Binary Image Watermarking in Ridgelet Domain

Marzieh Amini
Department of Electrical and Computer Engineering
Semnan University
Semnan, Iran
m_amini@semnan.ac.ir

Hamidreza Sadreazami
Department of Electrical and Computer Engineering
Shahid Beheshti University
Tehran, Iran
hm.sadreazami@mail.sbu.ac.ir

Abstract— **Binary images have only two distinct pixel color values so the capability of data hiding is very limited. To improve the robustness of watermarking algorithm, we proposed a novel ridgelet based watermarking for binary images. Ridgelet transform is efficient for representing images with line singularities. So, binary host image is partitioned into several non-overlapping blocks to make edges in each block similar to straight edges. Ridgelet transform is applied to each single block. To embed the watermark bits, directions with highest variance are selected in ridgelet coefficients matrix. To extract the watermark logo, detector response is computed for several sample watermarks and the maximum value is chosen as the extracted watermark. The proposed method has great robustness against different kinds of attacks.**

Keywords; Binary Image Watermarking; Finite Ridgelet Transform; Blind Extraction.

I. INTRODUCTION

Watermarking is a way of embedding a key into the original data in order to increase security and copyright protection. Nowadays, documents are major form of communication and a large number of them are daily exchanged. A lot of scanned important data such as personal files, handwriting signatures and academic certificates have turned into digital documents so copyright protection and information security maintenance of binary images are very important. Binary images have only two distinct pixel color values. Changing pixels in these images is more visible, therefore watermarking in binary images is very challenging task. [1-3]

Image watermarking algorithms are revolving around two categories based on the domain which is used for embedding the watermark: Spatial and Frequency domain techniques. In spatial domain techniques, modifying the pixel value of host image is the way for embedding the watermark. Frequency domain techniques such as watermarking based on discrete cosine transform [4], discrete Fourier transform and digital wavelet transform [1, 2], [5] are commonly used in recent works.

Although the discrete wavelet transform has strong performance for smooth functions in one dimension, it does not provide good results in higher dimensions such as lines where are singularities in 2-D and planes where are singularities in 3-D. The ridgelet transform was introduced in [6] as a sparse expansion for functions which have discontinuities along lines but are otherwise smooth. Finite ridgelet transform (FRIT) was proposed in [7], which is an orthonormal version of the ridgelet transform for discrete and finite size images. Since the ridgelet transform represents an image in small amount of space, it can be concerned as an appropriate transformation for digital watermarking [8, 9].

Here in this work, we propose a new watermarking scheme for binary document images in ridgelet domain. Firstly, the host image is partitioned into several non-overlapping blocks such that an edge appears as a straight line singularities. After applying ridgelet transform with directional sensibility, we acquire the direction with highest variance intensity for each single block in order to insert the watermark bits.

The rest of this paper is structured as follows: In Section II a brief review of finite ridgelet transform are discussed. In Section III, embedding and extraction steps of proposed method are expressed. Experimental result and discussion are presented in Section IV.

II. FINITE RIDGELET TRANSFORM

The finite ridgelet transform (FRIT), proposed in [7], is developed on the basis of finite radon transform (FRAT) as shown in Fig. 1. The FRAT of the real valued function on the 2-D grid Z_p^2 is defined as

$$r_k\lfloor l \rfloor = FRAT_I(k,l) = \frac{1}{\sqrt{p}} \sum_{(i,j)\in L_{k,l}} I(i,j) \quad (1)$$

Here $I(i,j)$ is the pixel value of the image at position (i,j). And also $Z_p = \{0,1,2,...,p-1\}$ and p is a Fermat prime number of the form $p = 2^n + 1$. $L_{k,l}$ is the set of points that form a line in the lattice of Z_p^2.

$$L_{k,l} = \begin{cases} \{(i,j): j = ki + l(\bmod p), i \in Z_p\}, & 0 \le k \le p-1 \\ \{(l,j): j \in Z_p\}, & k = p \end{cases} \quad (2)$$

Where $k = p$ corresponds to the vertical line. By taking 1-D discrete wavelet transform on each FRAT projection sequence $(r_k[0], r_k[1], r_k[2],...,r_k[p-2])$ for each direction k, FRIT coefficients are obtained.

978-1-4244-5900-1/10/$26.00 ©2010 IEEE

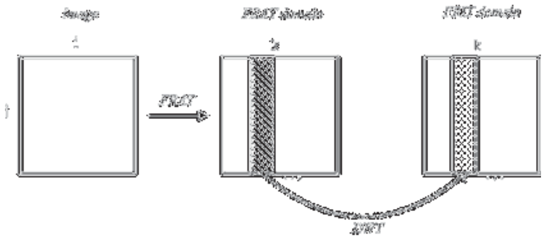


Figure 1. Diagram of computing FRIT

III. WATERMARKING ALGORITHM

A binary document is selected as a host image I of size $N \times N$ and digital binary logo W is selected as watermark with size of $M \times M$.

A. Embedding Algorithm

The embedding steps are:

- The watermark image matrix is rearranged into a 1-D sequence.
- Binary presentation of watermark sequence and host image are mapped from {0,1} into {-1,1}.

$$W_i \in \{-1,1\}, \; I(x,y) \in \{-1,1\}$$

- The original image is divided into B blocks in size of $P \times P$ that P must be primary number and obey the equation $P = 2^n + 1$.

$$I(x,y) = \bigcup_{b=1}^{B} I_b(x',y'), 1 \le x', y' \le P \quad (3)$$

- The FRIT is applied to each single block I_b. The matrix F is FRIT coefficients for each block which its size depends on both filter order and decomposition level of 1-D wavelet.

$$F = FRIT_{I_b}, 1 \le b \le B \quad (4)$$

In matrix F each column represents one of the directions in ridgelet domain.

- Calculate the variance of each column in matrix F. The column with maximum variance is considered as the best direction in ridgelet domain for inserting the watermark. It can be formulated as

$$l_b = \max_{l}(\mathrm{var}(FRIT_{I_b}(1:P+1,l))) \quad (5)$$

Which $B = M^2$ and S_b is the matrix of selected direction for b^{th} block.

$$S_b = \left[FRIT_{I_b}[1,l_b],...,FRIT_{I_b}[P+1,l_b]\right]^T, b = 1:B \quad (6)$$

- Then selected columns are put in matrix S in the same order as their blocks.

$$S = [S_1, S_2, ..., S_B] \quad (7)$$

- The proposed embedding equation is

$$S_w = S + \alpha.S.W_{ss} \quad (8)$$

B. Extracttion Algorithm

The proposed algorithm is a blind watermarking method in which the host image is not required in extraction process. I^* is the corrupt watermarked image after facing with certain type of attack which is the input element of detector. The extracting steps are:

- The ridgelet transform is applied to each single block, obtained from the same block partitioning as embedding part, of the watermarked image.
- The coefficients belonging to the best directions are selected with regard to variance intensity. These selected directions are put in ridgelet coefficient matrix S^*.
- For a blind extraction process, the correlation method needs to be applied between S^* and Y to get the detector response. Y is randomly generated marks including the original watermark.

$$z = \frac{1}{M}\sum_{i=1}^{M}\left(\frac{1}{M^2}\sum_{j=1}^{M^2} S^*(i,j).Y(j)\right) \quad (9)$$

- By comparing z parameter obtained from some sample marks denoted by Y, with the threshold in (10), presented in [10], the original watermark is the one with the highest correlation value.

$$T = \frac{1}{M}\sum_{i=1}^{M}\left(\frac{\alpha}{3M^2}\sum_{j=1}^{M^2} S^*(i,j)\right) \quad (10)$$

IV. EXPERIMENTAL RESULTS AND DISCUSSION

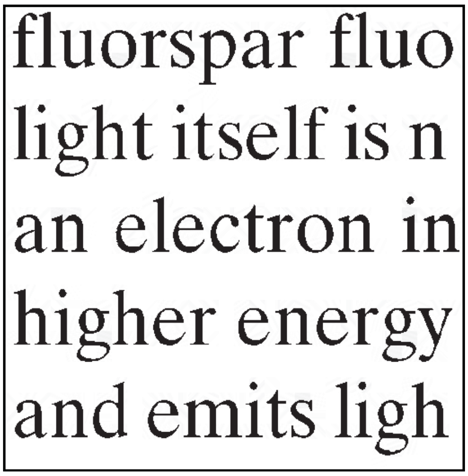
To verify the proposed algorithm, we have tested the proposed algorithm on binary document images with size of 510×510. Watermark image is binary logo of size 30×30. The partitioning step is to ensure that data would be uniformly hidden through the host image. The host image is divided into B=900 blocks of 17×17 pixels. Then watermark embedding is done by the method described in Section III. Detector response is computed for 1000 randomly generated marks.

The original and watermarked images are shown in Fig. 2 and watermark logo is shown in Fig. 3. The detector response of the detected watermark by proposed algorithm is shown in Fig. 4. The response of a given mark is compared with a threshold, T, to decide whether mark is present or not. The largest response is selected as the original watermark. The peak signal to noise ratio (PSNR) of watermarked image is equal to 44.270 dB.

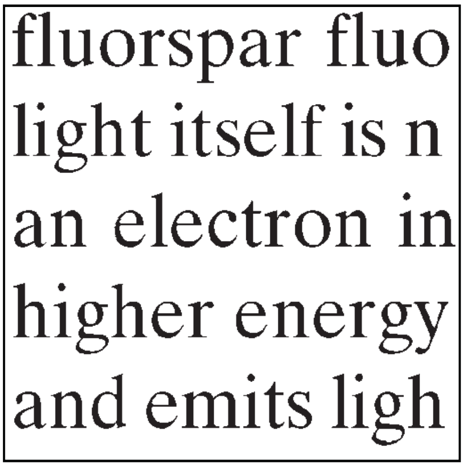
The proposed method is tested against some common attacks. The detector provides a correlation value far higher than threshold only for actual embedded watermark out of 1000 random generated testing marks.

The detector response of proposed method against rotation attack, 1° rotation, is shown in Fig. 5 with PSNR= 3.6894 dB. Also, the watermarked image was filtered with median filter and Gaussian filter of window size 7×7. Result from these attacks are shown in Fig. 6 and Fig. 7 , respectively.

As a further test, the watermarked image was corrupted by the Salt & Pepper, additive Gaussian and speckle noise. PSNR of the watermarked image, first and second peak of detector response of detected watermark in presence of noise with variance of 0.1 are listed in Table I.


fluorspar fluo
light itself is n
an electron in
higher energy
and emits ligh

(a)


fluorspar fluo
light itself is n
an electron in
higher energy
and emits ligh

(b)

Figure 2. (a) Original image document.
(b) Watermarked image PSNR= 44.270.

Figure 3. Watermark logo

Table I . PSNR after adding some common noise to watermarked image and threshold for detecting the watermark.

Type of noise Variance=0.1	**PSNR (dB)**	**First Peak**	**Threshold**	**Second Peak**
Salt & pepper	6.9821	0.111	0.03379	0.02770
Gaussian	6.3927	0.122	0.03202	0.02907
Speckle	7.3053	0.123	0.03097	0.02327

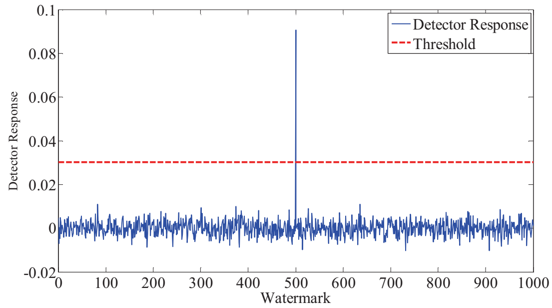


Figure 4. Detector response of detected watermark with PSNR= 44.270 dB.

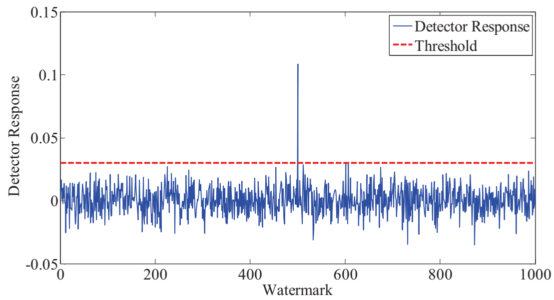


Figure 5. Detector response of detected watermark against rotation attack of 1° with PSNR= 3.689 dB.

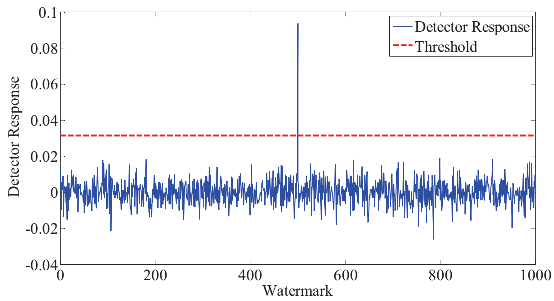


Figure 6. Detector response of detected watermark in presence of median filtering 7×7 with PSNR= 10.215 dB.

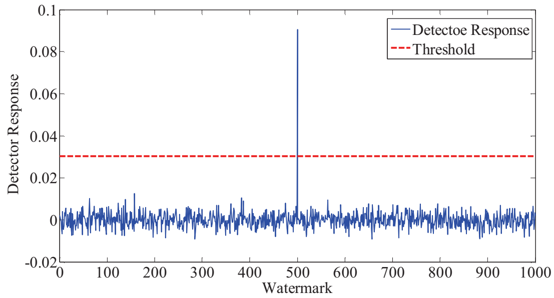


Figure 7. Detector response of detected watermark against Gaussian Filtering of size 7×7 with PSNR= 16.178 dB.

IV. CONCLUSION

Considering the binary document's characteristics of simple pixel, complex texture and difficulty in invisibility of any modification, binary image watermarking method is proposed in ridgelet domain. The watermark is embedded into direction of each block ridgelet transform which has the highest variance intensity. The detector is able to retrieve original watermark embedded in the image out of all sample marks. The proposed method exhibits perfect perceptual invisibility and simultaneously good robustness to general signal processing attacks such as rotation, Gaussian filtering, median filtering, Salt & pepper noise, Gaussian noise and Speckle noise.

REFERENCES

[1] H. Yingkun, Z. Xiangcai, Z. Lili and L. Mingxia, "Image with Less Information Watermarking Algorithm Based on DWT", Eighth ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing,vol. 3,pp. 383-387, August 2007.

[2] H. Lu and W. Xia, "A Robust Binary Image Watermarking Based on Wavelet Domain and Krawtchouk Moments", International Conference on Research Challenges in Computer Science, 2009.

[3] H. Zhihua, "Binary Image Watermarking Algorithm Based on SVD," International Conference on Intelligent Human-Machine Systems and Cybernetics, pp. 400-403, 2009.

[4] I. J. Cox, J. Killian, F. T. Leighton and T. Shamoon. "Secure spread spectrum watermarking for multimedia", IEEE Trans On Image Processing, vol. 6(12), pp. 1673-1687, 1997.

[5] C. T. Hsu and J. L.Wu, "Multiresolution watermarking for digital images", IEEE Transactions on Circuits and SystemII: Analog and Digital Signal Processing, vol. 45(8), pp. 1097-1101, 1998.

[6] E. J. Candes, "Ridgelets: Theory and applications", Ph.D. dissertation. Dept. Statistics, Stanford Univ., Stanford, CA, 1998.

[7] M. N. Do and M. Vetterli, "The finite ridgelet transform for image representation", Image Processing IEEE Transaction; vol. 12, pp. 16-28, 2003.

[8] P. Campisi, D. Kundur and A. Neri, "Robust digital watermarking in the ridgelet domain", Signal Processing Letters, IEEE; vol. 11, pp. 826-30,2004.

[9] Z. Zhang, H. Yu, J. Zhang and X. Zhang, "Digital image watermark embedding and blind extracting in the ridgelet domain", Journal of Communication and Computer USA, vol. 3, pp.75-81, 2006.

[10] M. Barni, F. Bartolini, V. Cappellini and A. Piva, "A DCT domain system for robust image watermarking", Signal Processing 1998 Elsevier Science, vol. 66, pp. 357–72, 1998.