International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 07
March 2018

Ultimate Security System

Authors: Anup Dinakar Chandavar, Vineeth Pai, RohanKumar Shetty, Bibin TE
Department of **Computer Science**
Shree Devi Institute of Technology and Management
Email id:- anupchandavar21@gmail.com, vineethpai007@gmail.com, rohanshetty2727@gmail.com, bibithayyil007@gmail.com

Under the guidence of Asst.Prof Sadanada L

***Abstract*—the system proposed in this paper is a security system that uses both biometrics and non biometrics to overcome the downsides of each other. This system can be broken into three parts password protection, Face recognition and Fingerprint recognition. In Password protection user has to input set of characters as username and password which is later compared with previously stored data for user authentication. In Face recognition 'Face' and 'Eye' haar cascade are used for identification of human facial features which are extracted from set of grayscale images acquired from the camera then stored for comparison with the Images acquired while user authentication. Fingerprint recognition consists of three main parts, image acquisition, processing and identification and recognition. A fingerprint image is acquired and fed into the image processing program. In image processing acquired image is enhanced by performing image cropping, grayscale enhancement, binarization, ridge filtration. After the image has been processed, it is fed into the Harris corner detection algorithm for feature extraction and then the data obtained is stored in the database. While user authentication acquired image again goes through the image processing and then it is compared with the previously stored data for recognition. User needs to pass all these security checkups to gain access to the confidential data.**

Keywords—fingerprint recognition; face recognition; password protection; U.S; haar cascade; LBP;

I. INTRODUCTION

Nowadays security is one of the prominent topic of discussion and fingerprint recognition is one of the most trusted security system in around the globe but it has its own downsides such as spread of contagious diseases as user has to place his/her finger on the fingerprint scanner which is reused by other user too. But we have developed a system which doesn't contain any scanner avoiding the major problem of typical scanner based fingerprint recognition system but this has its own downside too the quality of image acquired during image acquisition is relatively poor so sometimes outcome may be undesired so to overcome this deficiency this system contains two more security checkups they are password and face recognition which in turn produces a security system that is no less compared to the typical fingerprint recognition system but also relatively low-cost too.

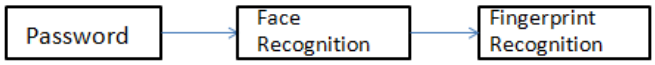


Fig 1: Flowchart of Ultimate security system

This system can be divided into two main parts they are Non Biometric that is password protection system and Biometric system. Biometric system can be further divided into Face recognition and Fingerprint recognition systems.

II. NON BIOMETRIC SYSTEM

Here user inputs a user name and a password which is compared with the previously stored data for user authentication. If both the data matches exactly then user can proceed further.

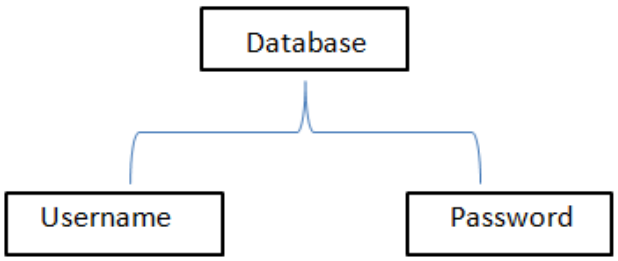


Fig 2: representation of working of Password Protection

III. BIOMETRIC SYSTEM

Biometric system is on those system which is more secure than other security system i.e. Password, card etc. The meaning of Biometrics is as bio means live and metrics means measure. Biometrics system is used to measure the part of human body characteristics to authenticate the user. And each individual have their own unique characteristics which cannot be copied by other human. That's why biometric system is

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 07
March 2018

more secure. Here Biometric system can be divided into two types Face recognition and Fingerprint recognition.

A. Face recognition system:

A.1 Face Detection

In this system, OpenCv is used to implement the haar cascade classifier [6]. Haar features are used to check the presence of features in the input image. Each features result in a single value which is calculated by subtracting the sum of pixels under white rectangle from the sum of pixels under black rectangle. It is a machine learning based approach where a cascade function is trained from a lot of positive (Images of Face) and negative images (Images without Face). It is then used to detect faces in other images.

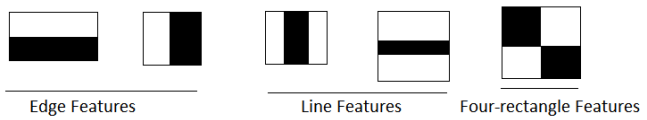


Fig 3. Haar Features

For each feature calculation, we need to find sum of pixels under white and black rectangles. To solve this concept of integral images is used. It simplifies calculation of sum of pixels, how large may be the number of pixels, to an operation involving just four pixels

If 24×24 window is used as the base window size to start computing these features in any input image then it has to calculate about 160, 000 features if all the parameters of haar features are considered which is nearly impossible to solve this problem adaboost algorithm is used. Adaboost is a machine learning algorithm which determines the best features among 160,000 features these features are the weak classifiers. Adaboost constructs a strong classifier as a linear combination of these weak classifiers as shown in (2).

$$\mathbf{A(x) = \alpha 1F1(x) + \alpha 2F(x) + \cdots\cdots\cdots\cdots (1)}$$

The face detection is performed using Haar like features by passing an image as input then if the image passes all the stages it is considered to be an image of human face and if not then the image doesn't contain any human face.

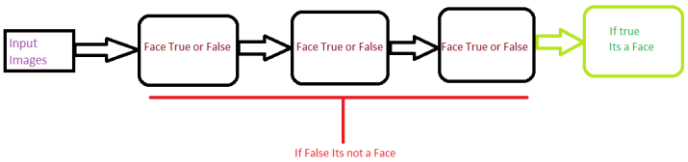


Fig 4. Cascade classifier

A.3 Face Recognition [5]

Here Face recognition is carried out by extracting the feature out of multiple images of the user face and storing it in the database which is later used to train the detector program to identify the user out of other faces. Here we used Local Binary Patterns (LBP) [3] to process images for recognizing as they are not affected by lightning changes as some other algorithms do.

formal description of the LBP operator can be given as:

$$LBP(x_c, y_c) = \sum_{p=0}^{P-1} 2^p s(i_p - i_c)$$

Here i_c is the intensity of the central pixel (x_c,y_c), i_n is the intensity of the neighboring pixel and s is the sign function as $s(x) = 1$ if $x \geq 0$ else 0.

This description enables you to capture very fine grained details in images. But here it cannot encode the details differing in scales. To solve this variable neighborhood is used by aligning an arbitrary number of neighbors on a circle with a variable radius, which enables to capture the neighborhoods:

For a Point (x_c, y_c) the position of the neighbor $(x_p, y_p), p \in P$ can be calculated by:

$$x_p = x_c + R\cos(\frac{2\pi p}{P})$$
$$y_p = y_c - R\sin(\frac{2\pi p}{P})$$

Where R is the radius of the circle and P is the number of sample points. If a points coordinate on the circle doesn't correspond to image coordinates, the point get's interpolated. The OpenCV implementation does a bilinear interpolation:

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 07
March 2018

$$f(x,y) \approx \begin{bmatrix} 1-x & x \end{bmatrix} \begin{bmatrix} f(0,0) & f(0,1) \\ f(1,0) & f(1,1) \end{bmatrix} \begin{bmatrix} 1-y \\ y \end{bmatrix}.$$

By definition the LBP operator is robust against monotonic gray scale transformations.

Thus using LBP operator dataset of images are created which are later used while recognizing the image.

A.4 Experimental Results

OpenCv 2.7is used to implement the haar cascade based face detector and recognition system based on LBP. We tested our face recognition system using multiple images of 4 different faces and set of 50 images each and also in different lightning conditions and the result obtained were correct and quick.

B. *Fingerprint recognition system:*

In this fingerprint recognition system user has to place his/her finger in front of a camera few inches away depending on focal length of camera lens. An image of the users finger is captured which is fed into the image processing program where the image acquired is converted into grayscale and is cropped, resized for faster computation of the data acquired by the image. But image acquired is of very low quality so to produce image with enough details for further computation it is fed into multiple filtration programs. Here image is first binarized as non binarized image contains floating value ranging from 0 to 1 which provides extra detail not suitable for further computation so to eliminate all those intermediate values binarization is carried out.

Fig 5: Image without binarization(On left) Binarized Image (On right)

This binarized image is then fed into Harris corner detection algorithm to extract the features from the image, which is stored for the further use in the database.

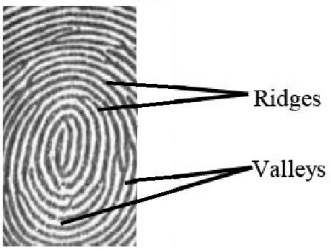


Fig 6: Ridges and Valleys in the fingerprint

C. *Standard Harries Corner Detection algorithm [1]*

The main purpose of this algorithm is to look for and since corners represent a variation in the gradient in the image, we will look for this "variation".

Consider a grayscale image I. We are going to sweep a window $w(x,y)$ (with displacements u in the x direction and v in the right direction) I and will calculate the variation of intensity.

$$E(u,v) = \sum_{x,y} w(x,y)[I(x+u,y+v) - I(x,y)]^2$$

where:

$w(x,y)$ is the window at position (x,y)
$I(x,y)$ is the intensity at (x,y)
$I(x+u,y+v)$ is the intensity at the moved window $(x+u,y+v)$

Since we are looking for windows with corners, we are looking for windows with a large variation in intensity. Hence, we have to maximize the equation above, specifically the term:

$$\sum_{x,y} [I(x+u,y+v) - I(x,y)]^2$$

Using *Taylor expansion*:

$$E(u,v) \approx \sum_{x,y} [I(x,y) + uI_x + vI_y - I(x,y)]^2$$

Expanding the equation and cancelling properly:

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 07
March 2018

$$E(u,v) \approx \sum_{x,y} u^2 I_x^2 + 2uvI_xI_y + v^2 I_y^2$$

- Which can be expressed in a matrix form as:

$$E(u,v) \approx \begin{bmatrix} u & v \end{bmatrix} \left(\sum_{x,y} w(x,y) \begin{bmatrix} I_x^2 & I_xI_y \\ I_xI_y & I_y^2 \end{bmatrix} \right) \begin{bmatrix} u \\ v \end{bmatrix}$$

- Let's denote:

$$M = \sum_{x,y} w(x,y) \begin{bmatrix} I_x^2 & I_xI_y \\ I_xI_y & I_y^2 \end{bmatrix}$$

- So, our equation now is:

$$E(u,v) \approx \begin{bmatrix} u & v \end{bmatrix} M \begin{bmatrix} u \\ v \end{bmatrix}$$

- A score is calculated for each window, to determine if it can possibly contain a corner:

$$R = \det(M) - k(\mathrm{trace}(M))^2$$

where:

- $\det(M) = \lambda_1\lambda_2$
- $\mathrm{trace}(M) = \lambda_1 + \lambda_2$

a window with a score R greater than a certain value is considered a "corner"

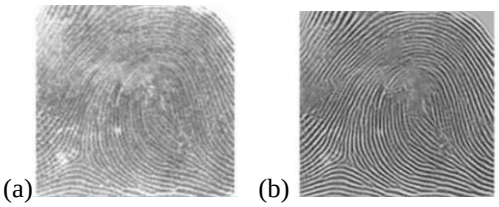
But as Harris corner detection algorithm has its own downsides we weren't able to use it to extract desired features from a fingerprint so we turned towards **Improved Harries Corner and Edge Detection** algorithm [4].

D. Image Enhancement

Before feeding image to Harries corner detection algorithm image has to face some filtration processes so that the low quality image is enhanced enough to be able to contain extractable details. This is achieved by image enhancement algorithms [3]. As our system takes images of fingerprint from a portable camera device high quality image cannot be accepted so to filter the gained low quality image corrupted region of the image must be recovered.

Fig 7: Corrupted Fingerprint image

Recovering the fingerprint details is done by first normalizing the image then orienting the image estimated from the normalized input image followed by computation of the frequency of the image from normalized input fingerprint image and the estimated orientation image then each block of the image is checked for recoverable or unrecoverable region later the image is fed to multiple gabor filtration process to obtain the final image.



(a) (b)

Fig 8: (a) Fingerprint before enhancement, (b) Fingerprint after enhancement

E. Fingerprint Matching

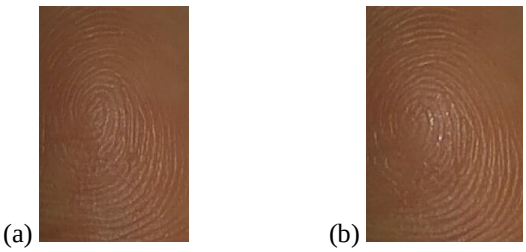
After enhancement the image is fed into feature extraction program where some keypoints are generated at ridge birification and at ridge ends and keypoints distances are computed and stored which are later used for fingerprint matching. While matching if the keypoints do not exceed the threshold value, fingerprints are considered as matched and if not then they are considered as mismatched.

Fig 9: Keypoints on a fingerprint

F. Experimental Results

Test 1

International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 07
March 2018



(a) (b)

Fig 10: (a) Fingerprint input image while signup, (b) Fingerprint input image while login

(a) (b)

Fig 11: Binarized images of (a) and (b) input images

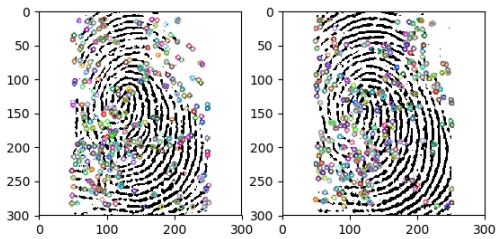
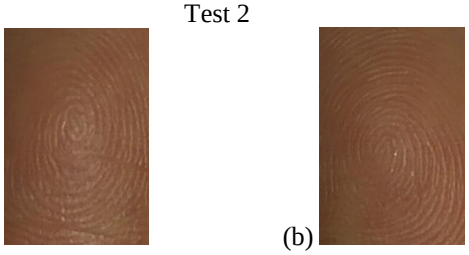


Fig 12: Keypoints drawn on the fingerprint images b and a
The above images are of low quality but because of all the filtering processes and enhancement we finally obtained the correct result of being matched as both the fingerprints were obtained from the same finger.

Test 2



(a) (b)

Fig 13: (a) Fingerprint used while signup and (b) Fingerprint used while login

(a) (b)

Fig 14: Binarized image of fingerprints a and b

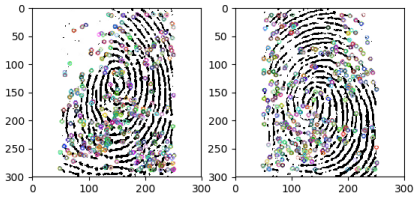


Fig 15: Keypoints drawn on the fingerprints a and b
The result obtained was correct as the fingerprints were of two different fingers result was fingerprint mismatched.

Even though the time consumption of this system is more than the typical scanner based finger print recognition system because number of image enhancement processes is carried out to make the low quality image suitable for recognition the result obtained was up to the mark.

IV. WORKING OF U.S

First user has to enter the username and password which is compared with the previously stored (while signup) password and username in the database and if both are matched then an image of users face is captured through face recognition program which is checked with the trained data and if the face is recognized user has to place his/her finger in front of the camera such that the finger covers the UI displayed on the camera which is fed into the fingerprint recognition program and if the fingerprint is matched then user can access the data stored inside the locked folder but this can also be used as replacement for any other locking system where digital locks are used.

V. *CONCLUSION*

We have created a security system that provides security to your valuable information by eliminating all the hassle of installing an expensive fingerprint or any other security system and also eliminating the spread of contagious skin diseases through its **Touch less Fingerprint recognition system** and also adding benefits of traditional password and a 2D face recognition system making it a mixture of Biometrics and Non Biometrics to create an ultimate system which covers the deficiency of each other.

References

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 07
March 2018

[1] Harris Corner Detector Wikipedia.

[2] Hong, L., Wan, Y., and Jain, A. K. Fingerprint image enhancement.

[3] Face recognition using Local Binary Patterns (LBP) By Md. Abdur Rahim, Md. Najmul Hossain, Tanzillah Wahid & Md. Shafiul Azam.

[4] Improved Harris Corner Detection algorithm for low contrast images by Liang Sun, Shuang-qing Wang, Jian-chun Xing.

[5] Image based face detection and recognition by Faizan Ahmad, Aima Najam and Zeeshan Ahmed.

[6] Object detection using Haar-cascade Classifier by Sander Soo