Chaotic Modeling and Simulation (CMSIM) 8: 343-353, 2017

Applications of Chaotic Systems in Steganography Algorithms

Turker Tuncer

Department of Digital Forensics Engineering, Technology Faculty, Firat University, Elazig / Turkey
(E-mail turkertuncer@firat.edu.tr)

Abstract. Chaotic systems are used in many information security applications due to their rich features. One of these application areas is steganography. In this study, a new CRT based chaotic steganography application is proposed and chaotic steganography algorithms have been examined.
Keywords: Chaos, steganography, computer science application.

1 Introduction

Nowadays, mobile devices with internet connection, social media platforms and internet of things are frequently used in daily life. Thus, a number of data have been storage and shared in digital platforms. With digitalization of information and ease to access information, providing information security necessarily. In recent years, information security is becoming one of the hot-topic research area [1-10].

Chaos is one of the most studied research topics in the nonlinear dynamics. In steganographic application, chaotic dynamics have been utilized to provide confidentiality. The examined chaotic steganographic applications which presented in the literature are given as follow. Valandar et al. proposed a chaotic image steganography method. The authors used modified logistic map in this method and they used color images for data embedding. In this method, seed values of the used chaotic map are calculated by using integer wavelet coefficients of the Cover image and keys are generated by using these seed values. The Stego key which is generated by using modified logistic map was used for pixel selection [11]. Roy et al. proposed edge adaptive image steganography method based on chaos. They used Arnold cat map to scramble Secret data and LSB to embed Secret data. The edge detection methods were used to extract ROI and RONI [12]. Xiang et al. presented steganographic image encryption method to provide cloud security. In their method, they used chaotic image encryption and 2LSBs data embedding function. In their paper, a multi-level security application was proposed [13]. Ghebleh and Kanso suggested a robust chaotic algorithm for image steganography. In their paper,

Received: 29 May 2017 / Accepted: 10 July 2017

ISSN 2241-0503

they presented a 3D chaotic cat map. To embed data, they used lifting wavelet transform. The lifting wavelet transform provides integer-to-integer transform. Chaotic map used as a PRNG (pseudo random number generator) and they applied XOR operation on secret message and random numbers, then they embedded encrypted secret data into host color image. To evaluate their method, PSNR (Peak Signal-to-Noise Ratio) and SSIM (Structural Similarity) were used and they reached 2.25 bpp (bit per pixel) data embedding capacity in their method [14]. Shivani et al. suggested a text steganography method which used logistic map. In their method, they converted binary format to text messages and they used logistic map as PRNG to determine embedding location of the text [15]. Keyvanpour and Merrikh-Bayat presented an image watermarking method based on chaotic fractal coding. They used Arnold Cat map. To embed watermark, they used fractal image coding [16]. Kanso and Own proposed chaotic map based steganographic algorithm. They used spatial domain and single chaotic map. The used chaotic map determined embedding pixel position in their method. RGB (Red Green Blue) images were used in this method. So they used Arnold cat map to generate stego-key. To evaluate their method, they used statically tests [17].

In this article, a new chaotic image application is presented. The data embedding method is a block based method and it used CRT (Chinese remainder theorem) for data embedding and extraction. A modified logistic map is used as stego key in this paper. To provide confidentiality of the stego key, seed values of the logistic map are updated periodically. The stego key is used to select hidden pixel in block based method.

The rest of this article is given as follows. CRT is presented in Chapter 2, chaotic image steganography application is proposed in Chapter 3, experimental results are demonstrated in Chapter 4, discussions are presented in Chapter 5 and conclusions and recommendations are given in chapter 6.

2 Chinese Remainder Theorem

Chinese remainder theorem (CRT) is a method which is applied to integer number by using modulo function. In this theorem, M set that is $M = \{M_1, M_2, \ldots, M_n\}$ is used. M values must be relatively prime in order to use CRT. CRT obtains more than one values using a number. The equation of CRT is given in Eq. 1.

$$Z = R_i \ (mod \ M_i) \tag{1}$$

Inverse CRT is explained in Eq. 2.

$$Z = \sum_{i=1}^{n} R_i \frac{M}{M_i} K_i \ (mod\ M)$$
$$M = M_1 M_2 \dots M_n \quad (2)$$
$$K_i \frac{M}{M_i} = 1 \ (mod\ M_i)$$

In Eq. 8, M is multiplication of relatively primes, K is inverse value according to M [18-21].

3 The Chaotic Image Steganography Application

Chaos is the most famous study in nonlinear dynamics and the random number generators, S-Box generation, machine learning, geometry, electronic motor control, meta heuristic optimization, information security, etc are used chaotic dynamics. In this study, a chaos based steganography application is proposed. The proposed application is called as chaotic CRT (Chinese Remainder Theorem) steganography application (CCRTSA). Firstly, random numbers are generated by using a logistic map. In this article, seed values of the logistic map are updated periodically to provide confidentiality. Equations of the proposed chaotic map are given below [22].

$$x_i = hx_{i-1}(1 - x_{i-1}), x_0 = (0,1)\ and\ x_0 \neq \{0.25,0.5,0.75\}, h = [3.57,4] \quad (3)$$
$$if\ i\ (mod\ T) = 0, h = h + 10^{-10} \quad (4)$$

x is an array which includes randomly generated numbers, h is chaos multiplier, i is index and T is period. In this article T is 32. This chaotic map is used as PRNG (Pseudo Random Number Generator) in this article.

The second section of this application, CRT based steganography method is used. The block diagram of the data hiding of the CCRTSA is shown in Fig. 1.

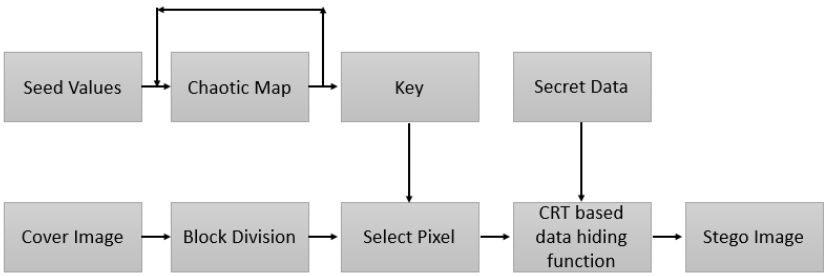

Fig. 1. Embedding diagram of the CCRTSA.

The data hiding steps of CCRTSA are given below.

Step 1: Generate random numbers by using seed values of the proposed chaotic map.

Step 2: Select two relatively prime numbers which are N_1 and N_2.

$$N_1 = \{2,3,4,\dots,255\} \ \ and \ N_2 = \{2,3,4,\dots,255\} \tag{5}$$

Step 3: Divide cover image into b x b size of non-overlapping blocks.

Step 4: Select embedding pixel by using the presented chaotic map which is P.

Step 5: Calculate T1 and T2 values by using CRT.

$$T_1 = P \ (mod \ N_1) \tag{6}$$

$$T_2 = P \ (mod \ N_2) \tag{7}$$

Step 6: If secret data is 1 and $T_1 < T_2$,apply first pixel modification algorithm.

Pseudo code for this algorithm is shown in Algorithm 1.

Algorithm 1: The pseudo code used to embed 1.
1: d=N_2-T_2
2: **if** P+d≥256 **then**
3: P=P+d- N_2;
4: **else**
5: P=P+d;
6: **endif**

Step 7: If secret data is 0 and $T_1 \geq T_2$,apply second pixel modification algorithm. Pseudo code for this algorithm is shown in Algorithm 2.

Algorithm 2: The pseudo code used to embed 0.
1: $d=N_1-T_1$
2: **if** $P+d \geq 256$ **then**
3: $P=P+d-N_1$;
4: **else**
5: $P=P+d$;
6: **endif**

Step 8: Repeat steps 4-7 until reaching to the size of secret data.

In data extraction phase, firstly, seed values of the proposed chaotic system, size of blocks which is b, N1 and N2 are sent to receiver side. The receiver side generates key by using seed values. The extraction diagram of the CCRTSA is shown in Fig. 2.

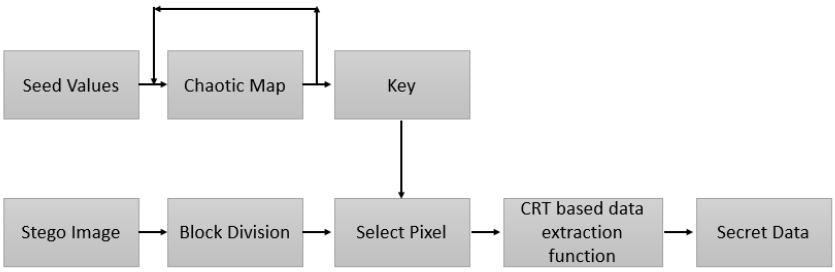

Fig. 2. The extraction diagram of the CCRTSA.

The data extraction steps of the proposed CCRTSA are given below.

Step 1: Generate random numbers by using seed values.

Step 2: Divide stego image into b x b size of blocks.

Step 3: Select P which is stego pixel by using random number which is used as key.

Step 4: Calculate T1 and T2 by using CRT.

Step 5: Extract secret data by using Eq. 8.

$$SD_{i,j} = \begin{cases} T_1 < T_2, 0 \\ T_1 \geq T_2, 1 \end{cases}, i = \left\{1,2,3,\ldots,\frac{W}{b}\right\}, j = \left\{1,2,3,\ldots,\frac{H}{b}\right\} \quad (8)$$

SD is secret data, b x b is size of used blocks, W is width of the stego image, H is height of the stego image, i and j are indices of the secret data.

Step 6: Repeat steps 3-5 until reaching to the size of the secret data.

4 Experimental Results

In this chapter, experiments are obtained by using test images. The used test images are shown in Fig. 3.

Fig. 3. The general test images [23].

Capacity, visual quality and key depended security are discussed in this chapter.

Capacity: The proposed steganography application is a block based application. In this application, one bit is embedded into a block. The used blocks are non-overlapping blocks. Thus, the general capacity equation can be defined. The general equation of the capacity is given below.

$$Capacity = \left\lfloor \frac{W}{m} \right\rfloor \left\lfloor \frac{H}{n} \right\rfloor layer \tag{9}$$

Capacity is expressed as bits and layer defines number of layers in the stego image. If users use color image, layer is 3. In case of grayscale image, layer is 1.

Visual Quality: MSE (Mean Square Error) and PSNR (Peak Signal Noise-to-Ratio) measurements are used for visual quality. Equations of MSE and PSNR are given in Eq. 10 and 11.

$$MSE = \frac{1}{WH} \sum_{i=1}^{W} \sum_{j=1}^{H} (OI_{i,j} - WI_{i,j})^2 \tag{10}$$

$$PSNR = 10 log_{10} \left(\frac{255^2}{MSE} \right) \tag{11}$$

The obtained PSNR values of CCRTSA according to block size are shown in Fig. 4.

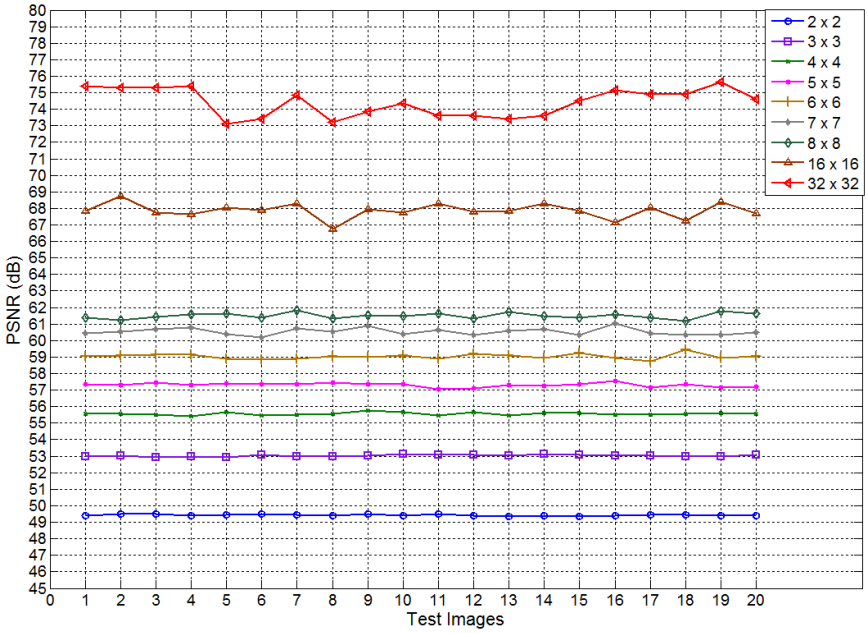

Fig. 4. The PSNR values of CCRTSA.

In Fig. 4. we used 4 for the N_1 and 5 for the N_2.

Security: In this article, logistic map is used as PRNG and seed values of the logistic map are updated periodically to provide key security. Key size of the CCRTSA is defined in below.

$$KeySize = \left\lfloor \frac{W}{m} \right\rfloor \left\lfloor \frac{H}{n} \right\rfloor \lceil \log_2(mn) \rceil \tag{12}$$

512 x 512 size of grayscale images are used in this chapter. The obtained key sizes are shown in Table 2. according to variable size of blocks.

Table 1. Key size of the CCRTSA according to block size.

Image size	2 x 2	4 x 4	8 x 8	16 x 16	32 x 32
256 x 256	32,768	16,384	6144	2048	640
512 x 512	131,072	65,536	24,576	8192	2560
256 x 256 x 3	98,340	49,152	18,432	6144	1920
512 x 512 x 3	393,360	196,608	73,728	24,576	7680

The reason for why the proposed CCRTSA should has sufficient size of the keys is to provide confidentiality.

5 Discussions

In this section, the previously proposed methods related to chaos are discussed. In Ref. [11], authors used classical steganographic methods. They presented modified logistic map as a technical innovation. In Ref. [11], they presented a 3D logistic map using 3 parameters. Firstly, 8 x 8 sized blocks were used for block division. To obtain integer wavelet coefficients LWT was applied on the host image. Then, they used 3D which is modified for generating chaotic pixels. LSB (least significant bit) insertion which is like a data hiding method is used for data embedding. Briefly, this method is a classical steganography application. They only used a new chaotic map but they didn't point out advantages of the modified 3D logistic map. The Ref. [11] showed that, the 3D logistic map has not any advantages in this article. This map was not increased visual quality and payload capacity. This map only effected confidentiality of the Ref. [11]. They evaluated Ref. [11] as an image encryption method.

In Ref. [12], they used only LSB and Arnold Cat map. Arnold cat map is a well chaotic map but we know that Arnold cat map can be crack easily. In Ref. [13] experimental results are not enough for a stenographic application.

In Ref. [13], authors presented a multi-level security application. They used steganography and chaotic image encryption together and they created a multi-level security framework to provide cloud security. They used 3LSBs for data hiding. The 2LSBs of the pixel carried data and 3rd LSB was a flag bit. In this aspect, Ref. [13] has a fragile structure. If stego-image was attacked on the cloud. Users cannot reach their data. To encrypt this images, a chaotic image encryption method was used in Ref. [13]. Their encryption method consisted of permutation and XOR masking. Characteristics of the Ref. [13] same as the 2LSBs. Their experiments are not enough to evaluate steganography.

In Ref. [14], authors used LWT (Lifting Wavelet Transform) to obtain integer wavelet coefficients and they used 3D chaotic cat map. The presented chaotic cat map is used as stego key. They embedded secret data into color cover image but they calculated the payload capacity incorrectly, because they used 2m x 2n x 3 size of images as host image and they embedded 9(m-2)(n-2) size of secret data into these host images. For example, m=256 and n=256, the payload capacity is obtained by the equation of $\frac{9(m-2)(n-2)}{2m\ x\ 2n\ x\ 3} = 0.7383 \cong \frac{9}{12} = 0.75$, but in this paper, authors obtained approximately 2.25 bpp (bit per pixel) as payload capacity.

In Ref. [15], authors presented a chaos based text steganography algorithm. The authors generated random numbers by using logistic map and they used these random numbers as stego key. In Ref. [15], h is said to be in range of 3.54-4 but true range of the h should be 3.57-4. Also, the experiments of the Ref. [15] are insufficient.

In Ref. [16], authors gave information about only Arnold cat map and fractal coding, this paper is not well organized and experiments are insufficient.

In Ref. [17], authors used spatial domain for data embedding and they used 2D chaotic cat map to provide confidentiality. 2D chaotic map was used to generate

stego key. In the experimental results, they presented statically tests, but we know that, if we use any random number generator in steganographic application, statistically well results will be obtained.
In CCRTSA, logistic map is used to generate stego key and this key is used to select embedding pixel. In this paper, payload capacity, key length and perceptual quality are expressed mathematically. In steganographic application, Patra et al.'s [18] method is improved. To provide confidentiality, CRT and logistic map are used together. Also, seed values of the logistic map are updated periodically. In CCRTSA, the visual quality, N_1 and N_2 have inverse ratio. CCRTSA is proposed as a new secure chaotic steganography application in this paper.

Conclusions and Recommendations

In this article, a new chaotic image steganography application is proposed. Logistic map is used in this paper and logistic multiplier is updated periodically to provide security. This map is used as PRNG. The CRT based data hiding and data extraction function are used in this method. The used CRT based algorithm is proposed by Patra et al. in Ref. [18]. In this study, data hiding codes of the CRT based method are optimized and the complexity of the CRT based data hiding algorithm is reduced from $O(n^3)$ to $O(n^2)$. The optimized codes are shown in Algorithm 1 and Algorithm 2. The capacity of the presented application is proved mathematically and this application has high payload capacity. The visual quality results of the proposed CCRTSA are obtained with variable size of blocks. These experiments demonstrated that CCRTSA has high visual quality. Also, a few chaos based steganography applications are examined and their weaknesses have been listed in this paper.
In future studies, the presented CCRTSA will be used in real applications.

References

1. Y. Xiang, S. Guo, W. Zhou, S. Nahavandi,, Patchwork-based audio watermarking method robust to de-synchronization attacks, IEEE/ACM Trans. Audio Speech Lang. Process. 22 (9) (2014) 1413–1423.
2. A. Akter, N. E-Tajnina, M. A. Ullah, Digital image watermarking based on DWT-DCT: evaluate for a new embedding algorithm, in: Third Int. Conf. On Informatics, Electronics & Vision, May 2014, Dhaka,Bangladesh, 2014, pp. 1–6.
3. Q. Su, Y. Niu, Q. Wang, G. Sheng, A blind color image watermarking based on DC component in thespatial domain, Optik 124 (23) (2013) 6255–6260.
4. C.Y. Lin, S.F. Chang, A robust image authentication method distinguish JPEG compression from malicious manipulation, IEE Trans. Circuits Syst. Video Technol. 11 (2), (2001),153-168.
5. X. Qi, X. Xin, A quantization-based semi-fragile watermarking scheme for image content authentication, J. Vis. Commun. Image Represent. 22 (2) (2011), 187-200.

6. Y.-C. Hu, C.-C. Lo, W.-L. Chen, Probability-based reversible image authentication scheme for image demosaicking, Future Generation Computer Systems 62 (2016), 92-103.
7. T. Tuncer, E. Avci, Block based fragile watermarking algorithm for image authentication and tamper detection, 9th International Conference On Information Securıty and Cryptology, pp. 5-10, 2016, Ankara/Turkey.
8. L. Yuan, Q. Ran, T. Zhao, Image authentication based on double-image encryption and partial phase decryption in nonseparable fractional Fourier domain, Optics & Laser Technology 88 (2017) 111–120.
9. X. Li, X. Meng, Y. Yin, X. Yang, Y. Wang, X. Peng, W. He, X. Pan, G. Dong, H. Chen, Hierarchical multilevel authentication system for multiple-image based on phase retrieval and basic vector operations, Optics and Lasers in Engineering 89 (2017) 59–71.
10. T.-S. Nguyen, C.-C. Chang, X.-Q. Yang, A reversible image authentication scheme based on fragile watermarking in discrete wavelet transform domain, Int. J. Electron. Commun. (AEÜ) 70 (2016) 1055–1061.
11. M. Y. Valandar, P. Ayubi, M. J. Barani, A new transform domain steganography based on modified logistic chaotic map for color images, Journal of Information Security and Applications, (2017), 1-10.
12. R. Roy, A. Sarkar, S. Changder, Chaos based Edge Adaptive Image Steganography, Procedia Technology 10, (2013), 138 – 146.
13. T. Xiang, J. Hu, J. Sun, Outsourcing chaotic selective image encryption to the cloud with steganography, Digital Signal Processing, 43, (2015), 28-37.
14. M. Ghebleh, A. Kanso, A robust chaotic algorithm for digital image steganography, Commun. Nonlinear Sci. Numer. Simulat.,19, (2014), 1898-1907.
15. Shivani, V. K. Yadav, S. Batham, A Novel Approach of Bulk Data Hiding using Text Steganography, Procedia Computer Science 57, (2015), 1401 – 1410.
16. M. Keyvanpour, F. Merrikh-Bayat, An Effective chaos-based image watermarking scheme using fractal coding, Procedia Computer Science, 3, (2011), 89–95.
17. A. Kanso, H. S. Own, Steganographic algorithm based on a chaotic map, Commun. Nonlinear Sci. Numer. Simulat.,19, (2012), 3287-3302.
18. J. C. Patra, A. Karthik, C. Bornand, A novel CRT-based watermarking technique for authentication of multimedia contents, Digital Signal Processing, 20, (2010), 442–453.
19. J. C. Patra, J. E. Phua, C. Bornand, A novel DCT domain CRT-based watermarking scheme for image authentication surviving JPEG compression, Digital Signal Processing, 20, (2010), 1597–1611.
20. B. Schneier, Applied Cryptography, 2nd ed., John Wiley & Sons, New York, 1996.
21. J. Huang, Y.Q. Shi, Y. Shi, Embedding image watermarks in DC components, IEEE Trans. Circuits Systems Video Technol. 10 (6), (Sep. 2000), 974–979.
22. Y.-Q. Zhang, X.-Y. Wang, L.-Y. Liu, Y. He, J. Liu, Spatiotemporal chaos of fractional order logistic equation in nonlinear coupled lattices, Commun Nonlinear Sci Numer Simulat, 52, (2017), 52–61.
23. C. Qin, X. Chen, D. Ye, J. Wang, X. Sun, A novel image hashing scheme with perceptual robustness using block truncation coding, Information Sciences, 361–362, (2016), 84–99