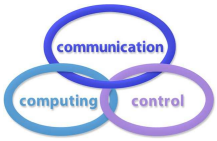
INTERNATIONAL JOURNAL OF COMPUTERS COMMUNICATIONS & CONTROL
Online ISSN 1841-9844, ISSN-L 1841-9836, Volume: 15, Issue: 6, Month: December, Year: 2020
Article Number: 3824, https://doi.org/10.15837/ijccc.2020.6.3824



CCC Publications

Watermarking for the Secure Transmission of the Key into an Encrypted Image

A. Khalfallah, M.K. Abdmouleh, M.S. Bouhlel

Ali Khalfallah*
Research Unit: Sciences and Technologies of Image and Telecommunications
Higher Institute of Biotechnology
University of Sfax
Sfax, Tunisia
*Corresponding author: ali.khalfallah@enetcom.usf.tn

Med Karim Abdmouleh
Research Unit: Sciences and Technologies of Image and Telecommunications
Higher Institute of Biotechnology
University of Sfax
Sfax, Tunisia
medkarim.abdmouleh@isggb.rnu.tn

Med Salim Bouhlel
Research Unit: Sciences and Technologies of Image and Telecommunications
Higher Institute of Biotechnology
University of Sfax
Sfax, Tunisia
medsalim.bouhlel@isbs.usf.tn

Abstract

Ensuring the confidentiality of any data exchanged always presents a great concern for all communication instances. Technically, encryption is the ideal solution for this task. However, this process must deal with the progress of the cryptanalysis that aims to disclose the information exchanged. The risk increases due to the need for a dual transmission that includes the encrypted medium and the decryption key. In a context of chaotic encryption of images, we propose to insert the decryption key into the encrypted image using image watermarking. Thus, only the watermarked encrypted image will be transmitted. Upon reception, the recipient extracts the key and decrypts the image. The cryptosystem proposed is based on an encryption using a dynamic Look-Up Table issued from a chaotic generator. The obtained results prove the efficiency of our method to ensure a secure exchange of images and keys.

Keywords: image encryption, image watermarking, crypto-watermarking, cryptanalysis, chaos.

1 Introduction

Recent research presents various information-processing techniques to ensure the confidentiality of data exchange. These concerns also affect the exchange of images. In this context, encryption is the solution most solicited for this kind of application. Several algorithms have been used, including the Advanced Encryption Standard (AES) [32], Data Encryption Standard (DES) [13], chaotic encryption [5, 7], and quantum encryption [1]. These different methods differ in terms of the relationship between the encryption and decryption keys, the complexity, and the size of the information to be encrypted. Yet, they all require a total or partial transmission of the decryption key. This key is typically used in any encrypted communication between the two communicating entities. Thus, besides the encrypted information, the communication must include the key which is the necessary component for decryption. The sending of this key which is presented in the form of a small data frame can arouse the suspicions of its possible interception, and the consequent breaking of the cryptosystem.

Other techniques are proposed to ensure the confidentiality of the communication by hiding the information to be transmitted in another host medium referring to the watermarking and the steganography. The watermarking consists in inserting the information to be hidden in an image without introducing a great distortion to the host document [2]. This limitation reduces the insertion capacity, which makes it unsuitable for hosting a large image. On the other hand, steganography [14, 20, 29, 31] allows the mixing of two or more images leaving the cover image visible while allowing to hide the other images [10]. Unfortunately, this mixing can cause visible distortion on the cover image and the embedded images during their extraction, which is not suitable for certain applications such as in the medical or industrial domains.

In this paper, we propose a security approach that combines encryption and watermarking. This combination was mentioned previously by W. Puech and J.M. Rodrigues in [34] and it was based on the RSA encryption and watermarking in the image frequency representation. In this work, we have opted for chaotic encryption and an image watermarking in the space domain. In addition, we deepened our cryptanalysis study and studied the impact of watermarking on the security of the image to be transmitted. Indeed, the image is encrypted by a chaotic cryptosystem whose key is hidden using the watermarking in the same encrypted medium. Thus, a single file will be transmitted to the receiver and it will be easily deciphered. On the other hand, the ignorance of the decryption key or the watermarked components of the image leads to the failure of decryption. Moreover, this new condition will constitute another obstacle for any attempt at cryptanalysis and allows the communicating entities to regularly and easily change the parameters of their cryptosystem. To explain our approach, we present the principle of image watermarking in the first section. Next, we present the principle of image encryption. In Section 4, we detail our approach of image watermarked encryption. The obtained results are illustrated and discussed in Section 5. Finally, we end the paper with our conclusions and perspectives.

2 Image watermarking

Image watermarking consists in the insertion of a digital sequence (real or binary), called signature, in an image. This insertion can be done in one of the different representations of the image such the spatial [8], frequency [28], and multiresolution [22] domains. It is carried out in the association of selected components of the image with the elements of the signature using one of the following Equations (1-4) [19].

$$y_i = x_i + \alpha w_i \tag{1}$$

$$y_i = x_i \left(1 + \alpha\right) w_i \tag{2}$$

$$y_i = x_i e^{\alpha w_i} \tag{3}$$

$$y_i = x_i \left(1 + \frac{\alpha}{\log(|x_i|)} w_i\right) \tag{4}$$

where x_i, y_i, w_i, i, α are the image components selected to carry the mark, the watermarked components of the resulting image, the signature element, the index of the image element to watermark, and the visibility coefficient of the signature to insert, respectively.

The second phase is to extract the inserted signature or to detect its presence by exploiting the watermarked image for blind watermarking, the signature supposed to have been inserted in the case of the semi-blind and the original image for the non-blind watermarking.

The insertion of the signature must be imperceptible and robust by allowing its extraction or detection as long as the image is exploitable. Thus, the assessment of watermarking essentially affects the distortion of the watermarked image which can be quantified by the Peak Signal Noise Ratio (PSNR) [21] derived from the Mean Square Error (MSE) or the Structural Similarity Index Metric (SSIM) [24] and the signature distortion by comparing the extracted signature with the inserted signature. This can be quantified in terms of correlation and by the Bit Error Rate (BER).

Image watermarking has emerged as a copyright protection [23] tool by inserting the work owner signature to conquer new areas such as fingerprinting [25] disclosing illegal copies, integrity checking and indexing [27] of images by inserting into the host medium its summary, medical ethics by inserting the patient record in its medical image [33], and image compression based on image resizing by embedding an enlargement technique code in each block of the reduced image [9].

3 Image encryption

In the digital world of today, the security of transmitted digital images/videos becomes more and more vital, against increasingly vicious web attacks. Cryptography is used to ensure security in open networks because of its being the science that uses mathematics to offer encryption algorithms to protect information. Researchers have focused on the image encryption in an attempt to cope with the recent fast exchange and transmission of digital images over the internet [39].

3.1 Encryption techniques

Many cryptographic methods have been proposed. These techniques are classified into three main categories. First, symmetric cryptography uses the same key for encryption and decryption. Data Encryption Standard (DES), Advanced Encryption Standard (AES) and chaotic encryption [3, 4, 30, 38] are the best known examples of symmetric encryption. Second, asymmetric cryptography uses two different keys. The earliest realization of a public key algorithm, called RSA [35] following the names of its inventors Rivest, Shamir and Adelman, is the most used algorithm in asymmetric encryption. The third category of methods is the hybrid cryptography which combines the best features of symmetric and asymmetric cryptographic methods [17].

3.2 Cryptanalysis

While cryptography is the discipline that ensures the security of confidential information, cryptanalysis is the discipline that studies and validates the robustness of cryptosystems against attacks [38]. According to Kerckhoffs, the security of a cryptosystem depends on the secrecy of the key and not on that of the encryption algorithm. To study the cryptosystem security, we can utilize the Kerckhoffs principle. In this case, the cryptanalyst must be unable to find the key even if s/he has access to the plaintext and its corresponding ciphertext. S/He tries to apply more attacks such as ciphertext-only, chosen plaintext, known plaintext and chosen ciphertext attacks.

3.3 Assessment metrics

The large size, the high redundancy and the correlation that exist between the neighboring pixels of an image are interesting properties that differentiate the image information from that of the visual

and textual information. These properties are at the origin of some evaluation criteria defined by key space analysis, key sensitivity, differential and statistical attacks. A good cryptosystem must be immune to all types of attack.

In fact, to have a secure encryption system, the key space must be expanded to withstand the Brute-Force Attack. Therefore, it is recommended to encode the decryption key on at least 512 bits [6]. Moreover, a small modification on the decryption key must not provide any information about the original image [6]. On the other hand, differential analysis quantifies the effect of a slight variation of the clear message on the encrypted message [12]. In fact, a single pixel modification yields an NPCR (Number of Pixels Change Rate) of more than 99% and a UACI (Unified Average Changing Intensity) close 33% when comparing the encrypted original and the encrypted modified images [18, 36, 40]. Lastly, statistical analysis highlights the image encryption impact. An encrypted image must be totally different from the original image and without any static resemblance in terms of histograms and neighbor pixels correlation. Thus, the entropy of a grayscale encrypted image must be very close to 8 bits/pixel [37] and the adjacent pixels correlation must be almost zero [11].

4 Proposed approach

The purpose of this work is to insert the decryption key into the encrypted image. Therefore, only one file is sent to the recipient. From this file, the recipient retrieves the decryption key inserted in the image and uses it to decrypt the received image. This requires a combination of watermarking and encryption. This technique is called watermarked encryption, and its principle is detailed in this section.

4.1 Principal

During this exchange of images, only 2 entities intervene: the sender and the recipient. Each of these two entities has an identifier necessary for the encryption/decryption of the exchanged image. To further complicate the task of the hackers, a third key of decryption will be added in our cryptosystem. To transmit this last decryption key, the sender inserts it into the encrypted image using Least Significant Bit (LSB) watermarking.

As shown in Figure 1, the encryption of the image begins with a chaotic rearrangement of the image pixels (CRP_1) parameterized by the identifier of the recipient (Subkey: Key_1). The ordered pixels ($CiphIm_1$) will be split into 2 sub-groups: GRP_1 and GRP_2. The 7 most significant bits of GRP_1 will be encrypted by a chaotic cryptosystem (CRP_3) based on the dynamic Look-Up Table (7-bit Ch. Dyn. LUT) parameterized by a subkey (Key_3) chosen by the sender. We continue in the same encryption procedure to encrypt GRP_2 by spreading out the chaotic dynamic LUT to cipher 8 bits (CRP_4: Ch. Dyn 8-bit LUT). The Key_3 subkey that can change value must keep the same structure for any encrypted image exchange. The number of pixels of GRP_1 will be equal to the number of bits of Key_3. The concatenation of ciphered GRP_1 and ciphered GRP_2 will then form the encrypted image $CiphIm_2$. The sender must cipher the Key_3 subkey by a chaotic cryptosystem based on the 8-bit dynamic LUT (CRP_2: 8-bit Ch. Dyn. LUT) parameterized by its identifier (Key_2). After its encryption, the subkey Key_3 will be inserted into the least significant bits of the first pixels of $CyphIm_2$, which corresponds to the LSB of the ciphered GRP_1. The image resulting from this watermarking will be named $CiphIm_2W$. The last step of our cryptosystem consists in restoring the initial order of pixels by the decryption of $CiphIm_2W$ by the cryptosystem CRP_1. Thus, we get our final encrypted image $CyphIm$.

Thus, upon reception, the recipient begins by encrypting the received image ($CiphIm$) by CRP_1. Then, the ciphered subkey $CiphKey_3$ is extracted and deciphered by CRP_2 to recover Key_3. The pixels of the resulting image will be split into two subgroups to recover the ciphered GRP_1 ($CiphGRP_1$) and the ciphered GRP_2 ($CiphGRP_2$). After that, the 7 most significant bits of $CiphGRP_1$ are deciphered by CRP_3 to have GRP_1 and the pixels of $CiphGRP_2$ using CRP_4 to recover CRP_2. The concatenation of GRP_1 and GRP_2 gives $CiphIm_1$. Finally, the pixels of this image will be repositioned at their initial distribution by applying the decryption scheme of CRP_1 to retrieve the decrypted image.

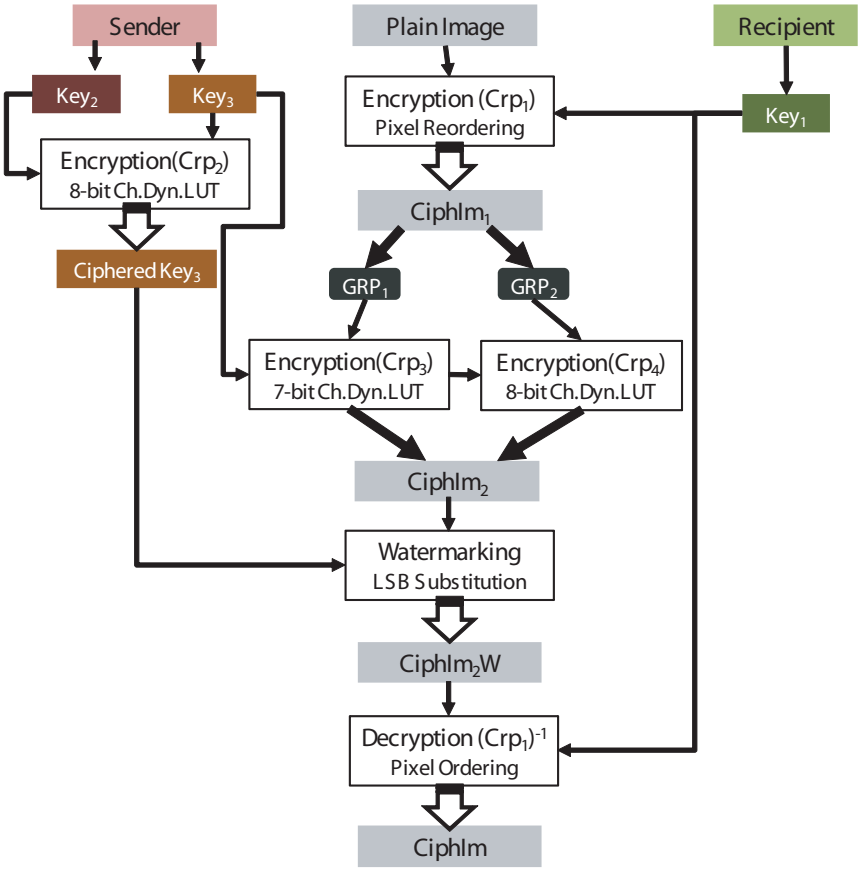


Figure 1: Principle of the proposed approach

4.2 Logistic Map function for chaotic encryption

A chaotic system is very sensitive to its initial value and its parameters [5]. Such a system presents a random and deterministic aspect [7]. Therefore, it is widely used in cryptography and particularly for image encryption [16, 26]. In this context, the Logistic Map (LM) function is one of the most used kernels to generate a chaotic signal. The expression of this function is as follows [11, 15]:

$$X_{n+1} = \mu \times (1 - X_n) \tag{5}$$

With: X_n belongs to $[0, 1]$ whatever is n, and μ is a control parameter where $0 < \mu \leq 4$.

Yet, to ensure a perfectly chaotic behavior, we must have μ between 3.9 and 4 and the generated chaotic values are included in the interval $[0, 1]$. The LM function will be the kernel of our chaotic sequence generator while imposing some conditions such as the exclusion of values outside an interval $[V_{\min}, V_{\max}]$and the first N values generated. The figure below depicts the principle of our generator:

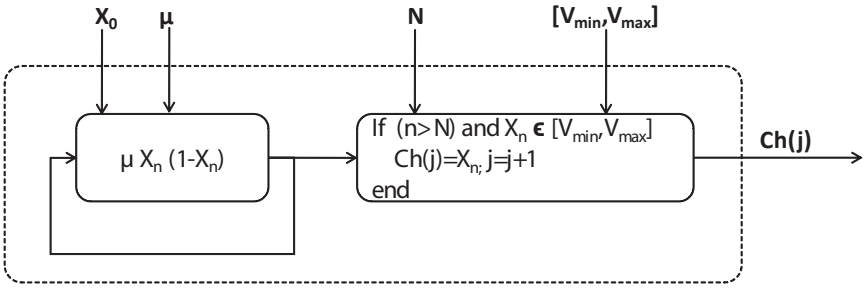


Figure 2: Principle of our chaotic sequence generator

We note that our chaotic generator is parameterized by 5 parameters, namely X_0 (initial condition of the LM function), μ, N, V_{min} and V_{max}. These consist of three reals $(X_0, V_{\min}, V_{\max})$ included in $]0, 1[$, one real (μ) included in $]3.9, 4[$, and a positive integer (N).

4.3 Chaotic encryption by pixel reordering

The encryption of the image starts with a pixels reordering (CRP_1) in order to introduce a discontinuity on the image's profiles. This will make it difficult to break the sub cryptosystems to be used in the following steps. To do this, we will use a chaotic generator based on the chaotic logistic map function parameterized by the identifier of the recipient. Thus, we generate a real chaotic sequence that will be used to reorder the appearance of the pixels. This same chaotic generator will be used at the end of our encryption procedure to reposition the pixels ciphered by CRP_2, CRP_3 and CRP_4 to their initial position.

4.4 Chaotic encryption based on Dynamic Look-Up Table

The generation of a chaotic LUT is a reordering of the gray levels values the pixel can have to cipher it. Indeed, a chaotic LUT generated for a pixel of value P coded on Nb bits consists in reordering the natural integer values ranging from 0 to $2^{Nb}-1$ and to consider the P^{th} value as the encrypted value of P. To create this LUT (Figure 3), we use our chaotic generator parameterized by an initial condition equal to the mean of $Ch\left(2^{Nb}-1\right)$ (the last chaotic value from the chaotic sequence used to create the chaotic LUT of the previous pixel) and the normalized value of the original pixel ($P/2^{Nb}$), the number of iterations to be ignored is none other than the encrypted value of the last pixel P_c. The parameters μ, V_{min} and V_{max} are extracted from Key_2 for the encryption of Key_3 and from Key_3 for the encryption of GRP_1 and GRP_2.

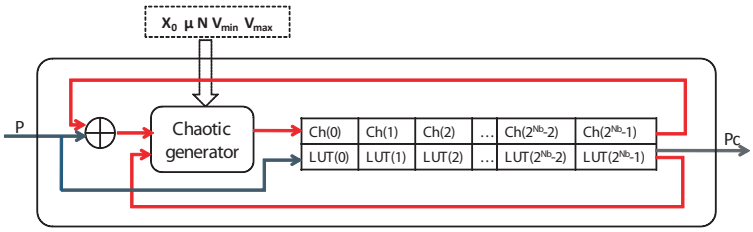


Figure 3: Principle of chaotic dynamic Look-Up Table

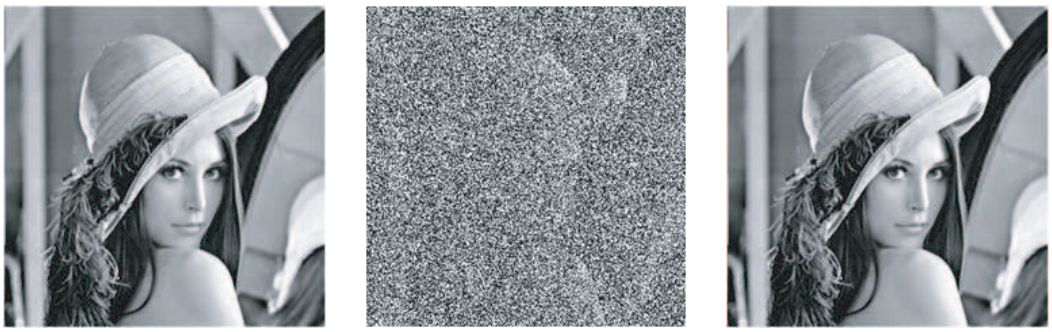
To compute the encrypted value of the first original pixel, the number of ignored iterations N is provided from the cryptosystem's key (Key_2 for CRP_2, Key_3 for CRP_3) while the previous original pixel is considered zero. It is worth noting here that the result of CRP_3. is utilized to cipher GRP_2 by CRP_4.

5 Results and discussion

To assess our proposed cryptosystem, we encrypted and decrypted an image database including 50 grayscale images having 256×256 size using MATLAB 7.6. This mathematical tool codes a real in 8 bytes. Consequently, each one of Key_1 ($\{X_1, \mu_1, N_1, V_{\min 1}, V_{\max 1}\}$), Key_2 ($\{X_2, \mu_2, N_2, V_{\min 2}, V_{\max 2}\}$), and Key_3 ($\{X_3, \mu_3, N_3, V_{\min 3}, V_{\max 3}\}$) is coded on 40 bytes which provides us a global key ($Key = \{Key_1, Key_2, Key_3\}$) coded on 120 bytes, which means 2^{960} combinations of the secret key and space key width equal to 960 bits. However, during an information exchange, Key_1 and Key_2 are fixed by the sender and the recipient, thereby reducing the number of secret key combinations to 2^{320} for a single image exchange.

In fact, Key_3 is inserted into the encrypted image. This watermarking could introduce a slight dissemblance between the original image and the decrypted one. In Figure 4, we illustrate an original image (Figure 4a) and its encrypted (Figure 4b) as well as decrypted counterparts (Figure 4c).

According to Figure 4a and Figure 4c, there is no visual difference between the original image and the decrypted one. Nonetheless, there is a slight difference with a PSNR equal to 74.77dB. This PSNR which is higher than 60dB reflects an imperceptible image distortion. By applying our cryptosystem on the images test bank, we obtain an average PSNR of 74.32dB, which means very high resemblance

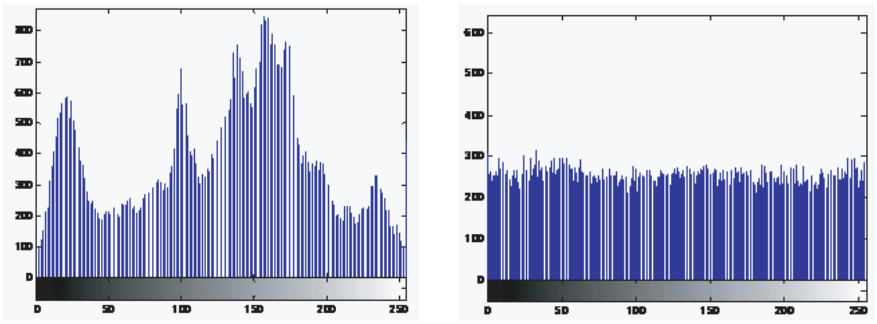


(a) (b) (c)

Figure 4: Example of encrypted/decrypted image using our proposed cryptosystem: (a) Original image, (b) Encrypted image, (c) Decrypted image

between the original images and their decrypted counterparts. Thus, we conclude that the distortion introduced by the watermarking is invisible.

Moving to the statistical analysis, we could visually confirm the great difference between the original image (Figure 4a) and the encrypted image (Figure 4b). Moreover, the histograms of these images (Figures 5a-5b) are very different.



(a) (b)

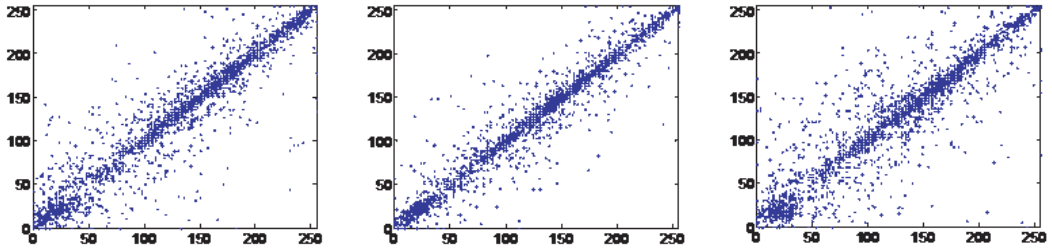
Figure 5: Histogram analysis: (a) Histogram of the original image, (b) Histogram of the encrypted image

The second analysis consists on the study of the correlation between adjacent pixels. This study concerns adjacent pixels horizontally, vertically or diagonally from original and encrypted images. Generally, adjacent pixels of original image are highly correlated as shown in Figures 6a-6c while two adjacent pixels of encrypted should be very different. Figures 7a-7c prove that the adjacent pixels of most pixels of test encrypted image are different from the horizontal, vertical and diagonal neighbors.

According to Figure 5b, we note that the encrypted image has an almost uniform histogram. This result is confirmed analytically by an average entropy of the encrypted images equal to 7.9806 bit/pixel which is very close to an 8 bits/pixel code and conform to the image encryption standards.

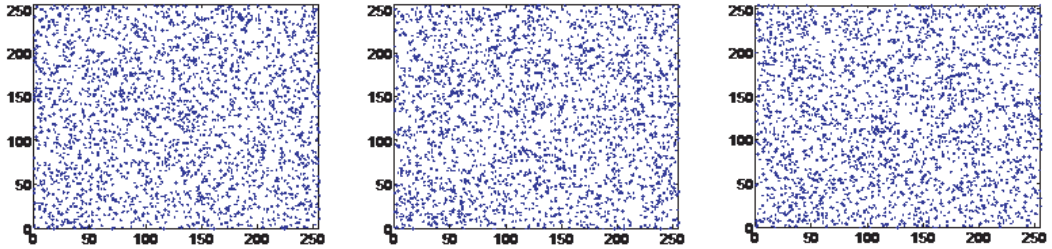
The second analysis consists in the study of the correlation between adjacent pixels. This study concerns adjacent pixels horizontally, vertically and diagonally from original and encrypted images. Generally, adjacent pixels of the original image are highly correlated as shown in Figure 6, while two adjacent pixels of the encrypted image should be very different. Figure 7proves that the adjacent pixels of most of the test encrypted image pixels are different from the horizontal, vertical and diagonal neighbors.

In Table 1, we summarize the adjacent pixel correlations of the 50 images of our image test bank before and after their encryptions. These results confirm the continuous aspect of original images expressed by a high correlation rate exceeding 0.9. On the other hand, the correlation rates between the adjacent pixels of the encrypted images are almost null, reflecting a strong introduction of the randomness in these images.



(a) (b) (c)

Figure 6: Correlation of adjacent pixels of the original image: (a) Horizontal neighbor pixel correlation, (b) Vertical neighbor pixel correlation, (c) Diagonal neighbor pixel correlation



(a) (b) (c)

Figure 7: Correlation of adjacent pixels of the encrypted image: (a) Horizontal neighbor pixel correlation, (b) Vertical neighbor pixel correlation, (c) Diagonal neighbor pixel correlation

Table 1: Average correlation of adjacent pixels of the original and the encrypted images

	Adjacent pixels horizontally	**Adjacent pixels vertically**	**Adjacent pixels diagonally**
Original images	0.9330	0.9691	0.9481
Encrypted images	0.0093	-0.0110	-0.0018

Moving to the study of the encryption/decryption keys sensitivity, as the encryption/decryption key is compounded by 3 subkeys, namely Key_1, Key_2 and Key_3, we suggest using three new keys K_1, K_2, and K_3 where we introduce a slight variation (10^{-15}) on X_1 (from Key_1), X_2 (from Key_2) and X_3 (from Key_3) of our initial key Key, respectively.

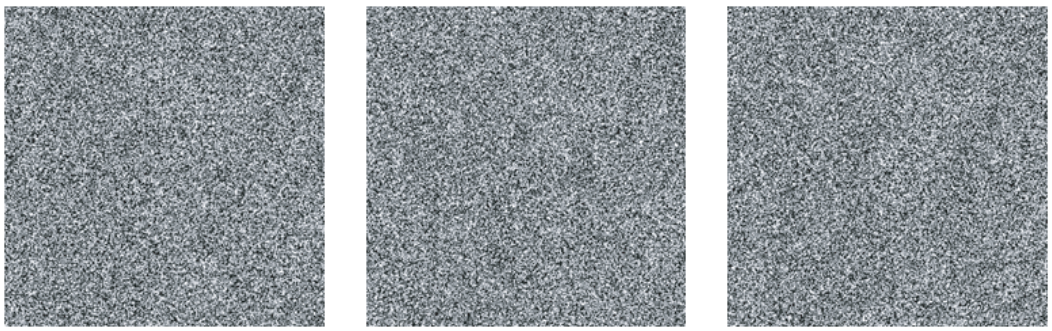
Firstly, we decipher encrypted images (encrypted using our initial key Key) K_1, K_2, and K_3, respectively. In Figure 8, we illustrate the results obtained for the decryption of our image test (Figure 4b).

This failure is observed every time an encrypted image is decrypted by means of a wrong key. In Table 2, we report the results of the comparison between the original image and its decrypted counterparts using K_1, K_2, and K_3 in terms of average NPCR, average UACI, and average PSNR.

Table 2: Sensitivity assessment of the decryption key

	Decryption using K_1	**Decryption using K_2**	**Decryption using K_3**	**Decryption using Key**
Average NPCR (%)	99.5950	99.5868	99.5888	0.2426
Average UACI (%)	31.5339	31.5308	31.5189	0.0010
Average PSNR (dB)	8.5044	8.5041	8.5095	74.3220

By introducing a tiny modification (10^{-15}) in the decryption key, the decryption process yields a blatant failure expressed by a high NPCR exceeding 99%, a UACI higher than 31%, and a weak PSNR well below 30dB. On the other hand, the decrypted image using the true key Key shows a small and



(a) (b) (c)

Figure 8: Failed decryption using unsuitable key: (a) Failed decryption using K_1, (b) Failed decryption using K_2, (c) Failed decryption using K_3

invisible distortion. This slight dissemblance is due to the use of the watermarking to insert Key_3.

Secondly, we focus on the influence of the key variation on the encryption process. To do so, we compare the encrypted images by Key to those encrypted by K_1, K_2, and K_3, respectively. Visually, the obtained images seem similar due to the randomness introduced in the images while encrypting them. Therefore, we use assessment metrics to quantify the difference between these images. Table 3 includes the outcome of this comparative study of the encrypted images by Key to their counterparts encrypted by K_1, K_2, and K_3, respectively.

Table 3: Sensitivity assessment of the encryption key

	Encryption using K_1	**Encryption using K_2**	**Encryption using K_3**
Average NPCR (%)	99.5845	99.5773	99.5895
Average UACI (%)	31.0517	31.0265	31.0165
Average PSNR (dB)	8.6262	8.6342	8.6358

Based on the high NPCR exceeding 99%, the high UACI of more than 31%, and the weak PSNR (much less than 30dB), we could confirm the great sensitivity of our proposed cryptosystem to the encryption key variation.

Indeed, the chaotic behavior and the great dependence of the chaotic generator on its parameters $\{X_0, \mu, N, V_{\min}, V_{\max}\}$ explain the high sensitivity of our cryptosystem to any change in the encryption/decryption key.

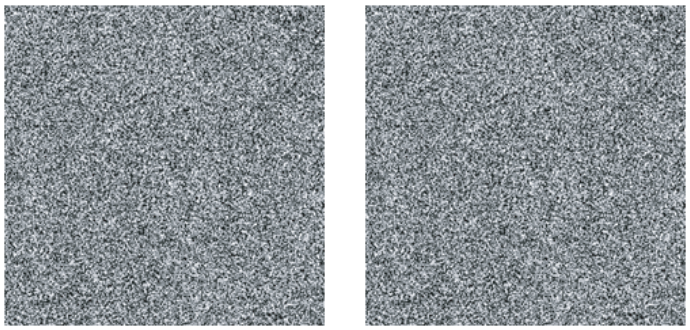
We continue our evaluation by undertaking a differential analysis where we study the effect of the change of a pixel on the encryption and decryption processes. The encryption differential analysis consists in the encryption of two very similar original images. In fact, the second image is none other than the first one where we modified only one pixel. Then, we proceed to comparing the encrypted image to the modified encrypted one obtained using the same cryptosystem and the same key. We note that, even in the case of a slight difference between two plain images, an efficient cryptosystem should provide very different encrypted images. Additionally, the decryption differential analysis is achieved by decrypting two images that differ in the value of a single encrypted pixel. The resulting images should present a great dissemblance. The results of this analysis are provided in Table 4.

Table 4: Differential analysis

	Encryption differential analysis	**Decryption differential analysis**
Average NPCR (%)	99.5824	99.6069
Average UACI (%)	33.5320	31.5697
Average PSNR (dB)	7.7489	8.4966

The obtained results from the application of this analysis on the images of our test bank result in NPCRs exceeding 99%, UACIs greater than 30%, and PSNRs well below 30dB. These mean values reflect the efficiency of our proposed cryptosystem following this differential analysis. These good performances derive from the chaotic aspect of the LUT generation and the involvement of the previous original and encrypted pixels values during the encryption of a new pixel.

Next, we focus on the impact of the watermarking in our encryption/decryption method. We use image watermarking to insert the subkey Key_3 in the encrypted image. Before its embedding, Key_3 should be ciphered using an 8-bit chaotic dynamic LUT parameterized by Key_2. It is evident that a false decryption of Key_3 leads to a failure of the decryption of $CiphGRP_1$ and $CiphGRP_2$, and, subsequently, the failure of the decryption of the encrypted image. This is well demonstrated earlier in the key sensitivity study of the subkey Key_3 (using the global key K_3). In what follows, we assume that a hacker knows Key_1, Key_2, and Key_3 , but cannot locate the pixels embedding the watermark. Thus, the hacker must either decrypt the pixels by a 7-bit chaotic dynamic LUT or by an 8-bit chaotic dynamic LUT. In Figure 9, an example of this cryptanalysis attack is depicted as performed on the encrypted image shown in Figure 4b.



(a) (b)

Figure 9: Decryption failure following the omission of the watermarking: (a) Decryption failure following the omission of the watermarking and CRP_4, (b) Decryption failure following the omission of the watermarking and CRP_3

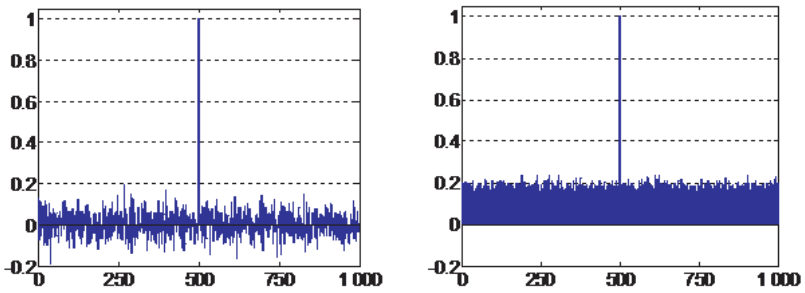
Neglecting the used watermarking implies the omission of CRP_3 or CRP_4. Given the sensitivity of our cryptosystem to its encryption/decryption keys (Tables 2-3) and its good performance against differential analysis (table 4), it is expected that this cryptanalysis attempt results in a failed decryption as shown in Figure 9. In addition, correct decryption requires a correct extraction of the subkey Key_3 inserted in the encrypted image.

Suppose a hacker knows the structure of this subkey Key_3, s/he must, at first, locate the carriers of this mark inserted, which means the knowledge of the subkey Key_1 placing the watermarked pixels at the beginning of the image. Simulating the brute force attack with 1000 randomly selected keys whose Key_1 is placed at position 500, we compare the extracted signatures from this key bank to our inserted signature. The obtained results (Figure 10a) reveal a correlation peak equal to 1 at position 500 (which corresponds to the position of Key_1 in the test bank) accompanied by weak correlations for the rest of the extracted signatures. These weak correlations (less than 0.2) highlight a failure to locate the carriers of the marks and lead to the failure of the inserted signature extraction.

Furthermore, this extracted signature must be deciphered to recover the subkey Key_3. This requires knowledge of Key_2. However, the cryptosystem CRP_2 is very sensitive to any modification of the key; hence, a wrong key causes a decryption failure (Table 2). A slight modification of the cryptogram decrypted by the subkey Key_2 will not recover Key_3 (Table 2).

As a consequence, we have to try to decipher the false extracted signatures (false cryptograms) by CRP_2 using various keys similar to Key_2. To do so, we choose to apply to each extracted signature a decryption by 1000 different keys (of which the subkey Key_2 is part). Then, we retain for each extracted signature the decrypted signature that is closest to subkey Key_3. The summary of this brute force attack attempts is portrayed in Figure 10b. This figure shows a correlation peak equal to 1 at position 500, which means Key_3 recovery. This peak corresponds to the decryption by the subkey

Key_2 of the encrypted subkey Key_3. Conversely, the other decrypted signatures extracted reveal weak correlations (less than 0.25) with Key_3, meaning a failure to recover subkey Key_3.



(a) (b)

Figure 10: Brute force attack cryptanalysis to recover the subkey Key_3: (a) correlation of extracted signatures and ciphered Key_3 following brute force attack cryptanalysis applied on CRP_1, (b) correlation of decrypted extracted signatures and Key_3 following Brute force attack cryptanalysis applied on CRP_1 and CRP_2

To sum up, the failure of the watermarking extraction phase and/or an incorrect decryption of the extracted signature prevent the subkey Key_3 recovery, which obviously leads to a failure of the deciphering phase of our proposed cryptosystem.

As a final test of robustness, we assess our cryptosystem against the known plaintext attack. In this case, the hacker owns the original image (Figure 4a) and its ciphered counterpart (Figure 4b). Moreover, we assume that s/he knows Key_1 used in the sub cryptosystem CRP_1. Thus, s/he can extract a stream key compounded by all the LUT used in the encryption/decryption processes applied to both of their images. Then, we verify this attack on the owned encrypted image (Figure 4c). Next, we use this verified stream key to decipher another encrypted image issued from the same cryptosystem parameterized by the key Key. The result of this cryptanalysis attempt is illustrated in Figure 11.

(a) (b) (c)

Figure 11: Failed known plaintext attack: (a) Encrypted image to attack, (b) Failed attack, (c) Decrypted image sought

6 Conclusion

In this paper, we presented a new cryptosystem for image encryption based on a dynamic Look-Up Table generated by the chaotic logistic map function. The proposed technique ensured a secure key transmission operation by embedding a part of the secret key in the encrypted image. In fact, this secret key was compounded by three subkeys, namely Key_1, Key_2, and Key_3. Of these three, the first one was computed from the recipient identifier while the second was derived from the sender identifier. However, the third Key_3 was randomly defined by the sender. This last subkey was inserted in the encrypted image. Consequently, to decipher the received image, the recipient should first reorder

pixels positions and then extract Key_3 from the watermarked pixels. Before its use to decipher the host image, Key_3 should be decrypted using Key_2. Thus, in addition to the sub-cryptosystem CRP_1 which was used to cipher the image by reordering the pixels positions, our cryptosystem included three others sub-cryptosystems, namely CRP_2, CRP_3, and CRP_4. CRP_2 and CRP_4 were based on an 8-bit dynamic LUT while CRP_3 used a 7-bit dynamic LUT parameterized by Key_3 to cipher watermarked pixels. This same subkey was used by CRP_4 to cipher non-watermarked pixels. On the other hand, CRP_2 set by Key_2 was used to cipher Key_3 before its insertion in the encrypted image. Each one of these keys was encoded on 320 bits, which provided 2^{320} combinations of the embedded part of the secret key for a single image exchange. This key space width reached 2^{960} combinations for a global secret key formed by Key_1, Key_2, and Key_3.

Experimental results provided by the assessment performed on our cryptosystem proved a high sensitivity to any modification of the encryption/decryption key of the original and encrypted images. Moreover, the encrypted image was clearly very different from the original image in terms of appearance and histograms. In fact, the entropy of the encrypted image was very close to 8 bits due to its uniform histogram aspect engendered by the randomness introduced during the encryption process. Furthermore, the encrypted image revealed a low neighbors pixels correlation. Under the known plaintext attack, our cryptosystem was proven robust. We noted also that watermarking strengthened the efficiency of our proposed encryption scheme. As a matter of fact, its omission, a failure on the extraction phase or a wrong decryption of the extracted mark would lead to a failure of the decryption process.

This proposed watermarked cryptosystem could be exploited for medical records exchange between distant hospitals to preserve any given patient's medical condition by encrypting medical images and inserting medical diagnoses on those encrypted images.

Acknowledgements

The authors would like to express their deepest gratitude to Prof. Ali M. Amri of ENET'Com, University of Sfax, for his painstaking editing of their paper.

References

[1] Abd El-Latif, A.A.; Li, L.; Wang, N.; Han, Q.; Niu, X. (2013). A new approach to chaotic image encryption based on quantum chaotic system, exploiting color spaces, *Signal Processing*, 93(11), 2986–3000, 2013.

[2] Abdelhakim, A.M.; Saleh, H.I.; Nassar, A.M. (2017). A quality guaranteed robust image watermarking optimization with artificial bee colony, *Expert Syst. Appl.*, 72(C), 317–326, 2017.

[3] Abdmouleh, M.K.; Khalfallah, A.; Bouhlel, M.S. (2012). Image encryptionwith dynamic chaotic look-up table, In 6^{th} *International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT)*, 331–337, 2012.

[4] Abdmouleh, M.K.; Khalfallah, A.; Bouhlel, M.S. (2013). Dynamic chaotic look-up table for MRI medical image encryption, In *International Conference on Systems, Control, Signal Processing and Informatics (SCSI)*, 241–246, 2013.

[5] Abdmouleh, M.K.; Khalfallah, A.; Bouhlel, M.S. (2014). A new watermarking technique for medical image using hierarchical encryption, *International Journal of Computer Science Issues (IJCSI)*, 11(4), 27–32, 2014.

[6] Abdmouleh, M.K.; Khalfallah, A.; Bouhlel, M.S. (2014). An overview on cryptography and watermarking, In *International Conference on Computers, Automatic Control, Signal Processing and Systems Science*, 99–104, 2014.

[7] Abdmouleh, M.K.; Khalfallah, A.; Bouhlel, M.S. (2016). A chaotic cryptosystem for color image with dynamic look-up table, In *Proceedings of the* 7^{th} *International Conference on Image and Signal Processing (ICISP'16)*, Springer International Publishing, Trois-Rivieres, QC, Canada, 91–100, 2016.

[8] Amri, H.; Khalfallah, A.; Gargouri, M.; Nebhani, N.; Lapayre, J.C.; Bouhlel, M.S. (2017). Medical image compression approach based on image resizing, digital watermarking and lossless compression, *J. Signal Process. Syst.*, 87(2), 203–214, 2017.

[9] Amri, H.; Khalfallah, A.; Lapayre, J.C.; Bouhlel, M.S. (2016). Watermarking for improving the reduction-expansion process of medical images (WREPro), *International Journal of Imaging and Robotics (IJIR)*, 16(3), 124–139, 2016.

[10] Atee H.A.; Ahmad, R.; Noor, N.M.; Rahma, A.M.S.; Aljeroudi, Y. (2017). Extreme learning machine based optimal embedding location finder for image steganography, *PLoS ONE*, 12(2), 1–23, 2017.

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

[12] Biham, E.; Shamir, A. (1991). Differential cryptanalysis of DES-like cryptosystems, In *Proceedings of the* 10^{th} *Annual International Cryptology Conference on Advances in Cryptology (CRYPTO'90)*, Springer-Verlag, 2–21, 1991.

[13] Biham, E.; Shamir, A. (2012). *Differential cryptanalysis of the data encryption standard*, Springer-Verlag, 2012.

[14] Bucerzan, D.; Ratiu, C.; Manolescu, M.J. (2013). SmartSteg: A New Android Based Steganography Application. *International Journal of Computes Communications & Control*, 8(5), 681-688, 2013.

[15] Devaney, R. L. (2003). *An Introduction to Chaotic Dynamical Systems*, 2^{nd} ed., Westview Pr (Short Disc), 2003.

[16] Furht, B.; Socek, D.; Li, S.; S. Magliveras, S. (2005). Enhanced 1-D chaotic key-based algorithm for image encryption, *in International Conference on Security and Privacy for Emerging Areas in Communications Networks*, IEEE Computer Society, Los Alamitos, CA, USA, 406–407, 2005.

[17] Garfinkel, S.; Spafford, G. (1996). *Practical UNIX and Internet security*, 2^{nd} ed, O'Reilly, Cambridge, 1996.

[18] Huang, C.K.; Nien, H.H. (2009). Multi chaotic systems based pixel shuffle for image encryption, *Optics Communications*, 282(11), 2123–2127, 2009.

[19] Kammoun, F.; Khalfallah, A.; Bouhlel, M.S. (2006). New scheme of digital watermarking using an adaptive embedding strength applied on multiresolution filed by 9/7 wavelet, *Int. J. Imaging Systems and Technology*, 16(6), 249–257, 2006.

[20] Karamchandani, S.H. et al.(2015). PCA Encrypted Short Acoustic Data Inculcated in Digital Color Images. *International Journal of Computes Communications & Control*, 10(5), 678-685, 2015.

[21] Kaushik, P.; Sharma, Y. (2012). Comparison of different image enhancement techniques based upon PSNR & MSE, International Journal of Applied Engineering Research, 7(11), 2010–2014, 2012.

[22] Khalfallah, A.; Kammoun, F.; Bouhlel, M.S.; Olivier, C. (2006). A new scheme of watermarking in multi-resolution filed by 5/3 wavelet: Family signature combined with the adapted embedding strength, In 2^{nd} *International Conference on Information Communication Technologies*, 1145–1152, 2006.

[23] Kishore Kumar, K.; Pavani, M. (2016). A new PCA based hybrid color image watermarking using cycle spinning - sharp frequency localized contour let transform for copyright protection, In *First International Conference on Smart Trends in Information Technology and Computer Communications (SmartCom 2016)*, Jaipur, India, 355–364, 2016.

[24] Kumar, S.; Dutta, A. (2016). A novel spatial domain technique for digital image watermarking using block entropy In *International Conference on Recent Trends in Information Technology (ICRTIT)*, 1–4,2016.

[25] Kuribayashi, M.; Schaathun, H.G. (2015). Image fingerprinting system based on collusion secure code and watermarking method, In *IEEE International Conference on Image Processing (ICIP)*, 2120–2124.

[26] Li, P.; Li, Z.; Halang, W.A.; Chen, G. (2007). A stream cipher based on a spatiotemporal chaotic system, *Chaos Solitons & Fractals*, 32(5), 1867–1876, 2007.

[27] Liu, X.L.; Lin, C.C.; Chang, C.C.; Yuan, S.M. (2016). A survey of fragile watermarking based image authentication techniques, *Journal of Information Hiding and Multimedia Signal Processing*, 7(6), 1282–1292, 2016.

[28] Lutovac, B.; Daković, M.; Stanković, S.; Orović, I. (2017). An algorithm for robust image watermarking based on the DCT and Zernike moments, *Multimedia Tools and Applications*, 76(22), 23333–23352 , 2017.

[29] Manglem Sing, K.; Chanu, Y.J.; Tuithung, T. (2014). Steganalysis of ± Steganography based on Noncausal Linear Predictor. *International Journal of Computes Communications & Control*, 9(5), 623-632, 2014.

[30] Masmoudi, A.; Bouhlel, M.S.; Puech, W. (2010). A new image cryptosystem based on chaotic map and continued fractions, In 18^{th} *European Signal Processing Conference (EUSIPCO)*, 1504–1508, 2010.

[31] Mazurczyk, W.; Karas, M.; Szczypiorski, K. (2013). SkyDe: a Skype-based Steganographic Method. *International Journal of Computes Communications & Control*, 8(3), 432-443, 2013.

[32] Paar, C.; Pelzl, J. (2010). The Advanced Encryption Standard (AES), In *Understanding Cryptography: A Textbook for Students and Practitioners*, Springer, Berlin, Heidelberg, 87–121, 2010.

[33] Priyanka, S.M. (2017). Region-based hybrid medical image watermarking for secure telemedicine applications, *Multimedia Tools and Applications*, 76(3), 3617–3647, 2017.

[34] Puech W.; Rodrigues J.M. (2004). *A New Crypto-Watermarking Method for Medical Images Safe Transfer*, In 12^{th} *European Signal Processing Conference (EUSIPCO'04)*, 1481–1484, 2004.

[35] Rivest, R.L.; Shamir, A.; Adleman, L.M. (1983). A method for obtaining digital signatures and public-key cryptosystems, *Commun. ACM*, 26(1), 96–99, 1983.

[36] Sam, I.S.; Devaraj, P.; Bhuvaneswaran, R.S. (2010). Enhanced substitution-diffusion based image cipher using improved chaotic map, In *ICT*, 116–123, 2010.

[37] Shannon, C.E. (1948). A Mathematical Theory of Communication, *The Bell System Technical Journal*, 27(3), 379–423, 1948.

[38] Stinson, D.R. (2006). Cryptography: theory and practice, Discrete mathematics and its applications, Chapman; Hall/CRC, Boca Raton.

[39] Uhl, A.; Pommer, A. (2004). *Image and Video Encryption: from Digital Rights Management to Secured Personal Communication (Advances in Information Security)*, Springer-Verlag TELOS, Santa Clara, CA, USA, 2004.

[40] Wang, Y.; Wong, K.W.; Liao, X.; Chen, G. (2011). A new chaos-based fast image encryption algorithm, *Appl. Soft Comput.*, 11(1), 514–522, 2011.

Journal's webpage: http://univagora.ro/jour/index.php/ijccc/

This journal is a member of, and subscribes to the principles of,
the Committee on Publication Ethics (COPE).
https://publicationethics.org/members/international-journal-computers-communications-and-control

Cite this paper as:

Khalfallah, A.; Abdmouleh, M.K.; Bouhlel, M.S. (2020). Watermarking for the Secure Transmission of the Key into an Encrypted Image, *International Journal of Computers Communications & Control*, 15(6), 3824, 2020.

https://doi.org/10.15837/ijccc.2020.6.3824.