ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 1, Issue 8, October 2012

A Survey on Security in Palmprint Recognition: A Biometric Trait

Dhaneshwar Prasad Dewangan[1], Abhishek Pandey[2]

Abstract— **Biometric based authentication and recognition, the science of using physical or behavioral characteristic for identity verification is becoming a security principal in many areas. Their utilization as an authentication and recognition technology has become widespread from door access to electronic commerce. Security is a very important aspect in the biometric system itself. Biometric recognition system includes one of the biometric trait as palmprint, Palmprint recognition has been investigated over last fifteen years. During this period, many different problems related to palmprint recognition and securities in the system have been addressed. This paper provides an overview of palmprint research, describing in capture devices, preprocessing, verification, palmprint -related fusion and measures of security and for protecting users' privacy and palmprint system. Finally some conclusion and suggestion is offered.**

Keywords—**Biometrics, security, privacy, template protection**

1. INTRODUCTION

The inner surface of the palm normally contains three flexion creases, secondary creases and ridges. The flexion creases are also called principal lines and secondary creases are called wrinkles.

Palmprint research employs either high resolution or low resolution images. High resolution images are suitable for forensic applications such as criminal detection. Low resolution images are more suitable for commercial and civil application such as access control. Most of the research using palm print verification uses low resolution images [2]. In general the high resolution can be 400 dpi or more and low resolution can be 150 dpi or less. Figure 1 shows a part of a high resolution palmprint image and a low resolution palmprint image. One can extract ridges, singular points and minutia points as features from high resolution images while in low resolution images principal lines, wrinkles and textures can be extracted.

The design of a biometric system takes care of five objectives: cost, accuracy, computation speed, security and user acceptance and environment constraints (figure 2). Reducing accuracy can increase speed (example hierarchical approaches). Reducing user acceptance can improve accuracy. For instance, users are required to provide more samples for training. Increasing cost can enhance security. We can embed more sensors to collect different signals for liveness detection. In some applications, environmental constraints such as memory usage, power consumption, size of templates and size of devices have to be fulfilled. A biometric system installed in PDA (personal digital assistant) requires low power and memory consumption but these requirements may not be vital for biometric access control systems. A practical biometric system should balance all these aspects.

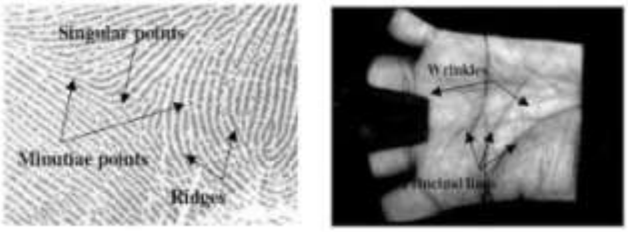

Figure 1: Palmprint features in

(a) a high resolution image and (b) a low resolution image.

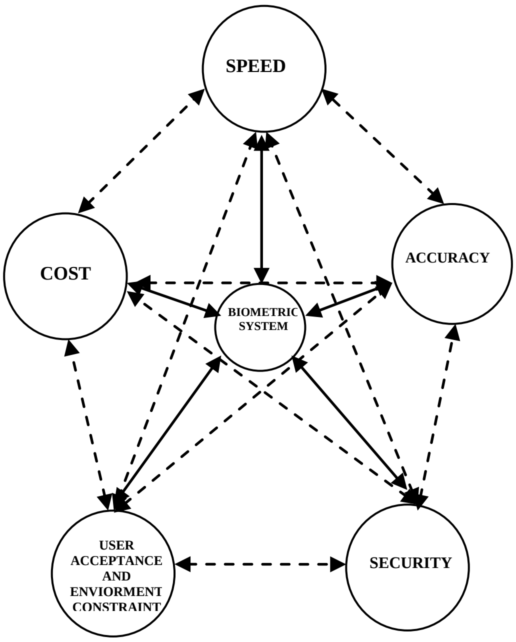

Figure 2: Key Objective of a Biometric system design [1]

A comparison of the biometric techniques (biometric traits) based on seven factors [3] is provided in Table1. Table1 shows the comparison of different biometric traits based on Universality, Distinctiveness, Permanence, Collectability, Performance, Acceptability, and Circumvention as Low, Medium and High.

Biometric identifier	**Universality**	**Distinctiveness**	**Permanence**	**Collectability**	**Performance**	**Acceptability**	**Circumvantion**
DNA	H	H	H	L	H	L	L
Ear	M	M	H	M	M	H	M
Face	H	L	M	H	L	H	H
Facial Thermogram	H	H	L	H	M	H	L
Fingerprint	M	H	H	M	H	M	M
Gait	M	L	L	H	L	H	M
Hand geometry	M	M	M	H	M	M	M
Hand vein	M	M	M	M	M	M	L
Iris	H	H	H	M	H	L	L
Keystroke	L	L	L	M	L	M	M
Odor	H	H	H	L	L	M	L
Palmprint	M	H	H	M	H	M	M
Retina	H	H	M	L	H	L	L
Signature	L	L	L	H	L	H	H
Voice	M	L	L	M	L	H	H

Table 1: Comparison of various biometric technologies based on the perception of the authors. High, Medium, and Low are denoted by H, M and L, respectively.

A palmprint recognition system generally consists of five parts: palmprint scanner, preprocessing, feature extraction, matcher and a database. Palmprint scanner is to collect palmprint images. Preprocessing is to setup a coordinate system to align palmprint images and to segment a part of palmprint image for feature extraction. Feature extraction obtains effective features from the preprocessed palmprints.

Finally, a matcher compares two palmprint features. All the images, templates generated are stored in a local or remote database.

The remaining section is organized as follows: Palmprint reviews and preprocessing algorithms are reviewed in Section 2. Verification algorithms are listed in Section 3. Various fusion approaches for enhancing verification accuracy are summarized in Section 4. The algorithms for real-time

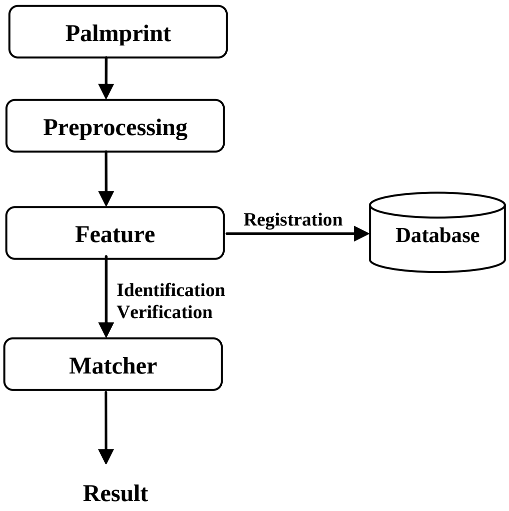

Figure 3: A Typical Biometric Recognition system

2. PALMPRINT SCANNERS AND PREPROCESSING

2.1 Palmprint Scanners

Researchers utilize four types of sensors: CCD-based palmprint scanners, digital cameras, digital scanners and video cameras to collect palmprint images. Figure 4 shows a CCD-based palmprint scanner developed by The Hong Kong Polytechnic University[1]. CCD-based palmprint scanners capture high quality palmprint images and align palms accurately because the scanners have pegs for guiding the placement of hands. These scanners simplify the development of recognition algorithms because the images are captured in a controlled environment.

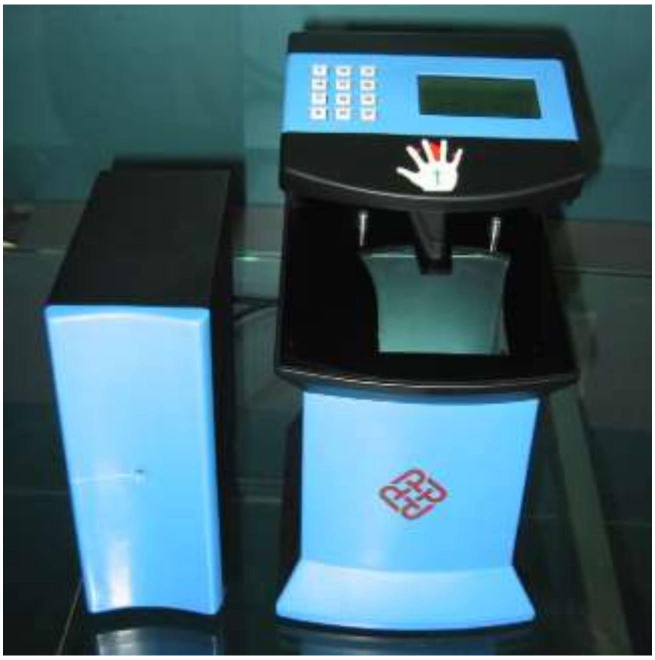

Figure 4: A CCD-based palmprint scanner [1]

Collection approaches based on digital scanners, digital cameras and video cameras require less effort for system design and can be found in office environments. These approaches do not use pegs for the placement of hands. Some researchers believe that this increases user acceptance.

Digital and video cameras can be used to collect palmprint images without contact, an advantage if hygiene is a concern. However, these images might cause recognition problem as their quality is low because they collect is in an uncontrolled environment with illumination variations and distortions due to hand movement. Digital scanners are not suitable for real-time applications because of the scanning time.

2.2 Preprocessing

Preprocessing is used to align different palmprint images and to segment the center for feature extraction. Most of the preprocessing algorithms employ the key points between fingers to set up a coordinate system. Preprocessing involves five common steps: (1) binarizing the palm images, (2) extracting the contour of hand and/or fingers, (3) detecting the key points, (4) establishing a coordination system and (5) extracting the central parts. Fig. 5(a) illustrates the key points and Fig. 5(b) shows a preprocessed image.

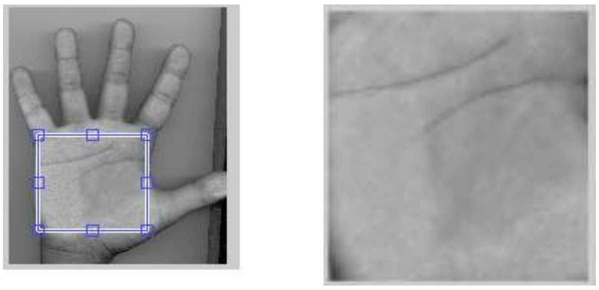

Figure 5: Illustration of Preprocessing (a) Keypoints on figure boundary (b) The central parts for feature extraction

The first and second steps in all the preprocessing algorithms are similar. However, the third step has several different implementations including tangent, bisector and finger-based to detect the key points between fingers. The tangent-based approach considers the two boundaries—one from point finger and middle finger and the other from ring finger and last finger—as two convex curves and computes the tangent of these two curves. The two intersections are considered as two key points for establishing the coordinate system. Tangent-based approaches have several advantages. They depend on a very short boundary around the bottom of fingers. Therefore, it is robust to incomplete and the presence of rings. Bisector-based approach constructs a line using two points, the center of gravity of a finger boundary and the midpoint of its start and end points. The intersection of the line and the finger boundary is considered a key point. Han and his team propose two approaches to establish the coordinate system, one based on the middle finger and the other based on the point, middle and ring fingers. The middle finger approach uses a wavelet to detect the fingertip and the middle point in the finger bottom and construct a line passing through these two points. The multiple finger approach uses a wavelet and a set of predefined boundary points on the three fingers to construct three lines in the middle of the three fingers. The two lines from point and ring fingers are used to set the orientation of the coordinate system and the line from the middle finger is used to set its position. These approaches use only the information on the boundaries of fingers.

After obtaining the coordinate systems, the central parts of palmprints are segmented. Most of the preprocessing algorithms segment square regions for feature extraction but some of them segment circular and half elliptical regions. The square region is easier for handling translation variation, while the circular and half elliptical regions may be easier for handling rotation variation.

3. VERIFICATION

Once the central part is segmented, features can be extracted for matching. There are two types of recognition- verification and identification. Verification algorithms must be accurate. Identification algorithms must be accurate and fast (matching speed). This section concentrates on verification algorithms and identification algorithm. Verification algorithms are line, subspace and statistic based. Some algorithms in this section can support a certain scale of identification.

3.1 Line-Based Approaches

Line-based approaches either develop edge detectors or use existing edge detection methods to extract palm lines. These lines are either matched directly or represented in other formats for matching.

3.2 Subspace-based approaches

Subspace-based approaches also called appearance-based approach in the literature of face recognition. They use principal component analysis (PCA), linear discriminant analysis (LDA) and independent component analysis (ICA). The subspace coefficients are regarded as features. Various distance measures and classifiers are used to compare the features. In addition to applying PCA, LDA and ICA directly to palmprint images, researchers also employ wavelets, Gabor, discrete cosine transform (DCT) and kernels in their methods. Generally speaking, subspace-based approaches do not make use of any prior knowledge of palmprints.

3.3 Statistical approaches

Statistical approaches are either local or global statistical approaches. Local statistical approaches transform images into another domain and then divide the transformed images into several small regions. Local statistics such as means and variances of each small region are calculated and regarded as features. Gabor, wavelets and Fourier transforms have been applied. The small regions are commonly square but some are elliptical and circular. To our knowledge, no one has yet investigated high order statistics for these approaches.

3.4 Other approaches

Some approaches are difficult to classify because they combine several image-processing methods to extract palmprint features and employ some standard classifiers such as neural networks to make the final decision.

4. FUSION

Fusion is a promising approach that may increase the accuracy of systems. Many biometric traits including fingerprint, palm vein, finger surface, face, iris, and hand shape have been combined with palmprints at score level or at representation level. Combining other hand features such as hand geometry and finger surface with palmprints allows these features and palmprints to be extracted from a single hand image. Only one sensor is needed. Researchers have examined various fusion rules including sum, maximum, average, minimum, SVM and neural networks. Researchers also fuse features including appearance-based, line and texture features from palmprints. Although fusion increases accuracy, it generally increases computation costs and template sizes and reduces user acceptance.

5. IDENTIFICATION IN LARGE DATABASES

5.1 Classification and hierarchical approaches

The problem of real-time identification in large databases has been addressed in three ways: through hierarchies, classification and coding. Hierarchical approaches employ simple but computationally effective features to retrieve a sub-set of templates in a given database for further comparison. These approaches increase matching speed at the cost of accuracy. Classifiers can remove target palmprints by using simple features. Classification approaches assign a class to each palmprint in a database.

5.2 Coding approaches

Coding approaches use one matching function to search entire databases. This avoids introducing errors from the classification or hierarchical systems but it is difficult to identify effective features for the matching function. Several coding algorithms have been proposed for palmprint identification. Palm Code always generates highly correlated features from different palms.

6. SECURITY AND PRIVACY

The biometric system work well if the verifier can verify two things:

- The biometric come from the genuine person at the time of verification.
- The biometric matches the master biometric on file.

But a variety of problems hinder the ability to verify the above[4].

- Noise in acquired data – Noisy biometric data caused by

defective sensors, defective physical characteristics and unfavorable ambient conditions. This causes the data to be incorrectly matched or incorrectly rejected.

- Intra-class variations – The data acquired during

authentication may be different from the data used to generate the template during enrollment, affecting the matching process.

- Distinctiveness – Every biometric trait has an upper

bound in terms of its discrimination capabilities.

- Non-universality – A subset of the users not possessing

a particular biometric.

The above-mentioned problems form the basis for many types of attacks against biometric systems.
There are 8 points in a generic biometric system which can be attacked [5].

6.1 Attacking the Sensor

In this type of attack a fake biometric such as a fake palm or image of the palm is presented at the sensor.

6.2 Resubmitting Previously Stored Digitized Biometric Signals

In this mode of attack a recorded signal is replayed to the system by passing to the sensor.

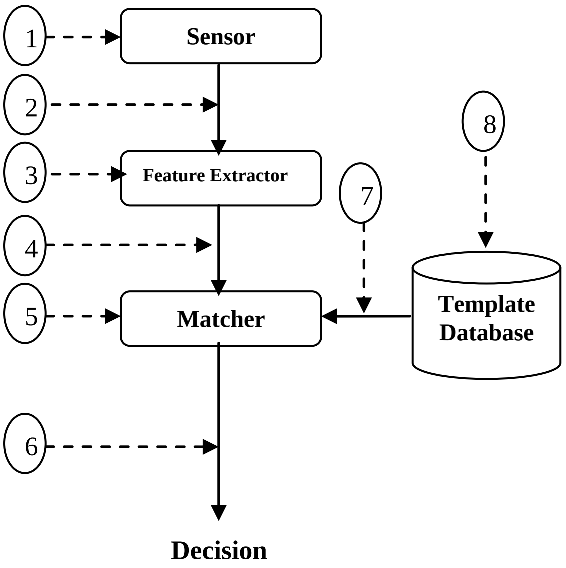

Figure 6: Attack points in a Biometric system

6.3 Overriding the Feature Extractor

The feature extractor is forced to produce feature sets chosen by the attacker, instead of the actual values generated from the data obtained from the sensor.

6.4 Tampering With the Biometric Feature Representation

The features extracted using the data obtained from the sensor is replaced with a different fraudulent feature set.

6.5 Corrupting the Matcher

The matcher component is attacked to produce pre-selected match scores regardless of the input feature set.

6.6 Tampering With the Stored Templates

Modifying one or more templates in the database, which could result either in authorizing a fraud or denying service to the person, associated with the corrupted template? A smart card based system where the template is stored in the smart card is also vulnerable to this form of attack.

6.7 Attacking the Channel between the Stored Template and the Matcher

Data travelling from the stored template to the matcher is intercepted and modified in this form of attack.

6.8 Overriding the Final Decision

Here the final match decision is overridden by the hacker disabling the entire authentication system.

Biometric systems are vulnerable to many attacks including replay, database and brute-force attacks. Compared with verification, fusion and identification, there has been little research on palmprint security. Biometric traits contain information not only for personal identification but also for other applications. For example, deoxyribonucleic acid (DNA) and retina can be used to diagnose diseases. Palmprints can also indicate genetic disorders. To protect private information in palmprints, databases store encrypted templates because the line features can be reconstructed from raw templates.

7. DISCUSSION AND CONCLUSION

Before the end of this paper, we would like to re-mention some papers that are very worthy to read carefully. Our first suggestion is Han's work [6], which is a very complete work. We especially appreciate his palmprint scanner described in this work that can collect images of whole hands and use pegs for hand placement. For verification, we recommend relation filter approach. For real-time large database identification, PalmCode, Fusion Code and Competitive Code and the theory of coding methods will be more suitable. Biometric fusion is in fact an application of information fusion and combined classifiers. Many excellent papers have been published in these two fields security, we also do not emphasize on any paper because the literature of palmprint security is very small. In face recognition literature, many researchers design algorithms based on prior knowledge of the face. To optimize the recognition performance in terms of speed and accuracy, we expect that more algorithms are designed based on the prior knowledge of palmprints. Different template formats may require different measures for tem- plate protection. More research should be put into security and privacy issues. For biometric fusion, the authors recommend combining Iris Code—the commercial iris recognition algorithm and Competitive Code or other coding methods for high-speed large-scale personal identification because these algorithms share a number of important properties (e.g. high speed matching). Even though Iris Code does not accumulate false acceptance rates when the number templates in database increases, its false reject rate still increases. Some issues in using palmprints for personal identification have not been well addressed. For instance, we know that ridges in palmprints are stable for a person's whole life but the stability of principal lines and wrinkles has not been systemically investigated

REFERENCES

[1] Adams Kong[a],* ,DavidZhang[b], MohamedKamel[c] , ,"*A survey of palmprint recognition*", Pattern Recognition 42 (January, 2009 Elsevier) 1408 – 1418.

[2] W. K. Kong, D. Zhang, "*Palmprint texture analysis based on low-resolution images for personal authentication",* in: Proceedings of 16th International Conference on Pattern Recognition, vol. 3, 2002, pp. 807–810.

[3] Anil K. Jain, Arun Ross and Salil Prabhakar. "*An Introduction to Biometric Recognition*", Appeared in IEEE Transactions on Circuits and Systems for Video Technology, Special Issue on Image- and Video-Based Biometrics, Vol. 14, No. 1, January 2004.

[4] Matyas, V and Riha, Z, "*Toward reliable user authentication through biometrics*," Security & Privacy Magazine,IEEE, Volume: 1, Issue: 3, May-June 2003.

[5] Ratha, N.K., J.H. Connell, and R.M. Bolle, *"Enhancing security and privacy in biometrics-based authentication system"*, IBM Systems Journal, vol. 40, no. 3.

[6] C.C. Han, "*A hand-based personal authentication using a coarse-to-fine strategy*", Image and Vision Computing 22 (11) (2004) 909–918.

Author :

1. **Dhaneshwar Prasad Dewangan,**
MTech (Information Security), Mtech Scholar in C.S.E. Department from Disha Institute of Management and Technology, Raipur Chhattisgarh Under the CSVTU University. Received MCA from CSVTU Univesity, Bhilai.

Address: DIMAT, VIDHANSABHA, CHANDKHURI MARG, RAIPUR, CHHATTISGARH

2. **Mr. Abhishek Pandey,**
Assistant Professor, C.S.E. Department, Disha Institute of Management and Technology, Raipur. He Received his BE (CSE), and MTech (CSE) from NIT, Rourkela, His Interests are Digital Image Processing, MANET, Data Mining.

Address: DIMAT, VIDHANSABHA, CHANDKHURI MARG, RAIPUR (C.G.), PH 0771-4231000, FAX: 0771-4200110