SECURE IRIS VERIFICATION

Shenglin Yang[1] and Ingrid Verbauwhede[1,2]

[1]Department of Electrical Engineering, UCLA, Los Angeles, CA 90095 and [2]K.U.Leuven, Belgium

ABSTRACT

In this paper, we present a novel secure iris verification system, where a transformed version of the iris template instead of the plain reference is stored for protecting the sensitive biometric data. An Error Correcting Code (ECC) technique is adopted to perform the comparison in the transformed domain. A two-segment method is proposed to execute the feature verification, where a Bose-Chaudhuri-Hochquenghem (BCH) code of a random bit-stream is introduced to eliminate the considerable differences between the features extracted from different scans of irises. A reliable bits selection process during the iris feature generation stage reduces the system error rate from 6.0% to 0.8%. The appropriate size of the set of reliable bits is determined by investigating the best match between the associated error correct cutting edge and the actual verification accuracy.

Index Terms— iris, personal verification, data security

1. INTRODUCTION

Biometric verification provides authentication of a person based on the unique characteristics possessed by the individual. Biometric systems have been developed based on various features, such as fingerprint, facial image, voice, hand geometry, handwriting, iris, and retina. Among them iris is considered as one of the most reliable and accurate candidates because, first, iris forms during gestation and remains the same for the rest of one's life and it is unique for individuals; second, it is well protected and extremely difficult to be modified.

Generally the biometric verification is based on the comparison between the features extracted from the input and the template. Due to the uniqueness of the biometric characteristics, the storage of the reference template is a key factor for the entire system security. Therefore it is essential to protect the template from possible attacks. One approach is to encrypt the template using a secret key before storing it. When a verification task is requested, the matcher decrypts the template and performs the comparison. However, some dedicated attacks still can extract the secret key during the decryption procedure, and in turn, the template by tracking the information revealed by the physical implementation. An example is Side Channel Attacks (SCA) [1]. A clean solution to this problem is to store a noninvertible transformed version, for instance a hash, of the template on an embedded device, and the comparison is performed in the transformed space. However, the main property of a cryptographic random hash function is that the output hash value will not give any information about even part of the input [2]. Therefore, the similarity in the input will not reflect in the output hash value. Unfortunately, for most biometrics the exactness for different captures is not available, and match algorithms are normally based on the similarity. In order to address this issue, we adopt the idea of the template protection scheme to conduct the iris authentication by integrating the biometrics with modern cryptographic techniques [3].

2. RELATED WORK

Beginning from 1987, automatic iris recognition systems have been proposed. In [4], Daugman developed an iris recognition system using 2D Gabor filter for feature extraction and hamming distance for verification. It became the basis for most of the current commercial iris verification products. Besides Daugman's method, various approaches for feature extraction have been studied. Wildes' algorithm used the first derivative of Laplacian of Gaussian filters to locate the iris in eye-contained images [5]. Boashash and Boles proposed a new approach based on zero-crossings, which can handle noise in the image data and also is invariant to image translation and rotation [6]. Li Ma, et al. used circular symmetry filters to capture the local texture information of the iris and construct a fixed length feature vector [7].

As mentioned before, the main challenge for embedded biometric authentication is to provide a secure storage for the reference template. Embedded devices are especially vulnerable to eavesdropping and attacks. Thus alternative protection mechanisms need to be investigated. Recently, a novel cryptographic technique called a fuzzy commitment scheme was proposed [8][9]. This scheme integrates the well-known BCH error-control coding method to construct the cryptographic system. Instead of an exact, unique decryption key, a reasonable close witness can be accepted to decrypt the commitment. This characteristic makes it possible for protecting the biometric data using traditional cryptographic techniques. Following this direction, Clancy et al. [10] employed the fuzzy vault scheme on a secure smart card system, where the fingerprint authentication is used to protect the private key. Yang, et al. [11] further addressed the alignment issue in a systematic way to make the fuzzy vault based fingerprint authentication system automatic and adaptive. In [12], Linnartz, et al. precisely formulated the requirements for protecting biometric authentication systems, and also presented a general algorithm that met the requirements. The feasibility of template-protected biometric authentication systems was further demonstrated with a fingerprint recognition system [3]. In this paper, we adopt the idea of Tuyls, et al. and propose an algorithm for the template protection of an authentication system based on iris.

The paper is organized as following: Section 3 presents the algorithm of the feature coding for iris verification; Section 4 shows the implementation of the proposed secure matching

strategy. The results and discussion are presented in section 5, with the conclusions following in section 6.

3. IMAGE PROCESSING ALGORITHM FOR IRIS FEATURE EXTRACTION

Like most other biometric authentication systems, the input eye-contained images need to be processed so that the characteristic iris features can be extracted for comparison. Shown in the following is the block diagram of the iris process algorithm implemented in the proposed system. Algorithms are derived from [15].

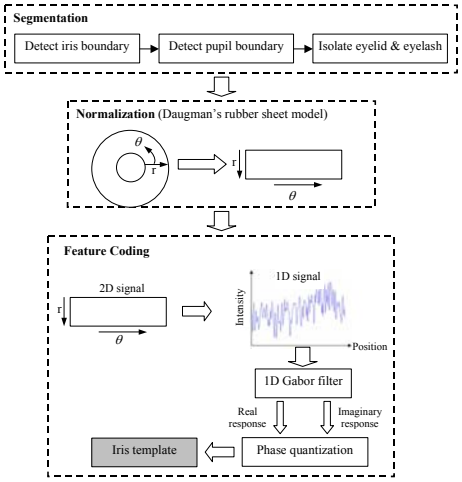


Fig.1. Block diagram for iris feature extraction

As shown in Fig.1, the iris image processing consists of three phases: segmentation, normalization, and feature encoding, which are discussed individually below:

1) Segmentation: The first step of the image process algorithm is to extract the iris from the input eye-contained image. For approximation, the iris area is considered as a circular region between two circles. After the boundaries of both the outer and inner circles are defined, the iris region is then located. The circular Hough Transform is adopted in this work to search for the boundaries. Eyelids are detected by fitting two lines using the linear Hough Transform, and eyelash is isolated by a simple threshold technique.

2) Normalization: In order to perform comparison between irises, the segmented iris region needs to be aligned to a fixed size. Normalization is performed using Daugman's rubber sheet model [13], where the circular region is mapped to a rectangular as shown in Fig.1. During the normalization, the center of the pupil is considered as the reference point, while the radial vectors circle through the iris region.

3) Feature encoding: Feature encoding is implemented by first breaking the two-dimensional normalized iris pattern into a one-dimensional signal and then convolving it with a Log-Gabor wavelet. The resulting phase information for both the real and the imaginary response is quantized, generating a bitwise template. In this work, the angular and radial resolutions are set as 240 and 20 pixels, respectively. Two bits are used to represent the quantized phase information for each pixel. Therefore, the total size of the iris template is 9600 bits.

4. TEMPLATE-PROTECTED IRIS MATCHING

For existing iris verification systems, common approaches used to perform feature matching are based on hamming distance, weighted Euclidean distance, or normalized correlation. Hamming distance is the most widely chosen metric due to its simplicity and efficiency. However, this approach requires direct on-device storage of the iris feature template, which leads to security problems as mentioned in section 1. In order to address this issue, we propose a template-protected matching scheme for iris verification.

The main idea of the template-protected scheme is to generate a non-invertible form of the iris feature. The overall diagram of this scheme is illustrated in Fig.2. During the enrollment phase, the iris feature is extracted as a bit array. At the same time a random bit-stream (S) is generated and coded by the error correct coding technique, forming a BCH code (C), which is then xored with the extracted feature to generate a secret (W). In the meanwhile the random bit stream (S) goes through a one-way hash function. Both the secret (W) and the hashed value of the BCH code are stored on the embedded device. During the verification phase, an input iris feature is extracted, which can be considered as a noisy version of the iris template from the enrollment phase. The stored secret (W) is output from the embedded storage, and together with the input iris feature, a noisy version of the error correct code (C') is generated and then put through the decode block. The decoded value is hashed using the same function used in the enrollment phase, and the comparison is then performed between the two hash values. If they are matched, an access is granted, otherwise, the verification fails.

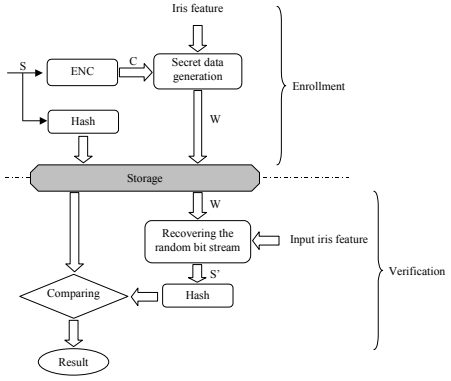


Fig. 2. Template-protected iris matching algorithm

The encode block (ENC) and the hash block (Hash) are implemented straightforwardly. Several special strategies for the feature coding are explained below, followed by the discussion of the detailed procedures of the template-protected algorithm.

4.1. Reliable bits selection

As mentioned in the feature encoding procedure, the total size of the iris template is 9600 bits. However, among them a considerable number of bits are affected by noise information such as eyelash

and eyelid. Therefore, the reliable bits selection step is implemented to make sure that the bits chosen for authentication are relatively stable for different scans of the iris input. Usually the eyelid and eyelash affect the feature extracted from the outer part of the circular region. So when selecting reliable bits, we want the bits associated with pixels closer to the iris center as shown in Fig. 3 in lighter colors. After applying Daugman's rubber sheet model [13] during the feature coding step, the two-dimensional signal is unwrapped to a one-dimensional signal as presented in Fig. 3, where the bits coming first are those associated with smaller radial indexes.

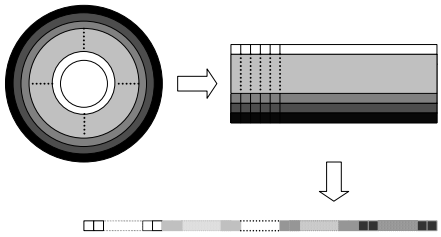


Fig.3. Signal unwrapping for iris feature coding

In this work, three iris images are taken as the templates to extract the reliable bits. The bits which are the same for all the three template irises are defined as "reliable" here. During the selection procedure, a flag (F) is set for each bit. If the bit is chosen as "reliable", the flag associated with it is set to be "1"; otherwise it is set to be "0". The number of the reliable bits varies from one case to another, but typically, there are more than 4000 reliable bits in total.

4.2. Two-segment matching strategy

For each user, a bit-stream (S) is randomly generated and ported into a binary BCH error correct encoding block described by the triplet (K,s,d), where K denotes the length of the code words, s is the number of the information symbols and d is the number of the errors that can be corrected. Since the feature vectors extracted from the irises of different persons are two independent random bit series, the hamming distance between them is around 50%, while for the features extracted from the iris of the same person, the hamming distance is usually significantly smaller. Taking advantage of this characteristic, a BCH code is constructed to verify the owner of an input iris. The most straightforward approach is to choose K reliable bits to generate the secret information (W). According to the BCH error correcting rule, the highest error rate which the system can stand is d/K. However, experimentally this is lower than the typical distinguish threshold for iris verification and can lead to a higher system failure rate.
The distinguish threshold is a hamming distance based on which the matched and mismatched iris pairs can be distinguished correctly.

In order to address this problem, a two-segment method based on a reliable bits division is proposed for the iris feature matching in this work to lift the actual error tolerance level. The detailed algorithm diagram for the two-segment template-protected iris verification is illustrated in Fig. 4.

Instead of xoring the K reliable bits and the BCH code directly, a certain number of bits are selected from the reliable bits pool and are equally divided into two sets. If the number of the

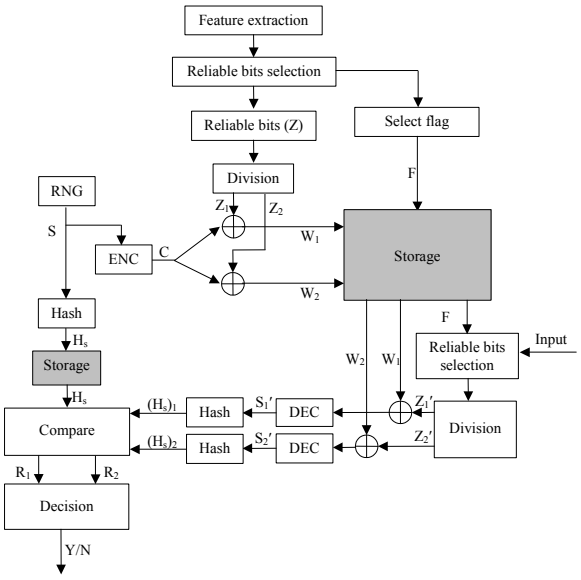


Fig. 4. Detailed algorithm diagram for the two-segment template-protected iris verification

selected reliable bits is smaller than 2×K, dummy "0" bits are added for each set to form two K-bit arrays, Z1 or Z2. Using this, two sets of secret data, W1= C⊕Z1, W2= C⊕Z2, are constructed, where C is the encrypted BCH code. The secret data, W1 and W2, and the vector of selection flags F are then stored on the embedded device. Meanwhile, the random bit-stream S is hashed and the hash value is stored too. For verification, the input iris feature is passed through the reliable bits selection procedure. The reliable bits selected based on the selection flag F are divided into two parts, Z1′ and Z2′, just as we did in the enrollment phase for the template iris. The secret data W1 and W2 are released from the storage to generate W1 ⊕ Z1′ and W2 ⊕ Z2′, which are ported into the ECC decoder to get the recovered random bit-streams, S1′ and S2′. The bit-streams are then hashed using the same hash function as used in the enrollment phase and the comparisons are performed between the two pairs of hash values. Finally, the two subsets results go through a decision-making block to achieve the final decision.

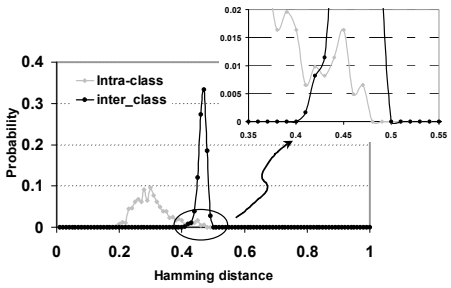
Among all the possible triplets available for the BCH codes, it is necessary to select one that is capable to distinguish irises from different persons and to achieve desirable security requirements as well. For this reason, triplet (1023, 46, 219) is adopted for the BCH code in this work. The two BCH codes are able to correct up to 219*2=438 bits errors. The desired, distinguish threshold can be achieved by choosing the appropriate size of the actual bits from iris, the valid bits in the 1023-bit array.

Since the errors only happen in the valid bits, given the valid bits size of X, the resulting error tolerant rate becomes 438/X. On the other hand, the matching accuracy can be affected by the size of the valid bits as well. The next section will discuss how the size of the optimal number of valid bits is determined experimentally.

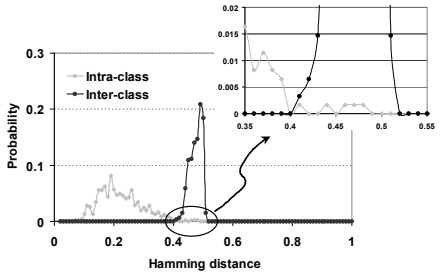
5. RESULT AND DISCUSSIONS

The secure matching algorithm using cryptographic techniques is implemented with the proposed reliable bits based scheme. The

reliable bits selection not only makes the implementation of such algorithm feasible, but also provides improved performance for the verification accuracy. This is illustrated in Fig. 5 with the distributions of the intra- and inter-class hamming distances for iris matching. The performance of conventional methods using all the iris feature bits and the proposed method based on 2500 reliable bits are shown in Fig. 5(a) and (b), respectively. The overlapping areas of the intra- and inter-class distributions are enlarged for better visibility. It can be seen that for the lowest-FAR (False Accept Rate) system, the FRR (False Reject Rate) decreases significantly from 6.0% to 0.8% by adding the reliable bits selection stage.



(a)



(b)

Fig. 5. Matching result for algorithm based on (a) all feature bits; (b) reliable feature bits

Using the two-segment matching strategy based on the error correct code (ECC), the verification threshold is determined by the size of the selected reliable bits set. In order to obtain the best verification performance, different sizes of the reliable bits are investigated to check how well the associated error correct rate fits the match-mismatch iris feature cutting edge. Experimentally, the best performance is achieved by selecting 1096 as size of the reliable bits set with a corresponding verification threshold of 40%.

6. CONCLUSIONS

We present a template-protected secure iris verification system based on the ECC cryptographic technique with the reliable bits selection to improve the verification accuracy. The two-segment strategy is proposed to balance the desired verification accuracy and the error correct capability of the BCH code. The dependence of the matching accuracy on the reliable bits size is investigated to achieve the best performance. The optimal size of the reliable bits is found to be around 1096, which results in an FRR and FAA of 0.8% and 0.0%, respectively.

7. ACKNOWLEDGEMENTS

The authors would like to acknowledge the funding of NSF accounts CCR-0310527 and CCR-0541472, and UC MICRO. Portions of the research in this paper use the CASIA iris image database collected by the Institute of Automation of the Chinese Academy of Sciences [14].

8. REFERENCES

[1] Tiri, K. and Verbauwhede, I., "A Logic Level Design Methodology for a Secure DPA Resistant ASIC or FPGA Implementation," *Design, Automation and Test in Europe Conf.*, pp. 246-51, 2004, Paris, France.

[2] Anderson, R. J., *Security Engineering: A Guide to Building Dependable Distributed Systems*, John Wiley & Sons, 2001.

[3] Tuyls, P., Akkermans, A. H. M., Kevenaar, T. A. M., Schrijen, G-J., Bazen, A. M., and Veldhuis, R. N. J., "Practical Biometric Authentication with Template Protection," *5th Int. Conf. on Audio- and Video-Based Personal Authentication*, pp. 436-41, 2005, Rye Brook, NY, Springer-Verlag Berlin LNCS 3546.

[4] Daugman, J. G., "High Confidence Visual Recognition of Persons by a Test of Statistical Independence," *IEEE Trans. Pattern Anal. Machine Intell.*, vol. 15, pp. 1148-61, Nov. 1993.

[5] Wildes, R., Asmuth, J., Green, G., Hsu, S., Kolczynski, R., Matey, J., and McBride, S., "A System for Automated Iris Recognition," *Proc. IEEE Workshop on Applications of Computer Vision*, pp. 121-8, 1994, Sarasota, FL.

[6] Boles, W. W. and Boashash, B., "A Human Identification Technique Using Images of the Iris and Wavelet Transform," *IEEE Trans. on Signal Processing*, vol. 46, pp. 1185-8, 1998.

[7] Ma, L., Wang, Y., and Tan, T., "Iris Recognition Using Circular Symmetric Filters," *Proc. 16th Int. Conf. on Pattern Recognition*, vol. 2, pp. 414-7, 2001, Los Alamitos, CA.

[8] Juels, A. and Sudan, M., "A Fuzzy Vault Scheme," *Proc. IEEE Int. Symposium on Information Theory*, pp. 408-13, 2002, Piscataway, NJ.

[9] Juels, A. and Wattenberg, M., "A Fuzzy Commitment Scheme," *6th ACM Conf. on Computer and Communications Security*, pp. 28-36, 1999, New York, NY.

[10] Clancy, T.C., Kiyavash, N., and Lin, D.J., "Secure Smartcard-based Fingerprint Authentication," *ACM Workshop on Biometrics: Methods and Applications*, pp. 45-52, 2003, Berkeley, CA.

[11] Yang, S. and Verbauwhede, I., "Automatic Secure Fingerprint Verification System Based on Fuzzy Vault Scheme," *IEEE Int. Conf. on Acoustics, Speech, and Signal Processing*, pp. 609-12, 2005, Philadelphia, PA.

[12] Linnartz, J-P. and Tuyls, P., "New Shielding Functions to Enhance Privacy and Prevent Misuse of Biometric Templates," *4th Int. Conf. on Audio- and Video-Based Personal Authentication*, pp. 393-402, 2003, Guildford, U.K., Springer Verlag LNCS 2688.

[13] Daugman, J. G., "How Iris Recognition Works," *Proc. 2002 Int. Conf. on Image Processing*, vol.1, pp. I-33-6, 2002, Piscataway, NJ.

[14] CASIA Iris Image Database, http://www.sinobiometrics.com.

[15] Masek, L., "Recognition of Human Iris Patterns for Biometric Identification", *BE Dissertation*, University of Western Australia, 2003, www.csse.uwa.edu.au/~pk/studentprojects/libor/index.htm.