# 2^N Discretisation of BioPhasor in Cancellable Biometrics

Andrew Beng Jin Teoh[1], Kar-Ann Toh[1], and Wai Kuan Yip[2]

[1] Biometrics Engineering Research Center (BERC)
Yonsei University, Seoul, South Korea
{bjteoh,katoh}@ieee.org
[2] Faculty of Information Science and Technology (FIST)
Multimedia University,
Jalan Ayer Keroh Lama, 75450 Melaka, Malaysia
wkyip@mmu.edu.my

**Abstract.** BioPhasor was introduced as a form of cancellable biometrics which integrates a set of user-specific random numbers (RN) with biometric features. This BioPhasor was shown to fulfil diversity, reusability and performance requirements in cancellable biometrics formulation. In this paper, we reformulate and enhance the BioPhasor in terms of verification performance and security, through a $2^N$ stage discretisation process. The formulation is experimented under two scenarios (legitimate and stolen RN) using 2400 FERET face images. Apart from the experiments, desired properties such as one-way transformation and diversity are also examined.

**Keywords:** BioPhasor, Cancellable biometrics, $2^N$ stage discretisation, Face Biometrics.

## 1 Introduction

When a biometric is compromised, it is compromised forever because it cannot be changed. Cancellable biometrics has thus been proposed, whereby a biometric image is distorted in a repeatable but non-reversible manner before template generation. If the cancellable template is compromised, it can be disposed of. The distortion characteristics can then be changed, and the same biometric is mapped to a new template for subsequent use. There are four principal criteria to be fulfilled before a cancellable biometric template can be considered useful [1]:

i. Diversity: No same cancellable template can be used in two different applications.
ii. Reusability: Straightforward revocation and reissue in the event of compromise.
iii. One-way transformation: Non-invertibility of template computation to prevent recovery of biometric data.
iv. Performance: The formulation should not deteriorate the recognition performance.

Ratha et al [2] was the first to concretise the idea of cancellable biometrics. They sketched an idea regarding an intentional distortion of a biometric signal based on a chosen transform function. The biometric signal was distorted in a similar fashion at

S.-W. Lee and S.Z. Li (Eds.): ICB 2007, LNCS 4642, pp. 435–444, 2007.

each presentation, that is, during enrolment and for every subsequent authentication. With this approach, every instance of enrolment can use a different transform function thus rendering cross-matching impossible. Furthermore, if one variant of the biometric templates is compromised, then the transformation can simply be changed to create a new variant for re-enrolment. Since then, many constructs have been proposed [3].

In this paper, we focus only on the constructs which combine external factors such as tokenized random data with biometrics. Soutar et al [4] proposed a cancellable biometrics which was generated from fingerprints using optical computing techniques. The templates consisted of correlation patterns derived from training images, which are subsequently mixed with random data to generate identification codes. However, the scheme was not explained in a satisfactory manner regarding the cryptographic security aspects of the transformations where no related results can be found. Teoh et al. [5] introduced a cancellable biometrics/key, known as BioHash, via inner product between randomized token and biometric data. This method is advantageous in comparison to that of Soutar et al since the transformation is a one-way process. However, the verification performance degraded when the genuine token was stolen and used by an imposter to claim as the genuine user (stolen-token scenario). This violated the performance criterion. Savvides et al. [6] proposed a cancellable biometrics scheme which encrypted the training images by synthesizing a correlation filter for biometrics authentication. They demonstrated that convolving the training images with any random convolution kernel prior to building the biometric filter does not change the resulting correlation output peak-to-sidelobe ratios, thus preserving the authentication performance. Despite that, the security can be jeopardized via a deterministic deconvolution with a known random kernel, thus against the criterion of non-invertibility. Recently, BioPhasor was proposed as a non-linear extension of BioHash [7]. The BioPhasor was shown to fulfil diversity, reusability and performance criteria. However, Bio-Phasor's non-invertible property is unknown. In this paper, we present an enhanced version of BioPhasor which incorporates a 2^N discretisation, thereby offering a better verification performance, particularly in generic stolen-token scenario as well as fulfilling diversity and one-way transformation properties.

## 2 Brief Introduction of BioPhasor

BioPhasor is originally described as follow:

(a) Feature Extraction. A feature extraction technique is used to extract the biometric feature. The biometric feature is represented in a vector form, $\boldsymbol{x} \in \Re^n$, with $n$ denoting the feature length of $\boldsymbol{x}$.

(b) Use token to generate a set of pseudo-random vectors, $\{\boldsymbol{r}_i \in \Re^n \mid i = 1,...,m\}$ which is distributed according to $\mathcal{N}(0, 1)$ and apply the Gram-Schmidt process to transform the basis $\{\boldsymbol{r}_i \in \Re^n \mid i = 1,...,m\}$ into an orthonormal set of $\boldsymbol{r}$, $\{\boldsymbol{r}_{\perp i} \in \Re^n \mid i = 1,...,m\}$.

(c) Mix $\boldsymbol{x}$ with $\boldsymbol{r}_{\perp i}$ repeatedly to form a set of complex vectors, $\left\{z_i = \boldsymbol{x} + \boldsymbol{r}_{\perp i}\ \mathrm{j} \in C^n \mid i = 1,...,m\right\}$, where j=√-1, and then calculate the complex argument of each element in $z_i$, where $z_i=\{\arg(\tilde{z}_k) \mid k=1,\ldots,n\}$, ie. $\left\{\arg(\tilde{z}_k) \in \Re \mid k = 1,...,n\right\}$.

(d) Average the complex arguments, $\left\{\alpha_l = \frac{1}{n}\sum_{k=1}^{n} \arg(z_k) \in \Re^m \mid l = 1,...,m\right\}$ where $-\pi \leq \alpha_j \leq \pi$ and $m \leq n$.

In general, the BioPhasor formulation can be rewritten as

$$\alpha_j = \frac{1}{n}\sum_{i=1}^{n} \tan^{-1}(x_i / r_{ij}),\ j = 1,\ldots,m,\ m<n \text{ and } r \neq 0 \tag{1}$$

For the sake of simplicity and security concern of not to reveal the actual value of $\alpha_j$, a quantization is carried out. Since $\alpha_j$ is a principle value, it makes sense to divide the complex plane into two sectors to convert $\alpha_j$ into a single bit as follows: $b_i = \begin{cases} 0 & \text{if} \quad 0 \leq \alpha_i < \pi \\ 1 & \text{if} \quad -\pi < \alpha_i \leq 0 \end{cases}$ where $i = 1,...,m$ . For implementation purpose, the BioPhasor template can be stored in a central database during enrolment. During the verification stage, the extracted feature image is mixed with the genuine token (*legitimate-token scenario*) and the resulting BioPhasor template is compared with the enrolled template by using Hamming distance (the difference in the number of bits). One should note that this cancellable biometrics approach, of mixing the user-specific pseudo-random number with the biometric features, has the drawback when an impostor B steals the pseudo-random numbers of A and tries to verify as A. We call this a *stolen-token scenario*.

## 3 $2^N$ Stage Discretisation

The quantization of BioPhasor may bring to performance degradation due to information lost. In the original algorithm, complex plane can be further divided into $2^q$ sectors and thus $q$ bits can be assigned per sector. This enables an algorithm to render a more refined feature representation, $\boldsymbol{b}^q = \{ b_k^q \mid k = 1,\ldots,m,\ q=1, 2, 3,\ldots\}$ with higher number of bits per user and thus higher accuracy [5]. However, a direct extension of the scheme is still confined to the accuracy level that can be achieved by equation (1).

To increase the stability of the resulting bitstrings, we propose to transform the BioPhasor feature set $\boldsymbol{\alpha} = \{\alpha_i \mid i=1,\ldots, m\}$ (computed using equation (1)) such that each transformed feature is discernible to separate the genuine user from potential impostor users. Specifically, we transform $\alpha_i$ from the real into the index space and convert the resultant indices to Gray code. We assume that $\alpha_i$ is distributed according to normal distribution, $\alpha_i \sim \mathcal{N}(0, \pi^2/9)$ and the element values fall within twice of user-dependent standard deviation from the mean value. The feature element space is next divided into $2^N$ segments by adjusting the user-dependent standard deviation, $\sigma_{ij}$. The $\alpha_i \sim \mathcal{N}(0, \pi^2/9)$

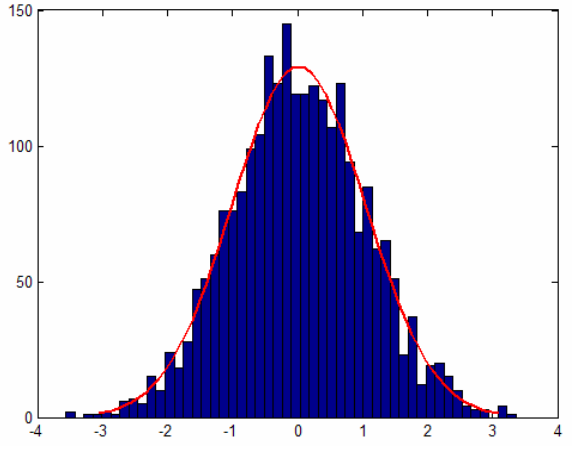


**Fig. 1.** Distribution of $\alpha_i$ is close to $\mathcal{N}(0, \pi^2/9)$. The red line represents $\mathcal{N}(0, \pi^2/9)$.

assumption is verified by using the 2400 samples of $\boldsymbol{\alpha}$ which shall be described in section 4. This leads to a distribution of $\left\{ \bar{\alpha}^{k} = \frac{1}{m}\sum_{i=1}^{m} \alpha_i^k \mid k = 1,...,2400 \right\}$ with mean and standard deviation being $0.0001 \approx 0$ and 3.21 respectively. As shown in Fig. 1, the histogram distribution closely approaches $\mathcal{N}(0, \pi^2/9)$.

Our implementation is outlined below:

a) At enrolment, we compute the standard deviation of $\alpha_i$ of user $j$, $\sigma_{ij} = \sqrt{\left( \sum_{k=1}^{p} ( \alpha_{ijk} - \bar{\alpha}_{ij} )^2 \right) / p}$ , $i = 1, \ldots, m$ where $p$ is the number of training samples and $\bar{\alpha}_{ij}$ is the mean of $\alpha_{ij}$.

b) For a user $j$, the feature space is divided into $2^N$ segments with range $[L\ R]$ and the segment width, $w$ which varies according to $w = \arg\min_{N} \left( \left| \frac{R - L}{2^N} - 2\sigma_{ij} \right| \right)$ for feature element $i$ of user $j$. In this case, $L$ and $R$ are the right and left boundaries of entire feature space and they take the values $-\pi$ and $\pi$, respectively, due to the observation that $\alpha_i \sim \mathcal{N}(0, \pi^2/9)$. The number of bits in each segment, $n_i$ can be determined by enumerating a set of $N$ values, $\psi_j = \left\{ \left| \frac{R - L}{2^N} - 2\sigma_{ij} \right|, i = 1,...,m \text{ and } N = 1,...,c \right\}$ where $n_i$ is the smallest $N$ value in set $\psi$. Alternatively, $n_i = N_{\min(\psi_j)}$ where $\psi_j = \left\{ \left| 2^{1-N} - 2\sigma_{ij} \right|, i = 1,...,m \text{ and } N = 1,...,c \right\}$. In this paper, $c$ is arbitrarily set to 10 to avoid too many bits being used for a single representation.

c) At verification, the *genuine segment index* $\alpha_i$ of user $j$ can be obtained from $d_i = \left\lfloor \left( \frac{\alpha_i - L}{R - L} \right) 2^{n_i} \right\rfloor$ or $d_i = \left\lfloor \left( (\alpha_i + \pi)/\pi \right) 2^{n_i - 1} \right\rfloor$ and its binary representation of $\alpha_i$ is rendered by Gray Coding, $b_i = \text{gray}(d_i)$.

With the above procedure, a BioPhasor with length $\gamma = \sum_{i=1}^{m} n_i$ can be generated by cascading all Gray encoded indices of genuine segments from the $m$-dimensional $\boldsymbol{\alpha}$. Our $2^N$ discretisation functions as an error correction mechanism to further reduce the real-valued BioPhasor which combined vector to bit strings. Discretising each value in the combined vector forces closely located values to be replaced by a single index integer, which indirectly correct the fuzziness within the biometric data.

## 4 Performance Evaluations

In this paper, the proposed method is evaluated using face images from FERET database [8]. EigenFace [9] is adopted as the feature extractor and the Euclidean distance is used for matching. For the eigenbasis training, we use 400 images ie. 40 subjects with 10 images per identity, from ORL Face Database (http://www.uk.research.att.com/facedatabase.html). In the experiments using FERET database, we randomly selected a subset of 400 subjects, each having 6 essentially normalised frontal images with variations in pose, ie. within ±25 degree of angles, scale and illuminations. We randomly select 2 images from each subject to be the training samples and the others for testing purposes. However, 2 samples per subject are too few to estimate reliable statistics for $2^N$ discretisation (see step (a) in section 3), we employ the method proposed by [10] to derive multiple samples from 2 images. We perform geometric transforms, such as translation, rotation in plane, scale variance etc. and gray-scale transforms, such as simulative directional lighting, man-made noise etc. Then, we carry out FERET geometrical, lighting normalization [8] and BioPhasoring on the training (synthesized) and testing images. As such, we generated 20 training samples. We randomly select $p$ (≥10) BioPhasor templates for $2^N$ discretisation and we repeat the same process 20 times for each run and the results are averaged to reduce the statistical frustration caused by the varying random numbers.

To generate the impostor distribution, the first template of each subject is matched against the first template of all other subjects, and the same matching process was repeated for subsequent templates, leading to (400x399)/2 x 4 = 319,200 impostor attempts. For the genuine distribution, each template of each subject is matched against all other templates of the same subject, leading to 2,400 ((3x4)/2 attempts of each subject x 400). For the stolen-token scenario, we consider the worst case where the impostors always manage to obtain the genuine token. In other words, only one set of pseudo-random numbers is mixed with all face features and the matching is performed according to the impostor match described above. In this paper, pca, bioh, biop, biop2N denote EigenFace, BioHash [5], BioPhasor [7] and $2^N$ discretised BioPhasor, respectively. Note that the feature length of pca, $n$= 150 is used while $m$= 100 is applied for BioHash and BioPhasor and evaluated using $p$= 10, 15 and 20

training samples for $2^N$ discretised BioPhasor. The performance will be evaluated using Equal Error Rate (EER) and Receiver Operating Curve (ROC).

Table 1 shows the performance comparisons of pca, bioh, biop and biop2N. It is clearly shown that bioh, biop and biop2N in legitimate token case significantly outperform pca, as what we had expected to see in all user-specific token mixing algorithms [5][7]. However, we are more interested in the stolen-token scenario which is generic in real world applications. From the experiments, the length of biop2N that we obtained is the range [210 290] and we take an average of 250 by appending zeros within those lesser than 250 and discard those which are longer.

Table 1 and ROC in Fig. 2 show that BioHash is the poorest compares to original PCA, BioPhasor and $2^N$ discretised BioPhasor in the stolen-token scenario. The $2^N$ discretised BioPhasor achieves the best performance especially in the case with large

**Table 1.** Performance comparisons of pca, bioh, biop and biop2N (both legitimate and stolen-token scenarios)

| EER(%) | pca | bioh | biop | biop2N (*p*=10) | biop2N (*p*=15) | biop2N (*p*=20) |
|---|---|---|---|---|---|---|
| Genuine-token | 15.63 | 0.01 | 0 | 0 | 0 | 0 |
| Stolen-token | - | 16.21 | 14.91 | 6.21 | 4.81 | 2.11 |

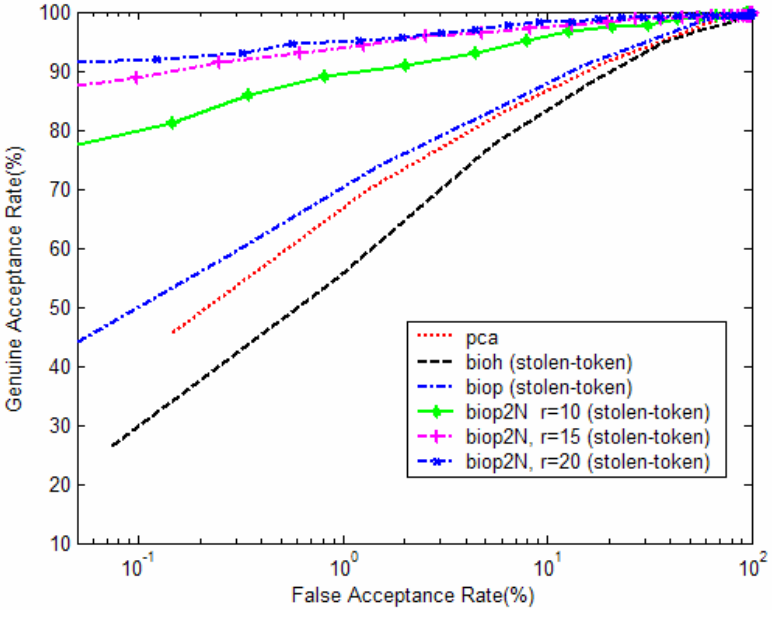


**Fig. 2.** ROC for performance comparisons in stolen-token scenario

number of training samples. The significant performance improvement observation indicates the potential generic discrimination capability of the BioPhasor based $2^N$ formulation. This phenomenon shall be explored in our subsequent works.

## 5 Diversity Property

Next we examine the diversity property of $2^N$ discretised BioPhasor by evaluating whether the random numbers, $\boldsymbol{r}_A$ mixed $2^N$ discretised template and the $\boldsymbol{r}_B$ mixed $2^N$ discretised template (with similar face identity) are correlated with each other. In other words, we wish to avoid the old template from falling into the region of acceptance of the refreshed template. In this case, the evaluation is exactly the same as the imposter distribution generation which has been discussed, but different $\boldsymbol{r}$ is used to mix with the same face feature and $2^N$ discretisation with training samples, $p$=20 is applied. According to [1], the comparisons of two truly uncorrelated binary bitstrings with length γ can be interpreted as a binomial distribution which have the functional form $f(x)=\frac{\gamma!}{\lambda!(\gamma-\lambda)!}0.5^{\gamma}$, with expectation $\pi$=0.5 and standard deviation $\frac{0.5}{\sqrt{\gamma}}$ where $x = \lambda/\gamma$, is the fraction of bits that happen to agree when two uncorrelated bitstrings are compared.

As shown in Fig. 3, the imposter distribution closely resemblance the theoretical fractional Binomial distribution where $\pi$=0.5 and standard deviation is $0.5/\sqrt{250}$ = 0.0316. This implies that the refreshed $2^N$ discretised BioPhasor has almost no

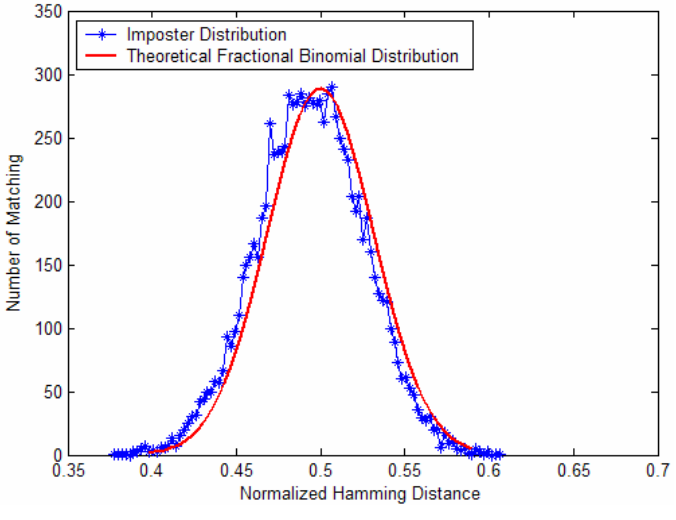


**Fig. 3.** $2^N$ discretised BioPhasor Diversity Distribution

correlation with $2^N$ discretised BioPhasor, and hence random number refreshment is equivalent to issuing the user a new template.

## 6 One-Way Transformation Property

BioPhasor is essentially designed for cancellable biometrics and its security concern such as whether it is one-way transformation is crucial. An examination of the one-way transformation property of $2^N$ stage discretised BioPhasor lies in two important dispositions: (1) irreversible random extraction of biometrics information via BioPhasor, and (2) transformation from real-valued biometric features to index space. The overall effect of these two steps is a one-way transformation of the real-space biometric vector into binary-space hashes without compromising the biometrics itself. We proceed to show the security proofs of the proposed scheme.

**Proposition 1:** Factoring out biometric feature, $\boldsymbol{x}$ from $\boldsymbol{\alpha}$, given random vector $\boldsymbol{r}$, is an intractable problem, even if $\boldsymbol{r}$ is known and is used multiple number of times.

**Proof:** Consider the scenario when $\boldsymbol{r}$ is used once and, $\alpha_i$ and $\boldsymbol{r}$ are known. The BioPhasor elements, $\alpha_j = \frac{1}{n}\sum_{i=1}^{n} \tan^{-1}\frac{x_i}{r_{i,j}} = \frac{1}{n}\sum_{i=1}^{n}(\frac{\pi}{2} - \tan^{-1}\frac{r_{i,j}}{x_i})$ form $m$ system of equations where $\boldsymbol{r}_i \perp \boldsymbol{r}_j$ for $i \neq j$ and $\boldsymbol{r}_\mathrm{i} \neq \boldsymbol{r}_\mathrm{j}$. Since there are $n$ number of unknowns and only $m<n$ number of equations, the system of equations has infinite number of solutions and hence, $\boldsymbol{x}$ is not recoverable in polynomial time. Therefore, factoring $\boldsymbol{x}$ out from $\boldsymbol{\alpha}$ and $\boldsymbol{r}$ is an intractable problem if $\boldsymbol{r}$ is known and used once.

Next consider when $\boldsymbol{r}$ is replaced multiple times. If there are multiple tokens $\boldsymbol{r}$, $\boldsymbol{r}$', $\boldsymbol{r}$'', we can form $m = m_1+m_2+\ldots= n$ number of instances of the BioPhasor equations with $m_i$ representing the length of the BioPhasor for each use where $\boldsymbol{r}_\mathrm{i} \neq \boldsymbol{r}_\mathrm{j}$. The system of equations is non-linear, i.e. $\tan(n\alpha_j) = \sum_{i=1}^{n} x_i r_{i,j}^{-1}$ which means that we cannot apply Gaussian Elimination to solve for $\boldsymbol{x}$. Using general formula for tangent addition, the expansion of each the equation is precisely defined as $\tan(n\alpha_k) = i\frac{\prod_{j=1}^{n}(1-i\frac{x_j}{r_{k,j}}) - \prod_{j=1}^{n}(1+i\frac{x_j}{r_{k,j}})}{\prod_{j=1}^{n}(1-i\frac{x_j}{r_{k,j}}) + \prod_{j=1}^{n}(1+i\frac{x_j}{r_{k,j}})}$. Note that even though the system of equations has unique solution, there is no efficient algorithm or method for solving this non-linear system as shown by Blondel and Tsitsiklis [11].

If there are $m = m_1+m_2+\ldots> n$ number of instances of the BioPhasor equations, the system of equations becomes over determined and normally it will have no solution. □

Note that BioPhasor mixing has higher security compared to BioHashing method. This is because of the $\tan^{-1}(.)$ function which converts the mixing formula to a non-linear operation.

**Proposition 2:** The vector $\boldsymbol{\alpha}$ cannot be recovered exactly from $2^N$ discretised vector $\boldsymbol{d}$.

**Proof:** Let the $2^N$ discretisation be defined as $f : (-\pi, \pi)^m \rightarrow Z_{2^N}^m$ (discretisation) and $f \circ g$ where $g : Z_{2^N}^m \rightarrow \{0,1\}^\gamma$ (binarisation and Gray encoding) with $m < \gamma$. Since range($g$) $\neq$ domain($f$), hence $g \circ f$ is not possible. Since $f$ is a transformation from real to index space, information will be lost. In particular, the continuous to discrete entropy lost is $\log(2^{n_i})$ based on individual segment size $n_i$ as mentioned in Joy and Thomas [12]. Hence the $2^N$ stage discretisation is irreversible. □

The overall effect of $2^N$ discretised BioPHasor is a one-way transformation of the real-space biometric feature into binary-space hashes based on the product principle of Shannon [12], which stated the systematic cascading of different types of ciphers in single cryptosystems will increase the cipher strength provided that the product ciphers are associative but not commutative. We let the BioPhasor mixing be defined as $h$: $\Re^n \times \Re^n \rightarrow (-\pi, \pi)^m$ and let $2^N$ discretisation be $k$: $(-\pi, \pi)^m \rightarrow \{0, 1\}^\gamma$ with $m < \gamma$. Clearly $h \circ k$ is associative but not commutative since the domain and range cannot be interchanged. Since $h$ and $k$ are non-invertible and due to the product principle, $h \circ k$ is a one-way transformation.

## 7 Conclusion

In this paper, we proposed an extension of BioPhasor which incorporates a $2^N$ discretisation instead of using simple quantization scheme. From our experimental results on FERET dataset, the $2^N$ discretised BioPhasor survives the simulated stolen-token attacks. Consequently, the $2^N$ discretised BioPhasor could function as an effective cancellable biometrics technique to protect the privacy of biometric data without compromising the recognition performance in the event of compromised token. We also showed that $2^N$ discretised BioPhasor fulfils two other crucial requirements for a cancellable biometrics formulation, namely the diversity and non-invertible properties.

## Acknowledgement

This work was supported by the Korea Science and Engineering Foundation (KOSEF) through the Biometrics Engineering Research Center (BERC) at Yonsei University.

## References

[1] Andrew Teoh, B.J., Goh, A., David Ngo, C.L.: Random Multispace Quantisation as an Analytic Mechanism for BioHashing of Biometric and Random Identity Inputs. IEEE Transactions on Pattern Analysis and Machine Intelligence 28(12), 1892–1901 (2006)

[2] Ratha, N., Connell, J., Bolle, R.: Enhancing security and privacy in biometrics-based authentication systems. IBM Syst. J. 40(3), 614–634 (2001)

[3] Uludag, U., Pankanti, S., Prabhakar, S., Jain, A.K.: Biometric Cryptosystems: Issues and Challenges. Proceedings of the IEEE 92(6), 948–960 (2004)
[4] Soutar, C., Roberge, D., Stoianov, A.R., Gilroy, Vijaya Kumar, B.V.K.: Biometrics Encryption. In: Nichols, R.K. (ed.) ICSA Guide to Cryptography, pp. 649–675. McGraw-Hill, New York (1999)
[5] Andrew, B.J., David Ngo, C.L.: Cancelablle Biometrics Featuring With Tokenised Random Number. Pattern Recognition Letter 26(10), 1454–1460 (2005)
[6] Savvides, M., Vijaya Kumar, B.V.K., Khosla, P.K.: Cancelable Biometrics Filters for Face Recognition. Int. Conf. of Pattern Recognition 3, 922–925 (2004)
[7] Andrew Teoh, B., David Ngo, C.: Cancellable Biometrics Realization through BioPhasoring. In: 9th IEEE International Conference on Control, Automation, Robotics and Vision, ICARCV 2006, pp. 201–205 (2006)
[8] Phillips, P., Moon, H., Rauss, P., Rizvi, S.: The FERET Database and Evaluation Methodology for Face Recognition Algorithms. In: Proc. IEEE Conf on Computer Vision and Pattern Recognition, pp. 137–143. IEEE Computer Society Press, Los Alamitos (1997)
[9] Turk, M., Pentland, A.: Eigenfaces for Recognition. Journal of Cognitive Neuroscience 13(1), 71–86 (1991)
[10] Shan, S., Cao, B., Gao, W., Zhao, D.: Extended Fisherface for face recognition from a single example image per person. Proc. IEEE Int. Symp. Circ. Syst. 2, 81–84 (2002)
[11] Blondel, V.D., Tsitsiklis, J.N.: A Survey of Computational Complexity Results in Systems and Control. Automatica 36(9), 1249–1274 (2000)
[12] Joy, T.M., Thomas, J.A.: Elements of Information Theory, 2nd edn. John Wiley & Sons Inc., Chichester (1991)