Research on the Security Algorithm of Reversible Information Hiding in Communication Encrypted Image

Jijun Wang*, SooFun Tan, Yi Yuan
Faculty of Computing and Informatics, University Malaysia Sabah (UMS), Sabah, Malaysia

*Corresponding author: wangjijun@ums.edu.my

Abstract. Considering the embedding capacity and the security of the algorithm, the paper proposes a reversible information hiding algorithm for encrypted images based on. The information concealer can find the transformed pixel group in the encrypted image according to the same key and use the embedding key to replace the corresponding pixel's LSB to complete the reversible embedding of secret information. Simulation tests show that the proposed hiding method can realize the lossless recovery of the carrier image and the original image, which effectively reduces the transmission load and has high security.

Keywords: Image encryption, information hiding, differential expansion.

1. Introduction
In recent years, cloud storage and Internet services have become very popular all over the world. While providing people with information storage convenience, they have also brought problems such as data leakage and information tampering. Therefore, preventing information leakage has become the focus of the attention of individuals and organizations. Data encryption and hiding techniques are practical tools to provide security for these multimedia data. This paper intends to present a reversible information hiding technology based on chaotic systems and, including chaotic encryption and information hiding. The improved chaotic system is used to generate a chaotic encryption watermark. Then, the difference expansion and threshold between the carrier image's adjacent pixels are used to hide the chaotic encryption information into the carrier image to achieve the double encryption effect [1]. There is no need to record the correspondence table to retrieve confidential information and recover the carrier image in the recovery phase, only the least significant bit (LSB) of the block pixel that cannot be hidden in the recording part, which reduces the storage space.

2. Two-way chaotic security algorithm

2.1. Laser chaotic all-optical bidirectional chaotic security system
The chaotic system model based on the all-optical mutual coupling semiconductor laser is shown in Figure 1. The output lights of the two semiconductor lasers SL1 and SL2 under their respective bias currents are injected into each other at the same time, forming a mutual coupling system.
The rate equations describing the two-way chaotic synchronization system are:

\[
\frac{dE_1(t)}{dt} = \frac{1}{2(1+ia_1)} \left[ G_1 - \frac{1}{\tau_{p1}} \right] E_1(t) + \frac{k}{\tau_n} E_2(t-\tau) + \sqrt{2\beta N_1(t)} \xi_1, \tag{1}
\]

\[
\frac{dE_2(t)}{dt} = \frac{1}{2(1+ia_2)} \left[ G_2 - \frac{1}{\tau_{p2}} \right] E_2(t) + \frac{k}{\tau_n} E_1(t-\tau) + \sqrt{2\beta N_2(t)} \xi_2.
\]

In the formula, the subscripts 1 and 2 respectively represent the two mutually coupled lasers SL₁, SL₂, E and N are the slowly varying complex amplitude. The number of carriers in the active layer of the laser, respectively, is α the linewidth enhancement factors and \(\tau_{p1}, \tau_{p2}\) are the photon lifetimes, respectively. And carrier lifetime, f is the free-running frequency of SL, \(\Delta f (\Delta f = f_1 - f_2)\) is the frequency detuning between SL₁, SL₂, \(\tau_n\) is the round-trip time in the cavity, k and \(\tau\) are the coupling coefficient and coupling delay time between the two lasers, and i is Current, e is the unit charge, \(\beta\) is the spontaneous emission rate, and \(\xi\) is the field amplitude Gaussian white noise. G is the gain, which can be expressed as

\[
G_{i,j} = g_{i,j} \left( N_{i,2} - N_0 \right) \quad \text{(2)}
\]

In the formula, g is the linear gain coefficient, s is the gain saturation coefficient, and \(N_0\) is the number of transparent carriers.

2.2. Two-way chaotic security system based on incoherent optical feedback

In the study of two-way chaotic communication systems based on incoherent optical feedback semiconductor lasers, since the system's output is insensitive to phase, it is easier to achieve good synchronization than optical feedback systems [2]. On the other hand, incoherent optical feedback systems are all-optical systems. Not limited by the bandwidth of electronic devices, it can meet the needs of information transmission, so we propose a two-way chaotic communication system based on incoherent optical feedback. The model is as follows:
In the above system architecture, the dynamic behavior of the laser can be described by the following rate equation:

\[
\begin{align*}
\frac{dP}{dt} &= (G_i - \gamma_p) P_i(t) + \beta_i N_i(t) + F_i(t) \\
\frac{dN}{dt} &= \frac{I}{e} - \gamma_s N_i(t) - G_i \left[ P_i(t) + k_i (t - \tau_i) + \sigma_i P_i(t - \tau_s) \right]
\end{align*}
\]  

(3)

In the formula, subscripts 1, 2 correspond to SL, SL respectively, P is the number of photons in the laser cavity, N is the number of carriers, N0 is the number of transparent carriers, \( \gamma_p \) is the photon lifetime, I is the injected current, and e is the electron charge, K is the feedback coefficient, \( \sigma \) is the injection coupling coefficient, \( \tau \) is the optical feedback delay time, \( \tau_s \) is the injection coupling delay time, \( \beta \) is the spontaneous radiation rate, and F is the Langevin noise. When there is no parameter mismatch, the system can achieve high-quality chaotic synchronization without delay and can successfully achieve two-way real-time communication; parameter mismatch has a particular impact on the synchronization performance and communication quality of the system, but the internal parameter mismatch of the laser is within \( \pm \) in the range of 10\%, the system correlation coefficient is above 0.86, which has good synchronization performance, so the system can successfully recover the signal and realize two-way communication.

3. Information hiding

According to the algorithm principle of the reversible conversion function concealment proposed by Alattar, a method of using odd and even numbers to determine whether to hide confidential information is proposed, and this method is used to solve the problem of additional transmission of a large number of correspondence tables in the literature [3]. First, use the improved Henon chaotic encryption algorithm in Chapter 2 to encrypt the watermark data into chaotic encryption information, and then use the proposed information hiding algorithm to embed the chaotic encryption information into the carrier image to achieve the effect of double encryption and further improve the security of the watermark information. The schematic diagram of information hiding is shown in Figure 3.
According to the schematic diagram of Fig. 3, after the carrier image is divided into blocks, the chaotic encrypted bit information is embedded into the last 3 pixels of the sub-block through the consistent numbering, difference expansion, and parity embedding methods. The first pixel is used as the flag bit for embedding information, and only the lowest bit that cannot be embedded in the first pixel in the information block needs to be recorded [4].

3.1. Concealment technology

Concealment is the earliest proposed chaotic secure communication method, also known as chaotic concealment or concealment. At the sending end, the basic idea is to use chaotic signals as carrier waves to hide the transmitted signals or conceal the information to be transmitted. In this, chaotic signals are a kind of carrier, and at the receiving end, the synchronized chaotic signals are demodulated, thereby demodulate to recover the information to be transmitted [5]. There are three main ways of concealment in chaotic concealment technology: addition, multiplication, or a combination of addition and multiplication. Use the synchronized chaotic signal to perform the corresponding inverse operation to recover useful information at the receiving end. The realization degree of chaotic system synchronization depends on the realization degree of this communication method.

Add: \[ AB(t) = A(t) + B(t) \]

Multiply: \[ AB(t) = A(t)B(t) \]

Combination of addition and multiplication: \[ AB(t) = [1+kA(t)] B(t) \]

For the chaotic concealed secure communication system, to ensure that the chaotic signal does not deviate from the original chaotic trajectory, the signal's amplitude to be transmitted is generally small. However, channel noise always exists in the communication system. If the transmitted signal's amplitude is small, it is easy to be interfered with by channel noise. Therefore, chaotic concealment is very sensitive to channel noise and is limited by the line bandwidth, and confidentiality is also low. There are difficulties in practical applications. It is only suitable for slow-changing signals and cannot be handled well. Fast-varying signals and time-varying signals [6].

This chaotic concealment communication method's characteristics are: chaotic concealment sends analog signals directly, and the implementation is simple; but it requires strict synchronization of the chaotic system at the sender and receiver and to ensure the security of confidential communication, it requires the information signal. The power is much lower than the power of the chaotic mask signal. Otherwise, it will not be guaranteed, and its security will be significantly affected. It must meet for a secure communication system: First, a high degree of fidelity and the recovered signal distortion...
should be as small as possible. The signal demodulated by the receiving end should be consistent with the useful signal covered by the transmitting end; the second is a high degree of security. Therefore, it is difficult for illegal signal stealers to demodulate the signal covered by the intercepted signal's starting end. To solve this kind of communication system's problems and make the system have higher fidelity and security, Kuang Jinyu proposed multi-stage concealing communication system in 1999. The system also designed two-stage at the sending end and the receiving end. The system improves the fidelity and safety of the system.

3.2. Parameter modulation technology
Amplitude modulation, frequency modulation, and phase modulation are three basic modulation methods that modulate the amplitude, frequency, or phase of a carrier wave with analog or digital signals transmitted in traditional communication systems. In a chaotic communication system, analog or digital signals to be sent can also be used to modulate various parameters of the chaotic signal carrier, resulting in various methods of chaotic parameter modulation. The basic idea of the chaotic parameter modulation technology is: use the signal transmitted by the transmitter to modulate the parameters of the chaotic system and use the chaotic synchronization signal at the receiving end to extract the corresponding chaotic system parameters and then recover the transmitted signal.

4. Simulation experiment
Select the threshold range to meet the conditions of \(|T_{n-1}| > T_P, T_n < 0, T_p > 0\), as far as possible to meet the threshold of 0 pixels in the middle. The experiment takes \([-2, 1]\) as an example, Pixels in the range can be represented by 2-bit binary numbers, and the remaining six bits can be used to embed information. The test image is a 512×512 uncompressed grayscale image. To prove that this paper's encryption algorithm can resist the ciphertext attack, Lena, Airplane, and Barbara in the test image are selected to extract the high eight bits of the sampled pixels, and the classification scrambling encryption of literature and this paper are used, respectively. Use the method of literature to conduct a COA attack on the encrypted high eight-bit image. Here, only 10 known images are selected to use document XOR encryption, and this text classification scrambling encryption to be encrypted to estimate the random number used for XOR encryption [7]. Table 1 shows the similarity between the estimated random number and the original random number.

| Image | Algorithm | Similarity (%) |
|-------|-----------|----------------|
| Lena  | Ref. [2]  | 94.08          |
|       | Proposed  | 50.26          |
|       | Ref. [2]  | 90.01          |
|       | Proposed  | 50.22          |
| Airplane | Ref. [2]  | 90.00          |
|       | Proposed  | 51.01          |
| Bar   | Ref. [2]  | 90.00          |
|       | Proposed  | 51.01          |

The results of Table 1 show that the encryption algorithm only uses the XOR encryption algorithm in the literature, and the random number of XOR encryption can be estimated with 10 known images, and the similarity is as high as 90%. Because the algorithm in this paper disrupts the correlation between pixels, the COA attack method cannot estimate the random number used for encryption and cannot decrypt the plaintext content.

5. Conclusion
This paper proposes a reversible information hiding algorithm for encrypted images based on. The algorithm has the characteristics of large capacity and high security. The content owner can select two adjacent pixels as a group for through the key. After the transformation, the two adjacent pixels in the pixel group are constrained by the characteristics so that the original pixel can still be restored after the
LSB of one of the pixels is replaced. Therefore, the information concealer finds the transformed pixel group in the encrypted image according to the same key and uses the embedding key to replace the LSB of the designated pixel in each pixel group to complete the information embedding. Only by possessing both the change key and the embedded key can the embedded information be correctly extracted from the ciphertext image; only when the receiver has both the change key and the encryption key can the recipient recover the original image losslessly. After the experimental comparison, the algorithm in this paper has a high embedding rate. While ensuring a large embedding capacity, it can strengthen embedded information protection, which has a particular significance for ciphertext data management.

Acknowledgements
This work was supported by Young and Middle-aged Teachers' Ability Improvement Project of Guangxi (2020KY16021), Research Fund of Guangxi Key Lab of Multi-source Information Mining & Security (MIMS18-05), School of Information and Statistics, Guangxi University of Finance and Economics (2019XTZZ11)

The authors would like to thank the anonymous reviewers for their valuable suggestions.

References
[1] Kadhim, O. N., & Hussain, Z. M. Information Hiding using Chaotic-Address Steganography. J. Comput. Sci, 14(9) (2018) 1247-1266.
[2] Taheri, M., & Mozaffari, S. Phase mask generation for DRPE method using and hash function. Optik, 124(16) (2013) 2363-2367.
[3] Anwar, S., & Meghana, S. A pixel permutation based image encryption technique using chaotic map. Multimedia tools and applications, 78(19) (2019) 27569-27590.
[4] Muhammad, K., Ahmad, J., Rehman, N. U., Jan, Z., & Sajjad, M. CISSKA-LSB: color image steganography using stego key-directed adaptive LSB substitution method. Multimedia Tools and Applications, 76(6) (2017) 8597-8626.
[5] Peng, F., Lin, Z. X., Zhang, X., & Long, M. Reversible data hiding in encrypted 2D vector graphics based on reversible mapping model for real numbers. IEEE Transactions on Information Forensics and Security, 14(9) (2019) 2400-2411.
[6] Chuang, C. H., & Chen, Y. L. Steganographic optical image encryption system based on reversible data hiding and double random phase encoding. Optical Engineering, 52(2) (2013) 028-033.
[7] Lei, B., Tan, E. L., Chen, S., Ni, D., Wang, T., & Lei, H. Reversible watermarking scheme for medical image based on differential evolution. Expert Systems with Applications, 41(7) (2014) 3178-3188.