A Secure Touch-less based Fingerprint Verification System

Hiew Bee Yan[1], Andrew Teoh Beng Jin[2], Ooi Shih Yin[1], Fathin Fakhriah Abdul Aziz[1]

[1]Faculty of Information Science and Technology
Multimedia University, Jalan Ayer Keroh Lama,
75450 Melaka, Malaysia.
{byhiew, syooi, fathin.abd.aziz}@mmu.edu.my

[2]School of Electrical and Electronic Engineering,
Yonsei University, Seoul,
South Korea.
bjteoh@yonsei.ac.kr

ABSTRACT

Touch-less based fingerprint verification systems are free from the problems of image deformation, latent fingerprint issues and so forth that appear in the contemporary touch based fingerprint verification systems. Coupled with template protection mechanism, a touch-less fingerprint verification system is further enhanced. In this paper, a secure end-to-end touch-less fingerprint verification system is presented. The fingerprint image captured with a digital camera is first pre-processed via the proposed pre-processing algorithm. Then, Multiple Random Projections-Support Vector Machine (MRP-SVM) is proposed to secure fingerprint template while improving system performance.

Keywords

Touch-less based Fingerprint Verification, Template Protection, Support Vector Machine.

1. INTRODUCTION

A preponderance of the fingerprint sensors available today use "touch" method. However, the durability of a touch-based fingerprint scanner is weakened if it is used heavily. Additionally, the pressure of the physical contacts degrades the quality of the touch-based fingerprint images. Conversely, touch-less fingerprint acquisition technology is free from these problems [Son04]. Furthermore, touch-less based fingerprint verification systems have great potentials in building secure verification systems provided that they are free from latent fingerprint (the trail of the fingerprint on the contact surface of the sensor) issues which can lead to fraudulent use [Lee06a]. Hence, with the incorporation of cancellable biometrics in these fingerprint features, the security and privacy protection of fingerprint biometric templates are enhanced. Cancellable biometrics is a concept initiated to secure biometric templates. This concept is important because biometric templates are not revocable and their compromise is permanent [Sch99]. A good cancellable biometric formulation must fulfill four requirements [Mal03]: (i) diversity; (ii) reusability; (iii) one way transformation; (iv) performance.

1.1 Related Works

1.1.1 Touch-less Fingerprint Recognition

Digital Descriptor System Inc. (DDSI) [Mai06] produced the world first contact-less fingerprint capture device which can be integrated with Fingerprint Matching Solution [Dig00]. Later, TST Corona-GmbH developed biometric recognition systems using novel touch-less optical fingerprint scanning technology. Song et al. proposed a pre-processing technique for their custom designed touch-less sensor [Son04]. Using a strong view difference image rejection method, [Lee06a] resolved the three-dimensional (3D) to two-dimensional (2D) image mapping problem which appeared in [Son04]. Pre-processing of the fingerprint images captured with mobile camera has been proposed by [Lee06b]. To make 3D touch-less fingerprints interoperable with the current Automated Fingerprint Identification System (AFIS),

Chen et al. [Che06] proposed an unwrapping algorithm that un-folds the 3D touch-less fingerprint images into 2D representations which are comparable with the legacy rolled fingerprints.

1.1.2 Cancellable Biometrics

Ratha et al introduced the first notion of cancellable biometric formulation. The underlying idea is to generate deformed biometrics data by distorting the biometric image in a repeatable but non-reversible manner [Rat01]. Teoh et al. [And04] introduced another cancellable biometrics approach using iterative inner product between tokenized pseudo-random numbers (PRN) and biometric data. But, this formulation suffered from the stolen-token scenario when the genuine token is stolen and utilized by impostor to claim as the genuine user. Savvides et al. [Sav04] encrypted the training images which are used to synthesise the correlation filter for biometrics authentication. They showed that different templates can be obtained from the same biometrics by varying the random convolution kernels. Thus, those templates can be cancelled. Ang et al. [Ang05] generated a cancellable fingerprint template via a key-dependent geometric transformation on a minutiae based finger-print representation. Nevertheless, the matching accuracy is degraded notably in the distorted domain. In [Bou06], the authors introduced the concept of biometric-based tokens that support robust distance computations, which offers cryptographic security such that it can be revoked and replaced by a new one. Teoh and Chong [And07] introduced Multispace Random Projection (MRP) as one of the cancellable biometrics approaches that fulfils good cancellable biometrics requirements as stated above. However, the Equal Error Rate (EER) result is only 30% due to the poor classification capability of the matching metric.

1.2 Our Approach

A secure digital camera based fingerprint verification system is presented in this paper. This system uses "touch-less" method with a digital camera to capture fingerprint images. The problems appeared in the digital camera acquired fingerprint images are: (i) low ridges valleys contrast; (ii) defocus; and (iii) motion blurriness. To reduce these problems, the fingerprint images are pre-processed using the proposed method [Hie06]. To protect the template and improve the system performance, a variant of MRP [And07], named as Multispace Random Projections-Support Vector Machine (MRP-SVM), is proposed. MRP-SVM is performed after pre-processing. In MRP-SVM, MRP, which used normalized dot product, is replaced with a more powerful classifier – Support Vector Machine (SVM) while still retains the properties of MRP.

The outline of the paper is as follows: Section 2 provides the details of the proposed system. Section 3 shows the experiment results. Discussions are presented in Section 4. Finally, conclusions are given in Section 5.

2. TOUCH-LESS FINGERPRINT VERIFICATION ALGORITHM

2.1 Pre-processing

Initially, the captured fingerprint image in Red-Green-Blue (RGB) format is converted to grey scale [0-255]. To reduce the problem of non-uniform lighting in the image, local normalization is adopted to reduce the intensity variations in the image. Local normalization of $o(x_o, y_o)$ is computed as follows [Bio02]: $S(x_o, y_o) = \frac{o(x_o, y_o) \quad m_o(x_o, y_o)}{\sigma_o(x_o, y_o)}$ where $o(x_o, y_o)$ is the original image, $m_o(x_o, y_o)$ denotes an estimation of a local mean of $o(x_o, y_o)$, $\sigma_o(x_o, y_o)$ indicates an estimation of the local standard deviation. Next, the fingerprint region is segmented from the raw image by applying skin color detection, adaptive thresholding, and morphological processing [Hie06]. Then, the local normalized image is multiplied with the fingerprint binary mask to get the segmented image. The resulting image is cropped and enhanced by using the Short Time Fourier Transform (STFT) analysis [Chi05]. Subsequently, the ridge orientation is calculated and the core point is detected from the enhanced image [And03]. The true and false core point detections are obtained by: (number of true core point detected images/total number of fingerprint images) and (number of false core point detected images/total number of fingerprint images) respectively. The detail description can be obtained in [Hie06]. After the core point detection, the pre-processed image is created by cropping the local normalized image into a size of 200 x 200 with the core point as the centre.

2.2 Multispace Random Projections-Support Vector Machine (MRP-SVM)

2.2.1 Brief Review of Multispace Random Projections (MRP)

MRP covers two stages: (i) feature extraction: feature vector, $\boldsymbol{f} \in \Re^d$, with fixed length d is extracted; (ii) random projections: the feature vector is projected onto a random subspace, which is formed by externally derived random matrix, $\boldsymbol{R} \in \Re^{m \times d}$, where $m \leq d$. The $\boldsymbol{R}$ is formed by the independent, zero

mean and unit variance Gaussian distributed random bases. Thus, the user-specific random-projected vector, $\boldsymbol{p} \in \Re^m$ is described as

$$\boldsymbol{p} = 1/\sqrt{m}\boldsymbol{R}\boldsymbol{f} \quad (1)$$

During verification, the extracted feature vector is mixed with the genuine $\boldsymbol{R}$. The resulting vector is compared with the enrolled template using the normalised dot product, a dissimilarity measure, $\gamma = 1 - \boldsymbol{x}^T \boldsymbol{y}$, where $\boldsymbol{x}$ and $\boldsymbol{y}$ are the normalised feature vectors. From the performance perspective, three scenarios are considered when MRP is applied: (i) *Legitimate-token*: in which the genuine biometric is mixed with the user-specific token; (ii) *Stolen-token*: wherein an impostor has possessed genuine token and used by the impostor to claim as the genuine user; (iii) *Stolen-biometrics*: where an impostor assesses intercepted biometric data of high possibility to be considered genuine. Through the theoretical and experimental analysis [And07], Figure 1 illustrates the original system performance and performance behaviour of MRP in the legitimate-token, stolen-token and stolen-biometrics scenarios using the genuine-impostor distributions. By referring to Figure 1, MRP's genuine, impostor and genuine-impostor distributions in the legitimate-token, stolen-token and stolen-biometrics scenarios with its respective recognition performance are summarised in Table 1.

2.2.2 Multispace Random Projections-Support Vector Machine (MRP-SVM)

MRP-SVM is applicable to biometrics features represented in feature vector format. This technique consists of three stages: (i) feature extraction, (ii) random projection, and (iii) SVM classification.

2.2.2.1 Feature Extraction

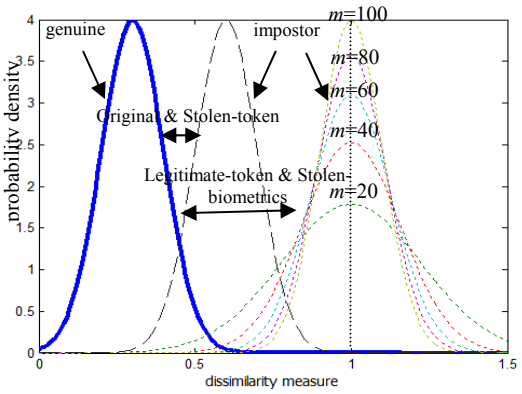

Figure 1. Genuine-impostor distributions of the original system and performance behavior of MRP in the legitimate-token, stolen-token and stolen-biometrics scenarios.

The individual's feature matrix is extracted from the pre-processed image through Gabor filter feature extractor. The adopted feature extraction method is similar to the method described in [Lee99]. Initially, the pre-processed images are sampled by Gabor filters. Given that a band of Ω Gabor filters is applied in an experiment, the filtered images are divided into a set of MxM non-overlapping blocks, respectively. The resulting magnitude will be next converted to a scalar number by calculating its standard deviation value. The scalar numbers form the Gabor features of each image. Finally, $N = (200/M) \times (200/M) \times \Omega$ Gabor features are extracted from each image.

Then, PCA is used to compress the feature vectors. An eigenspace is built during the training phase. During the testing phase, each testing Gabor feature vector is projected onto the eigenspace to form eigenGabors, $\boldsymbol{f}$ with feature length d [Tur91]. Before

Scenario	Genuine distribution (intra-class variation)	Impostor distribution (inter-class variation)	Genuine-Impostor Distributions	Recognition Performance
Legitimate-token Stolen-biometrics	Preserved	Impostor distribution is amplified. The mean is 1 whereby the curve is centred at 1; the distribution profile's shrinking rate (standard deviation) follows $1/\sqrt{Y}$.	Clear separation can be attained, hence zero EER, if Y is sufficiently large as depicted in Figure 1.	Significantly improved.
Stolen-token		Preserved	Reverts to its original state in feature vector level and thus the performance is retained as like original state before the random projection is performed.	Reverts to its original state in feature vector before MRP is applied.

Table 1. MRP's genuine, impostor and genuine-impostor distributions in the legitimate-token, stolen-token and stolen-biometrics scenarios with its respective recognition performance

applying Multi-space Random Projection, each eigenGabors is normalised to unit length, $\|\boldsymbol{f}\| = 1$.

2.2.2.2 Random Projection

Subsequently, the unit length feature vector is projected onto a random subspace as described in Section 2.2.1. The user-specific random-projection (RP) vector, $\boldsymbol{p} \in \Re^m$ is produced through the random projection process, which is defined in Eq. 1. The one way transformation property can be assessed by looking at Eq. (1). $\boldsymbol{p}$ can be regarded as a set of underdetermined systems of linear equations (more unknowns than equations) if $m < d$. Thus, it is impossible to find the exact values of all the elements in $\boldsymbol{f}$ by solving an underdetermined linear equation system in $\boldsymbol{p} = 1/\sqrt{m}\boldsymbol{R}\boldsymbol{f}$ if $m < d$, based on the premise that the possible solutions are infinite [And07]. The detail of the analysis can refer to [Kar05]. In the event of compromised, the template could be renewed by just changing $\boldsymbol{R}$ in Eq. (1) of the compromised biometric template. From this way, reusability property of MRP-SVM is fulfilled.

2.2.2.3 Support Vector Machine (SVM) classification

Then, the random projected vector $\boldsymbol{p}$ is fed into SVM [Bur98] to discriminate genuine and impostor. Let a training set be $(\boldsymbol{p}_i, q_i), i = 1, \cdots Q, \boldsymbol{p} \in \Re^m, q \in \{+1, -1\}$, where $\boldsymbol{p}_i$ either belongs to genuine's or impostor's random projection vector, q_i indicates the label (+1 for genuine, -1 for impostor), Q denotes the number of training samples, and m signifies the feature length. During training, SVM looks for an optimal hyper-plane, which takes the form $\boldsymbol{w}^T \boldsymbol{p} + b = 0$ where $\boldsymbol{w}$ is the normal to the plane, b denotes the bias term. The optimal hyper-plane is a separating hyper-plane, which gives the largest margin. Assuming that genuine and impostor samples are linearly separated, the Langrage Dual optimisation problem for maximal margin separation is:

$$\max. L_D = \sum_{i=1}^{Q} \alpha_i - 1/2 \sum_{i=1}^{Q} \sum_{j=1}^{Q} \alpha_i \alpha_j q_i q_j \boldsymbol{p}_i^T \boldsymbol{p}_j \quad (2)$$

subject to $\sum_{i=1}^{Q} \alpha_i q_i = 0$ and $C \geq \alpha_i \geq 0$ where α_i are the Langrage multipliers, C is the regularisation constant.

The extension to non-linear boundaries is determined through projecting each data point to a higher dimensional feature space [Bur98], which may be carried out through the use of kernels: (i) polynomial kernel as (the order of the polynomial) or (ii) radial basis function (RBF) kernel as (the width of the radial basis function). Subject to constructing the optimal hyper-plane for SVM with non-linear kernel involves the following dual:

$$\max. L_D = \sum_{i=1}^{Q} \alpha_i - 1/2 \sum_{i=1}^{Q} \sum_{j=1}^{Q} \alpha_i \alpha_j q_i q_j K(\boldsymbol{p}_i, \boldsymbol{p}_j) \quad (3)$$

During verification, $\boldsymbol{w}$ and b learned from training phase are used. The decision value, G_{dv} of a test sample of vector $\boldsymbol{p}$ for linear SVM and non-linear SVM are calculated by Eq. 4 and Eq. 5 respectively, where $\boldsymbol{p}_j$ are the support vectors.

$$G_{dv} = \boldsymbol{w}^T \boldsymbol{p} + b = \sum_{j=1}^{N_S} \alpha_j q_j \boldsymbol{p}_j^T \boldsymbol{p} + b \quad (4)$$

$$G_{dv} = \boldsymbol{w}^T \boldsymbol{p} + b = \sum_{j=1}^{N_S} \alpha_j q_j K(\boldsymbol{p}, \boldsymbol{p}_j) + b \quad (5)$$

$\boldsymbol{p}_j^T \boldsymbol{p}$ (in Eq.4) and $K(\boldsymbol{p}, \boldsymbol{p}_j)$ (in Eq.5) are a similarity measure comparing $\boldsymbol{p}$ (test sample) and $\boldsymbol{p}_j$ (support vectors) in input space and feature space respectively. G_{dv} is a weighted sum of the similarity between $\boldsymbol{p}$ and $\boldsymbol{p}_j$. Comparison is made between G_{dv} and a threshold, Th_{dv}. The claimed user is accepted if $G_{dv} < Th_{dv}$ and rejected if $G_{dv} \geq Th_{dv}$.

3. EXPERIMENT EVALUATION

3.1 Pre-processing Experiment Results

Pre-processing experiments are conducted by using all digital camera acquired fingerprint images (1938 images) described in [Hie06]. The results are assessed subjectively by visual inspection. The proposed pre-processing provides admirable results as shown in Figure 2. By counting the number of false core point detection, it reveals that the proposed pre-processing algorithm can achieve an accuracy of 95.44% of core point detection whereas the false core point detection is only 4.56%. Deep wrinkle, motion blurriness and defocus problems are the causes of the core point detection failure [Hie06].

Figure 3 depicts the comparison of the proposed algorithm to those of existing enhancement methods in the literature by using cropped local normalised images of our independent database. As illustrated by the region rounded by circles shown in Figure 3, some portions of the images are not enhanced fittingly by Hong enhancement and root filtering. It can be witnessed that the proposed algorithm performs more competent than Hong's and root filtering. It signifies that image cropping is needed to eliminate the gratuitous noisy background; local normalisation succours in reducing the non-uniform lighting effect.

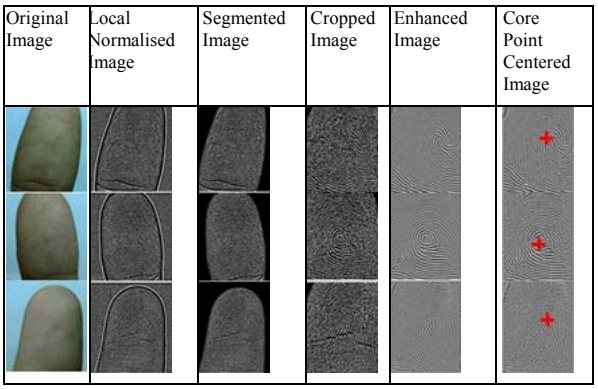

Figure 2. Results for the proposed pre-processing

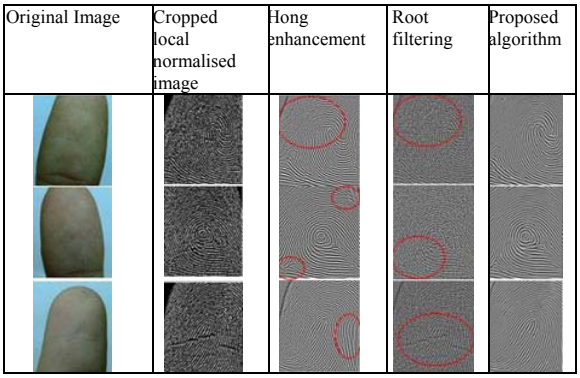

Figure 3. Comparative results for different enhancement algorithms

3.2 Verification Experiment Results without MRP

In lieu of using all of the raw images described in [Hie06] directly, a total of 1030 core point centred local normalised fingerprint images are used in performing the verification experiments. These fingerprint images originate from 103 different fingers with 10 images for each finger. The system performance is determined by using EER, i.e. False Accept Rate (FAR) = FRR. The lower the EER, the more accurate the system is considered to be.

The parameters of the Gabor filter feature extractor are set as: (i) number of Gabor filters (Ω)=6; (ii) frequency (f_g)=10; (iii) variance ($\sigma_{x_g}^2$ and $\sigma_{y_g}^2$)=128; (iv) number of non-overlapping blocks (M)=8. To get eigenGabors, the features derived from the Gabor filter based feature extractor are compressed using PCA. One Gabor feature vector from each finger class is used for training, while the rest will be used as testing data. The eigenGabors are normalised to be of unit length before verification test is conducted. The experiment setting is fixed and shown in Table 2. To enhance the reliability of the assessment, we perform ten runs for each of *Tr* samples with different random partitions between training and testing images, and the results are averaged.

The verification accuracy is tested using linear SVM, polynomial SVM and RBF SVM. To fix the feature length, the eigenvectors are extracted from the Gabor feature vectors with the dimensionality of 100.

Setting	No. of Training Image, *Tr*	No. of Testing Image, 9- *Tr*	No. of Client	No. of Impostor
1	1	8	8x103 =824	8x103x102 =84048
2	2	7	7x103 =721	7x103x102 =73542
3	3	6	6x103 =618	6x103x102 =63036
4	4	5	5x103 =515	5x103x102 =52530

Table 2. Configuration for the experiments using SVM on eigenGabors

Before comparing the performance of linear, polynomial and RBF SVM, the optimal parameter values for polynomial (degree) and RBF SVM (gamma and C) are investigated. This investigation is necessary as these parameter values will affect the results. In this study, the polynomial of degree between 2 and 5 are tested. Besides, different parameter values of RBF SVM (gamma=1, C=10; gamma=10, C=1; gamma=1, C=1; gamma=10, C=10) for both uncompressed Gabor features and eigenGabors are investigated. After the parameter value tuning, the best parameter values of polynomial SVM (degree=2) and RBF SVM (gamma=1 and C=10) are fixed for further evaluation tests. Table 3 shows the EER (%) results for linear, polynomial and RBF kernel with different number of training image, *Tr*. For *Tr*=1…4, it can be seen that the EER results of Linear SVM kernel is the worst while the EER results of RBF SVM kernel is the best. The best result (EER=1.23%) is obtained when *Tr*=4 and RBF SVM kernel is adopted as indicated in the table below.

Tr / SVM kernel type	1	2	3	4
Linear	18.89	9.47	6.48	4.21
Polynomial (degree=2)	14.57	6.26	3.25	1.76
RBF(gamma=1, C=10)	5.09	2.75	1.83	1.23

Table 3. EER Results (%) of linear SVM, polynomial SVM and RBF SVM using eigenGabors (dimensionality = 100) with different number of training image, *Tr*

3.3 Multispace Random Projection (MRP) Experiments

3.3.1 Performance Results

To evaluate the performance of MRP on the best performing SVM classifier, we conceal the eigenGabors through MRP before feature matching. During the experiment, setting 4 of Table 2 is adopted. Again, we perform ten runs for each of 4 samples with different random partitions between training and testing images. Then, the results are averaged. egsvm, mrpsvm-m, mrpsvm-m(stolen-token), mrpsvm-m(stolen-biometrics) denote eigenGabors, legitimate-token, stolen-token and stolen-biometrics scenarios respectively. The feature length of eigenGabors (egsvm) are fixed as $d = 100$. Besides, the eigenGabors is normalised to unit length before MRP. To infer the recognition performance, three different scenarios (as described in Section 2.2.1) are considered, i.e. legitimate-token, stolen-token and stolen-biometrics scenarios. For these three scenarios, the eigenvectors are extracted from the Gabor feature vectors with the dimensionality varied from 10 to 100 in intervals of 10. Later on, the normalized eigenGabors are used in these three different scenarios.

Table 4 shows the performance comparison of eigenGabors, legitimate-token, stolen token and stolen biometrics scenarios. From Table 4, for d=10…100, it is clearly shown that legitimate-token's EER results outperform the eigenGabors's EER results (egsvm in this context). Legitimate-token and stolen-biometrics scenario attain better EER results than the eigenGabors in the range of $40 \le m \le 100$. On the other hand, the EER of eigenGabors and stolen-token scenarios are equal when $m \approx d$. In other words, stolen-token scenario reverts the system to its original state when $m \approx d$.

For legitimate-token and stolen-biometrics scenarios, the MRP performance can be boosted through a classifier with better separation whilst the classifier quality will determine the performance of MRP in stolen-token scenario. However, it would not be poorer than its original method i.e. classification using eigenGabors without MRP. This is favourable in practical application whereby MRP survives either in stolen-token or in stolen-biometrics attack and also capable to offer significant improvement in verification setting with better classifier.

From Table 5, it can be observed that the impostor distribution's mean and standard deviation for both eigenGabors and stolen-token scenario are the same when $m \approx d$. Similar result can be seen in the genuine distribution where the mean and standard deviation of stolen-token scenario are equivalent to the mean and standard deviation of eigenGabors when $m \approx d$. This indicates that the preservation of genuine-impostor distribution is maintained under SVM framework when $m \approx d$. It is also depicted in Figure 4 where the separation of genuine-impostor class distribution for eigenGabors and stolen-token scenario is almost identical. The preservation of the intra-class variations (genuine distribution) as well as inter-class variations (impostor distribution) asserts that SVM statistical properties are preserved under the MRP framework.

3.3.2 Diversity Test

In order to fulfil the diversity requirement of cancellable biometrics, Pairwise Independent Test is conducted to inspect whether the MRP template with PRN A and MRP template with PRN B (both with same fingerprint feature) are associated. The same fingerprint feature is mixed with different PRNs. We observe that the scores generation procedure has followed the impostor distribution as described above. Figure 5 exhibits the Pairwise Independent Test of MRP. As indicated in Figure 5, the mean and standard deviation are 1.0177 and 0.2982, respectively. It can be concluded that MRP is Pairwise independent as the histogram of Figure 5 approaches the independent and similarly distributed (i.i.d) random variables drawn from Gaussian distribution, **N**(-1610.2, 407.3). This means that there is almost no correlation between the refreshed MRP template and old MRP template. Therefore, random number refreshment is equivalent to issue a new template to the user. In the real application, every user is assigned a unique random number. Hence, only the respective template is renewed in the event of compromise.

scenario \ *d*	10	20	30	40	50	60	70	80	90	100
mrpsvm-m	36.69	10.38	1.84	0.63	0.37	0.36	0.31	0.30	0.37	0.48
mrpsvm-m (stolen-biometrics)	35.98	11.06	2.23	0.87	0.70	0.56	0.43	0.42	0.49	0.57
mrpsvm-m (stolen-token)	39.75	14.58	4.80	2.31	1.58	1.51	1.16	1.12	1.19	1.23
egsvm										1.23

Table 4. EER results (%) of egsvm, mrpsvm-m, mrpsvm-m(stolen token) and mrpsvm-m(stolen biometrics) for RBF SVM with different feature length, *d*

scenario	m	$\mu_{genuine}$	$\mu_{imposter}$	$\sigma_{genuine}$	$\sigma_{imposter}$
egsvm	-	-0.6445	1.0668	0.4428	0.3188
mrpsvm-m (stolen-token)	100	-0.6445	1.0668	0.4428	0.3188
	90	-0.6582	1.1212	0.4410	0.3463
	80	-0.6742	1.1880	0.4380	0.3776
	70	-0.6867	1.2799	0.4363	0.4298
	60	-0.6935	1.3971	0.4549	0.5094
	50	-0.6897	1.5195	0.4517	0.5755
	40	-0.6440	1.6600	0.5040	0.6513
	30	-0.3766	1.7365	0.5865	0.6831
	20	0.4513	1.3946	0.3854	0.5092
	10	0.9244	1.0647	0.2172	0.3227

Table 5. Statistics measurement of egsvm and mrpsvm-m(stolen-token) for RBF SVM

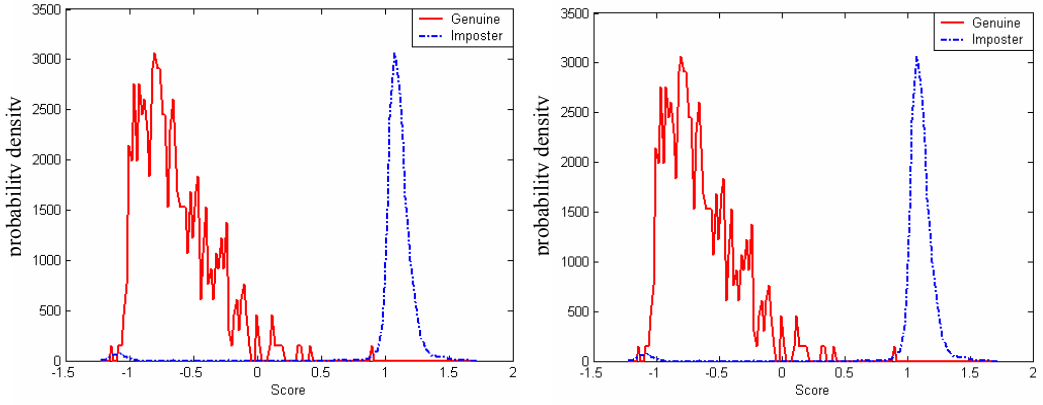

Figure 4. Genuine and impostor class distribution for: (a) egsvm; (b) mrpsvm-m (stolen- token).

4. DISCUSSIONS

MRP maps the data onto a random subspace while preserving the pair-wise distance that is quantified by dot product. Hence, MRP can be generalised for Linear SVM as the original data points are quantified by the dot product, $\boldsymbol{p}_i^T \boldsymbol{p}_j$ in Lagrange dual optimisation problem as shown in Eq. 2. Furthermore, a dot product $\boldsymbol{p}_j^T \boldsymbol{p}$ also appears in decision stage as exhibited in Eq. 4. Therefore, SVM inherited the MRP characteristics that described in [And07]. As stated in Section 2.2.2.3, to extend the idea to non-linearly separable data, a non-linear kernel is needed. The dot product of $\boldsymbol{p}_i^T \boldsymbol{p}_j$ in input space is substituted with $K(\boldsymbol{p}_i, \boldsymbol{p}_j)$ in the Langrage dual optimisation problem as displayed in Eq. 3. On the other hand, the dot product of $\boldsymbol{p}_j^T \boldsymbol{p}$ in input space is substituted with $K(\boldsymbol{p}, \boldsymbol{p}_j)$ in deciding the decision value as shown in Eq. 5. The non-linear kernel measures the similarity between two feature vectors. Typically, it represents the dot product between two representations in the transformed space in which the data are linearly separable.

The inheritance of the MRP characteristics (e.g. reusability and diversity properties) by MRP-SVM is concretised by the experiment results given in Section 3.3.2. The experiment results shown in Table 5 and Figure 4 deliver our assertion that SVM statistical properties are preserved under the MRP framework.

In short, SVM is another classifier that can be used in MRP as it contains the property of dot product and non-linear kernel. SVM is still preserved under MRP framework. Moreover, it has better discrimination power compared with normalised matching metric.

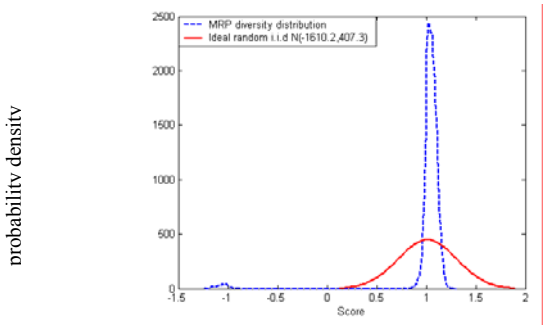

Figure 5. Pairwise Independent Test of MRP using RBF SVM

5. CONCLUSIONS

A complete secure digital camera based fingerprint verification system is proposed. This system uses "touch-less" based method. The proposed pre-processing which encompasses of skin colour detection, local normalisation, fingerprint segmentation, image enhancement, and core point detection resolves the problems exist in its images. After pre-processing, MRP-SVM which comprises Gabor feature extraction, PCA, MRP and SVM verification is performed. The employment of MRP-SVM protects the template whilst improving system performance. In MRP-SVM, SVM with high discrimination power is preserved under MRP framework as it has the property of dot product and non-linear kernel. Experiments show that MRP-SVM contributes high recognition performance and functions well without compromising the verification performance in the event of compromised token. MRP-SVM is proven to fulfil other cancellable biometrics properties, i.e. diversity property and non-reversible property into the bargain.

6. REFERENCES

[And03] Andrew Teoh, B. J., Ong, T. S., David Ngo, C. L. and Sek, Y. W.. Automatic Fingerprint Center Point Determination by Using Modified Directional Field and Morphology. in *AI 2003: Advances in Artificial Intelligence: 16th Australian Conference on AI*, 2003.

[And04] Andrew Teoh, B.J., David Ngo, C.L and Alywn Goh. Personalised Cryptographic Key Generation Based on FaceHashing. *Computers and Security J.*, No. 23, pp. 606-614, 2004.

[And07] Andrew Teoh, B.J. and Chong, T.Y. Cancellable Biometrics Realization with Multispace Random Projections. *IEEE Transaction on Systems, Man and Cybernetics Part B - Special Issue on Recent Advances in Biometrics Systems* 37, No. 5, pp.1096-1106, 2007.

[Ang05] Ang, R., Rei, S. N. and McAven, L. Cancelable Key-Based Fingerprint Templates. in *Proceedings of The 10th Australasian Conference on Information Security and Privacy*, pp. 242-252, 2005.

[Bio02] Biomedical Imaging Group. Local Normalization. [Online] http://bigwww.epfl.ch/demo/jlocalnormalization/, 11 February 2002.

[Bou06] Boult, T. Robust Distance Measures for Face-recognition supporting revocable biometrics token. in *7th International Conference Automatic Face and Gesture Recognition* 2006.

[Bur98] Burges, C. J. C. A Tutorial on Support Vector Machines for Pattern Recognition. *Knowledge Discovery and Data Mining* 2, No.(2), pp. 121-167, 1998.

[Che06] Chen, Y., Parziale, G., Diaz-Santana, E. and Jain, A. 3D Touchless Fingerprints: Compatibility with Legacy Rolled Images. in *Proceedings of Biometric Symposium, Biometric Consortium Conference*, 2006.

[Chi05] Chikkerur, S., Cartwright, A. and Govindaraju, V. Fingerprint Image Enhancement Using STFT Analysis. in *Pattern Recognition*, pp. 198-211, 2005.

[Dig00] Digital Descriptor Systems Inc. Amendment to Registration of Securities of a Small-Business Issuer. [Online]http://www.secinfo.com/dsvrb.52N5.htm, 2000.

[Hie06] Hiew, B.Y., Andrew Teoh, B.J. and David Ngo, C.L. Preprocessing of Fingerprint Images Captured with a Digital Camera. in *9th International Conference on Control, Automation, Robotics and Vision (ICARCV 2006)*, 2006.

[Kar05] Kargupta, H., Datta, S., Wang, Q., Sivakumar, K. Random-data perturbation techniques and privacy-preserving data mining. *Knowledge and Information Systems* 7, No.4, pp. 387-414, 2005.

[Lee99] Lee, C. J. and Wang, S. D. Fingerprint Feature Extraction using Gabor filters. *Electronics Letters* 35, No. 4, pp. 288-290, 1999.

[Lee06a] Lee, C., Lee, S. and Kim, J. A Study of Touchless Fingerprint Recognition System. in *Proceedings of Joint IAPR International Workshops, SSPR 2006 and SPR 2006*, pp.358-365, 2006.

[Lee06b] Lee, C., Lee, S., Kim, J. and Kim, S. Preprocessing of a Fingerprint Image Captured with a Mobile Camera. in *Proceedings of International Conference on Biometrics*, pp. 348-355, 2006.

[Mai06] Mainguet, J. F. Fingerprint Sensing Techniques. [Online] http://perso.orange.fr/fingerchip/biometrics/types/fingerprint_sensors_physics.htm, 2006.

[Mal03] Maltoni, D., Maio, D., Jain, A. K. and Prabhakar, S. *Handbook of Fingerprint Recognition*, New York: Springer-Verlag, 2003.

[Rat01] Ratha, N., Connell, J. and Bolle, R.. Enhancing Security and Privacy in Biometrics-based Authentication Systems. *IBM System Journal* 40, No. 3, pp. 614–634, 2001.

[Sav04] Savvides, M., Vijaya Kumar, B. V. K. and Khosla, P. K. Cancelable Biometrics Filters for Face Recognition. *Int. Conf. of Pattern Recognition*, No. 3, pp.922-925, 2004.

[Sch99] Schneider, J. Biometrics: Uses and Abuses. *Commun. ACM.*, No. 42, pp.136, 1999.

[Son04] Song, Y., Lee , C. and Kim, J. A New Scheme for Touchless Fingerprint Recognition System. in *Proceedings of International Symposium on Intelligent Signal Processing and Communication Systems*, pp.524- 527, 2004.

[Tur91] Turk, M. and Pentland, A. Eigenfaces for Recognition. *Journal of Cognitive Neuroscience*, 1991.