

Different Digital Watermarking Techniques for Secure Data Transmission

Evline.J.Alappatt^{#1}

Master Of Technology

Computer Science And Engineering

*Sahrdaya college of Engineering And Technology
Calicut University, Kerala*

JsameyDavies^{#2}

Assistant Professor

Computer Science And Engineering

*Sahrdaya college of Engineering And Technology
Calicut University, Kerala*

Vince Paul^{#3}

Head Of the Department

Computer Science And Engineering

*Sahrdaya college of Engineering And Technology
Calicut University, Kerala*

Mr.Sankaranarayanan P.N^{#4}

Assistant Professor

Computer Science And Engineering

*Sahrdaya college of Engineering And Technology
Calicut University, Kerala*

Abstract— Watermarking is a technique for labelling digital pictures by hiding secret information in the images. A digital watermark is a kind of marker covertly embedded in a noise tolerant signal such as audio or image data. It is typically used to identify ownership of the copyright of such signal. An original image is decomposed into wavelet coefficients. Then, multi-energy watermarking scheme based on the qualified significant wavelet tree (QSWT) is used to achieve the robustness of the watermarking. Unlike other watermarking techniques that use a single casting energy, QSWT adopts adaptive casting energy in different resolutions. In conventional watermarking schemes certain amount of distortion to the recovered image is acceptable. This does not apply to all applications, particularly in military applications, space and medical imagery etc., loss of a single bit of information from the original image is not acceptable. In reversible watermarking, the embedding process has an additional burden of embedding extra information in the payload that includes the recovery data that is used by the decoder to reconstruct the original image bit by bit. Various lossless watermarking schemes are discussed in this paper.

Keywords— Digital watermark, Discrete Wavelet Transform, Qualified wavelet coefficients.

I. INTRODUCTION

The success of the Internet allows for the prevalent distribution of multimedia data in an effortless manner. Due to the open environment of Internet downloading, copyright protection introduces a new set of challenging problems regarding security and illegal distribution of privately owned images. One potential solution for

declaring the ownership of the images is to use *watermarks*. Watermarking is a technique for labelling digital pictures by hiding secret information in the images. The studying key point is that the embed information can neither be removed nor decoded without the required secret keys. Indeed, there are a number of desirable characteristics that a watermarking technique should exhibit. That is, a watermarking technique should at least respect the following requirements.

- **Readability:** A watermark should convey as much information as possible. Moreover, retrieval of the digital watermark can be used to identify the ownership and copyright unambiguously.
- **Security:** A watermark should be secret and must be undetectable by an unauthorized user in general.
- **Imperceptibility:** The digital watermark should not be noticeable to the viewer.
- **Robustness:** The digital watermark is still present in the image after attacks and can be detected by the watermark detector, especially on the attacks from compression.

II. PRELIMINARIES

In this section, we first give a brief review of the wavelet representation of an image. We further outline qualified significant wavelet tree (QSWT) which is based on the definition of EZW.

A. Wavelet Transform of Images

The wavelet transform is identical to a hierarchical subband system, where the subbands are logarithmically spaced in frequency. The basic idea of the DWT for a two-dimensional image is described as follows. An image is first decomposed into four parts of high, middle, and low frequencies (i.e., $LL1, HL1, LH1, HH1$ subbands) by critically subsampling horizontal and vertical channels using subband filters. The subbands labeled $HL1, LH1$, and $HH1$ represent the finest scale wavelet coefficients. To obtain the next coarser scaled wavelet coefficients, the subband $LL1$ is further decomposed and critically subsampled. This process is repeated several times, which is determined by the application at hand. An example of an image being decompose into ten subbands for three levels is shown in Fig. 1. Each level has various bands information such as low-low, low-high, high-low, and high-high frequency bands.

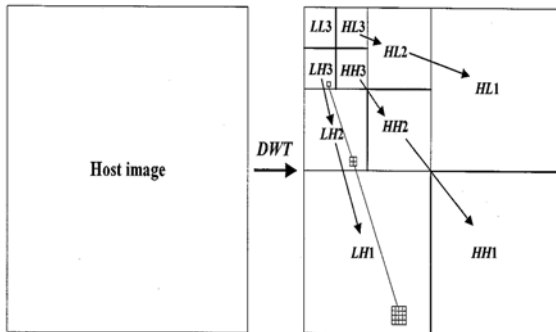


Fig. 1 DWT decomposition of an image

Furthermore, from these DWT coefficients, the original image can be reconstructed. This reconstruction process is called the inverse DWT (IDWT). If represents an image, the DWT and IDWT for can be similarly defined by implementing the DWT and IDWT on each dimension and separately. An original 512×512 Lena image and its DWT decomposition are shown in Fig. 2.

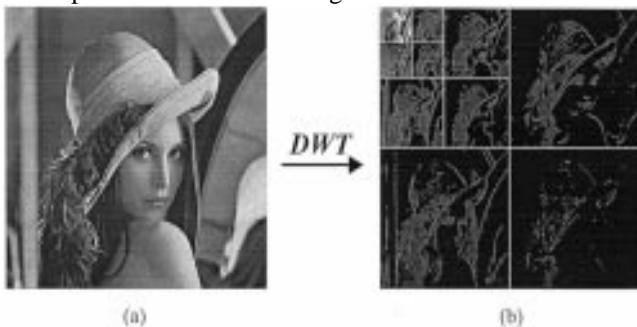


Fig. 2. A real case of DWT decomposition. (a) The original 512×512 Lena image (b)it's DWT decomposition

B. QSWT

In this section, coefficients with local information in the subbands are chosen as the target coefficients to be cast. The coefficients selection approach is based on the QSWT. QSWT is derived from EZW, and the basic definitions are given as follows. A parent-child relationship can be defined between wavelet coefficients at different scales corresponding to the same location. Excepting the highest

frequency subbands (i.e., $HL1, LH1$, and $HH1$), every coefficient at a given scale can be related to a set of coefficients at the next finer scale of similar orientation. The coefficient at the coarse scale is called the parent, and all coefficients corresponding to the same spatial location at the next finer scale of similar orientation are called children. For a given parent, the set of all coefficients at all finer scales of similar orientation corresponding to the same location are called descendants. A wavelet tree that descending from a coefficient in the subband $LH3$ is shown in Fig. 1.

III. WATER MAKING IN THE DWT DOMAIN

The proposed embedded digital watermarking can hide visually recognizable patterns in images. The goal of digital watermarking is invisible to human eyes but also robust under different attacks. In the proposed method, watermarks are redundantly embedded in the host image by modifying them in the location of QSWT coefficients. Note that we construct a QSWT for one of three pairs of subbands ($LH3, LH2$), ($HL3, HL2$), and ($HH3, HH2$). The visually recognizable watermark is the image of binary, gray image, or color image. Watermarking in the DWT domain includes two parts: embedding and extracting.

A. Watermark Embedding Method

To embed a watermark in the host image is shown below:

- Step 1:** In the embedding part, we first decompose an image into three levels with ten subbands of a pyramid structure as shown in Fig. 1
- Step 2:** Subband ($LH3, LH2$) is selected to be cast
- Step 3:** Next, we calculate the summation of coefficients of $QSWT[i]$.
- Step 4:** Sort the gray level of watermarks W in descending order.
- Step 5:** In the casting stage, watermarks W are redundantly embedded into subbands of $LH3$ and $LH2$ for robustness.
- Step 6:** Save the embedded position, subband label, then, we take the two-dimensional IDWT of the modified DWT coefficients and the unchanged DWT coefficients to form watermarked image.

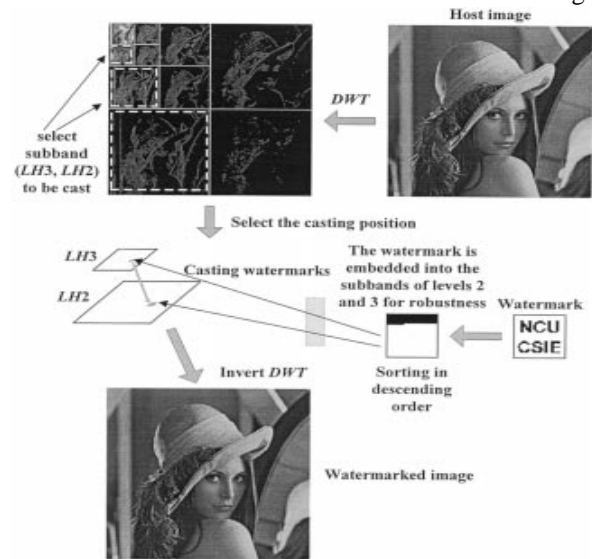


Fig3. Watermark Embedding Method

B. Watermark Extracting Method

On the other hand, the watermarks are detected by using the embedded position and scaling parameter after the wavelet decomposition of the watermarked image and the original image, as follows:

- Step 1) We first decompose a watermarked image and the original image with DWT into three levels of ten subbands.
- Step 2) We subtract the same index of coefficients of subband LH3 (or LH2) of Y by the coefficients of subband LH3 (or LH2) of Y' for the length of watermark.
- Step 3) After arranging the index of watermarks W', we have the extracted watermarks .
- Step 4) In our scheme, the extracted watermarks W' are a visually recognizable image.

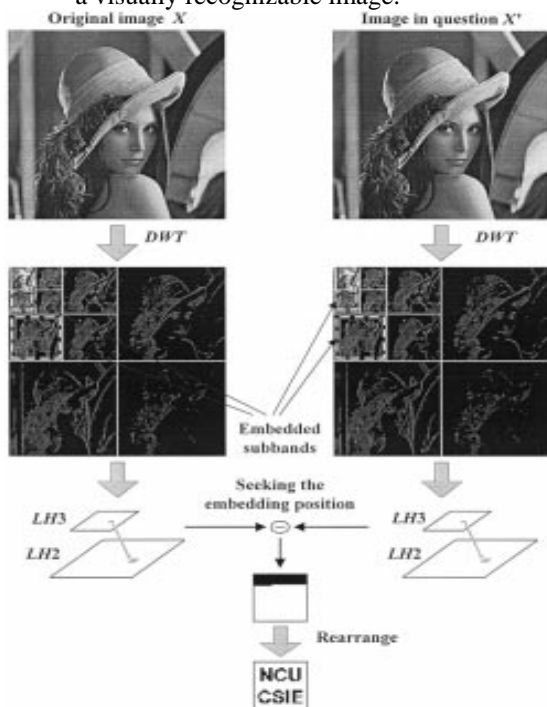


Fig4: Watermark Extracting Method

IV. BLIND WATER MARKING TECHNIQUE

A blind watermarking algorithm based on a qualified significant wavelet tree (QSWT) is proposed by Lin. In this method, the image is transformed into wavelet coefficients using three-level DWT, and the LH3 subband is considered to embed the watermark as it is more significant than the HL3, HH3, and LL3 subbands.

This technique is mainly based on the significant difference of wavelet coefficient quantization in which every seven non-overlapping wavelet coefficients of the host image are grouped into a block.

After a three-level DWT is applied in the input image frame n , wavelet subbands LH2 and LH3 are regenerated. The next step is to convert LH2 and LH3 to a set of smaller subblocks. $T1$ and $T2$ are acquired by calculating the mean of these subblocks in LH3 and LH2, respectively. For each coefficient at location $LH3(i, j, m)$ in subblock m , if it is greater than the threshold $T1(m) + D1$, the system will check if at least

three of its child coefficients ($LH1(2i - 1, 2j - 1, m)$, $LH1(2i - 1, 2j, m)$, $LH2(2i - 1, 2j - 1, m)$, and $LH2(2i, 2j, m)$) are greater than the threshold $(T2(m) + D2)$.

If they are, $LH3(i, j)$ will be set as one of the QSWTs (m). The coefficient values of the parent and all its children are summed. Then QSWT(m) will be sorted in decreasing order, and these trees are output. All coefficients that do not meet these two adaptive thresholds are discarded. The original image is transformed using three-level DWT. From the 10 bands obtained, LH3 is used to embed the watermark.

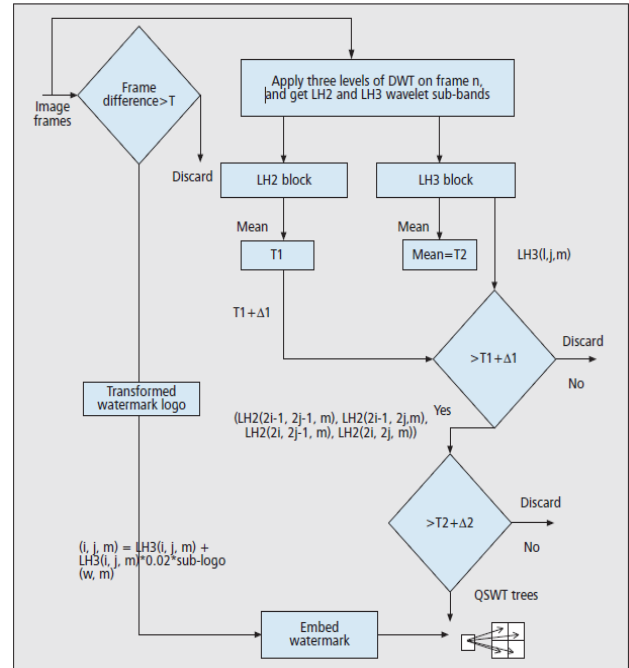


Fig5: Watermark Embedding Algorithm

A. Joint Design of Watermark Authentication and Error Correction Codes for Media Cloud

The number of parity/redundant symbols that must be added to the message is determined by the amount of required capability of error corrections. The parity symbols must contain enough information to detect the values of the erroneous information symbols. While there are several forward error correction (FEC) techniques available, Reed-Solomon (RS) codes provide powerful correction with high channel efficiency. With the advent of very large-scale integration (VLSI) techniques, RS codes can be useful in both high and low data rate systems at low cost. The efficiency of RS codes is almost as the same as that of Hamming codes, except that RS codes deal with multibit symbols rather than individual bits. The main idea behind this work is to detect and extract the watermark data in which the watermarked data is subjected to noise caused by transmission. These noises might result in failure to detect watermarked data from the media cloud. The joint design mechanism could also extract more watermarking bits (higher robustness) than the general extraction algorithm. In the design, RS code plays an important role, extracting the watermarked bits, due to its ability to correct errors. For the joint design of RS and watermarking, two approaches have been considered. In the first method, the full watermarked image is given as input to an RS encoder. In the second method, only the LH3 band is given as input to

the RS encoder. After the process of detecting and correcting errors, we replace the LH3 obtained from the RS code in the original image, and apply inverse DWT to reconstruct the image. In this scheme, packets are discarded if they cannot be corrected due to the bit errors caused by the noise. There is a trade-off between the quality and RS code protection in general. For example, having more RS protection will improve the quality with increased redundancy.

V. LOSSLESS WATERMARKING TECHNIQUES

In traditional watermarking schemes, watermarking is performed by embedding a digital signal into a digital host signal resulting in watermarked signal. This process of embedding the watermark introduces certain amount of distortion into the host media and results in loss of imperceptibility resulting in reduction of Peak Signal-to-Noise Ratio (PSNR). For applications pertaining to military, space, medical, legal etc. even certain amount of distortion is not acceptable as it results in loss of signal fidelity.

Hence these applications require reversible watermarking, which care cover the original host signal perfectly after the watermark extraction. Reversible watermarking basically comes in two flavors.

The first type tests for underflow and overflow conditions prior to embedding the watermark and the second type of reversible watermarking schemes involves preprocessing of the source digital media content prior to embedding the watermark.

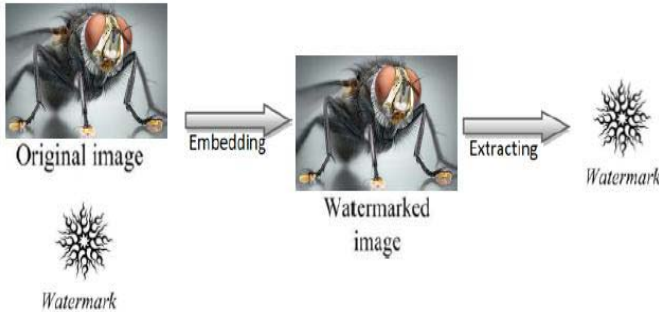


Fig6: Conventional Watermark Process

Various techniques of reversible watermarking are: Lossless Watermarking using Difference Expansion Tian presented a reversible data embedding approach based on expanding the pixel value difference between neighboring pixels, which will not overflow or underflow after expansion.

The difference is represented in binary form and right shifted by one bit to embed a single bit in the difference. The difference is said to be embeddable or changeable by substituting the LSB bit of the expanded difference with the watermark bit. The expanded difference should meet the overflow (pixels values > 255) and underflow (pixel values < 0) conditions. The original image is completely recovered from the watermarked images using reversible watermark embedding.

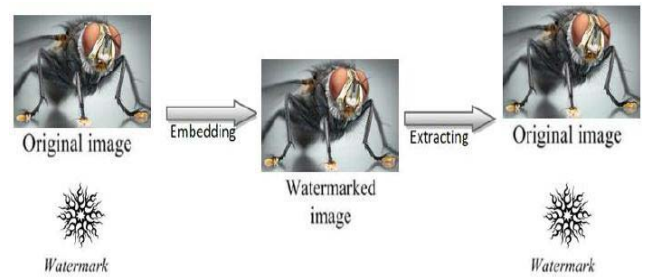


Fig7: Reversible Watermark Process

VI. CONCLUSIONS

The watermarking technique authenticates multimedia data from the media cloud. The embedding and extracting methods of the DWT based approach have been described. In the proposed method, the embedding schema takes the relationships of DWT coefficients and spatial information into consideration, and the desirable characteristics of a watermark could be exhibited. Wavelet transforms is a new time-frequency analyzing method to localize spatial and frequency domain. DWT based techniques are the most popular schemes used by researchers to embed the watermark into a source media in transform domain. Watermarks can be embedded within source media by modifying the transform domain DWT coefficients. These methods provide better robustness and quality as compared with methods of spatial domain. Reversible watermarking algorithms are attracting huge interest in recent times. Its key advantage is not only the secret data but also the host image can be accurately recovered during the extraction process. Because of this lossless feature it plays an important role in some specific scenarios such as military, medical diagnosis, law enforcement and so on, where the cover images must be accurately reconstructed after data extraction.

ACKNOWLEDGMENT

I express my deepest thanks to “Ms. Jasmy Davies” the mentor of the seminar for guiding and correcting various documents of mine with attention and care. She has taken the pain to go through the seminar and make necessary correction as and when needed. I also extended my heartfelt thanks to my family and well wishers.

REFERENCES

- [1] M.-S. Hsieh, D.-C. Tseng, and Y.-H. Huang, “Hiding Digital Watermarks using Multiresolution Wavelet Transform,” *IEEE Trans. Industrial Electronics*, vol. 48, no. 5, Oct. 2001, pp. 875–82
- [2] Security Protection between Users and the Mobile Media Cloud. Honggang Wang, University of Massachusetts Shaoen Wu, Ball State University Min Chen, Huazhong University of Science and Technology Wei Wang, South Dakota State University.
- [3] Evaluation of Lossless Watermarking Techniques Dr. Smitha Rao M.S Reva Institute of Technology and Management Bangalore, India.
- [4] R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne, “A digital watermark,” *Proc. IEEE Int. Conf. Image Processing*, vol. 2, pp. 86–90, 1994.
- [5] W. R. Bender, D. Gruhl, and N. Morimoto, “Techniques for data hiding,” *Proc. SPIE: Storage and Retrieval of Image and Video Database*, vol. 2420, pp. 164–173, Feb. 1995.
- [6] N. Nikolaidis and I. Putas, “Copyright protection of images using robust digital signatures,” in *Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing*, vol. 4, May 1996, pp. 2168–2171.