Selecting a Hiding Locations For Fingerprint Images

Dr. Amir S. AL-Malah
AL-Mustansiriyah University
College of Science
Computer Science Dept.
Baghdad – IRAQ
E-mail: al_malahasmy@yahoo.com
Mob. No/ 07902244945

Abstract

With the wide spread utilization of biometric identification systems, establishing the authenticity of biometric data itself has emerged as an important research issue. We propose here a new scheme that finds hiding locations for fingerprint images. The method determines the locations which are suitable for embedding the watermark into fingerprint image. Watermark data are embedding according to certain conditions.

Keywords: Information hiding; Watermarking; Biometric; Fingerprint.

1. Introduction

Information hiding represents a class of processes used to embed data into various forms of digital data such as image, audio, and video. In digital images the information hiding applications could be divided into two groups depending on the relationship between the embedded message and the cover image. The first group is formed by steganographic applications. The second group of applications is frequently addressed as digital watermarking [1].

With the proliferation of information exchange across the Internet, and the storage of sensitive data on open networks, information hiding is becoming an increasingly important feature of computer security. A biometrics-based verification system works properly only if the verifier system can guarantee that the biometric data came from the legitimate person at the time of enrollment [2].

In order to promote the wide spread utilization of biometric techniques, an increased level of security of biometric data, especially fingerprints, is necessary because the fingerprints are digitized, stored, and transmitted over a network; they become susceptible to malicious as well as accidental attacks. In order to preserve the fidelity of this information and prevent alterations from being made at will, a protective scheme must be used. Steganography and watermarking are among the possible techniques to achieve this [3].

Steganography involves hiding critical information in unsuspected carrier data. As a result, steganography- based techniques can be suitable for transferring critical biometric information, such as minutiae data, from a client to a server. Steganographic techniques reduce the chances of biometric data being intercepted by a pirate, hence reducing the chances of illegal modification of the biometric data [4].

On the other hand, watermarking involves embedding information into the host data itself, so it can provide security even after decryption. Furthermore, encryption can be

applied to the watermarked data. However, embedding watermark may change the inherent characteristics of the host image (e.g., locations of minutia points in fingerprints). Therefore, the verification performance based on (decoded) watermarked images should not be inferior compared to performance based on non-watermarked images [5].

Digital 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), and (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 [3].

There have been only a few published papers on watermarking of fingerprint images. Ratha et al. [6] proposed a data hiding method, which is applicable to fingerprint images compressed with WSQ wavelet-based scheme. The discrete wavelet transform coefficients are changed during WSQ encoding, by taking into consideration possible image degradation. Pankanti and Yeung [7] proposed a fragile watermarking method for fingerprint image verification. A spatial watermark image is embedded in the spatial domain of a fingerprint image by utilizing a verification key. The proposed method can localize any region of image that has been tampered. Pankanti and Yeung conclude that their watermarking technique does not lead to a significant performance loss in fingerprint verification. A semiunique key based on local block averages is used by Jain [8] to detect tampering of host images, including fingerprints and faces. Gunsel et al. [3] described two spatial domain watermarking methods for fingerprint images. The first method utilizes gradient orientation analysis in watermark embedding, so the watermarking process alters none of the features extracted using gradient information. The second method preserves the singular points in the fingerprint image, so the classification of the watermarked fingerprint image (e.g., into arch, left loop, etc.) is not affected.

The paper is organized as follows. The fingerprint system is explained in Section 2. The possible attacks in biometric system are provided in Section 3. The proposed method for selecting the locations where the watermark is embedded is described in Section 4. Conclusions are summarized in Section 5.

2. Fingerprint System

Fingerprints are fully formed at about seven months of fetus development and finger ridge configurations do not change throughout the life of an individual except due to accidents such as bruises and cuts on the fingertips. This property makes fingerprints a very attractive biometric identifier [9].

The fingerprint of an individual is unique. A fingerprint is formed from an impression of the pattern of ridges on a finger. A ridge is defined as a single curved segment, and a valley is the region between two adjacent ridges. The minutiae, which are the local discontinuities in the ridge flow pattern, provide the features that are used for identification.

Fingerprint system can be separated into two categories *Verification* and *identification* [10].

Verification system authenticates a person's identity by comparing the captured biometric characteristic with its own biometric template(s) pre-stored in the system. It conducts one-to-one comparison to determine whether the identity claimed by the individual is true. A verification system either rejects or accepts the submitted claim of identity.

Identification system recognizes an individual by searching the entire template database for a match. It conducts one-to-many comparisons to establish the identity of the individual. In an identification system, the system establishes a subject's identity (or fails if the subject is not enrolled in the system database) without the subject having to claim an identity.

A fingerprint system works in two modes they are Enrollment mode and Authentication mode. Enrollment mode: fingerprint system is used to identify and collect the related information about the person and his/her fingerprint image. Authentication mode: fingerprint system is used to identify the person who is declared to be him/her.

3. Possible Attacks in Biometric System

There are eight basic sources of attacks that are possible in a generic biometric system. In the first type of attack, a fake biometric (such as a fake finger) is presented at the sensor. Resubmission of digitally stored biometric data constitutes the second type of

attack. In the third type of attack, the feature detector could be forced to produce feature values chosen by the attacker, instead of the actual values generated from the data obtained from the sensor. In the fourth type of attack, the features extracted using the data obtained from the sensor is replaced with a synthetic feature set. In the fifth type of attack, the matcher component could be attacked to produce high or low matching scores, regardless of the input feature set. Attack on the data which stored in databases is the sixth type of attack. In the seventh type of attack, the channel between the database and matcher could be compromised to alter transferred template information. The final type of attack includes altering the matching result itself. All of these attacks have the possibility to decrease the credibility of a biometric system [2].

4. The Proposed Method

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, therefore this method is determines hiding locations of watermark which not use in feature extraction operation thus prevents watermarking of regions used for fingerprint classification and recognition. The most commonly used fingerprint features in the fingerprint features extraction methods are ridge bifurcations and ridge endings which resulted by the thinning process, collectively known as minutiae. Therefore locations these minutiae must be avoided in the hiding operation of watermark. The proposed method consists of the following steps:

Image Acquisition: from plain scanners (for inked fingerprint) or through live-scanners. Through them, a digital gray-level image of the fingerprint is captured; the image is shown in Fig.1. This figure is an example of input fingerprint images from scanner.

Fig.1. The fingerprint image.

Image Enhancement: It is usual that during the acquisition step, some noise appears resulting in cutting of the ridges and other undesirable effects. Because of this, a process that improves the quality of the fingerprint is needed in order to improve the clarity of ridge structures of fingerprint image and to prepare fingerprint image for next step. In this step, the filter which used to remove various types of noise in fingerprint image is mean filter; the mean filter is expressed as:

$$\text{Mean} = \frac{1}{9} \sum_{r=1}^{3} \sum_{c=1}^{3} \text{Image}(r, c) \quad \dots (1)$$

where r is number of rows in filter, c is number of columns in filter.

Binarization: In this step, the fingerprint image is transformed from a gray-level image into a binary image**.** This improves the contrast between the ridges and valleys in a fingerprint image, and consequently facilitates the extraction of features. Ridge extraction, or ridge segmentation, is main task from binarization process for fingerprint image. One ways of accomplishing this process is by using the edge detection operation and global thresholding technique.

The Sobel operator is followed by a global thresholding operation in which each pixel in the image is assigned a value representing either white or black depending on the magnitude of the gradient at that point as follow:

$$B(x, y) = \begin{cases} 1 \text{ if } EM(x, y) > T \\ 0 \text{ if } EM(x, y) \le T \end{cases} \quad \dots (2)$$

where $EM(x, y)$ is the edge magnitude value which results from convolution a Sobel operator. The Sobel operator is described in

[11], which performs the edge detection operation using horizontal and vertical filters.

Thinning (Skeletonization): After the fingerprint image is converted to binary form, it is then submitted to the thinning algorithm which reduces the ridge thickness to one pixel wide. The thinning must be performed without modifying the original ridge. The purpose of thin image which produced from the thinning algorithm is play very important role to determine the hiding locations in which the watermark bits will be stored in the original fingerprint image.

The standard thinning operation is described in [12], which performs the thinning algorithm using two subiterations.

Selecting the Locations for Embedding the Watermark: In this step, the method determines the locations which are suitable for embedding the watermark into fingerprint image. Watermark data are embed onto fingerprint image according to the embedding condition given below:

If α (i, j) =1Then Insert watermark bit (W) in I(i, j).

where *I(i, j)* are pixel values referring to original pixels at watermark embedding location *(i, j*). The value of watermark bit is denoted as *W*, where $W \in [0, 1]$. The *α (i, j)* term guarantees the pixels (called marked pixels) which will store watermark bit are not belonging to region which used in the feature extract process from fingerprint images, therefore the performance of a method which will using the watermarked image (e.g., fingerprint verification in the case of watermarked fingerprint images) is unchanging; *α (i, j),* takes the value 0 if the pixel (i, j) under consideration belongs to a fingerprint feature region; it has value 1 otherwise.

To obtain *α (i, j)*, it is got the resulted binary image file from the binarization step, and get the resulted thin image file from thinning operation, if binary pixel *(i, j)* =1and thinning pixel *(i, j)* =0 then α *(i, j)* =1 otherwise α *(i, j)* =0, this will be used to determine the places in which the watermark bits will be stored in the original fingerprint image. For example Fig.2. shows three matrices are binarization results, the thinning results, and the suitable hiding locations selection. These matrices consisting of two values are one and zero. The third matrix is play main role in determines the hiding locations where the each location in third matrix consisting (1) this location is suitable hiding location in original fingerprint image.

1	1	1	1	0	1	0	1
0	1	0	1	0	0	1	0
0	0	0	1	0	1	1	0
0	0	0	1	0	1	0	1
0	1	1	1	1	0	1	1
1	1	0	0	1	0	1	1
0	1	1	1	1	1	1	1
1	1	0	1	1	0	1	1

(a)

1	1	1	0	0	1	0	1
0	0	0	1	0	0	1	0
0	0	0	1	0	0	1	0
0	0	0	1	0	1	0	1
0	0	1	1	1	0	1	0
0	1	0	0	1	0	1	0
0	1	1	1	1	1	1	0
1	0	0	0	0	0	1	0

(b)

0	0	0	1	0	0	0	0
0	1	0	0	0	0	0	0
0	0	0	0	0	1	0	0
0	0	0	0	0	0	0	0
0	1	0	0	0	0	0	1
1	0	0	0	0	0	0	1
0	0	0	0	0	0	0	1
0	1	0	1	1	0	0	1

(c)

Fig.2. Three matrices :(a) Binarization results, (b) Thinning results, (c) The hiding locations

5. Conclusions

The watermark is hidden in such a way that the fingerprint features that are used in matching are not changed during encoding/decoding. As a consequence, the verification accuracy based on decoded watermarked fingerprint images is very similar to that with original fingerprint images.

Because the hiding locations are the edge pixels regions only The proposed method made the changes visibility to the host image are unobserved. Due to the fact that human visual system is relatively less sensitive to changing pixel value in busy image regions and edge image regions, the visibility of the watermark does not increase significantly.

References

[1] Jessica .F, Miroslav .G and Rui .D, "***Lossless Data Embedding – New Paradigm in Digital Watermarking***", SUNY Binghamton, Binghamton, NY 13902, 2001.

[2] Jain A. K. and Uludag Umut, "***Hiding Biometric Data***", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 25, No. 11, November 2003.

[3] Gunsel Bilge, Uludag Umut, and Ballan Meltem, "***A Spatial Method for Watermarking of Fingerprint Images***", TUBITAK Marmara Research Center, Information Tech. Research Institute, Turkey, 2002.

[4] Jain Anil K., Umut Uludag and Rein-Lien Hsu, "***Hiding a Face in a Fingerprint Image***", Computer Science and Engineering Department, Michigan State University, USA, 2002.

[5] Jain A. K. and Uludag Umut, "***Hiding Fingerprint Minutiae in Images***", Computer Science and Engineering Department, Michigan State University, 2002.

[6] N.K. Ratha, J.H. Connell, and R.M. Bolle, "***Secure Data Hiding in Wavelet Compressed Fingerprint Images***", Proc. ACM Multimedia, pp. 127-130, Oct. 2000.

[7] S. Pankanti and M.M. Yeung, "***Verification Watermarks on Fingerprint Recognition and Retrieval***", Proc. SPIE, vol. 3657, pp. 66-78, 1999.

[8] S. Jain, "***Digital Watermarking Techniques: A Case Study in Fingerprints & Faces***", Proc. Indian Conf. Computer Vision, Graphics, and Image Processing, pp. 139-144, Dec. 2000.

[9] Davide M., Dario M. and Anil k., "***Fingerprint Image Recognition***", Hand Book, 2002.

[10] F.A. Afsar, M. Arif and M. Hussain, "***Fingerprint Identification and Verification System using Minutiae Matching***", Pakistan Institute of Engineering & Applied Sciences, Proceedings of the National Conference on Emerging Technologies, session VII paper No 2 (P 141-146), 2004.

[11] Scott E. Umbaugh, "***Computer Vision and Image Processing: a Practical Approach Using CVIP Tools***", Prentice Hall, 1998.

[12] Gonzalez, R. and Woods, R., "***Digital Image Processing***" Second Addition, Prentice-Hall Inc., 2002.