Nonlinear Dynamics and Systems Theory, **13** (1) (2013) 55–68

Double Hyperchaotic Encryption for Security in Biometric Systems

E. Inzunza-González[1] and C. Cruz-Hernández[2*]

[1] *Faculty of Engineering, Architecture and Design, Baja California Autonomous University (UABC), Km. 103 Carret. Tijuana-Ensenada, Ensenada, B.C., 22860, México.*
[2] *Electronics and Telecommunications Department, Scientific Research and Advanced Studies of Ensenada (CICESE), Carretera Ensenada-Tijuana No. 3918, Zona Playitas, 22860 Ensenada, B.C. México.*

Received: November 12, 2012; Revised: January 21, 2013

Abstract: In this paper, a novel method for double image encryption is proposed by using different hyperchaotic maps. The proposed algorithm is implemented in a biometric system. In particular, for face pattern recognition, the eigenfaces approach is used, and to encrypt biometric information the Rössler and Chen hyperchaotic maps are exploited. The simulation and experimental results show that the security analysis performed to the double encryption algorithm implemented, is strong against known different attacks, such as: brute force, statistical, differential, and information entropy. Therefore, the proposed double encryption algorithm is suitable for use in biometric systems based on face recognition which operate remotely.

Keywords: *chaotic encryption; hyperchaotic maps; biometric systems; eigenface; face recognition; information security.*

Mathematics Subject Classification (2010): 68P25, 94A60, 11T71, 14G50, 68T10.

[*] Corresponding author: mailto:ccruz@cicese.mx

1 Introduction

A facial recognition system is an application run by computer to automatically identify a person from a digital image, by comparing selected facial features from a digital image or a frame from a video source. One way to do this is by comparing selected facial features with a facial image database, see Figure 1. The face recognition systems have less uniqueness than recognition systems based on fingerprint and iris, however, provides a more direct form of identification, friendly and is more acceptable compared with other biometric personal identification systems [32]. Therefore, research on face recognition has become one of the most important issues in biometric systems.

The first semi-automated system for face recognition required the administrator to located features (such as eyes, ears, nose, and mouth) on the photographs before it calculated distances and ratios to a common reference point, which were compared with reference data. Goldstein *et al.* [14] used 21 specific subjective markers such as hair and lip thickness to automate the recognition. The problem was that the measurements and locations were manually computed.

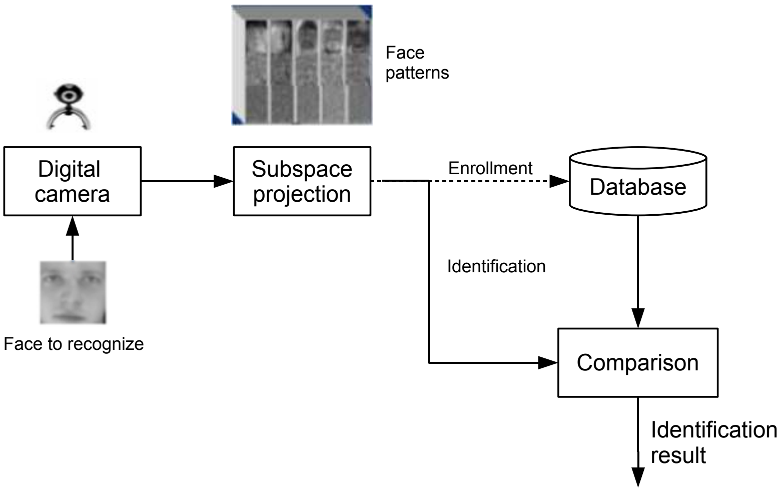

Figure 1: Scheme of a general biometric system based on face image.

On the other hand, the idea of using eigenfaces was motivated by a technique developed by Sirovich and Kirby in [28] and by Kirby and Sirovich in [19] for efficiently representing pictures of faces by using *Principal Components Analysis (PCA).* They argued that a collection of face images can be approximately reconstructed by storing a small collection of weights for each face and a small set of standard pictures. PCA method reported in [28] and [19] is also called *eigenfaces* by Turk and Pentland in [29, 30], this appearance-based technique is used widely for the dimensionality reduction and recorded a great performance in face recognition. PCA is a standard linear algebra technique, to the face recognition problem [28]. This was considered somewhat of a milestone as it showed that less than one hundred values were required to accurately code a suitably aligned and normalized face image [28]. Turk and Pentland discovered that while using the eigenfaces technique, the residual error could be used to detect faces in images [29,30].

This was a discovery that enabled reliable real-time automated face recognition systems. Although the approach was somewhat constrained by environmental factors, it nonetheless created significant interest in furthering development of automated face recognition technologies. Among the most important methods for face recognition are: eigenface [32], fisherface [7], dual eigen space [32], and neural networks [20].

Current literature reports many techniques for human face recognition, see e.g. [7, 14, 16, 19, 20, 25, 28–30, 32], on the other hand, there are many works about image encryption algorithms based on chaos for secure communications, see e.g. [1–3,6,9,10,21,24]. Recently, encryption in biometric systems has been applied, see e.g. [4, 5, 8, 15, 18, 22] with the purpose of protecting biometric information. Nevertheless, to our knowledge, any approach of a secure biometric system, particularly about face patterns recognition that works remotely with double hyperchaotic encryption has not been reported. Hyperchaotic maps are theoretically proofed with good randomness, infinite period, and unpredictability on long term [11]. These complex maps are usually defined as a system characterized at least by two positive Lyapunov exponents which provide more complex waveforms than simply chaotic maps. Consequently, these hyperchaotic maps have the characteristics of high capacity, high security, and high efficiency [11].

The aim of this paper, is to improve the security encryption in a biometric system based on human face recognition. In particular, we use a double hyperchaotic encryption in a face recognition system which works remotely, the eigenface method to get the face patterns is used, see e.g. [7, 29, 30, 32], next, Rössler and Chen hyperchaotic maps to encrypt face patterns are used. In this work, the proposed secure biometric system, is similar to the reported in [22], but there are fundamental differences with respect to that work: (1) they encrypt iris templates by using the generalized Hénon map and 1D logistic map. In this paper, the Rössler and Chen hyperchaotic maps for face pattern double encryption are used; (2) they used in the quantizer a threshold equal to 0.5, however, we optimize the threshold to improve security; (3) they extracted iris features, in this work we extract face patterns; (4) for features extraction they used a test of statistical independence reported in [12], we use eigenface method reported in [29, 30]; (5) they only reported brief analysis on sensitivity of initial conditions. Nevertheless, we provide a complete security analysis.

The organization of this paper is as follows: In Section 2, a brief review on eigenfaces approach is given. In Section 3, the proposed algorithm to encrypt and decrypt is described. In Section 4, the main results of this work are presented. The paper is concluded with some remarks in Section 5.

2 Review on Eigenfaces Approach

PCA approaches include two phases: enrollment and identification (see Figure 1). In the enrollment phase, an eigenspace is established from the training samples by using PCA and the training face images are mapped to the eigenspace for identification. In the identification phase, an input face is projected to the same eigenspace and identified by an appropriate classifier. For details of this method, see e.g. [29, 30, 32]. The approach for face recognition involves the following initial operations:

1. Acquire an initial set of face images (the training set).

2. Calculate the eigenfaces from the training set, keeping only M images that correspond to the highest eigenvalues. These M images define the face space. As new

faces are experienced, the eigenfaces can be updated or recalculated.

3. If it is a face, classify the weight pattern as either a known person or as unknown.
4. Update the eigenfaces and/or weight patterns (optional).
5. If the same unknown is seen several times, calculate its characteristic weight pattern and incorporate into the known faces (optional).

2.1 Calculating eigenfaces

A human face image can be considered as a stochastic sample, and each face image is considered as a higher dimensional vector and each pixel corresponds to a component. If all the face images lie in the same subspace of the higher dimensional space, this subspace is a good representation of face images because it shows the common features of faces. So, detection of faces is to find the subspace.

Suppose $A = [a_{ij}]_{r\times c}$ as a human face image, where r and c are the number of rows and columns of the images, respectively; a_{ij} is the gray value of the pixel in *i-th* row and *j-th* column. Re-arrange a_{ij} and make it a column vector

$$x^i = [a_{11}\ a_{21}\ ...\ a_{r1}\ a_{12}\ a_{22}\ ...\ a_{r2}\ ...\ a_{1c}\ a_{2c}\ ...\ a_{rc}]^T, \tag{1}$$

where x^i is a *D-dimensional* vector, $D = r \times\ c$.

Next, the images are *mean centered* by subtracting the mean image from each image vector,

$$\overline{x}^i = x^i - m, \tag{2}$$

where m is the average vector of the training specimens set, and is given by

$$m = \frac{1}{M}\sum_{i=0}^{M-1} x^i. \tag{3}$$

Vectors from Eq. (2) are combined side by side to create a data matrix of size $D \times M$, where M is the number of images in the training specimens set,

$$\overline{X} = \left\{\ \overline{x}^1 \mid \overline{x}^2 \mid ... \mid \overline{x}^P\ \right\}, \tag{4}$$

the covariance matrix can be calculated as

$$\Omega = \overline{X} \cdot \overline{X}^T. \tag{5}$$

This covariance matrix has up to d eigenvectors associated with non-zero eigenvalues, assuming $d < D$.

Let $\lambda_1, \lambda_2, ..., \lambda_d$ ($\lambda_1 \geqslant \lambda_2 \geqslant ... \geqslant \lambda_d > 0$) and $u_1, u_2, ..., u_d$ be eigenvalues and corresponding eigenvectors of the covariance matrix Ω, respectively. So, every human face image, x^i, can be represented by the linear combination of the eigenvectors. According to the algebra theory, we know that $u_1, u_2\ , ..., u_d$ will be orthogonal one another and unit vector. Usually, $M < D$, can be satisfied because D is larger than the number of the specimens. Then $d < D$ is derived. In other words, the given human face image can be represented by fewer base vectors (d vectors) [32].

Some values λ_i, in d eigenvalues are very small, whose corresponding eigenvectors give little contribution to represent the face image specimens, hence they can be ignored. Thus, we sort the eigenvectors according to the decreasing eigenvalues, and select the top k eigenvectors to represent the specimens [32].

If we choose k as a very big number, for example $k = d$. But we know some eigenvectors have little contribution to face space. On the contrary, if we select k as a very small number, for example $k = 1$, then the subspace is not sufficient to represent the face image specimens. Usually, we can select the smallest k which satisfies the following expression [32]

$$\frac{\sum\limits_{i=0}^{k} \lambda_i}{\sum\limits_{i=0}^{M-1} \lambda_i} \geqslant \alpha, \tag{6}$$

where α is a real number, which is close to 100%, such as 99%. It states that the top k axes have 99% energy of all axes.

2.1.1 Ordering eigenvectors

Order the eigenvectors $u_i \in U$ according to their corresponding eigenvalues λ_i from high to low. Keep only the eigenvectors associated with non-zero eigenvalues. This matrix of eigenvectors is the eigenspace U, where each column of U is an eigenvector,

$$U = [\, u_1 \mid u_2 \mid \cdots \mid u_d \,]. \tag{7}$$

2.1.2 Projecting training images

To project the training images, each of the centered training images from Eq. (2) must be projected into the eigenspace. To project an image into the eigenspace, we need to calculate the dot product of the image with each of the ordered eigenvectors from Eq. (7) as follows,

$$\widetilde{x}^{\,i} = U^{T} \overline{x}^{i}. \tag{8}$$

Therefore, the dot product of the image and the first eigenvector will be the first value in the new vector. The new vector calculated from Eq. (8) of the projected image must contain the same values as eigenvectors.

2.1.3 Identifying test images

Each test image is first mean centered by subtracting the mean image, and is then projected into the same eigenspace defined by U as follows,

$$\overline{y}^{\,i} = y^{i} - m, \tag{9}$$

where m is calculated from Eq. (3), and $\overline{y}^{\,i}$ is the centered test image.

Then project this centered test image according to

$$\widetilde{y}^{i} = U^{T}\, \overline{y}^{\,i}. \tag{10}$$

The projected test image ($\widetilde{y}^{\,i}$) is compared to every projected training image and the training image that is found to be nearest to the test image is used to identify the input image (test images).

These images can be compared by using any number of similarity measures, the most common is the L_2 norm or Euclidian distance as follows,

$$\varepsilon^2 = \left\|\widetilde{y}^{\,i} - \widetilde{x}^{\,k}\right\|_2 , \tag{11}$$

where $\widetilde{x}^{\,k}$ is a vector describing the k^{th} face class. A face is classified as belonging to class k when the minimum ε is below some chosen threshold θ_ε. Otherwise the face is classified as “unknown”.

3 Encryption and Decryption Algorithm

3.1 Double encryption algorithm

The Rössler hyperchaotic map is described by the following equations [2]:

$$\begin{aligned} x_1(k+1) &= \alpha x_1(k)(1-x_1(k)) - \beta(x_3+\gamma)(1-2x_2(k), \\ x_2(k+1) &= \delta x_2(k)(1-x_2(k)+\zeta x_3(k), \\ x_3(k+1) &= \eta((x_3(k)+\gamma)(1-2x_2(k))-1)(1-\theta x_1(k)), \end{aligned} \tag{12}$$

with parameters $\alpha = 3.8$, $\beta = 0.05$, $\gamma = 0.35$, $\delta = 3.78$, $\zeta = 0.20$, $\eta = 0.10$, $\theta = 1.9$, and initial conditions: $x_1(0) = 0.10$, $x_2(0) = 0.15$, and $x_3(0) = 0.01$; the map (12) exhibits hyperchaotic dynamics [2]. Figure 2 shows the hyperchaotic attractor generated by the Rössler map projected on the (x_1, x_2, x_3)-plane.

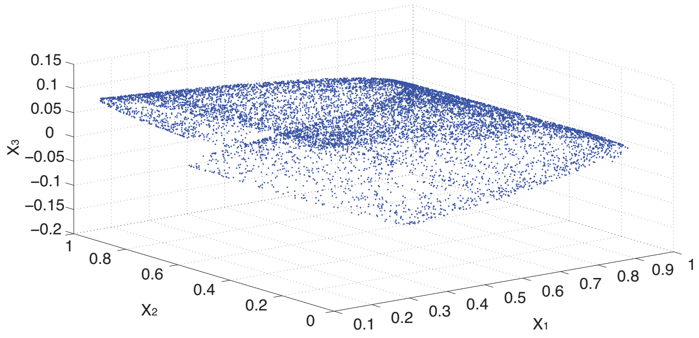

Figure 2: Hyperchaotic attractor generated by Rössler map (12).

On the other hand, the Chen hyperchaotic map is described by the following equations [1]:

$$\begin{aligned} x_1(k+1) &= 1 - a(x_1^2(k) + x_2^2(k)), \\ x_2(k+1) &= -2abx_1(k)x_2(k), \end{aligned} \tag{13}$$

with parameters $a = 1.95$ y $b = 1$, and initial conditions: $x_1(0) = 0.025$ and $x_2(0) = 0.025$; the map (12) exhibits hyperchaotic dynamics [1]. Figure 3 shows the

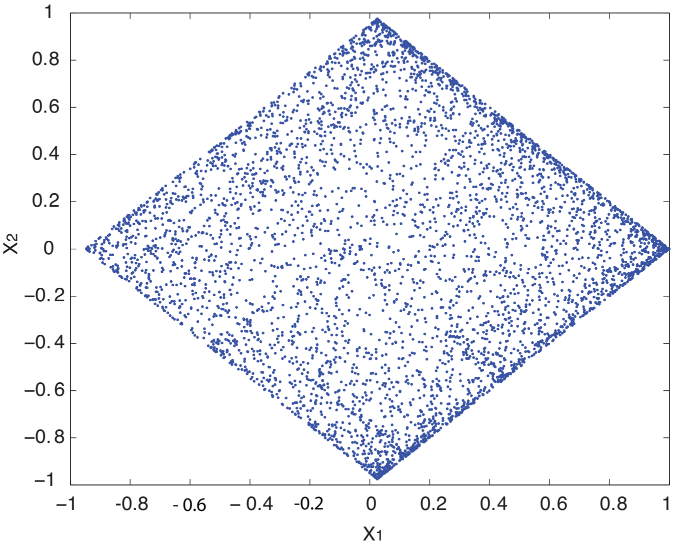

Figure 3: Hyperchaotic attractor generated by Chen map (13).

hyperchaotic attractor generated by the Chen map projected on the (x_1, x_2)-plane.

The proposed double encryption scheme in this work to encrypt face patterns is shown in Figure 4. Where the inputs to the scheme are the face patterns and initial conditions as encryption key for the hyperchaotic maps Eq. (12) and (13). Later, the face pattern is converted to binary secuence, and then the two X-OR operation is performed with the generated hyperchaotic signal by Rössler map, prior to operating X-OR, the hyperchaotic signal, also has to be digitized, this is done by using a quantizer. In the quantizer a threshold can be established between 0 and 1, for example in [22] 0.5 was used for the Hénon map. When the amplitude of the hyperchaotic signal is greater than or equal to 0.5, the output of the quantizer is at a higher level, whereas when the amplitude of the hyperchaotic signal is less than 0.5, the quantizer output is at a low-level. In this work, the threshold was optimized to obtain the best entropy and therefore better security levels, so the best threshold for Rössler and Chen hyperchaotic map are 0.59 and 0.14 respectively. Then, the result of the X-OR operation between the digitized face pattern and the hyperchaotic signals in binary format, also is a binary signal called encrypted face pattern, which is sent through a public network.

3.2 Double decryption algorithm

Figure 5 shows the double decryption scheme, to recover the original face pattern at the receiver end, the reverse process of encryption must be followed, i.e., it receives the encrypted face pattern and introduces the same key used for the encryption (the same initial conditions of the two hyperchaotic maps). Similarly, the generated hyperchaotic signal, is applied to a quantizer to be converted to a binary format, the threshold of the quantizer has to be the same as the two used to encrypt the face pattern. Then apply the two X-OR operation between the encrypted face pattern and hyperchaotic binary signals. The result of this operation is also a string of bits, then these bits are grouped

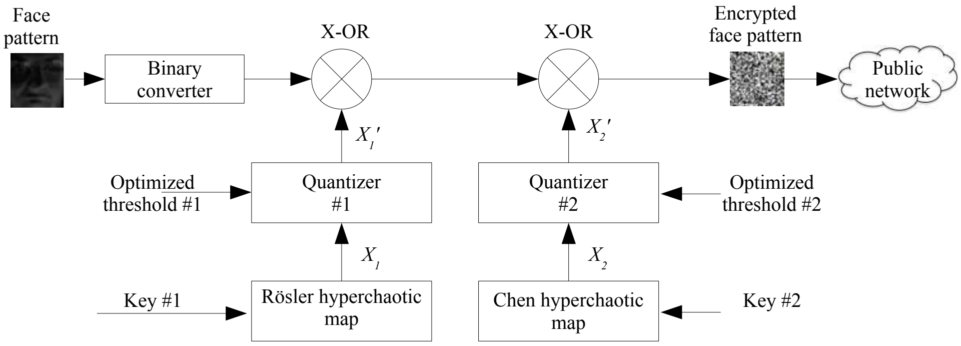

Figure 4: Double encryption scheme for face patterns.

into 8 bits to form the corresponding level of gray of each pixel, lastly it rebuilds the image of the recovered face pattern.

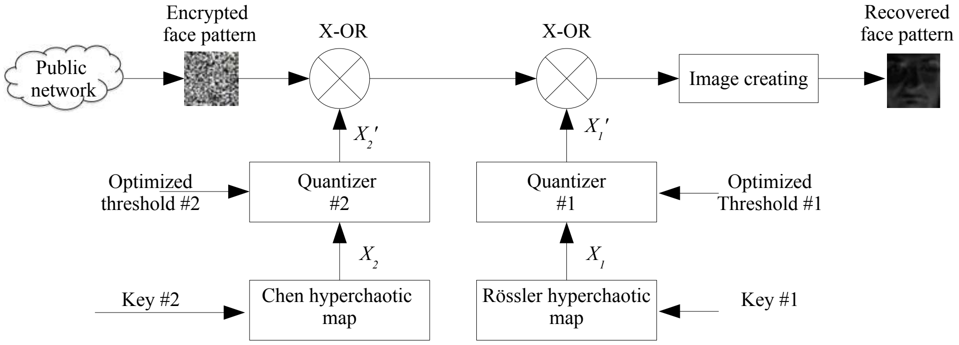

Figure 5: Double decryption scheme for recovered face patterns.

4 Results

4.1 Security analysis

4.1.1 Key space analysis

The key of the proposed cryptosystem consists of two parts: a) the initial conditions of the two hyperchaotic maps (Rössler and Chen), (b) the control parameters of these maps. Thus, there are five initial conditions and nine parameters in our algorithm. According to the IEEE standard for floating point arithmetic [17], the computational precision of 64 bits numbers is 1×10^{-16}, so the secret key's space is $10^{16} \times 10^{16} \times 10^{16} \times 10^{16} \times 10^{16} \times 10^{16} \times 10^{16} \times 10^{16} \times 10^{16} \times 10^{16} \times 10^{16} \times 10^{16} \times 10^{16} \times 10^{16} = 10^{224}$, therefore in a binary system it is equal to 2^{744}, so the secret key's space is large enough to resist exhaustive attack.

4.1.2 Statistical analysis

Figure 6(a) shows the face pattern #1 and the Figure 6(d) shows its corresponding histogram, this pattern was encrypted by using the Rössler and Chen hyperchaotic maps and approach explained in Section 3. Figure 6(b) shows the encrypted face pattern with different maps using the initial conditions as an encryption key: $x_1(0) = 0.10$, $x_2(0) = 0.15$, $x_3(0) = 0.01$ and $x_1(0) = 0.025$ and $x_2(0) = 0.025$ of Rössler and Chen maps, respectively. The optimized threshold for quantizing the state x_1 of the Rössler map is 0.59, while the optimized threshold for quantizing the state x_2 of the Chen map is 0.14. Figure 6(e) shows its corresponding histogram, we can see, in the histogram from the original image 6(d), that most of the information is concentrated among the pixels that are in the range of gray level between 0 and 100. While in the histogram in Figure 6(e) the information is distributed over the entire range from 0 to 255 of the grayscale level, therefore, we can say that the system is robust against statistical attacks. Figure 6(c) shows the recovered face pattern at the receiver end, and Figure 6(f) shows its corresponding histogram, we can see that both, the recovered face pattern and the histogram are equal to the original pattern, therefore recovering 100% of the original information.

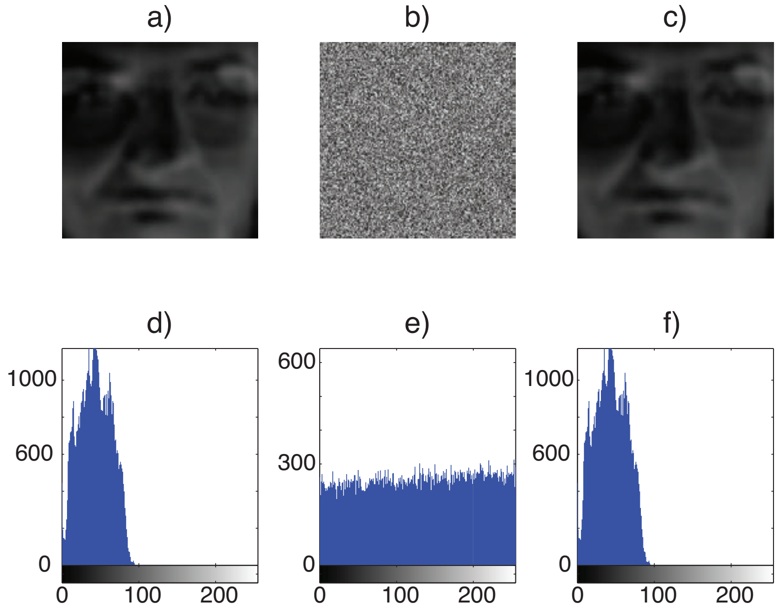

Figure 6: Top: (a) Original face pattern, (b) Encrypted face pattern, (c) Recovered face pattern. Bottom: (d) Histogram of the original face pattern, (e) Histogram of the face pattern, (f) Histogram of the recovered face pattern.

4.1.3 Correlation analysis of adjacent pixels

Shannon proposed two techniques based on the design of encrypters [26,27], the *diffusion* and *confusion*, these two properties above can be demonstrated by a test correlation of adjacent pixels in the encrypted image [9]. The correlation between two adjacent pixels was examined horizontally, vertically and diagonally. To do this, we randomly selected 2025 pairs of pixels (x_i, y_i) of the image pattern under analysis (original or encrypted), generated by scattering graphics with these pairs of adjacent pixels, i.e., the pixel is plotted x_i vs y_i. Then their corresponding correlation coefficients (r_{xy}) are calculated [9] by using the next expression,

$$r_{xy} = \frac{cov(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{14}$$

with

$$cov(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)), \tag{15}$$

where $cov(x,\ y)$ is the covariance, $D(x)$ is the variance, x and y denote the scale values of gray level in the image pattern under analysis. For this numerical case, the following discrete forms were used:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i, \tag{16}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))), \tag{17}$$

where $E(x)$ is the average gray levels of pixels.

Figure 7(a) shows the correlation distribution of two adjacent pixels in horizontal direction of the original face pattern. Using Eq. (14), we obtain the correlation coefficient of 0.9976. Figure 7(b) shows the correlation distribution of two adjacent horizontal pixels from the encrypted face pattern, in the same way, using (14) to compute the correlation coefficient, which is -0.0082. Table 1 shows the horizontal, vertical and diagonal correlation coefficients of adjacent pixels in the original face pattern and in the encrypted face pattern. From the results of Table 1, we find that the correlation coefficients of the encrypted face pattern are close to zero, it can clearly be seen that our algorithm can destroy the relativity effectively; the proposed image encryption algorithm has a strong ability to resist statical attack.

Table 1: Correlation of adjacent pixels in the original face pattern and in the encrypted face pattern.

Pixels	**Original face pattern**	**Encrypted face pattern**
Horizontal	0.9976	-0.0082
Vertical	0.9986	0.0073
Diagonal	0.9961	0.0089

4.1.4 Differential attacks

To perform an analysis against differential attacks [9] and understand the differences between encrypted images, two measures in common are used, NPCR (Number of Pixels

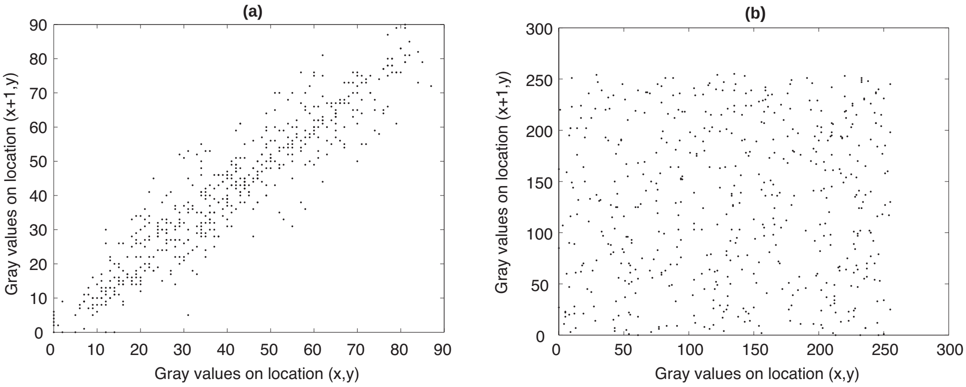

Figure 7: Correlations of two horizontally adjacent pixels in the original image and in the ciphered image: (a) Original face pattern, (b) Encrypted face pattern.

Change Rate) and UACI (Unified Average Changing Intensity). These measures are used to test the influence of change of a pixel in the whole encrypted pattern.

Number of pixels change rate (NPCR) Measures the percentage of the number of different pixels between two encrypted image patterns and can be calculated by using the following expression [9, 24],

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\%, \tag{18}$$

where $D(i,j)$ is a binary arrangement, so that:

$D(i,j) = 0$, if $C_1(i,j) = C_2(i,j)$,
$D(i,j) = 1$, where $C_1(i,j \neq C_2(i,j)$,

C_1 and C_2 are encrypted image patterns obtained with keys (initial conditions) that are very similar. W and H define the size of the image under analysis.

Unified average changing intensity (UACI) Measures the average intensity differences between two encrypted images (C_1 and C_2) by the expression [9, 24],

$$UACI = \frac{1}{W \times H} \sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100\%, \tag{19}$$

where C_1, C_2, W, and H were computed previously.

To realize the analysis against differential attacks, very similar keys are used to encrypt the original face pattern. In this case, the first encryption keys used for Rössler map are $x_1(0) = 0.10$, $x_2(0) = 0.15$, and $x_3(0) = 0.01$, for Chen map are $x_1(0) = 0.025$ and $x_2(0) = 0.025$, also we used the same parameters described in Section 3 for Rössler and Chen maps, so with these keys we obtain the encrypted face pattern C_1, the following keys used for Rössler map are $x_1(0) = 0.10 + 1e^{-10}$, $x_2(0) = 0.15$, and $x_3(0) = 0.01$, for Chen map are $x_1(0) = 0.025$ and $x_2(0) = 0.025$, also we used the same parameters described in Section 3, so we obtain the encrypted face pattern C_2. Using expressions

(18) and (19), we obtain $NPCR = 99.71\%$ and $UACI = 34.26\%$. These results show that the encryption algorithm is strong against differential attacks, because the $NPCR$ is approximate the ideal value of 100% and $UACI$ is slightly higher than 33%.

4.1.5 Information entropy

Shannon [26, 27] introduced the mathematic fundamentals of the information theory applied to communications and data storage. The information entropy is a criterion that shows the randomness of the data. In addition, it can be used to evaluate the security of encryption [31]. To calculate the entropy $H(s)$ [6] from a source (s), we have

$$H(s) = \sum_{i=0}^{2^N-1} P(s_i) \cdot Log_2(\frac{1}{P(s_i)})\ bits, \tag{20}$$

where $P(s_i)$ represents the probability of the symbol s_i.

For a purely random source, which is emitting 2^N symbols with same probability, after evaluating Eq. (20), we have an entropy $H(s) = N$, in this case, encrypted images with completely random pixels in 8 bit grayscale, have entropy $H(s) = 8$ bits. When images of patterns are encrypted, ideally its entropy must be 8. When a cryptographic system emits symbols with entropy less than 8, the encrypter has some degree of predictability, so its security is set at risk [6].

To evaluate the information entropy, from the algorithm of hyperchaotic encryption used in this paper, Eq. (20) was used. First, we calculate the probability of occurrence of each symbol (pixel), with the help of the corresponding histogram of the encrypted face pattern. In the case, of the encrypted face pattern obtained with the encryption keys $x_1(0) = 0.10$, $x_2(0) = 0.15$, and $x_3(0) = 0.01$, the entropy calculated is $H(s_i) = 7.9956$. This is a good result, because it is near (similar) to its ideal value of 8.

5 Conclusion

In this paper, we have applied double hyperchaotic encryption to face patterns in a biometric system, particularly in face recognition system which operates remotely and uses eigenface approach, this was for illustrative purposes, but other methods can be implemented easily. The double encryption algorithm presents an extremely large key space and very good statistical properties, so it effectively resists statistic attacks. Also, it has a high sensitivity to withstand differential attacks. Therefore, because the algorithm used in this work has a high security level, it can be suggested to encrypt confidential biometric information (face, iris, fingerprint, palmprint, retina, hand geometry, and facial thermogram, etc.), that will be transmitted securely through a public network, such as the internet. As future work, we propose to use 3D Discrete Generalized Hénon Map [13] and quantum dynamics [23] to encrypt biometric information.

Acknowledgment

This work was supported by CONACYT, Mexico under Research Grants No. 166654.

References

[1] Aguilar Bustos, A.Y. and Cruz-Hernández, C. Synchronization of discrete time hyperchaotic systems: An application in communications. *Chaos, Solitons and Fractals* **41**(3) (2009) 1301–1310.

[2] Aguilar Bustos A.Y., Cruz-Hernández C., López-Gutiérrez R. M. and Posadas Castillo C. Synchronization of Different Hyperchaotic Maps for Encryption. *Nonlinear Dynamics and Systems Theory* **8**(3) (2008) 221–236.

[3] Aguilar Bustos A.Y., Cruz-Hernández C., López-Gutiérrez R. M., Tlelo Cuatle E. and Posadas Castillo. C. Hyperchaotic Encryption for Secure E-mail Communication. In: *Emergent Web Intelligence, Advanced Information Retrieval.* Springer, London, 2010, 471–486.

[4] Anil K. J., Karthik N. and Abhishek N. Biometric Template Security. *EURASIP Journal on Advances in Signal Processing* **2008**(1) 1–17.

[5] Anil, K. J. and Umut Uludag. Hiding Fingerprint Minutiae in Images. In: *Third Workshop on Automatic Identification Advanced Technologies (AutoID).* IEEE, Tarrytown, New York, 2002, 97–102.

[6] Behnia S., Akhshani A., Mahmodi H. and Akhavan A. A novel algorithm for image encryption based on mixture of chaotic maps. *Chaos, Solitons and Fractals* **35**(2) (2008) 408–419.

[7] Belhumeur P. N., Hespanha J. P. and Kriegman D. J. Eigenfaces vs. Fisherfaces: Recognition using class specific linear projection. *IEEE Trans. on Pattern Analysis and Machine Intelligence* **19**(7) (1997) 711–720.

[8] Bremananth, R. and Chitra, A. An efficient biometric cryptosystem using autocorrelators. *International Journal of Signal Processing* **2**(3) (2005) 158–164.

[9] Chen G., Mao, Y. and Chui, C. K. Asymmetric image encryption based on 3D chaotic maps. *Chaos, Solitons and Fractals* **21**(3) (2004) 749–761.

[10] Cruz-Hernández, C. Synchronization of time-delay Chua's oscillator with application to secure communication. *Nonlinear Dynamics and Systems Theory* **4**(1) (2004) 1–13.

[11] Cruz-Hernández, C. and Martynyuk, A. A. Advances in chaotic dynamics and applications, In: Stability, Ocillations, and Optimization of Systems, Cambridge Scientific Publishers, Kiev, 2010.

[12] Daugman, J. High confidence visual recognition of persons by a test of statistical independence. *IEEE Trans. on Pattern Analysis and Machine Intelligence* **15**(11) (1993) 1148–1161.

[13] Filali R. L., Hammami S., Benrejeb M. and Borne P. On Synchronization, Anti-synchronization and Hybrid Synchronization of 3D Discrete Generalized Hénon Map. *Nonlinear Dynamics and Systems Theory* **12**(1) (2012) 81–95.

[14] Goldstein A.J., Harmon L.D. and Lesk, A.B. Identification of human faces. In: *Proceedings of the IEEE* **59**(5) (1971) 748–760.

[15] Haiping L., Karl M., Bui F., Plataniotis K. N. and Hatzinakos D. Face recognition with biometric encryption for privacy-enhancing self-exclusion. In: *16th international conference on Digital signal processing*, Aegean island of Santorini, 2009, 1–8.

[16] Hsu, C. W. and Lin, C. J. A comparison of methods for multi-class support vector machines. *IEEE Trans. Neural Networks* **13** (2) (2002) 415–425.

[17] IEEE Computer Society. IEEE Standard for Floating-Point arithmetic. In: IEEE std 754 – 2008, New York, 2008, 1–58.

[18] Inzunza-González E., Cruz-Hernández C. and Serrano-Guerrero H., Hyperchaotic encryption: An application in biometric systems based on face recognition, submitted in *AEÜ - International Journal of Electronics and Communications.*

[19] Kirby, M. and Sirovich, L. Application of the Karhunen-Loeve procedure for the characterization of human faces. *IEEE Transactions on Pattern Analysis and Machine Intelligence* **12**(1) (1990) 103–108.

[20] Kresimir Delac, M. G. and Stewart, B. M. Recent advances in face recognition. In-Teh, Vienna, 2008.

[21] López-Mancilla, D. and Cruz-Hernndez, C. Output synchronization of chaotic systems: model-matching approach with application to secure communication. *Nonlinear Dynamics and Systems Theory* **5** (2) (2005) 141–15.

[22] Muhammad K. K., Zhang J. and Tian L. Chaotic secure content-based hidden transmission of biometric templates. *Chaos, Solitons and Fractals* **32**(5) (2007) 1749–1759.

[23] Mukhopadhyay S., Demircioglu B. and Chatterjee A. Quantum Dynamics of a Nonlinear Kicked Oscillator. *Nonlinear Dynamics and Systems Theory* **11**(2) (2011) 173–182.

[24] Peng J., Zhang D. and Xiaofeng L. A digital image encryption based on hyper-chaotic cellular neural network. *Fundamenta Informaticae* **90**(3) (2009) 269–282.

[25] Sani M. M., Ishak K. A., Samad S. A. Classification using adaptive multiscale retinex and support vector machine for face recognition system. *Journal of Applied Sciences* **10**(6) (2010) 506–511.

[26] Shannon C. E. Communication theory of security systems. *The Bell System Technical Journal* **27**(3) (1948) 379-423, 623–656.

[27] Shannon C. E. Communication theory of secrecy system. *The Bell System Technical Journal* **28**(4) (1949) 656–715.

[28] Sirovich, L. and Kirby, M. A low-dimensional procedure for the characterization of human faces. *J. Optical Soc. Am. A* **4**(3) (1987) 519–524.

[29] Turk, M. and Pentland, A. Eigen face for recognition. *Journal of Cognitive Neuroscience* **3**(1) (1991) 71–86.

[30] Turk, M. and Pentland, A. Face recognition using eigenfaces. In: Proceedings of IEEE Conf. on Computer Vision and Pattern Recognition. IEEE, La Haina Maui, 1991, 586–591.

[31] Yongyi, M. and Zichao, D. A New Image Encryption Algorithm of Input-Output Feedback Based on Multi-chaotic System. Applied Mechanics and Materials **40-41** (1) (2011) 924–929.

[32] Zhang, D. D. Automated biometrics technologies and systems. Kluwer Academic Publishers, Beijing, 2000.