Survey of Transform Domain Digital Image Watermarking

Ms. Nitika Agarwal[1] Ms. Neha Singh[2]
[1]Scholar, M.Tech, Institute of Engineering and Technology, Alwar
[2]Associate. Prof., Dept. of ECE, Institute of Engineering and Technology, Alwar
nitika.agarwal9@gmail.com, nneha.singh01@gmail.com

Abstract: - Digital watermarking is the process of embedding information into digital multimedia content such that the information can later be extracted or detected. This paper provides an overview of the transform domain of watermarking technique for digital images which includes Discrete Cosine Transform domain, Singular Value Decomposition domain and Discrete Wavelet Transform domain. Individual and even combinations of any of these domains are also surveyed.

Keywords: - Steganography, Digital Watermarking, Hybrid watermarking, transform domain watermarking, Wavelet domain watermarking, Discrete Cosine Transform, Singular Value Decomposition.

1. INTRODUCTION

The techniques involved in hiding some information in digital content are collectively referred to as *information hiding techniques*. When used on digital images, these can be classified [1] as steganography or watermarking techniques. *Steganography* refers to the science of invisible communication striving to hide the very presence of the message itself. Digital watermarking is the process of embedding information into digital multimedia content such that the information can later be extracted or detected for a variety of purposes [2] including copy prevention and control. A digital watermark [3] is used for this purpose which is a digital signal or pattern inserted into a digital image and may also serve as a digital signature. It helps to determine the authenticity and ownership of an image.

It is desirable that the watermark is irremovable from the cover image and resists several intentional and unintentional operations with the watermarked image which may possibly disable the watermark. Commonly, these operations (especially the intentional ones) are referred as attacks against watermarks and include [4, 5] geometric distortions like rotation, translation, scaling and cropping, resampling and requantization, recompression, filtering, rewatermarking, forgery and collusion. For protection against these attacks, the watermarking technique need to trade off between [2, 4] the security, imperceptibility, capacity, robustness, tamper resistance, computational cost, data payload and key restrictions.

The terms Steganography and watermarking are exchangeable. The important areas of application [2, 5, 6] for watermarking are owner identification, copyright protection, broadcast monitoring, medical applications, fingerprinting and data authentication.

The paper is organized as follows: Section 2 gives the classification of watermarking techniques followed by exploration of transform domain of watermarking techniques in sections 3. Section 4 discusses results of some of the techniques covered in sections III.

2. CLASSIFICATION OF DIGITAL WATERMARKING

On the basis of domain for watermark embedding the watermarking technique is either spatial domain or transform domain. Spatial-domain watermarking techniques change the intensity of original image or gray levels of its pixels. This kind of watermarking is simple and computationally less complex, because no transform is needed. However, there must be tradeoffs between invisibility and robustness, and it is hard to resist common image processing and noise. Transform domain watermarking embeds the watermark into the transformed image. It is complicated but has the merits which the former approach lacks. The mostly used transforms are frequency transforms. A new and promising class of Wavelet transform is exploited nowadays.

According to how watermark is detected and extracted [7-9], the technique is either blind or nonblind. Blind-extracting watermarking means watermark detection and extraction does not depend on the availability of original image. The drawback is when the watermarked image is seriously destroyed; watermark detection will become very difficult. Nonblind-extracting watermark can only be detected by those who have a copy of original image. It guarantees better robustness but may lead to multiple claims of ownerships.

According to the ability of watermark to resist attack [7, 9], the techniques are classified as fragile and robust. Fragile watermarks are destroyed by random image processing methods. The change in watermark is easy to be detected, thus can provide information for image

completeness. Robust watermarks are unaffected under most image processing methods and can be extracted from heavily attacked watermarked image. Thus it is preferred in copyright protection.

3. Transform Domain Watermarking Techniques

The transform domain watermarking obtains much more attention as compared to spatial-domain watermark, because watermarking in transform domain is more robust and compatible to popular image compression standards. To embed a watermark, the transformation is applied to the host data and modifications are made to the transform coefficients. A well known transform domain is frequency transformations which include the Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT) and others. Other than the frequency transformations, Wavelet or SVD or any other transform can be used.

3.1 Discrete Cosine Transform (DCT)

The DCT breaks up the image into different frequency bands. Embedding watermark into the middle frequency bands of an image provides additional resistance to lossy compression techniques, while avoiding significant modification of the cover image. Embedding in DCT domain is simply done by altering the DCT coefficients, for example by changing the least significant bit of each coefficient as for JSteg algorithm [16].

The simplest algorithm for watermarking using DCT is to directly embed the DCT coefficients of the watermark into the high frequency band of the DCT coefficient matrix of the cover image. Since most of the high frequency DCT coefficients are zero and thus a watermark is easily embedded in the high frequency band after flipping the DCT matrix of the watermark so that its low frequency components fall to the high frequency side of the DCT matrix of cover image. The watermark is recovered by taking the DCT of the lower right square of the watermarked image. This works well if 8 bit image is hidden in a 16 bit image.

Another approach is to divide the image into blocks and then comparing two middle-band DCT coefficients [17] to encode a single bit into a DCT block. The two coefficients are chosen, from the standard JPEG quantization table [17], which has identical quantization values. The DCT block will encode a "1" if first coefficient is greater than the second otherwise it will encode a "0". The coefficients are then swapped if the relative size of each coefficient does not agree with the bit that is to be encoded. The comparison of the coefficients directly can be replaced by comparison of their difference [17] to some threshold value.

Another possible technique is to embed a PN sequence W into the middle frequencies (F_M) of the DCT block I using the following equations:

$$I_{W(i,j)}(u,v) = \begin{cases} I_{(i,j)}(u,v) + k * W_{(i,j)}(u,v) & u,v \in F_M \\ I_{(i,j)}(u,v) & u,v \notin F_M \end{cases}$$

where gain factor is *k*, keeping the other coefficients unaffected. Each block is then inverse-transformed to obtain watermarked image I_W. For detection, the image is broken up into blocks, and a DCT performed. If correlation of the middle frequency values of the transformed block with same PN sequence exceeds some threshold T, a "1" is detected for that block; otherwise a "0". The factor *k* denotes the strength of the watermarking, where increasing *k* increases the robustness of the watermark at the expense of quality.

3.2 Singular Value Decomposition (SVD)

SVD decomposes matrix into three matrices of same size. Let A be M X N matrix with $M \geq N$, Then, A= UDVT where the diagonal elements of D are the singular values (SVs) [18,19] which specify the luminance of an image layer while the corresponding pair of singular vectors in U and V specify the geometry of the image. The main properties of SVD from the viewpoint of image processing applications are: 1) the SVs of an image have very good stability, i.e., when a small perturbation is added to an image, its SVs do not change significantly; and 2) SVs represent intrinsic algebraic image properties.

The simplest approach is where the watermark image is embedded directly in the SVD domain. A single image is used as watermark which is embedded in the whole image. This method is blind but requires the singular values or the orthogonal matrices for retrieving the watermark.

Liu and Tan [20] used a non-blind image watermarking method which adds the scaled watermark to the matrix D and takes the SVD of this modified D, (D+aW) matrix to get UW, DW and VW. Watermarked image, AW is obtained by multiplying U, DW and V'. The watermark is detected using UW, D and VW as the keys. The possibly attacked image AW* is decomposed using SVD to U, DW and V. The obtained D* W matrix is used with the keys UW and VW, to obtain the approximate S which is used to find the approximate watermark W = (D*W – S)/a. However the keys used already include the information of original watermark unintentionally. So the modified approach was proposed by [2] which avoided using SVD on the modified D but directly used it to produce watermarked image with original U and V. The recovery procedure remains the same with original U, V and D as the keys.

The matrix U along with matrix D is exploited by [18] using block based SVD to embed the watermark. The coefficients of D matrix are modified based on the Dither quantization [18,19,21], in such a way that the watermarked image quality is not degraded. The watermark bits are embedded in the columns of U matrix based on the difference in the values of these columns. [18,21] used these approaches to embed two watermarks in the same image at two different locations. Any modification of D component degrades the perceptibility of the watermarked image, so, [19] improved perceptibility by embedding the watermark in some selected complex blocks based on the number of edges in a block. A block is qualified as a complex block, if the number edges in it is greater than a threshold value.

3.3 Discrete Wavelet Transform

Discrete Wavelet Transform (DWT) allows images to be viewed and processed at multiple resolutions and provides a powerful insight into an image's spatial and frequency characteristics. The term DWT refers to a class of transformations that differ not only in the transformation kernels employed, but also the fundamental nature of those functions and in the way in which they are applied. Since the DWT encompasses a variety of unique but related transformations so each DWT is characterized by a transform kernel pair or set of parameters that defines the pair. The basis functions of DWT are based on small waves, called wavelets, of varying frequency and limited duration. To obtain DWT, filtering splits the signal into low-pass and high-pass components and down-samples each. On each successive step the lowest frequency signal component is split in to a low-pass and high-pass component, gaining better frequency resolution at the expense of temporal resolution. Level of DWT refers to the passes of DWT.

Each pass of DWT produces four frequency bands. The simplest approach is to embed watermark in the DWT coefficients. [4,25] embeds PN sequences to the coefficients of medium and high frequency bands based on watermark bits. Correlation is then used to recover the watermark. [22] embeds the watermark bits in the sub-band of middle frequency after 3 level decomposition which has minimum energy by modifying the coefficients according to some predefined rule. [23] used the horizontal band for embedding because embedding in the approximation sub-band produces perceptible artifacts in the watermarked image. [24] embeds the watermarking data on selected groups of wavelet coefficients of the input image. Two groups of coefficients are formed after detecting the edges using a Sobel edge detector and a threshold value. Another group is formulated by a morphological dilation operation applied on the edge coefficients. The selected coefficients reside on the detail sub bands and describe the edges of the image or the region around them. The watermark strength is tuned according to the subband level and the group that each coefficient resides in. Thus, exploiting the HVS, which is less sensitive to alterations on high frequencies, the embedded information becomes invisible. The evaluation of the proposed method shows very good performance as far as invisibility and robustness is concerned. The proposed scheme behaves very well in various common signal processing operations as compression, filtering, noise, scaling and cropping.

DWT is best suited to resist compression effects [26] on watermarking because JPEG2000 is the mostly used compression standard which itself is based on DWT. [26] preprocesses the cover image according to the JPEG2000 standard before embedding to develop a robust technique to compression.

2-level decomposition is used by [27] to preprocess the original image and compare the horizontal coefficients of the two levels by calculating local relationship of wavelet coefficient. The embedded region which is calculated with a threshold in the LH2 sub-band is decided by the priority order of interrelation. The algorithm is shown to be relatively robust in regard of such attacks as JPEG, Sharpening and Blurring.

Watermarking is done in the high frequency coefficients too. [30] decomposes an input image into non-overlapping blocks and embeds a watermark into the high frequency wavelet coefficients of each block. Arbitrary wavelet and block size are derived to avoid the underflow and overflow conditions. Embedded payload contains message and information for reconstructing exact original image.

Multiple watermarks can also be embedded to increase the robustness of the technique against cropping, scaling and compression. [18,28] exploited this second dimension of watermarking, by embedding two watermarks simultaneously in one cover image using DWT and [18] used this approach with SVD.

4. HYBRID WATERMARKING

Multiple techniques in the transform domains are simultaneously used to watermark the digital images. This forms a new class of watermarking: Hybrid watermarking. Many algorithms have been published and many are in process. This class attracts most researchers as it enables them to exploit the advantages of each of the transform used to suppress the limitations and disadvantages of the other transforms. [29] maps zigzag sequence of DCT coefficients of the cover image in to 4 quadrants followed by taking SVD for each block. The same process is done on the watermark. Thus, four watermarks are embedded one in each block. The coefficients of each block are modified with those of the watermark. The inverse

transforms in the reverse sequence, produces watermarked image.

5. CONCLUSION

In this paper, a survey of transform domain watermarking technique for digital images is presented. Discrete Cosine Transform domain, Singular Value Decomposition domain and Discrete Wavelet Transform domain are greatly used for watermark embedding. The last class of watermarking techniques, hybrid watermarking techniques are greatly exploited which overcomes the disadvantages of individual techniques and it is more robust. The DWT based techniques are resistant to compression so, they should be combined with other transforms discussed in this paper and beyond to develop robust watermarking techniques.

REFERENCES

1. Motameni H., Norouzi M., Jahandar M., Hatami A., "Labeling Method in Steganography". *Proceedings of World Academy of Science, Engineering and Technology*, Volume 24, October 2007, ISSN 1307-6884.
2. Pei S., Liu H., "Improved SVD based Watermarking for Digital Images", *Sixth Indian Conference on Computer Vision, Graphics and Image Processing, IEEE Computer Society*, 2008.
3. Singh Neha, Nandi Arnab," Digital Watermarking: Mark this Technology!".
4. Vallabha V.H.,"Multiresolution Watermark Based on Wavelet Transform of Digital Images", Multiresolution watermarking of Digital Images, Cranes Software International Limited.
5. Miller Matt L., Cox Ingemar J., Linnartz Jean-Paul M. G., Kalker Ton, "A Review of Watermarking Principles and Practices". *Chapter 18, Digital Signal Processing in Multimedia Systems*, Ed. K. K. Parhi and T. Nishitani, Marcell Dekker Inc., 461-485, (1999).
6. Potdar Vidyasagar M., Han Song, Chang Elizabeth, " A Survey of Digital Image Watermarking Techniques". *3rd IEEE International Conference on Industrial Informatics* , 2005.
7. Bleumer Gerrit," Watermarking". *Unknown*, 2004.
8. Genov P. Eugene," Digital Watermarking of Bitmap Images". *International Conference on Computer Systems and Technologies- CompSysTech '07*, 2007.
9. Schyndel Ron G. van, Trikel Andrew Z., Svalbe Imants. D., Hall Thomas E., Osborne Charles F., "Spread Spectrum Digital Watermarking Concepts and Higher Dimensional Array Canostruction". *Online symposium for Electronics Beginners*.
10. Chandramouli R., Memon Nasir, "Analysis of LSB based Image Steganography Techniques". *IEEE* ,0-7803-6725-1/01/2001, pages 1019-1022.
11. Lin Eugene T., Delp Edward J.,"A Review of Data Hiding in Digital Images", Prudune University.
12. Dijk Marten van, Willems Frans, "Embedding Information in Gray scale Images", Philips Research Laboratories, Eindhoven.
13. Curran Kevin, Li Xuelong, Clarke Roisin, "An investigation into the use of the Least Significant Bit Substitution Techniques in Digital Watermarking". *American Journal of Applied Science*, 2 (3):648-685, 2005, ISSN 1546-9239.
14. Wolfgangand Raymond B., Delp Edward J., "Overview of Image Security Techniques with Applications in Multimedia Systems". Prudune University.
15. Langelaar G., Setyawan I., Lagendijk R. L., "Watermarking Digital Image and Video Data". *IEEE Signal Processing Magazine*, Vol 17, pp 20-43, September 2000.
16. Provos Niels, Honeyman Peter, "Hide and Seek: An Introduction to Steganography", *IEEE Computer Society*, *IEEE Security and Privacy Journal*, 2003,
17. Tewari T.K., Saxena Vikas, "An Improved and Robust DCT based Digital Image Watermarking Scheme", *International Journal of Computer Applications*, Volume 3, No.1, June 2010.
18. Mohan B. Chandra, Kumar S. Srinivas, "A Robust Image Watermarking Scheme Using Singular Value Decomposition". *Journal of Multimedia*, Volume 3, No. 1, May 2008.
19. Mohan B. Chandra, Kumar S. Srinivas, Chhatterji B. N., "A Robust Digital Image Watermarking Scheme Using Singular Value Decomposition (SVD), Dither Quantization and Edge Detection". *ICGST-GVIP Journal*, ISSN:1687-398X, Volume 8, issue 1, June 2008.
20. Liu R., Tan Tieniu, "An SVD-Based Watermarking Scheme for Protecting Rightful Ownership", *IEEE Transactions of Multimedia*, Vol. 4, No. 1, March 2002.
21. Singh N., Sharma M.M., "Singular Value Decomposition Technique for Digital Image Watermarking", National Conference on Advances in Wireless and Optical Communication Technique, 2010.
22. Tay P., Havlicek J.P., " Image Watermarking Using Wavelets", IEEE, 2002.
23. Hajjara Suhad, Abdallah Moussa, Hudaib Amjad," Digital Image Watermarking Using Localized Biorthogonal Wavelets", *European Jounal of Scientific Research*, Vol.26 No. 4, 2009, 594-608.
24. Ellinas John N., "A Robust Wavelet-Based Watermarking Algorithm Using Edge Detection", *PWASET Volume 25 November 2007*, 438-443.
25. Maity Santi P., Kundu Malay K., " A Blind CDMA Watermarking Scheme in Wavelet Domain", *0-7803-8554-3, IEEE, 2004*, 2633- 2636.
26. Dazhi Zhang, Boying Wu., Jiebao Sun, "A Robust Image Watermarking Algorithm Against JPEG2000",

IEEE Proceedings of International Conference on Communications and Mobile Computing, 2009,430-434.

27. Park Ki Hong, Kim Yoon Ho, Lee Joo Shin, "Watermarking using the local relation of wavelet coefficient", IEEE *Proceedings of Second International Conference on Future Generation Communication and Networking*, 2008. 209-212.

28. Sharkas Maha, ElShafie Dahlia, and Hamdy Nadder, "A Dual Digital-Image Watermarking Technique", Proceedings of World Academy of Science, Engineering and Technology, Volume 5, April 2005, 136-139.

29. Sverdlov Alexander, Dexter Scott, Eskicioglu Ahmet M., " Secure DCT-SVD Domain Image Watermarking: Embeddig Data in All Frequencies", Unknown.

30. Lee Sunil and Yoo Chang D. and Kalker Ton, *Fellow, IEEE* "Reversible Image Watermarking Based on Integer-to-Integer Wavelet Transform"

