Secure multibiometric cryptosystems Using biohashing

P.SANGEETHA,
M.E VLSI Design,
Srinivasan Engineering College,
Perambalur.
sangece2@gmail.com

Mrs.B.REVATHY,
Associate Professor,
Department of ECE,
Srinivasan Engineering College,
Perambalur.
brevathysekar@gmail.com

Abstract-Multi biometric systems are being used in many large scales biometric applications (e.g., FBIIAFIS, UIDAI system in India). They have several advantages such as lower error rates and larger population coverage compared to uni biometric systems. It requires storage of multiple biometric templates (e.g., fingerprint, iris, and face) for each user; it leads to increased risk to user privacy and system security. The method to protect individual templates is to store only the secure sketch generated from the corresponding template using a hybrid biometric system. But this also requires the storage of multiple sketches. In this project a feature level fusion framework is proposed to simultaneously protect multiple templates of a single user as a single secure sketch. The feasibility of feature level fusion framework has been demonstrated using both fuzzy vault and Biohashing algorithm. This serves as a hybrid biometric cryptosystem thus combining the advantages of both template transformation and cryptosystem.

Index Terms—Multi biometrics, template security, biometric cryptosystem, fuzzy vault, fusion, biohashing.

I.INTRODUCTION

The term biometrics is defined as “automated recognition of individuals based on their behavioral and biological characteristics”. The sudden growth in the use of Internet applications and the great concern of security require a reliable personal identification system. Traditional automatic personal identification schemes can be divided into two categories: knowledge-based, such as a password and token-based, such as a physical key, an ID card and a passport. However, these approaches have many limitations. In the knowledge-based biometric approach, the “knowledge” can be guessed, forgotten or can be shared. In the token-based biometric approach, the “token” can be easily stolen or lost. These things strongly indicate that we need a more effective and reliable solution for human identity management. Biometrics is regarded as the potential solution. Biometric authentication refers to the technology for personal identification or authentication based on our physiological and/or behavioral characteristics. Biometrics can be divided into two types. Unimodal and multimodal. Many unimodal biometrics system suffer from limitations such as inability to tolerate deformed data due to noise, deformed data from the sensor device, distorted signal from environmental noise and variability of an individual’s physical appearance and pattern over time. Multimodal biometrics are able to solve some of these limitations by combining information from multiple biometric sources. eg fingerprint, face and iris etc. But storage requirements, processing time and computational demands of a multimodal biometric system can be higher than that of unimodel system.The design of a biometric system consists of five objectives : cost, user acceptance and environment constraints, accuracy, computation speed and security. Reducing accuracy can increase speed. Reducing user acceptance can improve accuracy. Increasing cost can enhance security. A practical biometric system should balance all the five objectives.

It is generally conceded that a substitute to biometrics for positive identification in integrated security applications is not used present. While the industry has long claimed that one of the primary benefits of biometric templates is that original biometric signals acquired to enroll a data subject cannot be reconstructed from stored templates, several approaches have proven this claim incorrect. Since biometric characteristics are largely unchangeable, a compromise of biometric templates results in permanent loss of a subject’s biometrics. Do not support the standard encryption algorithm for a comparison of biometric templates in encrypted domain and, thus, leave biometric templates exposed during every authentication attempt. Multibiometric systems accumulate evidence from more than one biometric template (e.g., iris and face, fingerprint) in order to recognize a person Compared to unibiometric systems that rely on a single biometric template, multibiometric systems can provide higher recognition system and maximum population coverage. Consequently, multibiometric systems are being widely adopted in many large-scale identification systems, including FBI’s IAFIS, Department of Homeland Security’s US-VISIT, and Government of India’s UID. Here the numbers of software and hardware multibiometric products have also been introduced by biometric vendors.

a. Iris b. face c. fingerprint

Figure.1Examples of biometric characteristics

.An ideal biometric template protection scheme should satisfy the following four properties.

Diversity: By avoiding the cross matching of database in secure template, thereby ensuring the user’s privacy.

Revocability: it is easy to revoke a compromised template and reissue a new one based on the same biometric data.

Security: To encover the original template from the secure template is difficult to find..This property prevents an adversary from creating a physical spoof of the biometric trait from a stolen template.

Performance: the biometric template protection scheme should not degrade the recognition performance (FAR and FRR) of the biometric system.

(Karthik Nandakumar and Anil K. Jain,2008) This paper is achieved by generating a single multibiometric template using feature level fusion and securing the multibiometric template using the fuzzy vault construct .And also implemented a fully automatic fuzzy vault system for securing the fingerprint minutiae and iris code templates. A salting transformation based on a transformation key is used to indirectly convert the fixed-length binary vector representation of iris code into an unordered set representation that can be secured using the fuzzy vault.

(E.J.C. Kelkboom, X. Zhou, J. Breebaart, R.N.J. Veldhuis, C. Busch) it is possible to apply fusion with the Helper-Data System at feature-, score-, and decision level. However, the Helper-Data System inherently has only a decision as the output; hence it had to be adapted in order to have a score as output for the score-level fusion. We took the number of the bits the ECC had to correct as the distance score measurement. The performance at all fusion levels is significantly better than the performance of the individual biometric sources.

(Y. Sutcu, Q. Li, and N. Memon ,2009)In this paper, study the fusion of fingerprint and face biometrics in the feature level, and the construction of secure templates that would not give attackers much advantage even when they are compromised. Geometric transformation for fingerprint minutiae is used to transform the minutiae sets to feature vectors of fixed lengths. Face feature extraction algorithm that makes use of SVD values of the face images, which is also of fixed lengths. In this way, the features for both modalities would have the same representations that make fusion at feature level much easier another important open problem is how to determine the exact information leakage due to the sketch.

II.MULTIBIOMETRIC CRYPTO SYSTEMS

A. Feature extraction:

Fingerprint:

The fingerprint is basically the combination of valleys and ridges on the surface of the finger. The steps involved in fingerprint recognition using minutiae matching approach after image acquisition are Image enhancement, Minutiae extraction as shown in figure1. Once a high-quality image is captured, there are a several steps required to convert its distinctive features into a compact template. This process is known as feature extraction.

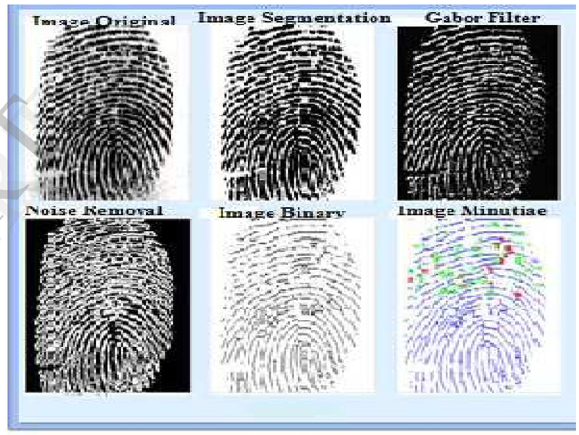


Figure.2.fingerprintfeatureextraction

The features extraction process is completed by the use of 2D Gabor wavelets to perform a multiscale analysis of the iris. The regions of the image are analyzed at different scales by frequency-selective filters. Thus the information about local phase, coded with two bits corresponding to the signs of the real and imaginary parts, is obtained. The result is a 256-byte code, which represents a specific iris and is called Iriscode.

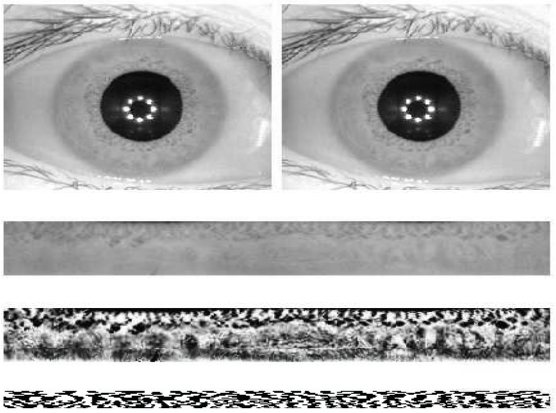
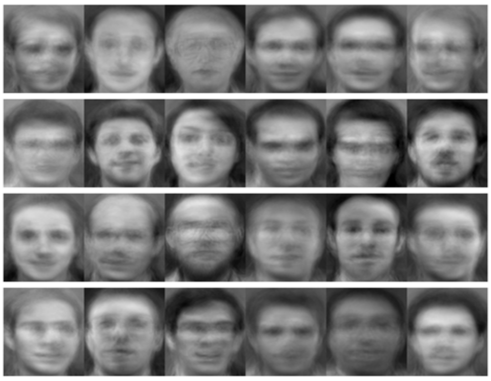


Figure. 3. Common processing chain in iris recognition: (a) image of eye (b) detection of pupil and iris (c) unrolled iris texture (d) preprocessed iris texture (e) sample iris-code.



Face

Figure.4.samples of eigenfaces

Principal Components Analysis commonly referred to as the use of eigenfaces. With PCA, the testing images must be the same size and must first be normalized to line up the eyes and mouth of the subjects within the images. The PCA approach is then used to reduce the dimension of the data by means of data compression basics and reveals the most effective low dimensional structure of facial patterns. This process of reduction in dimensions removes redundant information that is not useful and precisely decomposes the face structure into orthogonal (uncorrelated) components which known as eigenfaces or eigenimage. Eigenface is refer as standardized human face ingredient, every face image can be constructed by set combinations of the eigenfaces, Any human face can be considered to be a combination of these standard faces.

B.Fusion

But fusion of fingerprint, iris and face will give better result comparing to others. There are four levels of information fusion. Feature level fusion, score level fusion, pixel level fusion, and decision level fusion. Any biometric system is capable of producing matching scores for input user with those in the database. The set of all possible user identities can be ranked by sorting the matching scores in the descending order. Thus a biometric system can identify an unknown user by generating ranks, i.e., integer number for each of the user identity. In fingerprint, palmprint and hand geometry are fused using score level. Individual match score of the three modalities are were combined using sum rule. In decision level fusion, the biometric sensors send their final decisions through a communication network that finally fuses these decisions at a fusion center. Comparing to match score level fusion and decision level fusion, feature level fusion contains richer information about multimodel biometrics. So feature level fusion will give better performance. Fusion increases accuracy, but it generally increases template sizes, computation costs and reduces user acceptance.

C.Feature level fusion

1) Converting different biometric representations into a common representation space using various embedding algorithms: (a) binary strings to point-sets, (b) point-sets to binary strings, and (c) fixed-length real-valued vectors to binary strings.

2) Fusing different features into a single multibiometric template that can be secured using an appropriate biometric cryptosystem such as fuzzy vault.

3) Incorporating a minimum matching constraint for each trait, in order to counter the possibility of an attacker gaining illegitimate access to the secure system by simply guessing/knowing only a subset of the biometric traits.

D.Embedded Algorithm

The embedding algorithm transforms a biometric feature representation into a new feature representation. The input representation x can be a real-valued feature vector, a binary string, or a point-set. The output representation z could be a binary string or a point-set that could be secured using fuzzy commitment or fuzzy vault, respectively.

III. FUZZY VAULT

In fuzzy vault encoder, the biometric template will be given along with random secret key which is converted to a polynomial degree and polynomial is evaluated in a graph. The set of points is then secured by hiding them with chaff points. The set of genuine points along with polynomial evaluations together with chaff points constitute the sketch or vault. In fuzzy vault decoder, the biometric will be given and then by using the filter the vault points and the query are compared. If the biometric query set is sufficiently close to many genuine points and it can be correctly identified and polynomial is reconstructed successfully and key is generated which is used for validity check. In multibiometric vault the feature level fusion is used to combine the biometrics and then fuzzy vault scheme is addressed.

IV. BIOHASHING

Biohashing is a template protection approach in which the biometric features are transformed using a function defined by a user-specific key or password. Since the transformation is invertible to a large extent, the key needs to be securely stored or remembered by the user and presented during authentication. This need for additional information in the form of a key increase the entropy of the biometric template and hence makes it difficult for the adversary to guess the template. (Entropy of a biometric template can be understood as a measure of the number of different identities that are distinguishable by a biometric system.)In base biohashing multimodal biometrics can reduce the probability of denial of access without sacrificing the false acceptation performance. the authors, in order to solve the problem of tokenized pseudo-random number (generated by an Hash key) and the user specific fingerprint features; in this way, a set of user specific compact codes can be produced which is named “BioHash code”. Direct mixing of pseudo-random number and biometric data is an extremely convenient mechanism with which to incorporate physical tokens, such as a smart card or an USB token.

The main drawback of this method, which has been applied to various biometric characteristics (face, fingerprint, iris) , is the low performance when an “impostor” B steals the Hash key or the pseudo-random numbers of A and tries to authenticate as A. When this problem occurs, the performance of BioHashing can be
lower than that obtained using only the biometric data. The Hashing approach and conclude that the claim of having achieved a zero EER is based upon the impractical hidden assumption of no stealing of the Hash key. Moreover, they proved that in a more realistic scenario where an impostor steals the Hash key the results are worse than when using the biometric alone.

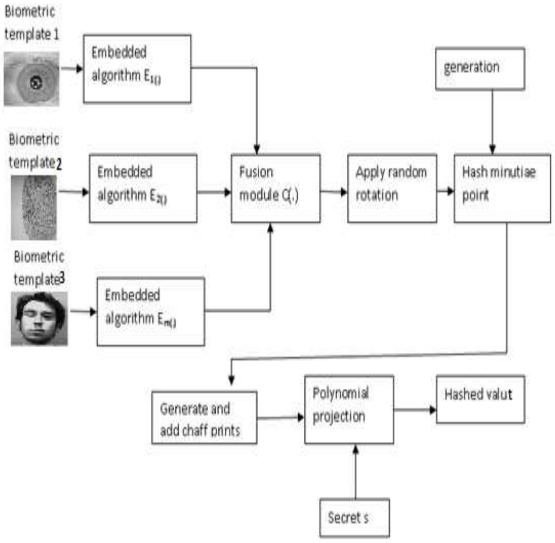


Figure.5.Block diagram of hybrid biometric systems

Finally, here combine the two techniques advantage that is.,get better security and low error rate,and designed to provide diversity and revocability.

.

V.EXPERIMENTS

The recognition performance and security of the proposed multibiometric cryptosystems on two different multimodal databases, each containing face, fingerprint,and iris modalities. The database is a multimodal database obtained by randomly linking subjects from FVC2002-DB-2 (fingerprint), CASIA Iris database Ver-1, and XM2VTS (face) databases. The performance of the quality-based product fusion rule was evaluated only on the WVU-Multimodal database since the other databases do not contain raw fingerprint and iris images to enable us to estimate the biometric sample quality. The performance of the fingerprint-based fuzzy vault implementation has been evaluated on FVC2002-DB2. FVC2002-DB2 was one of the benchmark databases used in the Fingerprint Verification Competition 2002 . The FVC2002-DB2 consists of 100 fingers with 8 impressions per finger obtained using an optical fingerprint sensor. This database was selected because it is a public-domain database and the images are of relatively good quality. The performance of the iris cryptosystem has been evaluated on the CASIA iris image database ver 1.0 . This database consists of images from 108 different eyes with 7 images per eye. These 7 samples were collected over two different sessions with 4 samples in one session and 3 in the other. We use one image from each session to evaluate the iris cryptosystem. The XM2VTS-Benchmark database consists of five face matchers and three speech matchers and was partitioned into training, fusion development and fusion evaluation sets according to the benchmark.

VI.CONCLUSION

The feature-level fusion framework for the design of multibiometric cryptosystems that simultaneously protects the multiple templates of a user using a single secure sketch is developed. The feasibility of such a framework has been demonstrated using both fuzzy vault and biohashing. These are the most well-known biometric cryptosystems. here different embedding algorithms used for transforming biometric representations and efficient decoding strategies for fuzzy vault and a mechanism to impose constraints such as minimum matching requirement for specific modalities in a multibiometric cryptosystem. Experiments on two different multibiometric databases containing fingerprint, face, and iris modalities demonstrate that it is indeed possible to improve both the matching performance and template security using the hybrid biometric cryptosystems. Here the four properties are satisfied with the combination of biometric cryptosystems and biohashing technique.

REFERENCES

[1].A. Jain, K. Nandakumar, and A. Nagar, “Biometric template security,” EURASIP Journal on Advances in signal processing,vol.2008,pp.1-17,2008.

[2]. A. Jules and M. Wattenberg, “A Fuzzy Commitment Scheme,” in Proc.sixth ACM Conference on computer and communications security, Singapore, November 1999, pp. 28–36.

[3]. B. Fu, S. X. Yang, J. Li, and D. Hu, “Multibiometric cryptosystem.Model structure and performance analysis,” IEEE Transactions on information forensics and security, vol. 4, no. 4, pp. 867–882, December 2009.

[4]. E. Kelkboom, X. Zhou, J. Breebaart, R. Veldhuis, and C. Busch, “Multialgorithm fusion with template protection “, in Proc.IEEE 3rd coference Biometrics:theory,applications,and systems,Washington, DC, September 2009.

[5].Y. Sutcu, Q. Li, and N. Memon, “Secure Biometric Templates from Fingerprint-Face Features,” in Proc.CVPR workshop on Biometrics,Minneapolis, June 2007.

[6]. A. Nagar, K. Nandakumar, and A. K. Jain, “Multibiometric cryptosystems,”Department of Computer Science and Engineering, Michigan State University, Tech. Rep. MSU-CSE-11-4, 2011.

[7].Maunel R.freire,Julian Fierrez,Javier Galblly,and Javier Ortega-Garcia,”Biometric recognition Group”-ATVS.Escuela Politecnica Superier ,Universidad autonoma de Madrid c/Francisco Thomas y valiente 11,E-28049 Madrid,Spain.

[8]. Alessandra Lumini, Loris Nanni, DEIS, IEIIT – CNR, Università di Bologna, Viale Risorgimento 2, 40136 Bologna, Italy Received 3 November 2005; received in revised form 24 March 2006; accepted 25 May 2006.

[9]. Abhishek Nagara Karthik Nandakumarb and Anil K. Jaina,c aMichigan State University, East Lansing, MI 48824, USA;bInstitute for Infocomm Research, A*STAR, Fusionopolis, Singapore;cDept. of Brain and Cognitive Eng., Korea University, Seoul 136-713, Korea.

[10] A. Juels and M. Sudan, “A Fuzzy Vault Scheme,” in Proc. IEEE International Symposium on Information Theory, Lausanne, Switzerland,2002, p. 408.

[11] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, “Generating Cancelable Fingerprint Templates,” IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 29, no. 4, pp. 561–572, April 2007.

[12] B. Fu, S. X. Yang, J. Li, and D. Hu, “Multibiometric cryptosystem: Model structure and performance analysis,” IEEE Transactions on Information Forensics and Security, vol. 4, no. 4, pp. 867–882, December 2009.

[13] K. Nandakumar, A. K. Jain, and S. Pankanti, “Fingerprint-based Fuzzy Vault: Implementation and Performance,” IEEE Transactions on Information Forensics and Security, vol. 2, no. 4, pp. 744–757, December 2007.

[14] Y. C. Feng and P. C. Yuen, “Protecting Face Biometric Data on Smartcard with Reed-Solomon Code,” in Proc. CVPR Workshop on Biometrics, New York, USA, June 2006.

[15] M. Freire-Santos, J. Fierrez-Aguilar, and J. Ortega-Garcia, “Cryptographic Key Generation Using Handwritten Signature,” in Proc. SPIE Conference on Biometric Technologies for Human Identification, vol.6202, Orlando, USA, April 2006, pp. 225–231.