Volume 4, Issue VI, June 2016
ISSN 2320-6802

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

DWT-SVD based Watermarking Techniques to provide Security in RGB Images

Deepak Sharma[1], Munna Singh Kushwaha[2]

[1]M.Tech student, [2]Assistant Professor
Electronics and Communication Department
S(PG)ITM, Rewari

1. Introduction

Digital watermarking is the process of embedding information into digital multimedia content such that the information (which we call the watermark) can later be extracted or detected for a variety of purposes including security, data authentication, identification of owner and copyright protection [1]. Digital multimedia content includes image, audio, video etc. Watermarking has been around for several centuries, in the form of watermarks found initially in plain paper and subsequently in paper bills. Now, it is being used for many different applications such as E-commerce, E-voting, copyright protection, content authentication, medical safety, broadcasting monitoring, military and indexing [2]. Several features of digital watermarking are Robustness, imperceptibility, security, capacity and data payload [4]. According to the type of document to be watermarked, watermarking techniques can be divided into four categories that are [5]: Text Watermarking, Image Watermarking, Audio Watermarking, Video Watermarking. Various applications of digital watermarking are broadcasting monitoring, fingerprinting, image and content authentication, temper detection, medical application, copyright protection, content protection, convert communication.

1.1 Digital watermarking life-cycle phases: Digital image watermarking use digital image for embedding the hidden information, after embedding the watermarked image is generated and the watermarked image is more robust against attacks. Figure 1 shows the life-cycle phases of digital watermarking [3]:

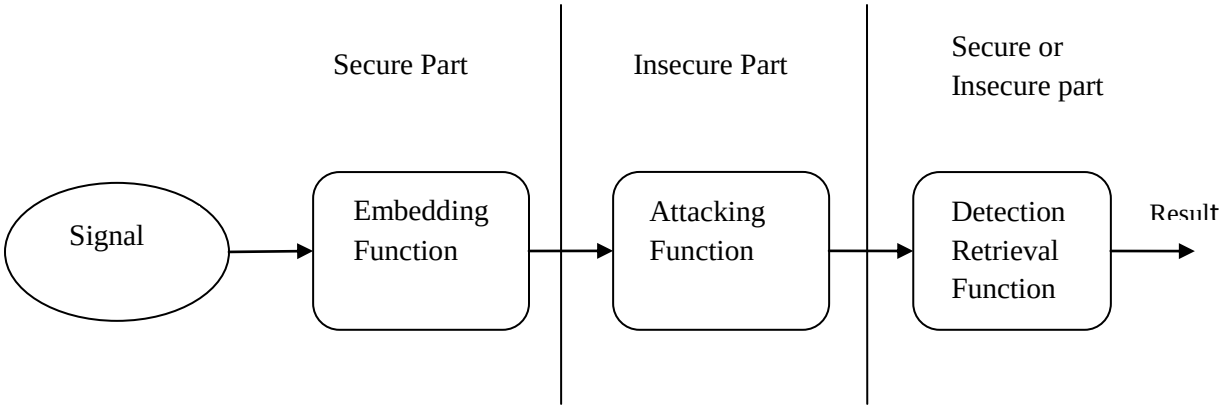

Figure 1: General Digital watermarking life-cycle phases (redrawn from [3])

i) Embedding: An algorithm accepts the host and the data to be embedded, and produces a watermarked signal. Then, the watermarked digital signal is transmitted to another person or stored.
ii) Attack: Unauthorized person try to make modifications. In this stage, when the data is transmitted over the network. Either some noise is added with the watermarked image or some attacks are performed on the watermarked image. So, our watermarked data is either modified or destroyed.
iii) Extraction: An algorithm which is applied to the attacked signal to attempt to extract the watermark from it. If the signal was unmodified during transmission, then the watermark still is present and it may be extracted.

***1.2 Types of Digital watermarking techniques*: Digital watermarking techniques may be classified as [6]:**
i) Spatial domain watermarking: Spatial domain methods are based on direct modification of the values of the image pixels, so the watermark has to be embedded in this way. Such methods are simple and computationally efficient, because they modify the color, luminance or brightness values of a digital image pixels, therefore their application is done very easily, and requires minimal computational power. Some of its algorithms are LSB; SSM Modulation based technique [6]. Modifications might include flipping the low-order bit of each pixel. However, this technique is not reliable when subjected to normal media operations such as filtering or lossy compression. Least Significant Bit Coding (LSB) [5] is one of the earliest methods. It can be applied to any form of

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

watermarking. In this method the LSB of the carrier signal is substituted with the watermark. The bits are embedded in a sequence which acts as the key. In order to retrieve it back this sequence should be known. The watermark encoder first selects a subset of pixel values on which the watermark has to be embedded. It then embeds the information on the LSBs of the pixels from this subset. LSB coding is a very simple technique but the robustness of the watermark will be too low. With LSB coding almost always the watermark cannot be retrieved without a noise component.

ii) Frequency domain watermarking: In Frequency domain the secret data are hidden in the lower or middle frequency portions of the protected image, because the higher frequency portion is more likely to be suppressed by compression. Embedding of a watermark is made by modifications of the transform coefficients, accordingly to the watermark or its spectrum. Finally, the inverse transform is applied to obtain the marked image. This approach distributes irregularly the watermark over the image pixels after the inverse transform, thus making detection or manipulation of the watermark more difficult [6]. Frequency (transform) domain methods are based on the using of some invertible transformations like discrete cosine transform (DCT), discrete Fourier transform (DFT), discrete wavelet transform (DWT) etc. to the host image. Discrete cosine transform (DCT) [7] is a process which converts a sequence of data points in the spatial domain to a sum of sine and cosine waveforms with different amplitudes in the frequency domain. The DCT is a linear transform, which maps an n-dimensional vector to a set of n coefficients. Discrete Fourier Transformation (DFT) is translation invariant and rotation resistant, which translates to strong robustness to geometric attacks.DFT uses complex numbers, while DCT uses just real numbers. Discrete wavelet transforms (DWT) [6] based methods enable good spatial localization and have multi resolution characteristics, which are similar to the human visual system. Also this approach shows robustness to low-pass and median filtering. However, it is not robust to geometric transformations.

2. Literature Review

Candik et.al [1] presented some basic principles and properties of digital watermarking in digital images. They are also more sophisticated algorithms in digital image watermarking that not need original unmarked image for watermark extraction. A novel dual watermarking mechanism was shown in [2] for digital media that embeds a recognizable pattern into the spatial domain and an invisible logo into the frequency domain. Undoubtedly, visible watermarking is important for protecting online resources from unauthorized reproduction. The new scheme utilizes visible and invisible watermarking to provide visual ownership identification and to achieve the robustness requirement. Hemdan et.al [3] presented a hybrid image watermarking technique for data hiding over Internet. The idea of the proposed technique was based on fusing multiple watermark images using wavelet fusion algorithm. Singh et.al [4] incorporated the detail study including digital watermarking definition, its concept and the main contributions in the field of ensuring and facilitating security, authentication, copyright protection and data integrity. In [5], they presented different techniques of digital image watermarking based on spatial & frequency domain, which shows that spatial domain technique provides security & successful recovery of watermark image and higher PSNR value compared to frequency domain. Mishra et.al [6] presented a comprehensive survey on various digital watermarking techniques such as robust, fragile and semi fragile watermarking techniques. They provided evidence that digital watermarking techniques are of increasing interest and are of gaining popularity. Singh et.al [8] presented a survey of different techniques on digital image watermarking. Digital watermarking is used as a key solution to make the data transferring secure from illegal interferences. Digital watermark techniques are used in various areas such as copyright protection, broadcast monitoring and owner identification. The authors in [9] focused on the various domains of digital image watermarking techniques like spatial domain techniques in which the values at the image pixels are directly modified using on the watermark which is to be embedded, frequency domain technique in which the transform coefficients are modified instead of directly changing the pixel values and feature based watermarking in which watermarking algorithms using a feature of an image were proposed as the second generation watermark. Bisla et.al [10] has done a comparative study of two most recent techniques used in digital image watermarking. They are DWT and hybrid DWT-SVD. Both these techniques are very much robust and imperceptible. In case of DWT, decomposition of the original image is done to embed the watermark and in case of hybrid DWT-SVD firstly image is decomposed according to DWT and then watermark is embedded in singular values obtained by applying SVD.

3. Methodology

3.1 Proposed DWT data hiding embedding algorithm: The algorithm works as follows:

Step1: The original N*N RGB image is transformed into sub-bands using single level 2-D DWT.

Step2: The watermark of size M*M RGB image is transformed into sub-bands using single level 2-D DWT.

Step3: The resultant watermark is then embedded into the lower frequency sub-band of original image using the scale factor (α) i.e.

$$WI = O + \alpha W \qquad (1)$$

Step4: Finally, inverse 2-D DWT is performed to produce the watermarked image.

3.2 Proposed DWT data hiding extraction algorithm:

The extraction algorithm for DWT based watermarking works as follows:

Step1: The original N*N RGB image is transformed into sub-bands using single level 2-D DWT.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY
WINGS TO YOUR THOUGHTS.....

Step2: The watermark of size M*M RGB image is transformed into sub-bands using single level 2-D DWT.
Step3: The watermarked image (output of embedding) is transformed into sub-bands using the single level 2-D DWT.
Step4: Then the extraction is applied to the decomposed watermarked image using the same value of scale factor (α) i.e.

$$EWI = (WM - O)/\alpha \quad (2)$$

Step5: Finally, inverse 2-D DWT is performed to get the extracted watermark image.

3.3 Singular Value Decomposition (SVD)

Singular Value Decomposition is a linear algebra transform which is used for factorization of a real or complex matrix with numerous applications in various fields of image processing. As a digital image can be represented in a matrix form with its entries giving the intensity value of each pixel in the image, SVD of an image M with dimensions m x m is given by [10]:

$$M = USV^T \quad (3)$$

Where, U and V are orthogonal matrices and S known as singular matrix is a diagonal matrix carrying non-negative singular values of matrix M. The columns of U and V are called left and right singular vectors of M, respectively. They basically specify the geometry details of the original image. Left singular matrix i.e., U represents the horizontal details and right singular matrix i.e., V represents the vertical details of the original image. The diagonal values of matrix S are arranged in decreasing order which signifies that the importance of the entries is decreasing from first singular value to the last one. This feature is employed in SVD based compression techniques.
There are two main properties of SVD to employ in digital watermarking schemes [10]:
1. Small variations in singular values do not affect the quality of image.
2. Singular values of an image have high stability.

3.4 Hybrid DWT-SVD

Hybrid technique is a fusion of two techniques. Here, DWT and SVD are used together to improve the quality of digital watermarking and hence increases the robustness and imperceptibility of an image.
3.4.1 Proposed hybrid DWT-SVD data hiding embedding algorithm: The embedding algorithm for DWT-SVD based watermarking is shown in figure 3.4. The algorithm works as follows:
Step1: The original N*N RGB image is transformed into sub-bands using single level 2-D DWT.
Step2: SVD is performed on LL sub-band (on RGB components) of decomposed RGB original image i.e.

$$S = USV^T \quad (4)$$

Step3: The watermark of size M*M RGB image is transformed into sub-bands using single level 2-D DWT.
Step4: SVD is performed on LL sub-band (on RGB components) of decomposed RGB watermark image i.e.

$$SW = U_w S_w V_w^T \quad (5)$$

Step5: After performing SVD on both original and watermark images, the resultant watermark image is then embedded with the original image using the scale factor (α) i.e.

$$SWI = S + \alpha(SW) \quad (6)$$

Step6: Inverse SVD is performed on embedded image.
Step7: Finally, inverse 2-D DWT is performed to produce the watermarked image.
3.4.2. Proposed hybrid DWT-SVD data hiding extraction algorithm: The extraction algorithm for DWT-SVD based watermarking is shown in figure 3.5. The algorithm works as follows:
Step1: The original N*N RGB image is transformed into sub-bands using single level 2-D DWT.
Step2: SVD is performed on LL sub-band (on RGB components) of decomposed RGB original image i.e. $S = USV^T$
Step3: The watermark of size M*M RGB image is transformed into sub-bands using single level 2-D DWT.
Step4: SVD is performed on LL sub-band (on RGB components) of decomposed RGB watermark image i.e.

$$SW = U_w S_w V_w^T \quad (7)$$

Step5: The watermarked image (output of embedding) is transformed into sub-bands using the single level 2-D DWT.
Step6: SVD is performed on LL sub-band (on RGB components) of decomposed RGB watermarked image i.e.

$$SWI = U_w S_w V_w^T \quad (8)$$

Step7: Then the extraction is applied to the resultant SVD image using the same value of scale factor (α) i.e.

$$EWI = (SWI - S)/\alpha \quad (9)$$

Step8: Inverse SVD is applied on resultant image after extraction.
Step9: Finally, inverse 2-D DWT is performed to get the extracted watermark image.

4. Results

The proposed DWT and hybrid DWT-SVD data hiding techniques are coded using MATLAB.

Figure 2: Host Image

Volume 4, Issue VI, June 2016
ISSN 2320-6802

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

Figure 3: Watermark Image

Figure 4: DWT based watermark embedding

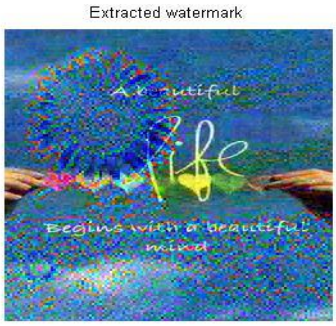

Figure 5: DWT based watermark extraction

Figure 6: DWT-SVD based watermark embedding

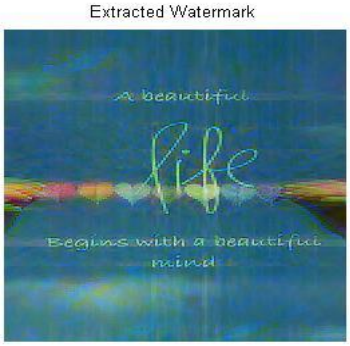

Figure 7: DWT-SVD based watermark extraction

5. Conclusion and Future work

DWT and DWT-SVD watermarking technique are applied to ensure the copyright protection and security of content or images and to increase the robustness of image. After applying both the watermarking techniques and comparing the values of PSNR at different values of scaling factor α, it is concluded that the hybrid DWT-SVD technique is much better than DWT technique. As at every value of scaling factor, value of peak signal to noise ratio (PSNR) is more in case of the hybrid technique. Less the value of PSNR more will be the degradation in the quality of the original image. This shows that after watermarking, the quality of original image degrades more when DWT technique is used for embedding the watermark in comparison with DWT-SVD technique embedding.

Although this scheme is able to hide sensitive information effectively and avoid disputes attention, it cannot completely resist various attacks during transmission in wireless sensor networks. Therefore, improvement in its robustness as well as security against various attacks may be considered as a future scope by using encryption algorithm with the help of secret key so that essential data can be prevented from unauthorized access.

REFERENCES

[1] Marek Candik and Dagmar Brechlerova, "Digital Watermarking in Digital Images", *ICCST 2008*, June 2008.

[2] Pei-Yu Lin, Jung-San Lee, and Chin-Chen Chang, "Dual Digital Watermarking for Internet Media Based on Hybrid Strategies", *IEEE Transactions on Circuits and Systems for Video Technology*, Vol. 19, No. 8, August 2009.

[3] Ezz El-Din Hemdan, Nawal El-Fishaw, Gamal Attiya and Fathi Abd El-Samii, "Hybrid Digital Image Watermarking Technique for Data Hiding", *30th National Radio Science Conference(NRSC 2013)*, *IEEE*, April 2013.

[4] Prabhishek Singh, R S Chadha, "A Survey of Digital Watermarking Techniques, Applications and Attacks", *International Journal of Engineering and Innovative Technology (IJEIT)*, Vol. 2, Issue 9, March 2013.

INTERNATIONAL JOURNAL FOR ADVANCE RESEARCH IN ENGINEERING AND TECHNOLOGY

WINGS TO YOUR THOUGHTS.....

[5] Namita Chandrakar and Jaspal Bagga, "Performance Comparison of Digital Image Watermarking Techniques: A Survey", *International Journal of Computer Applications Technology and Research*, Vol. 2, Issue 2, pp. 126 - 130, 2013.

[6] Sasmita Mishra, Amitav Mahapatra,Pranati Mishra, "A Survey on Digital Watermarking Techniques", *International Journal of Computer Science and Information Technologies (IJCSIT)*, Vol. 4 , pp. 451-456, 2013.

[7] Manoranjan Kr Sinha , Dr. Rajesh Rai and Prof. G. Kumar, "Literature Survey on Digital Watermarking", *International Journal of Computer Science and Information Technologies (IJCSIT)*, Vol. 5, pp. 6538-6542, 2014.

[8] Y. Shantikumar Singh, B. Pushpa Devi, and Kh. Manglem Singh, "A Review of Different Techniques on Digital Image Watermarking Scheme", *International Journal of Engineering Research*, Vol. 2, Issue 3, pp. 193-199, July 2013.

[9]Seema Malshe, Hitesh Gupta and Saurabh Mandloi, "Survey of Digital Image Watermarking Techniques to achieve Robustness", *International Journal of Computer Applications*, Vol. 45, May 2012.

[10] Nidhi Bisla and Prachi Chaudhary, "Comparative Study of DWT and DWT-SVD Image Watermarking Techniques", *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 3, Issue 6, June 2013.