Fingerprint Verification of ATM Security System by Using Biometric and Hybridization

Pramila D. Kamble, Dr.Bharti W. Gawali

Dr. BabasahebAmbedkarMarathwada University
Aurangabad 431004 (MS) India

Abstract- All the biometrics, fingerprint recognition is one of the most reliable and promising personal identification technologies. Fingerprints are plays an important role in biometric system. In biometrics technologies, fingerprint authentication has been in use for the longest time and bears more advantages than other biometric technologies do. Fingerprints are the most widely used biometric feature for person identification and verification. But in this paper we proposed that fingerprint verification of ATM (Automatic Teller Machine) security system using the biometric with hybridization. The fingerprint trait is chosen, because of its availability, reliability and high accuracy. The fingerprint based biometric system can be implemented easily for secure the ATM machine. In this system the working of these ATM machine is when the customer place on the fingerprint module when it access the ATM for draw the cash then, the machine wants to fingerprint of that user's which use the machine. Using biometric, it verify/identify fingerprint and gives accurate result that if it valid or not valid. In this way we can try to control the crime circle of ATM and do secure it.

Index Terms- Biometrics, Fingerprint verification, recognition, ATM (Automatic Teller Machine) terminal, features extraction.

I. INTRODUCTION

IN biometrics, identity of any unknown persons can be resolved in two ways .i.e. Verification and identification. In that fingerprint verifications are plays an important role in forensic application, criminal's investigation, terrorist identification, or any other security purpose. So in fingerprint verification is proved that it is one of the most reliable personal identification. Biometric refers to accurately identifying am individual based on his/her distinctive physiological (e.g. Fingerprint, face retina, iris) or behavioural (e.g. gait, signature, ATM) characteristics. Fingerprint verification methods include minutiae-based and image-based methods [4]. Yes there is no doubt to improve that fingerprint verification is based on these method so in addition to hybridization it also useful to fingerprint verification because fingerprint recognition refers to the automated method of verifying a match between two human fingerprint [5]. Suppose the twins are uses same account though they use same account but their fingerprint (thumb impression) different. We know about that when we use the biometric, same like that ATM. Using the ATM when provide customer with the convenient banknote trading is very common. However, the financial crime tamper with the ATM terminal, steal user's credit cards and password by illegal means. Suppose by mistake one user's card is lost and the password stolen, then the criminal draw all the cash in the shortest time [9]. How to carry on the valid identity to the customer becomes the focus in current financial circle. Therefore it is so important that the biometric thumb impression which gives the main identification proof of any unknown person. So, for ATM security using the hybridizing method with biometric fingerprint verification.

Fingerprint has intrinsic features that they do not change for whole life and are personally different. And they are easy to use, cheap and the most suitable miniaturization. So, fingerprint verification is an efficient personal verification method that has been the most widely used in comparison with other biometric information [4]. But all most here these two methods used.

II. RELATED WORK

It is most important that when the person enters bank to open his/ her account using ATM then it's necessary to give his/her thumb impression for security purpose. In minutiae-based fingerprint verification is fast verification execution is possible but though two fingerprints have the minutia, they do not necessarily have the same ridge. When the range of fingerprint image input is narrow as enough minutiae are not extracted, the verification confidence decreases but the size of fingerprint image is small, more exact verification is possible [4]. In general, the fingerprint image input for fingerprint verification is Gray image with lightness of 256. If the gray image is changed into a binary fingerprint image through binarization, the ridge and valley of the fingerprint will have consistent lightness and ridges which are discontinued by wrinkles, sweat, pores and finger pressure are connected. Fingerprint authentication is possibly the most sophisticated method of all biometric technologies and has been thoroughly verified through various applications. However, fingerprint is completely unique to an individual and stayed unchanged for lifetime [6]. For this reason this method is suitable for thumb impression on biometric whenever using the ATM (Automatic Teller Machine). This exclusivity demonstrates that fingerprint authentication is far more accurate and efficient than any other methods of authentication. Because fingerprints are now being used as a secure and effective authentication method in numerous fields, including financial, medical and any other entrance control applications. As saying that fingerprint is the most widely used biometric feature for person identification and verification in the field of biometric identification. Fingerprint possesses two main types of features that are used for automatic fingerprint identification and verification one is ridge and other is

minutiae. So the ridge and furrow structure that forms a special pattern in the central region of the fingerprint and the other minutiae details associated with the local ridge and furrow structure [7]. In a traditional biometric recognition system, the biometric template is usually stored on the central server during enrolment, and then the candidate biometric template captured by the biometric device is sent to the server where the processing and matching steps are performed. Same like when the person enters the security code on the ATM machine then the machine wants to get the fingerprint(thumb impression) about that persons who enter the security code if the person is right then the machine gives a positive result otherwise doesn't get result or say 'please try again'. Using this system firstly collect all the customers fingerprint when they draw bank account and add all fingerprint about that person identification information .Because the biometric machine recognize given fingerprint using False Rejection Rate (FRR) , this image database ,each sample is matched against the remaining samples of the same finger to compute the False Rejection Rate and False Acceptance Rate(FAR) .this also the first sample of each finger in the database is matched against the first sample of the remaining fingers to compute the False Acceptance Rate[11] , So using all these process we can control or stop that the criminal process which gives the duplicate number and draw all cash in ATM.In the former a person to be identified submits a claim , which is either accepted or rejected. In the latter, a person is identified without a person claiming to be identified. Generally in human identification is the association of an identity with a human being, traditionally, password and ID cards have been used for identification to restrict access to secure systems but these methods can be easily breached, for password can be guessed and ID card can be stolen , thus rendering them reliable[2]. One important thing is the fingerprint recognition systems are usually used only for adults. Because we might be able to recognize the fingerprints of infants, the common fingerprint recognition systems are suitable for adults only (due to the area and resolution of fingerprint sensors etc.).

(a) Registered image (b) Aligned input image(c) Result image

Figure 2. Binary image-based fingerprint matching

III. FEATURE EXTRACTION

To create a fingerprint by assuming that a set of feature extractors can identify significant features in the image [12]. Fingerprint is the pattern of ridges and valleys on the tip of a finger and is used for personal verification of people. The minutiae-based method requires accurate detection of the minutiae from a fingerprint image. Although the minutiae pattern of each finger is quite unique, noise and distortion during the acquisition of the fingerprint and errors in the minutiae extraction process result in a number of missing and spurious minutiae. And the smooth flow pattern of ridges and valleys in a fingerprint can be also viewed as an oriented texture. In biometric method it generate the feature extraction for using four steps, (i) Determine a reference point for the fingerprint image, (ii) Tessellate the origin around point for the fingerprint , (iii) Filter the region of interest in different directions , (iv) Define the feature vector[15].

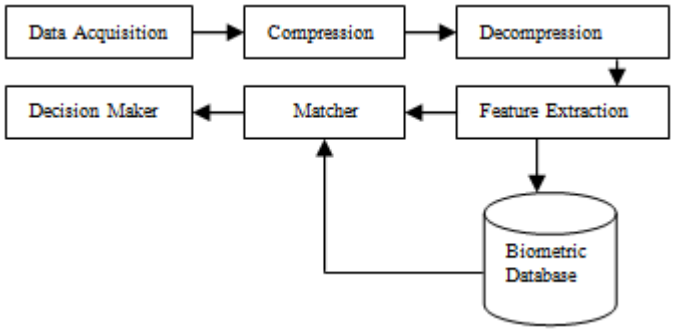

Figure 1 - A generic biometrics-based system. [1]

IV. CONCLUSION

It is essential that to first understand the basic of a biometric based security system. The implementation of ATM security system by using biometric method it is very important method. As well as very challenging and difficult. But for security purpose or control the criminal records it is very important to that produce this method. I think for future work it will implement also various technologies such that unique cards or any other method.

REFERENCES

[1] R. Vinothkanna, A. Wahi, 2012. A Novel Approach for Extracting Fingerprint Features from Blurred Images

[2] Z.A.Jhat, A. H. Mir, S. Rubab, 2011. Personal Verification using Fingerprint Texture Feature

[3] M. Ezhilarasan, D. S.Kumar, S. Santhanakrishnan, S. Dhanabalan, A.Vinod, 2010. Person Identification Using Fingerprint by Hybridizing Core Point and Minutiae Features

[4] J.K. Kim, S.H. Chae, S. J. Lim, S. B. Pan A Study on the Performance Analysis of Hybrid Fingerprint Matching Methods [5].Rakesh Verma, Anuj Goel, 2011, Wavelet Application in Fingerprint Recognition

[5] M. VLAD, A.ANISIE, M. S. VLAD, 2012. Automatic identification technologies

[6] C. Kant, R. Nath Reducing Process-Time for Fingerprint Identification System

[7] J. P. Chaudhari, P.M. Patil, Y.P.Kosta, 2012. Singularity Points Detection in Fingerprint Images

[8] P.KRISHNAMURTHY, MR. M. M REDDDY, 2012. Implementation of ATM Security by Using Fingerprint Recognition and GSM

[9] M.Drahansky, E.Brezinova, D.Hejtmankova, F.Orsag, 2010. Fingerprint Recognition Influenced by Skin Diseases

[10] S. Bana, Dr. D. Kaur Fingerprint Recognition using Image Segmentation

[11] P.Lamon1, I. Nourbakhsh, B. Jensen, R. Siegwart Deriving and matching image fingerprint sequences for mobile robot localization

[12] M. Dolezel, D.Hejtmankova, C. Busch, M.Drahansky, 2010. Segmentation Procedure for Fingerprint Area Detection in Image Based on Enhanced Gabor Filtering

[13] A. Ross, J. Reisman, A.Jain, 2002. Fingerprint Matching Using Feature Space Correlation

[14] M. Lourde R, D. Khosla, 2010. Fingerprint Identification in Biometric Security Systems

AUTHORS

First Author – Pramila D. Kamble, ShrikrishnaMahavidyalaya, Gunjoti, Dr. BabasahebAmbedkarMarathwada, University, Aurangabad 431004 (MS) India.

Email id - Shri_pad12285@yahoo.co.in

Second Author –Dr.Bharti W. Gawali, Department of Computer Science andInformation Technology, Dr. BabasahebAmbedkarMarathwadaUniversity, Aurangabad 431004 (MS) India