Chaos-based Spatial Steganography System for Images

D. Battikh, S. El Assad
Institut d'Electronique et de Télécommunications de Rennes
IETR UMR CNRS 6164; Image team, INSA/Rennes, Rennes, France
IETR UMR CNRS 6164; Image team -site of Nantes, Nantes, France

B. Bakhache, O. Deforges, M. Khalil
Lebanese University, Tripoli, Lebanon
LASTRE: Laboratoire des Systèmes électroniques, Télécommunications et Réseaux
Tripoli, Lebanon

Abstract

In this paper, we propose a chaos-based enhancement of two spatial steganographic algorithms; the AE-LSB and the EA-LSBMR and our objective is to study their performances. The first algorithm is an adaptive LSB (Least Significant Bit) steganographic method using pixel value difference that provides a large embedding capacity and imperceptible stego images. The second method is an edge adaptive scheme which can select the embedding region according to the size of secret message and the difference between two adjacent pixels in the cover image. The two methods suffer from low security against attacks that try to recover secret data.To overcome this weakness, we propose to enhance the message security of these methods. The enhancement consists of using an efficient chaotic system in order to choose in a pseudo-chaotic manner the pixels in the cover image where the bits of the secret message will be embedded. In this way, the inserted message becomes secure against message recovery attacks and becomes as well spread over the whole image in a uniform manner. Experiments show that the security of the algorithms is increased.

1. Introduction

The transmission of a large amount of data over the network communications requires security to protect data. Therefore, the steganography has an important role in secret communication. Steganography is an art of hiding data in a way which hides as well the existence of the secret data into a digital cover media such as digital audio, image, or video.

Steganography is a process of embedding information into digital content without causing perceptual degradation. Steganographic processes can be classified into two categories: spatial and transform domains approaches [1]. On one hand, the spatial domain based algorithms embed the sensitive information inside lower bits of the pixels of the cover image. On the other hand transform domain based algorithms embed sensitive information in the cover image by modulating coefficients in a transform space, such as the Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), or Discrete Wavelet Transform (DWT). The advantages of spatial methods are the easy realization and the high capability of hiding information. The Transform domain techniques are significantly more robust to noise or image processing such as quantization. However, they are computationally complex.

Two important spatial domain methods exist in the state of art: AE-LSB (Adaptive data hiding in Edge areas of images with spatial Low Significant Bit domain systems) and EA-LSBMR (Edge Adaptive Image Steganography Based on LSB Matching Revisited). The first algorithm is a variable-sized embedding algorithm inserting a variable number of secret bits in the pixels of the cover image [2]. The second one, EA-LSBMR is a fix-sized inserting a constant number of bits in all pixels [3]. Both algorithms; AE-LSB and EA-LSBMR are two important major techniques among the spatial steganographic ones. The information is inserted in a systematic manner and the message is inserted in consecutive series of pixels. Thus, the security of the steganographic algorithms is reduced. Therefore, and to overcome this weakness, we propose to distribute the information in different pixels choosing in a random manner that uses the chaotic system.

Indeed, important features of chaotic signals such as: pseudo-randomness, ergodicity, constant power, and sensitivity to initial conditions and parameters of the system encourage their use in hiding and data security [4] [5].

The security is then enhanced and the system becomes more robust against an adversary that tries to recover the secret embedding data.

This paper is organized as follows: Section II presents a brief description of the criteria of steganography. Section III presents the steganographic techniques. In section IV, the related works are shown. Section V describes the proposed chaotic system. In Section VI, the proposed enhancement of the two steganographic algorithms is described. Section VII, presents the experimental results as well as a comparative analysis of the two enhanced algorithms. In the last section, a conclusion of the whole paper is provided.

2. Criteria for Steganography

Three common requirements; imperceptibility, security, and capacity may be used to rate the performance of steganographic techniques.

2.1. Imperceptibility

Stego images should not have severe visual artifacts. The stego object must appear unchanged to the naked eye and remains as such. If the stego object changes significantly or if visual traces can ever be noticed on stego, an eavesdropper may see that information is being hidden and therefore could try to extract or to destroy it. The higher is the imperceptibility of the stego image, the better is the steganographic system.

2.2. Security

It is an important requirement for all steganographic systems. In case the system is broken (detestability of hiding information), the information can be destroyed but not extracted.

2.3. Capacity

This parameter should be as high as possible. The steganographic system must offer a high capacity for the hidden message, without affecting the security of the system in the efficient transmission.

3. Steganography techniques

Steganographic techniques that modify image files in order to hide information include the following:

Spatial domain;
Transform domain;
Distortion techniques;
Spread spectrum;
Statistical methods;

3.1. Spatial Domain Technique

There are many versions of spatial steganography, the most widely known steganography algorithm is based on hiding the secret message in the LSBs (sequentially or randomly) of pixel values without introducing visual traces. This technique is based on the fact that the least significant bits in an image could be thought of as random noise and changes in these would not have any effect on the image [6]. LSB matching, and Pixel value differences are examples of the spatial domain techniques.

3.2. Transform Domain Technique

This is a strong way of embedding data. The advantage of transform domain methods is the high capability of facing signal processing, compression, cropping, and image processing operations. However, methods of this type are computationally complex.

Transform domain methods hide messages in the significant areas of the transform image. Transform domain techniques are classified into:

Discrete Fourier transformation technique (DFT).
Discrete cosine transformation technique (DCT).
Discrete Wavelet transformation technique (DWT).

3.3. Distortion Techniques

Distortion techniques require knowledge of the original cover image during the decoding process (non blind technique). The decoder checks for differences between the original cover image and the stego-image in order to restore the secret message. The encoder, on the other hand, adds a sequence of changes to the cover image [7]. So, information is described as being stored by signal distortion [8]. Using this technique, a stego-object is created by applying a sequence of modifications to the cover image. This sequence of modifications is selected to match the secret message that requires transmission [9].

3.4. Spread spectrum

Spread spectrum communication describes the process of spreading the bandwidth of a narrowband signal across a wide band of frequencies [10]. This can be accomplished by modulating the narrowband waveform with a wideband waveform, such as white noise. After the spreading process, the energy of the narrowband signal in any one frequency band is low and therefore difficult to detect [10]. SSIS (Spread Spectrum Image Steganography) uses a variation of this technique to embed a message, typically a binary signal, within samples of a low-power white

Gaussian noise sequence consisting of real numbers. The resulting signal, which is perceived as noise, is then combined with the cover image to produce the stegoimage [10].

3.5. Statistical methods

Also known as model-based techniques, statistical methods tend to modulate or modify the statistical properties of an image in addition to preserving them in the embedding process. This modification is typically small, and it is thereby able to take advantage of the human weakness in detecting luminance variation [6].

4. Related works

Chan et al. proposed a data hiding scheme based on LSB substitution, and followed by an optimal pixel adjustment process [11]. The quality of the obtained stego-image is greatly improved as compared with the simple LSB substitution method.

Wu et al. proposed a method for embedding information into a gray-valued cover based on PVD (Pixel Value Differencing) [12]. In this process, a cover image is partitioned into non-overlapping blocks of two consecutive pixels. A difference value is calculated based on the values of the two pixels in each block. The number of bits which can be embedded in a pixel pair is determined by the width of the range that the difference value belongs to.

Chang et al. proposed a novel steganographic method using side information [13]. The method exploits the correlation between neighboring pixels in order to estimate the degree of smoothness or contrast of pixels. If the pixel is located in edge areas, then it may tolerate larger changes than the ones found in smooth areas.

Wu et al. proposed an approach based on the least-significant-bit (LSB) replacement and the pixel-value differencing (PVD) method [14]. First, a difference value between two consecutive pixels is calculated. In the smooth areas (small difference), the secret data is hidden into the cover image by LSB method while in the edged areas (large difference), the PVD method is used.

Wang et al. proposed a new image steganographic technique capable of producing a secret-embedded image that is totally indistinguishable by the human eye from the original image [15]. Additionally, this new method avoids the falling-off-boundary problem by using the pixel- value differencing and the modulus function.

Jung et al. proposed a novel data hiding method based on the least significant bit (LSB) substitution and the multi-pixel differencing (MPD) [16]. First, a sum of different values for a four-pixel sub- block is calculated. The low value of the sum can be located on a smooth block and the high value is located on an edged block. The secret data are hidden into the cover image by the LSB method in the smooth block, while the MPD method is concealed in the edged block.

Liaw et al. proposed a new hiding method based on secret data division and PVDLSB [17]. The hiding capacity of two consecutive pixels depends on the difference value of the pixels. Liaw et al. apply the modulus operation to embed the secret data.

In the LSB matching method, the corresponding pixel value is randomly incremented or decremented if it doesn't match the secret message bit [18].

Mielikainen proposed a modification to the least-significant-bit (LSB) matching [19]. The modified method permits the embedding of the same payload as that of the LSB matching but with fewer changes to the cover image.

Huang et al. proposed a method to find the fragile regions in an image to apply LSB matching revisited embedding [20]. This method can be considered as an improved method of the LSBMR (Least Significant Bit Matching Revisited) method.

Xi et al. proposed a new method that embedded two bits in a pair of complimentary pixels from the image with adjacent intensity [21]. That is achieved by adding 1 to the pixel with lower intensity and subtracting 1 from the pixel with higher intensity. This allows the elimination of the influence of the histogram of the LSB matching steganography method and the intensification of the capability of the statistical analysis resistance. The histogram remains unchanged and this method can be viewed as an improved version of the LSB Matching method.

Al-Taani et al. proposed a novel Steganographic method for hiding information within the spatial domain of the gray scale image [22]. The proposed approach works on dividing the cover into blocks of equal sizes and then embedding the message in the edge of the block based on the number of ones in the left four bits of the pixel.

5. Proposed chaotic system

This section introduces the proposed chaotic system that is used later in the modification and the enhancement of the steganographic algorithms (see fig 1). It consists of a perturbed PWLCM as chaotic generator and this is followed by a process of permutation based on a 2D cat map which gives the new pixel random position. The chaotic system allows the insertion of the message both in a secret and in a uniform manner.

The chosen generator (fig. 2) of chaotic discrete sequences is a very simplified version of the chaotic generator proposed by El Assad et al [23] [24] [25].

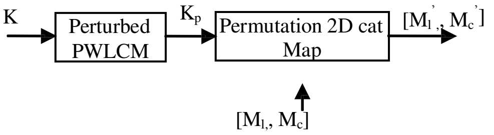


Figure 1. Scheme of the chaotic system

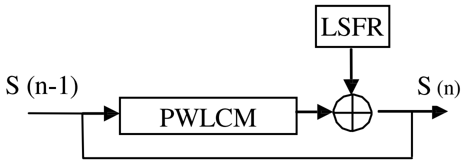


Figure 2. Perturbed PWLCM

5.1. Description of the perturbed PWLCM map

The perturbed PWLCM consists of discrete piecewise linear chaotic map PWLCM, which includes a technique of disturbance, based on a linear feedback shift register LFSR, (Fig 2). The PWLCM is a Non Linear Function (NLF) defined by the following equation (1):

$$s(n) = NLF[s(n-1), p]$$
$$= \begin{cases} \left\lfloor 2^N \times \dfrac{s(n-1)}{p} \right\rfloor & \text{if } 0 \le s(n-1) < p \\ \left\lfloor 2^N \times \dfrac{2^N - s(n-1)}{2^N - p} \right\rfloor & \text{if } p \le s(n-1) < 2^{N-1} \\ NLF\left[2^N - s(n-1)\right] & \text{otherwise} \end{cases} \tag{1}$$

Where $\lfloor \ \rfloor$ is the Floor function, p is the control parameter ranging from 1 to 2N-1-1, and N is the precision used for the simulations (N=32).

5.2. Description of the permutation process based on a new formulation of the 2D cat map

As Fig. 1 shows the Cat map has two inputs: one input K_p comes from the PWLCM to supply the parameters for the cat map, and another input, M_l and M_c which are two initial matrices used in the calculation of the new pixel positions. In comparison with the standard equation of the cat map, the calculus is done in a very efficient manner given by equation (2) [26]:

$$\begin{bmatrix} Ml' \\ Mc' \end{bmatrix} = \text{mod}\left\{ \begin{bmatrix} \begin{pmatrix} 1 & u \\ v & 1+uv \end{pmatrix} \times \begin{bmatrix} Ml \\ Mc \end{bmatrix} + \begin{bmatrix} rl+rc \\ rc \end{bmatrix}, \begin{bmatrix} M \\ M \end{bmatrix} \end{bmatrix} \right\} + \begin{bmatrix} 1 \\ 1 \end{bmatrix} \tag{2}$$

u, v, rl, rc are the dynamic parameters which are positive integers, with :

$$0 \le u_i, v_i, rl_i, rl_i \le M-1 = 2^q - 1 \tag{3}$$

Where M is the matrix size, and q is the necessary number of bits that represent each parameter of the cat map.

M_l, M_c and *M'_l, M'_c* are the initial and the permuted pixels positions (row and column indices) of *M x M* matrix. *M_l, M_c* are square matrices with the following form as:

$$M_l = \begin{pmatrix} 1 & 1 & . & . & 1 \\ 2 & 2 & & & 2 \\ . & & . & & . \\ M & M & . & . & M \end{pmatrix}; \quad M_c = \begin{pmatrix} 1 & 2 & . & . & M \\ 1 & 2 & & & M \\ . & & . & & . \\ 1 & 2 & . & . & M \end{pmatrix} \tag{4}$$

The structure of the dynamic key *Kp* is:

$$\begin{aligned} k_p &= \left[k_{p1}, k_{p2}, \ldots\ldots, k_{pr}\right] \\ k_{pr} &= \left\{u_i, v_i, rl_i, rc_i\right\}; \qquad i = 1, 2, \ldots\ldots, r \end{aligned} \tag{5}$$

The main advantages of the proposed chaotic system are: high degree of Security of the inserted data, and uniformity of inserted message over the whole cover image.

6. Embedding and Extraction Procedures

In the two next subsections, we present the algorithms Enhanced AE-LSB (EAE-LSB) and Enhanced EA-LSBMR (EEA-LSBMR).

6.1. First algorithm: AE-LSB

6.1.1. Insertion procedure. First of all, the image is divided into two-pixel blocks. For each block, we consider the pixels p_i, p_{i+1} and we calculate their difference to identify smooth and edge areas. Three difference levels are defined R_1= [0, 15], R_2= [16, 32], R_3= [32, 255], and k_1, k_2 and k_3 are the number of bits inserted in each pixel in the corresponding block according to the corresponding range [2].

The insertion procedure [27] consists of the following steps:

- Divide the cover image into two-pixel blocks (p_i, p_{i+1}) horizontally.

- Deal with the embedding units or block in raster scanning order.
- Compute the difference value $d=|p_i - p_{i+1}|$ for the pixels in the block and identify k_i (i=1, 2, 3).
- Change the k_i least significant bits (LSB) for each pixel in the block with the information from the message we want to hide. For each two-pixel block, $2k_i$ information bits are hidden. The new carrier information pixels from the block are p'_i and p'_{i+1}, use the modified LSB substitution to obtain the new pair (p'_i, p'_{i+1}) [11].
- Compute the new difference $d'=|p'_i - p'_{i+1}|$ between the neighbor pixels.
- In order to extract the correct secret message, the difference values before and after embedding (d and d') must belong to the same level. If the two differences d and d' are not in the same level we apply a sort of adjustment by using the following procedure [2]:

- Case 1: $d\in$ lower level and $d'\in$ middle level or $d\in$ middle level and $d'\in$ higher level, it introduces two cases.
  - If $p'_i \geq p'_{i+1}$, we replace the pair (p'_i, p'_{i+1}) with the best choice (the closest values to p_i and p_{i+1}) between $(p'_i, p'_{i+1} + 2^k)$ and $(p'_i - 2^k, p'_{i+1})$. Otherwise, we replace (p'_i, p'_{i+1}) with the best solution between $(p'_i, p'_{i+1} - 2^k)$ and $(p'_i + 2^k, p'_{i+1})$
- Case 2: $d\in$ middle level and $d'\in$ lower level or $d\in$ higher level and $d'\in$ middle level, so there are also two cases as well
  - If $p'_i \geq p'_{i+1}$ we replace the pair (p'_i, p'_{i+1}) with the best choice between $(p'_i, p'_{i+1} - 2^k)$ and $(p'_i + 2^k, p'_{i+1})$; otherwise,we replace (p'_i, p'_{i+1}) with the best solution between $(p'_i, p'_{i+1} + 2^k)$ and $(p'_i - 2^k, p'_{i+1})$.

Enhanced algorithm EAE-LSB: Pseudo-chaotic scan order.

The second point in the previous algorithm (insertion procedure) represents the raster scan order of images for embedding data, which is a sequential manner. At a later stage and to improve the security of the steganographic system, we replace the second step by the following one:

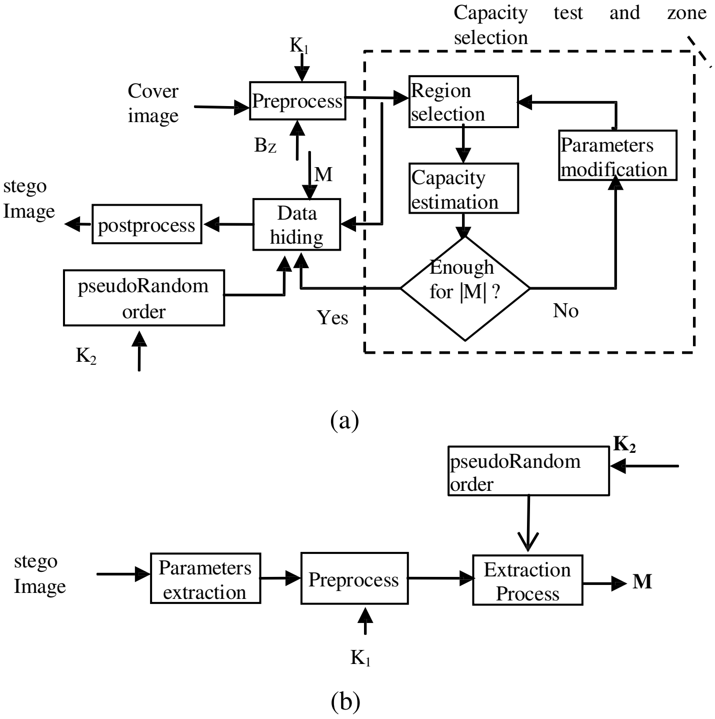
We apply the chaotic system, described in Section II, in order to find the new pixel positions (M'_l, M'_c) for the working block.

6.1.2. Extraction procedure. Once a receiver gets the stego image, the key of the chaotic generator K is needed to start the execution of the message extraction procedure. Without this key, the receiver will be in the same position as an eavesdropper who gets the image but cannot extract it, even if the algorithm and the stego image are known. With the correct key shared by both emitter and receiver, the latter can generate the indexes for the blocks used at the insertion and can start the message extraction procedure described as follows:

- Divide the stego image into two-pixel blocks.
- Repeat the chaotic algorithm to obtain the same positions of the two-pixel blocks used by the emitter to insert the message instead of raster scan order used to extract data in the original algorithm.
- Compute the absolute value d' for each block, and identify the corresponding k_i-value.
- Extract k secret bits from each pixel of the block (p_i, p_{i+1}).

6.2. Second algorithm: EA-LSBMR

6.2.1. Insertion procedure. The flow diagram of the scheme is illustrated in Fig. 3.



(a)

(b)

Figure 3. EEA-LSBMR methods (a): insertion procedure (b): extraction procedure

The insertion procedure is composed of four steps defined below [3]:

Step 1: Preprocess

The cover image is divided into non overlapping blocks of B_z x B_z pixels (B_z is the block size = 1, 4, 8 or 12) then each block is rotated by a random degree in the range of {0°, 90°, 180°, 270°} as determined by the secret key K_1. The resulting image is rearranged in a row vector V by raster scanning, and then the vector is divided into non overlapping embedding units constituted of two consecutive pixels (p_i, p_{i+1}).

The random rotation can prevent the detector from getting the correct embedding units without the rotation key K_1. Thus the security is improved.

Step 2: Capacity test and zone selection

According to the scheme of LSBMR, 2 secret bits can be embedded into each embedding unit (insertion of 1 bit information in each pixel). Therefore, for a given secret message M, the threshold T for region selection can be determined as follows:

$$T = \arg\max_t \left\{ 2*|EU(t)| \geq |M| \right\} \qquad (6)$$

Where *EU(t)* is the set of pixel pairs whose absolute differences are greater than or equal to a parameter t

$$EU(t) = \left\{ (p_i, p_{i+1}) / |p_i - p_{i+1}| \geq t, \forall (p_i, p_{i+1}) \in V \right\} \qquad (7)$$

Where t ∈ {1, 2,………, 31}, and is modified until we reach enough set of pixels for inserting the whole message M; |*EU(t)*| denotes the total number of elements in the set of *EU(t)*, and |*M*| is the size of the secret message M (number of bits).

Step 3: Data hiding

We deal with the embedding units in a pseudorandom order determined by a secret key K_2 and after computing the threshold T described in the previous step, we see if the chosen unit is able to hide the secret information, the pair of pixels (p_i, p_{i+1}) must respect the following condition:

$$|p_i - p_{i+1}| \geq T, \forall (p_i, p_{i+1}) \in V \qquad (8)$$

For a good unit (able to be modified), we perform the data hiding by calculating new pixels p'_i and p'_{i+1} according to the following four cases [19].

$$Case\,1:\ LSB(p_i) = m_i \,\&\ f(p_i, p_{i+1}) = m_{i+1}$$
$$\rightarrow (p'_i, p'_{i+1}) = (p_i, p_{i+1})$$
$$Case\,2:\ LSB(p_i) = m_i \,\&\ f(p_i, p_{i+1}) \neq m_{i+1}$$
$$\rightarrow (p'_i, p'_{i+1}) = (p_i, p_{i+1} + r)$$
$$Case\,3:\ LSB(p_i) \neq m_i \,\&\ f(p_i - 1, p_{i+1}) = m_{i+1}$$
$$\rightarrow (p'_i, p'_{i+1}) = (p_i - 1, p_{i+1})$$
$$Case\,4:\ LSB(p_i) \neq m_i \,\&\ f(p_i - 1, p_{i+1}) \neq m_{i+1}$$
$$\rightarrow (p'_i, p'_{i+1}) = (p_i + 1, p_{i+1})$$

Where m_i and m_{i+1} are the i^th and (i+1)^th secret bits of message M to be embedded, r is a random value belonging to{-1,1}, and the function f is defined as:

$$f(a,b) = LSB\left(\left\lfloor \frac{a}{2} \right\rfloor + b \right) \qquad (9)$$

After that, p'_i and p'_{i+1} may be out of the range [0,255], or the new difference $|p'_i - p'_{i+1}|$ may be less than the threshold T. In these cases, we need to readjust p'$_i$ and p'$_{i+1}$, and the new readjusted values, p''$_i$ and p''$_{i+1}$, are calculated as follows [3]:

$$(p''_i, p''_{i+1}) = \arg\min_{(e_1,e_2)} \left\{ |e_1 - p_i| + |e_2 - p_{i+1}| \right\} \qquad (10)$$

With:

$$\begin{cases} e_1 = p'_i + 4k_1 \\ e_2 = p_{i+1} + 2k_2 \end{cases} \quad k_1, k_2 \in Z \qquad (11)$$
$$|e_1 - e_2| \geq T,\ 0 \leq e_1, e_2 \leq 255$$

k_1, k_2 are two arbitrary numbers from Z .

So:

$$LSB(p''_i) = m_i \ \&\ f(p''_i, p''_{i+1}) = m_{i+1}$$
$$with\ \ 0 \prec p''_i, p''_{i+1} \prec 255,\ |p''_i, p''_{i+1}| \geq T \qquad (12)$$

The phase of readjustment is very important in order to guarantee that we can distinguish the same selected regions before and after data embedding with the same threshold T.

Step 4: Postprocess

The resulting image is divided into non overlapping B_z x B_z blocks. These blocks are then rotated by the opposite random number of degrees that are used in the insertion. Finally, we embed the two parameters (T, B_z) of the stego image into a preset region which has not been used for data hiding.

Proposed enhanced embedding process:

Fig. 3 shows that the data hiding is accomplished by a pseudorandom order. Therefore, we propose to replace this order manner by a chaotic order generated by the system shown in Section II.

In the original algorithm EA-LSBMR, the third step describes the **pseudorandom order** of embedding data. In order to improve the data hiding performance, we use the **chaotic random order** to hide data instead of the previous pseudorandom order for more security against attacks.

6.2.2. Extraction procedure. To extract data, we first extract the two parameters B_z and T from the stego image. Then, we do exactly the same operations of Step 1 in the insertion procedure: the stego image is divided into non overlapping blocks of B_z x B_z pixels, then we rotate each block by a random degree as determined by the secret key K_1. The resulting image is rearranged as a row vector V' by raster scanning. Finally, the vector V' is divided into non overlapping embedding units with every two consecutive pixels (p_i, p_{i+1}).

We generate the same chaotic sequences as done in the insertion procedure to obtain the same order of pixel units positions.

For each qualified embedding unit, say (p'_i, p'_{i+1}), where $|p'_i - p'_{i+1}| \geq$ T, we extract the two secret bits of M (m_i, m_{i+1}) as follows:

$$m_i = LSB(p'_i)\,\&\,m_{i+1} = f(p'_i, p'_{i+1}) \qquad (13)$$

7. Comparative Experimental Results and analysis

For the simulations, we used standard gray level cover images "Lena", "Peppers", "Baboon" of 512x512 of size and the secret messages with different sizes: 32x32, 64x64, 100x100, 128x128 and 256x256.

The two criteria used to evaluate the qualities of the stego images are the Peak Signal-to-Noise Ratio (PSNR) and the Image Fidelity (IF) given in eq. (14):

$$PSNR = 10 \times \log_{10}\left(\frac{Max\ p^2(i,j)}{\frac{1}{M \times N}\left(\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left[p(i,j) - p_s(i,j)\right]^2\right)}\right)(db)$$

(14)

$$IF = 1 - \frac{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left[p(i,j) - p_s(i,j)\right]^2}{\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\left[p(i,j)\right]^2}$$

Where $p_s(i,j)$ is the pixel value of the i^{th} row and j^{th} column of the stego image, and M and N are the width and height of the considered cover image.

The higher the PSNR and IF are, the better is the quality of stego image.

The obtained results of the two parameters PSNR and IF for both algorithms are showed in table 1. The PSNR_1 and IF_1 are the results of the first algorithm EAE-LSB, and PSNR_2 and IF_2 are the results of second one, i.e. EEA-LSBMR. The obtained values of EAE-LSB are lesser than the values of EEA-LSBMR. However, on the other side the embedding capacity of EAE-LSB is greater than the EEA-LSBMR, and this is due to its capacity to embed more than one bit in a pixel. In addition, for the EEA-LSBMR algorithm, the secret message of 256x256 of size cannot be embedded in the cover image. This is due to the limited embedding capacity of the used algorithm.

Moreover, we can notice that for both algorithms, the PSNR and IF values decrease when the size of the secret message M increases.

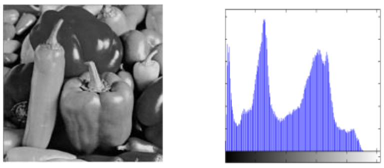
Table 1

Cover	**Message M**	**PSNR_1**	**PSNR_2**	**IF_1**	**IF_2**
Lena (512x512)	32x32	60.03	70.35	0.9998	1.0000
	64x64	54.42	64.41	0.9991	0.9999
	100x100	50.33	60.51	0.9978	0.9998
	128x128	48.32	58.35	0.9965	0.9997
	256x256	42.49	--	0.9867	--
Baboon (512x512)	32x32	57.55	70.52	0.9996	1.0000
	64x64	51.27	64.46	0.9981	0.9999
	100x100	47.19	60.59	0.9952	0.9998
	128x128	45.20	58.41	0.9924	0.9996
	256x256	39.40	--	0.9712	--
Peppers (512x512)	32x32	59.43	69.71	0.9998	1.0000
	64x64	54.52	63.78	0.9992	0.9999
	100x100	50.25	59.86	0.9979	0.9998
	128x128	48.04	57,70	0.9966	0.9996
	256x256	42.42	--	0.9875	--

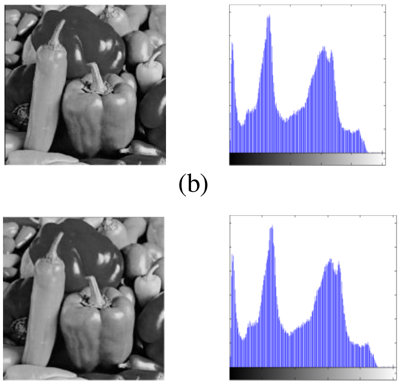
Furthermore, we subjectively evaluated the strength of the proposed algorithms, using visual tests. For that purpose, we used "couple" image of 64x64 of size, as a secret message M (Fig. 4).

Figure 4. Secret message.

The cover image "peppers" image of 512x512 of size and its histogram are shown in figure 5 (a). The stego images obtained by the two considered algorithms and their histograms are given in Fig. 5 (b), and 5 (c). The stego images are visibly similar and indistinguishable from the original cover image.



(a)

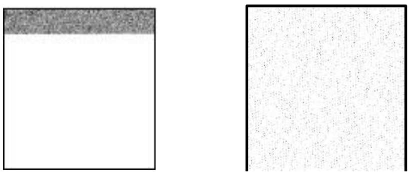


(b)

(c)

Figure 5. (a) Cover Image and its histogram (b) Stego image with EAE-LSB and its histogram (c) Stego image with EEA- LSBMR and its histogram

Fig. 6 (a) and 6 (b) show respectively the difference between the cover image and the stego images obtained by the AE-LSB algorithm and its enhanced version in case of short messages. As we can see, with the AE-LSB algorithm, the secret message is only inserted in the top part of the image "Fig 6 (a)" and this information can be used by an attacker whereas with the enhanced AE-LSB algorithm, the secret message is spread along the whole image uniformly. This ensures a good and a high security of the message.



(a) (b)

Figure 6. Difference between cover image and stego image : (a) AE-LSB (b) EAE-LSB

The extracted message from the stego images obtained by our two proposed algorithms is exactly identical to the inserted message (see Fig. 4).

Visual artifact with high embedding rate:

Note that when the size of the secret message increases, a distortion appears in the histogram of the stego image for the two studied algorithms. The larger is the secret message size, the worst the histogram can be. The second algorithm EEA-LSBMR has a limited capacity of embedding as it inserts only one bit in each pixel. For the considered cover image for example, we cannot embed a secret message bigger than 180x180 bits. In addition, we have noticed that when the size of the secret message is larger than 64x64, a small visible distortion appears in the histogram of the stego image. For the first algorithm EAE-LSB, the capacity of embedding is higher than the EEA-LSBMR. We can embed for example a big secret image of 256x256 of size but in this case the histogram in this case is very disturbed (as shown in Fig. 7).

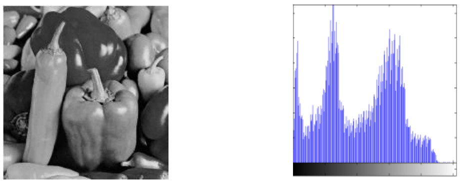
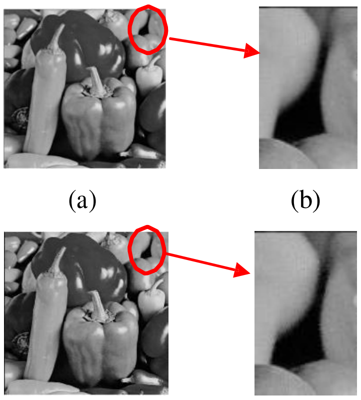


Figure 7. Stego image with EAE-LSB and its histogram

Among the most important types of steganalysis lies the visual attack which consists of examining the stego image with a naked eye to identify any obvious inconsistencies. For the EEA-LSBMR algorithm, as we change only one bit in each chosen pixel, the variations of the values of pixels are very small and they are not detectable or visible. While for the EAE-LSB algorithm, many bits can be inserted in a pixel in edge areas, where there is a large difference between consecutive pixels and the edge regions would be disturbed and some artifacts can appear in these regions.

Upon zooming in, these artifacts are more clearly observed, as illustrated in Fig. 8 (d), and one could utilize those artifacts to discover the presence of a hiding secret.



(a) (b)

(c) (d)

Figure 8. (a) cover image (b) edge areas of cover image (c) Stego image (d) Detectable and visual artifacts of edge areas

8. Conclusion

In this paper, we have presented an enhancement of two spatial steganographic algorithms, EAE-LSB and EEA-LSBMR which insert the data in a random order according to a proposed chaotic system. The pseudorandom distribution of information gives the algorithms more security. The EEA-LSBMR inserts one bit in the chosen pixel, so it has a limited embedding capacity. The EAE-LSB permits the insertion of many bits in the same pixel. So it has a bigger capacity than the other algorithm. But experiments show that it can present visual and detectable artifacts when the size of the secret message is large.

9. References

[1] A. Cheddad, J. Condell, K. Curran, P. Mc Kevitt, "Digital image steganography: Survey and analysis of current methods", Signal Processing, Volume 90, Issue 3, March 2010, Pages 727-752.

[2] C.-H. Yang, C.-Y. Weng, and S.-J. Wang, "Adaptive data hiding in edge areas of images with spatial LSB domain systems", IEEE Trans. on information forensics and security, vol. 3, no. 3, september 2008.

[3] Luo, W., Huang, F. et Huang, J. (2010). "Edge Adaptive Image Steganography Based on LSB Matching Revisited", IEEE transactions on information forensics and security, Vol. 5, NO. 2.

[4] T.S. Parker, L.O. Chua, "Practical Numerical Algorithms for Chaotic Systems", Springer-Verlag, 1989.

[5] A. Baranovsky, D. Dames, "Design of One-Dimensional chaotic maps with prescribed properties", International Journal of Bifurcationand chaos , vol. 5, Feb. 1995, pp. 1585-1598.

[6] M. Kharazi, H.T. Sencar, and N. Memon. (2004, Apr.). "Image steganography: Concepts and practice." WSPC/Lecture Notes Series: 9in x 6in, [On line], April 2004, pp. 1-49.

[7] R. Radhakrishnan, K. Shanmugasundaram, and N. Memon. "Data masking: a secure-covert channel paradigm", in IEEE Workshop on Multimedia Signal Processing, 2002, pp. 339-342.

[8] H.S. Majunatha Reddy and K.B. Raja. (2009). "High capacity and security steganography using discrete wavelet transform", International Journal of Computer Science and Security, [On line]. 3(6), pp. 462-472.

[9] S.C. Katzenbeisser. "Principles of Steganography" in Information Hiding Techniques for Steganography and Digital Watermarking, S. Katzenbeisser and F. Petitcolas, Ed. London: Artech House, 2000, pp. 43- 78.

[10] Marvel L.M., Boncelet Jr., C.G. and Retter C., "Spread Spectrum Steganography", IEEE Transactions on image processing, 8 (8), 1999.

[11] C.K. Chan and L. M. Chen, "Hiding data in images by simple LSB substitution", Pattern Recognit., vol. 37, no. 3, 2004, pp. 469–474.

[12] D.C. Wu and W.H. Tsai., "A Steganographic method for Images by Pixel Value Differencing", Pattern Recognition Letters, Vol. 24, Issue: 9-10, June 2003, pp.1613-1626.

[13] C.C. Chang, H. W. Tseng, "A steganographic method for digital images using side-match", Pattern Recognition Letters 25 (12) (2004) pp.1431-1437.

[14] H.C. Wu, N.I. Wu, C.S. Hwang, "Image steganographic scheme based on pixel-value differencing and LSB replacement methods", IEE Proceedings: Vision, Image and Signal Processing, Vol.152, Issue 5, Oct 2005, pp.611-615.

[15] C.-M. Wang, N.-I Wu, Chwei-Shyong Tsai, Min-Shiang Hwang,''A high quality steganographic method with pixel-value differencing and modulus function", The Journal of Systems and Software, 2007.

[16] Ki-Hyun Jung, Kyeoung-Ju Ha, Kee-Young Yoo, "Image Data Hiding Method Based on Multi-pixel Differencing and LSB Substitution Methods", International Symposium on Ubiquitous Multimedia Computing, 2008.

[17] J.-J. Liaw, W.-S. Wang, M.-Y. Chiu, "A Data Hiding Method Using Secret Data Division and Pixel Value Differencing", in Fourth International Conference on Genetic and Evolutionary Computing, 2010. pp. 650-653.

[18] Toby Sharp, "An implementation of Key based Digital Signal Steganography", in proceedings Information Hiding Workshop, Vol. 2137, Springer LNCS, 2001.pp.13-26.

[19] J. Mielikainen, "LSB matching revisited", IEEE Signal Process. Lett., vol.13, no.5, May 2006, pp.285-287.

[20] Q. Huang, W. Ouyang, "Protect Fragile Regions in Steganography LSB Embedding", in 3rd International Symposium on Knowledge Acquisition and Modelling, 2010. pp.175-178.

[21] L. Xi, X. Ping, T. Zhang, "Improved LSB Matching Steganography Resisting Histogram Attacks", IEEE 2010, pp.203.

[22] A.T. Al-Taani and A.M. Al-Issa, " A Novel Steganographic Method for Gray-Level Images", International Journal of Computer, Information and Systems Science, and Engineering 3,1,2009.

[23] S. El Assad, H. Noura, I.Taralova, "Design and Analyses of Efficient Chaotic Generators for Cryptosystems," wcecs, pp.3-12, Advances in Electrical and Electronics Engineering - IAENG Special Edition of the World Congress on Engineering and Computer Science 2008, 2008.

[24] S. El Assad (85%), H. Noura (15%), "Generator of chaotic Sequences and corresponding generating system", WO Patent WO/2011/121,218, 2011.

[25] S. El Assad, "Chaos Based Information Hiding and Security," in 7th International Conference for Internet Technology and Secured Transactions, IEEE, London, United Kingdom, 10-12 Dec. 2012, pp. 67-72. Invited paper.

[26] C.Y. Song, Y.L. Qiao, and X.Z. Zhang, "An image encryption scheme based on new spatiotemporal chaos," Optik, October 2012.

[27] R.L. Tataru, D. Battikh, S. El Assad, H. Noura, O. Deforges, " Enhanced Adaptive Data Hiding in Spatial LSB Domain by using Chaotic Sequences" . IIH-MSP 2012: 85-88