

Comparative Analysis of Various Watermarking Techniques for Digital Image

Vaishali Ghune

Acropolis Institute of Technology and Research Indore (M.P.)

Abstract

Three digital image watermarking techniques that have higher level of security compared to most of the existing algorithms have been proposed. Watermarking is a technique for labeling digital pictures by hiding secret information into the images. Watermarking is a technique for labeling digital pictures by hiding secret information into the image. In Digital watermarking technique, image is embedded information data within an insensible form for human visual system but in a way that protects from attacks such as common image processing techniques. In our approach, analysis the quality of image compression by(Discrete Cosine Transform(DCT)) and (Discrete Wavelet Transform(DWT)) and (least significant bit(LSB)). We embed the watermarks with visually recognizable patterns into the images by selectively modifying the middle-frequency parts of the image. Several variations of the methods will be addressed. The experimental results show that the technique successfully survives image processing operations and compare the results.

Keywords: Digital watermarking; Discrete cosine transform (DCT), discrete wavelet transform (DWT), least significant bit(LSB)

I. Introduction

Due to the rapid and extensive growth of electronic publishing industry, data can now be distributed much faster and easier. Unfortunately, engineers still see immense technical challenges in discouraging unauthorized copying and distributing of electronic documents[2].

Watermarking technique is to hide secret information into the digital signals so as to discourage unauthorized copying or attest the origin of the media. And the watermark is a digital code embedded in the image data and is invisible[4]. Watermark is an invisible mark containing information. In the form of text, images and multimedia or protected multimedia data placed on an image that can be detected when the image is compared with the origin[3]. There are some necessary characteristics for digital image watermarking. These requirements are:

Invisible: The digital watermark embedded into the image data should be invisible to the human.

Security: Unauthorized removal and detection of the watermark must be impossible even if the basic Scheme used for watermarking is known.

Robustness: Robustness is a measure of the immunity of the watermark against attempt to remove it by different types of attacks. We measure the similarity between the original watermark and the extracted watermark from the attacked image using the Normalized Correlation (NC) factor[7].

Watermarking is a technique for labeling digital pictures by hiding secret information into the images. The growth of networked multimedia systems has created the need for the copyright protection of various digital medium, e.g., images, audio clips, video, etc. In the literature, several techniques have been developed for watermarking. three coding methods for hiding electronic marking in document were proposed. the watermarks are applied on the spatial domain[1]. The major disadvantage of spatial domain watermarking is that a common picture cropping operation may eliminate the watermark. Other than spatial domain watermarking, frequency domain approaches have also been proposed. In a copyright code and its random sequence of locations for embedding are produced, and then superimposed on the image based on a JPEG model. The watermark is a Symbol or a random number which comprises of a sequence of bits, and can only be "detected" by employing the "detection theory." That is, during the verification phase, the original image is subtracted from the image in question, and the similarity between the difference and the specific watermark is obtained. Therefore, an experimental threshold is chosen and compared to determine whether the image is watermarked [8].

In our scheme, watermarks are embedded and extracted by modifying the middle-frequency coefficients within each image block of the original image in considering the effect of quantization using DCT techniques, LSB techniques and DWT techniques. There is a technique that has been used for digital watermarking. The experimental results

show and used DCT, DWT and LSB techniques apply on the several images after compare the results.

II. METHODS OF EMBEDDING

In our approach, a block DCT-based algorithm is developed to embed the image watermarking. Let X be the original gray-level image of size $(N_1 * N_2)$, and the digital watermark W be a binary image of size $(M_1 * M_2)$. In the watermark, the marked pixels are valued as one's, and the others are zeros. Since only the middle-frequency range of the host image will be processed during the watermark embedding, the resolution of a watermark image W is assumed to be smaller than that of the original image X. For example, for each 8*8 image block, only $(64 * M_1 * M_2 / N_1 * N_2)$ coefficients will be used for the Watermark embedding. Fig (a) shows the embedded watermark. The ratio of $(M_1 * M_2)$ and $(N_1 * N_2)$ determines the amount of information to be embedded into the image. In general, for more robust and invisible embedding, the amount of information can be embedded should be reduced. The original image X and digital watermark W are represented as

$$X = \{x(i,j), 0 \leq i < N_1, 0 \leq j < N_2\} \quad (1)$$

Where $x(i,j) \in \{0, \dots, 2^L - 1\}$ is the intensity of pixel $x(i,j)$ and L is the number of bits used in each pixel.

$$W = \{w(i,j), 0 \leq i < M_1, 0 \leq j < M_2\} \quad (2)$$

Where $w(i,j) \in \{0, 1\}$.

In X, there are $N_1/8 * N_2/8$ image blocks with size 8*8. To obtain the same number $N_1/8 * N_2/8$ of blocks as the image X, the watermark W is decomposed into several blocks with size $(M_1 * 8 / N_1) * (M_2 * 8 / N_2)$.

A- Pseudorandom Permutation of the Watermark

In our approach, the permutation is implemented as follows. First, number each pixel from zero to $(M_1 * M_2)$. Second, generate each number in random order. Finally, generate the coordinate pairs by mapping the random sequence number into a 2-D sequence. For example, for a digital watermark of size 128*128, use a "linear feedback shift register" [11] to generate a random sequence from 1 to 16383. Then, for each sequence element number, compute and $(M \bmod 128)$ and as the permuted vertical and horizontal coordinates. The watermark to disperse its spatial relationship, i.e.,

$$W_p = \text{Permute}(W)$$

B- Block-Based Image-Dependent Permutation of the Watermark

In order to improve the perceptual invisibility, For each image block of size 8*8, the variances (which is used as a measure of invisibility under watermark embedding) are computed and

sorted. For each watermark block of size $(M_1 * 8 / N_1) * (M_2 * 8 / N_2)$, the amount of information (i.e., the number of signed pixels) are sorted also. Then, shuffle each watermark block into the spatial position according the corresponding sorting order of the image block, i.e.,

$$W_p = \text{Permute}(W_p)$$

C- Block Transformation of the Image

Since the discrete cosine transform (DCT) used by JPEG [12] is performed on blocks of 8*8, the input image X is divided into blocks of 8*8, and each block is DCT Transformed independently. That is,

$$Y = \text{FDCT}(X)$$

Where FDCT denotes the operation of forward DCT.

D- Choice of Middle-Frequency Coefficients

The human eye is more sensitive to noise in lower frequency components than in higher frequency ones. However, the energy of most natural images are concentrated in the lower frequency range, and the information hidden in the higher frequency components might be discarded after quantization operation of lossy compression. To this end, for each 8*8 image block, only $(64 * (M_1 * M_2 / N_1 * N_2))$ coefficients are selected out of the 64 DCT coefficients. Those selected coefficients are then mapped into a reduced image block of size $(M_1 * 8 / N_1) * (M_2 * 8 / N_2)$. That is, the middle-frequency coefficients selected from the image of size $(N_1 * N_2)$ are collected to compose a reduced image of size $(M_1 * M_2)$, which has the same resolution with the binary watermark.

$$Y_r = \text{Reduce}(Y)$$

E. Modification of the DCT Coefficients

Now, a permuted digital watermark and a reduced image (Which contains only the middle-frequency components of the original image) both with size $(M_1 * M_2)$ are obtained. For each watermark block of size $(M_1 * 8 / N_1) * (M_2 * 8 / N_2)$, the reduced image block of size $(M_1 * 8 / N_1) * (M_2 * 8 / N_2)$ at the corresponding spatial position will be modified adequately to embed the watermarked pixels.

$$P = \text{Polarity}(Y_r)$$

F- Inverse Block Transform

Finally, map the modified middle-frequency coefficients Y_r Into Y to get Y. Then, inverse DCT (IDCT) of the associated result to obtained the embedded image

$$X = \text{IDCT}(Y)$$

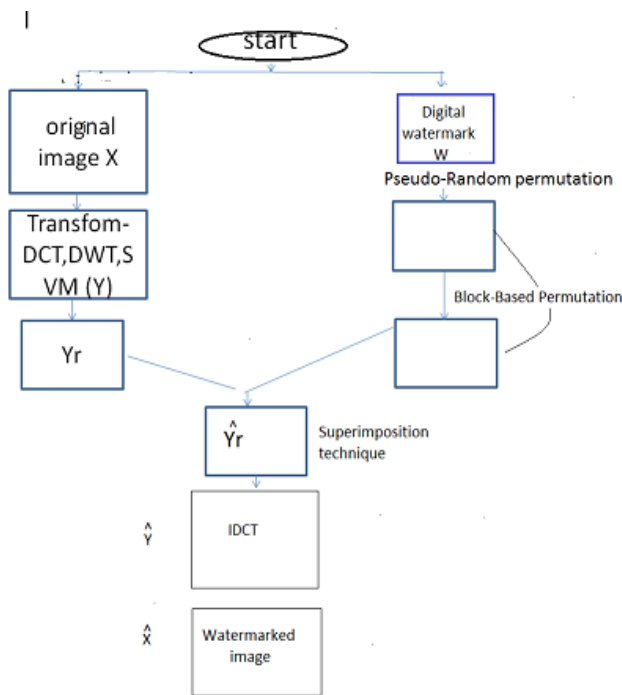


Fig-a Watermark embedding steps.

III. WATERMARK EXTRACTING METHOD

The extraction of watermark requires the original image, The watermarked image, and either the watermark or the Permutation mapping used in image-dependent permutation during the embedding steps. The extraction steps are described as follows .fig (b) shows the watermark extracting steps.

A- Block Transformation

Both the original image and the image in question are DCT transformed.

$$Y = \text{FDCT}(X)$$

$$\hat{Y} = \text{FDCT}(\hat{X})$$

B- Generation of Polarity Patterns

Generate the reduced images which contain only the middle frequency coefficients and then use these middle-frequency DCT coefficients to produce the polarity patterns. That is

$$Y_r = \text{Reduce}(Y)$$

$$\hat{Y}_r = \text{Reduce}(\hat{X})$$

And then

$$P = \text{Polarity}(Y_r)$$

$$\hat{P} = \text{Polarity}(\hat{Y}_r)$$

C- Reverse Block-Based Image-Dependent Permutation

The image-dependent permutation mapping could be obtained either by saving as a file during the embedding steps or recomputed from the original

image and the watermark. Based on the mapping, reverse permute W_b to get W_p .

D- Reverse Pseudorandom Permutation

Reverse-permute W_p to get the watermark W .

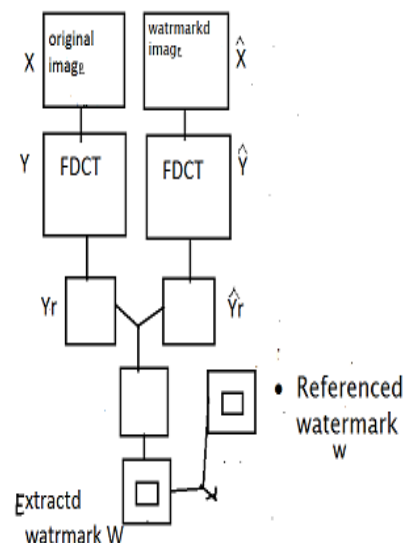


Fig -b Watermark extracting steps

IV. LSB TECHNIQUE

The best known Watermarking method that works in the Spatial Domain is the Least Significant Bit (LSB), which replaces the least significant bits of pixels selected to hide the information. This method has several implementation versions that improve the algorithm in certain aspects.

Techniques in spatial domain class generally share the following characteristics:

- The watermark is applied in the pixel domain.
- No transforms are applied to the host signal during Watermark embedding.
- Combination with the host signal is based on simple

Operations, in the pixel domain.

- The watermark can be detected by correlating the expected pattern with the received signal.

In a digital image, information can be inserted directly into every bit of image information or the more busy areas of an image can be calculated so as to hide such messages in less perceptible parts of an image.

If we use a greyscale bitmap image, which is 8-bit, we would need to read in the file and then add data to the least significant bits of each pixel, in every 8-bit pixel. In a greyscale image each pixel is represented by 1 byte consist of 8 bits. It can represent 256 gray colours between the black which is 0 to the white which is 255. The principle of encoding uses the Least Significant Bit of each of these bytes, the bit on the far right side. If data is encoded to only the last two significant bits (which are the first and second LSB) of each colour component it is most likely not going to be

detectable; the human retina becomes the limiting factor in viewing pictures[10].

V. Conclusion

This paper has presented a three digital watermarking techniques DCT, DWT and LSB. Embedding digital watermark and extracting digital watermark methods is DCT-based approach. After use this algorithm the result show that the quality of the watermarked image is higher. These algorithms apply for the image compression of original or digital image. The values of all particular point after image compression are compare based on the algorithm DCT, DWT and LSB. To increase the imperceptibility, the watermark image is adjusted by the weighted correction in the spatial domain. Here we present the comparison of PSNR value and NC factor. The results of experiments have showed that the algorithm has better visibility and has stronger robustness when it is attacked by JPEG compression, cropping, contrast adjustments, filtering, noises and so on.

References

- [1] B. M. Macq and J. J. Quisquater, "Cryptology for digital TV broadcasting," *Proc. IEEE*, vol. 83, pp. 954–957, June 1995.
- [2] I. Pitas and T. H. Kaskalis, "Applying signatures on digital images," in *Proc. IEEE Nonlinear Signal and Image Processing*, June 1995, pp.460–463.
- [3] O. Bruyndonckx, J. J. Quisquater, and B. Macq, "Spatial method for copyright labeling of digital images," in *Proc. IEEE Nonlinear Signal and Image Processing*, June 1995, pp. 456–459.
- [4] W. Bender, D. Gruhl, and N. Morimoto, "Techniques for data hiding," *Proc. SPIE*, vol. 2420, p. 40, Feb. 1995.
- [5] N. Nikolaidis, I. Pitas, "Robust image watermarking in the spatial domain," *Signal Process*, 66(1998) 385-403
- [6] Keshav S Rawat. "Digital watermarking schemes for authorization against copying or piracy of color images" *Member, IEEE Keshav S Rawat et. al. / Indian Journal of Computer Science Vol. 1 No. 4 295-300*
- [7] T. Jayamalar. "Survey on Digital Video Watermarking Techniques and Attacks on Watermarks" *International Journal of Engineering Science and Technology Vol. 2(12), 2010, 6963-6967*
- [8] Kritika Singla. "Invigible digital watermarking for color images" *International Journal of advanced of engineering sciences and technologies Vol No. 10, Issue No. 2, 270 – 274*
- [9] Mei Jiansheng. "A Digital Watermarking Algorithm Based On DCT and DWT"

Proceedings of the 2009 International Symposium on Web Information Systems and Applications (WISA'09) Nanchang, P. R. China, May 22-24, 2009, pp. 104-107.

- [10] Chiou-Ting Hsu and Ja-Ling Wu. "Hidden Digital Watermarks in Images" *Senior Member, IEEE. TRANSACTIONS ON IMAGE PROCESSING, VOL. 8, NO. 1, JANUARY.*
- [11] "Digital watermarking for digital media" Juergen Seitz University of Cooperative Education Heidenheim, Germany.
- [12] Gonzalez R, wood R. "Digital image processing", published by Pearson Education.