ISSN:0975-9646

A Survey on Multimodal Biometric

Sakshi Kalra , Anil Lamba

CSE Department, KUK University
Haryana, India

Abstract— **Multibiometric systems are being increasingly deployed in many large scale biometric applications because they have several advantages such as lower error rates and larger population coverage compared to unibiometric systems. A number of bio-crypto algorithms have been proposed, they have limited practical applicability due to the trade-off between recognition performance and security of the template. In this paper an attempt to improve the recognition performance as well as the security of a biometric cryptosystem has been made and also tried to identify some of the challenges and issues that confront research in multimodal biometrics.**

Keywords— ***multibiometric , unibiometric, cryptosystem, multimodal***

I. INTRODUCTION

The process of identifying an individual using security systems is called authentication. It simply ensures that the individual is who he or she claims to be, but tells nothing about the access rights of the individual. Current authentication methods can be classified into three main areas .

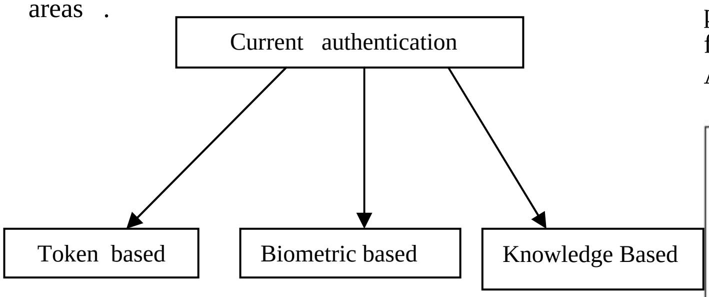

Fig. 1 Authentication Methods

Token based techniques are widely used for authentication using key cards, bank cards and smart cards. Many token-based authentication systems also use knowledge based techniques to enhance security. For example, ATM cards are generally used together with a PIN number [4].

Knowledge based techniques are the most widely used authentication techniques. These techniques include both text-based and picture-based passwords.

Biometric based authentication techniques uses a biometric authentication system which is essentially a pattern recognition system that operates by acquiring biometric data from an individual such as fingerprints, iris scan, or facial recognition, extracting a feature set from the acquired data, and comparing this feature set against the template set in the database. However, this technique provides highest level of security. Passwords and cards can be shared and thus cannot provide reliability [4].

Biometric systems serve one of two foundational purposes either verification/authentication or identification. Identification refers to the ability of a computer system to uniquely distinguish an individual from a larger set of individual biometric records on file (using only the biometric data). This is often referred as a “one-to many” match. Biometric verification or authentication involves a “one-to-one” search whereby a live biometric sample presented by an individual is compared to a stored sample previously given by that individual, and the match confirmed [3].The biometric system can also be attacked by the outsider or unauthorized person at various points.As biometric system can be either an 'identification' system or a 'verification' system, which are defined below.

Identification (1: n) – One-to-Many: Biometrics can be used to determine a person's identity even without his awareness or approval. Such as scanning a crowd with the help of a camera and using face recognition technology, one can verify matches that are already store in database.

Verification (1:1) One-to-One: Biometrics can also be used to verify a person's identity. Such as one can allow physical access to a secure area in a building by using finger scans or can grant access to a bank account at an ATM by using retina scan [3].

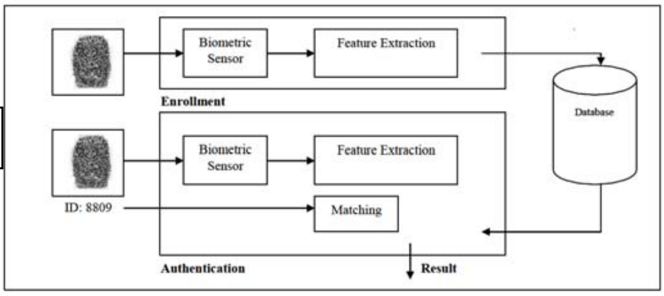

Fig.2. General biometric system

A. Biometric Recognition

Biometrics recognition is done through two distinct methods Evidence Identity, Confirmation of Template.

Evidence Identity: In identity provision the unknown person’s template is first checked with the stored database then identity is given to the unrecognized person. The identity is given with the name and the Identification Number and the record is stored successfully.

Confirmation of Template: When the identified person is giving his identity then the sensors should verified the person. In unimodal system we are using only one system as only single Fingerprint System, Iris System or Face Recognition System. Lots of problems has to face, when we are using uni modal biometrics system. [2] When the trait of biometrics has taken then the sometimes noise enters with the trait, that results in higher the false rejection rate. Also, when we are using the only single system then the database template can be stolen and it can be revoked by any intruder as it contains only one template. If person has been facing difficulty in giving template because of injury or damage of physical part of that person then the he can't use that system.

In this case multimodal system is the best choice for identification of the person without fail. In multimodal biometrics system we use two modalities for recognition of person.

Multi biometrics system has lots of advantage as follows:

(i) Its makes better system operation.

(ii) Its accuracy is better as compared to the unibiometric system.

(iii) It prevent from stolen the templates of biometric system as at the time it stores the two characteristics of biometric system in the database [2].

B. Biometric Authentication System

A biometric system consists of modules which work perpetually to authenticate and verify users. Widespread application of biometric based authentication leads to new problem of security and privacy. Security is a significant aspect of any authentication system and there are various ways to secure the system. The most potentially damaging attack on a biometric system is against the biometric templates that are stored in the system database. Biometric templates are actually compared in a biometric recognition system. So, special attention is given to Template Security which is achieved by Feature Transformations or Biometric Cryptosystems[1].

There are five major elements in a generic biometric authentication system, namely, sensor, feature extractor, template database, matcher and decision module.

a. Biometric Sensor: A biometric sensor is the interface between the user and the biometric system and its function is to acquire identifiable information from the users.

*b. Pre processing unit***:** This unit enhances the raw biometric (say by removing false minutiae points, removing spur and H-bridge from fingerprint image) to ensure that the acquired biometric can be reliably processed by a feature extractor.

*c. Feature extractor***:** Feature extractor processes the scanned biometric data to extract the salient information (feature set) that is useful in distinguishing between different users.

d. Template Generator: The extracted feature set is stored in a database as a template indexed by the user's identity information. A template is a small file derived from the distinctive features of a user's biometric data, used to perform biometric matches. Biometric systems store and compare biometric templates, not biometric data.

e. Matcher Module: The matcher module is usually an executable program, which accepts two biometric feature sets (from template and query respectively) as inputs, and outputs a match score (S) indicating the similarity between the two sets. This module compares query or test biometric data with the pre-stored template.

f. Decision module: Finally the decision module makes the identity decision and initiates a response to the query.

*g. Stored template***:** Since the template database could be geographically distributed and contain millions of records[1].

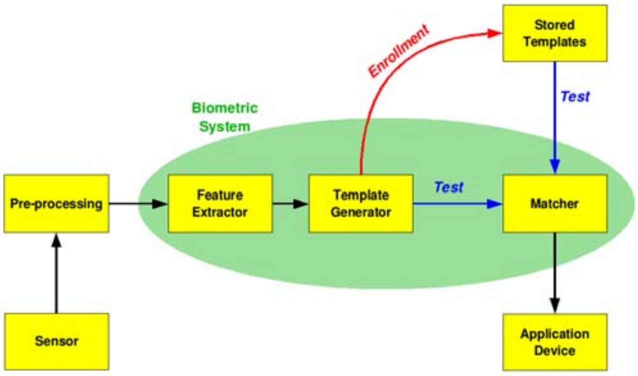

Fig.2. Biometric Authentication System

C. Security

Template security is one of the most important factor in designing a secure biometric system and it needs timely and severe attention. Most of the available template protection techniques fail to meet all the desired requirements of a practical biometric system like revocability, security, privacy, and high matching accuracy.

Table 1 Characterization of different outbreaks (attacks) on a biometric recognition system

ATTACKS	HAZARDS	EFFECTS	REMEDIES
Template database compromise	Privacy Loss (template theft, database cross-matching)	Gain access to the template database	Encrypt the templates
Fake enrolments	Denial of service (system's template database overflow) e.g. multiple email accounts	i) Generating fake biometric features ii)Enrolling fake biometrics	Controlled enrollment procedure
Hill Climbing	Privacy Loss (template theft)	i) Injecting biometric features ii) Obtaining match score	Avoid outputting the match scores
Biometric Spoof	Intrusion (multiple systems)	i) Acquiring biometric features ii) Creating reliable spoof	Liveness detection techniques

D. Evaluation

When it is time to use the biometric authentication, the degree of security is concerned. In this paper, we have discussed the various types of biometric authentication techniques. In this section, we will evaluate different techniques and find degree of security. There are various parameters with the help of which we can measure the performance of any biometric authentication techniques. These factors are described below

a). False Accept Rate (FAR) and False Match Rate (MAR**):** The probability that the system incorrectly declares a successful match between the input pattern and a non matching pattern in the database. It measures the percent of invalid matches. These systems are critical since they are commonly used to forbid certain actions by disallowed people.

b). False Reject Rate (FRR) or False Non-Match Rate (FNMR): The probability that the system incorrectly declares failure of match between the input pattern and the matching template in the database. It measures the percent of valid inputs being rejected.

c). Relative Operating Characteristic (ROC): In general, the matching algorithm performs a decision using some parameters (e.g. a threshold). In biometric systems the FAR and FRR can typically be traded off against each other by changing those parameters. The ROC plot is obtained by graphing the values of FAR and FRR, changing the variables implicitly. A common variation is the Detection Error Trade off (DET), which is obtained using normal deviate scales on both axes. This more linear graph illuminates the differences for higher performances.

d)Equal Error Rate (EER): The rates at which both accept and reject errors are equal. ROC or DET plotting is used because how FAR and FRR can be changed, is shown clearly. When quick comparison of two systems is required, the ERR is commonly used. Obtained from the ROC plot by taking the point where FAR and FRR have the same value. The lower the EER, the more accurate the system is considered to be.

e) Failure to Enroll Rate (FTE or FER**):** The percentage of data input is considered invalid and fails to input into the system. Failure to enroll happens when the data obtained by the sensor are considered invalid or of poor quality.

f). Failure to Capture Rate (FTC): Within automatic systems, the probability that the system fails to detect a biometric characteristic when presented correctly is generally treated as FTC.

g) Template Capacity: It is defined as the maximum number of sets of data which can be input in to the system.

II. Related Study

Summet Kaur [1] purposed that major catalyst to the rise of biometric methods is its eminence as an identity handling technique. This paper epitomizes the notion of biometric identification system, security, harms and benefits of fuzzy vault. It also points out the subsequent research that is needed to circumvent the attacks and vulnerabilities.

Rupesh Wagh [2] author ensured that while using biometrics, which is basically used for authentication and verification by the person's template. But that template can be misused if it is forged, by any enforcer. Converging on biometric template safekeeping was the prime discussion of his paper.

Renu Bhatia [3] laid emphasis on Biometrics which is a flourishing technology, which has been widely used in juristic, secured access and prison security. A biometric system is fundamentally a pattern recognition system that recognizes a person by determining the authentication by using his different organic features i.e. retina-scan, iris scan, Fingerprint, hand geometry, and face recognition are leading physiological biometrics and behavourial characteristic are keystroke-scan, Voice recognition and signature-scan. In this paper distinct biometrics techniques such as Iris scan, retina scan and face recognition techniques are discussed.

Shweta Malhotra [4] here author presents an approach to enhance the invisible watermarking technique with cryptography. The biometric trait is modified using invisible watermark information and is further secured using cryptography. The template is made more secure using encryption techniques like AES, MAES and finally stored in database.

Abhishek Nagar[5] discussed that Security concerns regarding the stored biometric data is impeding the widespread public acceptance of biometric technology. In this paper he improved the recognition performance as well as the security of a fingerprint based biometric cryptosystem, called fingerprint fuzzy vault. He incorporated minutiae descriptors, which capture orientation and frequency information in a minutia's vicinity, in the vault construction employing the fuzzy commitment approach.

Debnath Bhattacharyya [6]In his paper author laid emphasis on the biometric authentication techniques and some future possibilities in this field. The position of biometrics in the current field of Security has been depicted in his work .He has also outlined opinions about the usability of biometric authentication systems, correlation between distinct techniques and their loss & gain.

Table 2 Evaluation of Biometric Techniques

Biometric	EER	FAR	FRR
Face	Na	1%	10%
Fingerprint	2%	2%	2%
Hand	1%	2%	2%
Voice	6%	2%	10%
Keystrokes	1.8%	7%	.1%

III. Conclusion

The rank of biometrics in the current branch of Security has been depicted in this work. We have given the glimpse of utility of biometric authentication systems, contrast between distinct techniques and their pros and cons in this paper. While biometric authentication can offer a high degree of security, but it is not possible to definitely state if a biometric technique are successful run it is essential to locate factors that help to reduce affect system performance .The risks of compromise of distributed database of biometrics used in security application are high-particularly where the privacy is concerned. It is possible to eliminate the demand for such distributed databases through the careful application of biometric infrastructure without compromising security.

REFERENCES

[1] Sumeet kaur "Enhancing template security by a biometric key generating cryptosysytem", IJARCSSE, Vol. 3,Issue 8, pp 973-976, August 2013.

[2] Mr. Rupesh Wagh & Ms. Arati P Choudhari"Analysis of Mutlimodal Biometrics with Security Key ", IJARCSSE, Vol. 3, Issue 8, pp 1363-1365., August 2013

[3] Renu Bhatia "Biometrics and Face Recogniton Techniques ",IJARCSSE, Vol. 3, Issue 5 , pp 93-99, May 2013

[4] Shweta Malhotra & Dr. Chander Kant "A Novel approach for Securing Biometric Template " IJARCSSE , Vol. 3 , Issue 5 ,pp 397-403, May 2013

[5] Abhishek Nagar, Student Member, IEEE " Multibiometric Cryptosystems based on Feature Level Fusion"

[6] Debnath bhattacharya " Biometric Authentiction :A Review " Vol. 2 , Issue 3 , Sep 7 2009 , pp 13-26

[7]Parvinder S.Sandhu, Iqbldeep Kaur, Amit Verma, Samriit Jindal "Biometric Methods & Implementation of Algorithms " Vol.3 Issue 8 , 2009 , pp 492-496

[8]Harpreet Saini & Kanwal Garg "Comparitive Analysis of Various Biometric Techniques for database Security " IJSR (International journal of Science and Research) Vol. 2 Issue 4, pp150-153, April 2013

[9]Sulochana Sonkamble & Dr. Ravindra Thool "Survey Of Biometric Recognition Systems And Their Applications " Journal of Theoretical And Applied Information Technology(JATIT) , pp 45-51, 2005

[10]Nandakumar, K., 2008. "Multibiometric systems: Fusion strategies and template security". Ph.D.Thesis, Department of Computer Science and Engineering, Michigan State University.

[11]"Biometric template encryption" by A.K.Mohapatra, Madhvi Sandhu IGIT,GGSIP University,Kashmere GateDelhi Published in International Journal of Advanced Engineering & Application, Jan. 2010

[12]N. Kankrale, Prof. S. D. Sapkal. Template Level Fusion of Iris and Fingerprint in Multimodal Biometric Identification Systems, *Department of Information Technology SRES*

[13] R.N. Kankrale, Prof. S. D. Sapkal. Template Level Fusion of Iris and Fingerprint in Multimodal Biometric Identification Systems, *Department of Information Technology SRES*