Bachelor's Thesis (UAS)

Degree Program

Information Technology

2014

Ashish Shrestha

Multi-biometric systems

– Templates, Template Protection and Remote Authentication

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

BACHELOR´S THESIS | ABSTRACT
TURKU UNIVERSITY OF APPLIED SCIENCES

Degree programme | Information Technology

June2014| 61 Pages

Instructor: Almurrani Balsam

Ashish Shrestha

Multi-biometric systems

– Types, Remote Authentication and Template Protection

The intention behind writing this thesis was to provide a brief description on biometric security systems, multi-biometrics, implementation of multi-biometrics in remote authentication systems, and template protection. The thesis also discusses few of the available protocols proposed by researchers for template protection and remote authentication. The information for this thesis has been acquired through various articles, journals, books, internet resources, documentary films, magazines and dissertations. In addition, methods such as data collection and data mining have been implemented in order to gain an optimum understanding over the subject.

The study has attempted to reach throughout the history and provide a brief introduction to biometrics, its development throughout the human technological advancement since the initial establishment and hence the cumulative movement towards multi-biometrics security features and its fusion to various templates.

The result of the study is a review of the most popular methods of biometrics and, their advantages and disadvantages.

Keywords

Biometrics, Multi-biometrics, remote authentication, identification, verification, Biometric Templates, template fusions, security protocols

ACKNOWLEDGEMENTS

First and foremost, I have to thank my thesis supervisor, **Mr. Balsam Almurrani**. Without his assistance and dedicated involvement in every step throughout the process, this thesis would have never been accomplished. I would like to thank you very much for your support and understanding over the entire time.

I would like to extend my gratitude to my language instructor **Ms. Poppy Skarli**. Her teaching style and enthusiasm for the topic made a strong impression on me and I have always carried positive memories of her classes with me. Without her my thesis would have been ludicrous. I greatly thank my degree coordinator **Mr. Patric Granholm** for his unending support and flexibility during my entire study years and especially for the rough periods I inevitably experienced.

Getting through my thesis required more than academic support. Most importantly, none of this could have happened without my family. My mom, dad and sisters, who offered their encouragement through phone calls every week despite my own limited devotion to correspondence. It would be an understatement to say that, as a family, we have experienced some ups and downs in the past three years; however with their own brand of humor, they have been kind and supportive to me over the last several years and my entire life. Every time I was ready to quit, you did not let me and I am forever grateful. This thesis stands as a testament to your unconditional love and encouragement. My deepest gratitude extends towards my dear girlfriend **Johanna**, who persistently pulled me together with her love and care for my perseverance to complete this thesis.

I have many people to thank for listening to and, at times, having to tolerate me over the past year. I cannot begin to express my gratitude and appreciation for their friendship and encouragement; **Mangesh**, **Jouni** and **Nipoon** have been unwavering in their personal and professional support during the time I was endeavoring for my thesis. For many memorable evenings out and in, I must thank everyone above as well as **Bishwash** and **Rupesh** for their interminable support.

You all are the best!

CONTENTS

LIST OF ABBREVIATIONS (OR) SYMBOLS

FIGURES

TABLES

ACRONYMS, ABBREVIATIONS (OR) SYMBOLS

EURODAC	European Dactyloscopy
IAFIS	Integrated Automated Fingerprint Identification System
FBI	Federal Bureau of Investigation
DET	Detection Error Trade-off
NSA	National Security Agency
DoD	Department of Defense
DARPA	Defense Advanced Research Projects Agency
CRAM	challenge/response authentication mechanism
AES	Advanced Encryption Standard
SDK	Software Development Kit

1. INTRODUCTION

The human body is a sophisticated design, full of every required sense for identification, verification and authentication; and it is always on the verge to be understood in a greater extent. It is a complex structure, a splendid work of art, an ineffable allure and so vividly immaculate that it holds a true nature to remain an enigma for each and every single of us. For hundreds of thousands of years we, human beings, have been keeping up with endeavor in the hope of exploring ourselves and our inner secrets. Thus, the human body and its performance scope have been uncovered on a regular basis in order to maneuver the performance for its own greater purpose and betterment.

We humans have always used our natural instincts and the existing sensory organs within us to identify and authenticate others around us, be that living beings or non-livings. As the development of Information technology and the digital world escalates, the increased level of forgery practices and the successful establishment of dishonesty, distrust and deceptions among us has sky rocketed immensely; moreover, such activities have become natural survival instincts/techniques for some people. Thus, it is because of such array of participations in deception, it has now become an inevitable assignment for every single human being to correctly distinguish the person as to verify whether a person is truly and precisely herself/himself when one claims who she/he is. Hence, while entering the digitized world of authentication and verification, one is essentially introduced to biometrics.

The Greek words “bio” and “metrics” mean “life” and “to measure” respectively; this is where the word biometrics is derived from. The term “biometrics” in computer science is a basic way of defining the process/form of identifying and authenticating a person with minimal probability of error occurrences or no error, based on some precise and unique traits available in a human body. According to Free Dictionary, “biometry is the practice of digitally scanning the physiological or behavioral characteristics of individuals as a means of identification and verification, and the analysis of such biological data using mathematical and statistical methods”.[1] As the definition suggests, any biometric traits that belong to the aforementioned two categories are unique to every individual. The latter part of the category, i.e., behavioral characteristics is often widely accepted and termed as BEHAVIOMETRICS.

Despite the broad area of biometrics, this thesis will be particularly focusing on multi-biometric remote authentication protocols and the templates and their protection. The flow of this writing is initiated by presenting the short history of Biometrics in Chapter 1. Chapter 2 includes application areas; similarly Chapter 3 presents the details of various

templates being used and also those under development. Two different types and the performance metrics are described briefly in Chapter 4. Chapter 5 discusses the vulnerabilities of biometric systems and few schemes as to counter them; with the motive to protect templates. A proposed remote authentication protocol is mentioned briefly in chapter 6. Chapter 7 describes the issues of multi-biometrics remote authentication and finally Chapter 8 and 9 contain the conclusion and the future works respectively.

1.1 History

Based on few evidences collected, the use of fingerprints as per identification has been traced back to as early as 500 BC while Babylonians included the use of fingerprints in their business transactions which were recorded in clay tablets as to affirm correct identification and verification. Similarly, there is evidence around the same time period of the use of fingerprints by Chinese and Egyptians, too. However, it was no earlier than the mid-1800s that, the rapid use and development in biometrics started to escalate in different cities and countries around the world. This was because the involvement of a larger amount of people in industrialization and the need to avoid forgery and deceptions. According to the biohistory [2] presented by National Science and Technology Council (NSTC), the field called anthropometrics, originated in France, which successfully measured various body dimensions such as height, arm length or any other parameter was adopted and also the formal use of fingerprints in mid 1880s was adopted as to confirm the identity of an individual. Later in late the 1880s, fingerprint indexing, which was called Henry System, was developed by Azizul Haque in India; named after the then Inspector general of Police in Bangalore, India.[3] Although, the emergence of use of biometry can be traced back to centuries ago, the true development of it coincides with the birth of modern computer technology, which basically escalated in the late 1990s and simultaneously the daily use of biometrics was adopted and accepted for general purposes and daily application.

However, since the research and development in biometrics traits has been an on-going process, there are discoveries of newer and stronger traits which could be used more reliably in identification and authentication purposes. Because of this reason alone the traits already in use for such purposes are not confined to define and limit the biometrics traits. The basic biometric traits are as shown in the Figure 1 below.

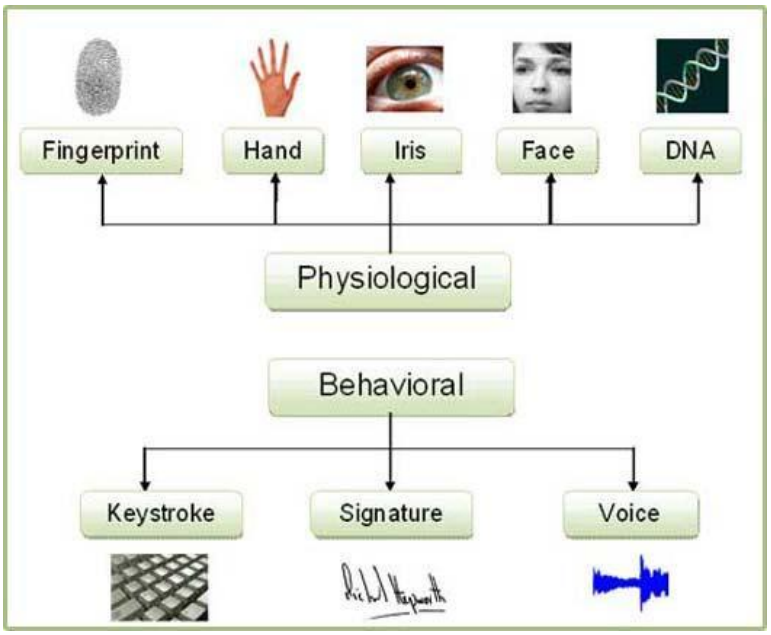

Figure 1. Biometrics traits. [3]

With such a huge progression, many countries, business giants, small business and individuals all over the world have implemented the biometrics security systems for avoiding forgery and deceptions. The various fields which increasingly use biometrics technology for example are airports, grocery stores, hotels, some theme parks etc. Below attached figure shows the approximation of the countries using biometrics technology in various fields of authentication:

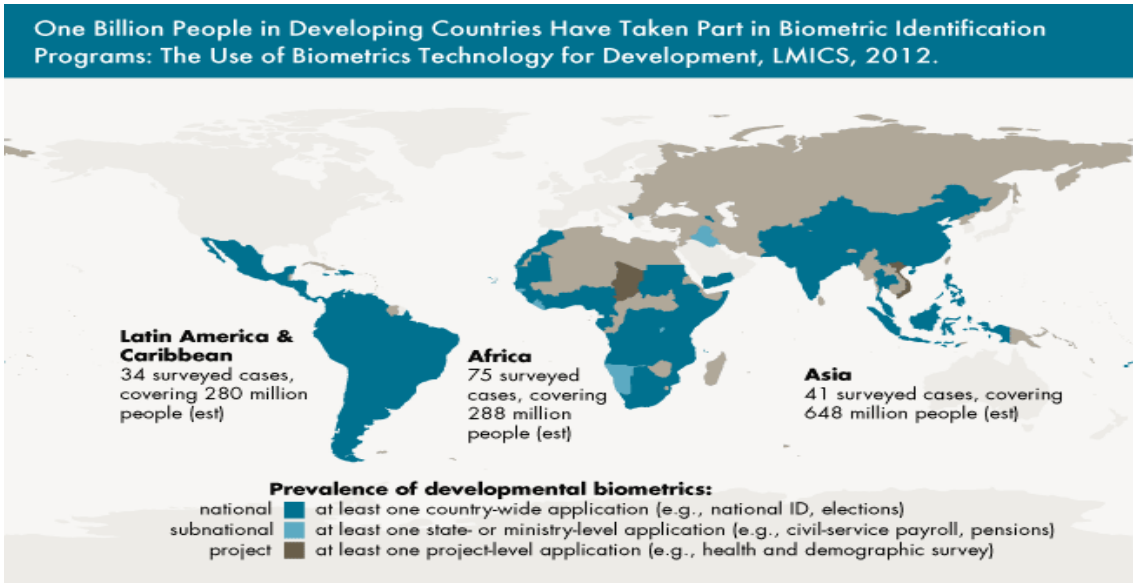

Figure (2): Approximation of countries and people implementing biometrics technology [39]

2. WHY BIOMETRICS

The traditional way to make and believe that something is secure and private is the use of passwords, keys and locks which come in various modes and functionalities ranging from mechanically manual to electronically automatic. However, the keys and passwords we buy and create have the possibility to be lost or forgotten, relatively easily. Biometrics systems eliminate such hazards and risks, make the optimum use of what we have integrated within our own body as our organs and parts, also which successfully defines and represents us, just us. It becomes easier to understand the significant need for biometrics when an individual loses her/his password which sometimes cannot be retrieved. As it is put in the article published by PBworks, " Aside from what's known as "logical" use—using a finger scan or another type of technology to determine if a user is allowed to access information—biometrics can also give appropriate people access to a school building or area. Biometrics isn't just for inside walls, either. Banks are looking at the technology to replace cards and PINs at ATMs. There's potential for using biometrics to verify payment in online purchases." [6]

Moreover, PBworks defines the gravity of the requirement of biometrics with a very practical example through a research conducted among the students and the teachers in a school in Stockholm. Focusing on the problem of password remembrance and the exchange of user names and passwords by students, Kvarnby School implemented a finger print logging system for every users which in total is numbered to 450. This had made the login process safer and easier and also proved to save 50% classroom time of a 40-minute lecture. [6]

As mentioned above, it is not only the ease of use that is the purpose of biometrics, it is also the elimination of expensive (some password creation, configuration and maintenance company has their price limit to $350) and overwhelming passwords (every of us who use online services, and digital devices has more than 5-10 passwords, and it becomes harder and harder to remember and determine the safety of passwords themselves) has become inevitable as the number of forgery, identity theft and nefarious activities increase every day. The overwhelming number of passwords will eventually lead an individual to write the password to some other devices which can be intercepted or hacked, or even the passwords sometimes are written in papers which has a high probability to be stolen or lost. Biometrics, in some level eliminates the use of paper while saving the passwords and aids in minimizing the access use of papers. Along with these benefits, biometrics helps in increasing financial accountability, physical security such as any kind of possessions, building entrances can be controlled and keep the flow as desired by the owner.

Since a biometric authentication system uses the binary code of an electronically stored unique and specific biological, physiological or behavioral characteristics called biometric template, of an individual, which is later compared with the templates present

in each and every individual while logging in or requesting for an access, it cannot fall prey to hackers and/or be lost, guessed by anyone, or be shared by anyone else.

2.1 APPLICATION AREAS OF BIOMETRICS

Applications of biometrics can be very diverse; the limitations can only be the imagination of an individual. It has become so manifold that different templates are being used in different areas for various types of functionalities. Below listed are the few applications of biometrics in different sectors:-

- Homeowners are facilitated by biometrics safes and biometric locks, which enable the highest security and reliability.
- Entrances of small offices or big organizations, residential, institutions and government can be secured greatly with the use of biometric access control systems.
- Implementation of biometrics in financial services such as ATMs, kiosks, bank account registration helps individualize and keep the privacy private.
- In areas like Social Services and Health Care, biometrics can prevent fraudulent entitlements and strengthen the medical records' privacy.
- In electronic devices, such as smart phones, tablets, phone cards, personal computers, network access, accessing and logging into internet can be made hugely private and secured.
- Biometrics is widely used in law enforcement for example, personalizing driver's license, controlled identification in correctional facilities and prisons, smart guns, confinement of home and apartments, investigating, identifying and authenticating criminals with high accuracy, enhanced airport security. [7]

As a means to control irregular and illegal border-crosses and the asylum applications, EU member states have enacted a scheme which requires registering fingerprints of every individual older than the age of 14 years which are sent to a central unit at the European Commission in digital form. These registered fingerprints are then automatically checked against other prints on the database to validate the non-ubiquity of the applicants received. European Dactyloscopy, abbreviated as **EURODAC**, is the European database which holds the entire fingerprint for identifying foreign individuals. [8] Similarly, the Integrated Automated Fingerprint Identification System, abbreviated as **IAFIS** is the largest biometric database in the world, maintained by the Federal Bureau of Investigation (FBI) which holds fingerprint and criminal history.

The variation of applications put forward above, shows the versatility and wide range of usability of biometric systems which is not limited to any individual

usage nor is it only for the legal purposes; it is everyone's tool to ensure Right to Privacy act and true identification practice. That shows a serious application for government to conduct its policy neatly for the people and by the people.

3. BIOMETRIC TEMPLATES

Through an irreversible process, the samples features which are extracted during the enrollment and acquisition phase are converted into TEMPLATES. Templates are created to facilitate the Storage and Matching phases during future log-ins and verifications. Templates can be centralized and thus be stored in a database or also be stored on a smart card which is decentralizing. Biometric templates are also referred to as biometric traits. Various biometrics templates have been deployed or pilot-tested in public and private organizations, by the government, or the people who seek to acquire highest security measures. With the emerging market and the realization of necessity of secure environment, the development in the security and privacy field is inevitable, and thus various studies for uncovering the unbreakable security trait have become a required consistency to be maintained.

The ongoing research and findings have uncovered several traits to biometric security, categorizing the traits themselves to two parts in accordance to the involvement in acquiring them: Contact Biometric Templates and the Contactless Biometric Templates. As the name of the category suggests, Contact templates require physically touching the sample acquiring device whereas Contactless templates do not include touching any devices. Few of the devices use sensors, whereas others use camera of different types and functionality depending upon the category chosen to be used for acquiring the templates. Below are some already developed and in use traits along with some under-developed traits.

3.1 Contact Biometric Templates

3.1.1 Fingerprints

Fingerprint patterns are one of the oldest methods used by humans to distinguish one from another individual with certainty. This means of authenticating and verifying an individual to prove that she/he really is who she/he claims to be is still in use digitally with complex algorithms and cryptography.

Our fingers have a Friction Ridge Skin (FRS) which acts as a friction for grips. FRS does not change with time unless it experiences a major permanent wound or scars. The FRS is arranged in a unique way in every individual. The characteristic of FRS are categorized based on its flow as: arch, whorl and loop as shown in the Figure 3 below:

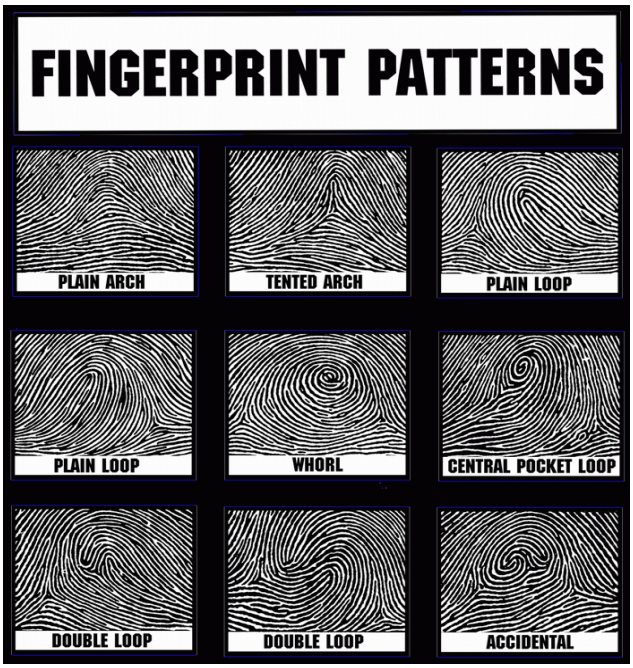

Figure 3. Arrangements of FRS in a finger. [40]

These arrangements of whorls, loops and arches are converted into digital images by using different types of sensors. There are various types of sensors: Optical sensors are the ones which use specialized digital cameras to capture an image of the fingerprint and can be successfully stored as a template. Ultrasonic sensors use the ultrasonography principles, i.e., very high frequency of sound waves are penetrated in the epidermal layer of the skin to get the visual image of fingerprint. Based on the dermal and epidermal layer of the skin which is electrically conductive and non-conductive which acts as dielectric respectively. Capacitance sensors use the principle of capacitance to form a template of a fingerprint. The ability of storing an electric charge of any matter is called capacitance. [32]

Later, once the templates are obtained, algorithms such as pattern-based algorithms are used to compare and authenticate an individual correctly. However, despite the confidence build up for correct identification via fingerprint, evidently there have been failed identifications in various cases. For example, as ABC News reported that in Japan, a 27-year old deported woman named Lin Rong had been reported to sneak back to the country by surgically swapping her fingerprints from one hand to another. [33] This led her to successfully pass through the checkpoint and increased the chances of fingerprint security compromisation.

3.1.2 Palm Prints and Footprints

Palm prints and footprints have the same logic as the fingerprints do. The benefits of using these two traits instead of fingerprints is that these are greater in size and thus can successfully help yield a greater number of minutiae points

to be used for comparison against the stored templates in system, during the authentication and verification procedure.

Palm print recognition involves three visible groups of marks present in one's hand namely: first, geometric features which simply includes the length and area of a palm, second, line features, principal line and wrinkles where features such as the depth, position, length and size of the lines and wrinkles are measured, and third is minutiae which are similar to fingerprints [34]. Templates of palm prints or footprints are obtained by using similar sensors as used whilst collecting templates for fingerprints. A picture demonstrating a scanner scanning a palm in Figure 4 for various features such as lines, wrinkles, minutiae is given below:

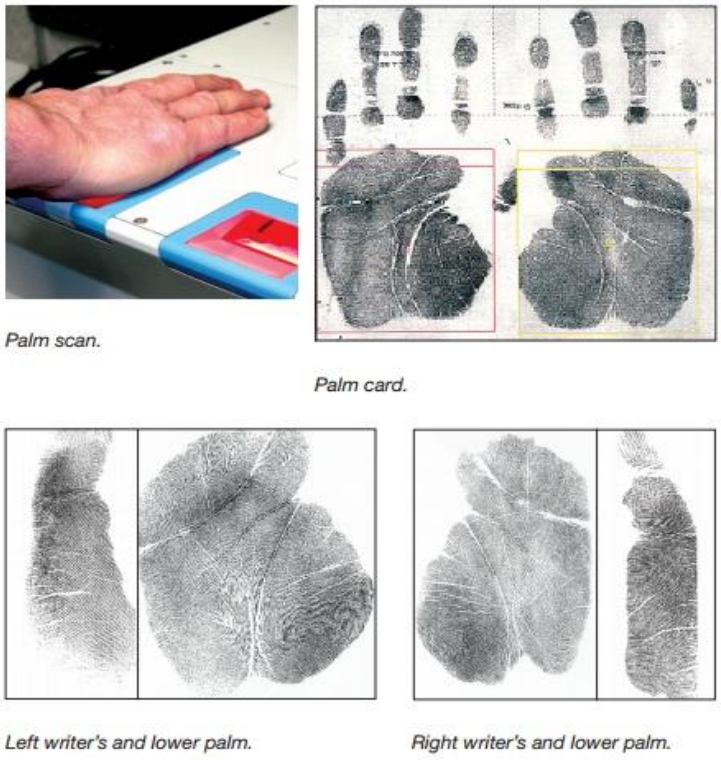

Figure 4. Palm print used for biometric authentication. [41]

However, the demerits are as fingerprints can be swapped and copied via various mediums such as soap, a glue tape etc., palm print and foot prints also can be imitated in a similar manner which raises the question of them being a secure means to verification.

3.1.3 Dynamic Signature Verification

Dynamic signature verification uses an electronic display surface where an individual uses a stylus to write in or in this case to provide a signature of his

own. It is an automated method used for verification that includes examining the dynamics of signature providing procedure, such as speed and direction of writing/signing; the pressure on the surface while signing; the total contact time spent between the stylus and the surface; the total time taken to sign in; and also gathering the high pressure points and low pressure points data onto the surface. Although, it is considered a good feature to have the signature examined and digitally recorded, DSV is the least reliable method for confirming identification. This is because the forgers have developed myriad methods to reproduce a similar looking signature. Figure 5 has an example of DSV:

Figure 5. Dynamic Signature verification using stylus and a sensor surface to sign digitally. [42]

3.1.4 Keystroke Dynamics

Keystroke Dynamics is a field of biometrics where the system examines several dynamics of typing of an individual. Almost similar to Dynamic Signature Verification, it tests the speed and pressure applied by a user while stroking certain keys, time spent by the user to type a certain word or a password and the time between typing certain keys. This technology could be successfully used in authenticating a computer user's identity and providing the access. Although, this technology is considered as a biometric technology, it is still an ongoing subject to perfect its distinctiveness and robustness during correct identification and verification. To mention its weakness, some software have been developed which hold the capability to record the keystrokes and can be used to falsely by-pass the security system.

3.1.5 Palm (Hand)/Finger Geometry

Hand geometry is another field in biometrics systems which includes hand and fingers but does not acquire prints from them. Here, the user lays her/his hand on the surface of the sensor which has the guiding poles for proper hand placement; these poles lie in

between the fingers before the reading process is initiated. However, finger geometry uses only 3-4 fingers. The spatial geometrical measurement of hand and fingers is done as the lower level of a hand is a unique trait for every individual. This system has a lower accuracy rate than other biometric systems but also has very low false reject rate. Many users find this system easier to use and thus gaining user acceptance, this technology has been already beta-tested and applied successfully in various fields for physical access control such as for San Francisco Airport employees' attendance system which includes around 3000 enrollees. It is also implemented in various small and large business offices.

Although hand geometry has been adopted and used in many areas already, this technology is not considered completely suitable for identification applications; this is because of its low degree of distinctiveness. However, the continuous development has gained some more refinement in the procedure which might, in the future, lead to a greater use of it such as in remote authentication over the internet. Figure 6 displays a device developed by Ingersoll Rand Security Technologies. This Schlage HandPunch hand geometry reader has the functionality to read 31000 points of a hand and recording capacity of 90 separate elements of an individual's hand which are used for verifying a person's identity [11].

Figure 6. Schlage HandPunch hand geometry reader. [11]

Furthermore, the weaknesses of hand geometry includes its failure to being ideal for children, jewelry marks may pose difficulties in gathering the templates and since the size of the template data is so large that it is rarely possible to use in all embedded systems. [43]

3.2 Contactless Biometrics

There are many traits that can be acquired and used by a biometric technology for identifying an individual which do not require physical contact with the devices being used. Below mentioned are some of the traits used.

3.2.1 Voice Recognition

The voice recognition technology is a method of verifying an individual which uses the vocal characteristics of a person by acquiring and examining her/his vocal properties using a password or a pass-phrase. Since this technology uses a telephone or a microphone as a sensor, it is proved to be the cheapest method of identification and verification of an individual. Although it is not yet clear whether the system scrutinizes the pronunciation or it actually recognizes the voice of a person, various telecommunication industries and the National Security Agency (NSA) have continued their work in developing and refining this recognition system to ensure the reliability. There are some drawbacks in using this technology, which are mainly caused by the background noises while recording a voice, voices can easily be recorded and used as false identification, overlapping speech and homonyms [35].

3.2.2 Facial Recognition

Similar to hand geometry, facial recognition uses spatial geometry to distinguish various unique features of the face. This technology includes the use of camera to acquire the key features of a face and analyze it for identification and verification. Although this technology was once a popular method in biometric identification, there are several negative points which suggest weak performance. The images taken for templates can be hugely affected by the surrounding factors, such as lighting whilst capturing an image, the pose and orientation of face, hair, any facial expression, illumination and also the fact that the human face changes with time. Further, the invention and development of more complex algorithms can successfully masquerade human faces, such as an algorithm developed by a researcher at the University of Ottawa. It is an exploit algorithm which can regenerate a face from a high quality image of a person from the templates being used. [12]

Because of such possibilities of being exploited and also the high presence of EER from 1.3% to 13%, facial recognition has been discarded until some measure of perfection and accuracy is obtained. However, because of the simplicity and certain level of user acceptance, an intensive research was conducted which was sponsored by Department of Defense (DoD), the Defense Advanced Research Projects Agency (DARPA) and the National Institute of Justice; this study concluded suggesting further research and development in the field. Based on so much negative criticism, facial recognition has slowly been

depleted from everyday use for identification and with its mundane state it has ended up being more of an entertainment purpose.

3.2.3 Facial Thermography

Facial thermography deploys an infrared camera which successfully captures the heat patterns emission which is generated by the vascular system of the face. These heat patterns, also known as aura, are the heat which passes through the facial tissues of an individual and are unique to every human being. Since these auras are a repeatable process, it is possible to convert them to digital data and store in the database as a template and use as comparison trait for authentication and verification. [44] The benefit of facial thermography over facial geometry is that the auras do not change over time. Below is a pictorial representation of a thermal image captured by using an infrared camera:

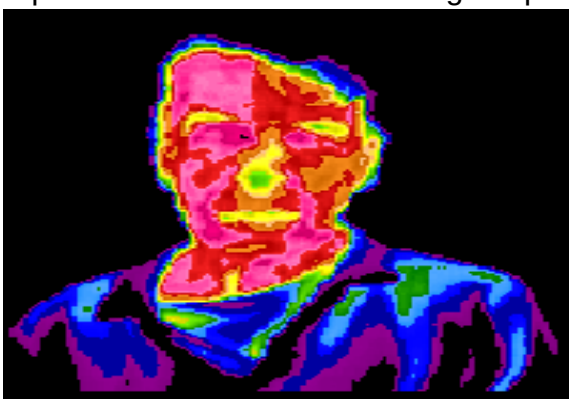

Figure 7. Depiction of facial thermography. [44]

However, on the weak side, the accuracy of facial thermography has been found to depend on the ambient temperature and various physiological and psychological conditions leading into declination identifying the correct individual whilst verifying.

3.2.4 Retinal Scan

Retinal scan was once a very popular method adopted for identification, which measures the pattern of blood vessel in retina or the back part of the eye. Blood patterns in retina are not genetically affected, thus resulting in being completely unique from one individual to another, even within twins. The device that measures these patterns requires a user to stand still within inches of the device which has a shining light source. However, over the time, as the knowledge of weaknesses of retinal information became public, the user acceptance rate has become really low. This is because the scanning device is rather expensive and not user friendly. In addition, it can change with body condition and diseases, such as high blood pressure, pregnancy, cataracts, astigmatism and AIDS [45].

Because of the intrusive perception developed by users, it has lost its popularity. A picture of blood vessel in retina is given below:-

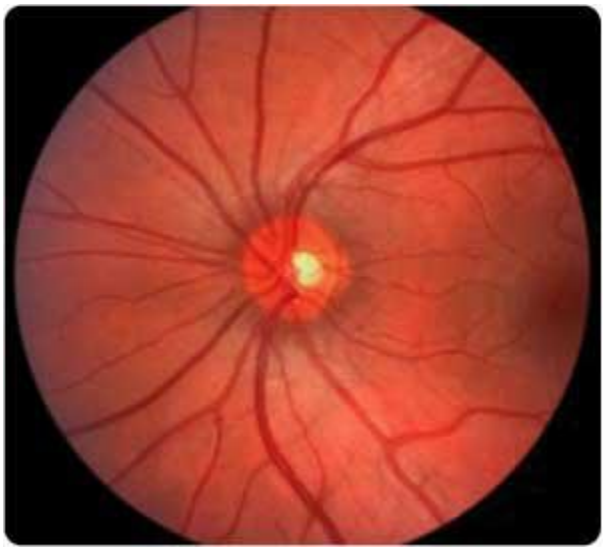

Figure 8 Blood vessel in human retina.[46]

3.2.5 Iris Scan

As the uniqueness of iris is collectively well known, the iris scan has become the most widely endorsed and most accurate biometric template for verification. As a result, many high profile industries have developed high quality iris scanning and identity verification products. Except for papillary response to light, the iris is not influenced by any environmental and surrounding factors; it is also one of the unchanging organs of one's body. Since, iris patterns are formed in complete randomness and have stable random texture, no two iris patterns match each-other; they even differ from left eye to right eye.

For scanning purposes a simple charged-coupled device (CCD) digital camera is used which uses near-infrared light and visible lights to capture a high contrast distinctively clear picture of an iris. The iris turns into dark black color, due to which the camera can distinguish and isolate iris from pupil. Once the camera is focused on the iris, it then locates and captures images of the center of the pupil, the edge of the pupil, the edge of iris and the eyelids and eyelashes which are converted into digital data as to be used as a template. Such templates provide 200 reference points to compare and verify [37]. A schematic representation of an iris is given below:-

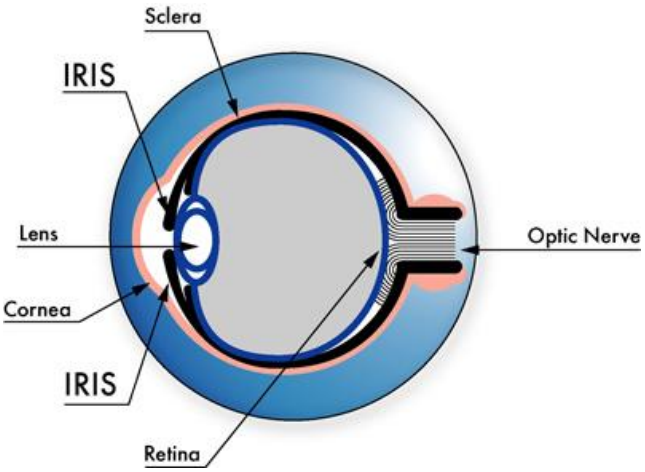

Figure 9. IRIS [36]

From the wide realm of iris applications, few of them already in everyday use are: ATMs also termed as Eye-TMs, Airport physical access, grocery stores use it for checking out, hotels have adopted iris scanning for better authentication and facility; and many companies and industries are increasingly considering to adopt iris scanning system for better count and saving time.

However, as it is a fact that no system can be totally flawless, iris recognition has the following weaknesses[48]:

- A detailed and sharply clear picture can be used to gain access by fooling the scanner.
- Iris codes can be reverse-engineered to create the templates.
- Iris scans cannot often be used for people who are blind and also those who suffer from color blindness.
- Setting up the scanning devices may be expensive, although the applications available for some smart phones lack accuracy.
- Bright or visible illumination reduces the image quality [49]
- The scan can be obscured by eyelashes, lenses, reflections[49]

As an example, researcher Galbally has been able to forge a real iris which was validated by 80% of the commercially available iris recognition systems. Airports in Manchester and Birmingham have stopped using iris recognition systems because they consume long usage time to validate and resulting into a loss of GBP 9 million [47].

3.3 Emerging Biometric Templates

As the importance and credibility of secure security system has been realized every day, the inevitability of advancement and development in biometrics system templates has been a vital field to explore. This research and exploration has been conducted on a continuous basis to refine and find the unbreachable traits for identification and verification. Below mentioned are some of the traits found and conducted beta-tests in small periphery.

3.3.1 DNA

The use of Deoxyribonucleic Acid (DNA) focuses mostly on the nitrogenous bases referred to as "bases" which are distinct and named as: Adenine (A), Cytosine (C), Guanine (G) and Thymine (T). DNA has been represented as a twisted ladder in a spiral; each molecule is made up of nucleotides which consist of *a sugar molecule, a phosphate molecule and a nitrogenous base.* It is believed that the accuracy rate by using DNA is 99.999%. DNA templates are acquired by professional lab technicians by using restriction enzymes and splitting the DNA into two separate parts. Although recognition via DNA sounds rather unique and plausible security means, it has its own complex weaknesses; the process of validation can be lengthy and-time consuming and also requires a calculation of complex mathematical algorithm which can only be calculated by high powered computers. Along with that, it fails in distinguishing monozygotic twins distinctively [15].

3.3.2 Vein Pattern

Vein pattern method uses the radiation of near-infrared rays which can capture the vascular pattern image of an individual and it offers vast level of accuracy which is 0.01% of FRR and less than 0.00008% of FAR. [16] This technology has been adopted by many Japanese banks for identification and verification since 2004. Vascular patterns are unique to each individual including the twins. There is almost no possibility of stealing any vascular pattern because these veins are inside the body and can only be obtained by using the two methods for photographing veins, namely: **Reflection** and **Transmission**. According to Fujitsu, *"The reflection method illuminates the palm and photographs the light that is reflected back from the palm, while the transmission method photographs light that passes straight through the hand. Both types capture the near-infrared light given off by the region used for identification after diffusion through the hand" [17].* Despite the minimal rate of error and being non-intrusive, vein pattern recognition has various flaws such as the noises appearing in the captured image because of the camera calibration and focus, humidity level, heat radiation of the body, temperature of body, closeness of vein to the surface of skin, not readily available in consumer market and its costly nature at the moment.

Figure 10 is the demonstration of vein patterns of a hand being scanned to capture a template:

Figure 10. Scanning vein patterns to bring up medical records in hospital [18].

3.3.3 Brainwaves

Basically brainwaves can be altered by any humans by the consumption of various drugs and other elements. However, the pattern used for authenticating in biometric is baseline brain-wave patterns which are not possible to be altered by any means [55]. This technology can be very well used by the mobility challenged people such as amputees, quadriplegics and paraplegics. According to *J. Gunkleman,* "Brainwaves resolve into nothing more than recognizable patterns. If we could identify at least one pattern that was unique, unchanging, and monotonous, then we would have a security protocol of peerless supremacy" [55]. Although there still has to be made a tremendous amount of development in using brainwaves as a security measure, it remains a potential template for authentication purpose. As the protocols and algorithms have just been proposed and not been tested for its pros and cons, it would not be the very best idea to jump into conclusion as to determine the integrity of brainwave identification for a new paradigm of security measure.

3.3.4 Body Odor Recognition

Dogs have been used to identify a person based on her/his odor. Similarly, as digitization of all things moves forward, sensors developed by University of Cambridge are capable of capturing and analyzing the olfactory of a human body scent from non-intrusive body parts like hand, which are extracted by the

biometric system and used as a template and authenticating means by converting those chemical properties into a unique data string [50]. Body odor recognition is one of the under-addressed biometric traits which yet hold a strong notion to identification. Pointing out its merits and demerits is still required to be confirmed by researchers, as its development and usage is rudimentary so far.

3.3.5 Fingernail Bed Recognition

The unique longitudinal structure present under the fingernail has parallel vascular rich skin rows along with the parallel dermal structures. This structure between the narrow channels can be used as a biometric template. The template is acquired by using an interferometer which detects the back-scattered light which is shone on the fingernail, which in return yields in construction of one distinct map of a fingernail bed [50]. This trait as well is in its rudimentary form, is still being tested without conclusive merits and demerits.

3.3.6 Body Salinity Identification

Human body becomes more conductive to electricity with the rise of salt level in it. This means that the human body can also carry data at a transfer rate of 2500-baud modem. This feature can be used for the communication between the devices such as watches and cell phones and the human body. With this characteristic, it is possible to acquire at the template based on body salinity level. [50] The drawback of this is that the body salinity is a consistently fluctuating feature, which suggests that if the salinity level is different at the time of identification than the time when template sample was acquired, correct recognition will fail.

3.3.7 Ear Pattern Recognition

A French company has developed Optophone which is like a telephone handset and it consists of two components namely; lighting source and cameras. Our outer ear's lobes, bone structure and the size are unique to every individual [19]. Along with that, human ear has various other features which can be used as biometric template for authentication. This method basically has three means of identification, namely [38]:

- Image of an ear
  This method includes comparison of images of ears. As suggested by Alfred Iannarelli, the distance between each physiological features of an ear shown in Figure 14 are measured and assigned an integer distance

value. Based on the acquired distance, the recognition is obtained. However, this method poses a distinct weakness of being erroneous if the first distance point is not defined accurately then the whole recognition procedure will go ashtray. Thus, in 1999 Moreno et al. proposed a new method of comparison which includes obtaining macro features, wrinkles and the whole ear shape.

- Earmarks
  Earmarks are obtained from videos, photographs or by pressing the ear against materials such as glass which accepts the marks of ear that can be used as biometric template. However, this method has been cumulatively discarded as it is considered as not dependable.

- Thermogram images of the ear
  As an intention to minimize the errors caused by hair present in ear, thermal images are used which helps easily mask out the hair from image to be compared. Different colors and textures are used to represent different parts of the ear.

Figure 11 is a brief demonstration of human outer ear and its various physiological features:

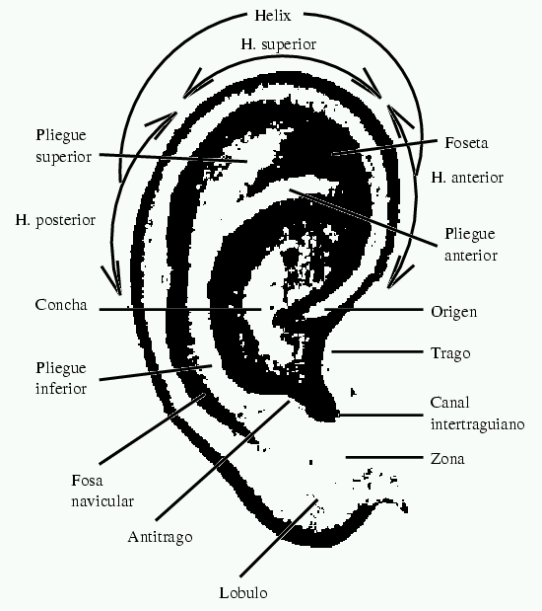

Figure 11. Outer human ear [38].

However, since the human ear changes with age, and the gravity [38] can cause stretching of ear, it is less likely to give the accurate identification; which leaves it as yet another trait to be corrected cumulatively as to eliminate errors.

Along with the above mentioned possible templates, Infrared Fingertip Imaging and Pattern Recognition which works similarly as Facial Thermography and the Gait Recognition which measures a person's manner of walking, can also be potential biometric templates.

4. Biometric Systems: Types and Performance Metrics:

All the biometric systems usually have four stages to be completed; Enrollment, Acquisition, Storage and Comparison for verification. Although, the four stages are required for a successful completion of complete biometrics phases, these four phases work in six detailed steps [50]. They are:

- Acquisition of a sample: A sample biometric data must be collected, e.g., fingerprint image capture, DNA sample, a picture for ear orientation.
- Extraction of the feature: This step includes converting the sample into numeric data, this numeric data is the template. However in some cases full images are used which eliminate the conversion of samples to numeric data.
- Quality confirmation: The quality confirmation includes the first two steps as to ensure the system has the finest template or sample for later use.
- Storage: Depending on the application, storage of the template is required if it is to be used later.
- Comparison: In this step, the comparison is conducted between the real-time input templates against the stored template(s).
- Outcome/result: This final step is directly proportional to the result of Comparison. This also often depends on the decision threshold used by the system, which might lead to the suggestion to further verification if required in accordance with the application-dependent criteria.

Depending on the threshold a biometric technology uses to determine a match or a mismatch during the verification phase, there might be two possible error occurrences: an erroneous match and an erroneous non-match. An erroneous match is the false verification and erroneous non-match is occurs when a right template is rejected. This is mostly because of the calculations and comparisons results based on the statistical nature of the acquisition phase and comparison for verification phase. Because of these errors, no biometric system/technology is 100% accurate till this day.

Along with the development and advancement in biometric technology, it has been categorized into two types/modes. The key factor that dissects these categories is just the template dependency to perform enrollment to the verification phase.A brief description is given below:-

4.1 Unimodal biometrics system

Unimodal biometrics systems use a single physiological trait such as iris, fingerprint, palm geometry etc., or a single behavioral trait such as voice, handwriting or typing rhythm of an individual. A simple process of enrollment and verification for access allowed or not allowed can be demonstrated by the below given in Figure 12.

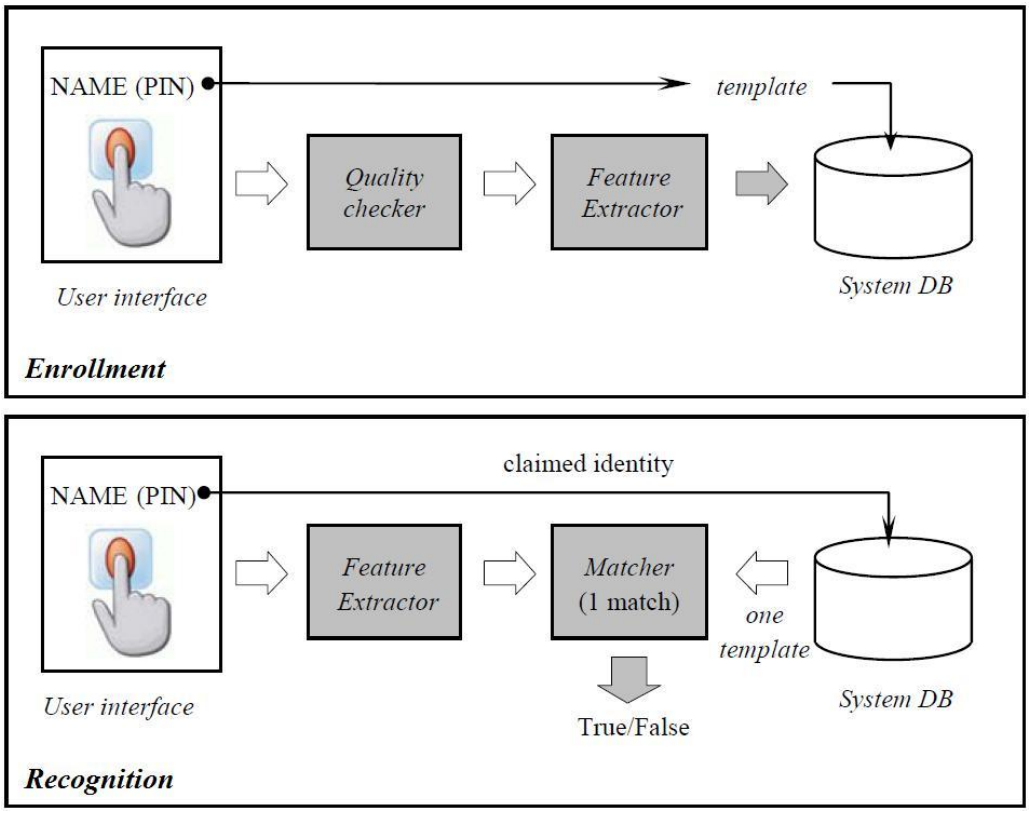

Figure 12. Enrollment and verification using biometrics trait as fingerprint. [51]

4.2 MULTIMODAL BIOMETRICS SYSTEMS:

As in the aforementioned applications of biometrics systems, EU border controls systems have implemented face and fingerprints recognition technology. In contradiction to unimodal biometrics, multimodal biometric systems use more than one biometric trait for Acquisition through Comparison phases using different mechanisms for biometric fusions. Unimodal biometric systems often fail to correctly authenticate and verify an individual with a desired outcome and accuracy. However, this problem is hugely eliminated by the use of multimodal biometric technology. Multimodal biometrics is often referred to as **MULTI-BIOMETRICS**. The below presented example Figure (13) explains the basic workflow of multi-biometrics:

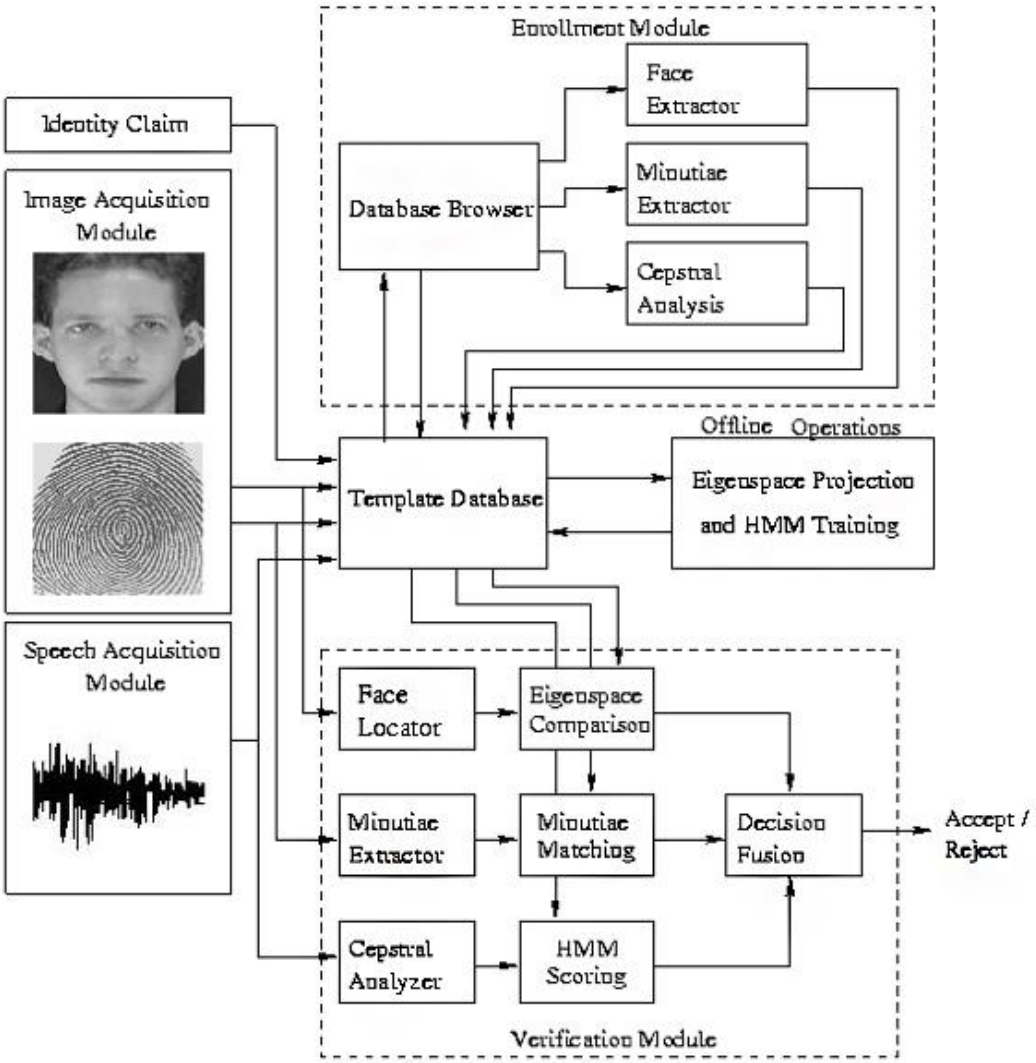

Figure 13. Enrollment and verification procedure using Multi-biometrics. [52]

The above figure demonstrates the basic workout of multi-biometrics which includes three templates; image acquisition module which processes Face recognition and fingerprint, plus Speech acquisition module.

The multi-biometrics procedure requires different points of biometric fusion which uses four basic mechanisms to correctly operate and verify. Below are the lists of biometric fusion mechanisms [53]:

- **Template Fusion:**
  Here the new biometric templates are formed by merging different forms of templates captured for fusion process using different biometrics sensors and systems. Below given Figure 14 demonstrates template fusion concept:

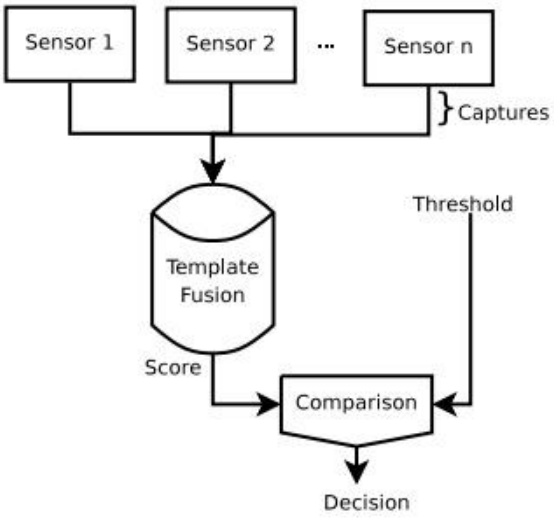

Figure 14. Template Fusion mechanism [53]

- **Decision Fusion:**
  Decision fusion includes taking different decisions given by various individual biometric authentication systems. Then combining and fusing them, the final decision is deducted.

- **Rank Fusion:**
  The method called majority vote is used to fuse various biometric templates' generated by identification systems.

- **Score Fusion:**
  This fusion mechanism considers the output generated by the classifiers to fuse the obtained templates. Figure 15. demonstrates the Score fusion:

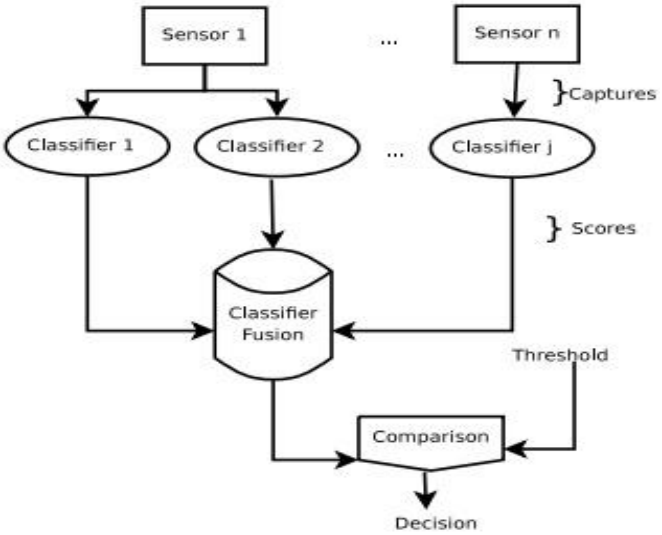

Figure 15. Classical score fusion mechanism. [53]

4.3 Performance metrics for biometrics systems

There are various vital factors for any biometric system to be operated and be accepted widely. Every effective biometric system should include the accuracy and the uniqueness of biometric organ and actions. Along with those two are throughput rate and speed, acceptability to users, ability to fight counterfeiting, data storage, enrollment time, data collection intrusiveness, requirements of system and the subject contact, and reliability. Below listed is a brief description of performance metrics used for any biometrics systems [9]:

- ### False Non-Match Rate or False Rejection Rate (FNMR or FRR)

FRR measures the incorrectly rejected percentage value calculated and performed by the system to the valid inputs. It is the probability when a biometric system shows failure performance to detect and match the input templates and a comparison template in the database.

- ### False Match Rate or False Acceptance Rate (FMR or FAR)

On contrary to FNMR or FRR, FAR is the percentage measure of incorrectly accepted input templates while comparing to the non-matching templates in the database. FAR is also dependent to the threshold value because in-case the individual is an imposter and the deducted value after comparison is higher than the threshold value, she/he is given a genuine tag, and thus granting the access as correct authentication.

- ### Half Total Error Rate (HTER)

For a given threshold value, HTER is the average value or mean between the FRR and FAR.

- ### Failure To Enroll Rate (FTE or FER)

If low quality inputs are detected, system rejects the enrollment procedure, thus FTE is a rate which is thrown out by the system whilst creating a template from an input source.

- ### Failure To Capture Rate (FTC)

Some automated biometric systems show the probability of failure to detect an input for the enrollment process even though the presented input is correct in every sense, this is termed as Failure to capture rate.

- Relative or Receiver Operating Characteristic (ROC)

The trade-off visual characterization within the FAR and the FRR is ROC. As mentioned earlier, the higher the threshold value, the higher will be the FRR rate, which in contrast is the reduction of FAR rate. This common variation is termed as Detection Error Trade-off **(DET),** which can be deduced by using the normal deviation scales on both the axes, x and y, which illuminates that if the graph is more linear, the minimum will the error rates.

- Area Under the Curve (AUC)

AUC is considered as a global way to compare the performance level of various biometric systems. It is simply the area which is covered under the ROC curve.

- Crossover Error Rate or Equal Error Rate (CER or EER)

CER is the rate of errors at which both acceptance and rejection error rates are equal. Using the ROC curves which gives the value to CER, CER is the easy way to compare the accuracy of different biometric devices. CER simply states that the lower the CER rate, the higher will be the accuracy of the device.

- Template Capacity

Template capacity is the capacity of a device/system to store the maximum number of templates in the system.

5. Biometric Template Protection:

As the world becomes digitally advanced, every communicably activated device can be accessed and modified locally or remotely; legitimately or illegitimately. The wide use of biometric security systems requires geographical distribution of the hundreds of thousands of templates acquired during the enrollment phase. Invention and development of unbreakable algorithms and cryptography has become a vital step to be embraced for the advancement of security of such templates to protect and ensure the prevention of attacks of any sort or infringement for fraudulent uses.

5.1 Biometric System Vulnerability:

The fish-bone model as shown in Figure 16 can be used to demonstrate the vulnerabilities of any biometric system and their consequences.

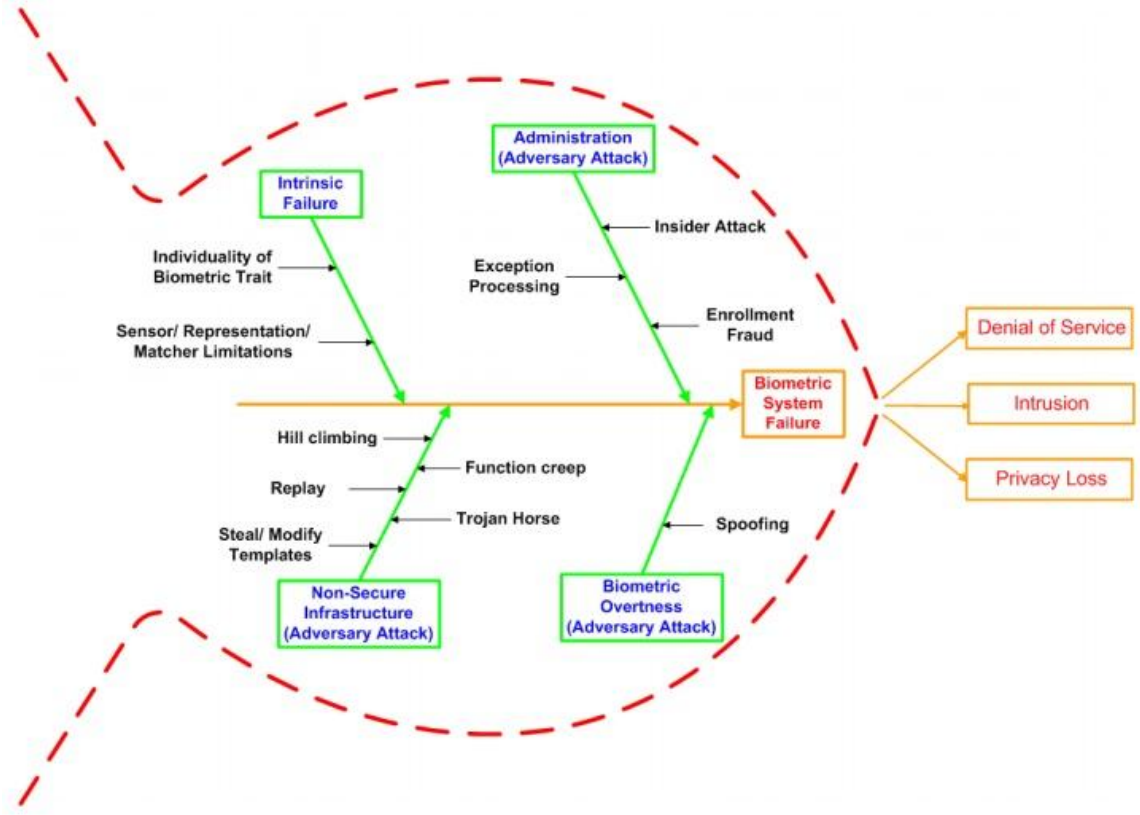

Figure 16. Fish-bone model representation of vulnerabilities and consequences. [21]

Furthermore, these vulnerabilities can be categorized into two modules: [20]

5.1.1 Intrinsic Failure:

Intrinsic failure is also often termed as *"zero-effort attack".* It is a false decision constructed by a biometric system during verification. This failure includes high false accept and false rejection rate. Most of the time, this type of failure occurs because of the failure of correct interaction of a user to the system, e.g., lighting effects and change in expression while capturing a picture, the residual left-overs on the sensor; and lack of uniqueness in the enrolled biometric template which is more common in twins. Taking these failures and weaknesses in account, continuous research has been conducted to design more reliable sensors to acquire templates with minimal errors. However, the accuracy rate depends on the target population and the environmental conditions. Table 1 shows the FAR and FRR rates in a verification system.

Table 1. FAR and FRR associated with state-of-the-art fingerprint, face, voice and iris verification systems [20].

Biometric template	Test	Test conditions	FRR	FAR
Fingerprint	FVC 2006 [9]	Heterogeneous population including manual workers and elderly people	2.2%	2.2%
	FpVTE 2003 [10]	US government operational data	0.1%	1%
Face	FRVT 2006 [11]	Controlled illumination, high resolution	0.8%-1.6%	0.1%
Voice	NIST 2004 [12]	Text independent, multi-lingual	5%-10%	2%-5%
Iris	ICE 2006 [11]	Controlled illumination, broad-quality range	1.1%-1.4%	0.1%

5.1.2 Adversary attacks

Depending on the authoritative access to the system, adversary attacks are those whose successes rely on the loopholes in the system. These attacks are categorized into three classes, given as below [20]:

5.1.2.1 Administration attack

The immature administration handling of biometric systems causes the improper registering of the templates which are affected by the collusion between the adversary and the administrations. It is not so unusual for an adversary to persuade (in a coercive manner) some member of the administration or a rightful user to abuse the system.

5.1.2.2 Biometric overtness

An adversary can successfully fool the system by creating a physical artifacts of fingerprints which are usually taken from the surface of the fingerprint scan surface. To prevent this type of attack and stop any circumventor, a system must be designed with a capacity to distinguish an artifact spoof from a live biometric template.

5.1.2.3 Non-secure infrastructure

This is one of the most occurring attack in any electronic system, thus, designing a system infrastructure to fight against various possible manipulation can solve this issue.

5.2 Countering biometric systems' vulnerabilities

As mentioned by Ratha et al. in every generic biometric system there are eight attack points. They claim that this framework can also be implemented in a password based authentication system where the input device is a '*Keyboard*', feature extractor is a password encryptor and the comparator module is the matcher. Therefore, the encrypted password database can act as the template database. The below mentioned Figure 17 portraits the idea of the team:

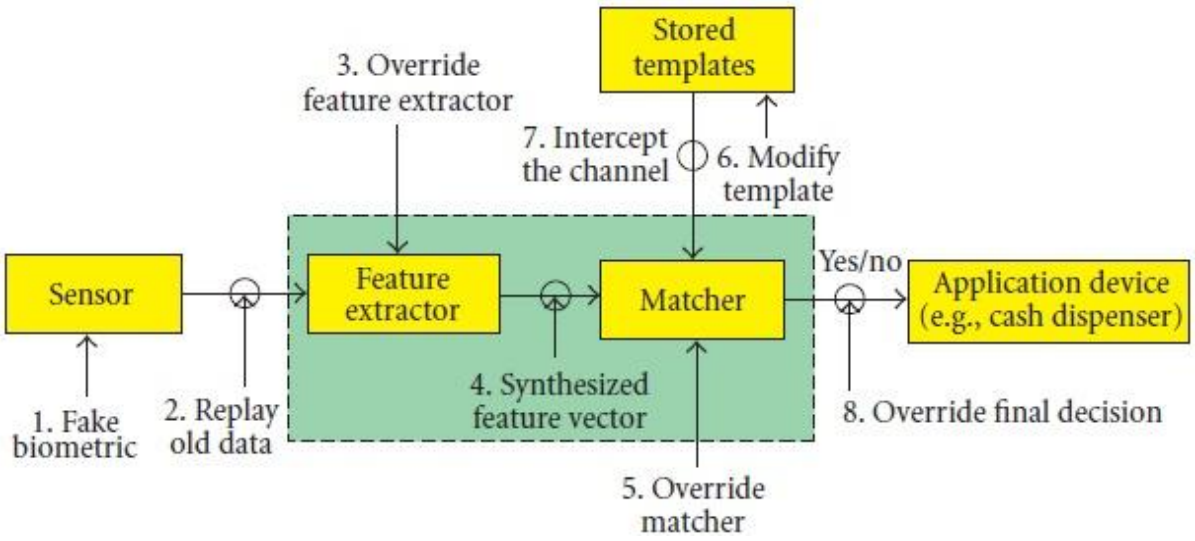

Figure 17 Attacks in generic biometric system [20].

However, in the review article published in 2007 by Jain et al., the aforementioned eight attack points has been categorized into four categories [20]:

i) Attacks at the user interface/input level
Development and innovation of the system which can correctly identify a biometric template while presenting between a live and a spoof artifact can eliminate this type of attacks.

ii) Attacks at the interface between modules
A physically and cryptographically weak system can allow an intruder to illegitimately by-pass and gain control of the templates by launching attacks such as, replay attack, hill-climbing or a brute force attack. In such cases, as a countermeasure, protocols such as time-stamps or a challenge/response authentication mechanism (CRAM).

iii) Attacks on the software modules

Attacks like Trojan-horse can be injected by an adversary so that the executable program outputs the desired values. In cases like these,

Secure Code Execution can be adopted which allows the rejection of any performance by the program other than defined in the log file.

iv) Attacks on the template database

The most damaging attack one can conduct is to attack the biometric template database. The vulnerabilities of such an attack can be devastating; a template can be stolen or replaced by an intruder so that she/he can gain an unauthorized access to the system, further-more she/he can create an artifact to spoof other systems which use the same biometric template.

As proposed by A.K. Jain et al. a secure way to protect templates would be by using smart cards or often referred to as match-on-card or system-on-card. Here, all the modules and the interfaces such as the templates, feature extractor, sensor and matcher are stored in the card; and none of these modules and interfaces leave the card which is the advantage of this system.

However, since the user is required to carry the card all the time with her/him, it has become less popular and possesses the threat to be stolen, shared and lost. This system also is expensive, and not very appropriate with the large-scale applications.

5.2.1 Multi-biometrics Template Protection Schemes

As proposed by Marco Grassi, an ideal biometric template protection should possess four properties, given as below [24]:

- **Diversity:** the secure template must not allow cross-matching across databases, thereby ensuring the user's privacy.
- **Revocability:** it should be straightforward to revoke a compromised template and reissue a new one based on the same biometric data.
- **Security:** it must be computationally hard to obtain the original biometric template from the secure template. 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.

The translation, distortion and rotation cause an occurrence of biometric intraclass variability. Due to this variability, it is not possible or safe to encrypt any biometric templates using standard encryption techniques such as AES, RSA etc. Using these standard encryptions will cause the template to be exposed during the authentication process, which increase the threat to adversary access and steal.

To cope with the above mentioned problem, Anil K. Jain et al. has proposed a biometric template protection scheme, which classifies it into two categories, namely, Feature Transformation approach and Biometric Cryptosystem. The below mentioned Figure 18 explains the brief procedure in defining the categorization:

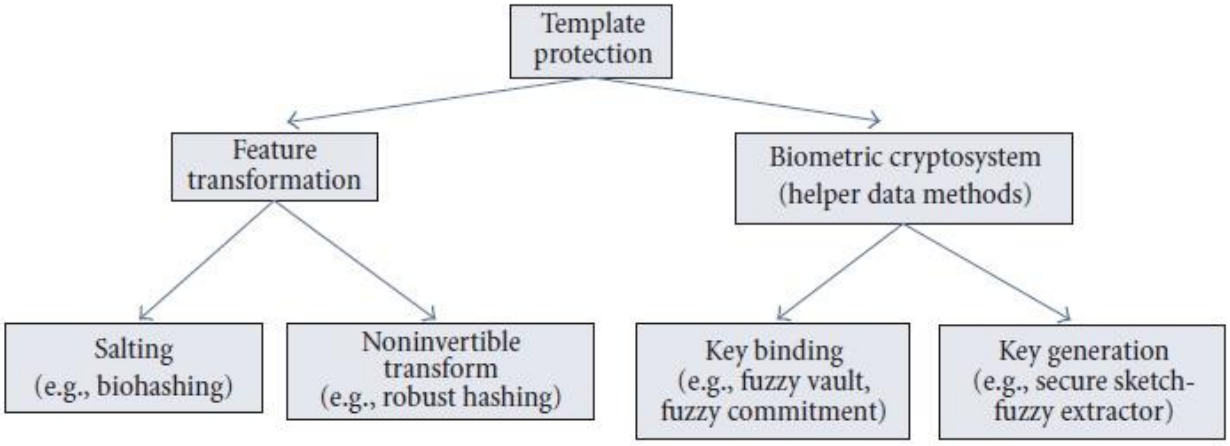

Figure 18. Categorization of template protection schemes [20].

Feature Transformation

As put by Anil K. Jain et al., “In Feature transformation approachatransformation function (F) is applied to the biometric template(*T*) and only the transformed template (F (*T*;*K*)) isstored in the database as shown in Figure (16). The parameters of thetransformation function are typically derived from a randomkey (*K*) or password. The same transformation functionis applied to query features (*Q*) and the transformedquery (F (*Q*;*K*)) is directlymatched against the transformedtemplate (F (*T*;*K*)).”

Figure 19 explains a feature transformation mechanism used to protect the template:-

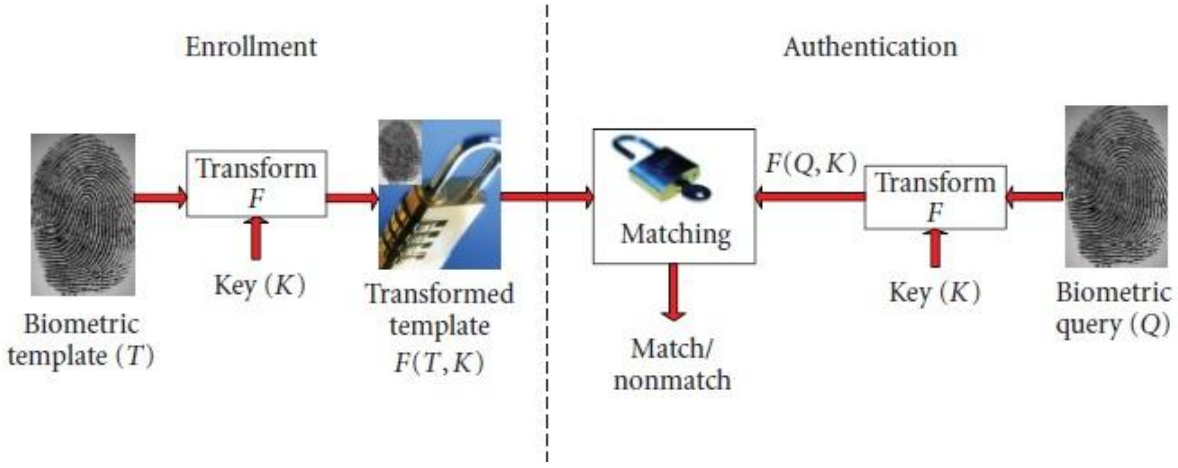

Figure 19. Authentication mechanism when the biometric template is protected using a feature transformation approach. [25]

The feature transformation can be further categorized into two classifications:

Salting

Salting (Salt) is a cryptography algorithm designed to defend against attacks such as *dictionary attacks* and *rainbow table attacks* which are pre computed. Salting is also referred to as *Biohashing;* in biometrics, “it is an approach to protect template in which the biometric features are transformed using a function defined by a user specific key or password.” [20] Here, during the authentication phase, the key or the passcode is required to be remembered by the user or it needs to be stored securely because of the invertible transformation. The *entropy* of the biometric template is increased because of the additional requirement of such keys and passcodes, which in return increases the difficulty for any adversary to guess the template. However, if the user-specific key is compromised, it is possible for any adversary to gain access and recover the original biometric template by accessing the key and the transformed template.

Noninvertible transform

Noninvertible transform uses a noninvertible transformation function which is a one-way function. Here, in terms of *brute force complexity,* even if the key (which must be presented during the authentication phase) or the transformed biometric template is obtained by an adversary, it is computationally almost impossible to recover the original biometric template for her.

Biometric Cryptosystems

Biometric templates and the raw data once lost have a disastrous outcome, they can be successfully used to cross-match through the different database for the

desired results by an adversary. Since these raw data are next to impossible to cancel when they are lost or stolen, it is important to resort to a more secure system named as Biometric Cryptosystem or *Biometric Encryption,* it is also termed as *helper data methods..* The two types of biometric cryptosystems are:

Key-binding biometric cryptosystem

According to Anil K. Jain et al., “In key-biding cryptosystem, the biometric template is secured by monolithically binding it with a key within a cryptographic framework.” The helper data stored in a database which is a single entity embedding both the template and the key makes it computationally difficult to decode the template. Here, the intrauser variations in biometric data can be tolerated which is determined by the capability of the code-word to correcting error.

Key generating biometric cryptosystem

In the context of biometrics key generation, Dodis et al. proposed the concept of *Secure sketch* and *Fuzzy extractor,* where a helper data is a secure sketch which leaks limited amount of data measured in terms of entropy loss. Still it can reconstruct the exact template if presented with a query which matches highly to the template. The fuzzy extractor is a cryptographic primitive which can generate a cryptographic key from the biometric features. However, it is a difficult task to generate such keys with high entropy and stability. Figure 20 below shows the helper data extraction and the validity check after extracted key, using the key generating cryptosystem:

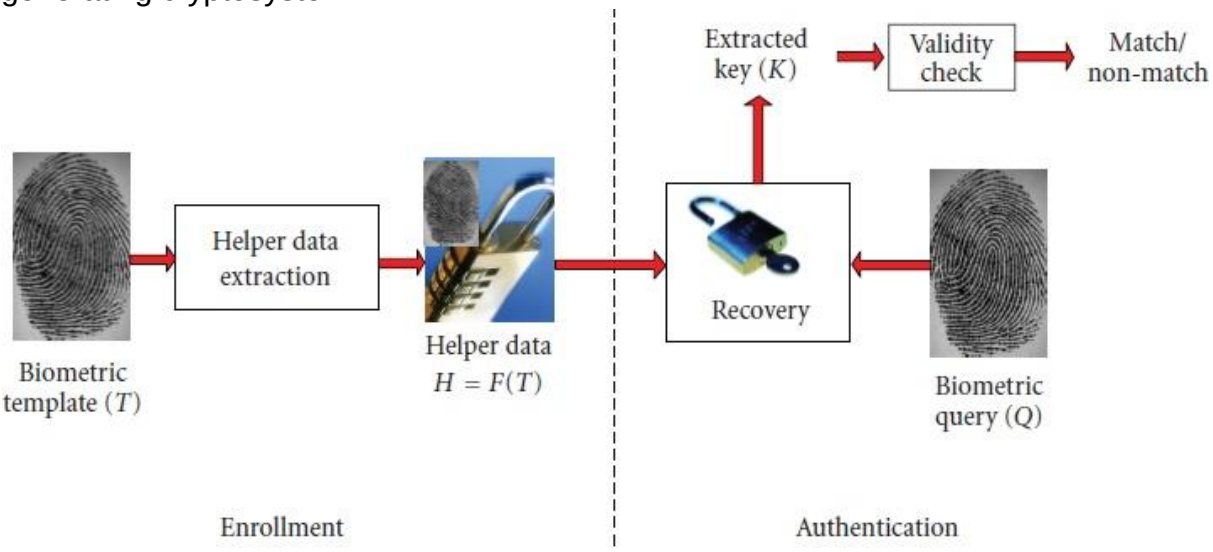

Figure 20. Authentication mechanism when the biometric template is secured using a key generation biometric cryptosystem. Authentication in a key-binding

biometric cryptosystem is similar except that the helper data is a function of both the template and the key K, that is, H = F (T; K). [20]

Based on Figure 19 and 20, the function used in all the schemes proposed by researchers has been simplified and fit together into Table 2.

Table 2. Summary of different template protection schemes. [20]

Approach	**What imparts security to the template?**	**What entities are stored?**	**How are intrauser variations handled:**
Salting	Secrecy of key K.	Public domain: transformed template F(T;K) Secret: Key K	Quantization and matching in transformed domain M (F(T;K), F(Q;K))
Noninvertible transform	Noninvertibility of the transformation function F.	Public domain: transformed template F(T;K), key K	Matching in transformed domain M(F(T;K), F(Q;K))
Key-binding biometric cryptosystem	Level of security depends on the amount of information revealed by the helper data H	Public domain: helper data H = F(T;K)	Error correction and user specific quantization K = M(F(T;K), Q)
Key-generating biometric cryptosystem	Level of security depends on the amount of information revealed by the helper data H	Public domain: helper data H = F(T)	Error correction and user specific quantization K = M(F(T), Q)

Here, T represents the biometric template, Q represents the query, and K is the key used to protect the template. In salting and non-invertibility feature transform, F represents the transformation function, and M represents the matcher that operates in the transformed domain. In biometric cryptosystems, F is the helper data extraction scheme and M is the error correction scheme that allows reconstruction of the key K.

Even though the perfect and best system or algorithm/cryptosystem has not been developed yet, the proposed schemes for template protection for both unimodal biometric systems and the multi-biometrics systems deployed in various areas seem to be compromising the minimal error rates occurred during the implementation. Further research in biometric encryption is a necessity as to guarantee the privacy and the security of each individual and organization with more accuracy (100% accuracy).

The below presented tables show the outcomes of implementation of various biometric and multi-biometrics template security schemes which use different modalities:

Table 3. Experimental results of key approaches to biometric template protection schemes. [30]

Author(s)	Applied Technique	Modality	FRR / FAR (%)	Remarks
Hao et al. (2006)	Fuzzy Commitment	Iris	0.42 / 0.0	small test set
Bringer et al. (2007)			5.62 / 0.0	short key
Clancy et al. (2003)	Fuzzy Vault	Fingerprints	20-30 / 0.0	pre-alignment, >1 enroll sam.
Nandakumar et al. (2007)			4.0 / 0.004	>1 enroll sam.
Wu et al. (2008)		Iris	5.5 / 0.0	–
Feng & Wah (2002)	Quantization	Online Sig.	28.0 / 1.2	>1 enroll sam.
Vielhauer et al. (2002)			7.05 / 0.0	short key
Monrose et al. (2001)	Password-Hardening	Voice	>2.0 / 2.0	short key
Teoh et al. (2004)	BioHashing	Face	0.0 / 0.0	non-stolen token
Ratha et al. (2007)	Block Permutation, Surface Folding	Fingerprints	$\sim 35 / 10^{-4}$ $\sim 15 / 10^{-4}$	–
Maiorana et al. (2010)	BioConvolving	Online Sig.	10.81 EER	–
Goh et al. (2006)	BioHashing	Face	0.0002 EER	non-stolen token

Table 4. Experimental result of approaches to multi-biometric template protection schemes. [30]

Author(s)	Applied Technique	Modality	FRR / FAR (%)	Remarks
Sutcu et al. (2007)	Multi-biometric Fuzzy Commitment	Fingerprint and Face	0.92 / >0.001	–
Kelkboom et al. (2009)		3D Face and 3D Face	$\sim$ 2.5 EER	single sensor scenario
Rathgeb et al. (2011)		Iris and Iris	5.56 / 0.01	single sensor scenario
Nandakumar & Jain (2008)	Multi-biometric Fuzzy Vault	Fingerprint and Iris	1.8 / 0.01	–
Nagar et al. (2012)		Fingerprint, Face and Iris	1.0 / 0.0	–
Jeong et al. (2006)	Token-based Scrambling	Face and Face	$\sim$ 15.0 EER	single sensor scenario

6. Remote Authentication

The world has been digitized continuously. With such development it has become virtually accessible to most of the people from anywhere to anywhere. Remote authentication is a form of authenticating an individual via the Internet or any network connection where a user submits her/his credentials as a proof of identity to verify the originality and the legitimacy of herself which she/he may or will claim to be. Since the traditional username and password methodologies for authentication have become vulnerable to different flaws and attacks which have been simplified and widely spread lately; innovation of rigorous security protocol against masquerades must be initiated.
Little few research and development has been attained in implication of multi-biometrics systems for remote authentication.

6.1 Kerberos, Cryptography and Biometric based Remote Authentication Protocol

Desai Karan and *Ruchir*have proposed a biometric remote authentication protocol which includes **Kerberos**and Cryptography. This protocol allows a remote user for single registration and multiple authentications with certain level of security. The major steps included in their protocol are: i) Registration, ii) Authentication and iii) Ticket granting [27]. Figure 21 demonstrates the basic ideas of these three steps:

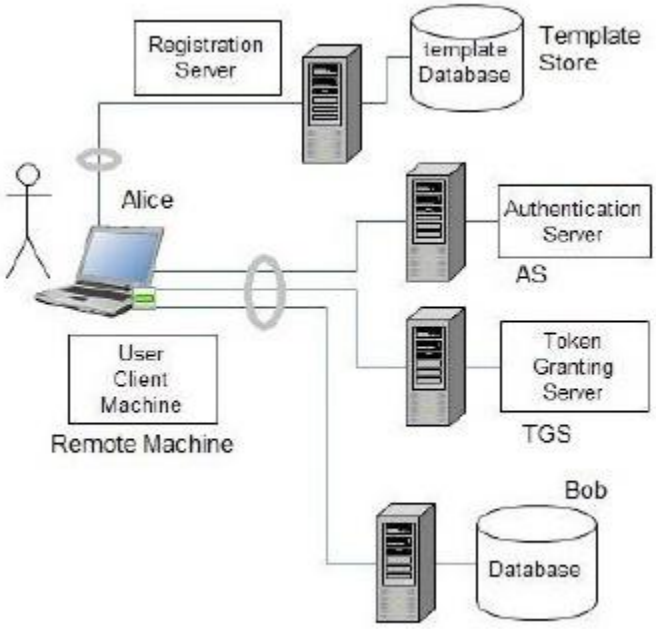

Figure 21. Authentication mechanism. [27]

Referring to Figure 21, assuming a remote client- 'Alice' has all the hardware requirements, she initially registers/enrolls herself to the Registration Server which also successfully saves the biometric templates received; second she authenticates herself with the authentication server which leads her to be granted with the tickets and session keys. These tickets and session keys have expiry time frame which allows higher security.

However, while accessing Bob, Alice does not necessarily have to undergo all the three steps mentioned above. Since the tickets can be reused for certain period of time, she can just invoke and authenticate to reach to Bob securely.

All the modulo-operations in the encryption domain uses the expression (M operation N)mod P, where P is directly dependent to the encryption scheme used. The summarization of overall client's side and all the three servers' side authentication calculation process can be demonstrated and better understood based on Figure (22) below:

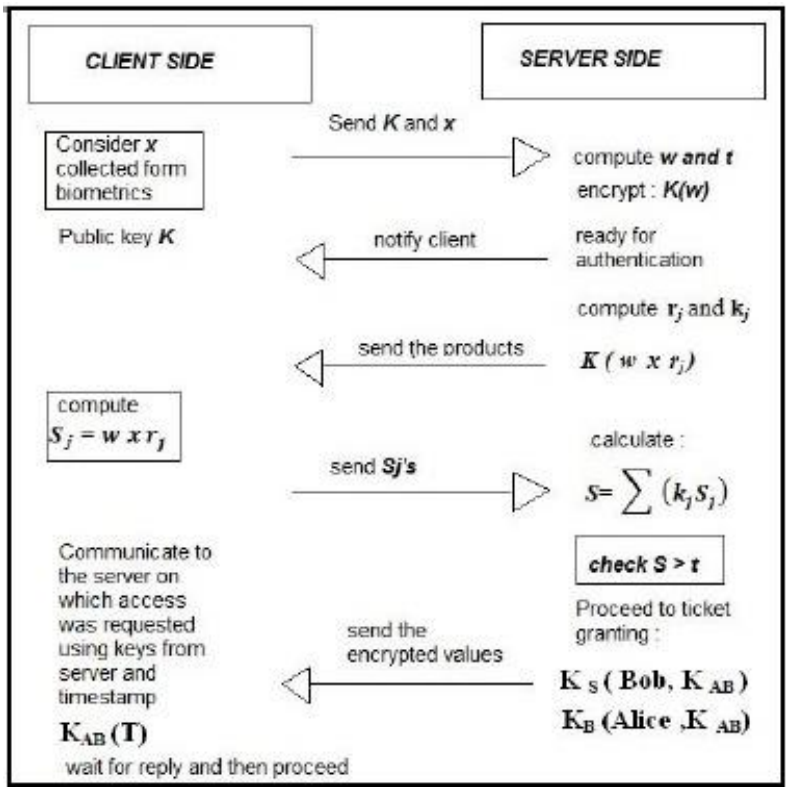

Figure 22. Sequential representation of the process [27].

According to the authors, security and privacy in different scenarios and conditions which the protocol provides are listed below. :-

- If the hacker gains access to the template.

- If the hacker is in the database server during authentication.
  - On the client side if the hacker gains access to the user's biometric or private key
- A passive kind of attack on the user's system.
- Network security.
- In cases of risks that the Kerberos protocol faces.
- If the user is concerned of being tracked and also is skeptical about the revelation of her private identity.
- In case of loose synchronization.
- The password theft problem.
- **DSA and Fast RSA**

The application as put forward by the authors is in both the small networks such as LANs and also the large networks such as WANs. A pictorial representation of the proposed protocol applied in a wide area network is given in Figure 23.

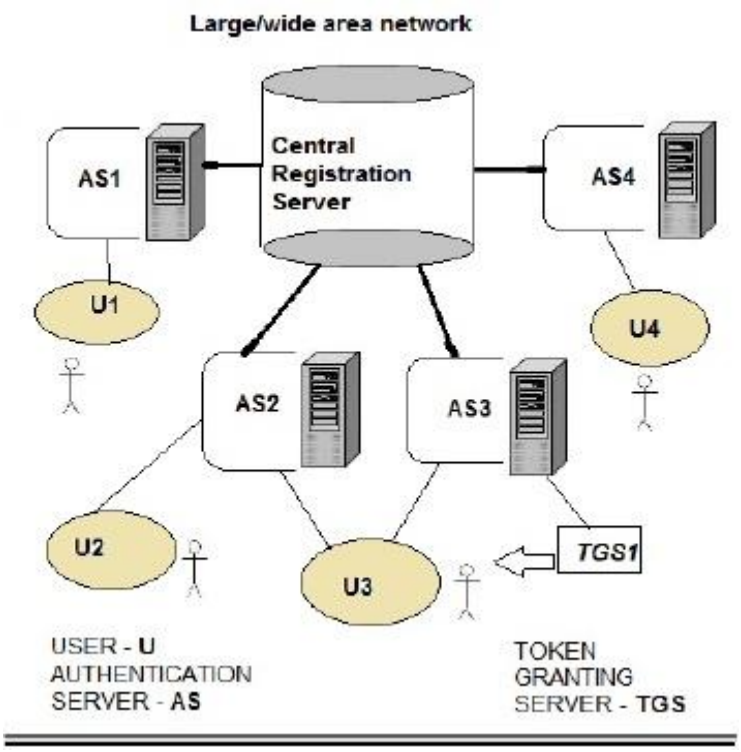

Figure 23. Application in large networks [27].

6.2 Practical Multi-factor Biometric Remote Authentication

Neyire Deniz has proposed a protocol for Multi-factor Biometric Remote Authentication (MFBA) which does not require a decryption key for the authentication purpose since the computations are executed in the encryption domain. This benefits in not affecting the security scheme even if the secret key of any system component is leaked as occurs in the cryptographic systems used in generic biometric systems. [28]

This protocol employees two schemes for ordered or unordered set of biometric features which successfully combines **Homomorphic Encryption scheme, Zero knowledge proofs, Bilinear Pairing**and different extraction methods.

Homomorphic Encryption:

In modern communication system, Homomorphic encryption is widely used and desired.

It is an encryption method which supports specific types of computations to be performed on *ciphertext*, which in return generates an encrypted result. These encrypted results when decrypted match the operations performed in plaintext.

Zero Knowledge Proof/Protocol (ZPK)

ZPK is a method where without needing to convey any additional information, a party *(the prover)*is successfully able to prove to another party *(the verifier)*that certain message/statement is legitimate. Here, the user who is trying to authenticate is the prover and the server is the verifier.

Bilinear Pairings

“A bilinear pairing is denoted by ê : G x G → F, where G,F are system parameters of the ellicptic curve ElGamal encryption with g the generator of the group G.”

Presuming the liveliness requirement is satisfied by the system, the security model provided includes:

- **Sensor Client (SC):** A device or an entity that captures fresh biometric templates during verification.

- **Service Provider (SP):**SP stores information such as names, personalized usernames etc. and the encrypted stable biometric templates for each user.

- **User U with a smart card:**Every user will have a tamper proof smart card which stores the non-stable parts of the biometric template extraction method parameter.

Figure 24 explains Deniz’s scheme for verification phase.

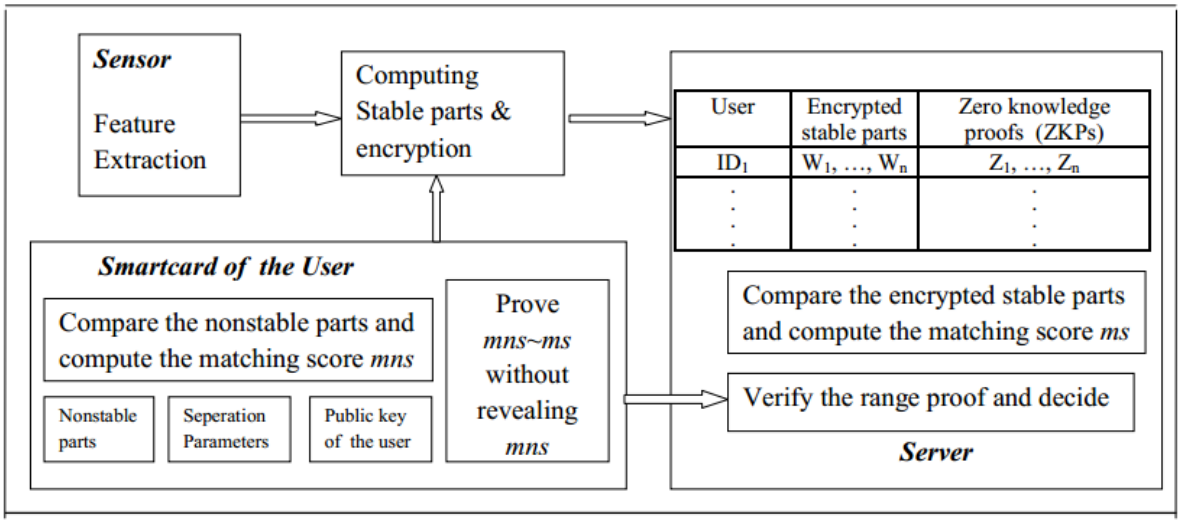

Figure 24. Verification phase of the Deniz's protocol [28].

6.3 Enhanced Biometrics-based Remote User Authentication Scheme Using Smart Cards

The remote authentication protocol which used a smart card proposed in 2010 by Li and Hwang had issues of insecurity where an attacker could successfully impersonate the user or gain access to her/his the then session key. Later recently, Li et al. proposed a scheme which is supposedly improved version of Li and Hwang's scheme. However, the proposed scheme is readily prone to attacks such as *replay attack* and *DoS attacks*, also once the template is leaked; their biometric authentication cannot be used safely. [54]

As a remedy, Jian-Zhu et al. proposed a scheme which enhances the remote user authentication using biometric templates. Their scheme consists of five phases, namely:

Initialization phase

- System Setup: It is implemented once to setup the overall enrollment system.
- Server Enrollment: Here, the legal server is provided a master secret key.

User Registration Phase

It consists of three basic steps; firstly the user inputs her/his personal biometrics features, provides the password, identity of the user via a secure channel.

User login phase

The user now inserts her/his smart card into the card reader which checks whether the matching score is beyond the defined threshold value. If the matching score is true, the biometric verification is correctly sent to the remote server.

Remote Authentication phase

Here, when the server receives the login credentials which include template and the message, it checks the validity of format of ID and if found correct it stores the ID and the template in the database. If the validity check fails then the server rejects login request and terminates the entire session.

For the reason of keeping this writing simple and understandable by a layman, the complex formula presented in the original literature by the authors has been excluded. However, for the demonstration purpose of the mutual authentication between the client side and the remote server side proposed in the scheme, the computational equations involved in the algorithm are demonstrated in Figure 25.

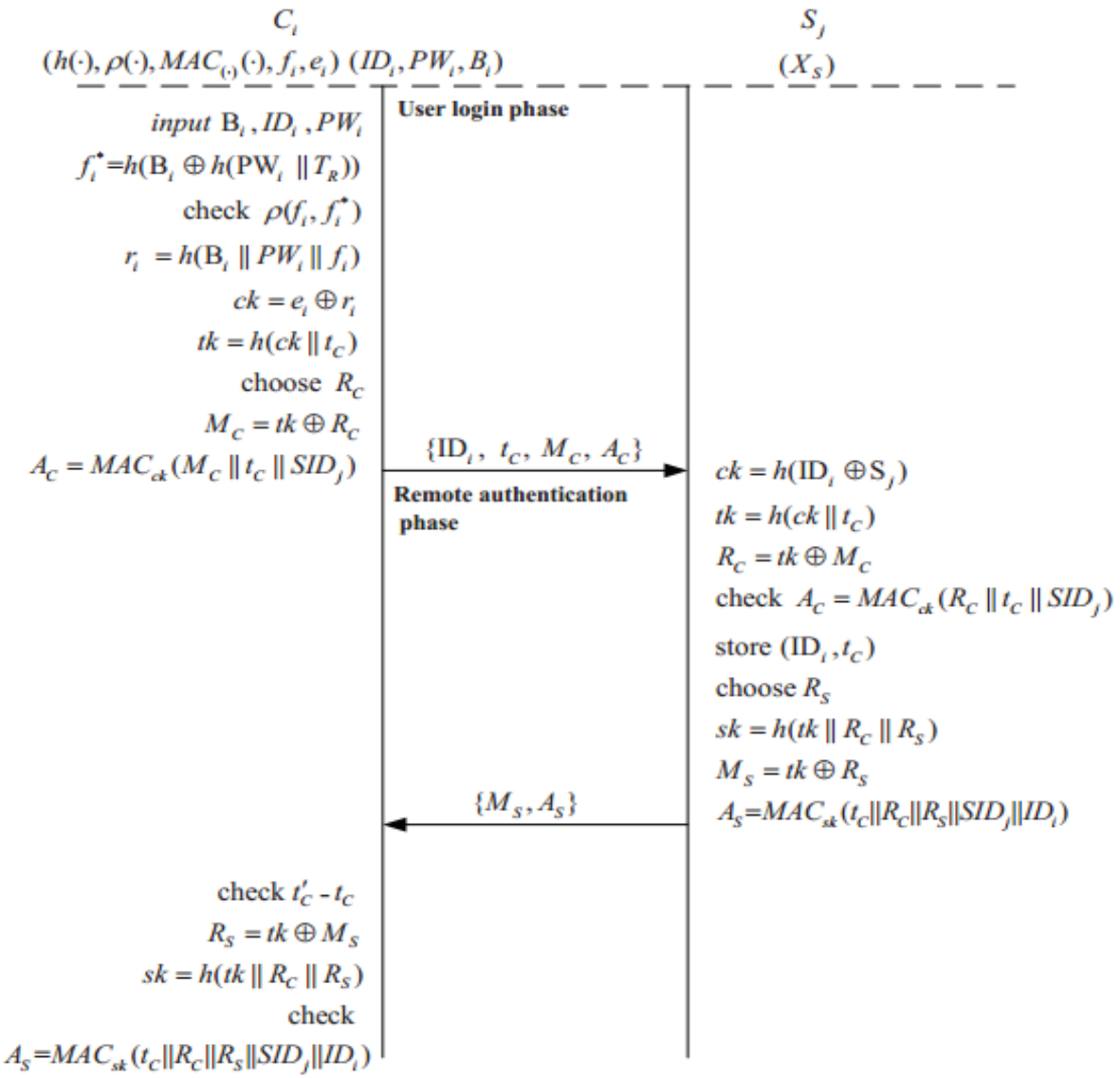

Figure 25. The mutual authentication between Client (C_i) and Server (S_j) in the scheme [54]

Password and template update phase

Here the user inserts her smart card in the specific device and inputs the password, which is checked for verification. If the verification is verified correctly, the system allows the user to input the new password, upon which the system deletes the old template and password stored previously.

According to the performance analysis, the scheme successfully reduces the computation and communication cost. Along with that, it enhances the security and can avoid attacks such as *Replay attack, the man-in-the-middle attack* and the *impersonating attack.*

Although research and development in remote authentication has become a focal point for the next step in proving the legitimacy of an individual, its complexity becomes more complex as the entire process is dependent in the conversion of human physical traits to digital and computational expanse. Despite the existing intricacies, few scheme and protocols have been designed as mentioned above and in addition that some other protocols for biometric remote authentication have also been proposed by Xavier Boyen, Yevgeniy Dodis, Jonathan Katz, Rafail Ostrovsky, Adam Smith, Karthik Nandakumar, Anil K. Jain, Arun Ross and few other scholars.

An example of a remote authentication device; a smart phone application named “Voicevault” has been developed by a US based company El Segundo, CA which provides voice biometric solutions for mobile, on-device and telephony applications.

7. Issues of multi-biometrics remote authentication system

The continuous research has not yet been able to achieve the accuracy required for correct verification yet. In 2001, Ratha et al. suggested that multi-biometrics systems can be compromised in a number of ways. While conventional biometric systems which use only single human trait for authentication and verification need lesser protocol, sensor and device implementation, multi-biometrics systems use multiple traits which involve usage of multiple reference data, multiple sources of information to be collected and multiple protection protocol to be implemented increases the complexity of multiple SDK to be maintained along with the development of multiple sensors and devices which require stronger dependency. [30] “For instance, in case ‘*n*’ different comparisons, scores are combined performing score level fusion, ‘*n*’ different biometric templates have to be stored for each subject registered with the system.”- Christian et al. state [30]. This increases the vulnerability of multi-biometrics remote authentication system as the biometric template fusion requires more complex cryptosystems for secure transferring and storing of such data.

One of the main issues that needs to be addressed is the user’s ethical belief in using one’s personal traits for verification which are stored and managed by third party and lingering in cloud databases. This raises the mode-of-use and privacy insecurities and skepticism. Inaccurate performance measure and unstable security schemes provide aid in such issues whilst using multi-biometrics systems.

8. Conclusion

Although it is reasonable to use one's unique trait/organ as a means of her/his identification and verification in today's digital world, it is of no use if the devices and sensors used in digitizing such traits are not trustworthy and dependable. The use of multi-biometrics sounds plausible in question; yet the practical notion of its use holds relatively complex construction of such hi-tech cryptosystems and algorithms which have not yet been perfected to its desired acme. Increment in discovery and verification of uniqueness of different biometric templates will not affect and help much in verification and security if the usability and accountability cannot be reliable and be accepted in a collective field.

However, due to the increased development of complex computer systems and cryptography to crack the passwords and security measures of today's security structure, it is rather credible to implement biometrics and multi-biometrics for authentication purposes. The daily realization of insecurity while privatizing one's belonging has escalated, protecting classified matters and freedom to keep ones secret a secret to oneself has slowly become jeopardized. This demands a rapid growth in development of high level security measures. Based on historical and present research and findings, biometric security systems have become the emerging and promising solution for such insecurities. Today's security system is created and governed by human generated techniques and devices; the future security means will include human itself.

9. Future work

Based on the aforementioned brief description of biometrics, multi-biometrics, biometrics templates and their protection, and the implementation of multi-biometrics in remote authentication system, it is wise to realize that the necessity of development in mentioned topics must cover a wide area. The list presented below includes some areas to be developed:-

- Establishing error free algorithms, protocols and databases for multi-biometrics.
- Feature extraction, template updates, recognition, data pre-processing and the precise matching schemes for multi-biometrics.
- Flawless and stable cryptosystems for multi-biometric and multi-biometric remote authentication systems
- Cloud based solutions made widely available and include other biometric templates
- Development of new data sensing technologies
- Unbreachable establishment of public databases for multi-biometrics.
- Performance and reliance assessment of multi-biometrics in various scopes in everyday life.
- Invention of accurate multi-sensor, multi-spectral fusion and new fusion architectures for use in multi-biometrics systems.
- Introducing machine learning techniques and signal processing for unmitigated performance in multi-biometrics.
- Inventing database indexing techniques, protocols, standards and interfaces for multi-biometrics systems.
- Enhancing security and privacy of multi-biometrics databases and thus by comforting user notion to privacy and the use of biometric templates.

REFERENCES

[1] Carl Zeiss Education, Gatwick, West Sussex, Optical biometry course. Retrieved September 17, 2013

http://www.thefreedictionary.com/biometry

[2] Kelly Smith, Peter Higgins, Nick Orlans, Jim Wayman: FBI contractors and NSA; , 7 August 2006, Retrieved September 19 2013

http://www.biometrics.gov/documents/biohistory.pdf

[3] Biometrics traits. Retrieved September 17, 2013 from: http://www.engineersgarage.com/sites/default/files/imagecache/Original/wysiwyg_image upload/1/biometric-chart-imgae.jpg

[4] Tracy V. Wilson. Retrieved October 4 2013

http://science.howstuffworks.com/biometrics.htm

[5] Pbworks, Authentication technologies. Retrieved October 7 2013

http://biometrics.pbworks.com/w/page/14811351/Authentication%20technologies

[6] Applications of Biometrics. Retrieved October 20 2013

http://www.questbiometrics.com/applications-of-biometrics.html

[7] EURODAC “Information and communication" unit, Directorate-General Justice, Freedom and Security, B-1049 Brussels – August 2004. Retrieved October 22 2013

http://www.biteproject.org/documents/EU_Biometrics_at_the_Frontiers.pdf

[8] Micki Krause, Harold F. Tipton, Information Security Management. Retrieved October 31.2013

http://www.ccert.edu.cn/education/cissp/hism/039-041.html

[9] William J. Lawson, Ph.D. Enhancing Assistive Technologies. Retrieved November 14 2013

http://www.icdri.org/biometrics/biometrics.html

[10] Voice sign. Retrieved November 18 2013

http://sites.bergen.org/ISTF/0185/component2.html

[11] Dec 1, 2009, Elizabeth Bernardi, Government Product News, Hand geometry reader. Retrieved November 19 2013

http://americancityandcounty.com/buildings-security-fire/hand-geometry-reader

[12] June 27, 2003, Michael. Biometric Face recognition Exploit. Retrieved November 21 2013

http://it.slashdot.org/story/03/06/27/197229/biometric-face-recognition-exploit

[13] 2003, William J. Lawson, “ENHANCING ASSISTIVE TECHNOLOGIES:THROUGH THE THEORETICAL ADAPTATION OFBIOMETRIC TECHNOLOGIES TO PEOPLE OF VARIABLE ABILITIES”, Facial thermography image. Retrieved November 22 2013

http://dc443.4shared.com/doc/yPOMELXi/preview.html

[14] January 2005, Julian Ashbourn, “The Social Implications of the Wide Scale Implementation of Biometric and Related Technologies”. Retrieved November 22 2013

http://www.statewatch.org/news/2005/apr/jrc-biometrics-julian-ashbourn.pdf

[15] 2004, Mamta Kothavale, Robert Markworth, Parmajit Sandhu, Computer Security SS3: Biometric Authentication. Retrieved November 26 2013

http://www.cs.bham.ac.uk/~mdr/teaching/modules03/security/students/SS3/old/handout/

[16] FRR and FAR rate of vein pattern, used by japan. Retrieved November 30 2013

http://eu.zksoftware.com/view.do?id=51

[17] 2006, Fujitsu Computer Products of America, Inc., Palm Vein PatternAuthentication Technology. Retrieved December 2 2013.

http://www.fujitsu.com/downloads/COMP/ffna/palm-vein/palmsecure_wp.pdf

[18] July 26, 2011, Mike Flacy, HAND-SCAN, vein pattern image. Retrieved December 8 2013

http://www.digitaltrends.com/gadgets/hospital-starts-scanning-vein-patterns-to-bring-up-medical-records/attachment/hand-scan/

[19] Carreira-Perpiñán, M. Á. (1995): Compression neural networks for feature extraction: Application to human recognition from ear images (in Spanish). MSc thesis, Faculty of Informatics, Technical University of Madrid, Spain. Retrieved December 14 2013.

http://faculty.ucmerced.edu/mcarreira-perpinan/papers/msc-thesis.html

[20] 4 December 2007, Anil K. Jain, Karthik Nandakumar, and Abhishek Nagar “Biometric Template Security”. Retrieved December 19 2013.

http://biometrics.cse.msu.edu/Publications/SecureBiometrics/JainNandakumarNagar_TemplateSecuritySurvey_EURASIP08.pdf

[21] Abhisek Nagar, “Secure Biometric Recognition” fish-bone model picture. Retrieved December 29 2013:

https://www.cse.msu.edu/~nagarabh/QualifierReport.pdf

[22] Nalini K. Ratha, Jonathan H. Connell, and Ruud M. Bolle, “An Analysis of Minutiae Matching Strength”, Figure (13). Retrieved January 1 2014http://pdf.aminer.org/000/060/741/an_analysis_of_minutiae_matching_strength.pdf

[23] 30 June 2006, Anil K. Jain, Sharathchandra Pankanti, “A Touch of Money, Biometric authentication systems for credit cards could put identity thieves out of business”. Attacks on the template database. Retrieved January 7 2014

http://spectrum.ieee.org/computing/hardware/a-touch-of-money

[24] Marco Grassi, Marcos Faundez-Zanuy, “A protection scheme for enhancing biometric template security and discriminability”. Retrieved January 11 2014

http://jrbp10.unizar.es/papers/S1.C1.pdf

[25] 2008, Karthik Nandakumar, “Multibiometric Systems: Fusion Strategies and

Template Security”, Feature transformation figure. Retrieved January 18 2014.

http://www.dtic.mil/dtic/tr/fulltext/u2/a488585.pdf

[26] July 21, 2007, Yevgeniy Dodis, Rafail Ostrovsky, Leonid Reyzin, Adam Smith, “Fuzzy Extractors: How to *Generate Strong Keys from Biometrics and Other Noisy Data*”. Retrieved January 23 2014.

http://www.cs.nyu.edu/~dodis/ps/fuzzy.pdf

[27] Desai Karan Ronak, Ruchir Patwa, “Kerberos, Cryptography and Biometric based RemoteAuthentication Protocol”. Retrieved February 2 2014

http://www.academia.edu/1300043/Kerberos_Cryptography_and_Biometric_based_Remote_Authentication_Protocol

[28] Neylre Deniz Sarler, “Practical Multi-factor Biometric Remote Authentication”. Retrieved February 9 2014

https://cosec.bit.uni-bonn.de/fileadmin/user_upload/publications/pubs/sar10d.pdf

[29] 2012, Voicevault Inc. Retrieved February 16

http://www.voicevault.com/about-us/

[30] Christain Rathgeb and Christoph Busch, “Multi-Biometric Template Protection: Issues and Challenges” Received February 22, 2014

http://www.fbi.h-da.de/fileadmin/gruppen/FG-IT-Sicherheit/Publikationen/2012/2012_10_Rathgeb_InTech.pdf

[31] Romain Giot, Christophe Rosenberger, Genetic Programming for Multi-biometrics. Retrieved Feb 23, 2014

http://hal.archives-ouvertes.fr/docs/00/67/19/52/PDF/gp_biometrics.pdf

[32] Glenn Langenburg. Retrieved May 5th 2014

http://www.scientificamerican.com/article/are-ones-fingerprints-sim/

[33] KI MAE HEUSSNER, abcNews, Surgically Altered Fingerprints Help Woman Evade Immigration. Retrieved May 6th 2014

http://abcnews.go.com/Technology/GadgetGuide/surgically-altered-fingerprints-woman-evade-immigration/story?id=9302505

[34] Biometric Palm Prints Feature Matching for Person Identification. Mr. Shriram D. Raut and Dr. Vikas T. Humbe. Retrieved on May 7th 2014.

http://www.mecs-press.org/ijmecs/ijmecs-v4-n11/IJMECS-V4-N11-6.pdf

[35] Ed Grabianowski, How Speech Recognition Works. Retrieved on May 12th 2014

http://electronics.howstuffworks.com/gadgets/high-tech-gadgets/speech-recognition3.htm

[36] Iris figure, retrieved May17th 2014

http://static.ddmcdn.com/gif/biometric-1.jpg

[37] Tracy V. Wilson, Iris Scanning, retrieved May 16th 2014

http://science.howstuffworks.com/biometrics4.htm

[38] Hanna-Kaisa Lammi, EAR BIOMETRICS, Retrieved May 20th 2014

http://www.it.lut.fi/kurssit/03-04/010970000/seminars/Lammi.pdf

[39] Pictorial presentation of countries which adopted biometrics. Retrieved 17 September 2013.

http://www.cgdev.org/publication/identification-development-biometrics-revolution-working-paper-315

[40] Fingerprint patterns image. Retrieved 20 November 2013.

http://sites.bergen.org/ISTF/0185/component2.html

[41] Palm print image. Retrieved 20 November 2013

http://www.bioenabletech.com/automated-fingerprint-identification-system-afis.html

[42] Dynamic signature verification image pad. Retrieved 24 November 2013

http://www.idpaq.com/images/products/Signature%20pad%20dubai%20uae.jpg

[43] 360 biometrics, Hand geometry. Retrieved: 27 May 2014

http://360biometrics.com/faq/Hand-Geometry-Biometrics.php

[44] William J. Lawson, Ph.D., ENHANCING ASSISTIVE TECHNOLOGIES:THROUGH THE THEORETICAL ADAPTATION OFBIOMETRIC TECHNOLOGIES TO PEOPLE OF VARIABLE ABILITIES. Retrieved: 27th may 2014

http://dc443.4shared.com/doc/yPOMELXi/preview.html

[45] Robert and chris. Biometrics. Retrieved: May 17th 2014.

[46] Retina image. Retrieved May 17th 2014

http://eu.zksoftware.com/view.do?id=51

[47] JAMES TOZER, Dailymail UK. Retrieved May 29th 2014.

http://www.dailymail.co.uk/news/article-2102076/Millions-drain-airports-SCRAP-iris-passport-scanners.html

[48] Sanjusanjeedha, Wikianswers, Advantages and disadvantages of Iris recognition. Retrieved May 28th 2014

http://wiki.answers.com/Q/Advantages_and_disadvantages_for_Iris_Recognition?#slide=3

[49] John Daugman, OBE FIMA FIAPR, Professor of Computer Vision and Pattern Recognition. Retrieved May 28th 2014

http://www.cl.cam.ac.uk/~jgd1000/addisadvans.html

[50] Pbworks, Retrieved January 25th 2014.

http://biometrics.pbworks.com/w/page/14811351/Authentication%20technologies

[51] Biometric Research group. Retrieved October 20th 2014

http://www.cse.msu.edu/rgroups/biometrics/info/index.html

[52] Biometric information resource. Multimodal biometrics. Retrieved October 20th 2014

http://www.biometricsdata.com/multimodalbiometrics.html

[53] Karthik Nandakumar, Anil K. Jain, and Arun Ross. Fusion in Multibiometric Identification Systems: Whatabout the Missing Data? Retrieved December 5th 2013.

http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.219.5112&rep=rep1&type=pdf

[54] Jian-Zhu Lu, Shaoyuan Zhang, and Shijie Qie. Department of Computer Science, Jinan University. Enhanced Biometrics-based Remote User: Authentication Scheme Using Smart Cards. Retrieved February 12th 2014.

http://eprint.iacr.org/2011/676.pdf

[55] William J. Lawson, Ph.D. ENHANCING ASSISTIVE TECHNOLOGIES: THROUGH THE THEORETICAL ADAPTATION OF BIOMETRIC TECHNOLOGIES TO PEOPLE OF VARIABLE ABILITIES. Retrieved January 21st 2014.

http://www.icdri.org/biometrics/biometrics.html