Computers, Materials & Continua
DOI:10.32604/cmc.2021.014418
Article

Tech Science Press

ExpressionHash: Securing Telecare Medical Information Systems Using BioHashing

Ayesha Riaz[1], Naveed Riaz[1], Awais Mahmood[2,*], Sajid Ali Khan[3], Imran Mahmood[1], Omar Almutiry[2] and Habib Dhahri[2]

[1]SEECS, National University of Science and Technology, Islamabad, Pakistan
[2]College of Applied Computer Science, King Saud University (Almuzahmiyah Campus) Riyadh, Saudi Arabia
[3]Department of Software Engineering, Foundation University Islamabad, Pakistan
[*]Corresponding Author: Awais Mahmood. Email: mawais@ksu.edu.sa
Received: 19 September 2020; Accepted: 06 December 2020

Abstract: The COVID-19 outbreak and its medical distancing phenomenon have effectively turned the global healthcare challenge into an opportunity for Telecare Medical Information Systems. Such systems employ the latest mobile and digital technologies and provide several advantages like minimal physical contact between patient and healthcare provider, easy mobility, easy access, consistent patient engagement, and cost-effectiveness. Any leakage or unauthorized access to users' medical data can have serious consequences for any medical information system. The majority of such systems thus rely on biometrics for authenticated access but biometric systems are also prone to a variety of attacks like spoofing, replay, Masquerade, and stealing of stored templates. In this article, we propose a new cancelable biometric approach which has tentatively been named as "Expression Hash" for Telecare Medical Information Systems. The idea is to hash the expression templates with a set of pseudo-random keys which would provide a unique code (expression hash). This code can then be serving as a template for verification. Different expressions would result in different sets of expression hash codes, which could be used in different applications and for different roles of each individual. The templates are stored on the server-side and the processing is also performed on the server-side. The proposed technique is a multi-factor authentication system and provides advantages like enhanced privacy and security without the need for multiple biometric devices. In the case of compromise, the existing code can be revoked and can be directly replaced by a new set of expression hash code. The well-known JAFFE (The Japanese Female Facial Expression) dataset has been for empirical testing and the results advocate for the efficacy of the proposed approach.

Keywords: Biometrics; TMIS; biohashing; multifactor authentication; medical information system

1 Introduction

Image based biometric systems have garnered considerable attention from researchers in the past two decades due to their innumerous application areas. However, such systems are susceptible to various kinds of attacks that can effectively undermine the integrity of the whole process. Biometrics provide promising solutions to the problems incurred during the usage of other means of authentications like passwords, PIN numbers, smart cards etc. [1]. However, biometric traits associated to the user are permanent in nature which results in the problems of diversity and revocability when the template database is breached or compromised [2]. Here, comes the concept of biometric template security. Over the years, many hardware and software-based solutions have been proposed. Hardware solution include smart cards, match on card or card-on-system for protection of biometric template data. All the modules and interfaces of the system are present in the card in the card-on-system; the major advantage in such systems is that the sensitive information remains on card and never leaves it. However, these systems are costly to implement on large scale and the user has to carry and safeguard the card all the time for valid accessibility but the card might get lost or stolen.

Software solution involves combining the biometric templates with a key or system generated random numbers such that the stored templates expose little or no information regarding the original templates. Software based biometric template protection techniques can be further classified into different categories like feature transformation schemes, cryptosystems, and biometric cryptosystems.

Cryptosystems [3,4] are made up of two processes; encryption and decryption. Both, symmetric and asymmetric cryptographic techniques like TDEA, AES, and RSA [5–7] can be used for biometric template security. However, while using classical cryptographic techniques the original template is exposed each time during the authentication phase and unbreakable cryptosystems are still facing the problem of management of key and size of the key.

Biometric Cryptosystems or Helper Data based schemes can be further classified as being either key binding model or key generation model schemes. In the former scheme, the biometric template obtained from the sensor is bound with a unique key at authentication time and helper data is generated. The correct unique code is reconstructed with the helper data and the query biometric instance for legitimate access. Key binding models include fuzzy commitment proposed by Juels et al. [8], and fuzzy vault methods by Juels et al. [9]. Error correcting codes are employed for tolerating Intra-user variability in the system. However, the use of these error correcting codes for the retrieval of keys inhibits the use of highly sophisticated matchers decreasing the overall performance of the system. Key binding models do not provide diversity and revocability or cancelability as helper data is designed cautiously to cater for intra-user variations. In key generation models, a unique key and helper data is generated from the biometric template at the time of authentication and helper data storage is unnecessary. On authentication, helper data and query biometric instance is used to retrieve the generated unique key for accessibility. Key generation model is based on secure sketches- fuzzy extractor method proposed by Chen et al. [10]. Direct generation of keys from biometric templates is tempting and is valuable in various cryptographic applications but generating keys with high stability and high entropy is not an easy task.

In feature transformation scheme, the user provides its biometric traits to the system at sensor. The received biometric template is processed into a biometric feature vector. The generated biometric feature vector is then passed through a transformation function triggered by some

external information defined by the user itself or the processing system. The transformed template is then recorded in the central database for authentication purpose. In the verification stage, the user provides his/her query template for verification, which is then processed and transformed using the same functions and parameters. This query transformed template is then matched with the template that was stored earlier in the database. In case the matching score is above the predefined threshold, successful authentication is carried out. Feature transformation schemes can be further classified as either non-invertible or invertible feature transformation schemes.

As the name suggests, the non-invertible scheme employ transformation functions that are non-invertible like the one-way functions. In such schemes, it is computationally hard to recover the original template of a user even if the key and the transformed template are known. Diverse transformed templates for various platforms can be obtained using different keys. The compromised template can be revoked and updated as multiple templates can be obtained using same biometric trait. However, it is not trivial to develop a transformation function which incorporates not only non-invertibility but also discrimination factor. It is a general consensus among researchers in this domain that the transformed templates should have large variations for different users (inter-user variability) as presented by the un-transformed templates. Yagiz et al. [11] presented a non-invertible transformation model for face images. Rathgeb et al. [12,13] proposed three non-invertible transformation schemes; polar, folding and Cartesian to generate secure transformed fingerprint templates. Jinyu et al. [14] demonstrated diverse algorithms for creating cancellable iris biometrics. Hammerle-Uhl et al. [15] applied classical algorithms to create non-invertible templates for iris biometrics.

The invertible schemes employ invertible functions for the transformation of templates. Biometric Salting or Biohashing is used as invertible transformation model. User defined random key addition results in low false acceptance ratio. Multiple transformed templates can be obtained using same biometric feature with various keys. It is easier to revoke and update a compromised template by using different random keys. However, Original template can be compromised if the random key is compromised as function used is invertible in nature. Such systems suffer from performance bottleneck as the query template is first transformed and then matched. Teoh et al. [16,17] anticipated biohashing method for face biometrics. Biohashing scheme is implemented to numerous biometrics like iris biometrics [18,19], fingerprints in [3] and palmprints [4]. The use of hashes generated after biohashing in key-binding models is proposed in [20]. Kong et al. [21] proposed the face hashing scheme and they have argued that using unique tokenized random numbers can lead to zero error rate. Teoh et al. [22] suggested that multi stage random projection can resolve the stolen token issue. Various improvements of the biohashing scheme are presented by Lumini et al. [23,24].

We have extensively discussed these different biometric template security techniques in [2]. The technique proposed in this work is an invertible biohashing scheme. Although, the concept of using expressions as authenticators is not new [25], to the best of our knowledge, it is the first time that an effective mechanism for biohashing of expressions has been proposed. The proposed technique has many advantages like

- Increased Security:- The technique involves authentication of face followed by expression authentication thus effectively providing the security advantage of multi-biometrics without adding the intrinsic complexities of such systems.
- Single Biometric Device:- Although the system effectively becomes a multi-biometric system but only single biometric capturing device is needed as a single image contains both the

facial information and expression information at the same time. This also simplifies the feature extraction, comparison, and decision modules.

- Spoofing Resistance:- General Face Recognition systems are vulnerable to a variety of spoofing attacks. However, our proposed scheme takes into account not only the face recognition but also expression recognition. Unlike face, which is unique, a variety of expression are available to the user for enrollment and authentication which decreases the likelihood of spoofing attacks. A user would also be able to use different expression for different biometric systems which would provide added security in case one of the system or template is compromised.
- Easy Revocability:- Still, if a biometric system or template is compromised, it would be very easy to cancel the previous template/s and generate another one using the proposed technique.
- Better Accuracy:- The results presented in Section 7 indicate that the proposed technique also improves the accuracy rate. The reason being that although an expression can be considered as an additional feature of a face, there is still a degree of independence between these two biometric traits. Furthermore, the fusion of identity information of user further improves the authentication.

There are two major sub-components of our proposed technique; Facial expression recognition, and respective biohash generation component. In Section 2, we enumerate the details of facial expression feature vector extraction process. In Section 3, we provide the steps for the generation of biohash employing the obtained expression feature vector. In Section 4, we delineate the Authentication process. Section 5 highlights the associated performance measures and the details about the experimental setup are provided in Section 6. The empirical results are provided in Section 7, and we conclude with Section 8.

2 Expressions for Authentication

As the usage of biometrics for authentication is on the rise; expression recognition in conjunction with face recognition is becoming a popular scheme [25].

In our proposed methodology, expressions are extracted using a framework proposed by Khan et al. [26]. It is basically a novel descriptor that employs some existing techniques like LBP (Local Binary Pattern), WLD (Weber Local Descriptor) and DCT (Discrete Cosine Transform) in effective manner. It is called WLBI-CT (Weber Local Binary Image Cosine Transform). Local level details are obtained using block LBP and robustness against real time variations is covered by WLD transform. Information about dominant orientation and spatial layout textures is present in Weber local binary image. Local representation information is obtained by using the orientation components in horizontal as well as vertical directions. To enhance the local representation blocks are used for binary image is division.

However, classification performance is degraded using LBP and WLD techniques because of the redundant features. Images are transformed in frequency domain to boost the discriminative power of the descriptor. DCT (discrete cosine transform) features are investigated by Dabbaghchian et al. [27] where high variance features are extracted by DCT in zigzag manner. After the application of DCT, middle features hold high recognition strength, so upper left corner and middle features are used.

Hence, classification performance is increased using relatively lesser features than the previously used state of art procedures. Block division is used for LBP images preserving texture information and exhibiting more discriminating power.

Following are the steps to calculate the feature vectors from an image.

- Image preprocessing
- Conversion to LBP orientation image
- Conversion to WLD orientation image
- Feature extraction using DCT in zigzag manner generate final feature vector

These steps are depicted in Fig. 1.

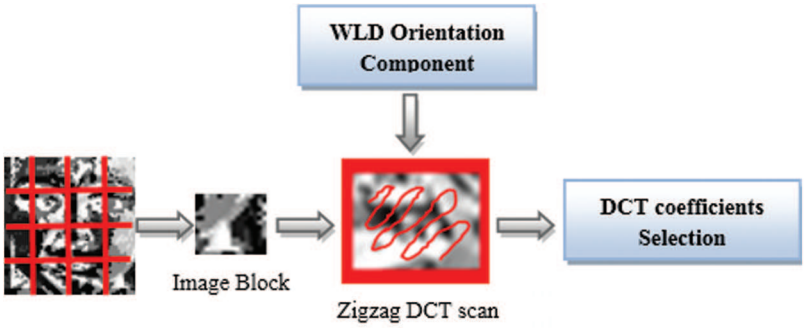

Figure 1: Steps to calculate feature vectors [26]

2.1 Image Preprocessing

Image preprocessing means training or preparing image for the algorithm application [28]. Face is detected from the image to locate the face region using face object detection algorithm. For the extraction of facial portion we have used most popular, robust and efficient algorithm developed by Viola et al. [29]. This algorithm works in real time and uses Haar-like features by utilizing image into smaller rectangular regions. It is based on the concept that all human faces have similar characteristics.

After face detection, the face region is cropped to get only the required portion of the image. To normalize the illumination effects on the image histogram equalization operation is applied.

2.2 Conversion to LBP Orientation Image

The normalized image is then converted to local binary image for texture classification. Ojala et al. [30] introduced LBP (Local binary pattern) which outperforms the other similar techniques in different applications [31,32]. Ahonen et al. [31] have advocated for the use of LBP in their research work. Silva et al. [33] conducted a survey on the improvements of the LBP.

To extract features with LBP image the image is first divided into N regions or blocks. Each cell contains equal pixels of the image. In each cell or block, each pixel is compared to its neighboring pixels in a circular manner i.e., clockwise or anti-clockwise. The value of central pixel is considered threshold value in each comparison. Values above the threshold value are one and below it is zero. Hence, an eight binary number is produced reading it in invariant manner which is often converted into decimal for convenience.

In the next step, for each pixel, extensions are made in the neighborhood size uniformly and rotation invariantly [32]. LBP operator is defined by following equation:

$$LBP_{X,R} = \sum_{i=1}^{X-1} 2^i S(X_i - X_c)$$

where, X is the total number of neighboring pixels, R is the radius and Xc is the central pixel.

The binary code is obtained using the following equation:

$$S(X_i - X_c) = \begin{cases} 1 & X_i - X_c \geq 0 \\ 0 & X_i - X_c < 0 \end{cases}$$

Uniformity, rotation invariance i.e., clockwise or anticlockwise and circular neighborhood is the parameters used in LBP [32]. Histogram of the computed values over the block is calculated showing the combinations of which pixel values are greater or smaller than the central pixel value. For a 3×3 neighborhood, eight binary numbers, $28 = 256$ dimensional histogram is obtained. The histogram of 256 LBP code is used for local texture features description of expression images. These steps are depicted in Fig. 2.

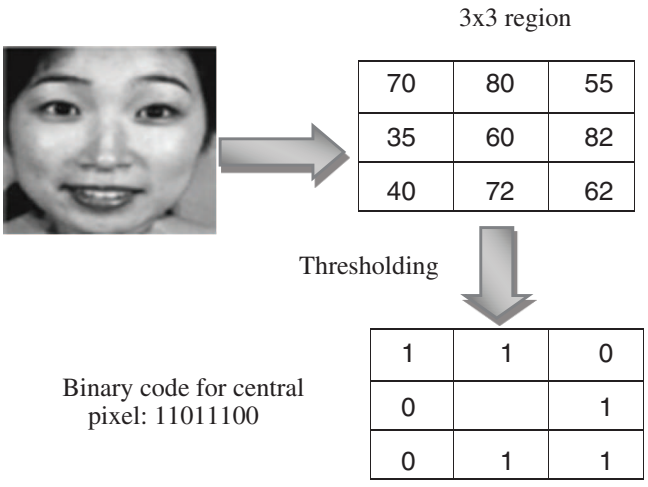

Figure 2: Binary value calculation for LBP image

2.3 Conversion to WLD Orientation Image

Chen et al. [34] developed WLD (Weber local descriptor) for capturing texture information exploiting the pixel intensity change ratio. There are two major components of WLD: differential excitation and orientation. Differential excitation $\varepsilon(p_c)$ is the ratio of relative intensity difference to the neighboring pixels and current pixel intensity. The differential excitation is given by:

$$\varepsilon(p_c) = \arctan\left[\sum_{i=0}^{x-1}\left(\frac{p_i - p_c}{p_c}\right)\right]$$

where, x denotes the neighbors and p_i is the ith neighbor of the p_c. The results are smoothed out using the arctan function. Differential excitation component captures the local patterns; high value indicates a spot or edge.

Here $\Theta\ (p_c)$ is the gradient orientation of the current pixel which represents the orientation component of WLD. Following equation is used for gradient orientation computation [35].

$$\Theta\ (p_c) = \arctan\left(\frac{p_7 - p_3}{p_5 - p_1}\right)$$

where, p_c is represented by p_1, p_3, p_5, p_7 as shown in Fig. 3. Information is lost when differential excitation is calculated by averaging in an interval. To, tackle this issue, LBP excitation component and WLD orientation component are combined by Khan et al. [26].

P_0	P_1	P_2
P_7	P_c	P_3
P_6	P_5	P_4

Figure 3: WLD based feature extraction neighborhood pixel arrangement

2.4 Feature Extraction Using DCT in Zigzag Manner

Discrete cosine transform is a popular transformation function for signal and image processing [36]. DCT (discrete cosine transform) and DFT (discrete Fourier transform) [37] are extensively used in expression recognition [38]. DCT is employed for transforming an image into frequency domain where maximum information is stored in low frequencies hence providing strong energy compaction and high computational efficiency. The highly variant components of the transformed DCT image are present in the top left corner of the image. Frequency domain methodologies are different from PCA and LDA as these are data independent and in comparison to spatial domain LBP, provide better analysis. The DCT transformation equation for N×M image is given by;

$$F\ (u,v) = \alpha_u.\alpha_v.\sum_{x=0}^{N-1}\sum_{y=0}^{M-1}\left[cos\left(\frac{\Pi u}{2N}\ (2x+1)\right).cos\left(\frac{\Pi v}{2M}\ (2y+1)\right).f\ (x,y)\right]$$

Here, f(x,y) represents the pixel intensity of xth row and yth column $u = 0, 1, \ldots, N-1$, $v = 0, 1, \ldots, M-1$

$$\alpha_u = \begin{cases} \sqrt{\frac{1}{N}} & for\ u = 0 \\ \sqrt{\frac{2}{N}} & for\ u \geq 0 \end{cases} \quad \alpha_v = \begin{cases} \sqrt{\frac{1}{M}} & for\ v = 0 \\ \sqrt{\frac{2}{M}} & for\ v \geq 0 \end{cases}$$

The highlight of DCT transformation is that it converts useful information into fewer coefficients with no decrease in recognition accuracy and increase in computational efficiency.

DCT transformation is applied to the WLD operated image wholly. For LBP, block division is applied to the image and DCT is applied for each block of LBP image.

2.5 Generate Final Feature Vector

DCT filters out the important information by image compression. The feature vectors generated by the zig zag scan of the image are selected on the basis high variance reducing the training time for classification as compared to the feature selection algorithms like GA (genetic algorithm) and PSO (particle swam optimization). Hence, the process proposed is computationally inexpensive.

3 Expression Hashing

Biohashing is an invertible feature transformation technique. Biometric sensors are one of the most essential part of any biometric system and their job is to capture the biometric traits of the user and then glean the requisite biometric information in the form of a feature vector or biometric template. This template is then transformed using a random key given to the user by the system at the time of enrollment. A set of orthonormal vectors are created using this random key. The dot product or the inner product of the feature vector and the orthonormal vectors is calculated. Finally, a predefined threshold is applied to all the product outputs and a Biohash is calculated. Following are the steps for biometric hashing:

- Generate a set of random numbers based on the token (seed) provided by the user.
- Apply the Gram-Schmidt process on the random numbers generated in the first step.
- Compute the dot product of the feature vector and the orthonormal vectors
- Apply a preset threshold to generate a string of 0's and 1's called the biometric hash or the biohash.

These steps are depicted in Fig. 4.

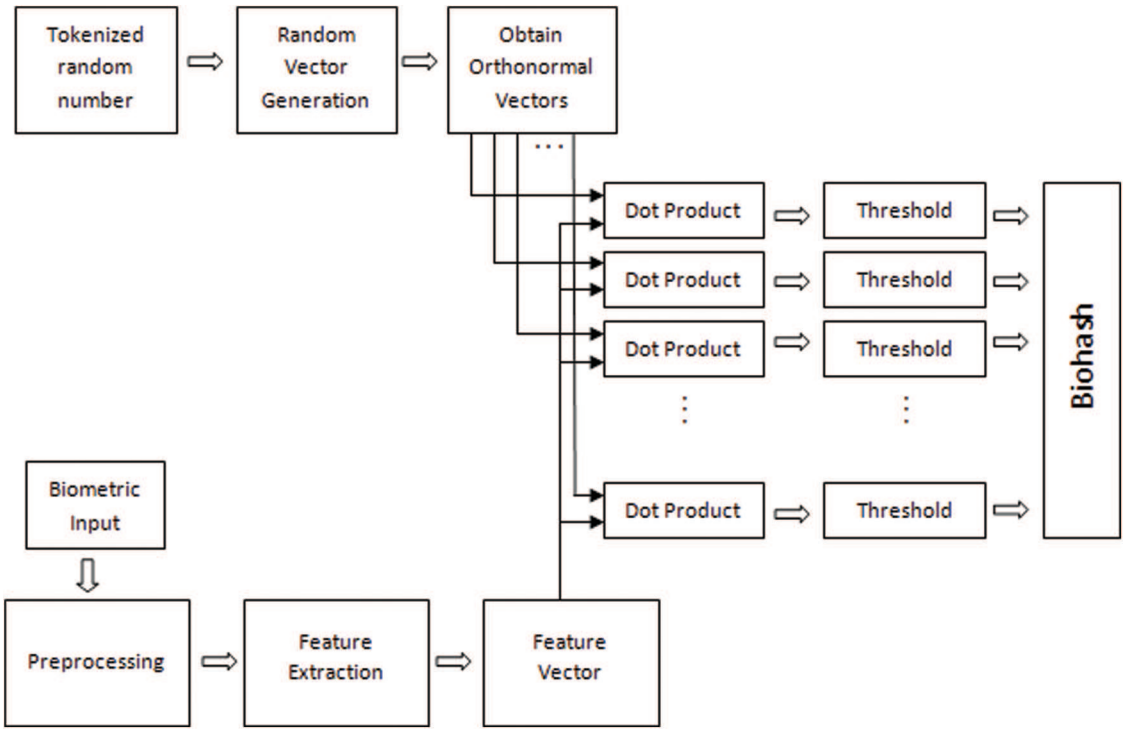

Figure 4: Steps of Biohashing process

3.1 Generate Random Number

Random numbers are a string of unpredictable numbers which are independent of predictable events but are based on natural random phenomenon. However, producing random numbers based on naturally occurring phenomenon is long, tiresome, expensive and non-repeatable. Thus, for daily applications pseudorandom numbers are used instead of real random numbers so the results produced can also replicable.

Blum et al. [39] proposed a cryptographically secure pseudo random generator which efficiently produces long well distributed sequences with small seed values. The pseudo random generator is based on computationally hard quadratic residuosity problem and it can be defined as a decision problem as: Given integers x and N, is x a quadratic modulo N? [40].

Generate two large prime numbers p and q that are congruent to 3 mod 4, $p \equiv q \equiv 3 mod 4$. It is important to select such numbers as it guarantees that each quadratic residue has a square root which is itself a quadratic residue. Then N is a multiple of p and q i.e., N=p.q. The seed s is chosen from the set [1, N-1] such that p and q are not factors of s i.e., s is co-prime to N. Thus

$$x_0 = s^2 \, mod \, N$$

$$x_i = x_{i-1}^2 \, mod \, N$$

3.2 Generate Orthonormal Vectors

The generated set of random numbers is converted into a set of orthonormal vectors. Orthonormal vectors are linearly independent, normalized and orthogonal in nature. The number of orthonormal vectors is equal to the number of feature vectors extracted. The set of random numbers is orthonormalized using Gram-Schmidt process.

3.3 Calculate Inner Product

Inner product is calculated so that the token based supplementary information can be added in the feature vector. The inner or dot product of the extracted feature vector and the orthonormalized random vectors is calculated to get scalar terms which are equal to the number of feature vectors.

3.4 Threshold

Threshold is the value or magnitude which creates a border line between two quantities. In our methodology threshold defines if the value is zero or one in the output, below threshold value, value is zero and above threshold value is one. Let $X = \begin{bmatrix} a_{11} \cdots a_{1n} \\ \vdots \ \ddots \ \vdots \\ a_{m1} \cdots a_{mn} \end{bmatrix}$ be a matrix of order $m \times n$then threshold is determined by calculating the mean$M$of all the values in the matrix. $M = \frac{\sum_{j=1}^{n} \sum_{i=1}^{m} a_{ij}}{m \times n}$ and the values above M are marked as one while values below$M$ are marked as zero.

3.5 Final Expression Hash

The output of the thresholding in the form of 0's and1's is called the expression hash. The expression hash is a combination of expression feature vector and the supplementary token

information in the form of random number vectors. This transformed biometric template is recorded in the database against its user's identity.

4 Authentication Process

The process of determining whether the claimed identity is true or not is called the Authentication process. There are two stages of this process namely enrollment and authentication. During enrollment, the users provide their identity and some unique authenticator which is stored in the database. In authentication phase, the claimant provides its identity and the related authenticator which is matched with the stored ones. Decision is made if the claimant is true or not. Following sections explain the proposed authentication process.

4.1 Enrollment Phase

The proposed enrollment phase is divided into following steps. First, the user provides his username as fist name and last name, and its biometric trait in the form of its facial expression. Then, the modifier converts the username into user ID, a token number is generated on the basis of user ID. Both user ID and the token number are provided to the user and user ID is stored in the database.

The biometric template is extracted in the form of feature vector from the biometric trait obtained from the sensor using the expression feature extraction method mentioned above. The token number generated based on user ID and the extracted feature vector are then biohashed to generate expression hash. The generated expression hash is then stored in the database next to where the user ID is stored. Fig. 5 provides the overview of this process.

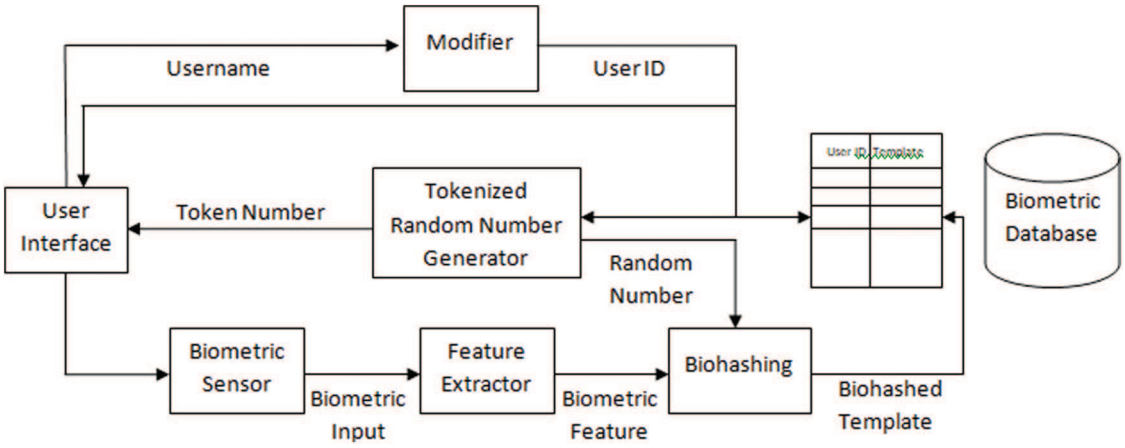

Figure 5: Enrollment phase

4.2 Authentication Phase

In the proposed authentication phase these subsequent steps are followed. The user provides its user ID, token number and biometric trait. Expression feature vector is extracted from the obtained biometric trait. This feature vector is then transformed to expression hash using the provided token number.

The matcher compares the expression hash stored against the given user ID and the newly created expression hash from the give biometric instance and outputs a match score. In the decision module, it is checked if whether the matching score is above the predefined threshold or not. If the match score is above the threshold, then access is granted else it is denied. Threshold is normally chosen using the error curves and in our experimentation settings, we have considered the point where both false acceptance rate and false rejection rate is equal i.e., equal error rate. These concepts are further elaborated in Section 5 and 6. The different stages of the Authentication phase are depicted in Fig. 6.

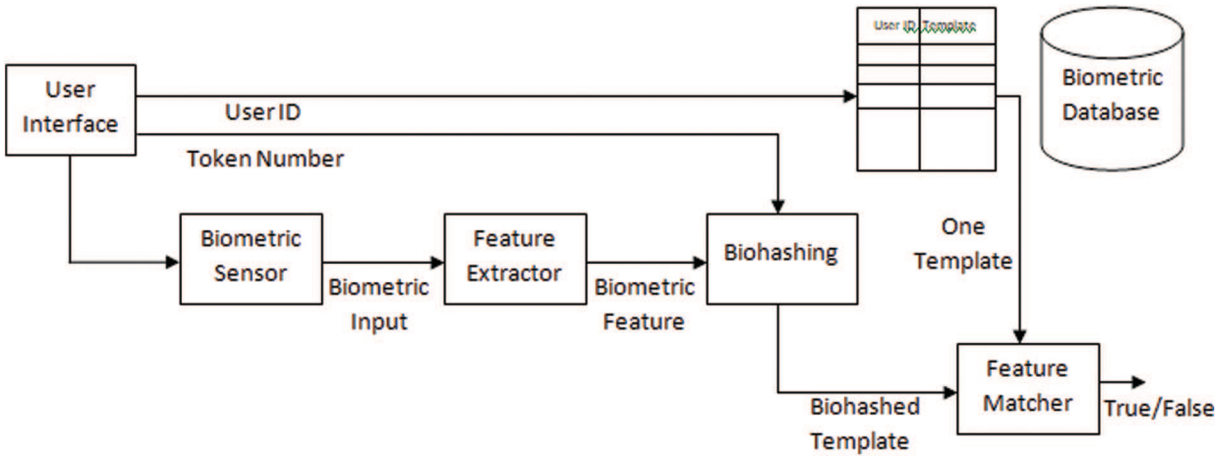

Figure 6: Authentication phase

5 Performance Measures

The results of the designed biometric authentication system are analyzed using these performance measures; FAR (False Acceptance Rate), FRR (False Rejection Rate), ERR (Equal Error Rate), ROC (Receiver Operating Characteristic) Curve and optimum threshold T_o.

Let M be the match score and T_M be be the pre-defined threshold level then decision for a query for a claimed identity I with the expression hash E_q will be;

$$(I, E_q) \in \begin{cases} granted, & if \ M(E_q, E_I) \geq T_M \\ denied, & if \ M(E_q, E_I) < T_M \end{cases}$$

Ideally, the match score of the genuine users is above the threshold level T_M and when an imposter tries to verify itself its score comes out to be less than T_M. Genuine match score distribution $P_m(M)$ for a set $A = \{A_1, A_2, \cdots, A_X\}$ of X genuine match scores is calculated as;

$$P_m(M) = \frac{1}{X} \sum_{i=1}^{X} 1(A_i = M) = \frac{1}{X} (\#A_i = M), \forall M$$

Imposter match score distribution $P_n(M)$ for a set $B = \{B_1, B_2, \cdots, B_Y\}$ of Y genuine match scores is calculated as;

$$P_n(M) = \frac{1}{Y}\sum_{i=1}^{Y} 1(B_i = M) = \frac{1}{Y}(\#B_i = M), \forall M$$

The percentage of rejection of *bona fide* users by the system due to a situation where the matching score M is less than threshold level T_M, $S \leq T_M$, is called false rejection rate (FRR). It is shown by the orange-lined region X in Fig. 7. The area X under the genuine score frequency curve when $S \leq T_M$ is expressed as function of T_M as;

$$FRR(T_M) = \int_{-\infty}^{T_M} P_m(M)\, dM$$

False rejection rate FRR for a set $A = \{A_1, A_2, \cdots, A_X\}$ of X genuine match scores is calculated as;

$$FRR(T_M) = \frac{1}{X}\sum_{i=1}^{X} 1(A_i \leq T_M) = \frac{1}{X}(\#A_i \leq T_M)$$

The percentage of acceptance of spurious users or imposters by the system because the matching score M is greater than the threshold value T_M is called the false acceptance rate (FAR). It is shown by the purple-lined region Y in Fig. 7. The area Y under the genuine score frequency curve when $S > T_M$ is expressed as function of T_M as;

$$FAR(T_M) = \int_{T_M}^{\infty} P_n(M)\, dM$$

False acceptance rate FAR for a set $B = \{B_1, B_2, \cdots, B_Y\}$ of Y imposter matches is calculated as;

$$FAR(T_M) = \frac{1}{Y}\sum_{i=1}^{Y} 1(B_i > T_M) = \frac{1}{Y}(\#B_i > T_M)$$

When FRR decreases FAR increases and vice versa. However, both the error rates are equal at one point called equal error rate ERR. At this point $FAR = FRR$. FAR and FRR are calculated for all points of threshold as shown in the graph below. ERR is the point of intersection of the two curves. The smaller the value of ERR, the better the system. The corresponding value of threshold to ERR is called the optimum value of threshold T_0. At this threshold both FAR and FRR will be equal. Fig. 8 provides a pictorial description of these parameters.

Another performance indicator of biometric verification system is receiver operating characteristic curve ROC. When FRR is plotted against FAR the resultant curve is called ROC (See Fig. 9). The closer is the curve to the point of origin, the better is the system considered.

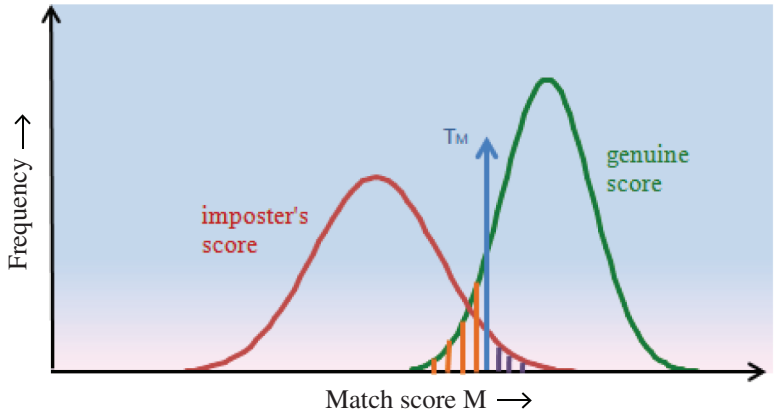

Figure 7: Non-ideal behavior of Biometric verification systems

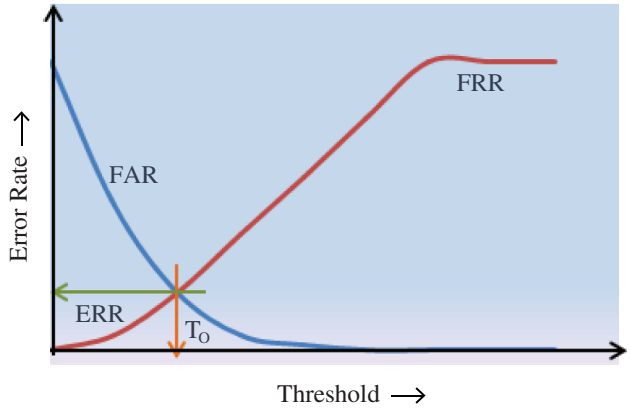

Figure 8: FAR and FRR at all values of threshold, ERR and T_O

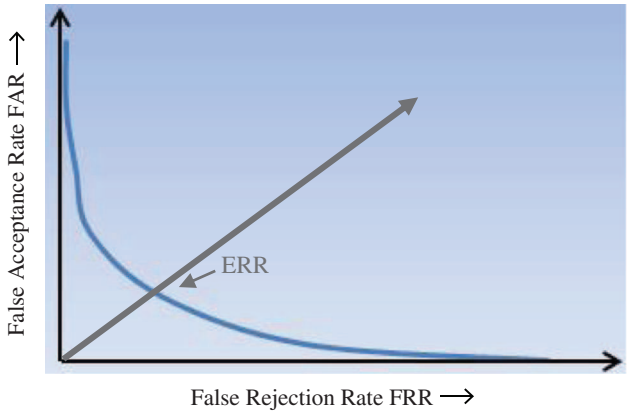

Figure 9: Receiver operating characteristic curve ROC

6 Experimental Setup

In this research, the proposed methodology is tested using a standard database for expression recognition called JAFFE [41]. FE stands for Japanese female facial expression and it is well-known publicly available dataset. M. Lyons, M. Kamachi, and J. Gyoba developed this dataset in 1998. It is famous dataset specially used for expressions/emotions classification. It is small database collected using images taken from 10 different Japanese female models. Total of 219 images taken from 10 models were collected using controlled environment in which no occlusion is used along with evenly balanced illumination. Hairs of the females were tied so that only facial information is used. All seven basic expressions (angry, sad, happy, disgust, fear, surprise and neutral) are present in the database samples. All the images used in the dataset are of 256×256 resolutions.

Table 1: Possible scenarios of expression hash verification system

		Identifier	Authenticators			
	Scenario	User ID	Token no.	Person	Expression	Access
Case I	1.	✓	✓	✓	✓	Granted
	2.	✓	✓	✓	✗	Denied
	3.	✓	✓	✗	✓	Denied
	4.	✓	✓	✗	✗	Denied
	5.	✓	✗	✓	✓	Denied
	6.	✓	✗	✓	✗	Denied
	7.	✓	✗	✗	✓	Denied
	8.	✓	✗	✗	✗	Denied
Case II		✗	–	–	–	Denied

There is one identifier i.e., the User ID that was assigned to the user during the enrollment stage and three authenticators; token number, facial ID and facial expressions. There are two cases; when User ID is correct and when User ID is incorrect. When User ID is incorrect, the system automatically prompts invalid user without any further processing. When User ID is correct there are eight scenarios for three authenticators as shown in Tab. 1. The first scenario is considered the legitimate attempt and rest of the scenarios are considered the illegitimate attempts from the attacker.

7 Results

The result analysis is shown in the Tab. 2, which shows that the frequency distribution curve of the legitimate scenario lies at the mean value of 116.822 with a standard deviation of 9.805 while the attacker's frequency distribution curve lies at 80.949 with a standard deviation of 13.860. Equal error rate is 4.45 at an optimum threshold level of 100. The ROC curve is close to origin showing the efficiency of the system to be excellent. The results are graphically presented in Fig. 10. In Fig. 10, P_m(M) represents the frequency distribution curve of genuine user while P_n(M) depicts the overall frequency distribution curve of imposters.

Scenarios 2–8 in Tabs. 1 and 2 can be considered as the illegitimate attempts to access the system.

In Tab. 3, we provide the comparison of our proposed technique with the WLD-LBP-CT [26] technique. The term Accuracy means the number of times the system correctly authenticates the incoming claimants in terms of percentage. Correct authentication means a valid user is detected to be a valid user and an invalid user is detected to be an invalid user. It is evident from the table that the performance of the proposed technique increases by the factor of 1% when expression recognition technique is used in conjunction with biohashing.

Table 2: Results of biometric authentication system

Scenario	Performance measures						ROC
	Frequency distribution		FRR	FAR	EER	To	
	Mean	SD					
1	116.822	9.805	4.444	–	–	–	–
2	89.595	10.611	–	19.047	8	103	Good
3	89.667	8.399	–	6.349	5	105.5	V. Good
4	84.622	9.745	–	4.762	4.7	100	Excellent
5	59.826	5.193	–	0		70–93	Ideal
6	58.829	5.909	–	0		70–93	Ideal
7	57.125	5.488	–	0		70–93	Ideal
8	58.619	5.518	–	0		68–93	Ideal
Total (2–8)	80.949	13.860	–	4.45	4.45	100	Excellent

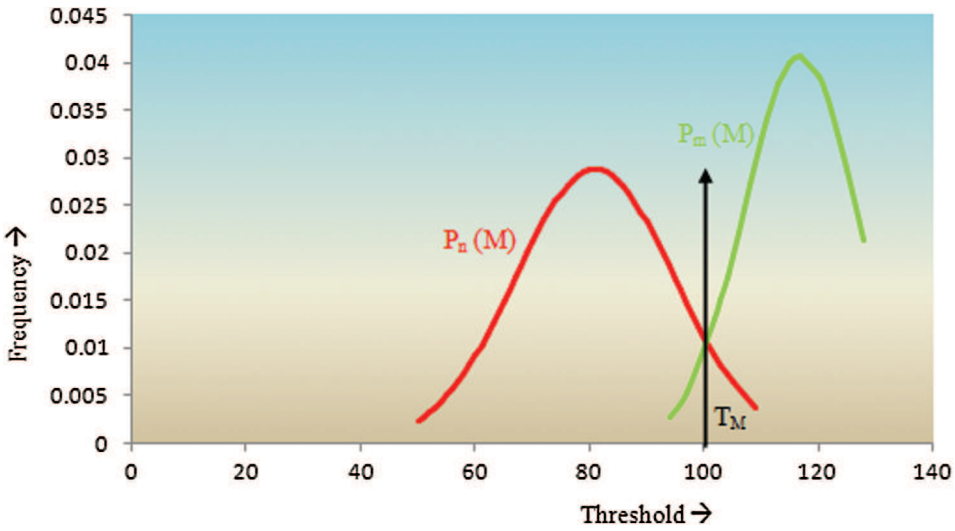

Figure 10: Frequency distribution curves of genuine user P_m(M) and imposter P_n(M)

Table 3: Comparison of previous and proposed technique

Technique	Accuracy (%)
WLD-LBP-CT	94.5
Proposed	95.5

8 Conclusion

The availability of multiple facial expressions for the biohashing process significantly increases the number of possible data set templates that can be used by a single user. The proposed technique provides the advantage of easy revocability and cancelability of biometric templates in case of compromise. Diversity can be insured by storing different expression templates in different biometric systems. The proposed technique considerably improves the security of the system as a single spoofed image of the user would be rendered useless, as the attacker would need to spoof the expression too. The overall system performance of the proposed system is better than the previous one by the factor of one percent.

Acknowledgement: The authors extend their appreciation to the Deanship of Scientific Research at King Saud University for funding this work through research group no. RG-1441-379.

Funding Statement: The author(s) received no specific funding for this study.

Conflict of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] W. Yang, S. Wang, J. Hu, A. Ibrahim, G. Zheng *et al.,* "A cancelable iris and steganography based user authentication system for the internet of things," *Sensors*, vol. 19, no. 13, pp. 2985, 2019.

[2] N. Riaz, A. Riaz and S. A. Khan, "Biometric template security: An overview," *Sensor Review*, vol. 38, no. 1, pp. 120–127, 2018.

[3] A. Jain, A. Ross and S. Prabhakar, "Fingerprint matching using minutiae and texture features," in *Proc. Int. Conf. on Image Processing*, Thessaloniki, Greece, pp. 282–285, 2001.

[4] H. Li, J. Zhang and Z. Zhang, "Generating cancelable palmprint templates via coupled nonlinear dynamic fiters and multiple orientation palmcodes," *Information Sciences*, vol. 180, no. 20, pp. 3876–3893, 2010.

[5] J. Connolly, E. Granger and R. Sabourin, "An adaptive classfication system for video-based face recognition," *Information Sciences*, vol. 192, pp. 50–70, 2012.

[6] K. Saraswathi, B. Jayaram and R. Balasubramanian, "Retinal biometrics based authentication and key exchange system," *International Journal of Computer Application*, vol. 19, no. 1, pp. 1–7, 2011.

[7] C. Sanchez-Avila and R. S. Reill, "Two different approaches for iris recognition using gabor filters and multiscale zero crossing representation," *Pattern Recognition*, vol. 38, no. 2, pp. 231–240, 2005.

[8] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *Proc. 6th ACM Conf. on Computer and Communications Security*, Singapore, pp. 28–36, 1999.

[9] A. Juels and M. Sudan, "A fuzzy vault scheme designs," *Codes and Cryptography*, vol. 38, no. 2, pp. 237–257, 2006.

[10] C. Chen, C. Wang, T. Yang, D. Lin, S. Wang *et al.,* "Optional multi-biometric cryptosystem based on fuzzy extractor," in *Proc. FSKD*, Xiamen, China, pp. 989–994, 2014.

[11] S. Yagiz, H. T. Sencar and N. Memon, "A secure biometric authentication scheme based on robust hashing," in *Proc. 7th Workshop on Multimedia and Security*, New York, USA, pp. 111–116, 2005.

[12] C. Rathgeb and A. Uhl, "Systematic construction of iris based fuzzy commitment schemes," in *Proc. ICB 2009*, Alghero, Italy, pp. 940–949, 2009.

[13] C. Rathgeb and A. Uhl, "Context-based texture analysis for secure revocable iris-biometric key generation," in *Proc. ICDP 2009*, London, UK, pp. 1–6, 2009.

[14] Z. Jinyu, N. K. Ratha and J. H. Connell, "Cancelable iris biometric," in *Proc. 19th Int. Conf. on Pattern Recognition*, Tampa, FL, USA, pp. 1–4, 2008.

[15] J. Hämmerle-Uhl, E. Pschernig and A. Uhl, "Cancelable iris biometrics using block re-mapping and image warping," in *Proc. ISC 2009*, Pisa, Italy, pp. 135–142, 2009.
[16] A. Teoh, D. Ngo and A. Goh, "Personalised cryptographic key generation based on FaceHashing," *Computers & Security*, vol. 23, no. 7, pp. 606–614, 2004.
[17] D. Ngo, A. Teoh and A. Goh, "Biometric hash: High-confidence face recognition," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 16, no. 6, pp. 771–775, 2006.
[18] J. Bringer, H. Chabanne, G. Cohen, B. Kindarji and G. Zemor, "Optimal iris fuzzy sketches," in *Proc. BTAS*, Washington, D.C., USA, pp. 1–6, 2007.
[19] C. Rathgeb and A. Uhl, "Adaptive fuzzy commitment scheme based on iris code error analysis," in *Proc. EUVIP*, Paris, France, pp. 41–44, 2010.
[20] T. S. Ong, A. T. B. Jin and D. C. Ngo, "Application-specific key release scheme from biometrics," *International Journal of Network Security*, vol. 6, no. 2, pp. 127–133, 2008.
[21] A. Kong, K. H. Cheung, D. Zhang, M. Kamel and J. You, "An analysis of BioHashing and its variants," *Pattern Recognition*, vol. 39, no. 7, pp. 1359–1368, 2006.
[22] A. Teoh, Y. W. Kuan and S. Lee, "Cancellable biometrics and annotations on biohash," *Pattern Recognition*, vol. 41, no. 6, pp. 2034–2044, 2008.
[23] A. Lumini and L. Nanni, "An improved BioHashing for human authentication," *Pattern Recognition*, vol. 40, no. 3, pp. 1057–1065, 2007.
[24] L. Nanni and A. Luminim, "Random subspace for an improved biohashing for face authentication," *Pattern Recognition Letters*, vol. 29, no. 3, pp. 295–300, 2008.
[25] D. B. M. Yin, A. Mukhlas, R. Z. W. Chik, A. T. Othman and S. Omar, "A proposed approach for biometric-based authentication using of face and facial expression recognition," in *Proc. ICCIS*, Singapore, pp. 28–33, 2018.
[26] S. A. Khan, A. Hussain and M. Usman, "Reliable facial expression recognition for multi-scale images using weber local binary image based cosine transform features," *Multimedia Tools and Applications*, vol. 77, no. 1, pp. 1133–1165, 2018.
[27] S. Dabbaghchian, M. P. Ghaemmaghami and A. Aghagolzadeh, "Feature extraction using discrete cosine transform and discrimination power analysis with a face recognition technology," *Pattern Recognition*, vol. 43, no. 4, pp. 1431–1440, 2010.
[28] S. W. Cho, N. R. Baek, M. C. Kim, J. H. Koo, J. H. Kim *et al.,* "Face detection in nighttime images using visible-light Camera Sensors with two-step faster region-based convolutional neural network," *Sensors*, vol. 18, no. 1, pp. 2985–2995, 2018.
[29] P. Viola and M. Jones, "Rapid object detection using a boosted cascade of simple features," in *Proc. CVPR 2001*, Kauai, HI, USA, pp. 490–511, 2001.
[30] T. Ojala, M. Pietikainen and T. Maenpaa, "Multiresolution gray-scale and rotation invariant texture classification with local binary patterns," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 24, no. 7, pp. 971–987, 2002.
[31] T. Ahonen, A. Hadid and M. Pietikainen, "Face recognition with local binary patterns," in *Proc. ECCV 2004*, Prague, Czech Republic, pp. 469–481, 2004.
[32] H. Liu, J. Sun, L. Liu and H. Zhang, "Feature selection with dynamic mutual information," *Pattern Recognition*, vol. 42, no. 7, pp. 1330–1339, 2009.
[33] C. Silva, T. Bouwmans and C. Fr'elicot, "An extended center-symmetric local binary pattern for background modeling and subtraction in videos," in *Proc. VISAPP 2015*, Berlin, Germany, pp. 395–402, 2015.
[34] J. Chen, S. Shan, C. He, G. Zhao, M. Pietikainen *et al.,* "WLD: A robust local image descriptor," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 32, no. 9, pp. 1705–1720, 2010.
[35] F. Dornaika, E. Lazkano and B. Sierra, "Improving dynamic facial expression recognition with feature subset selection," *Pattern Recognition Letters*, vol. 32, no. 5, pp. 740–748, 2011.
[36] X. Jing, Y. Tang and D. Zhang, "A fourier-lda approach for image recognition," *Pattern Recognition*, vol. 38, no. 3, pp. 453–457, 2005.

[37] Z. Yankun and L. Chongqing, "Efficient face recognition method based on DCT and lDA," *Journal of Systems Engineering and Electronics*, vol. 15, no. 2, pp. 211–216, 2004.

[38] S. A. Khan, M. Ishtiaq, M. Nazir and M. Shaheen, "Face recognition under varying expressions and illumination using particle swarm optimization," *Journal of Computational Science*, vol. 28, no. 4, pp. 84–94, 2018.

[39] L. Blum, M. Blum and M. Shub, "A simple unpredictable pseudo-random number generator," *SIAM Journal on Computing*, vol. 15, no. 2, pp. 364–383, 1986.

[40] A. Sidorenko and B. Schoenmakers, "Concrete security of the blum-blum-shub pseudorandom generator," in *Proc. 10th IMA Int. Conf. on Cryptography and Coding*, Cirencester, UK, pp. 355–375, 2005.

[41] M. J. Lyons, S. Akamatsu, M. Kamachi, J. Gyoba and J. Budynek, "The japanese female facial expression (jaffe) database," in *Proc. Third Int. Conf. on Automatic Face and Gesture Recognition*, Nara, Japan, pp. 14–16, 1998.