INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

MULTIBIOMETRICS FOR AUTHENTICATION BASED ON ALTERED FINGERPRINT DETECTION AND TEMPLATE BASED IRIS RECOGNITION

PRANJALI B.ULHE, KALYANI SATONE, MADHURI PAL

Dept. of CE, Suresh Deshmukh College of Engg.

Accepted Date: 15/03/2016; Published Date: 01/05/2016

Abstract*:* A Biometric system is essentially a pattern recognition system which makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user. Biometric technologies are defined as the automated methods of identifying or authenticating the identity of a living person based on a physiological or behavioral characteristic. Deployment of Automated Fingerprint Identification System is widespread in border control as well as law of enforcement applications that increases need of ensuring that these systems should not be compromised. There are several investigated issues in fingerprint system security which includes fake fingerprints as for masquerading identity as well as fingerprint alteration and many security related issues. In this paper an approach of Multi biometrics is used so as to make the system more secure which can avoid the problem of masquerading identity as well as alteration. So here we are discussing two most preferable and promising techniques of biometrics i.e. fingerprint and iris with decision level fusion for two designs 1) Serial Design and 2) Parallel Design for alteration detection and both are compared so as to achieve efficient accuracy.

Keywords: Fingerprint detection, Iris recognition, Fusion, Parallel design, Serial design

PAPER-QR CODE

Corresponding Author: MS. PRANJALI B.ULHE

Access Online On:

www.ijpret.com

How to Cite This Article:

Pranjali B. Ulhe, IJPRET, 2016; Volume 4(9): 1469-1486

INTRODUCTION

Biometrics makes use of physiological or biological characteristics to measure the identity of an individual. These features are unique to each individual and remain unaltered during a person's lifetime. The unaltered features make biometrics a promising solution to the society. The access to the secured area can be made by the use of ID numbers or password which amounts to knowledge based security. But such information can easily be accessed by intruders and they can easily breach the doors of security. The problem arises in case of monetary transactions and highly restricted to information zone. A biometric system is essentially a pattern recognition system which makes a personal identification by determining the authenticity of a specific physiological or behavioral characteristic possessed by the user. Biometric technologies are thus defined as the automated methods of identifying or authenticating the identity of a living person based on a physiological or behavioral characteristic.

The various biometrics traits available are face, fingerprint, iris, palm print, hand geometry, ear etc. Fingerprints have a long history as a tool for identification and forensic purposes. Technological advancement has led to the development of so-called Automated Fingerprint Identification Systems (AFISs) which are primarily used by border control and law enforcement agencies for identification purposes. The success of fingerprint recognition systems in accurately identifying individuals has prompted some individuals to engage in extreme measures for the purpose of circumventing these systems. The primary purpose of fingerprint alteration is to evade identification using techniques varying from abrading, cutting, and burning fingers to performing plastic surgery (see Figure 1.1).

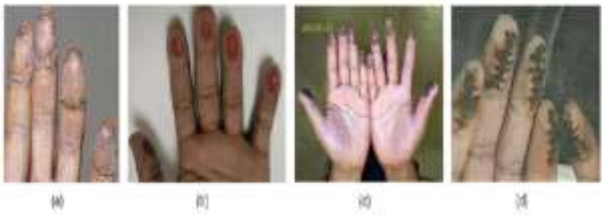


Figure 1.1 Photographs of altered fingerprints. (a) Transplanted friction ridge skin from sole. (b) Fingers that have been bitten. (c) Fingers burnt by acid. (d) Stitched fingers.[1]

The use of altered fingerprints to mask one's identity constitutes a serious "attack" against a border control biometric system since it defeats the very purpose for which the system was deployed in the first place, i.e., to identify individuals in a watch list.

It should be noted that altered fingerprints are different from fake fingerprints. The fake fingers are made of glue, latex, or silicone which is a well-publicized method to circumvent fingerprint systems. Altered fingerprints, however, are real fingers that are used to conceal one's identity in order to evade identification by a biometric system. While fake fingers are typically used by individuals to adopt another person's identity, altered fingers are used to mask one's own identity. Generally the altered fingerprint are divided into three types

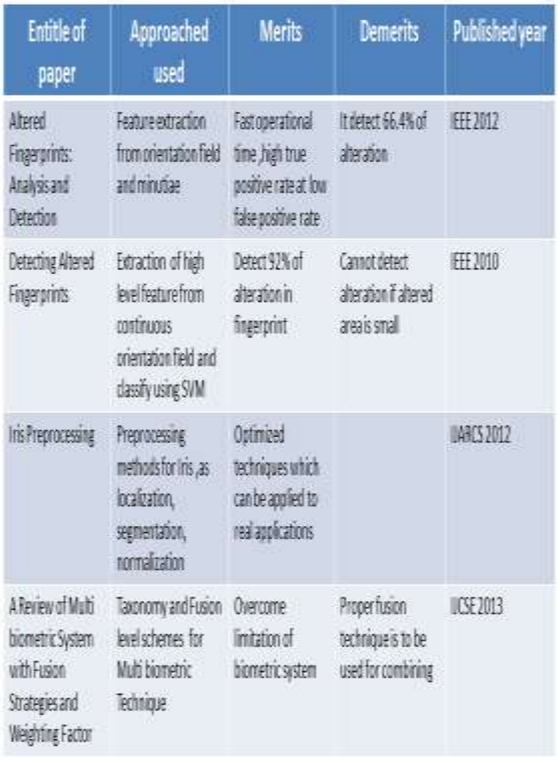
1) Obliteration

2) Distortion

3) Imitation

Unless the success of fingerprint recognition system, due to very minute differences in the normal fingerprints and altered fingerprints it has become a big challenge to detect the alteration for any fingerprint recognition system .So to avoid the masquerading identity and alteration problem, we propose to use multimodal biometric system so as to detect the growing threat of person evading the AFIS.

Related Works



Entitle of paper	Approached used	Merits	Demerits	Published year
Altered Fingerprints: Analysis and Detection	Feature extraction from orientation field and minutiae	Fast operational time ,high true positive rate at low false positive rate	It detect 66.4% of alteration	IEEE 2012
Detecting Altered Fingerprints	Extraction of high level feature from continuous orientation field and classify using SVM	Detect 92% of alteration in fingerprint	Cannot detect alteration if altered area is small	IEEE 2010
Iris Preprocessing	Preprocessing methods for Iris ,as localization, segmentation, normalization	Optimized techniques which can be applied to real applications		IJARCS 2012
A Review of Multi biometric System with Fusion Strategies and Weighting Factor	Taxonomy and Fusion level schemes for Multi biometric Technique	Overcome limitation of biometric system	Proper fusion technique is to be used for combining	IJCSE 2013

III. Problem Definition

It is seen from the literature survey that many unimodal biometric system are developed for safe, secure and efficient authentication in public sectors, law of enforcement etc. and there are many well developed system which are capable for safe and secure authentication in spite of which the offenders find new techniques to deploy these present system such as by masquerading their identity using alteration or by using fake identity. So there is a need to develop a system which will provide safe, secure and accurate authentication and will be able to detect the alterations efficiently.

IV. Proposed Methodology

Proposed Methodology is based on the use of Multi biometrics system for authentication as it is known that uni-modal biometric systems perform identification based on single source of biometric information. These systems are affected by many problems like noisy sensor data, nonuniversality, lack of individuality, lack of invariant representation, masquerading identity, alteration and susceptibility to circumvention. Because of these problems, the uni-modal biometric systems error rate is quite high which makes them unacceptable for security applications. Some of these problems can be alleviated by using two or more uni-modal biometrics as multi-biometric systems. The architecture of a multi-biometric system depends on the sequence through which each biometrics are acquired and processed. Typically these architectures are either serial or parallel.

In the proposed methodology two individual unimodal are used

1) Fingerprint Alteration Detection Modal
2) Iris Recognition Modal

I Method of Fingerprint Alteration Detection Modal

In the altered fingerprint detection modal it will check for whether the fingerprint image inputted is normal fingerprint or altered fingerprint. Firstly the fingerprint image is inputted then the following methods are applied

- Preprocessing
- Feature Extraction
- Minutiae Distribution

A Preprocessing

Preprocessing of fingerprint image consist of

1) Normalization
2) Segmentation
3) Histogram Equalization

Normalization

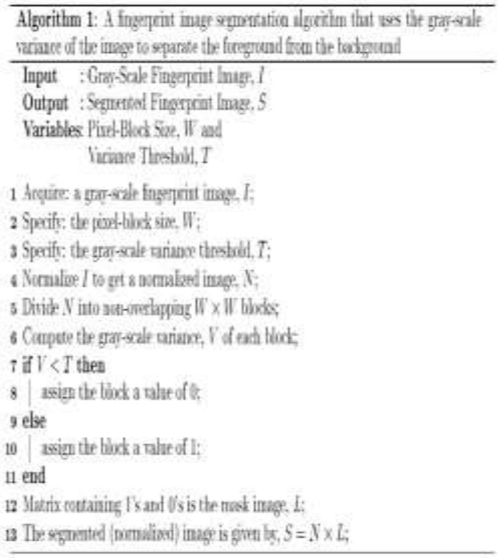
In image processing, the term normalization typically is a process of modifying the range of pixel intensity values. Here, it deals with adapting a common alignment and size of the fingerprint image to ensure invariance with respect to translation and rotation. A rectangular region of the fingerprint is located, rotated to be aligned along the longitudinal direction, and cropped using the fingerprint segmentation algorithm. The cropped image is resized to 512 x 480 pixels

Segmentation

An important image preprocessing operation is that of separating the fingerprint image ridge area the Region of Interest (ROI) from the image background. This is known as fingerprint segmentation. The input fingerprint image, I, is intensity normalized to have zero mean along with unit standard deviation. This is done by the following pixel-wise function:

$$I_n(x,y) = \frac{I(x,y) - avg(I)}{std(I)}$$

where avg (I) is the average pixel intensity of the input image and std (I) is the standard deviation. I(x; y) is the pixel intensity at pixel (x; y) of the input image. From I_n it is possible to generate a binary image, I_{mask}, known as the mask of the fingerprint where ones belong to the image ROI and zeros belong to the background.



```
Algorithm 1: A fingerprint image segmentation algorithm that uses the gray-scale
variance of the image to separate the foreground from the background
Input     : Gray-Scale Fingerprint Image, $I$
Output    : Segmented Fingerprint Image, $S$
Variables: Pixel-Block Size, $W$ and
           Variance Threshold, $T$
Acquire: a gray-scale fingerprint image, $I$;
Specify: the pixel-block size, $W$;
Specify: the gray-scale variance threshold, $T$;
Normalize $I$ to get a normalized image, $N$;
Divide $N$ into non-overlapping $W \times W$ blocks;
Compute the gray-scale variance, $V$ of each block;
if $V < T$ then
    assign the block a value of 0;
else
    assign the block a value of 1;
end
Matrix containing 1's and 0's is the mask image, $L$;
The segmented (normalized) image is given by, $S = N \times L$;
```

Histogram Equalization

Histogram equalization is a common method for enhancing the contrast of image. The method defines a mapping of grey levels p into grey levels q which attempts to uniformly distribute the grey levels q. A cumulative histogram of the enhanced image would show a relatively linear curve and the ideal mean would be right in the centre of the density value. Histogram equalization the contrast of grey levels are stretched near the histogram maxima using histogram equalization. This improves the detect ability of many image features. Applying this technique only on the ROI or maybe even using a block-wise approach of this method would probably yield better results. Functions used for histogram Equalization

```
I = imread ('pout.tif');

J = histeq (I);

Subplot (2,2,1);
```

```
imshow ( I );

subplot (2,2,2);

imhist (I)

subplot (2,2,3);

imshow ( J );

subplot (2,2,4);

imhist (J)
```

B Feature Extraction

Haar Wavelet Transform is used for feature extraction Wavelet transform (WT) represents image as a sum of wavelets on different resolution levels. The power of WT is that it offers high temporal localization for high frequencies while attempts good frequency resolution for low frequencies. Thus, WT is a good tool to extract local features of the image.

Wavelet transform is a mathematical tool based on many layer function decomposition. After applying wavelet transform, a signal can be described by many wavelet coefficients which represent the characteristics of signal. If the image has distinct features with some frequency and direction, the corresponding sub images have larger energies in wavelet transform. For this reason wavelet transform has been widely used in signal processing, pattern recognition and texture recognition.

By applying wavelet transform, vital information of original image is transformed into compressed image without much loss of information. Haar wavelet transform technique, the most popular amongst wavelets, is applied for feature extraction from Fingerprint. The benefit of Haar transform is its ease of implementation and also it can work well on non-linear intensity image.

C Minutiae Distribution

Minutiae distribution can be obtained by using following methods

1) Gabor Filter
2) Orientation
3) Binarization
4) Thinning
5) Minutiae extraction
6) False minutiae Extraction

Gabor Filter

The goal is to determine the clarity of friction ridges in a fingerprint so that found singularities can be classified based on the quality score of their position. Gabor filters will be used to measure the quality of friction ridges. Gabor filters are bandpass filters that have both frequency and orientation properties; they can therefore be constructed to present friction ridge frequency and orientation.

Orientation

The OFA uses a mathematical model for constructing an approximation of an estimated ridge of the fingerprint. The analysis identifies discontinuities based on differences of the ridge two approximation and estimation, e.g. areas where the approximation is unable to correctly simulate the actual fingerprint image.

Binarization

Image binarization is the process of turning a gray scale image to a black and white image. In a gray-scale image, a pixel can take on 256 different intensity values while each pixel is assigned to be either black or white in a black and white image. This conversion from gray-scale to black and white is performed by applying a threshold value to the image. In MATLAB, a value of one means the pixel is white, whereas a value of zero indicates the pixel is black. For a gray-scale image, the pixels are decimal values between zero and one. When a threshold is applied to an image, all pixel values are compared to the input threshold. Any pixel values below the threshold are set to zero, and any values greater than the threshold are set to one. By the end of this process, all pixel values within the image are either zero or one, and the image has been converted to binary format.

Thinning

After binarization, another major pre-processing technique applied to the image is thinning, which reduces the thickness of all ridge lines to a single pixel. Following thinning, the location and orientation of the minutiae should still be the same as in the original image to ensure accurate estimation of their locations.

Minutiae extraction

The skeleton image is used to extract minutiae points which are the points of ridge endings and bifurcations. The location of minutiae points along with the orientation is extracted and stored to form feature set. For extraction of minutiae points eight connected pixels are used. The Crossing Number method is used to perform minutiae extraction. This method extracts the ridge endings and bifurcations from the skeleton image by examining the local neighborhood of each ridge pixel using a 3×3 window.

False minutiae Extraction

The preprocessing stage does not totally heal the fingerprint image. For example, false ridge breaks due to insufficient amount of ink and ridge cross-connections due to over inking are not totally eliminated. Actually all the earlier stages themselves occasionally introduce some artifacts which later lead to spurious minutiae. This false minutiae will significantly affect the accuracy of matching if they are simply regarded as genuine minutia. So some mechanisms of removing false minutia are essential to keep the fingerprint verification system effective.

Following is the procedures in removing false minutia are:

1. If the distance between one bifurcation and one termination is less than D and the two minutia's are in the same ridge (m1 case). Remove both of them. Where D is the average inter-ridge width representing the average distance between two parallel neighboring ridges.

2. If the distance between two bifurcations is less than D and they are in the same ridge, remove the two bifurcations. (m2, m3 cases).

3. If two terminations are within a distance D and their directions are coincident with a small angle variation. And they suffice the condition that no any other termination is located between the two terminations. Then the two terminations are regarded as false minutia derived from a broken ridge and are removed. (case m4,m5, m6).

4. If two terminations are located in a short ridge with length less than D, remove the two terminations (m7).

D Matching

Minutiae distribution includes number of steps so that a processed template can be achieved for matching stage, then the template is saved to database with the name of person. In the matching stage the current fingerprint image is inputted and processed with all the methods of the algorithm and then the currently processed image will be matched with the template saved in the database, if the feature of the currently processed image and the template matches more than 90% then only the system will detect the person as authorized person else it will give the message as unauthorized user.

II Methods of Iris Matching Modal

Iris Matching modal will check for whether the iris template belong to same person or not for which firstly we need to input an iris image, process on it by using various methods and then need to save the template in the database for comparison. Let us see the proposed methods for Iris recognition modal

- Localization
- Segmentation
- Normalization

- Haar Wavelet Feature Extraction
- Feature extraction by using Block sum method

A Localization

Iris localization (i.e., iris position from distance) is still a big challenge. For localization Pupil is the darkest portion of the eye and is detected and removed from the rest of the eye image so that only iris pattern can be used for matching.

The first step involved in pupil detection is to find the contours of the acquired iris image. Since the pupil region contains the lowest intensity values its edges can be formed easily. After edge detection the next step is to find the center of the pupil. Thus the process starts with dilating the edge detected image and the dilated image with filled pupil circle is used to find the Euclidean distance between the non-zero points. By computing the distance between non-zero points the spectrum showing the largest filled circle can be formed within the set of pixels. Since the pupil is the largest filled circle in the image the overall intensity of the spectrum peaks in at the center. This spectrum image can be used to compute the center of the pupil. The pixel position having the maximum value in the spectrum image corresponds to the pupil center. The radius of the pupil is the distance between the pupil center and nearest non-zero pixel.

B Segmentation

In segmentation the first stage of iris recognition is to isolate the actual iris region in a digital eye image which can be approximated by two circles, one for the iris/sclera boundary and another, interior to the first, for the iris/pupil boundary. The eyelids and eyelashes normally occlude the upper and lower parts of the iris region. Also, specular reflections can occur within the iris region corrupting the iris pattern. A technique is required to isolate and exclude these artifacts as well as locating the circular iris region.

The success of segmentation depends on the imaging quality of eye images to find the outer iris boundary intensity variation approach is used. In this approach concentric circles of different radii are drawn from the detected center. The circle having maximum change in intensity with respect to previous drawn circle is iris circle. The approach works fine for iris images having sharp variation between iris boundary and sclera. The radius of iris and pupil boundary is used to transform the annular portion to a rectangular block, known as strip.

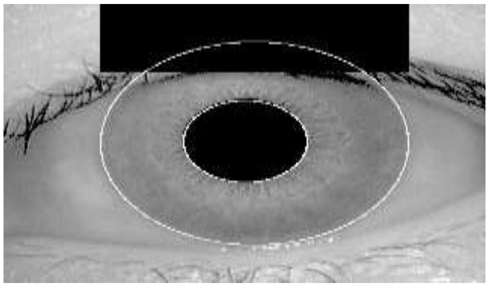


Figure 1.2 Example of segmented Image.

C Normalization

Once the iris region is successfully segmented from an eye image, the next stage is to transform the iris region so that it has fixed dimensions in order to allow comparisons. The dimensional inconsistencies between eye images are mainly due to the stretching of the iris caused by pupil dilation from varying levels of illumination. Other sources of inconsistency include, varying imaging distance, rotation of the camera, head tilt, and rotation of the eye within the eye socket.

The normalization process will produce iris regions, which have the same constant dimensions, so that two photographs of the same iris under different conditions will have characteristic features at the same spatial location. The localized iris image is transformed into strip. The transformed iris image consists of points taken from the pupil boundary to the outer iris boundary. Thus the same set of points is taken for every image. The iris image is normalized so that the size of strip does not vary for different images. Thus the size of iris strip is fixed for every iris image.

D Haar Wavelet Feature Extraction

Wavelets can be used to decompose the data in the iris region into components that appear at different resolutions. Wavelets have the advantage over traditional Fourier transform in that the frequency data is localized, allowing features which occur at the same position and resolution to be matched up. A number of wavelet filters, also called a bank of wavelets, is applied to the 2D iris region, one for each resolution with each wavelet a scaled version of some basis function. The output of applying the wavelets is then encoded in order to provide a compact and discriminating representation of the iris pattern**.**

The wavelet transform is also used to extract features from the iris region. Both the Gabor transform and the Haar wavlet are considered as the mother wavelet. From multi-dimensionally filtering, a feature vector is computed. Since each dimension has a real value ranging from -1.0 to +1.0, the feature vector is sign quantized so that any positive value is represented by 1, and negative value as 0. This results in a compact biometric template.

When compare the use of Gabor transform and Haar wavelet transform, it show that the recognition rate of Haar wavelet transform is slightly better than Gabor transform by 0.9%.

E. Matching

Iris matching algorithm includes number of steps so that a processed template can be achieved for matching stage, then the template is saved to database with the name of person. In the matching stage the current iris image is inputted and processed with all the methods of the algorithm and then the currently processed image will be matched with the template saved in the database, if the feature of the currently processed image and the template matches more than 90% then only the system will detect the person as authorized person else it will give the message as unauthorized user.

III. Fusion

In the methodology Decision level fusion is used for getting the final output. In this fusion strategy, a separate authentication decision is made for each biometric trait. These decisions are then combined into a final vote

In the proposed work two designs are used for fusion

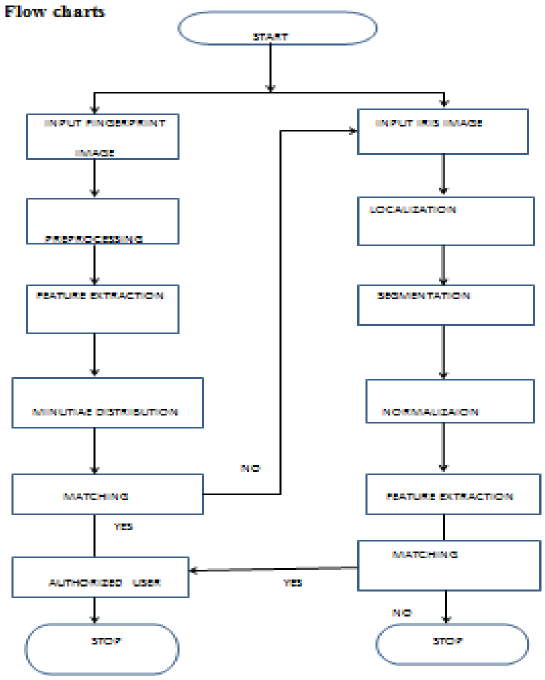
1) Serial Design

2) Parallel Design

1) Serial Design

In Serial Design the "OR" Rule is used for making the decision. In these design first the accuracy of one biometric trait is consider if the output from first trait is "True".

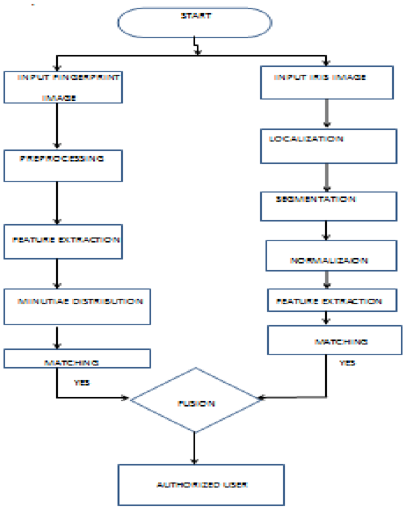
Then it will give the decision as authorized user and it will not check for the other biometric trait, but if the output from first trait is "False" then it will check for the other trait and then it will give the decision based on the output.



2) Parallel Design

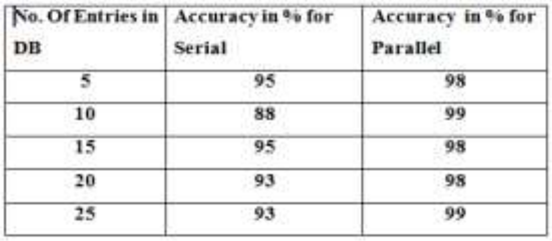
In Parallel Design the "AND" Rule is used for making the decision. In these design both the biometric trait are considered for the decision , if the output from both the trait are "True" then it will give the decision as authorized person but if the output from any one trait is "False" it will give the decision as unauthorized person.

Flow Chart



V. Result Analysis

In our proposed work we have used the concept of multi biometrics for authentication of a user, here we have fused the two most promising Techniques of biometrics for authentication. Here we have used the fusion at decision level with two designs 1) Serial design and 2) Parallel design. We have tested the data on both the designs to achieve the maximum accuracy. The designs were tested with 5,10,15,20 and 25 users for accuracy the results are as follows in Table 5.1



No. Of Entries in DB	Accuracy in % for Serial	Accuracy in % for Parallel
5	95	98
10	88	99
15	95	98
20	93	98
25	93	99

Table 5.1: Accuracy in serial and parallel Design

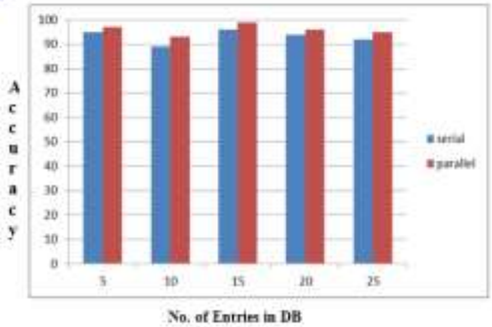


Figure 5.1 Comparison between serial and parallel design

Figure 5.1 shows the comparison between Serial design and Parallel Design which is about 94% for serial design and 98% for parallel design approximately. From the comparison it can be observed that the parallel design gives more accuracy than the serial design which can be more beneficial for authentication in the areas of law of enforcement as well as for security.

VI. Conclusion and future work

In this work a new system for authentication of an individual in public sectors, private sectors, law of enforcement, border control applications etc. by using multi biometrics concept. In our work Fingerprint detection and template based iris matching techniques by decision level fusion are used which are implemented for two designs 1) serial design and 2) parallel design. which gives and output of 94% for serial design and 98% for parallel design approximately, which shows that by using parallel design maximum accuracy can be achieved in multi biometrics. The parallel design will be beneficial and can be better implemented for the law of enforcement system and for the security so the problem of masquerading identity and alteration can be avoided to a great extent.

The system is tested for 25 user's data from CASIA for fingerprint images as well as iris images.

Future Scope

This study can be further extended along the following directions:

1) Determine the alteration type automatically so that appropriate counter measures can be taken.

2) Reconstruct altered fingerprints. For some types of altered fingerprints where the ridge patterns are damaged locally or the ridge structure is still present on the finger but possibly at a different location, reconstruction is indeed possible.

3) Multi biometrics can be implemented by using other recognition techniques as face, voice, palm etc. and by using different fusion level methods as matching score level etc.

References

1. Soweon Yoon, Student Member, IEEE, Jianjiang Feng, Member, IEEE, and Anil K. Jain, Fellow "Altered Fingerprints: Analysis and Detection", IEEE Transactions On Pattern Analysis And Machine Intelligence, Vol. 34 No.3 Year 2012
2. Jianjiang Feng, Anil K. Jain, Arun Ross (IEEE Members) "Detecting Altered Fingerprints" 2010 International Conference on Pattern Recognition IEEE computer society
3. Ram Kumar, Jasvinder Pal Singh, Gaurav Srivastava "A Survey Paper on Altered Fingerprint Identification & Classification" International Journal of Electronics Communication and Computer Engineering Volume 3, Issue 5, ISSN (Online): 2249–071X, ISSN (Print): 2278–4209
4. Michela Tiribuzi, Marco Pastorelli, Paolo Valigi, Elisa Ricci "A Multiple Kernel Learning Framework for Detecting Altered Fingerprints" 21st International Conference on Pattern Recognition (ICPR 2012) November 11-15, 2012. Tsukuba, Japan
5. Soweon Yoon, Qijun Zhao, and Anil K. Jain (IEEE Members) "On Matching Altered Fingerprints" International conference on biometrics New Delhi March 2012

6. Sheeba Jeya Sophia S. and Veluchamy S. "Security System Based On Iris Recognition" Research journal of engineering science VOL(2) March 2013, ISSN 2278-9472

7. Sowmya.B , Sreedevi.S.L "Iris Recognition System for Biometric Identification" Volume 2, Issue 6, June 2012 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering

8. Gargi Amoli, Nitin Thapliyal, and Nidhi Sethi "Iris Preprocessing" Volume 2, Issue 6, June 2012 ISSN: 2277 128X International Journal of Advanced Research in Computer Science and Software Engineering

9. Haryati Jaafar, and Dzati Athiar Ramli "A Review of Multi biometric System with Fusion Strategies and Weighting Factor" Haryati Jaafar et al./ International Journal of Computer Science Engineering (IJCSE) ISSN : 2319-7323 Vol. 2 No.04 July 2013