THE INTERNATIONAL JOURNAL OF SCIENCE & TECHNOLEDGE

Application Research of MD5 Algorithm in LSB Watermarking

Anand V. Kolapkar
PG Student, Department of Computer Engineering
Sinhgad Academy of Engineering, Pune, University of Pune, India
Balasaheb B. Gite
Professor & Head, Department of Computer Engineering.
Sinhgad Academy of Engineering, Pune, University of Pune, India

Abstract:
As malicious attacks greatly threaten the security and reliability of biometric systems, Authentication of biometric data is very important. In this paper multimodal authentication based on watermarking is proposed to address this problem. Face features of an individual are embedded into a fingerprint image which works as data credibility token and secondary authentication source. In first stage of authentication, validity of extracted patterns is checked with the input biometric data. Due to the specific characteristics of face feature, the face feature detection based classification strategies are used for reliable watermark verification. If token authentication is successful, the face features works as additional identity information to facilitate sub sequential biometric authentication.
In this framework, one critical issue is to guarantee the authentication to images and capacity of watermark while preserving the discriminating features of host fingerprints. Hence a MD5 algorithm is used to generate a key of face image and LSB watermarking approach is proposed to distribute watermark energy of fingerprints. Experimental results shows both watermarking and biometric authentication performance and demonstrate the effectiveness of this work.

Keywords*: Digital Watermarking, LSB, MD5, Biometrics*

1. Introduction

With the rapid use of internet the copying, tampering, copyright protection and Illegal modifying 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 hidden data into the given data. This hidden signal is called watermark or metadata and the given signal is called cover work. The watermark should be encrypted in the cover work, so that it should be robust to come through most common signal distortions as well as optical aberrations 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.

Following attributes are necessary to every watermarked media such as:

- Imperceptibility: there should be no visible difference between the cover signal and secret message.The watermarking process should not degrade the quality of the media.
- Robustness: different kinds of attacks could be worked on a secret data signal, by purpose or unintentionally to remove or destroy the watermark. These attacks contain addition of noise, filteration, resampling and lossy compression. If attacks such as: rotation, cropping or scaling are applied to target data. This signal attacks would not harm the watermark in a robust watermarking scheme unless it decreases the quality of the stego media
- Security: the secret message in a watermarked data should not be recognizable to an unauthorized individual. To achieve this, sometimes the secret message is encrypted and then embedded in the target data. There is always contradiction between imperceptibility and robustness. Enhancing the robustness makes the watermark more perceptible and vice versa. Some other watermarking characterstics which may be necessary in some situations are as follows:
- Fastness: in real-time communications the watermark process should be performed promptly.
- Capacity: the capacity of a watermark is the amount of information it contains. This can be expressed as a number of bits watermarks that might be inserted into a signal

Along with the widespread applications of biometric based authentication technique, authenticity and security of biometric data is becoming increasingly imporatnt [4]. Template protection is a classical countermeasure to this problem [3]. Inherited from traditional cryptographic tools, it mainly converts the extracted biometric features into secret domain and effectually guarantees their security by the secrecy of secret keys or transformation function. However, in some scenarios, especially when human interaction is needed, the biometric data have to be kept in explicit form rather than encrypted templates, such as: fingerprint images,face images on smart cards retained as legal proofs. Under these circumstances, digital watermarking turns out to be an

appropriate solution. Data embedded within digital content which are not visible, the watermark could serve as forensic token throughout the range-of custody. Jain *et al.* [4] suggest introducing watermarking as additional defensive line of biometric security.

Researches that apply digital watermarking to secure biometric systems could be generally divided into two types:

- *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].
- *Two-factor authentication:* Kim *et al.* [11,20] embed a small face features into fingerprint which establish data authenticity by watermark verification before fingerprint authentication. The secret face watermark only plays the role of conventional token; the identity information within itself is hardly displayed. None of work takes advantage of the biometric watermark, one strategy that establishes data credibility while efficiently employing watermark identity information is urgently required.

2. Architectural Approaches

Least Significant Bit is a fast and simple watermarking algorithm presenting a high embedding capacity.Changing the least significant bit of the cover signal produces a unit error to the signal. The error produced due to this unit error is imperceptible. As the LSB layer for embedding the secret bits increases, the error gets larger. Hiding information in the second least significant bit doubles the modification error. If the watermark is imperceptibly embedded in a higher LSB layer a stronger watermarking scheme is achieved [7]. 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 bits of the signal, the first to fourth least bits needed to be changed according to the embedded message. On the norm, only half of the bits in an image will need to be modified to conceal a secret message using a cover image. Changing the least significant bit of a pixel results in small changes in the intensity of the pixel colors. Human visibility system cannot visualise these changes. The pixel value of the cover image is 141(1000 1101)2 and the secret data is 0. It applies to LSB that the changed pixel value of the cover is 140(1000 1100)2. Least Significant Bit 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 mostly performed on image processing and has been applied to such as edge detection, data compression and noise reduction. It is consistent with the visual perception process of human eyes.Discrete wavelet transform used to decompose the original image into four sub-bands HL1, LL1, HH1 and LH1, which can be separate into higher frequency sub-bands and lower frequency sub-bands. The low frequency sub-band LL1 can be further decomposed into four sub-bands HL1, LL1, HH1 and LH1. To reach the final state it decomposition process is repeted. The LL and LH low frequency image usually has better stability against the image distortion. Mostly digital watermarking based on DWT is done in the low frequency sub-band to be robust to various classes of attacks like filtering, compression etc. Therefore, watermark is embedded into approximate sub-image to gain a better robustness.

The discrete cosine transform helps separate the image into parts spectral sub-bands of differing importance with respect to the image's visual quality.The Discrete Cosine Transform is like the discrete Fourier transform: it transforms a signal or image from the spatial domain to the frequency domain . It has been widely used because of its good capacity of energy compression and decorrelation. Discrete Cosine Transform is faster than Discrete Fourier Transform.

3 Algorithms

3.1. Message Digest 5

MD5 is short for Message-digest Algorithm 5, developed by the MD2, MD3 and MD4. It is the length of bytes at a series of changes in the length of a large integer. MD5 algorithms are based on MD4 increasing the notion of security. Though MD5 is a little slower than MD4, it is safer. This algorithm is marked by four stages which has little different with MD4 design. In MD5 algorithms, the size and fill of information abstract is all the same with MD4. Due to the use of Md5 algorithm needn't any copyright fees, under commonlycircumstances MD5 is a very good middle technical.

3.2. Least Significant Bit

This section describes the LSB watermarking 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, on sender side it will embed the data and then on receiver side it will extract data.Encryption and decryption are the important steps in the digital watermarking

Each pixel in the image is represented by values ranging from 0-255 for each channel (RGB or HSV). The most significant bit (MSB) is the first bit to the left in representation of the value in binary while the least significant bit (LSB) is the first bit to the right. For example, the number 141 in binary is 1000 1101 We are employing the least significant bit for watermarking because if the LSB is changed, the value only changes 1 (if we change LSB of 1000 1101 to 0, the value only changes from 141 to 140), and if doesn't appear much different to our eyes.

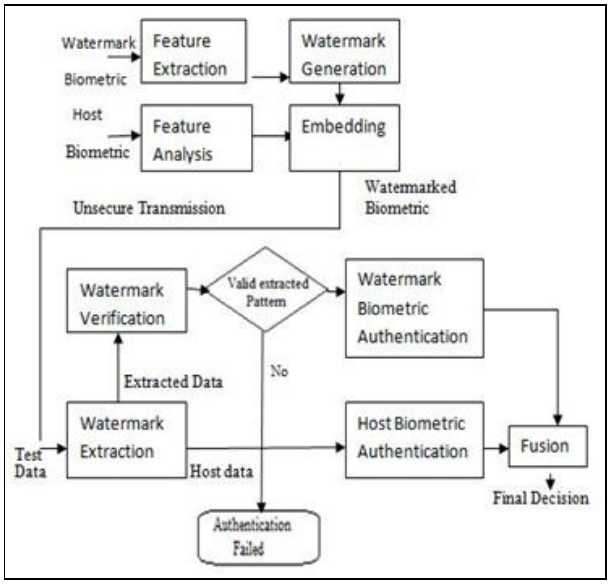

Figure 1: System Flow Diagram

To provide the authentication and security to images using MD5 and LSB watermarking with the help of multimodal authentication is proposed in system. MD5 key is generated from face image, which acts as face feature.MD5 key is embedded into fingerprint, which acts as token. Token embedded into image using LSB algorithm as watermark. In second stage of authentication face feature are authenticated. Matcher gives final decision based on the decisions given by validity of token and face feature authentication. On receiver end token is useful for biometric authentication.Secure Multimodal Authentication Using Watermarking

Here the objective is to minimize computation for face feature extraction. It also focuses on the simple manipulation for watermarking and face feature extraction. For performing this, there are various algorithms like Message Digest (MD5), Least Significant Bit (LSB) are used. Out of which MD5 produces as output a 128-bit message digest of the input.

4. Experiments

4.1. Dataset

In this system dataset used for fingerprints is FVC2002 which consists of 110 x 8 fingerprints.The dataset used for face feature is 110 × 8 FRGC2 Face database.Here face features are generated as MD5 key. MD5 key is embedded into fingerprint to generate token.Token is embedded into target image as watermark. On receiver end token is extracted from the image and validity of token is checked and finally based on the host biometric and data separated from token is used for Biometric authentication.

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

4.2. Result Set

The system implementation is done in Java using eclipse, where the user is allowed to enter face and fingerprint image for training. Query image is provided for testing . Above mentioned datasets can be used for the experiments. And results are then compared with existing systems results. The proposed methodology is used to provide the better results preventing loss of information. This section highlights the biometric authentication and watermarking results generated by system.

Face Image	Fingerprint	Target Image	Authentication (Successful or Failed)
Face1	FingPrint1	Wall1_Taj.png	Successful
Face2	FingPrint2	Wall2_Eiff.png	Successful
Face3	FingPrint3	Wall3_Butt.png	Successful
Face4	FingPrint4	Wall4_Flow.png	Successful

Table 1: Biometric Authentication Results

Above table shows that Biometric authentication result when face image and fingerprint images are provided to generate Token. This token is embedded into Target images and on receiver side decryption is done and token validity is checked and it gives successful results.

Sr. No	Image Name	Image Name	PSNR
1	Wall1_TajMsg.png	Wall1_Taj.png	44.32
2	Wall2_EiffMsg.png	Wall2_Eiff.png	44.08
3	Wall3_ButtMsg.png	Wall3_Butt.png	43.84
4	Wall4_FlowMsg.png	Wall4_Flow.png	42.10

Table 2: PSNR values of images.

Above table shows that PSNR values of two images In case of PSNR as we goes on increasing size of data for Embedding PSNR value decreases.
Above table shows that Biometric authentication result when face image and fingerprint images are provided to generate Token. This token is embedded into Target images and on receiver side decryption is done and token validity is checked and it gives successful results.

5. Conclusion

The proposed watermarking based multimodal authentication system is used to enhance biometric security. It is appropriate for any biometric data, and the multimodal strategy can be modified flexibly according to the practical requirements. The employment of face detection and nearest neighbour classifier offers a novel perspective of combining powerful pattern recognition tools with watermarking as promising intersections. Meanwhile, the proposed MD5 and LSB watermarking 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 cyber forensic etc.

6. References

1. Bin Ma, Chunlei Li, Yunhong Wang, Zhaoxiang Zhang and Di Huang "Enhancing Biometric Security with Wavelet QuantizationWatermarking based Two-stage Multimodal Authentication" 2416-2419 ICPR November 11-15, 2012
2. Wang Xijin, Fan Linxiu "The Application Research of MD5 Encryption Algorithm in DCT Digital Watermarking" ScieVerse ScienceDirect Physics Physics Procedia 25 (2012) 1264 – 1269
3. 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.
4. A. K. Jain, K. Nandakumar, and A. Nagar. "Biometric template security" EURASIP Signal Processing, 2008.
5. A. K. Jain and U. Uludag. "Hiding biometric data" Trans. Pattern Anal. Mach. Intell., 25(11):1494 – 1498.
6. T. Y. Jea and V. Govindaraju. "A minutia-based partial fingerprint recognition system" Pattern Recognition, 38:1672–1684, 2005.
7. Abdullah Bamatraf, Rosziati Ibrahim, Mohd. Najib B. Mohd Salleh "Digital Watermarking Algorithm Using LSB" 2010 International Conference on Computer Applications and Industrial Electronics (ICCAIE 2010), December 5-7, 2010, Kuala Lumpur, Malaysia
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."Key point Detection and local feature matching for textured 3d fac 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" Multimedia Tools Appl DOI 10.1007/s11042-013-1372-5 Springer 22 February 2013
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. B. Klare and A. Jain. "On a taxonomy of facial features" In Proc. BTAS, pages 1–8, 2010.
16. Li C, Wang Y, Ma B, Zhang Z (2012) "Multi-block dependency based fragile watermarking scheme for fingerprint images protection" Multimedia Tools Appl. doi:10.1007/s11042-011-0974-z
17. 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
18. Hämmerle-Uhl J, Raab K, UhlA(2011) "Watermarking as a means to enhance biometric systems: a critical surve" In: Information hiding. Springer, pp 238–254
19. W. Kim and H. Lee. "Multimodal biometric image watermarking using two-stage integrity verification" Signal Processing, 89(12):2385– 2399, 2009