HYBRID NONBLIND WATERMARKING BASED ON DWT FHT AND SVD

Kaviarasi.E, Mounika Suda.

Department of Electronics and Communication Engineering, Prince Shri Venkateshwara Padmavathy Engineering College, Tamil Nadu, India.

ABSTRACT

Watermarking the image files is an extremely proficient method used to the field of communication technology. When any information required to transmitting from one place to another security is vital. This security is provided by hiding data into the images, audio and video. It details about the different watermarking techniques gives the clear concept of the watermarking scheme. It proposed a digital watermarking technique which is based on hybrid watermarking. Using hybrid watermarking technique, watermark the image with another image it gives the watermarked image. Evaluate the performance of PSNR for watermarked image. Evaluating the three parameters of PSNR, MSE and SSIM for various types of attacks and the proposed watermarking technique is imperceptible. Explore the robustness of the proposed watermarking technique by evaluating the parameters of PSNR, MSE and SSIM.

Keyword: *Discrete Wavelet Transform, Singular Value Decomposition, Peak Signal to Noise Ratio (PSNR) and mean square value (MSE).*

1. INTRODUCTION

Watermarking is the solution for protect the copyright of multimedia data through Trans coding, because the embedded message is always included in the data. However, there is no evidence for the watermarking techniques can achieve the rights of owner information from the received data after all kinds of content-preserving manipulations. Because watermarks can only be embedded in a limited space in the multimedia data. There is always a biased advantage for the attacker whose target is only to get rid of the watermarks by exploiting various manipulations in the finite watermarking embedding space. Watermarking have the application on the image/video copyright protection.

1.1 Image Processing

Image processing is a physical process used to convert an image signal into a physical image. The image signal can be either digital to analog. The actual output itself can be an actual physical image or the characteristics of an image. The most common type of image processing is photography. In this process, an image is captured or scanned using a camera to create a digital or analog image. In order to produce a physical picture, the image is processed using the appropriate technology based on the input source type. In digital photography, the image is stored as computer file. This files translate using photographic software to generate an actual image. The colors, shading and nuances are all captured at the time. The photograph is taken and the software translates this information into an image. When creating images using analog photography ,the image is burnt into a film using a chemical reaction triggered by controlled exposure light .The image is process is decreasing in popularity due to the opening of digital photography ,which requires less effort and special training to produce images .

1.2 Digital Image Processing

This image may be defined as a two dimensional visual information are stored and displayed. An image is created by photosensitive devices which capture the reflection light from two dimensional surface of object in the three dimensional real in real world. Each image has intensity or gray value in x-y coordinate plane.

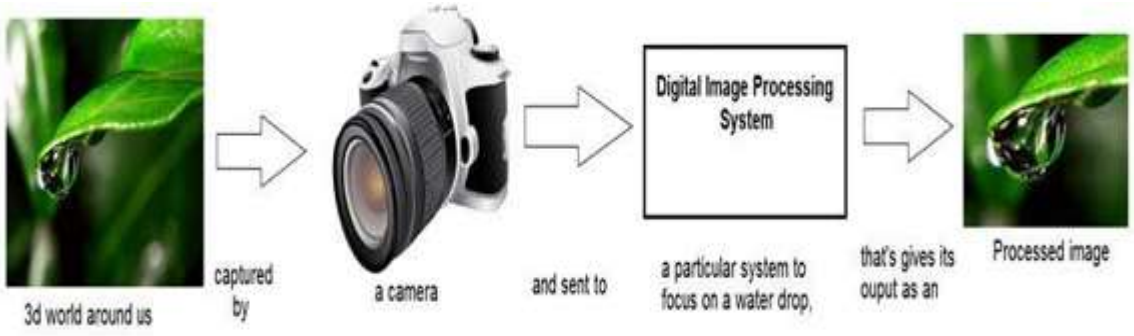


Figure 1 Image Processing

Digital image processing (DIP) has the different techniques for processing of digital images in figure 1 Manipulating data in the form of an image through several possible techniques. An image is usually interpreted as a two-dimensional array of brightness values, and is most familiarly represented by such patterns as those or a photographic print, slide, television screen, or movie screen. An image can be processed optically or digitally with a computer. To digitally process an image, it is first necessary to reduce the image to a series of numbers that can be manipulated by the computer. Each number representing the brightness value of the image at a particular location is called a picture element, or pixel. A typical digitized image may have 512*512 or roughly 250,000 pixels, although much larger images are becoming common.

1.3. Classification

Digital watermarking techniques are classified into various types. This classification based on several criteria in table 1.

S.no	Criteria	Classification
1	Watermark type	Noise and image
2	Robustness	Fragile, semi-fragile and robust
3	Domain	Spatial and frequency
4	Perceptivity	Visible and invisible watermarking
5	Host data	Image, text, audio and video
6	Data extraction	Blind, semi-blind and non-blind

Table 1 Types of watermarking basis of different Criteria

2. EXISTING SYSTEM

There are many resolutions that have been proposed like Cryptography, Steganography and Watermarking. The watermarking technique affords one of the best solutions among them. This technique embeds information so that it is not easily distinguishable to the others. The embedded watermark should not damage the quality of the image and should be perceptually invisible to maintain its protective secrecy. The robustness and perceptual quality of the watermarking done by using the DCT, DWT and SVD. Drawbacks are false positive problem, Diagonal line problem and PSNR is less.

2.1. Discrete Wavelet Transform

The DWT divides an image into four parts namely a lower resolution approximation component (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) detail components. The LL sub band is obtained after low-pass filtering both the rows and columns contains a rough explanation of the image. The HH sub band is high-pass filtered LH sub band contains mostly the vertical detail information which corresponds to horizontal edges. HL band represents the horizontal detail information from the vertical edges. The process can be repeated to obtain multiple 'scale' wavelet decomposition. Figure 1 shows the DWT decomposition. However, there are cases where the transformation is implemented using a block based approach to improve this problem. Because of these reasons, the wavelet based watermarking techniques are getting more significance. DWT is very useful to identify the areas in the host image where a watermark can be embedded commendably. This property allows

the exploitation of the masking effect of the human visual system. When a DWT coefficient is modified, the region corresponding to that coefficient alone is modified.

2.2. Singular Value Decomposition

The singular value decomposition is the proper tool for analyzing a mapping from one vector space into another vector space, possibly with a different dimension. Most systems of simultaneous linear equations fall into this second category. Any m by n matrix A can be factored in eq. (1)

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

Where U is orthogonal m by m matrix and the columns of the U are the eigenvectors of AA^T .Likewise, V is orthogonal n by n matrix and the columns of the V are the eigenvectors of A^TA.

The matrix S is diagonal and it is the same size as A. where its rank should followed by the stigmas like Eigen vectors.

$$AA^T = (USV^T)(VS^T U^T) = USS^T U^T \quad (2)$$

$$A^TA = VS^TSV^T \quad (3)$$

From eq. (2), U must be the eigenvector matrix for AA^T .The eigenvalue matrix in the middle is SS^T which is m by m with the eigenvalues $\sigma_1 = \sigma_2 \lambda_1 = \sigma^2_1$, . . .$\lambda_r = \sigma^2_r$ r on the diagonal. From eq. (3) V must be the eigenvector matrix for A^TA. The diagonal matrix S^TS has the same $\lambda_1 = \sigma^2_1$, $\lambda r = \sigma^2_r$, but it is n by n.an example of the density technique of the SVD process is obtained by a MATLAB code generation and flow diagram of SVD. This is calculated to determine the complexity of the block. Select greater convolution blocks using PRNG (pseudo random number generator) and also using the feature of D component. For each selected greater complexity block, in the first column of U, magnitude difference between the neighboring coefficients is calculated.

3. PROPOSED SYSTEM

The proposed Watermarking scheme is executed as in two phases first watermarking and then extraction. Apply the haar wavelet transform on the image and will get four sub band images. On sub band applying first FHT and on that FHT matrix we are going to apply SVD in all values. Then the watermarking step is performed by scaling down the pixel values of watermark and then embedding those values into the cover image. After this the watermarked image is attained on which various attacks are applied in order to achieve the robustness in watermarking. The extraction process where applying the wavelet transform, FHT and SVD and extract the watermark under attacks. Finally the correlation is determined between the watermark extracted and original watermark. Compensations of the proposed system is false positive problem is resolved, diagonal line problem is resolved and PSNR is good.

3.1Hadamard Transform

The Hadamard transform is also called Walsh transform or Walsh Fourier transform. Is an example for general class of Fourier transform, it performance orthogonal, symmetric, innovation, linear operation on 2^m real numbers, (or complex numbers, although the Hadamard matrices themselves are purely real) Hadamard matrices seem such simple matrix structures: they are square, have entries +1 or −1 and have orthogonal row vectors and orthogonal column vectors. The proposed Hadamard transform domain method is more robust again image/signal processing attacks. Elements of Hadamard transform matrices take only the binary value ±1.The Hadamard transform matrices, H_n are N x N matrices, where N=20n,n€1+

$$H_{2N} = \frac{1}{\sqrt{2N}} \begin{bmatrix} H_N & H_N \\ H_N & -H_N \end{bmatrix} \quad (4)$$

$$H_2{}^2 = \begin{bmatrix} H_2{}^1 & H_2{}^1 \\ H_2{}^1 & -H_2{}^1 \end{bmatrix} \quad (5)$$

$$H_2{}^2 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \quad (6)$$

Equation (5) provides the lowest order of the Hadamard matrix is 2 with the Hadamard matrices of dimension 2^k for K€N by recursive formula. Equation (6) gives the sequence Hadamard transform of matrix .the elements of the spectrum is different sequence components contained in the signal in a low to high order and reorder the rows based on the Hadamard sequence matrix .the conversion of sequence, into the equivalent index number in Hadamard order is a three-step method. (1) Represent in binary form (2) convert binary to gray code (3) bit reversal**.**

3.2 Blok Diagram

Block diagram are explain about the embedded and extraction process of watermarking in figure 1 and figure 2.

3.2.1Embedding process

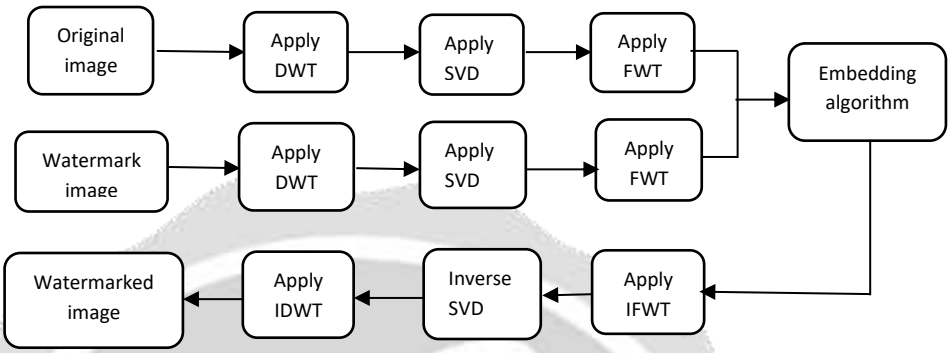


Figure 2 Block Diagram of Embedding Process

Before embedding the watermark in to the original image it will be transformed into coefficients by applying DWT, SVD and FHT. Original image also transformed into factors and then both are smeared to the embedding algorithm which is known as watermarked image, now inverse transforms are applied to obtain the frequency domain watermarked image as shown in figure 2 Selection of the coefficients to which a watermark is embedded is based on a predefined threshold and the watermark is cast into coefficients whose out-and-out values are greater than the threshold

3.2.1 Extraction Process

Watermark extraction process deals with the extraction of the watermark in the nonexistence of the original image as shown in figure 3. The purpose of the watermark extraction algorithm is to obtain the consistent an estimate of the original watermark from the watermarked image. The extraction process is inverse of the watermark embedding process. One of the benefits of watermarking is its ability to spread the watermark all over the image. If a part of the image is cropped, it may still contain parts of the watermark. These parts of watermark may be extracted by convinced appliance even if the image has been further scaled or rotate.

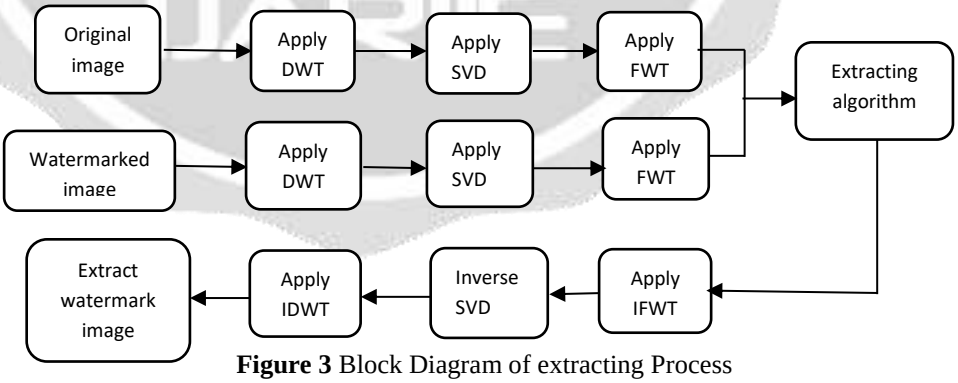


Figure 3 Block Diagram of extracting Process

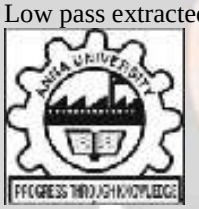
4. EXPERIMENTAL RESULT

In this paper the recreation process is implemented in MATLAB using different types of host and watermark images. For testing purpose gray scaled (JPEG format) image is used. The selected host (original) and watermark images are as follow. Figure 4 shows the embedding process.

Original image watermark image watermarked image

Figure 4 watermark embedding process

Table 2 contains the various Common signal processing techniques such as Low pass filtering, Median filtering and High pass filtering as well as geometrical attacks such as cropping is used for the exploration of the watermarked image. It explaining the watermarked image and extract image from after attacking process is applied.

watermarked image	**Extract image**	**Watermarked image**	**Extract image**
Low pass filter 	Low pass extracted logo 	Cropping attack 	Extracted cropping logo 
High pass filter 	High pass extracted logo 	Gaussian noise 	Gaussian noise Extracted logo 
Median filter 	Median filter Extracted logo 	DCT compression 	DCT extracted logo 

Watermarked image	**Extract image**	**Watermarked image**	**Extract image**
Block truncation compression 	Extracted logo 	Pyramid compression 	Extracted pyramid logo 

Table 2 Various Attacks in Watermark Image

4.2 PERFORMANCE ANALYSIS

Performance analysis shows crucial role in analyzing watermarked image and extracted watermark. Different statistical measures are used to analyze performance. The watermark robustness solely depends on the watermark embedding strength, which results in image visual degradation. These visual degradation are helpful in performance evaluation. Imperceptibility of watermarked image is qualitatively observed by analyzing visual artifacts. Various fictions has recommended many metrics. Following metrics are used for quantitative measure.

Notation used are enlisted below:

Im(i, j) : Original Image

Im (i, j)' : Watermarked Image

S : Size of image

- Mean Square Error (MSE)
  Original image and watermarked image metrics can be used for Computing Mean Square error using equation (7)

$$\mathrm{MSE} = \frac{1}{S}\sum_{i,j}(\mathrm{Im(i,j)} - \mathrm{Im'(i,j)})^2 \quad (7)$$

- Peak Signal to Noise Ratio (PSNR)
  PSNR value is calculated between original image and watermarked image. Perceptual quality is satisfactory if value of PSNR is more than 30DB.PSNR calculated from equation (8)

$$\mathrm{PSNR} = 10\log_{10}\frac{(255\times255)}{\mathrm{MSE}} \quad (8)$$

- Similarity Measure (SIM)
  Similarity measure is computed for assessment of extraction fidelity. It shows the similarity between extracted and embedded watermark. SIM is also known as Similarity Coefficient (SC). SC can be measured using equation (9)

$$\mathrm{SIM}(W_t, W_t') = \frac{\sum_i\sum_j w_t(i,j)w_{t'}(i,j)}{\sum_i\sum_j w_{t'}(i,j)^2} \quad (9)$$

4.3 Comparison of Performance Analysis

The performance of the watermarked image is analyzed using PSNR, MSE of the host image and the watermarked image. The similarity is used to define the robustness of the watermark which is compared between original logo and the extracted logo image. The proposed algorithm has been employed on 256x256 cover image. Some of the intrusions such as Gaussian noise are synchronized attacks while others such as cropping are biased numerical invasions. From the table (3) gives appraisal of different attacks. In that proposed PSNR value of watermarked image is increased (41.7682) when compare to the existing watermarked image of PSNR value (39.79). It provides the better performance of watermarked image and extracted watermarked image. Mean square error value is less for proposed watermarked image (4.3031) compare to the existing watermarked image (6.8421) of MSE value. Similarity is near 0 to 1 for both existing and proposed watermarked image.

Type of method		**Existing method**			**Proposed method**			
Types of hybrid transforms		**DWT-DCT-SVD**			**DWT-FWHT-SVD**			
Image before/after watermarking	Dependable parameters	PSNR	MSE	SIMILARITY	Dependable parameters	PSNR	MSE	SIMILARITY
Watermarked image	Alpha=0.1	39.79	6.8247	0.99513	Alpha=0.01	41.7682	4.3031	0.8694
Low pass filtering	3*3 mask filter	33.7164	27.634	0.81384	3*3 mask filter	41.7682	4.3031	0.8694
Median filtering	3*3 mask filter	41.761	4.3349	0.98557	3*3 mask filter	33.8377	26.8724	0.3387
High pass filtering	3*3 mask filter	624.072	254.58	0.030443	3*3 mask filter	6.3026	83.1748	0.3571
Pyramid compression	64*64 size	33.8349	26.889	0.83958	256*256 size	30.5875	56.7974	0.3364
DCT Compression	64*64 size	32.4206	37.240	0.78182	256*256 size	29.9455	65.8459	0.3256
Block truncation compression	64*64 size		0	1	256*256 size	22.4134	373.023	0.6923
Cropping	64*64 size	28.1225	100.19	0.539	256*256 size	19.1013	799.745	0.5183
Gaussian noise	Variance=0.01	41.0085	95.155	0.71412	Variance=0.01	20.0621	644.013	0.3836

Table 3 Comparison of Performance Analysis

5. CONCLUSION

The watermarking process sustains the cropping attack the watermark is highly recoverable even for the cropping block size of 256 x 256.The image pass through different attacks such as Geometric, Adding noise, Filtering , the logo is get extracted perfectly. The embedding algorithm is robust. More over the logo is extracted if the location of embedded is known, so the embedding algorithm is secure. The image after watermarking is imperiled to the low pass filtering and high pass filtering to remove the detailed coefficients. High pass filter removes the low frequency coefficients. Low pass filter is used to reduce the high frequency components. The watermarking algorithm sustains the compression attack; the watermark is highly recoverable even for the compression block size of M x N. Could say that even the image pass through different attacks such as Geometric, Adding noise, Filtering, the logo get extracted perfectly. Performs additional experiments to evaluate the robustness against more commonly used image processing attacks such as JPEG2000 compression, and DCT Compression. In future using different robust features and appropriate embedding techniques, robustness of watermarking techniques can be improved. Techniques which are truly imperceptible, secure and robust should be established. Several optimizations methods can be realistic to categorize regions of watermark embedding.

6. REFERENCE

[1] Abolfazl.S Hosseini and Saboori.A, (2015) "A new method for color image watermarking based on combination of DCT and PCA," International Conference on Communications, Signal Processing, and their Applications (ICCSPA'15), Sharjah, 2015,pp.1-5.doi:10.1109/ICCSPA.2015.7081310.

[2] Anthony T. S. Ho (2003) "Robust digital image-in-image watermarking algorithm using the fast Hadamard transform Conference Paper" DOI: 10.1109/ISCAS.2003.1205147 · Source: IEEE Xplore

[3] Biswas, S. Mukherjee and S. K. Bandyopadhyay, (2013) "DCT Domain Encryption in LSB Steganography,"5th International Conference and Computational Intelligence and Communication Networks, Mathura, 2013, pp. 405-408. DOI:10.1109/CICN.2013.

[4] Gupta.R and T. P. Singh, (2014) "New proposed practice for secure image combing cryptography steganography and watermarking based on various parameters," International Conference on Contemporary Computing and Informatics (IC3I) Mysore, 2014, pp.475-479.

[5] Islam et al.U., (2016) "An improved image steganography technique based on MSB using bit differencing," Sixth International Conference on Innovative Computing Technology (INTECH), Dublin, 2016, pp. 265-269