

A New Approach of an Image Watermarking Technique Based on DWT DCT and SVD, ARNOLD

Arpana Bhandari¹, Rajiv Shrivastava², Shailja Shukla¹

¹Department of Computer Science and Engineering, Rabindranath Tagore University, Bhopal, Madhya Pradesh, India

²Department of Computer Science and Engineering, Sagar Institute of Research & Technology Excellence, Bhopal, Madhya Pradesh, India

Article Info

Article history:

Received 5 January 2020

Received in revised form

20 February 2020

Accepted 28 February 2020

Available online 15 March 2020

Keywords: Watermark; DWT, DCT, SVD introduction

Abstract: There has been rising use of SVD, the digital watermarking tools in change domain has really evolved. It is based on DWT, DCT and SVD, we prepare a new watermarking system for algorithmic image. Our experimental results show that this practice combines the advantages of these three transforms. We can see compared with the SVD and the DCT plus SVD system the projected method has stronger robustness and faster speed in implanting and extracting.

1. Introduction

There is digital watermarking technology is the process of implanting useful info which can be convert into a digital media especially picture, acoustic, or videocassette for the purpose of copy control, content authentication, etc. Now it is observe an effective watermarking method should at least meet the following two uniqueness: imperceptibility, the disparity between the WI and OI cannot be distinguished by human eyes, and robustness, the unauthorized individuals or groups can not eliminate the watermark from the implanted useful info. The strength of robustness determines the watermarking technique's capacity of change during spread and storage space, including planned (such as malevolent attacks) and inadvertent (such as compression, noise, filtering, and rotation, etc.). In this we talk about generally speaking, watermarking can be grouped into two categories: spatial domain methods(SDM) and transform domain methods(TDM). In spatial domain approaches, the watermark is implanted directly to the pixel locations [3-10]. Now, In transform domain approaches, a mathematical transform is applied to the original image to implant watermark into the transform coefficients, then apply IT to get the implanted image. The most frequent used methods are Discrete Wavelet Transform (DWT), Discrete Cosine Transform(DCT), and Discrete Fourier Transform (DFT). As the transform domain methods always have good these are techniques which is having robustness to common image processing such as compression, noise, filtering cutting, and rotation, etc. They now come into more widespread used.

In recent years, Singular Value Decomposition (SVD) has been started to use in watermarking as a different transform [3]. It's a numerical technique that diagonalizes the matrix. In [2], the author proposed a non-blind watermarking system based on SVD. In [3], the author robustness and quicker calculating rate.

2. Preliminary

2.1 DWT

An Image applied DWT is divided into four sub- conjugate transpose of V , an $n*n$ unitary matrix[4].The non-negative components of S represent the luminance value of the image. Further we can see changing them slightly does not affect the image quality and they also don't change much after attacks, watermarking practice make use of these two properties [3]. Arnold Transform As Seen the digital image as a form of matrix $N * N$ matrix, then bands:

- LL
- HL
- LH
- HH

*Corresponding Author,

E-mail address: arpanabhandari08@gmail.com; drrajivsvri@gmail.com; shailjashukla@gmail.com

All rights reserved: <http://www.ijari.org>

The image's energy is mainly focused on the LFB.The other three bands characterize the marginal information of the corresponding direction and have little energy.

2.2 DCT

Furthermore it is observe DCT is one of the most popular linear transforms on DSP. It has been widely used [12-23]because of its good capacity of energy compression and de-correlation. DCT is faster than DFT because its transform kernel is real cosine function while it is complex exponential in DFT[5].For a given image $f(x, y)$.

3. Generate and Embed an Watermark Into an Image

Producing implanting tide marking into an images as see in figure 1.

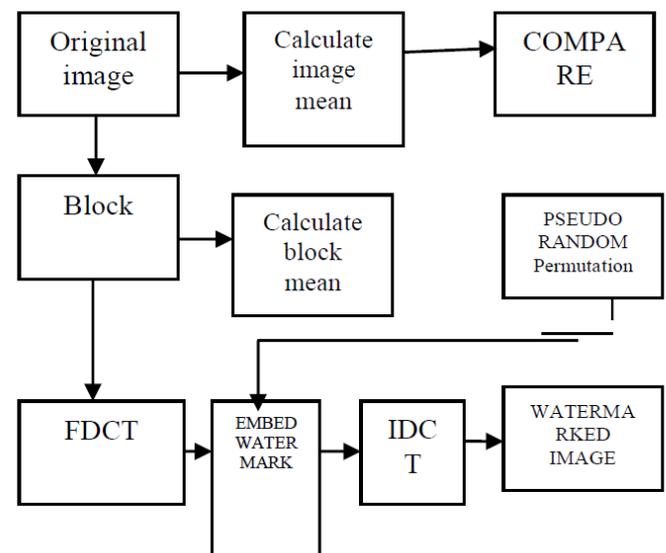


Fig.1: Generate and embed a watermark into an image

Firstly original image is resizing and then calculating image mean using eq. 1 and then comparing the block by which we calculate block mean. Using FDCT algorithm we embed watermark behind text image Performing IDCT algorithm on watermark image. Also calculating extracted coefficient in another side, in figure 2.

3.1 Extracting Watermark from Suspicious Image

During the process of extracting watermark from a suspicious image, the original image is not required, but the secret key (permutation rule). The block diagram of the watermark extraction is shown in First, the suspicious image X , is segmented into blocks with size $8*8$ and block-based DCT is performed on those blocks. That is

$$Y_s = \text{FDCT}(X_s) \quad (1)$$

Then eliminate the effects of the middle-coefficient modification. It is the reverse process of embedding watermark operation. For the block $X_s(k, l)$, form equation (1), it has

$Y_e(k,l)(m) = Y_s(k,l)(m)$ if $w_p(k,j) = 0$;

$$1/(1+\alpha) Y_s(k,l)(m)$$

If $w_p(k,j) = 1$ (2)

To obtain the extracted image which is the same size as the original image. IDCT operation performed on Y_e i.e.

$$x_e = \text{IDCT}(Y_e) \quad (3)$$

Then segment the extracted image X , and calculate the gray mean m , and the block means

M_{eb} , of the $N1/8 * N2/8$ blocks of the image X_e .

$$M_{ex} = 1/N1 * N2 \sum_{i=0}^{N1-1} \sum_{j=0}^{N2-1} X_e(i,j) \quad (4)$$

$$M_{eb} = \{M_{eb}(k,l); 0 \leq k < N1/8, 0 \leq l < N2/8\} \quad (5)$$

Compare the blocked mean $m_{eb}(k,l)$ with the mean value m_{ex} . The result is the binary pattern, i.e.

$$W_{sp}(k,l) = \begin{cases} 0 & m_{eb}(k,l) \leq m_{ex} \\ 1 & m_{eb}(k,l) > m_{ex} \end{cases} \quad (6)$$

$$W_{sp} = \{W_{sp}(k,l), 0 \leq k < N1/8, 0 \leq l < N2/8\} \quad (7)$$

In order to recover the normal sequence of the extracted watermark, inverse pseudo-random permutation is performed on W_{sp} . Then the extracted watermark is obtained, i.e.

$$W_s = \text{InversePermute}(W_{sp}) \quad (8)$$

To compare the extracted watermark with the reference watermark objectively, normalized correlation (NC) is used, which is the crosscorrelation normalized by the reference watermark energy to give unity as the peak correlation

$$NC = \sum_i \sum_j W_s(j) w_r(j) / \sqrt{\sum_i \sum_j W_s(j)^2 w_r(j)^2} \quad (9)$$

Because the watermark is generated from the image by comparing the gray mean of blocks and the gray mean of the entire image, the robustness of the watermark is inherent. The method presented in this paper is sensitive to the luminance or contrast alteration. For most image, the normalized correlation is over 0.95. The value can be a threshold to judge whether the image is changed.

In order to be compatible with the JPEG compression standard, the method of watermarking is based on JPEG lossy compression model. The original image is segmented into $N1/8 * N2/8$ blocks,

$$X_b = \{X_b(k,l), 0 \leq k < N1/8, 0 \leq l < N2/8\} \quad (10)$$

where image block $x_b(k,l)$ is expressed as

$$X_b(k,l) = \{x_b(k * 8 + i, l * 8 + j) = x(k * 8 + i, l * 8 + j), 0 \leq i < 8, 0 \leq j < 8\}$$

For $8 * 8$ value is computed in term of the following equation. For $8 * 8$ image block $X_b(k,l)$, the gray mean

$$m_b(k,l) = 1/64 \sum_{k=0}^7 \sum_{l=0}^7 x_b(k * 8 + i, l * 8 + j) \quad (11)$$

So the means of all image blocks is expressed as

$$M_b = \{m_b(k,l), 0 \leq k \leq N1/8, 0 \leq l < N2/8\} \quad (12)$$

The gray mean of the entire original image X is calculated according to the following equation

$$M_x = 1/N1 * N2 \sum_{i=0}^{N1-1} \sum_{j=0}^{N2-1} x(i,j) \quad (13)$$

The mean m , is considered as the reference value of watermarking. Then compare the means of the $N1/8 * N2/8$ blocks.

with the reference mean m_x . The comparison result is a binary pattern, i.e.

$$W = \{w(k,l), 0 \leq k \leq N1/8, 0 \leq l < N2/8\} \quad (14)$$

where $w(k,l)$ is obtained from the following equation

$$w_p(k,l) = \begin{cases} 0 & m_b(k,l) \leq m_x \\ 1 & m_b(k,l) > m_x \end{cases} \quad (15)$$

The element number of W is equal to the block number of the image X . W is derived from X and can be considered as a binary watermark.

Because the watermark is generated directly from the image, it is the visually recognizable pattern. So each element of the W can be regarded as a pixel of the watermark W . In order to eliminate the spatial correlation among pixels of the watermark, pseudo-random permutation is performed on W . A secret key (permutation rule) is generated from the permutation, i.e. $W_p = \text{Permute}(W)$

$$w_p(k,l) = \{w(k,l), 0 \leq k \leq N1/8, 0 \leq l < N2/8\} \quad (16)$$

where pixel (K,r) is shuffled to pixel (k,l) by the pseudo-random permutation. Since the human eye is more sensitive to noise in lower-frequency components than in higher-frequency ones and information hidden in higher-frequency components might be discarded after quantization of lossy compression, such as JPEG lossy compression. The traditional trade-off is embedding watermark into the middle-frequency range of an image. To embed the watermark into the image,

discrete cosine transform (DCT) is performed on each block with size 8×8 of X_b

where FDCT means forward discrete cosine transform. For image block $X_b(k,r)$, its DCT result $Y(k,l)$ has 64 coefficients. Those coefficients are ordered according to the zigzag-scan sequence. They are denoted as

$$Y_b(k,l)(0), Y_b(k,l)(1), \dots, y_b(k,l) \quad (16)$$

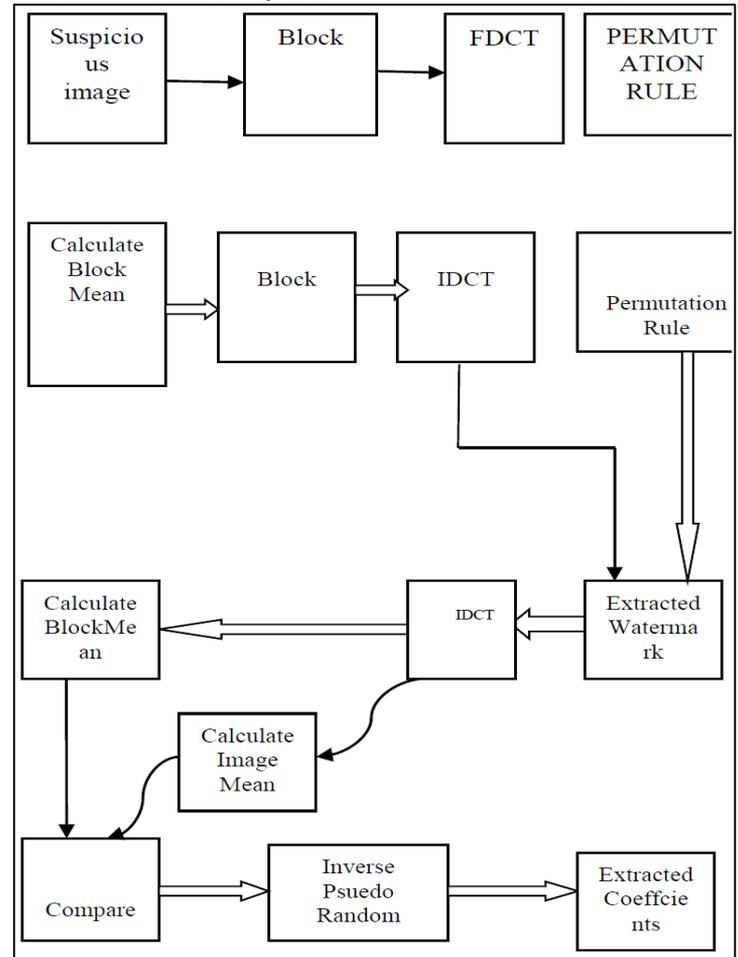


Fig.2: Extracting watermark from a suspicious image

For pixel $w_p(k,l)$, only one middle-frequency coefficient is selected and modified in corresponding image block $y_b(k,l)$. Suppose the selected middle frequency coefficient is $Y_b(k,l)(m)$, in which m is the index in the zigzag sequence. Embed the same watermark into the image according to the formula

$$Y_b(k,l)(m) = Y_b(k,l)(m) + \alpha w_p(k,l) Y_b(k,l)(m) \quad (17)$$

where α is the scale factor to control the modification value of the selected middle-frequency coefficient. It is defined by users and related to the texture complexity of the image. Finally, inverse discrete cosine transform (IDCT) is performed on each block of Y_b , and the watermarked image X , is obtained. That is

$$XW = \text{IDCT}(YW) \{ \text{IDCT}(Y_b(k,l)) \leq N1/8, 0 \leq l < N2/8 \} \quad (18)$$

3.Results



Fig.3: Original Image



Fig.4: watermarking image using eq.10



Fig. 5: Watermarking image using eq.17



Fig.6: Watermark image using eq 1

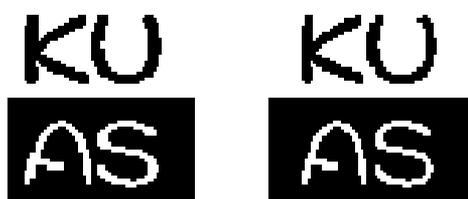


Fig.7: Extracted watermark image using IDCT

4. CONCLUSIONS

In this paper, it is planned a watermarking system for digital picture based on DWT, DCT and SVD. The experimental technique and test shows it has a better performance on imperceptibility and robustness. although It is robust to some common image processing including whereas GN, LPF, pepper & salt noise, contrast enhance, JPEG

compression, cutting, and rotation than a SVD or a DCT+SVD technique

References

- [1] K Satish. Chaos based spread spectrum image steganography. IEEE transactions on consumer electronics 50(2), 2004, 587-590.
- [2] M Schukat, C Pablo cortijo. Public key infrastructures and digital certificates for the internet of things. Signals and systems conference (ISSC), 2015 26th Irish. IEEE, 2015.
- [3] N Senthilkumaran, R Reghunadhan. Image segmentation-a survey of soft computing approaches. International conference on advances in recent technologies in communication and computing. IEEE, 2009.
- [4] S Sharda, S Budhiraja. Image steganography: a review. International journal of emerging technology and advanced engineering, 3(1), 2013, 707-710.
- [5] S Shahreza, M Hassan, MS Shahreza. A new approach to persian/arabic text steganography. Computer and information science, 2006 and 2006 1st IEEE/ACIS international workshop on component-based software engineering, software architecture and reuse. 5th IEEE/ACIS international conference, 2006
- [6] A Shrivastava, Lokesh Singh. A new hybrid encryption and steganography technique: a survey. International journal of advanced technology and engineering exploration 3(14), 2016.
- [7] DG Singhavi, PN Chatur. A new method for creation of secret-fragment-visible-mosaic image for secure communication. Innovations in information, embedded and communication systems (iciiecs), 2015 international conference on. iee, 2015.
- [8] S Sirsakar, J Salunkhe. Analysis of data hiding using digital image signal processing. Electronic systems, signal processing and computing technologies (ICESC), International conference IEEE, 2014.
- [9] NK Sreelaja, NK Sreeja. An image edge based approach for image password encryption. Security and communication networks 9(18), 2016, 5733-5745.
- [10] K Thangadurai, GS Devi. An analysis of lsb based image steganography techniques. Computer communication and informatics (ICCCI/IEEE), 2014
- [11] MJ Thenmozhi, T Menakadevi. A New Secure Image steganography using LSB and SPIHT based compression method. International journal of engineering 16, 2016, 17.
- [12] AJ Umbarkar, RP kamble, AV Thakre. Comparative study of edge based lsb matching steganography for color images. ICTACT journal on image and video processing 6(3), 2016.
- [13] A Valizadeh, ZJ Wang. Correlation-Aware Data hiding based on spread spectrum embedding. Image processing (ICIP/IEEE), 2010.
- [14] H Wang, S Wang. Cyber warfare: steganography vs. stag analysis. Communications of the ACM 47(10), 2004, 76-82.
- [15] X Wang. A novel color image encryption scheme using alternate chaotic mapping structure. Optics and lasers in engineering 82, 2016, 79-86.
- [16] Z Wang. Image quality assessment: from error visibility to structural similarity. IEEE transactions on image processing 13(4), 2004, 600-612.
- [17] WC Kuo. High magnitude data cloaking scheme based on multi-bit confidential function. 2015.
- [18] JW Woods, Sean o'neil. Sub-band coding of images. Acoustics, speech, and signal processing. IEEE/ICASSP-86, 11.
- [19] WD Chun, WH Tsai. A steganography method for images by pixel-value differencing. Pattern recognition letters 24(9-10), 2003, 1613-1626.
- [20] HC Wu. Image steganography scheme based on pixel-value differencing and LSB replacement methods. IEEE proceedings-vision, image and signal processing 152(5), 2005, 611-615.
- [21] D Xu, R Wang. Separable and error-free reversible data hiding in encrypted images. Signal processing 123, 2016, 9-21.
- [22] X Yan. New approaches for efficient information hiding-based secret image sharing schemes. signal, image and video processing 9(3), 2015, 499-510.

- [23] CT Yang. Optimizing PSNR for image watermarking using summation quantization on dwt coefficients. Computer software and applications conference IEEE, 39th annual. 1, 2015.
- [24] MAB Younes, A Jantan. A new steganography approach for images encryption exchange by using the least significant bit insertion. International journal of computer science and network security 8(6), 2008, 247-257.
- [25] YH Yu, CC Chang, IC Lin. A new steganographic method for color and grayscale image hiding. Computer vision and image understanding 107(3), 2007, 183-194.
- [26] T Zhang, XJ Ping. A new approach to reliable detection of LSB steganography in natural images. Signal processing 83(10), 2003, 2085-2093.
- [27] JY Zheng. A dct-based digital watermarking algorithm for image. Industrial control and electronics engineering (ICICEE/ IEEE), 2012.