



New Fingerprint Based Authentication Scheme

Vedpal Singh*

CSE Dept. UIET,

Kurukshetra University Kurukshetra

vedpalsiet101@gmail.com

Anu Kundu

CSE Dept. UIET,

Kurukshetra University Kurukshetra

anu.haryana@gmail.com

Joginder Singh Chauhan

CSE Dept., Shobhit Institute of Engg. & Technology,
Saharanpur (Uttar Pradesh Technical University, Lucknow)

mrjsc@in.com

Maheep Singh

CSE Dept., Shobhit Institute of Engg. & Technology,
Saharanpur (Uttar Pradesh Technical University, Lucknow)

Maheep.singh@rediffmail.com

Vishant Kumar

CSE Dept., Shobhit Institute of Engg. & Technology,
Saharanpur (Uttar Pradesh Technical University, Lucknow)

vishuk22@yahoo.com

Abstract: In the recent years biometric is a popular technology for authentication. Traditionally, authentication techniques introduce many security related attacks. To overcome these problems we can use biometric authentication techniques. This paper represents the user authentication based on fingerprint technology and represents their authentication methods.

Keywords: fingerprint authentication, biometric authentication techniques, cryptography, security and identification.

I. INTRODUCTION

[1] In the recent years, there is a trend of using the mechanism of biometrics for security purpose. There are the different types of human biological features that are used for authentication such as eye, retina, fingerprint, palm vein biometrics. For improving the security of smart card we use the biometric concept. Hackers can easily break the security of smart cards. For improving the security, we use the different types of authentication scheme such as fingerprint based authentication, palm vein authentication, eye based authentication etc. Fingerprint authentication used the fingerprint sensors and used a special type of identification system called AFIS (Automated Fingerprint Identification System). [2] Palm vein authentication uses the vascular pattern of an individual's palm as personal identification data. Palm has a broader and more complicated vascular pattern. Palm is an ideal part of the body for the biometric technology; palm does not have hair, it less susceptible to change in skin color, unlike a finger or back of the hand. [3] For recognizing a person's biometrics is an automated method which is based on physiological or behavioral properties. Biometrics systems are superior because they provide nontransferable properties. Nontransferable means of identifying people not just cards or badges. Nontransferable means it cannot be given or lent to another individual.

II. FINGERPRINT AUTHENTICATION

[4] There are the some restrictions are when we use the fingerprint based authentication. Smart card restrictions are

presented when technology is improved. The two big restrictions are clock frequency and data transmissions. Because of the above restrictions, the fingerprint verification can be performed into the following steps: i) Image capture, ii) Pre – processing, iii) Minutiae extraction, iv) Alignment and Matching.

A. Image capture

For capturing the image used the fingerprint sensors. But the advances sensors are used in fingerprint image capture are semiconductor sensors that obtain the image quality over 500dpi. This type of sensors suffer from different types of problems like latent fingerprint, death finger etc. For reducing the problems use the same anti – fraud elements.

B. Pre processing

For adaption of the image and reduced data we use the method of pre – processing. In the pre – processing method, firstly, a gradient map is captured. For obtaining, the reduced image with valleys and ridges by using the segmentation. Segmentation is performed based on the data available based on the data available at the gradient map. Then in the enhancement step finger pressure and humidity are reduced that affects the brightness and contrast. For finding, the tangent angles of all ridges in the finger image. We use the information from the orientation map of the finger image.

C. Minutiae Extraction

[5] Different kinds of methods are available for fingerprint feature extraction and recognition. For the

minutiae extraction we use the special kind of algorithm called “Ridge Following Algorithm”. This algorithm searches the ridges iteratively. For minutiae extraction use a method that use three steps

(1) Locate the fingerprint centre, (2) Extract the minutiae points, (3) Create the final set of minutiae.

After locating the centre point, the co – ordinate of the centre point is (0, 0) {origin}. Then create the co – ordinates for the fingerprint. Then we find the reference point that is the nearest minutiae point to the centre point. Then we recomputed the location of minutiae points. If we rotate or translate the fingerprint image then the centre point is not affected. In the final we create a final set of minutiae points.

D. Matching and authentication [6]

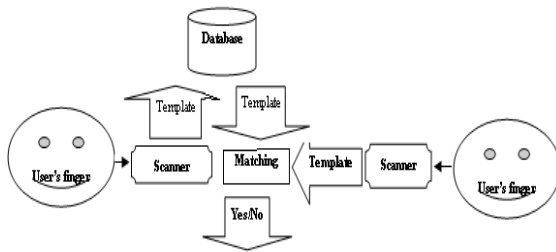


Fig. 1: Biometric matching and Authentication process

Fingerprint authentication as shown in figure there are the two phases: (1) Registration phase.

(2) Authentication phase.

In the registration phase, user's finger scan at the time of registration and scanned data is stored into the database for future authentication purpose. In the authentication phase, user's fingers are scan by the fingerprint scanner. For the matching previously stored data with the current input data that are scanned by the fingerprint scanner. We use the different - different matching algorithms. If the input template is match with the previously stored template then the user is authentic otherwise not. For the fingerprint verification we use the elastic matching algorithm because

the elasticity of the fingers introduces new variations. For example, distance between ridges etc.

III. CONCLUSION

At that time different types of biometric authentication techniques available such as fingerprint authentication, palm vein authentication, retina based authentication, face authentication etc. My paper shows that fingerprint authentication is best method for authentication. This paper shows the different authentication steps in fingerprint based authentication.

IV. REFERENCES

- (1) "Smart Card Technology and e-Governance" S.K.Sinha *e-notes*.
- (2) "SECURE SMART CARD USING PALM VEIN BIOMETRIC ON-CARD-PROCESS" International Conference on Convergence and Hybrid Information Technology 2008, R.Jeyaprakash, Jin Lee, S.Biswas, J.M.Kim, June14, 2010, pp. 548-551.
- (3) "Palm Vein Authentication System: A Review", International Journal of Control and Automation vol. 3, No. 1, I.Sarkar, F.Alisherov, T.H.Kim, D.Bhattacharyya, March, 2010, pp. 27-34.
- (4) "Microprocessor Smart Cards with fingerprintuser authentication" R.Sanchez – Reillo, C. Sanchez – Avila and L.Mengiber – Pozo, IEEE, 14June 2010, pp 46 – 49.
- (5) "Pass Phrase Based Speaker Recognition for Authentication" Heinz Hertlein, Dr. R. Rrichholz, Dr. Elmer Noth, 2003 working group BIOSIG, www.biosig.org
- (6) "A secure card system with Biometrics Capability" in proceedings of the 1999 IEEE Canadian conference on Electrical and Computer Engineering Shaw Conference Center, Edmonton, Alberta, Y.S.Moon, H.C.Ho, K.L.Ng, Canada may 9-12-1999, pp. 261-2.