# A Image Adaptive Steganography Algorithm Combining Chaotic Encryption and Minimum Distortion Function

Ge Jiao[1,2](✉), Jiahao Liu[1], Sheng Zhou[1], and Ning Luo[1]

[1] College of Computer Science and Technology, Hengyang Normal University,
Hengyang 421002, China
jiaoge@126.com
[2] Hunan Provincial Key Laboratory of Intelligent Information Processing and
Application, Hengyang 421002, China

**Abstract.** Digital image has the characteristics of high redundancy and convenient processing, which is the ideal carrier of information hiding application. Therefore, digital image steganography has become a hot research direction in the field of information security. In order to ensure the concealment, reliability and security of image steganographic information, an image adaptive steganographic algorithm combining chaotic encryption and minimum distortion function is designed. The algorithm generates random keys, encrypt the secret information using Logistic and ChebyShev mapping, and then embeds the key and the encrypted secret information into the carrier image using the HILL steganographic algorithm. The algorithm stores the embedded key and the decryption key separately, so the attacker cannot get the correct secret information even if he gets the embedded key, which improves the security of the key. Experiments show that the pixel change rate of the algorithm is 6.76%, the peak signal-to-noise ratio is 59.51 db, and it has a very good anti-steganographic analysis ability.

**Keywords:** Image adaptive steganography · Chaotic encryption · Cost · PSNR

## 1 Introduction

Steganography is a technique and science of information hiding, which means that no one other than the intended recipient is aware of the event or content of the transmission of information. Image steganography is a kind of covert communication technology in which secret messages are embedded in image carriers for information transmission. The early non-adaptive image steganographic methods mainly include LSB [1], F5 [2], OutGuess [3], MB [4], nsF5 [5], etc. These algorithms have the advantages of simple design and easy operation, but poor security.

In recent years, with the development of the steganographic techniques, adaptive steganography has gradually become a hot research direction in the field of current image steganography. Combined with the structural characteristics of the image itself, the algorithm adaptively selects the regions in the image that are relatively difficult to detect and insensitive to embed the message, which preserves the more complex image

Q. Liu et al. (Eds.): CENet 2020, AISC 1274, pp. 733–740, 2021.
https://doi.org/10.1007/978-981-15-8462-6_84

statistical characteristics and greatly improves the security of steganography. The algorithm is combined with the structure of the image features itself, adaptive selection is relatively difficult to detect, not sensitive areas of the image for message embedding, retain the more complex the statistical properties of the image greatly improves the security of steganography. At present, several mainstream adaptive stegographic algorithms, such as HUGO [6], WOW [7], S-UNIWARD [8], HILL [9], MiPOD [10], are mainly based on the minimum distortion cost function. Message embedding is realized in the form of encoding through the embedded generation value of different pixels, during which the total distortion value of all pixels should be kept to the minimum, which can effectively improve the anti-detection ability and maximize the original image characteristics. Finally, the corresponding steganographic image is obtained by the adaptive steganographic coding method STC [11]. Therefore, better definition of distortion cost function can effectively improve the security of adaptive steganographic algorithm.

## 2 Preliminaries on Chaotic Systems and Image Steganography

### 2.1 Logic Map

Logistic map is a typical non-linear chaotic equation, which can generate complex chaotic behavior [12, 13]. It generated chaotic sequence has better randomness, the $x_{n+1}$ are all distributed on (0, 1) when the $\mu \in (3.5699456,4]$.

$$\mathrm{x}_{\mathrm{n}+1} = \mu \mathrm{x}_{\mathrm{n}}(1 - \mathrm{x}_{\mathrm{n}}),\ \mathrm{x}_{\mathrm{n}} \in (0, 1) \tag{1}$$

### 2.2 ChebyShev Map

ChebyShev map has good initial sensitivity and long-term unpredictability of chaotic sequences, which is in chaos when $\mathrm{k} \geq 2$ [14, 15].

$$\mathrm{x}_{\mathrm{n}+1} = \cos(\mathrm{karccos}(\mathrm{x}_{\mathrm{n}})),\ \mathrm{x}_{\mathrm{n}} \in [-1, 1] \tag{2}$$

### 2.3 HILL-Based Minimized Distortion Function

HILL algorithm is a steganographic algorithm with excellent detection resistance and computational speed under minimum embedded distortion system. Compared with WOW algorithm, HILL algorithm uses a smaller and more concise filter. The HILL algorithm uses a high pass filter to determine the texture area and two low pass filters to aggregate the pixels with lower modification costs. The formula for calculating the modification cost for the HILL algorithm is shown below.

$$D(x,y) = \sum\nolimits_{i=1}^{n} \rho_i(x_i, y_i) \tag{3}$$

where, x = ($x_1$, $x_2$, …, $x_n$) is the carrier image to be embedded, y = ($y_1$, $y_2$, …, $y_n$) is the embedded secret image, and p($x_i$, $y_i$) is the distortion cost of modifying the ith carrier pixel $x_i$ to $y_i$.

### 2.4 Syndrome-Trellis Codes (STC)

STC code is binary steganographic code, and the calculation formula is as follows:

$$Emb(c,m) = \arg \min d(c,s) \tag{4}$$

The encoding process is the process of finding the code word s with the minimum hamming distance from carrier *c* in the cosset of the secret message *m*. After receiving *s*, the receiver can multiply *H* to obtain the secret message *m*. Where, *d(c, s)* is the hamming distance between *c* and *s*, and *H* is the check matrix of parameters Shared by both receiving and receiving parties.

## 3 Design and Implementation of Image Adaptive Steganography Algorithm

Our algorithm uses the Logistic and ChebyShev maps to the secret information is encrypted, according to the image noise and texture complexity, HILL cost function is used to calculate the corresponding embedding cost, and then the key and the encrypted secret information is embedded into the carrier image, statistics the total image distortion, to use on STC embedded coding minimizes the distortion in order to get the secret image. The algorithm process is as follows [16–18]: (see Fig. 1).

(1) Convert secret information into ASCII code *A[M*N]* by character;

(2) Convert *A[M*N]* into binary sequence *B[M*N]*;

(3) Randomly generated two keys are $key_L$ ($key_L \in (0,1)$) and $key_C$ ($key_C \in [-1,1]$), where $key_L$ is the initial key for Logistic mapping and $key_C$ is the initial key for ChebyShev mapping.

(4) Take $key_L$ as the initial key, use Logistic mapping to iterate for 100 times (eliminate the influence of transient), and use ChebyShev to iterate for 1 more time, and save the result in $C_x$.

(5) Take $key_C$ as the initial key, iterate 100 times with ChebyShev mapping (eliminate the influence of transient), take the absolute value of the result, use Logistic iteration for 1 time, and save it in $L_x$.

(6) Extract elements from *B[M*N]*. If the position number of this element is odd, then use ChebyShev chaotic map to iterate with $C_x$ as the initial key, and record the result of each iteration as the next odd element point iteration encryption; If the element's position number is even, Logistic chaos mapping is used to iterate with $L_x$ as the initial key, and the result of each iteration is recorded as the element point corresponding to the next even number point.

(7) Take the element point being encrypted and the element point at the previous position for xor operation;
(8) Repeat steps (6) and (7), and finally output ciphertext *A'*;
(9) Obtain the carrier image and extract the pixel matrix *I*;
(10) Use the HILL cost function to embed the key and encrypted secret information into the carrier image *I' = HILL(I, A')*;
(11) The corresponding steganographic image *SI = STC(I')* was obtained by the adaptive steganographic coding method STC.
(12) Obtain the carrier image and extract the pixel matrix with the embedded key;
(13) Extract key and secret information;
(14) Use the key to decrypt the secret information through the decryption algorithm;
(15) Convert binary secret information into a string, that is, decrypted information.

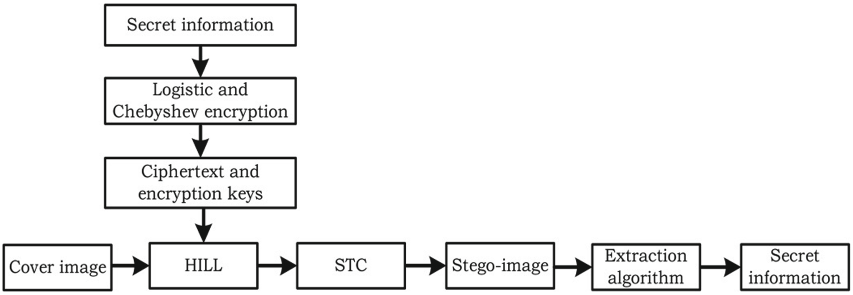


**Fig. 1.** Image steganography and steganalysis algorithm flow chart.

# 4 Experimental Results and Analysis

## 4.1 Imperceptibility Analysis

Imperceptibility refers to the comparison between the densified image and the original image to see whether it can achieve an indistinguishable effect, which is the simplest evaluation method for the image steganographic algorithm. Figure 2 shows the carrier image and the corresponding steganographic image, which show no difference from the naked eye.

## 4.2 Pixels Change Rate

The pixel change rate is one of the indicators to judge the steganographic algorithm of images. By comparing the pixel change rate between the original image and the densified image, we can see the change size of the whole image and the original image before and after embedding. The larger the pixel change rate is, the more the image changes and is more vulnerable to hackers and viruses. It can be seen from Table 1 that the pixel change rate of the proposed adaptive steganography algorithm is lower than that of the classic LSB image steganography algorithm, and it has better anti-detection ability.

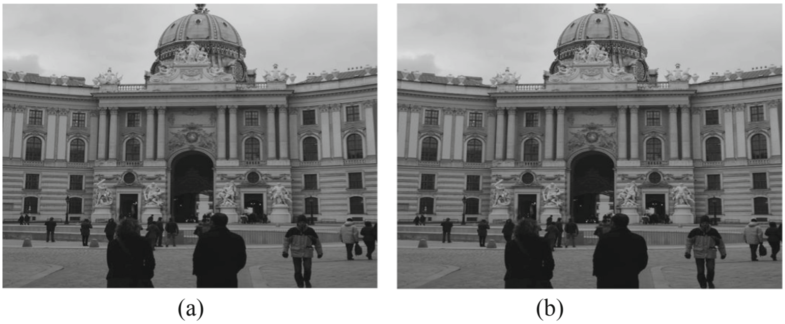


**Fig. 2.** (a) Cover image and (b) corresponding stego image.

**Table 1.** Comparison of pixel change rates based on different steganographic algorithms.

| Existing methods | Pixels change rate (%) |
|---|---|
| Classic LSB [19] | 52.42 |
| Ours | 6.76 |

### 4.3 PSNR

The PSNR (Peak signal-to-noise ratio) is an objective standard for image evaluation. When PSNR is greater than 38 dB, the image visual quality requirements are met.

$$MSE = \frac{1}{M \times N} \sum\nolimits_{i=1}^{m} \sum\nolimits_{j=1}^{n} [S(i,j) - C(i,j)]^2 \tag{5}$$

$$PSNR = 10 \times \lg \left[ \frac{(2^r - 1)^2}{MSE} \right] \tag{6}$$

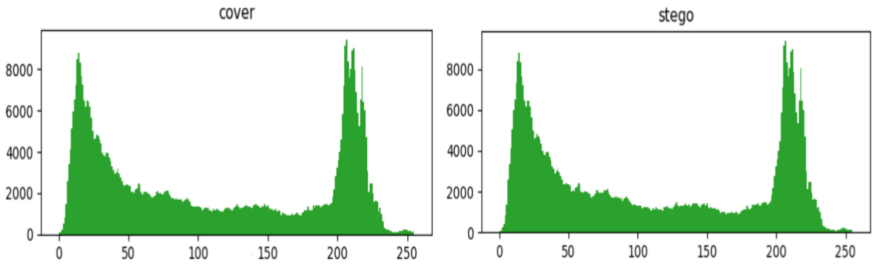
where $S$ is the densified image, $C$ is the original image, $m$ and $n$ are the height and width of the image, $r$ is the number of sampling bits of each pixel, and $MSE$ is the mean square deviation of the image. The larger the PSNR value of the image, the less distortion of the image. Table 2 shows that the PSNR of our algorithm is higher than that of reference [19–22], and slightly lower than that of reference [23]. This indicates that steganographic image distortion using our algorithm is less.

**Table 2.** Analysis of different image steganographic algorithms based on PSNR.

| No | Existing methods | PSNR values (dB) |
|---|---|---|
| 1 | Classic LSB [19] | 52.2416 |
| 2 | Karim [20] | 52.2172 |
| 3 | Channali et al. [21] | 51.9764 |
| 4 | SCC [22] | 52.2023 |
| 5 | Ours | 59.5053 |
| 6 | Khan et al. [23] | 63.0034 |

### 4.4 Histogram Analysis

Histogram describes the changes in the image and is a common method to evaluate the image processing. Figure 3 depicts the change of histogram before and after steganography. It is difficult to detect histogram changes in images after steganography with our algorithm, so there is little change in images after steganography, indicating that the algorithm has a good effect after steganography and can effectively resist attacks from statistical methods.



(a)

(b)

**Fig. 3.** (a) Histogram of the cover image and (b) histogram of the stego image.

### 4.5 Embedded Location Analysis of Secret Information

Different images have different textures, and embedding secret information in places with complex textures makes it harder to detect, in order to better deal with non-statistical attacks. The image steganographic analysis method based on convolutional neural network can extract the image features to analyze whether the image contains secret information. By comparing the embedding position of the original image and the secret information in the steganographic image, the ability of the image to resist the feature attack can be determined. Figure 4 (a) the texture of the mountains is more complex than that of the sky. The pixel value of the sky is single, while the pixel value of the mountains is rich with more changes. Our algorithm is used to embed the secret information in the mountains (see Fig. 4 (b)), which is better than the traditional LSB steganographic algorithm (see Fig. 4 (c)), so our algorithm can better resist the feature attack.

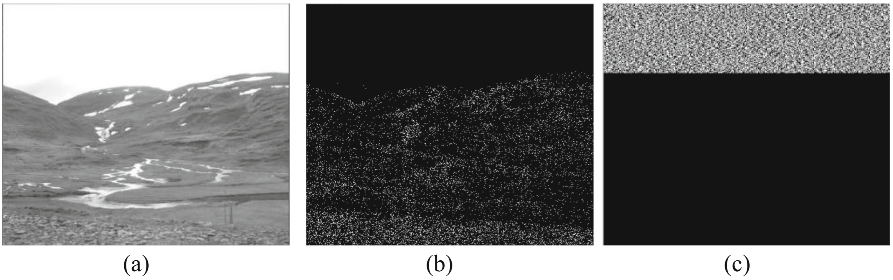


**Fig. 4.** (a) Cover image, (b) embedded pixel location based on HILL, (c) embedded pixel location based on LSB.

# 5 Conclusion

Combining chaos theory and HILL distortion function to design steganographic algorithm has the advantages of fast processing speed and high security. The algorithm uses randomly generated keys to encrypt secret information, and even the user does not know the encrypted keys, which increases the security of the algorithm. The encryption key is embedded into the densive-carrying image, and the densive-carrying image can be transmitted through the public channel due to its concealment. Even if the attacker steals the embedded key, the secret information cannot be obtained.

**Acknowledgement.** This work is supported by the Scientific Research Fund of Hunan Provincial Education Department (19B082), the Science and Technology Development Center of the Ministry of Education-New Generation Information Technology Innovation Project (2018A02020), the research supported by Science Foundation of Hengyang Normal University (19QD12), the Science and Technology Plan Project of Hunan Province (2016TP1020), the Application-oriented Special Disciplines, Double First-Class University Project of Hunan Province (Xiangjiaotong [2018] 469), the Hunan Province Special Funds of Central Government for Guiding Local Science and Technology Development (2018CT5001), the Subject Group Construction Project of Hengyang Normal University (18XKQ02).

# References

1. Petitcolas, F.A., Anderson, R.J., Kuhn, M.G.: Information hiding—a survey. Proc. IEEE **87** (7), 1062–1078 (1999)
2. Westfeld, A.: F5-a steganographic algorithm. In: International Workshop on Information Hiding, pp. 289–302. Springer, Berlin, Heidelberg (2001)
3. Provos, N.: Defending against statistical steganalysis. In: Usenix Security Symposium, vol. 10, pp. 323–336 (2001)
4. Sallee, P.: Model-based steganography. In: International Workshop on Digital Watermarking, pp. 154–167. Springer, Berlin, Heidelberg (2003)
5. Fridrich, J., Pevný, T., Kodovský, J.: Statistically undetectable jpeg steganography: dead ends challenges, and opportunities. In: Proceedings of the 9th Workshop on Multimedia & Security, pp. 3–14 (2001)

6. Pevný, T., Filler, T., Bas, P.: Using high-dimensional image models to perform highly undetectable steganography. In: International Workshop on Information Hiding, pp. 161–177. Springer, Berlin, Heidelberg (2010)
7. Holub, V., Fridrich, J.: Designing steganographic distortion using directional filters. In: 2012 IEEE International Workshop on Information Forensics and Security (WIFS), pp. 234–239. IEEE (2012)
8. Holub, V., Fridrich, J., Denemark, T.: Universal distortion function for steganography in an arbitrary domain. EURASIP J. Inf. Secur. **2014**(1), 1–13 (2014). https://doi.org/10.1186/1687-417X-2014-1
9. Li, B., Wang, M., Huang, J., Li, X.: A new cost function for spatial image steganography. In: 2014 IEEE International Conference on Image Processing (ICIP), pp. 4206–4210. IEEE (2014)
10. Sedighi, V., Cogranne, R., Fridrich, J.: Content-adaptive steganography by minimizing statistical detectability. IEEE Trans. Inf. Forensics Secur. **11**(2), 221–234 (2015)
11. Filler, T., Judas, J., Fridrich, J.: Minimizing additive distortion in steganography using syndrome-trellis codes. IEEE Trans. Inf. Forensics Secur. **6**(3), 920–935 (2011)
12. Yu, S.S., Zhou, N.R., Gong, L.H., Nie, Z.: Optical image encryption algorithm based on phase-truncated short-time fractional Fourier transform and hyper-chaotic system. Opt. Lasers Eng. **124**, 105816 (2020)
13. Zhou, N., Jiang, H., Gong, L., Xie, X.: Double-image compression and encryption algorithm based on co-sparse representation and random pixel exchanging. Opt. Lasers Eng. **110**, 72–79 (2018)
14. Zhou, N., Yan, X., Liang, H., Tao, X., Li, G.: Multi-image encryption scheme based on quantum 3D Arnold transform and scaled Zhongtang chaotic system. Quantum Inf. Process. **17**(12), 1–36 (2018). https://doi.org/10.1007/s11128-018-2104-6
15. Wen, W., Wei, K., Zhang, Y., Fang, Y., Li, M.: Colour light field image encryption based on DNA sequences and chaotic systems. Nonlinear Dyn. **99**(2), 1587–1600 (2019). https://doi.org/10.1007/s11071-019-05378-8
16. Jiao, G., Peng, X., Duan, K.: Image encryption with the cross diffusion of two chaotic maps. TIIS **13**(2), 1064–1079 (2019)
17. Jiao, G., Zhou, S., Li, L., Zou, Y.: Hybrid chaotic encryption algorithm for securing dicom systems. Int. J. Perform. Eng. **15**(5), 1436–1444 (2019)
18. Jiao, G., Li, L., Zou, Y.: Improved security for android system based on multi-chaotic maps using a novel image encryption algorithm. Int. J. Perform. Eng. **15**(6), 1692–1701 (2019)
19. Sharp, A., Qi, Q., Yang, Y., Peng, D., Sharif, H.: A video steganography attack using multi-dimensional discrete spring transform. In: 2013 IEEE International Conference on Signal and Image Processing Applications, pp. 182–186. IEEE (2013)
20. Yang, H., Sun, X., Sun, G.: A high-capacity image data hiding scheme using adaptive LSB substitution. Radio Eng. **18**(4), 509–516 (2009)
21. Channalli, S., Jadhav, A.: Steganography an art of hiding data, vol. 1, (3), pp. 137–141 (2009). arXiv preprint arXiv:0912.2319
22. Joo, J.C., Lee, H.Y., Lee, H.K.: Improved steganographic method preserving pixel-value differencing histogram with modulus function. EURASIP J. Adv. Sig. Process. **1**, 249826 (2010)
23. Muhammad, K., Sajjad, M., Mehmood, I., Rho, S., Baik, S.W.: A novel magic LSB substitution method (M-LSB-SM) using multi-level encryption and achromatic component of an image. Multimedia Tools Appl. **75**(22), 14867–14893 (2015). https://doi.org/10.1007/s11042-015-2671-9