ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 13, April 2016

FAKE BIOMETRIC DETECTION USING IMAGE QUALITY ASSESSMENT

R. Sivaranjani[1] , K. Stella[2], V.Karthikeyan[3].

[1]*PG student, Department of ECE, Vivekanandha College of Engineering for Women*
[2]*PG student, Department of ECE, Vivekanandha College of Engineering for Women*
[3]*AP/ECE, Department of ECE, Vivekanandha College of Engineering for Women*

ABSTRACT: ***In the recent era where technology plays a prominent role, persons can be identified (for security reasons) based on their behavioural and physiological characteristics (for example fingerprint, face, iris, key-stroke, signature, voice, etc.) through a computer system called the biometric system. Biometric system plays an important role in authentication but these systems are vulnerable to several attacks. Spoofing and anti-spoofing has become a prevalent topic in the biometrics community. This paper introduces the attacks on face biometric system and by using Image Quality Assessment for Liveness Detection.***

Keywords : liveness detection, biometric, attacks, authentication.

I INTRODUCTION

Fake biometrics means by using the real images of human identification characteristics create the fake identities like fingerprint, iris on printed paper. Fake user first capture the original identities of the genuine user and then they make the fake sample for authentication but biometric system have more method to detect the fake users and that's why the biometric system is more secure, Because each person have their unique characteristics identification. Biometrics system is more secure than other security methods like password, PIN, or card and key. A Biometrics system measures the human characteristics so users do not need to remember passwords or PINs which can be forgotten or to carry cards or keys which can be stolen.Multi biometric system means a biometric system is used more than one biometric system for one multi-biometric system. A multi biometric system is use the multiple source of information for recognition of person authentication. Multi biometric system is more secure than single biometric system. In this paper Base Image quality assessment for liveness detection technique is used for find out the fake biometrics. The most acceptable biometrics is Face recognition, because it is one of the most universal methods of identification that humans use in their visual interactions and acquisition of faces. The face recognition systems make different between the background and the face. It is most important when the system has to identify a face within a throng. The system then makes use of a person's facial features – its valleys and peaks and landmarks and treats these as nodes that can be compared and measured against those which are stored in the system's database. There are approximately 80 nodes comprising the face print that makes use of the system and this Includes the eye socket depth, jaw line length, distance between the eyes, cheekbone shape, and the width of the nose. It is very challenging to develop this recognition technique which can accept the effects of facial expressions, age, slight variations in the imaging environment.

II IMAGE QUALITY ASSESSMENT FOR LIVENESS DETECTION

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." Image quality is a characteristic of an image that measures the perceived image degradation (typically, compared to an ideal or perfect image). Imaging systems may introduce some amounts of distortion or noises in the signal, so the quality assessment is an important problem.

There are several techniques and metrics that can be measured objectively and automatically evaluated by a computer program. Therefore, they

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 13, April 2016

can be classified as full-reference (FR) methods and no-reference (NR) methods. In FR image quality assessment methods, the quality of a test image is evaluated by comparing it with a reference image that is assumed to have perfect quality. NR metrics try to assess the quality of an image without any reference to the original one. For example, comparing an original image to the output of JPEG compression of that image is full-reference – it uses the original as reference.

Liveness detection methods are usually classified into one of the two groups (fig 1)

1. Hardware based techniques
2. Software based techniques

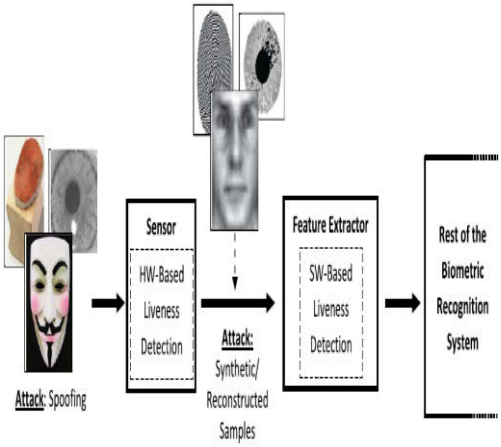

Fig:1 Liveness detection method

Hardware Based Techniques

It adds some specific device to the sensor in order to detect particular properties of a living trait (e.g., fingerprint sweat, blood pressure, or specific reflection properties of the eye).

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).

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. Furthermore, as they operate directly on the acquired sample (and not on the biometric trait itself), software-based techniques may be embedded in the feature extractor module which makes them potentially capable of detecting other types of illegal break-in attempts not necessarily classified as spoofing attacks. For instance, software-based methods can protect the system against the injection of reconstructed or synthetic samples into the communication channel between the sensor and the feature extractor.

III METHODOLOGY

FACE RECOGNITION

From a digital image or a video frame from a video source a person can be identified through the face recognition system. This can be done by comparing selected facial features from the image and a facial database. For this purpose PCA is used. This algorithm identifies facial features by extracting landmarks, or features, from an image of the subject's face. These features are then used to search for other images with matching features.

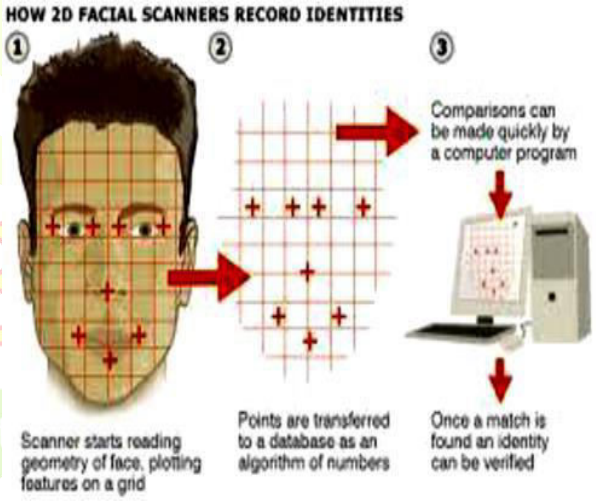

Fig:2 Face recognition

The issues of the design and implementation of the Face Recognition System (FRS) can be subdivided into two main parts. The first part is image processing and the second part is recognition techniques. The image processing part consists of Face image acquisition techniques and the second part consists of the artificial intelligence which is composed by PCA and Back Propagation Neural Network. Face image acquired in the first step by

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 13, April 2016

web cam, digital camera or using scanner is fed as an input to PCA, which converts the input image to low dimensional image and calculates its Euclidian distance. This Euclidian distance is then fed as an input to Back-propagation Neural Network.

CANNY EDGE DETECTION

Canny edge detection provides relatively simple but precise methodology for edge detection problem, with the more demanding requirements on the accuracy and robustness on the detection, the traditional algorithm can no longer handle the challenging edge detection task. The Process of Canny edge detection algorithm can be broken down to five different steps:

1. Apply Gaussian filter to smooth the image in order to remove the noise.
2. Find the intensity gradients of the image
3. Apply non-maximum suppression to get rid of spurious response to edge detection
4. Apply double threshold to determine potential edges
5. Track edge by hysteresis: Finalize the detection of edges by suppressing all the other edges that are weak and not connected to strong edges.

Gaussian Filtering

Edge detection results are easily affected by image noise, it is essential to filter out the noise to prevent false detection caused by noise. To smooth the image, a Gaussian filter is applied to convolve with the image. This step will slightly smooth the image to reduce the effects of obvious noise on the edge detector. This will increase the possibility to miss weak edges, and the appearance of isolated edges in the result. The equation for a Gaussian filter kernel with the size of 2k+1*2k+1 is shown as follows:

H_{ij}=\frac{1}{2\pi\sigma^2}*\exp(-\frac{(i-k-1)^2+(j-k-1)^2}{2\sigma^2})

Gradient Magnitude and Direction Calculation

For the gradient amplitude calculation, the canny edge detection algorithm uses center in a small 3*3 neighborhoods window to calculate the finite difference mean value to represent the gradient amplitude. This method is sensitive to noise and can easily detect fake edges and lose real edges. The equations are demonstrated as following:

$G_x(x,y)$ = [I(i,j+1)-I(i,j-1)+I(i-1,j+1)-I(i-1,j-1)+I(i+1,j+1)-I(i+1,j-1)]/2

$G_y(x,y)$ = [I(i+1,j)-I(i-1,j)+I(i+1,j-1)-I(i-1,j-1)+I(i+1,j+1)-I(i+1,j-1)]/2

Non-maximum Suppression

Non-Maximum suppression is applied to "thin" the edge. After applying gradient calculation, the edge extracted from the gradient value is still quite blurred. There should only be one accurate response to the edge. Thus non-maximum suppression can help to suppress all the gradient values to 0 except the local maximal, which indicates location with the sharpest change of intensity value

Determining the Dual-threshold Value

There will be two fixed global threshold values to filter out the false edges. However, as the image gets complex, different local areas will need very different threshold values to accurately find the real edges. In addition, the global threshold values are determined manually through experiments in the traditional method, which leads to complexity of calculation when large number of different images needs to be dealt with.

$$P_i=n_i/n$$

Where n is the total number of the pixel points in the image. The mean value of the gray level distribution probability is defined as:

$$u_T = \sum_{i=0}^{L-1} ip_i/w_0$$

$$w_0 = \sum_{i=0}^{L-1} p_i$$

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 13, April 2016

$$u_1 = \sum_{i=T+1}^{L-1} ip_i / w_1$$

$$w_1 = 1 - w_o$$

Edge Tracking By Hysteresis

Strong edge pixels should certainly be involved in the final edge image, as they are extracted from the true edges in the image. However, there will be some debate on the weak image pixels, as these pixels can either be extracted from the true edge, or the noise/color variations. To achieve an accurate result, the weak edges caused from the latter reasons should be removed. The criteria to determine which case the weak edge belongs to is that, usually the weak edge pixel caused from true edges will be connected to the strong edge pixel. To track the edge connection, Binary Large Object-analysis is applied by looking at a weak edge pixel and its 8-connected neighbourhood pixels. As long as there is one strong edge pixel is involved in the BLOB, that weak edge point can be identified as one that should be preserved.

FEATURE EXTRACTION

Feature extraction involves reducing the amount of resources required to describe a large set of data. When performing analysis of complex data one of the major problems stems from the number of variables involved. Analysis with a large number of variables generally requires a large amount of memory. Feature extraction is a general term for methods of constructing combinations of the variables to get around these problems while still describing the data with sufficient accuracy. Feature Extraction is performed by using PCA algorithm.

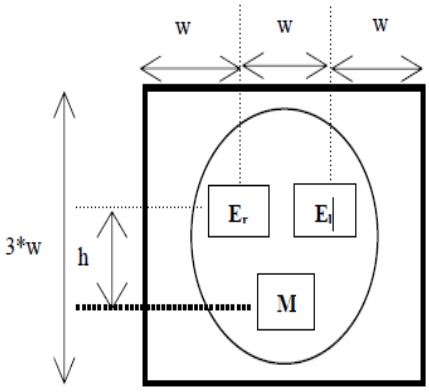

Fig:3 A Frontal Face view

A general view of a frontal face image containing a mouth and two eyes is shown in Fig.3 E_l and E_r represent left and right eyes respectively, while M represents the mouth feature. The distance between the two eyes is w, and the distance from the mouth to the eyes is h. In frontal face images, structural relationships such as the Euclidean distance between the mouth, and the left and right eye, the angle between the eyes and the mouth, provide useful information about the appearance of a face. These structural relationships of the facial features are generally useful to constrain the facial feature detection process. A search area represented by the square of size is also an important consideration in order to search for faces based on the detected eye feature positions in the image.

PRINCIPAL COMPONENT ANALYSIS (PCA)

Principal component analysis (PCA) is a statistical procedure that uses an orthogonal transformation. The PCA approach is used to reduce the dimension of the data by means of data compression basics and reveals the most effective low dimensional structure of facial patterns. This reduction in dimensions removes information that is not useful and precisely decomposes the face structure which involves transformation of number of possible correlated variables into a smaller number of orthogonal (uncorrelated) components known as Principal Components. Each face image may be represented as a weighted sum (feature vector) of the eigen faces, which are stored in a 1D array. The test image can be constructed using these weighted sums of eigen faces. When a test image is given, the weights are computed by

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 13, April 2016

projecting the image upon eigen face vectors. The distance between the weighted vectors of the test image and that of the database images are then compared. Thus one can reconstruct original image with the help of eigen faces so that it matches the desired image.

Algorithm for PCA

Let the training set of images be Γ_1, Γ_2…… Γ_M the average face of the set is defined by

$$\Psi=1/M\sum_{i=1}^{M}\Gamma i$$

Each face differs from the average by vector.

$$\Phi_{i=}\Gamma i-\Psi$$

Where i=1…….M. The co- variance matrix is formed by C = $A.A^T$ Where the matrix A is given by A = $[\Phi_1,\Phi_2,\ldots..\Phi_M]$ This set of large vectors is then subject to principal component analysis, which seeks a set of *M* orthonormal vectors. To obtain a weight vector W of contributions of individual eigen-faces to a facial image, the face image is transformed into its eigen-face components projected onto the face space by a simple operation.

$$W_k=u^t_k\Phi$$

For k=1... *M'*, where *M'* £ *M* is the number of eigen-faces used for the recognition. The weights form vector W = $[w_1,w_2,\ldots.w_m]$ that describes the contribution of each Eigen-face in representing the face image, treating the eigen-faces as a basis set for face images. The simplest method for determining which face provides the best description of an unknown input facial image is to find the image *k* that minimizes the Euclidean distance ϵ_k.

$$\epsilon k=\|(\Omega-\Omega_k)\|^2$$

Where W_k is a weight vector describing the k^{th} face from the training set. It is this Euclidean distance that is given as an input to the neural networks.

IV EXPERIMENTAL RESULTS

The evaluation experimental protocol has been designed with a two-fold objective:

- First, the multi-biometric dimension of the protection method is evaluated. For this purpose three biometric modalities have been considered in the experiments
- Second, the multi-attack dimension of the protection method is evaluated. It does not detect the spoofing attacks alone but also the fraudulent access of the synthetic samples or reconstructed samples.

Database

Here, we used the ORL database. That contains ten different images of each of 40 distinct subjects. For some subjects, the images were taken at different times, varying the lighting, facial expressions (open / closed eyes, smiling / not smiling) and facial details (glasses / no glasses). All the images were taken against a dark homogeneous background with the subjects in an upright, frontal position. A random subset with S = (1,2,…,10) images per individual was taken with labels to form the training set, and the rest of the database was considered to be the testing set. Each image in the training set contained 92 by 112 pixel of size.

Testing face image

A testing face image is captured and stored in computer system. The testing image is read from the system using 'imread' function in MATLAB image processing toolbox. Then the testing image is resized to 250 * 250 for further processing.

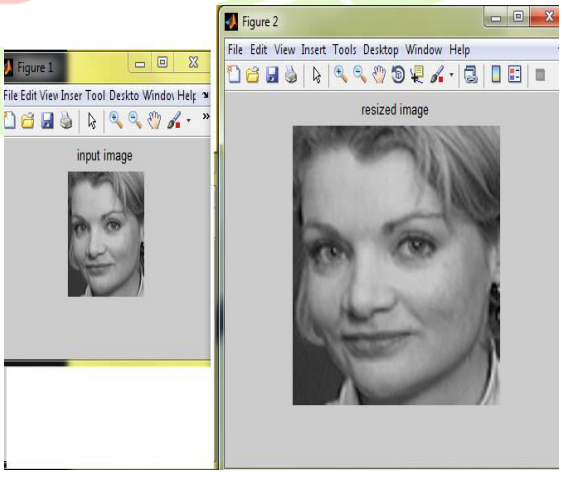

Fig:4 Input image for recognition process and Resized image

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 13, April 2016

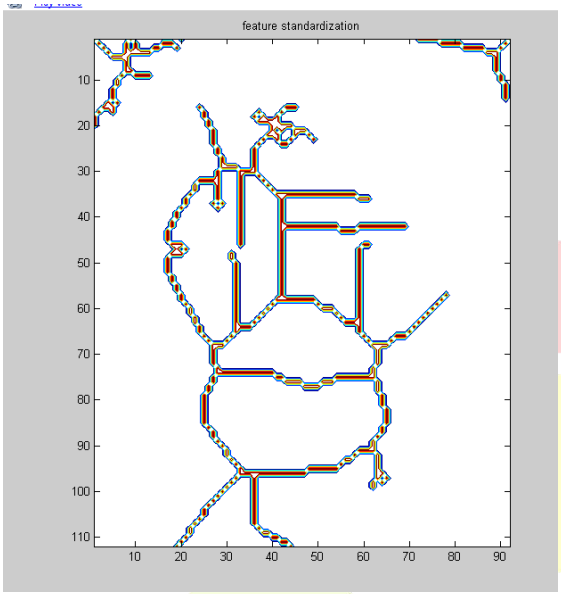

Fig:5 **Facial Feature Extraction**

Face Recognition

In face recognition, the classification is done by using classifier PCA. Then the testing image is compared with original images which are stored in database. If the testing image is located in the database, then "AUTHENTICATION SUCCESSFULL" is displayed on figure window (see.Fig.6).

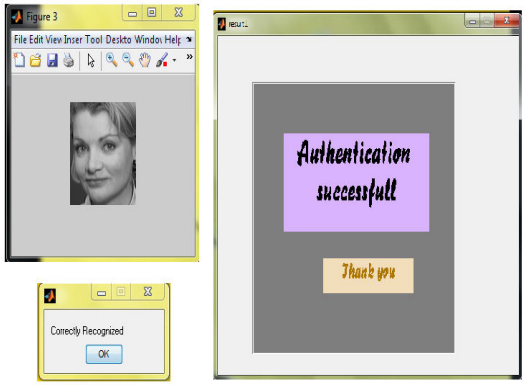

Fig:6 Simulation Result1

Otherwise, it displayed "INCORRECTLY RECOGNIZED" and return back to the starting process of the face recognition.

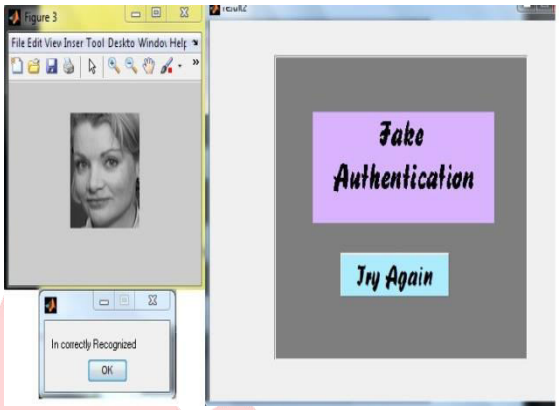

Fig:7 Simulation Result 2

V CONCLUSION

Biometric systems provide a greater degree of security and user convenience than the traditional authentication methods. Better recognition compared to existing method. Better Security, the multi-biometric system increases the security level. The attractiveness of using PCA is reported 96.2% correct recognition on ORL database of 400 images of 40 individuals. The classification time is less than 0.5 second. However, when the number of persons increases, the computing expense will become more demanding. In general, neural snetwork approaches encounter problems when the number of classes (i.e., individuals) increases. Moreover, they are not suitable for a single model image recognition test because multiple model images per person are necessary in order for training the systems to "optimal" parameter setting.

VI REFERENCES

[1] Javier Galbally, Sébastien Marcel, Member, IEEE, and Julian Fierrez (Feb 2014). 'Image Quality Assessment for Fake Biometric Detection: Application to Iris, Fingerprint, and Face Recognition', IEEE.Vol. 23, no. 2.

[2] Tiago de Freitas Pereira, Jukka Komulainen, André Anjos, José Mario De Martino. (2013). 'Face liveness detection using dynamic texture'. IEEE.Vol.43.

[3] Hewage C.T., Martini M.G., and Villarini.B (March 2012). 'Image quality assessment based on edge preservation,' Signal Process. Image Commun. Vol. 27, no. 8, pp. 875–882.

[4] Pankaj Bhandari, Pankaj K Gupta.(April 2012). 'Face recognition based on Edge detection'. IJIRCE. Vol 3.Issue 3.

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)
International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)
Vol. 2, Special Issue 13, April 2016

[5] .Biometrics Technology for Human Recognition , Anil K. Jain, Michigan State University http://biometrics.cse.msu.edu ,October 15, 2012.

[6] Z. Akhtar, G. Fumera, G. L. Marcialis, and F. Roli, "Evaluation of serial and parallel multibiometric systems under spoofing attacks," in Proc. IEEE 5th Int. Conf. BTAS, Sep. 2012, pp. 283–288.

[7] H. R. Sheikh and A. C. Bovik, "Image information and visual quality," IEEE Trans. Image Process., vol. 15, no. 2, pp. 430–444, Feb. 2006