Spatial Domain Approaches for Real-Time Ownership Identification

Mir Shahriar Emami
The National University of Malaysia (UKM), Bangi, Selangor, Malaysia
shemami85@yahoo.com

Khairuddin Omar, Shahnorbanun Sahran, and Siti Norul Huda Sheikh Abdullah
The National University of Malaysia (UKM), Bangi, Selangor, Malaysia

***Abstract*—An effective approach is a necessity for many digital watermarking applications including medical image ownership identification. To address this necessity, many watermarking techniques have been introduced by the researchers. Among the techniques introduced, spatial domain watermarking techniques are simpler and lower in computational cost due to direct embedding of the watermark. In contrast, transform domain and hybrid domain techniques require a lot of computation due to direct and inverse transformations. However, the spatial domain techniques are not robust enough against many watermarking attacks including geometric and image compression attacks. In this paper, the latest spatial domain approaches for real-time ownership identification have been studied. The results of this study shown that the spatial domain techniques using approximation approaches can provide real-time ownership identification even after geometric and JPEG2000 attacks**

***Index Terms*—Ownership Identification, Real-time, Watermarking, Spatial Domain**

I. Introduction

In insecure communications, digital watermarking is an approach to provide information protection against misuse, piracy, or illegal manipulations. In many digital watermarking applications including medical image ownership identification, an effective approach is a necessity. To address this necessity, many watermarking techniques have been introduced by the researchers. These techniques can be categorized into three main domains as follows:

A. Transform Domain Watermarking Techniques

Transform domain techniques are the techniques that perform some kind of transformation prior to embedding the watermark. There are several transform domain techniques in the literature. In Discrete Fourier Transform (DFT), firstly, the host image is segmented into coefficients (DFT coefficients) of a linear weighted summation of harmonically related complex exponentials. Subsequently, the watermark is embedded in some of these coefficients. Finally, the host image is retrieved from the frequency domain to the spatial domain (inverse DFT or IDFT). Thus, DFT watermarking requires a lot of computation. Similarly, in singular value decomposing (SVD) techniques, firstly, the host image is decomposed into some matrixes including a diagonal matrix which contains singular values. Subsequently, the singular values are modified in order to embed the watermark. Finally, the inverse SVD transform is performed to retrieve the host image. Hence, similar to DFT watermarking, the SVD watermarking requires a lot of computations. Likewise, other transform domain techniques including discrete wavelet transform (DWT) require a lot of computation devoting for direct and inverse transformations.

B. Spatial Domain Watermarking Techniques

In spatial domain techniques, one or more bit-planes are directly modified to embed the watermark [3, 7]. Therefore, they are simple and easy-to-implement algorithms. Contrary to the transform domain methods, the spatial domain watermarking techniques generally require lower computation due to the direct watermark embedding strategy. Therefore, the spatial domain approaches seems to be more effective for the real-time watermarking applications. However, the spatial domain techniques are not robust enough especially in influence of the geometric attacks [10]. In such a situation, the embedded watermark is desynchronized so that the ownership identification cannot be established using the extracted watermark from the attacked watermarked image (There are more discussions on the spatial domain watermarking techniques in Section II).

C. Hybrid Domain Watermarking Techniques

Some other researches introduced a combinational method using both transform domain and spatial domain approaches. In 2003, Shih and Wu [5] proposed a method using both spatial and frequency domain approaches. This technique, at first, splits the host image into the 8×8 block of pixels. Subsequently, the embedding watermark splits into two parts including more important and less important parts. Next, the most important part is embedded into the low frequency DCT coefficients, and the less important part of the watermark

doi:10.4304/jait.5.1.1-4

is embedded in the LSB (Least Significant Bit) bit-plane of the host image. Similar to the transform domain techniques, a hybrid domain approach is complex and time consuming due to the necessary transformations in the transform domain part of the algorithm.

II. Spatial Domain Watermarking Approaches

The earliest spatial domain watermarking techniques were based on the LSB [1, 2, 7]. In the LSB-based image watermarking techniques, the least significant bit of a host image is used for the watermark embedding. These techniques required low computation due to direct embedding of the watermark bits. However, the embedded watermark was simply corrupted by Gaussian noise and image compression attacks. In order to increase the robustness of the watermarked image, some other spatial domain techniques were exploited blocking strategies. However, some geometric attacks such as Rotation attack simply corrupted the blocks so that the embedded watermarks could not be extracted. Therefore, the ownership identification could not be established. The next watermarking techniques were used the ISB (Intermediate Significant Bits) [3, 4, 7] instead of the LSB to increase the robustness of the watermarked image. This strategy resulted in increasing the robustness of the watermarked image against simple noise and some of the image compression attacks such as JPEG [3, 4]. However, geometric attacks for the ISB watermarking techniques are the main problems. In the recent few years a new approach has been emerged in which the ownership identification has been established using an approximation perspective vs. a direct correlation view. Figure 1 demonstrates a general view of this approach. As it can be seen, after the watermark (or the attacked watermark) is extracted from the watermarked image (or the attacked watermarked image), a statistical information of the extracted watermark is obtained. Subsequently, this statistical information is compared with the statistical information which is obtained from the original watermark.

There are three main spatial domain techniques which are exploited the approximation approach for ownership identification:

A. EISB Method using L2Norm Technique

This technique was proposed in 2011 by Emami et al [6]. In this technique, the statistical information is in the form of a simple histogram. This histogram can be maintained approximately intact even after the image content changes partially by severe attacks such as geometric operations or image compressions. In the technique introduced, the histograms of the original watermark image and the attacked watermark image are compared using the L2Norm technique to estimate the similarity rate between them. The similarity rate between these two histograms can be used for ownership identification of the watermarked image (or the attacked watermarked image).

The similarity rate (S) using the L2Norm technique can be obtained using the following equation:

$$S = \sqrt{\sum_{i=1}^{|L|}\left(H_{O_i} - H_{E_i}\right)} \quad ; \quad S \in [0,1] \qquad (1)$$

where H_O and H_E are the histograms of the original watermark and extracted watermark, respectively. Also, $|L|$ indicates the number of components in each histogram.

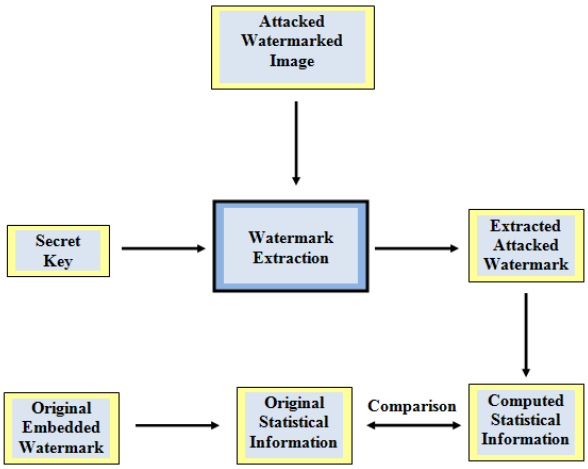

Figure 1. Spatial domain watermarking technique using approximation perspective.

B. BiISB Method using HI Technique

This technique was proposed by Emami et al [8] in 2012. In this technique, firstly, a sub-watermark is generated form the embedding watermark (called main watermark) using bit-pattern histogram in which a histogram can be established using any size of histogram components. For example, in the EISB method using L2Norm technique, 8-bit pixels (in an 8-bit gray-scale watermark image) are counting in order to form the histogram but here, any m-bit (say m=2) can be considered to establish the bit-pattern histogram. Finally, both of the main watermark and its inter-related sub-watermark are embedded in the lower-bit-plane and higher bit-plane of the host image, respectively. For the ownership identification (for example after an attack), both of the main watermark and its inter-related sub-watermark are extracted. Subsequently, for the extracted main watermark, a bit-pattern histogram is generated. Finally, in order for ownership identification, a pair-wise comparison is established using the histogram intersection (HI) technique among the computed bit-patter histogram (from the extracted main watermark), the extracted bit-pattern histogram (the extracted sub-watermark), and the original sub-watermark (obtained from the original watermark). The HI equations are as follows:

$$HI_{OC} = \sum_{i=1}^{n} \min(h_{O_i}, h_{C_i}) \qquad (2)$$

$$HI_{OE} = \sum_{i=1}^{n} \min(h_{O_i}, h_{E_i}) \qquad (3)$$

$$HI_{CE} = \sum_{i=1}^{n} \min(h_{C_i}, h_{E_i}) \qquad (4)$$

where h_O, h_C, and h_E are the histograms for original sub-watermark (bit-pattern histogram of the original watermark), computed sub-watermark (bit-pattern histogram of the extracted main watermark), and extracted sub-watermark (extracted bit-pattern histogram), respectively. Also, HI_{OC}, HI_{OE}, and HI_{CE} indicate the histogram intersection between h_O and h_C, h_O and h_E, h_C and h_E, respectively. Moreover, the parameter n shows the number of components in each bit-pattern histogram.

C. EISB Method using 1's against 1's and 0's

Recently, a new approximation technique is proposed by Emami et al. [9]. In this technique, at first, the ratio of the number of 1s over the number of both 1s and 0s is computed for the bit streams of both of the original watermark, N, and the extracted watermark (or the extracted attacked watermark), $\hat{N}_i$. In order for ownership identification, the following equation is computed to find the similarity rate (S) between the original watermark and extracted watermark.

$$S = 1 - Min\left(\left|N - \hat{N}_i\right|\right) \quad ; \quad S \in [0,1] \qquad (5)$$

III. Discussion

The transform domain and hybrid domain watermarking techniques are more robust compared to the spatial domain techniques. However, they are time consuming and complex. In contrast, the spatial domain watermarking techniques are simple and easy to implement due to the direct watermark embedding within a host image. However, they are not much robust. They cannot withstand against the geometric attacks due to the desynchronization effect of such attacks. Also, most of the spatial domain watermarking techniques cannot resist against some of the image compression attacks such as JPEG2000. Table I shows the properties of different watermarking approaches

TABLE I.
DIFFERENT WATERMARKING APPROACHES

Approach of Watermarking	Properties		
	Computational Cost	Robustness	Simplicity
Spatial Domain	Low	Low	Simple
Transform Domain	High	High	Complex
Hybrid Domain	High	High	Complex

Although, the spatial domain techniques are not robust enough, they could be suitable for the real-time application if the ownership identification could be established even after severe attacks such as geometric and image compression attacks. The latest research in the field of spatial domain watermarking revealed that some statistical characteristics of the watermarked image in the spatial domain can be maintained even after such attacks. In the EISB method using L2Norm technique [6] the common histogram (pixel-based histogram) is used to identify the rightful owner. However, this technique could not withstand against some severe geometric attacks such as rotation due to the long bit-pattern length (8-bit histogram in 8-bit gray-scale imaging). In contrast, in the BiISB method using HI Technique, the bit-pattern length can be short (for example, 2-bit bit-pattern histogram). This strategy increases the probability of the correct ownership identification even after the geometric attacks. Experimental investigations in Ref. [10] confirmed that this approach resisted against severe geometric attacks. However, in the BiISB method using HI Technique, two kinds of watermarks: the main watermark and the sub-watermark are embedded

concurrently in a host image. Another real-time method that has been introduced recently is the EISB method using 1's against 1's and 0's [9]. In this technique, only one watermark (the main watermark) is embedded in the host image. At the time of extraction, the ratio of the number of 1's over the number of both 1'0 and 0's of the bit-stream of the extracted watermark and the original watermark is used for ownership identification. Experimental results in Ref. [9] revealed that this approach resisted against JPEG2000 image compression attack.

IV. Conclusion

An instantaneous watermarking approach is a necessity for current applications including medical imaging. Among current watermarking approaches, the spatial domain approach seems to be more convenient for real-time applications. In this paper, the latest spatial domain techniques for real-time applications viz. EISB method using L2Norm technique, BiISB method using HI technique, and EISB method using 1's against 1's and 0's have been investigated. These techniques, exploits an approximation perspective for ownership identification instead of a simple direct correlation assessment. The results of the latest research in the field raveled that these approximation approaches have been successful to identify the rightful owner even after severe attacks including the geometric and image compassion attacks.

References

[1] C. Yang, "Inverted pattern approach to improve image quality of information hiding by LSB.", *Pattern Recognition*, Elsevier, Vol.41, pp. 2674 – 2683, 2008.

[2] C. Chan and L.M. Cheng, "Hiding data in images by simple LSB substitution", *Pattern Recognition*, Elsevier, Vol.37, pp 469 – 474, 2004.

[3] A. M. Zeki, , and A. A. Manaf, "A Novel Digital Watermarking Technique Based on ISB (Intermediate Significant Bit)", *International Journal of Information Technology*, 5(3), 2009.

[4] A. M. Zeki, , and A. A. Manaf, "ISB Watermarking Embedding: A Block Based Model", *Information Technology Journal*, 10(4), 841-848, 2011.

[5] F. Y. Shih, S. Y. T Wu, "Combinational Image Watermarking in the Spatial and Frequency Domains", Pattern Recognition, Elsevier, Vol. 36, pp. 969 -975, 2003

[6] M. S. Emami, and G. B. Sulong, " A Statistical Method based on L2Norm Technique for EISB Information Watermarking Scheme", *International Conference on Future Information Technology*, Vol.13, pp.139-143, 2011.

[7] M. S. Emami, G. B. Sulong, and J. M. Zain, "A New Performance Trade-Off Measurement Technique for Evaluating Image Watermarking Schemes", *Communications in Computer and Information Science*, Springer, 179, 567-580, 2011.

[8] M. S. Emami, G. B. Sulong, and S. B. Seliman, "An Approximation Approach for Digital Image Owner Identification using Histogram Intersection Technique", *International Journal of Innovative Computing, Information and Control*, 8 (7A), 4605-4620, 2012.

[9] M. S. Emami, K. Omar, S. Sahran, and S. N. H. S. Abdullah, "A Real-Time Ownership Identification Approach for Semi-blind Invisible Watermarking using Statistical Information of Watermark Bit Stream", proc. of TelSaTech, Indonesia, 2013.

[10] M. S. Emami, K. Omar, S. Sahran, and S. N. H. S. Abdullah, "A Study on the Resiliency of Spatial Domain Watermarking to Geometric Attacks using Approximation Perspective vs. Direct Correlation View", proc. of TelSaTech, Indonesia, 2013.