Proceedings of SEML 2025 Symposium: Machine Learning Theory and Applications
DOI: 10.54254/2755-2721/146/2025.TJ22522

Encryption Scheme Based on DES-CFB Encryption with A Source-Joint Encryption

Tailai Zhang

Hainan University, Haikou, China
Ztl584671407@gmail.com

Abstract: The joint-source encryption technology based on a multilevel diversity coding system in a multi-source network realizes information theoretic secrecy over the wiretap channel, and achieves threshold secrecy for the S-AMDCS system and prevents user overreach. However, this method is based on the assumption that all sources are independent binary sequences with the same rate, and the strong correlation between the pixels of the image is not fully considered. In order to solve the problem of information leakage in the image data with strong pixel correlation in the source-joint encryption system. To improve the anti-eavesdropping ability of image encryption, and generate an avalanche effect by enhancing the diffusion and confusion of information in the encryption process, this paper proposes a source-joint encryption scheme combined with DES-CFB stream encryption, and introduces a salt-based HMAC dynamic key generation mechanism and random initialization vector to ensure that the eavesdroppers are unable to recover the image content even if they can obtain multiple channels. The experimental results show that the proposed scheme significantly improves NPCR and UACI, and the difference between each pixel of the encrypted image and the original image is large, which improves the security of image transmission. In addition, the proposed scheme provides a powerful reference for the application of multimedia encryption, such as video encryption and medical image encryption.

Keywords: Encryption scheme, DES-CFB, image encryption, eavesdropping channel, step sampling

1. Introduction

The multilevel diversity coding system (MDCS) [1] and its development system, Secure Asymmetric MDCS (S-AMDCS) [2], are gradually gaining attention. These systems use threshold secret sharing (SS) and source-joint coding [3] to achieve information transmission with different security levels. The secret shares to be transmitted are generated by the threshold SS algorithm and distributed to each participant in the system [4,5]. This is a secure and efficient encryption method and can effectively prevent the user from overstepping his/her authority.

The source joint achieves threshold perfect secrecy, preventing information leakage if the eavesdropper's accessed channels remain below the security level [6]. However, due to the strong correlation between the pixels, the traditional source-joint encryption scheme often cannot completely disrupt the internal structure. As a result, the eavesdropper can recover the clear image outline by guessing the missing information even if he only gets the content of the number of access channels not exceeding the security level, so the confidentiality of the information cannot be realized.

Moreover, for ordinary users, this scheme cannot achieve information confidentiality. Additionally, the scheme does not fully ensure data security for regular users and struggles with key reuse, lacking strong diffusion, confusion, and avalanche effects.

In order to solve the above problems, this paper proposes a correlated source encryption scheme combining DES-CFB [7,8] encryption and source-joint encryption. The scheme can be regarded as the enhancement of the source-joint encryption scheme. After reducing the information source to be transmitted into a one-dimensional array, it is divided into groups by separating pixels, blurring the correlation, and adding DES-CFB for encryption. In DES-CFB encryption process, a random initialization vector (IV) and Salt are introduced. The Salt, combined with the channel's first source information by HMAC-SHA256-derived 8-byte DES keys, preventing key reuse. Then, the encrypted data is further processed by source-joint encryption to ensure that only the legitimate user who obtains enough channel information can restore the complete image, and the eavesdropper can only recover the distorted image even if he obtains part of the data. At the same time, NPCR, UACI [9] and adjacent pixel correlation [10] are used to evaluate the encrypted image. This secure image encryption scheme proposed for S-AMDCS can realize the encryption of correlated image sources, and has good diffusion confusion and avalanche effects.

2. Encryption scheme

2.1. Introduction to source-joint encryption schemes

There are L encoders and T decoders in S-AMDCS, each encoder can access all S binary sources, and their levels are increasing. The lower-level sources are used as keys to encrypt the higher-level sources. The SS threshold algorithm is added to the source-joint encryption scheme, and the security level of the model is set to be m. which means that if an eavesdropper eavesdrops on the number of channels that are not greater than m, the eavesdropper cannot obtain any effective information. Moreover, the decoding level of different users is set according to the number of channels more than m.

2.2. Generation of encrypted and decrypted messages

The source-joint scheme in order to achieve threshold confidentiality, the lowest level of source X1 is encrypted using the shamir algorithm (k, n) to generate SS data about X1 and distribute it to L encoders, and subsequently for each level X_n $(2 \leq n \leq S)$ that is higher than 1, which is encrypted doctoring it into the corresponding encrypted message Mn, using Xn−1 as the key with the following formula:

$$M_n = X_{n-1} \text{ xor } X_n \tag{1}$$

At the same time, each Ei generates a subset combinations (other than Ei) to distribute the ciphertext. Decryption is then the inverse of encryption, where first (k, n) computes the lowest-level source X1 using the SS data of the lowest threshold, and then based on:

$$X_n = X_{n-1} \text{ xor } M_n \tag{2}$$

Recovering a higher-level source, so once the previous Xn−1 source is recovered, whether the next source X_n can be recovered depends on whether the ciphertext Mn is known to the user in the selected channel.

2.3. The use of source-joint scheme under image

In MDCS, in addition to textual information, encrypted transmission of images is also required. Source joint encryption is proposed under the assumption that all sources are independent binary sequences with the same rate, but in practice, when transmitting image information, most of the pixel points are strongly correlated, and simple different-or encryption of two consecutive pixel points is undoubtedly the same correlation in ciphertext.

In addition, we assume that each source has a length of 8 and is somewhat correlated, forming common information patterns. The image pixel point distribution generally satisfies Gaussian, bimodal, uniform, or lognormal distribution, and under this assumption generally satisfies the normal distribution. In the joint source encryption scheme, the use of a low-level source as the key for the next source for encryption is not reasonable for a natural image that satisfies the normal distribution or a specific image that satisfies the bimodal distribution, lognormal distribution, or uniform distribution, because a specific message is conveyed in the image, and so in encryption the ciphertext correlated with the original image.

3. Des combined with source-joint encryption scheme

Since the source joint encryption scheme does not hide the image information perfectly in image encryption, in this experiment a file in jpg format is used as the source, while considering that after compressed jpg transmission, users who do not have access to the complete byte stream cannot restore the image either legally or illegally, it is assumed that the source of the information to be transmitted is the uncompressed or uncompressed jpg image file, and at the same time, it is employed that the RGB mode image be the input source.

3.1. Step sampling

Since there is still a certain correlation between adjacent or spaced n pixels, the step sampling method is introduced to digitize the image signal, and the original signal source is selected as the 0th, nth, 2nth, ……, and knth pixels are divided into groups, and the length of each group is padded where it can be divisible by S.

For S-AMDCS with L encoders and security level m, according to the formula:

$$S = T = \sum_{i=m+1}^{L} C_{L}^{i} \tag{3}$$

Calculate the number of elements of the source array that can be known at one time. First of all, the input RGB format image color channels are divided away from each other, and then step sampling for each channel, which is divided into a number of sub-block sets, each set of independently storing dispersed pixel points, to destroy the overall structure. Subsequently, the length of each sub-block is calculated to ensure that it is able to divide the preset chunk length S. If the sub-block length is insufficient, it is made up by random byte padding so that it is able to be divided by S. The length of random byte padding of the sub-block is also recorded, which can be recovered without loss. Different sampling strategies are supported by flexibly adjusting the size of parameter n, thus increasing the obfuscation of encrypted data.

3.2. Generation of encrypted messages

In order to achieve secure encryption of image data, fuzzy correlation, the proposed scheme uses DES-CFB combined with a source-joint encryption scheme. Firstly, the image data is preprocessed, and the color image is divided into three independent channels, R, G and B. The data of each channel is expanded in the form of a byte stream and grouped according to a fixed step size n.

In the encryption process, each data block is divided into sub-blocks of length S, and each byte is encrypted using DES-CFB. Key generation is done by splicing the first lowest level source X1 of the image data with 8 bytes of random Salt and then generating the message digest taking the first eight bytes as key.

$$\mathrm{combined} = X_1 || \mathrm{Salt}$$

$$\mathrm{HMAC}_{\mathrm{SHA256}}(\mathrm{Salt}, \mathrm{combined}) \tag{4}$$

The initialization vector IV is introduced in CFB mode to avoid duplicate ciphertexts, Pi denotes the ith plaintext block, each block is 1 byte in length, the first byte of IV iso-ortho with DES encryption to generate the ciphertext C1 for each group of P1, then the first byte of IV is discarded and the generated ciphertext is spliced with DES encryption, and the subsequent Pi is iso-ortho with Oi [0] to get the ciphertext Ci

$$O_1 = E_K(IV)$$

$$C_1 = P_1 \oplus O_1[0]$$

$$O_i = E_K(IV[1:]||C_{i-1})$$

$$C_i = P_i \oplus O_i[0] \tag{5}$$

The data is encrypted with DES into a new source data X_n , which is subsequently used to generate an encrypted message Mn using the joint source encryption method

$$M_n = X_{n-1} \oplus X_n \tag{6}$$

If and only if all of the initialization vector IV, step length n, Key, M_n, X_{n-1} known to all, X_n can be restored.

$$C_n = C_{n-1} \oplus M_n$$

$$P_n = D_k\left(C_n\right) \oplus C_{n-1} \tag{7}$$

Finally, the SS data and ciphertext are dispersed to different channels through the distribution method of the source-joint encryption method. The process formula is as follows:

$$\mathcal{L}(A) = 1 + f_1(n) \sum_{i=m+1}^{n-1} C_L^i + \sum_{k=1}^{n} f_2(k) \sum_{j=a_{k-1}+1}^{a_k - 1} C_{L-j}^{n-k}$$

$$f_1(n) = \begin{cases} 1, \text{if } n > m+1 \\ 0, \text{if } n = m+1 \end{cases}, f_2(k) = \begin{cases} 1, \text{if } a_k > a_{k-1}+1 \\ 0, \text{if } a_k = a_{k-1}+1 \end{cases}$$

$$\mathrm{Process}_i = \{A \subseteq \left\{\left\{E_1, E_2, \ldots, E_L\right\} \backslash E_i\right\} : |A| > m\}$$

$$\mathrm{store}_{E_i} = \mathcal{L}\left(P_i\right)$$

$$M_{E_i} = f_M\left(\mathrm{store}_{E_i}\right) \tag{8}$$

3.3. Recovery of sources

When the number of channels D_j that the decoder can access is greater than the security level m, it can recover C_1 by extracting at least m+1 SS data from the received data. In addition, through the received Mn, it can recover Cn, and then based on the known key and IV, it can recover X_n .

3.4. An example

An example will be presented to illustrate the combination of the proposed DES-CFB and the source union encryption scheme. When L= 5 and m = 2, according to operation (1), the number of sources at different levels is S = 16 with a step size of 2. Assuming source data

[[B1, G1, R1], … …, [B17, G17, R17]]

[[B18, G18, R18], … …, [B34, G34, R34]]

3.4.1. Encryption process

Fig. 1 shows the process of encryption. The first step of encryption is to extract different color channels, and then carry out step sampling with a step size of 2 to obtain. [[X1, X3, … …, X33], [X2, X4, … …, X34]]. The padding random byte is divisible by S. for example:

$$\left[\left[X_1, X_3, \dots, X_{63}\right], \left[X_2, X_4, \dots \dots, X_{64}\right]\right]$$

Each 1 byte in each group is noted as Pi, using operation (2) to generate the key, and continue to use operation (3) to encrypt out the Ci

The second step of encryption is to generate SS data by applying the (3,5) threshold SS algorithm to generate 5 SS data (SS1, SS2, … SS5), using the first data in Ci as the multi-party shared key, and distributing it to 5 encoders.

The third step of encryption is to generate the source-joint coded data. Also take the above generated data in E_1 as an example. Generated by operation (6) $\text{Process}_1 = \{\{E_2, E_3, E_4\}, \{E_2, E_3, E_5\}, \{E_2, E_4, E_5\}, \{E_3, E_4, E_5\}, \ \{E_2, E_3, E_4, E_5\}\}$

$$\text{store}_{E_1} = \{7,8,9,10,15\}$$

Generate the encrypted message as transmitted store_{E_1}

$$M_{E_1} = f_M\left(\text{store}_{E_1}\right) = \{M_8, M_9, M_{10}, M_{11}, M_{16}\}$$

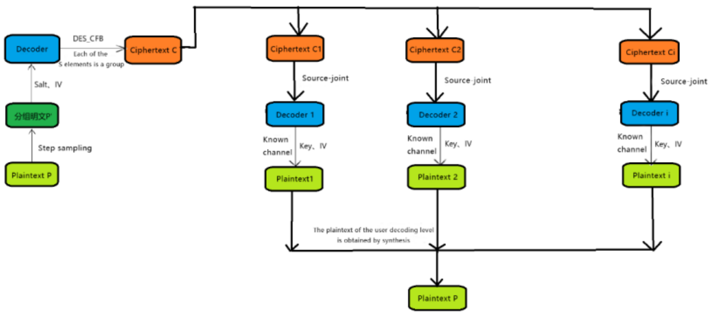

Figure 1: Process of applying DES-CFB combined with source-joint encryption and decryption in S-AMDCS with L=5 and m=21

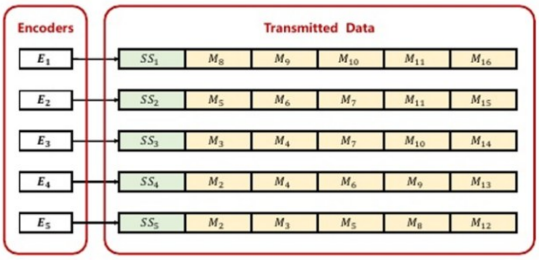
Encoders
Transmitted Data
E_1 SS_1 M_8 M_9 M_{10} M_{11} M_{16}
E_2 SS_2 M_5 M_6 M_7 M_{11} M_{15}
E_3 SS_3 M_3 M_4 M_7 M_{10} M_{14}
E_4 SS_4 M_2 M_4 M_6 M_9 M_{13}
E_5 SS_5 M_2 M_3 M_5 M_8 M_{12}

Figure 2: Ciphertext after DES-CFB encryption Ci result of source-joint co-allocation

According to equation (6), the encrypted message in ME1 will be transmitted through the channel corresponding to E1 while splicing the SS data SS1 as shown in Figure 2.

3.4.2. Decryption process

Consider a valid decoder Dj, among $\mathrm{In}(\mathrm{D_j}) = \{\mathrm{E_3}, \mathrm{E_4}, \mathrm{E_5}\}$, according to equation (6), the preset decoding level $\mathrm{D_j}$ which is $\mathrm{L}\left(\mathrm{l} = \mathrm{In}(\mathrm{D_j})\right) = 10$ if the channel corresponding to $\mathrm{E_3}, \mathrm{E_4}, \mathrm{E_5}$. The steps of decryption are firstly extracting the corresponding SS data ($\mathrm{SS_3}, \mathrm{SS_4}, \mathrm{SS_5}$), from the accepted data and using (3,5) threshold algorithm, recovering the lowest level source X1, then extracting the encrypted message from the accepted data:$\mathrm{M_2}, \mathrm{M_3}, \mathrm{M_4}, \mathrm{M_5}, \mathrm{M_6}, \mathrm{M_7}, \mathrm{M_8}, \mathrm{M_9}, \mathrm{M_{10}}, \mathrm{M_{12}}, \mathrm{M_{13}}, \mathrm{M_{14}}$, and recovering $\mathrm{X_2}, \mathrm{X_3}, \dots, \mathrm{X_{10}}$ according to equation (4). Since the accepted data does not contain M11, X11 and higher-level sources cannot be recovered, padding 0 to S bytes. As a result, it can recover $\mathrm{C_1}, \mathrm{C_2}, \dots, \mathrm{C_{10}}$, and then decrypts it according to equation (3), recovers the original text that meets the decryption level, and finally resamples it according to step n and reorganizes it into a picture.

4. Security analysis

4.1. Weaknesses of source federated encryption schemes

In the original scheme, although the higher BER improves coding performance, meanwhile, the individual pixel points have strong correlation, while the source joint encryption scheme only encrypts two consecutively independent ciphertexts in an exclusive OR manner, and the correlation of the ciphertexts still exists, which allows the attacker to obtain an encrypted image with original information and structural features by guessing an inaccurate X1, and then stitching the ciphertexts, while eavesdropper is able to steal m channels Information. Confidentiality of the message cannot be realized. This paper assumes that the eavesdropper is aware of the SS-based source-joint encryption scheme and can extract mmm channels of encrypted image information, and at the same time, estimate $\mathrm{X_n} = \mathrm{X_{n-1}}$ when the eavesdropper is unable to obtain Mn from the accepted data.

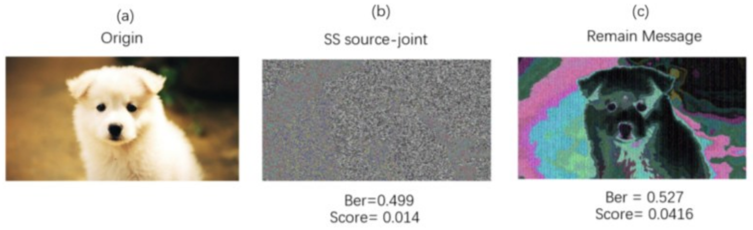

Figure 3: Wiretap image without grouping

Figure 3(b) is the eavesdropping image using the source joint scheme, and Figure 3(c) is the eavesdropping image under retaining the M_i as X_i, in order to reduce the interference between neighboring color channels. Figure 4 is the result of eavesdropping on the image based on the SS-based source union scheme under the separated color channels, which shows that decrypting the encrypted image after encryption with the original decryption mode will make the image even more confusing; Figure 5 is the result of decrypting the image under the separated color channels by guessing the decryption of X_1 and $X_n = M_n$, and the result is that the original image can be seen in the outline, which shows that there is still a correlation among the encrypted messages.

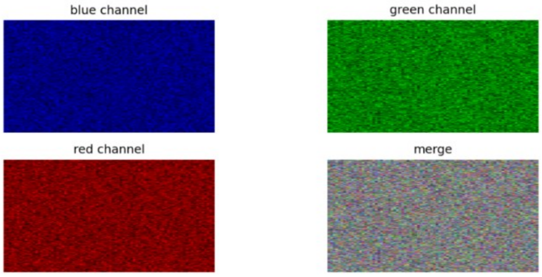

Figure 4: Eavesdropping of the picture in the separated color channel based on the SS source- joint scheme

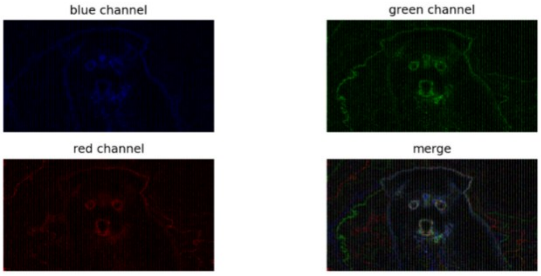

Figure 5: Decryption by guessing X_1 under separate color channels, making $X_n = M_n$

4.2. Mathematical analysis of eavesdropping results

Among the eavesdropping results, the eavesdropping method that directly uses the ciphertext Mn as the source X_n obtains the most information from the image (Figures. 3 and 5), whether it is encrypted by directly converting the color to a byte stream or by separating the color channels, and in the source joint encryption scheme according to (4) performing XOR encryption for the two neighboring sources X_{n-1}, X_n. Due to the characteristics of high correlation in the picture, the following argumentation is made.

For any image pixel Xi and key K_i:

$$M_i = X_i \oplus K_i$$

Given a pixel point (adjacent or non-adjacent) X_j, which has a key K_j and a ciphertext M_j , try to analyze the correlation:

$$M_i \oplus M_j = (X_i \oplus K_i) \oplus (X_j \oplus K_j)$$

After simplification:

$$M_i \oplus M_j = (X_i \oplus X_j) \oplus (K_i \oplus K_j)$$

If the key K has a periodic or fixed structure ($K_i = K_j$), then the ciphertexts retain their previous relationship to each other. We know that the structure comparison formula in SSIM is:

$$s(x, y) = \frac{\sigma_{xy} + c_3}{\sigma_x \sigma_y + c_3} \tag{9}$$

Where σ_x, σ_y is the standard deviation of x and y, σ_{xy} is the covariance of x and y, and c_3 is a constant avoiding a denominator of 0. There is S (M, X) approximating 1.

There are in the case of neighboring pixel points:

$$M_i = X_{i-1} \oplus X_i$$

$$M_{i+1} = X_i \oplus X_{i+1}$$

A change in a pixel Xi affects only its associated Mi and M_{i+1}, but has no effect on the rest of the ciphertext. Without making each bit change in the plaintext capable of affecting all bits of the multibit literals in the ciphertext, the eavesdropper may be able to recover in this scheme through linear recursion and low diffusivity.

The good performance in Figure 3(b) is due to the fact that the X1 decryption error leads to good diffusion in the subsequent decryption. The good threshold secrecy in the X1 decryption makes it almost impossible for the eavesdropper to decrypt the correct plaintext. Let the lowest level of the decrypted source be X1′.

$$X_2' = X_2 \oplus X_1 \oplus X_1'$$

Suppose there is a ciphertext M3 missing, making $X_3' = X_2'$, recovering X4′ then

$$X_4' = X_4 \oplus X_2 \oplus X_1 \oplus X_1'$$

Similarly, if there is a missing ciphertext, the resulting plaintexts will not be similar in structure.

5. Performance analysis

5.1. NPCR and UACI

Ideally, image encryption should be key sensitive; a change of a single bit in the key should produce a completely different encryption result called key sensitivity, where the sensitivity is evaluated using two parameters: Number of Pixel Change Rate (NPCR) and Uniform Average Change Intensity (UACI). The NPCR and the UACI denote the number of pixels of change between two encrypted images and the number of average change intensities. Their corresponding ideal values are NPCR=99.6094% and UACI=33.4635%, which are calculated as follows:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M * N}$$

$$D(i,j) = f(x) = \begin{cases} 1 & C_1(i,j)! = C_2(i,j) \\ 0 & \text{others} \end{cases} \tag{10}$$

In addition, UCAI can be used to evaluate the average value of color intensity contrast, and the formula is as follows:

$$UACI = \frac{\Sigma\left(C_1(i,j) - C_2(i,j)\right)}{M * N * 255} \tag{11}$$

5.2. Statistical analysis - correlation analysis of adjacent pixels

Correlation analysis refers to the analysis of two or more correlated variable elements to measure the degree of close correlation between variables. Due to the high correlation between adjacent pixels of an image, one pixel often leaks the information of its surrounding pixels. The attacker can use this feature to reason about the next pixel, so as to realize the recovery of the entire plaintext image. Adjacent pixels have similar intensities. Therefore, the strong correlations must be broken to avoid statistical attacks. The correlation coefficients in the horizontal, vertical and diagonal directions are calculated using the following formula:

$$R_{xy} = \frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} \left(x_i - E(x)\right)^2$$

$$\mathrm{cov}(x) = \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)) \tag{12}$$

Where y is the adjacent pixels of x, N is the total number of pixels in an M × N image, and R_{xy} is the correlation between two adjacent pixels, cov (x, y) is the covariance at pixels x and y, $\sqrt{D(x)}$ is the standard deviation, D(x) is the variance, and E(x) is the mean. In general, the correlation between adjacent pixels of a plaintext image is close to 1, while the correlation between adjacent pixels of a ciphertext image should be close to 0.

6. Experimental results

In this subsection, the ability of an image to be encrypted in the face of external eavesdropping is verified, analyzed in terms of NPCR and UACI and the adjacency correlation, and in each round of simulations, m channels are randomly set to be able to be eavesdropped on, and the attacker randomly guesses at the missing SS data, since in this case the eavesdropper theoretically obtains the most information.

6.1. NPCR vs UACI

For a system with L = 5 and m = 2, 1000 rounds of simulations were performed and the results are shown in Fig. 6. It can be seen that when the proposed scheme is used, the average value of each channel of NPCR of external eavesdropping results is 0.9961. In UACI, the average value of the blue channel is 0.3296, the average value of the green channel is 0.3056, and the average value of the red channel is 0.3118. Their corresponding ideal values are NPCR= 99.6094%, UACI=33.4635%, and the experimental results are close to these, which show that the encryption scheme can effectively disrupt the pixels in the image. The pixel difference between the ciphertext image and the original image is very large, and the eavesdropper cannot easily recover the original image by monitoring the encrypted image.

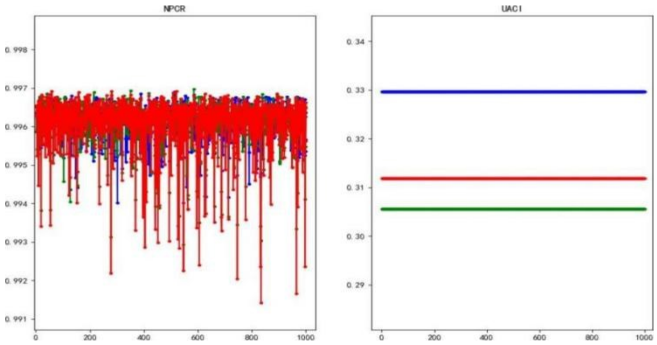

Figure 6: NPCR and UACI of encrypted image compared with original image

6.2. Adjacent pixel correlation

By randomly selecting 3000 pairs of adjacent pixels, the correlation coefficients in the horizontal, vertical and diagonal directions of the original image and the encrypted image are calculated respectively according to the above definition of correlation coefficient. The experimental results are shown in Figure 7 and Figure 8.

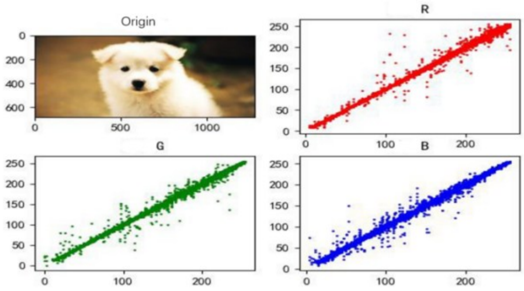

Figure 7: Correlation between adjacent pixels of the source image

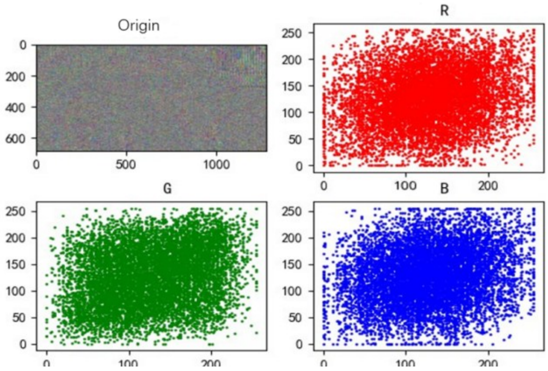

Figure 8: Neighboring pixel correlation of encrypted image

The correct number of pixels that can be restored is different for different user levels, so user access restriction can be realized to some extent, as shown in Figure 9.

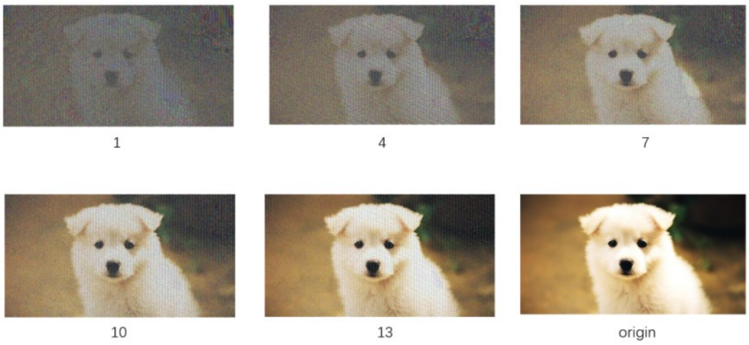

Figure 9: Images acquired at different levels

7. Conclusion

This study proposes an enhanced encryption scheme combining DES-CFB stream encryption with source joint encryption to address the information leakage risk in S-AMDCS when processing highly correlated images. The scheme disrupts pixel correlation using step sampling and introduces random initialization vectors (IV) and Salt to generate dynamic keys, preventing key reuse and improving ciphertext security and resistance to analysis.

Experimental results show that the proposed encryption scheme performs well in NPCR and UACI, which is close to the ideal encryption standard, and is able to effectively disrupt the pixel distribution of the original image, so that the eavesdropper cannot recover a clear image even if he obtains part of the channel information. Meanwhile, correlation analysis shows that this scheme can effectively reduce the pixel correlation of the encrypted image, so that the ciphertext image no longer has the recognizable features of the original image both visually and statistically. In addition, the scheme is able to realize the access control for different levels of users under the multi-level decryption model, restricting that the high-security data to authorized users.

Although the scheme in this paper has achieved significant results in improving ciphertext security and reducing the risk of information leakage, the scheme also has some limitations, particularly in encryption and decryption efficiency. Further research is needed to balance computational complexity and security, such as implementing parallel encryption and optimizing multi-core CPU performance. Additionally, refining the user privilege hierarchy is essential, as different user levels may still retain key information even if some data is lost. Future work should focus on further differentiating access levels. Furthermore, while the current study is based on RGB images, extending the approach to video and medical image encryption is a potential research direction.

Overall, the scheme proposed in this paper provides a method to hide information for highly correlated images, and shows good performance in terms of security analysis and anti-attack capability, which provides a new reference direction for multi-source secure transmission security.

References

[1] Yeung, Raymond W. (1995). Multilevel diversity coding with distortion. IEEE Trans. Inf. Theory, 41,412-422.

[2] Congduan Li, Xuan Guang. (2017). Asymmetric Multilevel Diversity Coding Systems With Perfect Secrecy. IEEE Transactions on Vehicular Technology, 66, 8558-8562.

[3] Lin, J., Gao, T., & Li, C. (2023). A Source-Joint Encryption Scheme for Asymmetric Multilevel Diversity Coding Systems. 2023 International Conference on Wireless Communications and Signal Processing (WCSP), pp.743-748.

[4] Shamir, A. (2021). How to Share a Secret (1979).

[5] Blakley, G.R. (1899). Safeguarding cryptographic keys. 1979 International Workshop on Managing Requirements Knowledge (MARK), 313-318.

[6] Ozarow, L.H., & Wyner, A.D. (1984). Wire-tap channel II. AT&T Bell Laboratories Technical Journal, 63, 2135-2157.

[7] *National Bureau of Standards, U.S. Department of Commerce, Washington D.C.(1977). Data Encryption Standard. Federal Information Processing Standard, FIPS 46.*

[8] *National Bureau of Standards, U.S. Department of Commerce, Washington D.C. (1980). DES Modes of Operation. Federal Information Processing Standard, FIPS 81.*

[9] *Wu, Y., Noonan, J.P., & Agaian, S.S. (2011). NPCR and UACI Randomness Tests for Image Encryption.*

[10] *Benesty, J., Chen, J., & Huang, Y. (2008). On the Importance of the Pearson Correlation Coefficient in Noise Reduction. IEEE Transactions on Audio, Speech, and Language Processing, 16, 757-765.*