International Journal of Scientific Engineering and Applied Science (IJSEAS) – Volume-2, Issue-1, January 2016
ISSN: 2395-3470
www.ijseas.com

An Efficient Personnel Authentication Through Multi modal Biometric System

Mr. ShanthaKumar H.C, Associate Professor
Janardhan Naidu.A, 1st sem, M.Tech
Department of CSE, SJBIT, Bangalor-60

***Abstract* -** In recent days biometric based identifications are widely adopted for personnel identification. Most biometrics are unimodal, which rely on single source of information, but these systems currently suffer from noisy data, spoofing attacks, data quality and sometimes unacceptable error rates. These drawbacks can be overcome by setting up multi-modal biometric systems consisting of two or more biometric modalities in a single identification system to improve the recognition accuracy. However features of different biometrics have to be statistically independent**.** This paper proposes a multimodal biometric systems using fingerprint and iris recognition. The use of Magnitude and Phase features obtained from Gabor Kernels is considered to define the biometric traits of personnel. The biometric feature space is reduced using Fischer Score and Linear Discriminate Analysis. Personnel recognition is achieved using the weighted K-nearest neighbor classifier.

Keywords: **Unimodal , Multi-Modal, Magnitude, Gabor Kernel, Fischer Score, Linear Discriminate.**

1. INTRODUCTION

The use of biometrics to identify personnel is widely adopted in the current day scenario. A biometric recognition system identifies varied personnel using one or more specific physiological characteristics possessed by the personnel. If one physiological characteristic is considered for recognition then they are termed as unimodal recognition systems. When multiple or a combination of personnel biometrics are considered then they are termed as multimodal biometric recognition systems.

Enrollment and verification of authorized personnel are the important functions of the recognition systems. The recognition systems enroll authorized personnel based on the data provided from the biometric sensors and store the data for future verification or matching. During verification the recognition systems check if the biometric data presented is valid or invalid. Predominantly unimodal systems are adopted for personnel identification.

A simple biometric system consists of four basic components:

- Sensor module which acquires the biometric data.
- Feature extraction module where the acquire data is processed to extract feature vectors.
- Matching module where attribute vectors are compared against those in the template.
- Decision-making module in which the user's identity is established or a claimed identity
is accepted or rejected.

Any human physiological or behavioral trait can serve as a biometric characteristic as long as it satisfies the following requirements:

- Universality: Everyone should have it.
- Distinctiveness: No two should be the same.
- Permanence. It should be invariant over a given era of time.
- Collectability: In real life applications, three extra factors should also be considered.

Performance (accuracy, speed, resource requirements), acceptability (it must be harmless to users), and circumvention (it should be robust enough to various fraudulent methods).

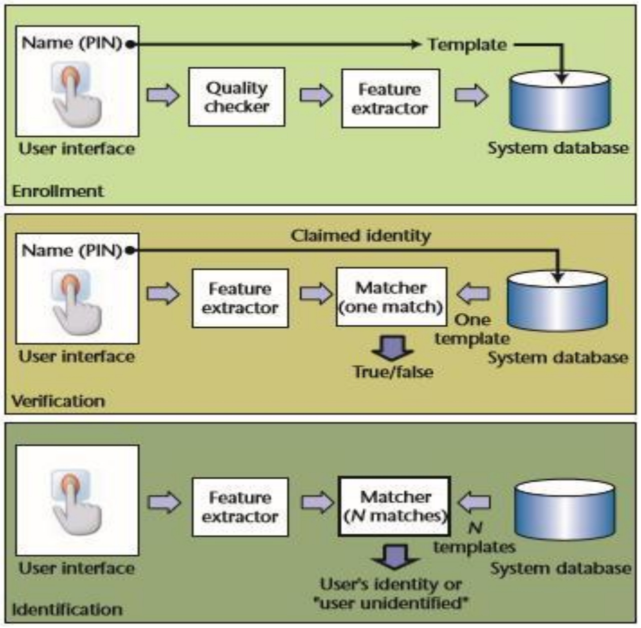


Fig 1.1: Working of biometrics

Verification mode: As in Fig 1.1, in the verification mode the system validates a person's identity by comparing the captured biometric data with the own biometric template(s) stored in the system database.

Identification mode: In this mode the system recognizes or authorizes an individual by searching the templates of all the users in the database for a match. Therefore, the system conducts a one-to-many comparison to establish an individual's identity.

- ***MOTIVATION:***

The use of multi-modal biometric recognition systems to overcome the drawbacks of the unimodal recognition systems has proved to be successful. Considering the research findings, this paper introduces a Multimodal Personnel Authentication using Finger vein and Face Images (MPAFFI). The state of art work presented by Shekar et al., considers the Iris, Finger print and Face biometrics for recognition. In the finger vein, vein patterns which are formed by blood vessels are considered for recognition.

- ***CONTRIBUTION:***

Limited work has been carried out by researchers with respect to multimodal recognition system considering such a comprehensive set of biometric features of personnel. In MPAFFI the personnel are identified on the basis of the Gabor kernel features extracted. To enable efficient feature extraction and recognition the biometric data obtained from the sensors is to be preprocessed to obtain the region of interest for the considered biometric traits. On obtaining the data feature extraction is performed using Gabor kernels. The novelty is that both the phase features and magnitude feature are considered. The research work carried out by other researchers considers either the magnitude features or the phase features. Limited work is carried out considering a combination of the phase and magnitude features for multimodal biometric recognition systems. In the research work presented in the phase and magnitude Gabor features are used for face recognition systems. In the research work presented in the use of Gabor phase and magnitude features is considered for face and fingerprint bimodal recognition systems. The extensive Gabor feature definitions of the biometric traits adopted in the results in large number of data points occupying a large space in which each personnel is considered as a sub- space. For dimensional reduction the use of Fisher Score and Linear Discriminate Analysis is considered. Fischer score enables efficient dimensional reduction, Linear Discriminate Analysis enables feature combinations and effective sub space projections of the personnel clusters. The multimodal biometric i.e. finger Vein and Face are fused using a linear fusion scheme in the use of the weighted K Nearest. Neighbor classifier is considered for verification or classification.

- ***KEY CHALLENGES IN UNIMODAL BIOMETIC SYSTEMS:***

The unimodal biometric recognition systems currently in place suffer from a large number of drawbacks. Biometric recognition systems solely rely on the data acquired from biometric sensors. The data presented to the recognition systems from the sensors are generally noisy in nature which can affect the verification results and also cause faulty enrollment techniques. The illumination, variation for face recognition systems is one such example. An interpersonal biometric similarity is another drawback of unimodal biometric systems. Considering the finger print the research work presented in clearly illustrates the biometric similarity problem. Spoofing attacks can also cause errors in unimodal recognition systems. Spoofing attacks are commonly notices when biometrics like signature, voice, face and finger prints are considered.

2. MODES OF BIOMETRICS

A. Fingerprints:

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, users no longer need to type passwords– instead, and 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. Fingerprints are the ridge and furrow patterns on the tip of the finger and have been used extensively for personal identification of people. The biological properties of fingerprint formation are well understood and fingerprints have been used for identification purposes for centuries. Since the beginning of the 20th century fingerprints have been extensively used for identification of criminals by the various forensic departments around the world. Due to its criminal connotations, some people feel uncomfortable in providing their fingerprints for identification in civilian applications.

However, since fingerprint-based biometric systems offer positive identification with a very high degree of confidence, and compact solid state fingerprint sensors can be embedded in various systems (e.g., cellular phones),fingerprint-based authentication is becoming more and more popular in a number of civilian and commercial applications such as, welfare disbursement, cellular phone access, and laptop computer log-in. The availability of cheap and compact solid state scanners as well as robust fingerprint matchers are two important factors in the popularity of fingerprint-based identification systems. Fingerprints also have a number of disadvantages as compared to other biometrics.

B. Iris Recognition:

This recognition method uses the iris of the eye which is the colored area that surrounds the pupil. Iris patterns are thought 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 (in systems performing one-to-many searches in a database).

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.

C. 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 image(s) that do not change over time while avoiding superficial features such asfacial 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 continuous and accepted by most users.

D. Voice Recognition:

Voice recognition has a history dating back some four decades, where the output of several analog filters were averaged over time for matching. Voice recognition uses the acoustic features of speech that have been found to differ between individuals. These acoustic patterns reflect both anatomy (e.g., size and shape of the throat and mouth) and learned behavioral patterns (e.g., voice pitch, speaking style).This incorporation of learned patterns into the voice templates (the latter called "voiceprints") has earned speaker recognition its classification as a "behavioral biometric."Voice recognition systems employ three styles of spoken input: text-dependent, text-prompted and text independent.

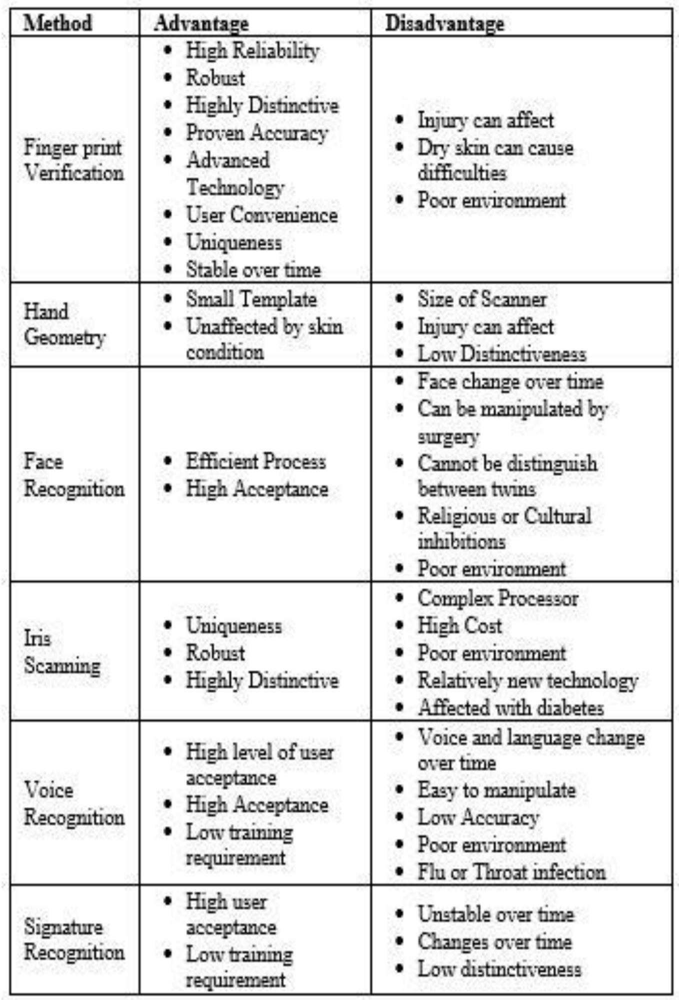
Most voice verification applications use text-dependent input, which involves selection and enrollment of one or more voice passwords. Text-prompted input is used whenever there is concern of imposters. The various technologies used to process and store voiceprints include hidden Markov models, pattern matching algorithms, neural networks, matrix representation and decision trees. 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 voice 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 (wire line or wireless).

E. Hand and Finger Geometry:

These methods of personal authentication are well established. Hand recognition has been available for over twenty years. To achieve personal authentication, a system may measure either physical characteristics of the fingers or the hands. These include length, width, thickness and surface area of the hand. One interesting characteristic is that some systems require a small biometric sample (a few bytes). Hand geometry has gained acceptance in a range of applications. It can frequently be found in physical access control in commercial and residential applications, in time and attendance systems and in general personal authentication applications.

F. 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.



Method	Advantage	Disadvantage
Finger print Verification	• High Reliability • Robust • Highly Distinctive • Proven Accuracy • Advanced Technology • User Convenience • Uniqueness • Stable over time	• Injury can affect • Dry skin can cause difficulties • Poor environment
Hand Geometry	• Small Template • Unaffected by skin condition	• Size of Scanner • Injury can affect • Low Distinctiveness
Face Recognition	• Efficient Process • High Acceptance	• Face change over time • Can be manipulated by surgery • Cannot be distinguish between twins • Religious or Cultural inhibitions • Poor environment
Iris Scanning	• Uniqueness • Robust • Highly Distinctive	• Complex Processor • High Cost • Poor environment • Relatively new technology • Affected with diabetes
Voice Recognition	• High level of user acceptance • High Acceptance • Low training requirement	• Voice and language change over time • Easy to manipulate • Low Accuracy • Poor environment • Flu or Throat infection
Signature Recognition	• High user acceptance • Low training requirement	• Unstable over time • Changes over time • Low distinctiveness

Table 2.1: Comparing different biometric traits

3. RELATED WORK

A number of researches have been done till for human traits based biometric identification system where some are emphasized for multi model consideration while taking into account of performance and classification accuracy as prime objectives. Some of them are as follows: Muhammad Imran et al., developed a multimodal biometric system comprising face and finger veins detection approach for enhancing biometric identification system. In their system they proposed a multilevel score fusion paradigm for face and finger veins for facilitating higher accuracy and ultimately, they exhibited better results in terms of reduction in the false rejection rate. Faten et al., developed a bimodal biometric identification system with face and fingerprint identification. In their work, they explored the advantages of the ability of individual biometrics score and efficiency. The authors advocated a scheme for evaluating a binary classification schemes with SVM to exhibit score fusion. The positive result of this system was its accuracy.

Sumit Shekhar et al., developed a multimodal sparse depiction approach that illustrates the test data using a sparse linear combination of training data. In their research correlation is taken into consideration as well as the coupling of varied information in different models under use. In order to achieve non-linearity they employed Kernels and further they enhanced their system using an alternative directional approach.

Zhenhua Chai et al.employed Gabor ordinal measures (GOM) scheme for face feature extraction and they enhanced the system using Gabor features with the effectiveness of ordinal estimations as a potential solution that could ensure both inter-person resemblance and intrapersonal deviations for face image data. In their system they employed varied categories of ordinal estimations derived from its intensity, phase, magnitude and real and imaginary components of Gabor filter. Ultimately, they employed a two phase cascade learning scheme and a greedy block selection approach that could be employed for training certain classifier for face data. In their research they emphasized on face recognition accuracy.

Monwar M et al., develop a multimodal biometric system using Fisher Extraction Scheme on the basis of PCA and Fisher's linear discriminant (FLD) approach which do employs face, ear and signature for identification. They employed rank-level fusion process and used Borda count paradigm (combination of ranks for individual model) and logistic regression technique. This system exhibited that the fusion of varied models could lead to performance enhancement

4. BACKGROUND WORK

In order to enhance the system by exploiting complementary details from multiple extracted features they proposed a multi-view cost sensitive subspace analysis scheme that needs a common feature subspace for fusing multiple features. In fact this work was an enhanced form of which has already employed certain cost-sensitive PCA and LPP (CSLPP) approach for face identification. On the other hand generic PCA and LPP approaches are unsupervised and author made it enhanced with supervised, which resulted into better results. In their work they have enriched the system with two discriminative subspace analysis approach called (LDA) and marginal Fisher analysis (MFA).

Some other works have also emphasized their system for multimodal biometric application and have tried to function on reduced dimensionality with linear subspaces. On the contrary the implementation of traditional LDA doesn't ensure optimal results. Therefore these all requirements become a motivation for this present research and we have proposed a highly robust and efficient system employing phase congruency with Gabor extraction, fisher 92 matrix enriched with LDA paradigm and the system has been further optimized with K-nearest neighbor classification system which makes the system optimal in terms of accuracy, efficiency and overall performance.

5. LIMITATIONS

A. Noise in sensed data:

The sensed data might be noisy or distorted. A fingerprint with a scar or a voice altered by cold are examples of noisy data. Noisy data could also be the result of defective or improperly maintained sensors (e.g., accumulation of dirt on a fingerprint sensor) or unfavorable ambient conditions

(e.g., poor illumination of a user's face in a face recognition system). Noisy biometric data may be incorrectly matched with templates in the database resulting in a user being incorrectly rejected.

B. Intra-class variations:

The biometric data acquired from an individual during authentication may be very different from the data that was used to generate the template during enrollment, thereby affecting the matching process. This variation is typically caused by a user who is incorrectly interacting with the sensor or when sensor characteristics are modified (e.g., by changing sensors—the sensor interoperability problem) during the verification phase. As another example, the varying psychological makeup of an individual might result in vastly different behavioral traits at various time instances.

C. Inter-class similarities:

While a biometric trait is expected to vary significantly across individuals, there may be large inter-class similarities in the feature sets used to represent these traits. This limitation restricts the discriminability provided by the biometric trait. Golfarelli et al. [4] have shown that the information content (number of distinguishable patterns) in two of the most commonly used representations of hand geometry and face are only of the order of and , respectively. Thus, every biometric trait has some theoretical upper bound in terms of its discrimination capability.

D. Non-universality:

While every user is expected to possess the biometric trait being acquired, in reality it is possible for a subset of the users not to possess a particular biometric. A fingerprint biometric system, for example, may be unable to extract features from the fingerprints of certain individuals, due to the poor quality of the ridges, thus, there is a failure to enroll (FTE) rate associated with using a single biometric trait. It has been empirically estimated that as much as 4% of the population may have poor quality fingerprint ridges that are difficult to image with the currently available fingerprint sensors and result in FTE errors. Den Os et al. [1] report the FTE problem in a speaker recognition system.

E. Spoof attacks:

An impostor may attempt to spoof the biometric trait of a legitimate enrolled user in order to circumvent the system. This type of attack is especially relevant when behavioral traits such as signature and voice are used. However, physical traits are also susceptible to spoof attacks. For example, it has been demonstrated that it is possible (although difficult and cumbersome and requires the help of a legitimate user) to construct artificial fingers/fingerprints in a reasonable amount of time to circumvent a fingerprint verification system.

6. MULTI-MODAL BIOMETRICS USING FINGER AND IRIS RECOGNITION

Multi-modal biometrics is the system that is capable of using more than one physiological or behavioral characteristic for enrollment, verification, and identification. Human identification based on multi-modal biometrics is becoming an emerging trend, and one of the most important reasons to combine different modalities is to improve recognition accuracy. There are additional reasons to combine two or more biometrics such as the fact that different biometric modalities might be more appropriate for unique deployment scenarios or when security is of vital importance to protect sensitive data.

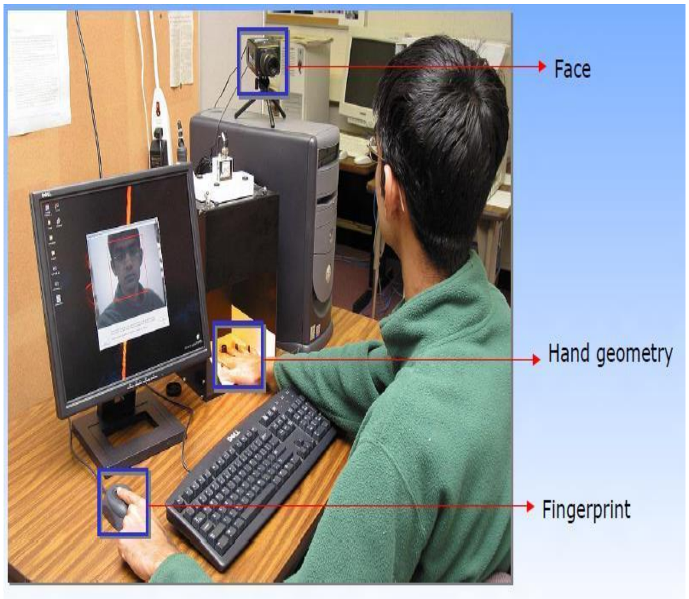


Fig 6.1: Multi-modal biometrics

Multi-modal biometric systems take input from single or multiple biometric devices for measurement of two or more different biometric characteristics as in Fig 6.1. For example, a multi-modal system combining fingerprint and iris characteristics for biometric recognition would be considered a multi-modal system regardless of whether fingerprint and iris images were captured by different or the same biometric devices. It is not a requirement that the various measures be mathematically combined in any way because biometric traits remains independent from each other, which results in higher accuracy when identifying a person. The flow of multimodal biometrics system is shown in fig 6.2.

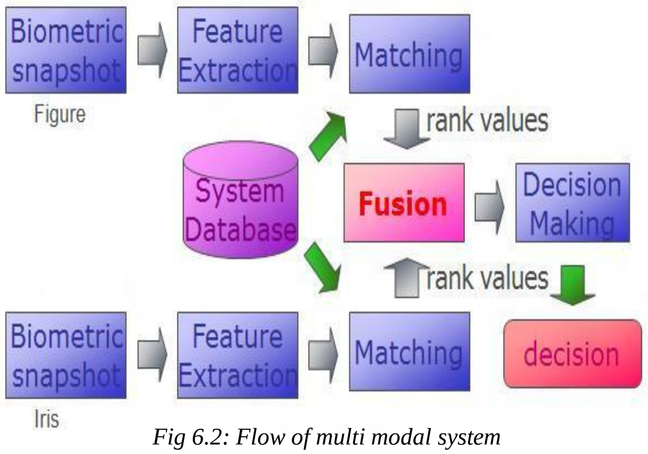


Fig 6.2: Flow of multi modal system

A. Finger Print Identification:

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 technology is fingerprint recognition, devices for desktop and laptop access are now widely available, 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. Fingerprints are the ridge and furrow patterns on the tip of the finger and have been used extensively for personal identification of people. The biological properties of fingerprint formation are well understood and fingerprints have been used for identification purposes for centuries. Since the beginning of the 20th century fingerprints have been extensively used for identification of criminals by the various forensic departments around the world. Due to its criminal connotations, some people feel uncomfortable in providing their fingerprints for identification in civilian applications.

However, since fingerprint-based biometric systems offer positive identification with a very high degree of confidence, and compact solid state fingerprint sensors can be embedded in various systems (e.g., cellular phones), fingerprint-based authentication is becoming more and more popular in a number of civilian and commercial applications such as, welfare disbursement, cellular phone access, and laptop computer log-in. The availability of cheap and compact solid state scanners as well as robust fingerprint matchers are two important factors in the popularity of fingerprint-based identification systems.

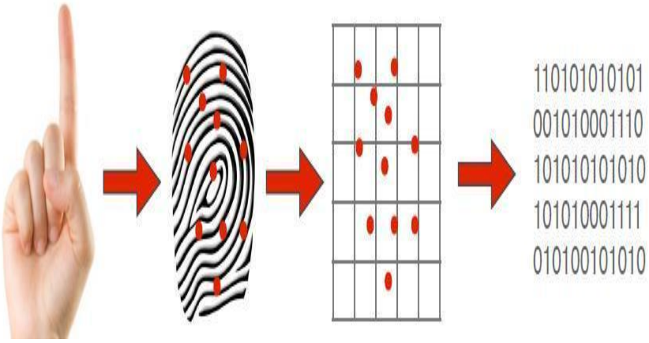


Fig 6.3: Finger print identification process

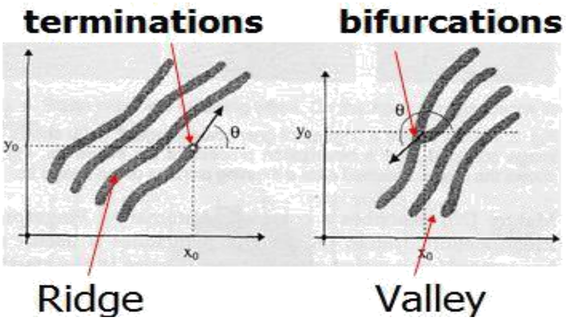


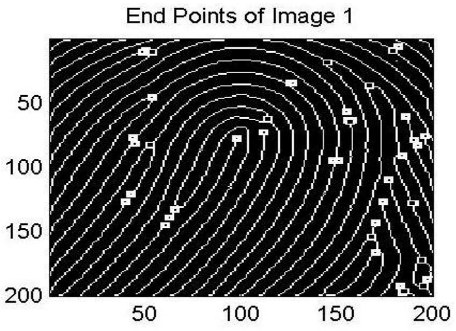
Fig 6.4: Identification of required features in finger print

A fingerprint scanner system has two basic jobs -- it needs to get an image of your finger, and it needs to determine whether the pattern of ridges and valleys in this image matches the pattern of ridges and valleys in pre-scanned images as in fig 6.4. Only specific characteristics, which are unique to every fingerprint, are filtered and saved as an encrypted biometric key or mathematical representation. No image of a fingerprint is ever saved, only a series of numbers (a binary code), which is used for verification. The algorithm cannot be reconverted to an image, so no one can duplicate your identity.

Feature Extraction:

Most Feature extraction algorithms function on the following four steps as shown in fig 6.5

- Determine a reference point for the fingerprint image,
- Tessellate the region around the reference point,
- Filter the region of interest in different directions, and
- Define the feature vector.



0	1	0
0	1	0
1	0	1

Terminations

0	0	0
0	1	0
0	0	1

Bifurcations

Fig 6.5: Feature Extraction Matrix of finger print

Fingerprint Matching:

Fingerprint matching refers to finding the similarity between two given fingerprint images. Due to noise and distortion introduced during fingerprint capture and the inexact nature of feature extraction, the fingerprint representation often has missing, spurious, or noisy features. Therefore, the matching algorithm should be immune to these errors. The matching algorithm outputs a similarity value that indicates its confidence in the decision that the two images come from the same finger. The existing popular fingerprint matching techniques can be broadly classified into three categories depending on the types of features used.

- Minutiae-based
- Correlation-based
- Euclidean distance-based

One of the main difficulties in the minutiae-based approach is that it is very difficult to reliably extract minutiae in a poor quality fingerprint image. The simplest correlation-based technique is to align the two fingerprint images and subtract the input image from the template image to see if the ridges correspond. For the third approach, matching is based on a simple computation of the Euclidean distance between the two corresponding feature showed in fig 6.6 and hence is extremely fast.

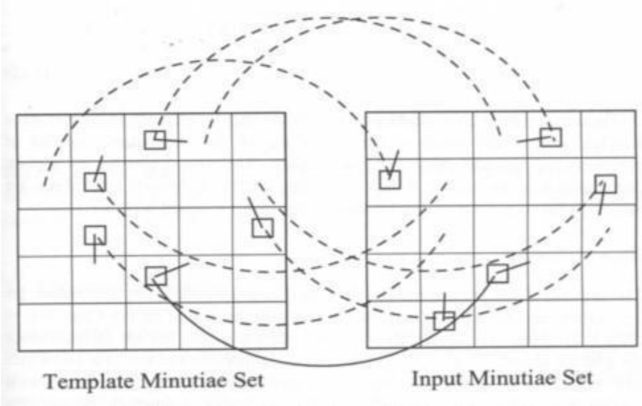


Fig 6 6: Matching of Finger Vector

B. Iris Recognition:

The critical attributes for any biometrics are: the number of degree-of-freedom of variation in the chosen index across the human population, since this determines uniqueness; its immutability over time and its immunity to intervention; and the computational prospects for efficiently encoding and reliably recognizing the identifying pattern. In the whole human population, no two irises are alike in their mathematical detail, even among identical (monozygotic) twins. The probability that two irises could produce exactly the same Iris Code is approximately 1 in 1078.(The population of the earth is around 1010B)Iris recognition is a method of biometric authentication, based on extraction features of the iris of an individual's eyes. Each individual has a unique iris; the variation even exists between identical twins and between the left and right eye of the same person.

A major approach for iris recognition today is to generate feature vectors corresponding to individual iris images and to perform iris matching based on some distance metrics. Most of the commercial iris recognition systems implement a famous algorithm using iris codes proposed by Daugman. One of the difficult problems in feature-based iris recognition is that the matching performance is significantly influenced by many parameters in feature extraction process (eg., spatial position, orientation, center frequencies and size parameters for 2D Gaborfilter kernel), which may vary depending on environmental factors of iris image acquisition. Given a set of test iris images, extensive parameter optimization is required to achieve higher Recognition Rate.

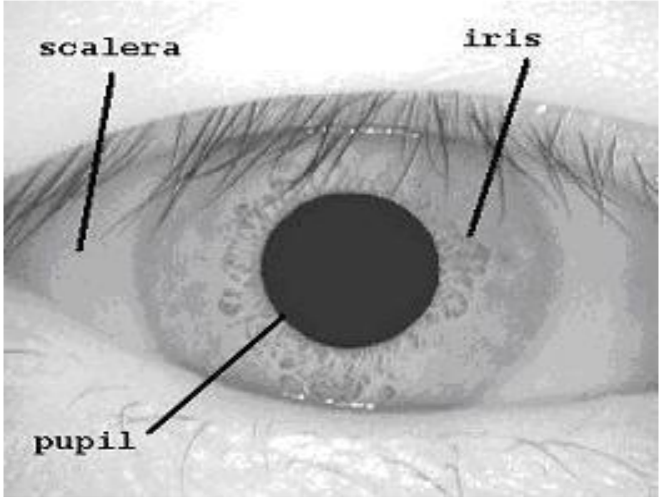


Fig 6.7 (a): Human eye

Iris Localization:

Both the inner boundary and the outer boundary of a typical iris can be taken as circles. But the two circles are usually not co-centric. Compared with the other part of the eye, the pupil is much darker. We detect the inner boundary between the pupil and the iris. The outer boundary of the iris is more difficult to detect because of the low contrast between the two sides of the boundary. We detect the outer boundary by maximizing changes of the perimeter-normalized along the circle as in fig 6.7(b). The technique is found to be efficient and effective.

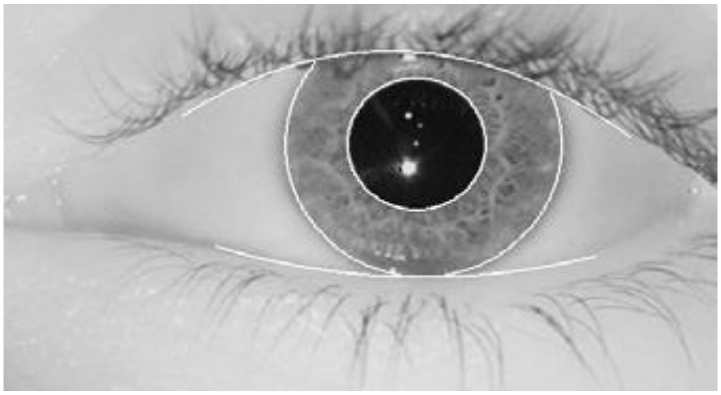


Fig 6.7 (b): White outlines indicate the localization

Iris Normalization:

The size of the pupil may change due to the variation of the illumination and the associated elastic deformations in the iris texture may interface with the results of pattern matching. For the purpose of accurate texture analysis, it is necessary to compensate this deformation. As in fig 6.8 both the inner and outer boundaries of the iris have been detected, it is easy to map the iris ring to a rectangular block of texture of a fixed size.

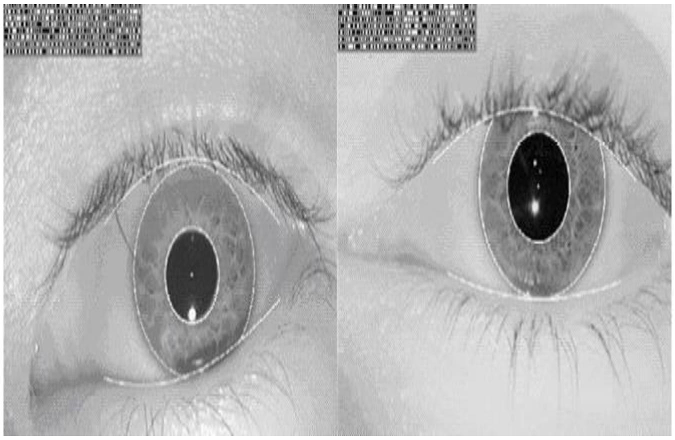


Fig 6.8: White outlines indicate the localization

Image Enhancement:

The original image has low contrast and may have non-uniform illumination caused by the position of the light source. These may impair the result of the texture analysis. We enhance the iris image reduce the effect of non-uniform illumination. The pictorial representation is as in fig 6.9

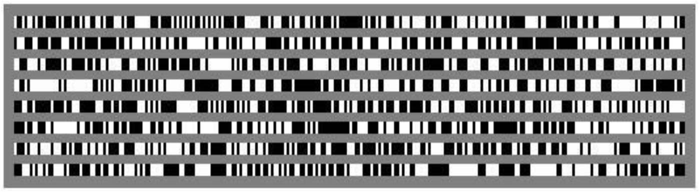


Fig 6.9: Pictorial Representation of Iris Code

Flow of iris recognition:

Before recognition of the iris, the iris is located using landmark features. These landmark features and the distinct shape of the iris allow for imaging, feature isolation, and extraction. Localization of the iris is an important step in iris recognition because, if done improperly, resultant noise (e.g., eyelashes, reflections, pupils, and eyelids) in the image may lead to poor performance of the iris and eyelid boundaries. Iris imaging requires use of a high quality digital camera. Today's commercial iris cameras typically use infrared light to illuminate the iris without causing harm or discomfort to the subject.

Upon imaging an iris, a 2D Gabor wavelet filters and maps the segments of the iris into phasors (vectors). These phasors include information on the orientation and spatial frequency (—what‖ of the image) and the position of these areas (—where‖ of the image). This information is used to map the Iris Codes. And the entire flow of iris recognition is as shown in the fig 6.10.

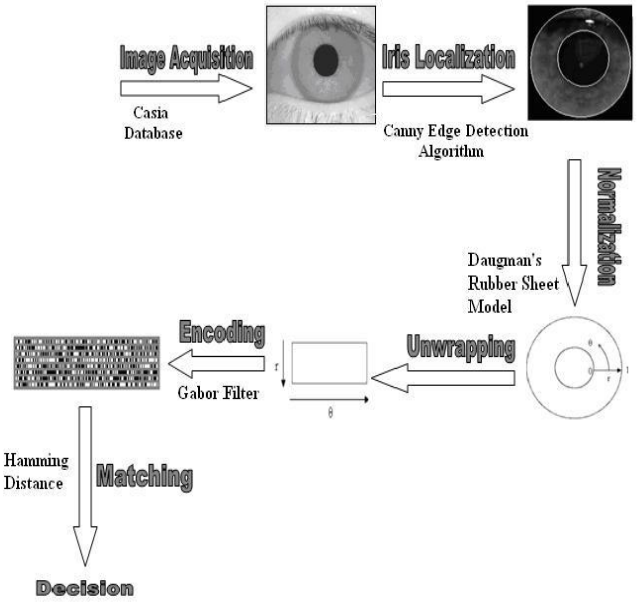
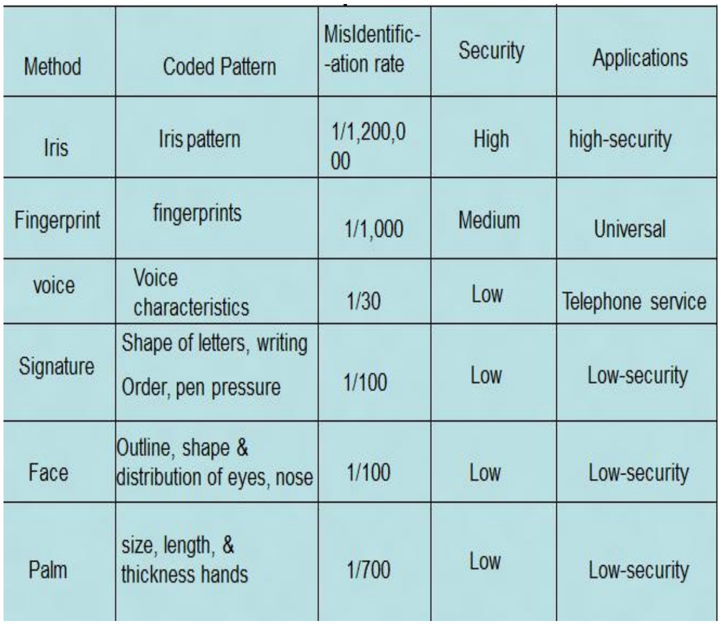


Fig6.10: Flow of Iris recognition

Iris patterns are described by an Iris Code using phase information collected in the phasors. The phase is not affected by contrast, camera gain, or illumination levels. The phase characteristic of an iris can be described using 256 bytes of data using a polar coordinate system. Also included in the description of the iris are control bytes that are used to exclude eyelashes, reflection(s), and other unwanted data.

To perform the recognition, two Iris Code are compared. The amount of difference between two Iris Code Hamming Distance (HD) is used as a test of statistical independence between the two Iris Codes. If the HD indicates that less than one-third of the bytes in the Iris Codes are different, the Iris Code fails the test of statistical significance, indicating that the Iris Codes are from the same iris. Therefore, the key concept to iris recognition is failure of the test of statistical independence.

COMPARISION



Method	Coded Pattern	MisIdentific- -ation rate	Security	Applications
Iris	Iris pattern	1/1,200,0 00	High	high-security
Fingerprint	fingerprints	1/1,000	Medium	Universal
voice	Voice characteristics	1/30	Low	Telephone service
Signature	Shape of letters, writing Order, pen pressure	1/100	Low	Low-security
Face	Outline, shape & distribution of eyes, nose	1/100	Low	Low-security
Palm	size, length, & thickness hands	1/700	Low	Low-security

Table .6.1: Comparison of different biometrics systems

ADVANTAGES

A. Accuracy: Multi-modal biometric uses multiple modalities to identify a person which ensures higher accuracy.

B. Security: Multi-modal biometric systems increase the level of security by **eliminating any chance of spoofing**. It is unlikely that a person would be able to spoof multiple types of biometric traits at once.

C. Liveness Detection: Multi-modal biometric systems ask end users to submit multiple biometric traits randomly which ensures strong **liveness detection** to protect from spoofing or hackers.

D. Universality: A multi-modal biometric system is universal in nature, even if a person is unable to provide a form of biometric due to disability or illness, the system can take other form of biometric for authentication.

E. Cost-effective: Multi-modal biometric systems are cost effective by providing higher levels of security to lessen the risk of breaches or criminal attacks.

APPLICATIONS

Network infrastructure has become essential to functions of business, government, and web based business models. Consequently securing access to these systems and ensuring one's identity is essential. Personal information and

Business transactions require fraud prevent solutions that increase security and are cost effective and user friendly. Key application areas include customer verification at physical point of sale, online customer verification etc.

The defense and intelligence communities require automated methods capable of rapidly determining an individual's true identity as well as any previously used identities and past activities, over a geospatial continuum from set of acquired data. A homeland security and law enforcement community require technologies to secure the borders and to identify criminals in the civilian law enforcement environment. Key applications include border management, interface for criminal and civil applications, and first responder verification.

Enterprise solutions require the oversight of people, processes and technologies. Network infrastructure has become essential to functions of business, government, and web based business models. Consequently securing access to these systems and ensuring one's identity is essential. Personal information and Business transactions require fraud prevent solutions that increase security and are cost effective and user friendly. Key application areas include customer verification at physical point of sale, online customer verification etc.

CONCLUSION:

Multi-modal biometric systems have performed well in addressing the problems of unimodal systems by combining information from different sources and improve the systems performance, The use of multiple biometric traits for recognizing persons, known as multimodal biometrics, has been shown to enhance precision and population coverage, while decreasing vulnerability to spoofing. Several studies prove the advantages of multimodal biometrics.

This paper has presented a multi-modal biometric approach based on fingerprint and iris recognition and tested using a database of gray scale fingerprints and a database of gray scale eye images. The final decision of the system uses the operator "AND" between decision coming from the fingerprint recognition step and that coming from the iris recognition one. Hence, nobody can be accepted unless both of the results are positive. This choice has been taken in order to highlight the system protection.

REFERENCES:

[1] Monwar M and Gavrilova, M.L., *"Multimodal Biometric System Using Rank-Level Fusion Approach,"* Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on , vol.39, no.4, pp.867,878, Aug 2009.

[2] A. Ross and A. K. Jain, —*Multimodal biometrics: an overview,"* Proc.European Signal Processing Conference, pp. 1221–1224, Vienna, Austria, Sept 2004.

[3] A. Ross, K. Nandakumar, and A. K. Jain, *Handbook of Multibiometrics,* Springer, 2006.

[4] Golfarelli, M. Maio, D. Malton, D., "*On the error-reject trade-off in biometric verification systems,"* Pattern Analysis and Machine Intelligence, IEEE Transactions on , vol.19, no.7, pp.786,796, Jul 1997.

[5] P. Krishnasamy, S. Belongie, and D. Kriegman, *"Wet fingerprint recognition:Challenges and opportunities,"* International Joint Conference on Biometrics, pp. 1–7, Washington DC, USA, Oct 2011.

[6] L. Hong, A. K. Jain, and S. Pankanti, "Can multibiometrics improve performance?," in Proceedings AutoID'99, (Summit(NJ), USA), pp. 59-64, Oct 1999.

[7] Shekhar S. Patel V.M. Nasrabadi N.M. Chellappa R., *"Joint Sparse Representation for Robust Multimodal Biometrics Recognition,"* Pattern Analysis and Machine Intelligence, IEEE Transactions on , vol.36, no.1, pp.113,126, Jan 2014.

[8] Chengjun Liu; Wechsler, H., *"Gabor feature based classification using the enhanced fisher linear discriminant model for face recognition,"* Image Processing, IEEE Transactions on , vol.11, no.4, pp.467,476, Apr 2002.

[9] S_truc, V.; Vesnicer, B.; Paves_i , N., *"The Phase-based Gabor Fisher Classifier and its application to face recognition under varying illumination conditions,"* Signal Processing and Communication Systems, 2008. ICSPCS 2008. 2nd International Conference on , vol., no., pp.1,6, 15-17 Dec. 2008.

[10] S. Gundimada, V. K. Asari, and N. Gudur, *"Face recognition in multi-sensor images based on a novel modular feature selection technique,"* Information Fusion, vol. 11, no. 2, pp.124–132, 2010.