Research Journal of Applied Sciences, Engineering and Technology 4(23): 4991-4995, 2012
ISSN: 2040-7467

Submitted: February 02, 2012 Accepted: April 30, 2012 Published: December 01, 2012

Steganography by using Logistic Map Function and Cellular Automata

Mehdi Alirezanejad and Rasul Enayatifar
Department of Computer, Firoozkooh Branch, Islamic Azad University, Firoozkooh, Iran

Abstract: A tradeoff between the hiding capacity of a cover image and the quality of a stego-image in steganographic schemes is inevitable. In this study a hybrid model of cellular automata and chaotic function is proposed for steganography. In this method, N-bits mask is used for choosing a pixel position in main image which is suitable for hiding one bit of secret data. This mask is generated in each stage by cellular automat and logistic map function. Using cellular automata and logistic map function cause more security and safety in proposed method. Studying the obtained results of the performed experiments, high resistance of the proposed method against brute-force and statistical invasions is obviously illustrated.

Keywords: Cellular automata, chaotic function, steganography

INTRODUCTION

Steganography is a technique, which facilitates hiding of a message in a cover in a way that the existence of a new message cannot be discerned (Beker and Piper, 1982). Steganography is part of the encryption technique with which the message can be sent without taking any notice. We can use the image, sound and text as a cover image (host image) to send the message. We use the image as the cover in this study. Using the image pixel LSB (Least Significant Bits) is one of the commonest ways for data Steganography in images (Zhang and Ping, 2003; Chan and Cheng, 2004; Ni *et al*., 2006). Those encrypting algorithm using the LSB image pixels which are subsequently adjusted for data embedding will be vulnerable against all kinds of attacks and manipulation which Westfield has brought in (Westfield and Pfitzmann, 1999). Therefore, in the researches done by so many researchers, the unsystematic data embedding in image LSB has attracted a lot of attention (Goljan *et al*., 2001). So many steganography researches employ the fact that in the area which have drastic gray phase changes (such as edges) we can hide more data compared to the smooth ones (Lin *et al*., 2008; Enayatifar *et al*., 2009). In trying to find the surfaces with more drastic changes of the gray area, some conducted researches used the neighboring pixel differences method (Lin and Hsueh, 2008) and in some others for separating the surfaces with drastic changes from the smooth ones, the mean score technique is used between the neighboring (adjacent) pixels (Enayatifar *et al*., 2009). In both groups after contrasting the two areas and based on their algorithm the data will be embedded in the areas. In Neumann (1966), a technique based on unsystematic data embedding in image LSB has been proposed in which embedding a character in an image is measured by two chaotic signals and the primary quantities of the two signals will be specified by two hidden keys.

In the proposed method we used N-bit mask for finding a best position in cover image for hiding a one bit of secret data. This mask is changed for hiding each bit of secret data. This is made with hybrid model of cellular automata and logistic map function. Two highlight advantages of this method are high capacity and homogeneous distribution. Proposed method causes secret data will have homogeneous distribution in cover image and this homogeneous distribution prevent some usual attack in this area.

What comes next is a short description of the chaotic function and cellular automata then the proposed technique will be offered and in the final section the empirical results of the proposed technique will be evaluated in different images.

METHODOLOGY

Cellular automata and chaotic function:

Cellular automata: Cellular automata were introduced by Preston and Duff (1984). They have been progressively used to model a great variety of dynamical systems in different application domains (Wolfram, 1985).

A cellular automaton is basically a computer algorithm that is discrete in space and time and operates on a lattice of sites (in our case, pixels). A (bi-dimensional, deterministic) Cellular Automaton (CA) is a triple A = (S;N: δ); where S is a nonempty set, called the state set, $N \subseteq Z^2$ is the neighborhood and $\delta : S^N \rightarrow S$ is

Corresponding Author: Mehdi Alirezanejad, Department of Computer, Firoozkooh Branch, Islamic Azad University, Firoozkooh, Iran

the local transition function (rule); the argument of δ indicates the states of the neighborhood cells at a given time, while its value the central cell state at the next time.

In order to define a neighborhood in a standard way we can use some norms h on R^2 such that N = B_h (0, r)$\cap -Z^2$ (where Bh (0, r) is the ball of radius r$\geq$1). The most common neighborhoods are:

- Von Neumann neighborhood using the norm:

$$R^2 \ni x \to h(x) := |x|_1 = |x_1| + |x_2| \in R_+, x = (x_1, x_2)$$

- Moore neighborhood attached to the norm:

$$R^2 \ni x \to h(x) := |x|_\infty = \max\{|x_1|, |x_2|\} \in R_+, x = (x_1, x_2)$$

A cellular automaton, A = (S; N; δ) is said to be symmetric if the value of the local rule is constant on symmetric inputs, i.e.,:

$$\delta(s_1, s_2, \ldots .s_{|N|}) = \delta(s_{\alpha(1)}, s_{\alpha(2)}, \ldots, s_{\alpha(N)})$$

for every $s_1, s_2, \ldots, s_N$ S

and $\sigma \in S_N$ (the permutation group of |N| degree)

Chaotic signal: Chaos is a phenomenon that occurs in definable nonlinear systems which are highly sensitive to initial values and trend to show random-like behavior. If such systems satisfy the conditions of Liapanov exponential equation, will continue to be in the chaotic mode. The main reason why these signals are utilized in image encryption is the definability of the system while being random-like; this caused the output of the system seem random to the invaders. Since it is definable by the encrypted, it is decodable. The advantages of these functions are studied in two parts:

Sensitivity to the initial value: This means that minor variation of the initial values can cause considerable differences in the next value of the function, that is when the initial signals varies a little, the resulting signal will differ significantly.

Random-like behavior: In comparison with the generators of ordinary random numbers, in which the series of generated random numbers are capable of regeneration, the random-number-generation methods utilized in chaotic function algorithms are able to regenerate the same random numbers, having the initial value and the transform function.

Equation (1) is one of the most well-known signals to have random-like behavior and is known as Logistic Map Signal:

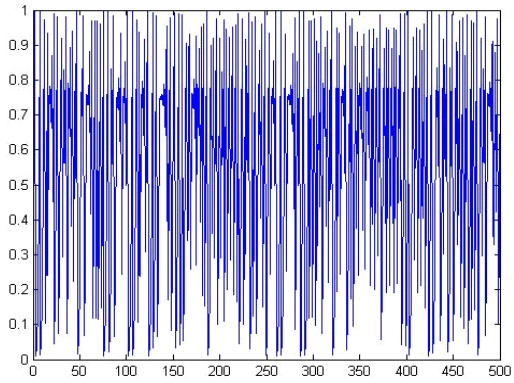

Fig. 1: The chaotic behavior of signal (1) in its 500 iterations

$$X_{n+1} = rX_n (1 - X_n) \quad (1)$$

The Logistic Map signal will have a chaotic behavior in case the initial value is $X_0 \in (0, 1)$ and r = 3.9999 In Fig. 1, the signal behavior with initial value is X_0 = 0.5 and r = 3.9999 can be seen.

Proposed methodology: In the proposed method we used N-bit mask for finding a best position in cover image for hiding a one bit of secret data. This mask is changed for hiding each bit of secret data. This is made with hybrid model of cellular automata and logistic map function. N value is determined in order to image dimension. In this study N value is equal to 8. It means image dimension is 256×256. The initial value for masking a 8-bit cell is defined by a 80-bit key. Then, to determine the new value of mask in every step, one of a 256 rules of standard cellular automata is used. To determine the cellular automata to be used, Logic map chaos function is implemented.

The steps of the proposed method:

Step 1: Defining a 80-bit key to determine the initial value of chaos function and 8-cell mask:

$$K = K_0, K_1, \ldots\ldots, K_9(Ascii) \quad (2)$$

In this key Ki represents a 8-cell block of the key that convert the mentioned key to binary value:

$$K = \begin{pmatrix} K_{01}, K_{02}, K_{03}, K_{04}, K_{05}, K_{06}, K_{07} \\ , K_{08}, \ldots\ldots\ldots\ldots, K_{91}, K_{92}, K_{93} \\ , K_{94}, K_{95}, K_{95}, K_{97}, K_{98}(Binary) \end{pmatrix} \quad (3)$$

In above-mentioned equation Kij is j^{th} bit of i^{th} block of the key. The initial value of chaos function is determined as follows. To calculate the initial value of the 8-cell mask, the key is used in the following fashion.

K_{00}	K_{01}	K_{02}	K_{03}	K_{04}	K_{05}	K_{06}	K_{07}

Step 2: In this step, X0, generated in the first step, is used to determine the initial value of chaos function for defining one of the 256-fold rules of cellular automata. As it was seen in the last section the interval changes of this signal is [0, 1]. This interval is divided to p segment with the following size:

$$\varepsilon = 1/p \quad (4)$$

The range if i^{th} segment is defined using the following equation:

$$((i-1) \times \varepsilon, i \times \varepsilon) \quad (5)$$

Regarding X0, the first value is generated using chaos function Eq. (1). Considering p = 255 (number of cellular automata rules varies from 0 to 255) and Eq. (1) and (5), one of the automata rules is determined by the following equation:

$$X_{Rule} = Round\ (P \times X_{n-1}) \quad (6)$$

The value of X_{Rule} is considered as the number of automata rule.

Step 3: The desired rule is applied on all cells of the 8-cell mask simultaneously to form the new mask. The first value is used as row number to hide a bit of code data. With reapplying the automata rule on the 8-cell mask, the column position for hiding the bit of code is determined. After determining row and column positions of the 8-cell mask, these values are converted to decimal values. To hide all bits of code, steps 2 and 3 are repeated. To better understand this process, an example is presented. In this example, it is assumed that the initial value of 8-bit mask is 11010001 according to key value. The initial value of chaos function is assumed 0.491. Regarding these assumed values, the row position of the desired pixel to hide a bit of code data is determined.

The 126^{th} rule of cellular automata is selected. This rule is presented in Table 1 according to Volfram rules.

Applying rule number 126 of cellular automata on the initial value of 8-cell mask (11010001) the value (11111011) is achieved. Converting to decimal values, the value 251 is obtained. This value is the row position of the cover pixel. To find the column position, first, the new value of chaos function is determined as follows:

Table 1: Cellular automata rule sample

F (111)	F (110)	F (101)	F (100)	F (011)	F (010)	F (001)	F (000)
0	1	1	1	1	1	1	0

Table 2: Entropy for images with size 128×128

Images	128×128	256×256
Photographer	39.62	42.23
Boat	37.98	41.90
Lena	36.46	43.14
Tiffany	38.22	39.94
Peppers	38.74	39.41

$$X_1 = 3.99 \times 0.497*(1-0.497) = 0.99717681$$

Considering this value, the corresponding cellular automata rule is determined as:

$$X_{Rule} = Round\ (256 \times 0.99717681) = 255$$

Finally, applying rule 255 on (11111011) the value (11111111) is achieved which equal to 255 in decimal scale and is used as the column position of the cover pixel. As a result, the first bit of the code is placed in (126,255) pixel for hiding. All other bits are placed in different pixels with the same process.

EXPERIMENTAL RESULTS

In this section we do some experiment for prove a efficiency of proposed method.

Peak Signal to Noise Ratio (PSNR): We used the PSNR as a scale for the image quality of the Stego-image. The value of the PSNR which is the ratio of signals to the noise, we use the Eq. (5) Neumann (1966):

$$PSNR = 10*\log_{10}\left(\frac{255^2}{\frac{1}{W*H}\sum_{i=1}^{W}\sum_{j=1}^{H}\left(O_{ij} - D_{ij}\right)^2}\right) \quad (7)$$

In which the O_{ij} and D_{ij} show the values of the gray levels of the main image pixels and Stego-image, respectively; and H and W show the image length and width.

We use five images with size 128×128 and 256×256 for getting entropy. Results show in Table 2.

Date quality analysis: In this section, the stability of the proposed methods against different conventional attacks in this field is investigated. The main purpose of this section is to find out to what extent the code data will be lost if Stego-Image is attacked.

To do so, first a code is hided in a cover image using the proposed methods. Then, a sheer-attack is applied to the image. Finally the code, covered in the image, is extracted and compared to the initial code. The results indicate the stability of the proposed algorithm against

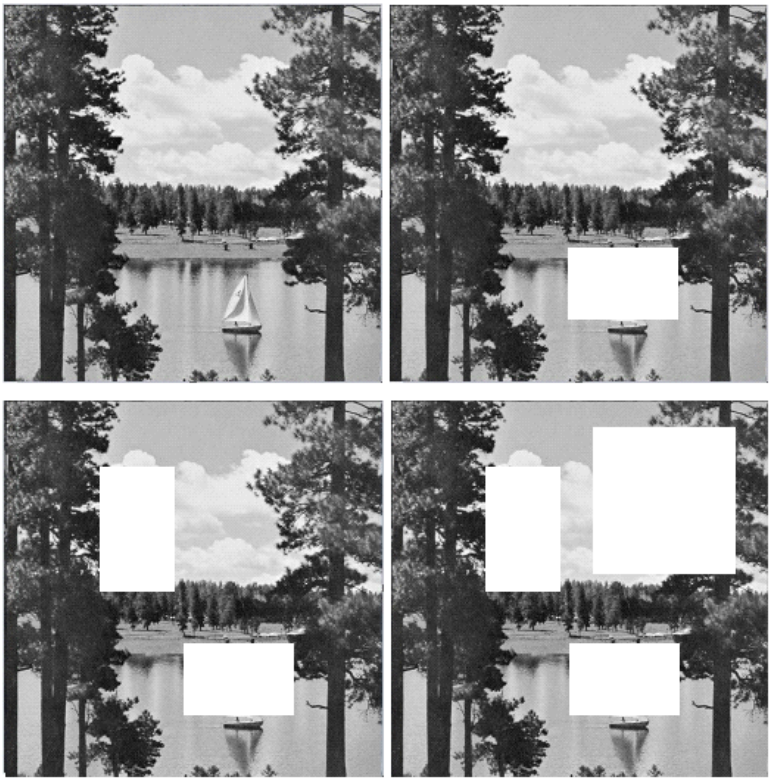

Fig. 2: Boat with 5, 10 and 20% cutting, respectively

Table 3: Losing number of bits after cutting

	Cutting rate		
Cover image	5%	10%	20%
Boat 128 ×128	238	562	1148
Boat 256 ×256	123	209	432
Boat 512 ×512	36	87	193

common attacks. In this experiment, after hiding 8000 bit of the code in the cover image, the cover image is being attacked to extent of 5, 10 and 20 (Fig. 2) to see the extent in which code is lost.

The code bits are extracted from Stego-Image after different attacks are applied. Table 3 presents the results and the percentage of the lost data. This experiment is also repeated for Boat image with 256*256 and 512*512 dimensions. The corresponding results are shown in Table 3.

Resisting the attacks: There are two common kinds of attacks in Steganography technique which are Brute force and book code.

Brute force: In this kind of attack all the possible keys will be tested on the coded image to uncover the original text. It means if the keys are long and complicated, there would be a lot of effort to decode the algorithm. Using keys with 80 bits holds 2^{80} possibilities for guessing. Therefore, the needed ability to for decoding will be increased as the length of the key increases.

Book code attack: In Code Book method, considered as classical kind of method, all the possible changes in original and Stego-image will be included under one certain key and after the analysis they try to find the key. Due to the fact that the chaotic functions technique are naturally unsystematic and because of their sensitivity to the primary values (a minor change in the primary values will bring about a drastic change at the end) the brute force attacks are not effective on the chaotic functions.

CONCLUSION

A new method was proposed for image Steganography in this study using the chaotic signal and cellular automata rules. Method, N-bits mask is used for choosing a pixel position in main image which is suitable for hiding one bit of secret data. This mask is generated in each stage by cellular automat and logistic map function. Using cellular automata and logistic map function cause more security and safety in proposed method. The high sensitivity of this technique to the primary values will stop the book code attacks and the achieved PSNR value of 43.14 proves the high efficiency of the technique.

REFERENCES

Beker, H. and F. Piper, 1982. Cipher Systems: The Protection of Communications. Northwood Books Landon

Chan, C.K. and L.M. Cheng, 2004. Hiding data in images by simpleLSB substitution. Pattren Recogn., 37(3): 469-474.

Enayatifar, R., S. Faridnia and H. Sadeghi, 2009. Using the chaotic map in image steganography. International Conference on Signal Processing Systems, Singapore

Goljan, M., J. Fredrich and R. Du, 2001. Distortion-free data embedding. Proceedings of 4th Information Hiding Workshop, pp: 27-41.

Lin, C.C. and N.L. Hsueh, 2008. A lossless data hiding scheme based on three-pixel block differences. Pattern Recogn., 41(4): 1415-1425.

Lin, C.C., W.L. Tai and C.C. Chang, 2008. Multilevel reversible data hiding based on histogram modification of difference images. Pattern Recogn., 41(12): 3582-3591.

Neumann, J., 1966. Theory of Self-Reproducing Automata. (Edited and Completed by Arthur Burks), University of Illinois Press, Champaign, IL.

Ni, Z., Y.Q. Shi, N. Ansari and W. Su, 2006. Reversible data hiding, circuits and systems for video technology. IEEE Trans., 16: 354-362

Preston, K. and M.J.B. Duff, 1984. Modern Cellular Automata. Theory and Applications, Plenum Press, London.

Westfield, A. and A. Pfitzmann, 1999. Attacks on steganographic system. 3rd International Workshop on Information Hiding, pp: 61-76.

Wolfram, S., 1985. Cryptography with cellular automata. Pro.Crypto., 85: 429-432.

Zhang, T. and X. Ping, 2003. A new approach to reliable detection ofLSBsteganography in natural images. Signal Proc., 83(10): 2085-2093.