ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 9(17), DOI: 10.17485/ijst/2016/v9i17/88568, May 2016* ISSN (Online) : 0974-5645

Detection of Fingerprints in Advanced Biometric System Design

Prasanna Kumar Lakkoju* **and T. N. Shankar**

Department of Computer Science and Engineering, K L University, Guntur – 522502, Andhra Pradesh, India;
lakkoju.prasannakumar@gmail.com, tnshankar2004@rediffmail.com

Abstract

The objective of this research is to incorporate fingerprint authentication to thwart the intruders attack in a network. A complete feature extraction process to propose an authentication scheme is presented in this paper. False Acceptance Error and False Rejection Error have been stressed to measure the performance of the proposed scheme. The main finding is to obtain an authentication system with a better strength. Majority of authentication techniques are unable to provide verification efficiency leads to competent negligence without being recognized. The primary goal of this document is to introduce and apply an innovative strategy that customs the finger print modus operandi to enhance a host based attack recognition program in to advance its level of verification.

Keywords: Biometric System Design. Distortion, Fingerprint, Fingerprint Matching, Host-based Intrusion Detection System (HIDS)

1. Introduction

In information technology era determining intruders is one of the major challenge to any organization who they are relying on electronic information system. Recently, Intrusion Detection System (IDS) is a most useful application for protection or recognition of any kind of intruders attack. Basically PCs are more vulnerable to the three kinds of attacks: (1) User-level, when a genuine customer uses his rights to metal information, (2) System-level, when a thief uses program calls to fight the program and (3) Network-level, when an enemy uses data stream to perform the strike. During the past years, important developments have been made in terms of handling program and network-level strikes. However, user-level strikes work in combination with system-level strikes. Security is one of the most essential factor for people. A sensible house is always equiped with the equipments which are possessed with better innovative techniques for tracking temperature, multi-media, windows, doors, alarm systems, signals and various additional tasks supervised by PCs and offers a remote user interface with the automated programs, wireless transmitting or the internet, supervised through internet browser, smart phone or a web internet browser.

A common robotized biometrics-based framework comprises of six important parts shown in Figure 1. The information securing segment obtains the biometric information in computerized design by utilizing a sensor. The second and third parts of the framework are flexible, in light of the framework's capacity necessities. The fourth segment utilizes an element extraction calculation to deliver an element vector whose segments are numerical portrayals of the hidden biometrics. The fifth segment of the framework is the matcher which analyzes highlight vectors to deliver a score which demonstrates the level of resemblance between the pair of biometrics information under thought. The 6th segment of the framework is a chief that can be modified to suit framework particulars. There exist several protection and verification mechanisms that can be included in a intelligent house. These include the use of mathematical requirements like security passwords, Personal Identification Number (PIN) and passphrases, protection wedding party like intelligent

* *Author for correspondence*

card and fingerprint verification methods. However, studies have shown that mathematical requirements, intelligent cards and physical keys mechanisms have their associated drawbacks.

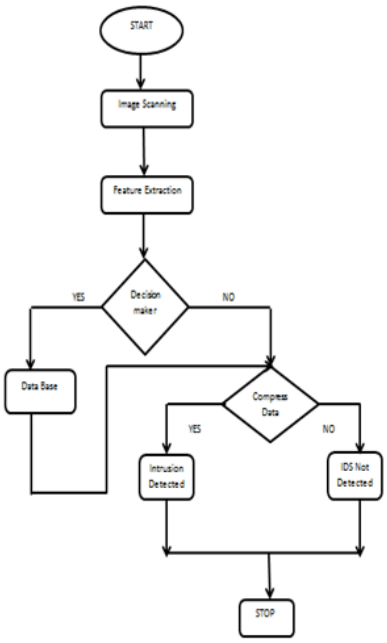


Figure 1. Fingerprint detection procedure in biometrics.

The confusing framework includes the blend of diverse human highlights. It is viewed as a standout amongst the most solid validation instruments to date. Unique Finger impression Recognition Technology (FRT) utilizes human unique mark to look at the unique mark designs so as to recognize a man. This paper exhibits the outline of a verification framework for brilliant home that consolidates the two-bio-measurements component: FRT. Our examination work means to characterize a structure that is most dependable for confirmation of brilliant homes.

Behavioral bio-measurements in light of PC mouse elements on the grounds of methodology that does not require a particular equipment to gather information[1,2]. Biometric solutions, such as identification systems using fingerprint, iris, face and palm print, hand geometry, signature, etc; have many advantages over the traditional authentication techniques. It can be used to defend the intruders attack to on the networks[3]. Rapid development of banking technology is changed the way of all most all transactions activities. An embedded fingerprint biometric authentication scheme for Automated Teller Machine (ATM) banking systems is better than password or PIN to solve an authentication related issues of each and every transcation[4–7]. Any transaction with the credit card is also must sensitive. Biometric can be used to prevent any kind of duplication or fraud[8]. Image processing technique is most essential to develop an authentication system of a finger print[9–11]. One noteworthy issue experienced in behavioral bio-measurements is the extraordinary estimation of False-Rejection-Rate (FRR), otherwise called the False-Pessimistic-Rate is the framework neglects to perceive an approval and rejection of the individual as an impostor and the False-Acceptance-Rate (FAR), otherwise called the False-Positive-Rate and is unapproved have been used to measure the performance of authentication systems[12].

2. Biometric Authentication based on HIDS

Figure 2 represents the fundamental structural planning of our framework. Each and every sensor of the IDS sends data to the focal IDS where the data should be broken and keep in mind. The goal is to inform the director about the real conduct of the client. It is obvious that the Fingerprint Identification System is one of the sensors which illuminates the focal IDS of all approved and unapproved login endeavors.

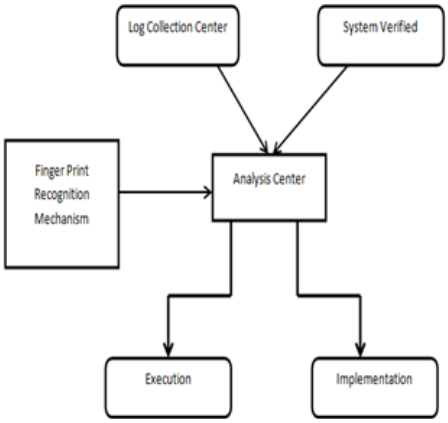


Figure 2. Architecture for IDS in fingerprints.

2.1 Unique Mark Identification System comprises of Two Procedures

2.1.1 The Enlistment Process

This procedure comprises of catching a persons unique mark utilizing a finger impression catching gadget. Amid

the enlistment handle, the framework spares the persons unique mark into a database.

2.1.2 The Confirmation Process

It is utilized to validate the guaranteed individual. This procedure compares enrolled unique mark and a selected unique mark to figure out the two matches. The PC is opened as soon as matching is over, but it is not convenient in terms of real time fingerprint applications.

2.2 Authentication using FRT

Biometric confirmation frameworks are picking up engaging quality as a method for giving access in diverse situations that needs protection and divides into 2 types: Physical based instruments and conduct based systems.

2.2.1 Physical Based Mechanisms

Psychological based instruments are the ones that draws attention on watching the natural and them physiological characters of the person. Samples of physical components are unique finger impression.

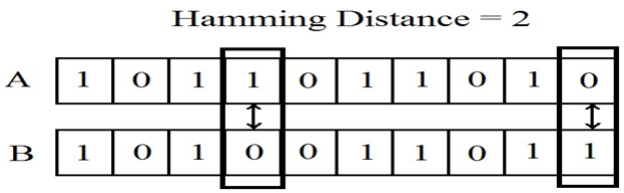
2.2.2 Conduct Based Mechanisms:

Conduct based systems are the ones that focuses on watching the non-organic or the non-physiological characters of the person. Cases of conduct based system incorporate the ones that include walk and writing examples biometrics.

Both mental and conduct based biometrics systems works by contrasting the information biometric and the spared biometric layout. The correlation gives a coordinating score utilizing hamming separation to judge whether the individual position should be matched or not. Hamming separation is a metric that measures the quantity of positions between two strings of equivalent length at which the relating images are distinctive. Hamming Distance is characterized as:

$$\frac{1}{n}\sum_{i=1}^{n} a_i \oplus b_i$$

Following process depicts how hamming distance works with the calculated hamming distance between the numbers being 2.



Example for hammig distance procedure in pixel calculation in real time applications.

This is one type of biometric security that uses a unique mark and thinks about its distiction. The acknowledgment innovation includes two stages: Enrolment and verification venture as appeared in Figure 3. In enrolment step client's finger impression is captured and stored in a database. For confirmation the client puts his enrolled finger on the scanner to capture the image for comparison. System allows to the client as soon as matching is over.

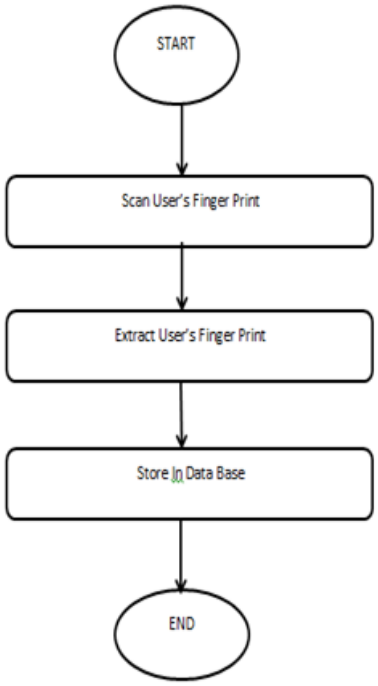


Figure 3. Fingerprint authentication mechanism for access/denied operations.

3. System Design

A wide range of unique mark bio-metric innovations are accessible today. A profoundly secure unique finger

impression bio-measurements may be troublesome and tedious to utilize. Then again, a helpful unique mark sensor may improve the simplicity and pace of utilization to the detriment of security. It is essential to comprehend the security prerequisites of an application and the level of comfort required by the clients of the biometric framework.

To start with, we characterize "Security" and Convenience' as far as known variables FAR and FRR:

Convenience = 1 – FRR (1)
Security = 1 – FAR (2)

The FRR is less helpful for application of more subjects are erroneously disapproved of administration or special case taking care of process. The higher the FAR, the less secure the application, since it will concede access to pernicious frauds. Consequently, it is essential to understand the Security/Convenience Trade-off. Sample fingerprint images as follows:

Contingent on the security or accommodation needs of a specific application, the creator can evaluate the FAR and FRR edges at which the framework would work. With regards to individual electronic gadgets, for example, portable workstations or cell phones, expense and client comfort will be critical contemplations. Since this application has a low number of individuals utilizing every gadget, a moderate FAR is a worthy security hazard. Since the sensor can be rapidly re-swiped in the event of a dismissal, a moderate FRR is adequate.

As shown in Figure 4 sensitivity of our proposed approach to build efficient security detection of fingerprints. In a restricted access office, the overriding concern will be security and not the comfort of the general population utilizing the framework or the expense of the sensor. In fact, this sort of use requires a low FAR, to guarantee that security is high. This implies the sensor and coordinating framework must be amazing to touch varieties. System could deny access to the clients of higher FRR for every once in a while which is the cost to pay for upgraded security. Security level must be high to defend the offenders and terrorists or different malevolent elements. Moreover, the application must be extremely helpful so that a substantial number can prepare rapidly to move the lines up. In fact, the security necessities of this application require a low FAR to keep the lines short and moving up. On account of FRR circumstances, a man will be hauled out of line and investigated physically by an outskirt control specification.

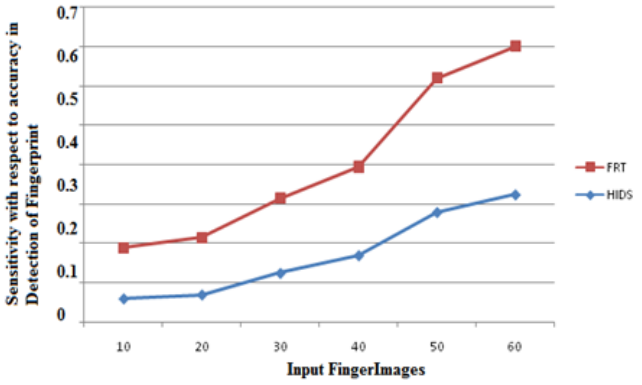


Figure 4. Sensitivity accuracy in finger print detection.

4. Simulation Results

The details based methodology talked about in IIIB is used, at low FARs it caught a decent measure of worldwide data and could recognize fingerprints that have a fundamentally the same worldwide structure. At the point when 25 sets of fingerprints (of predominant quality) were nourished into the product utilizing channel based calculation talked about as a part of area IIIC, the outcomes were as per the following: (Threshold Value = 35) No. of False Accepts = 2 (8%) No. of False Rejects = 1 (4%). Presently, here, we have a kind of a peculiarity. Since the false acknowledge rate is more noteworthy than the false reject rate, this would appear to propose that the calculation offers next to no security and is just about not powerful by any means. The reason for this kind of deviation may be ascribed to the way that the database that was utilized was little and not illustrative of the base dignity required for the best possible usefulness of the software. Possible, this could be helped by utilizing countless over which this mistake may bit by bit subside to the adequate cutoff points. From the information gave by the merchant, it can be seen that these blunders exist in worthy extents when the product was tried against a standard 10,000 print solid database.

Table 1 shows effective data presentation based on the progressive report of the false positive rate based on pixel frequencies.

By applying above considerable features on some of maximum related item sets based on microanyrisms rate

with proceedings of data presentation, which includes rotation of pixels in various uploaded images.

Table 1. Similarity matching with frequency of the fingerprint image

Uploaded Images	Normal FingerPrint		Host Based attacks	
	Frequency	Matching	Frequency	Matching
1	2	0.1	3	0.4
2	10	0.4	10	0.7
3	15	0.6	15	0.9
4	20	0.8	20	0.962

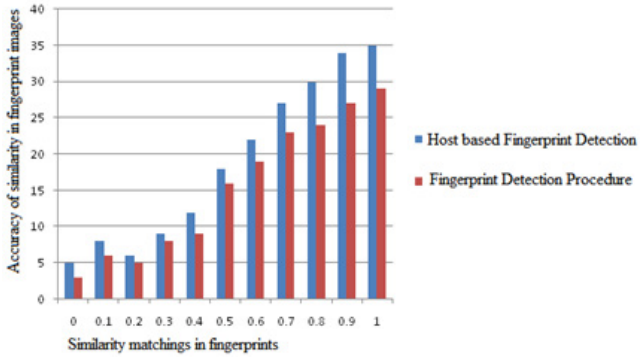


Figure 5. Distribution of matching similarity of the proposed method.

FOC (Fingerprint Online Challenge) based fingerprint images downloaded from different biomedical presentation with proceedings of relevant data presentation in real time application process. The measurement of similarity matching based on features of the fingerprint image and other configurations in common variants in uploaded fingerprint images. A systematic difference is occurred based on their relevancy of matching content. Also the performance of effective data presentation of microanyrism detection with specified features in semantic data variance and other configurations. Time efficiency is also maintain for calculating microanyrisms in fingerprint images of both Normal FI Detection and Biometric Oriented FI Detection process for detections of microanyrisms as shown in Table 2.

Table 2 shows comparison results of the uploaded fingerprint images with time comparator of the common feature processing events.

The range of retina pictures used in research is relatively large. Therefore the handling time can be reduced according to the variation of the range. Furthermore, Open CV Tool is a development environment, which can affect the time intake. In addition to it most of the related sets focus around the visual hard drive and boat network, which is effective to reduce time intake. Above all, the iterated spatial anisotropic sleek reduces the uninformative key points and reduced the time intake of the fingerprint recognition system.

Table 2. Data presentation based on time efficiency which includes microanyrisms detection

Number of Uploaded Images	Normal Finger Print	Host Based Attcks
1	7.0245	10.652
2	9.245	14.356
3	12.345	16.547
4	14.524	18.356
5	17.895	24.3256

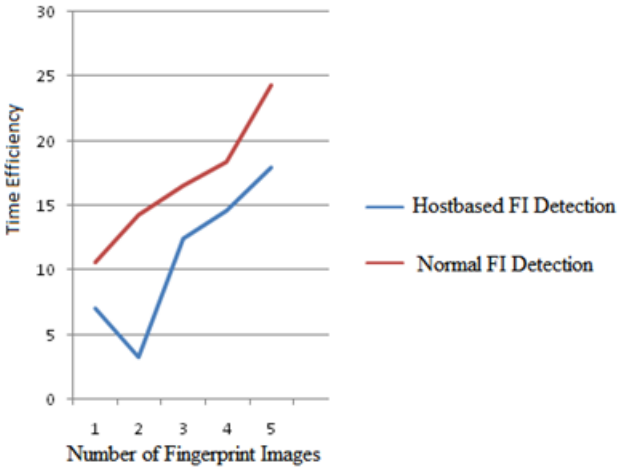


Figure 6. Time comparison results of both normal FI detection and biometric oriented detection.

5. Conclusion

The issue of determination of an ideal calculation for unique mark coordination keeping in mind the end goal to plan a framework that matches the desires in execution and exactness is of awesome worry to fashioners. It is fundamental to first get it the fundamental structural engineering of a bio-metric based security framework and after that continue onto figuring out how a run of the mill unique finger impression validation framework works. Keeping in mind the end goal is to accomplish fancied precision and framework execution, it is vital to completely see all particulars and afterward actualize a mix of existing calculations.

6. References

1. Ahmed AAE, Traore I. Detecting computer intrusions using behavioral biometrics. Third Annual Conference on Privacy, Security and Trust; St. Andrews, New Brunswick, Canada. 2005 Oct 12-14. p. 91–8.
2. Ahmed AAE, Traore I. A new biometric technology based on mouse dynamics. Transactions on Dependable and Secure Computing. 2007 Jul-Sep; 4(3):165–79.
3. Challita K, Farhat H, Khaldi K. Biometric authentication for intrusion detection systems. Proceedings in 2010 First International Conference on Integrated Intelligent Computing; Bangalore. 2010 Aug 5-7. p. 195–9.
4. Subha M. Vanithaasri S. A study on authenticated admittance of ATM clients using biometric based cryptosystem. International Journal of Advances in Engineering and Technology. 2012 Sep; 4(2):456–63.
5. Aru OE, Gozie I. Facial verification technology for use in ATM transactions. AJER. 2013; 2(5):188–93.
6. Onyesolu MO, Ezeani IM. ATM security using Fingerprint Biometric Identifier: An investigative study. International Journal of Advanced Computer Science and Applications. 2012; 3(4):68–72.
7. Lawan AM. Use of biometrics to tackle ATM fraud. International Conference on Business and Economics Research. Kuala Lumpur, Malaysia: IACSIT Press; 2011; 1:331–5.
8. Prithika M, Rajalakshmi P. Credit card duplication and crime prevention using biometrics. IOSR Journal of Computer Engineering (IOSR-JCE). 2013 Mar-Apr; 10(1):1–7.
9. Senapati RK, Pati UC, Mahapatra KK. A reduced memory, low complexity embeded image coding algorithm using hierarchical listless DTT. IET Image Processing. 2014; 8(4):213–38.
10. Shankar TN, Sahoo G, Niranjan S. Using the digital signature of a fingerprint by an elliptic curve cryptosystem for enhanced authentication. Information Security Journal., A Global Perspective, Taylor and Francis. 2012; 21(5):243–55.
11. Spurthy, et al. Intrusion-detection system in Manets with Elgamal digital signature. Far East Journal of Electronics and Communications. 2016; 16(2):40–54.
12. Kangra M, Kant C. Biometric system and its challenges. International Journal of Advanced Research in Computer Science and Software Engineering. 2015 Jun; 5(6):710–6.