Asian Journal of Engineering and Technology Innovation

ISSN : 2347-7385

REVIEW ARTICLE

**Received on: 01-10-2014**
**Accepted on: 10-10-2014**
**Published on: 22-10-2014**

**Darshan Parate**
**Mansi Tanna**
**Kajal Singh**
Dr. D.Y.Patil Institute of Engg & Technology, Ambi
darshanparate@gmail.com
mtanna650@gmail.com
kskajalsingh5@gmail.com

**QR Code for Mobile users**

Conflict of Interest: None Declared

# Palm Authentication using Biometric Security Systems

**Darshan Parate, Mansi Tanna, Kajal Singh**
Dr. D.Y.Patil Institute of Engg & Technology, Ambi

**ABSTRACT**

With identity fraud in our society reaching unprecedented proportions and with an increasing emphasis on the emerging automatic personal identification applications, biometric-base verification, especially Palm-base identification, is receiving lot of attention. There are two major short coming of the traditional approaches to Palm represntation. The widely used minutiae-base representation does not utilize a significant component of the rich discriminatory information available in the Palm. Local ridg structures cannot be completely characterized by minutae. Further, minutae-based matching has difficulty in quickly matching two Palm image containing different number of unregistered minutiae points. The proposed filter base algorithm use a bank of Gabor filters to capture both local and global details in a Palm as a compact fixed length Finger Code. The Palm match is based on the Euclidean distance between the two corresponding FingerCodes and hence is fast. We are able to achieve a verification accuracy which is only marginally inferior to the best results of minutiae-based algorithms published in the open literature [1]. Our system performs better than a state-of-the-art minutiae-based system when the performance requirement of the application system does not demand a very low wrong acceptance rate. Finally, we show this the matching performance can be improved by combining the decisions of the matchers based on complementary (minutiae-based and filter-based) Palm information.

**Keywords:** Finger codes, palm, biometric, verification, bio-security.

**Cite this article as:**
Darshan R parate, Maryam Mounesi, Palm Authentication using Biometric Security Systems. Asian Journal of Engineering and Technology Innovation 02 (05); 2014; 10-13.

**INTRODUCTION**

The term biometrics comes from the Greek words bios and metrics, meaning measure Biometrics can be defined as a measurable physiological and/or behavioral characteristics that can be utilized to verify the identity of an individual, and include Palm verification, retina scanning, iri scanning, face recognition and sign verification . Biometric authentication is considered the automatic identify, or identification verification, of an individual is done by either a biological feature they possess physiological characteristic like a Palm or something they do behavior characteristic, which is like a signature . In practice, the process identification and authentication is the ability to verify and gives a confirmation to an identity. It is a accomplished by using any one or a combination of the following three traditional identification techniques: something you possess; something you know; or something you are

1. Something you possess: often referred to as a token and can be produced from a multitude of different physical objects. There are two basic types of token in use today: manual and automated. If token is described as manual it means that the verification process requires some form of human intervention; in other words, a person will make the last decision of whether an identity is approved or not. Good examples of manual tokens are paper ID documents and passport. Automated tokens, on the next hand, do not involve human intervention the in identification process, but rather the identity is a verified by a system such as magnetic-stripe cards, memory cards, or smart cards .
2. Something you know: the knowledge should not be commonly hold, but secret. Examples of regularly used secrets are passwords, pass-keywords, and personal identification numbers PINs.
3. Something you are: recognizing an entity through what "they are" requires measuring one or more of their biological feature. Biological feature can be either physiological characteristics like Palms or behavioral traits like an individual's signature.

**Why are biometrics secure?**

• Unique: The various biometrics systems have been developed around unique characteristics of individual. The probability of 2 people sharing the same biometric data is virtually nil.
• Cannot be shared: Because biometric property is an intrinsic property of an individual, it is extremely difficult to duplicate or share (you cannot give a copy of your face or your hand to someone!).
• Cannot be copied: Biometric characteristic are nearly impossible to frog or spoof, especially with new technologies ensuring that the biometric being identified is from a live person.
• Cannot be lost: A biometric property of a individual can be lost only in case of serious accident.

Biometric characteristics be can separated into two main categories:

Physiological characteristics are related to the shape of body. The trait that has been used the longest, for over a hundred years, are Palms; other examples are face recognization, hand geometry and iri recognition.

Behavioral characteristics are related to the behavior of a person. The first characteristic be to used that is still widely used today is the signature.

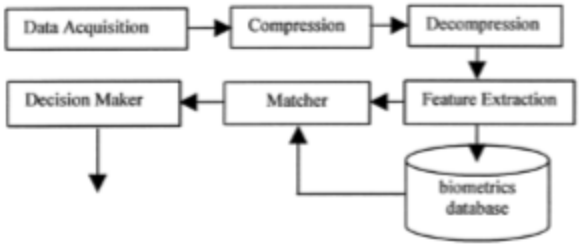


Figure 1 - A generic biometrics-based system.[1]

**Working:-**

The data acquisition component acquires the biometric data in digital format by using a sensor. The second and third components of the system are optional, based on the system's storage requirements. The fourth component employs a feature extraction algorithm to produce a feature vector whose components are numerical characterizations of the underlying biometrics. The fifth component of the system is the matcher which compares feature vectors to produce a score which indicates the degree of similarity between the pair of biometrics data under consideration. The sixth component of the system is a decision-maker that can be programmed to accommodate system specifications. System performance and accuracy is primarily determined by two parameters – FAR and FRR[7] . A genuine individual could be mistakenly recognized as an imposter. This scenario is referred to as "false reject" and the corresponding error rate is called the false reject rate (FRR); an imposter could be also mistakenly recognized as genuine. This scenario is referred to

as “false accept” and the corresponding error rate is called the false accept rate (FAR). FAR and FRR are widely used measurements in today’s commercial environment.

**Part to be used:-Palm biometrics**

Palm identification is one of the most well-known and publicized biometric. Because of there uniqueness and consistency ovre time, Palms have been used for identification for over a century, more recently becoming automate (i.e. a biometric) due to advancements in computing capabilities. Palm identification popular because of the inherent ease in acquisition, the numerous sources (ten fingers) available for collection, and there established use and collections by law enforcement and immigration.

Palms are made of a series of ridges and furrows on the surface of the finger and have a core around which patterns like swirl, loop, or arches are curved to ensure that each print is unique[3] . An arch is a pattern where the ridges enter from one side of the finger, rise in the center forming an arc, and then exit the next side of the finger. The loop is pattern where the ridges enter from one side of a finger, form curve, and tend to exit from the same side the enter. In the whorl pattern, ridges form circularly around a central point on the finger. The ridges and furrows are characterized by irregularities known as minite, the distinctive feature upon which finger scanning technologies are based. Minutiae points are local ridge characteristic that occur at either a ridge bifurcation or a ridg ending. The ridge ending is the point at which a ridg terminates. Bifurcations are points at which a single ridge splits into two ridgs. Minutiae and patterns are very important in the analysis of Palms since no two fingers have been shown to be identical. There are five stages involved in finger-scan verification and identification:

1. Palm Image Acquisition
2. Image Processing
3. Locating Distinctive Characteristics
4. Template Creation
5. Template Matching

A sensor takes a mathematical snapshot of the user's unique pattern, which is then helped in a Palm database. A Palm enhancement algorithm (that uses Gabor filters as band-pass filters to remove the noise and preserve true ridge/valley structures) is included in the minutiae extraction module to ensure that the performance of the system is not affected by variations in quality of Palm images.

The continuously changing direction of the ridges constitute an oriented texture possessing different spatial frequency, orientation, or phase; and hence, by decomposing the image in several spatial frequency and orientation channels Palms can be discriminated or matched.

**A. Feature Extraction**

Most Feature extraction algorithms function on the following four steps:-

1. Determine a reference point for the Palm image.
2. Tessellate the region around the reference point.
3. Filter the region of interest in different directions.
4. Define the feature vector.

**B. Palm Matching**

Palm matching refers to finding the similarity between two given Palm images. Due to noise and distortion introduced during Palm capture and the inexact nature of feature extraction, the fingerprnt representation often have missing, fake, or noisy features. Therefore, the matching algorithm should be immune to these error. The matched algorithm outputs a similarity value that indicates its confidence in the decision that the two images come from the same finger. The existing popular Palm matching techniques can be broadly classified into three categories depending on the types of features used:

1. Palm Image Acquisition
2. Image Processing
3. Locating Distinctive Characteristics
4. Template Creation
5. Template Matching

**CONCLUSIONS AND FUTURE WORKS**

Herein, a general and independent methodology has been implemented to assess the influence of usability factors in biometric performance. First, a common and controlled scenario was specified based on ISOIIEe 1 9795-2 and then, some modifications were defined (taking into account usability parameters to evaluate). After that, the methodology was validated with a Palm biometric system analyzing different usability aspects. Results have disclosed that this

methodology is feasible for carrying out independent and intercomparable tests and for quantifying usability effects. Nevertheless, this methodology cannot be checked with other modalities and there are usability parameters that could not be considered herein. Both issues are relevant and it is important to continue research in this area.

**REFERENCES**

1. Bolle R, Connell J, et al. Guide to Biometrics, Springer, 2003.
2. Jain LC, Intelligent Biometric Techniques in Palm and Face Recognition, CRC Press, 1999
3. Maltoni D, Jain AK, Maio D, Prabhakar S, Handbook of Palm Recognition, Springer, 2004
4. Vacca JR, Biometric Technologies and Verification Systems, Butterworth-Heinenmann, 2007
5. Munir MU, Javed MY; ''Palm Matching using Gabor Filters'', 2005
6. NTSC Subcommittee on Biometrics, ''Palm Recognition'', 2000
7. http://www.isc365.com/Biometrics_Security_Vs_Convenience.aspx
8. http://www.csse.uwa.edu.au/~pk/Research/MatlabFns
9. http://biometrics.cse.msu.edu/Palm.html