Constructing Chaotic Cipher Using Image Descriptors: A Secure Steganography System

Arezoo Abdollahi
Department of computer science
University of Manitoba
Email: abdollaa@myumanitoba.ca

Noman Mohammed
Department of Computer Science
University of Manitoba
Email: noman@cs.umanitoba.ca

***Abstract*—As the exchange of data over the open networks and the Internet is rapidly growing, security of the data becomes a major concern. Our primary goal in this paper is to give new insights on how to hide the fact of communication while the content of the communication is obfuscated. To reach this aim, steganography and cryptography are fused. Therefore, Cellular Neural Networks (CNN) will be used to create a chaotic system of 5-D CNN as the key source and encrypt image based on Logistic chaotic sequence. Then, the crypto message will embed in the cover image using transformation-based steganography in which the image is mapped to the frequency domain and then integrate into suitable transform coefficients. In addition, image quality metrics are used for evaluation of stego images.**

***Keywords*—Cryptography, Steganography, Chaotic map, Elementary Cellular Automata, Image Descriptor, Complexity.**

I. Introduction

Since the ancient era, people have been interested in providing secure messaging to preserve the privacy. Both cryptography and steganography could have facilitated to achieve this aim but by using a cipher or hide their existence. Steganography deals with composing hidden messages that only the sender and the receiver know about the existence of the message. Therefore, it does not attract unwanted attention. Cryptography is the study and art of hiding information which is used in case of communicating over a distrustful medium, where information needs to be protected from other third parties. In a place where the spying actions are predictable, the third parties may be suspicious of each message for having secret content. Hence, they do an investigation to uncover hidden content and in this condition adding the potential of encryption to steganography will ensure a very secure method of communication over any medium.

These techniques have many applications in computer science and many protected applications such as analyzing military satellite images, radar tracking object images, fingerprint images for identity authorization. Even in a remote medical system, according to the law, the electronic forms of medical records that include patient's medical images should be encrypted before they are sent over networks [1]. Since most steganographic systems use digital images as cover, the whole field has borrowed methods and ideas from the closely related fields of watermarking and fingerprinting which also manipulate digital audio and video, for copyright [2]. A preliminary prerequisite in a steganography system is to preserve the original essence of the cover as much as possible. Early image-based steganography systems aimed at making changes not detectable by the human eye [3]. This feature is not enough because statistical methods can detect the changes in the image even if it is not visible. Moreover, image compression methods play a critical role in the usefulness of a steganography method as they could change the embedded message in an irrecoverable fashion. Despite the fact that cryptography provides security solutions to a set of parties, the cyber attacker easily arouses these text and intercepts the communication to modify, inject, or drop of ciphered content. To improve these limitations, one could use the benefits of steganography as well, where sending invisible information is unlikely to draw attention. Indeed, utilizing both cryptography and steganography together can provide a higher level of privacy which each of them seems not to be capable of preserving such level.

Hopper et al. [4], [5] used a complexity-theoretic proof paradigm to show that the existence of one-way functions and access to a channel *oracle* are both necessary and sufficient conditions for the presence of secure steganography relative to any channel. They constructed a steganographic protocol that is provably secure and has nearly optimal bandwidth under these conditions when compared with known provably secure constructions, which is the first well-known example of a general provably secure steganographic protocol. We believe, however, that such integration would drastically increase the security of a steganographic system.

In this study, we add a chaotic cipher to the data has to be embedded in the cover. Without loss of generality, we assume that the data is an image and this chaotic map will classify the proposed system within the symmetric-key cryptography systems. Compared with the original image, the encrypted image can have the following two kinds of changes: the first is that the location relationships between the pixels are rearranged due to the image scrambling transformation that can effectively reduce the correlation of adjacent pixels; the second is that the gray-scale value of pixels are changed so as to make the information entropy of the encrypted image very close to the maximum value and the histogram of the encrypted image more smooth. The purpose of these changes is to make the encrypted image looks like a random one meanwhile keeping a capability of withstanding most common cryptographic attacks such as brute-force attack, statistical attack, and known-plaintext attack. This chaotic map constructs using a 128-bit key which was obtained by applying descriptors such as SIFT[6] to the cover image and passing it through elementary cellular automata with Rule 30 or 45. Besides the mentioned contribution towards ciphering, this

work also put emphasis on analyzing the complexity of the whole steganography system, as a complex system, by using different measures. Investigated measures in this study are absolute complexity, relative complexity, entropy followed by morphological richness [7], Levenshtein distance [8], and peak signal-to-noise ratio (PSNR) [9], number of pixels change rate (NPCR), unified average changing intensity (UACI), [10] histogram and correlation analysis.
The outline of this report is as follows: Section II surveys the background of this study. Motivate factors, proposed approach, and the analyzing criteria are mentioned in Section III. Finally, conclusive remarks are drawn in Section IV.

II. Related Work

Various image steganography techniques can be classified into spatial domain, transform domain, spread spectrum, and model-based steganography. In spatial domain, the secret message is embedded in pixel value directly. However, In transform domain methods, after transforming the image into the frequency domain, the image can be enclosed in proper transform coefficient. Least significant bit (LSB), gray-level modification, pixel value differencing, quantization index modulation, multiple based notational system, and predictive coding are among different sort of spatial domain approaches. [11]
In LSB, by replacing the least significant bit of the randomly chosen pixel in the cover image with the secret message bit embedding can be accomplished. There is a variety of Least significant bit based Steganography. Some of them include Adaptive LSB substitution based on brightness, edges and texture masking of the host image to estimate the number k of LSBs for data hiding, loss less generalized LSB data embedding, optimized LSB substitution using cat swarm strategy and genetic algorithm, data hiding based on histogram modification [12]. Multi-bit plane steganography technique is an extension to the simple LSB replacement technique. Secret message bits are hidden in multiple bit planes. However, one major defect with multi bit plane steganography is that non adaptive embedding manner may reduce the perceptual quality of the stego image if some of the high bit planes are involved in embedding arbitrarily without considering the local properties. Gray level modification, is used to map data by modifying the gray levels of pixels. Based on some mathematical function, a set of pixels is selected for mapping. This technique uses the concept of odd and even numbers to map data within a cover image. Advantages of this method include low computational complexity and high information hiding capacity. Pixel value differencing, is another embedding concept based on difference between pixel values. Cover image is divided into non overlapping blocks containing two connecting pixels and the difference in each block is modified. A larger difference in original pixel value allows a greater modification.
Quantization index modulation (QIM) [13] is one of the promising data embedding technique in digital watermarking and it can also be employed for steganography. QIM refers to embedding the information in cover medium by first modulating an index or sequence of indices with the embedded information and then quantizing the host signal with the associated quantizer or sequence of quantizers. QIM has high embedding capacity and it allows the embedder to control the robustness and the distortion induced while embedding. Multiple based notational system is one of the steganography method in which a system can be represented as a notational system with multiple bases to re-express a secret message to be hidden [14]. As the computer world is based on binary number system with base 2, in most of the cases the secret message is a binary stream and the amount of information contained in each symbol is exactly one bit. In order to embed more data in busy areas, the message can be expressed as an integer number using a variable base system. In other words, the message is converted into a series of symbols with different information carrying capabilities due to different bases used. The greater the base, the more information is contained in the corresponding symbol.
In MBNS steganography [15], secret data is converted into symbols in a notational system with multiple bases. Embedding by altering the pixel values directly leads to significant distortion in stego image resulting in less hiding capacity and poor visual quality. To overcome this issue, predictive coding approach is suggested where pixel values are predicted using predictor and instead of altering the pixel values, prediction error values (EV) are modified to embed secret data. Transform domain schemes are less prone to attack since detecting the low and high frequency areas greatly help to achieve efficient data embedding. To obtain the frequency domain representation, image transforms are used and are designed to possess two main properties: (a) Reduce image redundancy (b) Identify less important parts of image by isolating various frequencies in image.
Various image transforms that can be employed for data embedding include DCT, DWT, Haar transform, Hadamard transform, integer transform, contour let transform, DD DT DWT, Ridgelet transform, Ripplet transform etc. Not only the choice of transform but also the optimal data embedding locations affect the performance of the steganography system. Soft computing tools such as optimization algorithms, neural networks, fuzzy logic, hybrid networks etc. can be applied to improve embedding efficiency and perceptual quality.DWT decomposition of image results in four sub bands. Lowest sub band has the most important and relevant information and the higher sub band has finer details. Most of the energy is compacted into few transform coefficients an entropy coder locates them and encodes.Spread spectrum is another method for steganography which involves spreading the bandwidth of a narrow-band signal across a wide band of frequencies. Spread spectrum steganography, is a technique in which the bandwidth of a narrow-band signal is spreading over a wide-band of frequency.

III. Approach and measurement tools

The proposed method in this paper is hiding sensitive information within an image. In this method, Steganography is done with a cover image. The selection of cover image is important since the primary objective of steganography is to modify the carrier to avoid revealing the embedding message or the embedded secret message. Cover image refers to the image used for carrying the embedded bits, embedded data is known as payload and the image with embedded data is called as stego image.
After applying SIFT algorithm to the image, the extracted features are driven from the cover image. One of the descriptor which has 128 array is used to produce a key to embed data in

a cover image. For making a key, We use a 128-bit key to drive a CNN hyper-chaos system, i.e., a 128-bit key is mapped to the initial conditions of the CNN and used to calculate system parameters, which will then be deployed in the algorithm to generate binary chaotic sequences for the encryption process. [16] The steps of the algorithm is as follow: S is a original image with the size of $ih \times iw$, where ih and iw are the height and the width of a given image, and S is written as a set of $S_{i,j} i = 1, 2, ..., ih$ and $j = 1, 2, ..., iw$, T denotes the 128 bit key, and can be written as $T_1 T_2 ... T_{16}$.
Input: a 128 key and the original image
Output: encrypted image
Step1: The six system parameters for the algorithm are obtained through the following computational procedures:

$$H_1 = \oplus_{i=1}^{ih} \oplus_{j=1}^{iw} S_{i,j}, H_2 = (\sum_{i=1}^{ih} \sum_{j=1}^{iw} S_{i,j}) mod 256 \quad (1)$$

$$S = (T_1 + T_2 + ... + T_{16}) mod 256 \quad (2)$$

$$P = (T_1 \oplus T_2 \oplus ... \oplus T_{16}) \quad (3)$$

$$\lambda = (T_{10} + T_{11} + T_{12} + H_1 \times H_2) mod 256 \quad (4)$$

$$h = (T_{13} + T_{14} + T_{15} + T_{16} + H_1 \times H_2)/256 \quad (5)$$

Step2: Determine the initial condition $(x_{1,0}, x_{2,0}, x_{3,0})$ and iteration numbers N_0 of the CNN

$$x_{1,0} = (T_1 \times T_4 \times T_7 \times S \times P)/256^5 \quad (6)$$

$$x_{2,0} = (T_2 \times T_5 \times T_8 \times S \times P)/256^5 \quad (7)$$

$$x_{3,0} = (T_3 \times T_6 \times T_9 \times S \times P)/256^5 \quad (8)$$

Then iterate the CNN for $iw \times ih$ times from the initial condition $(x_{1,0}, x_{2,0}, x_{3,0})$ by using fourth-order Runge-Kutta Method (the time step size is 0.005) to solve the CNN differential equation (8.3). Here, to avoid the transient effect, the first N_0 iterations are considered. Let $\{(x_{1,i}, x_{2,i}, x_{3,i})\}_{i=1}^{iw \times ih}$ denotes the set of solutions of CNN. The size of the set is $iw \times ih$, and ith element has three points $(x_{1,i}, x_{2,i}, x_{3,i})$, $i = 1, 2, ..., iw \times ih$. Then we map $(x_{1,i}, x_{2,i}, x_{3,i})$ to a character that will be used to encrypt image pixel in the future, and the mapping procedure is described as follows: Assume $v_i = h(x_{1,i}^2 + x_{2,i}^2 + x_{3,i}^2)^{1/2} + \lambda$, and u_i denotes the decimal fraction of v_i, then u_i can be represented as a binary sequence $u_i = 0.b_{i,1} b_{i,2} ... b_{i,p}$ where p is a certain precision (here let $p = 32$). Let $w_i = (w_{i,0} w_{i,1} ... w_{i,7})_2$, where $w_{i,j}$ denotes the jth bit of w_i, and $w_{i,j} = b_{i,4j+1} \oplus b_{i,4j+2} \oplus b_{i,4j+3} \oplus b_{i,4j+4} \oplus, j = 0, 1, ..., 7$. Hence, we obtain a character w_i from $(x_{1,i}, x_{2,i}, x_{3,i})$. Finally, when the variable i changes from 1 to $iw \times ih$, we will obtain a pseudo-random key-stream $\{w_i\}_{i=1}^{iw \times ih}$ to encrypt the original image. Step4: Let us suppose e_i , w_i and $m + i$ denote the cipher-text (encrypted image), pseudo-random key-stream and plaintext (original image) respectively, where $i = 1, 2, ..., iw \times ih$. Then the encryption process is defined as follows:

$$e_i = (w_i + m_i) mod 256 \quad (9)$$

Since our algorithm is a symmetrical one, the decryption process is similar to the encryption process except for the extend key $T_E$used to generate w_i . The original image can be regenerated from the encrypted image through the following:

$$m_i = (e_i - w_i) mod 256 \quad (10)$$

The private image which carry sensitive information is encrypted with this rule, too. Then, by using one of the Steganography method the private image is putted in the cover image. For decryption purpose, all of these steps should be done in a recursive way. It means that, the Steganography method extract the private image from the cover image in the firs step.Then, by applying the key on a private image, the encrypted message is appeared. Image quality measures are used for the evaluation of stego image quality obtained after embedding. The algorithm used for data embedding should withstand against all these types of attacks making eavesdropper unable to retain the hidden message. To do so, different complexity measures as absolute complexity, relative complexity, entropy followed by morphological richness [7], Levenshtein distance [8], and peak signal-to-noise ratio (PSNR) [9], number of pixels change rate (NPCR), unified average changing intensity (UACI), [10] histogram and correlation analysis are used.
In literature, many steganography schemes are presented based on variety of parameters. Irrespective of the approach used for data embedding, some common attributes need to be defined to achieve uniqueness in performance rating. Some of them can be defined as follow:

- **Security against attack:** The steganographic system may suffer from different types of stego attacks, allowing eavesdropper to retrieve secret message bits embedded in cover media. The system is said to be γ secure if $TPRate - FPRate \leq \gamma$,where $0 \leq \gamma \leq 1$, and is said to be perfectly secure if $\gamma = 0$.
- **Payload capacity:** It is defined in terms of number of secret bits that can be embedded per pixel. It is also known as hiding capacity or embedding capacity and is measured in terms of bits per pixel or bits per transform coefficient.
- **Imperceptibility:** Steganography system should have high embedding capacity and capability to withstand against stego attacks. The stego image should not have severe visual artifacts. Higher the fidelity of the stego image, the better.

There are numerous ways to define security of steganography system which is the main criterion while designing the system.

- **Maximum mean discrepancy (MMD) security:** The task of identifying the differences between cover and stego image is a two sample problem that can be solved using MMD. It finds the discrepancy between pdf of cover and stego objects. It is given by, $MMD(F, X, Y) = sup_{f \epsilon F} (\frac{1}{D} \sum_{i=1}^{D} f(x_i) - \frac{1}{D} \sum_{i=1}^{D} f(y_i))$
- **ROC based security:** Another way to quantify security is with reference to ROC. AIt is the plot of false positive rate versus true positive rate [17]. The true positive rate is plotted on Y axis and false positive rate on X axis. Larger the area under the curve,

better the performance of the steganalytic system, e.g., performance of curve C is better than B, and that of B is better than A.

- **KullbackLeibler (KL) divergence:** KL divergence is one of popular security measures to analyze the steganography system. Let X and Y represent cover and stego image and p_x and q_y denote the probability distribution function of X and Y, respectively. KL divergence between two probability distribution functions is given by $D(p_x \parallel q_y) = \sum_{g \epsilon G} P_x(g) \log \frac{P_x(g)}{q_y(g)}$

REFERENCES

[1] Philip P Dang and Paul M Chau. Image encryption for secure internet multimedia applications. *IEEE Transactions on consumer electronics*, 46(3):395–403, 2000.

[2] Prabhishek Singh and RS Chadha. A survey of digital watermarking techniques, applications and attacks. *International Journal of Engineering and Innovative Technology (IJEIT)*, 2(9):165–175, 2013.

[3] Mohammad Shirali-Shahreza and Sajad Shirali-Shahreza. Collage steganography. In *Computer and Information Science, 2006 and 2006 1st IEEE/ACIS International Workshop on Component-Based Software Engineering, Software Architecture and Reuse. ICIS-COMSAR 2006. 5th IEEE/ACIS International Conference on*, pages 316–321. IEEE, 2006.

[4] Nicholas J Hopper, John Langford, and Luis Von Ahn. Provably secure steganography. In *CRYPTO*, volume 2442, pages 77–92. Springer, 2002.

[5] Nicholas Hopper, Luis von Ahn, and John Langford. Provably secure steganography. *IEEE Transactions on Computers*, 58(5):662–676, 2009.

[6] David G Lowe. Distinctive image features from scale-invariant keypoints. *International journal of computer vision*, 60(2):91–110, 2004.

[7] Andrew Adamatzky and Genaro J Martinez. On generative morphological diversity of elementary cellular automata. *Kybernetes*, 39(1):72–82, 2010.

[8] Gonzalo Navarro. A guided tour to approximate string matching. *ACM computing surveys (CSUR)*, 33(1):31–88, 2001.

[9] Quan Huynh-Thu and Mohammed Ghanbari. Scope of validity of psnr in image/video quality assessment. *Electronics letters*, 44(13):800–801, 2008.

[10] Guanrong Chen, Yaobin Mao, and Charles K Chui. A symmetric image encryption scheme based on 3d chaotic cat maps. *Chaos, Solitons & Fractals*, 21(3):749–761, 2004.

[11] Ali Soleymani, Zulkarnain Md Ali, and Md Jan Nordin. A survey on principal aspects of secure image transmission. In *Proceedings of World Academy of Science, Engineering and Technology*. World Academy of Science, Engineering and Technology, 2012.

[12] Zhi-Hui Wang, Chin-Chen Chang, and Ming-Chu Li. Optimizing least-significant-bit substitution using cat swarm optimization strategy. *Information Sciences*, 192:98–108, 2012.

[13] Brian Chen and Gregory W Wornell. Quantization index modulation: A class of provably good methods for digital watermarking and information embedding. *IEEE Transactions on Information Theory*, 47(4):1423–1443, 2001.

[14] Chin-Chen Chang, Thai Son Nguyen, and Chia-Chen Lin. A reversible data hiding scheme for vq indices using locally adaptive coding. *Journal of Visual Communication and Image Representation*, 22(7):664–672, 2011.

[15] Xinpeng Zhang and Shuozhong Wang. Steganography using multiple-base notational system and human vision sensitivity. *IEEE signal processing letters*, 12(1):67–70, 2005.

[16] Jun Peng and Du Zhang. Image encryption and chaotic cellular neural network. In *Machine Learning in Cyber Trust*, pages 183–213. Springer, 2009.

[17] Karimollah Hajian-Tilaki. Receiver operating characteristic (roc) curve analysis for medical diagnostic test evaluation. *Caspian journal of internal medicine*, 4(2):627, 2013.