



STUDY ON THE DISEASES AND DEFORMITIES CAUSING FALSE REJECTIONS FOR FINGERPRINT AUTHENTICATION

S.Rajarajan, S.Palanivel, K.R.Sekar, S.Arunkumar
School of Computing, SASTRA Deemed University, India.

ABSTRACT

Proper authentication of users is crucial for several applications. Traditional knowledge based authentication schemes of passwords and PIN numbers have been widely used. An alternative to knowledge based schemes is the biometric schemes that are based on the physiological characteristics. They alleviate the memory load of the users by just utilizing their unique physical attributes. Among the variety of biometric schemes fingerprints is the most popular and widely used scheme. Biometrics suffers from the issue of false rejections or false negative identifications. The actual user may get rejected during authentication process because of variations between the enrolled biometric sample and the sample taken at the time of authentication. This variation could be temporary or permanent. Certain biometric schemes are more prone to false rejections than others. The objective of this paper is to conduct a study on the possible conditions that could cause false rejections of fingerprint authentication and the possible measures to mitigate that.

Keywords: Fingerprint, Biometrics, Fingerprints, False rejection, Minutiae, Finger Ridge

1. INTRODUCTION

There are numerous applications demanding the verification of users to ensure that they are indeed the registered users. This is required to prevent impersonation of the actual users by attackers [1]. The common practice is to expect the users to possess some proof which only the system and the user has got. At the time of authentication users are asked to provide the secret proof and system will attempt to match it against the stored copy in its repository. Ever since the advent of computer based systems a combination of user id and password has been generally used as the authentication data. A password is a alphanumeric string made of alphabets, numbers and special characters [2]. The user is required to remember his password to produce it whenever he try to enter into his area. But the primary problem with passwords is that they are susceptible to various attacks. The usual attacks against passwords are guessing attacks, dictionary attacks, shoulder surfing attacks, brute force attacks and social keylogging attacks. To defend against attacks more stringent rules have been followed for the selection passwords. This leads to difficult to remember passwords. Besides the common memorability issue with passwords there are also specific medical conditions that affect the remembrance of passwords. The following are common ailments that diminish people's ability to remember their passwords.

- **Dementia** – It is a common term used to describe a variety of conditions that cause the degradation in the capability to remember and recall.
- **Alzheimer's disease** – It is one of the widely prevalent condition that affects millions of aged people across the world. It is a progressive condition that

slowly erodes the brain memory power. The condition may lead to people forgetting the names of their family members.

- **Frontotemporal dementia** – This condition primarily affects the frontal or temporal lobes of a person. It is termed as a progressive neuron loss.
- **Mild cognitive impairment** – This is more of an initial stage of a full fledged dementia. People in this condition will experience declined ability to use their memory.
- **Alcoholism** – Addiction to the consumption of alcohol could cause several ailments in the body. Sometimes chronic alcoholism could affect the memory of the person.
- **Brain diseases** – There could other diseases on the brain such a tumor, infection, brain injuries that could impair the user's memory.

There are also numerous other reasons for the memory of a person to get affected leading to difficulty in remembering the passwords. Restoring the ability to remember passwords requires that the person get treated for the underling condition. But certain conditions are irreversible and deteriorate further over a period. So other forms of authentication mechanisms that do not require the memory usage of the users are needed. Biometrics is popular choice because of its zero requirement of memory.

2. BIOMETRICS AUTHENTICATION

Every individual human being is born with lot of unique physical attributes. It is possible to recognize and distinguish individuals based on these physiological attributes. Biometrics is a collection of authentication schemes that are based on a number of unique identities of people that are distinctive, recordable and measurable. The major advantage of biometric schemes is that users could provide them without consciously remembering anything. They are also relatively harder to break through spoofing attacks. There are plenty of options available under biometric authentication schemes. Each has its merits and demerits. There are companies with biometric products specifically based on any one of these options. But multi-modal biometrics based on a combination of more than one physical feature is more popular due to its better accuracy in identification [3]. Some of the options are contactless meaning that they do not require the physical contact of the users with the sensing device to collect their biometric sample. Contactless schemes are desired more due to inconveniences, restrictions and cultural obstacles involved in physically touching the devices. For example in health care sector touching directly is not preferred due to the fear of infections or contagious diseases. The Table 1 summarizes the various types of biometrics with their merits and demerits. Fig 1. shows the model of a biometric authentication system.

Table 1: Various Biometric Options and their characteristics

Physical Part	Contact / Contactless	Characteristics
Fingerprint	Contact	Most common and highly reliable method. Widely adopted in mobile phones to unlock phones [4].
Finger vein	Contactless	Most promising option. Since the veins are inside the finger it is nearly impossible to replicate. [5]
Hand geometry	Contactless	A color photograph of a person's hand is taken and it is compared for a match against stored copy of photo. The shape, complexion and other measures are made use of for determining the identity. [6]
Face	Contactless	Comparatively weaker since it is easier to spoof. Requires some liveness detection scheme. Cheaper to integrate with mobile phones with cameras.
Ear	Contactless	Generally combined with face recognition. Unlike the face, ear goes through less changes through aging. [7]
Iris/Retina	Contactless	Strongest method since it is difficult to spoof. But expensive to implement.[8]
Signature	Contact	Rudimentary and weak. Easiest to spoof. Useful as an additional measure to verify.
Behavioral	Contactless	Useful for continuous authentication of mobile phone users, collection of user details is done without their knowledge.[9]
Voice	Contactless	More popular for authentications of transactions conducted over phones. [10]
Gait	Contactless	Authenticating a person based on his walking style is called gait authentication. But it is vulnerable to imitation attacks [11].

The performance of a biometric system is measured based on its rate of false positive identification (FPIR) and false negative identification (FNIR) [12]. When a wrong user's biometric found to be matching with the stored biometric sample it is termed as false positive identification. Whereas if a actual user's input is reported as mismatching against his stored template then it is a case of false negative identification. The relationship between FPIR and FNIR is described as $FPIR = 1 - (1 - FMR)^N$ where n indicates total number of users.

2.1 FINGERPRINT AUTHENTICATION SYSTEM

The usage of finger prints for identifying people has a long history. Several complicated crime cases have been resolved with the help of the finger prints of culprits collected from the crime sites. The basic characteristic of fingers that facilitate fingerprint based authentication is the presence of ridges on the skin over fingers. Finger ridges evolved over the years to permit humans to grip and hold objects [4]. They are unique for each person and do not change much as a person ages. Alterations to finger's ridges could be either temporary or permanent. The formation of friction ridges commences in the early stage of gestation. The ridges are associated with the skin layer of volar pads[13]. It's shape and size influences the pattern of the friction ridges on the fingers. A major advantage of fingerprints is that they persist over aging. There are four types of patterns identified on a fingerprint that are used to identify a person uniquely. They are namely arch type, left-loop, right-loop and tented arch type [14]. One of the widely used approaches of fingerprint representation is by using the minutiae. It is typically represented as (x,y,θ) where x and y indicate the position of minutiae and θ shows its direction. Fig 1. shows the four types of patterns.

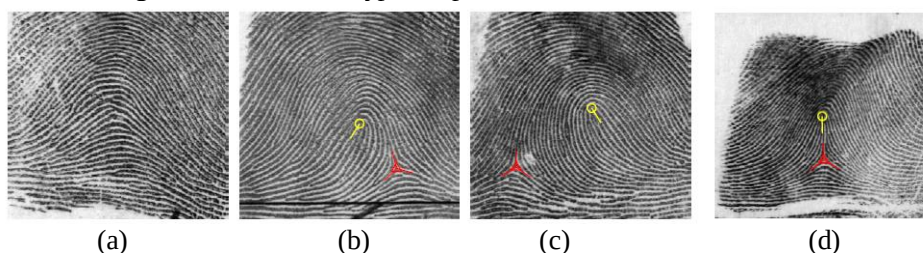


Fig. 1. (a). Fingerprint Patterns (a) Arch (b) Left-loop (c) Right-loop (d) tented-arch

A typical fingerprint authentication system comprise of a sensor, minutiae extractor, a database of fingerprints and a matching algorithm. Figure 2 presents the architecture of a fingerprint authentication system.

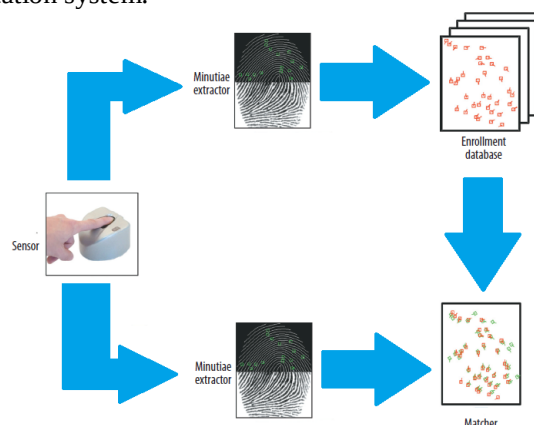


Fig 2. A typical Fingerprint Authentication System

2.2 CONDITIONS AFFECTING FINGERPRINT MATCHING

Tackling the issue of false rejections and false acceptance is a major goal for the researchers in the bio-metric domain. False rejections are not merely embarrassments to the users but they also cause inconveniences, frustrations and ultimately lack of trust in the system. So the biometric schemes have to be added with necessary measures to eliminate or curb the chances of false rejections due to slight or moderate physical changes occurring to the users. The superficial injuries occurring due to minor cuts, bruises scratches and swellings could temporarily affect the fingerprints but in few weeks the ridges will be restored with their original shape. But when the injuries on the finger are severe then it may permanently disable the fingerprint match. Besides the accidental injuries and wounds certain ailments might also hamper the proper identification through fingers. The disease conditions affecting the fingerprints are of two categories:

- Conditions that affect the skin over the fingers
- Conditions affecting the bone structure or shape of the fingers

When a skin disease affects the fingers it disrupts the ridges over the fingers disabling the person's ability to provide his fingerprints properly. It is either permanently affected or temporarily affected depending upon the type of disease. When a condition affects the structure or shape of the finger then it may not affect the ridges but disables the person to position his finger properly within the fingerprint sensor. When a physical alteration causes the failure of the authentication then it is termed as obliteration. Figure 2 presents a sample fingerprint with a physical injury affecting the finger pattern.



Fig 2. Fingerprint with an injury distorting the pattern of ridges

The following Table 2 is a summary of the most common conditions that commonly affect people across the world interfering with their usage of fingerprints.

Table 2: Summary of Common Conditions Affecting Fingerprints

		Diseases
Affected Fingers	Causes	Details
	Congenital Deformity	Unfortunately some children born with deformities or defects in their body. In the given example a person have born without proper growth of the fingers. There is no way such person could be enrolled for fingerprint authentication.
	Cellulitis	It is a type of bacterial infection. It affects the

		soft tissues on the deeper layers of the fingers. It could result in swelling, redness and sometimes pus forming. It generally responds to anti-biotic but if left untreated then the patient will have permanent swelling.
	Rattle snake bite	A snake bite injects a small volume of poison into the human body. If the snake bite happens on the finger then there could be swelling, redness and deformation of fingers might happen.
	Paronychia	This is also a type of infection but it is superficial. It affects the soft tissue on the skin around the fingernail. The fingers get swollen and become reddish. It could become oversized to place on the fingerprint reader.
	Rheumatoid Arthritis	It is a autoimmune disease affecting millions of people all over the world. This is a more serious and progressive disease. It causes permanent damage to the bone system. In its advanced stage people might not be able to use their fingers.
	Psoriasis	This is also a autoimmune disease causing patches on the skin and might lead to deformation of knee joints. There are several types of psoriasis varying on the area and severity of skin patches.
	Eczema	It is a itchy condition that causes patches on the affected region. It results in scaly, flaking and cracked skin.
	Dupuytren contracture	This is a genetically transmitted disorder. Generally affects people after they reach the age of 45. It results in progressive tightening of tissues in the palms. It eventually causes curling of the fingers disabling them to use their fingers properly.
	Leprosy	It is a chronic infectious disease caused by the bacterium Mycobacterium leprae. It is a contagious disease spread through cough or nose fluid. It may not immediately cause symptoms after infection.
	Blisters	It is a condition in which a region on the fingers

		is filled with fluid causing bulge of the region. . They are filled with serum, plasma or pus depending on the reason that caused. They usually contact and become normal in few days.
	Injured Finger	Generally injuries to fingers cause temporary disability to apply fingers for identification. But rarely severe injuries might result in permanent damage to ridges. Even in the case of minor scratches or cuts since the fingers are covered by blood and the bandage applied over that prevents the usage of fingers for some time.
	Burn Wounds	More number of people get burning injuries for a number reasons. Depending upon the severity of the injury it is classified into one to three degrees. Normally people who suffer from first degree burns get third fingers restored in few days or weeks. But with second to three degrees burns it result in permanent damage. Plastic surgeries may be carried out to restore the shape of the affected parts but it may not be possible to restore the exact finger ridges in this way.

Fig 2: Some of the deformities, diseases and injuries that incapacitate the fingerprint based biometric identification of a person

A large population people are free from these unfortunate conditions and are able to successfully subject themselves for fingerprint verification. But a small percentage of people are experiencing those hurdles that either temporarily or permanently affect their participation in fingerprint based authentications. Although it is only a small population that suffers still some measures are needed to rescue them.

3. MEASURES TO OVERCOME AUTHENTICATION FAILURE

Despite the limitations of biometrics they are becoming the gold standard for user authentication because they are user friendly, very difficult to spoof attack and are more reliable than knowledge based schemes. But an obstacle with biometrics is its demand for physical perfection users. A small deviation or variation might result in rejection of identity. In this section we are presenting some of the possible measures that could be employed to mitigate the chances of false rejections.

3.1 MULTI-MODEL BIOMETRICS

If fingerprint based authentication is the sole mechanism to authenticate and allow access to a user then a sudden disability due to any of the specified conditions denies the legitimate user entry into the system. To prevent such an embarrassing and humiliating situation nowadays a multi-model scheme combining more than one biometric scheme or

by combining password / PIN with fingerprint is widely preferred [15]. A single biometric field is less tolerable to noise in input due to physical changes. Whereas when multiple biometric schemes are used together it diminishes the error rate and thereby reducing the false rejections. Considering the security threats in storing different biometric data separately there is a way to bundle them together called fusion [16]. Y.J. Chin et. al. have proposed a multi-model biometric scheme that merges the fingerprint and palm print features to make a fusion of the two. Andrew Teoh Beng Jina et al.[17] have proposed a biohashing scheme in which fingerprint data is combined with a random number. Anil Jain et al. [18] have developed a score normalization scheme to integrate multiple biometrics at the score level to lessen the impact of one biometric on the final outcome. A multimodel biometric scheme by combining face, voice, and lip movement has been proposed by Frischholz et al.[6].

3.2 FINGERPRINT ENHANCEMENT ALGORITHMS

The success of the fingerprint matching may be increased with the help of good enhancement algorithms [19]. Usage of enhancement algorithm is vital for properly matching the minutiae since the structures of ridges are not clearly defined. So an enhancement algorithm is required to enhance the fingerprint image to clearly distinguish the minutiae. Gabor filter is one of the options suggested for this purpose [20]. A Fourier transform filter is used by analyzing local Fourier transforms by Pradenas et al. [21]. An approach that switch to isotropic smoothing when the ridge curvature grows high is proposed by Wang et al. [22]. A fast fingerprint enhancement algorithm that improves the clarity of ridge and valley structures was developed by Lin hong et al. [23]. The flow chart for their algorithm is shown in Figure 3.

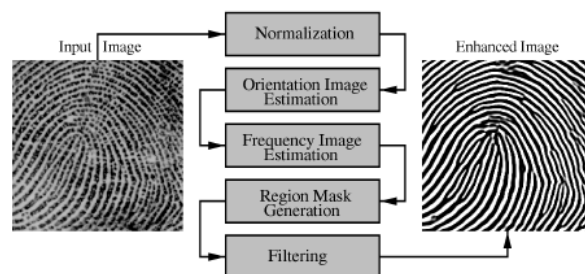


Fig 3. Flowchart of fingerprint enhancement algorithm [23]

3.3 NON-FINGERPRINT BIOMETRIC SCHEMES

Comparing to other biometric traits fingerprints are most vulnerable to physical damages that occur due to skin diseases, injuries and genetic disorders [24]. Unlike fingerprints, iris is less prone to changes. So these problems are overcome by replacing the fingerprint scheme by the usage of iris. But the cost of iris based authentication implementation is substantially higher over the fingerprint authentication. A promising option as an alternate for fingerprint is the finger vein based authentication. Because finger veins are

hidden inside the fingers they are immune against the skin disorders that generally affect the fingerprints [5].

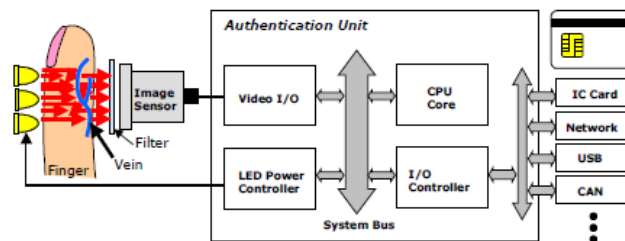


Fig 4. Finger-vein Authentication System [5]

4. CONCLUSION

The world is transforming from a knowledge based authentication to physical characteristic based biometric authentication. Already lot of smart phones come with the feature of fingerprint lock/unlock. A challenge to fingerprint authentication schemes will be the physical changes that people might undergo due to a variety of reasons. This results in false rejections of real users. This paper elaborately discussed the various conditions that could cause the deviation of fingerprints from their enrolled values and listed few possible solutions to counter their impact.

REFERENCES

- [1] Srinivasan, Rajarajan. "DragPIN: A Secured PIN Entry Scheme to Avert Attacks.
- [2] Rajarajan, S., et al. "Shoulder surfing resistant virtual keyboard for internet banking." *World Appl. Sci. J* 31.7 (2014): 1297-1304.
- [3] Gawande, Ujwalla, Mukesh Zaveri, and Avichal Kapur. "Multi-algorithmic approaches to iris recognition." *Biometric Technology Today* 2011.4 (2011): 8-10.
- [4] Banerjee, Salil P., and Damon L. Woodard. "Biometric authentication and identification using keystroke dynamics: A survey." *Journal of Pattern Recognition Research* 7.1 (2012): 116-139.
- [5] Hashimoto, Junichi. "Finger vein authentication technology and its future." *VLSI Circuits, 2006. Digest of Technical Papers. 2006 Symposium on*. IEEE, 2006.
- [6] Sanchez-Reillo, Raul, Carmen Sanchez-Avila, and Ana Gonzalez-Marcos. "Biometric identification through hand geometry measurements." *IEEE Transactions on pattern analysis and machine intelligence* 22.10 (2000): 1168-1171.
- [7] Abaza, Ayman, et al. "A survey on ear biometrics." *ACM computing surveys (CSUR)* 45.2 (2013): 22.
- [8] Burge, Mark J., and Kevin Bowyer, eds. *Handbook of iris recognition*. Springer Science & Business Media, 2013.
- [9] Yampolskiy, Roman V., and Venu Govindaraju. "Behavioural biometrics: a survey and classification." *International Journal of Biometrics* 1.1 (2008): 81-113.
- [10] Hasan, Md Rashidul, Mustafa Jamil, and M. G. R. M. S. Rahman. "Speaker identification using mel frequency cepstral coefficients." *variations* 1.4 (2004).

- [11] Gafurov, Davrondzhon, Kirsi Helkala, and Torkjel Søndrol. "Biometric Gait Authentication Using Accelerometer Sensor." *JCP* 1.7 (2006): 51-59.
- [12] Jain, Anil K., and Karthik Nandakumar. "Biometric Authentication: System Security and User Privacy." *IEEE Computer* 45.11 (2012): 87-92.
- [13] M. Kücken. Models for Fingerprint Pattern Formation. Forensic Science International, 171:85–96, 2007.
- [14] W. J. Herschel. The Origins of Finger-Printing. Oxford University Press, 1916.
- [15] He, Mingxing, et al. "Performance evaluation of score level fusion in multimodal biometric systems." *Pattern Recognition* 43.5 (2010): 1789-1800.
- [16] Chin, Yong Jian, et al. "Integrated biometrics template protection technique based on fingerprint and palmprint feature-level fusion." *Information Fusion* 18 (2014): 161-174.
- [17] Jin, Andrew Teoh Beng, David Ngo Chek Ling, and Alwyn Goh. "Biohashing: two factor authentication featuring fingerprint data and tokenised random number." *Pattern recognition* 37.11 (2004): 2245-2255.
- [18] Jain, Anil, Karthik Nandakumar, and Arun Ross. "Score normalization in multimodal biometric systems." *Pattern recognition* 38.12 (2005): 2270-2285.
- [19] Hong, Lin, and Anil Jain. "Fingerprint enhancement." *Automatic Fingerprint Recognition Systems*. Springer, New York, NY, 2004. 127-143.
- [20] L. Hong, Y. Wan, and A. Jain, "Fingerprint image enhancement: Algorithm and performance evaluation," *IEEE Trans. Pattern Anal. Machine Intell.*, vol. 20, pp. 777–789, Aug. 1998.
- [21] Pradenas, Richard. "Directional enhancement in the frequency domain of fingerprint images." *Human Detection and Positive Identification: Methods and Technologies*. Vol. 2932. International Society for Optics and Photonics, 1997.
- [22] Wang, Sen, and Yangsheng Wang. "Fingerprint enhancement in the singular point area." *IEEE signal processing letters* 11.1 (2004): 16-19.
- [23] Hong, Lin, Yifei Wan, and Anil Jain. "Fingerprint image enhancement: Algorithm and performance evaluation." *IEEE transactions on pattern analysis and machine intelligence* 20.8 (1998): 777-789.
- [24] Frischholz, Robert W., and Ulrich Dieckmann. "BiolD: a multimodal biometric identification system." *Computer* 33.2 (2000): 64-68.

