International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 4 | Issue 3| ISSN : 2456-3307

Image Watermarking is the Process of Embedding an Imperceptible Data (Watermark) Into Cover Image

Mrs. B. Arulmozhi[1], Mrs. S. Kavitha[2], Mrs. S. Shanthi[3]

[1]Head of the Department (BCA), Dept of Computer Science and Applications, D.K.M College for Women (Autonomous), Vellore, Tamilnadu, India

[2]Research Scholar, Dept of Computer Science and Applications, D.K.M College for Women (Autonomous), Vellore, Tamilnadu, India

[3]Assistant Professor, Dept of Computer Science and Applications, D.K.M College for Women (Autonomous), Vellore, Tamilnadu, India

ABSTRACT

Image watermarking schemes are used to protect the digital images. Image watermarking is the process of embedding an imperceptible data (watermark) into cover image. The image watermarking schemes have been widely used to solve the copyright protection problems of digital image related to illegal usage or distribution. Several image watermarking schemes are proposed, considering different view points. The image Watermarking schemes are classified into different types based on domain of processing, visibility of watermark and rigidity of scheme. Not very many watermarking plans have been proposed for characterizing the copyrights of shading picture. To resolve the copyright protection problem of color image, we propose an effective, robust and imperceptible colorimage watermarking scheme. This plan implants the watermark into cover picture in (Red, Green, Blue) RGB space. The combination of Discrete Wavelet Transformation (DWT) and Singular Value Decomposition (SVD) of Blue channel is used to embed the watermark. The singular values of different subband coefficients of Blue channel are modified using different scaling factors to embed the singular values of the watermark. The copy of the watermark is embedded into four subbandcoefficients which are very difficult to remove or destroy. The combination of DWT and SVD increases the security, robustness and imperceptibility of the scheme.

Keywords: DWT, Digital Water Mark, Perceptivity, Image, DCT-Domain, SVD, Data Embedding

I. INTRODUCTION

Illegal copying, modifying, tampering and copyright protection have become very important issues with the rapid use of internet. Digital Watermarking is the process of hiding or embedding an imperceptible signal(data) into the given signal(data).This imperceptible signal(data) is called watermark or metadata and the given signal(data) is called cover work. This cover work can be an image, audio or a video file. A watermarking algorithm consists of two algorithms, an embedding and an extraction (or detection) algorithm. Watermarking techniques can be broadly classified into two categories: Spatial and Transform domain methods. Spatial domain methods are less complex and not robust against various attacks as no transform is used in them.A singular value decomposition (SVD) is usedas a new transform for watermarking. The SVD based water marking algorithm is introduced by Liu et al. SVD transform was again applied on the resultant matrix for finding the modified singular values.

II. CHOINCE OF WATERMARK-OBJECT

The main inquiry we have to ask with any watermarking or stenographic framework is what shape will the implanted message take? The most straight-forward approach is insert Content strings into a picture, enabling a picture to straightforwardly convey data, for example, creator, title, date… et cetera. The drawback however to this approach is that ASCII text in a way can be considered to be a form of LZW compression, which each letter being represented with a certain pattern of bits. By compressing the watermark-object before insertion, robustness suffers.

Due to the nature of ASCII codes, a single bit error due to an attack can entirely change the meaning of that character, and thus the message. It would be very simple for even a basic undertaking, for example, JPEG pressure to lessen a copyright string to an arbitrary accumulation of characters. Or maybe then characters, for what reason not install the data in an as of now profoundly excess frame, for example, a raster picture? Not exclusively do pictures loan themselves to picture watermarking applications, yet the properties of the HVS can without much of a stretch be misused in acknowledgment of a corrupted watermark.

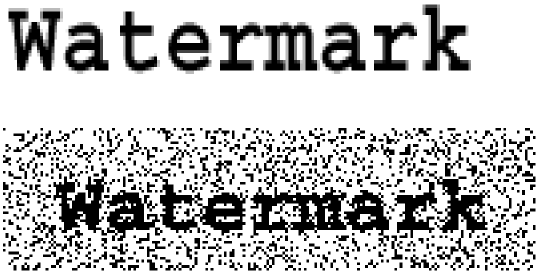


Figure 1. Ideal Watermark-Object vs. Object with 25%Additive Gaussian Noise

Note that despite the high number of errors made in watermark detection, the retrieved watermark is still highly recognizable.

III. OVERVIEW OF MULTIMEDIA DATA HIDING

The ideas of information hiding can be traced back to a few thousand years ago. In many rivalry environments, concealing the existence of communication is desirable to avoid suspicion from adversaries.

The word “steganography”, which originated from Greek and is still in use today, literally means “covered writing”. Stories of covert communications have been passed for generations, but they were mainly used by military and intelligence agencies. It is until the recent decade that information hiding began receiving wide attention from research community and information technology industry, with hundreds of publications and dozens of patents coming out in the past few years.

- Authentication or Tampering Detection: a set of secondary data is embedded in the multimedia source beforehand, and later is used to determine whether the host media is tampered or not. The robustness against removing the watermark or making it undetectable is not a concern as there is no such incentive from attacker point of view. However, forging a valid authentication watermark in an unauthorized or tampered media source must be prevented.
- Fingerprinting or labeling: the watermark in this application is used to trace the originator or recipients of a particular copy of multimedia source. For example, different watermarks are embedded in different copies of multimedia sources before distributing to a number of recipients. The robustness against obliterating and the ability to convey a non-trivial number of bits are required.

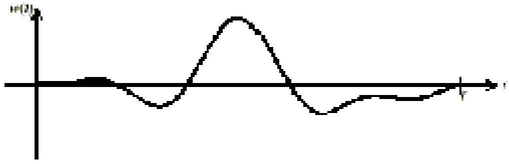
Using Least Significant Bit manipulation, a huge amount of information can be hidden with very little impact to image quality. This technique is performed in the spatial domain. The embedding of the watermark is performed choosing a subset of image pixels and substituting the least significant bit of each of the chosen pixels with watermark bits. The extracted bits do not have to exactly match with the inserted bits.

A correlation measure of both bit vectors can be calculated. If the correlation of extracted bits and inserted bits is above a certain threshold, then the extraction algorithm can decide that the watermark is detected. The implementation of this algorithm is quite simple. However, some policy decisions should be made. For example, how should the set of pixels to be modified be selected? One way to select these elements is by using a pseudorandom number generator also; the watermark extractor should have access to these selected elements.

IV. WAVELET TRANSFORM

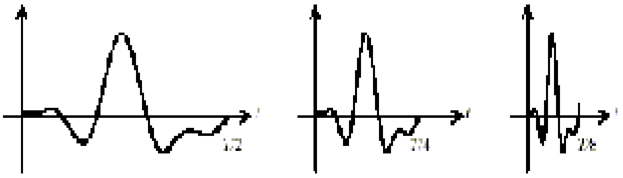
Wavelets are scientific capacities characterized over a limited interim and having a normal estimation of zero that change information into various recurrence parts, speaking to every segment with a determination coordinated to its scale.

The basic idea of the wavelet transform is to represent any arbitrary function as a superposition of a set of such wavelets or basis functions. These preface limits or newborn child wavelets are gotten from a singular model wavelet called the mother wavelet, by growths or withdrawals (scaling) and translations (shifts). They have advantages over traditional Fourier methods in analyzing physical situations where the signal contains discontinuities and sharp spikes. Numerous new wavelet applications, for example, picture pressure, turbulence, human vision, radar, and seismic tremor expectation are produced lately. In wavelet transform the basis functions are wavelets. Wavelets tend to be irregular and symmetric. All wavelet functions, $w(2kt - m)$, are derived from a single mother wavelet, $w(t)$.



Mother wavelet w(t)

Normally it starts at time $t = 0$ and ends at $t = T$. The shifted wavelet $w(t - m)$ starts at $t = m$ and ends at $t = m + T$. The scaled wavelets $w(2kt)$ start at $t = 0$ and end at $t = T/2k$. Their graphs are $w(t)$ compressed by the factor of $2k$ as , when $k = 1$, the wavelet is If $k = 2$ and 3, they are shown in (b) and (c), respectively.



Scaled wavelets

(a)w(2t) (b)w(4t) (c)w(8t)

The wavelets are called orthogonal when their inner products are zero. Wide wavelets are comparable to low-frequency sinusoids and narrow wavelets are comparable to high-frequency sinusoids.

V. SINGULAR VALUE DECOMPOSITON

A. The Watermark Embedding Procedure

To utilize the characteristics of the SVD domain for embedding a watermark, the coefficients of the D and U components were explored . In our observation, two important features of the D and U components were found. In the first feature, the number of non-zero coefficients in the D component could be used to determine the complexity of a block (matrix).Generally, the greater number of non-zero coefficients would indicate greater complexity. For a block-based watermarking scheme, a more complex block was favored for embedding a watermark with perceptibility. IN the second feature, the relationship between the coefficients in the first column of the U component could be preserved when general image processing was performed. Both features were supporting the idea to develop a robust SVD-based watermarking scheme.

In the proposed watermarking scheme , the host image was a gray-level image. The watermark W was a binary image consisting of wxh bits, where W=(w $_1$,w $_2$ ……w $_{nxh}$) and w $_1$ ε (0,1).

The host image was first partitioned into blocks with nxn pixels. And then the blocks were transformed by SVD. The number of non-zero coefficients in the D component of each block was calculated to determine the complexity of this block .A set of greater complexity blocks was selected according to pseudo random number generator (PRNG).And the feature of the D component. Using the PRNG increases the watermarking security. Applying the feature of the D component prevents the smooth blocks from being selected and benefits the perceptibility of the watermarked image.

On each selected block, the relationship between the first column coefficients in the **U** component was examined. This relationship could be taken as the magnitude difference between the neighboring coefficients. The magnitude difference could be either a positive or non-positive value. When the positive difference was computed, a positive relationship would be assigned. Otherwise, a negative relationship would be assigned. The relationship could be preserved when general image processing was performed. In other words, when one coefficient had a larger magnitude than the other, the positive relationship was not easily affected by image processing.

An example shown in Table 1 illustrates the relationship between the **U** component coefficients. Table 1(a) and (b) show the original block and the **JPEG** compressed block, respectively .Both the **SVD** transformed u components of Table 1(a) and (b) are shown in table 1(c) and (d) ,it can be observed that the positive relationships (i.e.), between the coordinates (1,1) and (1,2) were still preserved. As in Table 1(c) and (d) even though the compression processing was performed.

According to the features of the **U** component, it would seem that if a positive relationship is found, bit value of 1 would be hidden. Otherwise, a bit value of zero would be embedded. From that , the coefficients of the **U** component might be modified for embedding a watermark (e.g. positive relationship matching a bit value of 1 or negative relationship matching a bit value of 0), the coefficients are retained . Second, if the magnitude difference does not match the embedding watermark, the coefficients must be modified. However, the modification of **U** component coefficients may alter the original pixel values and degrade the quality of watermarked image. The larger the modification of the **U** component, the more the distortion of image quality and the stronger the robustness. On the other hand, the smaller modification implies that a better image quality and a weaker resistance have been achieved. There is, in other words, a tradeoff between robustness and quality.

To hold the picture quality and give a more grounded strength of a watermarking plan, the coefficient alteration is additionally considered. For each selected greater complexity block, the magnitude difference matched the watermark but was smaller than the predefined magnitude difference threshold, both coefficients had to be further modified. Both coefficients modification not only reduce the image perceptibility but also enhance the robustness to resist attacks. In addition, if the second scenario described in the above accounted , the magnitude difference between two modified coefficients must greater than or equal to the predefined magnitude difference threshold. It means that the gap between two modified coefficients must larger enough to against attacks.

VI. CONCLUSION

The Project presented a DWT- SVD based non-blind watermarking scheme. The SVD is an efficient tool for watermarking in the DWT domain. To embed the watermark into cover image the scaling factor is chosen from a wide range of values for all subbands. The transformed image has the approximation and detailed information. The same watermark is embedded into four subbands which are LH, HL, HH subbands because it is very difficult to remove or destroy. The extraction of logo image from the watermarked image is the opposite of embedding technique. The unbending nature of the proposed conspire is dissected by thinking about different sorts of picture handling assaults. The scheme was found robust to various types of image processing attacks. Finally, the performance validation shows the value of mean square error between the input and embedded image and peak signal to noise ratio factor for justifying the image quality.

VII. REFERENCES

[1] S. Kay and E. Izquierdo, “Robust content based image watermarking,” in Proc. Workshop on Image Analysis for Multimedia Interactive Services, WIAMIS’ 2001, Tampere, Finland, May 2001.

[2] S. Kak and A. Chatterjee, “On decimal sequences,” IEEE Trans. Information Theory, vol. IT—27, pp. 647–652, 1981.

[3] S. Kak, “Encryption and error-correction coding using D sequences,” IEEE Trans. Computers, vol. C-34, pp. 803–809, 1985.

[4] N. Mandhani and S. Kak, “Watermarking using decimal sequences,” Cryptologia, vol. 29, pp. 50–58, 2005, arXiv: cs.CR/0602003.

[5] R. B. Wolfgang and E. J. Delp, “A watermark for digital images,” in Proc. 1996 Int. Conference on Image Processing, Lausanne, Switzerland, Sept. 1996, vol. 3, pp. 219–222.

[6] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, “Secure spread spectrum watermarking for multimedia,” IEEE Trans. Image Processing, vol. 6, pp. 1673–1687, Dec. 1997.

[7] J. J. K. Ó Ruanaidh, W. J. Dowling, and F. M. Boland, “Watermarking digital images for copyright protection,” Proceedings of the IEEE, Vision, Image and Signal Processing, vol. 143, pp. 250–256, Aug. 1996.

[8] G. Schuller, “Time-Varying Filter Banks with Low Delay for Audio Coding,” in Proc. 105th Conv. Aud. Eng. Soc.,preprint #4809, Sep. 1998.

[9] F. Baumgarte, “Evaluation of a Physiological Ear Model Considering Masking Effects Relevant to Audio Coding,” in Proc. 105th Conv. Aud. Eng. Soc., preprint #4789, Sep. 1998.

[10] Y. Huang and T Chiueh, “A New Forward Masking Model and Its Application to Perceptual Audio Coding,” in Proc.ICASSP-99, Mar. 1999.

[11] C. Lanciani and R. Schafer, “Subband-Domain Filtering of MPEG Audio Signals,” in Proc. ICASSP-99, Mar. 1999.

[12] C. Neubauer and J. Herre, “Digital Watermarking and Its Influence on Audio Quality,” in Proc. 105th Conv. Aud. Eng. Soc., preprint #4823, Sep. 1998.