Research Article / Telecommunications Engineering http://dx.doi.org/10.15446/ing.investig.v40n3.81421

Entropy-Based Image Encryption Using Orthogonal Variable Spreading Factor (OVSF)

Cifrado de Imágenes Basado en la Entropía Utilizando el Factor de Propagación Variable Ortogonal (OVSF)

Dora Maria Ballesteros[1], Diego Renza[2], and Jimmy Peña[3]

ABSTRACT

The purpose of image encryption is to provide data privacy and security. The former ensures that only authorized personnel can access the original content, while the latter implies that there is no evident relationship between the encrypted and the original content, and that the key space is equally likely and large enough. In the current state of the field, there are several proposals of image encryption techniques with very high privacy (in terms of entropy) but weak in terms of security (i.e., small key space). Recently, a new encoding-based method that provides a long key space (namely $8{,}57 \times 10^{506}$) with a middle value of entropy (87%) was proposed. Our proposal preserves the strength of the image encryption methods based on encoding, but with a higher value placed on security than the preliminary works. Every pixel of an image is mapped into an orthogonal code based on 256 bits. The 8-OVSF codes are selected to encode the image, given that the entropy of the inter-symbol is near the possible maximum. Numerous test results verify that our ciphered data have a very high value of entropy (98,5%) with an equally likely and long key space ($8{,}57 \times 10^{506}$), thus providing an adequate balance between privacy and security.

Keywords: entropy, OVSF, image encryption, security, privacy, ciphered data agriculture

RESUMEN

El objetivo del cifrado de imágenes es proporcionar privacidad y seguridad a los datos. La primera garantiza que solo el personal autorizado pueda acceder al contenido original, mientras que la otra implica que no exista relación evidente entre el contenido cifrado y el original, y que el conjunto de claves tenga igualdad de probabilidad y sea lo suficientemente grande. En el estado del arte existen numerosas propuestas de técnicas de cifrado de imágenes con alta privacidad (en términos de entropía), pero con deficiencia en términos de seguridad (es decir, un conjunto de claves pequeño). Recientemente, se propuso un método basado en codificación que proporciona un espacio de clave grande (específicamente, $8{,}57 \times 10^{506}$) con un valor intermedio de entropía (87 %). Nuestra propuesta conserva la fortaleza de los métodos de cifrado de imágenes basados en codificación, pero con mayor valor de seguridad que los trabajos anteriores. Cada píxel de una imagen es mapeado a un código ortogonal de 256 bits. Los códigos 8-OVSF se seleccionan para codificar la imagen, debido a que la entropía del inter-símbolo es cercana al máximo posible. Los resultados de numerosas pruebas demuestran que nuestros datos cifrados tienen un valor de entropía muy alto (98,5 %) con un conjunto de claves grande ($8{,}57 \times 10^{506}$) e igualmente probable, lo que proporciona un equilibrio adecuado entre privacidad y seguridad.

Palabras clave: entropía, OVSF, cifrado de imágenes, seguridad, privacidad, datos cifrados

Received: August, 1st 2019
Accepted: July, 13th 2020

Introduction

Nowadays, the number of images that are published on social networks, chats, public web pages, and other digital mediums is rapidly increasing. In some cases, these images contain confidential content, which is why their originator wants only authorized personnel to have access rights (privacy) through robust key (security) encryption schemes. Accordingly, the security and privacy standards of multimedia content have aroused the interest of the scientific community in the field of information technologies. Therefore, the quantity and quality of state-of-the-art digital privacy and security methods have increased. One way to provide privacy and security to digital image content is through encryption, by applying the properties of diffusion and confusion (Shannon, 1949). Diffusion implies that, if the image is slightly changed, the encrypted data must change significantly; regarding confusion, the direct relationship between the key and the encrypted data must be null. Typically, pixel permutation guarantees confusion, whereas pixel substitution is used for the diffusion property. The ideal result is a ciphered image

[1]Ph.D. in Electronic Engineering, Universitat Politecnica de Catalunya, España. Affiliation: Full professor. Faculty of Engineering, Universidad Militar Nueva Granada, Colombia. Email: dora.ballesteros@unimilitar.edu.co
[2]Ph.D. in Computer Science, Universidad Politecnica de Madrid, España. Affiliation: Full professor. Faculty of Engineering, Universidad Militar Nueva Granada, Colombia. Email: diego.renza@unimilitar.edu.co
[3]Telecommunications Engineering, Universidad Militar Nueva Granada, Colombia. Affiliation: Young research. Faculty of Engineering, Universidad Militar Nueva Granada, Colombia. Email: u1401120@unimilitar.edu.co

How to cite: Ballesteros, D. M., Renza, D., and Peña, J. (2020). Entropy-Based Image Encryption Using Orthogonal Variable Spreading Factor (OVSF). *Ingeniería e Investigación*, *40*(3), 70-80. 10.15446/ing.investig.v40n3.81421

Attribution 4.0 International (CC BY 4.0) Share - Adapt

with a uniform distribution (histogram), regardless of the original image's pixel characteristics.

For two decades, one of the most popular methods for image encryption was based on chaotic mapping. Proposed initially by Fridrich (1998), this approach divides the image into several sub-blocks of non-fixed size. Next, after a quantized map is formed, pixel permutation (place) and bit permutation (grayscale level) are applied. The simpler chaotic 1D-map is known as a 'logistic map' (Ye and Huang, 2017; Telem, Segning, Kenne, and Fotsin, 2014). More recent proposals include 2D and 3D sequences (Saljoughi, and Mirvaziri, 2019; Hua, Jin, Xu, and Huang, 2018), as well as dynamic functions at runtime (Asgari-Chenaghlu, Balafar, and Feizi-Derakhshi, 2019). Although the uncertainty (entropy) of the ciphered data in these methods has reached a very high value, security remains a significant challenge, given that these methods have been cryptanalyzed due to weaknesses in the diffusion rounds (Li, Xie, Liu, and Cheng, 2014; Feng, He, Li, and Li, 2019). Currently, researchers focus their efforts on the following aspects: (1) improving the confusion property, (2) improving the diffusion property, and (3) changing the relationship between confusion and diffusion.

To enhance the diffusion property, chaotic sequences are mixed with DNA-based techniques, which consist of changing the value of the shuffled pixel by an encoding process into nucleotides (Zhang, Fang, and Ren, 2014; Chai, Gan, Yuan, Chen, and Liu, 2019). Nevertheless, DNA encoding has also been cryptanalyzed (Wen, Yu, and Lü, 2019; Akhavan, Samsudin, and Akhshani, 2019). Another solution consists of elliptic curves for obtaining pseudo-random sequences (Hayat, and Azam, 2019). This method was also cryptanalyzed (Khoirom, Laiphrakpam, and Themrichon, 2018). Unlike the afore-mentioned methods, in literature, there are proposals that differ from the traditional schemes which have yet to be broken. For instance, Kumar and Quan (2019) analyze images using polar decomposition and the Shearlet transform, whereas, in Ballesteros, Peña, and Renza, (2018) diffusion and confusion tasks are performed through an encoding process using scrambled Collatz conjecture-based codes. However, the entropy value of the ciphered data fails to reach the possible maximum.

In summary, many proposals of methods concerning image encryption have very high entropy values, but suffer from security weaknesses. However, there are some non-traditional proposals that have yet to be cryptanalyzed. The lingering issue with these proposals is that their entropy values are not high enough. Therefore, it can be generally stated that systems that focus on privacy do not possess optimal security, and vice-versa. As a result, the trade-off between security and privacy is still a challenge to be overcome. It is thus necessary to increase the key space and equalize the likelihood in encryption keys for methods based on chaotic mapping while also improving the degree of ciphered data uncertainty in non-traditional schemes.

The highlights of the proposed method in this study are the following:

- Image content privacy is provided through the Orthogonal Variable Spreading Factor (OVSF) coding process. Each pixel (8-bits) of the input image is encoded into an orthogonal code (256-bits) using a specific map obtained from a key. Due to the quasi-perfect symmetry between ones and zeros of the entirety of orthogonal codes, a very high entropy value is theoretically expected.
- The maximum number of possible mappings between the 8-bit pixel values and the 256-bit orthogonal codes provides security to the ciphered content. It corresponds to the number of permutations used to scramble the 8-OVSF codes; a very high value of 256!
- Since the number of bits in the encrypted data is 32 times greater than the input image, it may be more convenient to group them into 16-bit words and write them as an audio file (samples). In other words, our proposed method is image-to-audio encryption.

Background concepts

The aim of this section is to provide some basic concepts which are necessary to understand the proposed method.

Entropy

In information theory, a well-known parameter that measures uncertainty and data distribution is entropy (Robinson, 2008). The greater the homogeneity in data distribution, the greater the value of the entropy. The most famous entropy formula is Shannon's entropy equation, calculated in terms of the probability of each available data value. It is shown as Equation (1):

$$H(I) = -\sum_{k=0}^{L-1} p(k) \log_2 (p(k)) \, (1), \tag{1}$$

where I is the input image (or audio), $p(k)$ is the probability of occurrence of the value k in the image (or audio), and L is the total number of levels of the image (or audio), with $L = 2^q$ for q bits of quantization. For example, in grayscale images, $L = 2^8$. If all intensity values have equal occurrence, then entropy is equal to q (8 in the example). However, if occurrence is not homogenous, the entropy value will be lower because uncertainty decreases.

Orthogonal Variable Spreading Factor (OVSF)

OVSF codes are originally used for channelization in Wideband Code Division Multiple Access (WCDMA). These codes are characterized by being orthogonal to one another, as well as their length being determined in terms of the level (L). An L-OVSF has 2^L codes of 2^L bits each. A way to obtain OVSF codes is through the application of an iterative tree that uses the value of the predecessor code as the root of the current code (Saini and Bhooshan, 2006). Each root has two descendants that double its length. The first

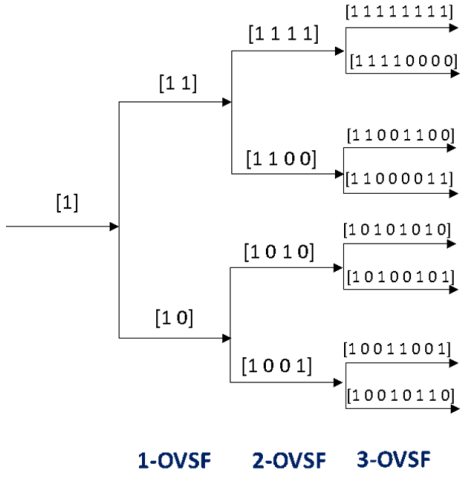

Figure 1. OVSF code tree.
Source: Authors

descendant repeats the predecessor code, and the second one complements it. Figure 1 shows the 3-OVSF code tree.

The first root is code "1", which does not have a counterpart. In the 1-OVSF, there are 2^1 codes of 2^1 bits, obtained as follows: the first code doubles its root and the result is "11". The second one uses the root in the first part and complements it in the second part, thus obtaining "10". In the second level (2-OVSF), there are 4-codes with four bits each. Each pair of codes has the same root. For the first descendant, the root is repeated; for the second, the root is complemented. This process is repeated until all codes are obtained.

The main advantage of OVSF codes is orthogonality, which results in 50% of the bits in a pair of codes being different for every available pair. For example, the codes '1100' and '1001' are equal in the first and third bit, but the second and fourth bits are different.

In terms of entropy, OVSF is expected to provide a high value of uncertainty for the encrypted image due to the quantity of zeros being similar to the quantity of ones. For example, for 3-OVSF, there are seven codes where the number of zeros is equal to the number of ones; only the first code has all bits equal to "1". In total, there are 28 zeros (0,44%) and 36 ones (56%). For 8-OVSF, the number of bits equal to 0 is 32640 (0,498%), while the number of bits equal to 1 is 32 896 (0,502%). For higher values of L, the quantity of zeros and ones is more symmetrical. Thus, the orthogonality property of OVSF codes is used in our proposal for obtaining high entropy values in encrypted images.

The proposed scheme

Recently, a scheme for image encryption based on the Collatz Conjecture was proposed (Ballesteros et al., 2018). Its proposal differs from classical schemes in some aspects: (i) an encoding block with a non-fixed length map is used to replace the permutation and diffusion processes; (ii) the output is not a ciphered image, but a ciphered audio; (iii) the number of available keys related to the security of the scheme is significantly higher than state-of-the-art methods. Since its encoding process uses binary codes obtained from the Collatz Conjecture, which does not have symmetry between zeros and ones, the entropy of the ciphered audio is not close to the highest possible value. The authors reported entropy values of 14 for audio files quantized to 16-bits. In the current proposal, the aim is to preserve the strengths of (Ballesteros et al., 2018) and improve upon its weaknesses by replacing the encoding block with 8-OVSF codes which should theoretically provide greater entropy given their orthogonality. As a result, the uncertainty about which image corresponds to the encrypted audio is greater compared to the scheme in Ballesteros et al. (2018).

Figure 2 shows the proposed general diagram. The inputs of the image coding are the image (I_{2D}) and the *seed*, the outputs are the ciphered audio (CA) and the *key*. In the image recovering module, the inputs are CA and the *key*, the output is the recovered image (RI_{2D}).

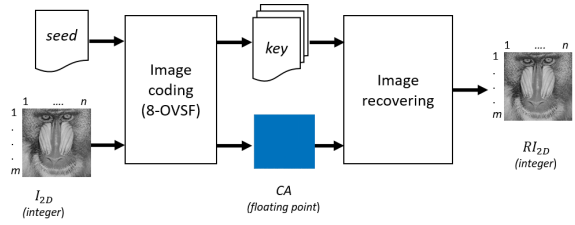

Figure 2. General block diagram of the proposed method.
Source: Authors

Each module in Figure 2 is explained as follows:

Image coding

This module is used at the transmitter stage in order to send the information with unintelligible content. Figure 3 presents the block diagram of this module, including the following blocks: generation of 8-OVSF codes, scrambling the 8-OVSF codes, mapping block, splitting the binary code, and creating the audio file. These blocks are detailed further below:

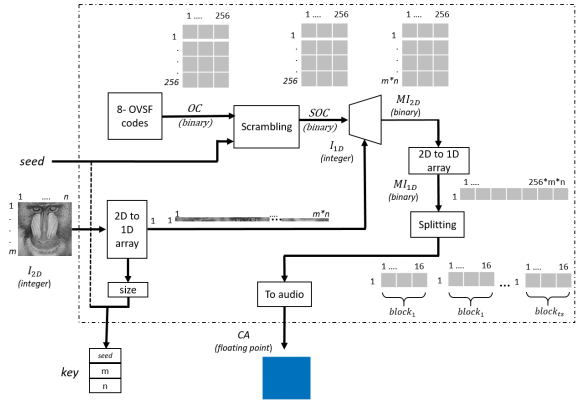

Figure 3. Specific block diagram of the image coding module.
Source: Authors

Generation of 8-OVSF codes: In this block, 256 orthogonal codes of 256 bits are obtained. The creation of these codes follows the theory presented in the *Orthogonal Variable Spreading Factor* section. The first code of the 8-OVSF has all bits equal to one, while the remaining binary codes have an equal number of zeros and ones. These 256 codes form a matrix with dimensions 256 x 256, with each row being an orthogonal code. Unlike the method proposed by Ballesteros et al. (2018), the length of each code is fixed. The output of the block is given the name "OC" (OVSF Codes).

Scrambling the 8-OVSF codes: The aim of this block is to disorder the matrix obtained in the previous block. Using a seed value, the order of the rows in the OC matrix is reorganized. The output is named "SOC" (Scrambled OVSF Codes) with dimensions being 256 x 256. This block provides security to the scheme (analyzed in detail in Section of Security analysis).

Mapping: The 2D image 'I_{2D}' is converted into a row vector, from left to right and top to bottom. The output is named 'I_{1D}'. Each value of I_{1D} is mapped to an orthogonal code. Therefore, every 8-bit pixel is represented by an orthogonal code of 28 bits (i.e., 256 bits). In this regard, I_{1D} is used as the multiplexor selector, where the inputs correspond to the rows in the SOC matrix. The output is a matrix of 256 columns (bits) with m x n rows, named 'MI_{2D}'.

Finally, the total number of bits of encrypted data will be 32 times greater than the original grayscale image. Once each pixel of the image has been mapped, values are arranged into a 1D vector. The output is named '$MI_{ID'}$ (Mapped Image).

Splitting the binary code and creating the audio file: Next, it is necessary to split the binary code into 16 bit words. Each orthogonal code has 16 sub-blocks of 16 bits by block. According to Equation 2, the total number of sub-blocks, ts, is equal to:

$$ts = 16 \times m \times n \tag{2}$$

The result is a matrix of $ts \times 16$, named 'S'. Finally, every sequence of 16 bits of S is transformed into a floating point value, in the range of [−1 1], as a sample of the ciphered audio. It is saved as a WAV file with a specific value for frequency sampling f_s (e.g., f_s = 8 kHz). Time (in seconds) of the ciphered audio is defined by Equation 3:

$$T = \frac{ts}{f_s} = \frac{16 \times m \times n}{f_s} \tag{3}$$

For example, if the original image is 128 × 128 and f_s = 8 kHz, then T = 32,768 (s). You can note that *ts* is the number of samples of ciphered audio.

Key: According to Shannon's theory, security of an encryption system must rely solely on the key. In our proposal, the key is composed of the seed, the number of rows (m), and the number of columns (n) in the image. However, security analysis is performed only on the seed.

The image encoding procedure is illustrated with the following example. Suppose that the system works with 2-OVSF codes (to simplify the example), and the orthogonal codes are '1111', '1100', '1010', and '1001'. The value of the OC matrix will be:

$$OC = \begin{pmatrix} 1111 \\ 1100 \\ 1010 \\ 1001 \end{pmatrix} \tag{4}$$

And now, suppose that from the seed value, the OC matrix is scrambled as follows:

$$SOC = \begin{pmatrix} 1001 \\ 1100 \\ 1111 \\ 1010 \end{pmatrix} \tag{5}$$

Suppose also that the 2D image is 2 x 2, with the following values:

$$I_{2D} = \begin{pmatrix} 1 & 3 \\ 2 & 0 \end{pmatrix} \tag{6}$$

Note that the highest value of I_{2D} for the current example is 3; thus, the system can work with 2-OVSF. For our proposed method, the highest intensity of a pixel is 255, and therefore, it is necessary to work with 8-OVSF.

Continuing the example, I_{2D} is rearranged into a 1D array, resulting in:

$$I_{1D} = \begin{pmatrix} 1 & 3 & 2 & 0 \end{pmatrix} \tag{7}$$

Then, each value of OI_{1D} is used as the multiplexor selector in which the input is SOC and the output is MOI_{2D}. For the current example, row 1 of SOC is selected, followed by row 3, row 2, and row 0. The following matrix is obtained:

$$MI_{2D} = \begin{pmatrix} 1100 \\ 1010 \\ 1111 \\ 1010 \end{pmatrix} \tag{8}$$

Next, MOI_{2D} is transformed to 1D array:

$$MI_{1D} = (1100101011111010) \tag{9}$$

With this 1D array, one sample of the ciphered audio is obtained. However, for the real method proposed in this study, 16 samples are obtained for each pixel of the original image.

Image recovery

The proposed scheme is intended to provide covert communication between a transmitter and receiver. The ciphered audio and the key are transmitted in separate channels, e.g., email, social networks, public webpages, and others. Once the receiver acquires both the ciphered audio and the key, the image can be recovered (see Figure 4).

Each block is explained as follows:

Generation of 8-OVSF codes: This block works in the same way as the corresponding block in the image coding module. The output is named 'OC', with a size of 256 x 256.

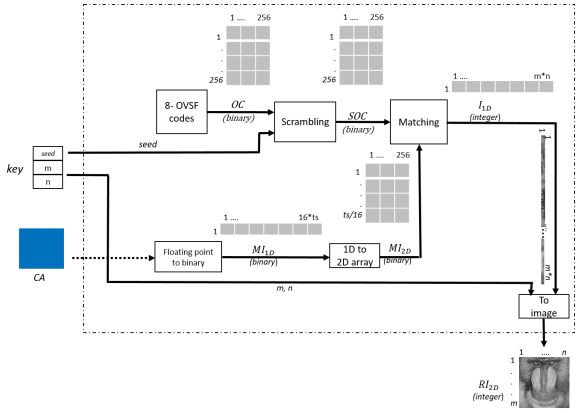

Figure 4. Specific block diagram of the image recovering module.
Source: Authors

Scrambling the 8-OVSF codes: Using the same seed of the image coding module, the OC matrix is reorganized in terms of its rows. The number of available options of the scrambled matrix was discussed in detail in the *Security analysis* section. The output is SOC.

Deciphering the audio: The inputs of this block are the unintelligible, ciphered audio files and the SOC matrix. First, every sample of the ciphered audio, CA, is represented by 16 bits. Second, a 1D array sequence is obtained by the concatenation of all binary representations of CA; this is called MI_{1D}. The total number of bits is calculated using

$$bits = 16 \times ts, (10), \tag{10}$$

where ts is the total number of samples of CA.

Next, MI_{1D} is split into sub-blocks of 256 bits. The number of sub-blocks is obtained by using the ratio between bits and 256; then, the result is $ts/16$. If the process has been performed successfully, $ts/16$ must be equal to $m \times n$. Next, the sub-blocks are arranged into a matrix of $ts/16$ rows with 256 columns named MI_{2D}. This means that every row of MI_{1D} is composed of orthogonal code. Finally, the MI_{2D} code is compared against any SOC code, and subsequently restores the row position of the corresponding match, named I_{1D}.

Creating the grayscale image: Inputs of this block include the key (specifically the values of m and n) and I_{1D}, which is reorganized into a matrix of $m \times n$. The result is the recovered image, I_{2D}.

The above steps are illustrated through an example:

In a similar way to the previously outlined example regarding the image coding module, suppose the system works with 2-OVSF codes and the orthogonal codes are '1111', '1100', '1010', and '1001'. The value of the OC matrix is:

$$OC = \begin{pmatrix} 1111 \\ 1100 \\ 1010 \\ 1001 \end{pmatrix} \tag{11}$$

From the same seed value of the image coding module, the OC matrix is scrambled as follows:

$$SOC = \begin{pmatrix} 1001 \\ 1100 \\ 1111 \\ 1010 \end{pmatrix} \tag{12}$$

In addition, suppose the binary sequence value obtained from the CA is $MI_{1D} = [1100101011111001]$. Since the system works with 2-OVSF, the length of every orthogonal code is 4 bits, and MOI_{1D} is split into 4-bit sub-blocks. The result is the following MI_{2D} value:

$$MI_{2D} = \begin{pmatrix} 1100 \\ 1010 \\ 1111 \\ 1010 \end{pmatrix} \tag{13}$$

The first MI_{2D} code, '1100', is compared against each SOC code as the algorithm searches for a match. It is found that if row zero of MI_{2D} is equal to the first row of SOC, then the returned value is 1. If the first row of MI_{2D}, '1010', is matched with the third row of SOC, then the returned value is 3. Next, the second row of MI_{2D}, '1111', is matched with the 2^{nd} row of SOC, and the returned value is 2. Finally, the 3^{rd} row of MI_{2D}, "1001", is matched with row zero of OC, and the returned value is 0. At the end, the returned value is $I_{1D} = [1320]$. With $m = 2$ and $n = 2$, the recovered image is:

$$RI_{2D} = \begin{pmatrix} 1 & 3 \\ 2 & 0 \end{pmatrix} \tag{14}$$

It is easy to verify that RI_{2D} is equal to I_{2D}.

Performance assessment

Certain metrics have been selected in order to evaluate the performance of the proposed method in terms of similarity between the input image and the recovered image, as well as the quality of the CA.

Metrics to evaluate image similarity

Among the metrics commonly used to measure the image similarity are the Structural Similarity Index (SSIM) and Peak Signal to Noise Ratio (PSNR). These metrics are explained below.

Structural Similarity Index (SSIM): Consider the comparison of two images (A and B), considering luminance (*l*), contrast (c), and structural (s) terms, as follows:

$$\begin{aligned} l(A,B) &= \frac{2\mu_A\mu_B+c_1}{\mu_A^2+\mu_B^2+c_1} \\ c(A,B) &= \frac{2\sigma_A\sigma_B+c_2}{\sigma_A^2+\sigma_B^2+c_2} \\ s(A,B) &= \frac{\sigma_{AB}+c_3}{\sigma_A\sigma_B+c_3} \end{aligned} \tag{15},$$

where μ is the mean, σ is the standard deviation, and CC_1, C_2, and C_3 are constants. With the above results, SSIM is obtained via the following multiplication:

$$SSIM(A,B) = l(A,B) \times c(A,B) \times s(A,B) \tag{15}$$

Using $C3 = 0.5 \times C2$, the Equation above is re-written as:

$$SSIM\,(A,B) = \frac{(2\mu_A\mu_B + c_1)\,(2\sigma_{AB} + c_2)}{(\mu_A^2 + \mu_B^2 + c_1)\,(\sigma_A^2 + \sigma_B^2 + c_2)} \tag{16}$$

SSIM ranges between 0 and 1. The lowest value implies that the structural similarity is null; otherwise, similarity would be high.

***Peak Signal to Noise Ratio* (*PSNR*)**: It is commonly used to compare two images. It is obtained as follows:

$$PSNR = 10 \times \log_{10}\left(\frac{255^2}{MSE}\right) \tag{17}$$

With

$$MSE = \frac{1}{m \times n}\sum_{i=1}^{m \times n}(A_i - B_i)^2 \tag{18}$$

where MSE is the Mean Squared Error, A and B are the images, and the index i represents the absolute position of the pixel (e.g., left to right and up to down). If A and B are equal, then MSE is 0 and PSNR is ∞. Higher values of PSNR are preferable.

Metrics to evaluate quality of the ciphered audio

A good CA file has unintelligible content, meaning that it should appear and sound like noise. Mathematically, this implies that neither neighboring samples are correlated, nor is its entropy low. One way to measure intercorrelation is by using DS metric through Equation (20):

$$DS = \frac{\sum_{i=2}^{m-1}\sqrt{|CA_i - CA_{i-1}| + |CA_i - CA_{i+1}|}}{m-2}, \tag{19}$$

where CA_i is the current sample of CA, CA_{i+1} is the right sample of CA_i, CA_{i-1} is the left sample of CA_i, and m is the total number of samples. Taking into account that natural audio signals are highly intercorrelated, the current sample should be very similar to its neighbors, with the resulting DS being very low. On the other hand, in CA files, the difference between paired neighbor samples is high. The highest value of DS is illustrated in Figure 5 as an example.

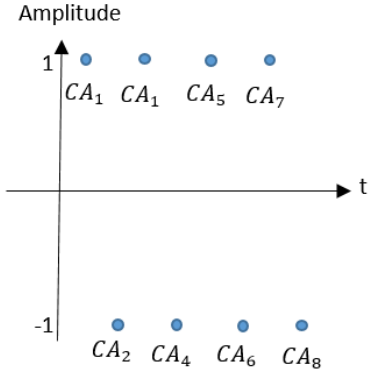

Figure 5. SHighest distance between neighbors.
Source: Authors

Suppose the odd samples are equal to 1; and the even samples, equal to −1. The dynamic range of that signal is 2. Then, by using Equation (20), DS is obtained:

$$DS = \frac{\sum_{i=2}^{m-1}\sqrt{|2| + |2|}}{m-2} = \frac{\sum_{i=2}^{7}(2)}{m-6} = 2 \tag{20}$$

The result above is the maximum DS value for audio signals with a dynamic range of 2. However, in a real-world scenario, if the audio signal is quantized to 16 bits, the total number of different values is 216, distributed in the range [−1 1], with a mean close to 0. Then, a maximum DS value would be:

$$DS_{\max} = \sqrt{|CA^+ - \mu| + |CA^- - \mu|} \tag{21}$$

Where $CA+$ is the highest value of CA, CA^- is the lowest value of CA, and μ is the mean of the audio signal. For $CA^+ = 1$, $CA^- = -1$, and $\mu = 0$, $DS_{\max}$ is equal to $\sqrt{2}$. This means that the ciphered data has unintelligible content.

On the other hand, entropy is a well-known metric to measure the uncertainty of data and quality of CA. For unintelligible audio content with a uniform distribution (i.e., all values being likely), entropy is equal to the number of quantization bits. For example, if the audio is represented with 16 bits, the audio content will be highly unintelligible, due to an entropy value of 16. In other words, the lower the entropy value, the higher the intelligibility of the audio. The formula for entropy was presented in the *Entropy* Section.

Validation

The aim of this section is to validate the performance of the proposed system in terms of the quality of the CA and the recovered image as well as the security analysis. A total of 20 grayscale images (128 x 128 pixels) were used as input for the image coding module; each image is ciphered with 200 keys. At the end, 4000 CA signals were obtained. Figure 6 shows the selected grayscale images.

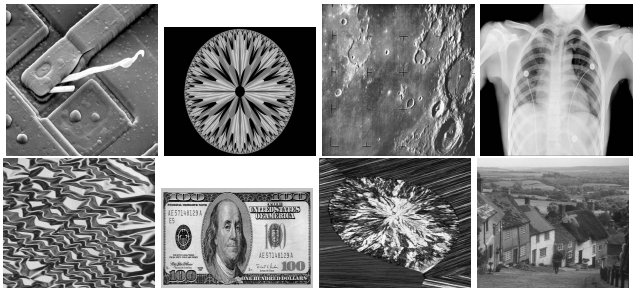

Figure 6. Twenty grayscale images for the validation stage.
Source: Open Source

Preliminary results

The performance of the proposed method is illustrated for three images. Figure 7 shows the original image, the CA, and the recovered image; Figure 8 shows the data distribution (image and CA); and Figure 9 shows the data correlation. According to the results shown in Figure 7, each recovered image is highly similar to the input image. In all three cases, the SSIM is higher than 0,999 and PSNR is ∞. Additionally, the ciphered signals look like noise, with a maximum value of 1 and minimum value of −1. Histograms of the CA signals (Figure 8(b), 8(d), 8(f)) are quasi-uniform, even though the histograms of the images are not uniform (Figure 8(a), 8(c), 8(e)). The entropy of the images is around 6 for 8 bits of quantization (75%), while the entropy of the CA files is 15,75 for 16 bits of quantization (98,5%). These results suggest that the system performed as expected. Finally, Figure 9 shows the behavior of adjacent (horizontal) pixels and neighboring samples. It is clear that the original image is highly correlated because the behavior of the adjacent pixels is around the main diagonal. However, in the case of neighboring samples (audio signal), the data is uncorrelated because the results are scattered in all directions.

Quality of the ciphered audio and the recovered image

This section tests the performance of the proposed method in terms of the quality of the recovered images and their CA files. For the first group of tests, SSIM (Figure 10) and PSNR between the input image and the recovered image were calculated. For the second group, the DS of the CA, entropy of the input image, and entropy of the CA were measured (Figure 11).

Figure 10 shows a very high structural similarity between the input image and the recovered images for all 4000 tests. SSIM values are around 1, and higher than 0,9999990. The PSNR values of 15 images were ∞, while the others were higher than 90 dB. Considering the results above, it means that the proposed method is reversible.

Figure 11(a) shows the entropy results for 4000 CA files. Most of the results (95% confidence) are between 15,75 and 15,78. Therefore, the CA signals are very close to perfectly demonstrating the behavior of unintelligible data (i.e., 16 for data quantized with 16-bits). Regarding DS (Figure 11(b)),

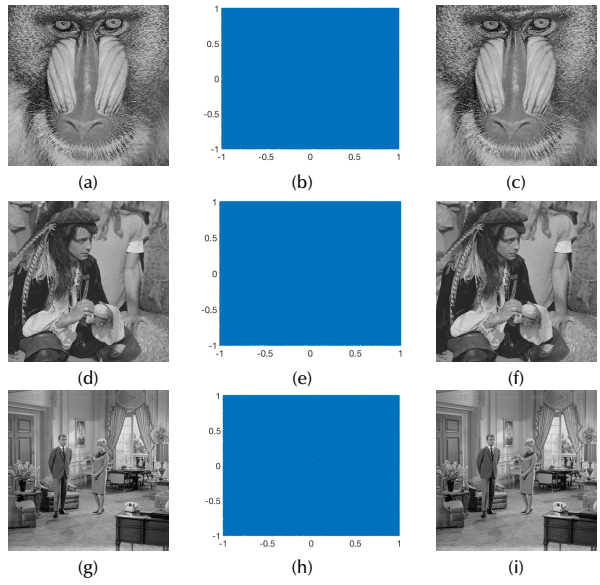

Figure 7. Quality analysis: (a-c) Show input images, (d-f) Show their ciphered audio signals, and (g-i) Show the recovered images.
Source: Open Source and Authors

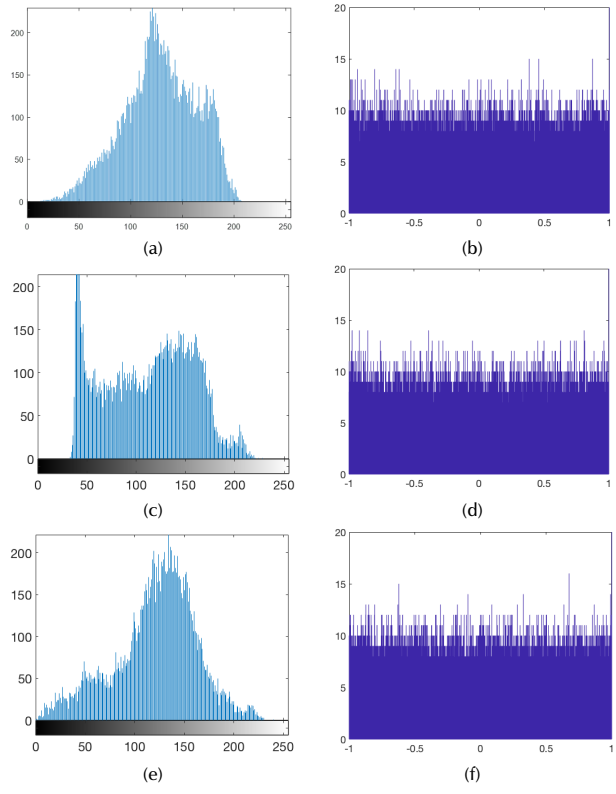

Figure 8. Data distribution analysis: Graphs (a, c, e) show the histogram of the input images, (b, d, f) show histograms of the ciphered data.
Source: Authors

most of the data is in the range [1,1 1,13], which is very close to the expected value (i.e., 1,41). Therefore, the high-quality standard of the ciphered data is verified.

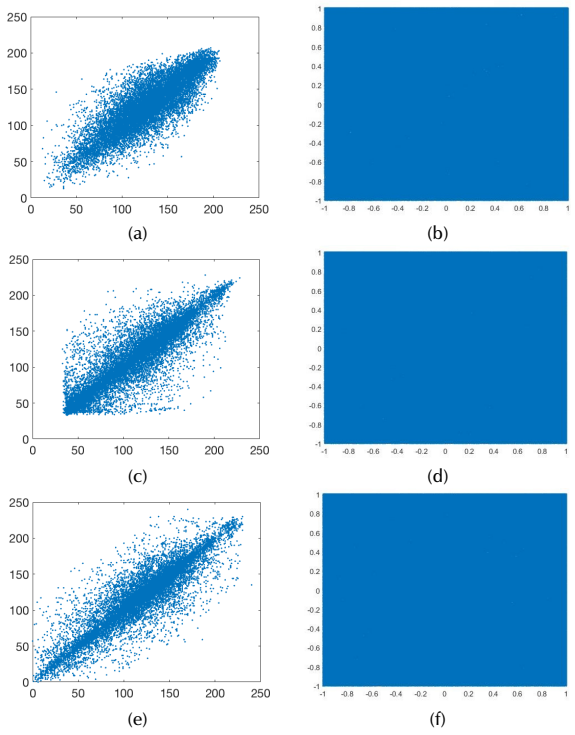

Figure 9. Data correlation: (a, c, e) Show adjacent pixels, graphs (b, d, f) show adjacent samples of their ciphered data.
Source: Authors

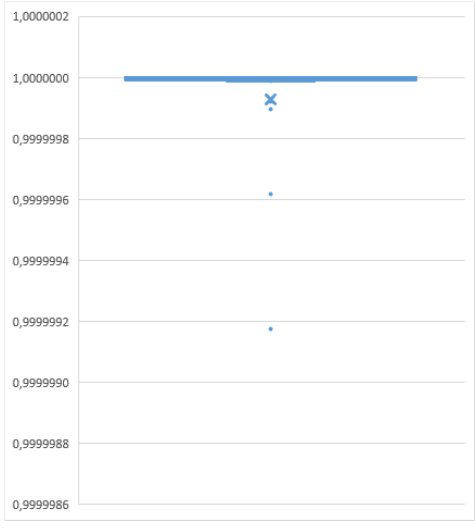

Figure 10. Quality of the recovered image: SSIM.
Source: Authors

Security analysis

The following step in the validation process consists of analyzing and testing the security of the proposed method. First, a theoretical analysis is performed on the key space. Secondly, key sensitivity is measured through several tests.

Key space: According to Shannon's theory, the security of a system must rely solely on the key. It is assumed that the details of the method (e.g., image coding and decoding modules) are known by a third person (e.g., eavesdropper). Then, the keys must satisfy the following conditions:

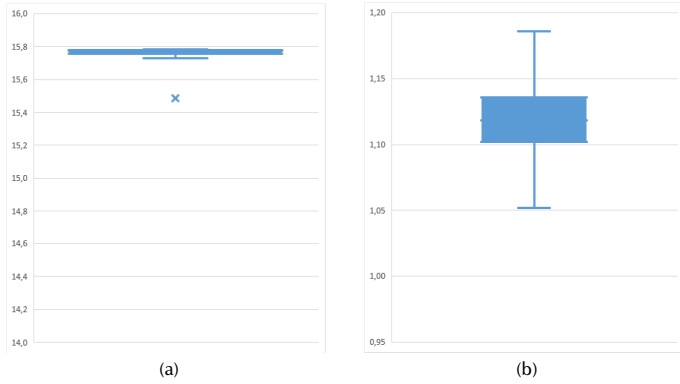

Figure 11. Quality of the ciphered data: (a) Entropy, (b) DS.
Source: Authors

- The number of keys must be large enough to resist a force attack, at least for a considerably long time.
- All keys must be of equal likelihood, which means that the uncertainty of the keys (entropy) must be as high as possible.
- Using a different key must provide a different output.

Albeit the third parties have enough time and hardware resources for testing all the keys, they have no certainty of which one is correct.

To satisfy the first condition, our proposed system uses a seed value as an input for a pseudo-random number generator, which reorganizes the 8-OVSF matrix. Then, there are many available scrambled matrices as the factorial of the number of orthogonal codes. That is, the key space is $256! = 8{,}57 \times 10^{506}$. The reader can then verify that the above-mentioned value is the same as in Ballesteros et al. (2018). For the second condition, the method works with seed values of different lengths and characteristics (e.g., only numbers, only letters, hybrid, uppercase and/or lowercase). The third condition is analyzed in the following section.

Key sensitivity analysis: Although the first two conditions of Shannon's theory are satisfied, the system can still be insecure if two slightly different keys provide the same results. This means that the key sensitivity must be verified as well. At the receiver, the original key is slightly changed (e.g., an upper case instead of a lower case of the same character), and next, the new key is used in the image recovering module. Thus, the dissimilarity between the input image and the recovered image is expected to be high. SSIM is selected to compare the images.

Figure 12 shows an example of this test, using the key "Shannon" in the transmitter, whereas the key "Shannon" is used in the receptor. Figure 13 shows the results (confidence range) of SSIM between the original image and the recovered image for 200 tests.

Figure 12. Example of recovered image using a slight change in the key in the recovering module.
Source: Authors

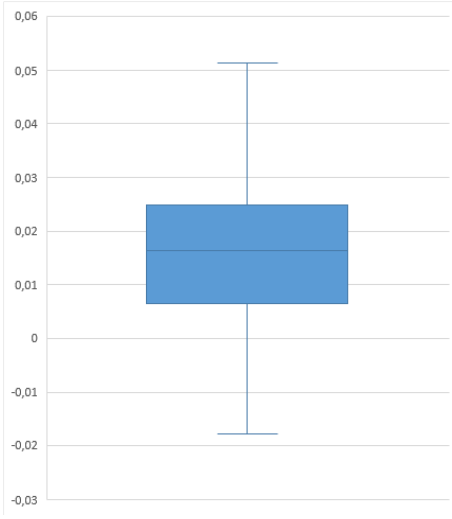

Figure 13. Key sensitivity analysis (confidence range of 95%): SSIM between the input image and the recovered image with a slight change in the key.
Source: Authors

According to Figure 12 and Figure 13, the structural similarity is very low. The ciphered data is very sensitive to the key. That is, if the non-authorized user has access to the ciphered data and knows the method but not the exact key, the original content will not be revealed.

Comparison with state-of-the-art methods

Most of the image encryption methods provide a ciphered image in which the size of the original image is preserved. In our proposal, the output is an audio signal instead of an image. For this reason, comparison to the state-of-the-art methods is divided into three parts: a) image-to-image encryption (Table 1), b) audio-to-audio encryption (Table 2), and c) image-to-audio encryption (Table 3). In all cases, the entropy of the ciphered data (quality of the process) and key space (security of the method) were taken into account.

According to Table 1, the image encryption methods reached a very high entropy value for the encrypted data. However, in audio encryption methods (Table 2), there is still a need for improvement in terms of entropy. In terms of the key space, audio encryption methods are better than image encryption ones. In conclusion, the strength of the image encryption methods is the weakness of the audio encryption methods and vice-versa.

Table 1. Image to image encryption: comparison with some related works

Reference	Core of the method	Entropy	Key space	Cryptanalyzed
Hayat et al., 2019	Elliptic curve	7,97 (8 bits) = 99,6%	10^{38}	Li et al., 2014; Feng et al., 2019
Ye et al., 2017	Logistic map (i.e., 1D chaotic map)	7,99 (8 bits) = 99,8%	10^{42}	
Asgari et al., 2019	Chaotic map (i.e., 2D or 3D)	7,99 (8 bits) = 99,8%	10^{48}	
Chai et al., 2019	DNA sequence	7,99 (8 bits)= 99,8%	10^{98}	

Source: Authors

Table 2. Audio to audio encryption: comparison with some related works

Reference	Core of the method	Entropy	Key space	Cryptanalyzed
Hameed et al., 2018	Logistic map	15,96 (16 bits) = 99,7%	10^{38}	No yet
Belmeguenai et al., 2017	Pseudo-random generator	Not reported	10^{154}	
Renza et al., 2019	Collatz coding	7,50 (8 bits) = 93,7%	10^{506}	
Kalpana et al., 2019	Bidirectional associative memory	Not reported	10^{540}	

Source: Authors

Table 3. Image to audio encryption: comparison with our predecessor

Reference	Core of the method	Entropy	Key space	Cryptanalyzed
Ballesteros et al., 2018	Collatz coding	14 (16 bits) = 87,5%	10^{506}	No yet
ours	8-OVSF coding	15,77 (16 bits) = 98,5%	10^{506}	

Source: Authors

Conclusions

The purpose of this research was to increase the entropy of encrypted data obtained by encryption methods (i.e. 87,5%), while preserving the key space (10^{506}). the mapping process between the pixels of an image and the resulting orthogonal codes provided ciphered data with a very high entropy percentage (98,5%) in a similar way to that of image encryption methods based on chaotic mapping (99,6%).

Taking into account that the image encryption methods based on this encoding method have yet to be been broken and the results of several tests demonstrated high key sensitivity (i.e., SSIM = 0,015 between the original image and the recovered image with a slight change in the key), it is concluded that the aforementioned challenge has been overcome, i.e., the transmitted content remains private and can only be revealed by authorized personnel.

Acknowledgements

This research was funded by "Vicerrectoría de Investigaciones, Universidad Militar Nueva Granada" under grant IMP-ING-2936 of 2019

References

Akhavan, A., Samsudin, A., and Akhshani, A. (2017). Cryptanalysis of an image encryption algorithm based on DNA encoding. *Optics and Laser Technology, 95*, 94-99. 10.1016/j.optlastec.2017.04.022

Asgari-Chenaghlu, M., Balafar, M. A., and Feizi-Derakhshi, M. R. (2019). A novel image encryption algorithm based on polynomial combination of chaotic maps and dynamic function generation. *Signal Processing, 157*, 1-13. 10.1016/j.sigpro.2018.11.010

Ballesteros, D. M., Peña, J., and Renza, D. (2018). A Novel Image Encryption Scheme Based on Collatz Conjecture. *Entropy, 20*(21), 901. 10.3390/e20120901

Belmeguenai, A., Ahmida, Z., Ouchtati, S., and Djemii, R. (2017). A novel approach based on stream cipher for selective speech encryption. *International Journal of Speech Technology, 20*(3), 685-698. 10.1007/s10772-017-9439-8

Broumandnia, A. (2019). Designing digital image encryption using 2D and 3D reversible modular chaotic maps. *Journal of Information Security and Applications, 47*, 188-198. 10.1016/j.jisa.2019.05.004

Chai, X., Gan, Z., Yuan, K., Chen, Y., and Liu, X. (2019). A novel image encryption scheme based on DNA sequence operations and chaotic systems. *Neural Computing and Applications, 31*(1), 219-237. 10.1007/s00521-017-2993-9

Feng, W., He, Y., Li, H., and Li, C. (2019). Cryptanalysis and improvement of the image encryption scheme based on 2D logistic-adjusted-sine map. *IEEE Access, 7*, 12584-12597. 10.1109/ACCESS.2019.2893760

Fridrich, J. (1998). Symmetric ciphers based on two-dimensional chaotic maps. *International Journal of Bifurcation and chaos, 8*(06), 1259-1284. 10.1142/S021812749800098X

Hameed, Y. and Ali, N. (2018). An efficient audio encryption based on chaotic logistic map with 3D matrix. *Journal of Theoretical and Applied Information Technology, 96*, 5142-5152.

Hayat, U. and Azam, N. A. (2019). A novel image encryption scheme based on an elliptic curve. *Signal Processing, 155*, 391-402. 10.1016/j.sigpro.2018.10.011

Hua, Z., Jin, F., Xu, B., and Huang, H. (2018). 2D Logistic-Sine-coupling map for image encryption. *Signal Processing, 149*, 148-161. 10.1016/j.sigpro.2018.03.010

Kalpana, M., Ratnavelu, K., and Balasubramaniam, P. (2019). An audio encryption based on synchronization of robust BAM FCNNs with time delays. *Multimedia Tools and Applications, 78*(5), 5969-5988. 10.1007/s11042-018-6373-y

Khoirom, M. S., Laiphrakpam, D. S., and Themrichon, T. (2018). Cryptanalysis of multimedia encryption using elliptic curve cryptography. *Optik, 168*, 370-375. 10.1016/j.ijleo.2018.04.068

Kumar, R. and Quan, C. (2019). Asymmetric multi-user optical cryptosystem based on polar decomposition and Shearlet transform. *Optics and Lasers in Engineering, 120*, 118-126. 10.1016/j.optlaseng.2019.03.024

Li, C., Xie, T., Liu, Q., and Cheng, G. (2014). Cryptanalyzing image encryption using chaotic logistic map. *Nonlinear Dynamics, 78*(2), 1545-1551. 10.1007/s11071-014-1533-8

Liu, J. M. and Qu, Q. (2010, October). Cryptanalysis of a substitution-diffusion based image cipher using chaotic standard and logistic map. In Qingling, l., Fei, Y., and Yun L. (Eds.) *2010 IEEE Third International Symposium on Information Processing* (pp. 67-69), Qingdao, China: IEEE. 10.1109/ISIP.2010.33

Patidar, V., Pareek, N. K., and Sud, K. K. (2009). A new substitution–diffusion based image cipher using chaotic standard and logistic maps. *Communications in Nonlinear Science and Numerical Simulation, 14*(7), 3056-3075. 10.1016/j.cnsns.2008.11.005

Renza, D., Mendoza, S., and Ballesteros L, D.M. (2019). High-uncertainty audio signal encryption based on the Collatz conjecture. *Journal of Information Security and Applications, 46*, 62-69. 10.1016/j.jisa.2019.02.010

Robinson, D. W. (2008). Entropy and uncertainty. *Entropy, 10*(4), 493-506. 10.3390/e10040493

Saini, D. S. and Bhooshan, S. V. (2006, July). Adaptive assignment scheme for OVSF codes in WCDMA. In Dini, P., Christer, Å., Dini, C., and Borcoci, E. (Eds.) *2006 IEEE International Conference on Wireless and Mobile Communications (ICWMC'06)* (pp. 65-65), Bucharest, Romania: IEEE. 10.1109/ICWMC.2006.15

Saljoughi, A. S. and Mirvaziri, H. (2019). A new method for image encryption by 3D chaotic map. *Pattern Analysis and Applications, 22*(1), 243-257. 10.1007/s10044-018-0765-5

Shannon, C. E. (1949). Communication theory of secrecy systems. *The Bell system technical journal, 28*(4), 656-715. 10.1002/j.1538-7305.1949.tb00928.x

Telem, A. N. K., Segning, C. M., Kenne, G., and Fotsin, H. B. (2014). A simple and robust gray image encryption scheme using chaotic logistic map and artificial neural network. *Advances in Multimedia, 2014*. 10.1155/2014/602921

Wang, B., Wei, X., and Zhang, Q. (2013). Cryptanalysis of an image cryptosystem based on logistic map. *Optik, 124*(14), 1773-1776. 10.1016/j.ijleo.2012.06.020

Wen, H., Yu, S., and Lü, J. (2019). Breaking an image encryption algorithm based on DNA encoding and spatiotemporal chaos. *Entropy, 21*(3), 246. 10.3390/e21030246

Ye, G. and Huang, X. (2017). An efficient symmetric image encryption algorithm based on an intertwining logistic map. *Neurocomputing, 251*, 45-53. 10.1016/j.neucom.2017.04.016

Zhang, J., Fang, D., and Ren, H. (2014). Image encryption algorithm based on DNA encoding and chaotic maps. *Mathematical Problems in Engineering, 2014*. 10.1155/2014/917147

Zhu, H., Zhao, Y., and Song, Y. (2019). 2D logistic-modulated-sine-coupling-logistic chaotic map for image encryption. *IEEE Access, 7*, 14081-14098. 10.1109/ACCESS.2019.2893538

redalyc
UAEMEX

Available in:
https://www.redalyc.org/articulo.oa?id=64379866007

How to cite

Complete issue

More information about this article

Journal's webpage in redalyc.org

Scientific Information System Redalyc
Diamond Open Access scientific journal network
Non-commercial open infrastructure owned by academia

Dora Maria Ballesteros, Diego Renza, Jimmy Peña

Entropy-Based Image Encryption Using Orthogonal Variable Spreading Factor (OVSF)
Cifrado de Imágenes Basado en la Entropía Utilizando el Factor de Propagación Variable Ortogonal (OVSF)

Ingeniería e Investigación
vol. 40, no. 3, p. 70 - 80, 2020
Facultad de Ingeniería, Universidad Nacional de Colombia.,
ISSN: 0120-5609
ISSN-E: 2248-8723

DOI: https://doi.org/10.15446/ing.investig.v40n3.81421