Palmprint based Cancelable Biometric Authentication System

Ying-Han Pang, Andrew Teoh Beng Jin, and David Ngo Chek Ling

Abstract— A cancelable palmprint authentication system proposed in this paper is specifically designed to overcome the limitations of the contemporary biometric authentication system. In this proposed system, Geometric and pseudo Zernike moments are employed as feature extractors to transform palmprint image into a lower dimensional compact feature representation. Before moment computation, wavelet transform is adopted to decompose palmprint image into lower resolution and dimensional frequency subbands. This reduces the computational load of moment calculation drastically. The generated wavelet-moment based feature representation is used to generate cancelable verification key with a set of random data. This private binary key can be canceled and replaced. Besides that, this key also possesses high data capture offset tolerance, with highly correlated bit strings for intra-class population. This property allows a clear separation of the genuine and imposter populations, as well as zero Equal Error Rate achievement, which is hardly gained in the conventional biometric based authentication system.

Keywords— Cancelable biometric authenticator, Discrete-Hashing, Moments, Palmprint.

I. INTRODUCTION

The existing biometric based authenticator is impuissance to compromise since the verification key- biometric feature employed in these systems is non- reissueable/ cancelable. In other words, when this biometric template is compromised, a new one cannot be issued since biometric is an intrinsic aspect to human being and is invariant over time [1]. In addition, this conventional biometric decision scheme is hardly to gain zero Equal Error Rate (EER) due to the fact that classes are difficult to be completely separated in the measurement space. Specification of low False Accept Rate (FAR) will increase False Reject Rate (FRR) which forbids the access of genuine.

In this paper, a cancelable palmprint authentication system is proposed based on the ideas that none of the same verification key is applied in two different applications and a new verification key can be reissued when compromised. In our proposed system, palmprint data is firstly decomposed

into various frequency subbands with lower resolution and dimensionality via wavelet transform. The only best subband just will be input into moment family for feature extraction in order to reduce moment computational load. Computation on subband with lower resolution and dimension is able to save at least 60% of moment computational time. Then the wavelet-moment based feature representation basis is adopted to generate cancelable verification key for our system.

In our authentication system, the cancelable mechanism is named as Discrete-Hashing, deriving from the concept of Discretization + Hashing mechanism. In Discrete-Hashing, wavelet-moment based palmprint feature template is inner product with a set of pseudo random number to generate a set of private binary string after discretization. This set of binary string is acted as verification key in our system. This verification key is replaceable because the direct mixing mechanism inner-products another new set of random data with the palmprint features to produce a new set of binary code. Moreover, Discrete-Hashing code also leads to zero EER, eliminated the occurrence of FAR without jeopardizing the FRR performance and clear separation in between the genuine and imposter populations [2]. Fig. 1 illustrates the overview of our proposed palmprint based authentication system.
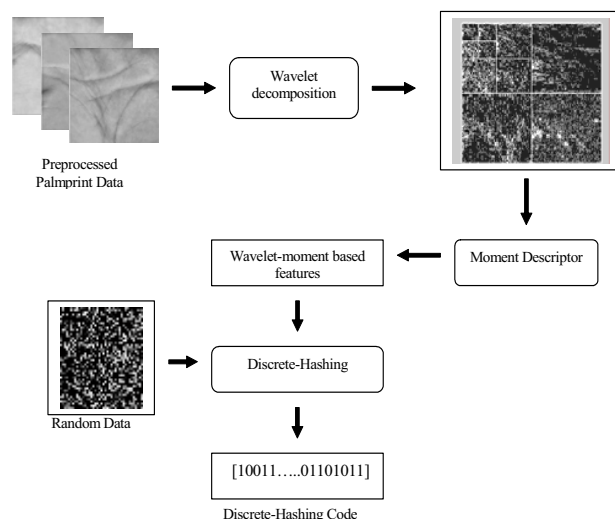

Fig. 1. The overview of our proposed palmprint based authentication system.

II. WAVELET TRANSFORM

The wavelet decomposition of a signal $f(x)$ can be obtained by convolution of signal with a family of real orthonormal basis, $\psi_{a,b}(x)$,

$$(W_{\psi}f(x))(a,b) = |a|^{-1/2} \int_{\Re} f(x)\psi((x-b)/a)dx \quad f(x) \in L^2(\Re) \quad (1)$$

where a, $b \in \Re$, a $\neq$ 0 are the dilation parameter and the translation parameter respectively.

For 2D signal such as images, there exists an algorithm similar to the one-dimensional case for two dimensional wavelets and scaling functions obtained from one-dimensional ones by tensiorial product. This kind of two-dimensional wavelet transform leads to a decomposition of approximation coefficients at level j-1 in four components: the approximations at level j, L_j and the details in three orientations (horizontal, vertical and diagonal), $D_{jvertical}$, $D_{jhorizontal}$, and $D_{jdiagonal}$ [3].

Discrete wavelet transform is used to decompose the palmprint image into a multiresolution representation in order to keep the least coefficients possible without losing useful image information. The multiresolution character of the wavelet decomposition leads to superior energy compaction (high image information content) and compact constitution of L_j subband. Commonly, frequency subband containing the highest energy distribution will contribute significant information about the image. Therefore, L_j subband is selected upon D_j's for palmprint representation as it obtains the highest recognition rate and energy distribution, see Table I.

TABLE I
ENERGY AND VERIFICATION RATE OF WAVELET SUBBANDS.

Haar Wavelet Basis (Level 1)			
Subband	L_j	$D_{j\,horizontal}$	$D_{j\,vertical}$	$D_{j\,diagonal}$
Energy (%)	97.07	1.75	1.01	0.14
TSR (%)	95.00	68.11	74.34	53.63
Daubechies order 2 level 1 Wavelet Basis			
Subband	L_j	$D_{j\,horizontal}$	$D_{j\,vertical}$	$D_{j\,diagonal}$
Energy (%)	98.30	1.03	0.59	0.06
TSR (%)	95.14	65.05	74.59	54.15
Symmlet order 2 level 1 Wavelet Basis			
Subband	L_j	$D_{j\,horizontal}$	$D_{j\,vertical}$	$D_{j\,diagonal}$
Energy (%)	98.30	1.03	0.59	0.06
TSR (%)	95.14	65.05	74.59	54.15

III. MOMENTS

Moment is a statistical measurement of data such as total mass, mean, variance value, etc.. Moments are applicable to many different aspects of image processing, ranging from invariant pattern recognition, image encoding to pose estimation [4]. Moment family is a well-known feature extractor to Chinese character [5][6]. Moments can describe Chinese character uniquely regardless how close the characters are in terms of local features [7]. Palmprint is

similar to Chinese character, which is also constructed from line structures. This inspired us to implement moment functions to extract palmprint characteristics for personal verification tasks.

A. Geometric Moments

Geometric moments (GM) are non-orthogonal moment functions, with the kernel function defined as a product of the pixel coordinates. GM has the form of the projection of the $f(x,y)$ function onto the monomial $x^p y^q$ basis. Unfortunately, $x^p y^q$ set is not orthogonal.

The two-dimensional $(p+q)^{th}$ order moments of lower resolution wavelet subband, L_j, are defined by [4]:

$$M_{pq} = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} x^p y^q L_j \, dxdy \quad (2)$$

where $p,q = 0,1,2,...$ and j= decomposition level.

The discrete version of Geometric moments for an image consisting of pixels $L_j(x,y)$, replacing the integrals with summations, is:

$$M_{pq} = \sum_{x=0}^{N-1}\sum_{y=0}^{N-1} x^p y^q L_j(x,y) \quad (3)$$

B. Pseudo Zernike Moments

The kernel of pseudo Zernike moments is the set of orthogonal pseudo Zernike polynomials defined over the polar coordinates inside a unit circle. The two-dimensional pseudo Zernike moments of order p with repetition q of a wavelet subband, L_j, are defined as [4][8]:

$$PZ_{pq} = (p+1)/\pi \int_0^{2\pi}\int_0^1 V_{pq}(r,\theta)L_j(r,\theta)rdrd\theta \quad (4)$$

where Zernike polynomials $V_{pq}(r,\theta)$ are defined as:

$$V_{pq}(r,\theta) = R_{pq}(r)e^{-\hat{j}q\theta}; \quad \hat{j} = \sqrt{-1} \quad (5)$$

and $r = \sqrt{x^2 + y^2}$, $\theta = \tan^{-1}(y/x)$, $-1 < x,y < 1$

The real-valued radial polynomials are defined as:

$$R_{pq}(r) = \sum_{s=0}^{p-|q|}(-1)^s((2p+1-s)!)/(s!(p+|q|+1-s)!(p-|q|-s)!)r^{p-s} \quad (6)$$

and
$$0 \rceil |q| \lceil p, \ p \geq 0$$

Since it is easier to work with real functions, PZ_{pq} is often split into its real and imaginary parts, PZ_{pq}^c, PZ_{pq}^s as given below:

$$PZ_{pq}^c = 2(p+1)/\pi \int_0^{2\pi}\int_0^1 R_{pq}(r)\cos(q\theta)L_j(r,\theta)rdrd\theta \quad (7)$$

$$PZ_{pq}^s = 2(p+1)/\pi \int_0^{2\pi}\int_0^1 R_{pq}(r)\sin(q\theta)L_j(r,\theta)rdrd\theta \quad (8)$$

where $p \geq 0$, $q > 0$.

In this paper, wavelet-moment based features are the magnitude of the moment descriptor output, denoted as $WM = \{M \mid PZ_{mag}\}$, due to their rotation invariant property whereas the phase information is omitted as the influence of phase information in recognition is rather insignificant especially when high order moments are included [9].

IV. DISCRETE-HASHING

At this stage, wavelet-moment based feature template (WM), with l feature length, is transformed into a set of single bit, $b \in \{0,1\}^m$, with m length, by inner product with a uniform distributed random number, $r \in \{-1,1\}$, see Fig. 2.

Specifically,

(1). Apply Gram-Schmidt process to transform random number $\{r_i \in \Re^i \mid i = 1, ..., m\}$ into an orthonormal set of matrices $\{r_{\perp i} \in \Re^i \mid i = 1, ..., m\}$.

(2). Compute $\{< WM \mid r_{\perp i} > \in \Re \mid i = 1, ..., m\}$ where $< \cdot \mid \cdot >$ indicates inner product operation.

(3). Compute m bits Discrete-Hashing, $b \in 2^m$ from

$$b_i = \begin{cases} 0 & if \ \langle WM \mid r_{\perp i} \rangle \ \tau \\ 1 & if \ \langle WM \mid r_{\perp i} \rangle > \tau \end{cases} \ m \ \rceil \ l$$

, where τ is a preset threshold. In this paper, the τ is set to 0 since the output of the product is a uniform distributed random number within the range [-1, 1].

Repetition of this procedure to obtain multiple bits renders the issue of inter-bit correlations, this issue is addressed via Gram-Schmidt process in step (1) to obtain orthonormal set $\varsigma = \{r_{\perp k} \mid k = 1, 2, ..., m\}$. Each bit b_i is hence rendered independent to all others.

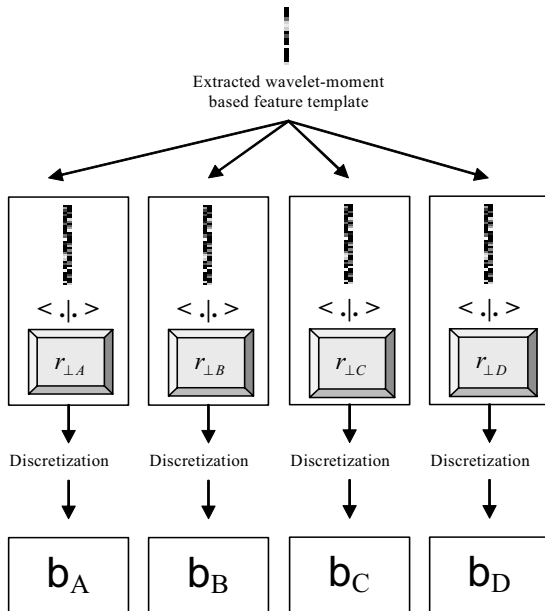Extracted wavelet-moment based feature template

Fig. 2. Discrete-Hashing code formulation.

V. EXPERIMENTAL STUDIES AND DISCUSSIONS

A. Experimental Setup

Our authentication system performance has been evaluated in terms of their Receiver Operating Characteristic (ROC), False Accept Rate (FAR), False Reject Rate (FRR), Equal Error Rate (EER), Total Success Rate (TSR) as well as the genuine and imposter population distributions. 100 palmprint classes from 50 users, in which the right and left palmprints are treated as different classes, are used as our experimental database. These palmprints are taken over different days and display differences in orientation and translation. Their resolution is 150 dpi. There are six samples in each palmprint class, where the first, third and fifth samples are selected as the testing set and the rest as training data.

B. Experimental Studies on Wavelet-moment-based Features

At the initial stage, an experiment is conducted to determine pertinent and optimal order moments, which can perfectly represent palmprint. From Fig. 3, we can observe that moment orders 17 and 12 obtain the highest recognition rate in Geometric (GM) and pseudo Zernike (PZM) moments, respectively. Thus, the moments in this order are selected as input features in the next experiments. It also reveals that higher moment order provides better recognition rate as higher order moments provide more and finer details about palmprint. However, this is only true to a certain level as the recognition rate will become stabilize, see GM plot, or even worse if the moment order is excessive high, see PZM plot.

From the figure, PZM performs well as feature descriptor to palmprint images over GM for all order n. This vindicates that orthogonality property of PZM is able to elicit the unique palmprint attributes into each order moment with minimum information redundancy, where information redundancy might influence the discrimination power of the moment function. GM which has non orthogonal monomial basis set, as a counterexample, shows its inferiority in terms of discrimination capability in palmprint image. GM's non-orthogonal property causes some characteristics of the images to be over-represented and thus the computed moments suffer from higher degree of information redundancy.

The integration of wavelet transform with moment family is known as *WMOMENT* for brevity: WT + GM = WGM and WT + PZM = WPZM. In this paper, wavelet basis with Daubechies orthonormal wavelet filter order 7, level 1 with moment order 17 is selected as feature representation for WGM. The verification rate with FAR=9.8597%, FRR=9.9886% and TSR=90.1390% is obtained. On the other hand, wavelet basis with Haar orthonormal wavelet filter, level 2 with moment order 12 possesses verification rate with FAR=4.3883%, FRR=4.4268% and TSR=95.6113% in WPZM. From Table II, it can be observed that integration of wavelet transform with moment family not only improves feature representation capability, but also reduces the computational load dramatically.
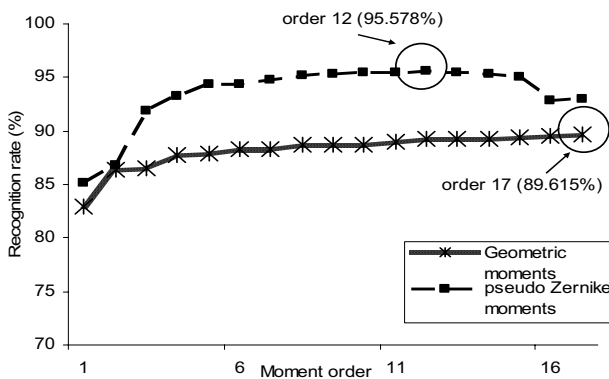
Fig. 3. Recognition rate VS moment order plot.

TABLE II
COMPARISON ANALYSIS OF DIFFERENT SCHEMES.

Scheme	Recognition rate (%)	Computational time (s)	Time saved (%)
GM (oder 17)	89.615	3.1100	
WGM (db7, level 1 + order 17)	90.139	1.0940	64.82
PZM (order 12)	95.578	6.8130	
WPZM (haar, level 2 + order 12)	95.611	0.5630	91.74

C. Experimental Studies on Discrete-Hashing

The optimal wavelet-moment based features of Geometric and pseudo Zernike moments are input into Discrete-Hashing to generate a set of cancelable/ replaceable verification key. The following abbreviations will be used for brevity in the subsequent discussion:

WGM: denotes Geometric moments on wavelet subbands

WPZM: denotes pseudo Zernike moments on wavelet subbands.

{WGM | WPZM}:D_m: denotes 2^m discretisation with the threshold value, τ, where m represents the bit length value.

The experimental data are acquired for m = 30, 50, 70 and 90 in all cases; while for the similarity matching, a simple Euclidean distance metric is adopted for WGM as well as WPZM whereas Hamming distance is used for the remaining.

Mean of iterated inner product operation distribution, $\overline{\langle WM | r_\perp \rangle}$ is generated and shown in Fig. 4. This figure reveals that the $\overline{\langle WM | r_\perp \rangle}$ distribution is approximated to a normal distribution with mean, $\overline{\langle WM | r_\perp \rangle}_\mu$ = -0.0012 ≈ 0 and standard deviation $\overline{\langle WM | r_\perp \rangle}_\sigma$ = 0.0109. Since the inner

product is distributed normally within the range of [-1, 1], mean value of 0 is used as threshold value to determine the binary Discrete-Hashing code.
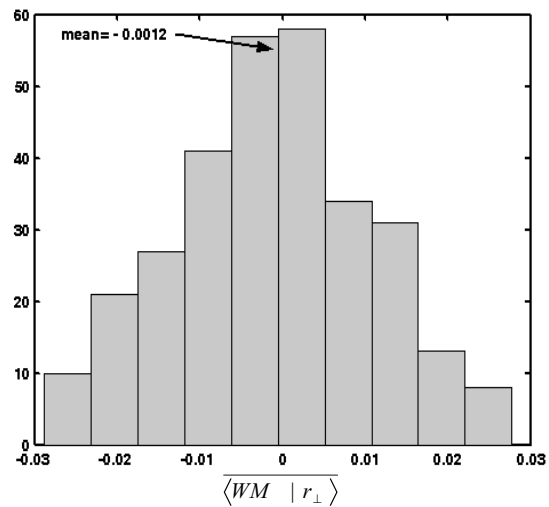

Fig. 4. Iterated inner product distribution.

Four performance criteria namely FAR, FRR, EER and TSR are adopted to determine the performance of {WGM | WPZM}: D_m. Table III shows the verification rates of WGM, WPZM and {WGM | WPZM}: D_m schemes. It can be observed that Discrete-Hashing technique manages to improve the overall performance of the wavelet-moment based methods. From the result, WGM:D_90, WPZM:D_70 and WPZM:D_90 yield 0% of FRR when FAR is reduced to zero. This is a significant enhancement to the contemporary biometric systems as the interdependency problem between FAR and FRR is eliminated. Fig. 5 demonstrates the ROC plots for {WGM | WPZM}: D_m schemes, in which the phenomenon of longer bit length, m, produces better result is illustrated. From the figure, we can see that {WGM | WPZM}: D_m plot with longer m is closer to the origin as lower FAR and FRR are attained.

TABLE III
VERIFICATION RATES OF WGM, WPZM AND {WGM | WPZM}: D_M SCHEMES.

Schemes	FAR (%)	FRR (%)	TSR (%)	EER (%)
WGM	9.8597	9.9886	90.1390	9.9227
WGM:D_30	2.1010	1.0000	97.9100	1.5505
WGM:D_50	0.7374	0	99.2700	0.3687
WGM:D_70	0.0202	0	99.9800	0.0101
WGM:D_90	0	0	100	0
WPZM	4.3883	4.4268	95.6113	4.4076
WPZM:D_30	0.1414	0	99.8500	0.0071
WPZM:D_50	0.0101	0	99.9900	0.0051
WPZM:D_70	0	0	100	0
WPZM:D_90	0	0	100	0

(a)

(b)
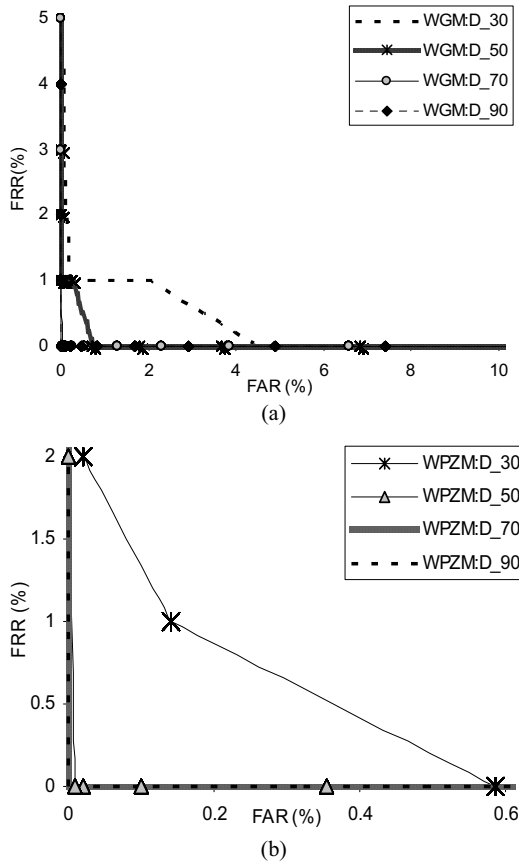
Fig. 5. ROC plots for (a) *WGM*: *D_m* , and (b) *WPZM*: *D_m*

Since *WGM:D_*90, *WPZM:D_*70 and *WPZM:D_*90 attain FAR = FRR = 0%, another performance indicator is through the observation of range of threshold values, $t \in [0 \; 100]$ when EER = 0%: the bigger range of threshold value yields the better performance, as large range of operating points (threshold) with zero errors can be obtained. Table IV provides a detail of the range of threshold when EER = 0%.

TABLE IV
PERFORMANCE EVALUATION IN TERMS OF EER AND FRR
WHEN FAR = 0% FOR {*WGM* | *WPZM*}: *D_M* SCHEMES.

Methods	EER (%)	FRR(%) (FAR=0%)	Threshold Range when EER=0% [t_{max}-t_{min}]
*WGM:D_*30	1.5505	56.0000	-
*WGM:D_*50	0.3687	2.0000	-
*WGM:D_*70	0.0101	1.0000	-
*WGM:D_*90	0	0	0.0150 [0.4324-0.4174]
*WPZM:D_*30	0.0707	7	-
*WPZM:D_*50	0.0051	2	-
*WPZM:D_*70	0	0	0.0410 [0.3954-0.3544]
*WPZM:D_*90	0	0	0.0980 [0.4424-0.3444]

Fig. 6 illustrates the genuine and imposter population distribution for {*WGM* | *WPZM*}:*D_*90 schemes. The genuine distribution in the graph shows the outcome when different images of the same palmprint are compared; but when bit strings from different palmprints are compared, the imposter distribution histogram is the result. Fig. 6 (a) shows that there is a relatively small overlapping in between the genuine and imposter frequency distribution for *WGM:D_*90, but there is a clear separation in between the genuine and imposter populations for *WPZM:D_*90. A particular attractiveness of the Discrete-Hashing genuine population is its steeper peak-to-plateau drop-offs, which allows specification of zero FAR without jeopardizing the FRR performance.

(a) WGM:*D_*90
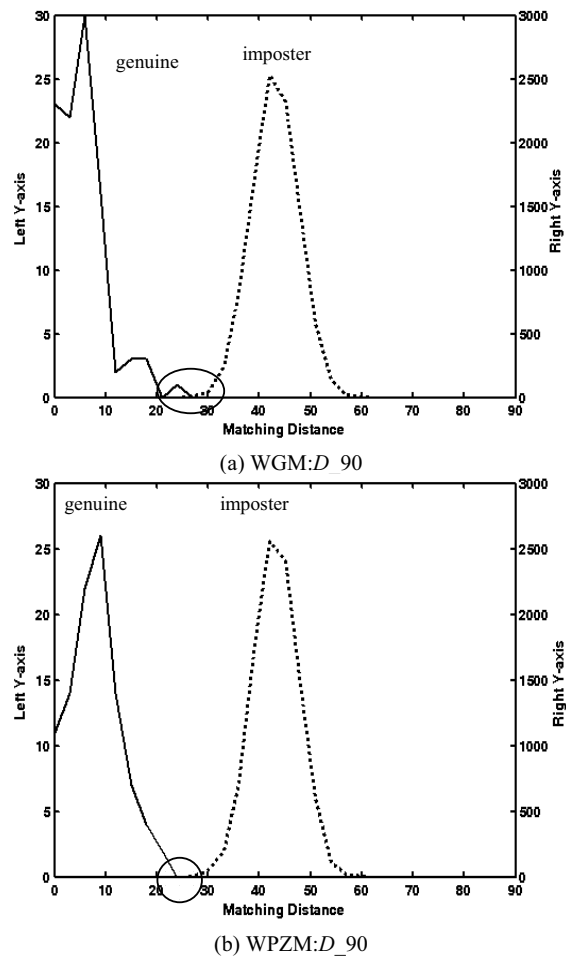
(b) WPZM:*D_*90

Fig.6. The genuine and imposter population distribution for {*WGM* | *WPZM*}:*D_*90 schemes.

Pseudo Zernike moments possess real and imaginary features as described in (7) and (8). Therefore, we utilize this property in our authentication system, in which we input both real and imaginary feature vectors of pseudo Zernike moments into Discrete-Hashing, instead of only one input (magnitude of wavelet-moment based features, WM_{mag}). Fig. 7 depicts

FAR and FRR versus threshold value plot for *WPZM:D_*90 and *WPZM:Dc_*90 where {*WPZM*}:*Dc_m* denotes Discrete-Hashing scheme with real and imaginary inputs.
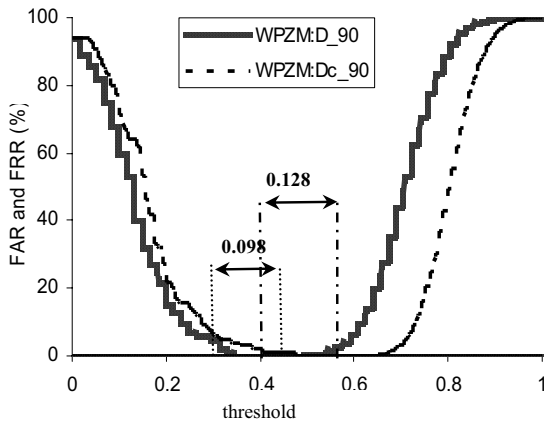

Fig. 7. Graph of FAR and FRR plotted against threshold value for *WPZM:D_*90 and *WPZM:Dc_*90 schemes.

From the above figure, we can see that *WPZM:Dc_*90 scheme has wider operating range with zero error than *WPZM:D_*90 scheme. Fig. 8 illustrates the genuine and imposter distribution populations for *WPZM:Dc_*90 with wider separation between the two populations.
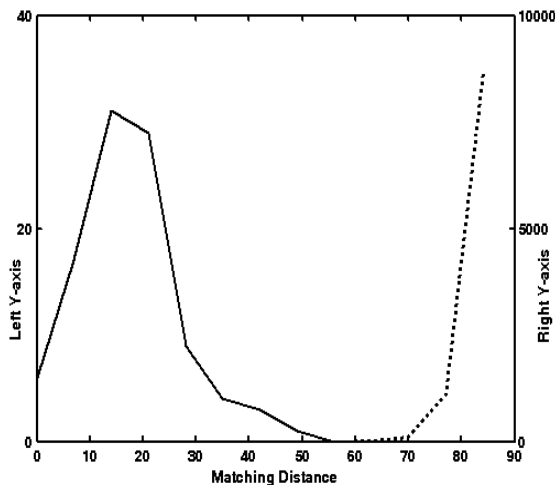

Fig. 8. Genuine and imposter distribution populations for *WPZM:Dc_*90 scheme.

Table V shows the statistical data for {W*GM* | *WPZM*}, {*WGM* | *WPZM*}:*D_m* and {*WPZM*}:*Dc_m* schemes. {*WGM* | *WPZM*}:*D_m* and {*WPZM*}:*Dc_m* schemes minimize the distance between images from the same class, which can be observed from mean and variance as shown in the table. The mean and variance values of both genuine and imposter in the {*WGM* | *WPZM*}:*D_m* and {*WPZM*}:*Dc_m* schemes are smaller than those in the {W*GM* | *WPZM*} schemes. This

reveals that Discrete-Hashing improves the verification performance of our palmprint based authentication system.

TABLE V
STATISTIC DATA FOR THE GENUINE AND IMPOSTER
POPULATIONS FOR VARIOUS SCHEMES.

Schemes	Genuine Population		Imposter Population	
	Mean	Variance	Mean	Variance
WGM	0.19160	0.01151	0.63493	0.05466
WGM:D_m	0.06429	0.00304	0.51217	0.00289
WPZM	0.17610	0.00659	0.51015	0.00859
WPZM:D_m	0.09221	0.00325	0.50162	0.00262
WPZM:Dc_m	0.09994	0.00326	0.50395	0.00129

VI. CONCLUSION

This paper presents a two-factor palmprint based authentication system which possesses credits of having replaceable/ cancelable verification key and providing a clear separation between genuine and imposter distribution populations. In this system, wavelet-moment based palmprint features are hashed with a set of pseudo random data to generate a set of unique binary code, Discrete-Hashing code. This code is used as verification key and is replaceable and cancelable. When it compromised, it can be replaced by hashing it with another set of pseudo random number. Besides, complex number property of pseudo Zernike moments even enhances the performance of this system by providing wider operating range with zero error. Experimental results show that the zero Equal Error Rate is attained in this authenticator.

ACKNOWLEDGMENT

REFERENCES

[1] R. M. Bolle, J. H. Connel, and N. K. Ratha, "Biometric perils and patches," *Pattern Recognition*, 35(12), pp. 2727-2738, 2002.
[2] T. B. J. Andrew, N. C. L. David, and G. Alwyn, "Biohashing: two factor authentication featuring fingerprint data and tokenised random number," *Pattern Recognition, Pattern Recognition Soc., Elservier Science*, to be published.
[3] S. Mallat, *A Wavelet Tour of Signal Processing*. San Diego: Academic Press, 1998.
[4] R. Mukundan, and K. R. Ramakrishnan, *Moment Functions in Image Analysis – Theory and Applications*. World Scientific Publishing, 1998.
[5] A. Chiang, S. Liao, Q. Lu, and M. Pawlak, "Gegenbauer moment-based applications for Chinese character recognition," *Proceedings of the 2002 IEEE Canadian Conference on Electrical & Computer Engineering*, 2002, pp. 908-911.
[6] X. L. Simon, and Q. Lu, " A study of moment functions and its use in Chinese character recognition," *Proceedings of the Fourth International Conference on Document Analysis and Recognition*, vol. 2 , 1997, pp. 572 – 575.

[7] Y. H. Pang, T. B. J. Andrew, N. C. L. David, and F. S. Hiew, "Palmprint verification with moments," *Journal of Computer Graphics, Visualization and Computer Vision* (*WSCG*), ISSN 1213-6972, 12(2), 2004, pp. 325-332.

[8]   C. H. Teh, and R. T. Chin, "On image analysis by the methods of moments," *IEEE Trans. Pattern Analysis and Machine Intelligence*, 10, 1998, pp. 496-512.

[9] A. Khotanzad, "Invariant image recognition by Zernike moments," *IEEE Trans. Pattern Analysis and Machine Intelligence*, vol. PAMI-12, no.5, 1990, pp. 489-497.
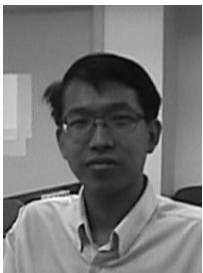
David Ngo Chek Ling is born in Sarawak, Malaysia, on November 15, 1966. He was awarded a BAI in Microelectronics & Electrical Engineering and Ph.D in Computer Science in Automatic Screen Design, Aesthetic Systems, Biometric Encryption and Knowledge Management.

He is an Associate Professor and the Dean of the Faculty of Information Science and Technology at Multimedia University, Malaysia. He has worked there since 1999. Besides, he is also a member of Review Committee of Displays and Multimedia Cyberscape.

Pang Ying Han is born in Melaka, Malaysia, on the date of February 11, 1980. She received her bachelor in Engineering Degree majoring in electronics with first class Honors from Multimedia University, Malaysia in year 2002.

She is now employed in the Faculty of Information Science and Technology in Multimedia University, Malaysia as an academic staff. Her current research interests include many aspects of biometrics, computer vision, image understandings and neural networks.

Andrew Teoh Beng Jin is born in Penang, Malaysia, on October 20, 1975. He obtained his Bachelor Engineering in electronics in 1999 and Ph.D degree in 2004 from National University of Malaysia.

He is currently working as a lecturer in the Faculty of Information Science and Technology, Multimedia University, Malaysia. He is also the associate dean of this faculty. His research interests are multimodal biometrics, pattern recognition, multimedia signal processing and Internet security.