Pertanika J. Sci. & Technol. 26 (1): 133 - 160 (2018)

SCIENCE & TECHNOLOGY

Journal homepage: http://www.pertanika.upm.edu.my/

Revocable and Non-Invertible Multibiometric Template Protection based on Matrix Transformation

Jegede, A.[1,2]*, Udzir, N. I.[1], Abdullah, A.[1] and Mahmod, R.[1]

[1]*Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, 43400 UPM, Serdang, Selangor, Malaysia*

[2]*Department of Computer Science, University of Jos, 930001 Nigeria*

ABSTRACT

Biometric authentication refers to the use of measurable characteristics (or features) of the human body to provide secure, reliable and convenient access to a computer system or physical environment. These features (physiological or behavioural) are unique to individual subjects because they are usually obtained directly from their owner's body. Multibiometric authentication systems use a combination of two or more biometric modalities to provide improved performance accuracy without offering adequate protection against security and privacy attacks. This paper proposes a multibiometric matrix transformation based technique, which protects users of multibiometric systems from security and privacy attacks. The results of security and privacy analyses show that the approach provides high-level template security and user privacy compared to previous one-way transformation techniques.

Keywords: Multibiometric, matrix transformation, performance, privacy, security

INTRODUCTION

Multibiometric authentication systems use a combination of two or more biometric modalities to verify the identity of users. Multibiometric systems can be implemented using image and voice data (Nishino et al., 2012), face and iris (Karmakar & Murphy, 2014), palm print and iris (Hariprasath & Prabakar, 2012), ear and finger knuckle images (Tharwat et al., 2012), as well as hand vein, iris and fingerprint (Xiuyan et al., 2011). Performance evaluation results from these studies show that multibiometric systems generally have much better recognition accuracy than unibiometric approaches. This is because multibiometric systems use a richer set of inputs that helps to improve recognition performance. However, multibiometric

ARTICLE INFO

Article history:
Received: 08 August 2016
Accepted: 15 August 2017

E-mail addresses:
abayomi.jegede@ymail.com (Jegede, A.),
izura@upm.edu.my (Udzir, N. I.),
azizol@upm.edu.my (Abdullah, A.),
ramlan@gmail.com (Mahmod, R.)
*Corresponding Author

ISSN: 0128-7680

approaches face challenges in terms of template security and fusion complexity (Kaur, 3013). Multibiometric systems are not exempted from security challenges, such as replay attacks. Legitimate users of multibiometric systems also face privacy violations, such as template sharing and cross-matching. The risk of identity loss also occurs if an attacker who obtains digital versions of users' biometric data is able to reconstruct original biometric images from compromised biometric templates (Feng & Yuen, 2012; Li & Cot, 2011). Loss of identity is a severe risk because biometric modalities cannot be easily replaced unlike a password, PIN, or chip. This implies that victims will lose two or more biometric means of identity because multibiometric systems use at least two or more modalities. This paper addresses security, privacy and risk of loss of identity in multibiometric systems by proposing a one-way (or non-invertible) transformation approach known as matrix transformation. Matrix transformation is a simple and effective method that prevents security attacks on multibiometric systems and protects users against a privacy violation as well as identity loss. This approach guarantees the security of stored biometric data and the privacy of legitimate users, even if protected biometric data and security parameters are disclosed to an attacker. This approach also supports revocability or template renewability because a new biometric template can be created and used to replace the one suspected to have been stolen, corrupted or compromised.

Non-invertible transformation belongs to a general class of techniques known as cancellable biometrics, whose goal is to achieve 'an intentional, repeatable distortion of a biometric signal based on a chosen transform' (Ratha et al, 2001). This provides template security, revocability, unlinkability, and resistance to cross-matching attacks. Non-invertible transformations provide template security by preventing the recovery of original biometric data from a transformed template, even if an attacker knows the transformation parameters. Revocability allows administrators to remove a compromised template and reissue a new one based on the same biometric data. Template revocability is achieved by changing the transformation parameters used for the previous enrolment. Moreover, multiple transformed templates can be constructed from a single biometric input of the same subject, which provides unlinkability and prevents cross-matching among transformed templates that are stored in multiple databases.

Non-invertible transformation can be divided into two categories, namely image-level transforms and feature-level transforms. Image-level transforms, such as grid morphing, block permutation (Ratha et al., 2001), blind deconvolution (Campisi & Egiazarian, 2007; He et al., 2008), block re-mapping, texture warping (Farberbock et al., 2010; Hammerle-Uhl et al., 2009), GREY-COMBO (Zuo et al., 2008) and Log-Polar transform (Plesca & Morogan, 2013) are used to create an irreversible version of a given biometric image prior to feature extraction. Feature-level transformation uses approaches such as Cartesian; polar and functional transforms (Ratha et al., 2006; Ratha et al., 2007); revocable biotokens (Boult, 2006; Boult et al., 2007); pseudo-random permutations (Grassi & Faundez-Zanuy, 2009); Gaussian distribution (Jeong & Teoh, 2010); partial Hadamard matrix (Wang & Hu, 2013); pulse active transform (Safie et al., 2014); BIN-COMBO (Zuo et al., 2008); user-specific secret permutations (Rathgeb & Uhl, 2010); alignment-free adaptive bloom filter (Rathgeb et al., 2014); and the Delaunay triangle (Sandhya et al., 2016) to create non-invertible templates from extracted biometric features. A

number of techniques, such as user-dependent multi-state discretisation (Teoh et al., 2010), a combination of multi-dimensional iris codes, bit permutation and key binding (Ouda et al., 2011) and spiral cube (Moujahdi et al., 2012) focus on improving the security and recognition accuracy of some existing non-invertible transformation techniques.

Definitions

Galois field. A Galois (or finite) field contains a finite number of elements. A Galois field consisting of q elements is denoted as $gf(q)$. Formally, a Galois field, $gf(p^n)$ is defined in Equation 1 as:

$$\begin{aligned} GF(p^n) = (0, 1, 2, \dots, p-1) \cup (p, p+1, p+2, \dots, p+p-1) \\ \cup (p^2, p^2+1, p^2+2, \dots, p^2+p-1) \\ \cup \dots \cup p^{n-1}, p^{n-1}+1, p^{n-1}+2, \dots, p^{n-1}+p-1 \end{aligned} \quad (1)$$

where $p \in \mathbb{P}$ and $n \in \mathbb{Z}^+$ p^n defines the order of the field or the number of elements in the field, p is the characteristic of the field and the degree of polynomial of each element is at most n-1 (Benvenuto, 2012). The binary (base-2 number) system represents each value as 0 or 1. The binary system provides an alternative way to represent the elements of a Galois field. Each decimal element, x of a Galois field, can be expressed in binary as $a_n 2^n$. That is,

$$x = \sum_{n \in \mathbb{N}} a_n 2^n \quad (2)$$

where a_n is the binary coefficient and n is the degree of the polynomial.

A Galois field of two elements (also known as binary field), (2) , contains values that are represented by 0 and 1. The concept of $gf(2)$ is applicable to digital systems (such as computers) which represent data and operations in binary (series of 0s and 1s).

Permutation matrices. A permutation matrix is a square matrix whose elements are all 0s and 1s, with each row and column containing exactly a 1 (Fuzhen, 2011). It is a square matrix obtained from an $n \times n$ identity matrix by a permutation of rows (Grinshpan, 2011). Formally, a permutation is defined in Equation 3 as:

$$\pi = \begin{pmatrix} 1 & 1 & \dots & m \\ \pi(1) & \pi(2) & \dots & \pi(m) \end{pmatrix} \quad (3)$$

where $\pi(1), \pi(2), \dots, \pi(m) \in (1, 2, \dots, m)$; thus, a permutation matrix can be expressed as

$$P_{ij} = \begin{cases} 1, & if\ i = \pi(j) \\ 0, & otherwise \end{cases}$$ (Berisha et al., 2012).

Non-Invertible matrices. Given any two square ($n \times n$) matrices A and B, matrix A is said to be invertible (non-singular or non-degenerate) if the following condition holds:

$$A * B = B * A = I_n \tag{4}$$

where I_n is an $n \times n$ identity matrix and * denotes ordinary matrix multiplication. The matrix B referred to as the inverse of A (denoted by A^{-1}) is uniquely determined by A. A square matrix which does not satisfy the condition above is said to be non-invertible. Non-invertible matrices are also called singular or degenerate matrices. A square matrix is singular if and only if its determinant is 0. A square matrix that is not invertible is called singular or degenerate. A square matrix is singular if and only if its determinant is 0. A singular matrix is obtained by performing a random selection based on a continuous uniform distribution of its entries.

Non-invertible matrices in a Galois field of two elements (or $gf(2)$) are obtained by performing an *xor* operation on a pair of permutation matrices in $gf(2)$. If $A = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ are two elementary permutation matrices, a non-invertible matrix, is computed by the operation $C=A$ *xor* B. That is, $C = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$

The matrix is non-invertible because the values for its determinant and inverse are undefined. That is, if $y=Cx$, then $x=yC^{-1}$. C^{-1} is undefined. Hence x cannot be computed given the value of y.

METHODOLOGY

This section discusses the methods used for feature extraction, implementation, performance evaluation and security analysis.

Feature Extraction

Binary feature vectors were extracted directly from pre-processed face images using the rotation invariant neighbour-based invariant local binary pattern (RINLBP) technique. RINLBP is a hybrid approach which integrates the generic local binary pattern (Ojala et al., 2002) and neighbour-based local binary pattern (Hamouchene & Aouat, 2014). The approach improves on the generic local binary pattern (LBP) by addressing poor recognition performance due to image rotation. The LBP is a texture classification method that combines a set of local texture descriptors to provide a global textural representation of an image. The LBP descriptor of a local circular region is computed by comparing the value of the central pixel with each of its

neighbours. The result of the comparison is 1 if the value of the pixel is greater that the central pixel, otherwise the result is 0. LBP is defined in Equation 5 as:

$$LBP_{R,P} = \sum_{p=0}^{P-1} s(g_p - g_c).2^p \tag{5}$$

such that

$$s(x) = \begin{Bmatrix} 1 & x \geq 0 \\ 0 & x < 0 \end{Bmatrix} \tag{6}$$

where
g_p is greyscale value of the neighbour pixel,
g_c is the value of the central pixel,
p is the index of the neighbour
R is the radius of the circular region
P is the number of sample points in the neighbourhood of the central pixel
(Ojala et al., 2002).

Figure 1 illustrates the operation of the generic LBP.

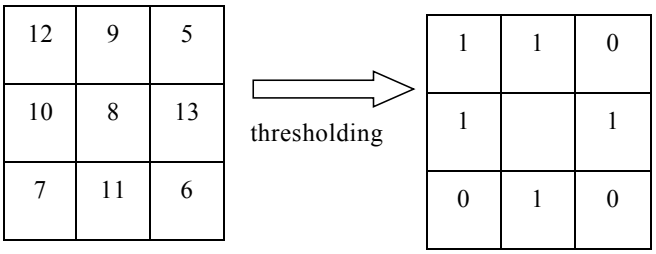

Figure 1. Generic LBP

The LBP is popular because it is simple to calculate and shows good performance. It is also robust against changes in illumination, which leads to changes in the values of pixel intensities. This is because features are not represented using the actual pixel values. Rather, they are computed by comparing the intensity values of a central pixel and its neighbours. A change in intensity value of a central pixel will lead to a corresponding change in the values of the neighbour pixels. Neighbour-based LBP (NLBP) compares the pixel value of each neighbour

of the central pixel with its next neighbour along the circular region. Neighbour-based LBP is defined in Equation 7 as:

$$NLBP_{R,P} = \sum_{p=0}^{P-1} s(g_p - g_{p+1}).2^p \quad (7)$$

such that

$$s(g_p - g_{p+1}) = \begin{cases} 1 & g_p \geq g_{p+1} \\ 0 & g_p < g_{p+1} \end{cases}$$

where
g_p is greyscale value of a neighbour pixel,
g_{p+1} is the value of the next pixel along the circular region,
p is the index of the neighbour
R is the radius of the circular region
P is the number of sample points in the neighbourhood of the central pixel (Hamouchene & Aouat, 2014).

The encoding begins with the topmost left neighbour and follows a clockwise direction (see Figure 2). This is unlike the generic LBP, which compares each neighbour with the central pixel. The generic LBP and the neighbour-based LBP generate different binary patterns from the same pixels.

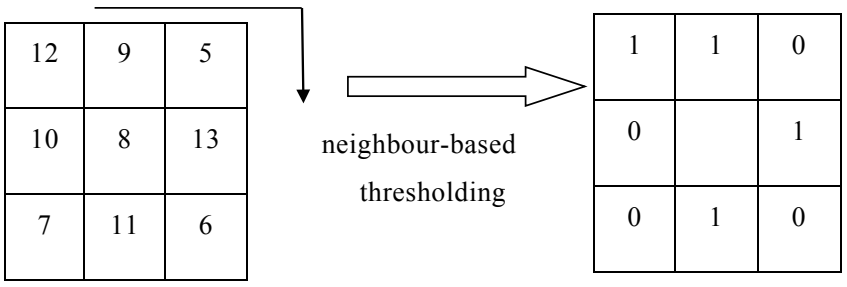

Figure 2. Neighbour-based LBP

The Rotation Invariant Neighbour-based LBP, $RINLBP_{R,P}$, is defined in Equation 8 as:

$$RINLBP_{R,P} = \sum_{p=0}^{P-1} s(g_p - g_{p+1}) . 2^{mod(p-d,P)} \quad (8)$$

such that

$$s(g_p - g_{p+1}) = \begin{cases} 1 & g_p \geq g_{p+1} \\ 0 & g_p < g_{p+1} \end{cases} \quad (9)$$

$$d = max|g_p - g_c| \quad (10)$$

$$p \in (0,1 \ldots P-1) \quad (11)$$

where
g_c, g_p, g_{p+1}, p, R and P are as previously defined,

d is the index of the neighbour pixel with the highest value, which defines the dominant direction in a neighbourhood. RINLBP provides rotation invariance by starting the encoding process with the neighbour pixel that has the highest value. This ensures that there is a corresponding rotation of the extracted binary pattern whenever the image is rotated.

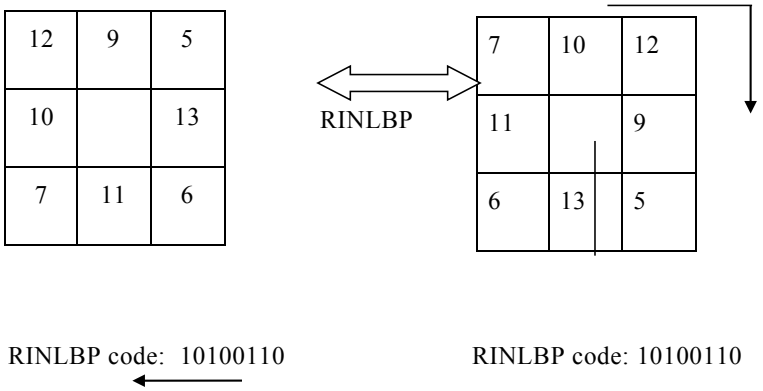

Figure 3. Rotation invariant neighbour-based LBP

The image in Figure 3 is rotated through an angle of 90° before applying the NLBP technique. The figure shows that RINLBP computes the same binary pattern from the original and the rotated images. This shows that image rotation does not affect the value of the binary pattern encoded by the RINLBP operator. We resized each face image to 16×8 before applying the RINLBP. This enabled us to obtain a 1,024-bit binary representation of the face image.

Segmentation isolates the iris from other structures that can affect the accuracy of the recognition process. This process involves detecting the inner and outer boundaries of the iris as well as the eyelids and eyelashes, which can interrupt the circular contour of the limbus boundary. The circular Hough transform is used for detecting the iris and pupil boundaries. Hough transform is defined as $x^2+y^2=r^2$, where (x,y) are the coordinates of the centre of the iris and pupil and r is the radius of the circular iris/pupillary boundaries. Figure 4 illustrates a segmented iris image.

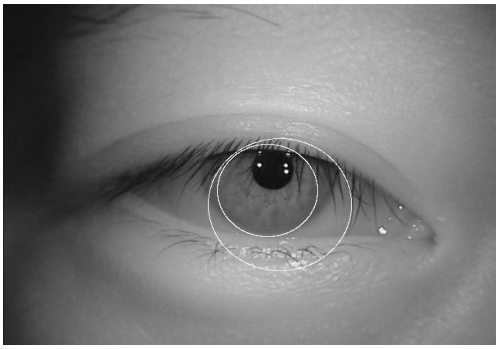

Figure 4. Segmented iris

Normalisation addresses variations in pupil size and provides for translation and scale invariance in order to ensure that irises of different individuals are mapped onto a common domain, since pupil size can vary across subjects. Normalisation is defined in Equation 12 as:

$$I(x(r,\theta),\ y(r,\theta)) \rightarrow I(r,\theta) \tag{12}$$

such that

$$x(r,\theta) = (1-r)x_p(\theta) + rx_l(\theta) \tag{13}$$

$$y(r,\theta) = (1-r)y_p(\theta) + ry_l(\theta) \tag{14}$$

where $I(x,y)$ is the iris image, (x,y) denotes the original Cartesian coordinates, (r,θ) are the corresponding normalised polar coordinates, (x_p,y_p) and $(x_l,y_l$ are the coordinates of the pupil and iris boundaries along the θ direction (Masek, 2003). Normalisation is usually carried out using the rubber sheet (Daugman, 2002) model. The rubber sheet model is illustrated in Figure 5.

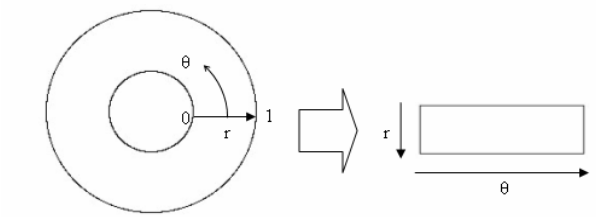

Figure 5. Rubber sheet model

Each point within the Cartesian coordinate is translated to a pair of polar coordinates (r, θ), where r lies within the range [0, 1] and θ is an angle in the range [0,2π]. Figure 6 illustrates a normalised iris image.

Figure 6. Polar iris image without noise

The rubber sheet model produces normalised irises of fixed dimension by taking both pupillary dilation and variations in pupil size into account. This ensures the extraction of iris codes of same dimension even if the size of the pupil varies across different subjects.

Feature extraction involves the application of a convolution operation to the 1D signals (obtained by breaking the 2D normalised iris image) using 1D Gabor wavelets. A Log-Gabor filter is defined in Equation 15 as:

$$G(f) = exp\left(\frac{-(log(f/f_0))^2}{2(log(\sigma/f_0))^2}\right) \quad (15)$$

where f_0 is the frequency and σ is the bandwidth of the filter (Field, 1987). The frequency response determines whether a given frequency value is quantised as 0 or 1. Feature extraction produces a binary template containing a number of bits of information that represent the iris image. The total number of bits in the template is two times the product of the angular resolution, the radial resolution and the number of filters used. A 1024-bit iris code is obtained by setting the values of angular resolution, radial resolution and filter to 8, 128 and 1, respectively.

The feature level fusion technique was used to create multibiometric templates from binary face and iris features. The process was carried out by transforming the templates into row vectors and appending one at the end of the other. That is,

$$MultiBio = FeatFace * FeatIris \quad (16)$$

where *MultiBio, FeatFace* and *FeatIris* are the multibiometric, face and iris feature vectors, respectively.

Implementation

The algorithm in Figure 7 describes the procedure for creating the transformation matrix.

Algorithm 1: *Computation of transformation matrix*

Input *P*

For *k = 1 to 2*

Read *i, j*

$row(i) \leftrightarrow row(i \pm j)$

Output m_1, m_2

$M_T = m_1 \oplus m_2$

End

Figure 7. Algorithm for computation of transformation matrix

Each elementary permutation matrix is computed by randomly selecting and interchanging a pair of rows of a general permutation matrix. Generally, a total of *n!* elementary permutation matrices can be computed from an $n \times n$ general permutation matrix. The combination of two elementary permutation matrices (from a given set of n! elementary permutation matrices) to obtain a non-invertible matrix produces a total of $\binom{n!}{2} = n!_{C_2} = \frac{(n!)!}{(n!-2)2!} = \frac{n!(n!-1) \ldots (n!-2+1)}{2!}$ non-invertible matrices. The non-invertible matrix (or transformation key), M_T is created by XORing two elementary permutation matrices, m_1 and m_2. That is,

$$M_T = m_1 \, XOR \, m_2 \tag{17}$$

The binary string, X (that is, the reference biometric template) is first converted into a one-dimensional column vector. A non-invertible template, X_T , is created by multiplying the transformation matrix, M_T , with the column vector representing X. That is,

$$X_T = M_T * X \tag{18}$$

The transformed template, X_T , is stored in the database instead of the original feature vector, X. The algorithm for enrolment is shown in Figure 8.

Algorithm 2: *Enrolment*

Input M_T, N

For *all* $i \in N$

Read X^i

$X_T^i = M_T * X^i$

End

Figure 8. Algorithm for enrolment

The algorithm in Figure 9 describes the procedure for authentication.

Algorithm 3: *Authentication*

Input M_T, N

For *all* $i \in N$

Read Y^i, X_T^i

$Y_T^i = M_T * Y^i$

Z=*hamming* (X_T^i, Y_T^i)

If $Z < \rho$ ***then***

accept

Else

reject

End

Figure 9. Algorithm for authentication

Performance Evaluation

The performance of the scheme was evaluated using 756 face images and 756 iris images of 108 subjects (or users) from CASIA Near Infrared face database (Li et al., 2007) and CASIA iris image database version 1 (biometrics.idealtest.org/dbDetailForUser.do?id=2), respectively. An additional dataset consisting of 196 face images of 100 subjects obtained from Labeled Faces in the Wild (Huang et al., 2008) was also used to evaluate the recognition accuracy of the proposed approach. The recognition accuracy was reported in terms of false acceptance

rate (FAR) and false rejection rate (FRR). False rejection results from a situation where the Hamming Distance between a pair of same-user templates is greater than the threshold. False acceptance occurs when the hamming distance between a pair of transformed templates belonging to different users is less than the threshold. The threshold used for the experiments was 0.30. The justification for the choice of this value is explained as follows. The range of intra-class variation between iris textures of the same person is 10-20% whereas irises of different subjects differ by 40-60% (Hao et al., 2006). This means that a threshold of at most 20% or 0.20 would effectively discriminate same-person iris images from those of different subjects. The same threshold was applied to face and multibiometric data in order to provide a fair comparison of the performance of the matrix transformation technique on different biometric modalities.

Table 1 presents the performance evaluation results for the application of matrix transformation on face images obtained from CASIA Near Infra Red (NIR) database.

Table 1
Performance results – Matrix Transformation (Face – CASIA NIR database)

Hamming distance	Recognition accuracy (%)	
	FRR	FAR
0.20	4.629	78
0.25	0.231	99
0.30	0.0	100
0.35	0.0	100

Results in the table show that FRR decreases as the hamming distance increases while FAR increases with a corresponding increase in threshold value. This is because an increase in hamming distance lowers the rate at which legitimate users are treated as impostors but with an increase in the number of impostors who are accepted as valid users. Conversely, a lower hamming distance results in an increase in FRR and a reduction in FAR. That is, there is more likelihood for legitimate users to be regarded as impostors and less likelihood for impostors to be accepted as valid users. An increase in hamming distance results in low intra-class variation and low inter-class distance. That is, there is higher correlation among the biometric data of same subjects and less variation among the biometric data of different subjects.

Table 2 shows the performance evaluation results for the application of matrix transformation on face images obtained from Labeled Faces in the Wild (LFW) dataset.

Table 2
Performance results – Matrix Transformation (Face – LFW database)

Hamming distance	Recognition accuracy (%)	
	FRR	FAR
0.20	0.0	14.4
0.25	0.0	33.1
0.30	0.0	88.9
0.35	0.0	100

The table shows that the FRR for all the Hamming distance values was 0%. This implies that a high correlation exists among face images of same users. The FAR increases with a corresponding increase in Hamming distance. A high Hamming distance value increases the collision among biometric data of different subjects. This leads to an increase in the rate at which impostors are accepted as valid users. A comparison of the results in Tables 1 and 2 shows that the proposed approach has better recognition accuracy for the LFW dataset than it does for the CASIA NIR database. This is because the LFW dataset consists of colour images while the CASIA NIR database contains greyscale images. The LBP and its variants have better recognition accuracy on colour images than greyscale images (Choi et al., 2012). However, both tables show that matrix transformation has low FRR (between 0% and ~4.63) but an intolerable FAR (between 14.4% and 100%). Hence, it is difficult to plot a suitable ROC curve based on the performance results obtained. This implies that the application of matrix transformation on face modality has poor recognition accuracy based on the chosen hamming distance values. Finding optimal hamming distance values required for good recognition accuracy for face (or any biometric) is outside the scope of this work. The focus of the work was to provide a fair comparison of the recognition performance of matrix transformation on face, iris and multibiometric data.

The result of the application of matrix transformation on iris data is presented in Table 3.

Table 3
Performance results – Matrix Transformation (Iris)

Hamming distance	Recognition accuracy (%)	
	FRR	FAR
0.20	64.35	0
0.25	32.02	0
0.30	8.769	0.007
0.35	1.466	0.139

The table shows that FRR decreases from 64.35% to 1.466% as the hamming distance increases from 0.20 to 0.35. On the other hand, the FAR increases from 0% to 0.139% for the chosen hamming distance values. Increasing the hamming distance results in lower intra-class variations among the biometric data of same subjects and higher correlation among the data of different subjects. Low intra-class variation leads to the rejection of fewer valid users (lower false rejection) and acceptance of more impostors (higher false acceptance). Moreover, increasing the hamming distance allows more impostors to be accepted as valid users and fewer valid users to be treated as impostors.

Figure 10 is the ROC curve for the application of matrix transformation technique on iris templates. The graph illustrates the relationship between FAR and FRR for different values of Hamming distance.

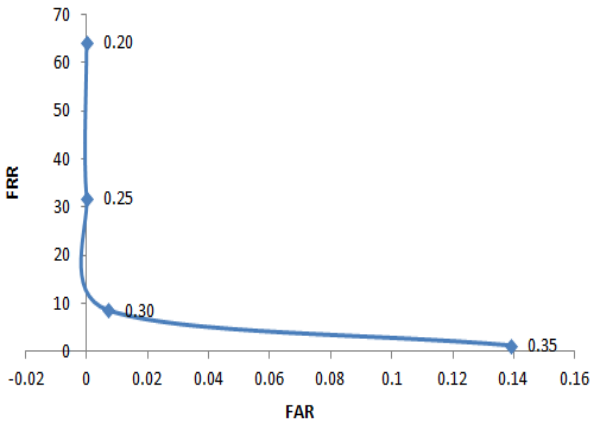

Figure 10. ROC curve for matrix transformation (iris)

The maximum value of FRR is approximately 64.4% and the minimum value of FRR is slightly below 1.47%. FAR has a maximum value of about 0.14% and a minimum value of approximately 0%. The curve shows that FRR reduces as FAR increases and vice versa. The value of FAR for each hamming distance is lower than the corresponding value of FRR. This implies that the approach sacrifices recognition accuracy and user convenience for security.

Table 4 shows the performance evaluation results for the application of matrix transformation on multibiometric data.

Table 4
Performance results – Matrix Transformation (Multibiometric)

Hamming distance	Recognition accuracy (%)	
	FRR	FAR
0.20	29.78	0.007
0.25	19.75	0.46
0.30	10.42	5.17
0.35	4.93	20.67

The FRR for the lowest hamming distance is ~29.8% while the highest hamming distance value has a false rejection rate of ~4.9%. Increasing the hamming distance leads to a reduction in both intra-class variation and inter-class distance. In other words, the rate at which genuine users are treated as impostors reduces with a corresponding increase in hamming distance. On the other hand, an increase in hamming distance results in the acceptance of more impostors as valid users. A lower hamming distance results in the rejection of more genuine users (higher FRR) and the acceptance of fewer impostors (lower FAR).

The relationship between the false rejection rate and false acceptance rate based on the application of matrix transformation on multibiometric data is illustrated by the ROC curve in Figure 11.

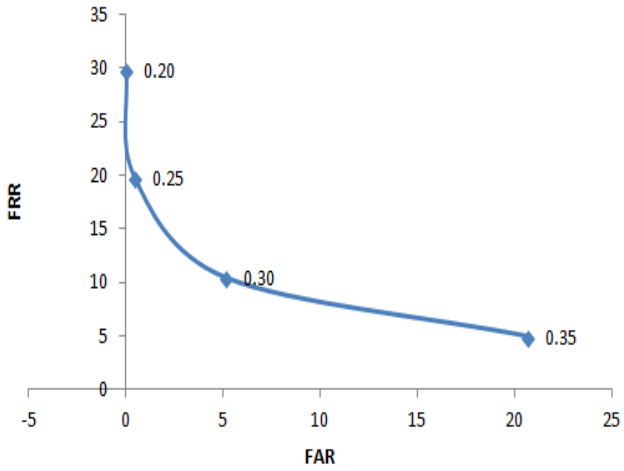

Figure 11. ROC curve for matrix transformation (multibiometric)

The maximum value of FAR is ~20.7% and the minimum value is ~0.007%. FRR has maximum and minimum values of approximately 29.8% and 4.9%, respectively. The curve shows that the FRR for each threshold is higher than the corresponding FAR. This implies that a higher premium is placed on security than on user convenience.

Security Analysis

The security of the proposed scheme was analysed using selected parameters, such as key length, key space, entropy and probability of correct guess in order to determine its resistance to security attacks (such as guessing and key exhaustion), privacy attacks (such as record multiplicity and cross matching) and template reconstruction attack.
Key length is the number of bits in the transformation key. It is expressed as the square of the dimension of the transformation matrix. Key length, K_l , is defined in Equation 19 as:

$$K_l = n^2 \tag{19}$$

where n is the dimension of the transformation matrix.

$\therefore$ key length 2^{20}= 1,048,576 bits. These keys are long enough to prevent guessing attack.

Key space, Ks_{pace} , is computed using the formula:

$$K_{space} = n!_{C_2} = \frac{(n!)!}{(n!-2)2!} = \frac{n!(n!-1)\ \ldots\ (n!-2+1)}{2!} \tag{20}$$

where n is the dimension of the transformation key.

The value of *n* used for the experiments is 1024.

$$\Rightarrow K_s = \frac{(1024!)!}{(1024!-2)2!} = \frac{1024!(1024!-1)\ \ldots\ (1024!-2+1)}{2!}$$

$\gg 1024!$ ($\gg$ is the symbol for much greater than)

The large key space prevents exhaustive search and cross-matching attacks.

Entropy, is expressed in Equation 21 as:

$$H = \log_2 N^K \tag{21}$$

where *N* is the symbol count and K is the key length (Shannon, 1948).

The value of key length is 2^{20} (or 1,048,576) bits

$\therefore H = \log_2 2^{1048576} = 1{,}048{,}576$ bits.

This is prohibitively large enough to prevent an attacker from carrying out a random guessing attack against the authentication system.

The probability of correct guess, $P_r\,(guess)$, measures the possibility that an attacker will guess a transformation key correctly. It is expressed as the inverse of the key space, K_{space} . That is,

$$P_r\,(guess) = {}^1\!/_{K_{space}} \tag{22}$$

$\therefore P_{guess} = {}^1\!/_{1024!} \ll 0$. The probability of guessing a transformation key is very low (much less than 0).

Theoretical analysis of irreversibility is used to determine the complexity of recovering an original biometric data from a transformed template and the transformation parameter. The analysis is presented as follows.

Consider a 4×4 general permutation matrix,

$$P = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

An elementary permutation matrix, p_a , is obtained by interchanging the first and second rows of *P*. That is,

$$p_a = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

The second elementary permutation matrix, p_b , is obtained by interchanging the third and fourth rows of P. That is,

$$p_b = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

The transformation matrix or key, is computed by the operation p_a *xor* p_b. Hence,

$$R = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}$$

Now consider a one-dimensional column vector, $x = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}$. The transformed template Y is computed by the multiplication operation, $y = Rx$. That is,

$$y = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix} \circ \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

The non-invertible analysis is carried out based on two scenarios, namely, "with respect to *R* scenario" (that is, when an attacker knows the transformation key) and "with respect to without *R* scenario" (that is, when an attacker does not have access to the transformation key).

(a) Non-invertible analysis with respect to R scenario

$x = {}^{y}/_{R}$, where R is the transformation matrix and y is the transformed template.

$=R^{-1}y$

Recall that $R = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}$,

hence $R^{-1} = \begin{bmatrix} inf & inf & inf & inf \\ inf & inf & inf & inf \\ inf & inf & inf & inf \\ inf & inf & inf & inf \end{bmatrix}$

The inverse of R is undefined because R is a singular matrix. That is, the determinant of R, $det(R) = 0$.

An alternative approach is to attempt to recover x from R and y using a system of simultaneous equations constructed from R and y (Li & Hu, 2013). Based on the example above, we attempt to retrieve the original biometric vector.

$x = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix}$ from the matrix $R = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}$ and transformed template $y = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$

using a system of linear equations

$$0x_1 + 0x_2 + x_3 + x_4 = 1 \quad (23)$$

$$0x_1 + 0x_2 + x_3 + x_4 = 1 \quad (24)$$

$$x_1 + x_2 + 0x_3 + 0x_4 = 1 \quad (25)$$

$$x_1 + x_2 + 0x_3 + 0x_4 = 1 \quad (26)$$

The solutions for the equation will be the original biometric vector $x = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix}$

By eliminating the variables containing 0, we have

$$x_3 + x_4 = 1 \quad (27)$$

$$x_3 + x_4 = 1 \quad (28)$$

$$x_1 + x_2 = 1 \quad (29)$$

$$x_1 + x_2 = 1 \quad (30)$$

Using Equation 27 and 28,

$$x_3 = 1 - x_4 \quad \text{(from Equation 27)}$$

Substituting for x_3 in Equation 28, we have

$$1 - x_4 + x_4 = 1 \quad \text{or } 1 - 0 = 1$$

Moreover, $x_4 = 1 - x_3$ (from Equation 28)

Substituting for x_4 in Equation 27, we have

$1 - x_3 + x_3 = 1$ or $1 - 0 = 1$.

Using Equation 29 and 30,

$x_1 = 1 - x_2$ (from Equation 29)

Substituting for x_1 in equ. 30, we have

$1 - x_2 + x_2 = 1$ or $1 - 0 = 1$

Moreover, $x_2 = 1 - x_1$ (from Equation 30)

Substituting for x_2 in Equation 29, we have

$1 - x_1 + x1 = 1$ or $1 - 0 = 1$

The result in all cases is 1. But we do not know which variable has the value of 1. This makes it difficult to assign values to each x_i in $x = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix}$

Hence, it is impossible to retrieve *x* from *y* even if *R* is known.

(b) Non-invertible analysis with respect to without R scenario

In this case, only the transformed template $y = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$ is available.

A compromise of the authentication scheme will require two steps:

(i) An attacker will have to generate all possible values of *x*. Each *x* is an *n*×1 dimensional vector, where n is the number of bits in the compromised transformed template. This requires an effort of *n!*

(ii) Each *x* is transformed using each of the possible values of *R*.
This requires an effort of $n!_{C_2} = \frac{(n!)!}{(n!-2)2!} = \frac{n!(n!-1) \ldots (n!-2+1)}{2!}$
For *n!* vectors, the total effort required = $n!\left(\frac{(n!)!}{(n!-2)2!}\right)$

(iii) Each transformed *x* is compared with the compromised *y* resulting in an effort of $n!\left(\frac{(n!)!}{(n!-2)2!}\right)$.

(iv) A match between a transformed *x* and a compromised *y* indicates that both of them are generated from the same feature vector.

The complexity of this analysis is defined in terms of the total effort required to obtain all possible transformed values of *x* (exhaustive search) and to match each transformed *x* with a compromised *y*

$$= n!\left(\frac{(n!)!}{(n!-2)2!}\right) + n!\left(\frac{(n!)!}{(n!-2)2!}\right) = 2\left(n!\left(\frac{(n!)!}{(n!-2)2!}\right)\right)$$

Using this approach for a 4-bit template, we substitute $n = 4$.

The total effort required $2\left(4!\left(\frac{(4!)!}{(4!-2)2!}\right)\right) = 6.768\times10^{23}$ iterations.

Table 5 illustrates the relationship between the dimension of biometric data and complexity of an exhaustive search attack.

Table 5
Relationship between dimension of biometric data and complexity of an exhaustive search attack

Length of biometric template (n)	Complexity of operation (iterations)
4	6.768×10^{23}
5	6.80×10^{198}
6	overflow
⋮	⋮
1024	overflow

The complexity of irreversibility with respect to without *R* scenario increases as the dimension of biometric data increases. Matrix transformation uses a 1024-bit template, which makes it computationally infeasible to retrieve an original template from only its transformed version.

Privacy Analysis

The privacy capability of matrix transformation is analysed using the requirements proposed in the ISO/IEC JTC 1/SC 27 (BioKeySIII Final Report, 2011) standard. These include irreversibility, unlinkability, confidentiality and data minimisation.

Irreversibility analysis. With respect to matrix transformation, irreversibility is defined in terms of the difficulty an attacker faces in an attempt to recover original biometric data, from a transformed template, *Y*. Detailed analysis of irreversibility has been using both "with respect to *R* and without *R*" scenarios. The analysis shows that an attacker faces a computationally difficult task in an attempt to recover original biometric data from a transformed template.

Unlinkability analysis. This is used to determine the effort (computational complexity) required to match biometric references across multiple databases or applications. A pair of biometric data is 'linkable' if it is possible to establish that they are obtained from the same user. The analysis of unlinkability is carried out by considering both the average case and worst-case scenarios.

Average case. The average case involves matching a compromised template with only half of the possible instances of transformed templates. The effort required, E_{CM}

$$= {}^{n!_{C_2}}/_2 = \frac{(n!)!}{2(n!-2)2!} = \frac{n!\,(n!-1)\ \ldots\ (n!-2+1)}{2(2!)}$$

$$= \frac{n!\,(n!-1)\ \ldots\ (n!-2+1)}{4}$$

By substituting n = 1024, we have

$\frac{1024!(1024!-1)\ \ldots\ (1024!-2+1)}{4} \gg$ 1024! iterations

Worst case. This involves matching all possible instances of transformed templates. The effort required, E_{CM}

$$= n!_{C_2} = \frac{(n!)!}{(n!-2)2!} = \frac{n!\,(n!-1)\ \ldots\ (n!-2+1)}{2!}$$

$= \frac{1024!(1024!-1)\ \ldots\ (1024!-2+1)}{2!} \gg$ 1024! iterations.

The effort required when the entire transformed templates is matched is twice that which is required for matching only half of the transformed templates. However, the effort in both cases is in excess of 1024! iterations. This is prohibitively large enough to prevent a cross-matching attack in matrix transformation.

Confidentiality analysis. A secured template, y is created by applying a transformation matrix, on a biometric data, x. That is,

$$y = Rx$$

The transformed template is stored in the database while the original biometric data, , is discarded. The example above shows that the transformed template, $y = \begin{bmatrix}1\\1\\1\\1\end{bmatrix}$ is distinguishable from the original biometric data, $x = \begin{bmatrix}1\\0\\0\\1\end{bmatrix}$. In other words, the transformation operation uses R to conceal x in y.

Data minimisation. Matrix transformation stores only transformed templates, , and possibly the transformation key, R. Sensitive biometric data that may violate users' privacy are not retained in the authentication system during enrolment and authentication.

DISCUSSION OF RESULTS

Results in Tables 1, 2, 3 and 4 show that matrix transformation has low FRRs (between 0% and ~4.63%) when it is applied to face biometric than it does when applied to iris or multibiometric modality. However, this is achieved at the expense of intolerably high FARs (between 14.4% and 100%). This is due to the low inter-class distance among face images of different subjects (Wu & Yuan, 2010). High FARs also imply a high correlation among transformed templates of different users for the chosen hamming distance values. Low FRR and high FAR imply high usability (or user convenience) and low security. The application of matrix transformation on iris results in high FRRs of 64.35% and 32.02% for hamming distance values of 0.20 and 0.25, respectively. However, the FARs recorded for both hamming distance values is 0%. Increasing the hamming distance values to 0.30 and 0.35 results in improvements in recognition accuracy as the FRRs reduce to 8.796% and 1.466%, respectively. The FAR also increases from 0% to 0.007% and 0.139% for the respective hamming distance values. This implies that hamming distance values of 0.30 and 0.35 provides a good balance between security and user convenience in an iris-based matrix transformation scheme. Applying matrix transformation on multibiometric data results in high FRRs of 29.78%, 19.75% and ~10.42% for hamming distances of 0.20, 0.25 and 0.30, respectively. Increasing the hamming distance to 0.35 results in a lower FRR (~4.9%) and high FAR (~20.67%). Results from experiments show that the matrix transformation has better recognition accuracy when applied to iris biometric (especially at hamming distances of 0.30 and 0.35) than it does when it is applied to face or multibiometric data. The iris is a more reliable biometric modality because it exhibits low intra-class variation and high inter-class distance (Bowler et al., 2007). Matrix transformation also achieves improved performance results when it is applied to multibiometric modality than it does when face modality is used. This is because the presence of iris bits in multibiometric templates minimises the impact of the pervasiveness of the face on the recognition accuracy of the system. Security analysis shows that matrix transformation has long key length, large key space, high key entropy and low probability of correct guess of the key. Thus, matrix transformation is resistant to random guessing and exhaustive search attacks. Privacy analysis shows that matrix transformation provides irreversibility, confidentiality and data minimisation. The complexity of unlinkability analysis in matrix transformation is very high. This enables the approach to provide sufficient resistance against cross-matching attacks. Irreversibility prevents the recovery of original biometric data from transformed templates. Legitimate users are protected against loss of identity as attackers cannot reconstruct actual biometric images from compromised biometric templates.

A comparison of the recognition accuracy of the proposed matrix transformation and related works is presented in Table 6.

Table 6
Comparison between our approach and previous studies (recognition accuracy)

Author	Technique	Dataset	Performance (%)			
			FRR	GAR	FAR	EER
Moujahdi et al., 2012	Spiral cube	Yale face	100		0	
Zuo et al., 2008	BIN combo			100	0.1	
	GREY combo	MMU1 iris data set		99.5	0.01	
Our approach	Matrix transformation		10		5.5	
Hammerle-Uhl et al., 2009	Block re-mapping					1.2
	Image warping					1.3
Rathgeb et al., 2010	User-specific permutation	CASIA iris V3	3.821		0	
Rathgeb et al., 2014	Alignment-free adaptive Bloom filter		2.05		0.01	
Our approach	Matrix transformation		7.889		2.74	

Results from previous works show that the proposed approach has lower recognition accuracy than the previous works. The alteration of the bits in the original template makes matching difficult in the transformation domain. Hamming distance provides limited error correction capability because it corrects only bit errors and does not address burst errors. The long dimension of biometric data (1024 bits) used by matrix transformation imposes a high overhead on the error correcting capability of hamming distance and this results in performance degradation. However, it is pertinent to mention that the main goal of matrix transformation is to provide high template security and user privacy.

Table 7 presents a comparison of the security of the proposed matrix transformation and related works.

Table 7
Comparison between our approach and previous studies (security)

Author	Modality	Technique	Security			
			Key length (bits)	Key Space	Entropy (bits)	Pr (correct guess)
Zuo et al, 2008	Iris image	Grey-combo	260	2^{260}	260	5.39×10^{-79}
	Binary iris code	Bin-combo	560	2^{560}	560	0
Rathgeb & Uhl, 2010	Binary iris code	User-specific permutation		38!		1.91×10^{-45}
Moujahdi et al., 2012	Face	Spiral cube		100^{200}		$\ll 0$
Sandhya et al., 2016	Fingerprint	Delaunay		2.5 billion/		
		triangle		8.35 billion		
Our approach	Face, iris and multibiometric	Matrix transformation	2^{20} or 1,048,576	1024!	2^{20}	$\ll 0$

The proposed scheme has much higher key length, larger key space and higher entropy than the previous approaches. Its keys also have a much lower probability of correct guess compared to the previous schemes. Security and privacy analysis in Sections 5.7 and 5.8 show that the level of template security and user privacy provided by a biometric cryptosystem depends largely on its key length and key space. The proposed approach has a much higher key length and larger key space compared to the previous schemes. Hence, it is more robust to security and privacy attacks than existing approaches.

CONCLUSION

This paper proposed and applied the matrix transformation technique to three different biometric modalities (face, iris and multibiometric) unlike previous approaches that used only one biometric modality. The study highlights the effect of the nature of biometric data on the performance accuracy of the proposed approach. Matrix transformation provides high-level template security and user privacy compared to other approaches. The low recognition accuracy of the proposed multibiometric template protection scheme can be addressed by integrating a key binding technique that uses better error correction techniques; This will result in a hybrid multibiometric template protection scheme that provides improved template security and user privacy without compromising recognition accuracy.

Results from previous works show that the proposed approach has lower recognition accuracy than the previous works. The alteration of the bits in the original template makes matching difficult in the transformation domain. Moreover, Hamming distance provides limited error correction capability. That is, it corrects only bit errors and does not address burst errors. The long dimension of biometric data (1024 bits) used by matrix transformation imposes a high overhead on the error correcting capability of Hamming distance and this results in performance degradation. However, it is pertinent to mention that the main goal of matrix transformation is to provide high template security and user privacy.

ACKNOWLEDGEMENT

This material is based upon work supported by the Ministry of Higher Education Malaysia under Grant No. FRGS 08-01-15-1721FR.

REFERENCES

Boult, T. (2006). Robust distance measure for face recognition supporting revocable biometric tokens. In *Proceedings of 7th International Conference on Automatic Face and Gesture Recognition* (pp. 560–566). New York, NY, USA: IEEE.

Boult, T., Scheirer, W., & Woodworth, R. (2007). Revocable fingerprint biotokens: Accuracy and security analysis. In *Proceedings of IEEE Conference on Computer Vision and Pattern Recognition*. New York, NY, USA: IEEE. Doi: 10.1109/CVPR.2007.303110.

Bowler, K., Hollingsworth, K., & Flynn P. (2007). Image watermaking for iris: A survey. *Computer Vision and Image Understanding, 110*(2), 281–307.

BIT. (2010). *CASIA Iris Image Database Version 2.0*. Biometrics Ideal Test. Retrieved from http://biometrics.idealtest.org/

Campisi, P., & Egiazarian, K. (2007). *Blind image deconvolution: Theory and applications*. Raton, Florida, USA: Boca CRC Press.

Choi, J. Y., Ro, Y. M., & Plataniotis, K. N. (2012). Color local texture features for color face recognition. *IEEE Transactions on Image Processing, 21*(3), 1366–1380.

Farberbock, P., Hammerle-Uhl, J., Kaaser, E., Pschernig, D., & Uhl, A. (2010). Transforming rectangular and polar iris images to enable cancelable biometrics. In A. Camilho & M. Kamel (Eds.), *Image analysis and recognition – Lecture notes in computer science* (Vol. 6112, pp. 276–286). Berlin Heidelberg: Springer.

Feng, Y. C., & Yuen, P. C. (2012). Vulnerabilities in binary face template. *2012 IEEE Computer Society Conference on Computer Vision and Pattern Recognition Workshop* (pp. 105–110). New York, NY, USA: IEEE.

Field, D. J. (1987). Relations between the statistics of natural images and the response properties of cortical cells. *Journal of the Optical Society of America 4*(12), 2379–2394.

Grassi, M., & Faundez-Zanuy, M. (2009). Protecting DCT templates for a face verification system by means of pseudo-random permutations. In J. Cabestany, F. Sandoval, A. Prieto & J. M. Corchado (Eds.), *Bio-Inspired systems: Computational and ambient intelligence – Lecture notes in computer science* (Vol. 5517, pp. 1216–1223). Heildelberg, Berlin: Springer.

Hammerle-Uhl J., Pschernig E., & Uhl, A. (2009). Cancelable iris biometrics using block re-mapping and image warping. In P. Samarati (Ed.), *Information security – Lecture notes in computer science* (Vol. 5735, pp. 135–142). Heidelberg, Berlin: Springer.

Hamouchene, I., & Aouat, S. (2014, August). A cognitive approach for texture analysis using neighbors-based binary patterns. In *Cognitive Informatics and Cognitive Computing (CICC), 2014 IEEE 13th International Conference on* (pp. 94-99). IEEE.

Hao F., Anderson, R., & Daugman J. (2006). Combining cryptography with biometrics effectively. IEEE *Transactions on Computers, 55*(9), 1081–1088.

Hariprasath, S., & Prabakar, T. N. (2012). Multimodal biometric recognition using iris feature extraction and palmprint features. In *IEEE International Conference on Advances in Engineering, Science and Management* (pp. 174–179). New York, NY, USA: IEEE.

He, Y., Yap, K. H., Chen, L., & Chau, L. P. (2008). A novel hybrid model framework to blind color image deconvolution. *IEEE Transactions on System, Man and Cybernetics – Part A: Systems and Humans, 38*(4), 867–880.

Huang, G. B., Ramesh, M., Berg, T., & Learned-Miller, E. (2008). Labeled faces in the wild: A survey. In M. Kawulok, M. Emre Celebi, & B. Smolka (Eds.), *Advances in face detection and facial image analysis* (pp. 189–298). New York, NY: Springer International Publishing.

Jeong, M. Y., & Teoh, A. B. J. (2010). Cancellable face biometrics system by combining independent component analysis coefficients. In H. Sako, K. Franke, & S. Saitoh (Eds.), *Computaional forensics – Lecture notes in computer science* (Vol. 6540, pp.78–87). Berlin, Heidelberg: Springer.

Karmakar, D., & Murphy, C. A. (2014). Generation of new points for training set and feature – Level fusion in multimodal biometric identification. *Machine Vision and Applications, 25*, 477–487.

Kaur, G. M. (2013). Multimodal-Based fuzzy vault using iris, retina and fingervein. In *Fourth International Conference on Computing, Communications and Networking Technologies*. New York, NY, USA: IEEE. doi: 10.1109/ICCCNT.2013.6726786.

Li, C., & Hu, J. (2013). Attacks via record multiplicity on cancelable biometric templates. *Concurrency and Computation: Practice and Experience, 26*(8), 1593-1605. doi: 10.1002/cpe.3042.

Li, S., & Cot, A. C. (2011). Attacks using reconstructed fingerprint. In *2011 IEEE International Workshop on Information Forensics and Security*. New York, NY, USA: IEEE. Doi: 10.1109/WIFS.2011.6123151.

Li, S. Z., Chu, R. F., Liao, S. C., & Zhang, L. (2007). Illumination invariant face recognition using near-infrared images. *IEEE Transactions on Pattern Analysis and Machine Intelligence (Special issue on Biometrics: Progress and Directions), 29*(4), 627–639.

Masek, L. (2003). *Recognition of human iris for biometric identification*. (Upublished MSc Thesis). University of Western Australia, Australia.

Moujahdi, C., Ghouzali, S., Mikram, M., Rziza, M., & Bebis, G. (2012, June). Spiral cube for biometric template protection. In *International Conference on Image and Signal Processing* (pp. 235-244). Heildelberg, Berlin: Springer.

Nishino, T., Kajikawa, Y., & Muneyasu, M. (2012). Multimodal person authentication system using features of utterance. In *2012 IEEE International Symposium on Intelligent signal Processing and Communication Systems* (pp. 43–47). New York, NY, USA: IEEE.

Ojala, T., Pietikainen, M., & Maenpaa, T. (2002). Multiresolution gray-scale and rotation invariant texture classification with local binary patterns. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 24*(7), 971–987.

Ouda, O., Tusamura, N., & Nakaguchi, T. (2011). Securing bioencoded iriscodes against correlation attacks. In *2011 IEEE International Conference on Communications*. New York, NY, USA: IEEE. doi: 10.1109/icc2011.5963247.

Plesca, C., & Morogan, L. (2014). Efficient and robust perceptual hashing using log-polar image representation. In *2014 10th International Conference on Communications*. New York, NY, USA: IEEE. doi: 10.1109/ICComm.2014.6866755.

Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal, 40*(3), 614–634.

Ratha, N. K., Connell, J. H., Bolle, R. M., & Chikkerur, S. (2006). Cancellable biometrics: A case study in fingerprints. In *Proceedings of 18th International Conference on Pattern Recognition* (pp. 370–373). New York, NY, USA: IEEE.

Ratha, N. K., Connell, J. H., Bolle, R. M., & Chikkerur, S. (2007). Generating cancellable fingerprints templates. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 29*(4): 561–572.

Rathgeb, C., & Uhl, A. (2010). Secure iris recognition based on local intensity variations. In A. Campilho & M. Kamel (Eds.), *Image analysis and recognition – Lecture notes in computer science* (Vol. 6112, pp. 266–275). Heildelberg, Berlin: Springer.

Rathgeb, C., Breitinger, F., Busch, C., & Baier, H. (2014). On the application of bloom filters to iris biometrics. *IET Biometrics, 3*(4), 207–218.

Safie, S. I., Nurfazira, H., Azavitra, Z., Soraghan, J. J., & Petropoulakis, L. (2014). Pulse active transformation: A non-invertible transformation with application to ECG biometric Authentication. In *2014 IEEE Region 10 Symposium* (pp. 667–671). New York, NY, USA: IEEE.

Sandhya, M., Prasad, M. V. N. K., & Chillarige, R. R. (2016). Generating cancellable fingerprint templates based on Delaunay triangle feature set construction. *IET Biometrics, 5*(2), 131–139.

Shannon, C. E. (1948) A mathematical theory of communication. *Bell System Technical Journal, 27*(3), 379–423.

Study of the Privacy and Accuracy of the Fuzzy Commitment Scheme. (2011). BioKeyS III-final report. *Bundesamt für Sicherheit in der Informationstechnik 2011*. Retrieved from http://www.bsi.bund.de

Teoh, A. B. J., Yip, W. K., & Toh, K. A. (2010). Cancellable biometrics and user-dependent discretization in biohash. *Pattern Analysis and Applications, 13*(3), 301–307.

Tharwat, A., Ibrahim, A. F., & Ali, H. A. (2012). Multimodal biometric authentication algorithm using ear and finger knuckle images. In *2012 7th International Conference on Computer Engineering and Systems,* Cairo (pp. 176–179). New York, NY, USA: IEEE.

Wang, S., & Hu, J. (2013). A Hadamard transformed-based method for the design of cancellable fingerprint templates. In *2013 6th International Congress on Image and Signal Processing* (pp. 1682–1687). New York, NY, USA: IEEE.

Wu, L., & Yuan, S. (2010). A face based fuzzy vault scheme for secure online authentication. In *2010 Second International Symposium on Data, Privacy and E-Commerce* (pp. 45–49). New York, NY, USA: IEEE.

Xiuyan, L., Changyun, M., Tiegen, L., & Chenhu, Y. (2011). Research on personal identity verification based on hand vein, iris and fingerprint. In *2011 International Symposium on Computer Science and Society* (pp. 16–19). New York, NY, USA: IEEE.

Zuo, J., Ratha, K., & Connell, J. H. (2008). Cancelable iris biometric. In *Proceedings of 19th International Conference on Pattern Recognition*. New York, NY, USA: IEEE. Doi: 10.1109/ICPR.2008.4761886.