Proposing an Effective Approach for Network Security and Multimedia Documents Classically using Encryption and Watermarking

Reza Abbasgolizadeh[1], Habib Izadkhah[2],Ramin Meshkabadi[1]
[1]Department of Electrical Engineering, Ahar Branch, Islamic Azad University, Ahar, Iran.
[2]Department of Computer Sciences,Faculty of Mathematical Sciences , University of Tabriz, Tabriz, Iran.
Email: abbasgholizadeh.reza@gmail.com (Corresponding author)

Abstract

Local binary pattern (LBP) operators, which measure the local contrast within a pixel's neighborhood, successfully applied to texture analysis, visual inspection, and image retrieval. In this paper, we recommend a semi blind and informed watermarking approach. The watermark has been built from the original image using Weber Law. The approach aims is to present a high robustness and imperceptibility with perfectly tamper detection zone. In this article, innovative image has been divided into blocks and the main pixel is chosen for watermark insertion, where the embedding/extraction operate in the spatial domain. Based on the experimental results, the imperceptibility and robustness of our watermarking approach are proven and showing perfectly the detection of the image.

Keywords: Image watermarking, Attacks, Robustness, Local binary pattern.

1. Introduction

The success of the internet and digital consumer devices profoundly changing our society and daily lives by making the capture, transmission, and storage of digital data extremely easy and convenient. However, this raises a big concern on how to secure these data and prevent unauthorized modification. This issue has become problematic in many areas, such as copyright protection [1–4], content authentication [6, 7], information hiding [5], and covered communications [8]. Many researchers have developed various algorithms of digital watermarking to address this issue [9–22], which intend to embed some secret data (called watermark) in digital content to mark or seal the digital data content. The watermark embedded into a host image is in such a way that the embedding induced distortion is too small to be noticed. At the same time, the embedded watermark must be robust enough to withstand common degradations or deliberate attacks. Human visual system (HVS) characteristics are usually employed in watermarking [6–8] to improve the imperceptibility. Hengfu Yang [6] proposed an image authentication algorithm based on HVS and gains good performance. The algorithm used the masking properties to calculate the Just Notice Distortion (JND) matrix based on the structure of the image block, and embedded the watermark into the wavelet coefficients in the horizontal and vertical components. In 2008, Huiyan Qi [7] built a HVS model to compute visual masking, and embedded the watermark into the low-frequency coefficients of the DCT block. In the same year, Min-Jen Tsai [8] used wavelet coefficients in low frequency component to construct watermark, and embedded the watermark into the high frequency component according to HVS characteristics.

Blind image watermark technology can be mainly classified into spatial and transform domains. Spatial domain watermarking is usually done by directly adjusting image pixels in accordance with the watermark. Methods such as least significant bit (LSB) [3] and vector quantization (VQ) [4] belong to this category. Spatial domain methods have the advantages of low complexity and easy implementation but suffer the disadvantage of weak resistance against malicious attacks. In contrast, the watermarks embedded by transform domain methods generally show better robustness and imperceptibility, but the required computation is relatively high as compared to that demanded by spatial domain methods. The merits of transform domain methods consist in the capability of converting spatial data to a representation more compatible to human perception. Commonly used transforms for digital watermarking are discrete wavelet transform (DWT) [5-10], discrete cosine transform (DCT) [11-16], discrete Fourier transform (DFT) [9, 17, 18], and singular value decomposition (SVD) [19-24], etc. Among these transforms, the DCT holds the advantage of excellent energy compaction for highly correlated image data. Imposing invisibility constraints is comparatively easy when working in the DCT domain [25].

Encryption of document images prevents an intruder from accessing the contents without a proper decryption key. But once the data are decrypted, they can be duplicated and distributed illegally. Digital watermarking is one of the best solutions to preclude illegal copying, modifying and redistributing digital document images. It is an effective solution to enforce Intellectual Property rights and preventing illegal duplication, interpolation and distribution of document images. The embedded data should maintain the quality of the host signal. The following properties need to be satisfied by any document image watermarking algorithm:

I. Imperceptibility: The watermark should not affect the quality of the original document image and watermark thus embedded should be imperceptible.
II. Robustness: The watermarked document image should not only be robust to common signal processing manipulations such as filtering, compression, rotation and noise but also to document image specific attacks like changing font size, type and style, changing color and background of the text and cropping some text contents.
III. Capacity: The number of bits that can be embedded defines the capacity and it should be very less
IV. Security: The watermark should be scrambled and impossible for an unauthorized person to detect.
V. Watermarking should be blind and detection should be done without referencing the original document image.
VI. The watermark should be undetectable without prior knowledge of the embedded watermark sequence.
VII. these requirements are often contradictory to each other and one needs to make a trade-off among them. For example,

increasing the amount of embedding in watermarking system results in quality degradation of the watermarked signal and decreases the robustness against attacks. Imperceptibility and robustness are the most important properties for many applications. These conflicting requirements pose many challenges to design a robust watermarking scheme.

2. Experimental Section

The local binary pattern (LBP) operator was proposed to measure the local contrast in texture analysis [22, 23]. It has been successfully applied to visual inspection and image retrieval [24, 25]. The LBP operator is defined in a circular local neighborhood. Using the center pixel as the threshold, its circularly symmetric P neighbors within a certain radius R are individually labeled as 1 when the value is larger than the center, or labeled as 0 when the value is smaller than the center. Note that P=(2R+1)2−1. Then, the LBP code of the center pixel is produced by multiplying the threshold values (i.e., 1 or 0) by weights given to the corresponding pixels, and summing up the result. For example, the LBP of a 3×3 window (where R=1and P=8) uses the center pixel as a threshold value, and the values of the threshold neighbors are multiplied by the binomial weight and summed to obtain the LBP number. In this way, the LBP can produce a number from 0to 255. The entire LBP numbers composite a texture spectrum of an image with 256 gray levels, which is often used to extract image features for classification or recognition.

Given parameters P and R, which control the quantization of the angular space and spatial resolution respectively, the LBP number, denoted by LBPp, indicating the local contrast in the neighborhood, is defined as

$$LBP_P = \sum_{p=0}^{P-1} S\left(g_p - g_c\right) \times 2^P \qquad (1)$$

Where $g_c$denotes the gray level of the center pixel c in the P neighborhood, g_p denotes the gray level of the neighboring pixels p, and S(x) refers to the sign function defined as

$$S(x) = \begin{cases} 1, & if \;\; x \geq 0 \\ 0, & \text{otherwise} \end{cases} \qquad (2)$$

More detailed information about the LBP operators and their applications can be referred to [25, 26].

3. The Proposed Spatial Watermarking Based on LBP Operators

3.1.Definitions on a (P, R) local region

Before presenting the proposed watermarking algorithms, we first provide some definitions. Let gc denote the gray level of the center pixel c in the P neighborhood, and let gp denote the gray level of the neighboring pixels p. For a (P, R) local region, we describe it as follows

$$g_p = \left\{ g_i \left| i = 0,...,c,...,P-1 \right. \right\} \qquad (3)$$

$$m_p = \left\{ m_i \left| m_i \left| g_i - g_c \right| , i = 0,...,P-1 \right. \right\} \qquad (4)$$

$$s_p = \left\{ s_i \left| s_i = sign\left(g_i - g_c \right), i = 0,...,P \text{ -} \right. \right\} \qquad (5)$$

Note that Eq. (5) uses the sign function, which is equivalent to Eq. (2). In this way, we divide the local region into three parts [28]: g_p is a vector composed of P pixels in the R radius, m_p is a vector built by the magnitude obtained from the difference between the p pixels and the center pixel g_c, and s_p is a sign vector from the difference. Fig. 1 shows an example of the three parts in a (P=8, R=1) local region.

In order to embed watermarks, we define Boolean functions $f\left(s_p\right)$ to be applied on the binary sign vector part sp. Two types of Boolean functions are chosen for illustration purposes, which are defined as follows:

$$f_{\oplus}\left(s_p\right) = s_0 \oplus s_1 \oplus \ldots \oplus s_{P-1} \qquad (6)$$

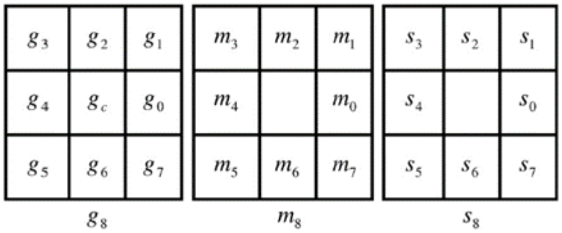
$$f\left(s_p\right) = Bool\left(1\left(s_P\right) - 0\left(s_P\right) > N\right) \qquad (7)$$

In Eq. (6), ⊕is the Exclusive OR (XOR) operator. Obviously, f⊕(sp)∈{0, 1}. It satisfies the associative and commutative properties, so any circular bit shifted on spclockwise or counterclockwise does not change the function value. However, any one bit change in spfrom 0 to 1 or from 1 to 0 will reverse the function value.

In Eq. (7), #1(sp)means the number of pixels with value“1” in sp, #0(sp) is the number of “0” in sp,N is an integer, and N≤P −1. If #1(sp)−#0(sp)NN, then f#(sp) returns 1; otherwise, it returns 0. In this way, f#(sp) is immune to bit shift and rotation.

3.2.Watermark embedding algorithm

We embed the watermarks by changing the value of f(sp) in a local region. The value of f(sp)is changed by altering the bits in sp. These changes are reflected by modification of pixels in the spatial local region. Different Boolean functions correspond to different algorithms. For instance, when using Boolean function f⊕(sp) in a (P, R) neighborhood, we select a pixel with the minimal magnitude in mpto alter for embedding the watermark, so that the quality of the original image block will be affected the least. In other words, we keep the value of f⊕(sp) to be consistent with the corresponding bit of watermarks.



g_3	g_2	g_1	m_3	m_2	m_1	s_3	s_2	s_1
g_4	g_c	g_0	m_4		m_0	s_4		s_0
g_5	g_6	g_7	m_5	m_6	m_7	s_5	s_6	s_7
	g_8			m_8			s_8	

Fig.1. An example of a (8, 1) local region, as divided into three parts: g8 is the pixel vector, m8 is the magnitude vector, and s8 is the sign vector.

The watermark embedding procedure can be summarized in the following two steps:

1) The original image is divided into (P, R) non-overlapping local region blocks. The LBP pattern is used to calculate mpand sp, as well as f⊕(sp). Let w be one of bits in the watermarks and β be the watermarking intensity factor.

2) For each (P, R) local neighborhood, if the value of f⊕(sp) equals to the value of w, we do nothing to the pixels in the neighborhood. Otherwise, we modify one of pixels by making the value of f⊕(sp) consistent with the corresponding w.

That is

```
$f\left(w=1 \;\; and \;\; f_{\oplus}\left(s_p\right)=0\right) \;\; or\left(w=0 \;\; and \;\; f_{\oplus}\left(s_p\right)=1\right)$
    $then\{select \;\; m_i = \min\left(m_P\right);$
        $if \;\; s_i = 1 \;\; then \;\; g_i = \left(g_i - m_i\right)\times\left(1-\beta\right);$
                $else \;\; g_i = \left(g_i + m_i\right)\times\left(1+\beta\right)\}.$
```

Note that min() is the minimal function. If there are more than one minimum, we select anyone of the minimums to determine the pixel to be changed. If a block's pixels are all “0” or “1”, we will modify the center pixel based on the corresponding watermarking bit before embedding it to the block.

3.3.Watermark extraction algorithm

The watermark extraction procedure in the proposed method becomes straight-forward. We judge the value of f⊕(sp) in the watermarked image to extract the watermark w. That is

$$if \quad f_{\oplus}\left(s_p\right)=1 \quad then \quad w=1 \quad else \quad w=0.$$

4. Experimental Results and Analysis

We use the Islamic Azad University Ahar Branch image of size 256×256 to test the performance of the proposed algorithms. The watermark is a binary image of size 84×84. The neighborhood is (8, 1), which is a 3×3 local region. One local region embeds one bit of watermarks. Therefore, the watermarking capacity is 1/9 of the original image size.

The notations are given below. W(i, j) denotes the original watermark binary image of size M×M, W*(i, j) denotes the extracted watermarked binary image of size M×M, F(i, j) denotes the original image of size N×N to be watermarked, and F *(i, j) denotes the watermarked image. We use PSNR (peak signal-to-noise ratio), EBR (error bit rate), and NC (normalized correlation), as shown in Eqs. (8), (9), and (10), respectively, to evaluate the performance.

The EBR is used to compute the rate of error bits on the whole watermark accurate bits. The NC is used to locate a pattern on the extracted watermark image that best matches the specified reference pattern from the original image base [30]. Evidently, NC measures the amount of altered information which is originally “1”, and we name it as white NC (WNC). In order to accurately calculate the effect of the attack, the amount of altered information which is originally “0” is also considered, and we name it as black NC (BNC). Note that the formula of BNC is the same as Eq. (9) with all 1's being changed to 0's and vice versa. The PSNR is often used in engineering to measure the signal ratio between the maximum power and the power of corrupting noise. We use it to compare between the original and the embedded images in the spatial domain.

$$EBR=\frac{\sum_{i=0}^{M-1}\sum_{j=0}^{M-1}\left(W(i,j)\oplus W^{*}(i,j)\right)}{M\times M} \qquad (8)$$

$$NC=\frac{\sum_{i=1}^{M}\sum_{j=1}^{M}W\left(i,j\right)\oplus W^{*}\left(i,j\right)}{\sum_{i=1}^{M}\sum_{j=1}^{M}\left[W\left(i,j\right)\right]^{2}} \qquad (9)$$

$$PSNR=10\ \log\left(\frac{255^{2}}{\sum_{i=1}^{N}\sum_{j=1}^{N}\left[F\left(i,j\right)-F^{*}\left(i,j\right)\right]^{2}/N^{2}}\right) \qquad (10)$$

By experiments, the proposed (8, 1) LBP based watermarking algorithm shows better transparency and robustness against some commonly-used image processing operations, such as additive noise, luminance variation, contrast adjustment, and color balance, Some examples of applying various operations on the watermarked image are shown in Fig. 2, where (a) is the original

Islamic Azad University Ahar Branch image, (b) is the original watermark, (c) is the watermarked Islamic Azad University Ahar Branch by the proposed algorithm with PSNR 42.67 and intensity factor β=0.08, and (d) is the extracted watermark with WNC=1 and BNC=1.

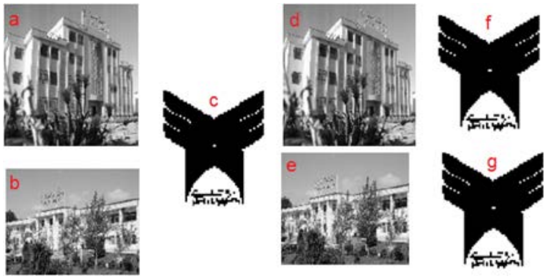


Fig.1. Examples of applying some image-processing operations on the watermarked image.(a) The original image, (b) The original image, (c) the original watermark, (d) and (e) the watermarked by the proposed algorithm, (f) and (g) the extracted watermark.

The watermarking system developed has been tested on some images and they are shown in Fig (2) and Fig (3). We can extract the watermark from the attacked watermarked image, and then by comparing the extracted watermark with the original watermark, we can localize the modification area. Fig (3) shows the differences between the watermarked images and tampered watermarked images. By these results, we can decide that the proposed tamper detection detect perfectly the tampered zones.

Table 1. PSNR values between the original and the watermarked images.

Images	A	B	C	D
Noise	0	10	20	30
EBR	0	3.7	7.2	9.8
PSNR	61.0831	62.4163	64.9135	67.9944

5. Conclusion

Based on the LBP operators, we propose a semi-fragile spatial watermarking scheme. The single-level watermarking methods are described and analyzed. The proposed methods are robust against some commonly-used image processing operations, such as additive noise, luminance change, and contrast adjustment. At the same time, they maintain good fragility to some window operations, such as filtering and blurring, and have better sensitivity to image tampering. It can also achieve tamper detection and location. For the future research, we will focus on the comprehensive comparison of different watermarking schemes based on different LBP operators, their reversibility, and security.

References

[1] M. Swanson, B. Zhu, A. Tewfik, Proc. IEEE Int. Conf. on Image Processing, vol. III, Sept. 1996, p. 211.

[2] I. Pitas, Proc. IEEE Int. Conf.on Image Processing, vol. III, Sept. 1996, p. 215.

[3] R. Schyndel, A. Tirkel, C. Osborne, Proc. IEEE Int. Conf. on Image Processing, vol. II, Nov. 1994, p. 86.

[4] X. Xia, C. Boncelet, G. Arce, Proc. IEEE Int. Conf. on Image Processing, vol. I, Oct. 1997, p. 548.

[5] K. Tanaka, Y. Nakamura, K. Matsui, Proc. IEEE ILCOM Int. Conf, 1990, p. 216.

[6] I.-K. Yeo, H.J. Kim, Proc. Int. Conf. information Technology: Coding Computing, 2001, p. 237.

[7] N. Cvejic, I. Tujkovic, Proc. IEEE Int. Symp. Consumer Electronics, U.K, 2004, p. 3.

[8] B. Chen, G. Wornell, J. VLSI Signal Process, 2001, p. 7V33.

[9] T.K. Tsui, X.P. Zhang, D. Androutsos, IEEE Trans. Forensics Security 3 (1) (March 2008) 16..

[10] Y. Shih, Digital Watermarking and Steganography: Fundamentals and Techniques, CRC Press, Boca Raton, FL, 2008.

[11] A. Reed, B. Hannigan, Proc. SPIE 4675, Apr. 2002, p. 222.

[12] P. Bas, N.L. Bihan, J. Chassery, Proc. ICASSP, Hong Kong, China, Jun. 2003, p. 521.

[13] I. Cox, J. Kilian, F. Leighton, T. Shamoon, IEEE Trans. Image Processing 6 (12) (Dec.1997) 1673.

[14] F.Y. Shih, S. Wu, Pattern Recognition 36 (2003) 969.

[15] Z. Wei, K.N. Ngan, IEEE Trans. Circuits Systems Video Technology 19 (3) (March 2009) 337.

[16] C. Podilchuk, W. Zeng, IEEE J. Sel. Areas Commun. 16 (4) (May 1998) 525.

[17] N. Kaewkamnerd, K.R. Rao, Electron. Lett. 36 (2000) 518.

[18] A. Piva, L. Boccardi, F.B.M. Barni, V. Cappellini, A.D. Rosa, Proc. IEEE Int. Conf. Multimedia Expo., New York, Jul. 30–Aug. 2, 2000, p. 1283.

[19] L.X. Luo, Z.Y. Chen, M. Chen, X. Zeng, X. Zhang, IEEE Trans. Forensics Security 5 1) (March 2010) 187.

[20] H.-T. Wu, Y.-M. Cheung, IEEE Trans. Instrumentation Measurement 59 (1) (Jan.2010) 221.

[21] Y. Yang, X.M. Sun, H. Yang, C.T. Li, R. Xiao, IEEE Trans. Circuits Systems Video Technology 19 (5) (May 2009) 656.

[22] V. Sachnev, H.J. Kim, J.N.S. Suresh, Y.Q. Shi, IEEE Trans. Circuits Systems Video Technology 19 (7) (July 2009) 989.

[23] T. Maenpaa, M. Pietikainen, T. Ojala, Proc. 15th International Conference on Pattern Recognition, Barcelona, Spain, 2000, p. 951.

[24] T. Ojala, M. Pietikainen, T. Maenpaa, IEEE Trans. Pattern Analysis Machine Intelligence 24 (7) (2002) 971.

[25] T. Ahonen, A. Hadid, M. Pietikainen, Proceedings of European Conference on Computer Vision, Prague, Czech, 2004, p. 469.

[26] T. Maenpaa, website, http://herkules.oulu.fi/isbn9514270762/2003Last accessed Dec. 20, 2008.

[27] W.Y. Zhang, N.D. Jin, Proc. the 6th International Conference on Fuzzy Systems and Knowledge Discovery, August 2009.

[28] G. Zhenhua, L. Zhang, D. Zhang, IEEE Trans. Image Processing 19 (6) (June 2010) 657.

[29] W. Zhang, F.Y. Shih, N. Jin, Y. Liu, Inter. J. Multiphase Flow 36 (2010) 793.

[30] C.-M. Kung, S.-T. Chao, Y.-C. Tu, Y.-H. Yan, C.-H. Kung, J. Multimedia 4 (3) (June 2009) 112.

[31] P. Lafferty, F. Ahmed, Proc. SPIE vol. 5561 (2004) 145.

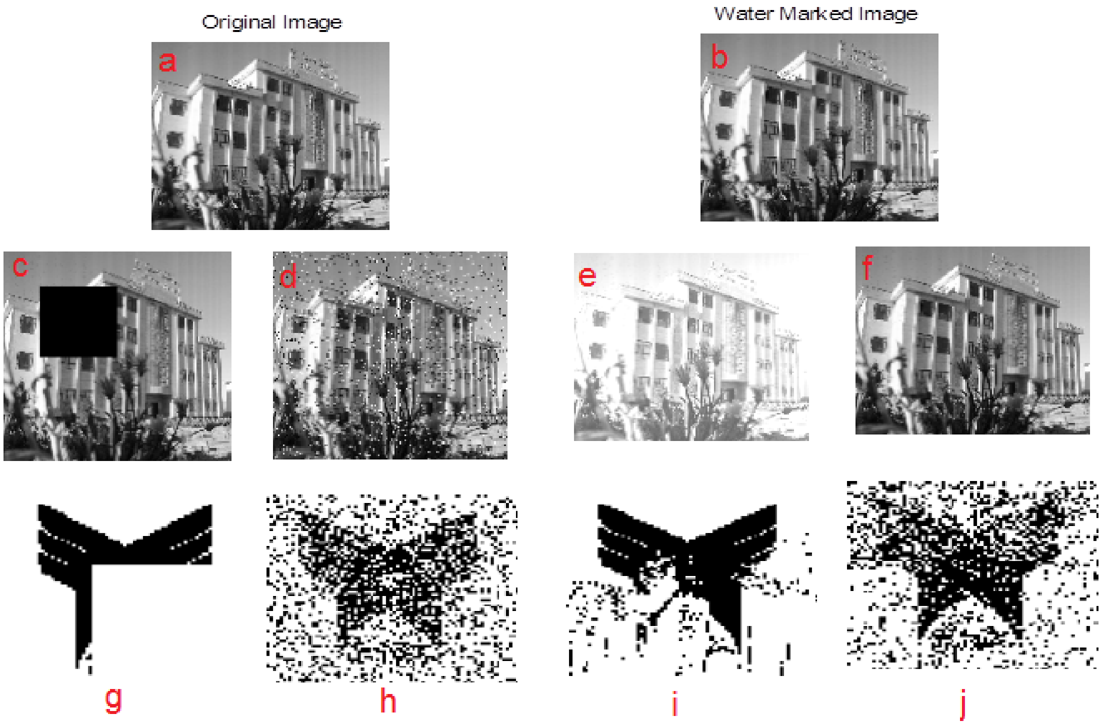


Fig.3. (a) The original image, (b) watermark image, and attack on watermarked image: (c) Cutting, (d) adding noise (e) change contrast, (f) compressing and the extracted watermark from (g) Cutting attack, (h) adding noise attack, (i) change contrast attack, (j) compressing attack.