A Spatial Method for Watermarking of Fingerprint Images

Umut Uludag, Bilge Gunsel and Meltem Ballan

gunsel@mam.gov.tr

TUBITAK Marmara Research Center, Information Tech. Research Institute, P.O.Box 21, 41470 Gebze-Kocaeli, Turkey

Abstract. This paper extends the watermarking method introduced in [1] in order to embed watermark data into fingerprint images, without corrupting their features. Two methods are proposed. The first method inserts watermark data after feature extraction thus prevents watermarking of regions used for fingerprint classification. The method utilizes an image adaptive strength adjustment technique which results in watermarks with low visibility. The second method introduces a feature adaptive watermarking technique for fingerprints, thus applicable before feature extraction. For both of the methods, decoding does not require original fingerprint image. Unlike most of the published spatial watermarking methods, the proposed methods provide high decoding accuracy for fingerprint images.

1 Introduction

The wide utilization of digital media as primary form of production, editing, distribution and storing of multimedia data has brought about the problem of protection of Intellectual Property Rights (IPR). This is due to the fact that digital data can be duplicated very easily without introducing any quality degradations to the content. Watermarking has been a very active research area lately and it seems to be the solution to the protecting IPR problem. By digital watermarking, the information like origin, legal destination, access rights, is embedded to the multimedia data without introducing any perceptible differences compared to the original. Generally, imperceptibility requirement is satisfied by utilizing some form of human sensory models (Human Visual System, Human Audible System) in watermark embedding ([2], [3]).

This work is the extension of the image watermarking method in [1] to include fingerprint image features. In [1], watermark data is embedded to blue channel pixels of color images via amplitude modulation. Namely, after determining watermark embedding locations by means of a secret key, the blue channel pixel values at these locations are decreased or increased to denote watermark bits 0 and 1, respectively. An image adaptive watermark embedding rule utilizing gradient magnitude and local standard deviation is used in watermark encoding. Watermark decoding does not need

the original image. The method is especially successful in textured or busy images in terms of watermark data decoding performance.

Biometrics technology is essential for today's personal identification / 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: a) Protecting the originality of fingerprint images stored in databases against intentional and unintentional attacks, b) Fraud detection in fingerprint images by means of fragile watermarks (which do not resist to any operations on the data and get lost, thus indicating possible tampering of the data), c) 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.

In literature, there are a few published work for fingerprint image watermarking. Recently, Ratha et. al ([4]) introduced a data hiding algorithm for wavelet compressed fingerprint images. The method presented in [4] has the advantage of working in compressed domain. In our work, we introduce two fingerprint watermarking techniques in which gradient directions of the feature pixels or feature regions do not change with watermarking.

The organization of the paper is as follows. Section 2 outlines the proposed watermarking methods and their application to fingerprint image watermarking. Section 3 presents experimental results. Conclusions are summarized in Section 4.

2 Fingerprint Image Watermarking

Most common fingerprint verification methods are based on point patterns called ridge endings and bifurcations (minutiae) in fingerprints. As a result of coarse level classification of point patterns, Wirbel (whorl and twin loop) and Lasso (arch, tented arch, right and left loop) classes can be specified . Thus, once these point patterns are extracted by directional images, they can be used to find out similarity (distance) between fingerprint patterns ([5]).

This paper introduces two fingerprint watermarking methods.

Method 1

The first method inserts watermark data after feature extraction thus prevents watermarking of regions used for fingerprint classification. Figure 1 illustrates the functional block diagram of the system.

The method utilizes an image adaptive strength adjustment technique which results in watermarks with low visibility. The watermark data is embedded to gray scale fingerprint images according to the embedding rule given by Eq. (1).

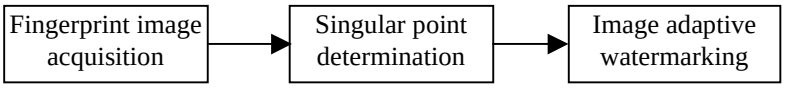

Fig. 1. Watermark encoding after feature extraction.

$$P_{WM}(i,j) = P(i,j) + (2s-1)P(i,j)q\left(1+\frac{SD(i,j)}{A}\right)\left(1+\frac{GM(i,j)}{B}\right)\beta(i,j) \quad (1)$$

where $P_{WM}(i,j)$ and $P(i,j)$ are pixel values referring to watermarked and original pixels at watermark embedding location (i,j), respectively. The value of watermark bit is denoted as s. Watermark embedding strength is denoted as q. $SD(i,j)$ denotes the standard deviation of pixel values around a local neighborhood of pixel at (i,j), and $GM(i,j)$ denotes the gradient magnitude at (i,j). A and B are normalization factors for the standard deviation and gradient magnitude, respectively. $\beta(i,j)$ takes the value 0 if the pixel (i,j) under consideration belongs to a fingerprint feature region like delta or core areas (singular points); it has value 1 otherwise.

Every watermark bit with value s in Eq. (1) is embedded multiple times to the fingerprint image pixels, whose locations are determined via the selected secret key. In addition to the real watermark data, two reference bits, 0 and 1, are embedded to the image. These reference data provides an adaptive threshold in determining the watermark bit value in decoding.

Decoding starts with finding the watermark embedding locations on the watermarked image, via the secret key used in watermark encoding stage. For every bit embedding location, the value of the original pixel, $\hat{P}(i,j)$, is estimated as the linear combination of pixels in a cross-shaped neighborhood of the watermarked pixel as in Eq.(2).

$$\hat{P}(i,j) = \frac{1}{4c}\left(\sum_{k=-c}^{c} P_{WM}(i+k,j) + \sum_{k=-c}^{c} P_{WM}(i,j+k) - 2P_{WM}(i,j)\right) \quad (2)$$

where c is the neighborhood size. The difference between the estimated and current pixel values is calculated by Eq. (3) as

$$\delta = P_{WM}(i,j) - \hat{P}(i,j) \quad (3)$$

These differences are averaged over all the embedding locations associated with the same bit, to yield $\bar{\delta}$. For finding an adaptive threshold, these averages are calculated similarly for the reference bits, 0 and 1, as $\bar{\delta}_{R0}$ and $\bar{\delta}_{R1}$, respectively.

Then, the watermark bit value $\hat{s}$ is estimated as

$$\hat{s} = \begin{cases} 1 & if\ \bar{\delta} > \dfrac{\bar{\delta}_{R0} + \bar{\delta}_{R1}}{2} \\ 0 & otherwise \end{cases} \quad (4)$$

In Eq. (1), standard deviation term *SD(i,j)* can be computed as the standard deviation of the set containing the pixel values in a cross-shaped neighborhood of the watermark bit embedding location *(i,j).* Gradient magnitude term *GM(i,j)* can be computed via Sobel operator.

SD(i,j) and *GM(i,j)* terms adjust the strength of watermarking in an image adaptive way. At locations where either *SD(i,j)* term is high (image regions with high variance) or *GM(i,j)* term is high (edge regions), the watermark signal is added more strongly to the host image. This leads to more accurate decoding of embedded watermark data, especially for busy or textured images. Although watermark decoding accuracy is increased as a result of the image adaptive increase in embedding strength, due to the fact that human visual system is relatively less sensitive to pixel value changes in busy and edge image regions, the visibility of the watermark does not increase significantly.

When the host image is a fingerprint image, additional requirements arise which must be satisfied by the watermarking system. Watermark embedding process must not introduce any changes to the fingerprint image which may alter the features extracted from that image for personal authentication - verification purposes.

In the proposed method, this requirement is satisfied. After extracting singular points from the fingerprint image and associated blocks corresponding to delta and core areas, watermark embedding is done according to Eq. (1). In this way, since $\beta(i,j)$ term is zero for those feature areas, watermarking does not change original pixel values and the singular points of the fingerprint image are preserved. As a result, the class of fingerprint image is not changed by watermarking.

Method 2

The second method introduces a feature adaptive watermarking technique for fingerprints that is applicable before feature extraction (Figure 2).

Fig. 2. Adaptive watermark encoding with gradient direction analysis.

Method 2 first utilizes an orientation analysis over the acquired fingerprint image. Then, the watermark embedding is performed by preserving the gradient orientations at and around watermark embedding locations specified by the secret key, within the quantization interval that original data belongs. Since the extraction of fingerprint features is based on gradient orientations, when watermark embedding does not change the quantized gradient orientation at considered pixel and its neighbors, the features of the fingerprint image is preserved. The same watermarking embedding technique is utilized for method 1 and method 2. Note that unlike method 1, the proposed watermark embedding scheme does not fix the actual gradient orientation at a pixel *(i,j)*, but limits its change within the original orientation quantization interval. Hence, the performance of fingerprint verification–identification system is not affected by watermarking.

The quantization levels of orientation of fingerprint images, which are called Poincare index in literature ([6]), divide the 2• pixel gradient orientation circle into 16 bands, with each band covering • / 8 radians, as shown in Figure 3.

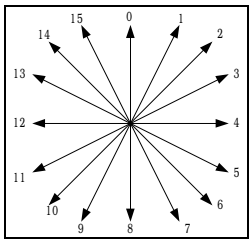

Fig. 3. Poincare index

Let *(i,j)* denote the watermark embedding pixel specified by the secret key and *D(k,l)* denote the eight neighbor pixels of *(i,j)*. Watermark encoder first calculates gradients at all pixels belonging to *D(k,l)*. In our work, Sobel operator is used for gradient calculations. Let $\alpha(i\text{-}1,j\text{-}1)$ denote the gradient orientation at pixel *(i-1,j-1)*. α can be calculated by Eq. (5), where $G_y(i\text{-}1,j\text{-}1)$ and $G_x(i\text{-}1,j\text{-}1)$ refer to the gradients in *y* and *x* directions, respectively.

$$\alpha(i\text{-}1,j\text{-}1) = \arctan\left(\frac{G_y(i\text{-}1,j\text{-}1)}{G_x(i\text{-}1,j\text{-}1)}\right) \quad (5)$$

The encoder then constitutes the inequality shown in Eq. (6) for all the pixels in *D(k,l)*, in order to specify the new gradient values that guarantees to preserve fingerprint features while embedding watermark data. In Eq. (6), α_q represents poincare index gradient direction associated with the pixel, and G_{yn}(i-1,j-1) and G_{xn}(i-1,j-1) are new values of vertical and horizontal gradients for pixel *(i-1,j-1)*. In fact, the embedding changes the actual gradient orientations, but preserves quantized gradient directions according to poincare index intervals. As a maximum, the value of the actual gradient at any pixel can change ± •/8 radians without altering the quantized poincare index.

$$(\alpha_q - \frac{\pi}{16}) < \arctan(\frac{G_{yn}(i\text{-}1,j\text{-}1)}{G_{xn}(i\text{-}1,j\text{-}1)}) < (\alpha_q + \frac{\pi}{16}) \quad \textbf{(6)}$$

Note that, watermark encoder modifies the watermark embedding strength *q* of Eq. (1) to preserve the quantized gradient directions of these pixels.

3 Experimental Results

In order to evaluate the results of proposed watermarking methods, fingerprint images shown in Figure 4, left column, are watermarked according to methods 1 and 2, as explained previously. These images represent main fingerprint image classes *tented arch, right loop* and *whorl* ([7]).

The images in the middle column shows the images watermarked with the method 1. Parameters used in watermarking are: q = 0.2, A = 100, B = 1000. The watermark data is the binary representation of the 22 character string *Fingerprint_watermark.* The embedded watermark data size is 156 bits. As a maximum, 7.6 % of the pixels in the image are modified in watermark embedding.

In Figure 4, last column shows fingerprint images which are watermarked with the method 2, which utilizes gradient direction analysis. In this method, the number of pixels which satisfy the watermarking criteria (not altering quantized gradient orientations of 8-neighbour pixels) is considerably small. Experiments showed that approximately 0.8 % of image pixels are valid candidates for watermark embedding. Since the watermarking capacity is reduced, the watermark data size is decreased to 12 bits as compared to 156 bits embedded with the previous method. In spite of this decrease in the capacity, the latter method has the advantage of not changing any of the fingerprint features which are used later in authentication.

For both of the watermarking methods, watermarked fingerprint images are decoded with 100 % decoding accuracy; also the watermarking does not change the

fingerprint features of the original images. Visibility of the watermark data is kept low as a result of utilizing image adaptive embedding in watermark encoding.

4 Conclusions

The image adaptive watermarking method introduced in [1] is extended to include fingerprint image properties. The proposed methods preserve fingerprint feature regions either by isolating singular point regions during watermark embedding or adjusting the watermark embedding strength in order to guarantee that gradient directions remain within the analytically computed intervals. Thus, fingerprint images are watermarked without changing the features associated with them. Furthermore, image adaptive watermark embedding rule increases decoding accuracy and satisfies the invisibility criterion. Alternatively, by utilizing gradient direction analysis in watermark embedding, none of the fingerprint features used in authentication are altered.

References

1. Uludag, U., Gunsel, B., Tekalp, A.M.: Robust watermarking of busy images. Proc. of SPIE Electronic Imaging 2001 Conference, Security and Watermarking of Multimedia Contents III, vol. 4314, 2001, CA, USA.
2. Hartung, F., Kutter, M.: Multimedia watermarking techniques. Proceedings of the IEEE, vol. 87, no. 7, pp. 1079-1107, July 1999.
3. Swanson, M.D., Kobayashi, M., Tewfik, A.H.: Multimedia data embedding and watermarking technologies. Proceedings of the IEEE, vol. 86, no. 6, pp. 1064-1087, June 1998.
4. Ratha, N.K., Connell, J.H., Bolle, R.: Secure data hiding in wavelet compressed fingerprint images. Proc. of ACM Multimedia 2000 Workshops, pp.127-130, 2000, CA, USA.
5. Jain, A.K., Hong, L., Pankanti, S., Bolle, R.: An identity-authentication system using fingerprints. Proceedings of the IEEE, vol. 85, no. 9, Sept. 1997, pp. 1365-1388.
6. Kawagoe, M., Tojo, A.: Fingerprint Pattern Classification. Pattern Recognition, vol. 17, no. 3, pp. 295-303, 1984.
7. Candela, G.T., Grother, P.J., Watson, C.I., Wilkinson, R.A., Wilson, C.L.: A Pattern Level Classification Automation System for Fingerprints. NISTIR 5647, Technical Report and CD, NIST, 1995.

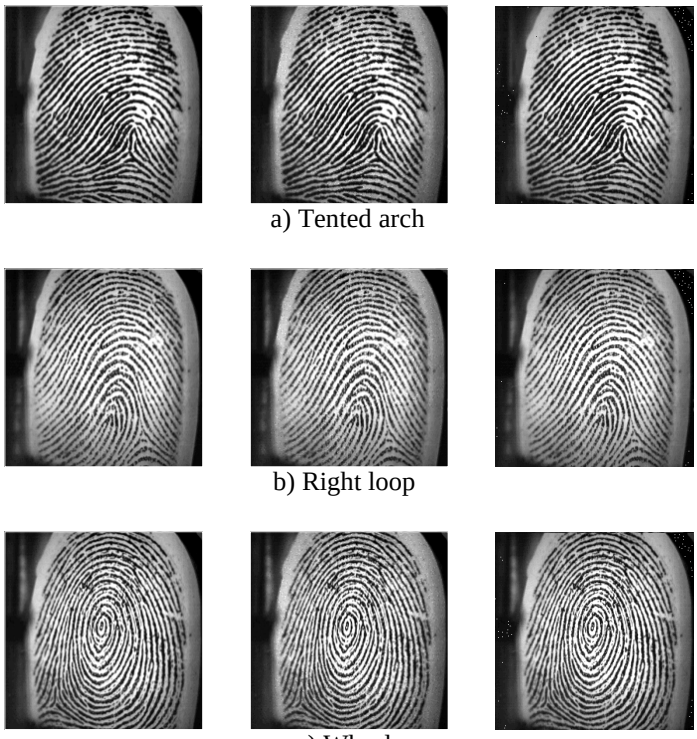

Fig. 4. Left column: Original fingerprint images, a) Tented arch, b) Right loop, c) Whorl. Middle column: Watermarked images by method 1. Last column: Watermarked images by method 2.