ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com

International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 2,Special Issue 6, March 2016

MULTIMODAL BIOMETRIC METHOD USING SPOOFING DETECTION

S.ABIRAMI
PG Student
Department of CSE
Rajas Engineering College
Vadakkangulam
abira93keertha@gmail.com

R.ANUJA
ASSISTANT PROFESSOR
Department of CSE
Rajas Engineering College
Vadakkangulam

Abstract—Biometric authentication systems are quite vulnerable to sophisticated spoofing attacks. To keep a good level of security, reliable spoofing detection tools are necessary, preferably implemented as software modules. The research in this field is very active, with local descriptors, based on the analysis of microtextural features, gaining more and more popularity, because of their excellent performance and flexibility. This paper aims at assessing the potential of these descriptors for the liveness detection task in authentication systems based on various biometric traits: fingerprint, iris, and face. Besides compact descriptors based on the independent quantization of features, already considered for some liveness detection tasks, will study promising descriptors based on the joint quantization of rich local features. The experimental analysis, conducted on publicly available data sets and in fully reproducible modality, confirms the potential of these tools for biometric applications, and points out possible lines of development toward further improvements. To keep a good level of security, reliable spoofing detection tools are necessary, preferably implemented as software modules. A Biometric System is a system for the automated recognition of individuals based on their behavioral and biological characteristics. Depending on the context, in a biometric system, there are two different ways to resolve a person's identity

- **Verification**
- **Identification**

I. INTRODUCTION

1.1 AREA OVERVIEW

1.1.1 IMAGE PROCESSING

Image processing is processing of images using mathematical operations by using any form of signal processing for which the input is an image, such as a photograph or video frame; the output of image processing may be either an image or a set of characteristics or parameters related to the image. Most image-processing techniques involve treating the image as a two-dimensional signal and applying standard signal-processing techniques to it.Image processing usually refers to digitalimage processing,but optical and analog image processing also are possible. This article is about general techniques that apply to all of them. The acquisition of images (producing the input image in the first place) is referred to as imaging. Closely related to image processing are computer graphics and computer vision. In computer graphics, images are manually made from physical models of objects, environments, and lighting, instead of being acquired from natural scenes, as in most animated movies.

Computer vision, on the other hand, is often considered high-level image processing out of which a machine/computer/software intends to decipher the physical contents of an image or a sequence of images (e.g., videos or 3D full-body magnetic resonance scans).In modern sciences and technologies, images also gain much broader scopes due to the ever growing importance of scientific visualization (of often large-scale complex scientific/experimental data). Examples include microarray data in genetic research, or real-time multi-asset portfolio trading in finance

1.2 SOFTWARE PROGRAM .

Enhancement programs make information more visible.

- Histogram equalization-Redistributes the intensities of the image of the entire range of possible intensities (usually 256 gray-scale levels).
- Unsharp masking-Subtracts smoothed image from the original image to emphasize intensity changes.

Convolution programs are 3-by-3 masks operating on pixel neighborhoods.

- Highpass filter-Emphasizes regions with rapid intensity changes.
- Lowpass filter-Smoothes images, blurs regions with rapid changes.

Math processes programs perform a variety of functions.

- Add images-Adds two images together, pixel-by-pixel.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 2,Special Issue 6, March 2016

- Subtract images-Subtracts second image from first image, pixel by pixel.
- Exponential or logarithm-Raises e to power of pixel intensity or takes log of pixel intensity. Nonlinearly accentuates or diminishes intensity variation over the image.
- Scaler add, subtract, multiply, or divide-Applies the same constant values as specified by the user to all pixels, one at a time. Scales pixel intensities uniformly or non-uniformly
- Dilation-Morphological operation expanding bright regions of image.
- Erosion-Morphological operation shrinking bright regions of image.

Noise filters decrease noise by diminishing statistical deviations.

- Adaptive smoothing filter-Sets pixel intensity to a value somewhere between original value and mean value corrected by degree of noisiness. Good for decreasing statistical, especially single-dependent noise.
- Median filter-Sets pixel intensity equal to median intensity of pixels in neighborhood. An excellent filter for eliminating intensity spikes.
- Sigma filter-Sets pixel intensity equal to mean of intensities in neighborhood within two of the mean. Good filter for signal-independent noise.

Trend removal programs remove intensity trends varying slowly over the image.

- Row-column fit-Fits image intensity along a row or column by a polynomial and subtract fit from data. Chooses row or column according to direction that has the least abrupt changes.

Edge detection programs sharpen intensity-transition regions.

- First difference-Subtracts intensities of adjacent pixels. Emphasizes noise as well as desired changes.
- Sobel operator-3-by-3 mask weighs inner pixels twice as heavily as corner values. Calculates intensity differences.
- Morphological edge detection-Finds the difference between dilated (expanded) and eroded (shrunken) version of image.

Image analysis programs extract information from an image.

- Gray-scale mapping-Alters mapping of intensity of pixels in file to intensity displayed on a computer screen.
- Slice-Plots intensity versus position for horizontal, vertical, or arbitrary direction. Lists intensity versus pixel location from any point along the slice.
- Image extraction-Extracts a portion or all of an image and creates a new image with the selected area.
- Images statistics-Calculates the maximum, minimum, average, standard deviation, variance, median, and mean-square intensities of the image data.

II. EXISTINGMETHODSANDSYSTEM ANALYSIS

LITERATURE SURVEY

2.1 A New Antispoofing Approach for Biometric Devices., P. Venkata Reddy, Ajay Kumar.

The deployment of fingerprint sensors is increasingly becoming common and has now gained high user acceptance. However, fingerprint sensors are susceptible to spoofing using artificial materials or in worst case to the dismembered fingers. Fake/ gummy fingerprints have shown to fool most commercial fingerprint systems. This proposes a new method of anti-spoofing using reliable liveness detection. The proposed method of liveness detection is based on the principle of pulse oximetry and involves the source of light originating from a probe at two wavelengths. The light is partly absorbed by haemoglobin, by amounts which differ depending on whether it is saturated with oxygen or deoxygenated haemoglobin. perform the computations for the absorption at two wavelengths to estimate the proportion of haemoglobin which is oxygenated. The computed percentage of oxygen in the blood, along with the heart pulse rate, determines the liveness of the enrolled biometric. The initial design of the proposed prototype device for liveness detection employed analog approach.Analogcomponents the response of the device was very sluggish, dueto the slow charging of the capacitors at the low pass filter stages, and the complexity of the device was high to extract a low amplitude biomedical signal in the presence of noise. In order to account the phase shift between the red and infra-red signals peak detectors were employed.This resulted in slow response time of the system as the capacitors charged to their peak value had to comeback to a lower voltage level. In orderto speed up the response and to facilitate the integration with a fingerprint sensor, the final implementation was initiated using a microcontroller that had most of the instructions implemented as single cycle instructions.An effective algorithm of fingerprint image enhancement, which can much improve the clarity and continuity of ridge structures based on the multiresolution analysis of global texture and local orientation by the wavelet transform.

Experimental results show that the enhanced image quality by using the wavelet-based enhancement algorithm is much better than the other existing methods for improving the minutiae detection.A fingerprint recognition system based on a novel application of the classifier DECOC to the minutiae extraction and on an optimized matching algorithm . To identify the different shapes and

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 2,Special Issue 6, March 2016

types of minutiae, a Data-driven Error Correcting Output Coding (DECOC) has been adopted to work as a classifier. This method has been applied throughout the fingerprint skeleton to locate various minutiae.Extracted minutiae have been used then asidentification marks for an automatic fingerprint matching that is based on distance and direction between two minutiae and type of minutiae. The extraction of minutiae from fingerprint images. A critical step in automatic fingerprint matching is to reliably extract minutiae from the input fingerprint images.

Advantages

- A new method of anti-spoofing using reliable liveness detection. it is used for reliable liveness detection.

Disadvantages

- Lack of standardization

2.2 Two-Stage Enhancement Scheme for Low-Quality Fingerprint Images by Learning From the Images, Jucheng Yang, Naixue Xiong.

Fingerprint authentication for content protection in the human–machine systems, cybernetics, and computational intelligence is very popular. Because of the complex input contexts, low-quality input fingerprint images always exist with cracks and scars, dry skin, or poor ridges and valley contrast ridges. Usually, fingerprint images are enhanced by one stage in either the spatial or the frequency domain.However, the enhanced performances are not satisfactory because of the complicated ridge structures that are affected by unusual input contexts. In this proposed a novel and effective two-stage enhancement scheme in both the spatial domain and the frequency domain by learning from the underlying images. To remedy the ridge areas and enhance the contrast of the local ridges, first enhance the fingerprint image in the spatial domain with a spatial ridge-compensation filter by learning from the images. With the help of the first step, the second stage filter, i.e., a frequency band pass filter that is separable in the radial- and angular-frequency domains is employed. Biometrics is the science of recognizing an individual based on physical or behavioural characters. The Fingerprint is one of the Biometric indicators that are used by forensic experts in criminal investigation, because of its universality, permanence, distinctiveness and accuracy. Input Fingerprint images are of low quality because of wetness, dryness, smears in the skin. In order to provide better clarity, these input fingerprint images are enhanced using two stage block wise enhancement scheme. The first stage enhances the input fingerprint image by connecting the broken ridges and separating the merged ridges.

Even though the first stage enhances the image, the output of the first stage will be a blurred image. This blurred image will be enhanced in the second stage using DWT. A discrete wavelet transform is any wavelet transform, for which the wavelets are discretely sampled. As with other wavelet transforms, a key advantage it has over Fourier transforms is temporal resolution it captures both frequency and location information. The fingerprint ridges can be recovered well. The help of the first step, the second-stage filter, i.e., a frequency bandpass filter that is separable in the radial- and angular-frequency domains, is employed. It is noted that the parameters of the bandpass filters are learnt from both the original image and the firststage enhanced image instead of acquiring from the original image solely. It enhances the fingerprint image significantly because of the fast and sharp attenuation of the filter in both the radial and the angular-frequency domains. The design of these systems and provide a novel modular framework, namely, novel approaches for biometric systems (NABS) that have implemented to address them. NABS encompasses two possible architectures based on the comparative speeds of the involved biometrics. It also provides a novel solution for the data normalization problem, with the new quasi-linear sigmoid (QLS) normalization function. This function can overcome a number of common limitations, according to the presented experimental comparisons. A further contribution is the system response reliability (SRR) index to measure response confidence. Its theoretical definition allows to take into account the gallery composition at hand in assigning a system reliability measure on a single-response basis.

Advantages

- User friendly

Disadvantages

- The reliability and the accuracy of biometric devices continues to improve

2.3 Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint,and Face Recognition., Javier Galbally, Sébastien Marcel.

To ensure the actual presence of a real legitimate trait in contrast to a fake self-manufactured synthetic or reconstructed sample is a significant problem in biometric authentication, which requires the development of new and efficient protection measures. presented a novel software-based fake detection method that can be used in multiple biometric systems to detect different types of fraudulent access attempts. The objective of the proposed system is to enhance the security of biometric recognition frameworks, by adding liveness assessment in a fast, user-friendly, and non-intrusive manner, through the use of image quality assessment. The proposed approach presents a very low degree of complexity, which makes it suitable for real-time applications, using 25 general image quality features extracted from one image (i.e., the same acquired for authentication purposes) to distinguish between legitimate and impostor samples. The experimental results, obtained on publicly available data sets of fingerprint, iris, and 2D

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 2,Special Issue 6, March 2016

face.A high level industry uses passwords like thumb, face, voice, iris, etc. So many security systems are available. But not so reliable. Here the developing system which is very precise and reliable. The system has two stages which is embedded system. Even if any stage is cracked falsely, unauthorized entry will be detected.Liveness detection methods are usually classified into two techniques. First is a Software-based techniques, in this case the fake trait is detected once the sample has been acquired with a standard sensor (i.e., features used to distinguish between real and fake traits are extracted from the biometric sample, and not from the trait itself). And second is a Hardware-based technique, which adds some specific device to the sensor in order to detect particular properties of a living trait (e.g., fingerprint sweat, blood pressure).The thumb samples are stored in the sensor If there is a fake samples which does not match with the stored samples (i.e.Face,Fingerprint) then the buzzer will beep continuously. The two types of methods present certain advantages and drawbacks over the other and, in general, a combination of both would be the most desirable protection approach to increase the security of biometric systems. As a coarse comparison, hardware-based schemes usually present a higher fake detection rate, while software-based techniques are in general less expensive (as no extra device is needed), and less intrusive since their implementation is transparent to the user. Keywords– PCB, AVR, studio, PCA, Buzzer etc. To design and implement a system that provides double security against the fake biometric scanning of face or fingerprint using two stages for confirmation that the user who gets access to the system is authorized.

The system is divided into the following modules:

1) PC (JAVA)
2) Microcontroller-ATmegA16
3) Buzzer- DC 5V
4) Fingerprint
5) Camera

Advantages

- Blocking attackers and allowing legitimate users in the systems.
- To enhance the security of biometric recognition frameworks

Disadvantages

- The effectiveness of the sample collection process is strongly influenced by environmental conditions, user training and usability.

2.4 Attack of Mechanical Replicas: Liveness Detection With Eye Movements, Oleg V. Komogortsev, Alexey Karpov.

This investigates liveness detection techniques in the area of eye movement biometrics. Investigate a specific scenario, in which an impostor constructs an artificial replica of the human eye. Two attack scenarios are considered: 1) the impostor does not have access to the biometric templates representing authentic users, and instead utilizes average anatomical values from the relevant literature and 2) the impostor gains access to the complete biometric database, and is able to employ exact anatomical values for each individual. Liveness detection is performed at the feature and match score levels for several existing forms of eye movement biometric, based on different aspects of the human visual system. The ability of each technique to differentiate between live and artificial recordings is measured by its corresponding false spoof acceptance rate, false live rejection rate, and classification rate. The results suggest that eye movement biometrics is highly resistant to circumvention by artificial recordings when liveness detection is performed at the feature level. The ability of each technique to differentiate between live and artificial recordings is measured by its corresponding false spoof acceptance rate, false live rejection rate, and classification rate. Liveness detection is an important problem in the biometric domain, due to the fact that it is relatively simple to create convincing replicas of many existing biometrics. For example, commercial iris identification systems can be spoofed by high-resolution images of the eye printed on paper, with a hole to present the intruder's pupil, bypassing liveness detection mechanisms.

There are further examples of fingerprint scanners being spoofed by common household items like gelatin, and face detection systems spoofed by printed images of the face .Related Work in Eye Movement Biometrics In the current work, we explore the liveness detection propertiesof four existing eye movement biometric techniques,based on various aspects of the human visual system. These techniques include: oculomotor plant characteristics (OPC), complex oculomotor behavior (COB), complex eye movement patterns (CEM-P), and complex eye movement behavior (CEM-B) biometrics. In 2011, Holland and Komogortsev [20] described complexeye movement pattern (CEM-P) biometrics. CEM-P compares.Based on different aspects of the human visual system. The ability of each technique to differentiate between live and artificial recordings is measured by its corresponding false spoof acceptance rate, false live rejection rate, and classification rate. The results suggest that eye movement biometrics is highly resistant to circumvention by artificial recordings when liveness detection is performed at the feature level. The ability of each technique to differentiate between live and artificial recordings is measured by its corresponding false spoof acceptance rate, false live rejection rate, and classification rate. The results suggest that eye movement biometrics is highly resistant to circumvention by artificial recordings when liveness detection is performed at the feature level.

Advantages

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 2,Special Issue 6, March 2016

- Liveness detection methods should posses other important properties being non-invasive.

Disadvantages

- Face detection systems spoofed by printed images of the face.

2.5 Pupil dynamics for iris liveness detection., Adam Czajka, Senior Member.

The primary objective of this paper is to propose a complete methodology for eye liveness detection based on pupil dynamics. This method may serve as a component of presentation attack detection in iris recognition systems, making them more secure. Due to a lack of public databases that would support this research, we have built our own iris capture device to register pupil size changes under visible light stimuli, and registered 204 observations for 26 subjects (52 different irides), each containing 750 iris images taken every 40 ms. Each measurement registers the spontaneous pupil oscillations and its reaction after a sudden increase of the intensity of visible light. The Kohn and Clynes pupil dynamics model is used to describe these changes; hence we convert each observation into a feature space defined by model parameters. To answer the question whether the eye is alive (that is, if it reacts to light changes as a human eye) or the presentation is suspicious (that is, if it reacts oddly or no reaction is observed), we use linear and non-linear Support Vector Machines to classify natural reaction and spontaneous oscillations, simultaneously investigating the goodness of fit to reject bad modeling. Our experiments show that this approach can achieve a perfect performance for the data we have collected: all normal reactions are correctly differentiated from spontaneous oscillations. We investigated the shortest observation time required to model the pupil reaction, and found that time periods not exceeding 3 seconds are adequate to offer a perfect performance.In this Existing System, Biometric systems have their own weaknesses; in particular they are relatively vulnerable to some sophisticated forms of spoofing. It is possible to fool a fingerprint-based system by reproducing the biometric pattern on simple molds made of materials such as silicone, clay or gelatin. Iris-based systems can be attacked with fake irises printed on paper or on wearable plastic lenses. Face-based systems can be fooled with sophisticated 3D masks or with faces printed on paper. A large number of methods have been proposed in recent years to combat spoofing .Some of them rely on the detection of vitality signs at the acquisition stage. Hence they require additional hardware embedded in the sensor which verifies vitality by measuring particular intrinsic properties of a living trait, such as temperature, odor, sweat, blood pressure, or reflection properties of the eye sometimes also in response to specific stimuli .By combining multiple sources of information, this approach turns out to be more resilient to specific attacks, providing a very good reliability. However, it is a relatively expensive and rigid solution, potentially vulnerable to attacks not considered at design time.

Lack of standardization. While the reliability and the accuracy of biometric devices continues to improve. Biometric systems must be able to accommodate changes to the biometric over time which may be caused by ageing, illness or injury. The effectiveness of the sample collection process is strongly influenced by environmental conditions, user training and usability. For example, lighting, facial orientations, , image resolution and the wearing of hats can affect the quality of the sample.

In this Proposed System, propose a face descriptor, Local Directional Number Pattern (LDN), for robust face recognition that encodes the structural information and the intensity variations of the face's texture. LDN encodes the structure of a local neighbourhood by analyzing its directional information.

Advantages

- Robust against illumination changes
- Performance Better

Disadvantages

- Lack of standardization.
- The biometric over time which may be caused by ageing, illness or injury.

III. PROPOSED SYSTEM

In this Proposed System, propose a face descriptor, Local Directional Number Pattern (LDN), for robust face recognition that encodes the structural information and the intensity variations of the face's texture. LDN encodes the structure of a local neighbourhood by analyzing its directional information. Consequently, compute the edge responses in the neighbourhood, in eight different directions with a compass mask. Then, from all the directions, choose the top positive and negative directions to produce a meaningful descriptor for different textures with similar structural patterns. This approach allows us to distinguish intensity changes.Biometric systems attacks have elicited a race towards some reliable anti-spoofing systems. In this proposed technology process with liveness detection techniques, which use various physiological properties to distinguish between real and fake traits.

To detect liveness by analyzing synthetic image features that are peculiar of vital biometric traits and not easily reproduced on fakes. The present effort, as the time seems mature for a reasoned review and analysis of LD-based techniques(local descriptors) applied to biometric liveness detection.

Advantages

1. Robust against illumination changes.
2. Performance Better.
3. Compact Mode.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 2,Special Issue 6, March 2016

3.1 PROJECT DESCRIPTION

Biometric authentication systems are quite vulnerable to sophisticated spoofing attacks. To keep a good level of security, reliable spoofing detection tools are necessary, preferably implemented as software modules. The research in this field is very active, with local descriptors, based on the analysis of micro textural features, gaining more and more popularity, because of their excellent performance and flexibility.This aims at assessing the potential of these descriptors for the liveness detection task in authentication systems based on various biometric traits: fingerprint, iris, and face. Besides compact descriptors based on the independent quantization of features, already considered for some liveness detection tasks, it will study promising descriptors based on the joint quantization of rich local features. The potential of these tools for biometric applications, and points out possible lines of development toward further improvements. A Biometric System is a system for the automated recognition of individuals based on their behavioral and biological characteristics. Depending on the context, in a biometric system, there are two different ways to resolve a person's identity.Local directional number pattern (LDN), for face analysis, i.e., face and recognition.LDN encodes the directional information of the face's textures (i.e., the texture's structure) in a compact way, producing a more discriminative code than current methods.

The structure of each micro-pattern with the aid of a compass mask that extracts directional information, and encodes such information using the prominent direction indices (directional numbers) and signs which allows us to distinguish among similar structural patterns that have different intensity transitions. The face into several regions, and extract the distribution of the LDN features from them.
System design is a transaction from a user-oriented document to a document oriented programmer or personnel. It emphasis on translating performance specification and it involves conceiving and planning and then carrying out the plan by generating the necessary reports and outputs. Design phase acts as an interface between the software requirement specification phases which satisfy the requirements. System design is concerned with the design of:

3.2 INPUT DESIGN

Input design converts the user oriented inputs to computer oriented formats, which requires careful attention. The collection of input data is the most expensive part of the system, in terms of both the equipment used and number of people involved. In input design, data are accepted for computer processing and input to the system is done through maps created using basic mapping support facility.Inaccurate input data are the most common cause of errors in data processing. The input screens are very carefully and logically designed. For data entry or for data access, different menus are used which makes the data entry as easy as possible. While entering data validation checks are done and message will be generated by the system in case of incorrect data entry.

3.2.1 Some of the features are

- The input data are validated to minimize data entry error.
- Appropriate messages are provided to inform user about a false entry.
- Fixed format is used for displaying titles and messages.
- The form title clearly states the purpose of the form.
- Heading for each data item are clearly given.
- Adequate space is given for the data item.
- Forms are not crowded, as forms are difficult to read or validate

3.3 OUTPUT DESIGN

In any system, the result of the processing are communicated to the user and to other systems using outputs. In output design, it is determined how the information is to be displayed for the immediate need and for the hard copy output. It is most important and direct source of information to the user. Efficient and intelligent output design improves the relationship of user with the system and helps in decision making. The output design includes reports in the specific formats, displays of enquires as well as simple profile of the database.

3.4 System Architecture

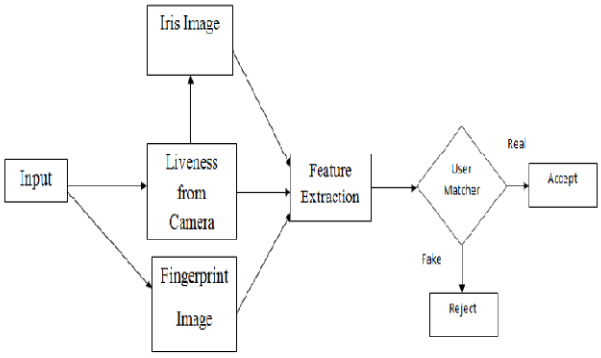

Fig 3.1 System Architecture

3.5 DATA FLOW

Data flow diagram shows the flow of data from external entities into the system, shows how data moves from one process to another, as well as its logical storage. They are represented as directed graphs in which the nodes

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 2,Special Issue 6, March 2016

specify processing activities and the arcs specify data items transmitted between processing nodes. These diagrams are used to specify the external characteristics of the software system.

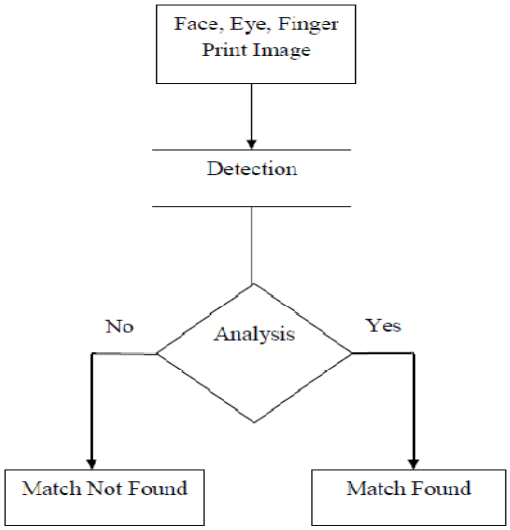

Fig 3.2 Data Flow

3.6 MODULES

3.6.1. Liveness detection module

In this module, securing automated and unsupervised biometric recognition systems used for the access control is one of the most critical and most challenging tasks in real world scenarios. A variety of methods can be used to get an unauthorized access to a system based on the automated biometric recognition. A biometric of a person enrolled in a database is easy to acquire, even without the user's cooperation. To discourage potential attackers from presenting a fake biometric prevent false acceptance to recognize if the biometric on the plate of the webcam is alive or not.

3.6.2 Feature extraction module

In this Module, The acquired biometric data is processed to extract a set of most important or unreasonable features. For example, the position and orientation of minutiae points (local ridge and valley singularities).In a Biometric image are extracted in the feature extraction module of a Iris, Fingerprint, and Face Recognition from live -based biometric system.

3.6.3 Matcher module

The biometric system to store the biometric templates of the enrolled users. The enrolment module is responsible for enrolling individuals into the biometric system database. During the enrolment phase, the biometric characteristic of an individual is first scanned by a biometric reader to produce a digital representation (feature values) of the characteristic. The data capture during the enrolment process may or may not be supervised by a human. In order to facilitate matching, the input digital representation is further processed by a feature extractor to generate a compact but meaningful representation.

3.6.4 System database module

In this module, facial recognition is discriminating input signals (image data) into several classes (persons). The input signals are highly noisy, yet the input images are not completely random and in spite of their differences there are patterns which occur in any input signal. Such patterns, which can be observed in all signals, could be - in the domain of facial recognition - the presence of some objects in any face as well as relative distances between these objects.These characteristic features are called eigenfaces in the facial recognition domain (or principal components generally). They can be extracted out of original image data by means of a mathematical tool called Principal Component Analysis (PCA). By means of PCA one can transform each original image of the training set into a corresponding eigenfaces. An important feature of PCA is that one can reconstruct any original image from the training set by combining the eigenfaces. Remember that eigenfaces are nothing less than characteristic features of the faces. Therefore one could say that the original face image can be reconstructed from eigenfaces if one adds up all the eigenfaces (features) in the right proportion.

3.7 METHODOLOGY

Principal Component Analysis:

PCA finds a linearprojection of high dimensional data into a lower dimensional subspace such as:

- The variance retained is maximized.
- The least square reconstruction error is minimized.
- LSI: Latent Semantic Indexing.
- Kleinberg/Hits algorithm (compute hubs and authority scores for nodes).
- Image compression (Eigen faces).
- Data visualization (by projecting the data on 2D).

IV. EXPERIMENTAL RESULTS ANDDISCUSSIONS

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 2,Special Issue 6, March 2016

Fig 4.1 Admin Form

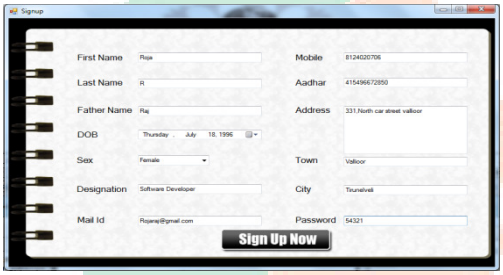

Fig 4.2 Sign up page

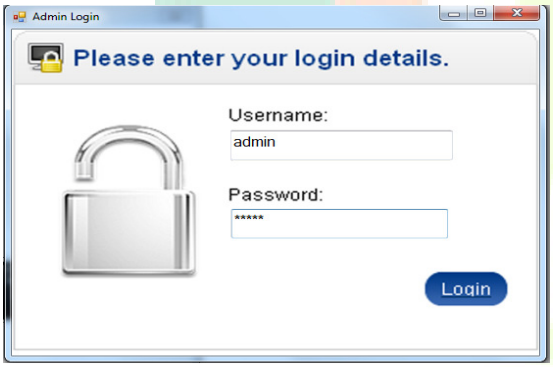

Fig 4.3 Admin login

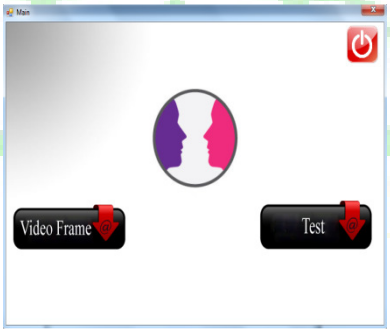

Fig 4.4 Main Form

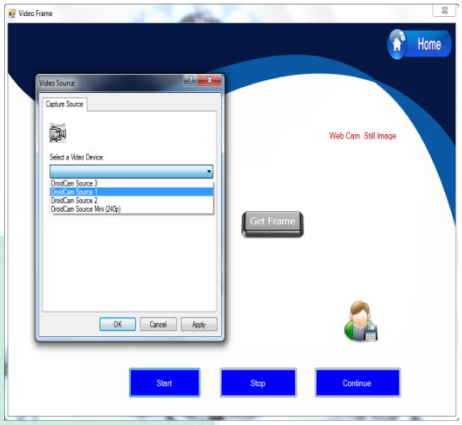

Fig 4.5 Webcam Setting

Fig 4.6 Get Frame Form

Fig 4.7 Save Image

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 2,Special Issue 6, March 2016

Fig 4.8 Pattern Identified Face

Fig 4.9 Generate Form

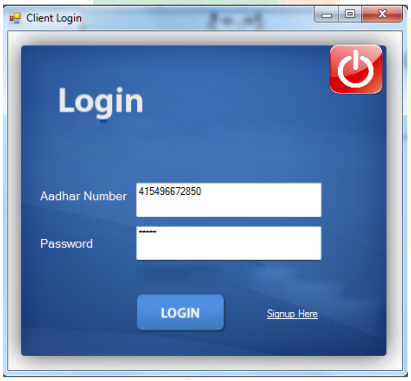

Fig 4.10 Client Login

Fig 4.11 Post Test

Fig 4.12 Scanning

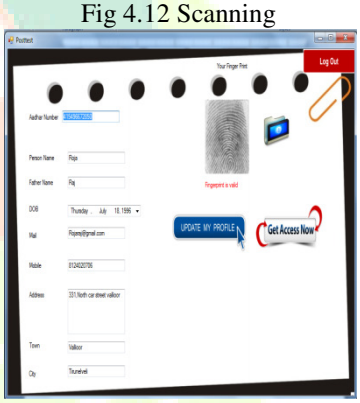

Fig 4.13 Check The Details

V. CONCLUSION

Image descriptors based on local features for the liveness detection of fingerprint, iris, and face images. facial recognition system proposed which is based on the LDPv representation, which encodes the spatial structure and contrast information of facial s. Extensive experiments illustrate that the LDPv features are effective and efficient for recognition. It is possible to take a still image and determine the on the face; however, there is still much work to be done. Some ideas considered were contours, weighting a face, and possibly a mixture of these. Contours, as described above, were briefly. By simply taking contours naively, the result is actually very noisy and it is very difficult to ascertain that is being made by the face.

REFERENCES

1. J. A. Unar, W. C. Seng, and A. Abbasi, "A review of biometric technology alon g with trends and prospects," Pattern Recognit. Aug. 2014.

ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 2,Special Issue 6, March 2016

2.T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, "Impact ofartificial'gummy' fingers on fingerprint systems, Apr. 2002.
3.J. Galbally et al., "An evaluation of direct attacks using fake fingers generatedfrom ISO templates," Pattern Recognit. Lett., vol. 31, no. 8,2010.
4.T. Matsumoto, "Artificial irises: Importance of vulnerability analysis",vol. 45. 2004.
5.V. Ruiz-Albacete, P. Tome-Gonzalez, F. Alonso-Fernandez, J. Galbally, J. Fierrez, and J. Ortega-Garcia, "Direct attacks using fake images in iris verification," in Computer Science), vol. 5372.
6.N. Kose and J.-L. Dugelay, "On the vulnerability of face recognition systems to spoofing mask attacks," in Proc. IEEE Int. Conf. Acoust., Speech, Signal Process. (ICASSP), May 2013
7.D. Maltoni, D. Maio, A. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition. New York, NY, USA: Springer-Verlag, 2009.
8.E. Marasco and A. Ross, "A survey on antispoofing schemes for fingerprint recognition systems," ACM Comput. Surv., vol. 47, no. 2, 2014
9.Y. N. Singh and S. K. Singh, "Vitality detection from biometrics: State-of-the-art," in Proc. World Congr. Inf. Commun. Technol., Dec. 2011.
10. D. Baldissera, A. Franco, D. Maio, and D. Maltoni, "Fake fingerprint detection by odor analysis," in Proc. Int. Conf. Biometrics, vol. 3832. Jan. 2006,
11.A. Pacut and A. Czajka, "Aliveness detection for iris biometrics," in Proc. 40th Annu. IEEE Int. Carnahan Conf. Secur. Technol., Oct. 2006,
12.E. C. Lee and K. R. Park, "Fake iris detection based on 3D structure of iris pattern," Int. J. Imag. Syst. Technol., vol. 20, no. 2, 2010.
13.S. B. Nikam and S. Agarwal, "Local binary pattern and wavelet based spoof fingerprint detection," Int. J. Biometrics, vol. 1, no. 2,
14.L. Ghiani, A. Hadid, G. L. Marcialis, and F. Roli, "Fingerprint liveness detection using binarized statistical image features," Sep./Oct. 2013.
15.D. Gragnaniello, G. Poggi, C. Sansone, and L. Verdoliva, "Wavelet-Markov local descriptor for detecting fake fingerprints," Electron. Lett., vol. 50, no. 6, Mar. 2014.
16.Z. Sun, H. Zhang, T. Tan, and J. Wang, "Iris image classification based on hierarchical visual codebook," IEEE Trans. Pattern Anal. Mach, Jun. 2014.
17.D. Yadav, N. Kohli, J. S. Doyle, R. Singh, M. Vatsa, and K. W. Bowyer, "Unraveling the effect of textured contact lenses on iris recognition," IEEE Trans. Inf. Forensics Security, vol. 9, no. 5, May 2014.
18.N. Erdogmus and S. Marcel, "Spoofing face recognition with 3D masks," IEEE Trans. Inf. Forensics Security, Jul. 2014.
19.J. Galbally, S. Marcel, and J. Fierrez,"Image quality assessment for fake biometric detection: Application to iris, fingerprint, and face recognition," Feb. 2014.
20.G. L. Marcialis et al., "First international fingerprint liveness detection competition—LivDet 2009," in Image Analysis and Processing. Berlin,Germany: Springer-Verlag, 2009.