DOI: http://doi.org/10.15446/ing.investig.108212

System and Computer Engineering

Facial Cryptograms Classification through their Local Texture Features

Clasificación de criptogramas faciales a través de sus características de textura local

José T. Guillen-Bonilla[1], Jorge Aguilar-Santiago[2], Juan C. Estrada-Gutiérrez[3], and Maricela Jiménez-Rodríguez[4]

ABSTRACT

With the increasing use of social networks, unauthorized individuals have become able to detect or intercept personal data, which could be used improperly, thereby causing personal damage. Therefore, it is essential to utilize a security mechanism that aids in protecting information from malicious attacks. In this work, facial recognition is proposed, using the local textural features of cryptograms. Red-Green-Blue (RGB) facial images were encrypted by applying the mathematical Logistic Map model, which generated a cryptogram. These cryptogram's local textural features were extracted via Coordinated Cluster Representation (CCR) transform. The high classification efficiency (97-100%) of the encrypted facial images was experimentally validated using two databases: the first one was generated by controlling parameters such as rotation, scale, and lighting; and the second one is a public database. This technique is suitable for a wide range of applications related to user authentication, and it safeguards the identity of authorized users when accompanied by additional layers of security involving images of interest, such as those employed by the medical field, enhancing the security of users whose diseases are graphically studied in hospitals. In addition, this technique can be deployed to protect new product launches where images are important, such as clothing, footwear, mosaics, *etc.*, since one does not need to decrypt the images in order to classify them.

Keywords: facial recognition, classification efficiency, chaos, cryptography, coordinated clusters representation, local textural features

RESUMEN

Con el uso creciente de las redes sociales, personas no autorizadas han conseguido detectar o interceptar datos personales, que podrían utilizarse de manera inapropiada, causando así daños personales. Por lo tanto, es esencial utilizar un mecanismo de seguridad que ayude a proteger la información de ataques maliciosos. En este trabajo se propone el reconocimiento facial, utilizando las características texturales locales de los criptogramas. Se cifraron imágenes faciales en formato Red-Green-Blue (RGB) aplicando el modelo matemático de Mapa Logístico, lo que generó un criptograma. Las características texturales locales de estos criptogramas se extrajeron mediante la transformación de representación de *cluster* coordinado (CCR). La alta eficiencia de clasificación (97-100%) de las imágenes faciales cifradas fue validada experimentalmente utilizando dos bases de datos: la primera fue generada controlando parámetros como la rotación, escala e iluminación; y la segunda es una base de datos pública. Esta técnica es adecuada para una amplia gama de aplicaciones relacionadas con la autenticación de usuarios, y protege la identidad de los usuarios autorizados cuando se acompaña de capas adicionales de seguridad que involucran imágenes de interés, como las utilizadas en el campo médico, mejorando la seguridad de los usuarios cuyas enfermedades se estudian gráficamente en los hospitales. Además, esta técnica puede desplegarse para proteger lanzamientos de nuevos productos donde las imágenes son importantes, como ropa, calzado, mosaicos, *etc.*, ya que no es necesario descifrar las imágenes para clasificarlas.

Palabras clave: reconocimiento facial, eficiencia de la clasificación, caos, criptografía, representación de *cluster* coordinado, características texturales locales

Received: November 29th 2022
Accepted: February 20th 2024

[1]Doctor of Sciences, Centro de Investigaciones en Óptica. Affiliation: full professor, Centro Universitario de Ciencias Exactas e Ingenierías, Universidad de Guadalajara, México. E-mail: trinidad.guillen@academicos.udg.mx

[2]Student of the Doctorate in Technology Sciences, Centro Universitario de la Ciénega. Affiliation: subject professor, Centro Universitario de la Ciénega, Universidad de Guadalajara, México. E-mail: jorge.asantiago@academicos.udg.mx

[3]Doctor of Sciences, Universidad de Guadalajara. Affiliation: full professor, Centro Universitario de la Ciénega, Universidad de Guadalajara, México. E-mail: jcarlos.estrada@academicos.udg.mx

[4]Doctor of Sciences and Technology, Universidad de Guadalajara. Affiliation: full professor, Centro Universitario de la Ciénega, Universidad de Guadalajara, México. Email: maricela.jrodriguez@academicos.udg.mx

Introduction

Currently, facial recognition is a very active area of research worldwide, given its large number of applications. Among these, the following can be mentioned: access to the control of mobile devices and computers, video surveillance, and access to facilities, among others (Kalech, 2019; Bello-Cerezo *et al.*, 2019; Peng *et al.*, 2019). However, all of these applications are prone to information theft (hacking) (fliphtml5.com, n.d.). Therefore, it is advisable to encrypt facial data, avoiding possible harm to people due to inadequate information handling. A facial image can be encrypted by applying a mathematical model governed by a nonlinear dynamic equation whose behavior is complex-chaotic when its control parameters are adequate. Commonly, it would be necessary to decrypt these images when aiming for facial recognition. To prevent this, it should be possible to apply a recognition technique with the cryptograms generated during the encoding process by using a descriptor. This paper proposes the combination of chaotic cryptography, a texture descriptor, and a multi-class classifier to perform facial recognition through cryptograms.

The remainder of this paper is divided into the following sections. In the *Literature review*, several related works are detailed. The section titled *Classification and encryption system* outlines the steps to encrypt and classify images. The *Results* section presents the experimental tests conducted and the results obtained, and the final section provides the conclusions reached in this research.

Literature review

The literature has proposed various dynamic nonlinear mathematical models in studying and applying chaos theory to information encryption. Some examples include the Lorenz attractor, the Rössler attractor (Kumar and Girdhar, 2021; Rodríguez *et al.*, 2016; Jiménez-Rodríguez *et al.*, 2018), the Henon attractor (Afifi, 2019), the Logistic Map, and the Sine Map (Xiang and Liu, 2020; Pan *et al.*, 2018; Suman *et al.*, 2022). This is due to the fact that, because of their properties, chaotic systems are closely related to cryptography. These properties include a high sensitivity to initial conditions and system parameters that are utilized as encryption keys, making it more difficult for an attacker to decode encrypted data and thereby increasing the security of the information that travels through the network. This helps to prevent malicious users from corrupting the integrity of said information and ensure that it can only be retrieved by those who have the right keys.

The Logistic Map approach is based on a mathematical function in parabolic form (a degree-two polynomial). This model can exhibit very wide dynamics by merely varying the value of a parameter, since there may be trajectories that are periodic or chaotic, tending towards a fixed point. Although the Logistic Map was first applied in studying the evolution of populations, it has been efficiently employed in the encryption of digital images (Pan *et al.*, 2018). Chaotic systems have been widely utilized in ciphering methods, as is the case of the research presented herein, which proposes the asynchronous Boolean network encryption technique, implementing a new two-dimensional (2D) chaotic system with a codification rule (Gao *et al.*, 2023a). Furthermore, a ciphering method based on three dimensions (3D) was developed in order to implement 2D-chaotic systems while employing Logistic Maps (Gao *et al.*, 2023c). Another facial encryption technique deploys a HASH key generator and a 2D-logististic tent modular map. For facial recognition, the Histogram of Oriented Gradients (HOG) has also been applied (Gao *et al.*, 2023b). Another work proposed an audio encryption system that combines a one-dimensional (1D)-infinite collapse map (1D-ICM) and a Logistic Map (Wu *et al.*, 2022).

A generated cryptogram is a random field that contains the information of an original image, together with a series of pseudo-random numbers. Furthermore, a cryptogram contains texture information that can be extracted by applying a specialized statistical technique. In this type of approach (Alaei *et al.*, 2019; Nanni *et al.*, 2019), the digital image is regarded as a source of detectable patterns, with an observation window of size I×J (commonly I×J=3×3 pixels) (Leyferman *et al.*, 2023). For each position, a texture unit is calculated and assigned to a function-of-probability distribution in terms of texture units. Such a probability function is interpreted as a texture spectrum and is used as a multi-dimensional characteristic vector in classifiers.

Multiple works have employed the textural characteristics of images in order to perform biometric recognition (*e.g.*, visual cryptography) and to distribute facial images in separate databases (Ren and Zhang, 2022). A facial recognition and authentication system was developed by Ibrahim *et al.* (2021). A visual authentication and facial recognition method in color was also proposed in the literature (Ibrahim *et al.*, 2019), wherein the image is encrypted and divided into two shared segments, with one stored in the memory card and the other one in a database. When the sensor reads the card, the images are overlaid to uncover the original.

Visual cryptography has been employed in facial recognition. Here, photographs are divided into two images that are stored in different servers. Both of these images must be obtained during the recovery process (Mohan and R., 2021). A secure communication system was implemented by Aguilar Santiago *et al.* (2020), employing OpenCV to perform facial detection and recognition. Ahmad Khan *et al.* (2021) developed a facial recognition technique that leverages the homomorphic properties of cryptosystems and the Euclidean distance. The novelty of this technique lies in not revealing the real image during the recognition process.

In this work, the cryptogram generated with the mathematical Logistic Map model is interpreted as a source of texture information, upon which facial recognition is performed through local texture features. The texture is extracted by applying the coordinated clusters representation (CCR) transform, which conducts a local autocorrelation analysis over a binary image. This approach is based on two mathematical theorems (Sánchez-Yáñez *et al.*, 2003). The texture spectrum generated with the CCR transform is utilized as a characteristic vector in a multi-class classifier based on the statistics of the image. In most research aiming for recognition through visual cryptography or authentication, different devices have been employed to enhance security (Ren and Zhang, 2022; Ibrahim *et al.*, 2019, 2021; Mohan and R., 2021) or to perform recognition prior to encryption. Conversely, the technique proposed in this paper does not require a distributed storage system; hence, time and resources are spared, since the images must not be decrypted for facial recognition.

This paper offers the following contributions and applications:

- Classification efficiency is increased by employing cryptograms while environmental conditions (such as rotation, scale, and lighting) remain invariant.

- The proposed recognition technique works directly with the stored encrypted photographs, thus avoiding the need for an image decryption algorithm.
- The security in storing or sending the ciphered data is enhanced.
- The computational cost is decreased in scenarios where security and recognition are required.
- This approach prevents the storage of image data across different devices as a security reinforcement.
- This method allows sharing encrypted images in social media while preventing non-authorized users from visualizing them.
- The use of secure databases containing underage user information is enabled, blocking the visualization or the tracking of their data.
- The databases can be stored in cloud services, preventing third parties from accessing and misusing the data.
- This method enables real-time facial identification, employing the cryptogram corresponding to the detected face and safeguarding user privacy.

Classification and encryption system

Figure 1 presents the proposed multi-class classifier system based on the coordinated cluster representation (CCR) transform and the encrypted facial images. In this classifier, RGB images are encrypted, cryptograms are binarized, binary images are represented as a texture spectrum (obtained using the CCR transform), the Hamming distance is employed to measure the similarity between a test image and a database (of images) previously identified by a human expert, and the facial image is finally classified. The classifier requires two phases (Sánchez-Yáñez *et al.*, 2003): learning and recognition.

In the learning phase, the classifier is trained within a five-step process:

1) A database of RGB facial images is generated, or a public database is employed. Each facial image is encrypted by applying the mathematical Logistic Map model.
2) All color cryptograms are converted into gray-level ones using the MATLAB software. Subsequently, these cryptograms are binarized with the fuzzy c-means algorithm (Dunn, 1973).
3) From each binary cryptogram obtained in step 2, Q random sub-cryptograms are extracted, with a size of ¼ of the original area. Their local textural features are extracted using the CCR transform. Thus, each sub-cryptogram is represented by a texture spectrum $F_{I\times J}^{q,m}(b)$, where q indicates the sub-cryptogram number, m indicates the class $(m = 1,2,\dots,M)$, and M is the total number of classes.
4) The prototype vector of the *m-th* cryptogram $F_{I\times J}^{m}(b)$ is determined using the histograms $F_{I\times J}^{q,m}(b)$.
5) Steps 1 and 4 are repeated for each class (cryptogram).

In the recognition phase, all facial cryptograms are classified. This phase consists of seven steps:

1) A facial image is acquired using a digital camera.
2) This test image is encrypted via the Logistic Map.
3) The resulting RGB cryptogram is converted into a gray-level one in MATLAB, and it is transformed into a binary facial cryptogram utilizing the fuzzy c-means algorithm.
4) P test random cryptograms, similar in size to those of the learning stage, are extracted from the facial cryptogram, and their local textural features are extracted from each sub-cryptogram, such that each sub-cryptogram is represented as a texture spectrum $F_{I\times J}^{Test,p}(b)$, where p $(p = 1,2,\dots,P)$ indicates the *p-th* sub-cryptogram.
5) Using the Hamming distance, the similarity between $F_{I\times J}^{Test,p}$ and $F_{I\times J}^{m}(b)$ is measured (in the CCR feature space). Subsequently, the test sub-cryptogram is assigned to class m if and only if the Hamming distance is minimal.
6) The cryptogram is decoded.
7) Steps 1-6 are repeated for each test cryptogram.

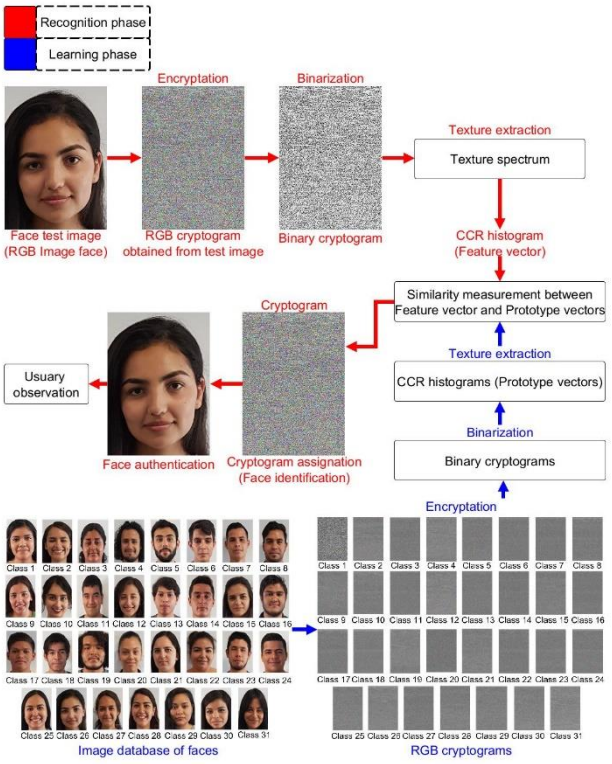


Figure 1. Proposed multi-class classifier system for facial identification
Source: Authors

Encryption

The mathematical Logistic Map model is governed by a nonlinear dynamic equation whose behavior is complex-chaotic (Xiang and Liu, 2020):

$$x_{n+1} = bx_n(1 - x_n) \qquad (1)$$

where b is a control parameter $(0 \le b \le 4)$, x_0 is the initial condition of the chaotic map $(0 \le x_0 \le 1)$, and x_{n+1} denotes the subsequent values obtained in the n^{ava} iteration of x_0. This system exhibits a chaotic behavior when the control parameter b takes a

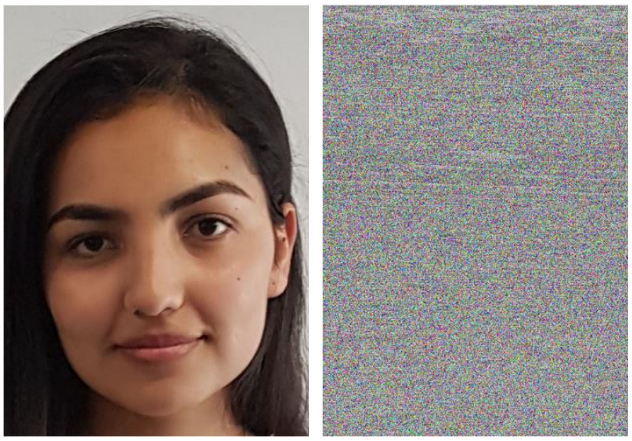
value within the interval $b \in [3{,}57,\ 4]$. In Jiménez-Rodríguez *et al.* (2015), we proposed an algorithm to generate a cryptogram from a color image. In this work, we adapted said algorithm for our application. The algorithm works with the RGB subpixels (red, green, blue) that make up each pixel of the image. These have an integer value between 0 and 255. The encryption keys are $b1$, the $x1_0$ parameter, and the initial condition. These keys are used to obtain orbit 1, which is applied in the diffusion process. Moreover, $b2$ and $x2_0$ correspond to a parameter and an initial condition that allow generating orbit 2, used in the confusion technique.

Encoding algorithm

The encoding process is presented below.

1) Store the subpixels in a vector called *SP*, which has a length $long = SP_n^R + SP_n^G + SP_n^B$, where $SP = [SP_1^R, SP_1^G, SP_1^B, \dots, SP_n^R, SP_n^G, SP_n^B]$.
2) Divide each element of SP by 255 to obtain values between 0 and 1: $SP = \frac{[SP_1^R, SP_1^G, SP_1^B, \dots, SP_n^R, SP_n^G, SP_n^B]}{255}$.
3) Create a vector named mix with length $long$ to store SP values chaotically.
4) Solve Equation (1) using the encryption keys $b1$ and $x1_0$, with each value of the orbit stored in $orb_{log} = [0.3452, 0.8970, 0.5673, \dots, 0.6787]$.
5) Generate a position between 1 and $long$, $pos = round(long * orb_{log}[i])$.
6) Verify whether the pos position in the mix vector is empty. Then, store an SP value; otherwise, save the subpixel in a vector called loc.
7) Repeat steps 5 and 6.
8) Proceed through the mix vector and, in each empty location, store a value of loc.
9) Solve Equation (1) using keys $b2$ and $x2_0$ to generate $rblog2 = [0.6958, 0.7968, 0.9854, \dots, 0.8456]$, a vector with $long$ chaotic values.
10) Add the values of vectors $orblog2$ and mix in an orderly fashion. Store the result in a vector denominated $cipher$, $cipher = orblog2 + mix$.

Figure 2a displays an RGB facial image, and Figure 2b shows its cryptogram (steps 1-10).



(a) (b)

Figure 2. a) RGB facial image; b) RGB cryptogram obtained by applying the Logistic Map
Source: Authors

As shown in Figure 2, the cipher algorithm efficiently encrypts the facial information, as the cryptogram is completely chaotic and the face is not recognizable.

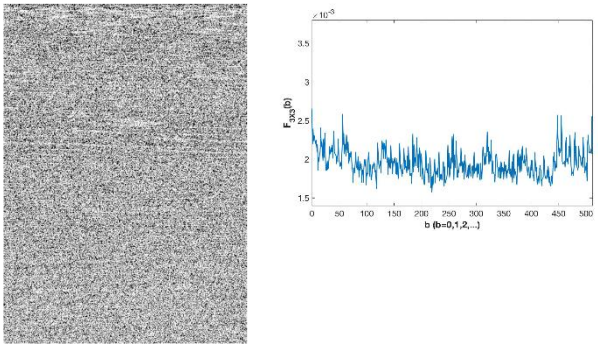
Coordinated cluster representation

Considering that the cryptogram is a random field (Figure 2b), and that the color channels retain the information of the original image, the RGB color cryptogram can be transformed into a gray-level one, losing only its color information. If the gray-level cryptogram is transformed by applying a binarization algorithm, its lighting information is eliminated, but the binary cryptogram retains sufficient information for its characterization through local textural features. This is possible because the binary cryptogram is a 2D random field that can be interpreted as a source of texture information. In this work, CCR is used to extract local textural features. To extract the texture of the facial cryptograms, the following steps are required:

1) The facial image is encrypted with the mathematical Logistic Map model. Thus, an RGB color cryptogram is obtained.
2) The RGB cryptogram is transformed into a gray- level one.
3) The gray-level cryptogram is transformed into a binary one. This binary cryptogram is interpreted as a source of texture information.
4) An observation window of $I \times J$ is established.
5) The observation window is moved pixel by pixel over the entire binary cryptogram. For each position, a texture unit is calculated, which is a discrete random variable *b*, whose value depends on the binary state within the observation window.
6) The texture unit is used as an index in the discrete histogram $H_{I\times J}(b)$, whose length is $2^{I\times J}$.
7) The histogram $H_{I\times J}(b)$ is divided by the total of binary patterns, obtaining a function-of-probability distribution $F_{I\times J}(b)$ in terms of texture units. This is a discrete equalized histogram $F_{I\times J}(b)$, and it is interpreted as a texture spectrum.

By applying the described algorithm (steps 1-7), the texture spectrum of an RGB facial image can be calculated. Figure 3a shows the binary facial cryptogram calculated from the RGB one (Figure 2b), and Figure 3b presents its texture spectrum $F_{3\times3}(b)$, where $I \times J = 3 \times 3$ pixels.

In Figure 3b, the texture spectrum fully represents the cryptogram (Figure 3a). This texture spectrum has two important characteristics: a) the histogram occupies a low-dimensional space (R^{512} $dimension$), and b) it can be used as a characteristic vector in texture classifiers.



(a) (b)

Figure 3. a) Binary facial cryptogram obtained using MATLAB and fuzzy c-means, b) texture spectrum F(3×3) calculated with an observation window of I×J=3×3 pixels
Source: Authors

Decoding algorithm

As shown in Figure 1, decoding is the last stage of the multi-class classifier system. The cryptogram (Figure 2b) preserves the information of the original image. This information can be recovered by following these steps (Jiménez-Rodríguez *et al.*, 2015):

1) Using keys $b2$ a $x2_0$, generate $orblog2 = [0.6958, 0.7968, 0.9854, \dots, 0.8456]$, a vector with $long$ chaotic values.
2) Perform the reverse process of step 10 in the encoding algorithm to encrypt $mix = cipher - orblog2$.
3) Regenerate orb_{log} as in step 4 of Encoding algorithm.
4) Calculate pos performing step 5 of the encoding algorithm.
5) Verify whether the location pos in the vector mix is not empty. Then, take the value and store it in the next position of the vector, called $original$. Otherwise, skip a location in the *original* vector.
6) Repeat steps 4 and 5 for each value of orb_{log}.
7) Proceed through the mix vector, and store each element in the empty positions of $original$ in an orderly fashion.
8) Multiply each original value by 255 and round out the result – in this way, the integers corresponding to the subpixels are retrieved.

Figure 4 presents the facial image retrieved from the cryptogram shown in Figure 2b, by following steps 1-8.

Figure 4. Facial image retrieved from the cryptogram
Source: Authors

Note that the decryption algorithm recovers the original image from the cryptogram, demonstrating the effectiveness of our proposal in retrieving information. This confirms that a facial image can be classified in the image space or in that of the cryptogram. Hence, the result must be the same.

Results

Database of facial images

To perform the corresponding experiments, two databases of facial images were used. The first database was generated by taking photographs of 31 students from La Ciénega University Center. During the capture process, the scale, rotation, lighting, and resolution of the camera were controlled. This simplified our facial classification issues, but also limited the potential applications. All facial images were in RGB color, their size was 480 x 576 pixels, and each facial image represented a mood: serious, smiling, happy, and merry. Each image was identified as a class. The classes can be seen in Figure 5.

The second database was the FEI face database (the Brazilian facial emotion identification database). This is a public database created by the Artificial Intelligence Laboratory of the FEI in São Bernardo do Campo, São Paulo, Brazil (Carlos Eduardo Thomaz–Personal Web Page, n.d.). We used the FEI database's facial images of 200 photographed individuals. All images were in RGB color and had the same size (260 x 360 pixels), and their background was white. Figure 6 shows 100 facial images taken from the FEI face database.

Encryption and decryption

The mathematical Logistic Map model was applied, as well as the encryption algorithm, with the encryption keys $b1 = 3.87756$, $x1_0 = 0.34342$, $b2 = 3.77$, $x2_0 = 0.8990$. Both of the databases used were encrypted, obtaining RGB cryptograms. The cryptograms and the original facial images were identical in size (480 x 576 and 260 x 360 pixels). Figure 7 presents the RGB cryptograms obtained from the first database (Figure 5). Note that these cryptograms are chaotic fields, and that the facial information is unrecognizable. It can thus be stated that the encryption process efficiently protects user information.

By applying the decryption algorithm described in the *Decoding algorithm* section, the RGB cryptograms were decrypted, once again obtaining the facial images shown in Figures 5 and 6. Subsequently, via a correlation analysis, the similarity between the original and the decrypted images was compared, with a correlation

coefficient always equal to one. This proved that each original image can be efficiently recovered from its cryptogram.

Classification efficiency

Using the previously described classifier system, the facial image cryptograms were classified. Four experiments were conducted, classifying the sub-cryptograms into their corresponding classes. The CCR histogram was utilized as a multi-dimensional characteristic vector, the facial images were encrypted with the mathematical Logistic Map model, and Q and P finally took a value of 80. In the first and second experiments, the generated database (Figure 5) was classified while calculating the CCR histogram with observation windows of $I \times J = 3 \times 3$ and $I \times J = 4 \times 4$ pixels. In the third and fourth experiments, the public database (Figure 6) was once again classified with the same CCR histogram size. The experimental results were in the form of a confusion matrix, where the guesses are in the main diagonal and the identification errors correspond to all elements outside it. In this vein, the efficiency (%) is given by Equation (2).

$$Ef(\%) = \frac{\sum_m diag(A)}{\sum_{mm} A} \times 100 \qquad (2)$$

where A is the confusion matrix, $diag(A)$ indicates the main diagonal of said matrix, and $Ef(\%)$ is the percent classification efficiency of the cryptograms. Figure 7 presents our experimental results regarding sub-cryptogram classification.

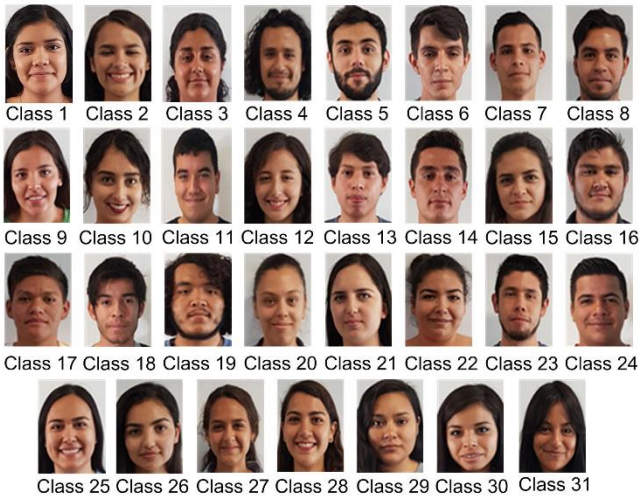


Figure 5. Database of facial images generated from La Ciénega University Center
Source: Authors

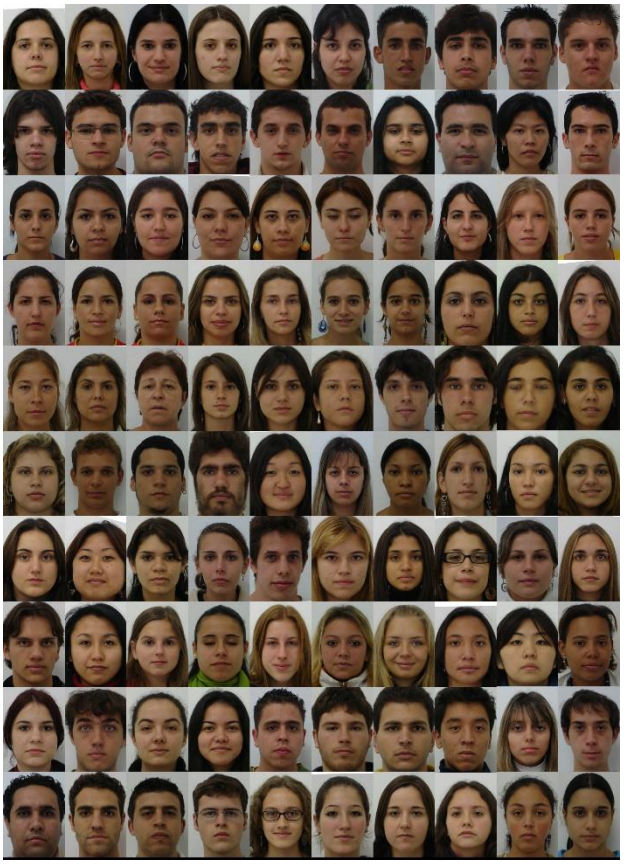


Figure 6. Public database used (FEI face database)
Source: (Carlos Eduardo Thomaz - Personal Web Page, s. f.)

Figure 7. Cryptograms generated from the facial images in Figure 5
Source: Authors

As seen in Figure 8, the classification efficiency is very high: it is 100% when the size of the observation window is 4 x 4 pixels (Figures 8b and 8d), and it reaches 97% when the size is 3 x 3 pixels (Figures 8a and 8c). These results are the same for the two databases. In the first case, the efficiency is 100% because the CCR transform extracts sufficient texture information from the cryptograms, and the classifier considers sufficient characteristics.

In the second case, the efficiency is 97% because the CCR transform, and the classifiers do not extract sufficient information from the cryptogram. This reduces the values obtained, which are high for both databases. The results agree with those of other studies in the literature that employ the CCR histogram as a multi-dimensional characteristic vector in classifier systems (Kurmyshev *et al.*, 2007; Kurmyshev and Sánchez-Yáñez, 2005; Guillen-Bonilla *et al.*, 2007).

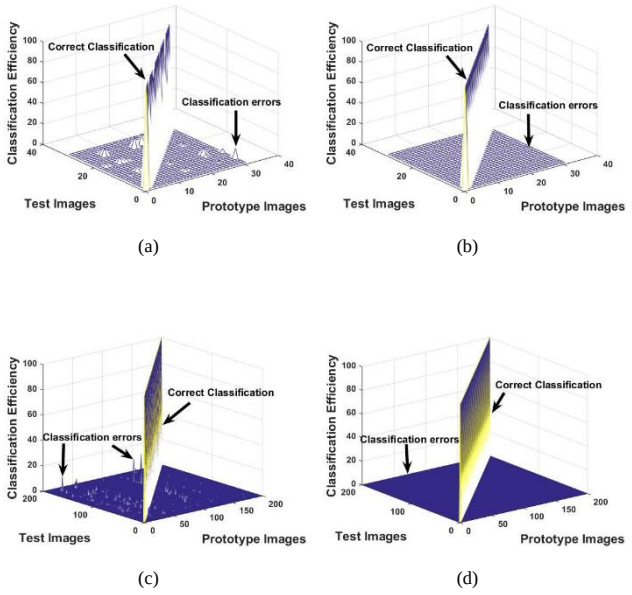


Figure 8. Experimental results regarding cryptogram classification efficiency: a) I x J = 3 x 3 (generated database); b) I x J = 4 x 4 (generated database); c) I x J = 3 x 3 (public database); d) I x J = 4 x 4 (public database)
Source: Authors

Comparison

Diverse texture extraction techniques have been reported in the literature and applied in facial recognition. Each technique has its own classification efficiency, which depends on the textural features extracted from the digital images and the classifier system. Nevertheless, when comparing CCR against other techniques (Table 1), our proposal shows a higher classification than the DLFace, MDLFR, CRC, H-CRC, LPP, LBP, and CS-LGC methods, demonstrating its promise for facial-image classification. Another important consideration is that CCR classified cryptograms (facial images encrypted using the mathematical Logistic Map model), while other texture-extraction techniques classified the actual photographs in the image domain.

Table 1. Comparison between CCR and other texture extraction techniques applied in facial recognition

Classification efficiency (%)		
Operators	*Minimum*	*Maximum*
DLFace (Peng *et al.*, 2019)	86.12	98.68
MDLFR (Luo *et al.*, 2019)	82.19	95.81
CRC (Zhang *et al.*, 2014)	84.16	92.73
H-CRC (Shi *et al.*, 2019)	95.41	99.17
LPP (Bansal *et al.*, 2014)	80.93	94.33
LBP (Yang *et al.*, 2019)	36.11	96.47
CS-LGC (Yang *et al.*, 2019)	39.51	98.33
CCR (our proposal)	96.39	100

Note: DLFace: deep local descriptor for cross-modality face recognition; MDLFR: multi-resolution dictionary learning for face recognition; CRC: collaborative representation-based classification; H-CRC: histogram-based CRC; LPP: locality preserving projection; LBP: local binary pattern; CS-LGC: central symmetric local gradient coding; CCR: coordinated cluster representation.
Source: Authors

In this work, we performed facial identification using the local textural features extracted from binary cryptograms. In our methodology (Figure 1), facial images are encrypted by applying the mathematical Logistic Map model, the CCR transform is used in textural feature extraction from the facial cryptogram, and a multi-class classifier is applied for cryptogram classification, wherein the CCR histogram is used as a multi-dimensional characteristic vector. During the classification of cryptograms, color and lighting information are eliminated via digital image processing techniques. However, CCR boasts a high classification efficiency because the binary facial cryptogram preserves sufficient texture information to be characterized through CCR (Sánchez-Yáñez *et al.*, 2003; Dunn, 1973; Jiménez-Rodríguez *et al.*, 2015; Carlos Eduardo Thomaz–Personal Web Page, n.d.; Kurmyshev *et al.*, 2007; Kurmyshev and Cervantes, 1996), obtaining an classification accuracy in the order of 96.39-100% (Table 1).

Four numerical experiments were conducted on two facial image databases, employing observation window sizes of 3 x 3 and 4 x 4 pixels. These experiments confirmed the high cryptogram classification accuracy of our proposal (Figure 1). When the CCR histogram was calculated with a 3 x 3 pixel window size, the resulting classification efficiencies are 97.70% (generated database) and 96.39% (public database). If the window size is 4 x 4 pixels, both efficiencies are 100%. This demonstrates that facial cryptograms can be classified through their local textural features or in the CCR feature space, and the obtained results agree with others reported in the literature (Sánchez-Yáñez *et al.*, 2003; Kurmyshev *et al.*, 2007; Guillen-Bonilla *et al.*, 2007).

Based on Table 1, combining the CCR transform and the encryption algorithm with the mathematical Logistic Map model offers two very important advantages. First, our proposal provides computer security, as chaotic mathematical models are used during the encryption of facial information, implying greater security for users. Second, the classification efficiency is high under controlled conditions (*i.e.*, rotation, scale, lighting, and resolution). If the conditions are not controlled, the efficiency can be reduced due to other physical variables.

The encryption system can be deployed to cipher any type of data. Once this data type is divided into blocks of bytes, it can be applied to a computing system for real-time encryption. Table 2 provides the ciphering times (s) for different image sizes.

Table 2. Encryption times in seconds

Image size	**Time (s)**
128 x 128	0.1368629
256 x 256	0.2126618

512 x 512	0.3767965
1024 x 1024	0.9764167

Source: Authors

Our proposal has potential applications in computer security because facial information is encrypted with chaotic mathematical models. This user-directed data protection scheme prevents any unintended use of personal information and increases data security during the information transfer through social networks and/or media. Therefore, future work shall consider the following directions: the development of security schemes in portable systems and the attainment of increased security in information transfer systems and social networks. In addition, we will consider making the classification system more robust by employing variables related to scale, rotation, lighting, and resolution.

Conclusions

Because our aim is user security, this work proposed a methodology for identifying facial images encrypted via the Logistic Map method. During the facial recognition process, local textural features were extracted from binary cryptograms, texture extraction was performed using the CCR transform, and classification was conducted by applying a multi-class classifier. The classifier was based on facial cryptogram statistics and utilized the CCR histogram as a characteristic vector. Our proposal was validated with four numerical experiments, wherein the CCR histogram was calculated using 3 x 3 and 4 x 4 pixel observation windows. Two databases of encrypted facial images were employed, and the efficiency increased from 96.39 to 100%. During image acquisition, the conditions (scale, rotation, camera resolution, and lighting) were controlled. If the conditions had not been controlled, the classification error would have increased, as more variables and more noise sources would have been involved in our experiments. Even so, our proposal shows a high potential for application in the field of computer security.

Acknowledgments

The authors thank Mexico's National Council of Science and Technology (CONACyT) for the support granted. J. Aguilar-Santiago expresses his gratitude to CONACyT for the scholarships received. The authors thank all students for their collaboration.

Author contributions

Author 1: investigation, methodology, and software. Author 2: software. Author 3: formal analysis. Author 4: investigation, methodology, and software. All authors participated in the writing, review, and editing of this manuscript.

Conflicts of interest

The authors declare no conflicts of interest regarding the publication of this paper.

Data availability

The algorithms, figures, and pixel data used to support the findings of this study are included within the article.

References

Afifi, A. (2019). A chaotic confusion-diffusion image encryption based on Henon map. *International Journal of Network Security & Its Applications*, *11*(4), 19-30. https://doi.org/10.5121/ijnsa.2019.11402

Aguilar Santiago, J., Flores Siordia, O., Guillen Bonilla, J. T., Estrada Gutiérrez, J. C., González Novoa, M. G., and Jiménez Rodríguez, M. (2020). Chaotic cryptosystem for selective encryption of faces in photographs. *Security and Communication Networks*, *2020*, 1-22. https://doi.org/10.1155/2020/8848356

Ahmad Khan, F., Bouridane, A., Boussakta, S., Jiang, R., and Almaadeed, S. (2021). Secure facial recognition in the encrypted domain using a local ternary pattern approach. *Journal of Information Security and Applications*, *59*, 102810. https://doi.org/10.1016/j.jisa.2021.102810

Alaei, F., Alaei, A., Pal, U., and Blumenstein, M. (2019). A comparative study of different texture features for document image retrieval. *Expert Systems with Applications*, *121*, 97-114. https://doi.org/10.1016/j.eswa.2018.12.007

Bansal, P., Mittal, S., and Gupta, M. (2014). *Using Locality Preserving Projections in Face Recognition*. *2*(3), 99-108. https://api.semanticscholar.org/CorpusID:212515605

Bello-Cerezo, R., Bianconi, F., Di Maria, F., Napoletano, P., and Smeraldi, F. (2019). Comparative evaluation of hand-crafted image descriptors *vs.* off-the-shelf CNN-based features for colour texture classification under ideal and realistic conditions. *Applied Sciences*, *9*(4), 738. https://doi.org/10.3390/app9040738

Carlos Eduardo Thomaz—Personal Web Page (n.d.). https://fei.edu.br/~cet/facedatabase.html

Dunn, J. C. (1973). A fuzzy relative of the ISODATA process and its use in detecting compact well-separated clusters. *Journal of Cybernetics*, *3*(3), 32-57. https://doi.org/10.1080/01969727308546046

fliphtml5.com (n.d.). *4243_0819_rp_qtrly-threats-aug-2019_lores*. https://fliphtml5.com/rshui/bhkw/4243_0819_rp_qtrly-threats-aug-2019_lores/

Gao, S., Wu, R., Wang, X., Liu, J., and Li, Q. (2023a). EFR-CSTP: Encryption for face recognition based on the chaos and semi-tensor product theory. *Information Sciences*, *621*, 766-781. https://doi.org/10.1016/j.ins.2022.11.121

Gao, S., Wu, R., Wang, X., Liu, J., Li, Q., Wang, C., and Tang, X. (2023b). Asynchronous updating boolean network encryption algorithm. *IEEE Transactions on Circuits and Systems for Video Technology*, *33*(8), 4388-4400. https://doi.org/10.1109/TCSVT.2023.3237136

Gao, S., Wu, R., Wang, X., Wang, J., Li, Q., Wang, C., and Tang, X. (2023c). A 3D model encryption scheme based on a cascaded chaotic system. *Signal Processing*, *202*, 108745. https://doi.org/10.1016/j.sigpro.2022.108745

Guillen-Bonilla, J. T., Kurmyshev, E., and Fernández, A. (2007). Quantifying a similarity of classes of texture images. *Applied Optics*, *46*(23), 5562. https://doi.org/10.1364/AO.46.005562

Ibrahim, D. R., Abdullah, R., and Teh, J. S. (2021). Multifactor authentication system based on color visual cryptography, facial recognition, and dragonfly optimization. *Information Security Journal: A Global Perspective*, *30*(3), 149-159. https://doi.org/10.1080/19393555.2020.1817633

Ibrahim, D. R., Abdullah, R., Teh, J. S., and Alsalibi, B. (2019). *Authentication for ID cards based on colour visual cryptography and facial recognition* [Conference

presentation]. 3rd International Conference on Cryptography, Security and Privacy. https://doi.org/10.1145/3309074.3309077

Jiménez-Rodríguez, M.., Flores-Siordia, O., and González-Novoa, M. G. (2015). Sistema para codificar información implementando varias órbitas caóticas. *Ingeniería, Investigación y Tecnología*, *16*(3), 335-343. https://doi.org/10.1016/j.riit.2015.05.004

Jiménez-Rodríguez, M., Padilla Leyferman, C. E., Estrada Gutiérrez, J. C., González Novoa, M. G., Gómez Rodríguez, H., and Flores Siordia, O. (2018). Steganography applied in the origin claim of pictures captured by drones based on chaos. *Ingeniería e Investigación*, *38*(2), 61-69. https://doi.org/10.15446/ing.investig.v38n2.64509

Kalech, M. (2019). Cyber-attack detection in SCADA systems using temporal pattern recognition techniques. *Computers & Security*, *84*, 225-238. https://doi.org/10.1016/j.cose.2019.03.007

Kumar, V., and Girdhar, A. (2021). A 2D logistic map and Lorenz-Rossler chaotic system based RGB image encryption approach. *Multimedia Tools and Applications*, *80*(3), 3749-3773. https://doi.org/10.1007/s11042-020-09854-x

Kurmyshev, E. V., and Cervantes, M. (1996). A quasi-statistical approach to digital binary image representation. *International Journal of e-Navigation and Maritime Security*, *42*(1), 104-116. https://doi.org/10.1016/j.enavi.2017.05.007

Kurmyshev, E. V., Poterasu, M., and Guillen-Bonilla, J. T. (2007). Image scale determination for optimal texture classification using coordinated clusters representation. *Applied Optics*, *46*(9), 1467. https://doi.org/10.1364/AO.46.001467

Kurmyshev, E. V., and Sánchez-Yáñez, R. E. (2005). Comparative experiment with colour texture classifiers using the CCR feature space. *Pattern Recognition Letters*, *26*(9), 1346-1353. https://doi.org/10.1016/j.patrec.2004.11.028

Leyferman, C. E. P., Bonilla, J. T. G., Gutiérrez, J. C. E., and Rodríguez, M. J. (2023). A novel technique for texture description and image classification based in RGB compositions. *IET Communications*, *17*(10), 1162-1176. https://doi.org/10.1049/cmu2.12601

Luo, X., Xu, Y., and Yang, J. (2019). Multi-resolution dictionary learning for face recognition. *Pattern Recognition*, *93*, 283-292. https://doi.org/10.1016/j.patcog.2019.04.027

Mohan, J., and R., R. (2021). Enhancing home security through visual cryptography. *Microprocessors and Microsystems*, *80*, 103355. https://doi.org/10.1016/j.micpro.2020.103355

Nanni, L., Brahnam, S., and Lumini, A. (2019). Texture descriptors for representing feature vectors. *Expert Systems with Applications*, *122*, 163-172. https://doi.org/10.1016/j.eswa.2018.12.052

Pan, H., Lei, Y., and Jian, C. (2018). Research on digital image encryption algorithm based on double logistic chaotic map. *EURASIP Journal on Image and Video Processing*, *2018*(1), 142. https://doi.org/10.1186/s13640-018-0386-3

Peng, C., Wang, N., Li, J., and Gao, X. (2019). DLFace: Deep local descriptor for cross-modality face recognition. *Pattern Recognition*, *90*, 161-171. https://doi.org/10.1016/j.patcog.2019.01.041

Ren, L., and Zhang, D. (2022). A privacy-preserving biometric recognition system with visual cryptography. *Advances in Multimedia*, *2022*, 1-7. https://doi.org/10.1155/2022/1057114

Rodríguez, M. J., González-Novoa, M. G., Estrada-Gutiérrez, J. C., Acosta-Lúa, C., and Flores-Siordia, O. (2016). Secure point-to-point communication using chaos. *DYNA*, *83*(197), 180. https://doi.org/10.15446/dyna.v83n197.53506

Sánchez-Yáñez, R. E., Kurmyshev, E. V., and Cuevas, F. J. (2003). A framework for texture classification using the coordinated clusters representation. *Pattern Recognition Letters*, *24*(1-3), 21-31. https://doi.org/10.1016/S0167-8655(02)00185-X

Shi, L., Song, X., Zhang, T., and Zhu, Y. (2019). Histogram-based CRC for 3D-aided pose-invariant face recognition. *Sensors*, *19*(4), 759. https://doi.org/10.3390/s19040759

Suman, R. R., Mondal, B., and Mandal, T. (2022). A secure encryption scheme using a composite logistic sine map (CLSM) and SHA-256. *Multimedia Tools and Applications*, *81*(19), 27089-27110. https://doi.org/10.1007/s11042-021-11460-4

Wu, R., Gao, S., Wang, X., Liu, S., Li, Q., and Erkan, U. (2022). AEA-NCS: An audio encryption algorithm based on a nested chaotic system. *Chaos, Solitons & Fractals*, *165*, 112770. https://doi.org/10.1016/j.chaos.2022.112770

Xiang, H., and Liu, L. (2020). An improved digital logistic map and its application in image encryption. *Multimedia Tools and Applications*, *79*(41-42), 30329-30355. https://doi.org/10.1007/s11042-020-09595-x

Yang, J., Wang, X., Han, S., Wang, J., Park, D. S., and Wang, Y. (2019). Improved real-time facial expression recognition based on a novel balanced and symmetric local gradient coding. *Sensors*, *19*(8), 1899. https://doi.org/10.3390/s19081899

Zhang, L., Yang, M., Feng, X., Ma, Y., and Zhang, D. (2014). *Collaborative representation based classification for face recognition*. https://doi.org/10.48550/arXiv.1204.2358