International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 04 Issue: 05 | May -2017 www.irjet.net p-ISSN: 2395-0072

A Digital Image Watermarking based on IWT and SVD for secure communication

Sumi choudhury[1], Swati Agrawal[2]

[1]*MTech Scholar, Dept. of Electronics and Telecommunication Engineering Bhilai Institute of Technology, Durg (C.G.)*

[2] *Associate Professor, Dept. of Electronics and Telecommunication Engineering Bhilai Institute of Technology, Durg (C.G.)*

Abstract - *Digital data can regularly have replicated by unapproved individual and claim to his proprietorship. In any case, we don't know who the genuine proprietor of that data is. Advanced Watermarking is a critical issue to tackle this sort of problems. Transform Domain methods are robust against both image processing generated noise and malicious attacks but a trade-off always exists among the robustness, capacity and im-perceptibility. Singular value decomposition (SVD) is presented for high embedding capacities and good imperceptibility. Thus, A new method have been presented based on Discrete Wavelet Transform (DWT), Integer Wavelet Transform (IWT) and Singular Value Decomposition (SVD). Computer simulation is done and comparative study of the proposed scheme with existing method shows improvements in effectiveness.*

Key Words: *Watermarking , Wavelet Transform , key.*

1.INTRODUCTION

Presently we can transmit any kind of data either data (in the type of picture) or images (pictures) by utilizing the Internet. The information may likewise open by unapproved people while transmit information through conventional business data transmitting channel like Internet. So, to provide information security we require propelled verification techniques. One of such verification technique is computerized watermarking. Advanced Watermarking alludes to systems that are utilized to counteract duplicating or ensure computerized information by imperceptibly hiding an approved check data into the first information. The hidden data can recover by the opposite procedure with right keys. An essential watermarking calculation, a picture for instance, comprises of a cover picture, a watermark structure, an installing calculation, and an extraction procedure.

A few procedures have been proposed for interactive media protection. Among the proposed strategies, much intrigue has concentrated on digital images. There are fundamentally two ways to deal with implant a watermark: spatial domain and Transform domain watermarking. The two principle requirements in the issue of watermarking are those of keeping up the strength of the watermark data while keeping visual view of the first picture in place. Aside from duplicate control and copyright protection; communicate observing, fingerprinting, ordering, medicinal application, content validations are other application regions of advanced watermarking.

Implanting the watermark into the spatial-domain part of the input image is the direct strategy. It has the benefits of low complication and simple execution. Notwithstanding, the spatial domain watermarking calculations are for the most part delicate to image handling operations or different assaults. on the contrary, the transform domain strategies insert the watermark by tweaking the value of coefficients in a transform domain . In spite of the fact that frequency domain strategies can yield more data to be embed and more strength against numerous basic assaults, the computational cost is higher than spatial-domain watermarking techniques.

Advanced watermarking is a procedure which includes two stages: (i) a calculation to implant little verification data called watermark content on the host content. (ii) A calculation to recover or extricate the implanted watermark with least changes. Robustness, maximum capacity, information payload, Peak Signal to Noise Ratio and security are the fundamental necessities identified with any watermarking framework. Robustness fluctuates starting with one operation then onto the next and starting with one plan then onto the next. All plans can't avoid all assaults, and thus, their resistance is application-dependent [1]. Watermark bits embedded is data and addition of all watermark data is called capacity [2]. Peak Signal to Noise Ratio (PSNR) gives the information about noise content in the output image; more PSNR shows better performance. The security term is utilized to portray a method that opposes numerous undesired attacks[3], many methods are robust but not secure .An exchange off dependably exists among the robustness and capacity; for instance, expanding the installing capacity in an image may upgrade its robustness while at the same time debasing its PSNR and the other way around. In this way, analysts have expanded their endeavors to create strategies that discover a compromise between these clashing parameters .Presently, enhancing the robustness against assaults by ensuring the visual quality is viewed as the center inspiration of most existing watermarking methods. Consequently, the motivation to create mixed methods that consolidate at least two transforms to use the properties of these transforms and accomplish the required objectives has emerged.

In spite of the fact that transform domain strategies can yield more data embedding and more immunity against numerous basic assaults, the computational cost is higher than spatial domain watermarking techniques. The DWT is very suitable to find areas in the cover image where a watermark can be embedded without the change in its view, due to its good spatio-frequency localization properties. Another wavelet transform is proposed by Sweldens [4]. Compared to Discrete Wavelet Transform (DWT), IWT has many improvements: such as integer coefficients and easy understanding. The transform coefficients of the DWT are the floating point values, adjusting these qualities to integer brings about losing their ideal recreation property. Be that as it may, the lifting plans in IWT maps integer to integer without adjusting mistakes. They are straightforward, execute and alter. They are additionally quick where all counts are performed set up, and assistant memory is not required. These properties of IWT can be used to protect the level of PSNR and upgrade the robustness[5-7].

Singular Value Decomposition(SVD) has been used in the watermarking schemes because of its mathematical property that that slight change in singular values don't influence the visual impression of the cover image, which lead the watermark implanting system to accomplish better clarity furthermore, robustness. Hence many methods have been proposed which combines DWT and SVD[8-10]. Watermarking schemes cannot rely on many of SVD based methods due to their security issues like false positive problem. Thence a hybrid watermarking system is proposed combining DWT, IWT and SVD for better security and robustness.

2.BACKGROUND

IWT is a sort of novel wavelet development technique. It is demonstrated that all traditional wavelets can be realized utilizing lifting techniques [11]. The IWT consist of three lifting steps as: splitting, prediction and updation.

- Split: Input signal is decomposed into odd and even parts, which are also known as lazy wavelets.
- Predict: In this step the new odd component is evaluated based on the combination of even components. This predict operation is also called as dual lifting.
- Update: In this step the new even component is evaluated based on the combination of difference samples obtained from predict step. This predict operation is also called as primal lifting.

This part of the paper describes the prerequisite for the understanding of the methodology i.e. DWT, IWT and SVD

2.1. DWT and IWT

The DWT has gotten extensive consideration in different signal processing applications, including image watermarking. The primary thought behind DWT comes about because of analysis of multiresolution images, which includes division of a images in frequency channels of consistent data transfer capacity on a logarithmic scale. It has points of interest, for example, comparability of information structure as for the determination and accessible division at any level. The DWT can be realized as a multilevel transformation .A image is divided into four subbands meant LL, LH, HL, and HH at level 1 in the wavelet domain, where LH, HL, and HH speak to the finest scale wavelet coefficients and LL remains for the coarse-level coefficients. The LL subband can further be divided to acquire another level of decay. The disintegration procedure proceeds on the LL subband until the coveted number of levels controlled by the application is attained. Since human eyes are a great deal more delicate to the low-frequency part (the LL subband), the watermark can be implanted in the other three subbands to keep up better picture quality.

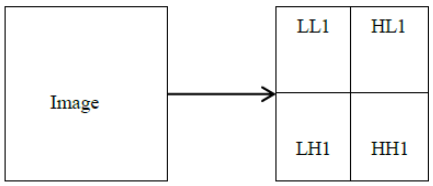

Fig -1: Single level DWT

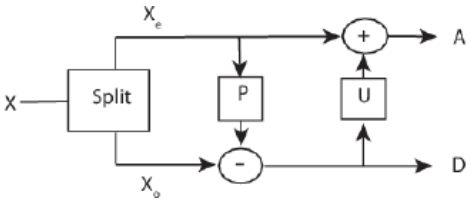

Fig- 2: IWT lifting step

2.2. SVD

SVD is an essential aid in mathematics, which is broadly connected in many research fields, for example, data compression, principal component analysis and others. From the perspective of image preprocessing applications, there are two fundamental properties of the SVD. In the first place, the stable SVs of a image, i.e., when a little information is added to a picture, its SVs don't change altogether. Second, SVs speak to inherent arithmetical image properties.

From the viewpoint of mathematics, a computerized picture can be seen as a network made out of various positive scalars, singular value decomposition (SVD) has a place with an

orthogonal change, it can make the picture framework diagonalization.[12]

Let consider an image matrix $X \in R^r$ with rank r, this matrix X can be represented as follows:

$$X = USV^T$$

Where $U = [u_1, u_2, \ldots \ldots, u_m] \in R^m$

$V = [v_1, v_2, \ldots \ldots, v_n] \in R$ and is a diagonal matrix. and are called singular value vectors. Diagonal elements are represented as

$$\lambda_1 \geq \lambda_2 \geq \lambda_3 \ldots \ldots \ldots \ldots \lambda_r \geq \lambda_{r+1} = \cdots \ldots = \lambda_N = 0$$

Is called as singular values and determined by SVD of input matrix. Utilization of SVD in digital image handling has a few benefits.

- SVD transformed matrix can be rectangle or square, it is not fixed.
- Effect of general image processing apllication is less on singular values because bigger singular values preserve the energy of the image and less affected by external assaults. Most of the times SVD matrix has small values.
- Singular values(S) of the input image represents algebraic properties like luminance but singular vectors(U & V) of input image represents geometric properties

3.METHODOLOGY

This paper adds the security feature with watermarking process by adding digital signature in the output image. This section portrayed the watermarking process and embedding and extraction process by utilizing flowchart for watermark embedding and watermark extraction individually that shows how watermark image is installed with host image and how the implanted watermark is extracted from the watermarked image.

3.1. Watermarking Process

Watermarking process includes watermark embedding and watermark extraction process, steps of which are mentioned below:

Watermark Embedding Process

Step 1. Perform 1-level IWT to decompose the host image into four sub-bands LL,HL,LH and HH and perform SVD to all

Sub-bands as

$$X_i = U_i S_i V_i^T$$

Where i represents sub-bands.

Step 2. Add watermark image to the singular values of each sub-bands and again perform SVD on modified singular value.

$$S_i + \alpha W = U_i^W S_i^W V_i^{TW}$$

Where represents robustness factor

Step 3. Now, change IWT coefficients for each sub-bands as

$$X_i modified = U_i S_i^W V_i^T$$

Step 4. Apply inverse IWT on all four sets of sub-bands

$$X^W = IWT^{-1}$$

Step 4. At last signature generation and signature embedding is done into the watermarked image with the procedure

mentioned in below section

Robustness factor is different for each sub-band. As LL sub-band contain more information robustness factor should be

more than other sub-bands(HL,LH & HH).

Watermark Extraction Process

Step 1. Check the received image to authenticate against attack or false positive problem by signature extraction and matching.

Step 2. Step 2. Apply 1-level IWT Add watermark image to the singular values of each sub-bands and again perform SVD on modified singular value.

$$S_i + \alpha W = U_i^W S_i^W V_i^{TW}$$

Where represents robustness factor

Step 3. Now, change IWT coefficients for each sub-bands as

$$X_i modified = U_i S_i^W V_i^T$$

Step 4. Apply inverse IWT on all four sets of sub-bands

$$X^W = IWT^{-1}$$

Step 4. At last signature generation and signature embedding is done into the watermarked image with the procedure mentioned in below section

3.2. Authentication Process

Proposed method also incorporates content authentication by producing the signature for the watermarked image utilizing the common mystery key (generation of Signature) and embedded it on the watermarked image in the sender side (signature installing) and the same is checked by contrasting the separated signature and the evaluated signature at the beneficiary side (Signature confirmation). On the off chance that matches found, the got watermarked image is validated, start watermark extraction (Watermark Extraction) else unauthenticated one, No extraction procedure. Ganeshan K.[] proposed a signature generation procedure with the

combination of IWT, Hilbert transform and PCA. We are using SVD in place of Hilbert transform to reduce additional computation requirement for PCA.

Signature generation and embedding procedure

Digital Signature for the watermarked image can generated using following steps:

Step 1. Compute Hash Value for the image using SHA-1 as,

DigSign = SHA-1

Step 2. Divide the DigSign into two equal parts as $DigSign_1$ and $DigSign_2$. In case off odd numbers leave last element.

Step 3. Now, grouping the Digital signature values of two haves using XOR operation as,

New_{DigSin}=XOR($DigSign_1$,$DigSign_2$)

Step 4. Select the secret key and XOR secret key with $New_{DigSign}$

$PreFinal_{DigSin}$=XOR(Secret key,New_{DigSin})

Step 5. Select the first eight bits of the $PreFinal_{DigSign}$ of authentication purpose. Which is represented as $Final_{DigSign.}$

Step 6. Apply 1-level DWT on the watermarked image and divide LL sub-band into 8X8 blocks.

Step 7. SelectDivided blocks randomly by secret key and perform SVD for each block.

Step 8. Multiply $U_{2,1}$ by 1o and round it to the nearest integer represented as U_i.

Step 9. Check following criteria based on $Final_{DigSign.:}$

If U_i is even and the $Final_{DigSign}$bit is 1, or U_i is odd and the $Final_{DigSign}$bit is 0, increase $U_i$by one and divide the result by 10. Otherwise keep unchanged. Modify the $U_{2,1}$based on result of above step.

Step 10. Conduct inverse SVD for all divided blocks and then conduct inverse DWT

Signature extraction

Step 1. Apply 1-level DWT on the watermarked image and divide LL sub-band into 8X8 blocks.

Step 2. SelectDivided blocks randomly by secret key and perform SVD for each block.

Step 3. Check the $U_{2,1}$based on following criteria,

$$Final_{DigSign}(i) = \begin{cases} 1 & mod\left(\lfloor \frac{U_{2,1}}{10} \rfloor, 2\right) == 0 \\ 0 & otherwise \end{cases}$$

Where i=1,2,…….8 length of signature.

Step 4. Compare, the generated signature with the extracted one as,

result = compare ($Final_{DigSign}$, $Final_{DigSign}$)

Step 5. If result is TRUE,

Received image is authenticated and can proceed with the extraction process Else, received image is unauthenticated and no extraction process.

4.RESULT AND DISCUSSIONS

The proposed hybrid method is implemented in MATLAB. In this segment, a few tests are done to assess the execution of the proposed watermarking plan. Basic gray-level images like lena, mandrel and peppers are used as cover images with the dimension of 512x512.Watermark images of copyright and cameraman are used with the size of 512x512. Fig 1 demonstrates the watermarked pictures at various limit values. See that there is no visual contrast between the first picture and the watermarked pictures; hence, this guarantees the devotion of the proposed strategy. Notwithstanding visual examination of the watermarked pictures, the PSNR (Peak Signal-to-Noise Ratio) of below equation is utilized as a measure of the quality of a watermarked image.

$$PSNR = 10.\log_{10}\frac{255^2}{MSE}$$

Where MSE is mean square error and can be calculated by the equation

$$MSE = \frac{1}{WH}\sum_{i}^{W}\sum_{j}^{H}(x_{ij} - x'_{ij})^2$$

Where W and H represents the width and height of the image. is the value of pixel in original image at the coordinate (i,j) and is the value of pixel the watermarked image at the coordinate (i,j). Table 1 shows the comparison of proposed method with other methods.

Table-1 comparative result

Method	RDWT–SVD[13]	DWT-SVD[10]	Proposed Method
PSNR	38.52	34.42	43.065

(a) (b) (c)

Fig- 3: Output of watermarking process (a) Input Cover Image (b) Watermarking Image (c) Watermarked Image

Authentication mechanism using signature embedding and extraction makes proposed method more secure in

attacks. Good PSNR compared to previous methods proves the imperceptibility of the proposed method. Optimal capacity of the proposed method proves as 256x256 size of the watermark image can be embedded into the 512x512 size image.

5. CONCLUSION

In this paper, we have exhibited a robust image watermarking scheme based on DWT, IWT and SVD. Here, we presented additional validation system, which tests the received content for its authenticity by the comparison of generated digital signature with extracted digital signature from the watermarked image. On the machinating on the signatures extraction process is performed otherwise not. Because of this, method is robust against various attacks. Due to the optimal use of IWT and SVD, imperceptibility of Watermarked image is good.

REFERENCES

[1] A. Koz, Digital watermarking based on human visual system, Master's thesis, Dept. of Electrical and Electronics Engineering, Orta Dogu Teknik University, 2002.

[2] E.T. Lin, et al., Video and Image Watermark Synchronization, Center for Educa-tion and Research in Information Assurance and Security, 2005.

[3] I. Cox, M. Miller, J. Bloom, J. Fridrich, T. Kalker, Digital Watermarking and Steganography, 2nd ed., Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2007.

[4] W. Sweldens, The lifting scheme: aconstruction of second generation wavelets, SIAM J. Math. Anal. 29(2) (1998) 511–546.

[5] A. Calderbank, I. Daubechies, W. Sweldens, B.L. Yeo, Wavelet transforms that map integers to integers, Appl. Comput. Harmon. Anal. 5(3), 332 – 369, 1998.

[6] Q, Su. Y. Niu, X. Liu, Y.Zhu, A blind dual color images watermarking based on IWT and state coding, Opt. Commun, 285(7), 1717 – 1724, 2012.

[7] W. Sweldens, The lifting scheme: a construction of second generation wavelets, SIAM J. Math. Anal. 29(2), 511-546, 1998.

[8] V. Aslantas, L. A. Dog˘an, and S. Ozturk, "DWT-SVD based image watermarking using particle swarm optimizer," in Proc. IEEE Int. Conf. Multimedia Expo, Hannover, Germany, 2008, pp. 241–244.

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

[10] E. Ganic and A. M. Eskicioglu, "Robust DWT-SVD domain image watermarking: Embedding data in all frequencies," in Proc. WorkshopMultimedia Security, Magdeburg, Germany, 2004, pp. 166–174.

[11] I. Daubechies, W. Sweldens, Factoring Wavelet Transforms into lifting steps, J. Fourier Anal. Appl. 4(3), 245- 267, 1998.

[12] Hongqin Shi, Fangliang Lv† & Yiqin Cao, "A Dual Color Image Watermarking Scheme Based on Non-overlapping Blocks with Circulation" ACADEMY PUBLISHER JOURNAL OF COMPUTERS, VOL. 9, NO. 8, AUGUST 2014 pp 1871-1880.

[13] S. Lagzian, M. Soryani, M. Fathy, Robust watermarking scheme basedon RDWT–SVD: embedding data in all subbands, in: International Symposium on Artificial Intelligence and Signal Processing (2A0I1S1P,)p,p.48– 52.

[14] Hongqin Shi, Fangliang Lv & Yiqin Cao "A Dual Color ImageWatermarking Scheme Based on Nonoverlapping Blocks with Circulation" JOURNAL OF COMPUTERS, VOL. 9, NO. 8, A20U1G4U. ST

[15] U. Gokhale, Y. Joshi, Asemi fragile watermarking algorithm based on SVD–IWT for image authentication, Int. J. Adv. Res. Comput. Commun. Eng. 1(4) (2012).

[16] Neha Solanki, Sanjay K. Malik, "ROI Based Medical Image Watermarking with Zero Distortion and Enhanced Security," I. J. Modern Education and Computer Science, pp. 4048, October 2014.

[17] Pameli Mukherjee, Saurabh Mitra, "A Review on CopyMove ForgeDreytection Techniques Based on DCT and DWT," International Joof uCronmalputer Science and Mobile Computing, vol. 4, issue 3, pp. 7028, March 2015.

[18] Khaled Loukhaoukha, Ahmed Refaey, Khalil Zebbiche and MakrNamabti,"On the Security of Robust Image Watermarking Algorithm boansDeidscrete Wavelet Transform, Discrete Cosine Transform and Singular Value Decomposition," International Journal of Applied Mathematics and Information Sciences, pp. 11591166.

[19] A. Koz, Digital watermarking based on human visual system, Master's thesis, Dept. of Electrical and Electronics Engineering, Orta Dogu Teknik University, 2002.

[20] E.T. Lin, et al., Video and Image Watermark Synchronization, Center for Educa-tion and Research in Information Assurance and Security, 2005.

[21] I. Cox, M. Miller, J. Bloom, J. Fridrich, T. Kalker, Digital Watermarking and Steganography, 2nd ed., Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2007.

[22] W. Sweldens, The lifting scheme: aconstruction of second generation wavelets, SIAM J. Math. Anal. 29(2) (1998) 511–546.

[23] A. Calderbank, I. Daubechies, W. Sweldens, B.L. Yeo, Wavelet transforms that map integers to integers, Appl. Comput. Harmon. Anal. 5(3), 332 – 369, 1998.

[24] Q, Su. Y. Niu, X. Liu, Y.Zhu, A blind dual color images watermarking based on IWT and state coding, Opt. Commun, 285(7), 1717 – 1724, 2012.

[25] W. Sweldens, The lifting scheme: a construction of second generation wavelets, SIAM J. Math. Anal. 29(2), 511-546, 1998.

[26] V. Aslantas, L. A. Dog˘an, and S. Ozturk, "DWT-SVD based image watermarking using particle swarm optimizer," in Proc. IEEE Int. Conf. Multimedia Expo, Hannover, Germany, 2008, pp. 241–244.

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

[28] E. Ganic and A. M. Eskicioglu, "Robust DWT-SVD domain image watermarking: Embedding data in all frequencies," in Proc. WorkshopMultimedia Security, Magdeburg, Germany, 2004, pp. 166–174.

[29] I. Daubechies, W. Sweldens, Factoring Wavelet Transforms into lifting steps, J. Fourier Anal. Appl. 4(3), 245- 267, 1998.

[30] Hongqin Shi, Fangliang Lv† & Yiqin Cao, "A Dual Color Image Watermarking Scheme Based on Non-overlapping Blocks with Circulation" ACADEMY PUBLISHER JOURNAL OF COMPUTERS, VOL. 9, NO. 8, AUGUST 2014 pp 1871-1880.

[31] S. Lagzian, M. Soryani, M. Fathy, Robust watermarking scheme basedon RDWT–SVD: embedding data in all subbands, in: International Symposium on Artificial Intelligence and Signal Processing (2A0I1S1P,)p,p.48– 52.

[32] Hongqin Shi, Fangliang Lv & Yiqin Cao "A Dual Color ImageWatermarking Scheme Based on Nonoverlapping Blocks with Circulation" JOURNAL OF COMPUTERS, VOL. 9, NO. 8, A20U1G4U. ST

[33] U. Gokhale, Y. Joshi, Asemi fragile watermarking algorithm based on SVD–IWT for image authentication, Int. J. Adv. Res. Comput. Commun. Eng. 1(4) (2012).

[34] Neha Solanki, Sanjay K. Malik, "ROI Based Medical Image Watermarking with Zero Distortion and Enhanced Security," I. J. Modern Education and Computer Science, pp. 4048, October 2014.

[35] Pameli Mukherjee, Saurabh Mitra, "A Review on CopyMove ForgeDreytection Techniques Based on DCT and DWT," International Joof uCronmalputer Science and Mobile Computing, vol. 4, issue 3, pp. 7028, March 2015.

[36] Khaled Loukhaoukha, Ahmed Refaey, Khalil Zebbiche and MakrNamabti,"On the Security of Robust Image Watermarking Algorithm boansDeidscrete Wavelet Transform, Discrete Cosine Transform and Singular Value Decomposition," International Journal of Applied Mathematics and Information Sciences, pp. 11591166