International Journal of Modern Engineering Research (IJMER)
www.ijmer.com Vol.2, Issue.5, Sep-Oct. 2012 pp-3376-3378 ISSN: 2249-6645

# Biometrics Security System using the Smart System concept

Nivetha. R[1], Shanmuga Priya. S[2]
[1,2](Department of information technology, Sri Manakula Vinayagar Engineering College, Puducherry

***ABSTRACT :*** *The Biometrics field has got much advancement each and every year. Each advancement aims at promoting a high level of security when compared to the previous model in that field. Our paper deals with providing a high level of security as well as efficient authentication system by using the "smart system" concept. According to the smart system concept, we have coupled the two existing efficient systems of biometrics such as the "Iris scanning" and the "Finger print recognition" systems.*

***Keywords*****:** *"CCD Camera, Finger Print Recognition System, Iris Scan and Smart System".*

## I. INTRODUCTION

In every biometrics systems there is some kind of drawbacks [1][7][8][9]. Our paper aims to overcome this in an efficient manner by using the smart system concept. Though biometric security is ahead of all other security systems, still intruders and hackers deprive its functionality. Improvising security just with the single body part seems to be lacking effectiveness. Hence, in this paper we have tried to devise a new security system in which both IRIS SCAN and FINGER PRINT recognition are combined to prove its worth. It's an attempt to couple the existing technologies rather than to go in for search of a new one. Based on our idea the implementation will replace the traditional ID methods such as P.I.N numbers for accessing ATMs and virtually every other electronic device used for conducting business where identification is a requirement and pre requisite. The smart system deals with combining IRIS SCAN and the FINGER PRINT Recognition Technologies and use the combined value as the security input data to provide security.

This can be done by following the two phases:

1. Registration Phase
2. Authentication Phase

## II. REGISTRATION PHASE

The Registration phase is done to the new individual who wants to gain access to the system. The Registration phase is the first phase where the individual undergoes an Iris scan and then the Finger print recognitions. The person's Iris is scanned images and the Finger print images are taken, stored in the security database for the first time when they comes for registration.

### 2.1THE IRIS SCAN

IRIS: The **iris** (plural: ***irides*** or ***irises***) is a thin, circular structure in the eye, responsible for controlling the diameter and size of the pupils and thus the amount of light reaching the retina. "Eye color" is the color of the iris, which in humans can be green, blue, or brown. [2] The image of the scanned Iris of the human eye is shown in the figure1.

The Iris Scanning is done with help of a CCD camera. CCD is abbreviated as charge-coupled-device. The person is made to stand 13 to 15'' from a CCD camera. The CCD camera captures very-high resolution of the images and the accuracy is also very high. Human Iris has 260 independent variables so no two individuals can have the same kind of Iris structure.

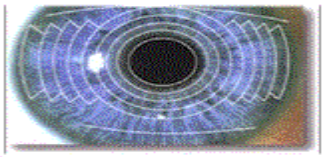

**Figure1. Iris scanned image**

### 2.2 FINGER PRINT RECOGNITION

MINUTIAE: The small lines on the surface of the finger.

The individual places his/her finger over the glass plate, which resides over the high-resolution CCD camera. These images are relatively large in size and so there can be many permutations and combinations to adjust the threshold value. [2][3][4][5][6]This technology is neither too expensive, nor does it require extensive user – training. It's also simple to implement since a fingerprint reader can sit on a mouse or a keyboard or simply connect like one. It also gives a high level accuracy with 35 independent variables. The finger print image is shown in the figure2.

The image captured is compared to that in the system's database. Positive identification or rejection, as the case may be, is based on the number of minutiae (small lines on the surface of the skin) that match. The number that must match for the result to be ***' hit '*** or ***'no hit '*** can be defined. After the Finger print is scanned it is stored in the security database as it was done in the Iris scan. Then the Smart system concept is done by coupling the Iris and the Finger print scanned images.


**Figure2. Finger print with minutiae**

## III. SMART SYSTEM CONCEPT

The concept of the security system is to combine the Iris and the Finger print value from the smart card. It follows the below mentioned algorithm.

**Step1: Take the Iris variable as Iris_val.**
During the registration of the concerned person into the security, his iris image has to be captured by a high – end CCD camera and then the captured image is stored in the database and in consequent with that an iris variable is generated. (number ranging from 0 to 9).

**Step2: Take the Finger print variable as Finger_val.**
The recorded image has to be converted as a unique number as follows, Positive identification or rejection, as the case may be, is based on the number of minutiae (small lines on the surface of the skin) that match.
Then a number is generated as follows

- Let X is the number of minutiae in contact with the surface and Y is the number of left out surface.
- Then the number Finger_val is given as XY (number varying from 0 to 9).

**Step3: Couple the Iris_val and the Finger_val.**
Consider for Example
The Iris_val is generated as 13579 and The Finger_val is generated as 24681.Then these two values are coupled and this coupled value (Couple_val) is used in the smart system to provide security. The two values are coupled as shown below.

**Iris_val = 13579 (x1x2x3x4x5)**
**Finger_val = 24681 (y1y2y3y4y5)**
**Couple_val= 1234567891(x1y1x2y2x3y3…)**

Where x1x2x3x4x5 are the digits of the Iris_val and y1y2y3y4y5 are the digits of the Finger_val. These two values are cross coupled and the coupled value obtained consist of x1y1x2y2x3y3x4y4x5yx5 which are the digits of the Iris_val and the Finger_val. The coupling process is represented diagrammatically in Figure 3.

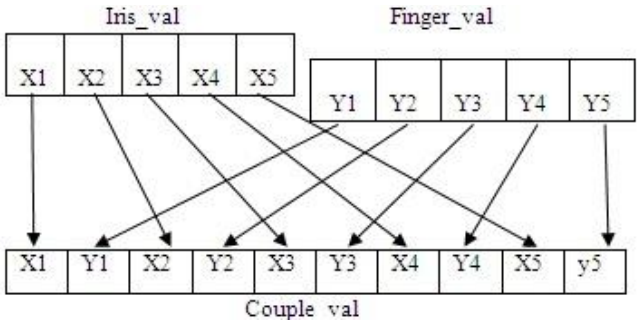


**Figure 3.Generating the coupled value (Couple_val)**

Then after creating the couple value apply the log to that value to obtain a high accuracy. This value can be called as the Authentication code or Identity code (Smart_Icode). The Smart Icode value is calculated as shown below.

**Smart_Icode = $\log_{10}$(Couple_val)**
**= $\log_{10}$(1234567891)**
**= 9.09151497752**

This **Smart Icode value is stored in the security database** to provide authentication to the individuals to access the system.

## IV. AUTHENTICATION PHASE

The authentication phase deals with providing authentication to the person. In this stage the individual's Iris and the Finger prints are scanned and the couple value (Couple_val) is calculated and its log value (Smart_Icode) is computed. Now this Smart_Icode value is compared with value in the database.

### 4.1 GRANTING ACCESS

If the computed Smart_Icode value matches with the value stored in the database then the person is considered as the valid user and the access is granted for that person. Otherwise the access will not be provided to that person. The granting of access will be done as shown in Figure4.

**CHECK** for the value **Smart_Icode value** in the database

IF **PRESENT** then

Compare the stored image in the database corresponding **Smart_Icode** value with the scanned image.

IF **SCAN MATCHES** then

**"VALIDUSER ACCESS GRANTED"**

Else

**"INVALID USER ACCESS DENIED"**

**Figure 4.Authentication Process**

## V. ARCHITECTURE OF THE SECURITY SYSTEM

The Architecture of the security system works as shown in the figure 5. The architecture or the working of the Smart security System is clearly represented diagrammatically the working of the couple system is also displayed.

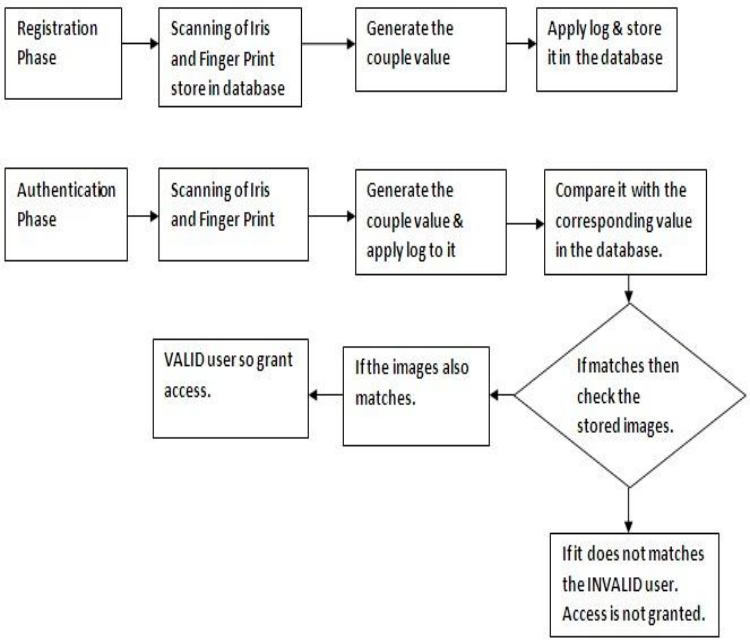


**Figure 5.Architecture of the Smart coupled security system.**

The working of the Registration and the authentication phase is separately displayed. The architecture show the flow in which the process is being carried out.

### 5.1 ADVANTAGES OF THIS SECURITY SYSTEM

The above design upon implementation would be much more advantageous and efficient than the present day designs that we use as a means that there is no other alternative way

- This new design is based on coupling the existing technologies rather trying our hands in a new sphere.
- The Hacker though possible of breaking into the first phase, his false identity would be revealed in our coupled design in the later part.
- There is no need to store FINGER PRINT IMAGES in the security database and hence efficient memory management.
- Comparison of numerical value is employed rather than image comparison hence the process is quickened and thus lot of time is saved
- The couple system value cannot be reversed and no intruders can understand the code even if they break it in the first stage.

## VI. CONCLUSION

The Smart couple system of Biometrics is very efficient to provide a high level of security and authentication. The algorithm for the Smart couple system is very much easier to implement. This algorithm can be easily implemented using any programming language. Any future enhancement can be made to this system without much modifications or changes in the baseline. This is simple but efficient one and it uses the existing resources which is already available and known to us.

***"You are the password No one else has it, but you"***

As our future work we are going to include the Psycho-Physiology[10]. Psycho-physiological involves the measurement of physical symptoms, which reflect the emotional arousal of a person. For this purpose, we consulted with leading psychiatrists who confirmed us that the emotional state of a person will definitely be reflected in his physical behaviors, particularly during stress, feeling of guilt, tendency to cheat etc. Research done for a different purpose in various universities also confirmed that the physical characteristics such as heart activity, muscle activity, respiration, skin conductivity etc definitely reflect an individual's mental state.

**Acknowledgements**

We would like to thank our institution for providing greater support in our Research.

### REFERENCES

[1] "Biometrics:Overview". Biometrics.cse. msu. edu. 2007-09-06.

[2] Reference for eye biometrics http://www.iris-scan.com/

[3] S. Dass and A. K. Jain, " Fingerprint Classification Using Orientation Field Flow Curves", *Proc. of Indian Conference on Computer Vision, Graphics and Image Processing*, (Kolkata), pp. 650-655, December 2004.

[4] Y. Zhu, S. C. Dass, and Anil K. Jain, " Compound Stochastic Models for Fingerprint Individuality", *Proc. of International Conference on Pattern Recognition (ICPR)*, Vol. 3, pp. 532-535, Hong Kong, August, 2006.

[5] S. C. Dass, Y. Zhu and Anil K. Jain, " Statistical models for assessing the individuality of fingerprints", *Fourth IEEE workshop on Automatic Identification Advanced Technologies*, pages 1-7,2005.

[6] S. Pankanti, S. Prabhakar, and A. K. Jain, "On the Individuality of Fingerprints", *IEEE Transactions on PAMI*, Vol. 24, No. 8, pp. 1010-1025, 2002. A shorter version also appears in *Fingerprint Whorld*, pp. 150-159, July 2002.

[7] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," IBM systems Journal, vol. 40, pp. 614–634, 2001.

[8] BIOMETRICS TO APPEAR Barry, S.C., Brooks, S.P., and Catchpole E.A. & Morgan B.J.T. (2002)

[9] BIOMETRICS REDUNDANT MODEL Catchpole E.A., Morgan B.J.T. & Freeman S.N. (1998).

[10] Hand book of Psycho-physiological second edition, editied by John T.Cacioppo,Louis G.Tassinary, Garry G.Berntson.