DESIGN OF A HAND GEOMETRY BASED VERIFICATION SYSTEM

A thesis report

Submitted in the partial fulfillment of the requirements for the award of degree of

Master of Engineering
in
Electronic Instrumentation & Control Engineering

Submitted by

Vivek Yadav
Roll No-800851028

Under the supervision of:
Ms. Gagandeep Kaur
Assistant professor, EIED

DEPARTMENT OF ELECTRICAL AND INSTRUMENTATION ENGINEERING
THAPAR UNIVERSITY
PATIALA –147004
JULY - 2010

DEDICATED

TO

MY PARENTS

CERTIFICATE

I hereby certify that the work which is being presented in the thesis entitled, **"Design of a Hand Geometry Based Verification System"** in partial fulfillment of the requirements for the award of degree of Master of Engineering in Electronic Instrumentation and Control Engineering submitted in Electrical and Instrumentation Engineering, Department of Thapar University, Patiala, is an authentic record of my own work carried out under the supervision of **Ms. Gagandeep kaur**(Assistant Professor) and refers other researcher's works which are duly listed in the reference section.

The matter embodied in this report has not been submitted anywhere for the award of any degree.

Vivek yadav

Date: 14-7-2010

Vivek Yadav

Roll No - 800851028

It is certified that the above statement made by the student is correct to the best of our knowledge and belief.

14/7/10

***Ms* Gagandeep kaur**

Assistant Professor, EIED

(Supervisor)

Thapar University, Patiala

S. Ghosh 14/7/10

Dr. Smarajit Ghosh

Professor & Head, EIED

Thapar University, Patiala

R K Sharma 16.7.10

Dr. R. K. Sharma

Dean of Academic Affairs

Thapar University, Patiala

ACKNOWLEDGEMENT

The real spirit of achieving a goal is through the way of excellence and austere discipline. I would have never succeeded in completing my task without the cooperation, encouragement and help provided to me by various personalities.

I shall be failing in my duties if I do not express my deep sense of gratitude towards **Dr. Smarajit Ghosh,** Professor & Head of the Department of Electrical & Instrumentation Engineering, Thapar University, Patiala who has been a constant source of inspiration for me throughout this work.

With deep sense of gratitude I express my sincere thanks to my esteemed and worthy supervisor, **Ms. Gagandeep kaur,** Assistant Professor, Department of Electrical and Instrumentation Engineering, Thapar University, Patiala for her valuable guidance in carrying out this work under her effective supervision, encouragement, enlightenment and cooperation. Most of the novel ideas and solutions found in this thesis are the result of our numerous stimulating discussions. Her feedback and editorial comments were also invaluable for writing of this thesis.

I am also thankful to all the staff members of the Department for their full cooperation and help.

This acknowledgement would be incomplete if I do not mention the emotional support and blessings provided by my friends. I had a pleasant enjoyable and fruitful company with them.

My greatest thanks are to all who wished me success especially my parents, my brother and sisters whose support and care makes me stay on earth.

Place: Thapar University, Patiala

Date: 14-7-2010

Vivek Yadav

Vivek Yadav

ABSTRACT

Biometrics which is used for identification of individuals based on their physical or behavioral characteristics. Biometrics has gained importance in today's world where information security is essential. Hand geometry, one of the most well-known biometrics, is implemented in many verification systems with various feature extraction methods. Hand geometry based biometric systems are gaining acceptance in low to medium security applications. Hand biometrics is extensively used for personal authentication.

The proposed system is a verification system which utilizes some hand geometry features for user authentication. The feature vector used in this proposed system consists of only those features which can not vary with small variation of palm position. Users can place their hands freely without the need for pegs to fix the hand placement. Most of the currently available systems for hand geometry use pegs for fixing the placement of the palm on the scanner. The proposed system aims to eliminate this constraint by allowing the user to vary the positioning of the palm on the scanner. Hence the proposed system is a restriction free verification system which utilizes these hand geometry features for user authentication.

It consists of a database where all the information about the authenticated users is stored. The system extracts the features from a test image and compares it with the stored information on the database. The experimental results show that the proposed system has an encouraging performance. The false acceptance rate and false rejection rate are reduced down to 0.02 and 0.072, respectively. The system is implemented using MATLAB.

ORGANIZATION OF THESIS

The whole of the work is divided into six chapters; the brief discussion is as follows.

1. The first chapter gives the introduction about the motivation and objective of this work.
2. The second chapter is the review of literature i.e. a summary about the developments in the subject so far.
3. The third chapter gives a detailed description of hand geometry biometrics system. It covers the description and function of each part which comes in this project.
4. The fourth chapter gives the problem definition and proposed solution.
5. The fifth chapter discusses the implementation and testing part of the thesis.
6. The sixth chapter shows the result of the proposed hand geometry biometrics system. Finally, concluding thesis with future scope.

TABLE OF CONTENTS

LIST OF FIGURE

ABBREVIATION

ATM	Automated Teller Machine
ANN	Artificial Neural Network
CER	Crossover Error Rate
EER	Equal Error Rate
FAR	False Acceptance Rate
FRR	False Rejection Rate
FTE	Failure to Enroll
PIN	Personal Identity Number
ROC	Receiver Operating Characteristic

CHAPTER -1
INTRODUCTION

1.1 Biometrics

As the personal and institutional security requirements increase, a person has to remember lots of passwords, pin numbers, account numbers, voice mail access numbers and other security codes. However passwords have their own weaknesses. The weak passwords can be easily guessed and the strong ones can be broken. It is recommended that people should not use the same password for two different applications and should change them regularly. In the modern world that would mean memorizing a large number of passwords. Biometric authentication is the ideal solution to all these requirements. In future, biometric systems will take the place of this concept since it is more convenient and reliable.

Biometric is automated methods of identifying a person or verifying the identity of a person based on a physiological or behavioral characteristic. Examples of physiological characteristics include hand or finger images, facial characteristics. Behavioral characteristics are traits that are learned or acquired. Dynamic signature verification, speaker verification and keystroke dynamics are examples of behavioral characteristics.

Biometric authentication requires comparing a registered or enrolled biometric sample against a newly captured biometric sample for example, a fingerprint captured during a login. During enrollment a sample of the biometric trait is captured, processed by a computer, and stored for later comparison.

Biometric recognition can be used in Identification mode, where the biometric system identifies a person from the entire enrolled population by searching a database for a match based solely on the biometric. This is sometimes called “one-to-many” matching. A system can also be used in Verification mode, where the biometric system authenticates a person’s claimed identity from their previously enrolled pattern. This is also called “one-to-one” matching. In most computer access or network access

environments, verification mode would be used. A user enters an account, user name, or inserts a token such as a smart card, but instead of entering a password, a simple touch with a finger or a glance at a camera is enough to authenticate the user.

1.2 Need of Biometrics

Using biometrics for identifying human beings offers some unique advantages. Biometrics can be used to identify you as you. Tokens, such as smart cards, magnetic strip cards, photo ID cards, physical keys and so forth, can be lost, stolen, duplicated, or left at home. Passwords can be forgotten, shared, or observed. Moreover, today's fast-paced electronic world means people are asked to remember a multitude of passwords and personal identification numbers for computer accounts, bank ATMs, e-mail accounts, wireless phones, web sites and so forth. Biometrics holds the promise of fast, easy-to-use, accurate, reliable, and less expensive authentication for a variety of applications. There is no one perfect biometric that fits all needs. All biometric systems have their own advantages and disadvantages. There are, however, some common characteristics needed to make a biometric system usable. First, the biometric must be based upon a distinguishable trait. For example, for nearly a century, law enforcement has used fingerprints to identify people. There is a great deal of scientific data supporting the idea that “no two fingerprints are alike.” Technologies such as hand geometry have been used for many years and technologies such as face or iris recognition have come into widespread use. Some newer biometric methods may be just as accurate, but may require more research to establish their uniqueness. [28]

Another key aspect of hand geometry based system is that it is user-friendly system. The process should be quick and easy, such as having a picture taken by a video camera, speaking into a microphone, or touching a fingerprint scanner. Low cost is important, but most implementers understand that it is not only the initial cost of the sensor or the matching software that is involved. Often, the life-cycle support cost of providing system administration and an enrollment operator can overtake the initial cost of the biometric hardware. The advantage biometric authentication provides is the ability to require more instances of authentication in such a quick and easy manner that users are

not bothered by the additional requirements. As biometric technologies mature and come into wide-scale commercial use, dealing with multiple levels of authentication or multiple instances of authentication will become less of a burden for users.

1.3 Origin of Biometric

The term biometrics is derived from the Greek words ‘bio’ means life and ‘metric’ means to measure. Interestingly, the term “biometrics” was not used to describe these technologies until the 1980s. The first reference found for the term “biometrics” was in a 1981 article in The New York Times. Centuries before automated biometric technologies became possible with the advent of computers, algorithm development, and processing power, there were several types of non-automated biometric methods used.

The first modern study of fingerprints was done by Johannes Evangelista Purkinje, a Czech physiologist and professor of anatomy at the University of Breslau. In 1823, he proposed a system of fingerprint classification.

In the late 19th century, Sir Francis Galton wrote a detailed study of fingerprints in which he presented a new classification system using prints of all 10 fingers. According to Galton’s calculations, the odds of two individual fingerprints being the same were 1 in 64 billion.

In 1903, the New York State Prison System began the first systematic use of fingerprints in the United States for criminals.

In 1904, the use of fingerprints began in Leavenworth Federal Penitentiary in Kansas and at the St. Louis police department.

In 1905, the U.S. army began using fingerprints. Two years later, the U.S. Navy began using fingerprints and was joined the following year by the Marine Corps.

The earliest work on machine recognition of faces can be traced back to the 1960s at a company called Panoramic Research in Palo Alto, California. This type of research, later referred to as artificial intelligence, was conducted by Woody Bledsoe, a pioneer in the field of automated reasoning. The technique he developed was called “man-machine facial recognition” and used a process known as feature extraction.

The year 1974 was a breakthrough year for automated biometrics, as the University of Georgia began using hand geometry in its dormitory food service areas. Both the Stanford Research Institute in the United States and the National Physical Laboratory in the United Kingdom had begun working on signature recognition systems.

In 1985, one of the first retinal scanning systems was deployed for securing access to a Defense Department facility at the Naval Postgraduate School. In the mid-1980s, the State of California began collecting fingerprints as a requirement for all driver license applications.

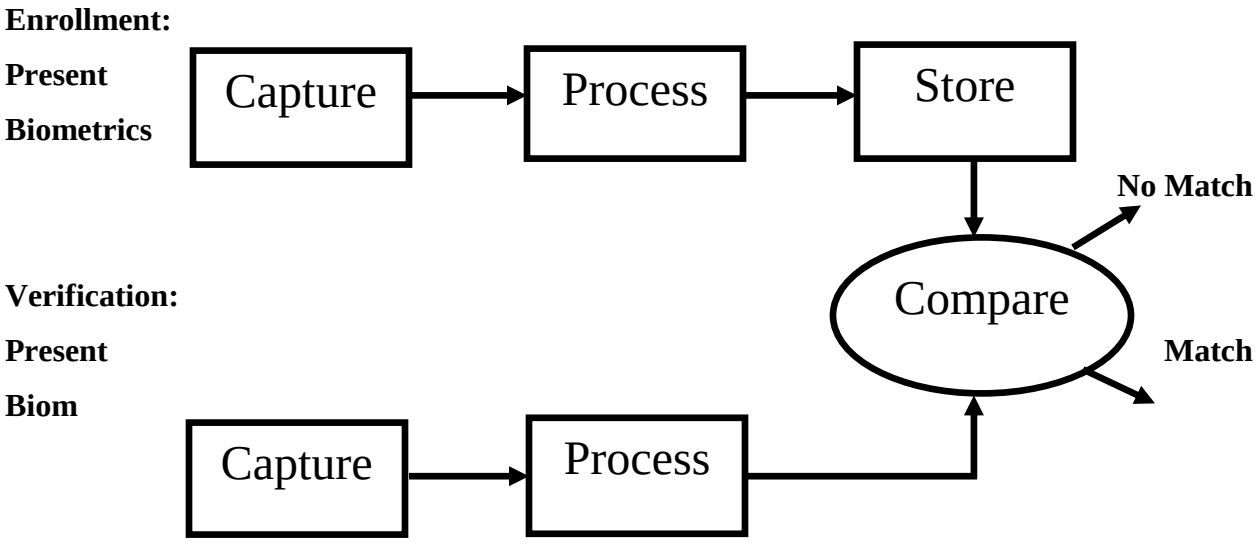
The first biometric industry organization, the International Biometrics Association, was founded in 1986–1987.

Iris recognition technology was developed in the 1980s by Dr. John Daugman at the University of Cambridge. Other new technologies produced during this time included facial thermography and the first commercially available facial recognition systems.

In 1998, the International Biometric Industry Association was founded in Washington, DC, as a non-profit industry trade association to advance the collective international interests of the biometric industry. The National Biometric Security Project was founded in 2001 to respond to the events of September 11, 2001, and the need for accelerated development and deployment of biometrics technologies. [28]

1.4 Working of Biometric Technologies

At their most basic level, biometric technologies are pattern recognition systems that use either image acquisition devices, such as scanners or cameras in the case of fingerprint or iris recognition technologies, or sound or movement acquisition devices, such as microphones or platens in the case of voice recognition or signature recognition technologies, to collect the biometric patterns or characteristics.



1.1 Generic biometric processes

The characteristics of the acquired samples considered the most distinctive between users and the most stable for each user are extracted and encoded into a biometric reference or template that is a mathematical representation of a person's biometric feature. These templates are stored in a database or on a smart card or other token. Then that template is used for comparison when recognition is warranted. Biometric systems are automated by hardware and software, allowing for fast, real-time decision making in identification situations.

Different biometric technologies offer varying features and benefits, which should be analyzed based on how and why they will be used. They all vary in performance, capabilities, infrastructure requirements, and cost, and all have their unique limitations and operating methodologies. While individual biometric devices and systems each have their own operating methodology, there are some generalizations that can be made as to what typically happens within a biometric system implementation.

Before an individual's identity can be verified via a biometric, a biometric template or model must first be created. This template serves as the template data against which subsequent samples/templates provided at time of verification are compared. For

some technologies, a number of templates or images are typically captured during enrollment in order to create a truly representative template via an averaging or best image candidate selection process. The template is then referenced against an identifier in order to recall it for comparison with a live sample at the transaction or entry point. The positive ID verification/identification of the subject during the enrollment procedure and quality of the resultant template or reference are critical factors in the overall success of a biometric application. The former refers to the corroborating identity documents, commonly referred to as breeder documents the user brings to the initial enrollment process. These documents, or other sources of validation, must undergo the highest scrutiny, lest the biometric be associated with a false identity.

1.5 Overview of Applications

Biometric technology has certain strengths and weaknesses which depending upon its application. It is therefore imperative that there is a clear understanding of the final application and their operational requirements before any purchase and implementation decisions are made. Although the use of each biometric is clearly different, some striking similarities can emerge when considering various applications.

Biometric applications can operate in either of two modes verification or identification. Verification is the process of comparing a presented biometric template with stored biometric references that are associated only with that specific user. Verification applications are often referred to as one-to-one matching or 1:1. During the verification process, a user will typically enter their name, unique ID number or present a token or ID card. This becomes their claim of identity. Then the user must authenticate or verify against their claim of identity by presenting their biometric sample and having the resulting template matched against the references associated with that user's enrollment record. In verification applications, the user is attempting to prove that they are the person that they claim to be. Verification is commonly used in access control applications where a person has already been granted privileges or access rights and the system needs to verify that the person seeking access under that name or identity is, in fact, that person.

In identification applications, the system is attempting to determine if the person is known to the system, with or without a claimed identity, by comparing the presented biometric sample and resultant template with all known references in the database. Identification is also referred to as one-to-many matching or 1:N. Identification applications are typically used for law enforcement investigations or to screen applicants for entitlement benefits to make sure that the person is not already enrolled in the system and receiving benefits under another name or identity. Identification is often performed during or immediately following the initial enrollment of the person and may not provide an immediate result depending on the matching speed of the technology and the number of records being matched.

1.6 Personal Biometric Criteria

Any human biological or behavioral characteristics can become a biometric identifier, provided the following properties are met [9]

(i) Universality
(ii) Distinctiveness
(iii) Permanence
(iv) Collectability

1.6.1 Universality

Every person should have the characteristic. There are always exceptions to this rule: mute people, people without fingers, or those with injured eyes. These exceptions must be taken into account through work-around such as conventional non-biometric authentication processes. Most biometric devices have a secure override if a physical property is not available, such as a finger, hand, or eye. In these cases, the person is assigned a special access device, such as a password, PIN, or secure token. This special access code or token is entered into the biometric device to allow access.

1.6.2 Distinctiveness

No two people should have identical biometric characteristics. Monozygotic twins, for example, cannot be easily distinguished by face recognition and DNA-analysis systems, although they can be distinguished by fingerprints or iris patterns.

1.6.3 Permanence

The characteristics should not vary or change with time. A person's face changes significantly with aging and a person's signature and its dynamics may change as well, sometimes requiring periodic re-enrollment. The degree of permanence of the biometric feature has a major impact on system design.

1.6.4 Collectability

Obtaining and measuring the biometric features should be easy, non-intrusive, reliable, and robust, as well as cost effective for the application

1.7 Biometric System-Level Criteria

The preceding personal biometric criteria may be used for evaluating the general viability of the chosen biometric identifier. Once incorporated into a system design, the following criteria are key to assessing a given biometric system for a specific application:

(i) Performance
(ii) Circumvention
(iii) Acceptability

1.7.1 Performance

Performance refers to the accuracy, resources, and environmental conditions required achieving the desired results.

1.7.2 Circumvention

Circumvention refers to how difficult it is to fool the system by fraudulent means. An automated access control system that can be easily fooled with a fingerprint prosthetic

or a photograph of a user's face does not provide much security—particularly in an unattended environment.

1.7.3 Acceptability

Acceptability indicates to what extent people are willing to accept the biometric system. Face recognition systems are personally not intrusive, but there are countries where taking photos or images of people are not viable. Systems that are uncomfortable to the user, appear threatening, require contact that raises hygienic issues, or are basically non-intuitive in practical use will probably not find wide acceptance.

1.8 Key Elements of Biometric Systems

There are four universal elements to all biometric systems. Key issues and considerations surrounding the four universal elements of all biometric-based systems can be described as follows

(i) Enrollment
(ii) Biometric Template or Reference
(iii) Comparison
(iv) Networking

1.8.1 Enrollment

Proper enrollment instruction and training are essential to good biometric system performance. Enrollment is the first stage for biometric system set-up because it generates the template that will be used for all subsequent comparison and user recognition. In enrollment, a biometric system is trained to recognize a specific person. Typically, the reader takes multiple samples of the same biometric that is presented by the user/enrollee and averages them or selects the best quality sample to produce an enrollment reference or template. Not all biometric systems require the linkage of users to "real world" identities. In fact, a number of companies have actively promoted the use of "anonymous" biometrics, linking users only to the biometric template, without any record of "real" name or other identifier. In most applications, however, there is a need to link

users to their legal identities for the purposes of accountability and certification of external authorizations. In these cases, the user/enrollee first provides his/her identification document, such as a government-issued ID card, passport, or driver license. Since the biometric template is linked in many biometric systems to the identity specified the identification document, this identification must be thoroughly authenticated. He/she then presents his/her biometric to the biometric reader. The features of the presented biometric are read, calculated, coded, and stored as the enrollment template for future comparisons.

Biometric template size varies, depending on the vendor and the type of biometric technology. Templates can either be stored in a central database, or within a biometric reader, or on smart cards or other tokens. For some biometric technologies, changes in the user's position or variations in the lighting surrounding the reader, for example, can affect template generation. Ideally, when the biometric system is deployed, enrollments and daily usage will be done in the same environment, using the same equipment. For example, if voice verification is used in an environment where there is background noise, both the enrollment voice template and live voice templates [presented for recognition] should be captured in the same environment. It is important to remember that the quality of the initial enrollment template and the absolute validity of the initial ID document that is used to verify a person's identity prior to biometric enrollment are critical to the overall success of the biometric- based system that requires linking of users to "real world" identities and authorizations.

A complete biometric system or sub-system should include a justification for the need to link to external identities, and if that justification proves adequate, incorporate a process or procedure for pre-validation of claimed identity before the candidate for enrollment is accepted.

1.8.2 Biometric Reference

The data that is captured during enrollment is stored in the biometric system as a template or reference. The biometric system software will use a proprietary algorithm to extract features that are appropriate to that biometric as presented by the user, or enrollee. It is important to note that biometric templates are only a record of distinguishing features

of a person's biometric characteristic or trait. Templates are usually not actual images of the fingerprint, iris, or hand, etc. Biometric templates are generally only numerical representations of key data points read in a person's biometric feature.

Typically, templates are relatively small in terms of data-storage size when compared with the original image or source pattern data and, therefore, allow for more efficient storage and quick processing. Each must be stored, whether in a central database or on a smart card or other token, so when the user attempts to access the system, the characteristics derived from the live biometric can be directly compared to the enrolled template. Biometric experts claim that it is virtually impossible to reverse-engineer or recreate exactly a person's original biometric image, such as a fingerprint or iris image, from a biometric template, although it is quite possible in some types of biometrics to reverse-engineer an artificial image capable of generating the same template.

1.8.3 Comparison

Comparison is the act of comparing one or more acquired biometric sample to one or more stored biometric templates to determine whether they "match," that is, come from the same source. Upon comparison, a score representing the degree of similarity between the sample and template is calculated, and this score is compared to the threshold to make a match or no-match decision. For algorithms for which the similarity between the two is calculated, a score exceeding the threshold is not considered a match. For algorithms for which the difference between the two is calculated, a score below the threshold is considered a match. Depending on the setting of the threshold in identification systems, sometimes several enrollment templates can be considered matches to the live, presented sample, with better scores corresponding to better matches.

1.8.4 Networking

There are possible variations on a theme with regard to networks. Some biometric systems/readers have integral networking functionality, often via RS485 or RS422, with a proprietary protocol. This may enable networking a number of readers together with little or no additional equipment involved, or maybe with a monitoring PC connected at one end of the network.

Alternatively, the networking, message passing, and monitoring system may be designed by the system integrator, taking advantage of generic biometric Application Program Interfaces for accessing reader functions directly. This allows the most flexibility and control over systems design, provided that the selected biometric reader and underlying device drivers and control software support network applications. Still, another option may be to use the vendor's network for message passing and primary interconnection, coupled with custom software at the monitoring point, which may in turn interface with other systems.

1.9 Biometric Performance Measures

The performance of a biometric system is measured in certain standard terms. These are main three types of standard terms given below-

(i) False Acceptance Rate (FAR)
(ii) False Rejection Rate (FRR)
(iii) Equal Error Rate (EER)

1.9.1 False Rejection Rate

FRR is the ratio of the number of number of authorized users rejected by the biometric system to the total number of attempts made**.** False Rejection Rate known as type 1 error, when a legitimate user is rejected because the system is not find that the current biometric data of the user similar to the biometric data in the templates that are stored in the database. Now since there is no zero error in a system that is in the real world, we calculate the FRR using a simple math equation:

$$\mathrm{FAR}(\lambda) = \frac{\text{Number of False Rejection}}{\text{Total Number of Attempts}}$$

1.9.2 False Acceptance Rate

FAR is the ratio of the number of unauthorized users accepted by the biometric system to the total of identification attempts to be made**.** This is also known as type 2 error, False Acceptance Rate is when an imposter is accepted as a legitimate user, This happens when the system find that the biometric data is similar to the template of a legitimate user. FAR is calculated by

$$FAR(\lambda) = \frac{\text{Number of False Attempts}}{\text{Total Number of Attempts}}$$

Where (λ) = Security Level

1.9.3 Equal Error Rate

Equal error rate is a point where FRR and FAR are same. The ERR is an indicator on how accurate the device is, the lower the ERR is the better the system.

Now if we have a score of the FAR & FRR we can create a graph that indicates the depends of the FAR & FRR on the threshold value. The following is graph is an example:

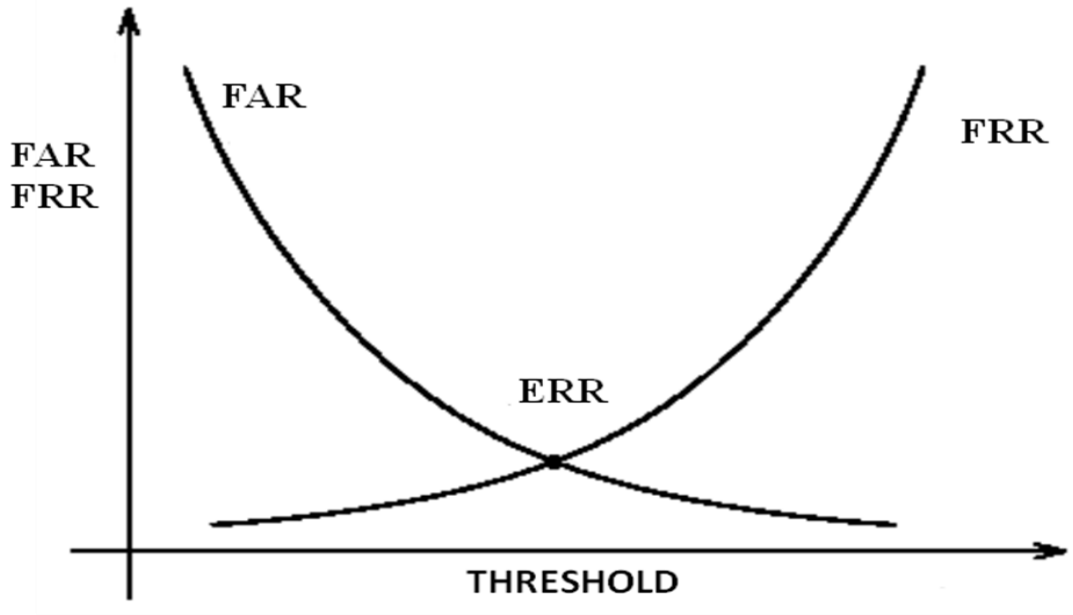


Fig 1.2: Equal error rate

As we can see the curves of FAR and FRR cross at a point where FAR and FRR are equal, this value is called Equal Error Rate or the Crossover Accuracy. If we have two devices with the equal error rates of 1% and 15% than we know that the first device with the ERR of 1% is more accurate than the other. Most manufactures often publish the best achieved rates and not all manufactures use the same algorithms for calculating the rates.

1.10 Commonly Used Biometric Technologies

When used for personal identification, biometric technologies measure and analyze human biological and behavioral characteristics. Identifying a person's biological characteristics is based on direct measurement of a part of the body, such as fingerprints, hand structure, facial features, iris patterns, and others. The corresponding biometric technologies are fingerprint recognition, hand geometry, facial, and iris recognition, among others.

Biometric systems using predominantly behavioral characteristics are based on data derived from actions, such as speech and signature, for which the corresponding biometrics are speaker verification and dynamic signature analysis. Almost all biometrics, however, incorporate both biological and behavioral components. Biometrics is an effective personal identifier because the characteristics measured are distinct to each person. [28]

Unlike other identification methods that use something a person has, such as an identification card to gain access to a building, or something a person knows, like a password or PIN to log on to a computer system, the biometric characteristics are integral to something a person is. Because biometrics is tightly bound to an individual, they are more reliable, cannot be forgotten, and are less likely to be lost, stolen, or otherwise compromised. Some commonly used biometrics system are given below-

1.10.1 Fingerprint Recognition

The patterns of friction ridges and valleys on an individual's fingertips are unique to that individual. For decades, law enforcement has been classifying and determining

identity by matching key points of ridge endings and bifurcations. Fingerprints are unique for each finger of a person including identical twins. One of the most commercially available biometric technologies, fingerprint recognition devices for desktop and laptop access are now widely available from many different vendors at a low cost. With these devices, users no longer need to type passwords – instead, only a touch provides instant access. Fingerprint systems can also be used in identification mode. Several states check fingerprints for new applicants to social services benefits to ensure recipients do not fraudulently obtain benefits under fake names. New York State has over 900,000 people enrolled in such a system. [13]

1.10.2 Face Recognition

The identification of a person by their facial image can be done in a number of different ways such as by capturing an image of the face in the visible spectrum using an inexpensive camera or by using the infrared patterns of facial heat emission. Facial recognition in visible light typically model key features from the central portion of a facial image. Using a wide assortment of cameras, the visible light systems extract features from the captured images that do not change over time while avoiding superficial features such as facial expressions or hair. Several approaches to modeling facial images in the visible spectrum are Principal Component Analysis, Local Feature Analysis, neural networks, elastic graph theory, and multi-resolution analysis. Some of the challenges of facial recognition in the visual spectrum include reducing the impact of variable lighting and detecting a mask or photograph. Some facial recognition systems may require a stationary or posed user in order to capture the image, though many systems use a real-time process to detect a person's head and locate the face automatically. Major benefits of facial recognition are that it is non-intrusive, hands-free and accepted by most users.

1.10.3 Speaker Recognition

Speaker recognition has a history dating back some four decades, where the outputs of several analog filters were averaged over time for matching. Speaker recognition uses the acoustic features of speech that have been found to differ between individuals. These acoustic patterns reflect both anatomy and learned behavioral patterns.

This incorporation of learned patterns into the voice templates has earned speaker recognition its classification as a behavioral biometric. Speaker recognition systems employ three styles of spoken input: text-dependent, text-prompted and text independent.

Most speaker verification applications use text-dependent input, which involves selection and enrollment of one or more voice passwords. Text-prompted input is used whenever there is concern of imposters. The various technologies used to process and store voiceprints include hidden Markov models, pattern matching algorithms, neural networks, matrix representation and decision trees. Some systems also use "anti-speaker" techniques, such as cohort models, and world models.

Ambient noise levels can impede both collections of the initial and subsequent voice samples. Performance degradation can result from changes in behavioral attributes of the voice and from enrollment using one telephone and verification on another telephone. Voice changes due to aging also need to be addressed by recognition systems. Many companies market speaker recognition engines, often as part of large voice processing, control and switching systems. Capture of the biometric is seen as non-invasive. The technology needs little additional hardware by using existing microphones and voice-transmission technology allowing recognition over long distances via ordinary telephones.

1.10.4 Iris Recognition

This recognition method uses the iris of the eye which is the colored area that surrounds the pupil. Iris patterns are usually unique. The iris patterns are obtained through a video-based image acquisition system. Iris scanning devices have been used in personal authentication applications for several years. Systems based on iris recognition have substantially decreased in price and this trend is expected to continue. The technology works well in both verification and identification modes. Current systems can be used even in the presence of eyeglasses and contact lenses. The technology is not intrusive. It does not require physical contact with a scanner. Iris recognition has been demonstrated to work with individuals from different ethnic groups and nationalities.

1.10.5 Signature Verification

This technology uses the dynamic analysis of a signature to authenticate a person. The technology is based on measuring speed, pressure and angle used by the person when a signature is produced. One focus for this technology has been e-business applications and other applications where signature is an accepted method of personal authentication.

1.10.6 Ear Recognition

This is a relatively new biometric trait. Although it may seem like it the human ear does not have a completely random structure. It is unique enough for a people to be identified using features collected from their ear. Moreover like face it does not suffer from expression changes and makeup effects. Hair present on the ear however may cause problems for the biometric system. Also a change in brightness of the surrounding environment will adversely affect the system.

1.10.7 Veins Recognition

Veins have also been recognized as a unique characteristic that can be applied as a biometric for verification. Veins are developed before birth and remain highly stable throughout life, even differing between twins. Vascular pattern recognition systems identify a person by using the patterns of veins on their finger, back of the hand, or palm. A camera captures the vein pattern with a focus on the shape and location of the vein structure. Venous pattern recognition is particularly popular in Japan, and is currently in use in selected banks and ATMs throughout the country. [10]

1.10.8 Retina Recognition

The retina is a sensory tissue of the eye that consists of millions of photoreceptors which gather light rays and transform them into electrical impulses which then travel through the optic nerve into the brain to be converted into images. In the 1930s it was discovered that every retina possesses a unique blood vessel pattern and, for this reason, photographs of the blood vessel patterns of the retina could be used as a means of identification.

Retina biometric systems use a light source projected into the eye to scan the vein pattern of the retina. The error rates are claimed to be very low, but retinal scanning is a relatively expensive and intrusive process that could only be considered for high security applications with willing users**.** For these reasons, retina biometrics has tended to be used by large government departments or organizations with willing participants requiring access to highly secure material or environments.

1.10.9 Gait Recognition

Gait refers to the unique combination of motions by which people walk. An analysis of temporal and frequency components of motion from a radar sensor may be used to identify people walking at a distance. The primary use would appear to be in covert surveillance applications and intelligence gathering, where the ability to recognize people at standoff ranges would be valuable.

1.10.10 Keystroke Recognition

This is a behavioral biometric and can be used in combination with passwords. It analyses the patterns in the way the user types in the keys, like the time required to find the keys, the total speed etc. Besides being considerably cheaper to implement than other biometrics it is also much more unobtrusive as typing on a keyboard is much easier on the user than the data collection method of most other biometrics. This however is not very robust as it is susceptible to user mood and fatigue. The keyboard being used also plays a major factor as a user will have different dynamics on keyboards with different layouts. Also the actual dynamics may change over time.

Recent advances in biometric technology have resulted in increased accuracy at reduced costs; biometric technologies are positioning themselves as the foundation for many highly secure identification and personal verification solutions. Today's biometric solutions provide a means to achieve fast, user-friendly authentication with a high level of accuracy and cost savings. Many areas will benefit from biometric technologies. Highly secure and trustworthy electronic commerce, for example, will be essential to the healthy growth of the global Internet economy. Many biometric technology providers are already delivering biometric authentication for a variety of web-based and client/server

based applications to meet these and other needs. Continued improvements in technology will bring increased performance at a lower cost. Interest in biometrics is growing substantially. Evidence of the growing acceptance of biometrics is the availability in the marketplace of biometric-based authentication solutions that are becoming more accurate, less expensive, faster and easy to use. While biometric authentication is not a magical solution that solves all authentication concerns, it will make it easier and cheaper for you to use a variety of automated information systems – even if you're not a secret agent.

1.11 Motivation

The practical problem of hand geometry based system involves the use of pegs to fix the position of palm. This is motivated by the limited ability of the hand shape acquisition system to implicitly register different hand images using the rigid pegs on the hand scanner platen. If the user has not been properly trained or if he/she does not cooperate properly, then the resulting images are not aligned and the system's verification performance degrades. Therefore, it is necessary to align the acquired hand shapes before extracting the feature vector used for verification.

1.12 Objectives of the Thesis

This thesis aims to develop a hand geometry recognition program in Matlab that uses the information of the hand geometry to find a feature vector from a set of hand images. Specifically, it aims to do the following:

(i) to detect the valley and tip point of the image of a hand;
(ii) to extract the features from the hand image;
(iii) to compare the features of the test image from the data existing on the database;
(iv) to show the decision of the system whether the owner of the test image is a valid user of the system or not.

CHAPTER-2

LITERATURE SURVEY

Y. Bulatov et.al has given a geometric classifier utilized in hand recognition. As in the proposed system in a document scanner is used to collect hand data. Also very few restrictions are imposed on the positioning of the hand on the scanner. A total of 30 different features are obtained from a hand. For each individual 3 to 5 of the persons data images are used as the training set. In the 30 dimensional feature space a bounding box is found for each of these training sets. The distance of the query image to these bounding boxes is used as the measure of similarity. The threshold is determined by experimentation on the database. [4]

Bahareh Aghili et.al has presented an approach to personal verification and identification using hand geometry. Having extracted, fifteen features of users' right hand, Fingers' width, Area and circumference, are classified with two different pattern recognition systems Euclidean and Absolute Distance. The algorithm has been tested on 500 pictures of 50 users. As the pictures are captured with a scanner without any special instrument for fixing the placement, the purposed method is an inexpensive and easy to use. The experimental result shows the system performance in identification and verification. [30]

Ahmed Mostayed et.al has proposed an authentication scheme from hand images. Instead of dealing with hand measurements, typically termed as 'hand geometry', this method verifies with entire hand shape. Peg free and position invariant features are calculated using Radon Transform. Low resolution hand images captured by a document scanner are processed to extract feature vectors. The proposed scheme is tested on a data set of136 images with simple Euclidian norm based match score. The method attained an Equal Error Rate (EER) of 5.1%. [32]

Márjory Cristiany et.al has presented benefit of a novel multi agent approach in a multimodal biometrics identification task. In this paper they evaluate the merits of using

multimodal structures, and investigate how fundamentally different strategies for implementation can increase the degree of choice available in achieving particular performance criteria. They illustrate the merits of an implementation based on a multi agent computational architecture as a means of achieving high performance levels when recognition accuracy is a principal criterion. They also set out the relative merits of this strategy in comparison with other commonly adopted approaches to practical system realization. In particular they propose and evaluate a novel approach to implementation of a multimodal system based on negotiating agents. [33]

Vivek Kanhangad et.al has given a new biometrics verification method by combining 2D and 3D hand geometry features. This paper investigates a new approach to achieve performance improvement for hand geometry systems by simultaneously acquiring three dimensional features from the presented hands. The proposed system utilizes a laser based 3D digitizer to acquire registered intensity and range images of the presented hands in a completely contact-free manner, without using any hand position restricting mechanism. Two new representations that characterize the local features on the finger surface are extracted from the acquired range images and are matched using the proposed matching metrics. This approach is evaluated on a database of 177 users, with 10 hand images for each user acquired in two sessions. The experimental results suggest that the 3D hand geometry features have significant discriminatory information to reliably authenticate individuals. [31]

Leong Lai Fong et.al has presented a comparison study on hand recognition approaches. They compare various approaches done in three categories, namely hand geometry, hand contour and palm print. After that, they further discuss the performance of the methodology as stated in the comparison. Thereby, this paper serves the purpose as a gateway for hand recognition literature survey to the novel or interested researchers. [34]

S. Selvarajan et.al has presented a new approach for human identification and recognition system. In this paper they present a model for hand geometry based human recognition. In this system some distinct features are used that enhance the accuracy of the recognition. They are using a simple and very fast algorithm for hand image

segmentation employing filtering, edge detection and region labeling techniques and arrived at comparable segmentation results. In addition to the above, they propose the usage of some distinct features, which would enhance hand recognition much more precisely. [26]

C Chandra Sekhar et.al has proposed a method to use hand contour as a feature vector for hand geometry. The aim of this hand based biometric system is to capture the uniqueness of the shape of an individual's hand. In this paper they explore traits like the shape of the hand contour and palm print texture as potential biometric verifiers. The novelty of this approach is the implicit capturing of the individual features in a single entity of hand contour. The sequence information of the contour is then fed to a hidden Markov model classifier. For palm print the feature vector used for classification is the texture energy measure. Texture provides a high-order description of the local image content. The texture analysis is based on the well documented Laws convolution masks. Linear and Gaussian kernel support vector machines are employed as classifiers. This scheme is viable for human authentication. [17]

Vit Niennattrakul et.al has proposed a hand geometry verification system using time series conversion techniques and dynamic time warping distance measurement with Sakoe-Chiba band. This system demonstrates many advantages, especially ease of implementation and small storage space requirement using time series representation. In this paper, they proposed a novel hand geometry verification system that exploits dynamic time warping distance measure and the R-K band learning method to further improve the system performance. In the system, two time series conversion techniques are applied, i.e., the centroid-based conversion technique and the angle-based technique. This experiment reveals that the centroid-based technique generally outperforms the angle-based technique by achieving lower EER and higher TSR. [29]

Raymond Veldhuis et.al has been presented comparison of the performance of hand geometry recognition based on high-level features and on low-level features. They have given a new method for hand-geometry verification, based on a model of the contour of the hand. In this method, the dimensionality of the feature vector is reduced by a combination of principal component and linear discriminator analysis. In an evaluation

experiment based on a data set containing a total of 850 hand contours of 51 subjects, an equal-error rate of 4% was measured. This is substantially better the equal-error rate of the standard method for hand-geometry verification, measured on the same data. [1]

Delac Kresimir et.al has given a survey of biometric recognition methods. Biometrics refers to an automatic recognition of a person based on her behavioral and/or physiological characteristics. Many business applications will in future rely on biometrics since using biometrics is the only way to guarantee the presence of the owner when a transaction is made. For instance, fingerprint-based systems have been proven to be very effective in protecting information and resources in a large area of applications. Although companies are using biometrics for authentication in a variety of situations, the industry is still evolving and emerging. At present, the amount of applications employing biometric systems is quite limited, mainly because of the crucial cost-benefit question: supposing biometrics does bring an increase in security, will it be worth the financial cost?The future probably belongs to multimodal biometric systems as they alleviate a few of the problems observed in unique modal biometric systems. Multimodal biometric systems can integrate information at various levels, the most popular one being fusion at the matching score level. Besides improving matching performance, they also address the problem of non universality and spoofing. [3]

Arafatur Rahman et.al has proposed an efficient technique for human verification using finger stripes geometry. Which is an efficient, simple, fast, easy to handle and cost effective compared with other biometric human verification technique. This finger stripe based verification consists of tow main attributes feature extraction by image processing and feature learning by ANN. The distance based nearest neighbor algorithm, which shows greater accuracy than NN. [24].

Aythami Morales et.al has presents a novel contact-free biometric identification system based on geometrical features of the human hand. The right hand images are acquired by a commercial modified webcam with a 320x240 pixels resolution. The hand is illuminated by an infra-red light to solve segmentation problems in a real environment. The geometrical features are obtained from the binary images and consist in normalized measures of the index, middle and ring fingers. A Support Vector Machines is used as

verifier. A decision level fusion has been used for the final recognition with an EER of 3.4%. [27]

Karen H. Suaverde et.al has proposed a hand geometry feature system designed to identify the users of a system and prevent non-users in using the said system. It consists of a database where all the information about the authenticated users are stored. The systems extract the features of a test image and compare it with the stored information on the database. The system outputs the information of the identified user or an error if the owner of the hand does not exist in the system. The system was implemented using C++. The program gave a successful rate of 95% in identifying a handprint, a 0% False Reject Error (Type I error), where both handprints from the same participant did not match and a 5% False Accept Error where handprints coming from different participants returned a match. [25]

Sotiris Malassiotis et.al has proposed a biometric authentication system based on measurements of the user's 3D hand geometry. The system relies on a novel real-time and low-cost 3D sensor that generates a dense range image of the scene. By exploiting 3D information the system able to limit the constraints usually posed on the environment and the placement of the hand, and this greatly contributes to the unobtrusiveness of the system. Efficient, close to real-time algorithms for hand segmentation, localization and 3D feature measurement are described and tested on an image database simulating a variety of working conditions. [23]

CHAPTER -3

HAND GEOMETRY BIOMETRICS

3.1 Introduction

Hand geometry recognition systems are based on a number of measurements taken from the human hand, including its shape, size of palm, and lengths and widths of the fingers. Commercial hand geometry-based verification systems have been installed in various places around the world. The technique is very simple relatively easy to use, and inexpensive. Environmental factors such as dry weather or individual anomalies such as dry skin do not appear to have any negative effects on the verification accuracy of hand geometry-based systems.

The hand images can be obtained by using a simple setup including a web cam. However, other biometric traits require a specialized, high cost scanner to acquire the data. The user acceptability for hand geometry based biometrics is very high as it does not extract detail features of the individual. Thus, for applications where the biometric features are needed to be distinctive enough for verification, hand geometry can be used.

An individual's hand does not significantly change after a certain age. Unlike fingerprints, the human hand is not unique. Individual hand features are not descriptive enough for identification. However, hand biometric recognition systems are accurate for the verification purposes when combined with various individual features and measurements of fingers and hands.

3.2 Hand Geometry System

Biometric hand recognition systems measure and analyze the overall structure, shape and proportions of the hand, e.g. length, width and thickness of hand, fingers and joints; characteristics of the skin surface such as creases and ridges. Some hand geometry biometrics systems measure up to 90 parameters. As hand biometrics rely on hand and finger geometry, the system will also work with dirty hands. The only limitation is for people with severe arthritis who cannot spread their hands on the reader. The user places

the palm of his or her hand on the reader's surface and aligns his or her hand with the guidance pegs which indicate the proper location of the fingers. The device checks its database for verification of the user. The process normally only takes a few seconds. To enroll, the users place his or her hand palm down on the reader's surface. A hand geometry system is shown in fig 3.1.

Fig 3.1 Hand geometry system

The benefits of hand biometric systems are given below-

(i) Small amount of data required to uniquely identify a user, so a large number of templates can be easily stored in a standalone device: Hand biometric systems will generally only require a template size of 10 bytes, which is much smaller than most other biometric technologies e.g. fingerprint systems require 250 to 1,000 bytes and voice biometric systems require 1,500 to 3,000 bytes.

(ii) Low FTE rates

(iii) Easy to use

(iv) Non intrusive

3.3 Module of Hand Geometry Biometric System

The module of hand geometry biometric system is shown in fig 3.2.

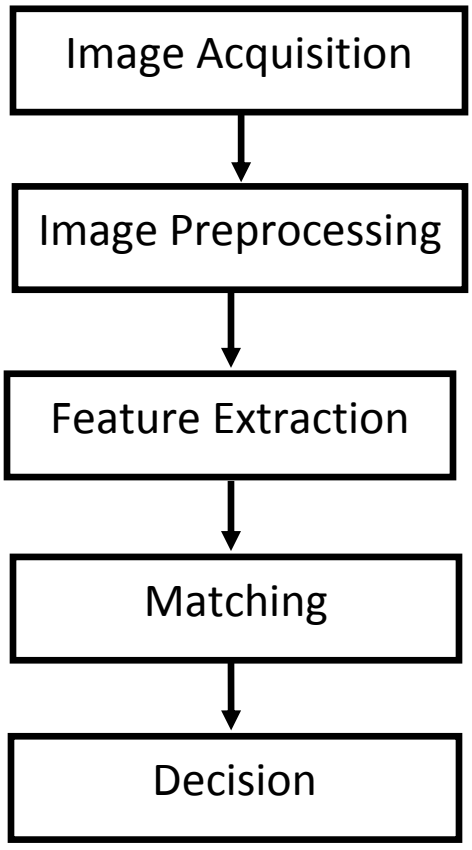


Fig 3.2 Module of hand geometry biometric system

A biometric system consists of five important modules image acquisition, image preprocessing, feature extraction, matching, and decision. Firstly image of hand is captured through a digital camera/scanner then it is fed to the next module i.e. image preprocessing module. The role of the preprocessing module is to clean up the noise because the input image having some noise due to dust on the palm, atmospheric conditions.

The processing module is used to prepare the image for feature extraction. The feature extraction module is very important module in a hand geometric system. The function of this module is to extract and store features from the input image. The output of the feature extraction module is the measure of features like finger length, finger width, palm width etc. The next module of this system is matching. Here the features extracted in the previous section are matched up with the features of that individual previously stored in the database. Therefore, matching is a straight one to one comparison between scanned and stored data. The last module of the hand geometrics biometric system is decision module. This module give a 'yes' or 'no' response to the question 'am I who I claim to be?' to a high degree of accuracy.

3.3.1 Image Acquisition

Image acquisition is the first step in a hand geometry biometrics system. The image acquisition involves capturing and storing digital images from vision sensors like color digital cameras, monochrome and color CCD cameras, video cameras, scanners etc. The image acquisition system comprises of a light source, a digital camera/scanner. The input image is a color/grayscale image of the hand palm. In this proposed system images are acquiesced through a digital camera. It is necessary that the fingers are separated from each other. However it is not required to stretch the fingers to far apart as possible. The hand should be placed in a relaxed state with fingers separated from each other. Since features such as length and width which are dependent on the image size and resolution are being used, it is critical that to have uniform size of images.

There are various format stored for the images such as .jpeg, .tiff, .png, .gif and bmp. The captured images are stored in one of the following formats on the computer for possible image processing.

Fig 3.3 Image acquisition

3.3.2 Image Preprocessing

The next stage is image preprocessing module. Image preprocessing relates to the preparation of an image for later analysis and use. Images captured by a camera or a similar technique are not necessarily in a form that can be used by image analysis routines. Some may need improvement to reduce noise; other may need to simplified, enhanced, altered, segmented, filtered, etc. The role of the preprocessing module is to prepare the image for feature extraction. The first step in the preprocessing block is to transform the color image into a gray scale image and this result to noisy gray scale image. In the next step, filtering is used in order to cancel the presented noise. Then, edge detection algorithm is applied for obtaining edge of the noiseless gray scale image. Image preprocessing module is consist of following operations-

(i) Gray scale image

(ii) Noise removal

(iii) Edge detection.

(i) Gray Scale Image

In this proposed system hand image is captured through digital camera so the original image is colored image. For digital image processing it is necessary first colored hand image convert in to grayscale image. Basically grayscale is an image in which the value of each pixel is a single sample, that is, it carries only intensity information. Images of this sort, also known as black-and-white, are composed exclusively of shades of gray, varying from black at the weakest intensity to white at the strongest.

Now color hand image is converted in to gray scale image with noise because there is some noise present in the input colored image due to dust and atmospheric conditions. This noise removal is therefore essential for the system.

(ii) Noise Removal

The next step in image preprocessing is noise removal. It is necessary to remove the noise from the image because it may produce difference between the actual palm and captured image. This causes the variation in data base feature and measured feature and also affected the accuracy of the system. Another reason of noise removal is that edge detection is difficult in noisy images, since both the noise and the edges contain high-frequency content

Basically the noise produced in the image is due to device using for capturing image, atmosphere condition or surrounding. There are many methods to remove the noise in Matlab. In this proposed system the noise is removed by wiener2 filter. So before extracting features from the image, it is very important to remove the noise from the image. Attempts to reduce the noise result in blurred and distorted edges. Operators used on noisy images are typically larger in scope, so they can average enough data to discount localized noisy pixels. This results in less accurate localization of the detected edges.

(iii) Edge Detection

In order to extract geometric features of the palmprint it is required that the image contains only edges. Edge detection is the process of localizing pixel intensity transitions. The edge detection has been used by object recognition, target tracking, segmentation, and etc. Let's consider the boundary detection under image enhancement because the goal is to emphasize features of interest i.e. boundaries and attenuate everything else.

An edge is a collection of connected high frequency points in an image. Visually, an edge is a region in an image where there is a sharp change in intensity of the image. Edge detection refers to the operation performed on an image to detect the edges in an image. Edge detection plays a vital role in object detection and feature extraction and plays pivotal role in machine vision. There are different types of edges – step edges, roof edges, line edges, color edges, gray level edges, texture edges etc. Not all edges are detected by all edge detection operators. Each operation has its specific specialty in edges and better the edge detection, usually; more complex and costly is the operation.

Therefore, the edge detection is one of the most important parts of image preprocessing. There mainly exist several edge detection methods Sobel, Prewitt, Roberts, Canny. These methods have been proposed for detecting transitions in images. It is very important for any edge detection algorithm not to miss any edges. It is also important that no non edges are recognized as edges. These two criteria define the error rate of the edge detection filter.

Edges play quite an important role in many applications of image processing, in particular for machine vision systems that analyze scenes of man-made objects under controlled illumination conditions. Detecting edges of an image represents significantly reduction the amount of data and filters out useless information, while preserving the important structural properties in an image.

3.3.3 Feature Extraction

The next module of hand geometry biometrics is feature extraction. In pattern recognition and in image processing, feature extraction is a special form of

dimensionality reduction. When the input data to an algorithm is too large to be processed and it is suspected to be notoriously redundant means much data, but not much information then the input data will be transformed into a reduced representation set of features also named features vector. Transforming the input data into the set of features is called feature extraction. If the features extracted are carefully chosen it is expected that the features set will extract the relevant information from the input data in order to perform the desired task using this reduced representation instead of the full size input.

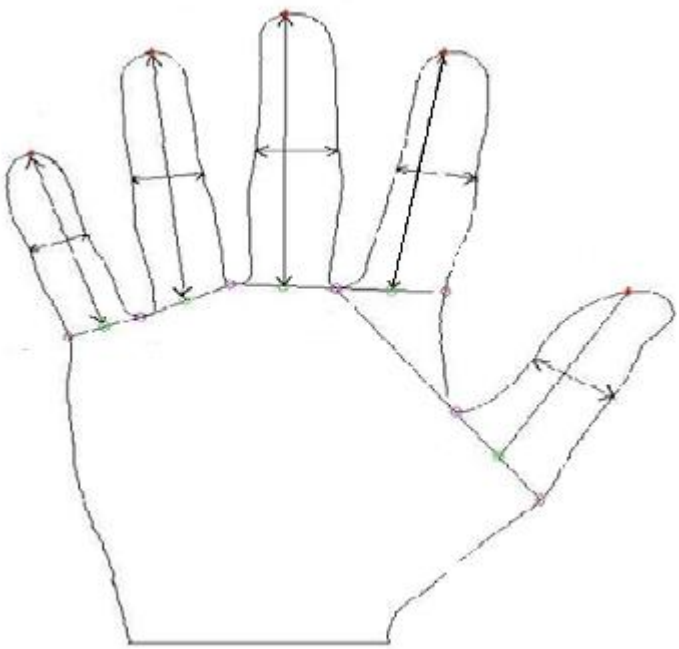


Fig 3.4 Features extracted from the input image

The hand geometry-based authentication system relies on geometric invariants of a human hand. Typical features include length and width of the fingers, aspect ratio of the palm or fingers, thickness of the hand, etc. The first feature that can be extracting is the length of a finger. The second major feature is the width of the finger. One or more measurements can be taken for the width at varying points along the finger. The length of the lines on the finger can also be used as the measure of finger width. Since the fingers may not have uniform width usually two or more measurements are taken for each finger along different points

3.3.4 Matching

The last module of the biometric system is matching. The feature matching determines the degree of similarity between stored feature vector and claimed feature vector. Here the features extracted in the previous section are matched up with the features of that individual previously stored in the database. The matching step actually quantifies the level of similarity between two hand templates. Besides that, most hand recognition systems also incorporate the optional step of updating the reference template in the enrollment database. Over the years, hand recognition is said to be more suitable for verification purpose only, as the hand features are not unique for everyone. The possibility for having two people with similar hand features increases with large population.

Distance functions are used to decide whether the claimer is the claimed person or not. In this proposed system absolute distance function is used for matching the feature vector. Absolute distance is defined as

$$D_a = \sum_{i=1}^{d} | y_i - f_i |$$

Where f_i = h (f_1, f_2 . . . f_d) is the feature vector with d dimension of a registered user in the database, and y_i = h (y_1, y_2 . . . y_d) is the feature vector of an unknown or a claimer. Therefore, the distance between claimer and register user is the distance between claimer feature vector y_i and database feature vector f_i.

3.3.5 Decision

After calculating the distance, the system compares the result with a predefined threshold and classifies the claimer. The system accepts the claimer if and only if the calculated distance is lower than the threshold, and it rejects the claimer if and only if the calculated distance is higher than the threshold.

3.4 Complete Block Diagram of Hand Geometry Biometrics System

Typical verification system usually consists of two major component enrollment and verification. First, data is acquired from a sensor then the input data is sent to a feature extractor to transform the data to numerical features. When the system is in an enrollment phase, input features, from the feature extractor, will be added to a database as a stored template labeled with a user identity. During the verification phase, a matcher retrieves the stored templates corresponding only to the claimed username, and a distance measure is used to calculate similarity between the input features and these retrieved templates. If the distance is less than a pre-defined threshold, the system accepts, otherwise, it rejects.

The main two phase of a hand geometry biometric system are given below-

(i) Enrollment phase

(ii) Verification phase

3.4.1 Enrollment Phase

Enrollment is the first stage for hand geometry biometric system set-up because it generates the template that will be used for all subsequent comparison and user recognition. Proper enrollment instruction and training are essential to good hand geometry biometric system performance. In enrollment, a biometric system is "trained" to recognize a specific person. Typically, the reader takes multiple samples of the same biometric that is presented by the user and averages them or selects the best quality sample to produce an enrollment reference or template.

It is important to remember that the quality of the initial enrollment template and the absolute validity of the initial ID document that is used to verify a person's identity prior to biometric enrollment are critical to the overall success of the biometric- based system that requires linking of users to real world identities and authorizations.

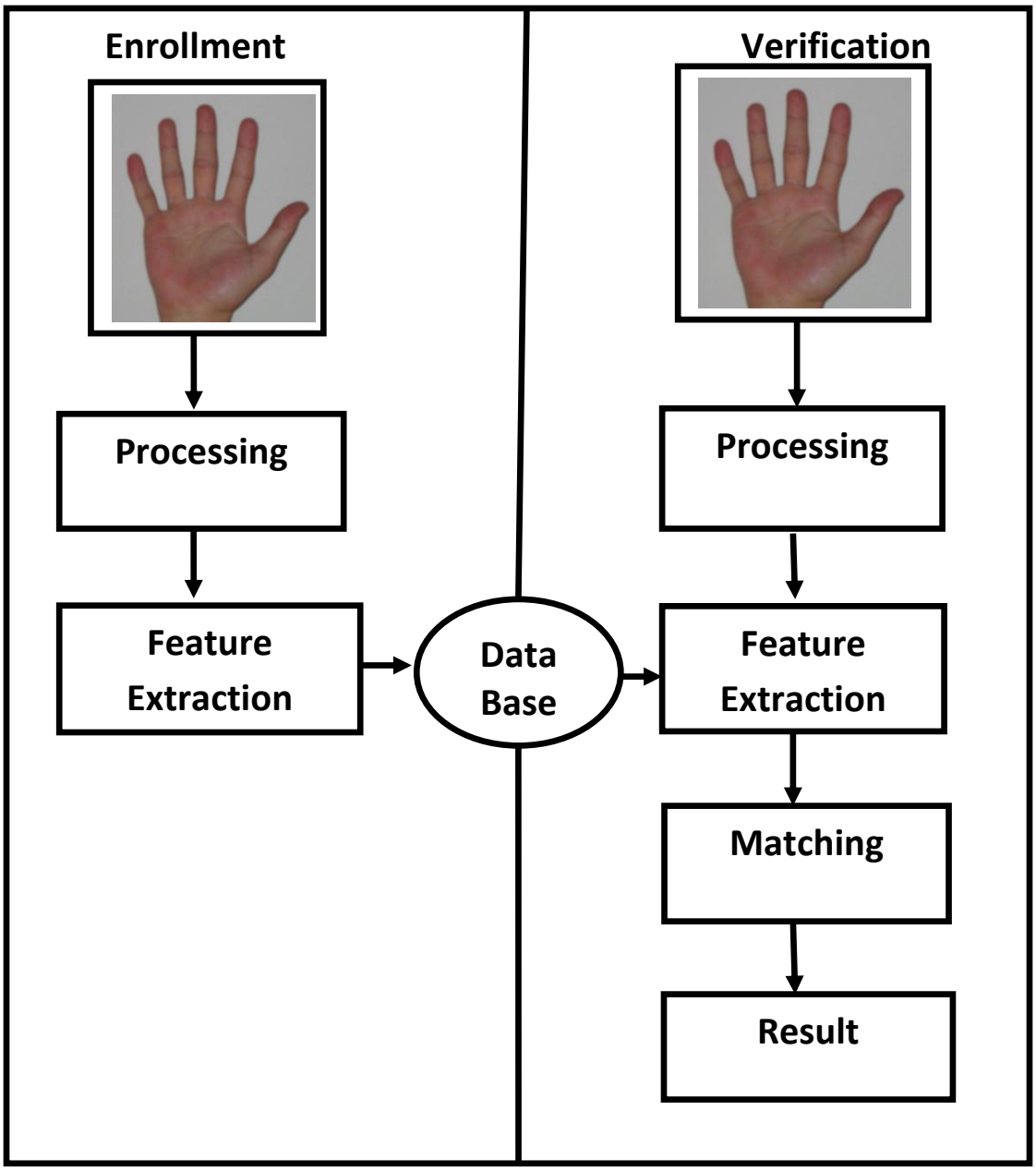


Fig3.5. Components of a biometric system

3.4.2 Verification Phase

In the verification phase, the system validates a person's identity by comparing the captured biometrics data with his/her own template stored in the system database. In

this phase first, data is acquired from a digital camera. Then the input data is sent to a feature extractor to transform the data to numerical features In such a system, an individual who desires to be recognized claims an identity, usually via PIN, a user name or a smart card and the system conducts a one to one comparison to determine whether the claim is true or not.

Biometric verification performs the same function as a PIN number, password or signature, but as it involves measurements performed on a physical biometric it is usually deemed to be more secure, as the physical biometric is hard to copy. Essentially, therefore, verification is a straight 'one to one' comparison between scanned and stored data.

3.5 Applications of Hand geometry Biometrics

Hand biometric systems are currently among the most widely used biometric technologies.

(i) Cash Vault Applications

A cash vault mantrap has two door and entry and an exit, and a hand scanner inside verifies the entrants. Number of people entering from the public side of mantrap is recorded by a personnel counter and a programmable logic controller reports the count to the hand scanner which must match the number of people using the scanner.

(ii) Dual Custody Applications

In dual custody access control, two different people must verify before the scanner sends an output. Dual custody concept common in physical security, has several variations and can be translated easily to hand scanner electronic access control.

(iii) Anti-pass Back

A common-access control function in which a user is prevented from passing a card to an accomplice. Anti-pass back seems redundant for hand scanner applications as its difficult at best to pass back a hand.

(iv) Time and Attendance

The first hand geometry time and attendance installations used hand scanners connected to a printer or access control software to record users' arrival and departure. This required manual sorting of the event data, though some ‘‘computer savvy" managers exported event data files to spreadsheet programs where they could sort and calculate the data.

(v) Point of Scale Applications

For the purpose of identity verification, point of scale application is used, like debit systems are becoming more common in our everyday lives as we move toward being a cashless society.

(vi) Interactive Kiosks

Hand scanners have found broad applications in the interactive kiosks. A host computer maintains user files and interacts with the user through a touch screen monitor or keyboard. It checks that the user is valid or not, if yes, monitor displays a menu of choices from which the user may select. The interactive kiosk communicates with the user after ID entry and verification. An automated border crossing is a popular application of the interactive biometric kiosk.

(vii) Parking Lot Application

Hand scanner used for access control in parking lots will be a welcome by the users as they don't need to carry cards. However, prevalent hand scanners are designed for use with the right hand making it difficult for left hand driven automobiles or by sports utility vehicles and sports cars which may require platen height to vary by as much as 0.9 meter.

CHAPTER-4

PROBLEM FORMULATION & PROPOSED SOLUTION

4.1 Problem Formulation

With the advancement of automation and the development of new technological systems personal identification is necessary in our daily lives. Biometrics technology allows determination and verification of one's identity through physical characteristics. Biometrics is a more foolproof form of authentication than typing passwords or even using smart cards, which can be stolen. Biometric systems replace conventional identification techniques since these are more convenient and reliable.

Hand geometry based biometric system plays a very important role in personal verification applications. Hand geometry biometric systems can be used in low to medium security applications. If this system combined with fingerprints and palmprints in a multi modal system it can prove very useful in high security applications. The advantage of combining these features lies in the fact that while taking the data for hand geometry, the data for fingerprints and palmprint can be collected simultaneously.

Most of the present available hand geometry system always uses pegs to fix the placement of the hand. The main weaknesses of using pegs are that pegs deform the shape of the hand and users might place their hands incorrectly. These problems can certainly reduce the performance of the biometric system. Another problem with these pegs is that it is not possible collect the data for hand geometry, fingerprints and palmprint, simultaneously in a multimode biometric system.

The purpose of this research is to design a biometric system based on hand geometry without pegs. Therefore, users can place their hands freely on the system platform. These types of biometric systems are not complex and yields good performance.

4.2 Proposed Solution

The proposed hand geometry biometric system provides a new approach to extract the hand geometry features. Data is read and processed independently of the position of the user hand. In this system, the selected features are not varying with variation of hand position. The main goal of this project work is to implement a system which can be able to acquire the images freely without any restriction by allowing the user to put his/her hand virtually in any position.

The proposed system extracts one measurement of length and three measurements of width for each finger. The thumb is not included in the feature extraction process. Also the palm width and four other distances between thumb valley points to other valley points are measured. The most important geometric part of the palm for feature extraction is the fingers. For each finger one measurement of length and three measurements of width are taken which makes it a total of 16 features for the four fingers. Including palm width and four other distances brings the number of total features to 21. All the landmark points on the right hand palm are defined below and shown in fig .4.1

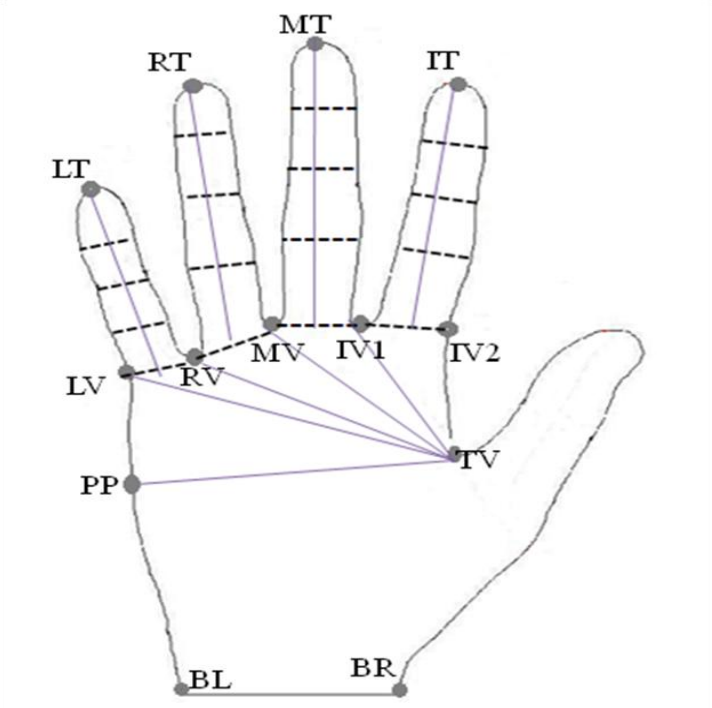


Fig 4.1 Define all landmark point and all features

IT- tip point of index finger

MT- tip point of middle finger

RT- tip point of ring finger

LT- tip point of little finger

IV1- valley point of index finger

IV2- assumed valley point of index finger

MV- valley point of middle finger

RT- valley point of ring finger

LV- assumed valley point of little finger

TV- valley point of thumb

PP- palm point

BL-bottom left point of palm

BR-bottom right point of palm

In this proposed system 21special features extracted from the palm. The definition of these features are given below

(i) The "finger lengths" are obtained by measuring the distances from the fingertips to the middle points of the finger baselines as shown in fig.4.1. The proposed system extracts one measurement of length from each finger so four features are taken from the finger length.

(ii) In this proposed system, the "finger widths" are the widths of a finger measured at 3 locations. The first one is measured at the middle of the finger length, the second one, at the one-third, and the last one, at the two-third of the finger length as shown in fig 4.1

(iii) The "palm width" is the distance from TV to PP shown in fig.4.1. The point PP is defined to be equal distance from LV which is the assumed valley point of the little finger as that of the distance from IV2 which is the assumed valley point of the index finger to TV as shown in fig. 4.1

(iv) Distance D1 is defined as it is distance between thumb valley point and little valley point.

(v) Distance D2 is defined as it is distance between thumb valley point and valley point of ring finger.

(vi) Distance D3 is defined as it is distance between thumb valley point and valley point of middle finger.

(vii) Distance D4 is defined as distance between thumb valley point and index valley point1.

Now the research project is to develop a hand geometry based verification system using with the help of Matlab software.

.

.

CHAPTER-5

IMPLEMENTATION

5.1 Matlab Software

MATrix LABoratory is a programming language for technical computing. This software is used for a wide variety of scientific and engineering calculations, especially for automatic control and signal, image processing, it also has extensive graphical capabilities. Matlab allows easy matrix manipulation, plotting of functions and data, implementation of algorithms, creation of user interfaces, and interfacing with programs in other languages.

5.2 Image Processing Toolbox

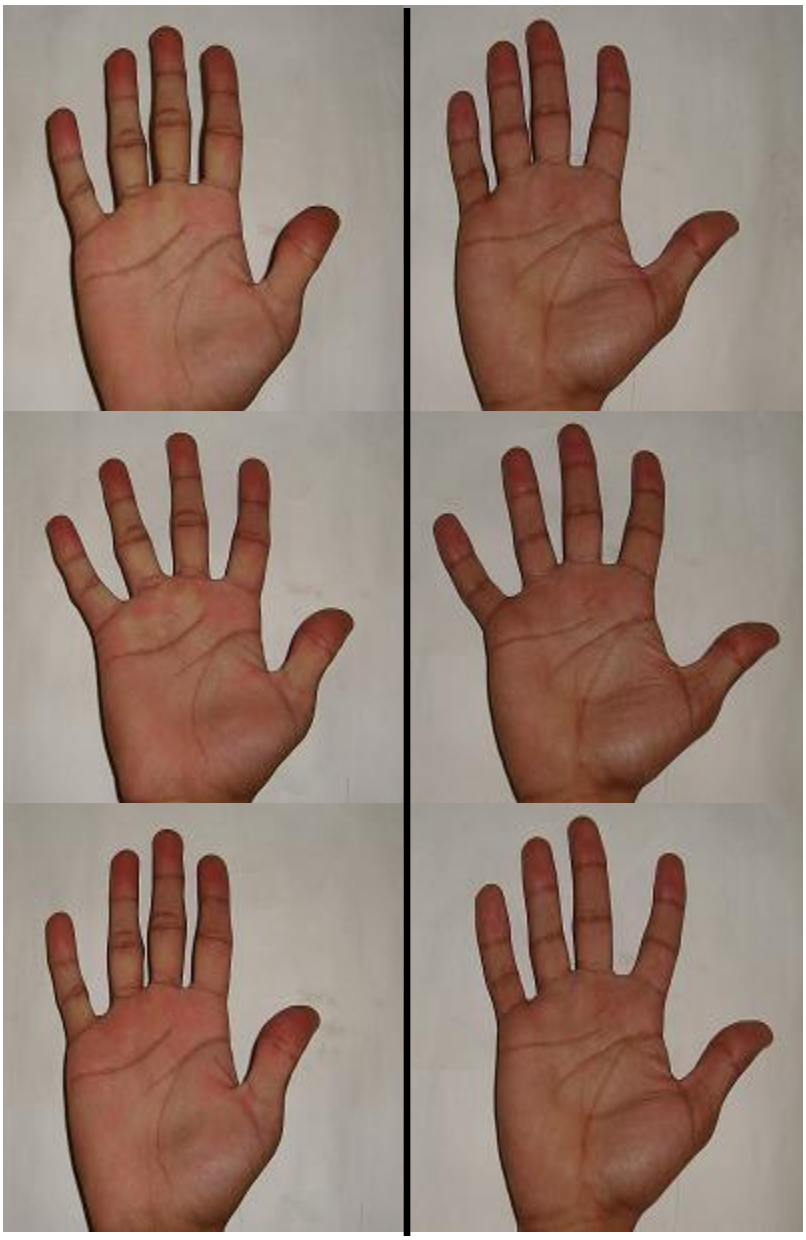
Image Processing Toolbox provides a comprehensive set of reference-standard algorithms and graphical tools for image processing, analysis, visualization, and algorithm development. You can perform image enhancement, image de blurring, feature detection, noise reduction, image segmentation, spatial transformations, and image registration. Many functions in the toolbox are multithreaded to take advantage of multi core and multiprocessor computers.

Basically Image Processing Toolbox is a collection of functions that extend the capability of the Matlab numeric computing environment. The toolbox supports a wide range of image processing operations. In this work Matlab version 7.5.0. is used.

5.3 Image Data Base

Hand images are obtained from a color digital camera placed a fixed distance above the platform, where the user's hand is placed. A user places one hand, pointing up, on the flat surface with the back of the hand touching the flat surface. The user can place a hand freely since there is no peg to fix the position of the hand. Users are only requested to make sure that their fingers do not touch one another and that the back of the

hand lies flat and stays on the flat surface. The images acquired by our set-up are shown in fig.5.1.



(a) **(b)**

Fig 5.1 Example images from the hand database.

It is clear from the fig 5.1 that hand positions and poses vary significantly between users. Although a slight rotation is acceptable the system is not completely rotation invariant.

There are 25 test users in this experiment. Ten right-hand images are acquired from each these images are divided into 2 groups. The first group consists of the images of all 25 users, 5 images from each user. They are used for the enrolment process to define the user's templates, or feature vectors. The rest of the images form the second image group. These images are used for testing the system performance. In this work a Kodak digital colored camera is used. It captures 3664*2748 resolution colored images of the hand. These images are resized and convert into a new size 360*324. The camera is placed at a distance of 0.5 meter from the hand.

In this experiment, only the right hand images of the users are acquired. To avoid any effects on the parameters of images like change in dimensions (pixel), change in texture values due to different sources, all the images have been taken from the same digital camera. The captured images are stored in bmp formats on the computer for possible image processing.

5.4 Methodology

The input image captured by digital camera is a colored image. Before features are extracted from an image, it may be useful to preprocess the image to reduce irrelevant information or noise and to enhance the image properties that will make feature measurement easier and reliable. There may be random noise that is generated due to different factors such as dirt, dust particles, etc. It can cause significant degradation in the feature extraction process which in turn may lead to higher error rates in the classification process. This noise removal is therefore essential for the system. These transforms may also result in loss of information from the original image. Hence, care must be taken while setting the parameters for applying a particular transform on the original image. There may be cycles of image processing before the final image is sent for feature extraction. Following steps have been performed to achieve this objective:

5.4.1 Algorithm for image preprocessing module

Image preprocessing module having following steps

Step-1 First load the image from the image storing folder. The syntax used is

I=imread (‘m1.bmp’)

This function reads a grayscale or color image from the file specified by the string filename.

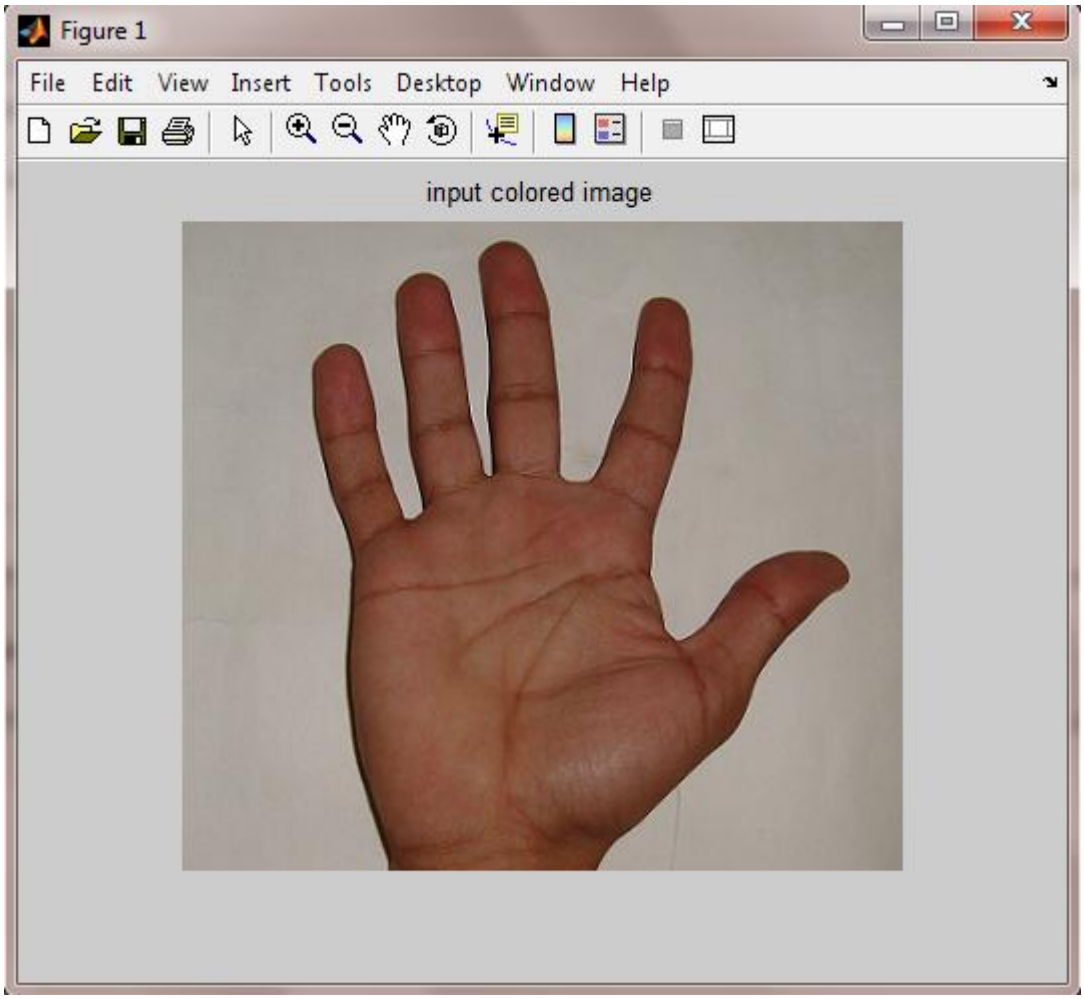


Fig 5.2 Input colored image

Step-2 Input colored image of hand is converted in to the gray scale image. The conversion command is set to convert all the colored images into black and white images also known as grayscale image. The syntax used is

A=rgb2gray (I)

rgb2gray converts RGB images to grayscale by eliminating the hue and saturation information while retaining the luminance. The grayscale image is of 2-D type. The 56 images were stored in the workspace of the MATLAB software from where they can be processed.

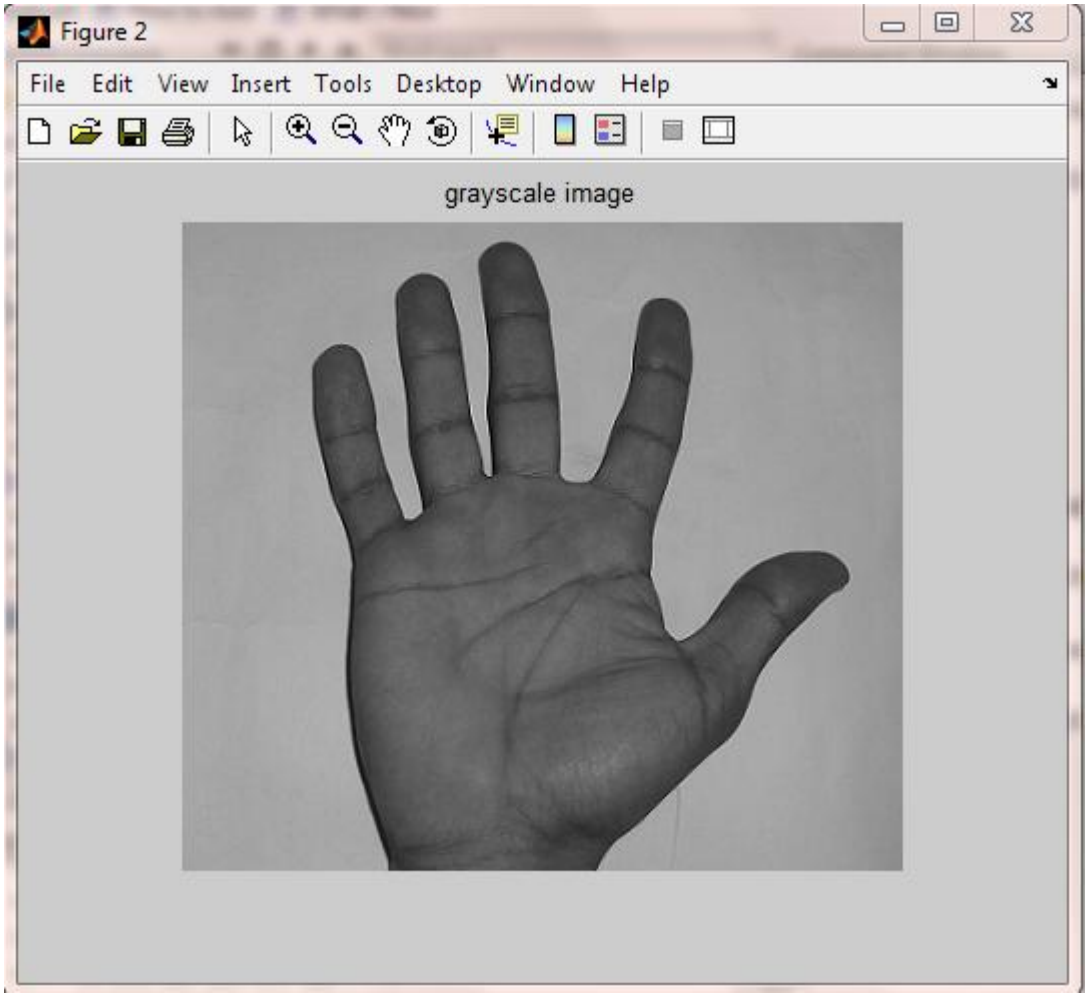


Fig 5.3 Gray scale image

This is an image consisting of intensity values. In Matlab, intensity images are represented by an array of class uint8, uint16, or double. Often use the variable name to represent an intensity image in memory. This term is synonymous with the term grayscale.

Step-3 Next step in image preprocessing is noise removal from the gray scale image. Image processing toolbox of Matlab has various filters for noise removal applications. Here wiener2 filter is used for noise removal. The syntax used is

T=wiener2 (A)

where A is the array of the gray scale image.

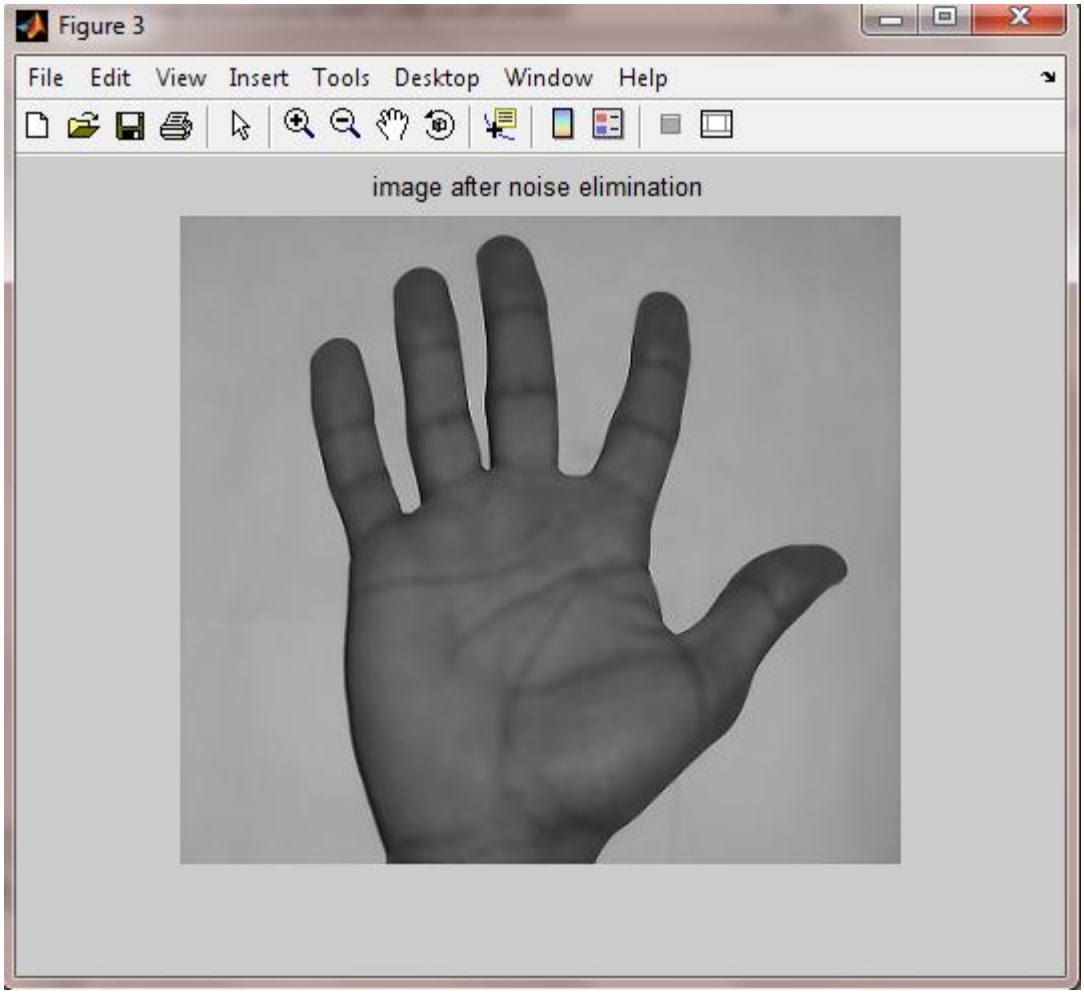


Fig 5.4 Image after noise removal

The wiener2 function applies a Wiener filter to an image adaptively and tailoring itself to the local image variance. Wiener2 smoothen the image to a very less extent when the variance is large and conversely when the variance is small, image get smoothened to a large extent.

Step-4 Last step in this module is edge detection. In order to extract geometric features of the palm it is required that the image contains only edges. This is achieved by using edge detection algorithm. There is various method of edge detection in Matlab image processing toolbox. Here sobel edge detector function is used. The syntax used is

E=edge (T, 'sobel')

where T is the array of the gray scale image after noise removal.

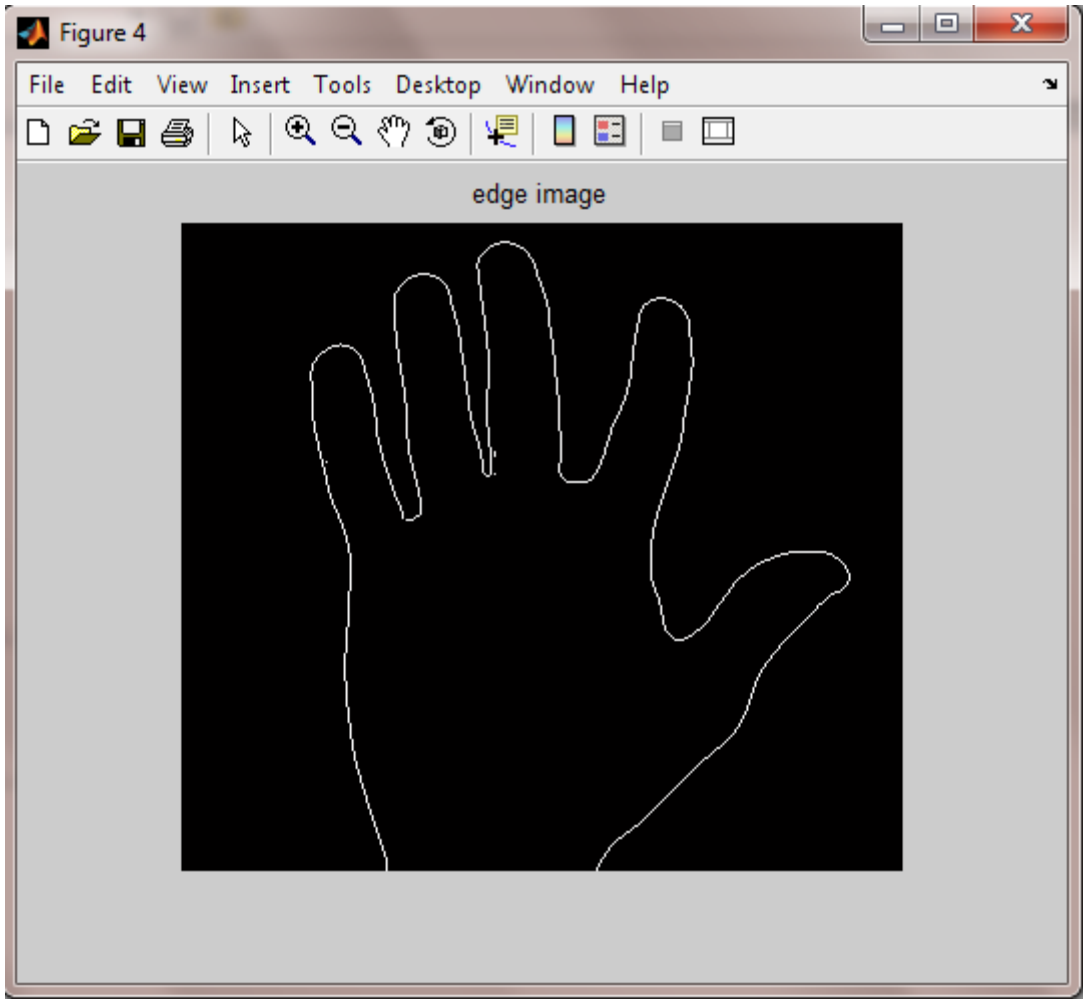


Fig 5.5 Image after edge detection

5.4.2 Algorithm for feature extraction

Next module of the hand geometry system is feature extraction module. There are several features that can be extracted from the geometry of palm. I am only interested in those feature that are consistent, i.e. features that are insensitive to hand pose variations.

The extracted features used in this research are the lengths of each finger; the widths of each finger at 3 locations the width of the palm and four distances between thumb valley point and other valley point. This results in 21 features all together. Feature that can be extracted from hand palm are showing in the fig 5.6.

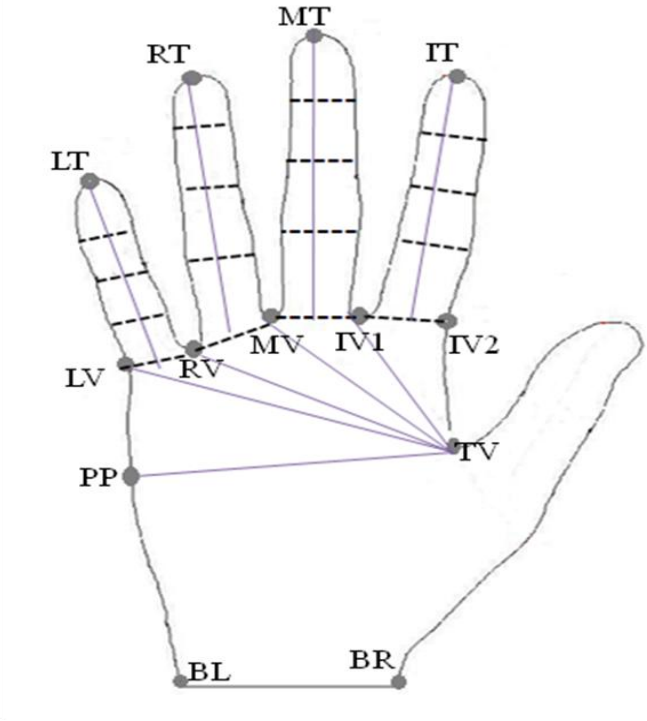


Fig 5.6 Hand geometry features

Before extracting the hand features, the landmark points have to be located. These landmark points include the fingertips and valley points. Firstly, the reference position on a palm i.e. bottom left and bottom right point, must be found. The next step is to find all the fingertips and valley points of the hand.

The finger baselines of a middle finger and a ring finger are obtained by connecting the valley points which are on both sides of that particular finger. However, for an index and a little finger; each has only one adjacent valley point. Thus, in this research, the other valley points are assumed to be on the opposite side of the finger with the same distance from the fingertip to the existing valley point. In this system all distances are measured in the unit of pixels. The thumb is not included in the feature extraction process.

(i) Algorithm for determining landmark points

Step-1 Firstly detect the bottom right and bottom left point of the palm. To detect bottom right point, start search from the bottom right pixel to bottom left pixel according to the pixel value and for detecting the bottom left point searching starts from bottom left pixel to bottom right pixel according to the pixel value. This searching stops at this moment. Now the two reference points are obtained- bottom right and left points of palm.

$$BR= (X_{BR}, Y_{BR})$$

$$BL= (X_{BL}, Y_{BL})$$

Step-2 To detect tip point of little finger a new searching is start from bottom left point. When the left bottom most point is reached then shifting is started along the boundary and this shifting is continue until the tip point of the little finger is reached. This shifting is done by moving towards the nearest pixel which lies on the boundary, and in the direction of tip of little finger. Now tip point of little finger is obtained

$$LT= (X_{LT}, Y_{LT})$$

Step-3 When the tip point of the little finger is reached then shifting is started along the boundary and this shifting is continuing until the ring valley point between the little finger and ring finger is reached. This shifting is done by moving towards the nearest pixel which lies on the boundary, and in the direction of valley point between the little finger and ring finger. Now valley point of ring finger is obtained.

$$RV= (X_{RV}, Y_{RV})$$

On the similar basis middle, index, thumb valley points and ring, middle, index tip points are obtained.

Step-4 As discuss earlier an index and a little finger has only one adjacent valley point. Thus, in this research, the other two valley points are assumed to be on the opposite side of the finger with the same distance from the fingertip to the existing valley point. To detect valley point of little finger, first count the no of boundary pixels between the little tip point and ring valley point and this value is assign to a variable i.e. count and a new searching is start from little tip point. When the little tip point is reached then shifting is started along the boundary and this shifting is continue until the valley point of the little finger is reached. This shifting is done by moving towards the nearest pixel which lies on the boundary, and in the direction of valley point of little finger. Similarly, find the index valley point2.

$$LV= (X_{LV}, Y_{LV})$$

$$IV2= (X_{IV2}, Y_{IV2})$$

Step-5 Now find the palm point which is defined as the distance between the little valley point and palm point which in turn is equal to the distance between the index valley point and thumb valley point. To detect palm point, first count the number of boundary pixels between the index valley point 2 and thumb valley point and this value is assigned to a variable i.e. count1 and a new search is start from little valley point. When the little valley point is reached then shifting is started along the boundary and this shifting continues until the palm point is reached. This shifting is done by moving towards the nearest pixel which lies on the boundary and in the direction of palm point. The palm point obtained is as follows

$$PP= (X_{PP}, Y_{PP})$$

Now with the help of this algorithm all the land mark points on the palm can be found.

5.4.3 Algorithm for determining the length of the finger

Step-1 First calculate the mid point on the base line between little valley point and ring valley point.

Step-2 Obtain the length of the line as the distance between mid point and tip point of the little finger. Length of the little finger can be obtained.

Similarly, find the length of ring finger, middle finger and index finger

5.4.4 Algorithm for determining the width of the finger

Step-1 For finger widths two fixed points are found on the finger boundary and the width is taken at these fixed points. The widths of a finger measured at 3 locations, the first one is measured at the one-third of the finger length, the second one, at the middle of the finger length, and the last one, at the two-third of the finger length. First of all count the no of boundary pixels between tip point of little finger and valley point of ring finger.

Step-2 For finding the first two fixed points on the little finger boundary first assigning a value to count variable which is equal to one third of the total no of pixels count between the tip point of little finger and valley point of ring finger and a new searching is start from little tip point. When the little tip point is reached then shifting is started along the boundary and this shifting is continue until the first left side little width point is reached. This shifting is done by moving towards the nearest pixel which lies on the boundary and in the direction of left side little width point.

For finding first right side little width point a new searching is start from little tip point. When the little tip point is reached then shifting is started along the boundary and this shifting is continue until the first right side little width point is reached**.** This shifting is done by moving towards the nearest pixel which lies on the boundary and in the direction of right side little width point. Now first left and right side little width point can be obtained.

Step-3 For finding the second two fixed points on the little finger boundary first we assigning a value to count variable which is equal to half of the total no of pixels count between the tip point of little finger and valley point of ring finger. Repeat step 2 and get second left and right side little width point.

Step-4 For finding the third two fixed points on the little finger boundary first assigning a value to count variable which is equal to two third of the total no of pixels count between the tip point of little finger and valley point of ring finger. Repeat step 2 and we will get third left and right side little width point.

The same algorithm can be applied for finding the width of ring finger, middle finger and index finger.

5.4.5 Algorithm for determining the palm width and other four distances

Step-1 Obtain the palm width of the line as the distance between thumb valley point and palm point.

Step-2 Obtain the distance D1 of the line as the distance between thumb valley point and little valley point.

Step-3 Obtain the distance D2 of the line as the distance between thumb valley point and little valley point of the ring finger.

Step-4 Obtain the distance D3 of the line as the distance between thumb valley point and valley point of middle finger.

Step-5 Obtain the distance D4 of the line as the distance between thumb valley point and index valley point.

5.4.6 Matching

The feature matching determines the degree of similarity between stored feature vector and claimed feature vector. The feature vector obtained from the input image is matched against the feature vector of images in the database. Even under the best of conditions it cannot be expected that the features obtained match exactly with the features of the previous image of the same individual. The extracted features are in the form of positive integers. These are referred to as magnitude of the features. Absolute distance function is used to decide the match value. Absolute distance function is defined as

$$D_a = \sum_{i=1}^{n} |Y_i - F_i|$$

Where F_i = h (f_1, f_2 . . . f_d) is the feature vector with d dimension of a registered user in the database, and Y_i = h (y_1, y_2 . . . y_d) is the feature vector of an unknown or a claimer. The F_i feature vector is mean of the 5 feature vectors of registered person 5 images. Therefore, the distance between claimer and register user is the distance between claimer feature vector Y_i and database feature vector F_i.

Now calculate match value which is defined as “the ratio absolute distance and total no of feature.

$$Match\ value = \frac{absolute\ distance}{No\ of\ feature}$$

After calculating the match, the system compares the result with a predefined threshold and classifies the claimer. The system accepts the claimer if and only if the calculated match value is lower than the threshold, and it rejects the claimer if and only if the calculated distance is higher than the threshold.

CHAPTER-6

RESULT AND DISSCUSSION

The hand geometry verification system has been tested by using a database of 250 images. Database of this system consists of 10 different acquisitions of 25 people. Most of the considered users were within a selective age range from 21 to 30 years old. Five images of each user's hand were selected to compute the feature vector which is stored in the database along with the user's name. The verification scheme depends on the feature vector. Verification refers to the problem of confirming or denying a claim of individuals and considered as one-to-one matching.

In order to study the effectiveness of system, the false rejection rate and false acceptance rate are plotted for different threshold value. A false rejection rate is obtained by comparing database feature vectors from the same hand feature vector while a false acceptance rate is obtained by comparing the feature vectors of different hands. When a feature vector in the database is matched against those feature vectors representing a different user and after comparing if the match value falls below the chosen threshold, it is considered to be a false acceptance by the system. This process is repeated for all the users in the database. On the other hand when a feature vector in the database is matched against those feature vectors representing a same user and if the match value is more than the chosen threshold then it is considered to false rejection.

In this experiment the value of false acceptance rate is calculated and then false rejection rate is calculated at different threshold values. The different value of FAR and FRR at different threshold are given in Table 6.1.

S.No	Threshold	FAR	FRR
1	0	0	100
2	0.5	0	100
3	1.0	0	64.40
4	1.5	0	31.20
5	2.0	1.09	15.20
6	2.5	2.61	7.2
7	3.0	8.42	4.8
8	3.5	10.66	2.4
9	4.0	17.90	1.6
10	4.5	26.95	0
11	5.0	38.23	0
12	5.5	49.33	0
13	6.0	56.85	0

Table 6.1 The value of FAR and FRR at different threshold value.

After testing with the images the arbitrary threshold proved to be fairly good. In 2100 tests for false acceptance there are a total of 177 false acceptances, giving the arbitrary threshold an FAR of 0.084. Also in 125 tests for false rejections it is found to be 6 false rejects giving the FRR a value of 0.04. The graph between error and threshold is shown in fig 6.1

.

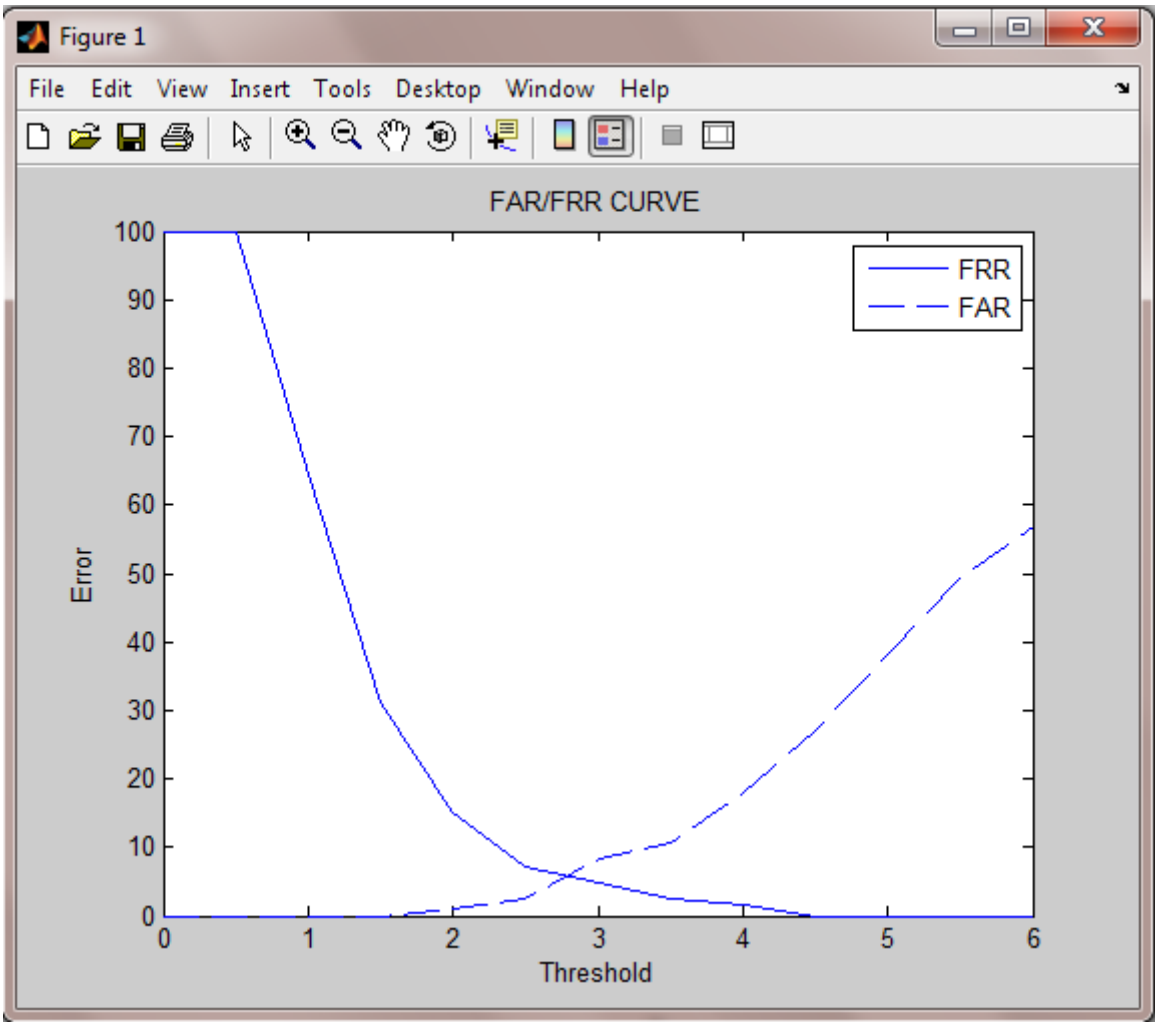


Fig 6.1 FAR - FRR curve

The false acceptance poses created a much more serious problem than false rejection. It is therefore desired that the biometric system keeps the FAR to the minimal possible limit. This can be achieved by setting a low threshold so that only very near matches are recognized and all other are rejected. The higher the security requirement from the system the lower the threshold required to maintain it.

However FRR also depends upon the threshold as the threshold decreases the FRR increases with it. This is because due to a low threshold matches which are correct but below the threshold due to noise or other factors will not be recognized. It is therefore

desired that a balance is maintained. Usually this balance point is the ERR where the FRR and the FAR are equal. However the security requirements from the system are the primary concern while deciding the threshold value and either of the FAR or FRR might be sacrificed for the other. In case of a very high security system the threshold may be raised while for a system where false rejects are of more concern the threshold might be lowered.

During these tests the match-score for each false acceptance has been noted. Also the match-score for each false rejection are noted. A comparison of these scores determines that the threshold can be raised so as to reduce the FAR to 0.02 with little increasing in the FRR i.e. 0.07 for the tested set of images. As more testing is performed the threshold can be narrowed down even further. The FAR-FRR curve is shown in fig 6.1 the ERR obtained from this curve is 5%.

Conclusion

A peg-free hand-geometry verification system has been developed in this thesis work which is independent of orientation and placement of the hand. The system is experimented with a database consisting of 250 images collected over time from 25 users. 10 sample images from each user were used for verification purpose. The verification system extracts the feature vector from the image and stores the template for later verification. FRR is obtained by comparing the two feature vectors of the same hand and FAR is obtained by comparing the feature vectors of two different hands.

The system shows effectiveness of results with accuracy around 95%. The FRR is found to be close to 0.07 and the FAR to be around 0.02.

This special project would detect a user is a member of a system or not. If he/she is a valid user of the system, then he/she is identified and the output is ‘Yes’. If the user could not be identified by the system, it output is ‘No’. Implementation of the program would result in a much secure and accurate system.

Future Scope

The results of the experiment show that hand-geometry based verification system can be used for access control in low-medium security zones and can also be combined with other forms of biometrics like finger print to increase the confidence levels in very high security zones. The proposed work relies upon the geometry of the hand. The palm creases and even the fingerprints can be extracted from the input image. The combination of all these biometric results in a multimodal system with very high accuracy. The use of neural network based classifier trained on a larger database may result in further improvement of the system accuracy.

REFERENCE

1. Raymond Veldhuis, Wim Booij, Asker Bazen and Anne Hendrikse, "A Comparison of Hand-Geometry Recognition Methods Based on Low- and High-Level Features", University of Twente, Netherlands, pp 326-330, 2002.
2. Guangming Lu, Zhang David, and Kuanquan Wang, "Palmprint Recognition Using Eigen Palms Features", Pattern Recognition. Letters, pp 143–146, 2003
3. Kresimir Delac, Mislav Grgic, "A Survey of Biometric Recognition Methods", 46th International Symposium Electronics in Marine, ELMAR-2004 Zadar, Croatia, pp 16-18, June 2004.
4. Bulatov Y., Jambawalikar S., "Hand Recognition Using Geometric Classifiers", ICBA-04, Hong Kong, China, pp 753–759, July 2004.
5. Y. L. Ma, Pollick F., and Hewitt W., "Using B-Spine Curves For Hand Recognition". Proc. of the 17th International Conference on Pattern Recognition (ICPR'04), pp 274–277, August 2004.
6. Schneiderman H. and Kanade T., "Object Detection Using the Statistics of Parts", International Journal of Computer Vision, pp 151– 177, 2004.
7. Faundez, Zanuy M., "Door-Opening System Using a Low-Cost Fingerprint Scanner and a PC", IEEE Aerospace and Electronic Systems Magazine. Vol. 19, pp.23-26, August 2004.
8. Fierrez-Aguilar J., Ortega-Garcia J., Gonzalez-Rodriguez, and Bigun J., "Kernel-Based Multimodal Biometric Verification Using Quality Signals," Proc. SPIE, Vol. 5404, pp. 544–554, 2004.
9. Jain, Ross and Prabhakar. "An Introduction to Biometric Recognition", IEEE Transaction on Circuits and Systems for Video Technology, January 2004.
10. Chih-Lung Lin and Kuo-Chin Fan, "Biometric Verification Using Thermal Images of Palm-Dorsa Vein Patterns", IEEE Transactions Circuits System. Video Techn. pp 199–213, 2005.
11. Cheung M., Mak M., and Kung S., "A Two Level Fusion Approach to Multimodal Biometrics Verification", IEEE International Conference on

Acoustics, Speech, and Signal Processing, (ICASSP ’05). pp 485– 488, March 2005.

12. Slobodan Ribaric and Ivan Fratric, “A Biometric Identification System Based on Eigen Palm and Eigen Finger Features”, IEEE Transaction, pp 1698-1709, 2005.
13. Faundez-Zanuy M. and Fabregas J., “Testing Report of a Fingerprint-Based Door-Opening System”. IEEE Aerospace and Electronic Systems Magazine. Vol.20 , pp 18-20, June 2005
14. Ledda and W. Phillips, “Majority Ordering and the Morphological Pattern Spectrum”, Conference Proc. Advanced Concepts for Intelligent Vision Systems, Antwerp, Belgium, pp 356-363, 2005.
15. Yun-Peng L., Fang-Cheng L., and Cheng-Rong, “Pattern Recognition of Partial Discharge Based on Its Pattern Spectrum”, Proc. International Symposium on Electrical Insulating Materials, Tokyo, Japan, 2005
16. Covavisaruch N., Prateepamornkul P., Ruchikachorn P., and Taksaphan P., “Personal Verification and Identification Using Hand Geometry,” ECTI Transaction on Computer and Information Technology, Vol.1, no.2, November, pp 432-4402005.
17. Sekhar Chandra C., Naidu Prakash and Shrivastava Sangeeta, “Biometric Verification Using Contour-Based Hand Geometry and Palmprint Texture”, Proc. of the 18th International Conference on Pattern Recognition, pp 1208-1214, 2006.
18. Amayeh G., Bebis G., Erol A., and Nicolescu M. “Peg-free Hand Shape Verification Using High Order Zernike Moments”. IEEE Computer Society Workshop on Multi-modal Biometrics, New York City, NY, June 17-18, 2006.
19. Kumar A., Wong M., Shen H., and Jain A. K., “Personal Authentication Using Hand Images”, Pattern Recognition. Letters, Vol. 27, no. 13, pp. 1478–1486, October 2006.

20. Badawi A. M., Shahin M. K., “Frequency Domain Spectral Hand Vein Patterns Authentication”, Proceedings of 3rd Cairo International Biomedical Engineering Conference, December 2006.
21. Kumar D.C.M., Shen H. C. “Personal Authentication Using Hand Images”, Pattern Recognition Letters, Vol. 27, pp 1478-1486, 2006
22. Yoruk E., Konukoglu, Sankur B., and Darbon, “Shape-Based Hand Recognition”, IEEE Transaction on Image Processing, Vol. 15(7), pp. 1803-1815, 2006.
23. Malassiotis Sotiris, Aifanti Niki and Strintzis G. Michael, “ Personal Authentication Using 3D Finger Geometry” BioSec IST-2002-001766, under Information Society Technologies (IST) priority of the 6th Framework Programme of the European Community, pp 1-23, 2006.
24. Rahman Arafatur, Azad Saiful and Anwar Farhat, “An Efficient Technique For Human Verification Using Finger Stripes Geometry” International journal of soft computing, pp 445-449, 2007.
25. Karen H. Suaverde and Dr. Vladimir Y. Mariano, “Biometric Identification Using Hand Geometry Features”, CMSC 190 special problem, institute of computer science, 2007.
26. Selvarajan S. and Palanisamy V. “Human Identification and Recognition System Using More Significant Hand Attributes”, Proc. of the International Conference on Computer and Communication Engineering Kuala Lumpur, Malaysia IEEE Transaction, pp 1211-1216, May, 2008.
27. Morales Aythami, Ferrer A. Miguel, Francisco Díaz, Jesús B. Alonso and Carlos M. Travieso “Contact-free Hand Biometric System for Real Environments” Technological Centre for Innovation in Communications University of Las Palmas de Gran Canaria Campus de Tafira, 35017, Las Palmas, Spain, 2008.
28. Biometric Technology Application Manual Volume One: Biometric Basics Compiled and Published by National Biometric Security Project Updated Summer 2008.

29. Niennattrakul Vit and Ratanamahatana Chotirat, “Making Hand Geometry Verification System More Accurate Using Time Series Representation with R-K Band Learning” Department of Computer Engineering, Chulalongkorn University Phayathai Rd., Pathumwan, Bangkok 10330 Thailand, pp 120-128, 2008.
30. Aghili Bahareh and Sadjedi Hamed “Personal Authentication Using Hand Geometry” Department of Electrical Engineering. Shahed University Tehran, Iran IEEE Transaction, 2009.
31. Kanhangad Vivek and Zhang David, “Combining 2D and 3D Hand Geometry Features for Biometric Verification”, Department of computing, The Hong Kong Polytechnic University, Kowloon, Hong Kong IEEE Transaction pp 39-44, 2009.
32. Mostayed Ahmed, Kabirt Ekramul Md, “Biometric Authentication from Low Resolution Hand Images Using Radon Transform”, Proc. of 12th International Conference on Computer and Information Technology (ICCIT 2009) Dhaka, Bangladesh IEEE Transaction pp. 587-592, December2009.
33. Cristiany Márjory, Fairhurst Michael “Analyzing the Benefits of a Novel Multiagent Approach in a Multimodal Biometrics Identification Task”, IEEE Systems Journal, Vol. 3, No. 4, IEEE Transaction pp 410-417 December 2009.
34. Fong Lai Leong and Seng Chaw Woo “A Comparison Study on Hand Recognition Approaches”, International Conference of Soft Computing and Pattern Recognition, IEEE Transaction, pp 364-368, 2009.
35. Casanova Guerra, Sierra Santos, “Silhouette-based Hand Recognition on Mobile Devices”, IEEE Transaction pp 160-166, 2009.