Design of a High Secure Authentication System Based on Fuzzy Fusion of Iris and Face and Incorporating 2D Baker and Henon Maps

Marwa M. Eid[1,*] and Mohamed A. Mohamed[2]

[1]Assistant Professor at ECE-Department
Delta Higher Institute for Engineering & Technology, Mansoura, Egypt

[2]Associate Professor at ECE-Department
Faculty of Engineering, Mansoura University, Mansoura, Egypt

[*]*Corresponding author's email: marwa.3eeed [AT] gmail.com*

ABSTRACT— ***The emergent concerns of identity theft problems and terrorism make the design of applicable accurate verification systems more crucial. No single biometric identifier could perfectly own all desired security properties. Moreover, the transmitted or stored biometric templates raise the opportunity of compromising user's privacy and identity breaching. This paper offers new scheme based on score level fuzzy fusion at decision level fusion to effectively combine face and iris identifiers. The proposed system allows an efficient identification procedure and introduces a new template locking approach based on chaos cryptography to protect the biometric data. In this study, CASIA and Faces94 databases are used to examine and appraise the robustness of the proposed schemes. The proposed template protection scheme offers new different uncorrelated secure forms of the base original templates in imperative and much speedy ciphering methodology. Furthermore, it could be rescinded at different points of probable attacks from sensed level to the final code and the matcher. It presents remarkably good key sensitivity and more robustness against different malicious attacks compared to classical encryption techniques. Furthermore, being noninvasive to the recognition process, simulation results on authentication rates introduces FAR and FRR of 0.0345%, and 0.001% respectively which illustrated a significant enhancement of the proposed fuzzy fusion over each unimodal system and existing multimodal fusion methods.***

Keywords— Crypto-biometrics, Iris Recognition, Face Recognition, Chaotic Encryption, and Fuzzy Logic Fusion

1. INTRODUCTION

The design of a reliable identification system plays a vital increasingly role in several critical applications that perform services to only legitimately enrolled users as in conceding access to nuclear facilities, offering remote services for financial transactions, etc. Moreover, due to the proliferation of web-based services and the huge prevalence of sharing networked computer resource, the pronounced need for robust identity management systems has been further intensified. Practically, for a trustable authentication system, the conventional security mechanisms (i.e. knowledge-based or token- based) might be employed as the first level of identity proof. Nevertheless, knowledge- based mechanism could be easily breached, divulged and guessed by means of dictionary attacks and the token-based authentication is not secure and predominantly easily stolen. Thus, non-repudiation problems cannot be avoided by these two means. So, the public demand for establishing identity in a reliable system has driven active investigation in the biometrics field. Biometrics grants an inherent and substantial solution to several aspects of user identification by utilizing their physical and/or behavioral characteristics. Today's environment, there is a great deal of interest in using facial recognition applications. The face image could be acquired from a distance by a camera without any explicit participation of the users. Being non-intrusive authentication methodology, it is taken into account to be very beneficial for surveillance purposes. Hence, border checkpoints, national IDs and criminal justice systems, etc. are considered to be the most common and critical facial recognition applications. However, definitely, several factors cause variations in the facial appearance like intrinsic factors and extrinsic ones i.e. facial paraphernalia, exposure time, and lens aberrations of the camera etc. Moreover, any simple changes of human appearance could dramatically interfere the face recognition technique and easily lead to system failure. For a reliable face recognition technique, pose manipulations, expression variations, skewed face images could produce disguising features and significantly drop the accuracy. Thus, up to now, the design of an accurate face recognition is still a challenging issue and a complicated enigma. The two main keys to the system are feature extraction and face classification. Therefore, towards improving the system performance, a perfect feature extractor and an efficient classifier must be essentially found. However, the matching performance cannot be gradually increased by attuning both of them. Several constraints limit the implicit upper bound of their performance like

intra-class similarities or inter-class variations between the employed feature sets of different distinguishable subjects plus the available template capacity.

From the perspective of precision, with the use of an efficient information fusion for automatic identification, more accuracy could be achieved than a single technique. Nevertheless, simply embedding multiple features sets together could bear much redundant information and little contributions to the recognition rate. The ideal biometric authentication system should possess certain properties like permanence, distinctiveness, acceptability, universality etc. However, no single optimal biometric identifier could perfectly own all of these properties without any vulnerabilities or penetration points. Hence, extra requirements about the security of a certain unimodal authentication system had been raised, especially in the case of access to top security domains. Some of these limitations and problems could be addressed by consolidating multiple sources of information through a single robust design as in multibiometric system. Several multibiometric systems had been introduced by employing a certain fusion strategy at separate levels (i.e. sensor fusion, feature fusion, match score fusion, and decision fusion etc.). This can be accomplished by fusing several traits, or multiple bases of features and matching multiple identifiers. It could improve the corresponding accuracy and deter spoof attacks and continue to operate even software malfunction, or deliberate user manipulation. D. Meva and C. Kumbharana proved that score level fusion provides more information about the biometric data compare to rank level and decision level fusion as in [1]. A. Ross and R. Govindarajan introduced the idea of feature fusion of PCA and LDA coefficients of face biometric to offer a lower error rate [2]. Additionally, they provide a methodology for fusing face and hand identifiers and demonstrated that it is very important that biometric vendors grant access to feature level information to permit development of efficient fusing approaches [2]. Bigun et al. represent a statistical framework based on Bayesian statistics to combine the human speech and face data of a user with estimating biases of each classifier through the fusion process [3]. Recently, another promising methodology of feature combination is the Fuzzy logic based fusion which has been extensively employed in numerous applications [4]. H. Benaliouche and M. Touahria suggested with their comparative study of multimodal biometric recognition based on iris and fingerprint that the fuzzy logic method for the matching scores combinations at the decision level is better than classical weighted sum rule and the classical sum rule in terms of matching time, error rates, and accuracy as in [4]. J. Gao et al. introduced kernel fuzzy discriminant analysis to deal with recognition problems by merging the advantages of fuzzy methods and a kernel trick to fuse the face features [5]. O. Sharifi and M. Eskandari introduce new schemes based on score level, feature level and decision level fusion based on Log-Gabor transformation for both face and iris identifiers [6].

Apart from several multimodal biometric systems that had been introduced and developed with different biometric traits and fusion approaches, the proposed multimodal biometric system based on both selected traits (iris and face signatures) could overcome the drawbacks related to each standalone unimodal biometric system. Moreover, their combination could allow an efficient and accurate identification procedure due to the high accuracy level of an iris and the convenience and passive recognition property of face. Since 1999 in US Houston, the iris identification had been adopted for business and cash access, via ATM customers of the United Bank [7]. Several researchers are concerned in building faster, flexible, and more reliable iris system. Iris is a biometric feature found to be reliable and accurate for the authentication process, comparing to other biometric traits. In general, it possesses multiple characteristics that address it as a perfect biometric identifier like stability, uniqueness, genetic independence, excessively data-rich physical structure and remarkably limited variations across the life's period. Additionally, being an externally visible, unique, accurate, protected organ and stable throughout adult life, iris features make it very attractive and important in high secure identification systems demand. Therefore, the iris recognition field is considered one of the most active and hastily expanding areas of inquiry. Actually, the iris recognition function is dramatically affected by the inferiority of the utilized images for recognition purposes. However, this area of research is still required different perfections to provide appropriate solutions against error factors. Additionally, for a precise biometric identification system which works accurately, the system must support that the biometric data came from a genuine person at the enrollment time.

However, from the privacy perspective, the most concern threatening the biometric system arises from the misuse of the stored or transmitted private data. The original biometric data set could not be reset or replaced, unlike passwords that can be reconstructed. Furthermore, due to the full expanse of incorporating biometrics technology in numerous vital applications, it is very probable that private biometric data are being broadcasted over non-secure channels. Various techniques are utilized to preserve biometric data such as encryption, or watermarking. Different kinds of intentional and friendly attacks could hamper a typical biometric system, such as tampering, modification, and distorting database templates within the inter-system stages besides overriding the final decision of the system matcher like on the channels between the matcher and the feature extractor or the database. Also, unreliability, complicated mathematic and expensive computational costs are not useful for securing biometric templates [8]. Furthermore, how to provide a fast, simple, and robust routine or technique to provide dissimilar updatable imprints for different applications to the same user is still an excessive mystery. In the last few years, towards addressing these concerns, significant approaches have been published and the ideas of cancelable biometrics and biometric cryptosystems have emerged improving the public confidence to the acceptable biometric systems. Commonly, in the area of biometric template protection, the introduced schemes are categorized as biometric cryptosystems and cancelable biometrics. Basically, cancelable biometric approaches apply non-invertible transformations to modify the original biometric data and the matching between the transformed data are

performed to authenticate users. Just the transformed template is revealed, a new one could be reissued by employing other parameters within the same transformation. Biometric cryptosystems as a solution are designed to secure binding a digital key to the biometric data or generation a digital encryption key from the enrolled data. Whereas, major of those systems essentially require storing of the employed helper data (the public biometric- dependent data) towards binding, retrieving or generating encryption keys. According to the derived helper data, the intended system could be classified as key-binding or key-generation system [9]. Through, the key generation schemes, indirectly the biometric comparisons are performed by approving key authenticity, where the output of the process is either the generated key or a failure message. However, it is not expedient for the most common biometric identifiers to directly extract digital keys due to the likely biometric variations and other distortion sources. Moreover, the stored helper data must not reveal the vital information about the private biometric templates during keys reconstructing [9]. F. Hao et al. offered the first practical routine to integrate the iris code with Hadamard and Reed-Solomon codes [9]. Mohammed et al.,[10] presented a security architecture by combing the iris templates with watermarking and visual cryptography. Yang and Dong [7] disseminated his conception for establishing a network security exploitation biometric and coupled map lattice chaotic map. However, none of this present or deal with the effect of corrupt attacks during transmitting in non-secure channel especially in the case of cropping. Besides, standard encryption techniques like AES, RSA, etc. are not smooth functions so it might degrade the performance of recognition rate.

This paper attempts to put forth all of these threats under one roof. To evade some threats related to multibiometric design, the proposed system invokes multiple features from both face and iris traits to improve the complete system performance by employing fuzzy sets classed with un-sharp boundaries. The introduced fuzzy sets within the proposed fuzzy logic will avoid the brute force attacks. Moreover, to override the biometric overtness, cryptological attacks, replay attacks, the important private user information will not exist in plain-text (raw data) form during transmission and saving within the system procedure at several points of probable attacks. Furthermore, to evade cross-matching, cracking, attacking, sneaking, juggling, and tracing from hackers from the transmitted or saved databases, the proposed system will provide updatable secure sketches of the private data. By recruitment diverse effective chaotic maps via rounds of substitution and diffusion through the proposed template protection scenario, the idea of creating an exceptional base template has been introduced. For secure applications, the same original templates are replaced by dissimilar uncorrelated versions of secure sketches and once the secure template is compromised, the system could rerelease a new one using different secure looking keys and those parameters must be kept secret. Contrary to typical encryption methods which may limit the system capacity as it can be computationally expensive [10], the proposed system based on nonlinear dynamic and effective acceleration of chaos cryptography will introduce a robust and fast routine for biometric protection without any degradation of the recognition rate. Furthermore, "strong" enough mechanism for extracting salient iris and face information irrespective of some of the possible malicious attacks or noises related to the communication channel such as blurring, cropping attacks is provided.

2. THE COMPLETE FRAMEWORK OF THE PROPOSED SYSTEM

Each biometric trait isn't a secret, several important questions that emerges from this, firstly, how the transmitted or saved biometric data could be revoked in case of any deception? During the authentication procedure, is there any secure way for transmitting or saving user data at any intermediate stage? The traditional image encryption techniques should not be utilized for a large amount of data and high-resolution images [8]. In order to overcome these problems, the idea of interpolating the chaos cryptography in the field of crypto-biometrics has been discussed. Contrary to the conventional encryption algorithms, the chaotic encryption techniques as a relatively new trend of cryptography will efficiently achieve the demand of reliable and secure protection, storage, real-time transmission of the iris data. The proposed crypto-biometric system is designed in such a way that inheriting the advantages offered by multimodal biometrics and chaotic cryptography while eliminating their disadvantages whereas the secure protected templates will be only stored. The key parts of the proposed design are the face recognition module, the iris recognition module, the fusion procedure, and the template protection module. Each security system could have the vulnerability points which possess the user's information and their corresponding identification templates and the identical codes. Based on the matching score and rank information of integrating face and iris traits will be presented as shown in Figure 1.

2.1 The Unimodal Iris Recognition

Chinese Academy of Sciences Institute of Automation (CASIA) iris image database version 1.0 [11], particularly, a dataset of 10 persons every person has a database of 7 images using a near-infrared (NIR) camera, i.e., 70 images, will be suited to assess the proposed system achievement. Generally, the common steps that followed iris acquisition procedure are iris localization, segmentation, feature extraction, normalization and feature encoding. An efficient and simple iris localization methodology based on morphological features and wavelet fusion has been introduced on previous experiment in details as in [12]. Based on morphological features, inner and outer iris radii had been extracted as shown in Figure 2. Due to variations in illumination, the pupil size might be randomly changed and resulted to deformation of the iris pattern and interference with the matching rates. To be invariant to size, position, and orientation fluctuations, a 2D array in polar coordinates that represented iris data is generated as in Daugman rubber sheet model which can be

represented as [12].

$$I(x(r,\theta),y(r,\theta)) \rightarrow I(r,\theta) \quad (1)$$

where r radius lies in the unit interval $(0,1)$ and θ is the angle between$(0,2\pi)$ for iris image I, and the remapping of the iris image $I(x,y)$from raw Cartesian coordinate to polar coordinates $I(r,\theta)$is through[12]

$$x(r,\theta) = (1-r) * x_p(\theta) + r * x_i(\theta)$$
$$y(r,\theta) = (1-r) * y_p(\theta) + r * y_i(\theta) \quad (2)$$

To derive the iris unique features, Gabor wavelets filters which composed of complex sinusoidal carriers and Gaussian envelopes are tended to be very beneficial at distinguishing iris patterns. Following the procedure of feature extraction, the encoding of iris features is conducted by involving a simplistic four-level quantization routine to the phase response [12]. Holding an individual filtered pattern, each pixel value in the real and imaginary response is assigned to a bit value of zero or one based on whether its value is lesser or greater than zero. Once the iris response has been quantized, a new black and white image could be extracted by embedding adjacent columns to derive the iris signature as shown in Figure 3. Thus, Hamming Distance (HD) [12][12][12]is utilized as a matching metric for comparing two final encoded iris patterns (1 bit per pixel) which has a size of 20×480 as in [12]

$$HD = \left(\frac{1}{N-\sum_{k=1}^{N} Xn_k\,(OR)\,Yn_k} \sum_{j=1}^{N} X_j(XOR)Y_j\,(AND)X\grave{n}_j(AND)Y\grave{n}_j\right) \quad (3)$$

where X_j and Y_j are the two bit-wise templates to compare, X_{n_j} and $Y_{n_j}$are the corresponding noise masks for X_j and Y_j, and N is the number of bits represented by each template

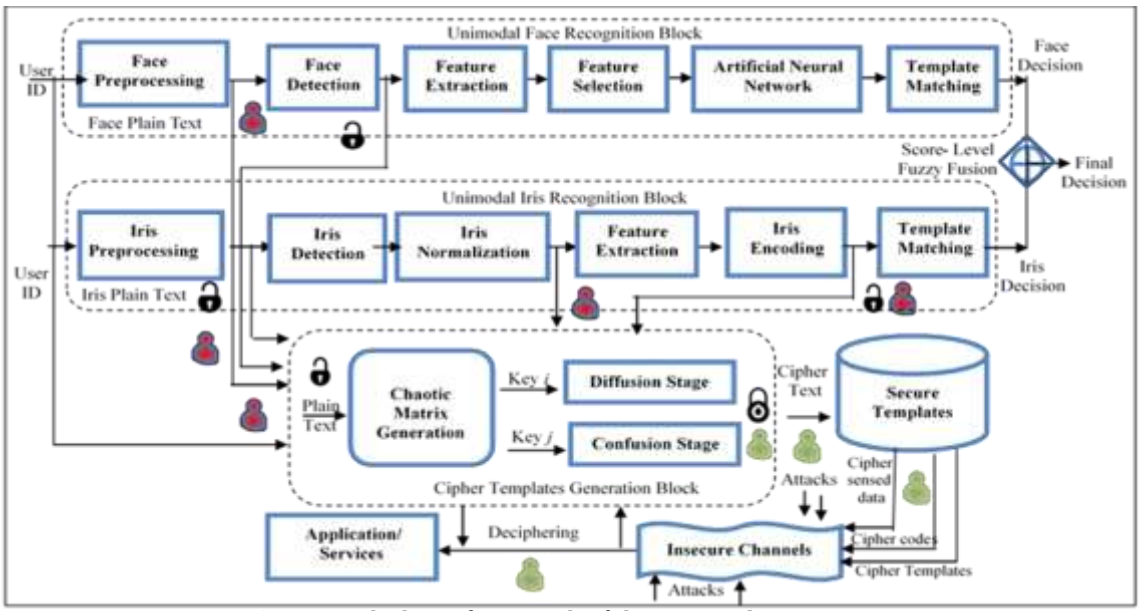

Figure 1: The basic framework of the proposed system

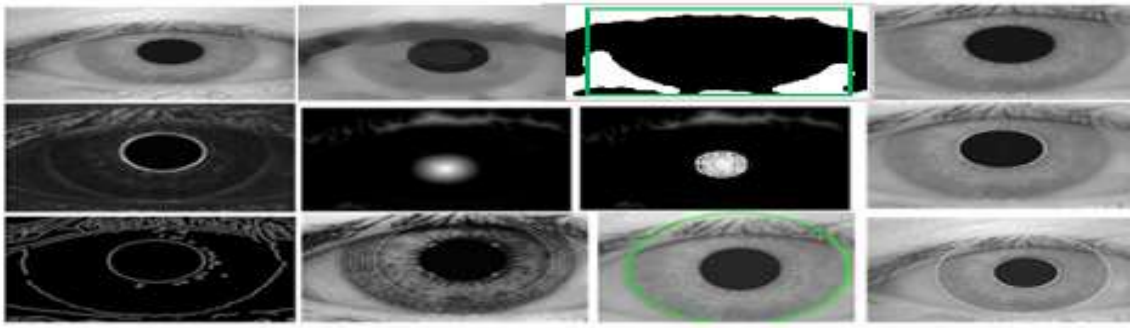

Figure 2: Sample of applying Localization process based on extracting morphological features.

Figure 3: Sample of encoded iris pattrn code.

2.2 The Unimodal Face Recognition

Usually, the variation between different images of unrelated faces is slighter than those which taken for the same face at a different environment due to strong disparities in human poses, illumination, physical challenges, etc. A collection of 200 images from Faces94 [13] database for 10 subjects each subject has 20 different images, will be chosen. All face images resolution is (180 × 200) pixels. Attempting to compare these images under the "identical" lighting conditions, after several previous experiment as in [14], main stages of the applied face detection stage are: (i) background subtraction, (ii) skin detection, (iii) extracting face contour, (iv) image normalization, and (v) detecting interior face features [14]. All the prospective faces had been normalized and cropped to be in a fixed size 106 × 106 pixels. An efficient face recognition methodology relies on the appropriate choice of the drawn features which represent face images. Thus, via evoking the data decomposition property of the wavelet transform (based on Daubechies 2 tap wavelets (db2)) mother functions with 1-level decomposition, it will preserve the major data from any intrinsic or extrinsic deformations as shown in Figure5. Feature determination in face recognition requires the derivation of conspicuous features from the raw pattern. Through thresholding technique, the numbers of these features had been determined empirically from experimentations. Thus, to provide valuable information about each face in much less memory separately only 500 DWT, for each subject had been drawn. Thus, Artificial Neural Network (ANN) classifier based on a set of driving features have been designed to represent supervised multi-layer perceptron (MLP), feed-forward ANNs. The weights are fixed by a supervised training back-propagation scheme as a type of gradient descent method, which seeks to fetch an adequate local minimum and reach to the minimal error with learning rate 0.001. In addition, the particular number of input nodes could be adapted according to the number of the introduced feature sets. The employed data set are randomly assigned as three subsets; 60% for the training, 20% to the validation, and the 20% to the testing set. Hence, different architectures of ANNs have been practically investigated through trial and error with a considerable number of adaptable parameters like transfer function and number of epochs. Due to its charming incessant properties and di[illegible]ayer. Thus, [illegible]rmed throug[illegible]

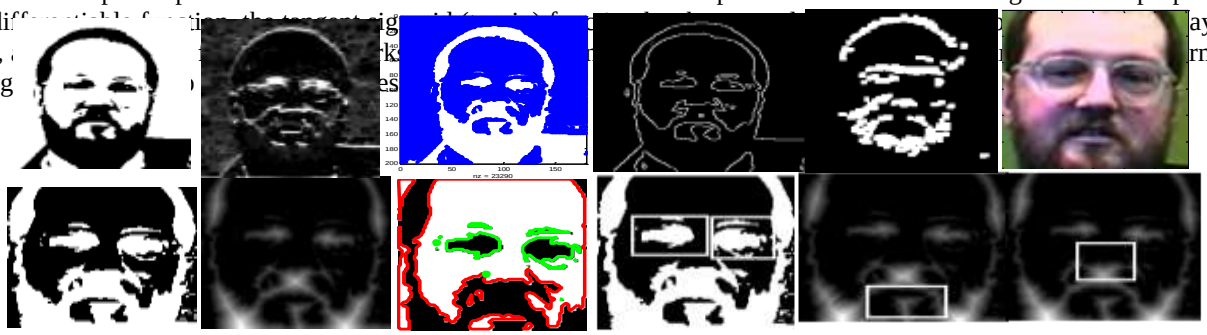

Figure 4: Applying facial feature detection process based on extracting morphological features.

Figure 5: 1-level decomposition using (db2).

In classical multimodal systems, the employed matching score fusion rules might be the sum rule based matching of fusion iris and face scores as [1]:

$$\acute{S} = \sum_{k=1}^{2} S \qquad (4)$$

where S is the fusion score or to be the weighted sum rule where the fusion score is calculated as [1]:

$$\acute{S} = \propto S_1 + (1-\propto)S_2 \qquad (5)$$

where S_1 and S_2 are the matching scores of both face and iris matchers respectively and α is the assigned weight to each identifier. For the proposed fuzzy Fusion Routine, a definite appreciation to each decision consistent with the proposed fuzzy rules which minimizing both false accept rate (FAR), false reject rate (FRR), according to the matching distance calculated for each modality as [12]:

$$FAR = \frac{No.of\ times\ different\ persons\ match}{No.of\ comparisons\ between\ different\ persons}$$
$$FRR = \frac{No.of\ times\ persons\ rejected}{No.of\ comparisons\ between\ same\ persons} \quad (6)$$

Fuzzy logic is certainly one of the interesting areas on the edge of the cognitive field and decision building. The main influence of fuzzy fusion approach is that it employs both matching score and ranking information from each single identifier. Additionally, inconsistent with classical systems rendering only either yes or no decision, the level of confidence with the matching probability in recognition outcomes of the multimodal system can be obtained using this method.

2.3 The Proposed Fuzzy Fusion Routine

Firstly, main parameters for each classifier are picked. With a view to full integration between effort and cost associated with assembling a qualified multimodal database, most of the multimodal biometric system researchers manipulate a virtual experimental dataset, which comprises such records created by compatible pairing a user from the unimodal face database (e.g., Faces94) with another user from the iris database (e.g., CASIA). Moreover, on the assumption of independent and confident biometric traits for the corresponding person, those virtual user's dataset will be created towards examine the proposed system processing speed including the confidence level of the proposed multimodal system recognition [4]. Therefore, the formulation of the virtual examined database is based on this assumption which contains only 10 (e.g. 5 genuine subjects and 5 imposters) randomly selected subjects' data from both unimodal iris and face database will be examined; Figure 6. Each system presents a matching score which indicates to the similarity of the compared feature vector with the stored template vector. By combining these scores, the veracity of the claimed identity will be asserted. Although the information included in this stage is not as rich as in images, it is deeper and much richer in ranks and decisions. Each unimodal identifier provides its own result and the proposed fuzzy fusion process combines them together to outputs particular decision for accepting or reject. A ranking of the "iris and face candidates" in the template database, sorted in a decreasing order of the match scores. Moreover, the scheme is required to designate a higher rank to a guide that is most similar to the inquiry. Besides, establishing on the proximity of face and iris feature vector and template, each subsystem computes its own matching score and these individual scores are eventually mixed into a total score, which is given to the final decision module. Fuzzy logic implies to all of the technologies and theories, which employ fuzzy sets classed with un-sharp boundaries. The essential procedure of fuzzy logic is established on the following conceptions as shown in Figure 7. The essential procedure for this strategy will be performed according to the following stages:

Step-1: Begin with the score normalization step, Min-max normalization technique for score normalization will be utilized to obtain all match score values in the range of 0 to 1. For the proposed multimodal system, suppose that $S_{k,m}$ represents the generated matching score for class k by m matcher, and after normalization it will be on this interval, $0 \le S_{k,m} \le 1$. In addition, S_j^i represents the match score output for i pattern by the j matcher, and $i = 1, 2, \dots, N$, where N is the number of enrolled classes, and $j = 1, 2$, i.e. face and iris traits, so $M = 2$. The min-max normalized score nS_j^i for the test score S_j^i is computed as [15]:

$$nS_j^i = \frac{S_j^i - \min(S_j^i)}{\max(S_j^i) - \min(S_j^i)} \quad (7)$$

Step-2: Thus, S_k, i.e., the average match scores are calculated by:

$$S_k = \frac{1}{M}\sum_{m=1}^{M} S_{k,m} \quad (8)$$

for identifying the desired similarity score for a certain subject.

Step-3: Since some classifiers might not be included in all of the rank lists, a precaution for the fusion module is presented using the definition of fuzzy linguistic variables as:

$$\begin{matrix} H, \text{when } S \ge 0.75 \\ M, \text{when } 0.75 > S > 0.55 \\ L, \text{when } S \le 0.55 \end{matrix} \quad (9)$$

where, H, M, and L represented high, medium, and low respectively.

Step-4: Establish the fuzzy rules, which represent the linguistic variables relations as in Table 1.

Step-5: Create the defuzzification procedure to imply the final decision according to the confidence level of that decision and get the fuzzy conclusion if necessary. Moreover, towards combining the fuzzy rules results, a suitable scalar output for the final classification has been acquired. By merging the algorithms for each separately recognizer with the average match scores according to a simple weighted sum matching rule technique for the ranked identity,

which is calculated as:

$$FSR = \left(\alpha(AMS) + \beta(IMS) + \gamma(FMS)\right) \quad (10)$$

while $\alpha, \beta, \text{and } \gamma$ are the supposed weights to individual classifiers. It will be assigned based on the accuracy considerations, i.e., based on the numerous trials as: $0.32;\ 0.43, \text{and } 0.25$ and the corresponding system responses have been assigned as:

$$\begin{cases} \text{SI, when FSR} \geq 0.75 \\ \text{WI, when } 0.75 > FSR > 0.5 \\ \text{NI, when FSR} \leq 0.5 \end{cases} \quad (11)$$

where SI, WI, and NI denoted to 'Strongly Identified', 'Weakly Identified', and 'Not Identified' respectively.

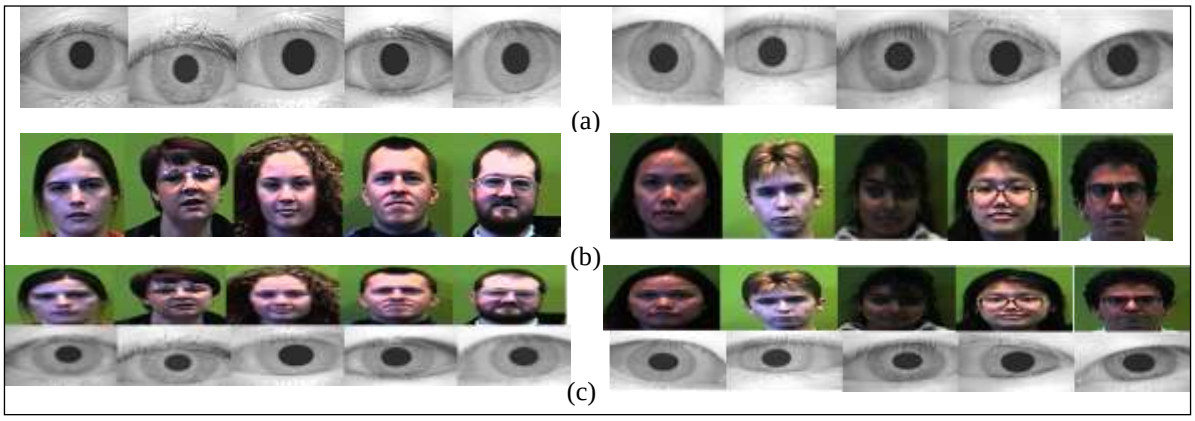

Figure 6: Virtual employed datasets; for 5 genuine candidates and 5 imposters respectively; (a) iris strategy, (b) face strategy evaluation, and (c) the combined multimodal virtual dataset.

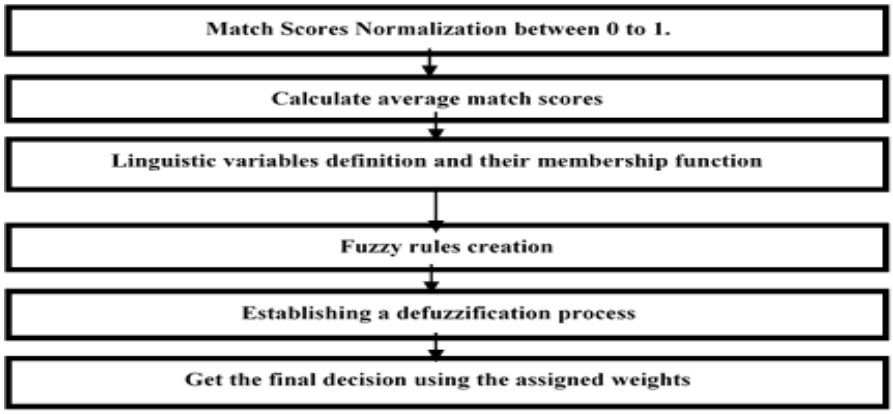

Figure 7: The proposed fuzzy fusion method.

Table 1: Fuzzy rules for the proposed fusion method.

Category	Average Matcher (AMS)	Iris Matcher (IMS)	Face Matcher (FMS)	Final System Result (FSR)
Fuzzy Rules	H	H	H	SI
	H	H	L	SI
	H	H	M	SI
	H	L	H	SI
	H	L	L	NI
	H	L	M	WI
	H	M	H	SI
	H	M	L	WI
	H	M	M	WI
	L	H	H	SI
	L	H	L	NI
	L	H	M	WI
	L	L	H	WI
	L	L	L	NI
	L	L	M	NI
	L	M	H	WI
	L	M	L	NI
	L	M	M	WI
	M	H	H	SI
	M	H	L	WI
	M	H	M	WI
	M	L	H	WI
	M	L	L	NI
	M	L	M	WI
	M	M	H	WI
	M	M	L	WI
	M	M	M	WI

Where: AMS, FMS, IMS, and FSR denote to Average Match score, Face matcher's score, iris matcher's score, and Final System Result respectively. In addition, (SI = Strongly Identified; WI = Weakly Identified; NI = Not Identified)

2.4 The Proposed Template Protection Scheme

Preventing any probable security crisis demands the precise association of vulnerabilities related to the proposed biometric system and their methodical bearing according to its structure, the biometrics identifiers used, and managerial strategies. Due to its computationally expensive, typical encryption mechanisms may restrict the wide-scale biometric systems capacity. High redundancy, bulk data capacity and other intrinsic features of biometric image might be the main causes for encryption failures in security systems. Confusion and diffusion are the keys of the chaos-based encryption schemes using a mixture of chaotic maps. Moreover, the control parameters and initial conditions will be the symmetric secret key, which properly selected within the involved maps in the chaotic regime. Therefore, two different chaotic maps will be employed in the proposed chaotic generator block (2D Baker map and 2D Henon map) to get a secure sketch of biometric data as the following steps.

Step 1: Performing the $2D$ Baker map that defined as [16]:

$$x_{n+1} = \begin{cases} \lambda_a x_n & if \;\; y_n < \alpha \\ (1-\lambda_b) + \lambda_b x_n & if \;\; y_n > \alpha \end{cases}$$
$$y_{n+1} = \begin{cases} y_n/\alpha & if \;\; y_n < \alpha \\ \frac{(y_n - \alpha)}{\beta} & if \;\; y_n > \alpha \end{cases} \qquad (12)$$

where $0 \leq x \leq 1$; $0 \leq y \leq 1, \beta = 1-\alpha$ and $\lambda_a + \lambda_b \leq 1$.The iterative relation of the baker's map used in the proposed scheme as follows [16]: $x_{n+1} = (x_n + y_n)|1,\ y_{n+1} = (x_n + 2y_n)|$

Noted that two non-overlapping vertical stripes within the square could be mapped, one in $0 \leq x \leq \lambda_a$ and the other in $(1 - \lambda_b) \leq x \leq 1$. where, $i = 0, 1, 2 \ldots$ Here $\alpha_1, \beta_1, \alpha_2, \beta_2$ are system control parameters. x_0 and y_0 are initial conditions. The equation generates sequence in the range of 0 and 1 with chaotic behavior $2.75 < \alpha_1 \leq 3.4, 0.15 < \beta_1 \leq 0.21, 2.7 < \alpha_2 \leq 3.45, 0.13 < \beta_2 \leq 0.15$ and the values of x_i and y_i in $(0,1)$, and performs iteration and records the result until have K values.

Step 2: Compute the 2D Henon map with taking initial conditions (x_0, y_0) and in 2D real plane, which secrete key values mapping it to the next point [16]:

$$\left.\begin{aligned} x_{i+1} &= 1 - \mathrm{a}x_i^2 + y_i \\ y_{i+1} &= \mathrm{b}x_i, \quad i = 1,2,3 \end{aligned}\right\} \qquad (13)$$

where: a, b represented the control parameters and (x_{i+1}, y_{i+1}) implied to the sequence of other keys. The sensitivity property in Henon exhibits chaotic behaviors as it dependent to initial secrete key and control parameters and $a = 1.4, b = 0.3$ then, iterated with k times.

Step 3: Compute the Henon map according to Eq.(13), firstly for $M/2$ times, and started to record $x_{n+1}$and $y_{n+1}$from $(M/2 + 1)^{th}$ iterations until reached the certain identified R values of X, and C values of Y.

Step 4: Accomplish the XOR-ing operation for both the data stream and the chaotic stream, which these result data are formulated to a 2D array producing the first cipher-image.

Step 5: Reach the final cipher-image pixel by diffusion each pixel using the created random values through theses transformation $x_n = (x_n \times 106)\ mod\ 256$ and $y_n = (y_n \times 106) mod\ 256$ and converted the result to $2D$ array.

Step 6: Fortunately, the original plain image will be recovered by employing the proposed scenario in such a reverse order; the result of applying this template protection scenario at different point of probable attacks as plain image levels and feature level and code in the case of the iris organized as the original image, the encrypted image and the corresponding decrypted one as shown in Figure 8.

4. Experimentations and Performance Analysis

The security of the proposed crypto-multibiometrics has been analyzed using a standard methodology in the area of image encryption for template protection schemes, and authentication performance metrics for the authentication. The proposed system will address the concerns of user's privacy, timing issues, template protection, and trust issues via a method for the secure sketch biometric data at certain points of probable attacks. The security and efficiency of any image encryption scheme are evaluated through a number of performance metrics parameters [17] such as Number of Pixel Change Rate (NPCR), visual testing, information entropy, correlation coefficient examinations, Unified Average Change Intensity (UACI) etc. Sample of iris protection methodology and its corresponding histogram is shown in Figure 9. For such a good image cryptosystem, the presented encryption methodology hides all plaintext image's attributes and their main characteristic in the corresponding histogram whereas the cipher images are intensely unrelated and completely random; Figure 9b. The histograms of chaotic based cipher images are uniformly distributed and considerably distinct from that of the corresponding plain image; Figure 9b. Moreover, the confusion and diffusion procedures are evaluated through an examination of the correlations between the neighboring pixels in the ciphered image. The correlation analysis of two adjacent pixels in horizontal, vertical, and diagonal correlation coefficients are scattered, unpredicted and uniformly distributed contrary to adjacent pixel correlation in the plain image; Figure 9c. The computed entropy of the image source is limited than the ideal value, i.e. 7.202 and 7.235 for the face and iris plaintext respectively, so that a degree of predictability might be occurred. To be complete resistant to the entropy attacks, the calculated entropy of the secure biometric sketch is ranged from 7.994 to 8 which rounded to the ideal value. The smartest feature of deterministic chaotic systems is the random-look nature with extremely unpredictable of chaotic based systems, which could lead to various novel security applications comparing to several of conventional encryption methods, i.e. Advanced Encryption Standard (AES), Data Encryption Standard (DES), International Data Encryption Algorithm (IDEA), and Blowfish. Accordingly, from experimental results, it will be noticed that the proposed chaos based techniques and are impervious and resistant against the differential attacks compared to the classical protection schemes at sensed data level of iris and face biometrics as shown in Figs.10, Figure 11. By comparing the applied algorithms, it will be stated that conventional algorithms consume much time in template protection (i.e. encryption and decryption) mechanism especially in case of AES iris ciphering, it reached 480.465 sec., and 524.560 sec. respectively while the recommended chaotic technique introduces an imperative and much speedy ciphering methodology as shown in Figure 12.

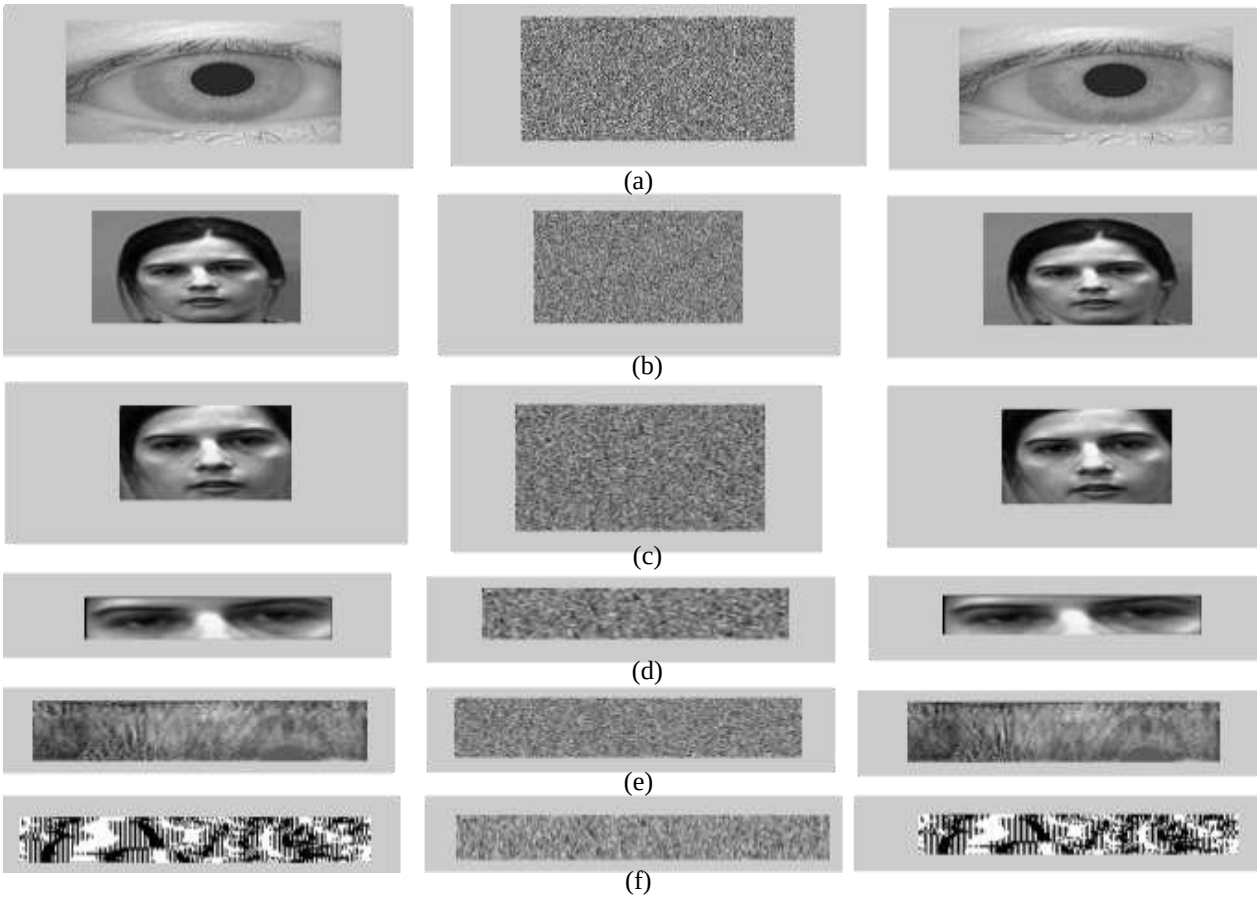

Figure 8: Results of testing template protection block as: (a) ciphering sample of the iris sensed data, (b) face sensed data, (c) detected face images, (d) detected eyes area, (e) the iris template and (f) the final iris codes.

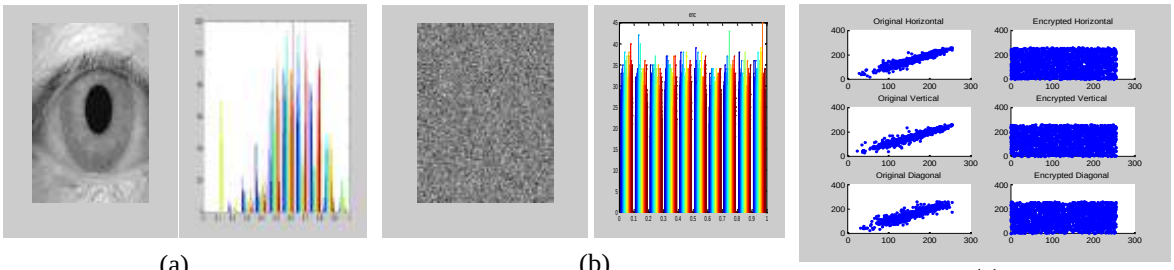

Figure 9: Sample of iris protection methodology: (a) the iris plaintext and it's corresponding histogram, (b) cipher text, and (c) the correlation analysis of two adjacent pixels.

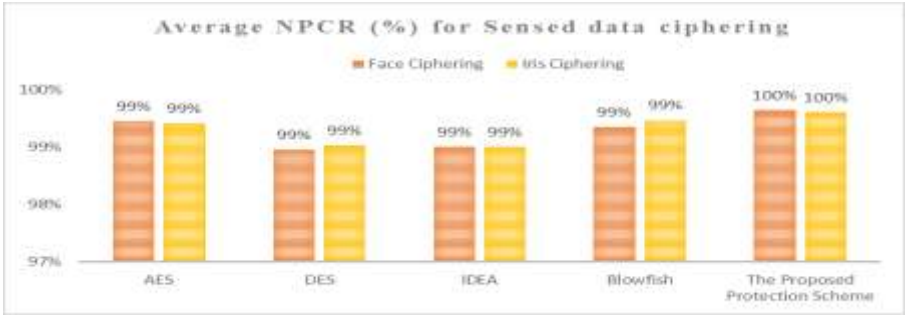

Figure 10: Average NPCR results.

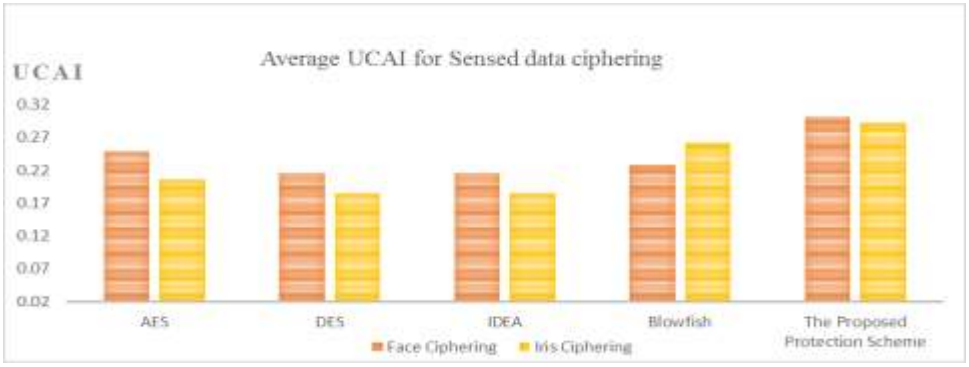

Figure 11: Average UCAI results.

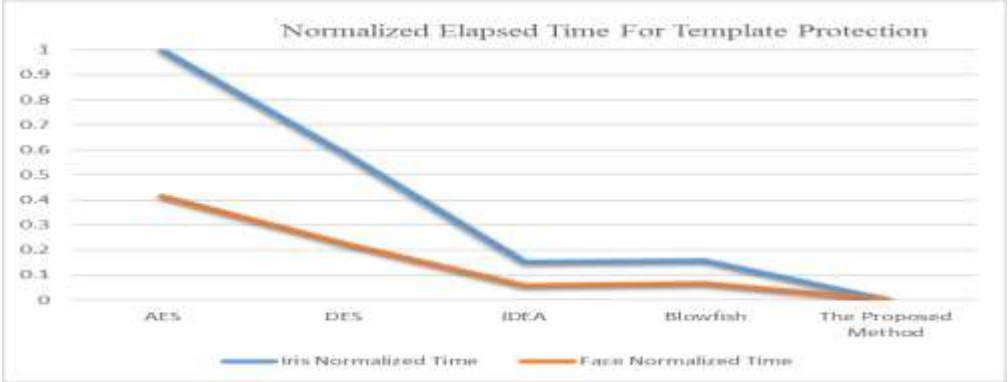

Figure 12: Normalized Elapsed template protection time.

3. RESULTS AND DISCUSSIONS

Many varied types of noise might be existent in public multimedia channels might have a momentous effect on the degradation of decrypted images quality. In order to capable of resisting different kinds of data destructions, analysis of noise attacks is one of the standards mechanisms for protection techniques evaluation. Thus, the cipher image had been imperiled to several friendly or intentional attacks at different levels (i.e., compression, noising, filtering, gamma correction, cropping, histogram equalization, and rotation). The classical encryption methods had been failed against reaching a satisfactory robustness against the accidental and malicious attacks contrary to the recommended chaotic approach. Samples of noisy iris cipher images of salt and pepper noise with different noise density levels, 0.02, 0.05, and 0.08 and their corresponding decrypted images respectively based on the proposed chaotic algorithm compared with the classical one as shown in Figure 13. Samples of attacked face cipher images with Haar and JPEG compression ratio= 50% and their corresponding decrypted images respectively are shown in Figure 14. In addition, any modification or interception of the cipher images during transmission might damage the corresponding decrypted one. The cropped images might be either in their center or on the image sides with different parameter values, which indicate the fraction of the encrypted image that has been attacked as shown in Figure 15.

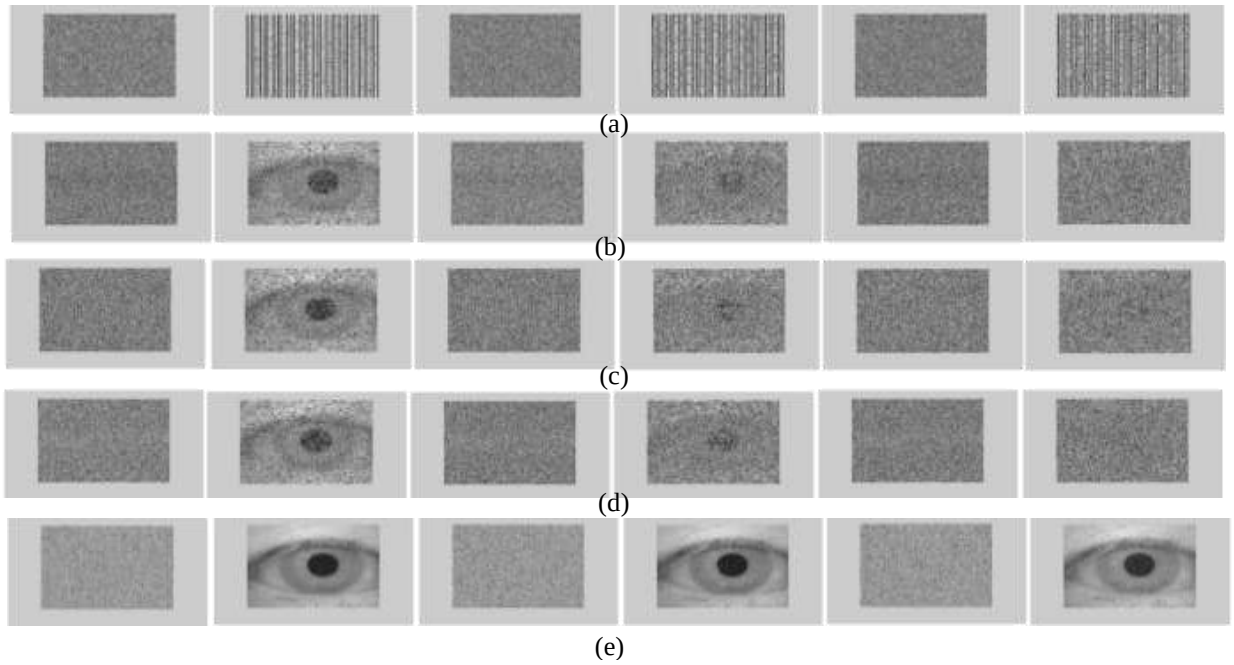

Figure 13: Samples of noisy iris cipher images of salt and pepper noise based on; (a) AES, (b) DES, (c) IDEA, (d) Blowfish, and (e) the proposed method.

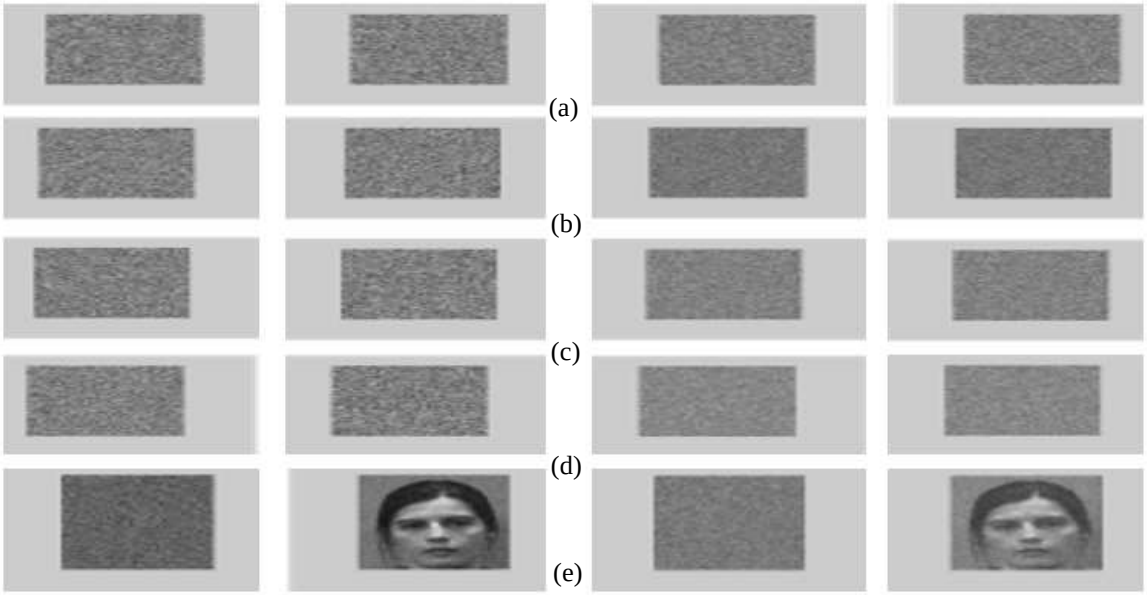

Figure 14: Samples of attacked iris ciphers with Haar and JPEG Compression with 50% compression ratio iris and its corresponding deciphered images repectively based on; (a) AES, (b) DES, (c) IDEA, (d) Blowfish, and (e) the proposed method.

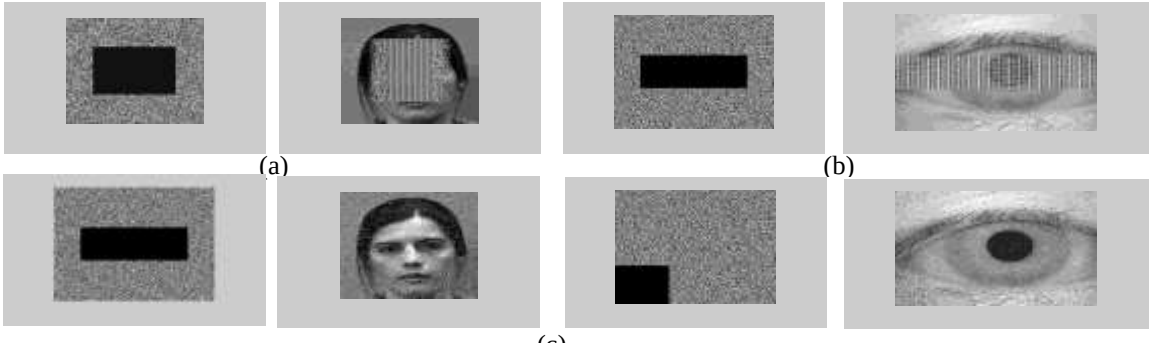

Figure 15: Samples of cropped attacked images and their corresponding decrypted images respectively based on; (a) AES, (b) Blowfish, and (c) the proposed method.

From these results, it will be concluded that the chaotic image encryption algorithms resist to the cropping attack by scattering the cropped data to the whole image while the classical one obscures the biometric data completely. Moreover, for system strength assessment, mean squared error (MSE) measures will be employed to analyze the visual quality of the decrypted images against these attacks [17]. Hence, lower MSE values are for the better algorithm with more resistance against this kind of attacks, From MSE analysis, easily it will be cleared that lower noise effects corrupted the decrypted image are offered by the proposed chaotic based method as appeared between the original sensed-face image and the decrypted images under different attacks for all encryption techniques; Figures. 16, 17. For the experimental analysis of the proposed system, the proposed locking approach prevent recovery of the original biometric data in every single stage through the whole system even if system aborting or hacking, but with the secure keys externally specified. As each information level at every interior stage (i.e. the sensed data, localized iris, detected face, normalized templates, and the extracted code) which likely being transmitted over non-secure or noisy channels will be fully secured. Moreover, with a small variation in the secret key it is not conceivable to get the private biometric template for each user. To assess the feature of control secure keys sensitivity of the recommended method, 0.0001 change had been performed in different initial values secret key and then used it to decrypt the cipher image and the results of validation is checked with correct and wrong keys. With decrypting the cipher image via utilizing the wrong key, the decrypted image is wholly dissimilar when comparing or matching with the decrypted image by employing the correct accurate key, furthermore, the original image is not able to be recovered. Thus, this is evidence that the proposed chaotic based template protection schemes could resist brute-force attack. Comparing the proposed system with other existing multimodal system, apart from not introducing the best recognition rate, the proposed method offered the lowest error rates as shown in Table 2. Moreover, providing the protected biometric templates that concealed within both biometric and encryption technologies, additional data information (i.e., security codes and control parameters) must be stored secretly. Contrary to typical encryption methods which limit the system capacity as it can be computationally expensive, the proposed system introduced a robust and fast routine for data protection without any degradation of the recognition rate. Furthermore, "strong" enough mechanism for extracting salient biometric information irrespective of some of the possible malicious attacks or noises related to the communication channel such as blurring, compression, and cropping attacks is provided. Furthermore, it has the ability to confirm the identity of the user with a high degree of confidence and privacy.

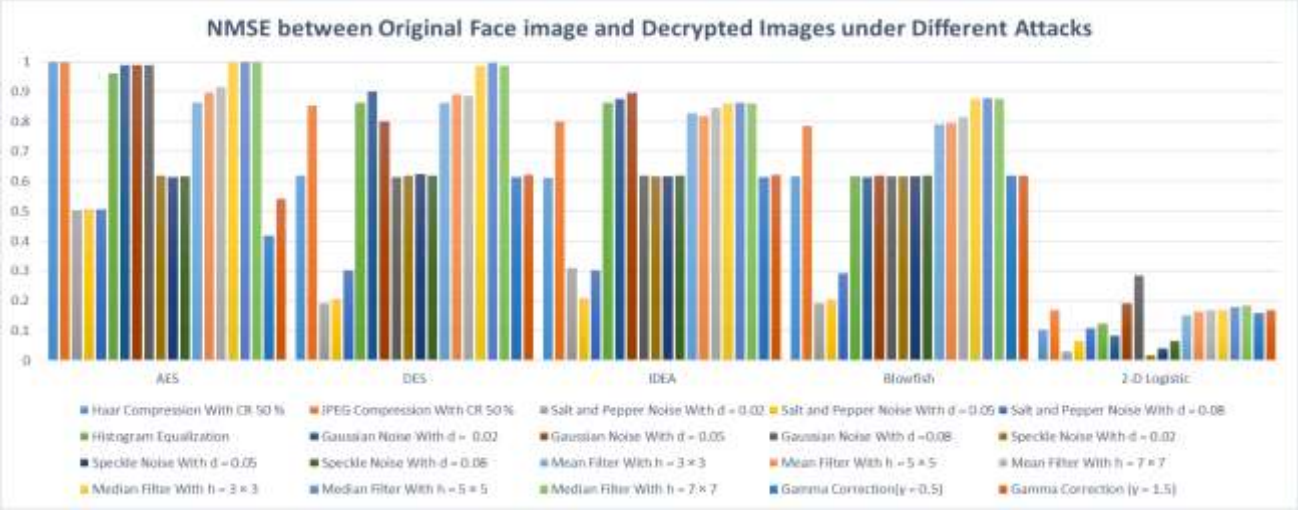

Figure 16: Normalized mean squared errors under different attacks at sensed-face data.

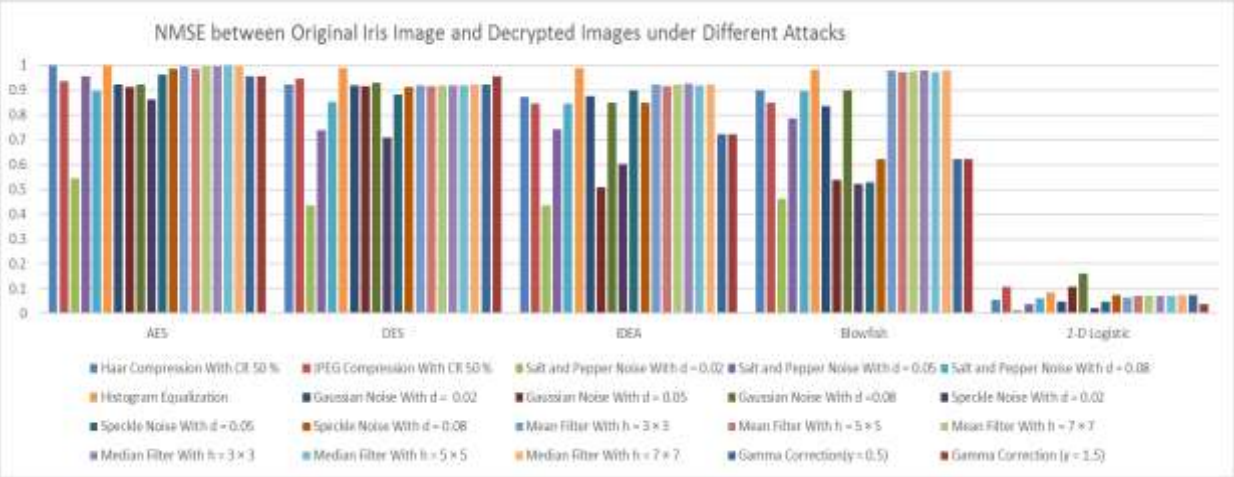

Figure 17: Normalized mean squared errors under different attacks at sensed-iris data.

Figure 18: Performance rates.

Table 2: Comparison some of existing multimodal recognition systems with the proposed system

Methods	TAR (%)	FAR(%)	FRR(%)
Kekre et al., 2011 [18]	99%	Not available	0.25
Viriri, and Tapamo, 2012 [15]	99.6%	0.08	0.01
Aboshosha et al., 2015 [19]	100%	0.54	Not available
Omid Sharifi and Maryam Eskandari, 2016 [6]	95%	Not available	Not available
The Proposed Secure Multimodal System	97%	0.03448	0.001

4. CONCLUSION

Not only the multimodal scenarios will add a higher level of the authentication performance but also their integration with the template protection schemes will combine the accuracy with the desired level of security for data transmitting and storing. The major advantages of the proposed cryptosystem over other conventional biometric system call for several applications as insufficiently long keys will be avoided. Moreover, it could offer significant advantages to enhance the privacy and security of biometric systems, providing reliable biometric authentication at a high security level. Also, the applied encryption schemes possess the properties of diversity, revocability, security, and real-time requirements. Chaotic signals have cryptographically desirable features such as high sensibility to the initial conditions, input parameters, it also possesses the prospective periodicity with high randomness furthermore its confusion properties. Thus, the proposed system achieves its main desired goal to establish a high secure authentication system for very critical applications supported with more secure database plus preserving the authentication performance rates. Especially, the 2D Baker map, which considered as an extension of 1D Baker map, increased the key space and the control parameters dependency towards more secret information through exhibiting a greater amount of chaotic behavior for sequence creation. Moreover, the data stream is generated using 2D Henon map permuted the organization of pixels of the image generated shuffled version of the image to introduce unrelated version to the source even a huge data as in the case of iris ciphering. The NPCR and UACI scores showed that proposed version is very sensitive to any slighter change in the plain-image. Moreover, the scrambled images could be recovered when subjected to noisy environments like intensity

variations and filtering which fails in almost traditional methods. From experimental tests through constructing the template protection module, it could be concluded that all the traditional encryption schemes like DES, IDEA, and AES had been proved to be inappropriate for Crypto-biometrics security system applications; this is because of intrinsic features of biometric data, plus high complexity, long keys, and much time consuming for those methods. During the proposed fuzzy fusion method at matching score level, the generated results from both iris and face matchers are not be homogeneous. In the proposed system, Min-max technique for score normalization into a comparable domain had been applied. The role of final decisions in authentication process which had been taken according to the confidence level of the defuzzification procedure, had a great effect on reducing both the FAR and FRR besides increasing the complete system accuracy and evading both override and replay attacks. Typically, it is perceived that the entropy of biometric templates is low. However, the average entropy of cipher templates stored in databases is close to the ideal value. After data locking, the ciphered biometric template stored in database at every point of probable attacks. One of the fundamental challenges of the proposed system is the timing issues of templates protection, which had been obviated using the recommended chaotic approach. From system experimentations, it had been proved that the chaotic based encryption possessing high security and robustness against numerous cryptanalytic attacks, plus they outperform deservedly in both timing and throughput issues. Moreover, it could fairly resolve the predicaments occurring due to cropping and plain image rotation. Furthermore, the fuzzy logic based fusion, could introduce an impressive information fusion approach, which provides a greater degree of privacy and security integration with user accessibility.

5. REFERENCES

[1] D. T. Meva, "Comparative Study of Different Fusion Techniques in Multimodal Biometric Authentication," vol. 66, no. 19, pp. 16–19, 2013.

[2] A. Ross and R. Govindarajan, "Feature level fusion using hand and face biometrics," *Proc. SPIE - Int. Soc. Opt. Eng.*, vol. 5779, no. March, pp. 196–204, 2005.

[3] J. Bigün, G. Chollet, and G. Borgefors, Eds., *Audio- and Video-based Biometric Person Authentication*, vol. 1206. Berlin, Heidelberg: Springer Berlin Heidelberg, 1997.

[4] H. Benaliouche and M. Touahria, "Comparative study of multimodal biometric recognition by fusion of iris and fingerprint," *Sci. World J.*, vol. 2014, 2014.

[5] J. I. A. N. Q. Gao, L. I. Y. A. Fan, L. I. Li, and L. I. Z. Xu, "A PRACTICAL APPLICATION OF KERNEL – BASED FUZZY DISCRIMINANT ANALYSIS," vol. 23, no. 4, pp. 887–903, 2013.

[6] O. Sharifi and M. Eskandari, "Optimal Face-Iris Multimodal Fusion Scheme," *Symmetry (Basel).*, vol. 8, no. 6, p. 48, 2016.

[7] H. Y. liu Yang, yue Xue Dong, Liu Ying Fei, "Iris Recognition System Based on Chaos Encryption," *2010 Int. Conf. Comput. Des. Appliations (ICCDA 2010)*, vol. 1, no. Iccda, pp. 537–539, 2010.

[8] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric Template Security," *EURASIP J. Adv. Signal Process*, vol. 2008, no. January, p. 113:1--113:17, 2008.

[9] F. Hao, R. Anderson, and J. Daugman, "Combining crypto with biometrics effectively," *IEEE Trans. Comput.*, vol. 55, no. 9, pp. 1081–1088, 2006.

[10] M. A. M. Abdullah, S. Dlay, W. Woo, and J. Chambers, "A Framework for Iris Biometrics Protection: A Marriage between Watermarking and Visual Cryptography," *IEEE Access*, vol. 3536, no. c, pp. 1–1, 2016.

[11] C. A. of S. Institute of Automation, "CASIA iris image database," 2004. [Online]. Available: http://biometrics.idealtest.org/dbDetailForUser.do?id=1. [Accessed: 25-Jan-2017].

[12] M. M. Eid, M. A. Mohamed, and M. A. Abou-El-Soud, "Development of Iris Security System Using Adaptive Quality-Based Template Fusion," in *Intelligent Data Analysis and Applications: Proceedings of the Second Euro-China Conference on Intelligent Data Analysis and Applications, ECC 2015*, A. Abraham, X. H. Jiang, V. Snášel, and J.-S. Pan, Eds. Cham: Springer International Publishing, 2015, pp. 265–278.

[13] "Face Recognition Data." [Online]. Available: http://cswww.essex.ac.uk/mv/allfaces/faces94.html. [Accessed: 03-May-2017].

[14] M. A. Mohamed, M. E. Abou-Elsoud, and M. M. Eid, "Automated face recogntion system: Multi-input databases," in *The 2011 International Conference on Computer Engineering & Systems*, 2011, pp. 273–280.

[15] S. Viriri and J. R. Tapamo, "Integrating iris and signature traits for personal authentication using user-specificweighting," *Sensors*, vol. 12, no. 4, pp. 4324–4338, 2012.

[16] H. G. Schuster, *Deterministic Chaos*. 2005.

[17] G. Ye and X. Huang, "A secure image encryption algorithm based on chaotic maps and SHA-3," *Secur. Commun. Networks*, vol. 9, no. 13, p. n/a-n/a, 2016.

[18] H. B. Kekre, V. A. Bharadi, V. I. Singh, V. Kaul, and B. Nemade, "Hybrid Multimodal Biometric Recognition using Kekre ' s Wavelets , 1D Transforms & Kekre ' s Vector Quantization Algorithms Based Feature Extraction of Face & Iris," pp. 29–34, 2011.

[19] A. Aboshosha and K. A. El Dahshan, "Score Level Fusion for Fingerprint , Iris and Face Biometrics," vol. 111, no. 4, pp. 47–55, 2015.