Proc. of the Second Intl. Conf. on Advances in Computer and Information Technology -- ACIT 2013
Copyright © Institute of Research Engineers and Doctors. All rights reserved.
ISBN: 978-981-07-6261-2

A High Capacity Image Steganography Method Using Lorenz Chaotic Map

Rezza Moieni
Universiti Teknologi Malaysia
Malaysia

Subariah Ibrahim
Universiti Teknologi Malaysia
Malaysia

Leyla Roohi
Universiti Teknologi Malaysia
Malaysia

***Abstract*—This paper proposed a high payload image steganography method based on modulus parts of Kekre's Advanced Multiple LSB Algorithm (KAMLA) and Lorenz chaotic map. In the proposed method a 256 by 256 color image is embedded in a 512 by 512 cover image with acceptable imperceptibility. Experimental results showed that proposed algorithm sustains a higher confidentiality and still can provide high capacity as compared to KAMLA hiding algorithm.**

***Keywords*— image, steganography, chaos, Lorenz, payload, KAMLA**

I. INTRODUCTION

Nowadays, data is the most precious assets of the organizations and the value of each company is measured by the value of its information. Information technology, and particularly data security, has become a very hot topic in recent years. Having a meaningful information security is the key for a successful competitive company. Today one of the top concerns of companies purchasing technology products or implementation services is the integrity, confidentiality and availability of the data. To meet the main characteristics of security, there are many specific security mechanisms including ciphering, digital signatures, access controls, data integrity, authentication exchange, traffic padding, routing control, notarization, etc. Information hiding is among most important security mechanisms.

Limitation of secret image size threatens the secrecy of current image steganography techniques. The main aim of this paper is to overcome the security weakness of hiding image in image where the secret image or images are relatively large and to increase the confidentiality of KAMLA Least Significant Bit (LSB) based algorithm.

II. SR=TEGANOGRAPHY TECHNIQUES

The main goal of steganography is to communicate securely in a completely undetectable manner and to avoid drawing suspicion to the transmission of a hidden data [12]. If a steganography method causes someone to suspect the carrier medium, then the method has failed [13].

It is possible to combine the techniques by encrypting message using cryptography and then hiding the encrypted message using steganography. The resulting stego image can be transmitted without revealing that secret information is being exchanged. Furthermore, even if an attacker were to defeat the steganography technique and detect the message from the stego object, the attacker would still require the cryptographic decoding key to decipher the encrypted message [1].

A. Image Based Steganography Techniques

Numerous steganography techniques that embed hidden messages in multimedia objects have been proposed. There have been many techniques for hiding information or messages in images in such a manner that the modifications made to the image are perceptually indiscernible. Common approaches include [7]:

(i) Low bitrate algorithms
(ii) High bitrate algorithms

In low bitrate image hiding, relatively small amount of data is embedded in the host image specially to dictate some ownership information. In high bitrate image hiding, relatively larger amount of data is hidden in the host image. Digital watermarking is the main application of low bitrate information or image hiding techniques. In spite of large amount of hidden information, high bitrate information hiding techniques can be elaborately designed to cause unnoticeable visual degradation to the host image. In high bitrate image hiding, four metrics are considered:

(i) Transparency: The embedding of protected data should not interfere with the visual fidelity of host image [17]
(ii) Channel Capacity: How many bits can be effectively embedded within the host image [4]
(iii) The impact of embedded information on the performance of Image compression [3]
(iv) Robustness against lossy compression: how much hidden information can survive the lossy image codec [5]

High bitrate image hiding algorithms can be categorized as spatial domain and frequency domain algorithms. Transform techniques embed the message by modulating coefficients in a transform domain, such as the Discrete Cosine Transform (DCT) used in JPEG compression.

Two main methods are developed in spatial domain. The most commonly used spatial domain algorithm in high bitrate algorithms is Least Significant Bit (LSB) algorithm. [15] proposed a methodology where data is embedded in each pixel of a cover image by changing its grey value without exceeding a threshold value. This method can be applied to color images as well. LSB insertion is a simple approach to embed

SEEK DIGITAL LIBRARY

Proc. of the Second Intl. Conf. on Advances in Computer and Information Technology -- ACIT 2013
Copyright © Institute of Research Engineers and Doctors. All rights reserved.
ISBN: 978-981-07-6261-2

information in an image file. This simple steganography technique embeds the bits of the message directly into the least significant bit plane of the cover-image. There are various LSB based methods for image steganography, which are shown in Figure 1.

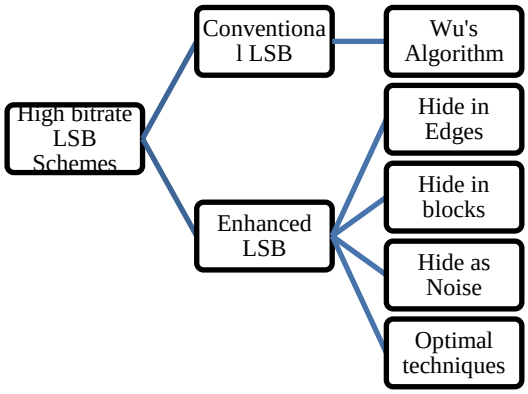

Figure 1. Categorizing LSB methods

[15] proposed an algorithm where data can be hidden in each pixel of the cover image by changing its grey value without exceeding a threshold value. Pseudo-random mechanisms may be used to enhance the level of security. It has been found from the experiments that the signal to noise ratio (SNR) of the stego image is larger than those observed in compressed images. This can prove that the visual distortion caused by the data embedded is less than that caused by compression of the image.

[1] proposed an image in image algorithm based on block difference to hide a secret-image into a cover-image such that an unintended observer will not aware of the hidden secret-image.

[17] proposed an adaptive algorithm based on human vision sensitivity (HVS) to hide a large amount of secret bits into a still image with a high imperceptibility. The more data can be hiding in more local variation areas. In this method, data to be embedded are converted into a series of symbols in a notation system with multiple bases. The specific bases used are determined by the degree of local variation of the pixel magnitudes in the host image so that pixels in busy areas can potentially carry more hidden data. Reference [17] proved that MBNS has better performance than PVD.

[3] proposed a scheme based on the search order coding (SOC) compression method of vector quantization (VQ) indices. Their goal is to embed secret data into the compression codes of the host image in a way that the eavesdropper will not be able to see the existence of the secret data. In this algorithm, the embedding process induces no extra coding distortion and adjusts the bitrate according to the size of the secret data.

[14] proposed a LSB embedding algorithm for hiding an encrypted message in non-adjacent and random pixel locations in edges of images. It first encrypts the hidden plain text using 3-DES and then employs a Laplacian detector on every 3 by 3 non-overlapping block within the cover to detect the edges in the cover image using Robert's edge detection algorithm. Then it performs data hiding on center pixels whose blocks are located at the sharper areas like edges, corners, thin straight lines and end of lines according to a threshold. Message bits are embedded in the LSB and random locations of the edge pixels.

[10] proposed an enhanced LSB scheme which is simple in implementation but still achieved a high level of embedding capacity and imperceptibility. Kekre's Advanced Multiple LSB Algorithm (KAMLA) is a Multiple LSB replacement technique; a spatial domain method. In this method up to four LSB'S of an image byte can be changed. The proposed method also can be applied to 24 bit color images and achieve embedding capacity much highest than PVD [7]. Before embedding the data 8 bit secret key is used and will be XOR with all the bytes of the message to be embedded. Message is recovered by XOR operation by the same key. Every pixel value in this image is analyzed and the following checking process is employed. Similarly, secret data can be retrieved from the gray values of the stego image by again checking the first four MSB's of the pixel value and retrieve the embedded data. The maximum MSE for this method is under 4%.[10].

B. Chaos

The security of steganography relies on secrecy of the hiding scheme. It is possible to combine the techniques by encrypting message and then hiding the encrypted message using steganography. Steganography and cryptography make great partners and it is common practice to use cryptography with steganography. If an attacker defeats the steganography technique and detected the message from the stego object, he would still require the cryptographic decoding key to decipher the encrypted message. There are various encryption algorithms. Chaotic signals are one of best choices for combination of encryption and steganography due to the following properties [16]:

(i) Similarity to the white noise
(ii) Complex structure
(iii) Difficult to analyze
(iv) Sensitive to initial conditions

These properties have made chaos algorithms attractive for security applications. Chaotic signals are dynamical, pseudorandom and irreversible signals that are generated by deterministic nonlinear equations. These equations process good characteristics of randomness sequences. Chaotic systems are highly sensitive to initial parameters and if different initial values are implied then the system will run in different orbits that are difficult to be calculated or analyzed. The stream in the output is much like the white noise that has randomness parameters and enough complexity.

C. Choosing Chaos Mapping

There are several types of chaotic maps and to design a chaos based algorithm and system, the first step is to choose a mapping between various types of chaos based mapping. Large cycle length and the uniformity distribution are two important properties that are important while choosing a mapping. Any different architecture and usage can use

SEEK DIGITAL LIBRARY

Proc. of the Second Intl. Conf. on Advances in Computer and Information Technology -- ACIT 2013
Copyright © Institute of Research Engineers and Doctors. All rights reserved.
ISBN: 978-981-07-6261-2

different mapping. Chaos based algorithms can be categorized as below:

(i) One dimensional (1-D)
(ii) Two dimensional (2-D)
(iii)Three dimensional (3-D)

Three-dimensional mapping is more complicated in comparison with others, but one iteration operation of three dimensional maps can develop three arbitrary streams in this category. Here are some types of three dimensional chaos based mappings:

(i) Lorenz Map
(ii) Lü and Chen Maps
(iii) 3-D baker map

D. Lorenz

Lorenz map are utilized in many new algorithms that proposed in recent years. Because of three random number sequences that are generated by Lorenz map, many forms of combination form can be proposed. Moreover, Lorenz map is suitable for color images which have been mentioned above. [9] proposed an algorithm for color image encryption with Lorenz map. In this algorithm each random number sequence is used for permutation of red, green and blue matrixes. In next step the permuted matrices are substituted by using random number sequences and XOR function. One iteration operation of Lorenz system can procedure three stochastic variables that makes it ideal for RGB images. Lorenz chaos system is more complex than one dimension ones, the chaotic sequence is more unpredictable, so it is strong against adaptive argument synchronization attack. While one dimension chaos system is weak against this kind of attack. Three initial parameters can becombined together as one encryption key, so the key space is 1048 ≈ 2158, which is larger than the acknowledged most security AES algorithm. While for one dimension system, the key space is only 1016 ≈ 253, which is smaller than the obsolete DES standard.

III. THE PROPOSED METHOD

The proposed algorithm in this paper contains three main components: encryption, compression and image hiding. In the proposed algorithm, the Lorenz 3-D Chaotic map is used for enhancing confidentiality of KAMLA high payload image steganography algorithm. For image encryption, chaotic maps have better security characteristics than AES [9]. The steps of the proposed algorithm are as follows which is shown in Figure 2:

(i) Encrypting the secret image in order to increase the confidentiality
(ii) Hiding the encrypted, compressed secret image into cover image using KAMLA algorithm

KAMLA algorithm does not use any encryption and since the encryption and decryption key is public, attackers can easily extract the secret data. The first step is for enhancing confidentiality of the algorithm and the second step will hide the encrypted, secret message inside the cover image.

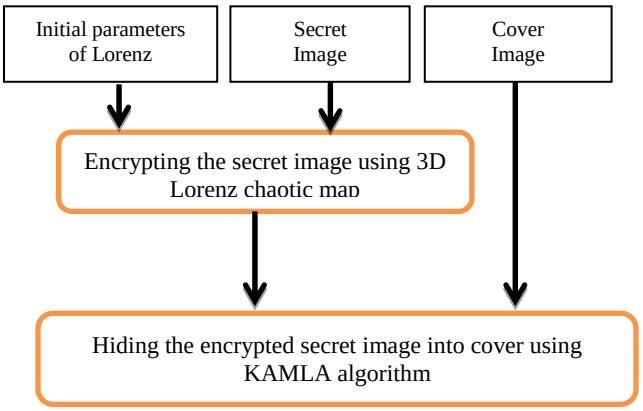

Figure 2. Proposed Method)

A. Lorenz Encryption Steps

Lorenz (1963) proposed his famous equation, which is defined as follows:

$$dx/dt = \sigma (y-x) \quad (1)$$
$$dy/dt = \gamma x - xz - y \quad (2)$$
$$dz/dt = xy - \beta z \quad (3)$$

In which t, x, y, z, σ, r, b ∈R and σ, r, b are positive constants. If σ = 10 and b = 8/3, when r > 24.74, the dynamical orbit will be chaotic [8]. Lorenz equation requires three constants (control parameters) which are σ, γ and β. These parameters can combine together as one key which increases the key space greatly [8]. In the proposed algorithm, the encryption process is done in the following steps which are shown in Figure 3:

(i) Key Initialization
(ii) Scrambling the secret image
(iii) Permutation of colors

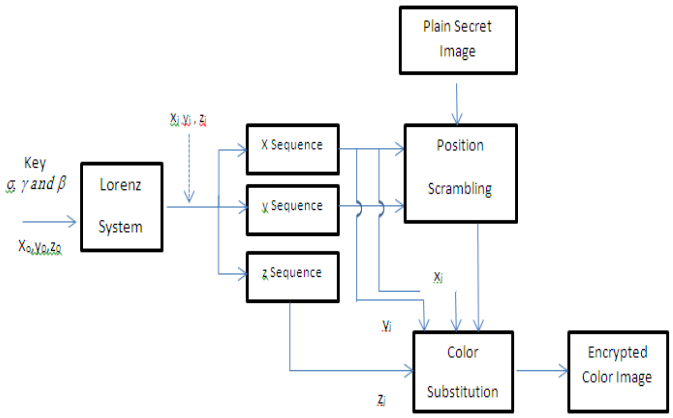

Figure 3. Encryption Process

SEEK DIGITAL LIBRARY

Proc. of the Second Intl. Conf. on Advances in Computer and Information Technology -- ACIT 2013
Copyright © Institute of Research Engineers and Doctors. All rights reserved.
ISBN: 978-981-07-6261-2

B. *Image Hiding Scheme*

Finally the encrypted secret image is embedded into cover image using KAMLA pattern. The Kekre's Advanced Multiple LSB Algorithm (KAMLA) [11], uses the pallet of 256 color, 8 bit depth and weakness of human eye to hide the secret message into cover image. According to four most significant bits of cover image and Table 1, variable bits of secret message named BRC (Bit replacement count) are hidden.

TABLE I. KAMLA BIT REPLACEMENT PATTERN [11]

4MSB	Max BRC	LSB bits changed
0000	1	XXXC
0001	1	XXXC
0010	2	XXCC
0011	2	XXCC
0100	2	XXCC
0101	2	XXCC
0110	3	XCCC
0111	1	XXXC
1000	2	XXCC
1001	2	XXCC
1010	3	XCCC
1011	2	XXCC
1100	3	XCCC
1101	3	XCCC
1110	4	CCCC
1111	4	CCCC

The process is described as followings:

(i) Read bits of encrypted secret image and reorder it in a sequence.
(ii) Use four most significant bits (MSBs) of cover image to hide bits of secret image into maximum of four least significant bits of the cover image. This is done using KAMLA algorithm. In KAMLA algorithm up to four LSB'S of an image byte can be changed. BRC (Bit replacement count) is determined as Table 1.

In TABLE I, Cs are changed bits and Xs are unchanged bits. According to Table 1 up to 4 bits can be embedded in each pixel of cover image. Now the embedding process is done.

IV. EXPERIMENTAL RESULTS

In the proposed algorithm, Lena (USC-SIPI Image Database) is used as cover image and Baboon (USC-SIPI Image Database)as secret image. The secret image has been used is 256 by 256. TABLE II shows the basic statistics of test images. Three image metrics entropy, histogram and PSNR are measured for evaluating the proposed algorithm

TABLE II. EXPERIMENTAL BASICS

	Resolution	File format	Size (KB)
Cover image (Lena)	512 * 512	TIFF- Uncompressed Color	768
Secret Image (Baboon)	256 * 256	TIFF- Uncompressed Color	220

A. *Histogram*

Comparison of histograms of stego image when using or not using Lorenz with histogram of cover image will illustrate the changes in cover image and whether or not there are any changes in colors.Figure 3 shows three histograms of cover image, stego image without using encryption and stego image with using encryption. Figure 3 demonstrates that the proposed algorithm has less effect on histogram and make it more robust against histogram attack

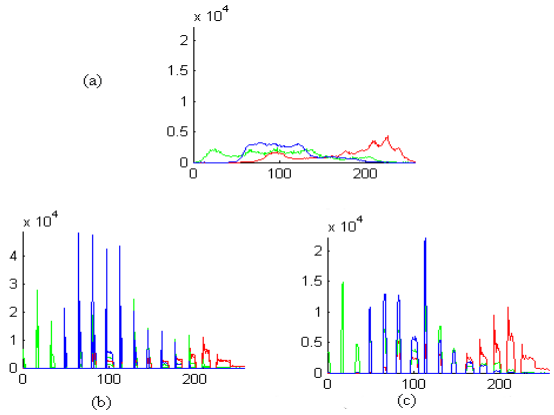

Figure 4. Histogram comparison of proposed method

B. *PSNR*

PSNR is among the important metrics for image steganography. Greater PSNR means less modification and changes of stego image in comparison with cover image. It has to be noted that measuring PSNR without other metrics does not guaranty security improvement of the algorithm. According to results for PSNR as shown in TABLE III, it can be seen that the PSNR has been improved for proposed method from 29.23 to 30. Improving PSNR is a result of encryption step. Lossy compression will also lead to even higher PSNR but according to encryption step, only lossless compression can be used that has a smaller redundancy rate.

SEEK DIGITAL LIBRARY

Copyright © Institute of Research Engineers and Doctors. All rights reserved.
ISBN: 978-981-07-6261-2

TABLE III. PSNR RESULTS OF PROPOSED ALGORITHM

	PSNR for Secret Image
KAMLA Algorithm	29.23
KAMLA with Lorenz	30

C. Entropy

Entropy is another metric for evaluating imperceptibility of secret image which is hidden into cover image. Entropy of cover image is examined before and after embedding process. The results are shown in Table 4. This metric has been measured for embedding the plain secret image as well as embedding encrypted secret image. Results show that value of entropy has least change in the case encryption is used. The entropy measurements are done for each color of test images and are shown in Table 4.

TABLE IV shows that using encryption has less effect on entropy of cover image. Table 3 shows that entropy of red color for cover image, which is 7.2501 becomes 6.2001 when inserting the plain secret image but it has been improved to 6.2310 while using Lorenz encryption which is the closest value to the original entropy of 7.25 which belongs to the cover image. Measuring this metric for green and blue values also show similar results as well

TABLE IV. ENTROPY MEASUREMENT OF PROPOSED ALGORITHM

	Entropy		
	Red	Green	Blue
Cover Image	7.2501	7.5940	6.9684
Stego Image - KAMLA	6.2001	4.2431	3.9144
Stego Image –KAMLA with encrotion	6.2310	5.4696	4.6801

V. CONCLUSION

We have proposed a high capacity image steganography method based on KAMLA and Lorenz chaotic map. In this method, secret image is encrypted using Lorenz chaotic map before inserting into least significant bits of cover image using KAMLA algorithm. Our experimental results have shown that the proposedmethods provided a better way to hide secret data comparedwith other methods without making noticeable distortions.

ACKNOWLEDGMENT

This work was supported by Universiti Teknologi Malaysia (UTM), Johor, Malaysia under the VOT: Q.J13000.7128.00J29.

REFERENCES

[1] C. Cachin, “An Information-Theoretic Model for Steganography”, in proceeding 2nd Information Hiding Workshop, vol. 1525, pp.306-318, 1998.

[2] Chan, C.-kwong, Cheng, L. M., Leung, K.-chi, Li, S.-ling, Technology, I., & Kong, H. (2004). Image Hiding Based on Block Difference, (December), 968-972.

[3] Chang, C. -., Chen, G. -., & Lin, M. -. (2004). Information hiding based on search-order coding for VQ indices. Pattern Recognition Letters, 25(11), 1253-1261.

[4] Cvejic,N. &Seppanen,T. (2004). Channel capacity of high bit rate audio data hiding algorithms in diverse transform domains. In Proceedings of the international symposium on communications and information technologies (ISCIT 2004)

[5] Gunsel, B., Uludag, U., &Tekalp, A.M (2002). Robust watermarking of fingerprint images. Journal of pattern recognition, 35(12), 2739-2747

[6] Hmood, A. K., Kasirun, Z. M., Jalab, H. A., Alam, G. M., Zaidan, A. A., & Zaidan, B. B. (2010). On the accuracy of hiding information metrics : Counterfeit protection for education and important certificates, 5(7), 1054–1062.

[7] Hamid.R. Nemati and Li Yang, Applied Cryptography for Cyber Security and Defense.. New York: Hershly, 244~254, 2011.

[8] Jiang, H.-yan, & Fu, C. (2008).An Image Encryption Scheme Based on Lorenz Chaos System.2008 Fourth International Conference on Natural Computation, 600-604. Ieee.

[9] Jiang, H.-yan, & Fu, C. (2008).An Image Encryption Scheme Based on Lorenz Chaos System.2008 Fourth International Conference on Natural Computation, 600-604. Ieee.

[10] Kekre, H. B., Athawale, A., Halarnkar, P. N., & Stage, A. E. (2008). Increased Capacity of Information Hiding in LSB ’ s Method for Text and Image, 246–249.

[11] Kekre, H. B., & Athawale, A. A. (2011). Increased Cover Capacity using Advanced Multiple LSB Algorithms, (Icwet), 25–31.

[12] N.F.Johnson & S.Jajodia, “Steganalysis of Images Created Using Current Steganography Software”, in Proceeding for the Second Information Hiding Workshop, Portland Oregon, USA, April 1998, pp. 273-289.

[13] N. Provos, P. Honeyman, “Detecting Steganography Content on the Internet”.CITI Technical Report 01-11, 2001.

[14] Singh,K. M., Singh, S .B., &Singh, S. S (2007). Hiding encrypted message in the features of images. International journal of computer science and network security (IJCSNS), 7(4)

[15] Wu, D. C., & Tsai, W. H. (2000). Spatial-domain image hiding using image differencing.IEE Proceedings - Vision, Image, and Signal Processing, 147(1), 29.

[16] Yu, L., Zhao, Y., Ni, R., & Li, T. (2010).Improved Adaptive LSB Steganography Based on Chaos and Genetic Algorithm.EURASIP Journal on Advances in Signal Processing, 2010(1).

[17] Zhang, W., Cheung, S., & Chen, M. (2005). Hiding privacy information in video surveillance system. In proceedings of the international conference on image proceeding (ICIP’2005), 3, II-868-71

SEEK DIGITAL LIBRARY