International Journal of Security and Its Applications
Vol.9, No.12 (2015), pp.149-164
http://dx.doi.org/10.14257/ijsia.2015.9.12.15

Face Recognition and Template Protection with Shielding Function

Abayomi Jegede[1,2], Nur Izura Udzir[1], Azizol. Abdullah[1] and Ramlan. Mahmod[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, Nigeria*
abayomi.jegede@ymail.com, {izura, azizol, ramlan}@upm.edu.my

Abstract

Biometric authentication is the use of unique human features to provide a secure, reliable and convenient access to an environment or a computer system. However, there are numerous security and privacy concerns associated with the use of biometrics as a means of authentication. Unprotected biometric data can be used by an impostor to impersonate legitimate uses, to violate their privacy and steal their identity. This paper proposes a simplified, secure and privacy-preserving authentication scheme for face biometric based on modified shielding function. The modified shielding function is a simplified version of the generic shielding function which does not require additional preprocessing steps of quantization and reliable bit selection. Rotation invariant neighbour-based local binary pattern (RINLBP) is used to extract fixed length binary features directly from pre-processed face images. RINLBP is simple to calculate and has good performance. It is also robust against changes in illumination and image rotation. Concatenated error correction technique is used to address errors due to noise and intra-class variation. The concatenated technique corrects errors both block and bit errors in contrast to the generic shielding function in which only bit level errors are corrected. Results of experiments based on 200 face images obtained from the CASIA near infrared face database show a false acceptance rate of 0.47% and a false rejection rate of 1.56%. Our scheme has a key length of 120 bits, which is higher than the minimum requirement of 50 bits for biometric keys. It also has a large key space and entropy which makes it less susceptible to guessing attack (Pr =0.008).

Keywords: *authentication, biometric cryptosystem, security, shielding function template protection*

1. Introduction

Face recognition is a process which measures a person's facial characteristics and uses the result to confirm his identity. The first automatic face recognition system [21] uses a flexible analysis scheme which recognizes human faces based on local information extracted from face images. The human face is a preferred means of authentication because it is easily accessible to the sensor. Face recognition is a contactless and non-intrusive technology. Face image can be captured without any physical contact with the sensor and with limited cooperation by the user. Humans are also more likely to make their faces available compared to other biometrics such as fingerprints or signatures. This is evidenced by the way people share their face images freely on social networks such as Facebook and Instagram. Moreover, the availability of large legacy and experimental databases of faces provides the resources for large scale analysis of the face modality. These reasons make face a suitable biometric modality for many applications such as surveillance systems, law enforcement, border control and access control [15, 37]. A

ISSN: 1738-9976 IJSIA

practical face authentication system should be scalable and possess high recognition accuracy as well as high speed of operation [6].

Biometric cryptosystems or template protection systems provide authentication while simultaneously guaranteeing the security and privacy of users. Template protection systems do not store biometric data directly (in plain form) in the databases. Rather, a secret information is combined with the biometric data before it is stored. This makes it difficult for an impostor to obtain such biometric data without knowing the secret information. Applying a biometric cryptosystem also makes it possible to revoke, update or replace stored biometric data in case of theft, data corruption or other forms of compromise. An ideal template protection system should provide diversity, revocability, security and good recognition performance [14]. Template protection schemes are generally classified based on their mode of operation. There are five main categories of biometric cryptosystems, namely: bio-cryptographic schemes, key binding schemes, key generation schemes, cancellable schemes and hybrid schemes [39].

Key binding schemes combine a secret key with biometric data using known cryptographic algorithms [39]. The secrecy of the key and the complexity of the algorithm used to implement the key binding function guarantee the security of biometric data. Typical examples of key binding schemes are biometric encryption, fuzzy commitment scheme, fuzzy vault and shielding functions. Biometric encryption (or bio-cryptography) is a direct application of standard cryptographic algorithms to secure biometric templates. An example of such is the use of Hill Cipher algorithm to protect face template [35]. This approach is secure, but it is considered too slow for real-time and large scale application. Recent advances in biometric encryption include the application of elliptic curve cryptography to biometric key management in wireless sensor networks [52] and a novel implementation which uses Bernoulli-logistic mapping and chaotic encryption to secure biometric data [28]. Another innovation is the hybrid scheme based on packed homomorphic encryption and ideal lattices techniques [51].

A fuzzy commitment scheme [20] uses cryptography and error correcting code techniques to protect stored biometric data. The binding of a secret information with the biometric data makes it difficult for an attacker to know the actual contents of the data. Fuzzy commitment scheme was applied to three types of face features obtained using different methods, namely Eigen faces, 2DPCA (two-dimensional PCA) and LBPH (local binary pattern histogram) [5]. Results from experiments show that fuzzy commitment scheme has better performance when features are fused compared to when individual features are used. The fuzzy commitment approach was also used to address security and privacy issues associated with unprotected 2D face templates stored in databases of biometric recognition system [48]. Simulation results show that the approach is feasible both in terms of recognition accuracy and security of stored templates. In a related work [46], real value face features are first converted into binary using thresholding before applying the reliable component scheme to select the most discriminative binary features. The selected features represent the binary template which is secured using the fuzzy commitment scheme. Results from experiments using Caltech face database yield FRR = 3.5% and FAR $\approx$ 0. Tests based on FERET database yield FAR $\approx$ 0, but a high FAR of 35%. Experimental results also show that this approach can achieve a maximum key length of 130 bits. A recent study proposed and implemented a novel application which uses fuzzy commitment scheme for secure key management in body sensor networks [53].

The fuzzy vault scheme [19] uses a secret key to lock data in a vault. The vault can only be unlocked if there is another set of secret which shares a substantial degree of similarity with the original key. Fuzzy vault is normally applied to unordered feature sets such as fingerprints, but it has also been adapted to ordered dataset such as face features. One of such adaptation is the face fuzzy vault for online authentication which generates keys from user-specific passwords [50]. A user specific password is used to transform the face template before using the key to lock the transformed template in a fuzzy vault. The

transformation of face templates before they are stored in the fuzzy vault provides revocability and diversity. The study uses nearest distance matching algorithm to address intra-class variation. Digital signature is also employed to detect illegal modification of the information stored in the fuzzy vault. Experimental results show that this approach has a high level of security, but with high false acceptance and false rejection rates. Another adaptation of the generic fuzzy vault to face biometrics is based on assigning weights to individual components in the feature set [33]. The weight reflects the relative significance of a feature component in discriminating between two sets of features. This scheme has lower computational complexity, but requires more storage than the one based on the generic fuzzy vault. MoC-based fuzzy eigenface vault [23] is a two-factor authentication mechanism used to secure Eigen faces in a fuzzy vault. The secret information used for constructing of the fuzzy vault is stored on a smart card. This prevents disclosure of stored biometric data even if the vault is compromised. Two-factor authentication enhances the security of the scheme, but reduces user convenience. Face fuzzy vault has also been proposed for authentication in a cloud environment [18]. Deploying fuzzy vault in a multiple and diverse users environment such as the cloud provides security not only for the data stored in the cloud, but also for the biometric information of enrolled cloud users. Moreover, it guarantees the privacy of legitimate users by preventing cross matching attacks and user profiling.

Shielding function [29] or helper data scheme provides security for stored biometric reference data. With this approach, the authentication system can verify a user's identity without having any knowledge of the user's biometrics. Helper data scheme has been used to secure binary features extracted from face images [22, 30]. In [30], real value face features are first extracted using principal component analysis (PCA). The PCA features are later binarized before binding them with a randomly generated secret. Results from experiments show that the scheme achieved zero FAR, FRR of 0.8529% and a maximum key length of 36 bits. The helper data scheme proposed in [22] is based on 3D face images. 3D face images contain a richer set of information compared to 2D face images. Hence, the system is able to achieve template protection and good recognition performance. Shielding functions, like all other key binding approaches, are not resistant to spoofing attacks [36]. They are also susceptible to record multiplicity attack [39].

Biometric key generation schemes [7] (also known as secure sketches or fuzzy extractors) are used to generate a cryptographic key or hash directly from a given biometric data. Key generation is performed by first creating the helper data from the biometric template, followed by the use of the helper data and a given biometric data to obtain the key [14]. There are two major approaches to biometric key generation: private template scheme and quantization scheme [39]. A proposed quantization scheme used biometric hashing to obtain multiple face hashes or keys from a single face image [42]. Experiments show that the approach provides a simple and effective solution to template security and privacy concerns associated with biometric systems. In a later work [41], an enhanced quantization scheme was proposed for face biometrics. This approach is based on two-level quantization and is robust against preimage attack.

Cancelable biometrics refers to "an intentional, repeatable distortion of a biometric signal based on a chosen transform" [38]. Cancelable biometrics promotes diversity and unlinkability by generating multiple versions of transformed templates from a biometric image. Moreover, different transformation parameters can be used for different applications. Templates which are suspected to have been stolen or corrupted can be replaced using new transformation parameters. The templates are never decrypted during authentication. Authentication is carried out by comparing a transformed query template with transformed reference template. There are two main categories of cancelable biometrics, namely: non-invertible transforms and invertible transforms (or biometric salting) [39]. Non-invertible transform is one-way and does not allow the recovery of an original template from the transformed version. Biometric salting on the other hand,

allows the recovery of an original biometric data from the transformed version if both the template and the transformation parameters are known.

A non-invertible transformation technique known as revocable biotokens [3] splits a real value feature such as face into stable and unstable parts. The integer part represents the stable part while the fractional part represents the unstable part. Another approach to non-invertible transformation is the use of pseudo-random permutations to alter the order of features in face templates [11]. The parameter used for transformation is user-dependent. Moreover, it is impossible for an attacker to break the authentication system without knowing the pseudo random ordering of the scheme. Non-invertible templates have also been created from face features extracted using independent component analysis (ICA) [16]. The face feature vector is first modified by using Gaussian distribution to carry out a random replacement of some of its components. This is to ensure that the original feature vector retain its mean and variance. The next step is a random scrambling of the elements of the modified feature vector. This scheme provides revocability and discriminability of stored templates. It also guarantees the security and privacy of users.

The salting technique was used to generate cancelable face templates by applying user-specific secret PINs as seeds for a random basis function of the minimum correlation filters [40]. The security of biometric salting depends largely on the secrecy of the transformation algorithms and the key. Hence, a template is invertible if an attacker obtains the transformation algorithm and the secret key. A suggested solution to this problem is the use of a technique known as multispace random projection [43, 44] as a solution to this problem. The technique is robust against key leakage attack and provides good recognition performance. Salted face templates can also be obtained by using transforms based on user-specific random projection and error minimizations [24].

A hybrid scheme involves the combination of two or more biometric cryptosystem to obtain a single system which provides better security. An example is the face template protection scheme which combined cryptographic key generation technique with fuzzy vault [49]. The approach uses a randomly generated key to secure binarized PCA vectors in a fuzzy vault. Real-valued features are first extracted using PCA. Binary features are then obtained from the real-valued features by a process known as quantization. The randomly generated key is encoded using cyclic redundancy code (CRC). Finally, the encoded key is used to bind the binary face template in a fuzzy vault. The approach offers both diversity and revocability of templates. It also achieves good performance with FAR = 0. A related work [2] presented a hybrid scheme which combines an enhanced Biohash algorithm with key binding to secure face biometric templates. This scheme achieves better security but with a reduction in recognition accuracy. The hybrid cryptosystem in [8] attempts to strike a balance between the security of stored templates and recognition performance. The scheme combines biometric key binding and transformed-based techniques. This scheme is secure and promotes diversity among stored templates. A recent study [47] applied one-way cryptographic hashing to biometric before securing the hashed data with fuzzy vault.

2. Materials and Methods

2.1. Mathematical Description of Shielding Function

Given a binary biometric data, X of length i and a randomly generated binary secret S of length j; that is, $X \in \mathbb{R}^i$ and $S \in \{0,1\}^j$, a shielding function, g performs enrollment by computing a helper data, $W \in \{0,1\}^k$ such that $g^{-1}(X, W) = S$. A hash value, $h_1 = f(S)$ of the secret is also computed. g^{-1} is referred to as the inverse delta contracting (δ-contracting) function. Both h and W are stored in the database. It is required that the dimensions of biometric data, random secret and helper data should be equal, i.e. $i = j = k$. During authentication, the delta contracting function g computes a new secret, S' from

the stored helper data, W and a probe biometric data, X' of the same user, $g(X', W) = S'$. A hash value of the secret, S' is also computed, $h_2 = f(S')$. Authentication is successful if $h_1 = h_2$. See Linnartz and Tuyls [29] for a detailed discussion and mathematical proofs relating to the shielding function.

2.2. Proposed Approach

In previous implementations of shielding function [13, 22, 30, 45], real-value features extracted from fingerprints or face images are converted to binary by a process known as quantization. These implementations also applied reliable component scheme to select the most stable and discriminative binary bits which are used to represent the template. BCH coding are used to correct errors caused by intra-class variation. BCH coding cannot support a biometric feature whose dimension is longer than 511 bits; hence the need for feature selection. The study in [30] used PCA to extract real value features from face images. PCA is an appearance based feature extraction technique and it is not invariant to image rotation and changes in illumination. However, we propose a modified implementation of the shielding functions which eliminates the need for additional preprocessing steps of binarization and bit selection. In our work, we use rotation invariant neighbour-based local binary pattern [12] to extract binary features directly from face image. RINLBP is a modified version of the generic local binary pattern (LBP) [41]. The generic LBP is not invariant to image rotation. It suffers poor recognition performance when images are captured in unconstrained scenarios such as face images involving tilting of heads. RINLBP is simple to compute. It is also robust against changes in illumination and image rotation. Our concatenated error correction scheme is based on the integration of Reed-Solomon and Hadamard error correction techniques. The concatenated approach corrects burst errors associated with multiple blocks of data as well as bit errors within each block. This makes our method suitable for feature vectors of large dimensions such as 1,024 bits and 2,048 bits.

2.3. Image Preprocessing

Image preprocessing phase (see Figure1) makes it possible for machine readable features to be extracted from a face image. Preprocessing tasks include image acquisition, face detection and cropping. Face images can be acquired in the form of conventional 2D photographs, 3D range or depth images and videos. During face detection, a local texture information is obtained from an image and a binary classifier is applied in order to distinguish between the facial portion and other parts. This paper uses the Viola-Jones face detection technique because of its accuracy, real-time capability and availability as an open source software [15]. Cropping is used to remove some parts of the head (such as the ears) that do not constitute a face from the detected face image.

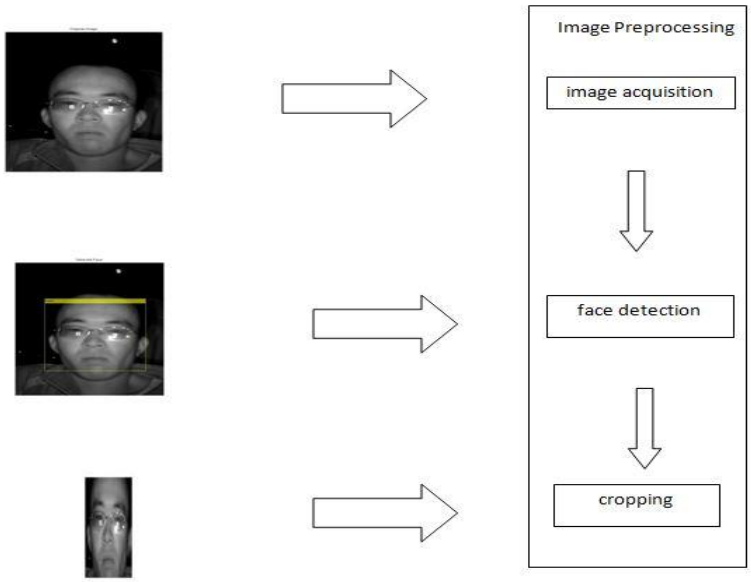


Figure 1. Image Preprocessing

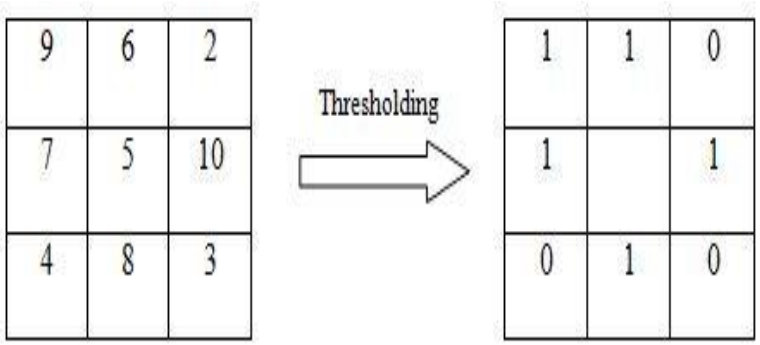
2.4. Feature Extraction

Feature extraction is a step to obtain useful components for representing images. These components are usually referred to as feature vectors. Each feature vector consists of a set of values. We used rotation invariant neighbour-based invariant local binary pattern for feature extraction. RINLBP improves on the generic LBP by addressing poor recognition performance due to image rotation. The LBP is a texture classification method which 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, that is,

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

$$s(x) = \begin{Bmatrix} 1 & x \geq 0 \\ 0 & x < 0 \end{Bmatrix} \quad (2)$$

where
g_p is grayscale 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 [34].



Local binary pattern: 11010101

Figure 2. Generic LBP in A 3 × 3 Window

Figure 2 describes the operation of the generic LBP. The LBP is popular because it is simple to calculate and has 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.

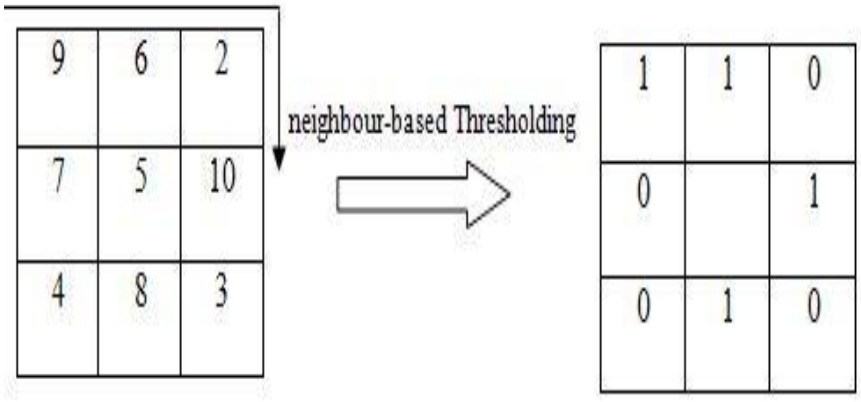
Neighbour-based LBP (NLBP) performs thresholding by comparing the pixel value of each neighbour of the central pixel with its next neighbour along the circular region. This is in contrast to the generic LBP which thresholds each neighbour by the central pixel. Neighbour-based LBP is defined as

$$NLBP_{R,P} = \sum_{p=0}^{P-1} s(g_p - g_{p+1}) . 2^p \quad (3)$$

$$s(g_p - g_{p+1}) = \begin{cases} 1 & g_p \geq g_{p+1} \\ 0 & g_p < g_{p+1} \end{cases} \quad (4)$$

where
g_p is grayscale 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.

The encoding process starts with topmost left neighbour and follows a clockwise direction. This is illustrated in figure 3 below. The generic LBP and the neighbour-based LBP generate different binary patterns from the same pixels.



Neighbour-based LBP code: 11010100

Figure 3. Neighbour-Based LBP Operator

Rotation Invariant Neighbour-based LBP is defined as

$$RNILBP_{R,P} = \sum_{p=0}^{P-1} s(g_p - g_{p+1}) \cdot 2^{mod(p-d,P)} \quad (5)$$

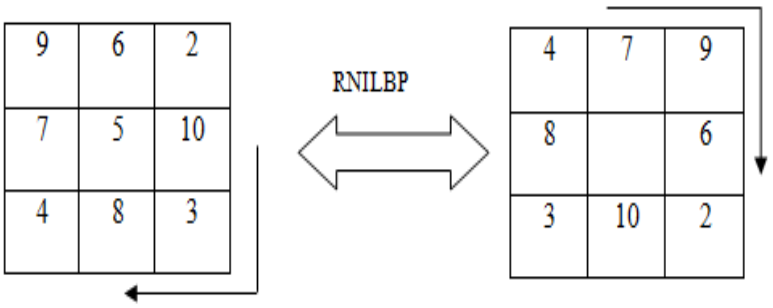
$$s(g_p - g_{p+1}) = \begin{cases} 1 & g_p \geq g_{p+1} \\ 0 & g_p < g_{p+1} \end{cases} \quad (6)$$

$$d = max|g_p - g_c| \quad (7)$$

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

where
g_c, g_p, g_n, 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.

Rotation invariance is achieved in Neighbour-based LBP scheme by starting the encoding process with the neighbour pixel which has the highest value. This ensures that there is a corresponding rotation of the extracted binary pattern whenever the image is rotated.



RNILBP code: 10100110 RINLBP code: 10100110

Figure 4. Rotation Invariant Neighbour-based LBP

The image in Figure 4 is rotated by through an angle of 90 degrees (90^0). But RINLBP obtained the same binary pattern from both the original image and the rotated image. This shows that image rotation does not affect the value of the binary pattern encoded by the

RINLBP operator. The face image is resized to 16×8 and RINLBP is applied to obtain a 1,024-bit binary representation of the face image.

2.5. Implementation

During enrolment, a random secret of 120 bits is generated using multiplicative congruential random number generation [9] method. This method is considered suitable for generating random numbers for cryptographic operations [10]. Error correction techniques are used address problems caused by noise and intra-class variation. Our concatenated error correction scheme integrates two error correction techniques, namely Reed-Solomon code [31] and Hadamard encoder [1]. Reed-Solomon error correction handles burst errors caused by noise from the camera shutter and occlusions when a subject wears an eye glass. Hadamard error correction addresses errors caused by natural intra-class variations in images of the same subject. A Reed-Solomon encoder takes in a set of k input blocks, and produces a set of n blocks as output. Each input and output block contains m bits. That is,

$$n - k = 2t, \tag{8}$$

where
k is the number of input blocks,
n is the number of output blocks,
t is the number of block errors that can be corrected.

Reed-Solomon encoder divides the 120-bit random secret into 20 blocks of 6 bits each. Next, it encodes the 20 blocks into 32 blocks, also of 6 bits each, which transforms the random secret into a 192-bit long value. Our encoder is able to correct 6 block errors. The output of Reed-Solomon encoder is passed to the Hadamard encoder. Our Hadamard encoder uses Reed-Muller [4] method. Each m-bit block (from Reed-Solomon encoder) is encoded into 2^{m-1} bits. Thus each 6-bit block output of the Reed-Solomon encoder is converted into a 32-bit block. We now have a total of 1,024 bits since each output block of the Reed-Solomon encoder contains 32 bits. This corrects up to $2^{m-3} - 1$ bit errors in each block. We are able to correct up to 7-bit errors in each 32 -bit block.

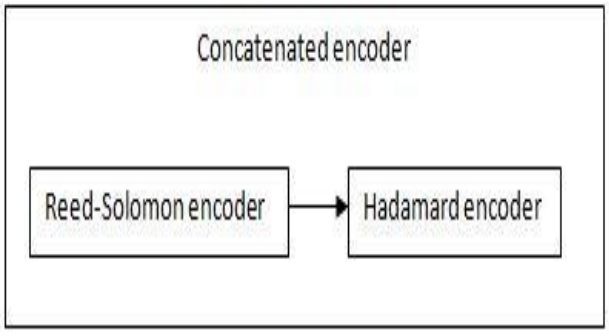


Figure 5. Concatenated Error Correction Encoding

Key binding is carried out by performing XOR operation on the output of the Hadamard encoder and the binary biometric data. This step computes a helper data, W from the secret, S and biometric data, X. That is, $S\ xor\ X = W$. We also compute the hash of S using SHA-256 hashing. NIST standards require hashing using a minimum of SHA-256 [32]. The helper data and the hash value of the secret are stored in the database. Authentication is performed by first extracting binary features from a probe biometric image, X'. An XOR operation is performed on the helper data, W (which is retrieved from

the database) and the binary value of the probe biometric data, X' to obtain a new secret,S'. That is, $W\ xor\ X' = S'$. The original length of S' is 1,024 bits. Error correction decoding is necessary before computing the hash value of the new secret because of the following reasons. Firstly, S' usually contains errors and hashing is very sensitive to bit errors. Secondly, the decoding process recovers a 120-bit value from the previously computed 1,024 bits. The same concatenated technique is applied, but in a reverse direction. Figure 6 illustrates the decoding process. After error correction, a hash of the 120-bit value, i.e. $hash(S')$ is computed. The new hash value is compared with the one stored in the database. A successful authentication requires an exact match between the two hash values.

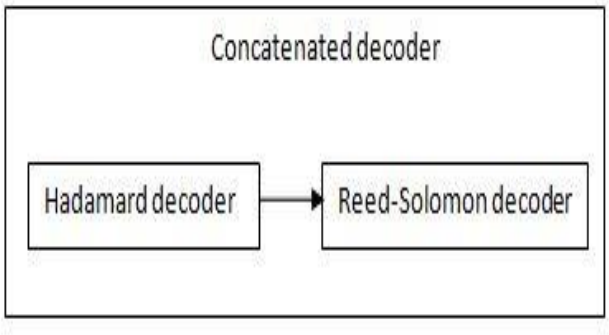


Figure 6. Concatenated Error Correction Decoding

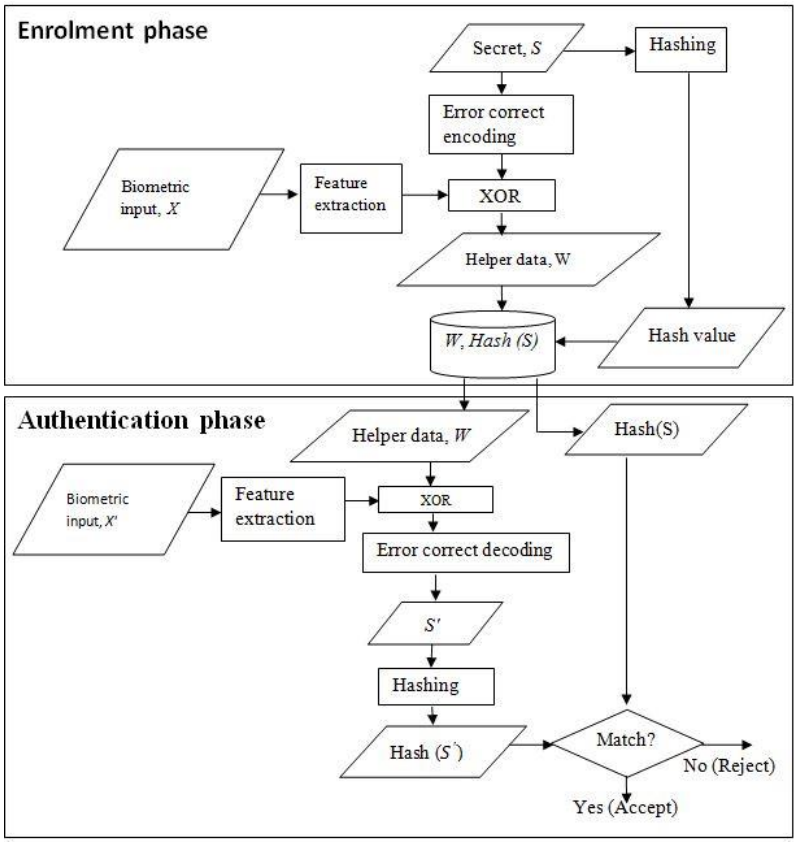


Figure 7. Framework of Modified Shielding Function

2.6. Performance Evaluation

Two criteria are used to access the performance of the proposed approach: false rejection rate (FRR) and false acceptance rate (FAR). False rejection rate measures the rate at which the system fails to authenticate legitimate users. False acceptance rate is the rate at which the system accepts impostors as legitimate users. The two parameters represent the degree of errors in the operation of the system. Our dataset consists of face images of 10 subjects from the CASIA near infrared database [25]. The database contains 20 samples per subject. The enrolment set consists of 16 images per subject while the verification set contains 4 images per subject. Verification is performed by carrying out a one-to-one comparison of the images in the enrolment set with those in the verification set. To compute false rejection, we compare each of the 4 images in the verification set with the 16 corresponding images in the enrolment set. Each attempt to compute FRR involves 64 comparisons; thus we have 640 comparisons for the 10 subjects. We calculate false rejection rate for each class based on the formula

$$FRR = \left({}^{no\ of\ false\ reject}/_{number\ of\ comparisons} \right) \times 100\ \% \tag{9}$$

Next, we calculate the total false rejection rate for all the classes and estimate the mean false rejection rate. The total FRR is 15.624% and mean FRR is 1.56%. Table 1 below shows the number of false rejection and the false rejection rate for each class.

Table 1. Computation of False Rejection Rate

Class	# Verification Attempts	False Reject	False Reject Rate (%)
0001	64	0	0
0002	64	0	0
0003	64	0	0
0004	64	0	0
0005	64	0	0
0006	64	0	0
0007	64	0	0
0008	64	9	14.062
0009	64	1	1.562
0010	64	0	0

False acceptance is calculated by carrying out a one-to-one matching between the enrolment set for each subject or class and the verification sets of the remaining 9 subjects (or classes). This involves a total of $9 * 64$ or 576 comparisons for each class and 5,760 comparisons for the 10 classes. We use the formula below to calculate the FAR for each class.

$$FAR = \left({}^{no\ of\ false\ accept}/_{number\ of\ comparisons} \right) \times 100\ \% \tag{10}$$

We also compute the total false acceptance rate for all the classes and the mean false acceptance rate. The values of total FAR and mean FAR obtained are 4.6874% and 0.47%, respectively. The number of false rejection and the false rejection rate for each class are shown in table 2 below.

Table 2. Computation of False Acceptance Rate

Class	# Verification Attempts	False Accept										False Accept Rate (%)
	9*64	0001	0002	0003	0004	0005	0006	0007	0008	0009	0010	
0001			0	0	0	0	1	0	0	0	0	0.1736
0002		0		0	0	0	1	0	0	0	0	0.1736
0003		0	1		0	0	0	0	0	0	0	0.1736
0004		0	0	0		0	3	0	0	0	0	0.5208
0005		0	0	0	0		0	0	0	0	0	0
0006		0	0	0	1	0		0	0	0	0	0.1736
0007		0	1	0	0	0	5		3	0	1	1.7361
0008		0	0	0	0	0	0	0		0	0	0
0009		0	0	0	0	0	0	0	0		0	0
0010		1	2	0	3	2	1	0	1	0		1.7361

2.7. Security Analysis

The security of the proposed approach is analyzed using four parameters, namely: key length, key space, entropy and probability of correct guess. The goal of the analysis is to determine the robustness of our system against cryptographic attacks such as guessing attacks and key exhaustion attacks.

Key length is defined as

$$\|K\| = m \times \left(\frac{dim}{2^{m-1}}\right) - 2t \tag{11}$$

where,
dim is the dimension of the biometric data,
m is the block size used for Reed-Solomon encoding,
t is the block error correction capability of the RS decoder.

Therefore, key length, $\|K\| = 6 \times \frac{1024}{2^{6-1}} - 2 * 6$
$= 120\ bits$

Key space is the set of all possible keys of a certain length. It is used to determine the possibility of a brute force attack against a cryptographic system.

$$\text{Key space, } k_s = 2^{\|K\|} \tag{12}$$
$$= 2^{120} = 1.329 \times 10^{36}$$

Entropy measures the degree of randomness of a biometric key. It is used to access the robustness of a key to random guessing attack. Entropy is measured in bits.

$$\text{Entropy, } H = \log_2 N^K \tag{13}$$
$$= K \log_2 N$$

where,
N is the symbol count (number of possible symbols),
K is the key length (number of symbols in the key),
$H = \log_2 2^{120}$
$= 120\ bits$

Probability of correct guess estimates the probability that an impostor will guess the key correctly. It is calculated by finding the inverse of the key length, *i.e.*,

$$P_{guess} = {}^{1}/_{K} \quad (14)$$

$$= {}^{1}/_{120} = 0.008$$

3. Results and Discussion

Results from experiments show FAR of 0.47% and FRR of 1.56%. Slight variations in performance may occur if low quality images are used (such as those obtained using natural wavelength camera). Image quality has significant impact on the recognition accuracy of biometric systems. The performance may also vary with the number of subjects or images in the test data. The security parameters are dependent on the dimension of the biometric feature. Increasing the feature length will lead to a corresponding increase in the security of the system. However, this will have a negative effect on the recognition accuracy because of the increase in the need for error correction. Table 3 shows a comparison between our approach and previous implementations of the shielding function.

Table 3. Comparison between our Approach and Previous Studies

Author	Modality	Feature Length (bits)	Error Correction Technique	Performance (%)			Security Analysis			
				FRR	FAR	EER	Key Length	Key Space	Entropy	Pr (correct guess)
Tuyls et al [45]	Fingerprint	512	BCH	0.054	0.0032	4.2	40	2^{40}	40	0.025
Huixian et al [13]	Fingerprint	512				2.33				
Kelkeboom et al [22]	Face	127	BCH	17.7	0.18	4.1	35	2^{35}	35	0.028
Lu et al [30]	Face		BCH	0.7941	0		36	2^{36}	36	0.027
Veen et al [46]	Face		BCH	3.5	0					
Our approach	Face	1,024	Concatenated coding	1.875	0.215		120	2^{120}	120	0.008

Our approach provides adequate security, but with a slightly lower recognition accuracy. A secure biometric cryptosystem should have a key length of at least 50 bits [46]. We are able to obtain a key length of 120 bits, which is higher than the minimum requirement for biometric keys. The size of the key ensures that our approach is less susceptible to guessing attack (Pr =0.008) and has the highest key space and entropy.

4. Conclusion

We have proposed and implemented a simplified, secure and privacy-preserving scheme for face biometric. Our scheme provides security for the biometric template and the randomly generated secret. It is difficult for an impostor to obtain either the secret key or the biometric data since they are not stored directly. Rather, a secret is bound with the biometric before it is stored in the database. Moreover, the secret is random (and difficult to guess) and only its hash value is saved in the database. In a future work, we will address the weaknesses of shielding functions such as the lack of resistance to spoofing attacks and susceptibility to record multiplicity attack.

References

[1] S. S. Agaian, "Hadamard Matrix and their Applications", Springer Berlin Heidelberg **(1985)**.
[2] M. Ao and S. Z. Li, "Near Infrared Face-based Biometric Key Binding", Advances in Biometrics, Edited M. Tistarelli and M. S. Nixon, Lecture Notes in Computer Science, Springer Berlin Heidelberg, vol. 5558, **(2009)**, pp. 376-385.
[3] T. Boult, "Robust Distance Measure for Face Recognition Supporting Revocable Biometric Tokens", Proceedings of 7th International Conference on Automatic Face and Gesture Recognition, Southampton, UK, **(2006)** April 10-12, pp. 560-566.
[4] B. Cooke, "Reed-Muller Error Correcting Codes", MIT Undergraduate Journal of Mathematics, **(2004)**, pp. 21-26.
[5] T. T. Dang, Q. C. Truong and T. K. Dang, "Practical Construction of Face-Based Authentication Systems with Template Protection using Secure Sketch", Information and Communication Technology, Edited K. Mustofa et al., Lecture Notes in Computer Science, Springer Berlin Heidelberg, vol. 7804, **(2013)**, pp. 121-130.
[6] N. P. Divyarajsinh and B. B. Mehda, "Face Recognition Methods and Applications", International Journal of Computer Technology and Applications, vol. 4, no. 1, **(2013)**, pp. 84-86.
[7] Y. Dodis, R. Ostrovsky, L. Reyzin and A. Smith, "Fuzzy extractors: How to Generate Strong keys from Biometrics and other Noisy Data", SIAM Journal of Computing, vol. 38, no. 1, **(2008)**, pp. 97-139.
[8] Y. C. Feng, P. C. Yuen and A. K. Jain, "A Hybrid Approach for Generating Secure and Discriminant Face Template", IEEE Trans. Information Forensics and Security, vol. 5, no. 1, **(2010)**, pp. 103-117.
[9] G. S. Fishman and L. R. Moore III, "An Exhaustive Analysis of Multiplicative Congruential Random Number Generators with Modulus", SIAM Journal of Science and Statistical Computing, vol. 7, no. 1, **(1986)**, pp. 24-45.
[10] G. S. Fishman, "Multiplicative Congruential Random Number Generators with Modulus 2^{β} : An Exhaustive Analysis for $\beta = 32$ and Partial Analysis for $\beta = 48$", Mathematics of Computation, vol. 54, no. 189, **(1990)**, pp. 331-334.
[11] M. Grassi and M. Faundez-Zanuy, "Protecting DCT Templates for a Face Verification System by means of Pseudo-random Permutations", Bio-inspired Systems: Computational and Ambient Intelligence, Edited J. Cabestany et al., Lecture Notes in Computer Science, Springer Berlin Heidelberg, vol. 5517, **(2009)**, pp. 1216-1223.
[12] I. Hamouchene and S. Aouat, "A Cognitive approach for Texture Analysis using Neighbour-based Binary Patterns", Proceedings of IEEE 13th International Conference on Cognitive Informatics and Cognitive Computing, Beijing, China, **(2014)** July 6-8.
[13] L. Huixian, W. Man, P. Liaojun and Z. Weidong, "Key Binding Based on Biometric Shielding Functions", 5th International Conference on Information Assurance and Security, Xi'an, China, **(2009)** August 18-20, pp. 19-22.
[14] A. K. Jain, K. Nandakumar and A. Nagar, "Biometric Template Security", EURASIP Journal of Advances in Signal Processing, Special Issue on Biometrics, **(2008)**, pp. 1-20.
[15] A. K. Jain, A. A. Ross and K. Nandakumar, "Introduction to Biometrics", Springer Science+Business Media, New York, **(2011)**.
[16] M. Y. Jeong and A. B. J. Teoh, "Cancellable Face Biometrics System by Combining Independent Component Analysis Coefficients", Computational Forensics, Edited H. Sako et al., Lecture Notes in Computer Science, Springer Berlin Heidelberg, vol. 6540, **(2011)**, pp. 78-87.
[17] B. H. Jing, P. P. K. Chan, W. W. W. Ng and D. S. Yeung, "Anti-spoofing System for RFID Access Control Combining with Face Recognition", Proceedings of the 9th International Conference on Machine Learning and Cybernetics, Qingdao, China, **(2010)** July 11-14.
[18] V. Joshi and P. Sanghavi, "Three Tier Data storage Security in Cloud Using Fuzzy Vault", International Conference on Computing, Communication and Applications, Dindigul, Tamilnadu, India, **(2012)** February 22-24.
[19] A. Juels and M. Sudan, "A Fuzzy Vault Scheme", Design Codes and Cryptography, vol. 38, **(2006)**.
[20] A. Juels and M. Wattenberg, "A Fuzzy Commitment Scheme", Proceedings of 6th ACM Conference on Computer Communications and Security, New York, **(1999)** November 01-04, pp. 28-36.
[21] T. Kanade, "Picture Processing System by Computer Complex and Recognition of Human Faces", PhD Thesis, Kyoto University, **(1973)**.
[22] E. J. C. Kelkeboom, B. Gokberk, T. A. M. Kevenaar and A. H. M. Akkermans, "3D Face: Biometric Template Protection for 3D Face Recognition", Advances in Biometrics, Edited S. W. Lee and S. Z. Li, Lecture Notes in Computer Science, Springer Berlin Heidelberg, vol. 4642, **(2007)**, pp. 566-573.
[23] A. Y. Kim and S. H. Lee, "Authentication Protocol using Fuzzy Eigenface Vault based on MoC", 9th International Conference Advanced Communication Technology, Gangwon-Do, South Korea, **(2007)** February 12-14.
[24] Y. Kim and K. Toh, 2007, "A Method to Enhance Face Biometric Security", Proceedings of IEEE 1st International Conference on Biometrics: Theory, Applications and Systems, Crystal City, VA, USA, **(2007)** September 27-29.

[25] S. Z. Li, R. F. Chu, S. C. Liao and L. Zhang, "Illumination Invariant Face Recognition Using Near-infrared Images", IEEE Transactions on Pattern Analysis and Machine Intelligence (Special issue on Biometrics: Progress and Directions), vol. 29, no. 4, **(2007)**, pp. 627-639.
[26] S. Z. Li and A. K. Jain, "Handbook of Face Recognition", Second Edition, Springer-Verlag Limited, London, **(2011)**.
[27] P. Liao, Y. Wang, M. Wang, S. Ding and H. Ma, "An Effective Preprocessing Scheme for Face Recognition based on Local Gabor Binary pattern Histogram Sequence", IEEE International Conference on Computer Science and Automation Engineering, Zhangjiajie, China, **(2012)** May 25-27, pp. 581-585.
[28] C. Z. Liew, R. Shaw, L. Li and Y. Yang, "Survey on Biometric Data Security and Chaotic Encryption Strategy with Bernoulli Mapping", Proceedings of International Conference on Medical Biometrics, Shenzhen, China, **(2014)** May 30-June 1, pp. 174-180.
[29] J. P. Linnartz and P. Tuyls, "New Shielding Functions to Enhance Privacy and Prevent Misuse of Biometric Templates", 4th International Conference on Audio- and Video- Based Person Authentication, Guildford, UK, **(2003)** June 9-11, pp. 393-402.
[30] H. Lu, K. Martin, F. Bui, K. N. Plataniotis and D. Hatzinakos, "Face Recognition with Biometric Encryption for Privacy Enhancing Self Exclusion", 16th International Conference on Digital and Signal Processing, Santorini-Hellas, Greece, **(2009)** July 5-7.
[31] F. J. MacWilliams and N. J. A. Sloane, "The Theory of Error-Correcting Codes", North Holland Publishers, Amsterdam, **(1991)**.
[32] NIST, "NIST's policy on hash functions", http://csrc.nist.gov/groups/ST/hash/policy.html (Accessed on June 10, 2015).
[33] D. H. Nyang and K. Lee, "Fuzzy Vault: How to Implement Fuzzy Vault with Weighted Features", Universal Access in Human Interaction: Coping with Diversity, Edited C. Stephanotis, Lecture Notes in Computer Science, Springer Berlin Heidelberg, vol. 4554, **(2007)**, pp. 491-496.
[34] T. Ojala, M. Pietikainen and T. Maenpaa, "Multiresolution Gray-Scale and Rotation Invariant Texture Classification with Local Binary Patterns", IEEE Transaction on Pattern Analysis and Machine Intelligence, vol. 24, no. 7, **(2002)**, pp. 971-987.
[35] S. K. Panigrahy and D. Jena, "On the Privacy of Biometric Traits: Palmprint, Face and Signature", Contemporary Computing, Edited S. Ranka et al., Communications in Computer and Information Science, Springer Berlin Heidelberg, vol. 40, **(2009)**, 182-193.
[36] M. Pudzs, R. Fuksis, R. Ruskuls, T. Eglitis, A. Arturs Kadikis and M. Greitans, "Fgpa-based Palmprint and Palm Vein Biometric Systems", International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, Germany, **(2013)** September 5-6.
[37] J. Qui, Y. Zhang and J. Sun, "Face Recognition in Open World Environment", Visual Communications and Image Processing, Kuching, Malaysia, **(2013)** November 17-20.
[38] N. K. Ratha, J. H. Connell and R. M. Bolle, "Enhancing Security and Privacy in Biometrics-based Authentication Systems", IBM Systems Journal, vol. 40, no. 3, **(2001)**, pp. 614-634.
[39] C. Rathgeb, A. Uhl and P. Wild, "Iris-biometrics: from Segmentation to Template Security", Advances in Information Security, Edited S. Jajodia, Springer, New York, **(2013)**.
[40] M. Savvides, B. Kumar and P. Khosta, "Cancelable Biometric Filters for Face Recognition", Proceedings of 17th International Conference on Pattern Recognition, Cambridge, UK, vol. 3, **(2004)** August 23-26, pp. 922-925.
[41] Y. Sutcu, Q. Li and N. Memon, "Protecting Biometric Templates with Sketch: Theory and Practice", IEEE Transactions on Information Forensics and Security, vol. 2, no. 3, **(2007)**, pp. 1825-1840.
[42] Y. Sutcu, H. T. Sencar and N. Memon, "A Secure Biometric Authentication Scheme based on Robust Biohashing", Proceeding of the 7th Workshop on Multimedia and Security, New York, NY, USA, **(2005)** August 01-02, pp. 111-116.
[43] A. B. J. Teoh and D. C. L. Ngo, "Biophasor: Token Supplemented Cancelable Biometrics", Proceedings of International Conference on Control, Automation, Robotics and Vision, Singapore, **(2006)** December 5-6.
[44] A. B. J. Teoh and C. T. Yuang, "Cancelable Biometrics Realization with Multispace Random Projections", IEEE Transactions on System, Man and Cybernetics, Part B, vol. 37, no. 5, **(2007)**, pp. 1096-1106.
[45] P. Tuyls, A. H. M. Akkermans, T. A. M. Kavenaar, G. J. Schrijen, A. M. Bazen and R. N. J. Veldhuis, "Practical Biometric Authentication with Template Protection", Audio-and Video-Based Biometric Person Authentication, Edited T' Kanade et al., Lecture Notes in Computer Science, Springer Berlin Heidelberg, vol. 3546, **(2005)**, pp. 436-446.
[46] M. V. D Veen, T. Kavenaar, G. J. Schrijen, T. A. H. Akkermans and F. Zuo, "Face Biometrics with Renewable Templates", Security, Steganography, and Watermarking of Multimedia Contents VIII, Edited E.J. Delp III and P.W. Wong, Proceedings of SPIE, vol. 6072, **(2006)**, pp. 1-12.
[47] T. T. L. Vo, T. K. Dang and J. Kung, "A Hash-based Index Method for Securing Biometric Fuzzy Vaults", Trust, Privacy and Security in Digital Business", Edited C. Eckert et al., Lecture Notes in Computer Science, Springer Berlin Heidelberg, vol. 8647, **(2014)**, pp. 60-71.

[48] Q. Wang, W. Huang, X. Niu and X. Jiang, "A Statistical Feature-based Scheme for the Template Protection of 2D face Recognition", International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Harbin, China, **(2008)** August 15-17.
[49] Y. Wang and K. N. Plataniotis, "Fuzzy Vault for face based Cryptographic Key Generation", 2007 Biometrics Symposium, Baltimore, Maryland, USA, **(2007)** September 11-13.
[50] L. Wu and S. Yuan, "A Face Based Fuzzy Vault Scheme for secure Online Authentication", 2010 International Symposium on Data, Privacy and E-Commerce, Buffalo, NY, USA, **(2010)** September 13-14.
[51] M. Yasuda, T. Shimoyama and J. Kogure, "Packed Homomorphic Encryption Based on Ideal Lattices and its Applications in Biometrics", Security Engineering and Intelligent Informatics, Lecture Notes in Computer Science, Springer Berlin Heidelberg, vol. 8128, **(2013)**, pp. 55-74.
[52] E. J. Yoon and K. E. Yoo, "A Biometric based Authenticated Key Agreement Scheme using ECC for Wireless Sensor Networks", Proceedings of Symposium on Applied Computing, Gyeongju, Korea, **(2014)** March 24-28, pp. 699-705.
[53] H. Zhao, J. Qin and J. Hu, "An Energy Efficient Key Management Scheme for Body Sensor Networks", IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 11, **(2013)**, pp. 2202-2210.

Authors

Abayomi Jegede, received his Bachelor and Master's degrees in Computer Science from the University of Ibadan, Nigeria. He is currently a PhD student in the Faculty of Computer Science and Information Technology, Universiti Putra Malaysia.

Nur Izura Udzir is an associate professor at the Faculty of Computer Science and Information Technology, Universiti Putra Malaysia (UPM) since 1998. She received her Bachelor of Computer Science (1995) and Master of Science (1998) from UPM, and her PhD in Computer Science from the University of York, UK (2006). She is a member of IEEE Computer Society and a Committee Member of Information Security Professionals Association of Malaysia (ISPA.my). Her areas of specialization are access control, secure operating systems, intrusion detection systems, coordination models and languages, and distributed systems. She is currently the Head of Department of Computer Science and a member of the Information Security Group (which she led in 2008-2013) at the faculty.

Azizol Abdullah is a senior lecturer at the Faculty of Computer Science and Information Technology, Universiti Putra Malaysia.

Ramlan Mahmod is a professor at the Faculty of Computer Science and Information Technology, Universiti Putra Malaysia.

