# Reissuable Biometrics through Image-Based Handwritten Signature Verification

**Shih Yin Ooi†, Andrew Beng Jin Teoh††, Ying Han Pang†††, Bee Yan Hiew††††, and Fu San Hiew†††††**

†, †††, ††††Faculty of Information Science and Technology, Multimedia University, Jalan Ayer Keroh Lama, 75450 Melaka, Malaysia
††School of Electrical and Electronic Engineering, Yonsei University, Seoul, South Korea
†††††Infineon Technologies (Malaysia) Sdn. Bhd., Free Trade Zone, Batu Berendam, 75450 Melaka, Malaysia.

**Summary**
The privacy invasion of the biometric technology is getting public concerns due to the fact that biometric characteristics are immutable. In other words, their compromise is permanent. Reissuable biometrics was devised to make the reissuable or replaceable of biometric templates possible once they are found compromised. *Biometric Strengthening* is a form of reissuable biometrics. It strengthens the biometric templates by transforming the original template values to form a new set of values through the Gaussian distribution. The performance of *Biometric Strengthening* is evaluated in three possible intrusion scenarios. Probabilistic neural network (PNN) is employed as classifier. The compatibility of *Biometric Strengthening* and PNN shows the potential of using them in real world application. The experiments are tested on own image-based handwritten signature data set due to the lack of benchmark database.

***Key words:***
*Biometrics (Cancellable); Biometrics (Verification); Image Classification; Image Feature Extraction*

## 1. Introduction

Biometrics itself contains no personal information, as in it never reveals the real name or address like what identification card does. This makes it more difficult to forge or steal. However, the real fear occurs when a biometric identifier (i.e. face image, fingerprint image, handwritten signature image, etc) and a person are linked together in a database. Unlike names, or addresses, which can be changed over time, most of the biometrics are relatively stable and cannot be replaced once it is compromised. Therefore, the most serious privacy dilemma confronting biometric technology is not one of physical intrusiveness, but rather one of personal autonomy.

## 2. Motivation and Contribution

Due to the privacy concerns, Bolle et al. [1] proposed the methodology of cancellable biometrics. It has received wide attentions to protect the secrecy of the biometrics database throughout the years. General idea of cancellable biometrics is to store a transformed version of the biometric data (cipher data). It provides a higher level of privacy in terms of its ability to generate multiple different templates from the same biometric data. Different templates can be created easily by just swapping the set of cancellable keys. This is to ensure that each template stored in every single application will not be repeated. The detailed survey of these approaches can be found in manuscript by Uludag et al. [2].

Cancellable biometrics consists of an intentional and repeatable distortion of a biometric data based on a specific transform. Once a transform method has been defined, the biometric data will be distorted in the same fashion at each presentation (from the process of enrollment to authentication). Some relevant works are discussed below.

Ratha et al. [3] used a high-order polynomials function to transform the fingerprint minutia features in non-invertible manner. Goh and Ngo [4] combined the extracted face features with a set of pseudo random data (one-way hash function) to generate a unique discretized code for every individual. This method is named as BioHashing. BioHashing is implemented through iterated inner product between the pseudo random number/key and the face features. Each bit on the sign is determined based on a predefined threshold. During verification process, the input face template is biohashed and matched against the stored non-invertible discretized code. This work was extended by Teoh et al. [5] later. The error rate was minimized when a legitimate token was used. However, the performance degraded remarkably when the legitimate token was stolen and used by the imposter to claim as the legitimate user (stolen-token verification scenario).

This creates a serious problem especially in practical application. This issue was widely discussed by Cheung et al. [6] and Nanni et al. [7]. Cheung et al. [6] commented that the non-invertible random mixing process, i.e. BioHashing will destroy the optimality of most feature

Manuscript received June 5, 2013
Manuscript revised June 20, 2013

representations. They believed this may lead to deterioration of recognition accuracy. Nanni et al. [7] rebutted Cheung et al.'s argument by using a multi-matcher fusion technique to alleviate the stolen-token problem. However, the reduction in error rate was not significant and the method used was complex. Later, Teoh et al. [8] employed a modified probabilistic neural network as the classifier to solve the problem.

In this work, we proposed the *Biometric Strengthening* as a reissuable biometrics. The idea is adopted in the application of handwritten signature verification. The word of "reissuable" denoted that a template can be reissue and replace once it is found compromised. The main function of *Biometric Strengthening* is to combine a helper data (strengthen data in our case) with biometric data. Posses the same problem as other cancellable biometric techniques, the performance degraded greatly in stolen-token verification scenario. However, this problem can be entirely solved by using the original probabilistic neural network (PNN) as the classifier. PNN able to learn the *Biometric Strengthening* training samples very fast and the new training data can be added anytime without the need to retrain the entire network. This is an important factor especially for real-time application. Furthermore, PNN discriminates the distinct templates very well and is able to provide low error rates in both legitimate token and the stolen-token scenarios.

## 3. Preprocessing

Any ordinary scanner can be used as an image acquisition device. However, the scanning hardware may introduce certain noises to a signature image. Another source of noise may be speckled paper background where the signature is signed on. These noises on signature image may affect the feature extraction process. Therefore, they need to be removed. But preprocessing methods should be selected carefully as they may also remove the signature properties which are peculiar to a signatory.

We used a median filter to smooth the image of a signature although the real noise distribution is not figured out. The using of median filtering is quite similar to the mean filtering. Each output pixel will be set to an average of the pixel values in the neighborhood of the corresponding input pixel. The only difference is during the median filtering, the value of an output pixel is determined by the median of the neighborhood pixels, instead of mean.

The median is calculated by first sorting all the pixel values from the surrounding neighborhood into numerical order, and the considered median would be the middle pixel value. If the neighborhood under consideration contains an even number of pixels, the average of the two middle pixel values is used.

The median is a more robust average than the mean. This is because the single very unrepresentative pixel in a neighborhood will not affect the median value significantly. Besides, due to the fact that median value must actually be the value of one of the pixels in the neighborhood, the median filter does not create new unrealistic pixel values when the filter straddles an edge. Therefore, we believed that the median filter is much better at preserving sharp edges than the mean filter.

## 4. Feature Extraction

### 4.1 Discrete Radon Transform (DRT)

Inspired by the works of Coetzer et al. [9], discrete Radon transform (DRT) is used to transform the signature images into a feature space. This transformed feature space is very useful in our subsequent matching process. Assume that each signature image consists of $N$ pixels in total, and intensity of the ith pixel is denoted by $I_i$, $i = 1,\ldots, N$. The DRT is calculated by using $\beta$ non-overlapping beams per angle and $\Theta$ angles in total. The cumulative intensity of the pixels that lie within the $j^{th}$ beam ($j^{th}$ beam sum) can be denoted as $R_j$, $j = 1,\ldots, \beta\Theta$. In discrete form, the Radon transform can therefore be expressed as below:

$$R_j = \sum_{i=1}^{N} w_{ij} I_i,\ j = 1,2,\ldots,\beta\Theta, \tag{1}$$

$w_{ij}$ indicates the contribution of the $i^{th}$ pixel to the $j^{th}$ beam sum. The value of $w_{ij}$ is determined through two-dimensional interpolation. Each projection contains the beam sums which calculated at a given angle ($\Theta$). In this work, $\Theta$ is set as 180°.

### 4.2 Principle Component Analysis (PCA)

The limitation is that the DRT-transform values are quite massive to process. Therefore, principle component analysis (PCA) (Turk et al., [10]) is adopted to compress the said values. The compressed group of signatures is known as *eigensignature*. If the training sets of signature images are $I_1$, $I_2$, $I_3$, …, $I_M$. Then, the average signature of the set can define as below:

$$\Upsilon = \frac{1}{M}\sum_{n=1}^{M} I_n \tag{2}$$

Each signature differs from the average by the vector $\Phi_i = I_i - \Upsilon$. This set of very large vectors is then

subject to principal component analysis, which seeks a set of *M* (number of images in the training set) orthonormal vectors $v_n$ and their associated eigenvalues $\lambda_k$ which best describes the distribution of the data. The vectors $v_n$ and scalars $\lambda_k$ are the eigenvectors and eigenvalues of the covariance matrix:

$$C = \frac{1}{M}\sum_{n=1}^{M} \Phi_n \Phi_n^{\mathrm{I}} = \frac{1}{M} AA^T, \quad (3)$$

where the matrix A = [$\Phi_1$, $\Phi_2$, …, $\Phi_M$]. Obviously, the matrix *C* is of dimensions $N^2$ X $N^2$ where $N^2$ is representing the number of pixels in the images. It is evident that the eigenvectors of *C* can span an algebraic eigenspace and provide an optimal approximation for those training samples in terms of the mean-square error.

## 5. Biometric Strengthening

The *Biometric Strengthening* transforming the feature values through the Gaussian distribution. It is believed to preserve enough actual identification markers to make the distortion repeatable. Each bit on the sign is decided based on the particular feature value. These transformed feature values are known as strengthen data (act as helper data in our algorithm). The general idea of methodology is described as below:

1. Feature extraction: DRT is used to extract the image-based signature feature. The dimensionality of the DRT-transformed values is reduced through PCA. The final output is in vector format. The normalized PCA extracted coefficient, *v*:

$$v = \{v_i \mid i = 1,...,n\}, -1 < v_i < 1, \quad (4)$$

2. The probability density function (*p.d.f*) of $v_i$ is computed with:

$$p_i = \frac{1}{\sqrt{2\pi}} e^{(-v_i)^2} \quad (5)$$

3. Compute the pi with $\underset{+,-}{\Lambda}$, where the operation may take in either $v_i + k^* p_i$ or $v_i - k^* p_i$. *k* denotes a constant value while the occurrence of addition (+) and subtraction (−) is followed by the sign of v, sign ($v_i$). There are two ways to assign the sign bit: (a) store the sign bit straightforward from the PCA feature during enrolment and use it for authentication; or (b) using the token to generate the sign bit and applying it in the *Biometric Strengthening* process.
4. Finally, the *strengthen* data, $v^s$ is done via:

$$v^s = \{\underset{+,-}{\Lambda}[v^i, k * p_i(v_i)] \mid i = 1,...,n\} \quad (6)$$

The *strengthen* data, $v^s$ is represented by real number instead of binary number. Despite of maintaining the original handwritten signature image, a template of the distorted image (*strengthen* data) will be stored in the centered database. When the user returned to the scanner, his or her signatures will be transformed according to the same pattern via the token-stored sequence map. This will create a match with the transformed image (cipher data) in the database.

## 6. Probabilistic Neural Network (PNN)

PNN is a kind of radial basis network based on the Bayes-Parzen classification ([11], [12]). PNN consists of three layers. Besides the input layer, it contains a pattern, summation and output layers. The pattern layer contains one neuron for each input vector in the training set, while the summation layer contains one neuron for each class to be recognized. The output layer merely holds the maximum value of the summation neurons to yield the final outcome.

In the learning mode, a collection of training signature samples is used to train PNN. Each of them models a Gaussian function centered at the training case. There is only one output unit per signatory. Each connected to all of the summation layers which are belong to the respective signatory, and at the same time, with zero connections from all other summation layers (representing other signatories). Hence, the output units simply add up the responses of the units which belong to the respective signatory. To estimate the probability density functions of the various signatories, each of the outputs is proportional to the kernel-based. This makes the interpretation of output easier.

PNN can be trained in a much easier way as compared to backpropagation. The network is established by setting the weights of the network with the training sets. The modifiable weights of the first layer are set by:

$$\varpi_{ij} = P_{ij} \quad (7)$$

where $\varpi_{ij}$ denotes the weight between $i^{th}$ neuron of the input layer and $j^{th}$ neuron in the pattern layer. $P_{ij}$ is the

value of the $i^{th}$ variable of pattern $j$ in training set. The second layer weights are set by:

$$\varpi_{jk} = T_{jk} \tag{8}$$

where $\varpi_{jk}$ is the weight between neuron $j$ in pattern layer and neuron $k$ of the output layer, and $T_{jk} = 1$ if pattern $j$ of the training set belongs to class $k$, else, $T_{jk} = 0$. After the network is trained, it can be used for classification task. The output of the pattern layer is calculated through the radial basis function:

$$out_j = \exp\left( -\frac{\sum_{i=1}^{n} \left( x_i \times \varpi_{ij} \right)}{\sigma_j} \right) \tag{9}$$

where $out_j$ is the output of neuron $j$ in pattern layer, $x_i$ is the value of variable $i$ for an input pattern in the testing set. The input of the summation layer is calculated with the following equation:

$$in_k = \sum_{j=1}^{n} out_j \times \varpi_{jk} \tag{10}$$

where $in_k$ is the input of neuron $k$ in output layer. The outputs of summary layer are binary values, $out_j = 1$ if $in_k$ is larger than input of other neurons, else $out_j = 0$.

The smoothing parameters ($\sigma_1$, $\sigma_2$, …, and $\sigma_j$) need to determine carefully in order to obtain an optimal network. This factor needs to be selected wisely so that a reasonable amount of overlap can be obtained; too small deviations will cause a very spiky approximation which makes the generalization impossible, while too large deviations will smooth out the details. The straightforward way to obtain an appropriate figure is to select a number which produces a low selection error. This can be done through experiments. Fortunately, PNNs are not too sensitive to the precise choice of smoothing factor.

For convenience sake, we use a straightforward procedure to select the best value for σ. Firstly, an arbitrary value of σ is chosen to train the network, and then test on a test set. This procedure is repeated for another σ's values and the σ giving the least errors will be selected.

The training time complexity can be represented as:

$$O(Mp) \tag{11}$$

$M$ denotes the input vector dimension (for our case, depicts the length of PCA-compressed feature data), while $p$ denotes the size of training samples.

## 7. Experiments and Discussion

### 7.1 Database Set-Up

Due to the lack of benchmark image-based handwritten signature database, we constructed own database with total of 1000 signatures: 500 genuine signatures, 250 casual forgeries and 250 skilled forgeries. They are collected from 50 signatories and 5 forgers for a period of 2 months. Due to the non-repetitive nature of variation in the produced signatures (even among the same writers), the data preparation was intentionally divided into two stages. In the first stage, five sample signatures were collected from each writer. This session producing 250 samples. Second stage was conducted one month after the initial session. Another five sample signatures were collected from each writer again. This yields another 250 samples.

To obtain casual forgeries, the forgers were allowed to view the writer's name but not the writer's real handwritten signatures. After obtaining the casual forgeries, the same group of forgers was requested to produce the skilled forgeries. In order to get high quality skilled forgeries, the forgers were provided with several real handwritten signature samples for each writer to refer and practice on.

The pen or pencil used is not prescribed but signatures are written within a pre-drawn 5 x 2 grid on A4 paper. These signatures were scanned into the computer using a 24-bit millions of colors, 600 dot-per-inch resolutions. The individual images are extracted and labeled with the writer names and the signature class number. Only 'perfect' signatures are considered, i.e. no deterioration of the signatures such as the introduction of smears, scratches, etc, is allowed.

The experiment schemes are designed as follow: four samples of each person are sequentially selected for Eigen basis construction and the remaining six samples are used for testing. The distance metric used is cosine angle.

### 7.2 Performance Evaluation

The system is evaluated based on false acceptance rate (FAR), false rejection rate (FRR), total success rate (TSR), equal error rate (EER) and genuine acceptance rate (GAR). Table 1 shows the verification rates for the different groups of forgery after combining with *strengthen* data.

*Biometric Strengthening* has significantly increased the overall performance of the three forgery types. This indicate that the more powerful the original method (in our case, when PCA length = 100), the higher verification rate can be yield when combined with *strengthen* data. From the result, it is able to yield EER of 1.10%, 1.20% and 2.10% for random forgery, casual forgery and skilled forgery respectively. This is a significant improvement to the accuracy of the contemporary biometric system as the

interdependency between FAR and FRR can be eliminated.

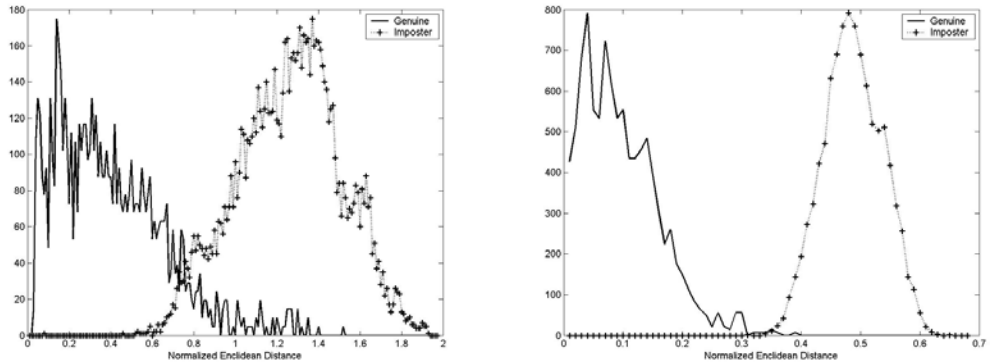
To fully utilize the *Biometric Strengthening*, a constant value, *k* needs to be determined. Different constant values ($k$ = 0.1; 0.3; 0.5; 0.7; 0.9) have been tested, and we found that the constant value of $k$ = 0.7 leads to a better result with low FAR and high GAR in this application. Thus, 0.7 has been set as *k* for the entire experiments.

Table 1: Verification rates of the three forgery types after combining with *strengthen* data, tested on bit lengths from 10 to 150

| Types of Forgery | Number of PCA Feature Length | FAR (%) | FRR (%) | TSR (%) | EER (%) |
|---|---|---|---|---|---|
| Random Forgery | 10 | 3.30 | 3.00 | 96.70 | 3.15 |
| | 50 | 2.93 | 3.00 | 97.07 | 2.96 |
| | **100** | **1.20** | **1.00** | **98.90** | **1.10** |
| | 150 | 1.20 | 1.00 | 98.90 | 1.10 |
| Casual Forgery | 10 | 4.21 | 3.00 | 95.80 | 3.61 |
| | 50 | 3.10 | 3.00 | 96.95 | 3.05 |
| | **100** | **1.25** | **1.15** | **98.80** | **1.20** |
| | 150 | 1.25 | 1.15 | 98.80 | 1.20 |
| Skilled Forgery | 10 | 5.27 | 5.07 | 94.83 | 5.17 |
| | 50 | 4.33 | 4.27 | 95.70 | 4.30 |
| | **100** | **2.11** | **2.09** | **97.90** | **2.10** |
| | 150 | 2.11 | 2.09 | 97.90 | 2.10 |

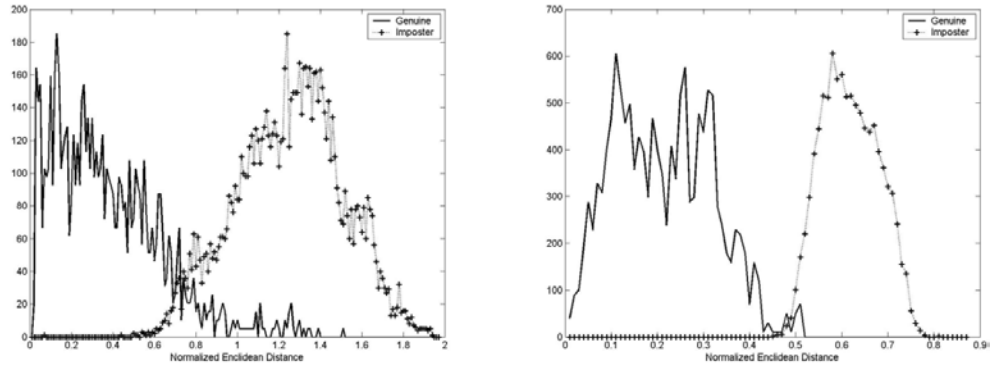
Besides being able to achieve high verification rate, another superiority of *Biometric Strengthening* is that it can separate the genuine and imposter into two clean distributions. Figures 1, 2 and 3 illustrate this phenomenon clearly by plotting the genuine and imposter population of the respective forgery.

From the figures, there are two peaks in the distributions at each histogram. One peak corresponds to genuine matching and another one corresponds to imposter matching. The left statistical distributions on each graph show the result when genuine population are compared; while the distributions on the right are the results for the comparison among different signatures (imposter populations).




(a) (b)

Fig. 1 Genuine and imposter distribution for random forgery when (a) original method and (b) combining with *strengthen* data.




(a) (b)

Fig. 2 Genuine and imposter distribution for casual forgery when (a) original method and (b) combining with *strengthen* data.

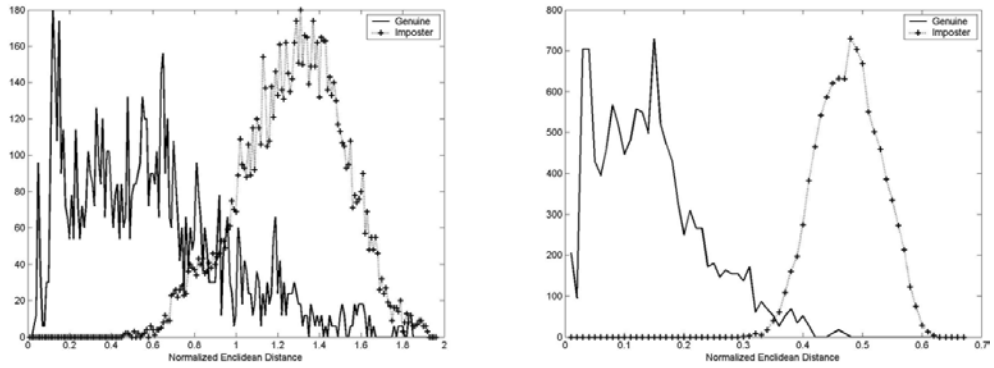



Fig. 3 Genuine and imposter distribution for skilled forgery when (a) original method and (b) combining with *strengthen* data.

The clear separation between the two populations is a good indicator for the FAR-FRR interdependency problem. Besides that, the decreasing mean and variance values obtained from the histograms denote that the *Biometric Strengthening* is able to minimize the intra-class (intrapersonal) distance while maximizing the inter-class (interpersonal) distance. The mean and variance values can be found in Table 2.

Table 2: Statistic data for the genuine and imposter population for: random forgery, casual forgery and skilled forgery

| Forgery Types | Genuine population | | Impostor Population | |
|---|---|---|---|---|
| | Mean | Variance | Mean | Variance |
| Random Forgery | 0.2146 | 0.0210888 | 0.7359 | 0.0093375 |
| Casual Forgery | 0.21401 | 0.0198979 | 0.61431 | 0.0123787 |
| Skilled Forgery | 0.14593 | 0.012269 | 0.6389 | 0.012636 |

From the result, we can see that the proposed technique – *Biometric Strengthening* is able to narrow the imposters' opportunities to gain access to the users' personal data.

## 7.3 Security Analysis: Performance Evaluation

Application of *Biometric Strengthening* for image-based signature verification presumes that each signatory is associated with a portable device (for instance, it can be a USB token or a smart card) where the unique formulation map sequence is derived. This could raise the possibility of two identity theft scenarios:

1. Stolen-token: the fraudulent verification which attempted using only the legitimate token without knowledge of the user-specific signature (applicable to random and casual forgeries).
2. Stolen-biometrics: the fraudulent verification which attempted using only the intercepted signature of sufficiently high quality (applicable to skilled forgery) associated with the genuine user, but without the associated token.

**Scenario 1:**

This case presumes that the identity theft gets hold of the genuine signatory's token credential without possessing the valid signature. To simulate the scenario, the respective external input (i.e., USB token or smart card) is used to generate the unique map sequence for all 50 user classes in our random and casual forgeries database respectively. The simulation results are shown in Figure 4 when random forgery combined with valid map sequence and Figure 5 when casual forgery combined with valid map sequence.

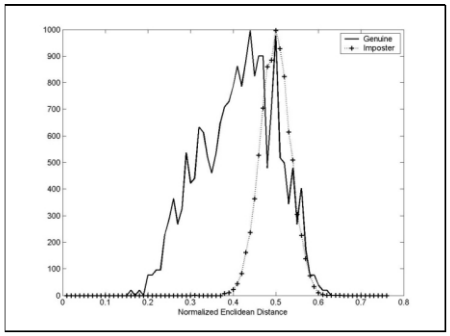



Fig. 4 Genuine and imposter populations of random forgery for stolen-token case.

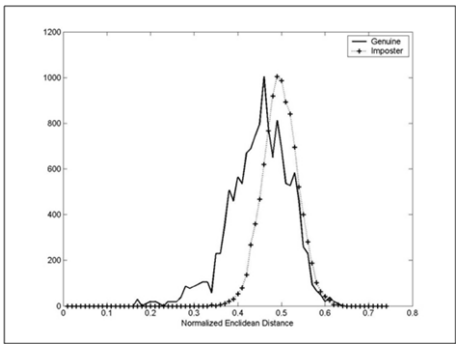



Fig. 5 Genuine and imposter populations of casual forgery for stolen-token case.

Both having strong overlapping in between two populations and blunt drop-off in the genuine population addressed the loss of unique map sequence for the genuine signatory. This depicts that when the respective map sequence combined with non-legitimate signatures, our system will treat it as a fraudulent validation.

**Scenario 2:**

This case presumes that the identity theft gets accessed to the signatory's original signature, and producing a high quality skilled forgery which is closely similar with the original signature without possessing the valid sequence map (token). To simulate the scenario, the different external input (i.e., USB token or smart card) is used to generate the non valid map sequence for all 50 user classes in our skilled forgery database respectively. The simulation result is shown in Figure 6.

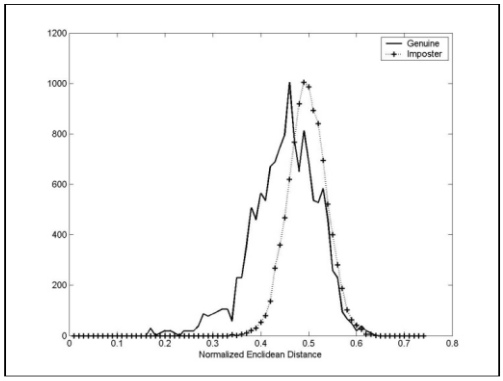



Fig. 6 Genuine and imposter populations of skilled forgery for stolen-biometrics case.

Again, a similar outcome as Figure 4 and 5 is obtained. The strong overlapping in between genuine and imposter population reveals that the uniqueness of combination for *strengthen* data and genuine signature vanished when different random sequence pattern is used to mix with the skilled forgery. This depicts that although identity theft can hold the actual signature, but without the valid sequence map (token), our system will treat it as fraudulent validation. This experiment also proving its diversity property in which the different map sequence will be used for different applications or agencies, where there is no chance for the identity theft to access through the signatory's other profiles even he has accessed through one of them.

However, it would not entirely solve the replaceability problem of biometrics in the sense that if an imposter gets hold of a user's actual signature (skilled forgery case) and makes a passable model (stolen-token case); he could still wreak havoc with it. By illustrating the reality of risk, our system would let the user to quickly reissue the compromised biometric profile (signature) and generate a new one, akin to replacing a lost or stolen credit card.

## 8. Compatibility with Probabilistic Neural Network (PNN)

As mentioned previously, the main drawback of *Biometric Strengthening* is its great degradation in performance when the legitimate token and legitimate biometrics are being stolen together and used by the imposter to claim as the legitimate user. Although the *Biometric Strengthening* alteration is invertible, in which there is no way to intercept the *strengthen* code by knowing either the alteration or biometric data (signature) alone; but if this is the case where the skilled forger can produce exactly the signature and by holding the *strengthen* code, he still can hack into the system. Therefore, detecting skilled forgery becomes a challenging task in real world application. To alleviate this problem, we proposed to employ a probabilistic neural network (PNN) as the classifier.

This method is evaluated by using only the skilled forgery from the same independent database. We randomly select 4 *Biometric Strengthening* templates for training and the other for testing purposes. ${}^{10}C_4 = 210$ runs are performed with different partitions between the training and testing sets by using a smoothing parameter of $\sigma = 10$. This process is repeated for five times per each run and the results are averaged to reduce the statistical frustration caused by the random alteration from *Biometric Strengthening* process. The association of *Biometric Strengthening* and PNN yielding EER of 1.5% with PCA length = 100, *Biometric Strengthening* constant value, $k$ = 0.7 and PNN smoothing parameter, $\sigma = 10$, which is better than the association of *Biometric Strengthening* and cosine angle (EER of 2.1%). The result is shown in Figure 7 (Legitimate-Token: PNN).

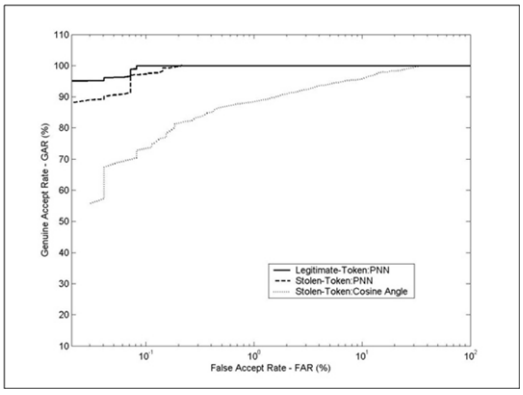



Fig. 7 ROC curve of skilled forgery for the association of *Biometric Strengthening* and PNN for: legitimate-token case and stolen-token case compared against the stolen-token case for the association of *Biometric Strengthening* and cosine angle.

This process is also applied to the stolen-token scenario, in which we mix the legitimate token with the imposter signature template (skilled forgery). From the Figure 7, it shows that the performance of *Biometric Strengthening* in the stolen-token scenario (Stolen-Token: Cosine Angle) is degraded significantly (EER = 20%), which is worse than result provided by the original method. However, the association of *Biometric Strengthening* and PNN (Stolen-Token: PNN) depicts prominent performance improvement in the stolen-token scenarios. Note that the error rate is reduced to 4.4%. This is an important performance improvement of practical concern. PNN works well in this context due to the high distinctive characteristic of the *Biometric Strengthening* training templates.

Besides, the experiment also shows that the computation time can be reduced significantly with just slight performance drop when only one template per user is used (as compared to the case of 4 training samples as shown in Table 3).

Table 3: Total time spent to run one course of experiment and the accuracy of PNN in stolen-token scenario

| Training Samples | Total time (minutes) | EER (%) |
|---|---|---|
| 4 | 10.8 | 4.40 |
| 1 | 2.6 | 6.00 |

In this case, the time complexity of PNN that depends on the input vector dimension, *M* and the number of training samples, *p* can be decreased notably due to the compressed feature data length through PCA and single training sample per user settings. As such, the association of *Biometric Strengthening* and PNN is feasible in practical usage due to its high speed and accuracy performance.

## 9. Conclusion

We have proven that the holistic analysis statistical approach is very suitable for image-based signature verification task. It is faster, less computationally intensive and less prone to misconceptions during the extraction stage as there is no priori assumptions will be made on the structure of the signature. *Biometric Strengthening* is able to increase the accuracy of the system. Given the robustness of our algorithm and the fact that only concern on global features, optimum results are obtained when our algorithm is applied to our own independent database of 1000 signatures from 50 writers and 5 forgers. PNN is used to rectify the problem when the legitimate token is stolen and used against by the imposter to claim as the legitimate user. The high accuracy and speed of the combination of *Biometric Strengthening* and PNN are feasible to be used in a practical verification scenario. To make this system applicable to real world transaction such as to verify the signatures from credit card transaction receipts or bank cheques, we need to know that a client's signature tends to evolve over a long period of time. Thus, to deal with this problem is to collect training signatures at regular intervals or direct replace those training signatures that differs the most from the client's current signature model with one or more test signatures, yet adapt the signature model accordingly.

## References

[1] R.M. Bolle, J.H. Connel, and N.K. Ratha, "Biometric perils and patches," Pattern Recognition, vol.35, no.12, pp 2727-2738, 2002.

[2] U. Uludag, S. Pankanti, S. Prabhakar, and A.K. Jain, "Biometric cryptosystems: issues and challenges," Proceeding in IEEE, vol.92, no.6, pp 948-960, 2004.

[3] N.K. Ratha, J. Connell, and R. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," IBM Systems Journal, vol.40, no.3, pp 614-634, 2001.

[4] A. Goh, and D.C.L. Ngo, "Computation of cryptographic keys from face biometrics," Lecture Notes in Computer Science, Springer-Verlag 2828, pp 1-13, 2003.

[5] A.B.J. Teoh, D.C.L. Ngo, and A. Goh, "Personalized cryptographic key generation based on FaceHashing," Computers and Security Journal, vol.23, no.7, pp 606-614, 2004.

[6] K.H. Cheung, A. Kong, D. Zhang, M. Kamel, J. You, and H.W. Lam, "An analysis on accuracy of cancellable biometrics based on BioHashing," Proceeding of Ninth International Conference on Knowledge-Based, Intelligent Information and Engineering Systems, LNAI 3683, pp 1168-1172, 2005.

[7] L. Nanni, L., and A. Lumini, "Human authentication featuring signatures and tokenized random numbers," NeuroComputing, 2005.

[8] A.B.J. Teoh, and C. Tee, "Remarks on BioHashing based cancellable biometrics in verification system," NeuroComputing, 2006.

[9] J. Coetzer, B.M. Herbst, and J.A.du Preez, "Offline signature verification using the discrete Radon transform and a hidden Markov model," Journal on Applied Signal Processing, vol.4, pp 559-571, 2004.

[10] M. Turk, and A. Pentland, "Eigenfaces for recognition," Journal of Cognitive Neuroscience, 1991.

[11] D.F. Specht, "Probabilistic neural networks for classification, mapping, or associative memory," Proceeding of the IEEE International Conference Neural Networks, vol.1, pp 525-535, 1988.

[12] D.F. Specht, "Probabilistic neural networks (original contribution)," Neural Networks, vol.3, no.1, pp 109-118, 1990.

**Ooi Shih Yin** received her Bachelor of Information Technology (Hons) and Master of Science (Information Technology) from Multimedia University, Malaysia in 2004 and 2006 respectively. Shih-Yin joined the Faculty of Information Science and Technology in Multimedia University, Malaysia where she is the currently the Program Coordinator of B. IT (Hons) Security Technology. She has authored few indexing journals and conference papers, and served as paper reviewer in the field of biometrics, image processing, machine intelligence, computer vision, and data mining. She is a member of ISPA Malaysia.

**Andrew Teoh Beng Jin** obtained his BEng (Electronic) in 1999 and Ph.D degree in 2003 from National University of Malaysia. His research interest is in biometrics security, watermarking and pattern recognition. He had published more than 130 international journal and conference papers in his area.

**Pang Ying Han** received her B.E. degree in Electronic Engineering in year 2002 and M.E. degree in year 2005 from Multimedia University. She is currently a PhD student at Multimedia University. Her research interests include face recognition, manifold learning, image processing and pattern recognition

**Hiew Bee-Yan** from Malaysia received her Bachelor of Information Technology (Hons) from University of Malaya, Malaysia in 2004. In 2008, she obtained her Master of Science (Information Technology) from Multimedia University Malaysia. She is presently a lecturer of Faculty of Information Science and Technology, Multimedia University, Malaysia. Her research interests include computer vision and image processing.

**Hiew Fu San** received his B.E. degree, majoring in Computer Engineering in year 2002 and M.E. degree in year 2008 respectively from Multimedia University, Malaysia. His research interests include pattern recognition and remote sensing.