Digital Watermarking based Secure Multimodal Biometric System*

Mayank Vatsa, Richa Singh, P. Mitra
Department of Computer Science & Engineering
Indian Institute of Technology
Kanpur, INDIA
mayank_richa@yahoo.com,
pmitra@iitk.ac.in

Afzel Noore
Lane Department of Computer Science & Electrical Engineering
West Virginia University, Morgantown, USA
afzel.noore@mail.wvu.edu

Abstract - *This paper presents a multimodal biometrics system using watermarking algorithms with two levels of security for simultaneously verifying an individual and protecting the biometric template. Iris template is watermarked in face, such that the face is visible for verification and the watermarked iris is used to cross authenticate the individual and secure the biometrics data as well. The accuracy of the multimodal biometrics system is around 96.8%. This system is also resistant to common attacks on biometric templates.*

Keywords: Watermarking, Multimodal Biometrics, Face, Iris, Radial Basis Function.

1 Introduction

In recent years there has been an explosive growth of business-to-customer activities over the Internet. The total value of these web-based transactions is over several billion dollars. At present, buyers are authenticated by service providers using a combination of user ID and password. The critical information about the transaction, such as the credit card number and amount, are sent over the web using secure encryption methods. However, current systems are not capable of assuring that the transaction was initiated by the rightful owner of the credit card. As Internet revenues grow, credit card owners and credit card issuers are likely to be increasingly concerned with the reliability and security of transactions.

To solve this problem, biometric techniques offer reliable methods for personal verification; but the problem of security and integrity of the biometrics data poses new problems. If a person's biometric data is stolen, it is not possible to replace it as in the case of a stolen credit card, ID or password. In order to promote the wide spread utilization of biometric techniques, an increase in the security level of biometric data is necessary [1]. Encryption and watermarking are among the possible techniques to achieve this, but encryption does not provide security once the data is decrypted. Watermarking involves embedding information into the host data to provide greater security. Since embedding the watermark may change the inherent characteristics of the host image, verification performance based on (decoded) watermarked images should not be inferior to the original non-watermarked images.

Recent work has been undertaken on watermarking of fingerprint images [3, 4]. Fingerprint images or minutiae (distinguishing characteristics of fingerprint images) are hidden in images. Jain et al. [6] have proposed an effective way of hiding Eigen faces in fingerprint images. These are the only works on biometric data hiding and these involve the use face and fingerprint images.

In this paper, two levels of security are proposed for simultaneously verifying any individual and protecting the biometric template. One biometrics template i.e. iris is watermarked in face, such that the face is visible for verification and the watermarked iris is used to cross authenticate the individual and secure the biometrics data (face) as well. For generating the watermark data i.e. iris template, an algorithm based on 1D log Gabor is used. 1D log Gabor is convolved with the transformed texture image of iris and thus the template is generated. This template called as iriscode is in the binary form and is unique for every individual. It is now embedded into the face image of the same individual to protect the face template as well as perform the multimodal operation. For watermarking, two algorithms namely Modified Correlation based algorithm and Modified 2D Discrete Cosine Transform based algorithm are presented.

2 Choice of Watermark Object

The first question we need to ask with any watermarking based multimodal biometric system, is what form will the embedded watermark take and which biometric template should be used as the watermark? Previous work on hiding face in fingerprint images [6] and hiding fingerprint minutiae in an image [3, 4] are designed to hide the extracted features of the watermark image. These algorithms allow an image to carry information in the form of features. The drawback however with these approaches is that by compressing the watermark-object before insertion, robustness suffers. So rather than using feature characters as watermark, we propose using the binary image as watermark.

* 0-7803-8566-7/04/$20.00 © 2004 IEEE.

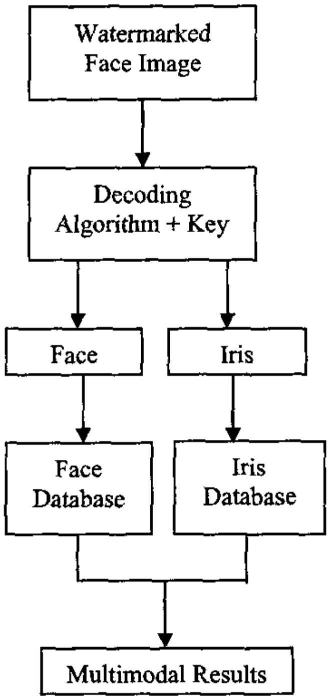

Figure 1. Flow Diagram of the Secure Multimodal Biometric System

In our study we found that only iris template generated using wavelet filters are capable of resisting the watermarking attacks as well as protecting the biometric template. Iris template generated from 1D log Gabor filter is in binary form and is unique to every individual. Minor changes in the bit pattern of iris template do not affect the overall matching performance and hence is a good choice.

3 Watermarking Algorithm

In general, a digital watermark is a code that is embedded inside an image. It acts as a digital signature, giving the image a sense of ownership or authenticity. Ideal properties of a digital watermark have been stated in many articles and papers [1-3]. These properties include:

1. A digital watermark should be perceptually invisible to prevent obstruction of the original image.
2. A digital watermark should be statistically invisible so that it cannot be detected or erased.
3. Watermark extraction should be fairly simple; otherwise the detection process requires too much time computation.
4. Watermark detection should be accurate. False positives, the detection of a non-marked image, and false negatives, non-detection of a marked image, should be few.
5. Watermark detection should be accurate. False positives, the detection of a non-marked image, and false negatives, non-detection of a marked image, should be few.
6. Watermarks should be robust to filtering, additive noise, compression and other forms of image manipulation.
7. The watermark should be able to determine the true owner of the image.

Two additional factors relating to capacity and speed are of major concern in securing the biometrics template in a multimodal biometric system. A watermarking system must allow for a sufficient amount of information to be embedded into the image. This can range from a single bit all the way up to an N x N image. Furthermore, in watermarking systems designed for embedded applications, watermark detection or embedding should not be overly computationally intensive so as to preclude its use in multimodal biometric systems. Based on the properties of watermarking algorithm and according to the need of securing multimodal biometrics system, we have chosen two watermarking algorithms:

1. Modified Correlation, and
2. Modified 2D Discrete Cosine Transform

It has also been stated in the literature [5] that these two algorithms are resistant to most of the watermarking attacks.

3.1 Modified Correlation based algorithm (MCBA)

For watermark embedding, correlation properties of additive pseudo-random noise patterns as applied to an image are used [2]. An iris code W(x, y) is added to the cover image I(x, y), according to Equation (1)

$$I_w(x,y) = I(x,y) + k * W(x,y) \tag{1}$$

where k denotes the gain factor and I_W is the resulting watermarked image. Increase in k increases the robustness of watermark at the expense of quality of the watermarked image. To retrieve the watermark, the iriscode is seeded with the same key and the correlation between the noise pattern and the possibly watermarked image is computed. If the correlation exceeds a certain threshold T, the watermark is detected and a single bit is set. This method is easily extended to a multiple-bit watermark by dividing the image into blocks and performing the above procedure independently on each block. The algorithm is modified by pre-filtering the image before applying the watermark, and then increasing the higher resulting correlation. This increases the probability of correct detection even after the

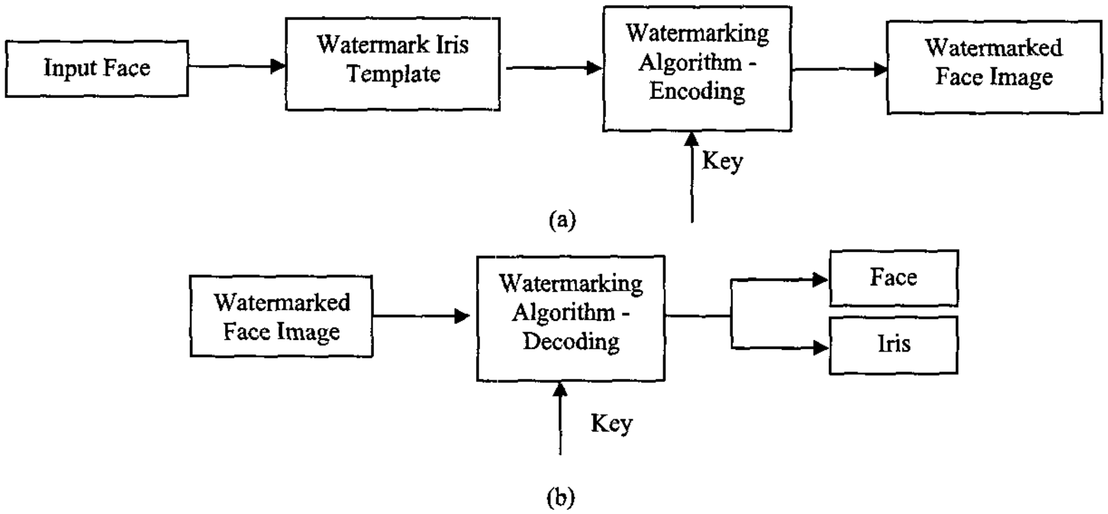

Figure 2 (a) Watermark Encoding, (b) Watermark Decoding

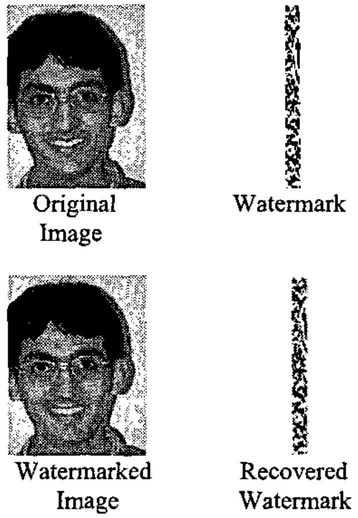

Figure 3. MCBA Watermark Embedding and Decoding

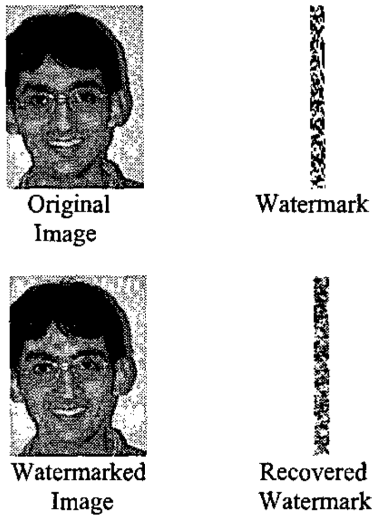

Figure 4. M2DCT Watermark Embedding and Decoding

image has been subjected to attack (addition of Gaussian Noise – 5% and filtering). Figure 3 shows the original face image, watermark iris template, the watermarked face image and the recovered iris template obtained after decoding.

3.2 Modified 2D Discrete Cosine Transform based algorithm (M2DCT)

The Discrete Cosine Transform (DCT) is a real domain transform, which represents the entire image as coefficients of different frequencies of cosines. DCT of the image is calculated by taking 8 X 8 blocks of the image and each block is then individually transformed. The 2D – DCT of an image gives the result matrix such that top left corner represents the lowest frequency coefficient while the bottom right corner is the highest frequency.

The DCT approaches for watermarking [7, 8] are able to withstand some forms of attack very well such as low-pass filtering, high-pass filtering and median filtering. This algorithm has been modified by using the fundamentals of Differential Energy Watermarking. Figure 4 shows the original face image, watermark iris template, watermarked face image and recovered watermark from the algorithm.

4 Multimodal Biometrics

The multimodal biometrics algorithm consists of iris template generation and recognition, face recognition and fusion algorithm. For face recognition, the well known Principal Component Analysis (PCA) [9] based face recognition algorithm has been implemented. To test the accuracy of the watermarking algorithm face recognition is performed on the original face image, watermarked face image and face image after decoding process. For generating the iris code from the iris image, 1D log Gabor based iris template generation algorithm is used. Iris detection is performed using the algorithm described in [12]. From the output of iris detection i.e., iris texture features are extracted using the algorithm based on 1D log Gabor [10]. These features are encoded into bit patterns called the Iriscode. For generating the iris template, 2D normalized pattern is transformed into a number of 1D signals and convolved with the 1D log Gabor wavelets. This iris code is the textural representation of the features of iris in binary form of size 10x100. Bit shifting based Hamming distance matching algorithm [11] is used for iris code matching and obtaining the results of iris recognition.

Similarly for face recognition, the decoded iris templates are also matched using the hamming distance algorithm to check the robustness of watermarking algorithms. The iriscode is matched before embedding in the face image and then compared after decoding from the face image.

Finally, the multimodal biometrics is implemented on the watermarked face images and the decoded iris templates using Radial Basis Function (RBF) [14] for decision making. RBF networks are used for fusion because of the less training time required and the possibility of learning positive as well as negative samples. Also the experimental results of [13] show that RBF network gives the highest accuracy compared to any other fusion algorithms. Face and iris gives their respective matching results based on their matching algorithms [9] and [11]. These matching results are then fused using the three-layered RBF network. The output of the network is the either 0 or 1 where 0 stands for mismatch and 1 stands for match using both the face and iris.

5 Experimental Results

An image database of 100 individuals was created to test the proposed secure and multimodal biometrics system. This database consists of five face images and five iris images per individual. Two face images and two iris images are used as the training set and rest of the images are used for testing.

Before watermarking, the accuracy of face recognition (using PCA) is 92.16% on frontal faces and it remains the same after watermarking. The accuracy of iris recognition (using 1D log Gabor) before embedding is 98.18% and after decoding around 94.5% using both the watermarking algorithm, which drops for the False Rejection Rate, while the False Acceptance Rate remains the same.

In MCBA watermarking algorithm the accuracy of face recognition and iris recognition is 92.16% (after watermarking) and 94.54% (after decoding) respectively. In M2DCT watermarking algorithm, the accuracy of face recognition and iris recognition is 92.16% (after watermarking) and 94.40% (after decoding) respectively. The two watermarking algorithms are also tested for common watermarking attacks such as filtering, noise addition, and JPEG compression. Both the algorithms are capable of resisting these attacks and there is no major change in the recognition accuracy of face and iris.

An accuracy of 96.85% was achieved for MCBA watermarking based multimodal biometrics system with enhanced data security. For M2DCT watermarking based multimodal biometrics system, 96.80% accuracy was achieved.

6 Conclusion

This paper presented the two levels of security for simultaneously verifying an individual and protecting the biometric template using the two watermarking algorithms. The iris biometrics template is watermarked in face such that the face is visible for verification and the watermarked iris is used for cross authentication and protecting the biometrics data. For watermarking, two algorithms based on Modified Correlation and Modified 2D Discrete Cosine Transform are used. The multimodal biometrics fusion algorithm is based on RBF network and the result of the multimodal system with MCBA is found to be 96.85% accurate and with M2DCT it is found to be 96.80% accurate. Both the watermarking algorithms are also found to be resistant to the common attacks.

References

[1]. R. M. Bolle, J. H. Connell, S. Pankanti, N. K. Ratha, A. W. Senior, "Guide to Biometrics", Springer Verlag, 2004.

[2]. G. Langelaar, I. Setyawan, R. L. Lagendijk, "Watermarking Digital Image and Video Data", IEEE Signal Processing Magazine, Vol. 17, pp 20-43, 2000.

[3]. A. K. Jain and U. Uludag, "Hiding Fingerprint Minutiae in Images", Proceedings of Third Workshop on Automatic Identification Advanced Technologies, pp. 97-102, 2002.

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

[5]. Peter Meerwald, Digital watermarking in the Wavelet Transform Domain, Master's Thesis, University of Salzburg, Austria, January 2001.

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

[7]. R. B. Wolfgang, C. I. Podilchuk, and E. J. Delp, "Perceptual Watermarks for Digital Images and Video", Proceedings of IEEE, Vol. 87, No. 7, pp. 1108-1126, 1999.

[8]. M. Barni, F. Bartolini, V. Cappellini and A. Piva, "A DCT Domain System for Robust Image Watermarking", Signal Processing, Vol. 66, No. 3, 1998, pp. 357-372.

[9]. M. Turk and A. Pentland, "Eigenfaces for Recognition", Journal of Cognitive Neuroscience, Vol. 3, No. 1, 1991.

[10]. J. Bigun and J. M. du Buf, "N-folded symmetries by complex moments in Gabor space and their applications to unsupervised texture segmentation", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 16, No. 1, 1994, pp. 80-87.

[11]. J. Daugman, "High confidence visual recognition of persons by a test of statistical independence", IEEE Transactions on Pattern Analysis and Machine Intelligence, Vol. 15, No. 11, 1993, pp. 1148–1161.

[12]. P. Richard Wildes, "Iris Recognition: An Emerging Biometric Technology, Proceedings of IEEE, Vol. 85, No. 9, 1999, pp. 1348-1363.

[13]. J. Kittler, M. Hatef, R. P. W. Duin, and J. Mates, "On combining classifiers", IEEE Transactions on Pattern Analysis and Machine Intelligence, 1998, Vol. 20, No.3, pp. 226–239.

[14]. S. Haykins, "Neural Networks: A Comprehensive Foundation", Second Edition, Pearson Education, 2002.