ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 3, Special Issue 4, April 2014

Two days National Conference – VISHWATECH 2014

On 21st & 22nd February, Organized by

Department of CIVIL, CE, ETC, MECHNICAL, MECHNICAL SAND, IT Engg. Of Vishwabharati Academy's College of engineering, Ahmednagar, Maharastra, India

Secure Multimodal Authentication Using Watermarking

Mr. Anand Kolapkar , Prof. B. B. Gite

ME student, Dept. of Computer Engineering, Sinhgad Academy of Engg. Pune, Maharashtra, India.

Head, Dept. of Computer Engineering, Sinhgad Academy of Engg. Pune, Maharashtra, India.

Abstract— As malicious attacks greatly threaten the security and reliability of biometric systems, Authentication of biometric data is very important. In this paper Two-stage authentication based on watermarking is proposed to address this problem. The facial features of an individual embed into a fingerprint image which works as data credibility token and secondary authentication source. At the first stage of authentication, the credibility token of input data is established by checking the validness of extracting patterns. Due to the specific characteristics of face watermarks, the face detection based classification schemes are applied for reliable watermark verification instead of conventional correlation based watermark detection. If token authentication is successful, the face patterns can further serve as supplemental identity information to facilitate sub sequential biometric authentication. In this framework, one critical issue is to guarantee the robustness and capacity of watermark while preserving the discriminating features of host fingerprints. Hence a wavelet quantization based watermarking and LSB watermarking approach is proposed to adaptively distribute watermark energy on significant DWT coefficients of fingerprint images.

Keywords: Biometrics, Digital watermarking, DWT, LSB

I.INTRODUCTION

With the rapid use of internet the copyright protection, Illegal modifying, copying and tampering and have become very important issues [7]. Hence, there is a strong need of developing the techniques to face all these problems. Digital watermarking [1] emerged as a solution for protecting the multimedia data. Digital Watermarking is the process of embedding an imperceptible data into the given data. This imperceptible signal is called watermark or metadata and the given signal is called cover work. The watermark should be embedded into the cover work, so that it should be robust to survive most common signal distortions as well as distortions caused by malicious attacks. This cover work can be an audio, image or a video file. A watermarking algorithm consists of two algorithms, an embedding and an extraction algorithm.

There are some critical attributes necessary to every watermarked media such as:

1. Imperceptibility: there should be no perceptible difference between the cover signal and the stego signal. In other words, the watermarking process should not degrade the quality of the media.
2. Robustness: different kinds of attacks could be exerted on a stego signal intentionally or unintentionally to remove or destroy the watermark. These attacks contain additive noise, resampling, lossy compression, filtering, and geometrical attacks such as: cropping, rotating, and scaling. This signal processes would not harm the watermark in a robust watermarking scheme unless it degrades the quality of the stego media
3. Security: the secret message embedded in a watermarked data should not be recognizable to an unauthorized person. To gain this purpose, sometimes the secret message is encrypted and then embedded in the cover data. There has always been a contradiction between robustness and imperceptibility. Enhancing the robustness makes the watermark more perceptible and vice versa.

There are some other watermarking attributes which may be necessary in some situations:

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 3, Special Issue 4, April 2014

Two days National Conference – VISHWATECH 2014

On 21st & 22nd February, Organized by

Department of CIVIL, CE, ETC, MECHNICAL, MECHNICAL SAND, IT Engg. Of Vishwabharati Academy's College of engineering, Ahmednagar, Maharastra, India

4. Fastness: in some applications, especially real-time communications, the watermark process should be done quickly.
5. Capacity: some applications need to embed large amount of data in their media.

Along with the widespread applications of biometric based authentication technique, insuring the security and authenticity of biometric data is becoming increasingly critical [4]. *Template protection* is a classical countermeasure to this problem [3]. Inherited from conventional cryptographic tools, it mainly transforms the extracted biometric features into secret domain and effectually guarantees their security by the secrecy of transformation function or secret keys. However, in some scenarios, especially when human interaction is required, the biometric data have to be kept in explicit form rather than encrypted templates, such as: face images on smart cards, fingerprint images retained as legal proofs. Under these conditions, digital watermarking turns out to be an appropriate solution. Hidden within digital content imperceptibly, the watermark could serve as forensic token throughout the chain-of custody. Consequently, Jain *et al.* [4] suggest introducing watermarking as another defensive line of biometric security.

Existing researches that apply digital watermarking to assist biometric systems could be generally divided into two classes:

A. Multimodal authentication.

Jain *et al.* [4] embeds Eigenface coefficients as watermark in fingerprint image and extracts them for fusion recognition with host fingerprint. However, since the Extracted pattern is given for identification without credibility verification, it only increases recognition performance under attack free circumstances thus provide no additional security [2].

B. Two-factor authentication.

Kim *et al.* [6] embed a small face image into fingerprint and establish data authenticity by watermark verification before fingerprint authentication. The hidden face watermark only plays the role of conventional token; the identity information within itself is hardly displayed. Neither type of work takes full advantage of the biometric watermark, one strategy that establishes data credibility while efficiently employing watermark identity information is urgently needed.

II. RELATED WORK

LSB is a simple and fast watermarking algorithm presenting a high embedding capacity. The main is advantage of LSB is its poor robustness. Changing the least significant bit of the cover samples produces a unit error to the signal. The noise produced due to this unit error is imperceptible. But anybody could omit the watermark without degrading the quality of the media by substituting the least significant bits with zero. As the LSB layer for embedding the secret bits increases, the error gets larger. For instance, hiding information in the second least significant bit doubles the modification error. In brief, if the watermark is imperceptibly embedded in a higher LSB layer a stronger watermarking scheme is achieved [2, 3].

The least significant bit (LSB) technique is used for simple operation to embed information in a cover signal. The LSB technique is that inside of a cover signal pixels are changed by bits of the secret message. Although the number was encrypted into the first 8 bytes of the grid, the 1 to 4 least bits needed to be changed according to the embedded message. On the average, only half of the bits in an image will need to be modified to hide a secret message using a cover image. Changing the LSB of a pixel results in small changes in the intensity of the pixel colors. Human visibility system cannot perceive these changes. However, an attacker can easily extract the changed bits, since; it has performed very simple operation. The pixel value of the cover image is 139(10001011)2 and the secret data is 0. It applies to LSB-1 that the changed pixel value of the cover is 138(10001010)2. LSB can store 1-bit in each pixel.

The Discrete Wavelet Transform is a powerful and useful multi-resolution decomposition method in digital watermarking. It is often applied on image processing, and has been applied to such as edge detection, noise reduction and data compression. It is consistent with the visual perception process of human eyes. DWT uses discrete wavelet transform to decompose the original image into four sub-bands LH1, LL1, HH1 and HL1, which can be separate into higher frequency sub-bands and lower frequency sub-bands. The low frequency sub-band LL1 which stands for the coarse level coefficients can be further decomposed into four sub-bands LH2, LL2, HH2, and HL2. We can reach the final satisfied scale by repeat this decomposition process. The low frequency image usually has better stability against the image distortion, so most time digital watermarking based on DWT is done in the LL sub-band to be robust to various classes of attacks like filtering, collusion and compression. DWT is easy to implement and can efficiently reduce the computation time.

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 3, Special Issue 4, April 2014

Two days National Conference – VISHWATECH 2014

On 21st & 22nd February, Organized by

Department of CIVIL, CE, ETC, MECHNICAL, MECHNICAL SAND, IT Engg. Of Vishwabharati Academy's College of engineering, Ahmednagar, Maharastra, India

III. PROPOSED METHOD

In this paper, a watermarking based two stage authentication framework (Fig. 1) for providing the security and reliability of biometric system is proposed. In data collection progress the face feature is embedded into fingerprint image of the same individual. During authentication, the authenticity of input data is established at the very first stage by checking the validness of extracted watermark. Only if the extracted watermark is authentic, the system will proceed with the second stage, where the face watermark could serve as supplemental identity information to facilitate biometric authentication.

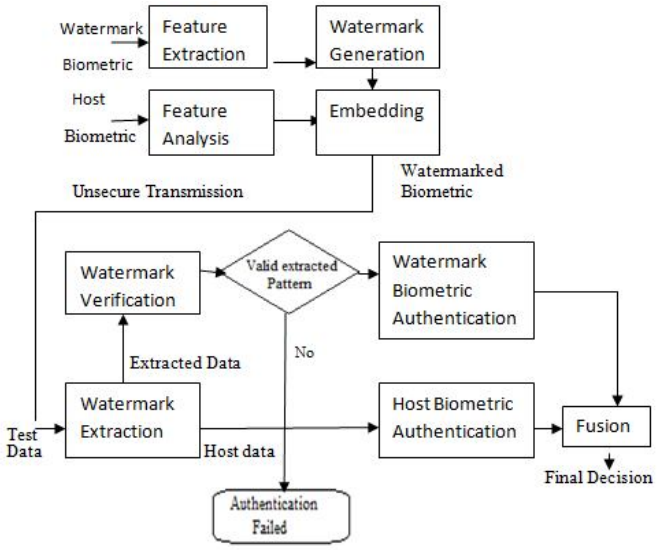

Fig. 1 System Architecture

In this progress, a wavelet quantization and LSB based watermarking method is proposed to increase watermark robustness while maintaining relative high capacity. Meanwhile, a sparse representation based classification approach is adopted to efficiently exploit the identity information within the compact face watermarks. The watermark verification along with low resolution faces identification perform A novel SVM based face watermark verification method is proposed to increase the data credibility authentication accuracy. Proposed DWT and LSB method can provide robust information hiding and high data payload.

A. DWT Algorithms

1) Watermark Generation

Biometric watermarking has its own characteristics. For authentication biometric watermark can be utilized, it should be discriminating and of advantage to have robustness to various distortions [19]. In most of watermarking applications either, watermark robustness or data payload is provided. Specifically, a compact feature allows high embedding robustness but poses challenges to verification, while a comprehensive feature facilitates verification at the expense of watermarking robustness. Employing a simple yet discriminative feature as watermark is an important issue for biometric watermarking.

Besides, since watermark embedded is usually assumed to be integrated with biometric sensor complex face features which require high computational ability and additional prior knowledge will greatly restrict the practical applicability of the system. Therefore, we only generate the face feature in a straight-forward manner by down sampling the face image with a high ratio and apply the thumbnail as watermark feature.

Gray scale pixel values of the thumbnail are extended into a feature vector Vf with *Nw* bits. A random binary sequence Sb of the same length is generated by the watermark secret key *Kw* with the logistic chaotic map [17][11] based method that applied in our previous work [16]. The final watermark *w* used for embedding is obtained by A:

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 3, Special Issue 4, April 2014

Two days National Conference – VISHWATECH 2014

On 21st & 22nd February, Organized by

Department of CIVIL, CE, ETC, MECHNICAL, MECHNICAL SAND, IT Engg. Of Vishwabharati Academy's College of engineering, Ahmednagar, Maharastra, India

$$W = \mathrm{Vf} \square Sb \qquad (A)$$

where □ denotes the Exclusive-OR (XOR) operation.

2) Watermark Extraction

Different from SDQ method which chooses the adaptive extraction threshold *y* according to the components of watermark sequence, the blind extraction of the proposed SDDM could be performed in a straightforward manner.

With the quantization step parameter *Q* and the embedding secret key *Ke*, the watermark extraction progress which is mainly the inverse operations of watermark embedding could be summarized as follows:

Step 1(*Wavelet decomposition):* Decompose the image with three-level wavelet transform, prepare LH3 and HL3 subband for watermark extraction.

Step 2(*Coefficients grouping):* Shuffle the subband coefficients using the embedding secret key *Ke*, and regroup non-overlapped coefficients into blocks. Localize the blocks Δi, $i \in [1, Nw]$ assigned for watermark bits.

Step 3(*Watermark bits extraction)n:* For each coefficient block Δi, $i \in [1, Nw]$, compute the positive significant difference Δi and decode the watermark bit as:

$$w_i' = \mathrm{mod}\left(\mathrm{round}\left(\frac{\hat{\Delta}_i}{Q}\right), 2\right)$$

Finally, the binary watermark bits seq eature vector as the inverse progress of watermark generation. After regenerating the random encrypting sequence *S* with the watermark private key *Kw*, the face watermark feature vector *v'* could be retrieved by (B):

$$V' = W' \oplus S \qquad (B)$$

B. LSB Watermarking:

1) Embedding Algorithm

This section describes the embedding algorithm. Input image and type of secret data, it transfers the secret data to binary values and determines the coordinates of the image which the data will be embedded in. First, it will embed the length of the data in five pixels starting from the first coordinate which it select and jump by 5 until it embed it in the five pixels in the 3rd and 4th LSB, but if the length of data is more than 1023 characters, it will ask to rewrite the data and it should be not more 1023 characters. Then, the data will be embedded in the image in the 3rd and 4th LSB. Then, watermarked image will be produced and it will be saved.

2) Extraction Algorithm

It describes the extracting algorithm. It takes watermarked image as input, it produces the length of the secret data from the 3rd and 4th LSB in the five pixels starting from the determined coordinates and jump by 5 until it get it from the five pixels. Then, it will get secret data also from the 3rd and 4th LSB in binary values. After that, transfer the binary values to characters which will be shown as the secret data.

IV. RESULTS AND DISCUSSION

A. Data set

1. FVC2002 DB2- 110 × 8 Fingerprint database.
2. FRGC2 - 110 × 8 Face database.

Above datasets can be used to evaluate the working of the system.

B. Result Set

The implementation is done in java using NetBeans where user is allowed to enter an image for training and query image for testing as an input. Above mentioned datasets can be used for the same purpose. And results are then compared with existing systems results. Proposed methodology is used to provide the better results preventing loss of information.

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 3, Special Issue 4, April 2014

Two days National Conference – VISHWATECH 2014

On 21st & 22nd February, Organized by

Department of CIVIL, CE, ETC, MECHNICAL, MECHNICAL SAND, IT Engg. Of Vishwabharati Academy's College of engineering, Ahmednagar, Maharastra, India

V. CONCLUSION AND FUTURE SCOPE

Proposed watermarking based two-stage authentication system is used to enhance biometric security. It is theoretically appropriate for any biometric data, and the two-stage strategy can be modified flexibly according to the practical requirements. The employment of face detection and SRC classifier offers a novel perspective of combining powerful pattern recognition tools with watermarking as promising intersections. Meanwhile, the proposed DWT and LSB method can also facilitate robust information hiding applications where both high data payload and robustness are demanded.

In future work, this system can be used for security purpose in various domains such as medical etc.

REFERENCES

[1] Bin Ma, Chunlei Li, Yunhong Wang, Zhaoxiang Zhang and Di Huang "Enhancing Biometric Security with Wavelet Quantization Watermarking based Two-stage Multimodal Authentication" 2416-2419 ICPR
[2] J. H¨ammerle-Uhl, K. Raab, and A. Uhl. Watermarking As a means to enhance biometric systems: A critical survey. In *Proc. Information Hiding*, pages 238–254, 2011.
[3] A. K. Jain, K. Nandakumar, and A. Nagar. Biometric template security. *EURASIP Signal Processing*, 2008.
[4] A. K. Jain and U. Uludag. Hiding biometric data. *Trans. Pattern Anal. Mach. Intell.*, 25(11):1494 – 1498.
[5] T. Y. Jea and V. Govindaraju. A minutia-based partial fingerprint recognition system. *Pattern Recognition*, 38:1672–1684, 2005.
[6] W. Kim and H. Lee. Multimodal biometric image Watermarking using two-stage integrity verification. *Signal Processing*, 89(12):2385 – 2399, 2009.
[7] B. Klare and A. Jain. On a taxonomy of facial features. In *Proc. BTAS*, pages 1–8, 2010.
[8] W. Lin, S. Horng, T. Kao, and et al. An efficient watermarking method based on significant difference of wavelet coefficient quantization. *IEEE Trans. Multimedia*, 10(5):746–757, 2008.
[9] A. Mian, M. Bennamoun, and R. Owens. Keypoint Detection and local feature matching for textured 3d face recognition. *IJCV*, 79(1):1–12, 2008.
[10] J. Wright, A. Y. Yang, A. Ganesh, and et al. "Robust face recognition via sparse representation." *IEEE Trans.Pattern Anal. Mach. Intell.*, 31(2):210 – 227, 2009.
[11] Bin Ma, Yunhong Wang, Chunlei Li, Zhaoxiang , Di Huang " Secure multimodal biometric authentication with wavelet quantization based fingerprint watermarking" Multimed Tools Appl DOI 10.1007/s11042-013-1372-5
[12] Gaurav Bhatnagar, Balasubramanian Raman " A new robust reference watermarking scheme based on DWT- SVD". 0920-5489/$-see front matter 2008 Elsevier
[13] Cvejic, N. and T. Seppanen," Digital Audio watermarking Techniques and Technologies: Applications and Benchmarks, IGI Global, pp.328-330, 2207.
[14]N. Verma, Mumbai Maharashtra, " Review of Steganography Techniques" ACM, ICWET, pp. 990-993, 2011
[15] Abdullah Bamatraf, Rosziati Ibrahim, Mohd. Najib B Mohd Salleh "Digital Watermarking Algorithm Using LSB"
[16] Li C, Wang Y, Ma B, Zhang Z (2012) Multi-block dependency based fragile watermarking scheme for fingerprint images protection. Multimed Tools Appl. doi:10.1007/s11042-011-0974-z
[18] Zhang J, Tian L, Tai H (2004) A new watermarking method based on chaotic maps. In: IEEE international conference on multimedia and expo, 2004, vol 2,
pp 939–942
[19] Hämmerle-Uhl J, Raab K, UhlA(2011) Watermarking as a means to enhance biometric systems: a critical survey. In: Information hiding. Springer, pp 238–254