Dermatological Disorder a Hindrance for Biometric Fingerprint Authentication

T. Rudra, Member IEEE, D. Tien, Member IEEE, G. Sahoo

Abstract: This paper raises one of the critical issues in using fingerprint impression in biometric scanners for identity authentication. Human fingerprints can be used in numerous identity verification and authentication applications ranging from airport security check to credit card purchases. The authors of this paper believe that it is vital for fingerprint scanning biometric devices to cater for seasonal dermatological changes in a large number of individuals across the world.

Index Terms – Biometric encryption, dermatology, minutiae.

I INTRODUCTION

Biometrics is the study to identify or verify the identity of an individual using the measurable physical or psychological characteristics or behavioral traits. The biometric characteristics being used for automatic recognition are fingerprints, face, voice, iris, retina, keystroke and signature. Epidermolysis bullosa simplex (EBS) is an inherited skin disorder caused by mutations in keratins K5 (keratin 5) and K14 (keratin 14), with fragility of basal keratinocytes leading to epidermal cytolyis and blistering [1]. There is also a large population suffering with dermatitis and genodermatosis and some of them can be seasonal.

When Jonathan Larsen, CEO and Country manager of Citibank Singapore said in the end of 2006 that Citibank is launching a biometric payment solution to replace credit cards, the world was anxious to see the success of the operations. Biometric ATMs are already in use in Colombia and a few locations in Japan, but haven't caught on in much of the rest of the world.

As a pilot program, India is testing 15 biometric ATMs at village kiosks in five districts across southern India [2]. The machines will have fingerprint scanners, rather than ATM cards and PIN’s, authenticate users. Owing to the demand of 75% of its customer who cannot sign their names, Banco Azteca, the Latin American bank based in Mexico City, has introduced fingerprint and PIN based banking to its customers [3].

The paper is organized as follows; in the second section we explain the process of biometric encryption. In the third section, we list the advantages of biometric encryption. In the fourth section we present the process of fingerprint authentication. In the fifth section we list some of the applications of fingerprint biometric devices. Finally we present the conclusion.

II BIOMETRIC ENCRYPTION PROCESS

The process of biometric encryption is shown in figure 1. It consists of two major parts – biometric enrolment and biometric verification.

Biometric verification consists of the following steps:

1. The sensor scans the biometric image (fingerprint, iris, face etc).
2. A random biometric encryption (BE) private key is generated by the key generator and bound with the scanned image by a binding algorithm.
3. The binding algorithm creates a BE template and a storage for the BE template.
4. The key enters an application, such as a Public Key Infrastructure (PKI). Each application has its unique key.
5. The biometric image is discarded at the end of the verification process.

Mr. T. Rudra is with the Department of Computing, Macquarie University, Sydney - 2109, Australia.

Dr. D. Tien is with the School of Accounting and Computer Science, Charles Sturt University, Bathurst - 2795, Australia.

Professor G. Sahoo is the head of the Department of Computer Science, B.I.T. Mesra - 835215, Ranchi, Jharkhand, India.

III ADVANTAGES OF BIOMETRIC ENCRYPTION

The advantages of biometric encryption are given as follows [4]:

1. No retention of the biometric image or template – BE does not store any personally identifiable information (PII) to the fullest extent possible thus eliminating the possibility of subsequent abuse.

2. Multiple/cancelable/revocable identifiers - Biometric Encryption allows individuals to use a single biometric for multiple accounts and purposes without fear that these separate identifiers or applications will be linked together by a single biometric image or template. Thus, if a single account identifier becomes compromised, there is a lesser risk that all the other accounts will also be compromised.

3. Improved authentication security - stronger binding of user biometric and identifier Account identifiers are bound with the biometric and recomputed directly from it on verification. This results in much stronger account identifiers or passwords which are –
   a) Longer, more complex identifiers.
   b) No need for user memorization.
c) Less susceptible to security attacks.

4. Improved security of personal data and communications.

5. Suitable for large-scale applications – BE can not only be used for verification or identifications but also for large scale authentication. Advantage Systems Solutions [5], have successfully completed the largest trials of biometric technology with face, iris, fingerprint, palm vein recognition technologies for British Airports Authority (BAA) in Heathrow airport, London.

IV FINGERPRINT AUTHENTICATION

Fingerprints for BE has a False Reject Rate (FRR) greater than 10% and are more prone to distortions that degrade accuracy in verification than iris. It is more complex to account for those factors in the case of biometric encryption, since BE works in a “blind” mode, and the enrolled fingerprint or its minutiae template are not seen. There are several ways to overcome this problem, for example, by using a free air or contact less fingerprint sensor, or by using more than one finger from the same person or by combining several biometrics or multi-modal technique.

Fingerprint authentication is considered to be the oldest and most reliable biometric authentication technique. Due to its uniqueness and immutability, fingerprints have been used in different legal and financial applications for decades as a substitute for hand written signatures for illiterate masses across the world.

The surface of our fingers is made of a series of ridges, furrows and minutiae points [6]. A minutiae point is local ridge characteristics that occur at either a ridge bifurcation or a ridge ending.

The process of fingerprint authentication is preceded by fingerprint scanning. There are two methods used in fingerprint scanning [6]:

1. Optical method – It starts with the visual image of the finger.
2. Semiconductor-generated electric field to image a finger.

There are two types of fingerprint matching techniques: minutiae-based and correlation based [7].

1. Minutiae-based techniques first find minutiae points and then map their relative placement on the finger. The disadvantages of this approach are, it is difficult to extract the minutiae points accurately when the fingerprint is of low quality and this method skips the global pattern of ridges and furrows.
2. The correlation-based method can overcome some of the shortcoming of minutiae-based approach; however it requires the precise location of a registration point and is affected by image translation and rotation.

Although these techniques can be used in multiple applications like laptop security, office entry etc, we cannot use it for financial transactions (ATMs) without human interventions. The reason being genodermatosis, where skin in the fingers can peel off with seasonal variations. There can be a temporary minor change in friction ridge of fingers due to accidents. In our research we will use state of the art biometric hardware to pursue our goal to implement a software solution to interpolate and extrapolate the minutiae points of the fingers with zero False Acceptance Rate (FAR) for use in fingerprint-biometric credit card applications.

V APPLICATION OF BIOMETRIC DEVICES

As no technology is full proof there are some security issues with biometrics technology too [4]. But the application of biometrics has started to emerge in a big way. Some of the application of this technology is listed below:

1. Secure border management [8].
2. Credit/cheque/savings card replacement.
3. Network/PC login security [9].
4. Web page security [9].
5. Employee Recognition [9].
6. Time and Attendance Systems [9].
7. Voting Solutions [9].
8. People surveillance for law enforcement [10].

VI CONCLUSION

Although all technology is fraught with drawbacks, false matching associated with non-live or fake (made of latex) fingers can be detected with sensors that capture
temperature, blood-oxygen level, pulse, blood flow, humidity or skin conductivity. The sensors can be integrated within the system for maximum accuracy in verification and authentication. Our research will endeavor to reduce False Rejection Rate (FRR) with zero percent tolerance for FAR for use in high risk fingerprint related biometric applications.

REFERENCES


