

DWT Coefficient Based Image Watermarking Method for Security Purposes using Mat-Lab

Mamatha H¹
Student
Dept. E & C
Tumkur, India

Anitha Devi M D²
Asst.Professor
Dept. E & C
Tumkur, India

Dr. M Z Kurian³
Head of the department
Dept. E & C
Tumkur, India

Abstract: This paper considers a situation where the copyright of distributed images/photos is violated. Since the images/photos published on social networks or any networks are usually modified and/or compressed to the match the template provided by the service providers, this paper propose a digital image watermarking based on DWT coefficients modification to be used for such images/photos. Basically, there are two parts in the image processing, in the embedding process, the blue component of original host image is decomposed by the Discrete Wavelet Transform (DWT). Then image is transmitted. At the receiver end, original components of the watermark image are extracted by using adaptive mean filter.

Keywords: Digital watermarking, discrete wavelet transforms, mean filter.

I. INTRODUCTION

Presently, social networking services, e.g. Facebook, Google+, Instagram and etc., have more influence to our daily life than they did in the past, judged from an on-going increasing number of social network subscribers. Because of attractive features provided for multimedia data, subscribers can simply publish and/or exchange these data. However, multimedia data published in the social networks is easy to be copied and distributed without any permission from the real owner and very difficult to differentiate the copied version from the original one. In order to protect the copyright of the distributed data, digital watermarking techniques have been developed and implemented. Because the images/photos published on them are always changed and/or compress by the uploading process such as JPEG quantization table, pixel resolution and related metadata. Therefore, the digital watermarking techniques developed for social

networking services should be robust against image compression attacks.

Despite being primarily used to communicate and socialize with friends, the diverse and anonymous nature of social networking websites makes them highly vulnerable to cyber crimes. Publishers, fraudsters, child predators, and other cyber criminals can register to these services with fake identities, hiding their malicious intentions behind innocent appearing profiles. Social networks also

encourage the publication of personal data, such as age, gender, habits, whereabouts, and schedules. The wealth of personal information uploaded to these websites makes it possible for cyber criminals to manipulate this information to their advantage and use it to commit criminal acts. Other abusive activities that can be committed on these websites include uploading illegal or inappropriate material, defaming, and stalking. The large number of criminal acts that can be performed through social networks raises the importance of digital forensics in this area. Electronic evidence retrieved from social networking activities on a suspect's machine can be of great assistance in investigating a criminal case by incriminating or proving the innocence of a suspect. Hussein [8] proposed a digital watermarking method based on log-average luminance. Some 8×8 pixels blocks were chosen and used for watermark embedding if they had a log-average luminance greater than or equal to the log-average luminance of the whole image.

This paper proposes a digital image watermarking for social networking services based on DWT coefficients modification. In the embedding process, the blue component of original host image is decomposed by the Discrete Wavelet Transform (DWT) to obtain the coefficients in LL sub-band in order to embed watermark. In the extraction process, original coefficients prediction based on mean filter is used to increase the accuracy of the extracted watermark. The performance obtained from the proposed method.

II. LITERATURE SURVEY

Jamal a.hussein has proposed a new watermarking scheme on log average luminance. A colored image is divided into blocks after converting the rgb color image into ycbcr color space. To embed the watermark selected blocks are chosen and to extract the watermark, the selected blocks are chosen [1].

Aree ali mohammed has proposed an image watermarking scheme based on multi bands wavelets transformation method. In this work three methods are developed to embed the watermark [2]

Guangyong gao et al., has proposed a new technique based on composite chaos and rmsbm in nsct domain. The watermark is embedded according to the principle of

human visual system in nonsubsampling contourlet(NSCT) domain and maximum likelihood(ml) detector is used for extraction of watermark [3].

Aleksey kovel et al., has proposed a new method of a pseudo-random pixel rearrangement algorithm based on gaussian integers for image watermarking. It improves the security of most image watermarking techniques [4].

Yuan-hui yu et al., has suggested a steganographic method for embedding a color image in a true color image. Secret data are protected by the conventional crypto system des. This was compared with previous method. The results are improved compare to previous methods [5].

Ali-al-ataby et al., has proposed a method pre-adjusts the original cover image in order to guarantee that the reconstructed pixels from the embedded coefficients would not exceed its maximum value and hence the message will be correctly recovered [6].

S.a.m.gilani et al., has suggested a novel scheme for watermarking of color images. Color spaces with linear relation to rgb color space with uncorrelated components. Watermark detection is fast and blind [7].

Atallah m. Al-shatnawi has proposed a new method in image steganography with improved image quality. The proposed method hides the secret message based on searching about the identical bits between the secret messages and image pixels values [8].

Komwit surachat has proposed a method for improving the watermark extraction performance of the digital watermarking based on the modification of image pixels. Embedding watermark data with a multiple sections technique in the blue channel [9].

The technique of digital watermarking has always been a topic of great research. The DCT algorithm provides security to the data, but hackers can hack the data from trail, and error method. This paper proposes the one basic technique of digital watermarking by using the wavelets decomposition and mean filter bank.

III. PROPOSED METHOD

The watermarking algorithm is shown in Fig.1. Consider a cover image and watermark image. The 2D-DWT is applied to cover image as well as watermark image. And only low frequency band (LL) is selected for further processing.

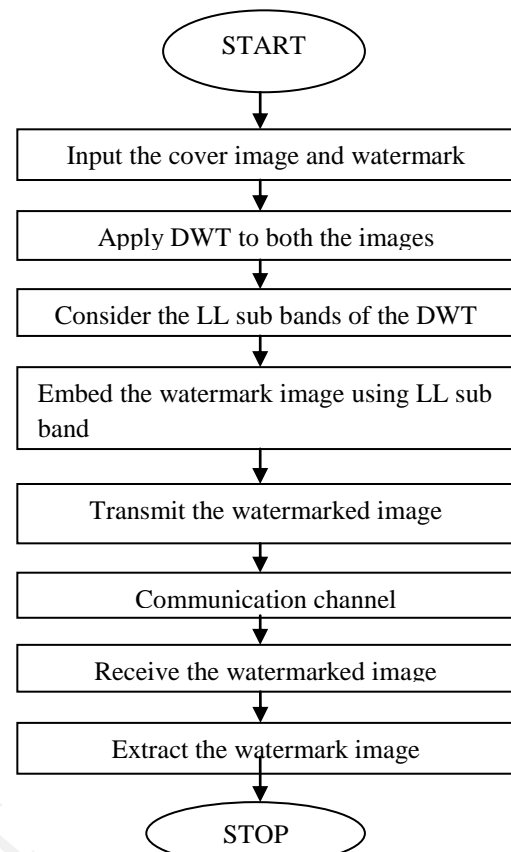


Figure1. Watermarking methodology flow chart

The next step is embedded the watermark image into the cover image. Then transmit the watermarked image through communication channel. At receive the watermarked image and extract the watermark image.

IV. IMPLEMENTATION

The proposed watermarking method is separated into two processes:

Watermark embedding and extraction processes.

A. Watermark embedding process:

In this process, a black and white logo image (I) with the same size ($M \times N$) as original host image (I) is considered as a watermark logo. It is decomposed by 2D-DWT to obtain four sub-bands. Fig 2 show watermark logo and its sub-bands respectively

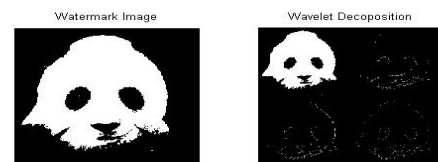


Figure 2: Watermark logo and its sub-bands respectively



Figure 3 shows the host image and its sub-bands respectively.

Then, the watermark coefficients in LL sub-band whose value can be 0, 1, 1.5, and 2 are selected and converted to two-value coefficients, 1 or 0, as follow.

$$WNew\Phi(i,j) = \begin{cases} 1; & \text{if } W\Phi(i,j) \geq 1.5 \\ 0; & \text{if } W\Phi(i,j) < 1.5 \end{cases}$$

After that $W^{New}_{\psi}(i,j)$, is permuted by using Gaussian distribution for spreading the watermark bits pattern, and XORed with a pseudo-random bit stream generated from a key based stream cipher to provide security to finally obtain $W^E_{\psi}(i,j)$. The resultant coefficient is converted to 1 and -1 before embedding it to the coefficients in LL sub-band of the original host image, one bit by one coefficient. Figure 4 shows the block diagram of proposed watermark embedding process.

The blue component of original host image (B) is decomposed by the 2D-DWT to obtain 4 sub-bands, which are approximation sub-band ($B_{\psi}(i,j)$), horizontal sub-band ($B^H_{\psi}(i,j)$), vertical sub-band ($B^V_{\psi}(i,j)$) and diagonal subband ($B^D_{\psi}(i,j)$).

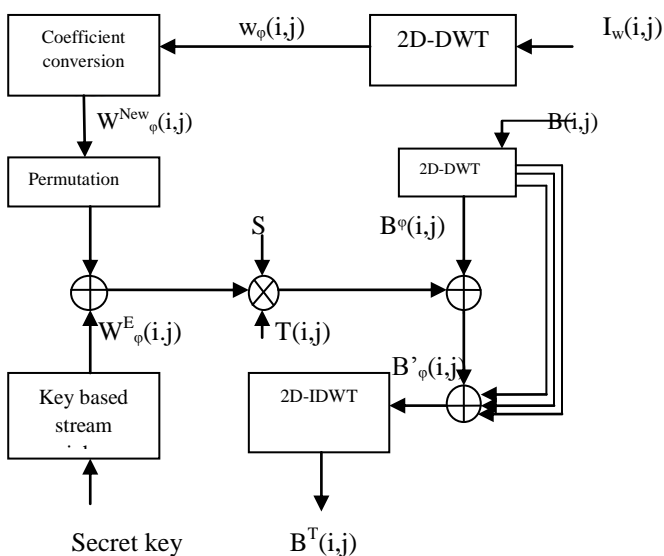


Figure 4: Block diagram of proposed watermark embedding process

The coefficient in LL sub-band ($B_{\psi}(i,j)$) is selected to embed watermark ($W^E_{\psi}(i,j)$) by using equation

$$B^{\psi'}(i,j) = B^{\psi}(i,j) + W^E_{\psi}(i,j) * S * T(i,j)$$

Where $B^{\psi'}(i,j)$ is watermarked coefficient, s is signal strength which is a constant factor used for the entire watermarking area and $T(i,j)$ is the tuned coefficient value for each embedding bit which is derived from resizing the luminance of original host image, $L(i,j) = 0.2999R(i,j) + 0.587G(i,j) + 0.114B(i,j)$

Finally $B^{\psi'}(i,j)$, $B^H_{\psi}(i,j)$, $B^V_{\psi}(i,j)$, and $B^D_{\psi}(i,j)$ are inverse transformed by using the 2D-IDWT, and then the result $B^T(i,j)$ is combined with original red (R) and green (G) components to construct the watermarked image (I').

B. Watermark Extraction Process

It can also be seen from equation (2) that embedding the permuted watermark into the coefficients in LL sub-band of the original host image is similar to adding the high frequency noise to those coefficients. Therefore, the watermarked coefficients are considered as noisy coefficients ($B^{\psi'}(i,j)$) formed by the addition of random noise ($n(i,j)$) to $B^{\psi}(i,j)$. The equation (2) can be rewritten as

$$B^{\psi'}(i,j) = B^{\psi}(i,j) + n(i,j)$$

To extract the embedded watermark, $B^T(i,j)$ is decomposed by the 2D-DWT to obtain noisy coefficients for a prediction of original coefficients in LL sub-band. With the assumption that at every pair of coefficient (i,j), the noise is uncorrelated [9].

These predicted coefficients are finally subtracted from watermarked coefficients in LL sub-band to extract the embedded watermark. This step can be described by equation

$$E\{B''_{\psi}(i,j)\} = \frac{1}{9} \sum_{m=-1}^1 \sum_{n=-1}^1 B^{\psi'}(i+m, j+n)$$

To recover the original watermark logo, the value of $W^{\psi'}_{\psi}(i,j) = 0$ is set as a threshold, and its sign is used to estimate the value of $W^{\psi}_{\psi}(i,j)$. That is, if $W^{\psi'}_{\psi}(i,j)$ is positive (or negative), $W^{\psi}_{\psi}(i,j)$ is 1 (or -1, respectively).

After that $W^{\psi}_{\psi}(i,j)$ is XORed with the same pseudo-random bit stream as used in the embedding process and then the result is passed to invert permutation to obtain $W''_{\psi}(i,j)$. Finally, $W''_{\psi}(i,j)$ is combined with coefficients in LH ($WH_{\psi}(i,j)$), HL ($WH_{\psi}(i,j)$), and HH

sub-band ($WD\psi(i,j)$) set to 0, and the result is inverse transformed using the 2D-IDWT to obtain the extracted watermark $\Gamma^w(i,j)$.

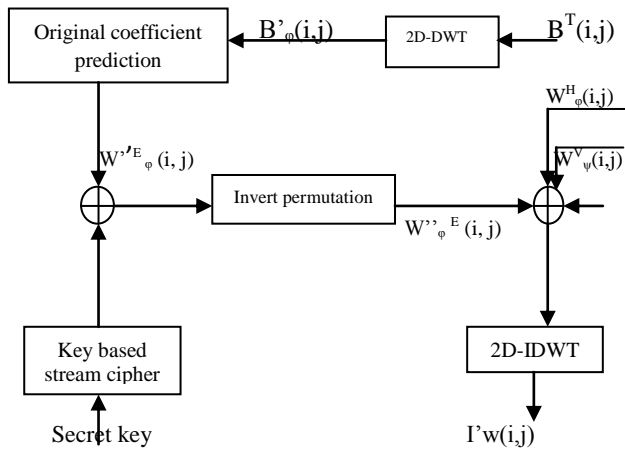


Figure 5: block diagram of proposed watermark extraction process

V. CONCLUSION

In this paper the digital watermarking method based on DWT coefficients modification for social networking services embedding process has been presented. In the embedding process, the coefficients in LL sub-band were used to embed watermark. In this paper the embedding process and extraction process both are implemented. Future this method can also apply to 3-D images and to the videos.

REFERENCES

1. J. A. Hussein, "Spatial Domain Watermarking Scheme for Colored Images Based on Log-Average Luminance," *Journal of Computing, Journal Of Computing*, Vol. 2, Issue 1, January 2010.
2. Aree Ali Mohammed, College of Science and Haval Mohammed Sidqi, "Robust Image Watermarking Scheme Based on Wavelet Technique" *International Journal of Computer Science and Security (IJCSS)*, Volume (5), Issue (4), 2011.
3. Guangyong Gao and Guoping Jiang "Water resisting local geometric attacks using composite chaos and RMSBM in NSCT domain" *Journal of Information & Computational Science* Vol. 8, issue 3, 511-519, 2011.
4. Aleksey Koval, Frank Y. Shih, Boris S. Verkhovsky "A pseudo-random pixel rearrangement algorithm based on gaussian integers for image watermarking" *Journal of Information Hiding and Multimedia Signal Processing*, Volume 2, Number 1, January 2011.
5. Yuan-Hui Yu, Chin-Chen Chang and Iuon-Chang Lin "A new steganographic method for color and grayscale image hiding", *Computer Vision and Image Understanding*, 2006.
6. Ali Al-Ataby1 and Fawzi Al-Naima., "A Modified High Capacity Image Steganography Technique Based on Wavelet Transform" *The International Arab Journal of Information Technology*, Vol. 7, No. 4, October 2010.
7. S.A.M.Gilani, I.Kostopoulos and A.N.Skodras Electronics Laboratory, University of Patras, "Color image-adaptive watermarking" *IEEE*, 2002.
8. Atallah M. Al-Shatnawi, "A New Method in Image Steganography with Improved Image Quality", *Applied Mathematical Sciences*, Vol. 6, no. 79, 3907 – 3915, 2012.
9. Komwit Surachat, "Pixel-wise based Digital Watermarking Using a Multiple Sections Embedding Technique", *International Journal of Future Computer and Communication*, Vol. 1, No. 2, August 2012.
10. K B Shiva Kumar , K B Raja, R K Chhotaray, Sabyasachi Pattnaik "Steganography Based on Payload Transformation", *IJCSI International Journal of Computer Science Issues*, Vol. 8, Issue 2, March 2011.
11. K B Shiva Kumar, K B Raja, Sabyasachi Pattnaik, "Hybrid Domain in LSB Steganography", *International Journal of Computer Applications (0975 – 8887) Volume 19– No.7, April 2011.*