ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Volume 1, Issue 6, August 2013

Imperceptible Digital Image Watermarking

AR.Arunachalam

Assistant Professor, Department of Computer Science & Engineering, Bharath University, Chennai, Tamilnadu, India

ABSTRACT : The procedure of digital image watermarking can be delineated as a method for embedding information into another image. The embedding image can be either visible or hidden from the user. In this project we will concentrate on imperceptible watermarks. The principal intention of digital watermarks is to provide copyright protection for intellectual property that is in digital format. One of the main challenges of the watermarking problem is to achieve a better tradeoff between robustness and perceptivity. Robustness can be achieved by increasing the strength of the embedded watermark. DWT technique is used as it provides both a simultaneous spatial localization and a frequency spread of the watermark within the host image. This scheme is highly efficient as the watermark is employed with chaotic map to shuffle the pixel position of the image. Embedding process produced good results for images of different sizes and formats.

KEYWORDS: DWT, Digital Watermark, Robustness, Perceptivity, Chaotic Map, Spatial Localization

1. INTRODUCTION

Image processing is any form of signal processing for which the input is an image, such as a photograph or video frame; the output of image processing may be either an image or, a set of characteristics or parameters related to the image. Most image-processing techniques involve treating the image as a two-dimensional signal and apply standard techniques to it. Image processing usually refers to digital image processing, optical and analog image processing also are possible. This article is about general techniques that apply to digital image processing.
Digital watermarking is a process of embedding information into a digital media such as image, audio, text etc. Watermarking is similar to steganography. Both will embed information inside a multimedia data with little to no degradation of that data. Watermarking adds an additional requirement of robustness. An ideal steganographic system would embed a large amount of information, securely with no visible degradation to the multimedia data. An ideal watermarking system would embed an amount of information that could not be removed or altered without making the multimedia data entirely unusable.

The aim of Frequency Domain technique is to embed watermark in the spectral coefficients of the image. The reason for watermarking in the frequency domain is that the characteristics of the human visual system (HVS) are better captured by the spectral coefficients. For example, the HVS is more sensitive to low-frequency coefficients, and less sensitive to high frequency coefficients. In other words, low-frequency coefficients are perceptually significant, which means alterations to those components might cause distortion to the original image. On the other hand, high-frequency coefficients are considered insignificant.

In the case of one-dimensional signal, the signal is to be divided into two groups of frequency component as low frequency components and high frequency components which are mainly determined as the 1st pass of the low-pass and high-pass frequencies. While the high-band frequency group would remain unchanged, the low-band frequency group is then divided into two other inner groups of frequencies causing the 2nd pass of the low-pass and high-pass frequencies. The same process is to be continued in such an arbitrary number of times making the next passes by dividing the low-pass frequency blocks.

With regard to a still image that consist of a two-dimensional signal, it is to be decomposed into DWT pyramid structure with various frequency bands such that low-low frequency band, low-high frequency band, high-low frequency band and high-high frequency band components.

DWT based watermarking algorithm of color images is proposed (Guangmin, 2007). In his scheme the RGB color space is converted into YIQ color space and watermark is embedded in Y and Q components. This method dealt with JPEG Compression attack and achieved good result. Watermarking using multi-resolution wavelet decomposition is proposed (Kundur, 1998). He decomposed the cover image into non overlapping multi-resolution discrete wavelet decomposition and used the decomposed level for watermarking. His scheme proved increased robustness of watermarked images and resist to most image processing attacks. A robust logo image watermarking is proposed (Hien, 2004). He used a binary logo as the watermark image. Independent Component Analysis is done for the images and then embedded with the logo watermark which proved high imperceptibility of watermarked images.

III. PREVIOUS RESEARCH

Sanjay Rawat et al (2011) proposed a novel chaos based watermarking scheme for image authentication and tamper detection. This scheme provides both integrity and authenticity for digital watermarking. Extracting the right watermark is only possible if someone has correct keys. Since chaotic maps are sensitive to initial values, they are used as key in this scheme. A person with wrong keys will not be able to forge the watermark. In order to thwart counterfeiting attacks it is essential to break pixel wise independency, this scheme employs chaotic maps to break the corresponding position relation between pixels in the watermarked image and the watermark. Provides high fidelity and is capable of localizing modified regions in watermarked image.

Chih-Chin Lai et al (2011) proposed an image watermarking technique based on Singular Value Decomposition and Tiny-Genetic Algorithm. The singular values of the cover image are modified to embed the watermark. The Tiny-GA offers a systematic way to consider the improvements of the scaling factors that are used to control the strength of the embedded watermark. With this scheme, embedded watermark successfully survived after attacked by image-processing operations. Simulation results show that the proposed scheme outperforms the other similar works.

Yong-Gang Fu et al (2012) proposed a novel asymmetric watermarking scheme. Both the user side watermark and copyright owner’s one are generated from the copyright owner’s private keys, and the watermark detection can be finished either by public watermark or the copyright owner’s private one. Given the public watermark, it is impossible to guess or remove the embedded watermark. Experimental results against removal attack and Jpeg compression show good robustness in this scheme.

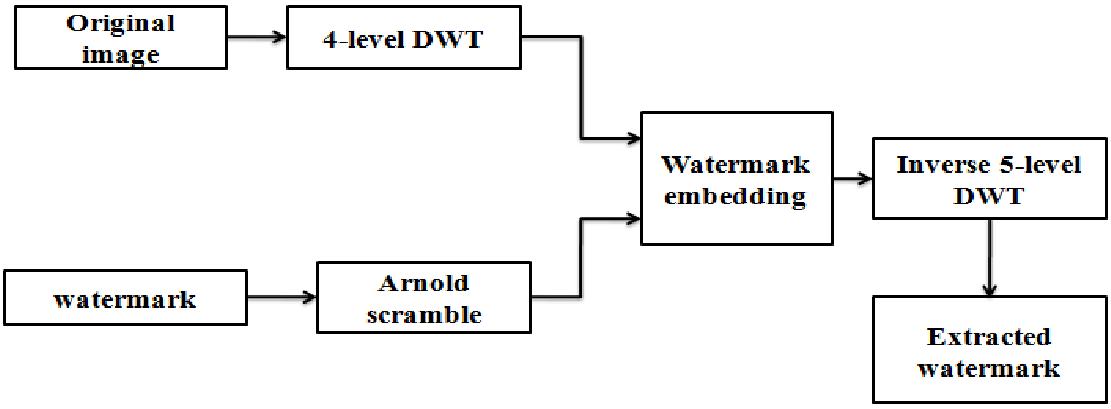
Zhou Zude et al (2006) proposed a novel digital watermarking scheme for color image, watermarking image was embedded into the corresponding wavelet coefficients of the original image's R, G, B sub images via discrete wavelet transform. The availability of the extracted watermark is evaluated by comparing the normalized correlation coefficients of the extracted watermark with the original one. Experiment results show high robustness of this approach to the common image processing technique such as JPEG compression and additive noise etc.

J. Dittmann et al (1999) Development of new multimedia services and environments requires new concepts both to support the new working process and to protect the multimedia data during the production and distribution. This scheme addresses image video authentication and copyright protection as major security demands in digital marketplaces. First a content-based signature technique for image and video authenticity and integrity is presented. Based on this technique, a tool for interactive video authentication and propose content fragile watermarking, a concept which combines watermarking and content-based digital signatures to ensure copyright protection and detection of integrity violation has been implemented.

III. PROPOSED SYSTEM

3.1 Architecture

Figure1: Image Watermarking Architecture



The original gray scale image is taken as the input. Apply DWT on the cover image and separate levels based on low and high frequencies. Bitmap gray scale image of size n×n is read, which is taken as the watermark image. Shuffle the bitmap image by applying Arnold's Cat Map Transform on the watermark. After decomposition embed the 4^{th} level horizontal coefficients of cover image with the shuffled watermark image. Merge the resultant image with all the other decomposed coefficients. Apply inverse 4-level DWT on the extracted image coefficients and the resultant outcome will be the watermarked image. Apply the same process from the beginning to extract the shuffled watermark image. Arnold's Cat Map is applied k times to get the original watermark image.

3.2 Algorithm

3.2.1 Discrete Wavelet Transform

- Input Image: Gray scale image of size 512*512 is taken as the original cover image.
- Bitmap image of size 256*256 is taken as the watermark image.
- Watermark image is decomposed if necessary.
- 4-level DWT equation is as follows,

$y(2n+1) = x(2n+1) - [(x(2n)+(2n+2))/2]$

$y(2n)=x(2n)+[(y(2n-1)+y(2n+1))/4]$

- Apply wavelet decomposition on cover image and get the image coefficients.

3.2.2 Arnold Cat Map Transform

- Read watermark bitmap image of size n × n.
- Employ 2D Arnold cat map to shuffle the pixel positions of the watermark image.
- This map has the form,

$\bar{p} = p + x \text{ (mod L)}$

$\bar{x} = x + \bar{p} \text{ (mod 1)}$

- The resultant will be shuffled watermark image.

3.2.3 Watermark Embedding

- The formula for watermark embedding is,

$C_w(i) = Y_o(i)+\alpha 1w(i)$

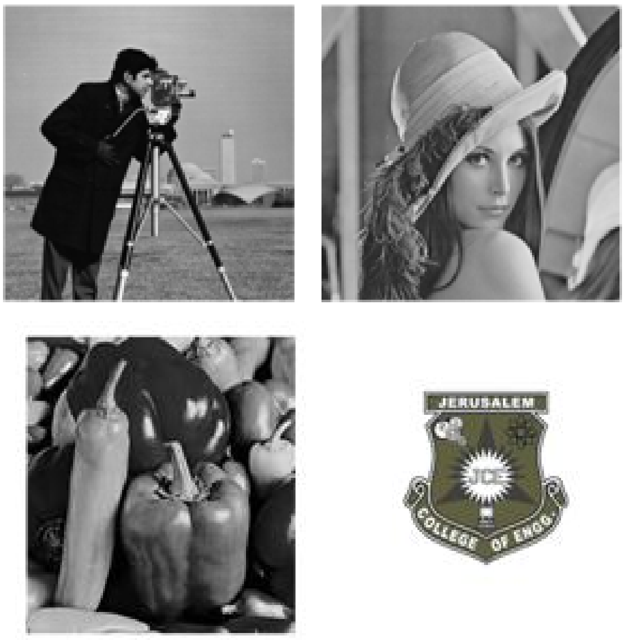
- Shuffled watermark image and DWT applied cover image are embed to get the embed coefficients.
- Apply inverse DWT on the embed coefficients to get the Watermarked Image.

IV. IMPLEMENTATION RESULTS

Figure 2(a) shows the standard input images of dimension 512x512.Initially I experimented with 256x256 size gray scale and color image and then with 512x512 gray scale image. Images of any size and any formats can be taken as the cover image since the experimental results have proved good imperceptible watermarking for all images.

Figure 2(b) shows the watermark images of size 256x256.These images are resized if necessary based on the level of decomposition of input image. Images of different sizes can be taken as watermark. If the watermark size is greater than that of the 4th level decomposed cover image then resize the image using any suitable preprocessing operation.

Figure2: (a) Original Images (b) Watermark Images



(a) (b)

Figure 3 shows the experimental result of 4-level wavelet decomposition done in cameraman image of size 512*512. The figure shows only the horizontal components from all the levels since we will embed only the horizontal coefficients of the cover image. Since horizontal level is impossible for an unauthorized user to predict and the watermark will be very much secure it is taken for embedding process.

Figure3: Horizontal levels of cover image from level1-level4

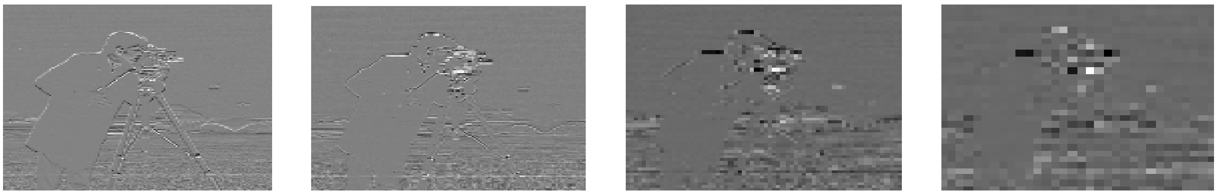
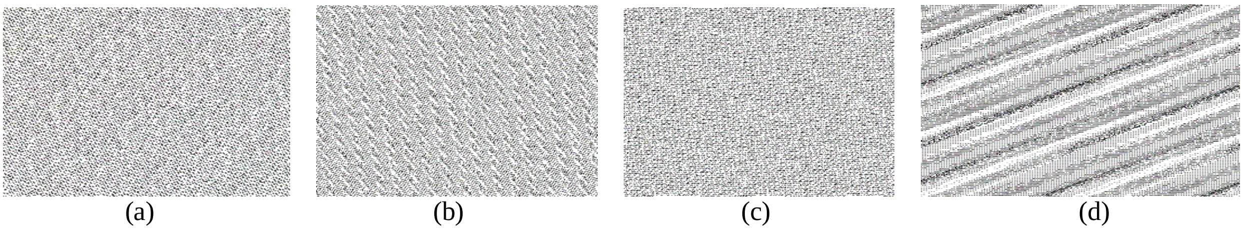


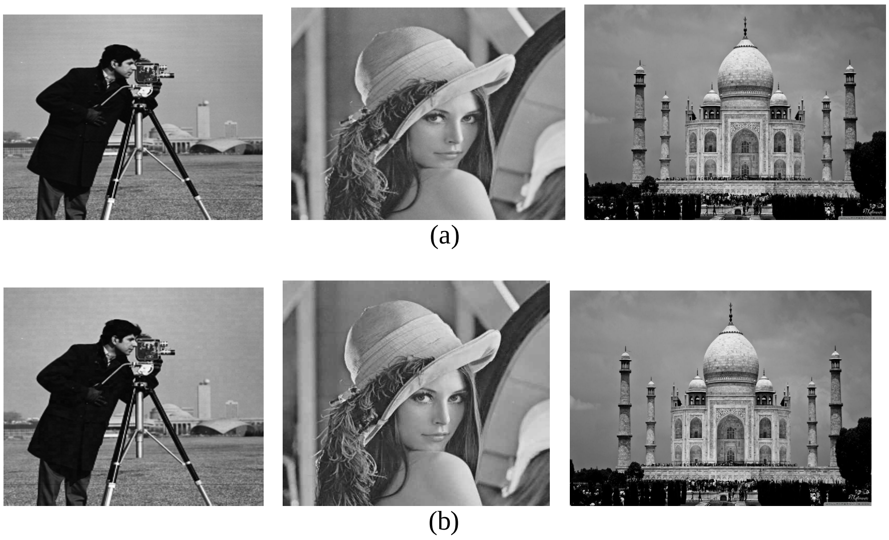
Figure 4 shows the Arnold Cat Map transformed watermark with different key values. Note that the key value should not be in the multiple of reconstruction periodic level of watermark. Since chaotic map is sensitive to initial values it is taken as the key for shuffling the image.

Figure4: Shuffled Images with different key values (a) k=8 (b) k=35 (c) k=62 (d) k=98



(a) (b) (c) (d)

Figure5: (a) Original Images (b) Watermarked Images



(a)

(b)

Figure 5 shows the original images and the watermarked images. As we can see this scheme is highly effective for digital image watermarking since it support all the image sizes and of various image formats. The watermark taken is shuffled to certain extent and the image taken to embed is the 4th horizontal level of wavelet decomposition.

VI. CONCLUSION

An effective digital watermark scheme must meet three main properties: security, imperceptibility and robustness. Imperceptibility property can be described as the characteristic of hiding a watermark so that it does not degrade the visual quality of the image. Whichever modifications occurred by means of watermark embedding should be below the perceptible threshold. Robustness is the capability of the watermark to withstand distortion that has been introduced by malicious image processing. No person has the ability to modify, or damage the watermark without the owner’s consent.

Security is the ability that watermark can resist malicious attacks. Images can be securely watermarked so that no unauthorized person can detect or remove watermark from the watermarked image. By invisibly embedding the 4th level approximation level of cover image with Arnold transformed watermark image the first two properties are met. Watermarked image is compared with various attacks and produced good results.

In future Image Security can be checked well with extracting the watermark from the original image without image quality degradation.

REFERENCES

[1] Sanjay Rawat and Balasubramanian Raman, 2011. “A chaotic system based fragile watermarking scheme for image tamper detection,” *Int. J. Electron. Commun*, Vol. 65, pp. 840-847.

[2] Chih-Chin Lai, 2011. “A digital watermarking scheme based on singular value decomposition and tiny genetic algorithm,” *Int. Conf. Digital Signal Processing*, Vol. 21, pp. 522–527.

[3] Yong-Gang Fu, 2012. “Asymmetric Watermarking Scheme Based on Shuffling,” *Int. WIEE*, Vol. 29, pp. 1640-1644.

[4] Zhou Zude, Ai Qingsong, and Liu Quan, 2006. “Digital Watermarking Scheme for Color Image Based on Image Fusion,” *Proc. ICWMM.*

[5] J. Dittmann, A. Steinmetz, and R. Steinmetz, 1999. “Content-based digital signature for motion pictures authentication and content-fragile watermarking,” *in Proc. IEEE Int. Conf. Multimedia Computing System*, pp. 209-213.

[6] JJ. Eggers and B. Girod, 2001. “Blind watermarking applied to image authentication,” *in Proc. IEEE Int. Conf. Acoustics, Speech and Signal Processing*, pp. 1977–1980.

[7] M. Yeung and F. Mintzer, 1997. “An invisible watermarking technique for image verification,” *in Proc. IEEE Int. Conf. Image Processing*, pp. 680–683.

[8] J. Fridrich, M. Goljan, and A. C. Baldoza, 2000. “New fragile authentication watermark for Images,” *in Proc. IEEE Int. Conf. Image Processing*, Vol. 1, pp. 446–449.

[9] Snehal V. Patel and Arvind R. Yadav, 2011. “Invisible Digital Video Watermarking Using 4-level DWT,” *National. Conf. Recent Trends in Engineering & Technology*.

[10] Baisa L. Gunjal and Suresh N.Mali, 2011. “Secured color image watermarking technique in DWT - DCT domain,” *in Proc. Int. J. Computer Science, Engineering and Information Technology (IJCSEIT)*, Vol. 1, No. 3.