61

S.E.S. COLLEGE OF ENGINEERING , NAVALNAGAR

→ Jointly With ←

IEEE Bombay Section
IEEE BOMBAY SECTION

IEEE Computer Society IEEE
Computer Society

Proudly Presents

INTERNATIONAL CONFERENCE ON SCIENCE, ENGINEERING & SPIRITUALITY

ICSES' 10

April -1st & 2nd, 2010

Co-Sponsored by

MIR Labs (USA)
&
Prof. Subra. Ganesan, Director,
Real Time Systems Lab ,
Oakland University (USA)

Oakland UNIVERSITY

MIR Labs

Spatial Domain Image Watermarking: Very Easy Approaches to hide one image behind other image

A..C. Suthar[1], *G. R. Joshi*[2], *A. M.Kothari*[3]

[1,2,3] C. U. Shah College of Engineering and Technology, Wadhwan city, Gujarat, India,
acsuthar@ieee.org
grjoshi@yahoo.com
amkothari@aits.edu.ac.in

ABSTRACT

A lossless data embedding method that inserts data in images in the spatial domain is proposed in this paper. The proposed method restores the original image as well as extracts hidden data from an image in which data are embedded. One and only one parameter based on statistics of pixels is used to embed and extract data. This method requires neither any reference images nor memorization of positions of pixels in which data are hidden to extract embedded data. In addition, the proposed method can control the payload of hidden data and the quality of an image conveying hidden data by controlling the parameter. Simulation results show the effectiveness of the proposed method.

KEY WORDS

Watermarking, Watermark Detection, Spatial Domain, Frequency Domain,

1. Introduction

The rapid development of computer network and multimedia technology makes it easier to assess digital media all over the world. Since the problem of illegal reproduction and modifications has become more serious than before, it is important to protect the intellectual property of digital media. To tackle the problem, digital watermark has been proposed as a means to identify the owner of digital media such as text, image, video and audio. The watermarking technique embeds authors' information into digital media and provides the corresponding authentication mechanism. Satisfactory digital watermarking must meet the following requirements: Robustness, Imperceptibility, and Security. In general, the proposed image watermarking techniques are divided into two groups, namely embedding watermark in spatial domain and in frequency domain, depending on the processing domain of cover image in which the watermark is embedded.

The paper is divided in nine sections; in section 2 we have discussed characteristics watermarking. Watermarking techniques are classified in section 3. Requirements of digital watermarking are elaborated in section 4. In section 5 some watermarking applications are listed. Our approach procedures of the watermarking are explained in section 6. Watermark generation and watermark detection results are discussed in section 7. Section 8 concludes the paper.

2. Characteristics of Digital Watermarking

Digital watermarks have several desirable characteristics. The watermark should not degrade the image to a degree that interferes with its usefulness. The watermark should not require additional image formats or storage space. The watermark should be integrated with the image content so that it cannot be removed easily without severely degrading the image. The watermark should be fairly tamper-resistant and robust to common signal distortions, compression, and malicious attempts to remove the watermark. However, this is not achieved by many watermarks. The watermark can be made invisible to the human eye, but should be still readable by computer to prove the ownership.

Digital watermarks may be perceptible (visible to human eye) or imperceptible to the human senses. If the watermark is to be imperceptible, then the existence of the watermark should not be advertised. Advertising the presence of watermarks invites \pirates to attempt to alter or disable the watermarks. Other authors prefer visible watermarks, or clearly advertise the existence of watermarks as a deterrent against illicit duplication or theft. Both viewpoints have merit; but the determination must be made by the owner of the images and depends on the intended use of the watermarked work.

Various sorts of information can be stored in a watermark, including license, copyright, copy control, content authentication, and tracking information. This information can be used for copy protection, document identification, ownership designation, or as a means to track works to and from licensed users.

3. Classification of Watermarking Techniques

The current watermarking scheme is divided into two areas: spatial domain approach and frequency domain approach. Watermarks are embedded into images by changing some bits in image representation. Some methods operate on least significant bits, while others embed information into perceptually more significant image components. It may be grouped under two general classifications: those that fall into the spatial domain and those that fall into the transform domain. In spatial domain it represents the LSB (Least Significant

Bit) however; in the frequency domain it represents the high frequency components [1].

3.1. Spatial Domain Watermarking: The methods of spatial domain approach [2, 3] modify spatial characteristics of an image to embed a watermark. For example, the brightness of individual pixels has high frequency watermarking in watermarked image. In general, the advantage of spatial domain approach is better computing performance. Techniques that provide additive image information such as masking techniques without applying a function of the image to determine the watermark location are also categorized as being in the spatial domain, though they share the survivability properties of transform domain watermarking techniques.

In [4], authors proposed two digital watermark techniques in spatial domain. The first technique is based on manipulate the bit plane of the LSB, while the second utilizes linear addition of the watermark to cover image. In [5], authors presented a watermark technique based on color space transformation. The color space of cover image is transformed from RGB to HSI space and then embedded watermark into saturation channel. This method is able to resist some attacks. Watermark is embedded additively. The novelty of this technique lies in the use of secret image instead of host image for watermark extraction and use of image dependent and image independent permutations to de-correlate the watermark logos [6]. However, Common disadvantage of spatial domain watermarking are lower security and weaker robustness.

3.2. Frequency Domain Watermarking: Frequency domain approach [7, 8], inserts watermark signal by modifying image with coefficients of transformation. Transformation can be Fourier transformation, DCT, or wavelet transformation, etc. It is based on the perceptual significance of the transformed coefficients. A watermark is cast into transformed coefficients of relatively significant areas of the cover image. The watermarked image is generated by inverse transformation with all of the coefficients. Therefore, frequency domain approach is more robust and provides high security, but the watermark capacity that can be cast is limited and the computing is more complicated [9]. In [10], authors proposed a color image watermark technique based on DCT in frequency domain. This method embedded the watermark into middle frequency coefficient of transformed blocks; therefore this method is more robust against the attacks.

In [11], authors proposed a method of embedding the watermark in the DC component of transformed blocks. In [12], watermarking method based on the qualified significant wavelet tree (QSWT) is proposed. In this method, the embedding schema takes the relationships of DWT coefficients and spatial information into consideration. In [13], authors presented an image authentication technique by embedding digital watermarks into image. In their approach, watermark is embedded with visually recognizable patterns into the images by selectively modifying the middle-frequency parts of the image. Frequency domain watermarking and masking techniques are more robust against attacks such as lossy compression, cropping, and other image processing techniques in which significant bits are changed.

Fourier Mellin transform is similar to applying Fourier Transform to log-polar coordinate system for an image. This scheme is robust against RST attacks [14]. Magnitude of DWT coefficients is larger in the lowest bands (LL) at each level of decomposition and is smaller for other bands (HH, LH, and HL) [15]. A method of data hiding scheme based on DFT, where they modify the magnitude component of the DFT coefficients is proposed in [16].

Their simulations suggest that the proposed technique survives practical compression. This can be attributed to the fact that most practical compression schemes try to maximize the PSNR. Hence using magnitude DFT is a way to exploit the loop-hole in most practical compression schemes. The proposed technique is shown to be resistant to JPEG and SPIHT compression. The scheme in which the watermark is inserted by directly modifying the mid frequency bands of the DFT magnitude component is proposed in [17].

Computational complexity of DWT is compared to DCT [18]. Watermark embedding is based on a chaotic (mixing) system. Original image is not required for watermark detection. The watermark is embedded in spatial domain by modifying the pixel or luminance values. A similar approach is presented for the wavelet domain [19], where the authors proposed a watermarking algorithm based on chaotic encryption. If the watermark is embedded in high frequency components, it is robust against contrast and brightness adjustment, gamma correction, histogram equalization and cropping and vice-versa. Thus, to achieve overall robustness against a large number of attacks the authors proposed to embed multiple watermarks in low frequency and high frequency bands of DWT [20] .

Later the authors proposed another technique termed as Fuse Mark [21], which includes minimum variance fusion for watermark extraction. DFT embedded the watermarks in magnitudes is also resistant to cropping because effect of cropping leads to the blurring of spectrum. If the watermarks are embedded in the magnitude, which are normalized coordinates, there is no need of any synchronization. Rotation of image results in cyclic shifts of extracted signal and can be detected by exhaustive search [22]. In [23] Coefficient Selection Criteria is used to embed the watermark. Modification to the low frequency coefficients can cause visible artifacts in the spatial domain and high frequency coefficients are not suitable because they are removed during JPEG compression. Therefore, authors suggested that the best location to embed the watermark is the mid frequency.

Both spatial domain and transform domain methods may employ patchwork, pattern block encoding, or spread spectrum concepts which add redundancy to the hidden information [24]. These approaches help to protect against some types of image processing such as cropping and rotating. Watermarking techniques could also be classified based on whether an original (non-watermarked) image is needed for watermark recovery.

Some watermarking techniques extract the watermark by comparing the original image and the watermarked image [25]

In [26, 27] transform domain watermarking techniques were introduced that do not require original image to extract the watermark.

4. Requirements of Digital Watermarking

There are three main requirements of digital watermarking; transparency, robustness, and capacity.

I) Transparency or Fidelity: The digital watermark should not affect the quality of the original image after it is watermarked. In [28], authors define transparency or fidelity as, "perceptual similarity between the original and the watermarked versions of the cover work". Watermarking should not introduce visible distortions because if such distortions are introduced it reduces the commercial value of the image.

ii) Robustness: In [28], authors define robustness as, "the ability to detect the watermark after common signal processing operations". Watermarks could be removed intentionally or unintentionally by simple image processing operations like contrast or brightness enhancement, gamma correction etc. Hence watermarks should be robust against variety of such attacks. Stirmark[2] classifies attacks into four basic categories, attacks that try to remove watermarks totally, attacks that try to remove the synchronization between the embedder and the detector, cryptographic attacks and protocol attacks.

iii) Capacity or Data Payload: In [28], authors define capacity or data payload, "The number of bits a watermark encodes within a unit of time or work". This property describes how much data should be embedded as a watermark to successfully detect during extraction. Watermark should be able to carry enough information to represent the uniqueness of the image. Different application has different payload requirements.

5. Watermarking Applications

The main applications of digital watermarking are discussed here.

I) Copyright Protection: Watermarking can be used to protecting redistribution of copyrighted material over the untrusted network like Internet or peer-to-peer (P2P) networks. Content aware networks (p2p) could incorporate watermarking technologies to report or filter out copyrighted material from such networks.

ii) Content Archiving: Watermarking can be used to insert digital object identifier or serial number to help archive digital contents like images, audio or video. It can also be used for classifying and organizing digital contents. Normally digital contents are identified by their file names; however, this is a very fragile technique as file names can be easily changed. Hence embedding the object identifier within the object itself reduces the possibility of tampering and hence can be effectively used in archiving systems.

iii) Meta-data Insertion: Meta-data refers to the data that describes data. Images can be labeled with its content and can be used in search engines. Audio files can carry the lyrics or the name of the singer. Journalists could use photographs of an incident to insert the cover story of the respective news. Medical X-rays could store patient records.

iv) Broadcast Monitoring: Broadcast Monitoring refers to the technique of cross-verifying whether the content that was supposed to be broadcasted (on TV or Radio) has really been broadcasted or not. Watermarking can also be used for broadcast monitoring. This has major application is commercial advertisement broadcasting where the entity who is advertising wants to monitor whether their advertisement was actually broadcasted at the right time and for right duration.

v) Tamper Detection: Digital content can be detected for tampering by embedding fragile watermarks. If the fragile watermark is destroyed or degraded, it indicated the presence of tampering and hence the digital content cannot be trusted. Tamper detection is very important for some applications that involve highly sensitive data like satellite imagery or medical imagery. Tamper detection is also useful in court of law where digital images could be used as a forensic tool to prove whether the image is tampered or not.

vi) Digital Fingerprinting: Digital Fingerprinting is a technique used to detect the owner of the digital content. Fingerprints are unique to the owner of the digital content. Hence a single digital object can have different fingerprints because they belong to different users

6. Watermarking Algorithm

6.1. Watermark Embedding Algorithm

Watermark embedding in spatial domain is as shown in figure 1., and in frequency domain as shown in figure 2. The original image X represented as:

$$X\,(i, j),\ 0 \leq i, j \leq M \text{ ---------------------------}(1)$$

Where $X\,(I, j)$ is intensity pixel of cover image and M represents the size of the image.

W is the digital watermark, $W \in \{-1, 0, 1\}$---------(2)

i) Spatial Domain: Scaled watermark is embedded in the original image:

$$X^*\,(i,j) = X(i,j) + \beta W(i, j) \text{ ----------------------}(3)$$

6.2. Watermark Extraction Algorithm:

i) Spatial domain: Watermark is extracted from the watermarked image as well as attacked image by using following process:

$$W^*(i, j) = (X^*\,(i, j) - \mathrm{X}\,(i, j))/\,\beta \text{ ----------------------}\ (5)$$

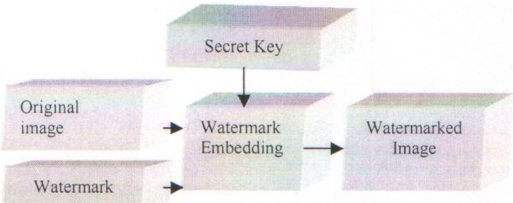


Figure1.Watermarking in spatial domain

7. Results

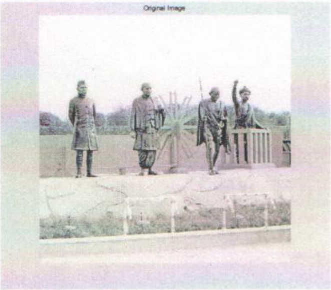


Figure.2(a) Original Image

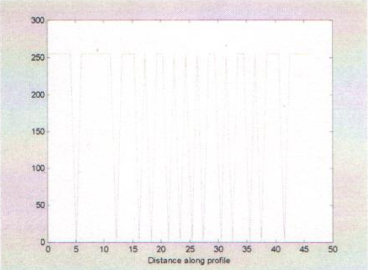


Figure.2(b) Distance along profile of Original Image

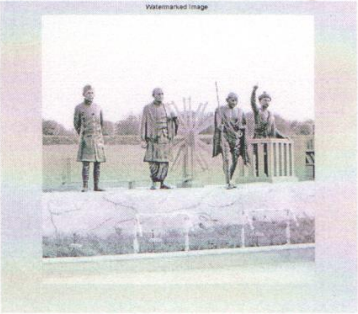


Figure.3(a) Watermarked Image

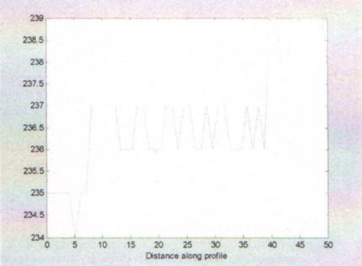
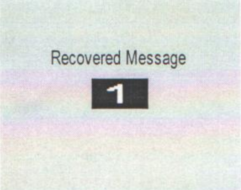


Figure.3(b) Distance along profile of Watermarked Image


Recovered Message

1

Figure. 5 Recovered Image

Table.1 Results for various Watermarked images

	Parameters			
Name of Images	PSNR (dB)	Average Difference	The Bit Correction Ratio (%)	Normalised Absolute Error
sculpture.bmp	75.000315	0.001789	100	0.000015
statues.bmp	73.974100	0.001764	99.9969	0.0000149
garden.bmp	27.021786	-6.466818	100	0.085422

8. Conclusion

In this paper we implemented spatial domain image watermarking. Watermarking is needed to prove the ownership of a digital image. Fidelity for Human Visual System (HVS) and robustness again different attacks are the main characteristics of watermarking. Mainly digital watermarking is classified into two different domains namely spatial domain and frequency domain. We have tested various images on the algorithm and analyses some of the parameters which is shown in Table.

In these results the distance along profile of watermarked image will be change due to embedding the image.

References:

[1] Guan-Ming Su, "An Overview of Transparent and Robust Digital Image Watermarking". Available online at www.watermarkingworld.org LWMMLArchive/0504/pdf00000.pdf.

[2] R.G.van Schyndel, A.Z. Tirkel and C.F. Osborne, "A digital watermark," in *Proc. IEEE Int. Conf. Image Processing*, 1994, vol. 2, pp. 86-92.

[3] Lu, C. S., Huang, S.-K., Sze, C.-J., Liao, H.-Y., "A new watermarking technique for multimedia protection," in Multimedia Imnage and Video Processing, L. Guan, S.-Y. Kung, and J. Larsen, Eds. Boca Raton, FL: CRC, 2001, pp. 507--530.

[4] I. J. Cox, J. Kilian, T. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia" *IEEE Transactions* on *Image processing,* Vol. 6, No. 12, Dec. 1997, pp. 1073-1687.

[5] C. T. Hsu and J. L. Wu, "Hidden Digital Watermarks in Images", *IEEE Transactions* on *Image Processing,* Vol. *8,* No. I, Jan. 1999, pp. 58-68.

[6] M. D. Swason, M. Kobayashi, and A. H. Tewfik. "Multimedia Data Embedding and Watermarking Techniques," *Proceedings of IEEE,* Vol. *86,* No. 6, Jun. 1998, pp. 1064-1087

[7] Chiou-Ting Hsu and Ja-Ling Wu, "Hidden digital watermarks in images," in *IEEE Trans. Image Processing*, 1999, vol. 8, pp. 58-68.

[8] Pereira, S., Pun, T., "Robust Template Matching for Affine Resistant Image Watermarks," in *IEEE Transactions on Inage Processing,* vol. 9, no. 6, pp. 1123-1129, June 2000.

[9 Cox, LI, Miller, ML & Bloom, JA 2002, "Digital Watermarking", *Morgan Kaufmann Publisher, San Francisco, CA, USA*.