Middle-East Journal of Scientific Research 22 (6): 937-947, 2014
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2014.22.06.21973

An Efficient Biometric Multimodal Face, Iris and Finger Fake Detection using an Adaptive Neuro Fuzzy Inference System (ANFIS)

[1]S. Wilson and [2]A. Lenin Fred

[1]Department of Computer Science and Engineering,
Manonmaniam Sundaranar University, Tirunelveli, India
[2]Mar Ephraem college of Engineering and Technology, Elavuvillai,
Marthamdam,Tamilnadu, India

Abstract: The face, iris and finger print are among the most promising biometric authentication that can precisely identify and analysis a person as their unique textures can be quickly extracted during the recognition process. This biometric detection and authentication often deals with non-ideal scenarios such as blurred images, off-angles, reflections, expression changes. These precincts imposed by uni modal biometrics can be pound by incorporating multimodal biometrics. for this reason, in this paper, we present a new Effective fake detection method that can be used in multiple biometric systems to detect different types of fake access attempts. An important feature and objective of the proposed system is to enhance the image quality and very low degree of complexity for security of biometric recognition frameworks. For the preprocessing we used score level approach Median filter with canny edge detection and Hough transform with Anisotropic Gaussian Filter. For the Feature Extraction we have used Gabor filter. The classification is done by ANFIS which is an efficient classification. The performance of the proposed approach is validated and is efficient.

Key words: Median filter · Canny edge detection · Gabor filters · Hough transforms · ANFIS

INTRODUCTION

Biometrics technology is used to security problems, recognizes persons in a fast and reliable performance through the use of unique biological characteristics. The human different characteristic used as a biometric characteristic is universality, distinctiveness, Permanence, collectability. performance acceptability and circumvention. Biometrics has two types that us unimodal and multimodal. Many unimodal biometrics systems endure from inability to tolerate deformed data due to noise, deformed data from the sensor device, distorted signal from environmental noise and variability of an individual's physical appearance and pattern over time. Multimodal biometric is able to solve several of these limitations by combining information from multiple biometric sources. The storage requirements, processing time and computational demands of a multimodal biometric system are good compare with unimodel system. Biometrics can use behavioral characteristics or physical characteristics.The fake attack reduces reliability and security of biometric system. Because fake identities at all times have some different features than original it always contains different color and luminance levels, quantity of information and quantity of sharpness [1].

Image quality assessment for liveness detection technique is used to detect the fake biometrics. A biometric system should have the uniqueness, stability, collectability, performance, acceptability and forge resistance. Image quality measurements it is easy to find out real and fake users. Image quality assessment for liveness detection technique is used for find out the fake biometrics [2].

The multi-biometric systems can remove some of the drawbacks of the unibiometric systems by grouping the multiple sources of information [3]. Biometric Detection and recognition in face, iris and fingerprint may solve this problem. It's nontransferable. The system is compare

Corresponding Author: S. Wilson, Department of Computer Science and Engineering,
Manonmaniam Sundaranar University, Tirunelveli, India.

scans to records stored in a central or local database. The Predictable quality differences between real and fake samples may contain color and luminance levels, general artifacts, quantity of information and quantity of sharpness, found in both type of images, structural distortions or natural appearance Among the different threats analyzed, the direct or spoofing attacks have forced the biometric area to study the vulnerabilities against this type of fraudulent actions in modalities such as the iris [3], the fingerprint [4], the face [5], the signature [6], or even the gait [7] and multimodal approaches [8]. In these attacks, the intruder uses some type of unnaturally formed artifact like as gummy finger, printed iris image, face mask or tries to copy the behavior of the genuine user to fraudulently access the biometric system.

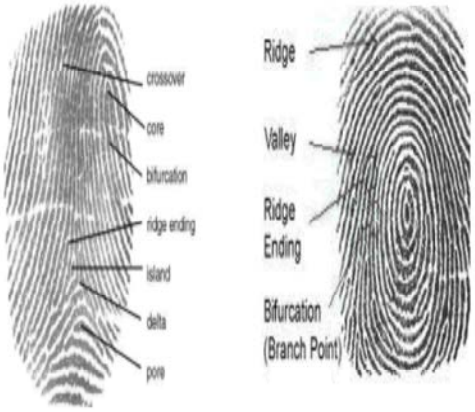

Fig. 1: Basic Finger print Minutiae

Face Detection: The main objective of face detection is to find whether there are any faces in the image or not. If the face is present, then it returns the location of the image and extent of the each face. Face detection is the first stage of an automatic face recognition system, since a face has to be located in the input image before it is recognized. There are a lot of factors due to which the face detection is a challenging task [9].

Face detection is a two-step procedure first the whole image is examined to find regions that are identified as face. After the rough position and size of a face are estimated, a localization procedure follows which provides a more accurate estimation of the exact position and scale of the face. The face detection systems make different between the background and the face. There are approximately 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. Face detection has direct relevance with the face recognition because before recognition the image must be analyzed and the location of the face must be detected [10-30].

The face detection process consists of four steps. First step is Input image passed to the system as input.The image may vary in format, size and resolution, second step is Pre-processing, the image is pre-processed to remove the background noise. This is also called image normalization. Third step is Classifier it takes decision whether the image belong to the face or non-face class. Fourth step is Result Output this indicates the location of the face in the original image input.

Finger Print Detection: Every fingerprint of each person is considered to be unique. Fingerprint detection and recognition is the most accepted biometric recognition method. Fingerprints have been used from long time for identifying persons. A good quality fingerprint contains 30 - 80 minutiae points. Fingerprints consist of a regular texture pattern composed of ridges and valleys. These ridges are characterized by several landmark points, known as minutiae, which are mostly in the form of ridge endings and ridge bifurcations.

The minutiae points is be unique to each finger, it is the collection of minutiae points in a fingerprint that is primarily employed for matching two fingerprints. There exists some gap between the ridges, called valleys [15, 19]. In a fingerprint, the dark lines of the image are called the ridges and the white area between the ridges is called valleys.

Singularity points detection is the most challenging and important process in biometrics Fingerprint Detection. Singular points are used for Fingerprint classification, Fingerprint matching and Fingerprint alignment. The various singularity points [28] present are called the core' and delta'. Cores are the position that occurs when there is a circular region in the Fingerprint. Delta is present where three different directional lines are present [31-40].

Iris Image Detection: Iris detection and recognition is a computerized method of biometric identification which uses mathematical Model techniques on images of the irises of an individual's eyes, the iris is the colored ring around the pupil of every human being and like a snowflake no two are the same [6]. Each one is unique. An identification system consists of four phases that are image scanner, preprocessing, feature extraction and identification [2].An attack on the iris is not so easy but how to attack on the system To create a fake iris, first Original images are capture for a better quality, then second involved Pre-processing phase that is Reduction

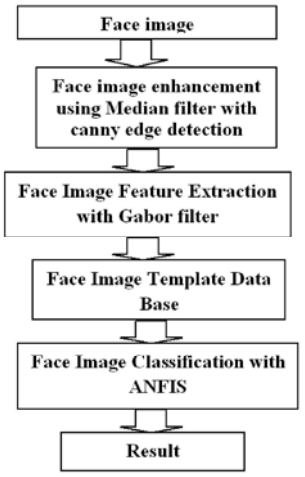

Fig. 2: Fake biometric methodology for Face Detection

Fig. 3: Fake biometric methodology for Iris Detection

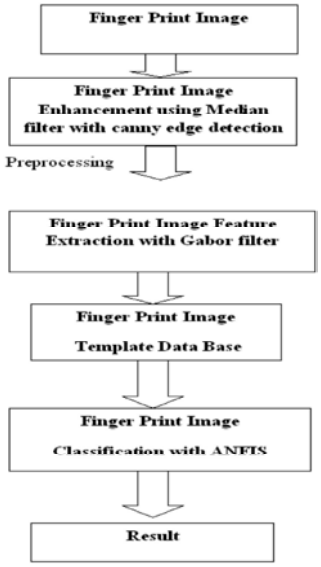

Fig. 4: Fake biometric methodology for Finger Print Detection

of the size of the image from the original size of the images 256 by 256 pixels size is reduced to 128 by 128 pixels. Pre processing is process of removing the low frequency background noise and normalizing the intensity of individual pixels in the image.

Preprocessing: This paper investigates about the preprocessing, feature extraction phase and classification phase of the bimodal biometric system for face detection, fingerprint detection and iris detection. This paper ANFIS classifier is used. Classifier must have the ability to correctly identify and retain the minute variations observed in the applied pattern. It is a problem solving mechanism that has received wide acceptance. ANFIS is a fuzzy inference system implemented in a framework of adaptive network.

Pre-Processing: The idea of the pre-processing is to reduce or eliminate some of the image variations for the illumination of the image. After the image is captured it may be unclear or imprecise.

Face Detection Preprocessing: In face detection, Median filter and canny edge detection is used for preprocessing, Median filtering is a nonlinear method used to remove noise from images and very effective at removing noise while preserving edges also salt and pepper type noise. The median filter works by moving through the image pixel by pixel, replacing each value with the median value of neighboring pixels. The pattern of neighbors is called the window which slides, pixel by pixel over the entire image pixel, over the entire image. The median is calculated by first sorting all the pixel values from the window into numerical order and then replacing the pixel being considered with the middle (median) pixel value then use Canny Edge Detection Algorithm. The Canny Edge Detection Algorithm processed following steps

- Smoothing: Blurring of the image to remove noise. To decrease the influence of noise and smooth the image using Gaussian Smooth Mask.
- Finding gradients: The edges should be marked where the gradients of the image has

Large Magnitudes: Computing derivatives of the image using vertical and horizontal Sobel Operator, so to get the derivatives along both x and y directions, based on which we can get the final gradient magnitude and the norm direction of the edge. Hence two images in this step, one derivative magnitude image and one image recording the gradient directions of corresponding pixels.

$$|G| = \text{sqrt}(G\_x\text{^}2 + G\_y\text{^}2) \quad (1)$$

$$\text{Theta} = \text{atan}(G\_y / G\_x) \quad (2)$$

$$KGX = \begin{pmatrix} -1 & 0 & 1 \\ -2 & 0 & 2 \\ -1 & 0 & 1 \end{pmatrix} \quad (3)$$

$$KGY = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 0 & 0 \\ -1 & -2 & -1 \end{pmatrix} \quad (4)$$

$$|G| = \sqrt{G^2x + G^2y} \quad (5)$$

$$|G| = |Gx| + |Gy| \quad (6)$$

$$\square = \arctan\left(\frac{|Gy|}{|Gx|}\right) \quad (7)$$

Non - Maximum Suppression: Only local maxima marked as edges. Round the gradient direction to nearest 45°, corresponding to the use of an 8-connected neighborhood. Compare the edge strength of the current pixel with the edge strength of the pixel in the positive and negative gradient direction. I.e. if the gradient direction is north (theta = 90°), compare with the pixels to the north and south. If the edge trength of the current pixel is largest; preserve the value of the edge strength.

Double Thresholding: Possible edges are determined by thresholding. The edge-pixels remain after the non-maximum suppression step is marked with their strength pixel-by-pixel. Many of these will probably be true edges in the image, but some may be caused by noise or color variations for instance due to rough surfaces. This method to differentiate between these thresholds, so only edges stronger that a certain value preserved. The Canny edge detection algorithm uses double thresholding. Edge pixels stronger than the high threshold are marked as strong; edge pixels weaker than the low threshold are suppressed and edge pixels between the two thresholds are marked as weak.

Edge Tracking by Hysteresis: Final edges are determined by suppressing all edges that are not connected to a strong edge. Strong edges are interpreted and directly be included in the final edge image. Weak edges are included if and only if they are connected to strong edges. The noise and other small variations are unlikely to result in a strong edge. Thus strong edges only are due to true edges in the original image. The weak edges can either be due to true edges or noise/color variations. The latter type will probably be distributed independently of edges on the entire image and thus only a small amount will be located adjacent to strong edges. Weak edges due to true edges are much more likely to be connected directly to strong edges.

Fingerprint Detection Preprocessing: In fingerprint detection, the fingerprint image is to increase the clarity of the ridge structure then minutiae points can be easily extracted. So An Anisotropic Gaussian Filtering is used for filtering in a particular direction and remove noise from a biometric image. Because a fingerprint has ridges or lines oriented in different directions. This filter is directional dependent also proceed in all directions. It has different variances in X direction and Y direction with the orientation obtained for the finger print ridges. The Anisotropic Gaussian filter is rotated with particular orientation. This filter is applied to a ridge line the kernel appears as an ellipse. Therefore smoothing is performed along ridges but not across a ridge line. It cannot be applied directly to an entire finger print image, because a finger print pattern will have ridge lines oriented in different pattern. For this purpose the whole image is divided into blocks. Each block will have ridge lines with some particular orientation. Then Hough transform can be applied to a block which gives orientation and with that orientation the filter is rotated and in this way the noise can be removed along the ridge lines.

To construct general anisotropic Gaussian filters, consider arbitrary positive definite covariance matrices Σ. The form of the Gaussian function remains the same as in the left-hand side. Such Gaussians in n dimensions have $\frac{n(n+1)}{2}$ degrees of freedom. N is variance parameters and remaining parameters can be interpreted as rotation angles for the filtering directions. An anisotropic Gaussian filtering of an image is processing following procedure:

The first step, Calculate the Triangular Factorization of Cholesky Type of the covariance matrix Σ. A decomposition $\Sigma = V\,DV$, where D is a diagonal matrix and V is upper-triangular with unit diagonal. The second step, Transform the image linearly using the matrix V^{-1}. Because of the special form that V has, this operation is a shear. Third step, to apply axis-aligned Gaussian filtering with covariance matrix D.

The Final Step: Shear the image back, transforms it linearly using the matrix V.

An oriented anisotropic Gaussian filter in two dimensions is:

$$g_{\square}(\upsilon,\nu;\sigma_{\upsilon},\sigma_{\nu},\square) = \frac{1}{\sqrt{2\pi\sigma\upsilon}}\exp\{-\frac{1}{2}$$

$$\frac{\upsilon 2}{\sigma 2u}\}^{*}\frac{1}{\sqrt{2\pi\sigma\upsilon}}\exp\{-\frac{1}{2}\frac{\nu 2}{\sigma 2\nu}\} \quad (8)$$

Where * denotes convolution,

$$\begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} cos\theta & sin\theta \\ -sin\theta & cos\theta \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} \quad (9)$$

A suitable computational perspective, the separation in u and υ is UN interesting. The decomposition into a filter in the -direction and a filter along another direction. To separating the anisotropic Gaussian filter into

$$g_{\square}(\upsilon,\nu;\sigma_{\upsilon},\sigma_{\nu},\square) = \frac{1}{\sqrt{2\pi\sigma x}}\exp\{-\frac{1}{2}$$

$$\frac{x2}{\sigma 2x}\}^{*}\frac{1}{\sqrt{2\pi\sigma\varphi}}\exp\{-\frac{1}{2}\frac{t2}{\sigma 2\varphi}\} \quad (10)$$

Representing the Gaussian filter along the -direction, followed by filtering along a line $xcos\varphi + ysin\varphi$the impulse response of equation. From the equation (11)

$$G\square(\upsilon,\nu;\sigma_{\upsilon},\sigma_{\nu},\square)$$

$$= \frac{1}{2\pi\sigma x\sigma\varphi}\,\mathrm{Exp}\{-\frac{1}{2}\left(\frac{(x-y/tan\varphi)2}{\sigma 2x}+\frac{(y/sin\varphi)2}{\sigma 2\varphi}\right)$$

$$g_{o}(\upsilon,\nu;\sigma_{\upsilon},\sigma_{\nu},\square) = \frac{1}{2\pi\sigma u\sigma v}\exp\{-$$

$$\frac{1}{2}\left(\frac{(xcos\theta/ysin\theta)2}{\sigma 2u}+\frac{(-xsin\theta/xcos\theta)2}{\sigma 2v}\right) \quad (12)$$

$$\left(\frac{\chi 2}{\sigma 2x} = \chi 2\,\frac{cos^{2}\theta}{\sigma 2u} + \chi 2\,\frac{sin^{2}\theta}{\sigma 2v}\right) \quad (13)$$

$$\left(\frac{y2}{\sigma 2x tan^{2}\varphi} = \frac{y^{2}}{\sigma 2\varphi sin^{2}\varphi}\right) = y2\,\frac{cos^{2}\theta}{\sigma 2\,\nu} + y2\,\frac{sin^{2}\theta}{\sigma 2\upsilon} \quad (14)$$

$$\frac{2xy}{\sigma 2x tan\varphi} = 2xy_{cos\theta sin\theta}\left(\frac{1}{\sigma 2\upsilon}+\frac{1}{\sigma 2\nu}\right) \quad (15)$$

Solving the equations yields the decomposition of the anisotropic Gaussian into a Gaussian along the -x axis, with standard deviation

$$\sigma x = \frac{\sigma\upsilon\,\sigma\nu}{\sqrt{\sigma 2\nu cos^{2}\theta+\sigma 2\upsilon sin^{2}\theta}} \quad (16)$$

and a Gaussian along the line t: y-xtan □ = 0, with standard deviation

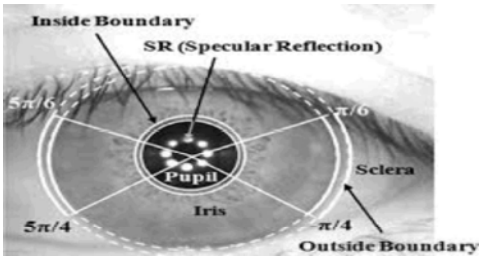

Fig. 5: Basic Iris Image

Fig. 6: Original image

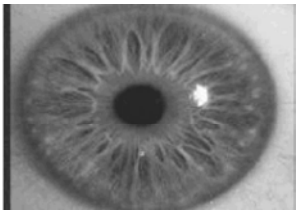

Fig. 7: Grayscale image

$$\sigma\varphi = \frac{1}{sin\varphi}\sqrt{\sigma 2\nu cos^{2}\theta+\sigma 2\upsilon sin^{2}\theta} \quad (17)$$

And intercept

$$tan\varphi = \frac{\sigma 2\nu cos^{2}\theta+\sigma 2\upsilon sin^{2}\theta}{(\sigma 2\upsilon-\sigma 2\nu)cos\theta sin\theta} \quad (18)$$

Iris Image Detection Preprocessing: In iris detection pre processing, the noise Reduction use to the Median filter, then Detection of edges used for detection of edges by canny edge detection algorithm. In Preprocessing done following steps Iris Localization, iris Normalization and iris Enhancement. An eye image contains not only the iris region but also some unuseful parts, such as the pupil, eyelids, sclera and so on. Segmentation will be done to localize and extract the iris region from the eye image.

Iris localization is the detection of the iris area between pupil and sclera. So need to detect the upper and lower boundaries of the iris and determine its inner and outer circles. consists of localizing both inner and outer boundaries of the iris and those two circles are detected using polar coordinate system separately because they are not co-centric so to Find Inner and outer boundaries of Iris, inner radius and center of pupil.

In iris Normalization the two images of the iris are definitely different because of the size of the image and pupil and also orientation of the iris. So the image is normalized by converting it into doubly dimensionless polar. Daugman's rubber sheet model is used to normalize the iris model which makes the computation Very simple.

The rubber sheet is a linear model that signs to each pixel of the iris, despite its size and pupil dilation, a pair of real coordinates (r, θ), where r is unit interval [0, 1] and θ

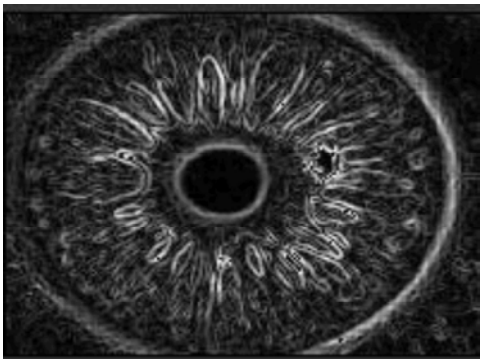

Fig. 8: Edge detected image

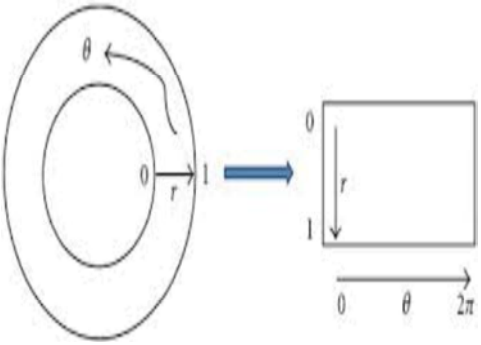

Fig. 9: Daugman's rubber sheet model

is an angle in range [0, 2π]. The iris image remapping is I(x, y) from raw Cartesian coordinates (x, y) to the dimensionless non concentric polar coordinate system (r, θ) represented

$$x_{p=(} x_{p+} x_{p)/2} \quad (19)$$

$$y_{p=(} y_{p+} y_{p)/2} \quad (20)$$

$$I(x(r, \theta),y(r, \theta)) > I(r, \theta) \quad (21)$$

Where x(r, θ) and y(r, θ) are linear combinations of both the set of pupil Boundary points (xp(θ), yp (θ)) and the set of limbus boundary points along the outer perimeter of the iris (xs(θ), ys(θ)) bordering the sclera.

$$x(r, \theta) = (1- r)* x_p(\theta)+ r*x, (\theta) \quad (22)$$

$$y(r, \theta) = (1- r)* y_p(\theta)+ r*y, (\theta) \quad (23)$$

I(x, y) is the iris region image, (x, y) are the original Cartesian coordinates, (r, θ) are the corresponding normalized polar coordinates (xp, yp) and (xi, yi) are the

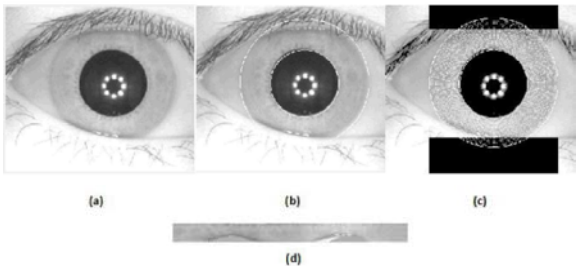

Fig. 10: (a)normal iris image (b) localizes iris image (c) segmented iris image (d) normalized linear iris image

coordinates of the pupil and iris boundaries along the θ direction. In iris Enhancement to extract the iris pattern it is necessary one to enhance the image. The iris enhancement involves in two activities. First, the image has to be sharpened with a sharpening mask. Second, the effect on non-uniform illumination has to be reduced.In this Reduction of noises use to the Median filter, then to Detect edges used by canny edge detection algorithm.

Feature Extraction: The feature extraction phase the input data is transformed into a reduced set of features. In this feature extraction phase used for Go bar filter. Fingerprint detection Feature extraction for extracting the features from the fingerprint image, a fingerprint is made of a series of ridges and furrows on the surface of the finger. To find out the minute points from the fingerprint and then map their relative position on the finger. When the fingerprint is of low quality, it will be difficult to extract the minutiae points. For that only we used different filters and other image enhancement techniques at the pre-processing stage. The output of this Algorithm will be the image template containing the minutiae details. There are two types of minutiae points. Ridge ending and Ridge bifurcation [4]. In [26] an advanced fingerprint feature extraction method is introduced through which minutiae are extracted directly from original gray-level fingerprint images without binarization and thinning. Therefore Gabor filter used to extract features from fingerprint [24].

Gabor Filter: Gabor filter is a band pass filters which are used in image processing for feature extraction and texture analysis. Its frequency and orientation are similar to that of the human visual system and to found appropriate for texture discrimination and representation. Gabor filters are formed by modulating a complex sinusoid by a Gaussian

function. Gabor filters have been used widely in pattern analysis application and it has been proved in extracting more salient features both in the face [24] and fingerprint [25-27] images, which are the two modalities being used in this paper. A set of Gabor filters with different frequencies and orientations was used for extracting salient features from both face and fingerprint images. It is invariant against translation, rotation and variations due to illumination and scale. Gabor filter also presents desirable characteristics of spatial locality and orientation selectivity. During feature extraction the dimension or size of the image does not change. For instance, in this paper the dimension of face, fingerprint and iris, after applying Gabor filter to extract the salient features the dimension still remains the same. Gabor filters at different scales and spatial frequencies.

The Gabor filter based feature extraction is the 2D Gabor filter function is

$$\Psi(x, y) = \frac{f2}{\pi\gamma 2\eta} e^{-\left(\frac{f2}{\gamma 2}x'^2 + \frac{f2}{\eta 2}y'^2\right)} e^{j2\pi fx'}$$

$$X' = x\cos\square + y\sin\square \quad (24)$$

$$Y' = x\sin\square + y\cos\square$$

The equation (24) is spatial domain the Gabor filter is a complex plane wave that is 2D Fourier basis function, multiplied by an origin-centered Gaussian. f is the central frequency of

The filter, $\square$ the rotation angle, γsharpness (bandwidth) along the Gaussian major axis and η sharpness along the perpendicular to the wave. The phase Ratio of the Gaussian is $\frac{\eta}{\gamma}$. This function has the following analytical form in the frequency domain

$$\Psi(u, \upsilon) = e^{-\frac{\pi 2}{f2}\left((\gamma 2u' - f)^2 + \eta 2\upsilon^2\right)}$$

$$u' = u\cos\square + \upsilon\sin\square \quad (25)$$
$$\upsilon = -u\sin\square + \upsilon\cos\square$$

The equation (25) is frequency domain the function is a single real-valued Gaussian centered at f at equation (2). The Gabor filter in (1) and (2) is a simplified version of the general 2D form devised. enforces a set of filters self-similar scaled and rotated versions of each other, regardless of the frequency and orientation $\square$. Gabor feature, are constructed from responses of Gabor filters by using multiple filters on several frequencies fm and orientations $\square$n. Frequency in this case corresponds to scale information and is thus drawn from [10]

$$f_m = k^{-m} f_{max},\ m = \{0\ldots..m-1\}$$

Where f_m is the m^{th} frequency, $f_0 = f_{max}$ is the highest frequency desired and $k > 1$ is the frequency scaling factor. The filter orientations are drawn from [10]

$$\square_n = \frac{n2\pi}{N},\ n=\{0\ldots\ldots N-1\}$$

where N is the total number of orientations and $\square$n is the n^{th} orientation. The parameters f_{max}, k, M, N, γ and η are redundant Scales of are selected from exponential spacing and orientations from linear spacing. The most intuitive parameterization is achieved by defining the function envelope cross point at p = 0:5, i.e. two filter Gaussians cross on the half magnitude. The cross point parameter p is fixed and the adjustable parameters are now the highest frequency f_{max}, number of frequencies m and number of orientations n. The bandwidths γ and η are automatically set using the formula.

Classification: The classification phase the individual is identified based on the traits. The ANFIS used for classification phase. The result can either be accepted or rejected.ANFIS is a fuzzy inference system (FIS) implemented in the framework of an adaptive fuzzy neural network. It combines the explicit knowledge representation of an FIS with the learning power of artificial neural networks. The objective of ANFIS is to integrate the best features of fuzzy systems and neural networks. Using a given input and output data set, ANFIS constructs a FIS whose membership function parameters are adjusted using either a back propagation algorithm alone or in combination with a least squares type of method [34, 35]. This adjustment allows your fuzzy systems to learn from the data they are modeling. ANFIS architecture has five layers of different functions which constitute the system. Layer 1 is the input layer. In this layer the external inputs are transmitted to the next layer. layer 2 is the fuzzification layer. This layer includes the antecedent fuzzy set of fuzzy rules. the Third layer Fuzzy rule layer. This layer receives the input from the first layer. Then comes the layer 4 which is the normalization layer. Last layer is the defuzzyification layer [36], [37-38]. ANFIS consists of if-then rules that couples input and output.

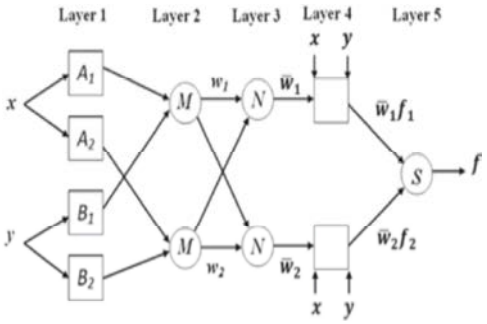

Fig. 11: Basic structure of ANFIS

Also for ANFIS training, ANFIS learning algorithm of neural network is used. To assumed two inputs (x and y) and one output (z). For a first order of Sugeno fuzzy model, a typical rule set with base fuzzy if-then rules can be expressed as

Rule 1: If x is A1 and y is B1 then f1=p1x+q1y+r1

Rule 2: If x is A2 and y is B2 then f2=p2x+q2y+r2

Where p, r and q are linear output parameters. These parameters are calculated based on the information from [37]. problems. Assume that the fuzzy inference system has two inputs x and y and one output z.

In first layer, Ol, i is the output of the i th node of the layer l. Every node i in this layer is an adaptive node with a node function

$O_1,i = \mu_{Ai(x)}$ for i = 1, 2, or

$O_1,i = \mu_{Bi-2}(x)$ for i = 3, 4

x (or y) is the input node i and A_i (or B_{i-2}) is a linguistic label associated with this node

Therefore O_1,i is the membership grade of a fuzzy set (A1,A2,B1,B2)

$$\mu A(\text{◎◎}) = \frac{1}{1+\left|\frac{(X-Ci)}{ai}\right|^{2bi}} \quad (26)$$

ai, bi, ci are the parameter set. Parameters are referred to as premise parameters. In second layer, every node in this layer is a fixed node labeled Product. The output is the product of all the incoming signals. Each node represents the fire strength of the rule, Any other T-norm operator that perform the AND operator can be used

$O_2,i = \mu_i = \mu_{Ai}(\text{◎◎}) \bullet \mu_{Bi}(\text{◎◎})$, i = 1, 2

In third layer, every node in this layer is a fixed node labeled Norm. The it node calculates the ratio of the it runlet's firing strength to the sum of all runlet's firing strengths. Outputs are called normalized firing strengths

$$O_3, i = \omega\square_i = \frac{(\omega i)}{\omega 1+\omega 2}, \; i= 1,2 \quad (27)$$

In fourth layer Every node i in this layer is an adaptive node with a node function:

$$O_{4,1} = \omega\square_i f_i = \mu\square_i (p\,\text{◎◎} + q_i\,\text{◎◎} + r_i)$$

$\omega\square_i$ is the normalized firing strength from layer 3. $\{p_i, q_i, r_i\}$ is the parameter set of this node. These are referred to as consequent parameters In fifth layer, The single node in this layer is a fixed node labeled sum, which computes the overall output as the summation of all incoming signals:

$$\text{output} = O_{5,1} = \Sigma_i \square_i f_i = \frac{\sum i\ \omega i f i}{\sum i\ \omega i}$$

Anfis Learning Algorithm: In the ANFIS structure, it is observed that given the values of premise parameters, the final output can be expressed as a linear combination of the consequent parameters. The output can be

$$f = \frac{\omega 1}{\omega 1+\omega 2} f_1 + \frac{\omega 1}{\omega 1+\omega 2} f_2 \quad (27)$$

$$= \omega\ \square_i f_{1\,+} \omega\ \square_2 f_2 \quad (28)$$

$$= (\omega\square_1\,\text{◎◎})\ p_1 + (\omega\square_1\,\text{◎◎}) q_1 + (\omega\square_1)\ r_1 + (\omega\square_2\,\text{◎◎}) p_2 + (\omega\square_2\,\text{◎◎}) q_2 + (\omega\square_2)\ r \quad (29)$$

f is the consequent parameters (p1, q1, r1, p2, q2, r2).

In the forward pass of the learning algorithm, consequent parameters are identified by the least squares estimate. In the backward pass, the error signals, which are the derivatives of the squared error with respect to each node output, propagate backward from the output layer to the input layer. In this backward pass, the premise parameters are updated by the gradient descent algorithm [39-41].

RESULTS

Fig. 12: Expermental Result Fake Detection for Face, Iris and Finger Print

Fig. 13: Expermental Result Fake Detection for Finger Print

(a)

(b)

(c)

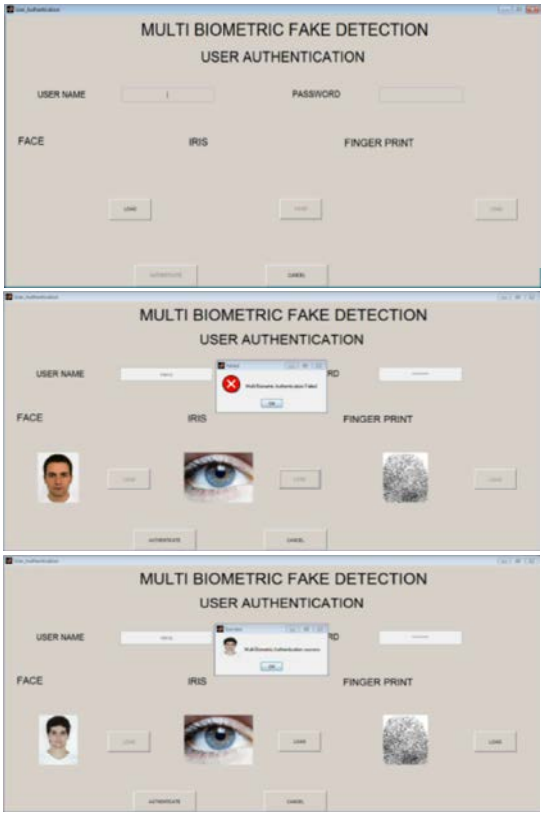

Fig. 13: (a)(b)(c) Fake Detection user authentication for Face, Iris and Finger Print

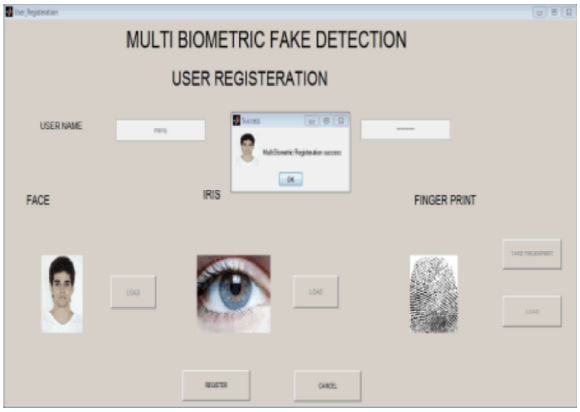

Fig. 14: Expermental Result Fake Detection for Iris Image

CONCLUSION

In this work, we developed a efficient face, iris and finger print fake detection system using Adaptive Neuro fuzzy inference system (ANFIS). The main aim of this fake system is to find accuracy level of face, iris and finger print detection by preprocessing phase, feature extraction and classification. In pre processing phase we

implemented median filter and canny edge detection algorithm for face fake biometric system. Anisotropic Gaussian filters for finger print fake detection system. Median filter and canny edge detection algorithm, polar coordinate system and Daugman's rubber sheet model for fake iris detection system. This preprocessing proposed work was carried on removing noise from a face, iris and fingerprint Image. In this proposed algorithm work Experimental results is conceptually simple, faster and efficient. In feature extraction a set of Gabor filters with different frequencies and orientations was used for extracting salient features from face, iris and fingerprint images. Which can reflect face, iris and finger images of texture information more effectively. In classification phase, the test performance of the ANFIS was determined by the computation of the statistical parameters such as specificity, sensitivity and accuracy. This technique is fast in execution, efficient in classification and easy in implementation. The experimental results have a remarkable improvement in the accuracy level achieved. Experimental result indicates that the technique is workable with accuracy greater than 93.78 %.

REFERENCES

1. Stephanie, A. and C. Schuckers, 2002. Spoofing and anti-spoofing measures,Information Security Technical Report, 7(4): 56-62.
2. Prabhakar, S., S. Pankanti and A.K. Jain, 2003. Biometric recognition: Security and privacy concerns, IEEE Security Privacy, 1(2): 33-42.
3. Matsumoto, T., 2004. Artificial irises: Importance of vulnerability analysis,in Proc. AWB.
4. Galbally, J., R. Cappelli, A. Lumini, G.G. De Rivera, D. Maltoni and J. Fierrez,, 2010. An evaluation of direct and indirect attacks using fake fingers generated from ISO templates," Pattern Recognit. Lett., 31(8): 725-732.
5. Anjos, A. and S. Marcel, 2011. Counter-measures to photo attacks in face recognition: A public database and a baseline, in Proc. IEEE IJCB, pp: 1-7.
6. Hennebert, J., R. Loeffel, A. Humm and R. Ingold, 2007. A new forgery scenario based on regaining dynamics of signature, in Proc. IAPR ICB, vol. Springer LNCS-4642, 366-375.
7. Hadid, A., M. Ghahramani, V. Kellokumpu, M. Pietikainen, J. Bustard and M. Nixon, 2012. "Can gait biometrics be spoofed?" in Proc. IAPR ICPR, pp: 3280-3283.
8. Akhtar, Z., G. Fumera, G.L. Marcialis and F. Roli, 2012. Evaluation of serial and parallel multibiometric systems under spoofing attacks, in Proc. IEEE 5th Int. Conf. BTAS, Sep., pp: 283-288.
9. Hui, H.P.S., H.M. Meng and M.K. Mak, 2007. Adaptive Weight Estimation in Multi-Biometric Verification Using Fuzzy Logic Decision Fusion, IEEE International Conference on Acoustics, Speech and Signal Processing, ICASSP 2007, 1: 501-I-504.
10. Jain, A.K. and A. Ross, 2004. Multibiometric systems, Communications of the ACM, 47(1): 34-40.
11. Ross, A., D. Nandakumar and A.K. Jain, 2006. Handbook of Multibiometrics, Springer, Heidelberg.
12. Ross A. and A.K. Jain, 2003. Information Fusion in Biometrics, Pattern Recognition Letters, 24(13): 2115-2125.
13. Jain, A.K. and A. Ross, 2004. Multibiometric systems, Communications of the ACM, 47(1): 34-40.
14. Chang, K.I., K.W. Bowyer and P.J. Flynn, 2005. An Evaluation of Multimodal 2D+3D Face Biometrics. IEEE Transactions on Pattern Analysis and Machine Intelligence, 27(4): 619-624.
15. Graig T. Diefenderfer, 2006. Thesis on ¯Fingerprint Recognition? at Naval Postgraduate School, Monterey, California.
16. Rajharia Jyoti, Dr. P.C. Gupta and Arvind Sharma, Fingerprint-Based Identification System:-A Survey. International Journal of Computer Technology and Electronics Engineering (IJCTEE), 1(3).
17. Afsar, F.A., M. Arif and M. Hussain, 2004. Fingerprint Identification and Verification System using Minutiae matching, National Conference on Emerging Technologies.
18. Krithika Venkataramani a, Vaibhav Kumar Singh. Fingerprint Identification: a Brief Literary Review.
19. Sangram Bana and Dr. Davinder Kaur. Fingerprint Recognition using Image Segmentation, (IJAEST) International Journal of Advanced Engineering Sciences and Technologies, 5(1): 012-023.
20. (Fingerprint database online source), Available: http://bias.csr.unibo.it/fvc2000/download.asp, Last visit: on July 2014.
21. (Iris database online source), Available: http://biometrics.idealtest.org/findTotalDbByMode.do?mode=Iris, Last visit: on July 2014.
22. Bansal, A., R. Agarwal and R.K. Sharma, 2012. FAR and FRR based analysis of iris recognition system (Published Conference), *IEEE SignalProcessing, Computing and Control*, pp: 1-6.

23. (Accuracy and Precision Online Source), Available: http://en.wikipedia.org/wiki/Accuracy_and_precision, last visit: on July 2014.
24. Bouzalmat, A., N. Belghini, A. Zarghili, J. Kharroubi and A. Majda, 2011. Face Recognition Using Neural Network Based Fourier Gabor Filters & Random Projection". International Journal of Computer Science and Security (IJCSS), 5(3).
25. Lee, C. and S. Wang, 1999. Fingerprint Feature Extraction Using Gabor Filters, Electronics Letters, 35(4): 288-290.
26. Yang, J., L. Liu and T. Jiang, 2002. Member, IEEE, An Improved Method for Extraction of Fingerprint Features, Proc. the 2nd Int. Conf. Image and Graphics, Anhui, PR China.
27. Rajanna, U., A. Erol and G. Bebis, 2010. A comparative study on feature extraction for fingerprint classification and performance improvements using rank-level fusion, Pattern Analysis and Applications, 13(3): 263-272.
28. Mohammed Sayim Khalil, Dzulkifli Muhammad, Muhammad Khurram Khan and Khaled Alghathbar, 2010. Singular points detection using Fingerprint orientation field reliability, ? International Journal of Physical Sciences, 5(4): 352-357.
29. Gonzalez, R.C. and R.E. Woods. 2002. Digital Image Processing, Prentice Hall, Upper Saddle River, NJ.
30. Maltoni, D., D. Maio, A.K. Jain and S. Prabhakar, 2003. Handbook of Fingerprint Recognition, Springe,
31. Germain, R.S., A. Califano and S. Colville, 1997. Fingerprint matching using transformation parameter clustering, IEEE Computational Science and Engineering, pp: 42-49.
32. Prabhakar S., A.K. Jain and S. Pankanti, 2003. Learning fingerprint minutiae location and type, Pattern Recognition, 36(8): 1847-1857.
33. Zhao, F. and X. Tang, 2007. Preprocessing and post-processing for skeleton-based fingerprint minutiae extraction, Pattern Recognition, 40(4): 1270-1281.
34. Chang, F.J. and Y.T. Chang, 2006. Adaptive neuro-fuzzy inference system for predictionof water level in reservoir, Advances in Water Resources, 29: 1-10.
35. Shing, J. and R. Jang, 1993. ANFIS: Adaptive neuro fuzzy inference system, IEEE Tranction on Systems, Man and Cybernetics, 23: 3.
36. Boyacioglu, M.A. and D. Avci, 2010. An Adaptive Network-Based Fuzzy Inference System (ANFIS) for the prediction of stock market return: The case of the Istanbul Stock Exchange" Expert Systems with Applications.
37. Shing, J. and R. Jang, 1993. ANFIS: Adaptive neuro fuzzy inference system, IEEE Tranction on Systems, Man and Cybernetics, 23: 3.
38. Loganathan, C. and K.V. Girija, Hybrid Learning For Adaptive Engineering and Science, 2: 6-13.
39. Haykin, S., 2003. *Neural Networks - A Comprehensive Foundation*, 4th ed. Pearson Education (Singapore) Pvt. Ltd. Indian Branch.
40. Zurada, J.M., 1999. *Introduction to Artificial Neural Systems*, Jaico Publishing House Mumbai, pp: 121.