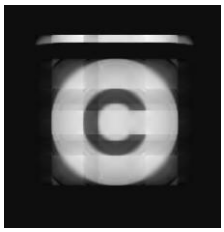

Fig 4.b Median attacked image and extracted watermark


Fig 4.c Crop attacked image and extracted watermark


Fig 4.d Rotation attacked image (45deg) and extracted watermark

International Journal of Electrical and Electronics Engineers
Vol. No. 9, Issue No. 01, January-June 2017
ISSN (O) 2321-2055
ISSN (P) 2321-2045


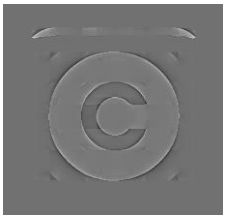

Fig 4.e Shear attacked image and extracted watermark


Fig 4.f Noise attacked image (Salt & pepper noise var=0.02) and extracted watermark


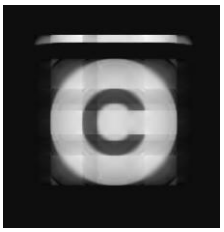

Fig 4.g jpeg compression attacked image (Q=70) and extracted watermark

Table II shows the PSNR and correlation values when the cameraman image is subjected to various attacks.

TABLE II. ATTACKS

Type of Attack	*PSNR*	*Correlation factor*
Mean (5×5)	29.6740	0.9907
Median (3×3)	38.2783	0.9987
Crop Attack (30%)	15.3004	0.8044
Rotation Attack (45deg)	16.0109	0.8434
Shear Attack	16.2094	0.8599
Salt & Pepper noise (var=0.02)	22.1198	0.8449
Jpeg compression (Q=70)	33.5275	0.9962

V. CONCLUSION

In this experiment a blind watermarking scheme has been proposed which combines SVD along with DWT. The watermark embedding and extraction algorithm were successfully implemented using MATLAB. From the result it is observed that this scheme yields higher PSNR value. Thus better imperceptibility is achieved. The correlation factor obtained is also high in case of attacks. Thus proving its robustness property.

VI. ACKNOWLEDGMENT

I would like to express my sincere gratitude to Prof. Nayana Shenvi for her constant guidance and valuable inputs. Also I would like to thank all those who have helped me and supported me throughout my dissertation work.

REFERENCES

[1] Farhan Alenizi, Fadi Kurdahi, Ahmed Eltawil, Abdullah Aljumah, "DWT based watermarking technique for video authentication", IEEE International Conference, December 2015.

[2] Md. Abul Kayum Hawlader, Md. Moniruzzaman , Md. Foisal Hossain, "SVD Based Robust and Secure Dual Stages Watermarking Scheme for Copyright Protection", IEEE Strategic technology (IFOST) 9th International Forum, December 2014.

[3] Haohao Song, Jian Gu "Curvelet Based Adaptive Watermarking for Images" Computer Science and Network Technology (ICCSNT), IEEE 2nd International Conference, December 2012.

[4] Jagdesh Prasad, Mahendra Kumar, Garima Mathur, R P Yadev, Rajesh Kumar, "Robust Image Watermarking Using DCT based Pyramid Transform via Image Compression", Communication and Signal Processing (ICCSP), IEEE International Conference, November 2015..

[5] Maryam Karimi, Majid Mohrekesh, Shekoofeh Azizi, Shadrokh Samavi, "Transparent Watermarking Based on Psychovisual Properties Using Neural Network", Machine Vision and Image Processing (MVIP), 8th Iranian Conference, IEEE March 2013.

[6] Myasar Mundher, Dzulkifli Muhamad, Amjad Rehman, Tanzila Saba, Firdous Kausar, "Digital Watermarking for Images Security using Discrete Slantlet Transform", Applied Mathematics and Information Science, International Journal 8, No.6, November 2014.

[7] Akshya Kumar Gupta and Mehul S Raval, "A robust and secure watermarking scheme based on singular values replacement", Sadhana Vol. 37, Part 4, August 2012, pp. 425–440, Indian Academy of Sciences.

[8] Qingmei Wang, Fengyan Sun, Fengyu Lui, "Research on public-key digital watermarking system", Communication Software and Network (ICCSN), IEEE 3rd International Conference, May 2011.

[9] S. Craver, N. Memon, B. L. Yeo, M.M. Yeung, "Resolving rightful ownerships with invisible watermarking techniques: limitations, attacks, and implications," IEEE Journal on Selected Areas in Communications, Vol. 16, Issue: 4, pp. 573-586, May 1998.

[10] N.F. Johnson, S.C. Katezenbeisser,"A Survey of Steganographic Techniques" Information Techniques for Steganography and Digital Watermarking, pp 43-75, Artec House, Dec. 1999.

[11] W. K. Pratt, "Digital Image Processing," New York: Wiley, 1991.

[12] R. Liu and T. Tan, "A SVD-Based Watermarking Scheme for Protecting Rightful Ownership," in IEEE Transactions on Multimedia, 4(1), pp. 121-128,March 2002.

[13] E. Ganic and A. M. Eskicioglu, "Secure DWT-SVD Domain Image Watermarking: Embedding Data in All Frequencies," ACM Multimedia and Security Workshop 2004, Magdeburg, Germany, September 20-21, 2004.

[14] R.Kakarala and P.O. Ogunbona,"Signal analysis using multiresolution form of the Singular Value Decomposition", IEEE Trans. On Image processing, vol. 10, No. 5, May 2001.

[15] Raval M S and Rege P P 2003 Discrete wavelet transform based multiple watermarking scheme. TENCON, Conference on Convergent Technologies for Asia-Pacific Region 3(1): 935–938