IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 6, Ver. III (Nov.-Dec. 2016), PP 66-70
www.iosrjournals.org

Enhancing Security of Fingerprinting Technique with Watermarking

Arpana Bharani[1], Dr. Jitendra Sheetlani[2]
[1]Research Scholar, Sri Satya Sai University of Technology & Medical Science, Sehore, India
[2]Associate Professor, SOCA Sri Satya Sai University of Technology & Medical Science, Sehore, India

Abstract: *To increase the security in biometric system data there is the need to use steganography techniques with the biometric techniques. The establishment of direct personal identity is uniquely identified by using fingerprints. But fingerprints are also at risk to accidental attacks. Nowadays the most important concerns is the protection of biometric data and therefore it is gaining interest among researchers. The storing and transferring of biometric data, needs many security concerns that are sensitive and if this data is lost, counterfeited, or hacked, it may be impossible to recover. The security of biometric data can be increased by the application of steganography and watermarking techniques. In this the fingerprint data can be hidden in the host image and this image is transferred to the receiving end instead of the actual minutiae data. Then by using a secret key, the hidden biometric data are extracted accurately from the carrier image. The data is hidden in such a way to minimize the degradation of actual minutiae data. In this paper a method is described to handle attacks on the carrier image.*

I. Introduction

Biometric techniques such as face, facial thermo gram, fingerprint, iris, etc., use physiological or behavioral characteristics, are becoming increasingly popular compared to traditional token-based or knowledge-based techniques such as identification card (ID), passwords, etc. Among these techniques fingerprint-based techniques are the most extensively studied and the most frequently deployed. A fingerprint-based biometric system has four stages: acquisition, representation, feature extraction and matching. In the acquisition stage, a fingerprint image is captured via live-scan methods. In the representation stage, the aim is to find invariant and discriminatory information inherent in the fingerprint image. In minutiae-based systems, the discontinuities in the regular ridge structure of fingerprint images, called ridge endings and ridge bifurcations, are identified in feature extraction stage. During matching, a similarity value between the features extracted from the template and the input fingerprint images is calculated. This similarity value is used to arrive at an accept/reject decision [4], [5].

While biometrics techniques have inherent advantages over traditional personal identification techniques, the problem of ensuring the security and integrity of the biometrics data is critical. For example, if a person's biometric data (e.g., his/her fingerprint image) is stolen, it is not possible to replace it unlike replacing a stolen credit card, ID or password. Schneier [12] points out that 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. Furthermore, while biometrics data provide uniqueness, they do not provide secrecy. For example, a person leaves fingerprints on every surface he/she touches and face images can be surreptitiously observed anywhere that person looks. Ratha *et al*. [9] identify eight basic sources of attacks that are possible in a generic biometric system. Examples of these attacks include presenting a “fake” finger at the sensor and intercepting the transmitted template and/or sensed fingerprint. All of these attacks have the possibility to decrease the credibility of a biometric system.

In order to promote the wide spread utilization of biometric techniques, an increased security of the biometric data, especially fingerprints, seems to be necessary. Encryption, watermarking and steganography are possible techniques to achieve this. Steganography, derived from the Greek language and meaning secret communication, involves hiding critical information in unsuspected carrier data. While cryptography focuses on methods to make encrypted information meaningless to unauthorized parties, steganography is based on concealing the information itself. Digital watermarking techniques can be used to embed proprietary information, such as company logo, in the host data to protect the intellectual property rights of that data [3], [10].

On the other hand, since watermarking involves embedding information into the host data itself, it can provide security even after decryption. Furthermore, encryption can be applied to the watermarked data. Another option is to use steganograpy: by hiding fingerprint features in a carrier image, the security of fingerprint information can be increased. In this paper, an applications of an amplitude modulation-based watermarking method are introduced.

II. Watermarking Techniques

Digital watermarking, or simply watermarking, which is defined as embedding information such as origin, destination, access level, etc. of multimedia data (e.g., image, video, audio, text, etc.) in the host data, has been a very active research area in recent years [3], [7]. General image watermarking methods can be divided into two groups according to the domain of application of watermarking. In spatial domain methods (e.g., [5]), the pixel values in the image channel(s) are changed. In spectral-transform domain methods, watermark signal is added to the host image in a transform domain such as the full-frame DCT domain [1], Fourier-Mellin domain [11], etc.

There have been only a few published papers on watermarking of fingerprint images. Ratha *et al*. [7] 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. Message bits are encoded as the least significant bits of selected coefficients. Pankanti and Yeung [6] 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. To increase the security of the watermark data, the original watermark image is first transformed into another mixed image, and this mixed image is used as a new watermark image. The mixed image does not have a meaningful appearance, contrary to original watermark image that can contain specific logos or texts. Pankanti and Yeung conclude that their watermarking technique does not lead to a significant performance loss in fingerprint verification.

Uludag *et al*. [12] described two spatial domain watermarking methods for fingerprint images. The first method utilizes gradient orientation analysis in watermark embedding; pixel values at watermark embedding locations are changed in a way to preserve the quantized gradient orientations around those pixels. As a result, 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.

III. Hiding Minutiae Data

In this paper, an application scenario of fingerprint is considered. The basic data hiding method depends upon the host image in carrying the minutiae data and the medium of data transfer.

3.1. Application Scenario

The application scenario involves a steganography-based application (Figure 1). The fingerprint minutia which is to be transmitted is hidden in a cover image, whose function is to carry the data. The host image and the hidden data are not related. As a result, the host image can be any image available to the encoder. In our application, we have considered a synthetic fingerprint image. The synthetic fingerprint image is obtained after a post-processing of the image generated using the algorithm described by Cappelli *et al*. [2].

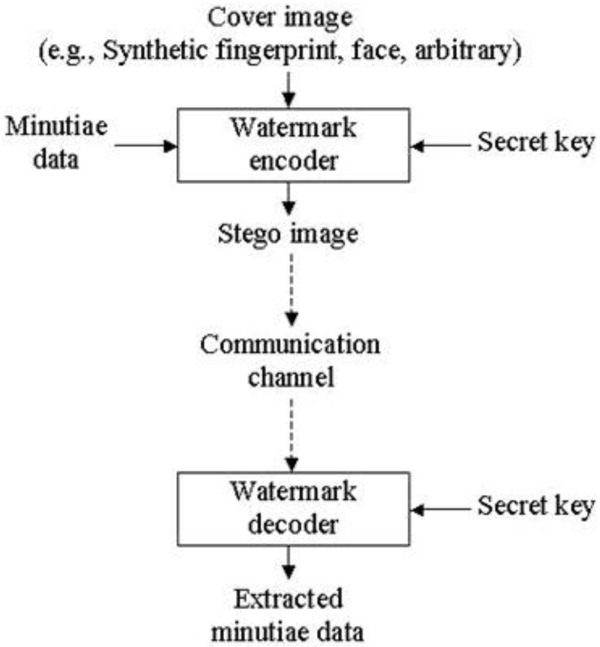
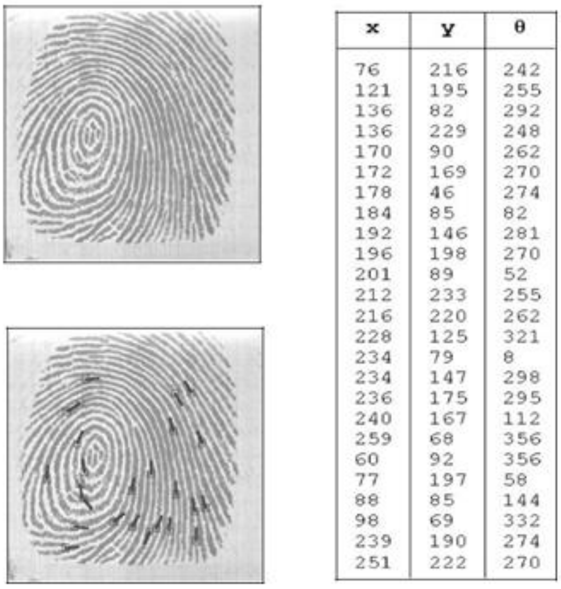


Figure 1. Steganograpy-based minutiae hiding

Figure 2. Sample cover image: synthetic fingerprint.

Figure 3 shows an input fingerprint image, overlaid minutiae image and the attributes (x, y, θ) of the extracted minutiae. These attributes constitute the data to be hidden in the host images. The fingerprint image which was used here was captured by a solid state sensor manufactured by Veridicom. The minutiae are extracted using the method outlined in [4]. The minutiae data shown in Figure 3(c) contain three fields per minutiae: x-coordinate, y-coordinate and orientation, for a total of 25 minutiae. The minutiae data ((x_i , y_i ,θ_i), i = 1, 2, ..., 25) are hidden in the cover image using the method explained in Section 3.2. To increase the security of the hidden data a secret key is utilized in encoding. The image with embedded data (stego image) is sent through the channel. the hidden data is recovered at the decoding site, using the same key that was used by the encoder.



x	y	θ
76	216	242
121	195	255
136	82	292
136	229	248
170	90	262
172	169	270
178	46	274
184	85	82
192	146	281
196	198	270
201	89	52
212	233	255
216	220	262
228	125	321
234	79	8
234	147	298
236	175	295
240	167	112
259	68	356
60	92	356
77	197	58
88	85	144
98	69	332
239	190	274
251	222	270

Figure 3. Minutiae data: (a) input fingerprint image, (b) overlaid minutiae image, (c) minutiae point attributes.

The first step of the method include to covert hidden minutiae data into a bit stream. Every field of individual minutia is converted to a 9-bit binary representation. Such a representation can code integers between [0, 511] and this range is adequate for x-coordinate ([0, #rows-1]), y-coordinate ([0, #columns-1]) and orientation ([0, 359]) of a minutia. A random number generator initialized with the secret key generates locations of the host image pixels to be watermarked.

The magnitude of watermarking is adjusted by image adaptivity terms. Standard deviation and gradient magnitude terms utilize contrast/texture masking properties of the human visual system HVS. The visibility of an image component reduced due to the presence of another component is masking [8]. The high contrast image areas are masked more strongly than changes in smooth image areas.

Every watermark bit is embedded at multiple locations in the host image. The correct decoding rate of the embedded information is increased by this redundancy. Image capacity (size) and visibility of the changes in pixel values limits this redundancy.

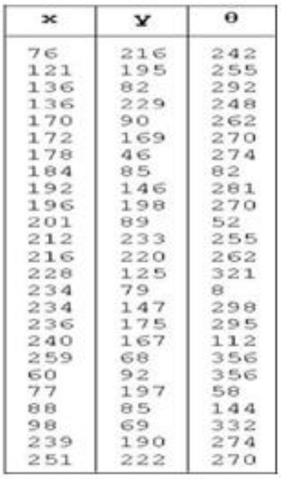
Also two reference bits, 0 and 1, are embedded in the image in addition to the binary minutiae data to determine the minutiae bit values during decoding. The secret key which is used during the watermark encoding stage is used to find the data embedding locations in the watermarked image during decoding.

The linear combination of pixel values is used to estimate the value for every bit embedded in location, (*i*, *j*). In order to increase the decoding accuracy, the encoder uses a controller block. The minutiae data hidden in the host image is extracted from decoded watermark bits.

IV. Experimental Results

Figures 5 show the stego images, which carry the minutiae data shown in Figure 3, for the cover images in Figure 2. Nearly 17% of the stego image pixels are changed during data hiding. The key used in generating the locations of the pixels to be watermarked is selected as the integer 1,000. However, the exact value of key does not affect the performance of the method. Other watermarking parameters are set to: q =0.1, A =100 , B = 1000 . A higher q value increases the visibility of the hidden data.

Increasing A or B decreases the effect of standard deviation and gradient magnitude in modulating watermark embedding strength, respectively.



x	y	θ
76	216	242
121	195	255
136	82	292
136	229	248
170	90	262
172	169	270
178	46	274
184	85	82
192	146	281
196	198	270
201	89	52
212	233	255
216	220	262
228	125	321
234	79	8
234	147	298
236	175	295
240	167	112
259	68	356
60	92	356
77	197	58
88	85	144
98	69	332
239	190	274
251	222	270

Figure 5. Stego images and decoded data: (a) synthetic fingerprint,(b) extracted minutiae data.

Table 1. Host image and watermarking characteristics

Host	Overall Pixel	Changed Pixel	Avg. Change in
Image	Average	Average	Pixel Values
Figure 2)	221.8	222	24.9

V. Conclusions

The biometric based identification techniques are so popular than traditional identification techniques as in this it is possible to identify an authorized person and a fraud. But the security and integrity of the biometric data is an important issue. Encryption, watermarking and steganography are possible techniques to secure biometrics data. In this paper, an application of a watermarking method is presented which is related to increasing the security of biometric data exchange, which is based on steganography. The data decoding performance in the case of several attacks on host images is analyzed..

References

[1] M. Barni, F. Bartolini, V. Cappellini and A. Piva, "A DCT domain system for robust image watermarking", *Signal Processing*, vol. 66, no. 3, May 1998, pp. 357-372.

[2] R. Cappelli, A. Erol, D. Maio and D. Maltoni, "Synthetic fingerprint image generation", *Proc. ICPR*, Sept. 3-7, 2000, Barcelona, vol. 3, pp. 475-478.

[3] F. Hartung and M. Kutter, "Multimedia watermarking techniques", *Proc. IEEE*, vol. 87, no. 7, July 1999, pp. 1079-1107.

[4] A.K. Jain, L. Hong and S. Pankanti, "Biometric identification", *Comm. ACM*, vol. 43, no. 2, Feb. 2000, pp. 91-98.

[5] M. Kutter, F. Jordan and F. Bossen, "Digital signature of color images using amplitude modulation", *Proc. SPIE EI*, San Jose, Feb. 1997, vol. 3022, pp. 518-526.

[6] S. Pankanti and M.M. Yeung, "Verification watermarks on fingerprint recognition and retrieval", *Proc. SPIE EI*, San Jose, Jan. 1999, vol. 3657, pp. 66-78.

[7] N.K. Ratha, J.H. Connell and R.M. Bolle, "An analysis of minutiae matching strength", *Proc. 3rd AVBPA*, Halmstad, Sweden, June 2001, pp. 223-228.

[8] N.K. Ratha, J.H. Connell and R.M. Bolle, "Secure data hiding in wavelet compressed fingerprint images", *Proc. ACM Multimedia 2000*, pp. 127-130.

[9] B. Schneier, "The uses and abuses of biometrics", *Comm. ACM*, vol. 42, no. 8, Aug. 1999, pp. 136.

[10] M.D. Swanson, M. Kobayashi and A.H. Tewfik, "Multimedia data-embedding and watermarking technologies", *Proc. IEEE*, vol. 86, no. 6, June 1998, pp. 1064-1087.

[11] The USC-SIPI Image Database. [Online]. http://sipi.usc.edu/services/database/Database.html.

[12] U. Uludag, B. Gunsel and M. Ballan, “A spatial method for watermarking of fingerprint images”, *Proc. 1st Intl. Workshop on Pattern Recognition in Information Systems*, Setúbal, Portugal, July 2001, pp. 26-33.

[13] U. Uludag, B. Gunsel and A.M. Tekalp, “Robust watermarking of busy images,” *Proc. SPIE EI*, San Jose, Jan. 2001, vol. 4314, pp. 18-25.

[14] J.J.K. Ruanaidh and T. Pun, “Rotation, scale and translation invariant spread spectrum digital image watermarking”, *Signal Processing*, vol. 66, no. 3, May 1998, pp. 303-317