Security System Based on Face, Fingerprint and Iris

Pallavi Suryavanshi, Samruddhi Bhange, Trushali Jamdade
Under The Guidance of: ***Prof.Yelpale M.U.***
Department of Electronic and telecommunication, Fabtech Technical Campus, College of Engineering and Research, Sangola,India.

***Abstract*—A biometric system is a computer system, which is used to identify the person on their behavioral and physiological characteristic (for example fingerprint, face, iris, key-stroke, signature, voice, etc). A typical biometric technology consists of sensing, feature extraction, and matching modules. But now a day's biometric systems are attacked by using fake biometrics. . This paper introduce three biometric techniques which are face recognition, fingerprint recognition, and iris recognition (Multi Biometric System) and also introduce the attacks on that system and by using Image Quality Assessment For Liveness Detection how to protect the system from fake biometrics.**

***Keywords*—**Face detection, face recognition, fingerprint detection, fingerprint recognition, iris detection, iris recognition, ARM7, MATLAB.

I. INTRODUCTION

EVERY prison has his own precious accessories such as gold, ornaments or cash. In old day to keep it the bank locker system is used. In that a private key system which is associated with the concern user and every time he or she has headache to carry key with him or has keep burden of key lost or key duplication problem. So that to overcome this problem Biometric System is invented. Biometric is the computer system. Biometric systems including fingerprint, face, voiceprints, palm print, and iris recognition identify a person by using physiological and/or behavioral characteristics [1]. Biometrics canbe sorted into two classes1. Physiological (example: face, fingerprint, iris) 2. Behavioral (example:signature and voice)

Single biometric systems have limitations like uniqueness, high spoofing rate, high error rate, non-universality and noise. For example in face recognition, it is affected by position, sadness, happiness and the amount of ambient light [2].So that multi- biometric has more advantage than single-biometric.

In this system not onlyfeatures fingerprint but also face and iris detection technique.face detection technique which gives us effective and fast access.Secondly fingerprint detection technique gives easy access to system which contains specified finger pattern of that person. Third iris detection technique gives fast access to system which contains iris pattern of that person. So in the system MATLAB software is used. By combination of all three techniques system gives the advanced security.

II. BLOCK DIAGRAM OF PROPOSED SYSTEM

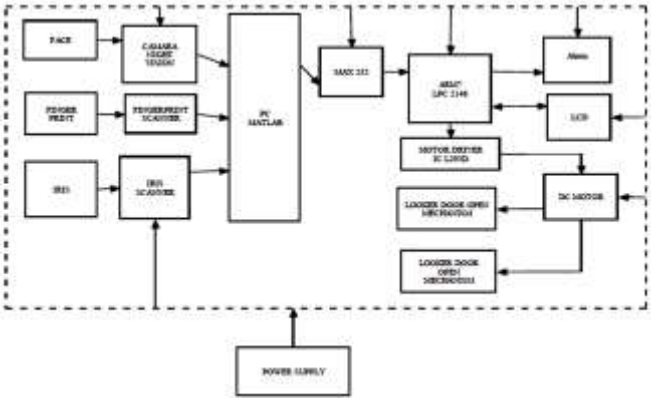

Fig.1.1. Block Diagram of proposed system

For face reorganization we are using the principle component analysis algorithm in MATLAB is used for face reorganization technique. For image recognition and compression PCA is most successful techniques that have been used. PCA can perform various operation prediction, redundancy removal, feature extraction, data compression etc. Because PCA is a classical technique which can do something in the linear domain, applications having linear models are suitable, such as signal processing, image processing, system and control theory, communications, etc. The main idea of using PCA for face recognition is to express the large 1-D vector of pixels constructed from 2-D facial image into the compact principal components of the feature space. This can be called Eigen space projection. Eigen space is calculated by identifying the Eigen vectors of the covariance matrix derived from a set of facial images (vectors). All this process is done in Matlab software & captured image is compared with database stored in the PC and if it is match with the stored database then first gate of locker will be open automatically [3].

A fingerprint is made of a series of ridges and furrows on the surface of the finger. The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as the minutiae points. Minutiae points are local ridge characteristics that occur at either a ridge bifurcation or a ridge ending. Fingerprint matching techniques can be placed into two categories: minutiae based and correlation based. Minutiae-based techniques first find minutiae points and then map their relative placement on the finger. In Matlab for fingerprint recognition we use Gabor filter. For Fingerprint recognition is considered using a combination of

Fast Fourier Transform (FFT) and Gabor Filters to enhancement the image. An input fingerprint is first matched at a coarse level to one of the pre-specified types and then, at a finer level, it is compared to the subset of the database containing that type of fingerprints only. If captured image is compared with stored database in PC [3].

When a subject wishes to be identified by iris recognition system, his/her eye is first photographed and then a template (iris code) created for his/her iris region. This template is then compared with the other templates stored in a database until either a matching template is found and the subject is identified or no match is found and the subject remains unidentified. There are several method for accomplishing single task as edge detection Sobel Operator, Prewitt Operator, Canny Edge Detection, Roberts method and so on, for boundary detection as Hough Transformation, Circular Hough Transformation, Integro-Differential Operator, Gradient based approach, Clustering algorithms and so on, for feature extraction phase based methods, zero crossing and texture analysis based methods[4].

For face reorganization we are using the principle component analysis algorithm in MATLAB is used for face reorganization technique.

The coordinate of an unauthorized person are received by the microcontroller through serial communication. The coordinate is passed from laptop to microcontroller through RS-232 using DB9 cable. Microcontroller accepts the coordinate at USART (Universal Synchronous Asynchronous Receiver Transmitter) pin by means of MAX233 transceiver.

RM processors are extensively used in consumer electronic devices such as Smartphone‟s,tablets, multimedia players and other mobile devices, such as wearable‟s. Because of their reduced instruction set, they require fewer transistors, which enable a smaller die size for the integrated circuitry (IC). The ARM processors smaller size reduced complexity and lower power consumption makes them suitable for increasingly miniaturized devices.

III. PROPOSEDMETHODOLOGY

1. *Face recognition*

Facial images are the common biometric feature used for personal identification. Face recognition is mainly performed by two approaches, they are Eigen face based recognition and 3D face recognition.

The Eigen face based recognition works by analyzing face images and computing Eigen faces which are faces composed of eigenvectors. The comparison of Eigen faces is used to identify the presence of a face and its identity. The Eigen face technique is straightforward, efficient, and yields generally good results in controlled circumstance. There are also some limitations of Eigen faces. There is limited robustness to changes in lighting, angle, and distance. 2D recognition systems do not capture the actual size of the face, which is a fundamental problem. These limitations affect the technique‟s application with security camera.

1.1 *Face Detection*

We detected the face from the lighted-compensated frame by skin color (local feature) analysis. Color processing is chosen as it is faster than the processing of other local features and has small effect to the variation in pose and expression. However, the problem that can occur is that the skin color is different for different persons. For this, many color spaces such as RGB, normalized RGB, YCbCr, HSV, etc., are used to model the skin color. We preferred YCbCr color space because it separates the luminance and chrominance components for real-time CCTV surveillance. The human skin pixels are detected by exploiting the restricted range of chrominance red component from 133-173[3].

Facial image enhancement is an important step for better recognition performance, namely for low facial image quality. Such process aims at extenuate the side effects that can diverge the process during the learning phase and maintain all wavelet sins inside the face to encode its component features. Detection is the most important step in our study, it is carried out manually on the original image, it allows us to point out areas of interest, this step is accompanied by image registration and allows to overlay the qualifier zones of the face (eyes, nose and mouth) for different images in the dedicated database. An example of a face sample, detected and realigned [1].

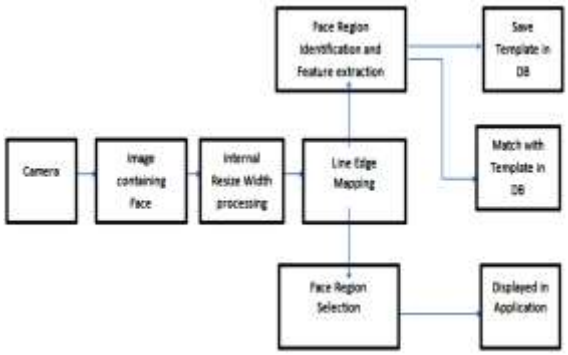

Fig.1.2 Block dia. of face matching

1.2 System flow:-

STEP-1 Face Reorganization using PCA algorithm

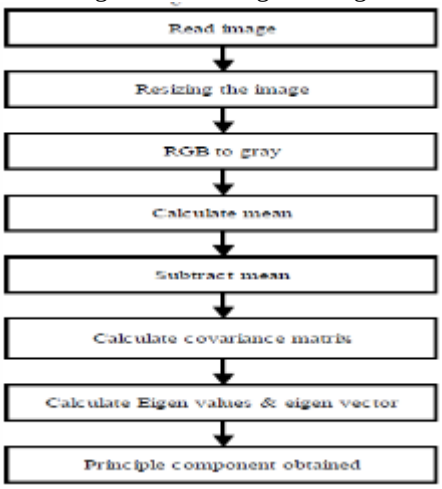

Fig:-1.3System flow for Face Reorganization

For face reorganization we use principle component analysis algorithm. Initially we are acquiring data through camera night vision xpro. Read image operation is performed in which image is shown on screen. After resizing operation of image is done in which we are predefined setting the format of image. The basic purpose is to make image in gray color because RGB format image contains each pixel of three values i.e. from 0-255 each for Red, green and blue color. If RGB to gray conversion is there then time is reduced used for each pixel of RGB color and for gray color each pixel contains only one value i.e.0-255. So we use RGB to gray conversion. After gray conversion unnecessary part of image is removed so that concatenation of faces should be done then create tensor image then calculate the mean of captured image then subtract the mean image from the tensor image vector. Find covariance matrix for captured image & then calculate Eigen values & Eigen vectors. Finally we got principle component of image[3].

2. Fingerprint Recognition

2.1. Finger print enhancement:-

The enhancement module is an important module for better identification. Such process aims at increasing the clarity of ridge structure so that minutiae points can be easily and correctly extracted. The enhanced fingerprint image is normalized, filtered and submitted to thinning algorithm which reduces the ridge thickness to one pixel wide for precise location of endings and bifurcation.

Minutiae extraction:-

After the module of enhancement of the image, the next module is the extraction of minutiae. the more there are minutiae detected, the better is the probability to obtain accurate results. To ignore the false minutiae and have statistically less corrupt, we just have to find the region of interest (ROI) area. This area makes all the ridge-ends located in border blocks invalid[1].

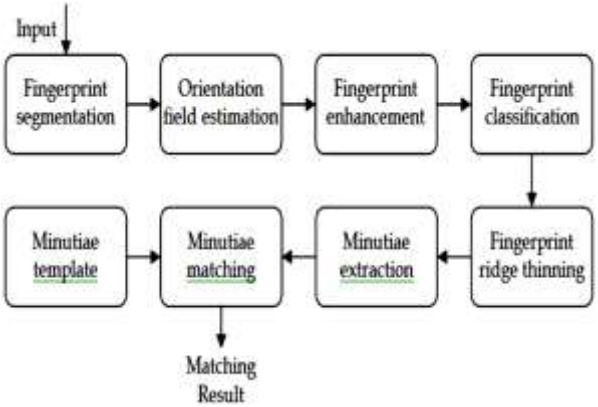

Fig.2.1 Block diagram of finger print matching

2 System flow:-

STEP-2 Face Reorganization

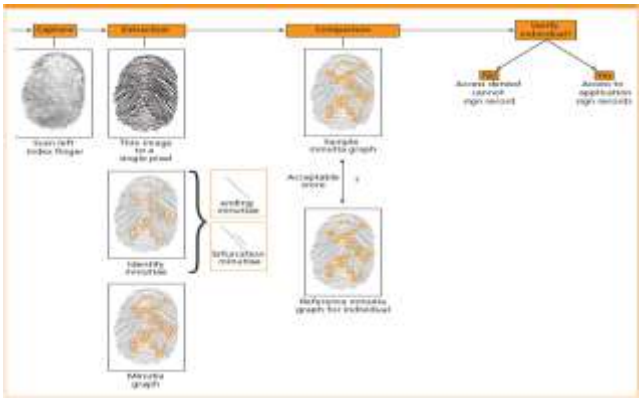

Fig.2.2 fingerprint detection flow

A fingerprint is the pattern of ridges and grooves on the surface of a fingertip. The fingerprints are highly stable and unique. The uniqueness of fingerprint is determined by global features like valleys and ridges, and by local features like ridge endings and ridge bifurcations, which are called minutiae. The recent studies reveal that probability of two individuals, having the same fingerprint is less than one in a billion.

There are various fingerprint matching algorithms like minutiae based matching correlation based matching, genetic algorithms based. Among these, minutiae based matching is the dominated one.

In minutiae based matching the similarity of two fingerprints is determined by computing the total number of matching minutiae from the scanned fingerprints. Extraction of minutiae features before matching needs a series of processes, containing alignment computation, image segmentation, image enhancement, and ridge extraction and shinning, minutiae extraction and filtering.

3. Iris Recognition

Iris recognition systems make use of the uniqueness of the iris patterns to identify a person. This system uses a high-quality camera to capture a black-and-white, high-resolution image of the iris (the colored ring surrounding the pupil).

3.1 System flow

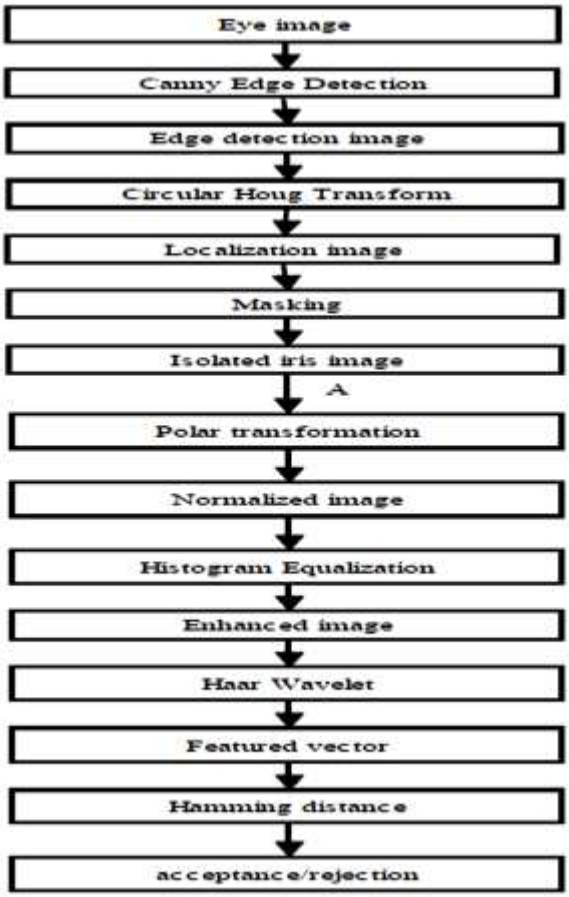

Fig.3.1 System flow of iris recognition

3.2 Steps for iris detection

Image acquisition:-This is our very first step of the entire process. When a person wishes to be identified by iris recognition system, his/her eye is first photographed. The camera can be positioned between three and a half inches and one meter to capture the image. In the manual procedure, the user needs to adjust the camera to get the iris in focus and needs to be within six to twelve inches of the camera. This process is much more manually intensive and requires proper user training to be successful. We must consider that the occlusion, lighting, number of pixels on the iris are factors that affect the image quality.

Localization:-The acquired iris image has to be preprocessed to detect the iris, which is an annular portion between the pupil (inner boundary) and the sclera (outer boundary). The first step in iris localization is to detect pupil which is the black circular part surrounded by iris tissues. The center of pupil can be used to detect the outer radius of iris patterns.

The important steps involved are:

1. Pupil detection
2. Outer iris localization

Well-known methods such as the Integro- Differential Operator, Hough Transform and Active Contour models have been successful techniques in detecting the boundaries. The iris localization proposed by Tisse et al. is a combination of the Integro-Differential Operator and the Hough Transform. The Hough Transform is used for a quick guess of the pupil center and then the Integro- Differential Operator is used to accurately locate pupil and limbus using a smaller search space. But in this using Prewitt Edge Detection for detecting edges in the entire eye image after that applying Circular Hough Transformation for detecting outer boundary of iris by using pupil center and inner boundary of iris.

Isolation:- Now the task is to isolate the iris. In the images used, there is some presence of the white of the eye. This was done by using a masking technique by choosing best technique among other so use Gaussian Mask and then cropping the image to minimize the area that does not contain any edge data. The mask is a circular one which has the same radius as the iris. It thus passes all pixels that are contained in the circle which are all the pixels forming the iris. By making use of the center and the radius which are calculated in advanced step, we set the polar coordinate system. In this coordinate system, the feature of the iris is extracted.

Normalization:- For the purpose of accurate texture analysis, it is necessary to compensate this deformation. Since both the inner and outer boundaries of the iris have been detected so it is easy to map the iris ring to a rectangular block of texture of a fixed size. The Cartesian to polar reference transform suggested by Daugman authorizes equivalent rectangular representation of the zone of interest. In this way compensate the stretching of the iris texture as the pupil changes in size, and unfold the frequency information contained in the circular texture in order to facilitate next feature extraction. Also this process is very necessary because feature extraction and matching process becomes easy.

Enhancement and denoising: -The normalized iris image still has low contrast and may have non- uniform illumination caused by the position of light sources. In order to obtain more well-distributed texture image, we enhance iris image by means of local histogram equalization and remove high frequency noises by filtering the image with an appropriate filter.

Feature Extraction:- The Wavelet Transform to extract features from the iris region. Both the Gabor Transform and the Haar Wavelet are considered as the Mother Wavelet. Laplacian of Gaussian (LoG) is also used in previous papers. In my paper, using Haar Wavelet, decomposing upto 4th level a feature vector with 87 dimensions is computed. Since each dimension has a real value ranging from -1.0 to +1.0, the feature vector is sign quantized so that any positive value is represented by 1 and negative value as 0. This results in a compact biometric template consisting of only 87 bits.

Storing and Matching:- Now this is our final phase for completing our system.

Here we will store the 87 bit iris code or template in our database for future matching and this matching is done with the help of an efficient matching algorithm here we are using Hamming Distance algorithm for the recognition of two samples that is reference template and enrollment template. It is basically uses an exclusive OR (XOR) function between

two bit patterns. Hamming Distance is a measure, which delineate the differences, of iris codes. Every bit of presented iris code is compared to the every bit of referenced iris code, if the two bits are the same, e.g. two 1‟s or two 0‟s, the system assigns a value „0‟ to that comparison and if the two bits are different, the system assigns a value „1‟ to that comparison[4].

IV. ADVANTAGES

- Better Security: - The multi-biometric system increases the security level.
- Single biometric system is easy to attack but the multi-biometric system is not so easy because attacker cannot obtain two traits of the same individual.
- More secure than other system.
- Multiple Fingerprint scanner support
- Multiple IRIS Scanner support[5]

V. APPLICATION

1. Multi-biometric system is used in India for making Aadhar card this multi-biometric system is used face recognition, iris recognition, and fingerprint recognition.
2. Multi-biometric system used in Airport.
3. Multi-biometric system is used in banking.
4. ATM machine use
5. Travel and tourism
6. Telephone transactionsPersonal computer, workstation security
7. Medical information systems
8. Any password-based application
9. Home or domestic application
10. Industrial application

VI. FUTURE SCOPE

- Security
- Access and attendance control
- Travel control
- Financial and other transactions requiring authorization
- Remote voting
- Use of automated working devices

VII. DISCUSSION

In this review paper I show how a person can be identified by a number of ways but instead of carrying bunk of keys or remembering things as passwords we can use us as living password.Proposed security system only allows the authorized people to enter the sensitive area without targeting.Experiments with face, fingerprint, iris recognition indicate that it is considerably challenging to obtain good recognition rates in real-time scenarios. The true accept rate does not have to be 100%, but the false accept must be extremely low. The recognition rate of our security system is about 2 out of 100 in terms of false accepts. In our experiments, these errors are mostly due to variation in pose and expression.

REFRENCE

[1] 2011 8thInternational Multi-Conference on Systems, Signals &Devices a new human identification based on fusion fingerprints and faces biometrics using LBP and GWN descriptors Norhene GARGOURI BEN AYED, A lima DAMAK MASMOUDI and Dorra SELLAMI MASMOUDI Computers Imaging Electronics and Systems Group(CIELS) ICOS Research Unit

[2] International Journal of Advanced Research in Computer Science and Software Engineering Research Paper" Concept of Unimodal and Multimodal Biometric System"KomalSondhi ,YogeshBansal

[3] "Smart Bank Locker Access System Using Iris ,Fingerprints,Face Recognization Along With Password Authentication And Billing System"Asst.Prof.T.A.More, 1, SarwadeSukanya 2,Hajare Nikita3,Bhakre Ashok4 ,March 2015

[4] Personal Identification Using Iris Recognition System, a Review HimanshuSrivastava Department of Computer Science & Engineering, Roorkee Institute of Technology, Roorkee (U.K.), India, June 2013

[5] A Survey Based on Fingerprint, Face and Iris Biometric Recognition System, Image Quality Assessment and Fake BiometriPradnya M. Shend International Journal of Computer Science Engineering and Technology(IJCSET) April 2014