ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

A Secure Multimodal Biometric System

Akhil S, Neeraja M.Nair, Asst. Prof. Vidhya P.M

Final Year M.Tech Student (Cyber Security), Dept. of Computer Science, SNGCE, Kerala, India

Final Year M.Tech Student (Cyber Security), Dept. of Computer Science, SNGCE, Kerala, India

Asst. Professor, Dept. of Computer Science, SNGCE, Kerala, India

ABSTRACT: Among tangible threats and vulnerabilities facing current biometric systems are spoofing attacks. A spoofing attack occurs when a person tries to masquerade as someone else by falsifying data and thereby gaining llegitimate access and advantages. Now a days spoofing attacks using 3D masks are very common due to the advancements in 3D printing technologies. Existing system against this spoofing attack is a unimodal biometric system and have many drawbacks. Hence there is a requirement to preventing this attack in biometrics. Here introducing a new secure multimodal biometric system. Multimodal biometric systems are accurate ,secure, increased and reliable recognition and better user acceptance.

KEYWORDS: biometric, multimodal, spoofing

I. INTRODUCTION

Being the most commonly used biometric trait by humans, face recognition has become an active research topic for many decades now and it has found great application in consumer electronics and software. Face owes its reputation mainly to being easily and non-intrusively accessible compared to other biometric traits like finger print or iris. However, this advantage becomes a weakness in malicious circumstances, enabling attackers to create copies and spoof face recognition systems without any difficulties. Spoofing attack is the act of outwitting a biometric system by presenting a fake evidence in order to gain authentication. It is relatively simple to forge such an attack for facial recognition systems, due to the fact that the photographs or videos of a valid user can be easily captured from a distance or obtained via internet, e.g. through social networks. Valid users (simply users or clients) can be defined as the persons that are enrolled in a face recognition system. An attacker can attempt to gain access by simply showing their printed photos or replaying their recorded videos to the sensor. This apparent vulnerability of face has evoked great interest in the biometric community and many papers have been published on countermeasure studies. Mainly as a result of their simplicity and low-cost, the previously mentioned photo print and video replay attacks constitute the focus of research activities in this domain.

Recently, several studies have been published that present methodical and reproducible analyses of several of these and some other methods, with a shared purpose of providing comparable results on public databases .Work on fraud detection capabilities for face is still limited and a substantial part of it is based on the flatness of the captured surface in front of the sensor during an attack. This is also true for approaches that examine the 3D nature of the face by employing additional devices, which is much more realistic now with the introduction of affordable consumer depth cameras like Kinect. For instance, in, 3D data acquired with a low-cost sensor is utilized to localize face and at the same time to test its authenticity to decrease their systems vulnerability to spoofing attacks. Unfortunately, methods that depend on the assumption of a planar surface for a fake face are rendered futile in case of 3D facial mask attacks. With the help of the advancements in 3D manufacturing technologies, easily attainable facial masks take the spoofing attacks one step further and introduce new challenges for counter measure studies. To the best of our knowledge, there have been very few studies published addressing this issue and they are detailed in the next section. Here we implement a strong face recognition and anti-spoofing approach against 3D mask spoofing attacks. The technique of biometric security can be increased by considering a multi modal biometric system as the extension.

Existing anti-spoofing approaches against these type of attacks can be roughly classified into three groups: texture analysis, motion analysis and liveness detection .And most of the studies deals with private date data bases which is a difficult task for future studies and further modifications. Unfortunately, methods that depend on the assumption of a

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

planar surface for a fake face are rendered futile in case of 3D facial mask attacks. Though the unimodal biometric systems have many advantages, it has to face with variety problems.

An attacker can attempt to gain access by simply showing their printed photos or replaying their recorded videos to the sensor. It is relatively simple to forge such an attack for facial recognition systems, due to the fact that the photographs or videos of a valid user can be easily captured from a distance or obtained via internet, e.g. through social networks. Here a strong method of biometrics is proposed which can prevent various attacks. The technique of biometric security can be increased by considering a multi modal biometric system as the extension.

II. RELATED WORK

Being the most commonly used biometric trait by humans, face recognition has become an active research topic for many decades now and it has found great application in consumer electronics and software. Face owes its reputation mainly to being easily and non-intrusively accessible compared to other biometric traits like finger print or iris. However, this advantage becomes a weakness in malicious circumstances, enabling attackers to create copies and spoof face recognition systems without any difficulties. Spoofing attack is the act of outwitting a biometric system by presenting a fake evidence in order to gain authentication. It is relatively simple to forge such an attack for facial recognition systems, due to the fact that the photographs or videos of a valid user can be easily captured from a distance or obtained via internet, e.g. through social networks. Valid users (simply users or clients) can be defined as the persons that are enrolled in a face recognition system. An attacker can attempt to gain access by simply showing their printed photos or replaying their recorded videos to the sensor. This apparent vulnerability of face has evoked great interest in the biometric community and many papers have been published on countermeasure studies.

Nesli Erdogmus et al. [24], proposed Spoofing Face Recognition With 3D Masks with aim to inspect the spoofing potential of subject-specific 3D facial masks for different recognition systems and address the detection problem of this more complex attack type.

A. Mask Attack Database

The 3D Mask Attack Database (3DMAD) is a face spoofing database which currently contains 76500 frames of 17 different users, recorded using Microsoft Kinect sensor for both real access and spoofing attacks using 3D facial masks. Each frame consists of:

_ a depth image (640 X 480 pixels - 1 X 11 bits)
_ the corresponding color image (640 X 480 pixels - 3 X 8 bits)
_ manually annotated eye positions (with respect to the color image)

The production of the database can be divided into two stages: manufacturing the 3D masks and recording the videos that will be explained in detail in the following subsections.

B. Manufacturing the 3D Masks

It is said that spoofing attacks using 3D facial masks cannot become a common practice in the literature, mainly because of the high cost of client-like masks. However, recently 3D printing services have sprung up and become a rapidly growing market, unfortunately, smoothing the way for different mask attack possibilities to face recognition systems.

Figure 1: 17 hard resin masks from 3DMAD

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

The technique used to manufacture the masks in the Morpho database requires the 3D models of the valid users to be captured in order to be constructed using a regular 3D printer.

C. Recording of the Database

Microsoft Kinect for Xbox 360 is utilized to record all samples in the database both for real accesses and mask attacks. Its sensor captures both color and depth data in the scene at 30 frames per second. The main reason behind the selection of this device over other conventional cameras is the additionally provided depth information, which makes it possible:

_ To explore the attacks and devise countermeasures in 3D,

_ To analyse the vulnerability of 3D face recognition systems to mask attacks in addition to their 2D counterparts.

Figure 2: Creation of masks from 3D MAD

D. Baseline Face Recognition Algorithm

Before moving on to develop counter measures against mask attacks, it is important to assert the threat they pose on the security of face recognition systems. In other words, it is required to evaluate the vulnerability of commonly employed face recognition algorithms to these type of spoofing attempts. For 2D and 2.5D, LBP histograms are extracted and compared using the Ï2 distance metric for both 2D and 2.5D images. For 3D face matching, Thin Plate Spline (TPS) warping parameters are obtained by aligning each face model with a generic one and comparison is done by computing cosine distances between corresponding feature vectors. In a similar manner to these studies, ISV algorithm is selected to be applied on both grayscale texture images and depth maps for 2D and 2.5D face recognition, respectively. As for the 3D, since both databases do not include any facial expressions, Iterative Closest Point (ICP) method is selected to register surface pairs to each other and ICP error is simply taken as a measure of how well they match. These algorithms are selected simply to expand the number of different face recognition methods whose vulnerabilities are analysed against 3D mask attacks.

E. ICP Method for 3D Face Recognition

Iterative Closest Point (ICP) algorithm is a well-established technique used for rigid registration of 3D surfaces. In order to minimize the distance between two cloud points (which is the sum of distances calculated for all points in one of the surfaces, finding the closest point on the other), ICP computes and revises the translation and rotation iteratively. This registration is used to establish point to point correspondences between two face models. In fact, this is the chosen approach for our 3D face recognition baseline system. Two main shortcomings of ICP are that it needs a good initialization for an accurate result and it cannot handle non rigid transformation which is crucial in the presence of surface deformations, such as occlusions or facial expressions. But then, these issues are irrelevant in our case, since in both databases face samples are neutral and frontal. It is aware that there exist many other more powerful methods but we are just interested in providing a baseline study on the vulnerabilities to 3D mask attacks that is open source and available for the research community to reuse.

F. Anti-Spoofing Algorithm

As explained in the Introduction section, it is more difficult to detect 3D mask attacks with motion analysis and liveness detection methods. For this reason, texture analysis remains as a more reliable approach that can be adopted. Naturally, human skin is different from mask materials with its optical characteristics, such as reflectance or scattering. This fact facilitates utilization of texture properties to discriminate between real faces and masks. Local Binary Patterns

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

(LBP) is a simple and efficient texture operator which has become a popular approach in various computer vision applications . As a matter of fact, LBP and its variations have been successfully applied in counter measures against 2D spoofing attacks . In our work, we aim to study and compare discriminative properties of various types of LBP operators including the one proposed in real face / mask classification, using both 3DMAD and Morpho databases.

G. Extraction of LBP Based Features

The original LBP value for each pixel is calculated by comparing its adjacent pixels in 3 X 3 neighbourhood with the value of that pixel and forming a 8-bit binary number from the results (LBP8,1). A common extension to the original operator is to eliminate patterns with more that two bitwise transition. This reduces the number of different labels and results in 59 uniform patterns (LBPu2 8,1). The LBP operator can also be extended to use neighbourhoods of various size (different circle radius (R) and different number of sampling points (P) - LBPP,R) or to change the encoding method. The occurrences of the LBP labels in the whole image or in blocks are collected into histograms and then considered as feature vectors to be classified. It results in an enhanced feature histogram of length 833. In this manuscript, three more extensions from are included and analyzed: modified (mLBP), transitional (tLBP) and direction-coded (dLBP). Instead of the pixel value, the mLBP uses the average of the neighbouring pixels for comparison. In tLBP, two consecutive neighbour pixels are compared circularly in clock-wise direction and in dLBP, intensity variation is encoded for only four base directions into two bits, again resulting in 8-bit value.

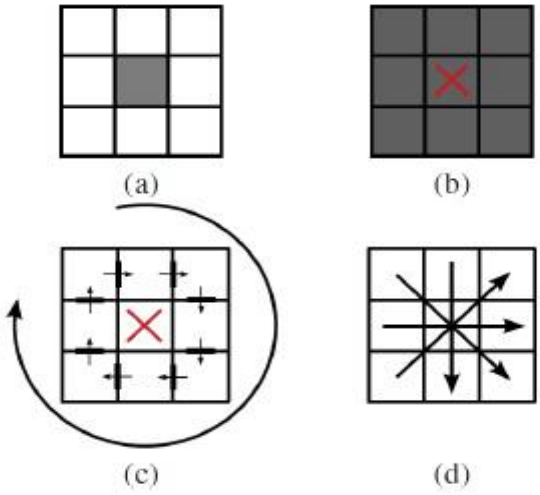

Figure 3: Extended set of LBPs:(a)Conventional LBP (b)8-bit coded modified LBP (c)transition coded LBP (d) direction coded LBP

Additionally, the influence of dividing face images into blocks is assessed for each extended LBP type. The face image is broken into 3 Ã 3 non-overlapping blocks after the LBP values are computed. Histograms are calculated separately for each block and the final feature vector is formed by concatenation.

H. Feature Classification

Since the extracted LBP codes are collected into histograms, the classification can be simply performed by computing histogram similarities. So firstly, two reference histograms are calculated as the average of real access and mask attack samples in the training set and the features extracted from test samples are compared with these two using X2 metric, resulting in two distances: Dreal and Dmask. The final score is computed as Dmask Dreal . In this study, a comparison between the two kernels is made with respect to their mask attack detection capabilities. Additionally, Linear Discriminant Analysis (LDA) is tested in addition to X2 and SVM. Prior to LDA classification, Principal Component Analysis (PCA) is applied to reduce dimensionality while preserving 99 percent of the energy.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

III. PROPOSED ALGORITHM

Existing anti-spoofing approaches against these type of attacks can be roughly classified into three groups: texture analysis, motion analysis and liveness detection. And most of the studies deals with private date data bases which is a difficult task for future studies and further modifications. The spoofing face recognition with 3D masks propose a method to prevent against spoofing attacks.
The main drawbacks of current system are:

_ There are chances of : False Fake and False Living conditions.
_ Enrollment and Extraction Processes are time consuming.
_ Unimodal biometric system has limitations in accuracy, enrollment rates etc.
_ There is no encryption methods for the protection of database used.
_ System doesn't provide an opportunity to Add, Delete or Modify/Replace access of individuals.

Existing system is not 100 percent successful in detecting spoofing attacks. Hence there is a requirement to identify a method to prevent against the attacks in biometrics. Though the uni-model biometric systems have many advantages, it has to face with variety problems. Hence a multi model biometrics can be used as a better solution. Some of the limitations imposed by unimodal biometric systems can be overcome by including multiple sources of information for establishing identity. Such systems, known as multimodal biometric systems, are expected to be more reliable due to the presence of multiple, (fairly) independent pieces of evidence. These systems are able to meet the stringent performance requirements imposed by various applications. They address the problem of non-universality, since multiple traits ensure sufficient population coverage. They also deter spoofing since it would be difficult for an impostor to spoof multiple biometric traits of a genuine user simultaneously. Furthermore, they can facilitate a challenge response type of mechanism by requesting the user to present a random subset of biometric traits thereby ensuring that a live user is indeed present at the point of data acquisit. Advantages of using Multi model biometrics:

_ Accuracy: Multimodal biometrics uses information from two or more biometrics (e.g. fingerprint and finger vein pattern; or fingerprint and iris and voice) whereas unimodal biometric systems use information from one biometric (e.g. fingerprint, iris, palm, signature, voice, hand shape, or face). The accuracy of a multimodal biometrics system is normally calculated in terms of image acquisition errors and matching errors. Image acquisition errors consist of failure-to-acquire (FTA) and failure-to enroll (FTE) rate whereas matching errors comprise false non-match rates (FNMR) in which a legitimate person is rejected and a false match rate (FMR) where an impostor is granted access. Multimodal biometric systems have almost zero FTE, FMR FTA rates because in this system, each and every subsystem has a viewpoint or a determination on the users claim. The examiner module utilizes various fusion strategies in order to combine each single subsystem decision or opinion and then come up with a conclusion. This is the reason that multimodal biometrics are more accurate than unimodal or any other authentication system.

_ Increased and Reliable Recognition: A multimodal biometric system permits a greater level of assurance for an accurate match in verification as well as identification modes. As multimodal biometric systems utilize multiple biometric traits, each single trait can offer additional evidence about the authenticity of any identity claim. For example, the patterns of movements (gaits) of two individuals of the same family or coincidentally of two different persons can be similar. In this particular circumstance, a unimodal biometric system based only on gait pattern analysis might lead to a false recognition. If the same biometric system additionally includes fingerprint matching or finger vein matching, the system would certainly results in increased recognition rate, as it is nearly impossible that two different individuals have same gait as well as fingerprint/finger vein pattern.

_ Enhanced Security: Another advantage of a multimodal biometric system is that by making use of multiple methods of identification, a system can preserve higher threshold recognition settings and a system administrator can make a decision on the level of security that is needed. For an extremely high security site/area, you might need to use up to three biometric identifiers and for a lower security site/area, you could possibly require one or two credentials. If one of the identifiers fails for any unknown reason, your system can still utilize another one or two of them in order to provide the accurate identification of a person. In this way, it significantly reduces the probability of admitting an imposter.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

_ User Acceptance: As multimodal biometric systems are more accurate, reliable, have larger security options, and have the ability to avoid spoofing attacks, these systems are more widely accepted in many countries that cover large to larger deployments. Biometric deployments that encompass large scale population databases are turning to multimodal systems. However, in deployments where security and accuracy are paramount, no matter how small, multimodal systems have become ubiquitous. Here we consider Iris scan along with face recognition. Feature extraction within this system is done using image quality assurance measures. Main advantages of proposed system are:
_ Enrollment and extraction time is reduced.
_ Database as well as employee credentials are encrypted.
_ Provision for Add, Delete and Modifying individuals access.
_ The proposed system enhances 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 use of image quality assessment for liveness detection is motivated by the assumption that: It is expected that a fake image captured in an attack attempt will have different quality than a real sample acquired in the normal operation scenario for which the sensor was designed. Expected quality differences between real and fake samples may include: degree of sharpness, color and luminance levels, local artifacts, amount of information found in both type of images (entropy), structural distortions or natural appearance. Gaussian filtering is used to blur images and remove detail and noise. Full reference (FR) IQA methods rely on the availability of a clean undistorted reference image to estimate the quality of the test sample. No Reference IQA try to handle problem of assessing the visual quality of images in the absence of a reference. After final parameterization , classification is done using LDA classifier.

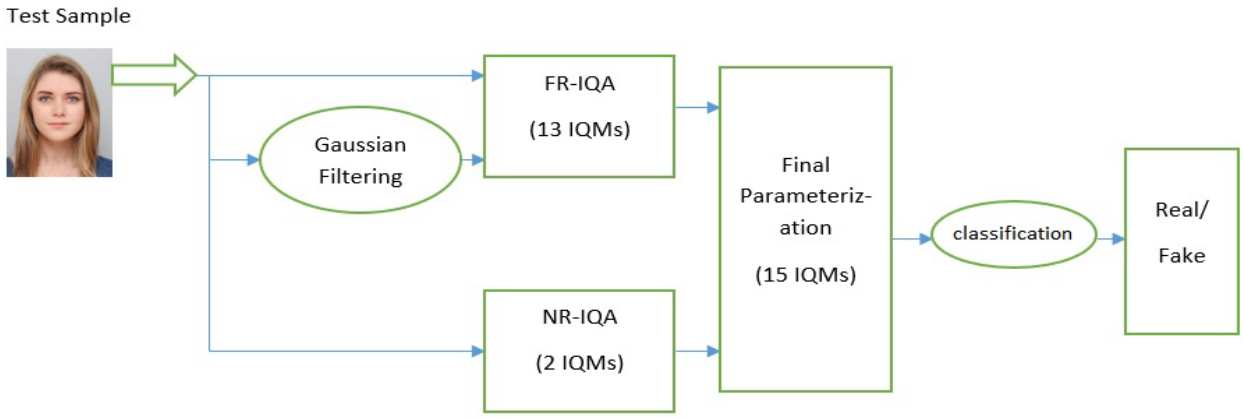

Figure 4: DFD of the system

IV. RESULTS AND DISCUSSION

The overall security of system is enhanced through multimodal biometric. Main achievements of proposed system are enrollment and extraction time is reduced, database as well as employee credentials are encrypted, provision for add, delete and modify employee access. Thus new system addresses the spoofing attack threat and enhances the overall security. The system has been implemented and the figure 5 shows the verification of users access based on the proposed method.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

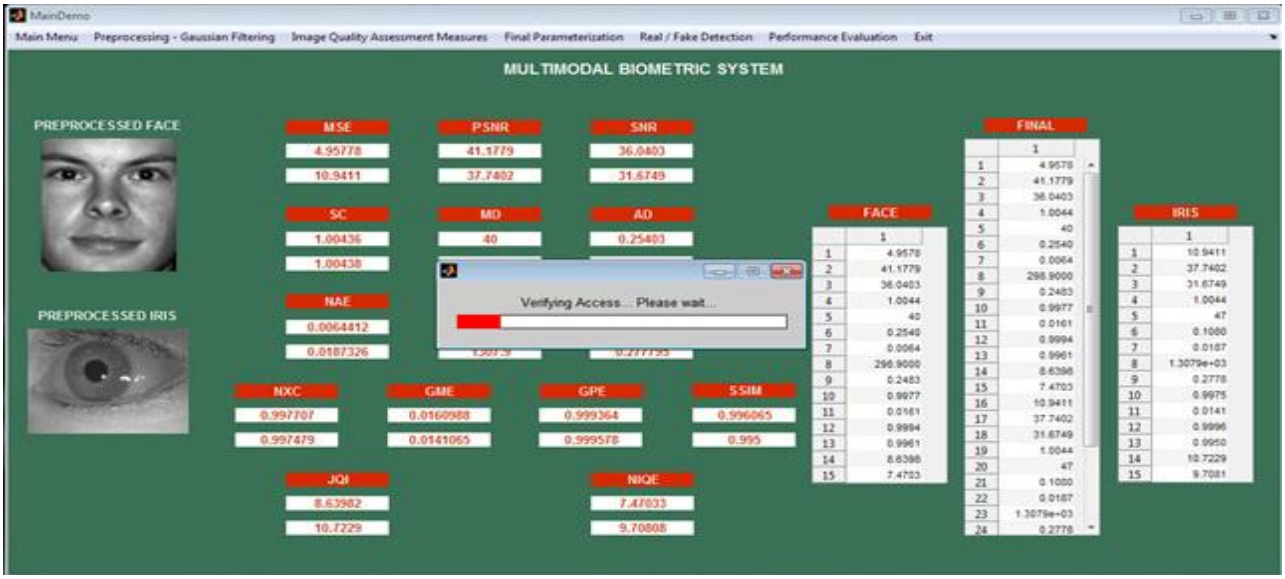

Figure 5: Verifying access after all processes

The user after gaining access will be then redirected to view the users details that is secured and encrypted using the biometric traits. The figure 6 shows the users accessing the secured details.

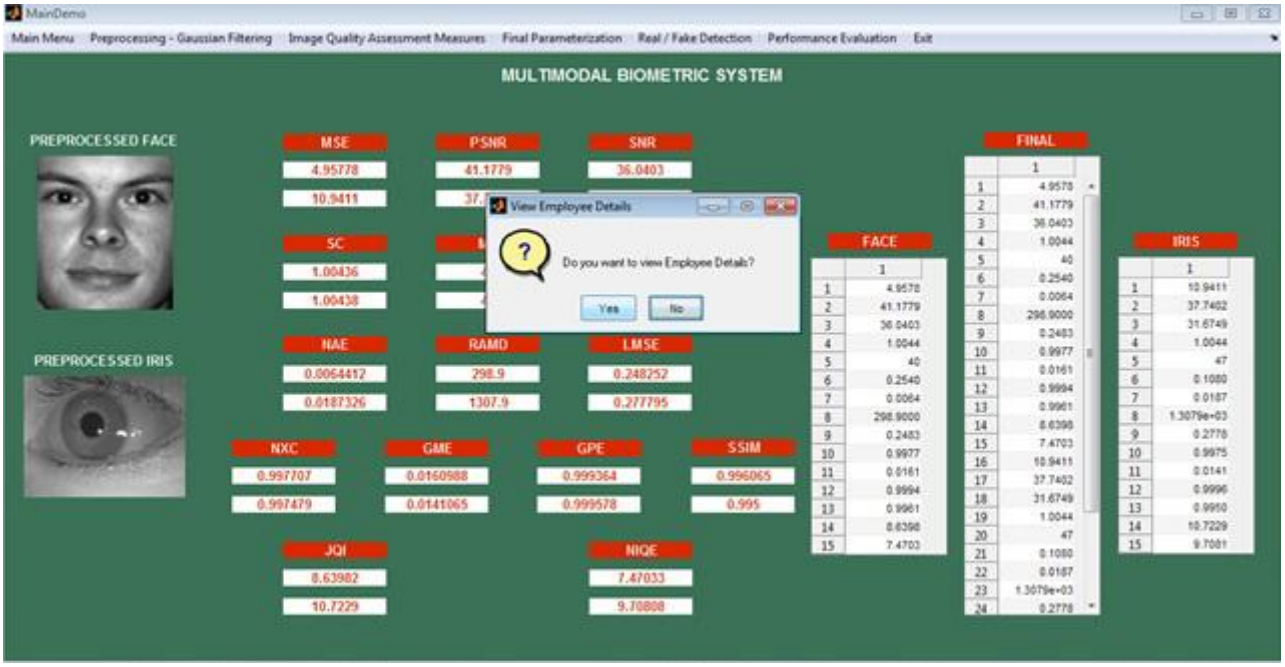

Figure 6: Message for whether employ details must be revealed or not

V. CONCLUSION AND FUTURE WORK

Though the uni-model biometric systems have many advantages, it has to face with variety problems. Hence a multi model biometrics can be used as a better solution. The multimodal biometrics is frontier to the unimodal biometrics as

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

it overcomes the problems related with unimodal biometrics like noisy data, interclass similarities, intra class variation, non universality and spoofing. We can conclude that overall security of system is enhanced through multimodal biometric.Main achievements of proposed system are enrolment and extraction time is reduced, database as well as employee credentials are encrypted, provision for add, delete and modify employee access. Thus new system addresses the spoofing attack threat and enhances the overall security.

REFERENCES

[1]Y. Kim, J. Na, S. Yoon, and J. Y , Masked fake face detection using radiance measurements in proc. NCBI , 2009 Apr;26(4):760-6
[2]Z. Zhang, D. Yi, Z. Lei, S. Z. Li. "Face Liveness Detection by Learning Multispectral Reflectance Distributions". IEEE Int. Conf. on Automatic Face and Gesture Recognition and Workshops, pp. 436-441, 2011.
[3]N. Kose and J.-L. Dugelay. Countermeasure for the protection of face recognition systems against mask attacks. In IEEE International Conference on Automatic Face and Gesture Recognition, April 2013.
[4]N. Kose and J.-L. Dugelay, On the vulnerability of face recognition systems to spoofing mask attacks, in Proc. IEEE ICASSP, May 2013, pp. 2357 2361. 5
[5]Kose, N. ; Dugelay, J.-L. , Shape and Texture Based Countermeasure to Protect FaceRecognition Systems against Mask Attacks. .In Computer Vision and Pattern Recognition Workshops (CVPRW) , 2013 , Page(s): 111 116
[6]Kose, N., Reflectance analysis based countermeasure technique to detect face mask attacks , in Digital Signal Processing (DSP), 2013 18th International Conference on, July 2013.
[7]Z. Zhiwei et al., "A face antispoofing database with diverse attacks," in Proceedings of the 5th IAPR International Conference on Biometrics (ICB'12), New Delhi, India, 2012.
[8]F. Tsalakanidou, C. Dimitriadis, and S. Malassiotis. A secure and privacy friendly 2D+3D face authentication system robust under pose and illumation variation . In International Workshop on Image Analysis for Multimedia
Interactive Services, page 40, June 2007.
[9]N. Kose and J.-L. Dugelay. Countermeasure for the protection of face recognition systems against mask attacks . In IEEE International Conference on Automatic Face and Gesture Recognition, April 2013.
[10]K. Kollreider, H. Fronthaler and J. Bigun, "Evaluating Liveness by Face Images and the Structure Tensor," Proc. Fourth IEEE Workshop Automatic Identification Advanced Technologies (AutoID ',05), pp. 75-80, 2005.
[11]G. Pan, L. Sun, Z. Wu, and S. Lao, "Eyeblink-based anti-spoofing in face recognition from a generic we-bcamera," IEEE 11th International Conference on Computer Vision (2007), pp. 1-8, 2007.
[12]J. Yan, Z. Zhang, Z. Lei, D. Yi, and S. Z. Li, Face liveness detection by exploring multiple scenic clues, in Proc. 12th ICARCV, Dec. 2012, pp. 188 193.