Synopsis

On

Advanced Biometric Security using Multibiometric Fusion strategy

For Registration

Of

DOCTOR OF PHILOSOPHY

Submitted By
XYZ

Under the Guidance of

Name of Guide
Designation
Department of Computer Science & Applications
Kurukshetra University, Kurukshetra.

Department Name
Name of University, State

1. Introduction

Biometrics is automated methods of recognizing a person based on a physiological or behavioral characteristic such as face, fingerprints, finger knuckle print, voice and iris. Because such characteristic are physically associated to the user, biometric recognition is a natural and more reliable mechanism for ensuring that only authorized users are able to enter a facility, access a computer system, or cross international restrictions such as border of any country. It is basically a pattern-recognition system that is used to identify or verify a human beings or users. If we talk about the computer security there are three levels of computer security schemes. Firstly a person carries, such as an identity proof with a photograph. Secondly relies on something a person knows, such as a password or a code number. Finally the third and highest level relies on something that is a part of a person's biological makeup of behavior, such as a fingerprint, a knuckle print, a facial image, or a signature etc.

Table 1: Different type of user authentication schemes

Methods	Examples	Problems
What we Know?	Password, PIN, ID	Forgotten, Shared, easy to guess
What we have?	Key, Cards, etc	Lost or Stolen, Can be duplicated
What we are?	Fingerprint, Face, Iris…	Non-Repudiable authentication

First and second level of computer security schemes aren't sufficient and can be easily forgotten, lost, guessed, stolen, or shared. Associating an identity with an individual is called personal identification. In computer technology, biometrics relates to identity-confirmation and security techniques that based on measurable, individual biological characteristics (fingerprints, handprints, or voice) patterns might be used to enable access to a computer, to a room, or to an electronic commerce account. Biometric authentication systems can be more suitable for the users since there is no password to be forgotten or key to be lost and a single biometric trait (e.g., fingerprint) can be used to access several accounts without the burden of remembering passwords. Biometric-based solutions are able to provide for confidential financial transactions and personal data privacy. The need for biometrics can be found in federal, state and local governments, in the military, and in commercial applications. Enterprise-wide network security

infrastructures, government IDs, secure electronic banking, investing and other financial transactions, retail sales, law enforcement, and health and social services are already benefiting from these technologies. It is widely believed that biometrics will become a significant component of the identification technology as (i) the prices of biometrics sensors continue to fall, (ii) the underlying technology becomes more mature, and (iii) the public becomes aware of the strengths and limitations of biometrics. Like any other user verification method, a biometric system can be circumvented by a skill full imposter given the right circumstances and plenty of time and resources. Justifying such concerns is essential to gaining public confidence and acceptance of biometric technology.

The attacks on the world trade center towers and the pentagon on September 11, 2011, devastated the whole nation. Americans were looking at ways that could have prevented this terrible tragedy. This tragedy raised the concern for better information security. It has increased the emphasis on developing new ways to protect a person's most important and private information. One fairly new way that has been proposed to protect a person's information is biometrics. Humans have used body characteristics such as face, voice, gait, etc. for thousands of years to recognize each other. Alphonse Bertillon, chief of the criminal identification division of the police department in Paris, developed and then practiced the idea of using a number of body measurements to identify criminals in the mid 19th century. Just as his idea was gaining popularity, it was obscured by a far more significant and practical discovery of the distinctiveness of the human fingerprints in the late 19th century. Soon after this discovery, many major law enforcement departments embraced the idea of first "booking" the fingerprints of criminals and storing it in a database (actually, a card file). Later, the leftover (typically, fragmentary) fingerprints (commonly referred to as *latents*) at the scene of crime could be "lifted" and matched with fingerprints in the database to determine the identity of the criminals. Although biometrics emerged from its extensive use in law enforcement to identify criminals (e.g., illegal aliens, security clearance for employees for sensitive jobs, fatherhood determination, forensics, positive identification of convicts and prisoners), it is being increasingly used today to establish person recognition in a large number of civilian applications.

1.1 Biometrics Operations

Enrollment- A biometric system first records a sample using an appropriate sensor according to user's biometric trait. Enrollment is the process where a user's initial biometric sample or samples are collected, assessed, processed, and stored for ongoing use in a biometric system. Enrollment takes place in both 1:1 and 1:N systems. If users have any problems with a biometric system, they may need to re-enroll the biometric trait to gather higher quality data.

Biometric systems can provide two main functionalities after enrollment, namely, (i) verification and (ii) identification [WOO, 2005]. Figure 1 below shows the flow of information in verification and identification systems [RAV, 2007].

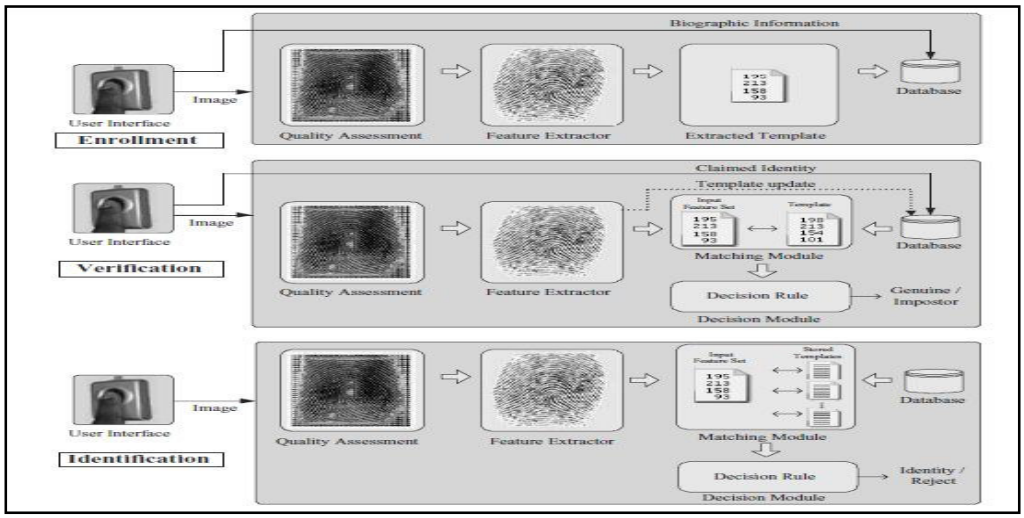

Fig. 1: Information flow in biometric systems.

i. **Verification-** Verification or authentication, the user claims an identity and the system verifies whether the claim is genuine. If the user's input and the template of the claimed identity have a high degree of similarity, then the claim is accepted as genuine. Otherwise, the claim is rejected and the user is considered a fraud. Table 2 below show some common biometric traits used for verification (authentication).

ii. **Identification-** In identification or recognition, the user's input is compared with the templates of all the persons enrolled in the database and the identity of the person whose template has the highest degree of similarity with the user's input is output by the biometric system. Typically, if the highest similarity between the input and all the templates is less than a fixed minimum

threshold, the system outputs a reject decision, which implies that the user presenting the input is not one among the enrolled users. Therefore, the matching is 1:N in an identification system

Table 2: List of biometrics and its traits

Biometric	Trait
Fingerprint	Finger lines, pore structure
Hand Geometry	Measurements of fingers and palm
Finger Geometry	Finger Measurement
Finger Knuckle Print	FKP image of left index, left middle, right index and right middle fingers
Facial Geometry	Distance of specific facial features (mouth, nose, eyes)
Iris	Iris pattern
Retina Eye	Pattern of the vein structure (background)
Vein structure	Vein structure of the back of the hand
Ear	form Dimensions of the visible ear
Voice	Tone or timbre
Gait	Gait energy image, user's height and walk length
Keystroke	Keystroke durations, finger placement and applied pressure on the keys
Signature	Writing with pressure and speed differentials
DNA	DNA code as the carrier of human genetic features

1.2 Biometric Techniques

There are many different techniques available to identify/verify a person based on biometrics as suggested by U.K. Biometric Working Group [UKBWG, 2003]. These techniques can be divided into physical characteristics and behavioral characteristics based techniques.

1.3 Popular Biometric Methodologies

Biometrics is divided broadly in two categories, physiological and behavioral as shown below in the figure 3. No single biometrics is expected to effectively satisfy the needs of all identification and authentication applications. Each biometrics has its strengths and limitations; and accordingly (discussed broadly in sec 1.5), each biometric appeal to a particular identification application. Summary of the popular biometric methodologies is described here.

i. **Fingerprints**

Fingerprints are graphical flow-like ridges present on human fingers [MOR, 2011]. Their formations depend on the initial conditions of development and are believed to be unique to each person. Fingerprints are one of the most mature biometric technologies used in forensic divisions worldwide for criminal investigations and therefore, have a shame of criminality associated with them

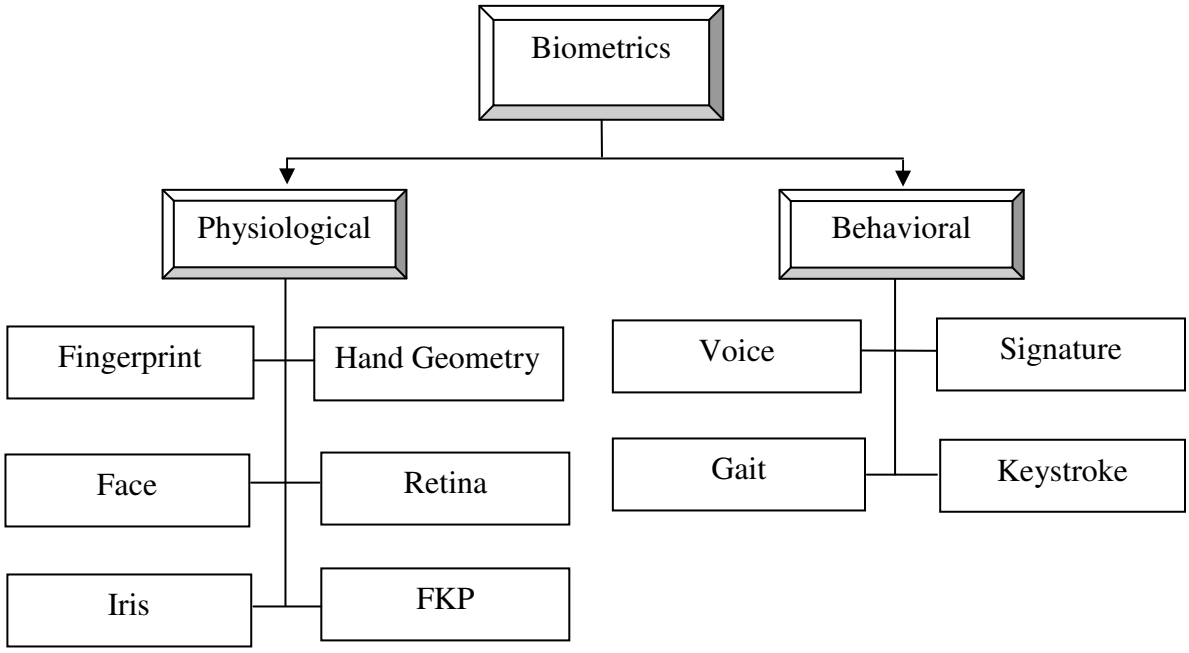

Fig. 3: Different biometrics methodologies

ii. **Face**

Face is one of the most acceptable biometrics because it is one of the most common methods of identification which humans use in their visual interactions. In addition, the method of acquiring face images is non-intrusive.

iii. **Iris**

Visual texture of the human iris is determined by the disordered morphogenetic processes during development and is posited to be unique for each person and each eye [ROS, 2006]. An iris image is typically captured using a non-contact imaging process. Capturing an iris image

involves cooperation from the user, both to register the image of iris in the central imaging area and to ensure that the iris is at a predetermined distance from the focal plane of the camera.

iv. **Voice**

Voice is a characteristic of an individual [ROS, 2006]. Voice is a behavioral biometrics. However, it is not expected to be sufficiently unique to permit identification of an individual from a large database of identities. Voice is affected by a person's health, e.g. cold, stress, emotions, etc.

v. **Gait**

Gait is the atypical way one walks and is a complex spatio-temporal behavioral biometrics. Although gait is not supposed to be unique to each individual, yet it may be sufficiently characteristic to allow identity authentication [JEO, 2006].

vi. **Signature**

The way a person signs her name is known to be a characteristic of that individual. Although signatures require contact and effort with the writing instrument, they seem to be acceptable in many government, legal, and commercial transactions [ARA, 2007] as a method of personal authentication.

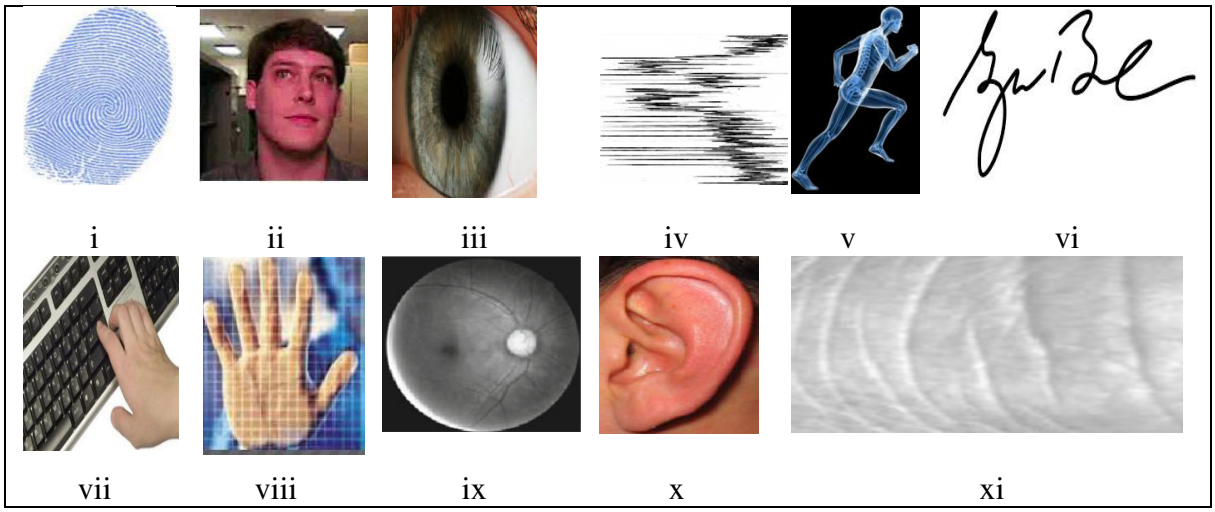

Fig. 4: Commonly used biometric traits: (i) fingerprint, (ii) face, (iii) iris, (iv) voice, (v) gait, (vi) signature, (vii) keystroke, (viii) hand geometry, (ix) retina, (x) ear, (xi) finger knuckle print

vii. **Keystroke Dynamics**

It is hypothesized that each person types on a keyboard in a characteristic way. This behavioral biometrics is not expected to be unique to each individual but it offers sufficient discriminatory

information to permit identity authentication [LEE, 2007]. Keystroke dynamics is a behavioral biometric; for some individuals, one may expect to observe a large variations from typical typing patterns.

viii. **Hand Geometry**

In recent years, hand geometry has become a very popular access control biometrics which has captured almost half of the physical access control market [SNE, 2005]. Some features related to a human hand, e.g., length of fingers, are relatively invariant and peculiar (although, not unique) to each individual.

ix. **Retinal Scan**

The retinal vasculature is rich in structure and is supposed to be a characteristic of each individual and each eye. It is claimed to be the most secure biometrics since it is not easy to change or replicate the retinal vasculature.

x. **Ear**

It is known that the shape of the ear and the structure of the cartilaginous tissue of the pinna are distinctive [ZHO, 2007]. The features of an ear are not expected to be unique to each individual. The ear recognition approaches are based on matching vectors of distances of salient points on the pinna from a landmark location on the ear.

1.4 Characteristics of an ideal Biometrics

On the above study of biometric methodologies there are some characteristic of ideal biometrics which are as follow:

i. Universality: It means that every person should possess the biometric traits.
ii. Uniqueness: It indicates that no two persons should be the same in terms of the traits.
iii. Permanence: It means that the traits should be invariant with time. A cue that changes significantly over time is not a useful biometric.
iv. Collectability: It means that it should be possible to acquire and digitize the cue using suitable devices without causing any inconvenience to user.
v. Performance: It refers to the achievable recognition accuracy, speed, robustness, and the resources required to achieve the accuracy and speed.
vi. Acceptability: It indicates the extent to which people are willing to accept a particular biometrics in their daily life.

vii. Circumvention: It refers to how easy it is to fool the system by fraudulent methods

1.5 Comparison of Different Biometric Methodologies

On the basis of characteristics of biometrics system table 3 has shown the comparison of various biometric systems. We have ranked each biometric based on the categories as being low, medium or high. A low ranking indicates poor performance in the evaluation criterion whereas a high ranking indicates a very good performance. In table 3 we have divided various biometric traits based on their performance characteristics as high (10), medium (7) and low (3). We can compute total percentage of each biometric trait, and based on this performance we can compute grade system of these biometric traits. Overall performance of each biometric trait is computed by dividing:

(Total assumed performance of each biometric trait / total expected performance*10)

Table 3: Performance comparison of various biometric traits (10=high, 7=medium, 3=low)

Identifier/Criteria	**Universality**	**Uniqueness**	**Permanence**	**Performance**	**Acceptability**	**Collectability**	**circumvention**	**Total Performance**
Fingerprint	7	10	10	10	10	7	10	**9.14**
Finger Knuckle	7	10	10	10	10	7	7	**8.71**
Iris	10	10	10	10	3	7	10	**8.57**
Ear	7	10	10	7	10	7	7	**8.2**
Retina	10	10	7	10	3	3	10	**7.57**
Hand Geometry	7	7	7	7	7	10	7	**7.42**
Hand Vein	7	7	7	7	7	7	10	**7.2**
DNA	10	10	10	10	3	3	3	**7**
Face	10	3	7	3	10	10	3	**6.57**
Gait	7	3	3	3	10	10	7	**6.14**
Voice	7	3	3	3	10	7	3	**5.14**
Signature	3	3	3	3	10	10	3	**5**
Keystroke	3	3	3	3	7	7	7	**4.71**

Now, as per this average performance of each biometric trait we can compute grade system which divides all biometric traits in good or bad quality performance, e.g. fingerprint trait is in A++ category. That means it have high level of performance among all biometric traits.

(i) ≤ 9.1 - 10.0 = A++ (ii) ≤ 8.1 - 9.0 = A

(iii) ≤ 7.1 - 8.0 = B++ (iv) ≤ 6.1 - 7.0 = B

(vi) ≤ 4.1 - 5.0 = C

1.6 Biometrics Deformations

Biometric system performance varies according to sample quality and the environment in which the sample is being submitted; it is possible to locate and minimize factors that can reduce/affect system performance [HAY, 2002]. These factors are known as biometrics deformations. The biometrics deformations for various traits are given below:

i. **Fingerprint**

- Cut sign on finger
- Dry/oily finger
- High or low humidity

ii. **Voice recognition**

- Cold that affects voice
- Capture devices
- Environments at time of recording voice (background noise)

iii. **Facial recognition**

- Change in facial hair
- Change in hairstyle
- Lighting conditions

iv. **Iris-scan**

- Too much movement of head or eye
- Glasses
- Colored contacts
- Too much movement of head or eye

v. **Hand geometry**

- Jewelry
- Change in weight
- Swelling of joints

vi. **Signature-scan**

- Marking too quickly
- Different marking positions (e.g., sitting vs. standing)

vii. **FKP print**

- Ring
- Fracture in finger

The performance of many biometric systems varies for specific populations. In addition, for many systems, an additional strike occurs when a long period of time has elapsed since enrollment or since one's last verification. If significant time has elapsed since enrollment, physiological changes can complicate verification. If time has elapsed since a user's last verification, the user may have forgotten how he or she enrolled, and may place a finger differently [JAI, 2005] or recite a pass phrase with different intonation.

2. Related Work

Biometrics deals with identifying individuals with the help of their biological and behavioral data such as fingerprints, iris patterns, and facial features, finger knuckle print and voice etc. Unibiometric systems are affected by a number of problems such as noisy sensor data, non-universality and lack of individuality of the chosen biometric trait, absence of an invariant representation for the biometric trait and susceptibility to circumvention. Some of these problems can be addressed by using multibiometric systems that consolidate the evidence from multiple biometric sources. Multibiometric systems combine the information presented by multiple biometric sensors, algorithms, samples, instances, or traits. The literature work discussed in the section focus on the area a) fusion strategies in multibiometric systems, b) Security and performance issues, c) Issues related to soft biometrics.

The literature shows that four possible levels of fusion are used for integrating data from two or more biometric systems [CAM, 2008]. These are the sensor level, the feature level, the matching score level, and the decision level. The sensor level and the feature level are referred to as pre-mapping fusion while the matching score level and the decision level are referred to as post-mapping fusion. In pre-mapping fusion, the data is integrated before any use of classifiers, while in post-mapping fusion; the data is integrated after mapping into matching score/ decision space.

Arun Ross and Rohin Govindarajan [ROS, 2005] in paper a "Feature Level Fusion Using Hand and Face Biometrics" author discussed fusion at the feature level in 3 different scenarios: (i) fusion of PCA and LDA coefficients of face; (ii) fusion of LDA coefficients corresponding to the R, G, B channels of a face image; (iii) fusion of face and hand biometric traits. Preliminary

results were encouraging and helped in highlighting the pros and cons of performing fusion at this level. The primary motivation of author's work was to demonstrate the viability of such a fusion and to underscore the importance of pursuing further research in this direction. Information from multiple sources could be consolidated in several distinct levels, including the feature extraction level, match score level and decision level.

Anil Jain, Karthik Nandakumar, and Arun Ross [JAI, 2005] in paper "Score Normalization in Multimodal Biometric Systems" have discussed the performance of different normalization techniques and fusion rules in the context of a multimodal biometric system based on the face, fingerprint and hand-geometry traits of a user. The matching scores output by the various modalities were heterogeneous; score normalization was needed to transform these scores into a common domain, prior to combining them. Experiments conducted on a database of 100 users indicated that the application of min-max, z-score, and tanh normalization schemes followed by a simple sum of scores fusion method has resulted in better recognition performance compared to other methods.

Lin Zhang et.al in their paper [ZHA, 2011] "Ensemble of local and global information for finger–knuckle-print recognition" based on the results of psychophysics and neurophysiology studies that both local and global information is crucial for the image perception, author present an effective FKP recognition scheme by extracting and assembling local and global features of FKP images. Specifically, the orientation information extracted by the Gabor filters is coded as the local feature. By increasing the scale of Gabor filters to infinite, actually anyone can get the Fourier transform of the image, and hence the Fourier transform coefficients of the image can be taken as the global features. Such kinds of local and global features are naturally linked via the framework of time–frequency analysis. The author proposed scheme of exploits both local and global information for the FKP verification, where global information is also utilized to refine the alignment of FKP images in matching. The final matching distance of two FKPs is a weighted average of local and global matching distances.

Michal K.O Goh, Connie Tee and Andrew B.J.Teoh [GOH, 2010] in paper "Bi-Modal Palm print and Knuckle Print Recognition System" presented a new approach for the personal identification using palm print and knuckle print. The Palm print and knuckle print features are

extracted using Wavelet Gabor competitive Code and Ridge Transform methods. The fusion of these features yields promising result of EER=1.25% for verification rate. The achieved results were significant since the two biometric traits were derived from the same image, unlike other bimodal biometric systems which required two different sensors. The author has shown the decision level fusion scheme, with weighted sum rule, achieved better performance than those for fusion at the representation level.

Chander Kant, Rajender Nath and Sheetal Chaudhary [KAN, 2008] in paper "Biometrics Security using Steganography", a biometric system is at risk to a variety of attacks. These attacks are proposed to either avoid the security meet the expense by the system or to put off the normal functioning of the system. Biometric have various risks while using biometric system. But proper use of cryptography reduces the risks in biometric systems as the dirty minded people have to find both secret key and template. In this paper authors presented a new idea to make system more secure by use of steganography. Here the secret key is in the form of pixel will be merged in the picture itself while encoding, and at decoding end only the authentic user will be allowed to decode.

D. Swangpol and T. Chalidabhongse [SWA, 2005] in paper "Automatic Person identification using multiple traits" describes a method for vision-based person identification that can detect, track, and recognize person from video using multiple traits: height and dressing colors. The method does not require constrained target's pose or fully frontal face image to identify the person. First, the system, which is connected to a pan-tilt-zoom camera, detects target using motion detection and human cardboard model. The system keeps tracking the moving target while it is trying to identify whether it is a human and identify who it is among the registered persons in the database. To segment the moving target from the background scene, authors employ a version of background subtraction technique and some spatial filtering. Once the target is segmented, we then align the target with the generic human cardboard model to verify whether the detected target is a human. If the target is identified as a human, the card board model is also used to segment the body parts to obtain some salient features such as head, torso, and legs. The whole body silhouette is also analyzed to obtain the target's shape information such as height and slimness. Author then use these multiple traits (at present, authors uses shirt color, trousers color, and body height) to recognize the target using a supervised self-organization process. Author preliminary tested the system on a set of 5

subjects with multiple clothes. The recognition rate is 100% if the person is wearing the clothes that were learned before. In case a person wears new dresses the system fail to identify. This means height is not enough to classify persons. Author plan to extend the work by adding more traits such as skin color, and face recognition by utilizing the zoom capability of the camera to obtain high resolution view of face; then, evaluate the system with more subjects

Chander Kant, Rajender Nath and Sheetal Chaudhary [KAN, 2009] in paper "Soft Biometric: An Asset for Personal Recognition", biometric systems automatically recognize individuals based on their biometric traits. There are certain human characteristic like gender, ethnicity, age, height, eye color and weight are not unique and reliable, and they provide some information about the user. The authors refer to these characteristics as "soft" biometric traits and argue that these traits can be integrated with the identity information provided by the primary biometric identifiers like fingerprint, face, iris, signature etc. Although soft biometric characteristics lack permanence to identify an individual uniquely and reliably, they provide some evidence about the user identity that could be beneficial.

3. Problem Domain

Biometric-based systems also have some limitations that may have adverse implications for the security of a system [VET, 2007]. While some of the limitations of biometrics can be overcome with the evolution of biometric technology and a careful system design, it is important to understand that foolproof personal recognition systems simply do not exist and perhaps, never will. Security is a risk management strategy that identifies, controls, eliminates, or minimizes uncertain events that may adversely affect system resources and information assets All the security system are not foolproof. Every system is breakable. In spite of their numerous advantages, biometric systems are vulnerable to attacks, which can decrease their security. Ratha et al. [RAT, 2001] analyzed these attacks, and categorized into eight types. Figure 7 shows these attacks along with the components of a typical biometric system. Type 1 attack involves presenting a fake biometric (e.g., synthetic fingerprint, face, iris) to the sensor. Type 2 attack constitutes submitting a previously intercepted biometric data (replay). In Type 3 attack, the feature extractor module is compromised to produce feature values selected by the attacker. In Type 4 attack genuine feature values are replaced with the ones selected by the attacker. In Type 5 attack matcher can be modified to output an artificially high matching score. Type 6 attack

involves the attack on the template database (e.g., adding a new template, modifying an existing template, removing templates, etc.). In Type 7 attack the transmission medium between the template database and matcher is attacked resulting in the alteration of the transmitted templates. In type 8 attack the matcher result (accepts or reject) can be overridden by the attacker. However, a big threat for biometric authentication is still compromise of a user's biometric information [JAI, 2004]. The reason is that many platforms and biometric systems are used without their untrustworthiness being detected.

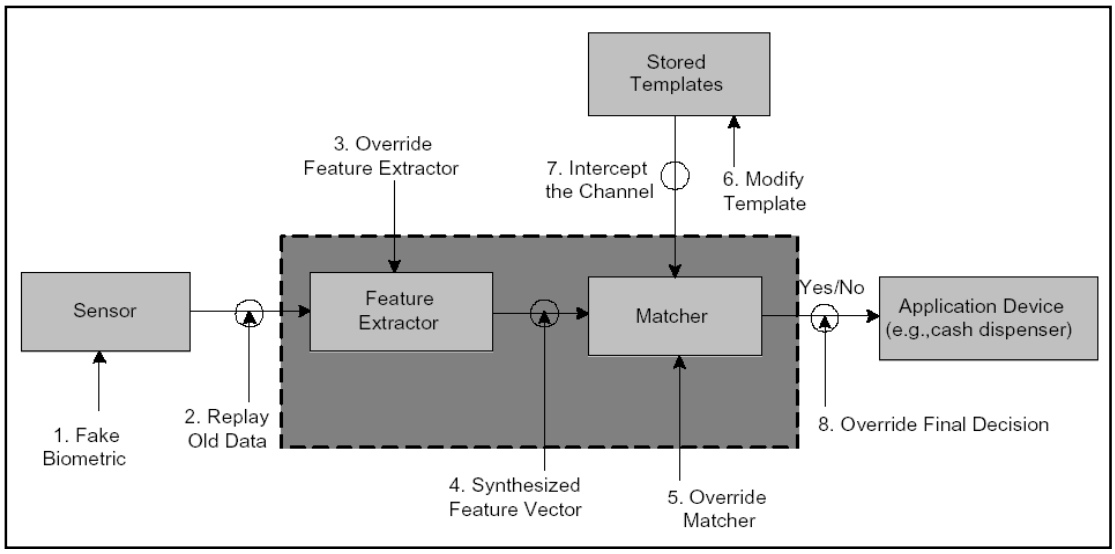

Fig. 7: Different attack points.

If an impostor is able to access a user's biometric information, he or she can then replay this information to a matching algorithm used for user authentication, and be accepted as a valid user, given that the matching algorithm is not able to recognize the origin of the biometric information[SAN, 2004] .

The problem of resolving the identity of a person can be categorized into two fundamentally distinct types of problems with different inherent complexities: (i) verification and (ii) identification.

4.Proposed Work

Security of biometric systems has been become a challenging task. Some of the factors that impact the accuracy of biometrics system include noisy input, non-universality, lack of invariant

representation and non-distinctiveness. Biometric systems are also vulnerable to various types of security attacks discussed in section 4. In the proposed work, we will address the issues related to security of biometric techniques by taking help of various biometric techniques

i. Multibiometric system
ii. Biometric Steganography
iii. Cancellable biometrics
iv. Liveness detection
v. Biometric cryptosystem

i. **Multibiometric systems**

Multibiometric systems collect data from more than one biometric trait (e.g., face, finger knuckle print and iris) in order to recognize a person. 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. A number of software and hardware multibiometric products have also been introduced by biometric vendors. A new approach to personal authentication using finger knuckle print (FKP), which has distinctive line features is introduced. In proposed, we will use finger knuckle print with face scan features to improve the security of biometric system.

ii. **Biometric Steganography**

Steganography is defined as the science of hiding or embedding data in a transmission medium. Its ultimate objectives, which are undetectability, robustness (i.e., against image processing and other attacks) and capacity of the hidden data (i.e., how much data we can hide in the carrier file), are the main factors that distinguish it from other sisters-in science techniques, namely watermarking and Cryptography. We have discussed various types of attacks that can be launched against a biometric system. We will use steganography principles to enhance the integrity and security of biometric templates.

iii. Cancellable Biometric

Cancellable biometrics offers a solution for preserving user privacy since the user's true biometric is never reveal in the authentication process. It ensures that template protection is

achieved at the feature level with the assistance of the auxiliary data/non-invertible transforms. On the other hand, cancellable biometrics has certain limitations that need to be taken into account. For instance in biometric salting design, the template may not longer secure when the auxiliary data is compromised. For non-invertible transforms, non-invertibility enhances the security of the template space by employing a transformation process to reset the order or position of the feature set. However, this weakens the discriminatory power (performance) of the transformed features due to the enlargement of intra-class variation in the biometrics. In this context, if performance is the main concern in the design of a biometric system, then the system is expected to be lacking in randomness as required for the design of a secure and unpredictable template space. Hence, it is very challenging to design a non-invertible function that satisfies both performance and non-invertibility requirements.

iv. **Liveness detection**

Liveness detection in biometric system means the capability of the system to detect during enrollment and identification/verification, whether the biometric sample presented is alive or not [SAN, 2004]. Furthermore, if the system is designed to protect against attacks with artificial input samples, it must also check that the presented sample belongs to the live human being who was originally enrolled in the system and not just any live human being. Liveness detection can be performed either at the acquisition stage or at processing stage. There are two approaches in determining if the input sample is alive or not; liveness detection and non-liveness detection. The material or data used to spoof a system often have a number of different non-liveness characteristics that could be used to detect non-liveness. An example of a non-liveness detection method would be to detect air bubbles in gelatin artificial fingerprints. Most biometric systems today have a decision process which first checks liveness [WAN, 2004]:

if data=live

perform acquisition and extraction

else If data= not live

do not perform acquisition and extraction

Liveness detection can be introduced into a biometric system using extra hardware to acquire life signs, using the information already captured by the system to detect life signs or using liveness information inherent to the biometric.

v. **Biometric Cryptosystem**

Biometric cryptosystems are designed to securely bind a digital key to a biometric or generate a digital key from biometric offering solutions to biometric-dependent key-release and biometric template protection. Biometric cryptosystems combine cryptography and biometrics to benefit from the strengths of both fields. In such systems, while cryptography provides high and adjustable security levels, biometrics brings in non-repudiation and eliminates the need to remember passwords or to carry tokens etc. While biometrics provides non-repudiation and convenience, traditional cryptography provides adjustable levels of security and can be used not just for authentication, but also for encryption. Biometrics-based key generation refers to extracting/generating a cryptographic key from a biometric template or construct. In this case, biometrics and cryptography are tightly coupled: the secret key is bound to the biometric information and the biometric template is not stored in plain form.

As a result the issue of biometric system security has several challenges, and it is necessary that further research be conducted in this direction. Different biometric techniques require different methodologies and tools. Specific type of sensors for acquiring biometric data and different feature interaction tools are needed for each of the technique. Hence, security of biometric system is an important yet challenging problem, due to the complexity of algorithms (e.g. feature extractor and matcher) in such system. As an increasing number of these systems are being deployed in both commercial and government applications, and thorough analysis of this challenge becomes necessary. A framework needs to be developed for combining the advantages of multibiometric system, biometric steganography, cancellable biometrics, liveness detection and biometric cryptosystem for making system totally foolproof.

5. Tools to be Used

The performance can be evaluated with the help of certain available tools like MUBI which are available free of cost at the websites. This MUBI tool provides the framework for conducting normalization and fusion evaluations.

6. Conclusion

The security of biometric systems has however been questioned and previous studies have shown that these systems can be fooled with artificial biometric cues. Even if the accuracy of biometric techniques is not perfect yet, there are many mature biometric system available low. The

challenge then is to design a secure biometric system that will accept only the legitimate presentation of the biometric characteristics without being fooled by the spoofed measurements injected into the system. Providing template security is one of the critical steps in designing a secure biometric system because stolen biometric templates cannot be cancelled and reissued. As biometric technology matures, there will be an increasing interaction among the biometric market, biometric technology, and the identification applications. It is certain that biometrics based identification will have a profound influence on the way we conduct our daily business. It is also certain that, biometric system security enhanced through the multibiometric, biometric steganography, cancellable biometric, liveness detection and biometric cryptosystem will remain an integral part of the preferred biometric-based identification solutions in the years to come.

References

[FRE, 2006] M. Freire-Santos, J. Fierrez-Aguilar, and J. Ortega-Garcia. Cryptographic Key Generation Using Handwritten Signature. In Proceedings of Biometric Technologies for Human Identification, Part of SPIE Defense and Security Symposium, volume 6202, pages 225-231, Orlando, USA, April 2006.

[HAN, 2013] Hu Han, Charles Otto, and Anil K. Jain. "Age Estimation from Face Images: Human Vs. Machine Performance". In 6th IAPR Internation Conference on Biometrics (ICB), June 4-7, 2013, Madrid, Spain.

[HAY, 2002] J. Hayashi, M. Yasumoto, H. Ito, and H. Koshimizu. Age and Gender Estimation based on Wrinkle Texture and Color of Facial Images. In Proceedings of the Sixteenth International Conference on Pattern Recognition, pages 405–408, Quebec City, Canada, August 2002.

[HON, 1999] L. Hong, A. K. Jain, and S. Pankanti, "Can multibiometrics improve performance?," in Proc. AutoID'99, Summit, NJ, Oct. 1999, pp. 59–64.

[JAI, 2004] Jain, Anil K. and Arun Ross, "Multibiometric systems," Communications of the ACM," January 2004, Volume 47, Number 1, 2004.

[JAI, 2005] Jain, Anil K. and Arun Ross and U. Uludag "Biometrics Template Security: Challenges and Solutions", in proc. of European Signal Processing Conference Sept. , 2005.

[JAI, 2012] A.K. Jain, K. Nandakumar. Biometric Authentication: System Security and User Privacy, IEEE Computer Society, Nov., 2012.

[JAI, 2012] A.K. Jain, K. Nandakumar and Abhishek Nagar. "Fingerprint Template Protection: From Theory to Practice",Springer, 2012.

[JEO, 2006] D. S. Jeong, H. A. Park, K. R. Park, and J. Kim. Iris Recognition in Mobile Phone Based on Adaptive Gabor Filter. In Proceedings of IAPR International Conference on Biometrics (ICB), pages 457-463, Hong Kong, China, January 2006.

[KAN, 2008] Chander Kant, Rajender Nath, Sheetal Chaudhary, "Biometrics Security using Steganography" published in CSC online Journal "International Journal of Security" Malashiya Vol-II Issue-I, PP 1-5. www.cscjournals.com. ISSN 1985-2320. (2008)

[KAN, 2009] Chander Kant, Rajender Nath, Sheetal Chaudhary, "Soft Biometric: An Asset for Personal Recognition" published in International Journal of Computing Science & Communication Technologies [IJCSCT]. Vol-I, Issue-II, 2009 PP 160-163. ISSN - 0974-3375.

[KUM, 2009] A. Kumar, Y. Zhou, Personal identification using finger knuckle orientation features, Electronic Letters 45 (20) (2009) 1023–1025.

[LEE, 2007] Y. J. Lee, K. Bae, S. J. Lee, K. R. Park, and J. Kim. Biometric Key Binding: Fuzzy Vault based on Iris Images. In Proceedings of Second International Conference on Biometrics, pages 800-808, Seoul, South Korea, August 2007.

[MOR, 2011] A. Morales, C.M. Travieso, M.A. Ferrer, and J.B. Alonso. Improved finger-knuckle-print authentication based on orientation enhancement. Electronics Letters, 47(6):380 – 381 (2011).

[RAV, 2007] Ravikanth, C., Kumar, A.: Biometric authentication using finger-back surface. In: Proc. CVPR, pp. 1–6 (2007).

[ROS, 2006] A. Ross, S. Shah, and J. Shah. Image Versus Feature Mosaicing: A Case Study in Fingerprints. In Proceedings of SPIE Conference on Biometric Technology for Human Identification, volume 6202, pages 1-12, Orlando, USA, April 2006.

[ROS, 2006] A. Ross, K. Nandakumar, and A. K. Jain. Handbook of Multibiometrics. Springer, (2006).

[SAN, 2004] Sandstrom, Marie, "Liveness Detection in fingerprint recognition systems", Linkoping University Electronic Press-Student Thesis, http://www.ep.liu.se/exjobb/isy/2004/3557/

[SCH, 2002] S. A. C. Schuckers. Spoofing and anti-spoofnng measures. Information Security Technical Report, 7(4):56{62, December 2002.

[SHA, 2001] G. Shakhnarovich, L. Lee, and T.J. Darrell. Integrated Face and Gait Recognition from Multiple Views. In IEEE Conference on Computer Vision andPattern Recognition (CVPR), pages 439-446, Hawaii, USA, December 2001.

[SNE, 2005] R. Snelick, U. Uludag, A. Mink, M. Indovina, and A. K. Jain. Large Scale Evaluation of Multimodal Biometric Authentication Using State-of-the-Art Systems. IEEE Transactions on Pattern Analysis and Machine Intelligence, 27(3):450-455, March 2005.

[RAT, 2001] N.K. Ratha, J.H. Connell, and R.M. Bolle, "An analysis of minutiae matching strength", Proc. AVBPA 2001, Third International Conference on Audio- and Video-Based Biometric Person Authentication, pp. 223-228(2001).

[ULU, 2004] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain. Biometric Cryptosystems: Issues and Challenges. Proceedings of the IEEE, Special Issue on Multimedia Security for Digital Rights Management, 92(6):948{960, June 2004.

[VET, 2007] A. Vetro and N. Memon. Biometric System Security. Tutorial presented at Second International Conference on Biometrics, Seoul, South Korea, August 2007.

[WAN, 2004] J. Li, Y. Wang, T. Tan, and A.K. Jain, Live face detection based on the analysis of fourier spectra. In Biometric Technology for Human Identification, SPIE Vol. 5404, pp. 296-303, 2004.

[WOO, 2005] Woodard, D.L., Flynn, P.J. Finger surface as a biometric identifier. Computer Vision and Image Understanding 100(3), 357–384 (2005).

[ZHA, 2009] L. Zhang, L. Zhang, and D. Zhang. Finger-knuckle-print verification based on band-limited phase-only correlation. In International Conference on Computer Analysis of Images and patterns, pages 141–148(2009).

[ZHA, 2010] L. Zhang, L. Zhang, D. Zhang, H. Zhu, Online finger–knuckle-print verification for personal authentication, Pattern Recognition 43 (7) (2010) 2560–2571.

[ZHO, 2007] X. Zhou. Template Protection and its Implementation in 3D Face Recognition Systems. In Proceedings of SPIE Conference on Biometric Technology for Human Identification, volume 6539, pages 214-225, Orlando, USA, April 2007.