Proceedings of the 3rd International Conference on Signal Processing and Machine Learning
DOI: 10.54254/2755-2721/6/20230370

New hide-in-dark image encryption algorithm

Hao Zhang

University of Science and Technology of China, No. 96, Jinzhai Road, Hefei City, Anhui Province, the people's Republic of China

sa1069@mail.ustc.edu.cn

Abstract. In order to protect image information, existing encryption methods pay more attention to transforming images into noise-like images with random pixels. It is acknowledged that attackers can easily notice these encrypted images for there is a striking difference between them and unencrypted ones visible to the naked eye. As a result, these noise-like images may suffer a lot of attacks which could increase the probability of information leakage. For this problem, a method based on discrete wavelet transform and previous encryption methods has been proposed which can make the encrypted images finally look like other pictures. However, the results do not have a high quality, for some obvious noise can be found in the details of the final images. In this paper, a new method called HID is introduced in which the information is hidden in a dark area. Both experimental results and security analysis prove that our method can not only transform images full of noise into meaningful images but also produce images with higher quality.

Keywords: image encryption, Discrete wavelet transform, Image embedding.

1. Introduction

In recent years, information security has been an essential topic. For example, with the development of computer science, cloud storage becomes a highly valued technology in enterprises. People can store their data (documents, videos, images) in third-party servers instead of their own servers, which saves the cost for enterprises and they can pay more attention to their core business. Apart from this, in this digital age, people usually take photos on smartphones to share their lives with others and record sweet moments. These photos could be uploaded to cloud storage and some of them are private and precious. However, data in third-party servers may be attacked. In order to preserve private and important information, some efficient and practical methods to encrypt images are needed.

However, classical data encryption technologies are not practical for image information due to redundancy and vulnerability [1-3]. An image pixel value is close to the pixels next to it. Actually, a large number of similar data being encrypted can cause a higher risk of data leakage. Thus, a safe and efficient image encryption method is especially important. A lot of existing technologies are based on changing pixels values or positions to prevent images from being attacked [4,5]. Specifically, there are two different kinds of encryption methods. One is frequency-domain image encryption and the other is spatial-domain image encryption.

Frequency-domain encryption methods are based on frequency domain data and scrambling algorithms. The first step is to get the frequency using special functions such as discrete cosine transform

DOI: 10.54254/2755-2721/6/20230370

(DCT) and discrete wavelet transform (DWT) [8]. The next step is to scramble these frequency domain data. Finally, the encrypted images are produced by inverse transformation. However, these operations can bring a disadvantage. Transforming images into the frequency domain for certain processing and inversely into the spatial domain can cause the loss of high-frequency information. In other words, frequency domain data-based methods cannot save all information of original images. However, compared to spatial domain-based methods, they are safer and can resist more and stronger attacks since attackers need to know which frequency bands are encrypted. If the frequency domain data are attacked, the content in the original images can be destroyed. Besides, they are less sensitive to noise and more robust against JPEG compression methods. In order to reduce distortion, some frequency domain methods transform images into a frequency domain in layers and blocks such as Haar domain scrambling encryption, Fibonacci-p coding-based image encryption, and matrix scrambling encryption in the DCT domain [6,7].

The spatial-domain image encryption methods usually include two steps: permutation and substitution. The former focuses on changing image pixel locations while substitution is used to change image pixel values. There are various methods based on this idea such as chaotic systems methods, scrambling encryption, and scan mode encryption [4-5,8-10]. Among these methods, chaotic systems draw much attention since they have the advantages of sensitivity to initial conditions, ergodicity, and mixing, which meet the requirements of cryptography [12-13]. Firstly, these methods usually design a new chaotic system whose chaotic behaviors are better than previous chaotic systems using classic chaotic maps such as logistic map, tent map, and sine map so as to change the image pixel values [4,14]. Secondly, a new algorithm is created to change the image pixel locations. However, these methods do not pay attention to the visual effect of encrypted images, for the final outputs of these algorithms look like random pictures and noise-like. This phenomenon is determined by the properties and purpose of these methods. There is a strong correlation between a pixel and its neighbors in a meaningful picture whereas the purpose of encryption is to destroy these correlations and make image distribution look uniform. It will lead to a problem that attackers may soon notice that this image is encrypted and try their best to decrypt it.

To solve this problem, a method was proposed by Bao that can transform noise-like images into meaningful images [15]. However, the quality of this method is not high, for some obvious noise in the details of the final results can be seen. In this paper, we proposed a new method that can transform an encrypted image into another meaningful image without loss of information in details and get higher quality. The method consists of an encryption process based on a chaotic system and an HID algorithm. The chaotic-based algorithm is used to encrypt an image which was proposed by Yicong Zhou while the HID is used to hide information in a dark area [4]. Therefore, these encrypted images get less attention from attackers. This method not only protects pictures from a data perspective but also from a visual perspective. Besides, the simulation results and security analysis are displayed. What is more, compared to Bao's method [17], our method can get clearer and higher-quality meaningful images.

This paper is organized as follows. Section 2 introduces our method for encryption in detail. Section 3 will present simulation results and then security analysis is provided in Section 4. Section 5 reaches a conclusion.

2. New hide-in-dark-based image encryption algorithm

Both frequency domain-based methods and spatial domain-based methods of image encryption tend to transform original images into random-like images. Although they are safe and efficient, the final images look like random noise and can draw much attention. If random-like encrypted images are transformed into good-looking images, they can reduce a lot of unnecessary attention so that the risk of being deciphered is decreased.

The most important problem is how to transform an encrypted image into a realistic image. This paper introduces a new image encryption method to solve this issue motivated by image hiding, image watermarking, and the method proposed by Yicong Zhou [4,16-18], as shown in figure 1. This method can be divided into four steps: encryption, DWT, HID, and inverse discrete wavelet transform (IDWT).

DOI: 10.54254/2755-2721/6/20230370

Discrete wavelet transform (DWT) is used to transform reference images into frequency domain data. If the values of high-frequency components are changed slightly, the whole image does not change obviously. Inspired by this idea, this paper hides the information of encrypted images in the dark area of high-frequency components in reference images. Ultimately, meaningful images are produced by IDWT which are similar to reference images.

As shown in figure 1, the original image is what will be encrypted while a reference image is what the final image looks like. The original image is encrypted in a spatial domain during the encryption process followed by embedding encrypted images in reference images in HID operation. As a result, the original image is protected in both spatial and frequency domains. Besides, the final image is a meaningful and good-looking image. Therefore, the original image is protected from both data and visual perspectives. Compared to existing methods, this method has less risk of leaking information.

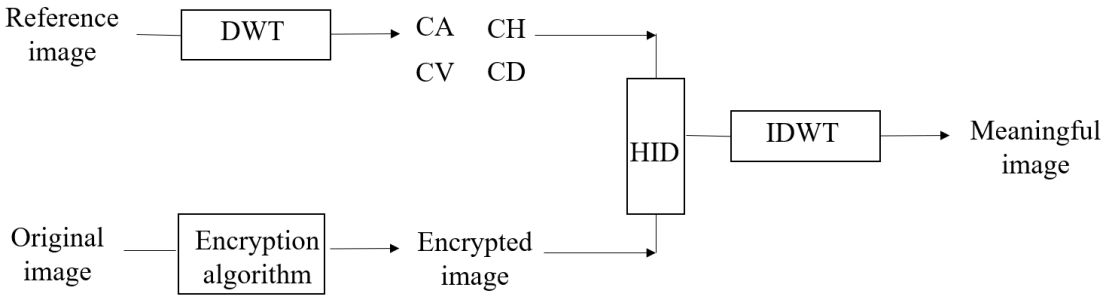


Figure 1. the flow chart of our method.

2.1. Encryption with chaotic systems

As shown in figure 1, original images will be encrypted first. In this step, a lot of existing methods can be used such as chaotic maps, Arnold Transform, and DNA encryption [17,19]. In this paper, the encryption algorithm which is based on a new chaotic map called the logistic-tent system (LTS) is used [4]. LTS has some advantages. First, it is a chaotic map so that LTS is ergodic and sensitive to initial conditions. Second, compared to general chaotic maps, LTS has a larger range of parameters and better chaotic behavior. Third, the structure of LTS is very simple and easy to be implemented. Thus, LTS can guarantee the high security of encrypted images.

2.2. DWT in reference images

DWT is used to pretreat the reference image to get frequency domain information. The results of DWT are four smaller pictures which are the proximate value, vertical detail, horizontal detail, and diagonal detail of the original image and the length and width of all smaller pictures are half of the reference image. For a conveniently describing, these four images are named CA, CV, CH, and CD. In this paper, CV and CH are used in the HID process since they are high-frequency components. The size of reference images and original images need to be restricted, for DWT changes the size of reference images. Assume that the size of the encrypted image is M*N, which means that the size of CV and CH is no less than M*N and the size of the reference image is no less than 2M*2N.

2.3. Hide information in dark area (HID)

When encrypted images and CA, CH, CV, and CD are produced, the final meaningful image can be constructed. The key idea is to hide the information of the encrypted image in the dark area of CH and CV (HID). To implement this idea, the encrypted image will be transformed into two low-value images, which are then embedded in CH and CV. Both CH and CV have the same size as the encrypted image. The following problem is what principle should be used to determine whether pixel values will be replaced in CH and CV. To solve this problem, two thresholds – *s_1, and s_2* – are computed by CV

DOI: 10.54254/2755-2721/6/20230370

and CH and the principle is that if a pixel value is lower than *s_1* in CV, it will be changed. The principle in CH is the same. The algorithm for computing the threshold is shown in the following pseudocode.

Algorithm of computing threshold
Input: CV and CH, the number of encryption image pixels *n*
1. Flatten the CV and CH matrix and get a vector called *CV_flatten* and *CH_flatten.*
2. Sort *CA_flatten* and *CH_flatten.*
3. choose the *n*th pixel value of sorted *CA_flatten* and *CH_flatten* as *s_1* and *s_2*.
Output: get the threshold s_1 and s_2.

Assume *n_1* and n_2 are the numbers of encrypted image pixels and CV pixels. In order to make the final meaningful image closer to the reference image, the reference image whose size is 4 times of the original image, or even larger, will be chosen. For example, if the original size is 256*256, in order to hide information more securely and get better results, the reference image with a size of 512*512 will be chosen. Therefore, the size of CA is 256*256. Besides, down sampling original images is also a good choice when image details are not important. For example, if the size of the encrypted image is 128*128, the reference image with a size of 512*512 will be chosen. In this situation, *n_1 / n_2* is 0.25 so a quarter of CA pixels will be changed. In this paper, all reference images are 4 times as large as the original images and down sample the original images.

Another key step in HID is transforming an encrypted image into two low-value images. These two images have the size of CV and CH. These two images are embedded in CV and CH to get the meaningful image without changing the reference image evidently. Thus, an encrypted image is transformed into a good-looking image so that it can draw less attention from attackers. This paper introduced a new method of dividing encrypted images. This process is described as follows: Where *bin* presents an 8-bit binary number, *f* and *g* are used to get decimal numbers with the first four bits and the last four bits. For example, if an image pixel p with value of 123 and position (*i,j*) is selected, value = *bin* (123) =01111011, CH[*i,j*] = *f* (0111) = 7, CV[*i,j*]=*g* (1011) =11. For every eight-bit binary number, the maximum value of *f* and *g* is 15 and it is a low value from 0 to 255.

Algorithm: divide encrypted image
Input: an encrypted image *E* with a size of M*N and a reference image with size of 2M*2N.
1. Get CA, CH, CV, CD with DWT
2. For m = 1 to M do
3. For n = 1 to N do
4. value = *bin*(*E*[m, n])
5. CH = *f*(value)
6. CV = *g*(value)
7. End for
8. End for
9. Do inverse DWT with CA, CH, CV, CD
Output: Get the final meaningful image *P* with 2M*2N

In the loop of this algorithm, the encrypted image is divided into two low-value images which replace the original CH, CV. Actually, these two images can replace any two of CH, CV, or CD.

2.4. Decryption process

The decryption process consists of two steps: to get the encrypted image from the final meaningful image and to get the original image from the encrypted image. The LTS system is used to encrypt images, so that only the chaotic sequence is used to decrypt images. As for getting the encrypted image from a meaningful image, IDWT is used to get CA, CV, CH, and CD from the final result. Besides, in order to get the encrypted values hiding in the CV and CH, the key information needed is the position information matrix M which records the positions of changed image pixels. Thus, CA, CH, CV, CD, and M are used to reconstruct the encrypted image directly by the following formula:

$$O[m, n] = \text{int}(\text{bin}(CH[m, n]) + \text{bin}(CV[m, n]))$$

DOI: 10.54254/2755-2721/6/20230370

In this formula, two binary strings are linked and the *int* function is used to transform a binary string into a decimal number.

2.5. Discussion

The proposed algorithm can solve the problem described in section 1 since both of them encrypt images from a data perspective and a visual perspective. This method can transform encrypted images with random pixel values into images similar to reference images without missing too many details. When private and valued images become meaningful but not important images, they can draw less attention from attackers.

The key idea of HID is hiding the encrypted image pixels in a dark area in CV and CH. This method thus has higher security for the information of which pixels are changed in CV and CH is needed so as to reconstruct the original image. Besides, the encrypted image is divided into two images with low pixel values, and then use these images to replace CH and CV. There are at least two advantages according to this procedure. One is that it takes little time to produce a meaningful image since DWT and IDWT are quite fast. The other is that the results are clearer since CV, CH, and two low-value images are not very different.

The figure 2-3 demonstrates a clear example of our method.

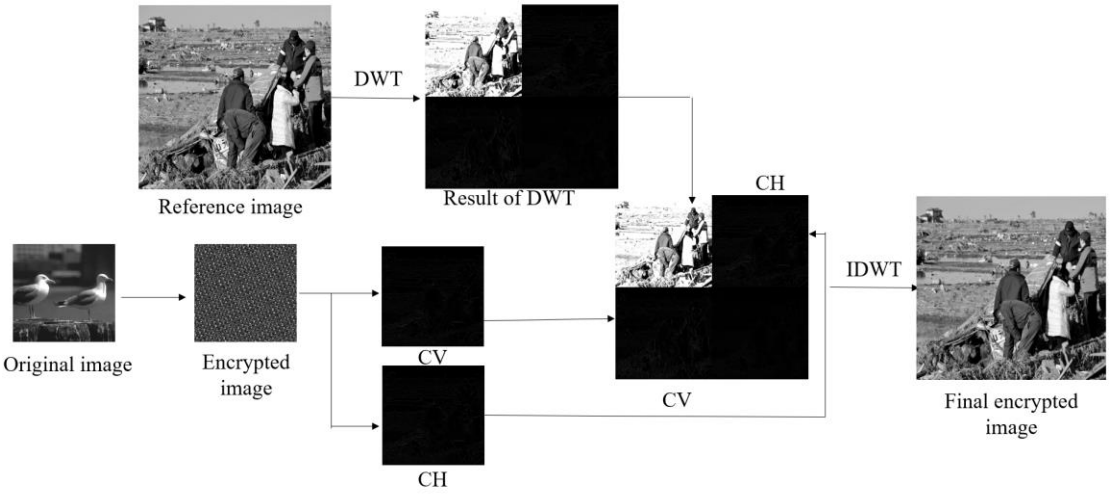


Figure 2. the illustrative picture of encryption method.

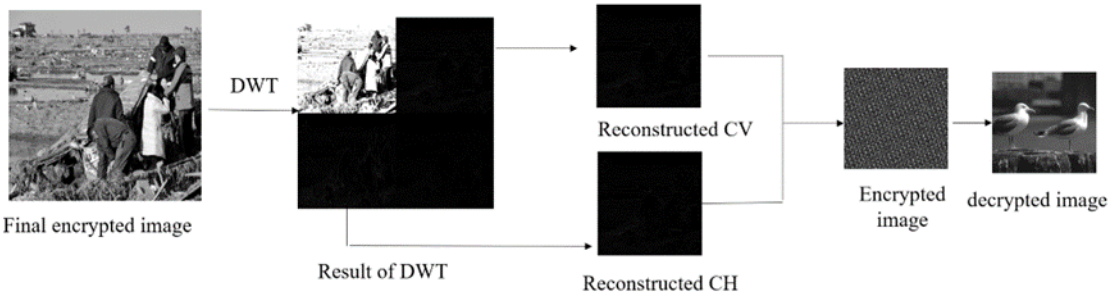


Figure 3. The illustrative picture of decryption method.

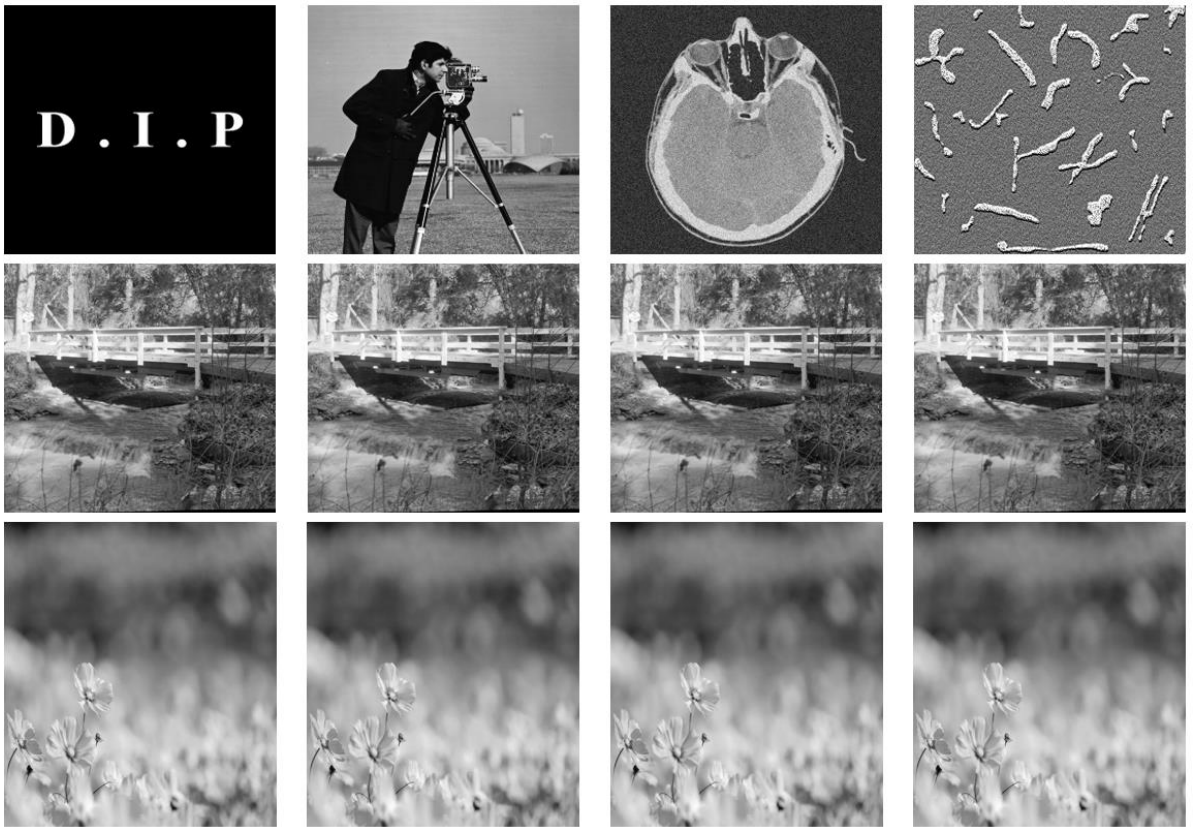
3. Experimental results and analysis

In this section, some experimental results and security analysis are shown. The algorithm in is used to transform original images into random pixel images [4]. In addition, the size of reference images is four times the size of original images. Besides, every original image is down sampled only once.

DOI: 10.54254/2755-2721/6/20230370

3.1. Experimental results

Four types of original images are selected in this section, including binary images, grayscale images, biometrics images, and medical images. The experimental results are shown in figure 4 which indicates that this method can transform quite different images into similar images using the same reference image. Meanwhile, this method can also be used to encrypt color images, as shown in figure 5. In addition, the reference image has a great impact on the visual effect of the final image. Figure 5 shows that different reference images can produce completely different final images regardless of the same original images. Finally, a conclusion is drawn from figure 6 that the final images of this method are clearer and have higher quality, for it can preserve details better in final images compared to Bao's method [8]. Thus, our method can draw less attention from attackers.



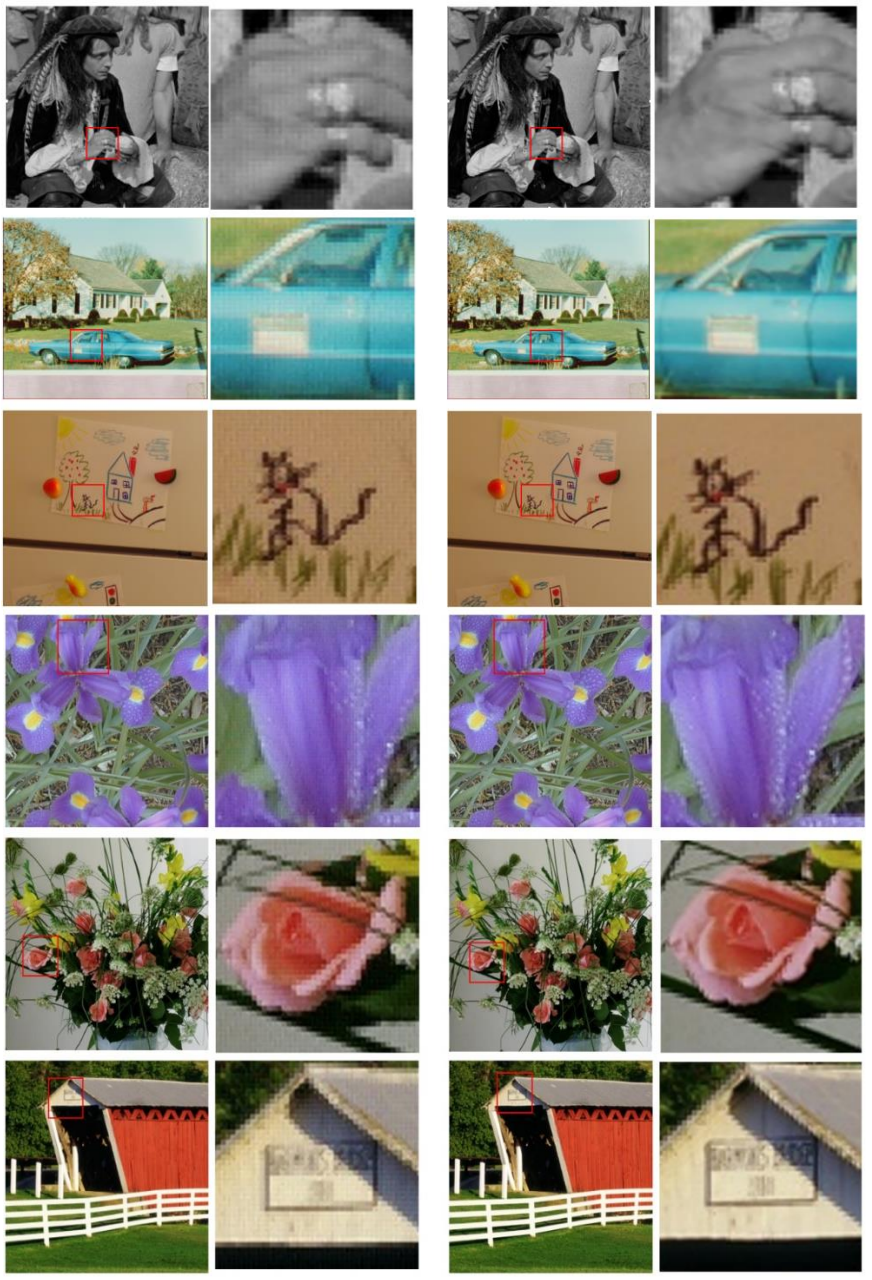
(a) (b) (c) (d)

Figure 4. Experimental results. The original images are in the first row while the second row and the third row represent the final encrypted images utilizing different reference images. (a) binary image (b) gray scale image of a character (c) medical image (d) bacteria image.

3.2. Security analysis

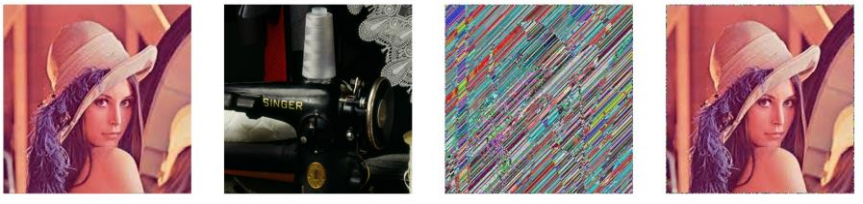
Data loss analysis. In this section, a patch with a size of 100*100 is chosen in the final image where the values of pixels are zero. As can be seen in figure 8, this has not changed the whole decrypted images, or rather only the pixels in the patch have been changed.

DOI: 10.54254/2755-2721/6/20230370



(a) (b) (c) (d)

Figure 6. The comparison of our method and Bao's method. (a) the final images using Bao's method (b) enlarged picture of the red boxes in (a). (c) the final images using our method. (d) enlarged picture of the red boxes in (a). It can be seen clearly in this figure that the quality of our method is higher.



(a) (b) (c) (d)

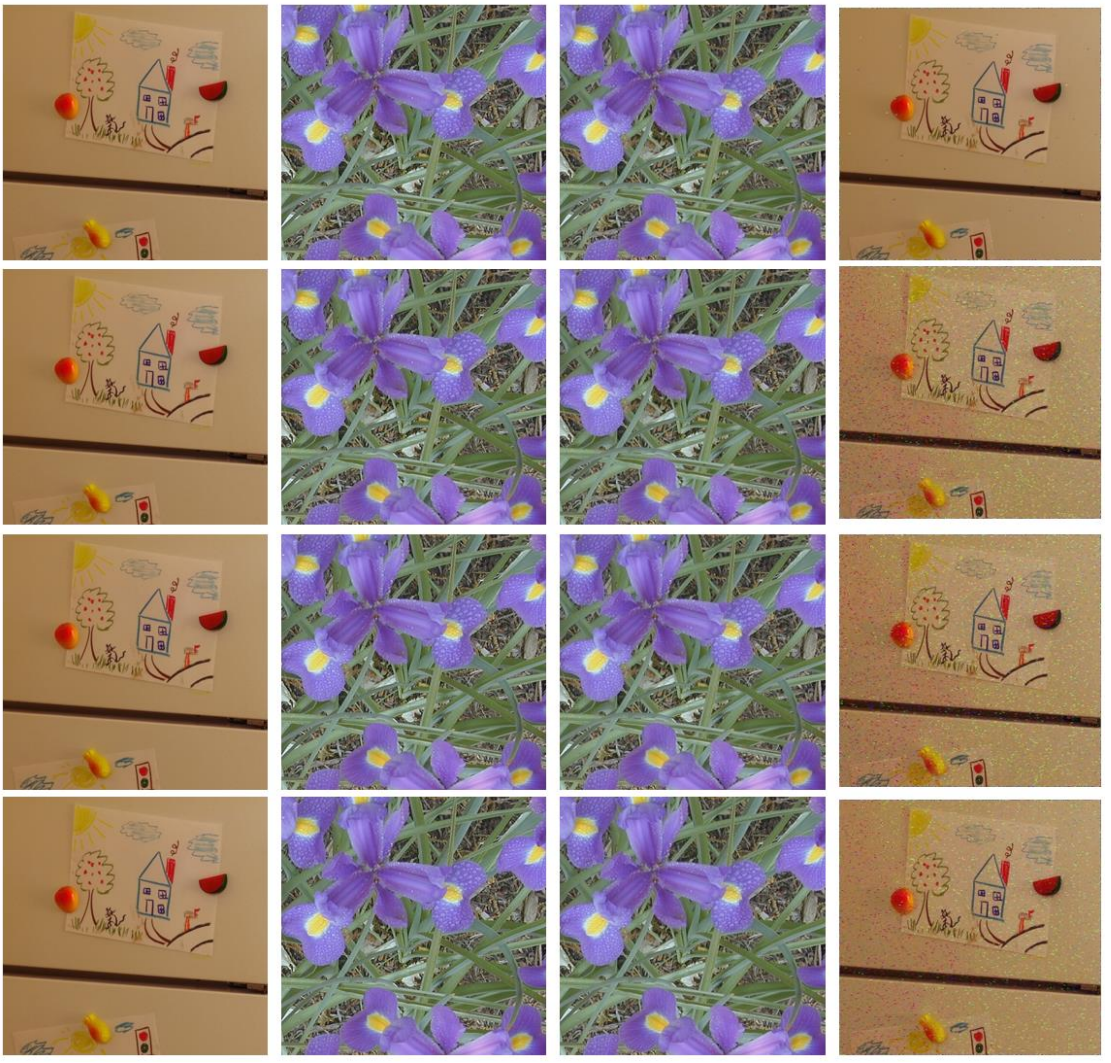
Figure 7. Key sensitive analysis. (a) original image. (b) final encrypted image. (c) encrypted image using K2. (d) encrypted images using K1.

DOI: 10.54254/2755-2721/6/20230370

(a) (b) (c) (d)

Figure 8. Data loss analysis. (a) the original image. (b) the final encrypted image. (c) data loss in (b). (d) the decrypted image.

3.2.4 Noise attack. In this section, four types of noise, including Salt and Pepper noise, Gaussian noise, Poisson noise, and Speckle noise with a density of 0.0001, are applied to the final images. The decrypted images are displayed in figure 9. It shows that our method can resist noise attacks.



(a) (b) (c) (d)

Figure 9. (a) the original images. (b) the final encrypted images. (c) the encrypted images with Salt & Pepper noise, Gaussian noise, Poisson noise, and Speckle noise. (d) the decrypted images.

DOI: 10.54254/2755-2721/6/20230370

4. Conclusion

To make meaningful images and improve the quality of results, HID based on DWT and chaotic systems is proposed in this paper. The encrypted images, which often look like noise, are changed into two low-value images which are hidden in the dark area selected in the results of DWT for reference images instead of directly replacing the low-frequency images of DWT. The experimental results and security analysis demonstrate that the results of our method are much safer and have higher quality, for the details in final meaningful images are better persevered.

References

[1] Smid M E, Branstad D K.1988 Data encryption standard: past and future[J]. Proceedings of the IEEE, 76(5): 550-559.
[2] Daemen J, Rijmen V. 2001 Reijndael: The advanced encryption standard[J]. Dr. Dobb's Journal: Software Tools for the Professional Programmer, 26(3): 137-139.
[3] Singh G. 2013 A study of encryption algorithms (RSA, DES, 3DES and AES) for information security[J]. International Journal of Computer Applications, 67(19).
[4] Zhou Y, Bao L, Chen C L P. 2014 A new 1D chaotic system for image encryption[J]. Signal processing, 97: 172-182.
[5] Pareek N K, Patidar V, Sud K K. 2006 Image encryption using chaotic logistic map[J]. Image and vision computing, 24(9): 926-934.
[6] Watson A B. 1994 Image compression using the discrete cosine transform[J]. Mathematica journal, 4(1): 81.
[7] Lai C C, Tsai C C. 2010 Digital image watermarking using discrete wavelet transform and singular value decomposition[J]. IEEE Transactions on instrumentation and measurement, 59(11): 3060-3063.
[8] Guan Z H, Huang F, Guan W. 2005 Chaos-based image encryption algorithm[J]. Physics letters A, 346(1-3): 153-157.
[9] Ye G.2010 Image scrambling encryption algorithm of pixel bit based on chaos map[J]. Pattern Recognition Letters, 31(5): 347-354.
[10] Yang B, Wu K, Karri R. 2004 Scan based side channel attack on dedicated hardware implementations of data encryption standard[C]//2004 International Conferce on Test. IEEE, 339-344.
[11] Ye G. 2010 Image scrambling encryption algorithm of pixel bit based on chaos map[J]. Pattern Recognition Letters, 31(5): 347-354.
[12] Wang X, Teng L, Qin X. 2012 A novel colour image encryption algorithm based on chaos[J]. Signal Processing, 92(4): 1101-1108.
[13] Zhu Z, Zhang W, Wong K, et al. 2011 A chaos-based symmetric image encryption scheme using a bit-level permutation[J]. Information Sciences, 181(6): 1171-1186.
[14] Gao H, Zhang Y, Liang S, et al. 2006 A new chaotic algorithm for image encryption[J]. Chaos, Solitons & Fractals, 29(2): 393-399.
[15] Bao L, Zhou Y. 2015 Image encryption: Generating visually meaningful encrypted images[J]. Information Sciences, 324: 197-207.
[16] Wang R Z, Lin C F, Lin J C. 2001 Image hiding by optimal LSB substitution and genetic algorithm[J]. Pattern recognition, 34(3): 671-683.
[17] Potdar V M, Han S, Chang E. 2005 A survey of digital image watermarking techniques[C]//INDIN'05. 2005 3rd IEEE International Conference on Industrial Informatics, 2005. IEEE, 709-716.
[18] Nikolaidis N, Pitas I. 1998 Robust image watermarking in the spatial domain[J]. Signal processing, 66(3): 385-403.
[19] Liu Z, Xu L, Liu T, et al. 2011 Color image encryption by using Arnold transform and color-blend operation in discrete cosine transform domains[J]. Optics Communications, 284(1): 123-128.
[20] Chai X, Fu X, Gan Z, et al. 2019 A color image cryptosystem based on dynamic DNA encryption and chaos[J]. Signal Processing, 155: 44-62.