A Steganographic Scheme for Secure Communications Based on the Chaos and Euler Theorem

Der-Chyuan Lou and Chia-Hung Sung

***Abstract*—Steganography has been proposed as a methodology for transmitting messages through innocuous covers to conceal their existence. This work proposes an asymmetric image steganographic method based on a chaotic dynamic system and the Euler theorem. The hidden message can be recovered using orbits different from the embedding orbits, and the original image is not required to extract the hidden message. Experimental results and discussions reveal that the proposed scheme possesses security, imperceptibility and survivability.**

***Index Terms*—Asymmetric orbit, covert communication, dynamic system, man-in-the-middle attack, steganography.**

I. Introduction

THE DEVELOPMENT of the Internet has allowed digital data to be transmitted conveniently over networks. However, users must be aware that unprotected data transmitted on an open network is not secure, and can easily be intercepted by unauthorized users. Consequently, protecting data during transmission is an important issue. The cryptography techniques discussed in [1], which transform messages into a clutter, are good for securing textual data, but unsuitable for digital media. For example, the RSA encryption algorithm [2] is unsuitable for large amounts of data because of its relatively slow performance. Furthermore, deciphering can be defeated by flipping one bit in the cipher stream.

Information-hiding techniques [3] such as steganography [4]–[7] and watermarking [8]–[11] provide another method of protecting digital data. These techniques embed the data into digital media such that the embedding results remain meaningful and yet appear innocuous to outsiders. The characteristics of information-hiding systems have been widely discussed, and some of their properties include robustness, tamper resistance, imperceptibility, low computational costs and false positive rate [12]. In practice, it is probably impossible to design a information-hiding system that excels in all of these properties, and instead a careful analysis of the application is required to determine an acceptable balance of these properties. For example, digital watermarking embeds a short signature into a digital image for copyright protection. Such a scheme may not require a large capacity, but must be robust to removal and detect the ownership reliably; even after image processes such as rotation, translation, cropping and quantization are applied. Steganography hides secret messages in digital covers to conceal the existence of the secret messages, and must include a method of embedding data invisibly, allow the extracted data to be readable only by the authorized user and incorporate a degree of survivability for covert communications.

The most general steganographic model was the prisoners' problem, presented by Simmon [13] in 1984. This scenario involves two separated prisoners, Alice and Bob, who wish to communicate covertly to hatch an escape plan. Alice hides a message in a cover-object to obtain the stego-object, where the cover-object can be an image, audio or video. Any communications between the pair are examined by the warden, who will place them in solitary confinement if she/he finds their secret messages.

Kurak and McHugh [4] presented a steganographic technique called image downgrading. Four least significant bits (LSB) of the pixels of a cover-image are exchanged with four most significant bits of a secret message. This method is restricted to LSB and generally achieves high capacity and low perceptibility, but is vulnerable to extraction by unauthorized parties. Bender *et al.* [5] presented a patchwork that alters the statistical properties of a cover-image. Pairs of image regions are selected by using a pseudorandom number generator (PRNG) and the pixel intensities in various regions are increased or decreased by a constant quantity. This kind of minor modification is generally unnoticeable. Furthermore, Matsui and Tanaka [6] presented a steganographic system on a quantized image. This system calculates the difference between adjacent pixels and feeds them into a quantizator, which outputs a discrete approximation of the difference. The system also uses a stego-key, which is a table that assigns a specific bit to every possible value in the error difference. If the approximate difference does not match the data bit on the table, it is replaced by the nearest difference with an associated bit that equals to the embedded data bit. Marvel *et al.* [7] presented an image spread spectrum steganographic method that both hid and recovered messages in the frequency domain. The secret message was encrypted using a conventional symmetric encryption scheme, and the resulting encoded message was then modulated using a PRNG. These steganographic schemes have symmetric properties, namely a shared key or table for messages embedding and extraction. Hence, the prisoners' problem assumes that the two communicating partners must share a secret in advance

Manuscript received August 8, 2000; revised Ocrtober 1, 2002. This work was supported in part by the National Science Council of Taiwan, R.O.C., under Grant NSC 91-2219-E-014-003. The associate editor coordinating the review of this manuscript and approving it for publication was Dr. Thomas R. Gardos.

The authors are with the Department of Electrical Engineering, Chung Cheng Institute of Technology, National Defense University, Taoyuan 33509, Taiwan, R.O.C. (e-mail: dclou@ccit.edu.tw).

Digital Object Identifier 10.1109/TMM.2004.827493

1520-9210/04$20.00 © 2004 IEEE

to secure their communications. However, an attacker is able to remove or read the embedded message completely once the shared key is known to the public. Moreover, there also exists the problem of the shared key distribution.

This work aims to design a chaotic asymmetric steganographic (CAS) methodology for covert communications. An asymmetric hiding system can be conceived as comprising two descriptions of a transformation mapping between embedding and extraction based on two different keys. The CAS system derivates the chaotic communication, which includes a stego-matrix, computable orbits and embedding method design. The asymmetric system is not only concerned with securing the message itself, but also with authenticating the sender to prevent problems of fraud.

The rest of this paper is organized as follows. Section II describes the dynamic chaotic system [14], while Section III details the embedding and extraction processes. Section IV then presents some experimental results and discusses on security, imperceptibility and survivability of the CAS scheme. Finally, Section V gives some conclusions.

II. Preliminary

A. Chaotic Dynamic System

A dynamic system can be considered as a specific state at each time point with the state changing with time. Two kinds of dynamic systems exist: discrete time and continuous time. In the discrete time dynamic system (DTDS), each state results from a chaotic mapping of the preceding state. For clarity, given an initial condition at $\mathrm{time} = 0$, a DTDS will be specified using the equations: $x(0) = x_0$, and $x(k+1) = f(x(k))$, and thus $x_0 = f^k(x_0)$ follows, where f^k denotes k iterations of f to x_0. Generally, a point of DTDS can return to its initial condition after k iterations of f to x_0, and the period k is thus termed the stable *orbit*.

An example of a chaotic mapping called Arnold's cat map [15] is based on modular arithmetic. The transformation is defined as $\mathbf{T}: \mathbf{R}^2 \rightarrow \mathbf{R}^2$ and can be represented by the following formula:

$$\mathbf{T}\left(\begin{bmatrix} x' \\ y' \end{bmatrix}\right) = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod 1. \tag{1}$$

Because the above computation includes "mod 1", $\mathbf{T}$ maps all points of $\mathbf{R}^2$ into the unit square $\mathbf{U} = \{(x,y)|0 \le x, x' < 1, 0 \le y, y' < 1\}$. Suppose that $\mathbf{U}$ is divided into p^2 pixels, where each pixel has a period to return to its initial position, all p^2 pixels on $\mathbf{U}$ then return to their initial positions after $\prod(p^2)$ iterations. Toral automorphism [14] is another chaotic map that performs "$\mathrm{mod}\ N$" modular arithmetic. The transformation is defined as $\mathbf{A}: \mathbf{L}_N \rightarrow \mathbf{L}_N$ and is represented by the following formula:

$$\mathbf{A}\left(\begin{bmatrix} x' \\ y' \end{bmatrix}\right) = \begin{bmatrix} 1 & 1 \\ k & k+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N \tag{2}$$

where $(x,y) \in \mathbf{L}_N = \{(x,y)|0 \le x, x' < N, 0 \le y, y' < N\}$ and $k \in [1, N]$. Once the matrix $\mathbf{A}$ and modular number N are given, the automorphism period can be investigated through an exhaustive search.

DTDS behavior is complex and its diffusion and confusion characteristics are good candidates for encryption algorithms. Unfortunately, most chaotic mappings are unstable. Some results related to the periodicity of the mapping in (2) were reported in [15]. This work notes that covert communications based on two-dimensional chaotic mapping can work properly if the stable orbit of a DTDS can be constructed.

B. RSA Cryptosystem

The RSA algorithm uses two asymmetric keys that work in pairs for encryption and decryption, respectively. Two primes, p and q, are chosen to compute $n = p \times q$ and $m = (p-1) \times (q-1)$, and an integer K_P is chosen such that K_P is in $[1, m-1]$ with relatively prime to m. Finally, select K_S in $[1, m-1]$ such that $K_P \times K_S \equiv 1(\bmod\ m)$, where K_P represents the public key and K_S denotes the private key. The encryption E and decryption D are defined as follows:

$$\begin{aligned} \mathrm{E(M)} &= \mathrm{M}^{K_P} (\mathrm{mod} n) = \mathrm{C} \\ \text{and } \mathrm{D(C)} &= \mathrm{C}^{K_S} (\mathrm{mod} n) = \mathrm{M} \end{aligned} \tag{3}$$

where M and C denote the plain-text and the cipher-text, respectively.

The RSA scheme allows two people to establish communications through an insecure channel without shared keys. However, in the prisoners' scenario, the warden could send a false message to Bob using Bob's public-key, and thus Bob must have a means of ensuring the identity of the sender. This problem is termed as man-in-the-middle attack [16].

III. Chaotic Asymmetric Steganography Scheme (CAS)

This section presents an asymmetric scheme for images steganography based on a dynamic chaotic system and the Euler theorem. The basic idea is to use a different secret for embedding to that used for extraction. The CAS scheme uses a chaotic mapping of a stego-matrix that provides confusion and diffusion analogous to cryptography to secure the encoded message. A lossless compression can maximize the payload of the embedded data and the error-control coding (ECC) [1] can effectively correct errors.

The embedding method uses local characteristics of the image blocks to adaptively modify pixel values and thus ensures imperceptibility. Another advantage is that no cover-image is required to retrieve the embedded message from the stego-image. Furthermore, when the receiver receives the stego-image, she/he can also build a stego-matrix to extract the embedded message. The chaos deciphering-message must be ECC decoded and decompressed in sequence for the receiver to obtain the original message.

The following subsections detail the stego-matrix generation, embedding and extraction processes.

A. Stego-Matrix Generation

Section II reveals that the period orbit can be investigated once the toral automorphism matrix and modular number are given. However, obtaining the closed form formula for the cycle period is difficult. Based on the above observation, the following

theorem was derived to generate the stego-matrix and compute the stable orbit.

Theorem 1: If p_1 and p_2 are two primes and both relatively prime to n, and let $\mathbf{Q}(k) = \begin{bmatrix} 1 & 1 \\ k & k+1 \end{bmatrix}$ be an automorphism matrix. A stego-matrix $\mathbf{S}$ can be defined as follows:

$$\mathbf{S} \equiv \left[\mathbf{Q}(k) \cdot \begin{bmatrix} p_1 & 0 \\ 0 & p_2 \end{bmatrix} \cdot \mathbf{Q}^{-1}(k)\right] (\bmod\, n). \tag{4}$$

Thus, $\mathbf{S}$ has a periodic orbit $P = \phi(n)$. This theorem implies $\mathbf{S}^{\phi(n)}(\bmod\, n) = \mathbf{I}(\text{identity})$, where $\phi(\cdot)$ denotes the *Euler phi-function*.

Proof : See (5)–(6) at the bottom of the page. Referring to the Euler theorem [1], if $n \geq 2$ and $gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$. Let p_1 and p_2 be primes relative to n. The Euler theorem becomes

$$p_1^{\phi(n)} \equiv 1 \pmod{n} \tag{7}$$

and

$$p_2^{\phi(n)} \equiv 1 \pmod{n}. \tag{8}$$

Hence,

$$\begin{bmatrix} p_1^{\phi(n)} & 0 \\ 0 & p_2^{\phi(n)} \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} (\bmod\, n) \tag{9}$$

then

$$\begin{aligned} &\mathbf{S}^{\phi(n)} \\ &= \begin{bmatrix} 1 & 1 \\ k & k+1 \end{bmatrix} \begin{bmatrix} p_1^{\phi(n)} & 0 \\ 0 & p_2^{\phi(n)} \end{bmatrix} \begin{bmatrix} 1 & 1 \\ k & k+1 \end{bmatrix}^{-1} (\bmod\, n) \\ &= \begin{bmatrix} 1 & 1 \\ k & k+1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ k & k+1 \end{bmatrix}^{-1} (\bmod\, n) \\ &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} (\bmod\, n) = \mathbf{I}. \end{aligned} \tag{10}$$

Thus, using Theorem 1 the periodic orbit of $\mathbf{S}^{\phi(n)}(\bmod\, n)$ is $\phi(n)$.

Example 1: Let $p_1 = 5$, $p_2 = 7$, and $k = 15$. The stego-matrix can be

$$\begin{aligned} \mathbf{S} &\equiv \begin{bmatrix} 1 & 1 \\ 15 & 16 \end{bmatrix} \begin{bmatrix} 5 & 0 \\ 0 & 7 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 15 & 16 \end{bmatrix}^{-1} (\bmod\, n) \\ &\equiv \begin{bmatrix} -25 & 2 \\ -480 & 37 \end{bmatrix} (\bmod\, n). \end{aligned} \tag{11}$$

If $n = 17$, we can obtain $\mathbf{S}^{\phi(17)}(\bmod 17) \equiv \mathbf{S}^{16}(\bmod 17) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, and that makes $\mathbf{S}^{17}(\bmod\, 17) \equiv \mathbf{S}\,(\bmod\, 17)$. Here, the periodic orbit of $\mathbf{S}(\bmod 17)$ is $\phi(17) = 16$.

The above example demonstrates that the period orbit can be obtained from the modular number and the stego-matrix. Both the stego-matrix $\mathbf{S}$ and modular number n can be varied if Theorem 1 is satisfied. Subsequently, Theorem 2 was derived to allow the CAS scheme to utilize the chaotic mapping for covert communications.

Theorem 2: For any integer lattice L_N of size N, $\mathbf{A}(k)$ is a toral automorphism transformation. Given a period orbit $P = \mathbf{A}(k, N)$ such that $\mathbf{A}_N^P(k)r(\bmod N) \equiv r(\bmod N)$, the extended orbit $P' = R \times P$ also exists such that $\mathbf{A}_N^{P'}(k)r(\bmod N) \equiv r(\bmod N)$ is satisfied, where $\forall r \in L_N$ and $R \in Z^+$. The action of $\mathbf{A}_N^{i+j\times P}(k)r(\bmod N) = r'(\bmod N)$ and $\mathbf{A}_N^{P'-i}(k)r'(\bmod N) = r(\bmod N)$ then hold for all positives i, j and r, $r' \in L_N$

Theorem 2 implies that any lattice point in L_N can be spread over the entire region L_N by applying the mapping $\mathbf{A}_N^i(k)$, where $i < P'$ and the lattice point returns to its initial condition by applying the mapping $\mathbf{A}_N^{P'-i}(k)$.

B. Embedding Process

We now detail the embedding procedure. Let X denote the cover-image of size $M \times N$, defined as $X = \{x_{i,j} | 0 \leq i < M, 0 \leq j < N\}$, where $x_{i,j} \in \{0, 1, \ldots, 2^l - 1\}$ denotes the intensity value, and l bits represent the pixel value. Assume that $\mathbf{B}$ of length L is the embedded message hidden in X, where $\mathbf{B} = \{b_k | 0 \leq k < L\}$, and $b_k \in \{0, 1\}$ is the binary value of the secret message. Meanwhile, the lossless compression can compress the hidden message in advance to maximize the payload of the embedding, and the ECC is padded with the compressed message to correct errors. The stego-matrix is used to generate the *chaos cipher-message* and adaptive modification is used to design the embedding procedure, as follows.

Step 1) Select p_1, p_2, and k, and then use Theorem 1 to build the stego-matrix $\mathbf{S}$.

Step 2) Two moduli N_S (modulus for the sender) and N_R (modulus for the receiver) are used to calculate period orbits P_S and P_R with $\mathbf{S}$, respectively, where $N_S \neq N_R$. Extend the period orbits to $P_S' = lcm(P_S, N_{pub})$ and $P_R' = lcm(P_R, N_{pub})$, where N_{pub} represents the public large number in

---

$$\mathbf{S} \equiv \left[\mathbf{Q}(k) \cdot \begin{bmatrix} p_1 & 0 \\ 0 & p_2 \end{bmatrix} \cdot \mathbf{Q}^{-1}(k)\right] (\bmod\, n) \equiv \begin{bmatrix} 1 & 1 \\ k & k+1 \end{bmatrix} \begin{bmatrix} p_1 & 0 \\ 0 & p_2 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ k & k+1 \end{bmatrix}^{-1} (\bmod\, n) \tag{5}$$

$$\begin{aligned} \mathbf{S}^P &= \underbrace{\left[\mathbf{Q}(k) \cdot \begin{bmatrix} p_1 & 0 \\ 0 & p_2 \end{bmatrix} \cdot \mathbf{Q}^{-1}(k) \cdots \mathbf{Q}(k) \cdot \begin{bmatrix} p_1 & 0 \\ 0 & p_2 \end{bmatrix} \cdot \mathbf{Q}^{-1}(k)\right] (\bmod\, n)}_{\phi(n) \text{ times}} \\ &\equiv \begin{bmatrix} 1 & 1 \\ k & k+1 \end{bmatrix} \begin{bmatrix} p_1^{\phi(n)} & 0 \\ 0 & p_2^{\phi(n)} \end{bmatrix} \begin{bmatrix} 1 & 1 \\ k & k+1 \end{bmatrix}^{-1} (\bmod\, n). \end{aligned} \tag{6}$$

the RSA cryptosystem and *lcm* denotes the least common multiple.

Step 3) Calculate the private orbits of the sender and receiver, namely $P_{SS} = (P'_S - K_{PS})(\mathrm{mod} P_S)$ and $P_{SR} = (P'_R - K_{PR})(\mathrm{mod} P_R)$, using Theorem 2, where K_{PS} and K_{PR} denote the public keys of the sender and receiver, which are used as the partial iteration.

Step 4) Compare the order of moduli N_S and N_R, and obtain the chaos cipher-message $\mathbf{B}'$ by applying $\mathbf{S}$, P_{SS} and K_{PR} using (12), where $\mathbf{B}$ denotes a secret message of length L and is represented by a matrix of size $M_{\mathrm{B}} \times N_{\mathrm{B}}$.

$$\mathbf{B}'(i',j') = \begin{cases} \mathbf{S}_{N_R}^{K_{PR}}(\mathbf{S}_{N_S}^{P_{SS}}(\mathbf{B}(i,j))), & \text{if } N_S < N_R, \\ \mathbf{S}_{N_S}^{P_{SS}}(\mathbf{S}_{N_R}^{K_{PR}}(\mathbf{B}(i,j))), & \text{if } N_S > N_R, \end{cases} \quad (12)$$

where $0 < i \leq M_{\mathrm{B}}$, $0 < j \leq N_{\mathrm{B}}$ and $0 < i' \leq N_R$, $0 < j' \leq N_R$.

The CAS scheme suffers a peculiar phenomenon called the "reblocking problem" [17] if the domain of the sender's permutation is not a subset of that of the receiver. Therefore, it is important that both sender and receiver agree upon the order of the applied functions to avoid this problem.

Image steganography attempts to conceal embedded messages inside a digital image, and thus the embedded message must be invisible to human eyes. The embedding method embeds messages bits using the local characteristics of the image blocks and adaptively modifies the pixel values to maintain invisibility of the embedded messages. Let x denote the pixel that hides an embedded message bit. Fig. 1 shows the relationship between the pixel and surrounding blocks. Here, $g_{u,x}$ and $g_{l,x}$ represent the block-mean values of the upper and lower blocks corresponding to x, while $g_{m,x}$ denotes the average value of $g_{u,x}$ and $g_{l,x}$. That is

$$g_{u,x} = \frac{a+b+c}{3}, \quad g_{l,x} = \frac{d+e+f}{3}, \quad \text{and } g_{m,x} = \frac{g_{u,x}+g_{l,x}}{2} \quad (13)$$

where a, b, c, d, e, and f denote the intensity values of x's neighboring pixels. Comparing the distance $D(g_{u,x}, g_{l,x}) = |g_{u,x} - g_{l,x}|$ with a predefined threshold reveals the local characteristics of the image blocks. For example, if D exceeds the predefined threshold, x can be considered as located in an edge region. The embedding process can modify pixels more than that of smooth regions because the luminance edges make surrounding signals less visible. On the other hand, if D does not exceed the predefined threshold then x could be located in the smooth region. In this case, x is less amended to embed the message bit because smooth regions are highly sensitive to modification.

The embedded bit b_i is either 0 or 1, and the embedding process modifies the intensity of the X pixels according to the following rules.

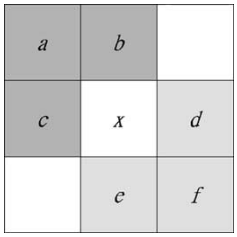

Fig. 1. Relationship of an image pixel and its surrounding pixels.

1) $b_i = 0$

i) when $D(g_{u,x}, g_{l,x}) \leq 3{*}T$, then $x' = g_{m,x} - T$. (14)

ii) when $D(g_{u,x}, g_{l,x}) > 3{*}T$, if $g_{u,x} \leq g_{l,x}$, then $x' = g_{u,x} - T$, else $x' = g_{u,x} + T$. (15)

2) $b_i = 1$

i) when $D(g_{u,x}, g_{l,x}) \leq 3{*}T$, then $x' = g_{m,x} + T$. (16)

ii) when $D(g_{u,x}, g_{l,x}) > 3{*}T$, if $g_{u,x} \leq g_{l,x}$, then $x' = g_{l,x} + T$, else $x' = g_{l,x} - T$. (17)

Here, x' denotes the modified pixel, while T represents a small value used to tune the x' intensity. Notably, the pixel values in the edge region are increased or decreased according to the mean values of the upper and lower blocks. The minimal distance between the pixels and their surrounding blocks is used to identify the embedded bit. In contrast, the pixel values in the smooth region are increased or decreased according to the average mean values of two blocks surrounding them. The resulting pixel values will be between the mean values of the two surrounding blocks and they will not produce suspicious artifacts. Based on the human visual system (HVS), modifying pixel values using the local characteristics of the image blocks can maintain the imperceptibility of the embedded data. Meanwhile, the extraction process will be robust because the local characteristics of the image blocks are still remained even after attackers use general image processing to remove the hidden messages. However, making a poor decision of the image block characteristic may cause incorrect extraction and a false positive. The use of an appropriate ECC code can correct such errors.

C. Extraction Process

The extraction process resembles the embedding process. In real applications a cover-image is not required to extract the hidden message, and thus g_{u,x^*}, g_{l,x^*}, and g_{m,x^*} of each pixel x^* from the stego-image are calculated using (13). Next, the retrieved bit value is determined using the following rules.

i) when $D(g_{u,x^*}, g_{u,x^*}) \leq 3{*}T$,

$$\text{if } x^* \leq g_{m,x^*}, \text{ then } b_i^* = 0, \text{ else } b_i^* = 1. \quad (18)$$

ii) when $D(g_{u,x^*}, g_{u,x^*}) > 3{*}T$,

$$\text{if } D(x^*, g_{u,x^*}) \leq D(x^*, g_{l,x^*}), \text{ then } b_i^* = 0, \text{ else } b_i^* = 1. \quad (19)$$

The receiver then generates the stego-matrix and applies the remaining orbits K_{PS} and P_{SR} to further permutes the extracted bits $\mathbf{B}'$ using (20) to obtain the encoded message $\mathbf{B}^*$.

$$\mathbf{B}^*(i^*,j^*) = \begin{cases} \mathbf{S}_{N_S}^{K_{PS}}\left(\mathbf{S}_{N_R}^{P_{SR}}(\mathbf{B}'(i,j))\right), & \text{if } N_S < N_R\,, \\ \mathbf{S}_{N_R}^{P_{SR}}\left((\mathbf{S}_{N_S}^{K_{PS}}(\mathbf{B}'(i,j))\right), & \text{if } N_S > N_R \end{cases} \tag{20}$$

where $0 < i \leq N_R$, $0 < j \leq N_R$, and $0 < i^* \leq M_{\mathrm{B}}$, $0 < j^* \leq N_{\mathrm{B}}$.

The ECC decoder and the decompression module are then used to reconstruct the secret message.

IV. Experimental Results and Discussions

This section presents some experiments and discussions on security, imperceptibility, survivability and computational cost to demonstrate that the CAS scheme is suitable for image steganography.

A. Multiple-Embedding

Substantially, the extracted message may contain numerous bit errors. Some pixels from the cover-image are not embedded message bits but could be mistaken for extracted message bits by the receiver. Anderson and Peitcolas [16] suggested using redundancy to cope with these errors. In the CAS scheme, redundancy comes from a synonym condition involving the different moduli between the sender and the receiver. The following example illustrates the synonym condition.

Example 2: Suppose a stego-matrix $\mathbf{S} = \begin{bmatrix} -25 & 2 \\ -480 & 37 \end{bmatrix}$, $N_S = 143$, $N_R = 253$, $K_{PS} = 10$, and $K_{PR} = 17$. Based on the Theorem 1, the orbits are $P_S = \phi(143) = 120$ and $P_R = \phi(253) = 220$, and private orbits are $K_{SS} = 110$ and $K_{SR} = 203$. Let the length of a message be 1024 bits, and let the message be represented by a matrix map with size 32×32. Suppose the matrix map contains a position $p = (13, 32)$, and using (12) can identify two positions in the cover-image, $p' = (79, 88)$ and $p'' = (224, 89)$. The embedding process modifies the pixel at position p'' to embed a message bit. However, when retrieving information from the stego-image, the position $q = (2, 50)$ in the stego-image is found to correspond to two positions, $q' = (79, 153)$ and $q'' = (13, 32)$ using (20). Here, $q'' = p$, but $q \neq p''$.

The synonym condition will influence the extraction results, and the same data bit can be embedded into these synonym positions to strengthen the correctness of the embedded data. This operation is termed the *multiple-embedding* rule, and while it degrades the quality of the stego-image and reduces the probability of incorrect extraction. The tradeoff is inevitable, and sacrificing visual quality to improve the extraction correctness is worthwhile.

B. Security Analyzes

Two stages are required to break a steganographic system, as follows [18]: first, an attacker must discover that steganography has been used; second, the attacker must manage to read the embedded message. This section discusses two types of attacks on steganographic systems [19].

One type of attack is the *stego-only* attack, where the attacker is assumed to have nothing but the stego-image. A stego-image must not contain any blocking artifacts associated with message embedding because an attacker could easily utilize those artifacts to detect the secret message. The CAS method modifies pixel values to embed messages based on the local characteristics of the image blocks, and the stego-image does not differ significantly from the cover-image. Hence, the stego-image maintains high fidelity and shall not arouse suspicion. If the hidden message is not advertised, a casual attacker will be unaware of its existence and therefore will not attempt to break it. Furthermore, incidental attacks such as rotation and scaling will not remove the embedded message and will only make it nonextractable. Finally, despite such attacks, the stego-image can still be synchronized with the cover-image to extract the embedded message.

The other type of attack is the *known-cover* attack. Obviously, the attacker can detect the difference between a cover-image and a stego-image if she/he has access to both images. Steganography is not secure against the known-cover attack. However, if the difference contains random signals then it is difficult for the attacker to break the system. Combining the steganographic method with traditional cryptography can increase security, but in this case embedding and extraction requires that both the sender and the receiver share the key (i.e., the seed of PRNG) in advance, and thus creates the shared key distribution problem. Moreover, combining prior enciphering with steganography also suffers from the problem that deciphering can be defeated by flipping one bit in the cipher stream.

To overcome the key distribution problem, the sender and receiver can use public-key cryptosystems to share a secret key without establishing a secure channel. The RSA algorithm can avoid slow performance by encrypting the secret key used for symmetrical cryptographic algorithms. However, this approach is susceptible to a man-in-the-middle attack, and fraud problem. For example, in the prisoner problem Alice can encrypt the secret key using Bob's public key and then embed it into the cover-object. The warden could also encrypt a fake secret key using Bob's public key and then generate a fake stego-object. Bob would be unable to verify the received secret key in this case because he cannot distinguish a message sent by Alice from one sent by the warden. However, the problem of authentication can be solved by using asymmetric keys.

Compared to contemporary approaches using a symmetrical key, the CAS scheme uses a chaotic dynamic system and the Euler theorem to develop asymmetric orbits in the embedding and extraction processes. The computable orbit is calculated using a nonlinear "mod" operation, based on the assumption that the knowledge of the embedding is not sufficient to allow an adversary to detect or read the embedded message for covert communications. The asymmetric method can also be used to ascertain that messages originate from the sender. For example, if Alice uses her private key to send messages to Bob, then the warden will be unable to forge a message from Alice. However, both Bob and warden will be able to read messages from Alice, because they know Alice's public key. The CAS scheme also protects the message with Bob's public key. The two-fold automorphism can keep the message secure and avoid fraud by

Fig. 2. (a) Original cover-image; (b) stego-image with PSNR $= 38.6432$ dB, $L = 1024$ bits; (c) stego-image with PSNR $= 35.5419$ db, $L = 2048$ bits; (d) stego-image with PSNR $= 32.5876$ db, $L = 4096$ bits.

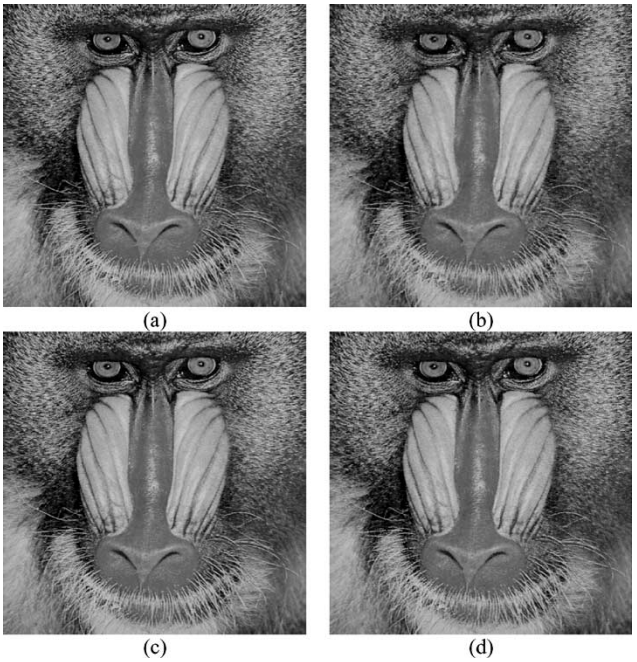

Fig. 3. (a) Original cover-image; (b) stego-image with PSNR $= 34.1444$ dB, $L = 1024$ bits; (c) stego-image with PSNR $= 31.3183$ dB, $L = 2048$ bits; (d) stego-image with PSNR $= 28.2366$ db, $L = 4096$ bits.

authenticating the identification of the sender. Another advantage is that the two-fold operation also secures this method from exhaustive and inverse attacks. The chaos cipher-message provided by the confusion and diffusion of a chaotic map is similar to that in cryptography but is not vulnerable to the flipping-attack. Consequently, it is appropriate to use DTDS for steganography because of the ability of distortion tolerance and cryptographic-like properties.

Based on the above discussion, the CAS scheme uses adaptive modification to make the embedded message undetectable and imperceptible. Asymmetric orbits then make the extracted chaos cipher-message not vulnerable to security attacks and fraud problem. Hence, we believe the proposed scheme is secure.

C. Imperceptibility

This subsection demonstrates the imperceptibility of the CAS scheme. Figs. 2(a) and 3(a) display test images of size 512×512 entitled Lena and Baboon, respectively. Messages of various lengths were hidden in these images to test the relationship between image quality and capacity. Table I illustrates the peak signal-to-noise ratio (PSNR) values of the stego-images. For each test image, the PSNR values were measured using both the CAS method and the downgrading method [4] to provide a comparison. Fig. 2(b) displays the stego-image (Lena) produced using the CAS method. The PSNR value is 38.6432 dB when the embedded message length is 1024 bits, and the quality of the stego-image is very close to that of the original image. Fig. 2(c) and (d) show two stego-images with PSNR values of 35.5419 dB and 32.5876 dB, respectively. Generally, the higher the PSNR value, the better the image quality. The measurements reveal that the quality of the stego-image declines with the number of bits embedded in the cover-image. However, the PSNR values were acceptable in all cases.

Fig. 3(b) shows another stego-image (Baboon) produced using the CAS method, with a PSNR value of 34.1444 dB. Fig. 3(c) and (d) show other stego-images with PSNR values of 31.3184 dB and 28.2366 dB, respectively. Clearly, all of these stego-images have good quality and are free of visible artifacts after the embedding. In Fig. 3(d), the stego-image has a lower PSNR value because of having more edge regions and a larger embedded message than other images. Notably, heavily textured images have the luminance edges to reduce the visibility and suspicion of the other signals around them; even more amendments and large messages are applied.

We observed that even for embedded messages up to 4096 bits in size, the image quality of the stego-image remains good when the downgrading method is used. This phenomenon occurs because the downgrading method only modifies four LSB bits from each selected pixel, and the modification ranges from 0 to 15. Although the PSNR value of the downgrading method is better than that of the CAS scheme, almost no visual artifacts exist between the stego-images and their original images when the CAS scheme is applied.

In the CAS scheme messages were also embedded into the cover-images using different stego matrices to exhibit the one-time pad property and to examine the imperceptibility of the embedded messages. The PSNR results listed in Table II show the quality of the stego-images measured with different randomly generated stego matrices. For each image, the embedded messages are 1024, 2048, and 4096 bits with different stego matrices. The measured quality differences among the images are imperceptible, and range between around $0.02 \sim 0.05$ dB with Lena and $0.23 \sim 0.29$ dB with Baboon. The measurements reveal that the quality of a stego-image is

TABLE I
COMPARISONS OF LSB SCHEME AND THE CAS SCHEME

Stego-images	L = 1024 bits	L = 2048 bits	L = 4096 bits
The method [4] (Lena)	53.6442	50.1237	47.4257
The method [4] (Baboon)	53.3499	50.2320	47.2027
CAS scheme (Lena)	38.6432	35.5419	32.5876
CAS scheme (Baboon)	34.1444	31.3183	28.2366

TABLE II
COMPARISONS OF EMBEDDING RESULTS USING DIFFERENT STEGO-MATRICES

Stego-images	L = 1024 bits	L = 2048 bits	L = 4096 bits
Stego matrix 1 (Lena)	38.6660	35.5013	32.5648
Stego matrix 2 (Lena)	38.6432	35.5419	32.5876
Stego matrix 1 (Baboon)	34.1444	31.3183	28.2366
Stego matrix 2 (Baboon)	33.8564	31.0215	28.0072

maintained by using different stego matrices. The distortions are so small that different stego matrices can provide unconditional security without reducing the imperceptibility.

D. Survivability

The stego-image must be resistant to added noise in a noisy channel. The Reed–Solomon (RS) ECC with symbols from $\mathrm{GF}(2^m)$ and RS (N, K) decode symbol errors correctly provided they are below $(N+1-K)/2$. This work uses the RS (31, 25) that has the ability of correcting three symbol errors. The tolerant bit-error rate (BER) is 0.0193, the maximum bit-error rate (MBER) is 0.0968, and the message payload is 0.8065. The normal distribution noise of $N(0, \delta^2)$ was added to the Lena stego-image, which embedded a message with a length of 1024 bits. The extracted BER was 0.0086 with added noise power $\delta = 10$, and increased to 0.0981 when the added noise power was increased to $\delta = 20$, slightly exceeding the MBER threshold for correction used here. However, increasing added noise power to $\delta = 30$ caused extracted BER to increase to 0.2274, and thus a stronger ECC code could be effective in coping with more added noise to ensure error-free message recovery. The same noise powers were added to the Baboon stego-image, in which case the extracted BER results were 0.0086, 0.0922, and 0.2048, respectively. These BER results indicate that the Baboon stego-image is more resistant to added noise than that of the Lena stego-image.

Moreover, JPEG compression with different quality factors (QF) was applied to stego-images to test images resistance to compression. Fig. 4 illustrates the BER values of messages of various lengths extracted from the compressed Lena stego-image. The figure shows that the BER is zero when the QF exceeds 60. Meanwhile, reducing the QF to 20 produces $0.8304 \sim 0.9416$ bits/pixel compressed images with BER values between 0.0726 and 0.0895, within our MBER range. Finally, decreasing QF to 10 produces the BER values of 0.1328 to 0.1783, beyond the MBER threshold. As noted previously, higher correcting code rates could be useful in correcting errors, but will reduce the message payload.

Fig. 5 shows the BER values of messages of various lengths extracted from the compressed Baboon stego-image. The resistance to JPEG compression is very similar to that for the Lena

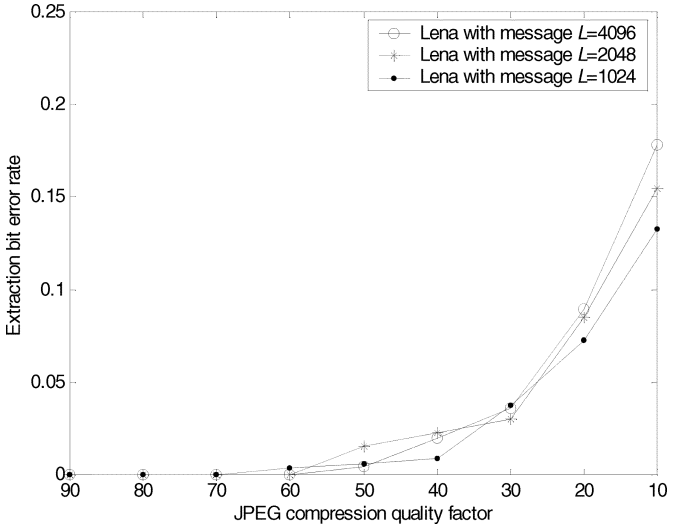

Fig. 4. BER results in comparison of JPEG compressed Lena stego-image with decreasing qualities.

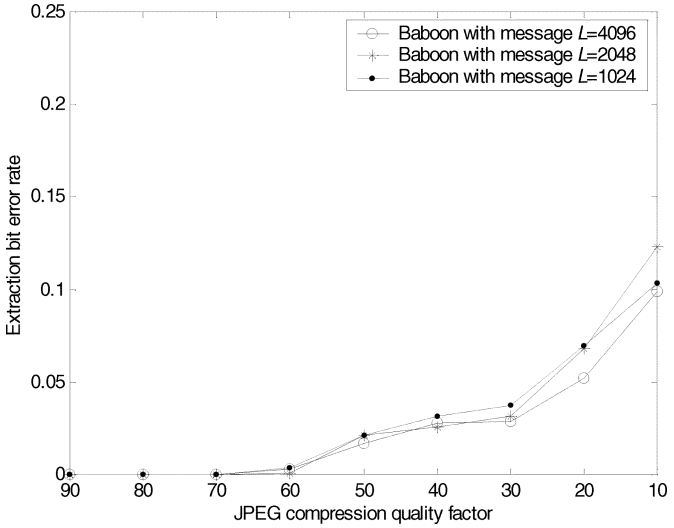

Fig. 5. BER results in comparison of JPEG compressed Baboon stego-image with decreasing qualities.

stego-image. Notably, the image with more edge regions has better resistance to JPEG compression and added noise. The resistibility characteristic yields a low BER given low QF compression and high noise power. In contrast, minor JPEG compression and added noise is sufficient to disable the bit plane of the embedded messages produced using the method in [4]. Hence, we believe that the CAS scheme can survive a noisy transmission channel.

E. Computational Costs

The stego-image capacity generally increases with the size of the cover-image. However, chaotic mapping computations also increase with large images, and this cost must be carefully considered for given applications. For example, if the content of the embedded message is time-dependent, the computational costs for the receiver to receive the message should be lower than that for the attacker to decode the message.

When the exponent e is a positive integer that exceeds than 512 bits, the operation of $\mathbf{S}^e(\mathrm{mod}n)$ is time-consuming. A binary method [20] can speed up the calculation, which scans the bits of the exponent e from left to right rather than multiplying $\mathbf{S}$ sequentially for e times. On average, the binary method can perform $\mathbf{S}^e$ in $1.5 * k$ multiplication rather than e multiplications, where k denotes the bit-length of exponent e in the binary representation [21]. Clearly, $e \gg 1.5 * k$ when e is a 512-bit number. Hence, the binary method effectively reduces the computational costs of the CAS scheme in real applications.

V. Conclusions

This work presents an asymmetric methodology for images steganography based on the chaotic dynamic system and the Euler theorem. This CAS scheme uses the local characteristics of image blocks to conceal secret messages inside a cover-image without increasing the dynamic range of the image content. The cover-image is not required to extract the hidden message. Meanwhile, the asymmetric orbits mean the steganography is designed such that an adversary is unable to use either of the keys to determine the other key. Combining both the encryption and signature in the secret data allows the receiver to assure the correctness and trustworthiness of the received data through decryption and authentication operations. A two-fold operation secures this method against exhaustive and inverse attacks, and verification of sender and receiver identification prevents fraud. An eavesdropper will be unable to decipher embedded messages because the permutation orbits of the embedding are not identical to those of extraction processes.

The performance of the CAS scheme was verified using messages with various lengths embedded into various images to produce stego-images. The stego-images do not differ significantly from the cover-images, reducing detection probability and leaving the observer unaware of the embedded data. The ability of this method to cope with added noise and JPEG compression affords to transmit stego-images over a noisy transmission channel. Moreover, the method presented here could be extended to color images to increase the total message payload.

Acknowledgment

The authors thank the anonymous reviewers and the Associate Editor for their valuable suggestions and many constructive comments that resulted in the improvement and readability of this paper.

References

[1] M. Y. Rhee, *Cryptography and Secure Communications*. New York: McGraw-Hill, 1994.
[2] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signature and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, 1978.
[3] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding-a survey," *Proc. IEEE*, vol. 7, pp. 1062–1078, July 1999.
[4] C. Kurak and J. McHugh, "A cautionary note on image downgrading," in *Proc. Computer Security Applications*, 1992, pp. 153–59.
[5] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," *IBM Syst. J.*, vol. 35, pp. 313–336, 1996.
[6] K. Matsui and K. Tanaka, "Video-steganography: How to secretly embed a signature in a picture," in *Proc. IMA Intellectual Property Project*, vol. 1, 1994, pp. 187–205.
[7] L. M. Marvel, C. G. Boncelet, and C. T. Retter, "Spread spectrum image steganography," *IEEE Trans. Image Processing*, vol. 8, pp. 1075–1083, Aug. 1999.
[8] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Processing*, vol. 6, pp. 1673–1687, Dec. 1997.
[9] C.-S. Lu, S.-K. Huang, C.-J. Sze, and H.-Y. M. Liao, "Cocktail watermarking for digital image protection," *IEEE Trans. Multimedia*, vol. 2, pp. 209–224, Dec. 2000.
[10] D.-C. Lou and J.-L. Liu, "Fault resilient and compression tolerant digital signature for image authentication," *IEEE Trans. Consumer Electron.*, vol. 46, pp. 31–39, Feb. 2000.
[11] D.-C. Lou and T.-L. Yin, "Adaptive digital watermarking using fuzzy clustering technique," *IEICE Trans. Fund. Electron., Commun., Comput. Sci.*, vol. E84-A, no. 8, pp. 2052–2060, Aug. 2001.
[12] I. J. Cox, M. L. Miller, and J. A. Bloom, "Watermarking applications and their properties," in *Proc. Int. Conf. Information Technology: Coding and Computing 2000*, Mar. 2000, pp. 6–10.
[13] G. J. Simmons, "The prisoners' problem and the subliminal channels," in *Proc. Annu. Int. Cryptology Conf.*, Santa Barbara, CA, 1984, pp. 51–67.
[14] R. L. Devaney, *An Introduction to Chaotic Dynamical System*. Redwood City, CA: Benjamin Cummings, 1986.
[15] F. J. Dyson and H. Falk, "Period of a discrete cat mapping," *Amer. Math. Mon.*, vol. 99, pp. 603–624, Aug.-Sept. 1992.
[16] R. J. Anderson and F. A. P. Petitcolas, "On the limits of steganography," *IEEE J. Select. Areas Commun.*, vol. 16, pp. 525–539, 1998.
[17] L. M. Konfelder, "On the signature reblocking problem in public-key cryptosystem," *Commun. ACM*, vol. 21, no. 2, p. 179, 1978.
[18] J. Zollner, H. Federrath, H. Klimant, A. Pfitzmann, R. Piotraschke, A. Westfeld, G. Wicke, and G. Wolf, "Modeling the security of steganographic systems," in *Proc. Second Workshop on Information Hiding*, Apr. 1998, pp. 344–354.
[19] N. Johnson and S. Jajodia, "Steganalysis of images created using current steganography software," in *Proc. Second Workshop on Information Hiding*, Apr. 1998, pp. 273–289.
[20] D. E. Knuth, *The Art of Computer Programming*. Reading, MA: Addison-Wesley, 1969, vol. II.
[21] D.-C. Lou and C.-C. Chang, "Fast exponentiation method obtained by folding the exponent in half," *Electron. Lett.*, vol. 32, no. 11, pp. 984–985, May 1996.

Der-Chyuan Lou was born in Chiayi, Taiwan, R.O.C., on March 18, 1961. He received the B.S. degree from the Chung Cheng Institute of Technology (CCIT), Taoyuan, Taiwan, in 1987, and the M.S. degree from the National Sun Yat-Sen University, Kaohsiung, Taiwan, in 1991, both in electrical engineering. He received the Ph.D. degree in 1997 from the Department of Computer Science and Information Engineering at the National Chung Cheng University.

Since 1987, he has been with the Department of Electrical Engineering, CCIT, National Defense University, where he is currently a Professor and the Director of the Computer Center of CCIT. His research interests include cryptography, steganography, algorithm design and analysis, computer arithmetic, parallel and distributed system. He is currently an Area Editor for security technology of the *Journal of Systems and Software*.

Dr. Lou is an honorary member of Phi Tau Phi, and a member of the IEICE Society and the Chinese Cryptology and Information Security Association. He is a recipient of research award that granted by the National Science Council of Taiwan in 1992 and 1993, respectively. He is the owner of the 11th AceR Dragon Ph.D. Dissertation Award. He has been selected and included in the 15th and 18th editions of *Who's Who in the World*, in 1998 and 2001, respectively.

Chia-Hung Sung was born in Chiayi, Taiwan, R.O.C., in 1966. He graduated from the Air force Institute of Technology, Kaohsiung, Taiwan, in 1988 and received the M.S. degree in computer science and information engineer from the National Chung Cheng University, Taoyuan, Taiwan, in 1997. He is currently pursuing the Ph.D. degree in electrical engineering with the Chung Cheng Institute of Technology, National Defense University, Taoyuan. His research interests include image compression, cryptography, and steganography.