A Meaningful Image Encryption Algorithm Based on Prediction Error and Wavelet Transform

Mengling Zou[1], Zhengxuan Liu[2] and Xianyi Chen[3, *]

Abstract: Image encryption (IE) is a very useful and popular technology to protect the privacy of users. Most algorithms usually encrypt the original image into an image similar to texture or noise, but texture and noise are an obvious visual indication that the image has been encrypted, which is more likely to cause the attacks of enemy. To overcome this shortcoming, many image encryption systems, which convert the original image into a carrier image with visual significance have been proposed. However, the generated cryptographic image still has texture features. In line with the idea of improving the visual quality of the final password images, we proposed a meaningful image hiding algorithm based on prediction error and discrete wavelet transform. Lots of experimental results and safety analysis show that the proposed algorithm can achieve high visual quality and ensure the security at the same time.

Keywords: Image encryption, meaningful, prediction error, wavelet transform.

1 Introduction

In the past ten years, the Internet-related industries have developed rapidly around the world. Image, video, audio and other formats of information transmission on the basis of the Internet is extremely convenient, but it brings many serious security problems [Wang, Zhang, Ren et al. (2013); Chai, Gan, Chen et al. (2016)]. As multimedia data transmitted through network channels, especially medical images and military images, may be private [Xiong and Shi (2018)], valuable or even confidential. Therefore, preventing the leakage of this important information in the transmission process has become a top priority for enterprises and individuals [Zanin and Pisarchik (2014); Liu, Sun and Zhu (2016); Cox, Kilian, Leighton et al. (1997); Hong, Chen and Wu (2012)]. Up to now, there have been many methods to protect image content, mainly including encryption and steganography [Hou, Zhang and Yu (2016)].

The idea of most existing IE algorithms is to convert the original image into a garbled image similar to noise or texture, which cannot be recognized by human visual system or machine [Yao, Tang, Qin et al. (2018)] see Figs. 1(a) and (b). However, such images with noise or texture characteristics are prone to arouse the suspicion of attackers, and it is difficult to protect privacy [Liu, Seah, Zhu et al. (2012); Zhou, Qiu, Li et al. (2018)]. To better protect the content of the image, we should encrypt the ordinary image into a visually normal image as shown in Fig. 1(c). Many researchers have made outstanding

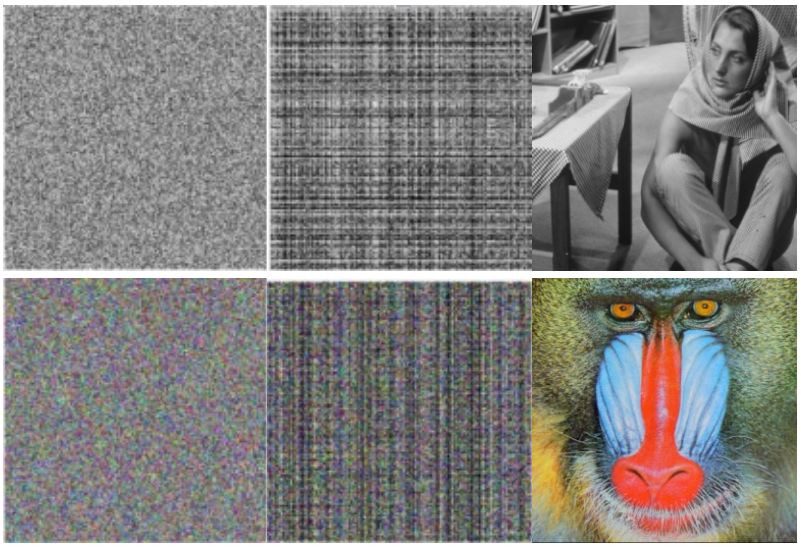
[1] School of Computer and Software Nanjing University of Information Science & Technology, Nanjing, China.

[*] Corresponding Author: Xianyi Chen. Email: 0204622@163.com.

contributions to reducing the noise and texture characteristics of encrypted images. Their methods effectively avoid attack types such as data cropping and illegal tampering [Juneja and Sandhu (2009); Cao, Wei, Guo et al. (2017); Qin, Chang and Chiu (2014)]. For example, in 2015, a novel image encryption method called visually meaningful image encryption (VMEI) was proposed by Bao et al. [Bao and Zhou (2015)], latter known as the BZ scheme. In 2017, Kanso et al. [Kanso and Ghebleh (2017)] proposed an improved meaningful image encryption algorithm (VMIMS) based on the BZ scheme.

Starting from the idea of encrypting an ordinary image into another image with visual significance [Bao and Zhou (2015); Gao, Deng, Li et al. (2010); Kanso and Ghebleh (2017); Yao, Liu, Tang et al. (2019)], this paper used a rhombus predictor to process the original image and combined it with discrete wavelet transform to reduce the texture features of the cipher image while guaranteeing the embedding capacity.

The following is the organizational structure of this article: the second part shows the algorithm of this paper. The third section introduces the experimental results, and the last part is the conclusion of this paper.



(a) (b) (c)

Figure 1: Three different encrypted images of grayscale and color images: (a) noise-like; (b) texture-like; (c) normal vision

2 Algorithm proposed in this paper

2.1 Encryption process

The framework of this scheme is shown in Fig. 2, which is mainly composed of (1) preprocessing stage and (2) embedding stage. In the pre-processing phase, we first use the rhombus predictor to calculate the prediction error value of original image I, store these values in the array R, and then encrypt R. The encryption process is shown in Eq. (1):

$$P = O(R, K) \tag{1}$$

where, O is the encryption method, K is the secret key and P is the encrypted error sequence.

In the second stage, we first divide the reference image into 8×8 image blocks, and then use two-dimensional DWTCT to decompose each image block into an approximate coefficient matrix and three detail coefficient matrices, then the parameters, the basic pixels and the encrypted prediction errors are embedded into the high-frequency coefficients of the host image to obtain the final cryptographic image E, so,

$$E = M(B, P, H, N) \tag{2}$$

where, M and N represent the DWTCT operation and its parameter set, respectively, and B represent the basic pixels.

2.2 Decryption process

Usually, image decryption is to reverse the encryption process, and the specific process is shown in Fig. 3. It can be clearly seen from the picture that the decryption algorithm proposed in this paper includes two main steps. When extracting the information, we first use a wavelet filter to divide the encrypted image into 4 sub-sections, then extract the scrambled prediction error value from C'_H, and finally, extract the modified basic pixels from C'_V and C'_D. To recover the prediction error value, we use the following formula to extract the basic pixels according to their order in the index.

$$P'(m,n) = 10C'_V(m,n) + C'_D(m,n) \tag{3}$$

In Eq. (3), C'_V and C'_D are the sub-bands obtained by the I2DWT of the encrypted image and $P'(m, n)$ is the reconstruct value of basic pixel.

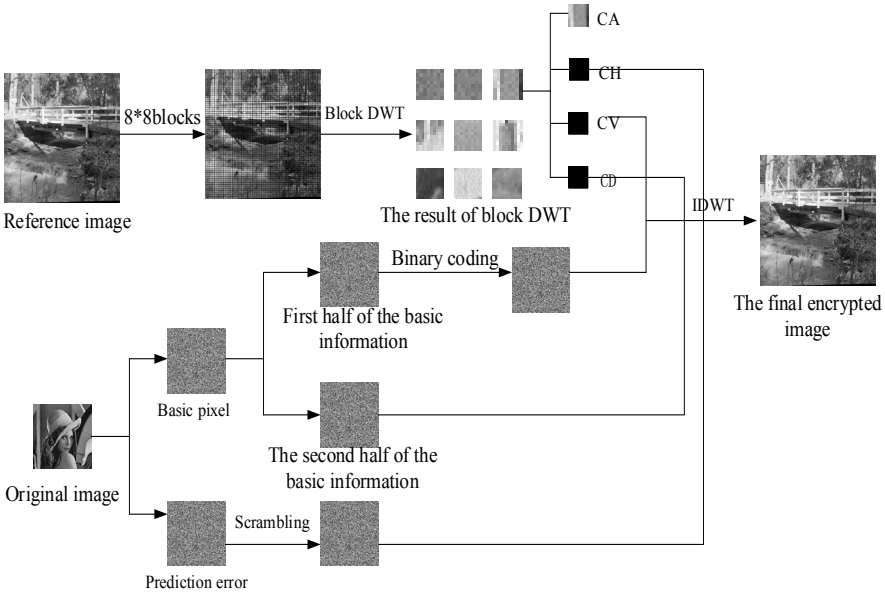


Figure 2: Framework of the proposed encryption scheme

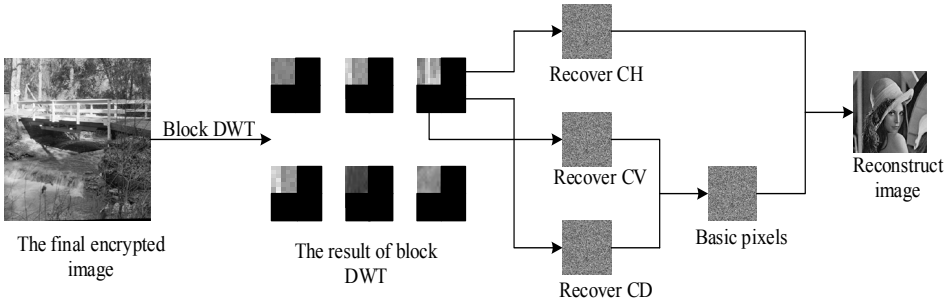


Figure 3: The framework of the proposed encryption scheme

Based on the Section 2.1 we describe the detailed encryption algorithm below:

Input: Original image O of size $\mathrm{m}\times n$, reference image H of size $2\mathrm{x}\times 2y$, where $\mathrm{x}\times y \geq m\times n$ and secret key=K.

1: Set $H'=\lceil \alpha-(\beta-\alpha)/255H \rceil$ where $\alpha=10,\ \beta=245.$

2: Divide H' into 8×8 blocks.

3: Applying 2DWT to each image block to get four coefficients: C_A, C_H, C_V, C_D.

4: Use the rhombus predictor to calculate the prediction error value of O.

5: Scramble the prediction error with the secret key K.

6: Extract and index the basic pixels which was used to restore the prediction error.

7: Divide the basic pixels into two parts according to the index order and store in two one-dimensional arrays.

8: For the first part of the basic pixels, we encode it in binary and the remaining half divided into two parts as follows: $C_V(m,n)=\lfloor P(\mathrm{m},n)/10 \rfloor \quad C_D=P(m,n)\bmod 10$

9: For each block of the reference image **do**

10: Embed the encrypted prediction error in the C_H.

11: Embed the first half of basic pixels in the C_D and the second half in the C_D.

12: Define the coefficient of embedded information as C_A, C'_H, C'_V, C'_D.

11: Apply the I2DWT to the modified coefficient matrix to get the final encrypted image.

Output: encrypted image S with size of $2\mathrm{x}\times 2y$

---

3 Experimental and evaluations

In this section, we performed several sets of experiments, including reversibility, resistance to cropping attacks, and visual effects, and compared with the BZ scheme.

Experimental results show that the difference of histograms between the final encrypted image in Fig. 4(f) and reference image in Fig. 4(d) are almost invisible. That is to say, they are similar in terms of appearance. Furthermore, the reconstructed image Fig. 4(g) from the final encrypted image is visually acceptable. Therefore, it will not cause the suspicion of attackers, and will largely protect the content of the image.

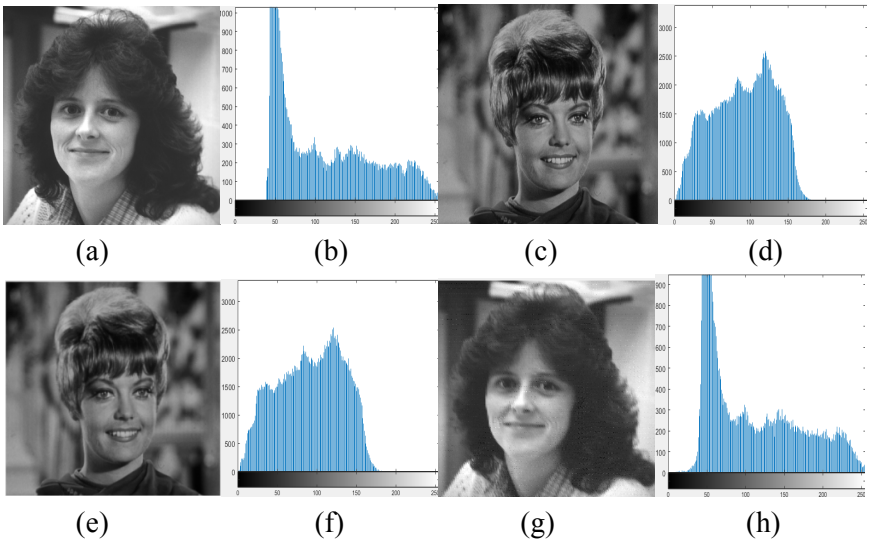


Figure 4: Test images and corresponding histograms: (a) original image, (b) histogram of Woman, (c) reference image, (d) histogram of Zelda, (e) the final encrypted image and (f) its histogram, (g) the restored image and (h) its histogram

To prove that our method is effective and superior to the BZ scheme, we selected 50 pairs of images from the test image database randomly for experiments. Fig. 5 shows the PSNR and SSIM of our method and BZ scheme [Horé and Ziou (2010)]. In addition, in order to compare the data of this paper and BZ scheme more intuitively, we calculated the mean values of PSNR and SSIM and show them in Tab. 1. Combine Fig. 5 and Tab. 1, we can draw the following conclusion: compared with BZ scheme, our method is generally better, and the average PSNR value of our scheme is increased by 3.421 dB and the average SSIM value is increased by 0.0269.

Table 1: Average result about PSNR and SSIM on 50 pairs of test images

Method	PSNR (dB)	SSIM
BZ scheme	28.596	0.9365
Proposed	32.017	0.9634

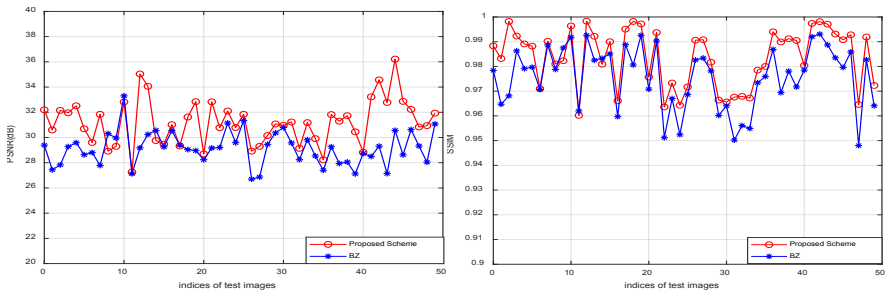
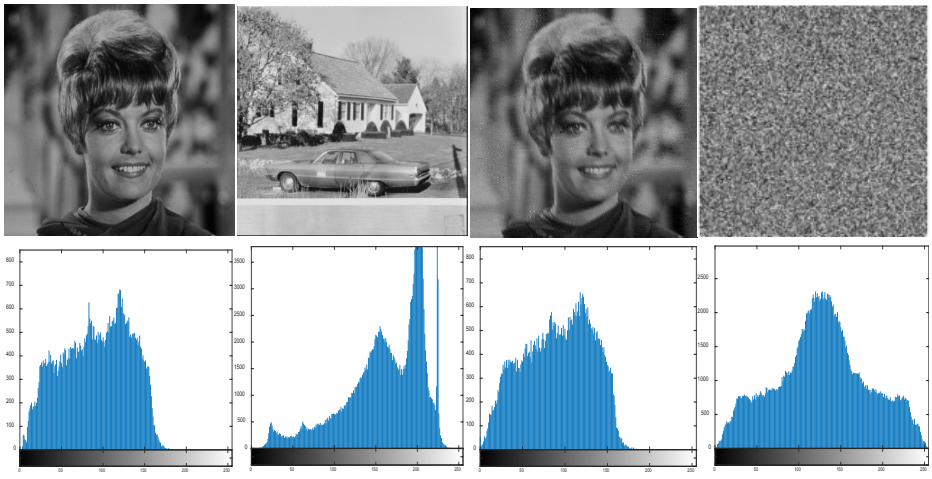


Figure 5: Comparison of proposed algorithm and BZ scheme: the PSNR and SSIM of 50 pairs encrypted images



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

Figure 6: Test of key sensitivity, first row: (a) original image, (b) encrypted image, (c) reconstructed image with the right key, (d) reconstructed image with incorrect key; second row: the corresponding histograms

Then, we analyzed the security of proposed scheme from the aspects of secret key sensitivity and anti-clipping attack. Figs. 6 and 7 are the results. In Fig. 6, the correct key can reconstruct the original image and Fig. 7 shows us the secret carrier diagram after clipping and the corresponding reconstructed image. Obviously, despite the large area of data loss in clipped encrypted images, the original image can still be well restored.

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

Figure 7: Clipping attack analysis (a) original image (b) the final encrypted image (c) the final encrypted image with 128×128 cut (d) original image restored from clipping image

4 Conclusion

This paper proposed an image encryption scheme based on prediction error and wavelet transform, which is meaningful from the perspective of human vision. The use of prediction error reduces the change to the reference image during embedding. This scheme can effectively protect the content of the image, because the encrypted image has different shapes, sizes, and appearances, it is difficult for an attacker to judge and locate the encrypted image from normal images. In addition, we compared the scheme proposed in this paper with the BZ scheme. Experimental results show that the quality of encrypted

image is better than that of the BZ scheme. Future work should focus on reducing the amount of auxiliary information and improving visual quality.

Acknowledgement: Thanks to JBD for providing us with a paper template and allowing us to modify. This work is supported by the National Key R&D Program of China under grant 2018YFB1003205; by the National Natural Science Foundation of China under grant U1836208, B1003205, U1836110,61602253,61672294; by the Jiangsu Basic Research Programs Natural Science Foundation under grant numbers BK20181407; by the Priority Academic Program Development of Jiangsu Higher Education Institutions (PAPD) fund; by the Engineering Research Center of Digital Forensics, Ministry of Education; by the Collaborative Innovation Center of Atmospheric Environment and Equipment Technology (CICAEET) fund, China.

References

Bao, L.; Zhou, Y. (2015): Image encryption: generating visually meaningful encrypted images. *Information Sciences*, vol. 324, no. 10, pp. 197-207.

Barni, M.; Bartolini, F.; Cappellini, V.; Piva, A. (1999): DWT-based technique for spatio-frequency masking of digital signatures. *Security and Watermarking of Multimedia Contents, International Society for Optics and Photonics*, vol. 3657, pp. 31-39.

Cao, X.; Wei, X.; Guo, R.; Wang, C. (2017): No embedding: a novel image cryptosystem for meaningful encryption. *Journal of Visual Communication & Image Representation*, vol. 44, pp. 236-249.

Chai, X.; Gan, Z.; Chen, Y.; Zhang, Y. (2016): A visually secure image encryption scheme based on compressive sensing. *Signal Processing*, vol. 134, pp. 35-51.

Cox, I. J.; Kilian, J.; Leighton, F. T.; Shamoon, T. (1997): Secure spread spectrum watermarking for multimedia. *IEEE Transactions on Image Processing: A Publication of the IEEE Signal Processing Society*, vol. 6, no. 12, pp. 1673-1687.

Gao, X.; Deng, C.; Li, X.; Tao, D. (2010): Geometric distortion insensitive image watermarking in affine covariant regions. *International Conference on Advances in Recent Technologies in Communication and Computing*, vol. 40, no. 3, pp. 278-286.

Hong, W.; Chen, T. S.; Wu, H. Y. (2012): An improved reversible data hiding in encrypted images using side match. *IEEE Signal Processing Letters*, vol. 19, no. 4, pp. 199-202.

Horé, A.; Ziou, D. (2010): Image quality metrics: PSNR *vs.* SSIM. *IEEE Computer Society*, pp. 23-26.

Hou, D.; Zhang, W.; Yu, N. (2016): Image camouflage by reversible image transformation. *Journal of Visual Communication and Image Representation*, vol. 40, pp. 225-236.

Juneja, M.; Sandhu, P. S. (2009): Designing of robust image steganography technique based on LSB insertion and encryption. *International Conference on Advances in Recent Technologies in Communication & Computing.*

Kanso, A.; Ghebleh, M. (2017): An algorithm for encryption of secret images into

meaningful images. *Optics and Lasers in Engineering*, vol. 90, pp. 196-208.

Liu, M.; Seah, H. S.; Zhu, C.; Tian, F. (2012): Reducing location map in prediction-based difference expansion fore visible image data embedding. *Signal Processing*, vol. 92, no. 3, pp. 819-828.

Liu, W.; Sun, K.; Zhu, C. (2016): A fast image encryption algorithm based on chaotic map. *Optics & Lasers in Engineering*, vol. 84, pp. 26-36.

Xiong, L. Z.; Shi, Y. Q. (2018): On the privacy-preserving outsourcing scheme of reversible data hiding over encrypted image data in cloud computing. *Computers, Materials & Continua*, vol. 55, no. 3, pp. 523-539.

Qin, C.; Chang, C. C.; Chiu, Y. P. (2014): A novel joint data-hiding and compression scheme based on SMVQ and image inpainting. *IEEE Transactions Image Process*, vol. 23, no. 3, pp. 969-978.

Wang, C.; Zhang, B.; Ren, K.; Roveda, J. M. (2013): Privacy-assured outsourcing of image reconstruction service in cloud. *IEEE Transactions on Emerging Topics in Computing*, vol. 1, no. 1, pp. 166-177.

Yao, H.; Liu, X.; Tang, Z.; Tian, Y. (2019): Adaptive image camouflage using human visual system model. *Multimedia Tools and Applications*, vol. 78, no. 7, pp. 1-24.

Yao, H.; Tang, Z; Qin. C.; Tian. Y. (2018): Adaptive image camouflage using human visual system model. *Multimedia Tools and Application*s, vol. 78, pp. 8311-8334.

Zanin, M.; Pisarchik, A. N. (2014): Gray code permutation algorithm for high-dimensional data encryption. *Information Sciences*, vol. 270, no. 2, pp. 288-297.

Zhou, Q.; Qiu, Y.; Li, L.; Lu, J.; Yuan, W. et al. (2018): Steganography using reversible texture synthesis based on seeded region growing and LSB. *Computers, Materials & Continua*, vol. 55, no. 1, pp. 151-163.