An Efficient Secure Image Watermarking Using Wavelet Transform

*J.S. LeenaJasmine, **L. Prabha

**Senior Grade Assistant Professor, ** PG Scholar*

Velammal Engineering College, Chennai

Abstract: Watermark is an invisible signature embedded inside an image to show authenticity or proof of ownership. The watermark pattern owner wants to keep their watermark patterns private during the watermark detection. In this paper, Lifting Wavelet Transform(LWT) technique is used for secure watermark detection. The Lifting Wavelet Transform(LWT) technique embeds ownership information into the host contents without degrading the perceptual quality of the host contents. Mainly this algorithm progresses the Peak to Signal Noise Ratio than the existing Discrete Cosine Transform(DCT) technique. Simulation results demonstrate the feasibility of the digital watermarking algorithms for use in multimedia standards. Our speculative analysis and new results show that secure watermark in the Compressive Sensing domain is possible. The experimental result shows that the proposed methods provides improved PSNR ratio.

Keywords: Digital Watermarking, Wavelet Transform, LWT, PSNR, Copyright Protection.

I. INTRODUCTION

Watermarking is a digital signal or pattern inserted intoa digital image or video or audio or software. Digital Watermarking is the process that embeds data called a watermark into a multimedia object such that watermark can be embedded or extracted later to make an assertion about the object. At the time of inserting the watermark into image some additional information is kept. This information contains identifiers of the owner, recipient,contractdates,consecutive numbers etc. which plays a great important role in adding values to watermarking products [1]. The types of watermarking are 1) Image watermarking 2) Video watermarking 3) Audio watermarking 4) Text watermarking. Image Watermarking based on human perception is divided into two types i) Visible watermark ii) Invisible watermark. Visible watermark is the secondary transparent covered into the primary image. The watermark app ars visible to a spontaneous viewer on a careful scrutiny. If the watermark given to the image is visible or perceptible then it is called visible watermark. The invisible watermark is embedded in such a way that change made to the pixel value is perceptually not observed and it can be recovered only with suitable decoding materials [2]. If the watermark is perceptible by human being then it is called invisible watermarking. In order to give an invisible watermark to an image the least significant bits of the pixels are reformed. The process of inserting watermark into multimedia object in such a way that the watermark can be detected or extracted later easily to make an assertion about the object and its owner's is called digital watermarking[2].

II EXISTING SYSTEM

According to Qia Wang et.al, Privacy is one of the critical issue once the data owners outsource data storage or processing to a third party computing service, such as the cloud. The author's recognized a cloud computing application scenario that requires concurrently performing secure watermark detection and privacy preserving multimedia data storage [1]. They also had proposed a compressive sensing (CS)-based framework using secure multiparty computation (MPC) protocols to report such a necessity. In order to protect the privacy, the multimedia data and secret watermark detection pattern are existing to the cloud for secure watermark detection in a CS domain in their framework. Throughout CS transformation, the privacy of the CS matrix and the watermark pattern is protected by the MPC protocols beneath the semi-honest security model. The correctness of the derived performance has been authenticated by their experiments. Thus speculative analysis and new results show that secure watermark detection in the CS domain is possible. Framework can also be extended to other common secure signal processing and data-mining applications in the cloud.

According to this paper, Wenjun propose a ROI image watermarking algorithm for hiding secrete information in key image. The ROI information is segmented and extracted in original image, and then gray value match is made in that region to generate the disguised cover image, in which the ROI image encrypted by disorder is embedded based on lifting wavelet transform. Tests show that the proposed watermarking scheme is of huge hiding information capacity as well as high inaudibility and robustness against various signals processing such as cropping, JPEG compression and noise attack. This algorithm has significantreal value of information security to the transmission of vital image such as isolated sensing, SAR images [3].

According to Zeng Fellow, A blind robust gray scale watermarking system that fights geometric attacks is proposed. Initially, 1-level lifting wavelet transform (LWT) is achieved on the cover image. The twisted gray scale watermarking image and the integral wavelet coefficients of the watermarking image are decoded into binary bits, which are then embedded into the corresponding frequency domains of the cover image according to perceptual importance. Secondly, to predict the geometric transformation parameters of the attacked image, low order Tchebichef moments as eigenvectors and an improved back propagation (BP) neural network are used to construct the predicting model, by which the attacked image can be geometrically corrected. Lastly the watermarking is extracted from the corrected image. Model results show that the proposed scheme is robust to both conservative signal processing and general regular attacks [4].

According to N.A. Weiss, A robust and secure technique is required to protect multimedia data as it can be easily produced as prohibited copies. Digital watermarking is used for Logical Property Rights protection and verification. In this paper, a lossless watermarking scheme based on Integer wavelet transform (IWT) and singular value decomposition (SVD) is implemented. The watermark image is inserted on the fundamentals of singular values of the low-low (LL) Sub band of original image. The Integer Wavelet Transform is implemented based on lifting scheme which is computationally efficient than Discrete Wavelet Transform. The watermark image is extracted which is highly correlated with the original watermark image. The proposed algorithm is robust and authenticated under different attacks [5].

According to Akio Miyazak, They propose a new Watermarking method for images using the lifting wavelet transform. Utilizing the Watermarking method they divide the watermarked content into watermark and original content perfectly after watermark detection and realize the digital watermarking for multimedia contents like medical images , electric documents, computer programs and data etc for which it is desired to restore the original content from watermarked on [6].

III METHODOLOGY

Lifting wavelet is the second generation fast wavelet transform. Translation and dilation are not fundamental for obtaining lifting wavelets. Up and down sampling is replaced simply by split and merge at each level during lifting wavelet transformation. In comparison with general wavelets, reconstruction of image by lifting wavelet is good since, it increases smoothness and decreases aliasing effects. Wavelet simplifies the frequency space relation[10]. Employing LWT reduces loss in information, increase the robustness of watermark and increases intactness of embedded watermark in the image. Watermark can be divided into 3 groups they are i) Robust ii) fragile iii) semi fragile [7]. The main motivation of this work is to provide a robust digital signature watermarking, using joint approach comprising of lifting wavelet transform to protect images against attacks and authenticate ownership of image without degrading the quality of image. LWT algorithm is spread spectrum, semi blind and non-invertible [8]. It also achieves higher robustness and improved fidelity, which is one of the important challenges of the watermarking. For example, in the video indexing application, evaluating the robustness of a watermarking scheme to any signal processing is meaningless, since there is no case that the video passes through some signal processing operation. In the concealed communication application, it is well to use a watermarking scheme that does not need the original data during the watermark detection process, if real TV broadcasting is used as the communiqué channel, while most of the watermarking systems in other applications need the original data during the detection process. If the presentation is the copyright protection, the owner of the original data may wait for several days to insert/detect watermark, if the data is valuable for the owner. On the other hand, in a broadcast observing presentation, the speed of the watermark detection algorithm should be as fast as the speed of real time broadcasting. As a result, each watermarking presentation has its own requirements and the efficiency of the watermarking scheme should be evaluated according to these requirements. The lifting scheme is a simple method for designing customized biorthogonal wavelets deal several advantages they are, 1) permits a faster implementation of the wavelet transform, 2) Keeps storage by providing an in- place calculation of the wavelet Transform, 3) Abridges determining the inverse wavelet transform, 4) Provides a usual way to say and think about wavelets. Watermarking is strictly related to steganography in which they are equally concerned with secret communication and belong to a broader subject known as information hiding [9].

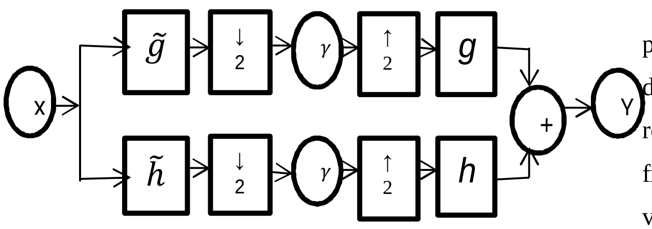

Fig. 1 Principle of lifting scheme

The Principle of Lifting Scheme is shown in the above figure 1.

The poly phase matrix is a matrix of Laurent polynomials and since we demanded that its determinant be equal to 1, we know that the filter pair (h, g) is complementary. The lifting theorem now states that any other finite filter g^{new}complementary to h is of the form

$$g^{new}(z) = g(z) + h(z)s(z^2)$$

where, $s(z^2)$ is a Laurent polynomial.[11]

IV PROPOSED SYSTEM

The proposed system of Secure Image Watermarking using Lifting Wavelet Transform is shown in figure 2

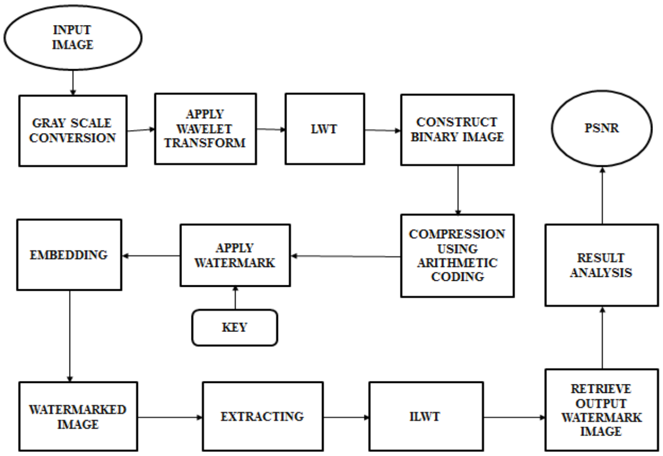

Fig. 2 Block diagram of LWT

A WAVELET TRANSFORM

In this paper, Lifting Wavelet Transform Technique is proposed and in the first level the wavelet transform decomposes the signal into windows of different resolutions. The wavelet transform is one of the tool for figure up functions, operators, or data into components of various frequency . In the initial stage the input image is selected, image had better be transformed into an Gray

Scale Conversion image. On applying the wavelet transformation technique, binary images are constructed in 5th bit coefficient of CH, CV and CD.

The 2 D LWT image split the image into four sub bands LH, HL, HH (LH- Horizontal Edge Data, HL- Vertical Edge Data, HH- Diagonal Edge Data. This LWT watermarking can embed only in HL, LH, HH sub bands then by selecting the sub bands threshold frequency is noted.

BEMBEDDING THE WATERMARK

After 1st-level LWT decomposition, both ROI image and cover image are decomposed into *LL*1, *LH*1,*HL*1. The sub-bands coefficients of ROI image are respectively embedded into the corresponding sub-bands of the cover image. Before embedding, the threshold coefficient should be set according to the length of the scrambling binary sequence, and then use the threshold to select important coefficients and their location, which are saved as the key.

CEXTRACTING THE WATERMARK

The secret file, generated in embedding, is necessary for extracting process. The file accounts the decomposition level, embedding location, coding length of sub-band coefficients and chaotic sequence key. The extracting process is the inverse of embedding process. Firstly, decompose the watermarked image and use LWT to obtain the coefficient matrix of low and middle frequency bands.

DGRAYSCALE CONVERSION

In Pre-Processing step we are going to convert the original color image into gray scale images. In Lifting Wavelet Transformation only gray scale images are used. So we going to convert it from RGB to gray scale images and improve the image enhancement process.

The size of the image requisitebe same as original image and converted output gray image.

EAPPLY LWT TRANSFORMATION

LWT2 performs a 2-D Lifting Wavelet decomposition with respect to a particular Lifted Wavelet that we specify. CA, CV, CH, CD computes the approximation coefficient matrix CA and detail coefficient matrices CH, CV, and CD obtained by a Lifting Wavelet Decomposition of the matrix X. W is the lifted wavelet name.

F INVERSE 2D LIFTING WAVELET TRANSFORM

ILWT2 performs a 2D lifting wavelet reconstruction with respect to the particular lifted wavelet that we specify.

G APPLY IMAGE WATERMARKING

Watermarking is the process of inserting predefined patterns into multimedia data in a way that the degradation of quality is minimized and remain at an imperceptible level. Digital watermarking algorithms have been proposed in spatial and transform domains. The spatial domain technique still have rather low-bit capacity and are not strong enough to lossy image compression and other image processing operations.

V EXPERIMENTAL RESULTS

The experimental result shows an improved amount of PSNR ratio, fig a) shows how to load an input image. fig b) show to load an watermarked image. Fig c) in the third step the watermarking technique is applied. The comparison of PSNR ratio is shown in table 1.

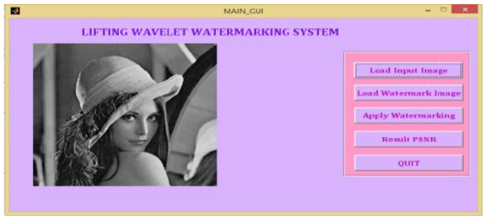

Fig. 3To load an input image.

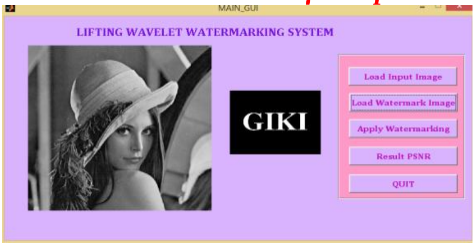

Fig. 4 Load Watermark image.

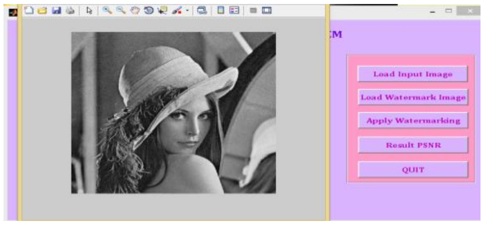

Fig. 5 Apply Watermarking

TABLE 1.COMPARSION OF PSNR RATIO.

S.NO	TECHNIQUE	PSNR
EXISTING SYSTEM	DISCRETE COSINE TRANSFORM(DCT)	32 dB
PROPOSED SYSTEM	LIFTING WAVELET TRANSFORM(LWT)	42 dB

From Table 1 our proposed method Lifting Wavelet Transform provides better PSNR ratio than the existing Discrete Cosine Transform Technique.

VI CONCLUSION

The work in this paper, mainly focus on to provide a good tradeoff between perceptual quality of watermarked image and its robustness to different attacks. Here we have discussed a digital watermarking algorithm in Lifting Wavelet Transform (LWT) by incorporating contrast sensitivity based on Compressive Sensing domain. This Watermarking is useful in real time application since split and merge process in LWT reduces complexity by 50%. Hence the loss in information is also less when compared with the existing system.The experimental result shows that the proposed technique increases the Peak-to-Signal-Noise Ratio (PSNR) than the existing techniques.

VII REFERENCES

[1] Qia Wang, "*A Compressive Sensing based Secure Watermark Detection and Privacy Preserving Storage Framework*", IEEE Trans. On image processing, vol.23, No. 3,March 2014.

[2]MitraAbbasfard, "*Digital Image Watermarking Robustness: A Comparative Study*". MSc Thesis, June 2009.

[3]DashunQue, "A ROI Image Watermarking Algorithm based on Lifting Wavelet Transform", ICSP2006 Proceedings, may 2006.

[4]GuangyongGao, GuopingGiang, "Gray Scale Watermarking Resistant To Geometric Attacks Based On Lifting Wavelet Transform And Neural Network", Proceedings of the 8th World Congress on Intelligent Control and Automation, June 6-9 2010.

[5] A.Kala, K. Thaiyalnayaki, "Robust Lossless Image Watermarking in Integer Wavelet Domain using SVD", IJCSE Vol. 2No.02 March 2013.

[6] Akio Miyazaki, "An Image Watermarking Method using Lifting Wavelet Transform", ISPACS, March 2006.

[7] Chaw-Seng Woo, "Digital Image Watermarking Methods for Copyrright Protection and Authentication", Information Security Institute Faculty of Information Technology Queensland University of Technology, March 2007.

[8] Sushma G Kejgir, Manesh Kokare, "Lifting Wavelet Transform with Singular Value Decomposition for Robust Digital Image Watermarking", International Journal of Computer Applications, Vol. 39, No. 18, February 2012.

[9]NatasaTerzija, "Robust Digital Image Watermarking algorithms for Copyright Protection",Oct 2006.

[10] Alexandre Panquet, "Wavelet Packet-based Digital Watermarking for Image Authentication", Department of Electrical and Computer Engineering, July 2002.

[11] (C) C.Valens, "The Fast Lifting Wavelet Transform", 1999-2004.

[12]Keys R. G, "Techniques and Applications of digital watermarking and content protection," IEEE Trans. on Acoustic, Speech, and Signal Processing, Dec 1981, vol. ASSP-29, no. 6, pp. 1153-1160.

[13] Kim C, Kim L. S, Lee J. A, and Seong S. M, "Special issue on signal processing for data hiding in digital media secure content delivery", IEEE Trans. Circuits Syst. Video Technol. , June 2003, vol. 13, no. 6, pp. 549-553.

[14] Marco Aurelio, Miguel O. Arias-Estrada, Nuno-Maganda,"Digital watermarking for DVD video copy protection", IEEE, International Conference on Reconfigurable Computing and FPGAs, 2005

[15] Wang Q and Ward R. K, "Image Adaptive Watermarking using wavelet transform" ,IEEE Trans. Image Process., Apr. 2007, vol. 16, no. 4, pp. 889-900.