

Research on Image Encryption Technology Based on Source Joint Coding Scheme

Yuhang Wu

*Academy of Cryptography and Cyberspace Security, Nankai University, Tianjin, China
2595797038@qq.com*

Abstract: Currently, common image encryption methods mainly include symmetric encryption (such as AES, DES) and public key encryption (such as RSA, ECC). Although these traditional encryption methods perform well in terms of data security, they still have certain limitations in terms of multi-source data protection, efficient encryption and decryption, key management and protection against eavesdropping attacks. For example, symmetric encryption requires a secure shared secret between both sides of communication, while public key encryption is computationally complex and difficult to meet the real-time requirements of large-scale data transmission. In addition, existing encryption methods are often unable to make full use of the relevance between sources to optimize the efficiency and security of data encryption. To this end, this paper studies a source joint coding scheme based on a multi-level diversity coding system (MDCS) and applies it to image encryption. The scheme combines Shamir threshold secret sharing and source joint encryption to achieve hierarchical encryption of data by dividing images into multiple source blocks, and uses joint coding technology to improve anti-eavesdropping capabilities. On this basis, this paper further improves the shortcomings of the original source joint coding scheme, optimizes the encryption process, and enhances the security, reliability and computing efficiency of the system. Experimental results show that the scheme can improve the ability to resist attacks while ensuring the security of image encryption, providing an effective solution for image data protection in cloud computing, the Internet of Things and distributed storage environments.

Keywords: Source joint coding, image encryption, security analysis, encryption scheme, multi-level diversity coding system

1. Introduction

In many communication networks, users may obtain information of different important levels from multiple available sources, which can be modeled with a multi-level diversity coding system (MDCS) [1]. The Multi-level Diversity Coding System (MDCS) is a special model of a multi-source network, which is developed from the Diversity Coding System (DCS). The source in MDCS is layered, and the decryption of high-level sources depends on the decryption of low-level sources. MDCS is divided into symmetric MDCS (SMDCS) and asymmetric MDCS (AMDCS). In SMDCS, all decoders that access the same number of encoders have the same decoding level; in AMDCS, all $2L-1$ access structures of L encoders correspond to different decoding levels [2]. In order to realize the informationological confidentiality of eavesdropping channels, the concept of threshold perfect

confidentiality is introduced into the SMDDCS model, called the secure symmetrical multi-level diversity coding system (S-SMDCS). This concept is also introduced into the AMDCS model, which is called the secure asymmetric multi-level diversity coding system. This method divides the secret into multiple parts (generally, the number of secret partitions is equal to the number of encoders). As long as the number of channels eavesdropped on by the eavesdropper does not exceed the security level, the information about the secret will not be leaked [3].

On the basis of the above research, this paper deeply analyzes a source joint coding scheme, which takes the threshold secret sharing algorithm (secret sharing) as the enhancement of the MDCS coding scheme. Using the threshold secret sharing algorithm, the data to be transmitted is divided into several shares and distributed to each user (encoder). Only more than the secret shares at the security level can the original secret be restored [4,5], and the low-level sources encrypted with high-level sources encrypted by the secret sharing algorithm are jointly encrypted to achieve the security and reliability of the source. This scheme can be extended to any system structure, not for specific security levels and access structures, and its security is based on a threshold secret sharing algorithm and joint encryption, rather than the absolute security of the key. This paper realizes the confidentiality of image information based on this scheme, and improves some shortcomings of image encryption in this scheme to further enhance its reliability and security in image encryption. The second part briefly introduces the scheme and analyzes its shortcomings; the third part proposes an improvement plan for its shortcomings in image encryption and analyzes the effect; the fourth part simulates eavesdropping; the fifth part summarizes the full text.

2. Source Joint Coding Scheme

2.1. Introduction to the Source Joint Coding Scheme

2.1.1. System Model

The security level of S-AMDCS is defined as m , which means that eavesdroppers can eavesdrop on subsets of up to m encoders, but still cannot recover any source information. Only a subset of an encoder greater than m can decode some or all of the source information.

S-AMDCS has L encoders, $E_1, E_2, \dots, E_L$ and T decoders, and S sources, which are independently distributed and have the same entropy $H(X_1) = H(X_2) = \dots = H(X_S) = n$. Their levels are incremental, and low-level sources must be decrypted before high-level sources. S sources are encoded into L data blocks, which are transmitted by the encoder E_i through noise-free channels. The decoder D_j can determine its decoding level g by accessing a subset of valid encoders (that is, a set of encoders greater than the security level of m), so as to decrypt the source $X_1, X_2, \dots, X_g$ of level 1 to g .

Therefore, the calculation formulas of S and T are:

$$S=T=\sum_{i=m+1}^L \binom{L}{i} \quad (1)$$

2.1.2. Encryption Method

The first step is to secretly divide the lowest-level source X_1 , and use the Shamir secret sharing threshold scheme to divide X_1 into L shares, and each encoder distributes a share.

The second step is to jointly encrypt the remaining 15 sources. The specific method is $M_n = X_{n-1} \oplus X_n$ ($n=2,3,\dots,16$).

The third step is to distribute the encrypted message to L encoders. The specific distribution algorithm of the encrypted message is:

- First, enumerate a valid subset E_i that does not contain P_i , that is $P_i = \{A \subseteq \{E_1, E_2, \dots, E_L\} \setminus E_i \mid |A| > m\}$

- Calculate the decoding level of the subset: $\text{store}_{E_i} = L(P_i)$
- Generate encrypted messages: according to store_{E_i} , $M_{E_i} = f_M(\text{store}_{E_i})$, where $f_M(l)$ is defined as: $f_M(l) = X_l \oplus X_{l+1} = M_{l+1}$
- Transmission of encrypted messages: transmit the encrypted messages contained in M_{E_i} through the channel corresponding to E_i .

In this way, each encoder E_i will transmit a specific collection of encrypted messages according to its corresponding P_i and store_{E_i} to ensure that the distribution of encrypted messages can meet both decryption needs and prevent unauthorized eavesdropping [6].

2.2. Limitations and Improvements

Although the secret sharing algorithm and the joint encryption of the source can achieve the reliability of perfect confidentiality and encryption, because we designed the secure asymmetric multi-level diversity coding system (S-AMDCS), we assumed that all sources are independent and distributed sequences, and they have the same entropy, but in the actual information In the process of encryption and transmission, it is very likely that there is some correlation between each source that is not independent of each other. Therefore, the difference or operation as the core step of the joint encryption of the source may bring some problems with encryption, resulting in a decrease in the security of encryption.

For example, this paper implements this scheme and simulates it using the Python language. The parameters are set to $L=5$, $m=2$, $S=T=16$, and the secret to be divided is $\text{secret}=42$. The same method is used to simulate 1000 rounds of eavesdropping and calculate the average bit error rate (BER) of 1000 rounds of When all sources are set to randomly generated 8-bit binary numbers, the average bit error rate is calculated to be 0.507; when all sources are set to randomly generated 4-bit binary numbers, the average bit error rate is 0.4964. Fig.1 and Fig.2 draw the average bit error rate of each round and 1000 rounds of simulated eavesdropping for an 8-bit binary number source and a 4-bit binary number source respectively. Fig.1 is a graph of 8-bit binary numbers and Fig.2 is a graph of 4-bit binary numbers.

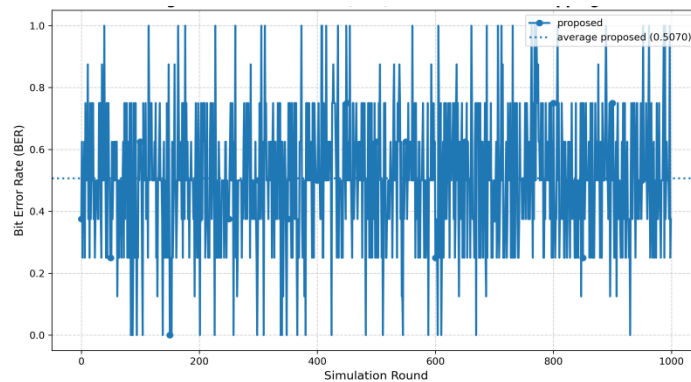


Figure 1: The bit error rate (BER) of external eavesdropping (8 bits).

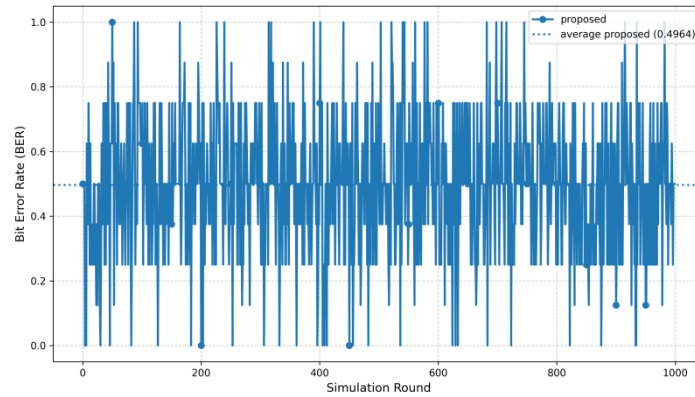


Figure 2: The bit error rate (BER)of external eavesdropping (4 bits).

Since there are 16 4-bit binary numbers and 256 8-bit binary numbers, for the number of sources with a number of 16, the correlation between 4-bit binary sources is obviously higher than that between 8-bit binary number sources, and the higher source correlation also results in the rate of eavesdropping (the result of this comparison experiment is not very large, and the conclusion is not obvious. We will further discuss it in the next part of the paper). This comparison experiment shows the shortcomings of this coding scheme; that is, when the correlation between the sources is high, the security of the scheme will decline. However, in real life, the source is very likely to be related, so we need to improve this scheme. The core idea of the improvement is to reduce the correlation between the sources and make the sources as independent as possible.

3. Encryption of Image

3.1. Results and Analysis of the Original Encryption Scheme

The above is encrypted with binary numbers as the source. The following is an example of the picture. Due to the smoothness and spatial correlation of the natural image, the pixel value of the image changes slowly in the local area, and the pixel value of adjacent pixels is relatively close, so the natural image usually has positive spatial self-correlation. If the pixel sequence of the image is used as the source to be encrypted, the encrypted image will be highly recognizable.

Take Fig.3 as an example. Fig.3 is a picture with a resolution of 960×953. The adjacent local pixel value of the picture is very close. We obtain the pixel sequence of this picture and use the secret sharing algorithm and the source joint encryption method for this pixel sequence. The encryption results are shown in Fig.4. In order to evaluate the correlation between the two pictures, this article found an indicator - Structural Similarity Index Measure, which is short for SSIM. It is an indicator to evaluate the similarity of two images. It is often used to measure the similarity before and after the distortion of the image. The range is [-1,1]. The closer it is to 1, the higher the similarity of the two pictures [7].

The calculation is $SSIM = 0.060009$, which is very small, indicating that the similarity between the two pictures before and after encryption is very low. These two pictures are very different in terms of structure, brightness, contrast and so on. Encryption seems to be very successful. However, through direct observation, it can be found that although a large number of details of the original image are hidden during the encryption process, the outline of a woman in the picture can still be judged by the encrypted image, and the outline is basically outlined by those pixels adjacent to the spaces in the picture, but the pixel value varies greatly. This is because the adjacent pixel difference or the value after the pixel value will be close to 0, while the adjacent pixel difference or the value after the pixel value is different from 0, and the visual information of the picture is contained in the visual difference

formed by different pixels, so the picture after different or encryption will display the approximate outline of the original image, which will cause the eavesdropper to easily obtain the general information of the image, which is a huge threat to the safe transmission of information, so it is necessary to improve the encryption scheme. Let's talk about specific improvements.



Figure 3: The original picture.

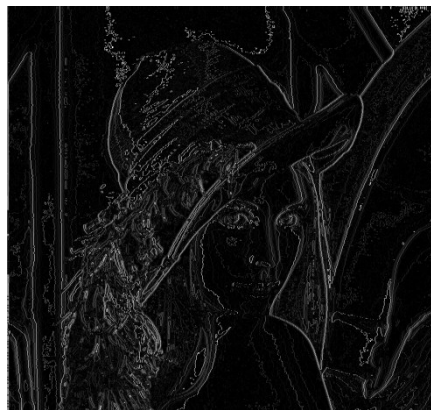


Figure 4: The encrypted picture.

3.2. Results and Analysis of the Improved Encryption Scheme

As mentioned earlier, the key to the problem is that the correlation between image pixels is large. The core idea of the improvement plan in this article is to reduce the correlation as much as possible. When encrypting, first read the image file and convert it into a numpy array, and then use random seeds (key) to generate an index of random disordered order, and then rearrange the pixel points according to the disordered index to form an encrypted image, and the new image after the disordered pixel is jointly encoded by the source. Become the image data to be transmitted [8], when decrypting, the image data is jointly decrypted by the source first, and then the same random seed is used to generate the same random disordered order index. Through inverse replacement, the order of the original pixel points is restored, and the original image can be restored to the pixel point sorting of the original image. Take Figure 1 as an example, use the above scheme to encrypt Fig.3, and the encryption result is shown in Fig.5. First of all, calculate the SSIM between Fig.3 and Fig.5. 0.00392, which is a scale smaller than the SSIM between Fig.3 and Fig.4, and completely hides all the information of the original image. The eavesdropper cannot obtain any useful information by observing the image, which enhances the security of encryption totality and reliability.

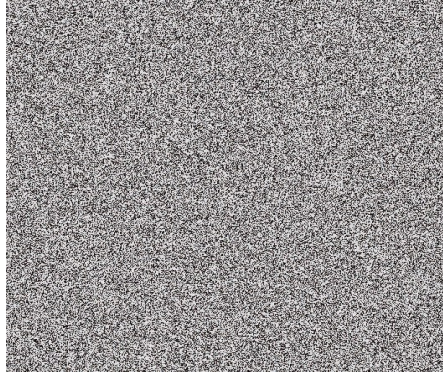


Figure 5: The image after disrupting the pixels and then encrypting it.

4. Simulated Eavesdropping on Encrypted Image Transmission

The above has improved the original coding scheme, reduced the correlation between the sources, and enhanced the security and reliability of encryption. The following is the eavesdropping recovery of the transmission of encrypted image information to verify the confidentiality of the encryption scheme. Here, according to Kerckhoffs's principle [9], it is assumed that the eavesdropper already knows the encryption scheme, including the main methods we use, such as the threshold secret sharing algorithm, the source joint encryption method, and the chaos of pixels.

The parameters are set to $L=5$, $m=2$, $S=T=16$, and divide the pixels of the image into 16-pixel sequences. Because the encrypted information generated by the joint encoding of the source cannot be cracked in information theory, the eavesdropper can only eavesdrop on m channels and cannot eavesdrop on all the encrypted messages. Therefore, this article assumes that when the encrypted information M_n cannot be obtained from the received data, the eavesdropper estimates the source $X_{n-1}=X_n$. For the image, that is, the estimated pixel sequence $X_{n-1}=X_n$, use the eavesdropped pixel sequence and the estimated pixel sequence to restore the image. Fig. 6 is the recovered image.

It can be intuitively observed that it and Fig. 5 are images similar to the white noise snowflake spots of old-fashioned TVs, and calculate the SSIM of Fig. 3 to get 0.0045425. From this point of view, the eavesdroppers have hardly recovered any useful information, and because we carried out a step-by-step operation of disrupting the image pixels before the joint encoding of the source, the resolution of this picture is 960×953 , the picture has a total of 914,880 pixels, and the size of the key space is the order of 914,880. Unless there is a huge computing power, it is almost impossible to solve the key by violent and exhausting methods. This encryption method effectively resists eavesdropping by disrupting pixels and source joint encoding.

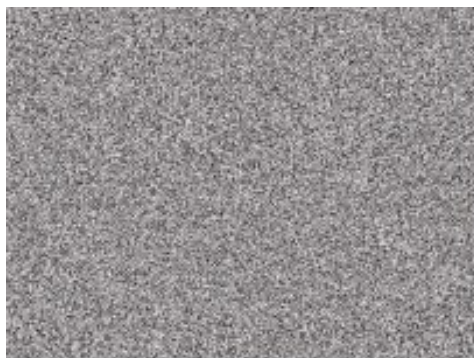


Figure 6: The image restored using the eavesdropped and estimated pixel points.

5. Conclusion

Based on the research of the existing security asymmetric multi-level diversity coding system (S-AMDCS), this paper deeply analyzes a source joint coding scheme and applies it to image encryption. First of all, this paper systematically studies the basic principle of source joint coding, and combines Shamir threshold secret sharing and XOR joint encryption to design an efficient image encryption scheme. Experimental analysis shows that this scheme can effectively improve the security of image data and enhance the anti-eavesdropping ability to a certain extent. However, theoretical analysis and experimental verification of this scheme found that the correlation between sources has a certain impact on encryption security, especially in image encryption scenarios. Due to the strong spatial self-correlation of natural images, the traditional source joint coding scheme may not be able to effectively hide the overall structure of the image, thus weakening the security of encryption.

In response to the above problems, this paper proposes an improved scheme based on random pixel replacement. The image pixels are randomly disrupted before the source is jointly encoded, thus reducing the correlation between pixels and making the encrypted image more difficult to analyze and restore by eavesdropping. The experimental results show that the improved scheme effectively enhances the visual concealment of the encrypted image, and the calculated SSIM (structural similarity index) is much lower than the original scheme, indicating that the encrypted image can hardly provide any original image information. In addition, in the simulated eavesdropping experiment, even if the attacker mastered the specific method of the encryption scheme, he still could not effectively recover the original image, which further verified the security and anti-attack ability of the scheme.

Generally speaking, the image encryption scheme based on source joint coding proposed in this paper achieves a good balance between computational complexity, encryption efficiency and security, and further improves the encryption effect of natural images through optimization strategies. However, there are still some directions that deserve further study, such as: (1) Improving encryption efficiency: The current scheme has high computational complexity, and there may be performance bottlenecks when processing ultra-high-resolution images. Parallel computing or a more optimized encryption process can be considered to improve efficiency. (2) Key management and distribution: This scheme relies on the keys of random pixel replacement. How to safely store and share keys in a distributed environment or cloud computing environment is still a problem worth studying in depth [10]. (3) Anti-noise and robustness optimization: In the future, the robustness of the encryption scheme in practical application scenarios such as noise interference and image compression can be studied to ensure that the encrypted image can still maintain high security and recoverability in harsh environments.

In summary, the research in this paper provides a new optimization direction for image encryption technology based on source joint coding, and further improves the application potential of encryption schemes in image security transmission. In the future, we will continue to explore more efficient and safer information source joint coding methods to meet the increasingly complex information security challenges.

References

- [1] Yeung, Raymond W. Multilevel diversity coding with distortion. *IEEE Trans. Inf. Theory* 41 (1995): 412-422.
- [2] Congduan Li, et al. Multilevel Diversity Coding Systems: Rate Regions, Codes, Computation, & Forbidden Minors. *IEEE Transactions on Information Theory*, 63 (2017): 230-251.
- [3] A. Shamir. How to share a secret, *Communications of the ACM*, vol. 22, no. 11, pp. 612-613, Nov. 1979.
- [4] C. Li, X. Guang, C. W. Tan, and R. W. Yeung. Fundamental limits on a class of secure asymmetric multilevel diversity coding systems, *IEEE Journal on Selected Areas in Communications*, vol. 36, no. 4, pp. 737-747, Apr. 2018.

- [5] Liaojun Pang, and Yumin Wang. *A new (t, n) multi - secret sharing scheme based on Shamir's secret sharing*. *Applied Mathematics and Computation* 167.2 (2005): 840-848. DOI:10.1016/j.amc.2004.06.120.
- [6] J. Lin, T. Gao, and C. Li. *A source-joint encryption scheme for asymmetric multilevel diversity coding systems*, in *Proceedings of the 15th International Conference on Wireless Communications and Signal Processing (WCSP)*, 2023, pp. 1-6.
- [7] V. Singh, V. Devgan, and I. Anand. *Determining image similarity with quasi-Euclidean metric*, *arXiv preprint arXiv:2006.14644*, 2020.
- [8] Zhang X. and Li Y. *A New Image Encryption Algorithm Based on Chaotic Mapping*, Hans Press, 2023, pp. 10-20.
- [9] Petitcolas, Fabien A. P. "Kerckhoffs Principle." *Encyclopedia of Cryptography and Security*, Springer, 2011, pp. 568-569.
- [10] J. Dean and S. Ghemawat. *MapReduce: Simplified data processing on large clusters*, *Proceedings of the 6th Symposium on Operating Systems Design and Implementation (OSDI)*, USENIX Association, 2004, pp. 137-150.