International Journal of Electronics and Electical Engineering

Volume 1 | Issue 3 Article 8

January 2013

A Survey Paper on Palm Prints Based Biometric Authentication System

Swati Verma
CSIT Durg, C.G., INDIA, swatiiverma09@gmail.com

Pomona Mishra
CSIT Durg, C.G., INDIA, poonampandey@csitdurg.in

Recommended Citation

Verma, Swati and Mishra, Pomona (2013) "A Survey Paper on Palm Prints Based Biometric Authentication System," *International Journal of Electronics and Electical Engineering*: Vol. 1 : Iss. 3 , Article 8.
DOI: 10.47893/IJEEE.2013.1037
Available at: https://www.interscience.in/ijeee/vol1/iss3/8

A Survey Paper on Palm Prints Based Biometric Authentication System

Swati Verma & Pomona Mishra

CSIT Durg, C.G., INDIA
E-mail : swatiiverma09@gmail.com , poonampandey@csitdurg.in

Abstract **-** In this paper we are providing an approach for authentication using palm prints. Reliability in computer aided personal authentication is becoming increasingly important in the information-based world, for effective security system. Biometrics is physiological characteristics of human beings, unique for every individual that are usually time invariant and easy to acquire. Palm print is one of the relatively new physiological biometrics due to its stable and unique characteristics. The rich information of palm print offers one of the powerful means in personal recognition.

Keywords **-** *Palm prints, Security system, authentication, CCD.*

I. INTRODUCTION

It is basically a pattern-recognition system that is used to identify or verify users based on his on her unique physical characteristics. Biometric systems offer several advantages over traditional authentication methods. Biometric information cannot be acquired by direct covert observation. It is impossible to share and difficult to reproduce. It enhances user convenience by alleviating the need to memorize long and random passwords. It protects against repudiation by the user. Biometrics provides the same level of security to all users unlike passwords and is highly resistant to brute force attacks. Moreover, biometrics is one of the few techniques that can be used for negative recognition where the system determines whether the person is who he or she denies to be. Using biometrics with password protected smart cards introduces all three factors of authentication simultaneously (something you know, something you have and something you are).

1.1 Basic structure of a biometric system

Every biometric system consists of four basic modules:

1.1.1 Enrollment Unit

The enrollment module registers individuals into the biometric system database. During this phase, a biometric reader scans the individual's biometric characteristic to produce its digital representation.

1.1.2 Feature Extraction Unit

Module processes the input sample to generate a compact representation called the template, which is then stored in a central database or a smartcard issued to the individual.

1.1.3 Matching Unit

This module compares the current input with the template. If the system performs identity verification, it compares the new characteristics to the user's master template and produces a score or match value (one to one matching). A system performing identification matches the new characteristics against the master templates of many users resulting in multiple match values (one to many matching).

1.1.4 Decision Maker

This module accepts or rejects the user based on a security threshold and matching score.

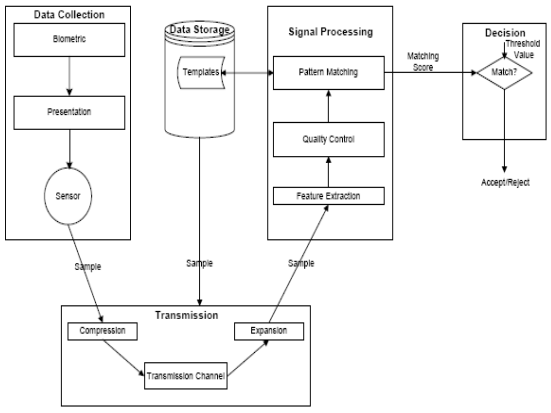


Fig. 1: Basic Structure of a Biometric Authentication System.

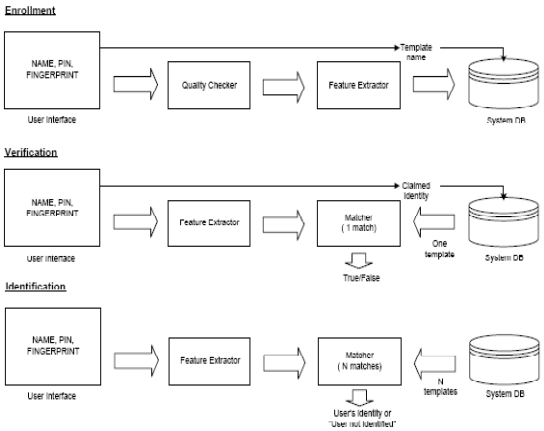


Fig. 2 : Enrollment, Identification and Verification in a Biometric System.

Biometric based personal identification is getting wide acceptance in the networked society, replacing passwords and keys due to its reliability, uniqueness and the ever increasing demand of security. Palm print is a new biometric modality which can be used for authentication of a person's identity because of its richness. Palm print not only has the information available on the fingerprint but it has far more amount of details in terms of principal lines, wrinkles and creases. Moreover it can easily be combined with hand shape biometric so as to form a highly accurate and reliable biometric based personal identification system. This type of identification has become an increasingly active research topic over the years. It has been analyzed for discriminating features like principal lines [1], geometry and texture [2].

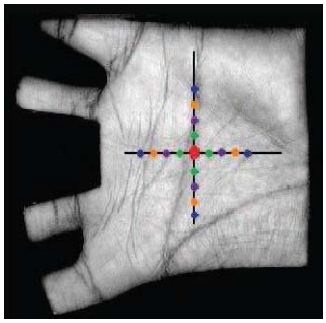


Fig. 3 : Palm with Master and Slave points

The inner surface of the palm normally contains three flexion creases, secondary creases and ridges. The flexion creases are also called principal lines and the secondary creases are called wrinkles. The flexion and the major secondary creases are formed between the 3rd and 5th months of pregnancy [6] and superficial lines appear after we born. Although the three major flexions are genetically dependent, most of other creases are not [2]. Even identical twins have different palm prints [2]. These non-genetically deterministic and complex patterns are very useful in personal identification. Human beings were interested in palm lines for fortune telling long time ago. Scientists know that palm lines are associated with some genetic diseases including Down syndrome, Aarskog syndrome, Cohen syndrome and fetal alcohol syndrome [18]. Palm print research employs either high resolution or low resolution images. High resolution images are suitable for forensic applications such as criminal detection [24]. Low resolution images are more suitable for civil and commercial applications such as access control. Generally speaking, high resolution refers to 400 dpi or more and low resolution refers to 150 dpi or less. Fig. 2 illustrates a part of a high-resolution palmprint image and a low resolution palmprint image. Researchers can extract ridges, singular points and minutia points as features from high resolution images while in low resolution images they generally extract principal lines, wrinkles and texture. Initially palmprint research focused on high-resolution images [9-10] but now almost all research is on low resolution images for civil and commercial applications. This is also the focus of this paper. The design of a biometric system takes account of five objectives: cost, user acceptance and environment constraints, accuracy, computation speed and security (Fig. 4). Reducing accuracy can increase speed. Typical examples are 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.

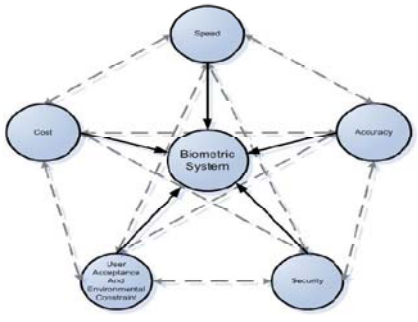


Fig. 4: Computation speed and security of Biometric system

Typical palm print recognition system consists of five parts: palm print scanner, preprocessing, feature extraction, matcher and database illustrated in Fig. 5. The palm print scanner collects palm print images. Preprocessing sets up a coordinate system to align palm print images and to segment a part of palm print image for feature extraction. Feature extraction obtains effective features from the preprocessed palm prints. A matcher compares two palm print features and a database stores registered templates.

II PALM PRINT SCANNERS AND PREPROCESSING

2.1 Palm print Scanners:

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 this increases user acceptance. Digital cameras and video cameras can be used to collect palm print images without contact [17], 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.

Fig. 5(a) is a palm print image collected with a CCD-based palmprint scanner and Fig. 5(b) is a palm print image collected with a digital scanner. Although Fig. 5(a) does not include the fingers, this does not mean that CCD-based palm print scanners cannot capture fingers. The scanner developed by Han can capture all information from a palm including fingers and palm. Capturing fingers may require increasing the size of the device. In Fig. 5(b), we can see that the palm is distorted because of contact with the scanners. This distortion does not happen in Fig. 5(a) because the scanner is better designed.

(a)

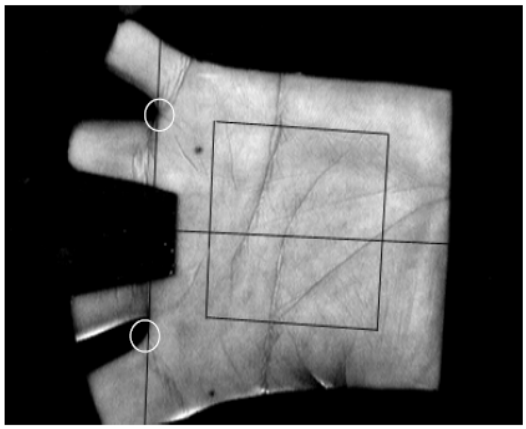
(b)

Fig. 5 : Collected Palm Prints

2.2 Preprocessing

Preprocessing is used to align different palmprint images and to segment the centre 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. 6(a) illustrates the key points and Fig. 6(b) shows a preprocessed image. The first and second steps in all the preprocessing algorithms are similar. However, the third step has several different implementations including tangent-based [7], bisector based [16, 28] and finger-based [9, 10] 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 fingers (as in the disabled) 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 [10] and the other based on the

point, middle and ring fingers [9]. 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 [10]. 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 while Kumar et al. proposed using all information in palms [30]. They fit an ellipse to a binary palmprint image and set up the coordinate system according to the orientation of the ellipse.



(a)

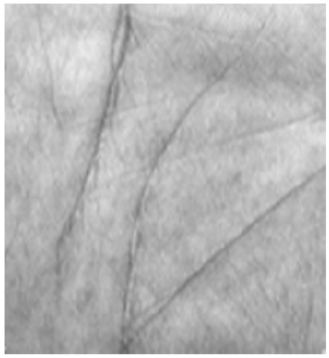


Fig. 6 : Processed Images

After obtaining the coordinate systems, the central parts of palm prints are segmented. Most of the preprocessing algorithms segment square regions for feature extraction but some of them segment circular [11] and half elliptical regions [21]. The square region is easier for handling translation variation, while the circular and half elliptical regions may be easier for handling rotation variation.

III. VERIFICATION ALGORITHMS

Once the central part is segmented, features can be extracted for matching. There are two types of recognition algorithms, 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 algorithms will be discussed in Section 5. Verification algorithms are line-based, subspace-based and statistic-based. Some algorithms in this section can support a certain scale of identification. However, most of the researchers do not report matching speed.

3.1 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) [8, 12-13, 18, 22, 23, 26-17, 20]. 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. Table 1 summarizes subspace approaches.

Table 1 Summary of Subspace Approach

Feature extraction	Subspace	Classifier	Ref
Wavelets: Haar, Daubechies and Symmlet	PCA, LDA, ICA	L_1 Measure L_2 Measure Cosine Measure Probabilistic neural network	8
Nil	LDA	Euclidean distance	12
Nil	PCA	Weighted Euclidean distance	13
DCT	Improved Fishface	Euclidean distance	18
Nil	Kernel PCA	Maximum a posterior classifier	39
Wavelet	ICA	Euclidean distance	42
Nil	PCA, ICA	Euclidean distance	66
Nil	ICA	Radial basis probabilistic neural network	67
Nil	Bi-directional PCA	Assembled Matrix distance metric	71
Nil	Kernel PCA + Locality preserving projections	Euclidean distance	73
Gabor filter + boosting algorithm	LDA	Cosine distance	89
Nil	Winner-take-all network based on ICA	Radial basis probabilistic neural network	90
Wavelet, DCT, FFT	Kernel PCA	Support Vector Machine, Weighted Euclidean Distance, Linear Euclidean Distance	91
Nil	Unsupervised discriminant project	Euclidean, Cosine measure	102, 103

3.2 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 [10, 15, 23, 24, 20-15, 27, 24]. 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 [29, 30]. To our knowledge, no one has yet investigated high order statistics for these approaches. In addition to directly describing the local region by statistics, Wang et

al. use histograms of local binary pattern as features [98]. Global statistical approaches [11, 14, 46, 49, 54] compute global statistical features directly from the whole transformed images. Moments, centers of gravity and density have been regarded as the global statistical features. Table 2 summarizes these algorithms.

Table 2 Summary of Statistical Approach

Feature extraction	Statistical feature	Shape of small regions	Classifier	Ref
Sobel filter, morphological operators	Mean	Square and rectangle	Backpropagation neural network	10
Direction masks	Standard deviation	Square	Cosine similarity	33, 50
Gabor filter	Mean and standard deviation	Circular	Cosine similarity	64
Directional line detector, Gabor, Haar Wavelet	Mean energy, number of line pixel	Rectangle, segments in elliptical half-ring	L_1 norm	29
Nil	Zernike moments	Global statistics	Euclidean, L_1 norm	11
Wavelet	center of gravity, density, spatial dispersivity and engery	Global statistics	Sum of individual percentage error	14
M-band wavelet	L_1-norm energy, Variance	Global statistics	Euclidean distance	46
Nil	Zernike moments	Global statistics	Modular neural network	49
Otsu binarization	Hu Invariant Moments	Global statistics	Euclidean distance	54

IV. IDENTIFICATION IN LARGE DATABASES

4.1 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 [14-16]. These approaches increase matching speed at the cost of accuracy. Classifiers can remove target palm prints by using simple features.

Classification approaches assign a class to each palm print in a database. Wu et al. define six classes based on the number of principal lines and their intersections [22] (Fig. 7). However, the six classes are highly unbalanced, e.g. about 80% of palm prints in

category 5 (Fig. 7(e)) and the algorithm has high bin errors of 4%. So these classes are not enough for identification. Li et al. proposed dealing with the unbalanced class [14] problem by further dividing the unbalanced class.

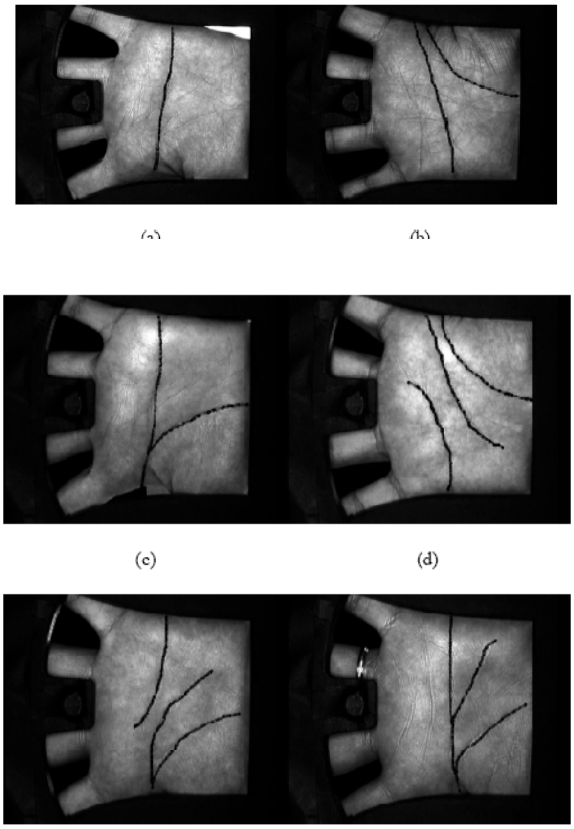


Fig. 7 : Feature Extraction

4.2 Coding Approaches

Coding approaches [1, 3-4, 7, 29] 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. Daugman, the inventor of Iris Code, has demonstrated that the bitwise hamming distance allows real-time brute force identification in large databases [25]. Several coding algorithms similar to Iris Code have been proposed for palm print identification. Palm Code uses a single Gabor filter to extract the local phase information of palm print [1, 7]. The phase is quantized and is represented in bits and the bitwise hamming distance is used to compare two Palm Codes. The computational architecture is the same as Iris Code. Palm Code always generates highly correlated features from different palms. To remove this correlation, in the first version of Fusion Code [25], we use four directional Gabor filters to generate four Palm Codes. These Palm Codes are combined. For each sample point, only phase information generated by the Gabor filter having maximum magnitude is quantized.

Hamming distance is still used to compare two Fusion Codes. In the second version of Fusion Code, the authors carefully examine the number of Gabor filters and their parameters and find out that the optimal number of Gabor filters is two. They replace the static threshold with a dynamical threshold. The second version of Fusion Code is much more effective than the first. Both Palm Code and Fusion Code (first and second versions) employ quantized phases as features and the hamming distance as a matcher. Competitive Code [3] uses the orientation field of a palm print, encoding it for high-speed matching using a novel coding scheme and bitwise angular distance. Like Palm Code and Fusion Code, Competitive Code uses translated matching to improve alignment in preprocessing. A second version of Competitive Code [5], generated 25 translated templates from an input palm print to match the templates in a database, producing more effective matching codes than the first version. Other researchers have studied this same feature [18, 6, 5]. Sun et al. used differences between Gaussians to extract orientation fields and bitwise hamming distances for use in matching [19]. Wu et al. modified Fusion Code to extract the orientation field. This algorithm uses the hamming distance but it is not bitwise [12, 13] so direct implementation of this algorithm does not support high-speed matching. However, it is possible to replace the non-bitwise hamming distance with the bitwise hamming distance if a suitable coding scheme is provided. Jia et al. also use the term code to describe their method. They modify a finite Radon transform and employ a winner-take-all rule, which is used in Competitive Code, to estimate the orientation field of palm prints. They design a matching scheme called pixel-to-area comparison to improve robustness. Because of the pixel-to-area matching scheme, the matching speed of this algorithm is slower than that of other coding algorithms, which uses bitwise hamming distance and bitwise angular distance

V. CONCLUSION & DISCUSSION

Biometric systems are vulnerable to many attacks including replay, database and brute force attacks [26]. Compared with verification, fusion and identification, there has been little research on palm print security. We have analyzed the probability of successfully using brute-force attack to break in a palm print identification system [5] and proposed cancelable palm prints for template re-issuance to defend replay attacks and database attacks [86]. Connie et al. combined pseudo-random keys and palm print features to generate cancelable palm print representations [27]. They claim that their method can achieve zero equal error rates. However, they assume [6] that the pseudo-random keys are never lost and shared and based on this assumption report zero equal error rates for different biometric traits [28]. Sun et al. apply watermarking techniques to hide finger features in palm print images for secure identification [30]. Wu et al. use palm print for cryptosystem [8]. Although some security issues have been addressed, it is still not enough. For example, liveness detection has not been well studied. A fake palm print can be found in [19]. Potential solutions of liveness detection include infrared and multiple spectrum approaches [2, 10].

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. Palm prints can also indicate genetic disorders. Most previous medical research related to the palm has concentrated on abnormal flexion creases, the Simian line and the Sydney line (Fig. 10) [18]. About 3% of normal population has abnormal flexion creases. Medical researchers also discover the association between density of secondary creases and schizophrenia [26]. To protect private information in palm prints, databases store encrypted templates because the line features can be reconstructed from raw templates. Both traditional encryption techniques and cancelable biometrics can be used for encryption. Cancelable biometrics matches in the transform domain while traditional encryption techniques require decryption before matching. In other words, decryption is not necessary for cancelable biometrics. When matching speed is an issue, e.g. identification in a large database, cancelable biometrics can hide private information.

REFERENCES

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

[2] A. Kong, D. Zhang and G. Lu, "A study of identical twins palm print for personal verification", Pattern Recognition, vol. 39, no. 11, pp. 2149-2156, 2006.

[3] A.W.K. Kong and D. Zhang, "Competitive Coding scheme for palmprint verification", in Proceedings of International Conference on Pattern Recognition, vol. 1, pp. 520-523, 2004.

[4] A. Kong and D. Zhang, "Palm print identification using feature-level fusion", Pattern Recognition, vol. 39, no. 3, pp. 478-487, 2006.

[5] A. Kong, D Zhang and M. Kamel, "A study of brute-force break-ins of a palmprint verification system", IEEE Transactions on Systems, Man and Cybernetics, Part B, vol. 36, no. 5, pp. 1201-1205, 2006.

[6] A. Kong, K.H. Cheung, D. Zhang, M. Kamel and J. You, "An analysis of Biohashing and its variants", Pattern Recognition, vol. 39, no. 7, pp. 1359-1368, 2006.

[7] D. Zhang, W.K. Kong, J. You and M. Wong, "On-line palm print identification", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 25, no. 9, pp. 1041- 1050, 2003.

[8] T. Connie, A.T.B. Jin, M.G.K. Ong and D.N.C. Ling, "An automated palmprint recognition system", Image and Vision Computing, vol. 23, no. 5, pp. 501-515, 2005.

[9] C.C. Han, "A hand-based personal authentication using a coarse-to-fine strategy", Image and Vision Computing, vol. 22, no. 11, pp. 909-918, 2004.

[10] C.C. Han, H.L. Cheng, C.L. Lin and K.C. Fan, "Personal authentication using palm-print features", Pattern Recognition, vol. 36, no. 2, pp. 371-381, 2003.

[11] Y.H. Pang, T. Connie, A. Jin and D. Ling, "Palmprint authentication with Zernike moment invariants", in Proceedings of the 3rd IEEE International Symposium on Signal Processing and Information Technology, pp. 199-202, 2003.

[12] X. Wu, D. Zhang and K. Wang, "Fisherpalms based palmprint recognition", Pattern Recognition Letters, vol. 24, no, 15, pp. 2829-2838, 2003.

[13] G. Lu, D. Zhang and K. Wang, "Palmprint recognition using eigenpalms features", Pattern Recognition Letters, vol. 24, no. 9, pp. 1463-1467, 2003.

[14] L. Zhang, D. Zhang, "Characterization of palmprints by wavelet signatures via directional context modeling", IEEE Transactions on Systems, Man and Cybernetics, Part B, vol. 34, no. 3, pp. 1335-1347, 2004.

[15] J. You, W.K. Kong, D. Zhang, K.H. Cheung, "On hierarchical palmprint coding with multiple features for personal identification in large databases", IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 2, pp. 234-243, 2004.

[16] W. Li, D. Zhang, Z. Xu, "Palmprint identification by Fourier transform", International Journal of Pattern Recognition and Artificial Intelligence, vol. 16, no. 4, pp. 417-432, 2002.

[17] S. Ribaric, D. Ribaric and N. Pavesic, "Multimodal biometric user-identification system for network-based applications", IEE Proceedings, Vision, Image and Signal Processing, vol. 150, no. 6, pp. 409-416, 2003.

[18] X.Y. Jing and D. Zhang, "A face and palmprint recognition approach based on discriminant DCT feature extraction", IEEE Transactions on Systems, Man, and Cybernetics − Part B: Cybernetics, vol. 34, no. 6, pp. 2405-2415, 2004.

[19] S. Ribaric and I. Fratric, "A biometric identification system based on Eigenpalm and Eigenfinger features", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 27, no. 1698-1709, 2005.

[20] S. Ribaric, I. Fratric and K. Kis, "A biometric verification system based on the fusion of palmprint and face features", in Proceeding of the 4th International Symposium on Image, Signal and Signal Processing and Analysis, pp. 15-17, 2005.

[21] A. Kumar and D. Zhang, "Personal authentication using multiple palmprint representation", Pattern Recognition, vol. 38, no. 10, pp. 1695-1704, 2005.

[22] X. Wu, D. Zhang, K. Wang and B. Huang, "Palmprint classification using principal lines", Pattern Recognition, vol. 37, no. 10, pp. 1987-1998, 2004.

[23] F. Yan, B. Ma, Q.X. Wang, D. Yao, C. Fang and X. Zhou, "Information fusion of biometrics based-on fingerprint, hand-geometry and palm-print" in Proceeding of IEEE Workshop on Automatic Identification Advanced Technologies, pp. 7-8, no. 247-252, 2007.

[24] NEC Automated Palmprint Identification System http://www.necmalaysia.com.my/Solutions/PID/products/ppi.html

[25] J.G. Daugman, "High confidence visual recognition of persons by a test of statistical independence", IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 15, no. 11, pp. 1148-1161, 1993.

[26] N.K. Ratha, J.H. Connell and R.M. Bolle, "Biometrics break-ins and band-aids", Pattern Recognition Letters, vol. 24, pp, 2105-2113, 2003.

[27] T. Connie, A. Teoh, M. Goh and D. Ngo, "PalmHashing: a novel approach for cancelable

biometrics", Information Processing Letters, vol. 93, no. 1, pp. 1-5, 2005.

[28] A.B.J. Teoh, D.C.L Ngo and A. Goh, "BioHashing: two factor authentication featuring fingerprint data and tokenised random number", Pattern Recognition, vol. 37, pp. 2245- 2255, 2004.

[29] C. Poon, D.C.M. Wong and H.C. Shen, "Personal identification and verification: fusion of palmprint representations", in Proceedings of International Conference on Biometric Authentication, pp. 782-788, 2004.

[30] L.S. Penrose, "Fingerprints and palmistry", The Lancet, vol. 301, no 7814, pp. 1239- 1242, 1973.

◈◈◈