Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.12785/amis/080115

Morphological Associative Memories for Gray-Scale Image Encryption

María Elena Acevedo[1,*], *José Ángel Martínez*[1], *Marco Antonio Acevedo*[1] *and Cornelio Yañez*[2]

[1] Escuela Superior de Ingeniería Mecánica y Eléctrica del IPN, México City, México
[2] Centro de Investigación en Computación del IPN, México City, México

Received: 1 Jun. 2013, Revised: 15 Sep. 2013, Accepted: 16 Sep. 2013
Published online: 1 Jan. 2014

Abstract: This work describes a novel method for encrypting gray-scale images using an associative approach. The image is divided in blocks which are used to build max and min Morphological associative memories. The key is private and it depends on the number of blocks. The main advantage of this method is that the cyphertext does not have the same size than the original image; therefore, since the beginning the adversary cannot know what the image means.

Keywords: Computational techniques, Artificial Intelligence, Associative Memories, Image processing, Encryption.

1 Introduction

Cryptrography [1] is the science of protecting data and communications. One of its main components involves communicating messages or information between designated parties by changing the appearance of the messages (or data) in ways that aim to make it extremely difficult or impossible for other parties to eavesdrop on or interfere with the transmission.

The advent of high-speed computers has had a tremendous impact on the standards for what are considered to be effective ciphers or cryptosystems, which are algorithms for rendering messages unintelligible except to the designated recipients. A cryptosystem has two parts: encryption, which is done at the sender's end of the message and means to put the actual plaintext (original messages) into cyphertext (secret code), and decryption, which is done at the recipient's end and means to translate the cyphertext back into the original plaintext message.

Generally an encryption or decryption algorithm will relay on a secret key [2], which may be a number with particular properties, or a sequence of bits; the algorithm itself may be well known, but to apply the decryption to a given cyphertext requires knowledge of the particular key used. There are two classes of cryptosystems:

Secret-key cryptosystems. Also called *symmetric cryptosystems*. Here the same key is used for both encryption and decryption.

Public-key cryptosystems. Here the keys for encryption and decryption are different. So you can publicize a "public key" which anybody can use to encrypt messages to you, but only you know the appropriate corresponding private decryption key.

The advent of personal computers and the Internet have made possible for anyone to distribute worldwide digital information. However, there are many applications that need to protect their information from people who can steal important data. Therefore, it is important to apply an encryption method.

Traditional image encryption algorithms are private key encryption standards (DES and AES), public key standards such as Rivest Shamir Adleman (RSA), and the family of elliptic-curve-based encryption (ECC), as well as the international data encryption algorithm (IDEA).

Current encryption algorithms can be classified into different techniques such as optical [3]-[8], value transformation [9]-[13], pixels position permutation [14]-[16] and chaos-based [17]-[21].

In this paper we propose a novel encryption method for gray-scale images by using an associative approach. In particular, we use the Morphological associative memory

[*] Corresponding author e-mail: eacevedo@ipn.mx

which has demonstrated to be a suitable tool for the Pattern Recognition area.

2 Associative Memories

An associative memory is a content-addressable structure that maps a set of input patterns to a set of output patterns. The input patterns are stimuli which are associated with their corresponding responses, i.e. output patterns. The application of the algorithm for association built an associative memory. The output pattern is recalled when its corresponding input pattern is presented to the associative memory.

There are several models of associative memories which can be of two types: classical and no-classical. Within the classical models, the most representative are: 1) Lernmatrix [22], the first model, 2) Correlograph [23], 3) Linear Associator [24], and 4) Hopfield [25] that is a neural net with associative behavior. There are two models with no-classical approach: Morphological [26] and Alpha-Beta [27] associative memories.

The input and output patterns are represented by vectors. The task of association of these vectors is called Training Phase and, the Recognizing Phase allows recovering patterns. The stimuli are the input patterns represented by the set $\mathbf{x} = \{x^1, x^2, x^3, ..., x^p\}$ where p is the number of associated patterns. The responses are the output patterns and are represented by $\mathbf{y} = \{y^1, y^2, y^3, ..., y^p\}$. Representation of vectors x^μ is $x^\mu = \{x_1^\mu, x_2^\mu, x_3^\mu, ..., x_n^\mu\}$ where n is the cardinality of x^μ. The cardinality of vectors y^μ is m, then $y^\mu = \{y_1^\mu, y_2^\mu, y_3^\mu, ..., y_m^\mu\}$. The set of associations of input and output patterns is called the fundamental set or training set and is represented as follows: $\{(x^\mu y^\mu) \mid \mu = 1, 2, ..., p\}$

There are two types of associative memories concerning to the nature of the input and output patterns.

A memory is **Autoassociative** if it holds that $x^\mu = y^\mu \forall \mu \in \{1, 2, ..., p\}$, then one of the requisites is that $n = m$.

A memory is **Heteroassociative** when $\exists \mu \in \{1, 2, ..., p\}$ for which $x^\mu \neq y^\mu$. Notice that there can be heteroassociative memories with $n = m$.

Now, we will describe the Morphological associative model.

The fundamental difference between classic associative memories (*Lernmatrix, Correlograph, Linear Associator* and Hopfield) and Morphological associative memories lies in the operational bases of the latter, which are the morphological operations: dilation and erosion. This model broke out of the traditional mold of classic memories which use conventional operations for vectors and matrices in learning phase and sum of multiplications for recovering patterns. Morphological associative memories change products to sums and sums to maximum or minimum in both phases.

The basic computations occurring in the proposed morphological network are based on the algebraic lattice structure $(\mathbf{R}, \vee, \wedge, +)$, where the symbols $\vee$ and $\wedge$ denote the binary operations of maximum and minimum, respectively. Using the lattice structure $(\mathbf{R}, \vee, \wedge, +)$, for an $m \times n$ matrix A and a $p \times n$ matrix B with entries form $\mathbf{R}$, the matrix product $C = A \nabla B$, also called the *maxproduct* of A and B, is defined by equation (1).

$$\begin{aligned} C_{ij} = \bigvee_{k=1}^{p} a_{ik} + b_{kj} = \\ = (a_{i1} + b_{1j}) \vee (a_{i2} \\ + b_{2j}) \vee ... \vee (a_{ip} + b_{pj}) \end{aligned} \tag{1}$$

The *minproduct* of A and B induced by the lattice structure is defined in a similar fashion. Specifically, the i, jth entry of $C = A \Delta B$ is given by equation (2).

$$\begin{aligned} C_{ij} = \bigwedge_{k=1}^{p} a_{ik} + b_{kj} = \\ = (a_{i1} + b_{1j}) \wedge (a_{i2} \\ + b_{2j}) \wedge ... \wedge (a_{ip} + b_{pj}) \end{aligned} \tag{2}$$

Suppose we are given a vector pair $\mathbf{x} = (x_1, x_2, ..., x_n)^t$ and $\mathbf{y} = (y_1, y_2, ..., y_n)^t \in \mathbf{R}^m$. An associative morphological memory that will recall the vector when presented the vector is showed in equation (3).

$$W = y \nabla (-x)^t = \begin{bmatrix} y_1 - x_1 & \cdots & y_1 - x_n \\ \vdots & \ddots & \vdots \\ y_m - x_1 & \cdots & y_m - x_n \end{bmatrix} \tag{3}$$

Since W satisfies the equation $W \Delta \mathbf{x} = \mathbf{y}$ as can be verified by the simple computation in equation (4).

$$W \nabla x = \begin{bmatrix} \bigvee_{i=1}^{n} (y_1 - x_i = x_i) \\ \vdots \\ \bigvee_{i=1}^{n} (y_m - x_i + x_i) \end{bmatrix} = y \tag{4}$$

Henceforth, let $(\mathbf{x}^1, \mathbf{y}^1)$, $(\mathbf{x}^2, \mathbf{y}^2)$, ..., $(\mathbf{x}^p, \mathbf{y}^p)$ be p vector pairs with $x^k = (x_1^k, x_2^k, ..., x_n^k)^t \in \mathbf{R}^n$ and $y^k = (y_1^k, y_2^k, ..., y_m^k)^t \in \mathbf{R}^m$ for $k = 1, 2, ..., p$. For a given set of pattern associations $\{(\mathbf{x}^k, \mathbf{y}^k) \mid k = 1, 2, ..., p\}$ we define a pair of associated pattern matrices (X, Y), where $X = (\mathbf{x}^1, \mathbf{x}^2, ..., \mathbf{x}^p)$ and $Y = (\mathbf{y}^1, \mathbf{y}^2, ..., \mathbf{y}^p)$. Thus, X is of dimension $n \times p$ with i, jth entry x_i^j and Y is of dimension $m \times p$ with i, jth entry y_i^j. Since $\mathbf{y}^k \nabla (-\mathbf{x}^k)^t = \mathbf{y} \Delta (-\mathbf{x}^k)^t$, the notational burden is reduced by denoting these identical morphological outer vector products by $\mathbf{y}^k \times (-\mathbf{x}^k)^t$. With each pair of matrices (X, Y) we associate two natural morphological $m \times n$ memories M and W defined by

With these definitions, we present the algorithms for the learning and recalling phase.

2.1 Learning phase

1. For each p association $(\mathbf{x}^{\mu}, \mathbf{y}^{\mu})$, the minimum product is used to build the matrix $\mathbf{y}^{\mu}\Delta(-\mathbf{x}^{\mu})^{t}$ of dimensions $m \times n$, where the input transposed negative pattern $\mathbf{x}^{\mu}$ is defined as $(-\mathbf{x}^{\mu})^{t} = (-x_1^{\mu}, -x_2^{\mu}, \ldots, -x_n^{\mu})$.
2. The maximum and minimum operators $(\vee$ and $\wedge)$ are applied to the p matrices to obtain M and W memories as equations (5) and (6) show.

$$M = \bigvee_{k=1}^{p} (y^k \times (-x^k)^t) \tag{5}$$

$$W = \bigwedge_{k=1}^{p} (y^k \times (-x^k)^t) \tag{6}$$

2.2 Recognizing phase

In this phase, the minimum and maximum product, Δ and ∇, are applied between memories M or W and input pattern x^{ω}, where $\omega \in \{1, 2, \ldots, p\}$, to obtain the column vector $\mathbf{y}$ of dimension m as equations (7) and (8) shows:

$$y = M\Delta x^{\omega} \tag{7}$$

$$y = W\nabla x^{\omega} \tag{8}$$

Now, we present an illustrative example for learning and recognizing phases of a Morphological associative memory.

Suppose we want to associate a set of three pairs of patterns, then $p = 3$. The cardinality of $\mathbf{x}$ and $\mathbf{y}$ will be $n = 3$ and $m = 4$, respectively. The three pairs of patterns are:

$$x^1 = \begin{bmatrix} -300 \\ 0 \\ 0 \end{bmatrix} \to y^1 = \begin{bmatrix} 29 \\ 128 \\ 100 \\ 14 \end{bmatrix}$$

$$x^2 = \begin{bmatrix} 0 \\ -300 \\ 0 \end{bmatrix} \to y^2 = \begin{bmatrix} 55 \\ 0 \\ 255 \\ 16 \end{bmatrix}$$

$$x^3 = \begin{bmatrix} 0 \\ 0 \\ -300 \end{bmatrix} \to y^1 = \begin{bmatrix} 255 \\ 255 \\ 255 \\ 0 \end{bmatrix}$$

We apply the step 1 from Learning phase to associate the first pair of patterns.

$$y^1 \times (-x^1)^t = \begin{bmatrix} 29 \\ 128 \\ 100 \\ 14 \end{bmatrix} \times -[-300\ 0\ 0] =$$

$$= \begin{bmatrix} 29+300 & 29-0 & 29-0 \\ 128+300 & 128-0 & 128-0 \\ 100+300 & 100-0 & 100-0 \\ 14+300 & 14-0 & 14-0 \end{bmatrix} = \begin{bmatrix} 329 & 29 & 29 \\ 428 & 128 & 128 \\ 400 & 100 & 100 \\ 314 & 14 & 14 \end{bmatrix}$$

The same process is performed to the remain pairs of patterns, and then the maximum of each element of every matrix is obtained as follows:

$$M = \begin{bmatrix} 329 & 29 & 29 \\ 428 & 128 & 128 \\ 400 & 100 & 100 \\ 314 & 14 & 14 \end{bmatrix} \bigvee \begin{bmatrix} 55 & 355 & 55 \\ 0 & 300 & 0 \\ 255 & 555 & 255 \\ 16 & 316 & 16 \end{bmatrix} \bigvee \begin{bmatrix} 255 & 255 & 555 \\ 255 & 255 & 555 \\ 255 & 255 & 555 \\ 0 & 0 & 300 \end{bmatrix}$$

$$M = \begin{bmatrix} 329 & 355 & 555 \\ 425 & 300 & 555 \\ 400 & 555 & 555 \\ 314 & 316 & 300 \end{bmatrix}$$

Now, we present the first input vector to the $max-type$ morphological associative memory

$$M\Delta x^1 = \begin{bmatrix} 329 & 355 & 555 \\ 425 & 300 & 555 \\ 400 & 555 & 555 \\ 314 & 316 & 300 \end{bmatrix} \Delta \begin{bmatrix} -300 \\ 0 \\ 0 \end{bmatrix} =$$

$$= \begin{bmatrix} 329+(-300) \wedge 355+0 \wedge 555+0 \\ 428+(-300) \wedge 300+0 \wedge 555+0 \\ 400+(-300) \wedge 555+0 \wedge 555+0 \\ 314+(-300) \wedge 316+0 \wedge 300+0 \end{bmatrix}$$

$$M\Delta x^1 = \begin{bmatrix} 29 \\ 128 \\ 100 \\ 14 \end{bmatrix} = y^1$$

When we present the other two input patterns (x^2 and x^3) to the memory, we recall their corresponding output patterns (y^2 and y^3).

3 Morphological Encryption/Decryption

In this section the proposed algorithm for encrypting images is described together with the algorithm to recall the original image.

The steps for the **Encryption Algorithm** are described as follows.

The image is partitioned in square blocks, i.e., $m \times m$ blocks. The software that implements our proposal automatically achieves this by calculating the greatest common divisor between the length and the width of the image, this value had to fall into the range of $[10,100]$ to avoid storing arrays that can occupy an excessive space of memory. If the greatest common divisor falls outside this range, it is multiplied (when it is minor) or divided (when it is greater) by ten until the condition is reached. Therefore, we obtain p blocks (or sub matrices) of $m \times m$ dimensions. We also know the number of blocks in the rows (BR) and in the columns (BC).

Each sub matrix is vectorized to obtain p vectors with $m \times m$ elements. These p vectors represent the output patterns y_j^i with $i = 1,2,\ldots,p$ and $j = 1,2,\ldots,(m \times m)$, these vectors will be used to build a Morphological Associative Memory (MAM). The input patterns are arranged in following way to build a $max-type$ MAM(M)

$$x_j^i = a \text{ and } x_j^i = 0 \text{ for } i = 1,2,\ldots,p, \\ j = 1,2,\ldots,p \text{ with } i \neq j \text{ and } a \in I \tag{9}$$

The input vectors to build a $min-type$ MAM (W) are formed as follows.

$$x_j^i = b \text{ and } x_j^i = 0 \text{ for } i = 1,2,\ldots,p, \\ j = 1,2,\ldots,p \text{ with } i \neq j \text{ and } b \in I \tag{10}$$

where b is the symmetric of a, then $b = -a$.

With this set of pairs of vectors, the fundamental set, we apply equations (5) and (6) to build *max* and *min* morphological associative memories which have dimensions of $(m \times m) \times p$. Both memories M and W represent the encryption of the original image. In both cases, we add one row at the top of the matrices. The values of these elements are random in the range of $[0,255]$ except for the three last elements: $(p-2)-th$ element. Means that is the element number $(p-2)$ is equal to the value of the rows (BR) and the last element has the value of the columns (BC). Therefore, what we can observe is just two positive integer matrices. In most of the cases, the cyphertext does not have the same dimensions of the plaintext; this is the main advantage of our proposal because it is expected that the encrypted image has the same dimensions than the original image, therefore the adversary will begin to work with this object thinking that it is just a modified version of the original image.

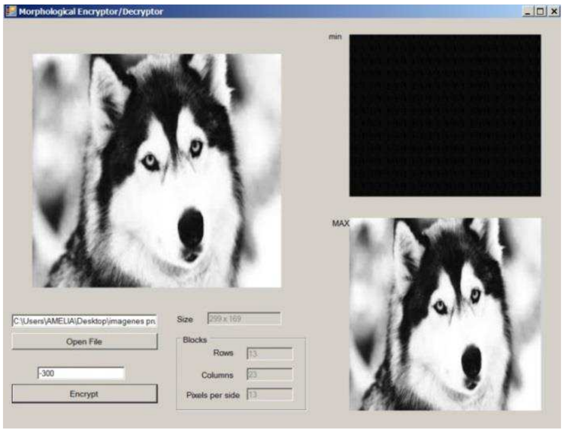
The plaintext is obtained by applying the **Decryption Algorithm**.

The first step is to extract the additional row at the top of both matrices, then we know the values of a, BR and BC.

Since we know that the dimensions of the encrypted image are $(m \times m) \times p$, we can build the p input vectors which will be presented to the *max* and *min* associative memories for recalling their corresponding output vectors. Therefore, we know that the cardinality of the input vectors must be p. Equations (9) and (10) are applied to build input vectors. One by one, each input vector x^i is operated with the associative memories M and W by using equations (7) and (8) and the output vector y^i is recalled. Now, we have to reconstruct the p blocks or sub-matrices. We obtain the square root of the number of the rows of any block and then we know that the width and the length of each block are m. With this information and the values of BR and BC, we can reconstruct completely the original image.

4 Experiments and Results

The proposed model was implemented by the use of the programming language Visual Studio 2010 C++. An example of the software is showed in Figure 1.



C:\Users\AMELIA\Desktop\imagenes pn

-300

Size 299 x 169

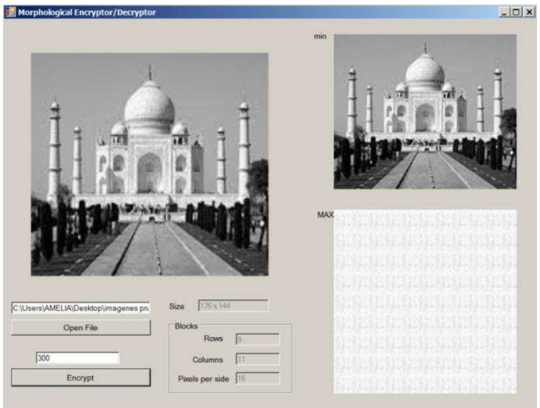
Rows 13

Columns 23

Pixels per side 13

Fig. 1: Screen sample of the software that implements the encryption/decryption algorithm proposed in this work.

From figure 1, we can observe the original image (on the left) and the decrypted images (on the right) when *min* and *max* morphological associative memories are used. The software presents the following options: we can select the file we want to encrypt and the program shows the size of the image (in pixels), in this example is 169 x 299, then we choose the value of a, in this case is -300. After click the button Encrypt, the program computes the pixels per side of each block and the BR and BC values. Then, the encryption and decryption processes are performed and the decrypted images are showed. Due to we used the value of -300, figure 1 shows that *max* memory recall the original image. If we would have used the value of 300, *min* memory would have recalled the original image which can be observed in Figure 2.



C:\Users\AMELIA\Desktop\imagenes pr
Size 176 x 144
300
Blocks
Rows 9
Columns 11
Pixels per side 16

Fig. 2: The results when we encrypt an image with the value of b = 300.

For testing our proposal we used six sets with ten images each of them. The images have different sizes. The sets show different concepts and their names are: animals, buildings, paintings, cartoons, electronic and robots. Figure 4 shows these sets of images.

Table 1 shows the dimensions of each image. Table 1 is arranged such that the images in Figure 4 correspond to the showed dimensions.

Table 1: Dimensions of the images showed in Figure 3.

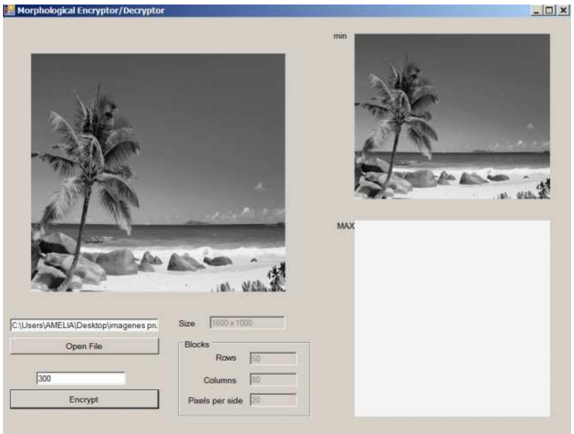
Animals		Buildings		Paintings	
259x194	262x192	176x116	246x205	258x165	265x190
276x183	290x174	259x194	260x194	250x202	257x196
225x192	225x225	284x177	225x225	242x208	266x189
299x169	276x183	176x144	189x267	277x182	259x194
304x166	215x235	260x194	303x166	225x225	206x154
Cartoons		Electronic		Robots	
200x252	213x236	259x194	193x261	176x245	186x271
192x263	199x253	176x132	266x177	225x225	231x218
259x194	259x194	259x194	254x198	190x256	272x185
302x167	225x225	225x225	249x202	228x221	225x225
232x217	259x194	256x197	212x237	259x194	225x225

Also, we test the algorithm with image with greater dimensions. Figure 5 shows these images which have the concept of landscapes and their corresponding dimensions are showed in Table 2.

Table 2: Dimensions of the images from the set of Landscapes

Landscapes				
1280x1024	1024x768	1600x1000	1920x1200	1518x1231
1920x1200	1600x1200	1920x1200	1600x1000	1920x1200

The complete process (Encryption/Decryption) is executed instantanely with the images showed in Figure 4. When the images have greater dimensions as the set of Landscapes, the process takes longer to be finished. However, the result is the same and the original image is recovered (see Figure 3).



C:\Users\AMELIA\Desktop\imagenes pr
Size 1600 x 1000
300
Blocks
Rows 50
Columns 80
Pixels per side 20

Fig. 3: Image with 1000 x 1600 pixels encrypted and decrypted with a value of $b = 300$. Min memory recovers the original image.

Now, we assure that the recovering is perfect but we show just a qualitative result. Therefore we need a quantitative way to prove that our proposal achieves favorable results. Then, we applied the correlation coefficient [28] which measures the closeness or similarity between two images. It can vary between -1 to +1. A value close to +1 indicates that the two images are very similar, while a value close to -1 indicates that they are very dissimilar. The formula to compute the correlation between two images A and B, both of size $N \times N$ pixels is given by Equation (11).

$$Corr(A\,|\,B) = \frac{\sum_{i=1}^{N}\sum_{j=1}^{N}(A_{ij}-\bar{A})(B_{ij}-\bar{B})}{\sqrt{\sum_{i=1}^{N}\sum_{j=1}^{N}(A_{ij}-\bar{A})^2\sum_{i=1}^{N}\sum_{j=1}^{N}(B_{ij}-\bar{B})^2}} \tag{11}$$

We applied the correlation coefficient (CC) between original and recovered images. The value of CC in all cases varied from 0.9999 to 1, which indicated that both images are equal.

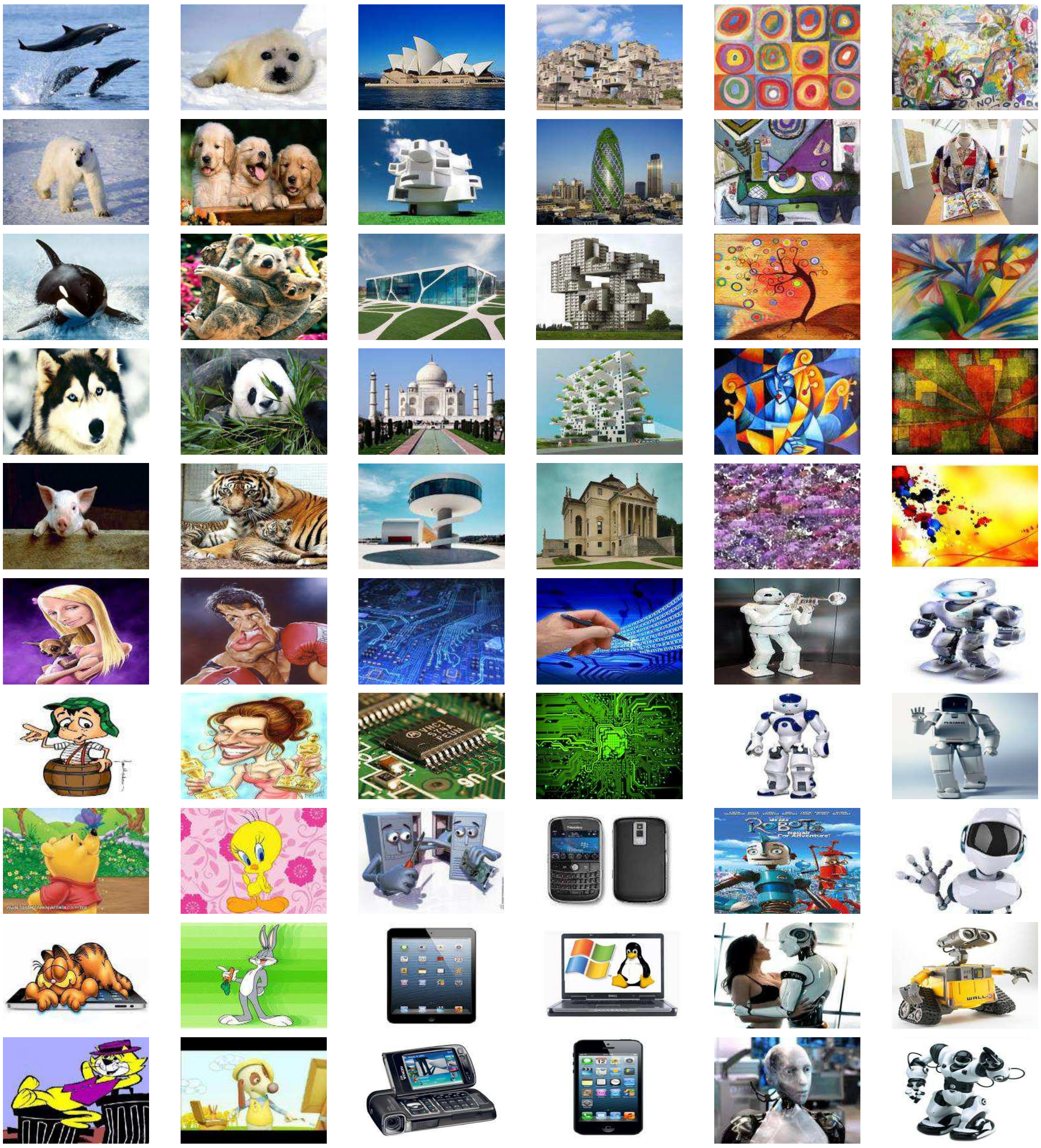


Fig. 4: Sets of images used for testing our proposal

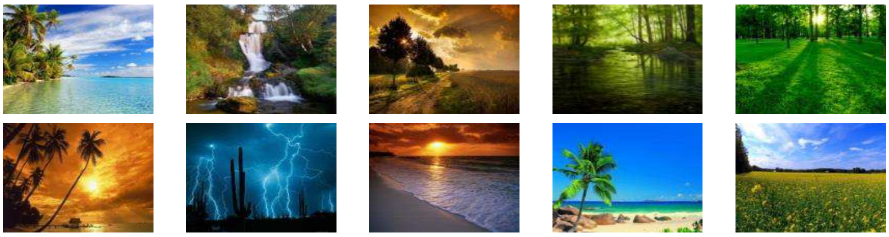


Fig. 5: Landscapes, images with greater dimensions than the images showed in Figure 3.

5 Summary and Concluding Remarks

Our proposal is a novel algorithm because there are no other works which had applied the associative approach to encrypt gray-scale images.

In this work, morphological associative memories show to be a suitable tool for encrypting images. The main feature of our algorithm is that the cyphertext does not have the same dimensions that the original image. Since the beginning, the adversary cannot guess the meaning of the cyphertext, It just can be seen a matrix (associative memory) with positive integer numbers, it is difficult to imagine that this set of numbers represent a gray-scale image. Furthermore, this matrix has to be operated to recover the blocks in which the original image was divided on, and then we have to attach these blocks to rebuilt the plaintext.

The obtained values of the correlation coefficient assure that the original image is always recovered no matter the dimension of the image. This is a consequence of divide the image in square blocks with a size of 100 x 100 pixels, maximum.

We have to highlight that our proposal works with images stored in noise-free devices. If the encryption is send through a noisy media, the original image cannot be recovered.

As a future work, we will apply this model to encrypt messages.

References

[1] Stanoyevitch A, Introduction to Cryptography with mathematical foundations and computer implementations, CRC Press, 1-2 (2011).

[2] McAndrew A., Introduction to Cryptography with open-source software, CRC Press, 4-5 (2011).

[3] Tao R., Xin Y. and Wang Y., "Double image encryption based on random phase encoding in fractional Fourier domain", Opt Express, **15**, 16067-16079 (2007).

[4] Ge F., Chen L. and Zhao D., "A half-blind image hiding and encryption method in fractional Fourier domains", Opt Commun, **281**, 4254-4260 (2008).

[5] Liu Z., Li Q., Dai J., Sun A., Liu S. and Ahmad M., "A new kind of double encryption by using a cutting spectrum in the 1-D fractional Fourier transform domains", Opt Commun, **282**, 1536-1540 (2009).

[6] Wang B. and Zhang Y., "Double images hiding based on optical interference", Opt Commun, **282**, 3439-3443 (2009).

[7] Meng X., Cai L., Wang Y., Yang X., Xu X., Dong G. et al., "Digital image synthesis and multiple-image encryption based on parameter multiplexing and phase-shifting interferometry", Opt Lasers Eng, **47**, 96-102 (2009).

[8] Weng D., Zhu N., Wang Y., Xie J., and Liu J., "Experimental verification of optical image encryption based on interference", Optics Communications, **284**, 2485-2487 (2011).

[9] Chen R. J. and Lai J. L., "Image security system using recursive cellular automata substitution", Pattern Recognition, **40**, 1621-1631 (2007).

[10] Guo Q., Liu Z., and Liu S., "Color image encryption by using Arnold and discrete fractional random transforms in HIS space", Optics and Lasers in Engineering, **48**, 1174-1181 (2010).

[11] Tao R., Meng X. Y., and Wang Y., "Image encryption with multiorders of fractional fourier transforms", IEEE Transactions on Information Forensics and Security, **5**, 734-738 (2010).

[12] Liu Z., Xu L., Lin C., Dai J., and Liu S., "Image encryption scheme by using iterative random phase encoding in gyrator transform domains", Optics and Lasers in Engineering, **49**, 542-546 (2011).

[13] Liu Z., Gong M., Dou Y., et al, "Double image encryption by using Arnold transform and discrete fractional angular transform", Optics and Lasers in Engineering, **50**, 248-255 (2012).

[14] Nien H. H., Huang W.T., Hung, C.M., et al, "Hybrid image encryption using multi-chaos-system", ICICS 2009, 8-10 Dec., 7th International Conference on Information, Communications and Signal Processing, 1-5 (2009).

[15] Prasad M. and Sudha K.L., "Chaos Image Encryption using Pixel Shuffling", Computer Science & Information Technology (CS & IT) CCSEA 2011, CS & IT 02, 169-179 (2011).

[16] Zhou X., Ma J., Du W. and Zhao Y., "Ergodic Matrix and Hybrid-key Based Image Cryptosystem", International Journal of Image, Graphics and Signal Processing, **4**, 1-9 (2011).

[17] Chen L., "A Novel Image Encryption Scheme Based on Hyperchaotic Sequences", Journal of Computational Information Systems, **8**, 4159-4167 (2012).

[18] Wang X. Y., Yang L., Liu R. and Kadir A., "A chaotic image encryption algorithm based on perceptron model", Nonlinear Dynamics, **62**, 615-621 (2010).

[19] Sakthidasan K. @ Sankaran and B.V.Santhosh Krishna, "A New Chaotic Algorithm for Image Encryption and Decryption of Digital Color Images", International Journal of Information and Education Technology, **1**, 137-141 (2011).

[20] Fu C., Chen J. J., Zou H., Meng W. H., et al., "A chaos-based digital image encryption scheme with an improved diffusion strategy", Optics Express, **20**, 2363-2378 (2012).

[21] Seyedzadeh S. M. and Mirzakuchaki S., "A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map", Signal Processing, **92**, 1202-1215 (2012).

[22] Steinbuch, K., "Die Lernmatrix", Kybernetik, **1**, 36-45 (1961).

[23] Willshaw, D., Buneman, O. and Longuet-Higgins, H., "Non-holographic associative memory", Nature, **222**, 960-962 (1969).

[24] Anderson, J. A., "A simple neural network generating an interactive memory", Mathematical Biosciences, **14**, 197-220 (1972).

[25] Hopfield, J. J., "Neural networks and physical systems with emergent collective computational abilities", Proceedings of the National Academy of Sciences, **79**, 2554-2558 (1982).

[26] Ritter, G. X., Sussner, P. and Diaz de Len J. L., "Morphological Associative Memories", IEEE Transactions on Neural Networks, **9**, 281-293 (1998).

[27] Acevedo, M. E., Yez, C. and Lpez, I., "Alpha-Beta Bidirectional Associative Memories: Theory and Applications". Neural Processing Letters, **26**, 1-40 (2007).

[28] Stathaki T., Image Fusion: Algorithms and Applications, Elsevier, 414 (2008).

María Elena Acevedo Received her BS degree in Engineering with specialization in Computing from the Escuela Superior de Ingeniería Mecánica y Eléctrica (ESIME) at Instituto Politécnico Nacional (IPN) in 1996. She has been teaching at ESIME since 1994. She received her MSc degree with specialization in Computing from the Centro de Investigación y de Estudios Avanzados (CINVESTAV) in 2001. She received her PhD from the Centro de Investigación en Computación (CIC) at IPN in 2006. Her main research area is Artificial Intelligence and Associative Memories.

José Ángel Martínez was born in San Cristobal de las Casas, Chiapas, Mexico in 1991. He is studying Electronics at Escuela Superior de Ingeniera Mecnica y Elctrica at IPN. He is a PIFI student (Programa Institucional para la Formacin de Investigadores, Institutional Program to Form Researches). One of his interests are the Associative Memories.

Marco Antonio Acevedo He was born in Mexico City in July 19th, 1968. He received his BS degree in Communications and Electronics Engineering in 1992 and his MSc degree with specialization in Electronics in 1996 from Escuela Superior de Ingeniería Mecánica y Eléctrica at Instituto Politécnico Nacional. Currently, he is a professor in ESIME. His main research area is Digital Signal Processing and Telecommunications.

Cornelio Yañez Received his BS degree in Physics and Mathematics from the Escuela Superior de Física y Matemáticas at IPN in 1989; the MSc degree in Computing Engineering from CINTEC-IPN in 1995, and the PhD from the Centro de Investigación en Computación (CIC-IPN) in Mexico City in 2002, receiving the Lázaro Cárdenas award 2002. Currently, he is a titular professor at the CIC-IPN. His research interests includes Associative Memories, Mathematical Morfology and Neural Networks.