Fingerprint Watermarking with Tamper Detection

Dr. Jasni Mohamad Zain[1] **Azma Abdullah**[2]

[1] *Image Processing and Graphic Group, Faculty of Computer Systems and Software Engineering, University College of Engineering & Technology Malaysia, Locked Bag 12, 25000, Kuantan, Pahang, Malaysia. Tel: +60-9-5492113, Fax: +60-9-5492140, E-mail: jasni@kuktem.edu.my*

[2] *Image Processing and Graphic Group, Faculty of Computer Systems and Software Engineering, University College of Engineering & Technology Malaysia, Locked Bag 12, 25000, Kuantan, Pahang, Malaysia. Tel: +60-9-5492119, Fax: +60-9-5492140, E-mail:azma@kuktem.edu.my*

Abstract

This paper proposes a watermarking method to embed watermark data into fingerprint images, without corrupting their features. The method does not require original fingerprint image to be able to detect tamper and thus authenticate the image. We used 256 x 256 grayscale fingerprint images in our experiment. The experimental results demonstrate that the precision of tamper detection and localization is close to 100% after level-2 detection.

Keywords

Watermarking, Tamper Detection, Fingerprint

Introduction

Biometrics technology is essential for today's personal identification or verification systems. The security requirements of present electronic transactions necessitate utilization of reliable factors such as fingerprint features. Watermarking of fingerprint images can be used in applications like: 1) protecting the originality of fingerprint images stored in databases against intentional and unintentional attacks, 2) fraud detection in fingerprint images by means of fragile watermarking 3) Guaranteeing secure transmission of acquired fingerprint images from intelligence agencies to a central image database, by watermarking data prior to transmission and checking the watermark at the receiver site.

There are a few published works for fingerprint image watermarking. Ratha et al [1] introduced a data hiding algorithm for wavelet compressed fingerprint images. Uludag et al [2] introduced two fingerprint watermarking techniques in which gradient directions of the feature pixels or feature regions do not change with watermarking. The watermark decoding does not need the original image.

P. Wong describes a fragile marking technique in [3], which obtains a digest using a hash function. The image, image dimensions, and marking key are hashed during embedding and used to modify the least-significant bit plane of the original image. This is done in such a way that when the correct detection side information and unaltered marked image are provided to the detector, a bi-level image chosen by the owner (such as a company logo or insignia), is observed. This technique has localization properties and can identify regions of modified pixels within a marked image. However, Holliman and Memon [5] soon presented a vector quantization (VQ) counterfeiting attack that can construct a counterfeit image from a VQ codebook generated from a set of watermarked images. To solve the problem of VQ counterfeiting attack, several enhanced algorithms were proposed [6][7]. Nonetheless, they either fails to effectively address the problem or sacrifice tamper localization accuracy of the original methods [8]. Celik et al.[8] then presented an algorithm based on Wong's scheme and demonstrated that their algorithm can thwart the VQ codebook attack while sustaining the localization property.

In this paper, we propose a watermarking method for image tamper detection. We are interested in local manipulation such as additional or removal of part of an image. Our method is efficient as it only uses simple operations such as parity checks and comparison between average intensities as compared to method proposed by Celik et. al. [8].

Approach and Methods

Watermark Embedding

The watermarking embedding procedure is described in this section. Each image is of size M x N pixels where M and N are assumed to be a multiple of six and the number of grey levels is 256.

- Preparation

We need to prepare a one to one block mapping sequence A → B→ C→ D → … → A for watermarking embedding, where each symbol denotes an individual block. The intensity feature of block A will be embedded in block B, and the intensity feature of block B will be embedded in block C, etc. We use a 1D transformation to obtain a one to one mapping among the blocks:

$$\vec{B} = [(k \times B) \bmod N_b] + 1, \tag{1}$$

where $B, \vec{B}, k \in [1, N_b]$, k is a secret key (prime number), and N_b is the total number of blocks in the image.

The generation algorithm of the block-mapping sequence is as follows:

1. Divide the image into non-overlapping blocks of 6x6 pixels
2. Assign a unique and consecutive integer $B \in \{1,2,3,...,N_b\}$ to each block from left to right and top to bottom, where N_b= (M/6) x (N/6)
3. Randomly pick a prime number $k \in [1, N_b]$
4. For each block number B, apply equation (1) to obtain $\vec{B}$, the number of its mapping block
5. Record all pairs of B and $\vec{B}$ to form the block mapping sequence

Table 1 - Mapping of Blocks with k=23,26 and Nb=40

k	**23**	**26**
B	$\vec{B}$	$\vec{B}$
1	24	27
2	7	13
3	30	39
4	13	25
5	36	11
6	19	37
7	2	23
8	25	9
21	4	27
22	27	13
23	10	39
24	33	25

Note that the secret key, k, must be a prime in order to obtain a one to one mapping; otherwise, the period is less than N_b and a one to many mapping may occur. Table 5.1 lists some parts of the mapping sequence generated with Nb=40, k=23 and 26 respectively. In this table, $\vec{B}$ starts to repeat at B=21 when k=26, which is not a prime.

- Authentication watermark and recovery watermark generation

In the schemes proposed by Wong [4] and Celik et al [8] a signature was generated for each block in order to localise tamper. Signature generation is computationally expensive and requires more bits for embedding, thus it will have an effect on the quality of the watermarked image.

In this section a case of using intensity average comparisons and parity bits as the authentication watermark is presented. To localise tamper in a block, the watermark needs to be embedded directly into that block. If a block is being tampered locally, the intensities of the pixels involved will be changed. This will also change the average intensity of the block concerned. To ensure that this is not changed, a parity check will be used. However, a parity check alone will not guarantee that the block has not been changed, because local tampering usually causes burst error [5], meaning that if more than one bit has been changed, a parity check is no longer useful. Using ECC will help solve this issue, but again more watermark bits will be needed. To overcome this, the intensity comparison is used as another guard if a parity check fails. This feature will also be used to break block wise independent. To break block wise independent, the intensity of the block is compared to the intensity of a larger block. Let B denote the bigger block (figure 1) and the smaller or sub block as B_s, then the average intensity of B is

$$Avg\_B = \frac{(P_1 + P_2 + P_3 + \ldots + P_{15} + P_{16})}{16} \quad (2)$$

and the average intensity of sub block is

$$Avg\_B_s = \frac{(P_1 + P_2 + P_5 + P_6)}{4} \quad (3)$$

P_1	P_2	P_3	P_4
P_5	P_6	P_7	P_8
P_9	P_{10}	P_{11}	P_{12}
P_{13}	P_{14}	P_{15}	P_{16}

Figure 1 - A 4x4 Block B

The intensity of each sub block will be used as the recovery watermark, and will be embedded in a block mapped by equation 1. This is to ensure that if the block is tampered with, the recovery bits will be highly likely to be available.

The choice of which signature image to use will depend on:

1. How many LSBs will be used, which is the answer to how much degradation is allowed for the watermark.
2. How will the recovered image be used? Will it be considered as authentic? If it is not, will it be used as an indication of the location and the nature of the tampering?

LSB is suggested, to minimise the degradation as medical images are very strict with the quality. The recovered image, however, will not be considered authentic and will not be used for any clinical purposes. One possibility for the purpose of recovery is to help in the investigation to find the motive and the person responsible for the tampering. A 3x3 sub block in a 6x6 block is suggested to accommodate two authentication bits and seven recovery bits to be embedded in the LSB of each pixel.

- Embedding

For each block B of 6x6 pixels, divide it into four sub-blocks of 3x3 pixels. The watermark in each sub-block is a 3-tuple (v, p, r), where both v and p are 1-bit authentication watermark, and r is a 7-bit recovery watermark for the corresponding sub-block within block A mapped to B. The

following algorithm describes how the 3-tuple watermark of each sub-block is generated and embedded:

1. Set the LSB of each pixel within the block to zero and compute the average intensity of the block and each of its four sub-blocks, denoted by avg_B and avg_B_s, respectively.

2. Generate the authentication watermark, v, of each sub-block as:

$$v = \begin{cases} 1 & if\ avg\_Bs \geq avg\_B, \\ 0 & otherwise, \end{cases} \quad (4)$$

3. Generate the parity check bit, p, of each sub-block as :

$$p = \begin{cases} 1 & if\ num\ is\ odd, \\ 0 & otherwise, \end{cases} \quad (5)$$

where num is the total number of 1s in the seven MSBs of avg_B_s.

4. From the mapping sequence generated in the preparation step, obtain block A whose recovery information will be stored in block B.
5. Compute the average intensity of each corresponding sub-block As within A, and denote it avg_A_s.
6. Obtain the recovery intensity, r, of A_s by taking the seven MSBs in avg_A_s.
7. Embed the 3-tuple watermark (v, p, r), 9 bits in all, onto the LSB of of each pixel in Bs.

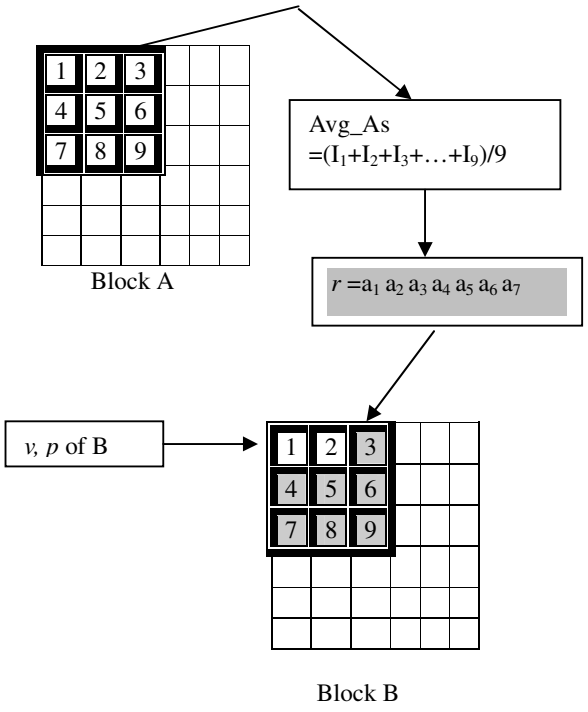

Figure 2 - Watermark Generation and Embedding Location

Results

In evaluating the proposed authentication watermarking with tamper detection, different manipulations on two fingerprint images were tested to obtain the miss detection rate for level-1 and level-2 detection.

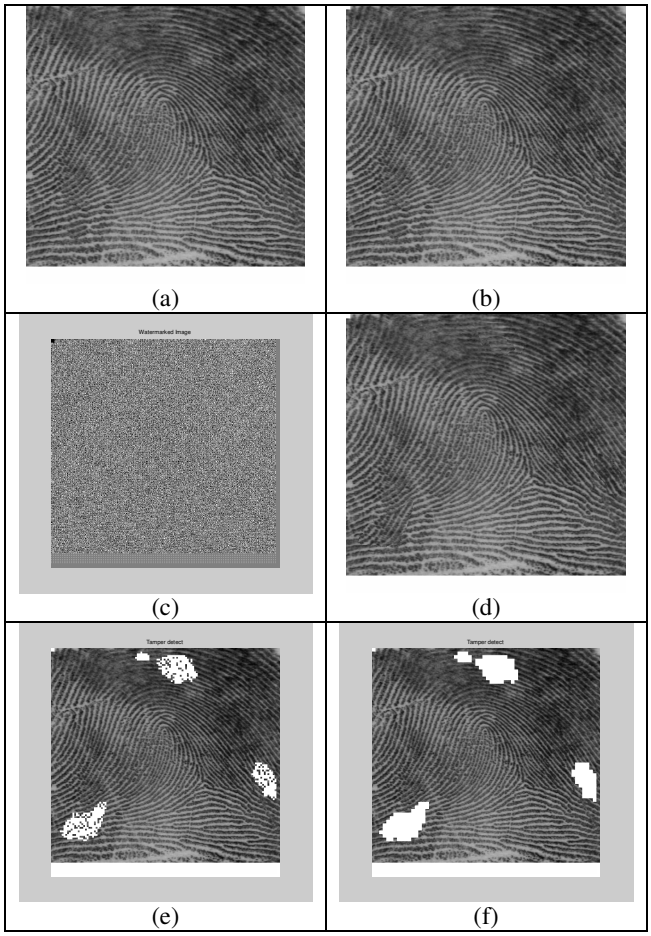

Figure 3 - (a) Original Fingerprint1 (from National Institute of Science and Technology [NIST] Science and Technical database http://www.nist.gov/srd/nistsd4.htm), (b) Watermarked Fingerprint1 PSNR = 54.5262 dB, (c) Watermark Embedded in Fingerprint1, (d) Tampered Watermarked Fingerprint1, (e) Level 1 Detection-Fingerprint1, (f) Level 2 Detection-Fingerprint1

Fingerprint1 was manipulated using healing brush tool and cloning tool. The manipulated sizes are ~60 x 50 and ~100 x 100 pixels. Figure 3(a) is the original Fingerprint1 followed by the watermarked image of fingerprint1 (3(b)) . Level 1 and level 2 detection results are shown in figure 3(e) and 3(f) respectively.

Fingerprint2 was manipulated using cut and paste and cloning tool. This time the manipulation size is smaller ranging from ~ 10 x10 to 40 x 100 pixels. Figure 4(a) shows the watermarked image of Fingerprint2 followed by

the manipulated Fingerprint2 (4(b)), the areas manipulated (4(c)) and the tamper detection for level 1 and level 2.

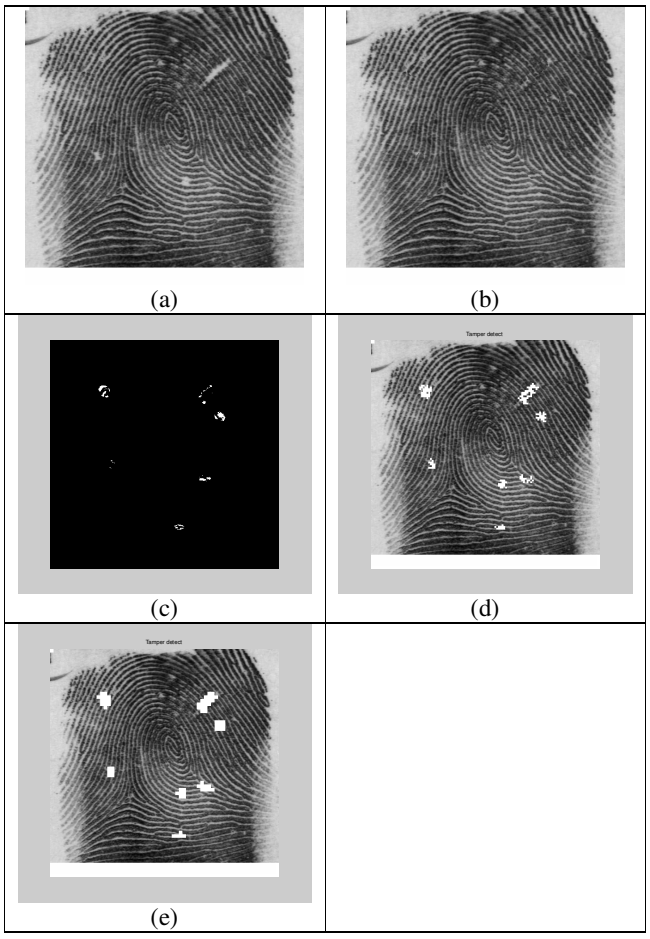

Figure 4. (a) Watermarked Fingerprint2 PSNR = 54.9982 dB,(b) Tampered Watermarked Fingerprint2, (c) Image Difference , (d) Level 1 Detection– Fingerprint2, (e) Level 2 Detection

Table 2 shows the missing detection rate using level-1 and level-2 detection. For level-1 detection, we have a maximum of 15% of missing detection rate. We achieved at least 99.94% detection rate for level-2 detection.

Table 2 - Miss Detection Rate

	Fingerprint1 (512x512)	Fingerprint2 (512x512)
Level1	15%	13%
Level2	0.06%	0.02%

Conclusion

We proposed a watermarking scheme that can detect and localize tampered images. The purpose is to verify the integrity and authenticity of fingerprint images. We presented our watermarking procedures that include data embedding and tamper detection procedure. The experimental results demonstrate that the precision of tamper detection and localization is close to 100% after level-2 detection.

References

[1] N. K. Ratha, J.H. Connell, R. Bolle, Secure data hiding in wavelet compressed fingerprint images. *Proc. Of ACM Multimedia 2000 Workshop*, pp. 127-130, 2000, CA, USA.

[2] U. Uludag, B. Gunsel, A.M. Tekalp, Robust Watermarking of Fingerprint Images, *Pattern Recognition*, **35** (12), pp. 2739-2747, Dec. 2002.

[3] P. Wong, A watermark for image integrity and ownership verification, *Final Program and Proceedings of the IS&T PICS 99*, 1999, GA, USA.

[4] P.W. Wong, "A public key watermark for image verification and authentication", in *Proceedings of the IEEE International Conference on Image Processing*, Chicago, IL, October 1998, pp. 455-459.

[5] M. Holliman, N. Memon, "Counterfeiting attacks on oblivious block-wise independent invisible watermarking schemes, *IEEE Trans. Image Processing*, 9(2000), pp. 432-441.

[6] J. Fridrich, M. Goljan, A.C. Baldoza, "New fragile authentication watermark for images", in Proceedings of the *IEEE International Conference on Image Processing*, Vancouver, BC, Canada, September 2000, pp. 10-13.

[7] P.W. Wong, N. Memon, "Secret and public key authentication schemes that resist vector quantization attack*", Proceeding SPIE 3971* (75), 2000, pp. 417-427.

[8] M.U. Celik, G. Sharma, A.M. Tekalp, Hierarchical watermarking for secure image authentication with localization, *IEEE Transactions on Image Processing*, **11**(6), 2002, pp. 585-594.

[9] I.J. Cox, M.L. Miller, J.A. Bloom, *Digital Watermarking*. San Francisco, CA: Morgan Kaufmann Publishers, 2002.