A NOVEL SECURE IMAGE STEGANOGRAPHY METHOD BASED ON CHAOS THEORY IN SPATIAL DOMAIN

Debiprasad Bandyopadhyay[1], Kousik Dasgupta[2], J. K. Mandal[3], Paramartha Dutta[4]

[1]Deptt. of CSE, Kalyani Government Engineering College, Kalyani-741 235, India
[2]Deptt. of CSE, Kalyani Government Engineering College, Kalyani-741 235, India
[3]Deptt. of CSE, Kalyani University, Kalyani-741 235, India
[4]Deptt. of CSS, Visva-Bharati University, Santiniketan-731 235, India

ABSTRACT

This paper presents a novel approach of building a secure data hiding technique in digital images. The image steganography technique takes the advantage of limited power of human visual system (HVS). It uses image as cover media for embedding secret message. The most important requirement for a steganographic algorithm is to be imperceptible while maximizing the size of the payload. In this paper a method is proposed to encrypt the secret bits of the message based on chaos theory before embedding into the cover image. A 3-3-2 LSB insertion method has been used for image steganography. Experimental results show a substantial improvement in the Peak Signal to Noise Ratio (PSNR) and Image Fidelity (IF) value of the proposed technique over the base technique of 3-3-2 LSB insertion.

KEYWORDS

Image Steganography, Dynamic System, Chaotic Maps, Human Visual System, Cover Image & LSB

1. INTRODUCTION

Since the rise of Internet one of the most important factors of information technology and communication has been the security of information. Cryptography was created as a technique for securing the secrecy of communication and many different methods have been developed to encrypt and decrypt data in order to keep the message secret. Unfortunately it is sometimes not enough to keep the contents of a message secret, it may also be necessary to keep the existence of the message secret. The technique used to implement this, is called steganography [1]. Steganography is the art of hiding messages in a medium called cover object in such a way that existence of message is undetectable. Imperceptibility is clearly is the most important requirement in steganographic schemes [2]. The cover object could be a digital image, an audio file, or a video file. The secret message called payload could be a plain text, an image, a video file or an audio. Steganographic methods are classified into spatial domain embedding and frequency domain embedding. In frequency domain, images are transformed into frequency components by using DCT, FFT or DWT and then messages are embedded either in bit level or in block level [3]. In spatial domain LSB replacing is the most widely used data hiding method. However most of the LSB Techniques are prone to attacks [4, 5]. Because of low computational complexity and high embedding capacity this paper mainly deals with LSB Steganography method.

DOI : 10.5121/ijsptm.2014.3102

Chaos theory, a mathematical physics, was developed by Edward Lorenz [6] and it is a deterministic and analogously stochastic process appearing in a non linear dynamical system [7, 8]. The theory studies the behavior of systems that follow deterministic laws but appear random and unpredictable or we can say a dynamical system that has a sensitive dependence on its initial conditions; small changes in those conditions can lead to quite different outcomes [9]. One of the fundamental principles of chaotic functions is sensitivity to initial conditions. A small difference in the starting values of the function will, after many iterations, lead to a great divergence in the produced behavior. This sensitivity has a fractal nature which can be utilized to find all solutions to a nonlinear equation [10]. Based on utilizing sensitive fractal areas to locate all the solutions along one direction in a variable space, a method for searching of global minima in optimization problems was introduced [11]. However, there are no mathematical proofs about the benefits of using chaotic sequence [12]. Confidentiality, non-periodicity, more randomness and easy implementation are the main advantages of using chaos theory in steganography technique.

In several fields the idea of using chaotic systems has been noticed. Using this novel approach in non-linear dynamics a large number of applications in real systems, both man-made and natural, are being investigated [13]. For the last few decades many chaos based steganographic methods have been proposed and discussed. K Ganesan et. al. [14] focused on developing algorithm that can be used to hide the secret messages using random number logic. They have concentrated upon using LSB conversion. In [15], Arnold and 2D logistic methods have been proposed. Here the secret message is encrypted chaotically and then embedded using two steganographic methods. A Steganography method is proposed in [16], to embed information within an encrypted image randomly. It provides a simple and strong way to hide the secret information in the encrypted image. Thus, reducing the chance of the encrypted image being detected and then enhance the security of the encrypted images. In [17], based on chaotic mapping and human visual characteristics a large capacity of steganographic technique is proposed and it can embed secret data adaptively into the still image. Experimental results show substantial improvement in capacity and invisibility. It is robust for the image processing techniques like image cropping compression, etc. In [18] the logistic map is used to generate a sequence as the watermark. The logistic map is used to shuffle the bits order of the secret message in [19]. In [20], based on the fractal theory, an optimization technique has been presented by modifying a chaos optimization algorithm (COA). Here the weighted gradient direction-based chaos optimization is implemented in which the chaotic property is used to determine the initial choice of the optimization parameters both in starting step and the mutations applied when a convergence to local minima occurred. In [21] the proposed technique uses a fractal image as the host image and then generated a random like sequence by chaotic map as the reference for embed positions, and uses a wavelet transform to realize the embedding procedure. A Haar wavelet transform is used in [22] to decompose the image into averaging and differencing components. In [23] once the message is embedded within the cover image, it is encrypted using triple-key chaotic image encryption. A hybrid model of chaotic function and cellular automata is presented in [24]. By using an N-bits mask pixel position is determined in the cover image for hiding one bit of secret message. The mask is generated in each stage by cellular automata and logistic map function. In [25] a new technique is presented based on chaotic steganography and encryption text in DCT domain for color images.

The rest of the paper is organized as follows. In Section 2 the proposed image steganographic technique has been described. In Section 3 the proposed technique is illustrated. In Section 4 the algorithm is proposed. An application of the proposed algorithm using a simulated environment is given in Section 5. Experimental results and performance evaluation are discussed in Section 6. Finally conclusions are addressed in Section 7.

2. CHAOS BASED LEAST SIGNIFICANT BIT STEGANOGRAPHY (C-LSB)

In the proposed method the logistic chaotic map is used to encrypt the secret message and then embedded into the cover image using the base embedding technique as described in Section 2.2. The logistic map is used to encrypt the secret data bits before embedding to enhance the security of the image steganography as the secret data bits are not embedded directly into the cover image.

2.1. Preliminary

This proposed technique adopts logistic mapping method to generate chaotic sequence. It is one of the simplest chaotic maps defined by the Equation 1 as bellow

$$X_{k+1} = \mu X_k(1 - X_k) \tag{1}$$

Here $0 \leq \mu \leq 4$ and $0 < X_k < 1$. The logistic map stands in chaotic region when $3.5699456 < \mu \leq 4$ [6]. Here μ is a control parameter. Thus, the sequence $\{X_{k,}\ k = 0, 1, 2, \ldots\}$ generated is non-periodic and non-convergent. In Figure 1, the chaotic behavior of logistic map with initial values $X_0 = 0.5$ and $\mu = 3.9999$ can be seen. The logistic sequences generated from different initial conditions are uncorrelated statistically. This means that the 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 [26].

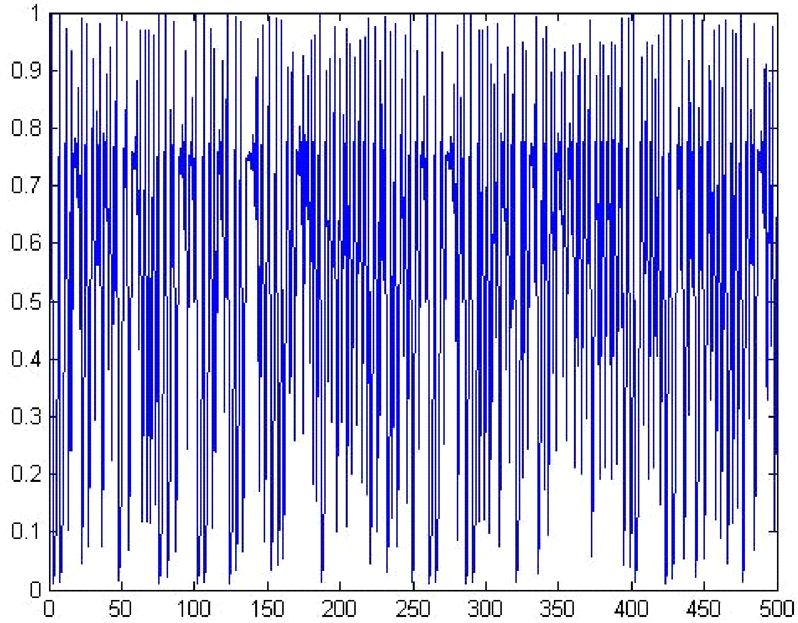


Figure 1: The chaotic behavior of Equation 1 in its 500 iterations.

2.2. Base Technique

In the base technique eight bits of secret data are considered for embedding at a time in the LSB of RGB pixel value of the carrier image in 3, 3, 2 order respectively. Thus first three bits of the secret message are concealed inside three (03) bits of LSB of Red pixel, next three bits in the three (03) bits of LSB of Green pixel. The remaining two bits of secret message are concealed in two (02) bits of LSB of Blue pixel. The detailed technique has been depicted in Figure 2. The particular distribution pattern is taken considering that the chromatic influence of blue to the human eye is more than that of red and green pixels [27].

The base technique of image steganography algorithm is enumerated bellow:

Step 1: Find four LSB bits of each RGB pixels of the cover image.

Step 2: Embed the eight bits of the secret message into 4 LSB of RGB pixels of the cover image in the order of 3, 3, 2 respectively.

Step 3: Form the stego image.

Whereas the decoding algorithm is explained bellow:

Step 1: Find four LSB bits of each RGB pixels of the stego image.

Step 2: Retrieve the bits of the secret message from LSB of RGB pixels of the stego image in the order of 3, 3, 2 respectively.

Step 3: Construct the secret message.

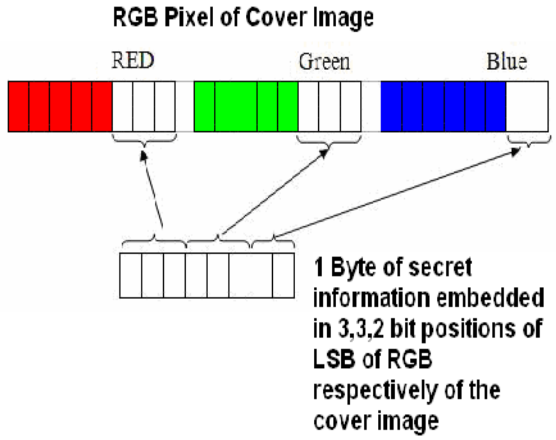

RGB Pixel of Cover Image
RED
Green
Blue
1 Byte of secret information embedded in 3,3,2 bit positions of LSB of RGB respectively of the cover image

Figure 2: Base embedding technique showing 1 Byte of secret data embedded inside 4 bits of LSB in 3, 3, 2 order into corresponding RGB pixels of carrier image

2.3. System Architecture

The system architecture of CLSB technique for Image Steganography has been depicted in the flow diagram in Figure 3.

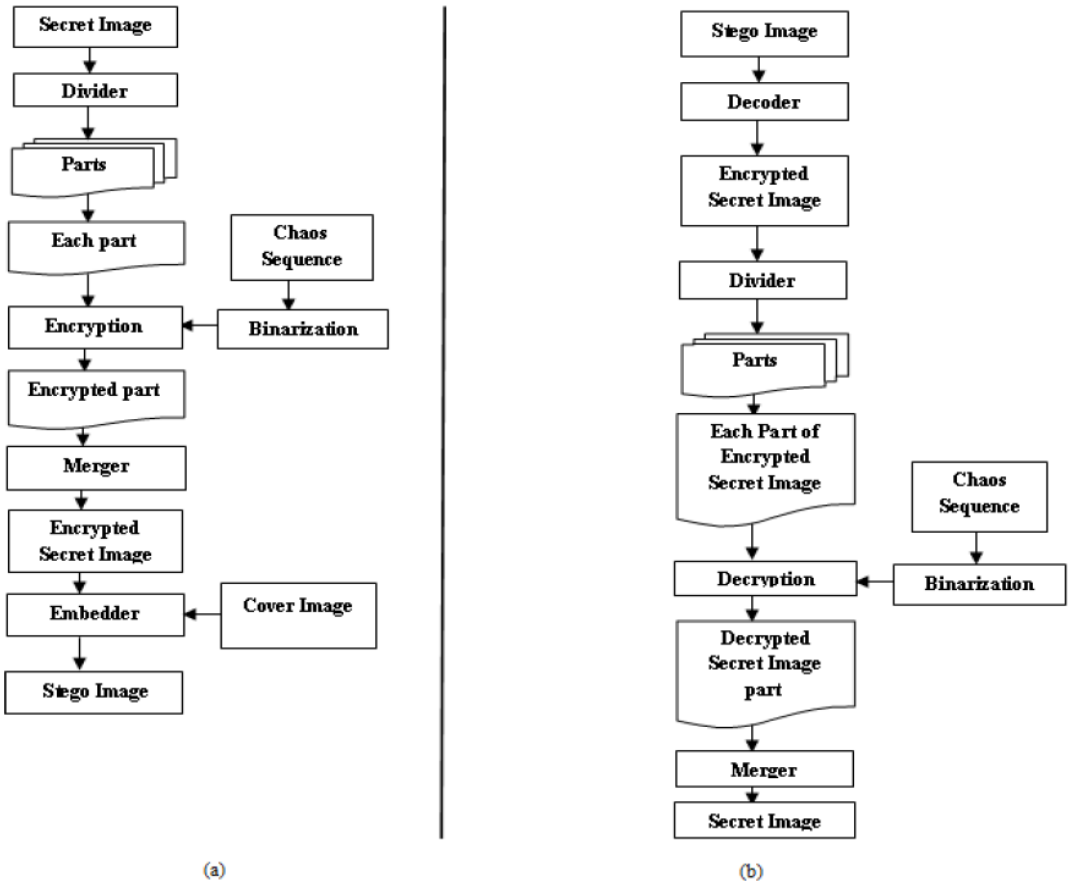


Figure 3: System Architecture of the CLSB Image Steganography technique (a) Encoding and (b)Decoding

The system architecture for Image Steganography (Encoding) is given in Figure 3(a). The carrier or cover image is first divided into multiple parts by the module called **Divider.** In the proposed technique eight parts are considered. Now each of the parts of the secret image is encrypted by the procedure illustrated in Section 3. The **Merger** module will merge these encrypted parts to form the encrypted secret image and this encrypted image is given as input to the **Embedder**. The embedding is done using the 3-3-2 base embedding technique (as described in Section 2.2). After all the bits are embedded in the cover image the stego image is obtained.

The system architecture of Decoding is depicted in Figure 3(b). The decoding is done to get back the secret image by following the reverse process. The stego image is passed through a **Decoder**. It extracts the encrypted secret image from the stego image. The encrypted secret image is divided into same number of parts by the **Divider** as done during encoding for the original secret image. Decryption is done by the procedure illustrated in Section 3. This process is repeated for each of the encrypted secret image part until all the bits are decrypted. The **Merger** module will merge these decrypted image parts to form the original secret image.

3. Illustration Of C-LSB Technique

Consider a secret image of resolution H×W where H is the height and W is the width of the image. Chaos theory can be applied in multiple parts of the secret image with different initial conditions for each part to take the advantage of its sensitiveness to initial conditions, provide unpredictability and enhance the security.

The secret image is divided into eight equal parts such that each part will have resolution of M×W where M is the height and W is the width of this part of the image. Thus the total number of pixels in each secret image part is M×W and each pixel has three 8 bit components R (Red), G (Green) and B (Blue). So the total number of components (N) in this secret image part is N=M×W×3.

Now using the logistic map as given in equation 1 a logistic chaotic sequence of N real numbers is generated as $\{X_k\}$ where k = 0, 1, 2, … N-1. The initial values of μ and X are considered as 3.60 and 0.65 respectively, as the logistic map stands in chaotic region when $3.5699456 < \mu \leq 4$ and $0 < X_k < 1$ [6].

With the initial values of μ and X considered as 3.60 and 0.65 the logistic chaotic sequence of N numbers is shown as bellow:

$\{X_k\}$ = {0.819000, 0.533660, 0.895921, 0.335687, 0.802805, 0.569913, 0.882404, 0.373563, …}
Next the arithmetic mean of these N real numbers is considered as threshold T.

Here $T = \sum_{k=0}^{N} X_k \big/ N = 0.646400$ for the first secret image part.

Thus for each k=0, 1, 2, …N-1 if $X_K \geq T$ then $B_k = 1$ otherwise 0. Thus for the first secret image part the binary sequence $\{B_k\}$ is generated as bellow:

$\{B_k\}$ = {1, 0, 1, 0, 1, 0, 1, 0, ….}

For each 8 bit component $C_{k(k=0,1,...N-1)}$ of the secret image part an XOR operation of each bit of C_k is done with a single bit of B_k in the binary sequence e.g. if C_k = 01010000 and B_k =1 then C_k' = 10101111. Where C_k' is the encrypted component. Repeat this procedure until all such components of the secret image part is encrypted.
The same procedure is followed for the remaining seven parts of secret image. Each part is encrypted using different logistic maps as given in Equation 1 with different initial conditions of and X. The pair of values (μ, X) considered are (3.60, 0.65), (3.61, 0.66), (3.62, 0.67), (3.63, 0.68), (3.64, 0.69), (3.65, 0.70), (3.66, 0.71), (3.67, 0.72). Finally the encrypted parts are merged to form the encrypted secret image.

At last embed each eight bit component of the encrypted secret image into 4 bits of LSB as described in Section 2.2, thus forming a stego image. An algorithm of the proposed encoding and steganography is given in Section 4.1 and depicted in Figure 3(a).

For decoding a reverse method is applied where all the bits are extracted from LSB of the RGB pixels of the stego image in the order 3, 3, 2 respectively [27]. The encrypted secret image so obtained of resolution H×W is divided into eight equal parts. Using the logistic map as given in equation 1 a logistic chaotic sequence of N real numbers is generated as $\{X_k\}$, considering the same initial values of μ and X as in encoding. Next the arithmetic mean of these N real numbers is considered as threshold value T and for each $X_K \geq T$ generate a binary sequence B_k = 1 otherwise 0. Thus a binary sequence $\{B_k\}$ is generated where k = 0, 1, 2, … N-1. For each 8 bit component C_k' of the encrypted secret image part where k=0, 1, 2, ... N-1 XOR each bit of the component with a single bit B_k in the binary sequence e.g. if C_k' = 10101111 and B_k =1 then C_k = 01010000.

Repeat this procedure until all the encrypted eight bit components of the secret image part are decrypted. This process is repeated for the remaining seven parts with the different initial conditions for logistic as assumed during encoding. After decrypting all the encrypted image parts the parts are merged to form the original secret image. An algorithm of the proposed decoding and desteganography is given in Section 4.2 and depicted in Figure 3(b).

4. Algorithm Of C-LSB

The proposed algorithm both for encoding and decoding are given in this section. Encoding and decoding techniques are given in Section 4.1 and 4.2 respectively.

4.1 Embedding Algorithm

The embedding technique is explained by the following steps:

Step 1: Input cover image, secret image.
Step 2: Read required information of the cover and secret image.
Step 3: Break the secret image into eight parts.
Step 4: For each of the eight parts generate a bit sequence by the procedure as described in Section 3.
Step 5: Encrypt eight bits of the secret image part by XOR operation with a single bit in the bit sequence generated for the corresponding secret image part obtained from step 4. Repeat this step for each of the secret image parts.
Step 6: Embed the encrypted eight bits of the secret image into 4 bits of LSB of RGB pixels of the cover image in the order 3, 3, 2 respectively until all the bits of the encrypted secret image are embedded.
Step 7: Stop.

4.2 Decoding Algorithm

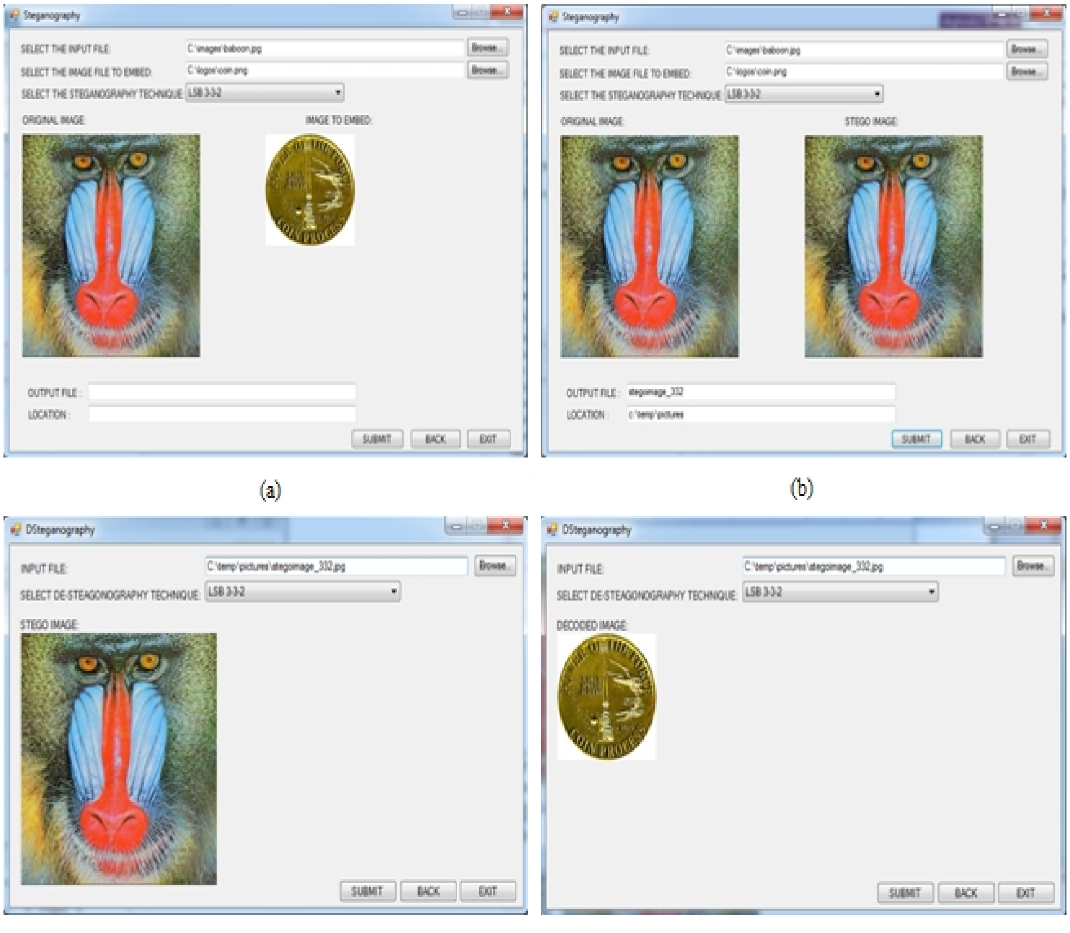
The decoding algorithm consists of eight steps as follows:

Step 1: Input stego image.
Step 2: Read required information from stego image.
Step 3: Retrieve the bits from LSB of RGB pixels of the stego image in the order 3, 3, 2 respectively to get the encrypted secret image.
Step 4: Break the encrypted secret image into eight parts.
Step 5: For each of the eight parts generate a bit sequence the procedure as described in Section 3.
Step 6: Each of the eight bits of encrypted secret image part will be XORed with a single bit in the bit sequence obtained from step 5 to construct original eight bits of the secret image. Repeat this step for each of the encrypted image parts.
Step 7: Form the secret image.
Step 8: Stop.

5. Application Of The Proposed Technique

A simulation environment is implemented as **ChaoticStego Engine** using Visual C++ 2012 as IDE (Integrated Development Environment) and OpenCV 1.0 as the graphics library. An application of the proposed algorithm with a test image (baboon.jpg) has been shown in Figure 4.

It shows a carrier image (baboon.jpg), a secret image (coin.png) and after steganography the corresponding stego image. On decoding the secret image (coin.png) is obtained back.



(a)

Steganography

SELECT THE INPUT FILE: C:\images\baboon.jpg

SELECT THE IMAGE FILE TO EMBED: C:\logos\coin.png

SELECT THE STEGANOGRAPHY TECHNIQUE: LSB 3-3-2

OUTPUT FILE :

LOCATION :

(b)

Steganography

SELECT THE INPUT FILE: C:\images\baboon.jpg

SELECT THE IMAGE FILE TO EMBED: C:\logos\coin.png

SELECT THE STEGANOGRAPHY TECHNIQUE: LSB 3-3-2

OUTPUT FILE : stegoimage_332

LOCATION : c:\temp\pictures

(c)

DSteganography

INPUT FILE: C:\temp\pictures\stegoimage_332.jpg

SELECT DE-STEAGONOGRAPHY TECHNIQUE: LSB 3-3-2

(d)

DSteganography

INPUT FILE: C:\temp\pictures\stegoimage_332.jpg

SELECT DE-STEAGONOGRAPHY TECHNIQUE: LSB 3-3-2

Figure 4: Simulation Environment (a) cover image and secret image and (b) cover image and stego image (c) stego image (d) Decoded secret image

6. EXPERIMENTAL RESULTS AND PERFORMANCE EVALUATION

Imperceptibility and capacity are the two important aspects of steganography. Imperceptibility means the embedded data must be imperceptible to the observer (perceptual invisibility) and computer analysis (statistical invisibility) [27]. For performance evaluation four different images are considered. Details of each are given in Table 1. The details of the secret image are also given in Table 1. The measures of capacity for the different carriers are listed in Table 2 in terms of payload (bits per byte or *bpB*). Increase or maintaining the payload and maintaining an acceptable level of stego quality is considered as good contribution. Two types of perceptibility measure are listed in Table 2 namely fidelity and quality. Fidelity means perceptual similarity between signals before and after processing. However to determine the goodness of a signal quality is an absolute measure to avoid any suspension and therefore detection. The quality measure is measured by PSNR [28] as given in Equation 2.

$$\mathrm{PSNR} = 10\log_{10} L^2 / MSE \tag{2}$$

Where L is peak signal level for a gray scale image and it is taken as 255. The value of MSE [28] is calculated by Equation 3.

$$\mathrm{MSE} = 1/\mathrm{HW} \sum_{i=1}^{H} \sum_{j=1}^{W} (P(i, j) - S(i, j))^2 \tag{3}$$

Where H and W are height and width and *P(i, j)* represents the original image and *S(i, j)* represents corresponding stego image. Whereas the fidelity measure is measured by Image Fidelity (IF) [28] as given in Equation 4.

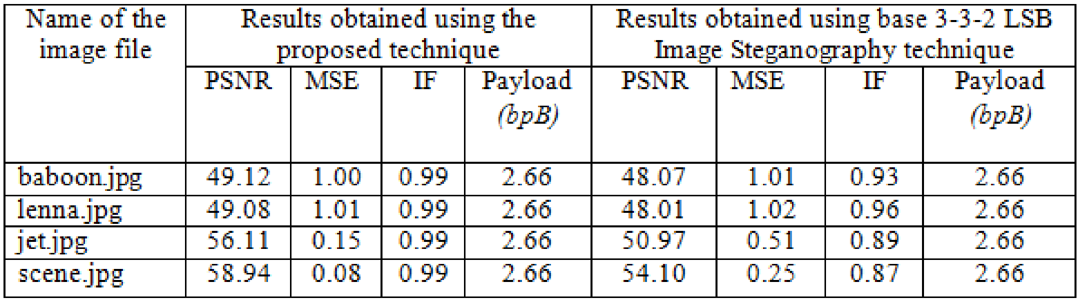
$$\mathrm{IF} = 1 - \sum_{\mathrm{H,W}} (\mathrm{P(i, j) - S(i, j)})^2 \Big/ \sum_{H,W} P(i, j) * S(i.j) \tag{4}$$

The results are also compared with the corresponding base embedding technique without chaos. As eight bits are embedded per three bytes, so payload is 2.66 *bpB*. Comparing the results it can be observed that, though the payload is same as that of the base method, but there is an improvement in PSNR and IF value.

Table 1: Cover Image Details

S. No.	Cover image file information		Secret image file information (Resolution) (H×W)
	Name	Resolution (H×W)	
01	baboon.jpg	256×256	64×64
02	lenna.jpg	256×256	
03	jet.jpg	512×256	
04	scene.jpg	512×512	

Table 2: Performance evaluation of the proposed C-LSB technique over base 3-3-2 LSB Image Steganography technique



Name of the image file	Results obtained using the proposed technique				Results obtained using base 3-3-2 LSB Image Steganography technique			
	PSNR	MSE	IF	Payload *(bpB)*	PSNR	MSE	IF	Payload *(bpB)*
baboon.jpg	49.12	1.00	0.99	2.66	48.07	1.01	0.93	2.66
lenna.jpg	49.08	1.01	0.99	2.66	48.01	1.02	0.96	2.66
jet.jpg	56.11	0.15	0.99	2.66	50.97	0.51	0.89	2.66
scene.jpg	58.94	0.08	0.99	2.66	54.10	0.25	0.87	2.66

7. Conclusion

A secure LSB technique for image steganography has been proposed in this paper using the concept of non-linear dynamic system (chaos). The chaotic system is highly sensitive to initial values and parameter of the system. The proposed algorithm provides added security to the base steganography technique. Application of separate chaotic sequence for encryption of each part of secret image provides an added security from attacks. The proposed technique uses host image files in spatial domain to hide the presence of sensitive information regardless its format. Performance analysis of the proposed technique after comparing with 3-3-2 LSB technique is quite encouraging. The proposed technique is applied to JPEG files; however it can work with any other formats. Further work includes adapting the free parameters of the logistic chaotic map using soft computing techniques as chaotic systems are highly sensitive to initial conditions.

References

[1] T. Morkel, J. H. P. Eloff, and M. S. Oliver, (2005) “An Overview of Image Steganography”, in Proc. of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa.

[2] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, (1999) “Information hiding-A survey,” in Proc. of IEEE, Vol. 87, No. 7, pp. 1062-1078.

[3] Min Wu and Bede Li, (2003) Multimedia Data Hiding, Springer, 1st edition.

[4] A. Westfield and A. Pfitzmann, (1999) “Attacks on Steganographic Systems”, in Proc. of 3rd Info. Hiding Workshop, Dresden, Germany, Sept. 28-Oct. 1, pp. 61-75.

[5] J. Fridrich, R. Du, and L. Meng, (2000) “Steganalysis and LSB Encoding in Color Images”, in Proc. of ICME 2000, N. Y., USA.

[6] E. Lorenz, (1995) The Essence of Chaos, CRC Press, 3rd edition, ISBN 978-0295975146.

[7] Z. Liu and L. Xi, (2007) “Image information hiding encryption using chaotic sequence,” in Proc. of the 11th International Conference on Knowledge-Based Intelligent Information and Engineering Systems and the XVII Itallian Workshop on Neural Networks, pp. 202-208.

[8] Y. Zhang, F. Zuo, Z. Zhai, and C. Xiaobin, (2008) “A new image encryption algorithm based on multiple chaos system”, in Proc. of the International Symposium on Electronic Commerce and Security (ISECS ’08), pp. 347-350.

[9] J. M. Amigo, L. Kocarev, and J. Szczepanski, (2007) “Theory and Practice of Chaotic Cryptography”, in Proc. of Physics Letters A 366, pp. 211-216.

[10] V.T. Jovanovic and K. Kazerounian, (1998) “Using Chaos to Obtain Global Solutions in Computational Kinemetics”, in Proc. of Journal of Mechanical Design, Vol. 120, No. 2, pp. 299-304.

[11] V.T. Jovanovic, and K. Kazerounian, (2000) “Optimal Design using Chaotic Descent Method”, in Proc. of Journal of Mechanical Design, Vol. 123, No. 2, pp. 265-270.

[12] M. Bucolo, R. Caponetto, L. Fortuna, M. Frasca, and A. Rizzo, (2002) “Does chaos work better than noise?”, in Proc. of IEEE Circuits and Systems Magazine, Vol. 29, No. 4, pp. 409-419.

[13] Bhavana. S and K. L. Sudha, (2012) “Text Steganography using LSB insertion Method Along With Chaos Theory”, in Proc. of International Journal of Computer Science, Engineering and Applications (IJCSEA), Vol. 2, No. 2, pp. 145-149.

[14] K. Ganesan, B. Venkatalakshmi, and R. Krishna Moothy, (2004) “Steganography using enhanced chaotic encryption technique”, Available: http://www.niitcrcs.com/iccs/iccs2004/Papers/145%20B%20Venkatalakshmi.pdf.

[15] Dr. K. L. Sudha, and Manjunath Prasad, (2011) “Chaos image encryption using pixel shuffling with henon map,” in Proc. of Elixir Elec. Engg. 38, pp. 4492-4495.

[16] Mohammad Ali Bani Younes and Aman Jantan, (2008) “A new steganography approach for image encryption exchange by using least significant bit insertion”, in Proc. of International Journal of Computer Science and Network Security(IJCSNS), Vol. 8, No. 6.

[17] Peipei Liu, Zhongliang Zhu, Hongxia Wang, and Tianyum Yan, “A novel image steganography Using chaotic map and visual model”, Available: www.atlantispress.com/php/download_paper.php?id=1452.

[18] Z. Dawei, C. Guanrong, and L. Wenbo, (2004) "A Chaos-based robust wavelet-domain watermarking algorithm", in Proc. of Chaos, Solitons and Fractals, Vol. 22, No. 1, pp. 47-54.

[19] L. Yu, Y. Zhao, R. Ni, and T. Li, (2012) "Improved Adaptive LSB Steganography Based on Chaos and Genetic Algorithm", in Proc. of EURASIP Journal on Advances in Signal Processing, Vol. 10, pp. 1-6.

[20] Mahammad Saleh Tavazoei and Mahammad Haeri, (2007) "An optimization algorithm based on chaotic behavior and fractal nature", in Proc. of Journal of Computational and Applied Mathematics 206), pp. 1070-1081.

[21] Yue Wu and Joseph P. Noonan, (2012) "Image Steganography Scheme using Chaos and Fractals with the wavelet Transform", in Proc. of International Journal of Innovation, Management and Technology, Vol. 3, No. 3, pp. 285-289.

[22] Nidhi Sethi and Deepika Sharma, (2012) "A novel method of image encryption using logistic mapping", in Proc. of International Journal of Computer Science Engineering (IJCSE), Vol. 1, No. 2, pp. 115-119.

[23] Arun A.S. and George M. Joseph, (2013) "High Security Cryptographic Technique using Steganographjy and Chaotic Image Encryption", in Proc. of Journal of Computer Engineering (IOSR-JCE), vol 2, pp 49-54.

[24] Mehdi Alirezaanejad and Rasul Enayatifar, (2012) "Steganography by using logistic map function and cellular automata" in Proc. of Research Journal of Applied Sciences, Engineering and Technology, pp. 4991-4995.

[25] Melad J. Saeed, (2013) "A new technique based on chaotic steganography and encryption text in DCT domain for color images", in Proc. of Journal of Engineering Science and Technology, Vol. 8, No. 5, pp. 508-520.

[26] Rasul Enayatifar, (2011) "Image Encryption via logistic map function and heap tree", in Proc. of International Journal of the Physical Sciences, Vol. 6, No. 2, pp. 221-228.

[27] Kousik Dasgupta, J. K. Mandal, and Paramartha Dutta, (2012) "Hash Based Least Significant Bit Technique For Video Steganography(HLSB)", in Proc. of International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, No. 2, pp. 1-11.

[28] M. Kutter and F. A. P. Petitcolas, (1999) "A fair benchmark for image watermarking systems", in Proc. of Electronic Imaging '99. Security and Watermarking of Multimedia Contents, The International Society for Optical Engineering, Vol. 3657, pp. 1-14.

Authors

Debiprasad Bandyopadhyay did his Bachelors in Computer Application from Burdwan University, Burdwan, India in 2007. Subsequently, he did his Masters in Computer Application in 2011 from West Bengal University of Technology, Kolkata, India. He served as an Assistant Teacher of Computer Science in Kendriya Vidyalaya Ballygunge, Kolkata, India. He is currently an M.Tech. scholar in the Dep artment of Computer Science and Engineering of Kalyani Government Engineering College, Kalyani, India.

Kousik Dasgupta did his Bachelors in Engineering in Electronics and Power Engineering from Nagpur University, Nagpur, India in 1993. Subsequently, he did his Masters in Computer Science & Engineering in 2007 from West Bengal University of Technology, Kolkata, India. He is currently Assistant Professor in the Department of Computer Science and Engineering of Kalyani Government Engineering College, Kalyani, India. He served industries like ABB and L & T during 1993-1996. He is a co-author of two books and about 20 research publications. His research interests include soft computing, computer vision and image processing and steganography. Mr. Dasgupta is a Life Member of ISTE, India, Associate Member of The Institute of Engineers, India and Chartered Engineer [India] of The Institute of Engineers, India. He is a Fellow of OSI, India

Jyotsna Kumar Mandal, M.Tech.(Computer Science, University of Calcutta), Ph.D.(Engg., Jadavpur University) in the field of Data Compression and Error Correction Techniques, Professor in Computer Science and Engineering, University of Kalyani, India. Life Member of CSI, CRSI, ACM, IEEE, Fellow member of IETE. Former Dean, Faculty of Engineering, Technology & Management, working in the field of Network Security, Steganography, Remote Sensing & GIS Application, Image Processing. 26 years of teaching and research experiences. Nine Scholars awarded Ph.D., one submitted and eight are pursuing. Total number of publications is more than three hundred in addition to publication of five books from LAP Lambert, Germany.

Paramartha Dutta did his Bachelors and Masters in Statistics from Indian Statistical Institute, Kolkata, India in 1988 and 1990, respectively. Subsequently, he did his Masters in Computer Science in 1993 from Indian Statistical Institute, Kolkata, India. He did his Ph.D. in 2005 from Bengal Engineering and Science University, Shibpore, India. He is currently a Professor in the Department of Computer and System Sciences of Visva Bharati University, Santiniketan, India since 2007. Earlier he served as a Professor in Kalyani Government Engineering College, Kalyani, India during 2001-2007. He was also an Assistant Professor and Head of the Department of Computer Science and Engineering of College of Engineering and Management, Kolaghat, India during 1998–2001. He has served as a Research Scholar in the Indian Statistical Institute, Kolkata, India and in Bengal Engineering and Science University, Shibpore, India. He is a co-author of eight books and about 150 research publications in various International Journals and National/International conference proceedings. His research interests include evolutionary computing, soft computing, pattern recognition and MANET. Prof. Dutta is associated to a number of professional bodies in the capacity of Fellow, Senior Member and Member.