*Journal of Network Intelligence* ©2025 ISSN 2414-8105 (Online)
**Taiwan Ubiquitous Information** Volume **10**, Number **1**, February **2025**

# The Image Encryption Method Based on ADA-DeepLab Image Segmentation and GAN Key Generation

Xian-He Sun, Hong-Bin Ma*, Meng-Sheng Wang

School of Electronic Engineering
Heilongjiang University, Harbin 150080, China
xh321076856@163.com, mahongbin@hlju.edu.cn, 18756045935@163.com

Qi-Tao Ma*

China Mobile Group Shanghai Co., Ltd., Shanghai, China
jack_coldsweat@163.com

*Corresponding author: Hong-Bin Ma, Qi-Tao Ma

Received March 4, 2024, revised June 30, 2024, accepted August 2, 2024.

Abstract. *Traditional image encryption methods usually focus on the encryption of the entire picture. However, only a small part of the data in the image may carry key information Using the same encryption method may pose a risk of being deciphered. Therefore, we propose an image adaptive encryption method. Firstly, in the process of image segmentation with small targets and multi-target scenarios, issues such as target omission, miscalculation, and prediction gap presence can lead to the loss of a large number of details and a significant reduction in the amount of information. We have designed the ADA-DeepLab image adaptive segmentation network, introduced the variable pyramid module to better localize the regions that need prediction in the adaptive perception domain, and added two attention mechanisms to complement each other, enhancing the recovery of semantic information more efficiently. The research in this paper has been experimentally demonstrated using the PASCAL VOC 2012 dataset. The results show that the proposed ADA-DeepLab model achieves a significant improvement in accuracy and is capable of segmenting the target more accurately. Secondly, we propose a new key generation model, R-GAN, to address issues of network instability and short chaotic cycles in GAN training. We introduce a residual network to generate sequences with larger periods using the GAN model by training on input chaotic sequences. The generator and discriminator are enhanced to stabilize the training process. Finally, the segmented important data rows are encrypted. Experiments have proven that the generated key is more secure and randomized, offering a better hiding effect on both the key regions and the entire image. This method is highly effective in safeguarding important data and holds significant potential for practical applications.*

**Keywords:** Image segmentation, Attention Mechanism, GAN, Identity privacy, Regional Encryption

1. **Introduction.** Image security is relevant to our lives, more and more attention has been paid to how to prevent unauthorized access and tampering to the images. Image sharing on social platforms involves the privacy of personal life [1–3], therefore image encryption is crucial in image security. This encryption process utilizes complex mathematical algorithms and keys to convert the original image into an encrypted form, effectively

protecting the image information from unauthorized access. The key is a confidential parameter that can only be decrypted by the person holding the correct key [4]. This step is the key link to maintain image security and privacy. Therefore, the selection and management of the key is critical to the effectiveness of the overall image encryption, which determines the reliability and protection capability of the encryption system. In summary, image encryption is a crucial technology in the digital era, providing an important safeguard for maintaining personal privacy and information security.

To address the issue of key security and complexity, researchers have commonly adopted chaotic sequences as a common key generation method. The core of this method is the utilization of chaotic systems [5], whose generation process relies on nonlinear dynamical systems such as chaotic equations or mappings. Chaotic systems can produce seemingly random sequences of outputs, and these parameters exhibiting chaotic states can be used as keys for encrypting and decrypting data. The outputs of chaotic systems are difficult to predict and reconstruct, so they can be applied to various image encryption techniques to improve the security of encryption algorithms. However, there are some shortcomings in chaos-based cryptographic schemes [6], for example, short cycle length due to the limited accuracy of computers is one of the important problems of chaotic keystream generators [7], to solve this problem, researchers have proposed several key generation schemes [8], one of the solutions is to increase the dimension of the chaotic system. A high dimensional chaotic system has multiple Lyapunov exponents, two or more of which are positive, it is a hyper chaotic system. The classical Lorenz and Chen chaotic system is a representative example of this [9]. By introducing high-dimensional chaotic systems, researchers have tried to overcome the short cycle length problem and increase the complexity of key generation, thus improving the security of image encryption.

Current image encryption methods usually encrypt the whole image, and relatively few studies have been conducted on encrypting the critical regions in the image, however, only a part of the sub-images in an image may be important [10], focusing on the confidential sub-image part can improve the processing efficiency and reduce the scale of encryption operations, thus reducing the consumption of computational resources and time, so in this paper, we also introduce an adaptive segmentation model for images to better delineate the important regions. Natsheh et al. [11] proposed a pixel threshold segmentation technique to encrypt the private regions of medical images in the spatial domain and Alsafyani et al. [12] proposed a method that combines cryptographic knowledge and deep learning architecture for encryption and decryption process of face region. Although the above research achieved encryption of regions of interest, it did not encrypt according to contours, but instead used region block encryption. One of the conditions for good encryption of contours is accurate image segmentation, in the field of image segmentation, researchers have extensively explored various methods and techniques to enhance the accuracy and efficiency of image segmentation.Many scholars are dedicated to improving traditional CNN methods [13], and Approaches based on Transformer [14] models have also emerged to meet the challenges in image segmentation, for example, FCN [15], by introducing the hopping connection and up sampling technique, which enables the network to retain more spatial information. Then, researchers proposed network structures such as SegNet [16], U-Net [17] and PSPNet [18], which further improve the segmentation accuracy by introducing encoder-decoder structure, multi-scale information fusion and spatial pyramid, etc. The DeepLab family came out of nowhere, and it made a The DeepLab family came out of nowhere and achieved amazing results at that time, but based on the DeepLabV3+ model, when dealing with small targets or multiple targets, DeepLabv3+ loses a lot of details about the object due to its network structure design and the up-sampling process, which results in the loss of target information.

## 2. Related work.

**2.1. Deformable convolution.** One of the key features of deformable convolution [19] is its adaptive nature, deformable convolution adapts to the deformation of the target by learning the pixel offsets, which enables the convolution kernel to adaptively adjust its shape and size to fit irregular target shapes. Traditional convolutional operations may not be able to adapt well to the deformation of the target, Deformable convolution adjusts the convolution kernel's pattern based on the target size and image contours. This enables the model to better adapt to a variety of targets and improves the robustness and generalization ability of segmentation, which is very important for irregular targets in segmentation tasks. In Figure 1, (a) denotes normal convolution and (b) denotes deformable convolution. The deformable convolution adaptively adjusts the sense field according to the target and is therefore well suited for adaptive image segmentation.

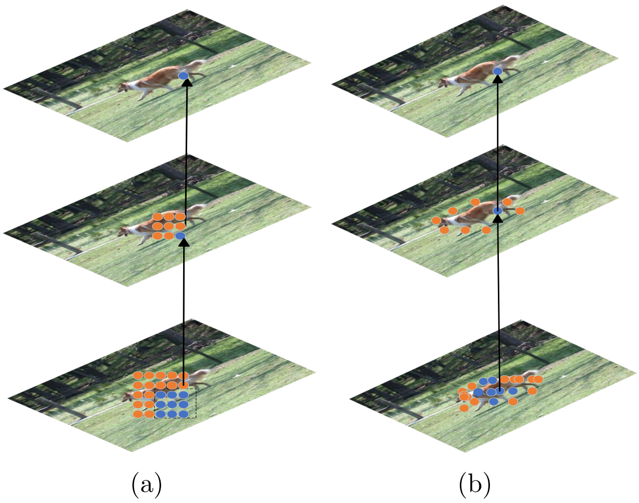

(a) (b)

Figure 1. Feature sampling method

**2.2. Generative adversarial network.** GAN [20] consists of two main components. The generator's objective is to learn the generation of pseudo-random sequences resembling real random sequences, while the discriminator is dedicated to accurately distinguishing between real and generated data. The adversarial nature of this training process enables the generator to continuously enhance its ability to generate authentic sequences, while the discriminator continually improves its accuracy in distinguishing between real and forged sequences. In each training round, GAN takes random noise as the input for the generator and employs the Chen chaotic system as input for the discriminator. Through the discriminator's comparison of real and generated data, the parameters of both the generator and discriminator are updated. In this paper, we leverage the non-linear and powerful generative capabilities of the Generative Adversarial Network to handle chaotic sequences, generating novel pseudo-random sequences as cryptographic keys.

**3. ADA-DeepLab network.** Firstly, after the original feature extraction of the input image, the inter-pixel interactions are obtained through the feature refinement module to eliminate the grid effect, and then the DCN module is utilized to make the network flexibly adjusted according to the target scale, to obtain the semantic information of the different receptive fields and merge them together, and the adaptive segmentation module is utilized to better locate the region to be predicted through the adaptive receptive field. The adaptive segmentation module can better locate the region to be predicted through the adaptive receptive field, obtain the positional correlation between pixels to improve the modeling ability of deformation. The ADA-DeepLab network model is shown in Figure 2:

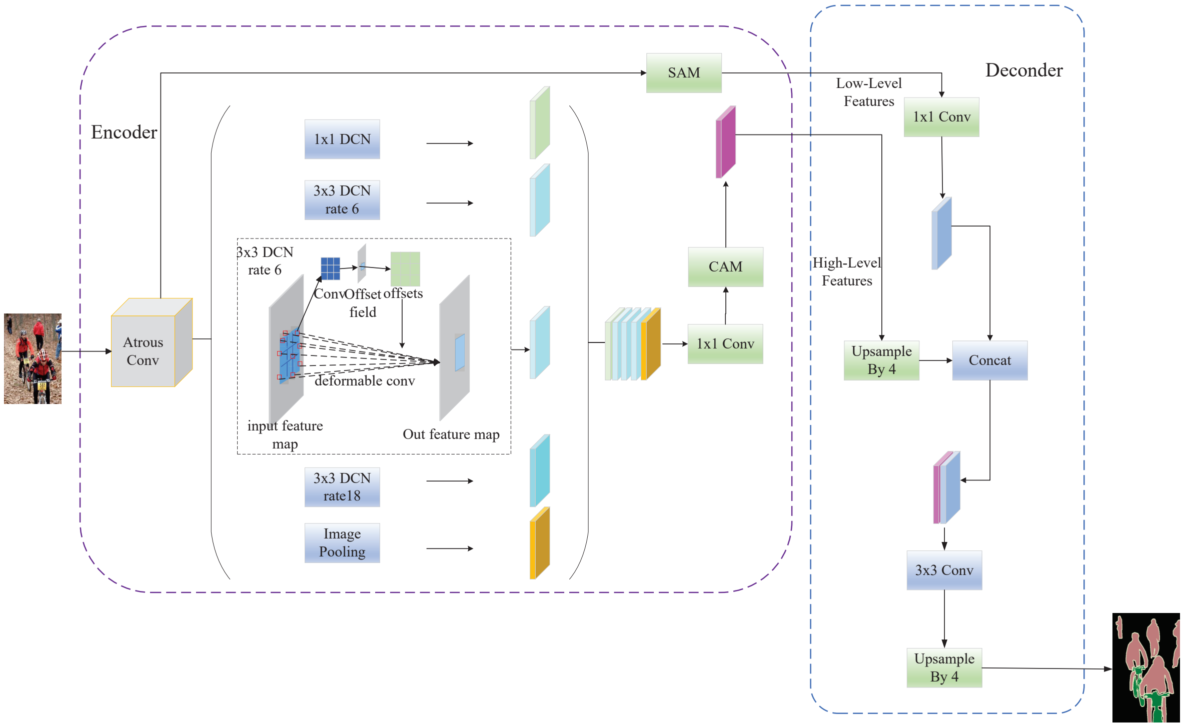


FIGURE 2. ADA-DeepLab network modeling

Specifically firstly, the $1 \times 1$ deformable convolution in the model, the 3x3 deformable convolution with different null rates and the global average pooling operation are processed separately and then the feature fusion operation is carried out on them, and the obtained feature maps are then subjected to the $1 \times 1$ convolution, and the dimensionality reduction operation is carried out to reduce the number of channels from 2048 to 256, and secondly, the channel attention is utilized to fusion the feature maps obtained from the adaptive segmentation module so as to enhance the response to specific semantics. Effective high-level features are obtained through weights. In the decoding phase, the high-level semantic information is up-sampled twice, once by a factor of 2 and again by a factor of 4. Low-level features are weighted to recover semantic information more efficiently, merging features to recover detailed target boundaries.

3.1. **DCN models.** The DCN module designed in this paper effectively breaks the original specification of point sampling, whereas the previous standard convolution samples through a fixed grid $R$ , and each sample point undergoes a weighting operation by a convolution kernel, the DCN module is based on the calculation of the standard convolution, and the offsets are added at the time of sampling, For example a $3 \times 3$ convolution kernel with rate 1, for a center sample point position $p_0$, Equation (1) is the output of a standard convolution:

$$y(p_0) = \sum_{p_n \in R} w(p_n) \cdot x(p_0 + p_n) \tag{1}$$

The input feature map is denoted as $x$, the output feature map is denoted as $y$, $x(p_n)$ denotes the weight of the $p_n$ position, and $x(p_n)$ denotes the pixel value of the input feature map at the point $p_n$ position. The offset vector is introduced by sampling the input feature map $x$ through Equation (2):

$$y(p_0) = \sum_{p_n \in R} w(p_n) \cdot x(p_0 + p_n + \Delta p_n) \tag{2}$$

$\Delta p_n$ is the offset of the $p_n$ position. Since $\Delta p_n$ is basically a small number and the value of $x(p_0 + p_n + \Delta p_n)$ may not be an existent point on the input feature map, a bilinear interpolation algorithm is used so that the sampling position can fall within the effective range of the input feature map. The new input feature map is formed by bilinear interpolation transformation, and the new feature map formed can still maintain the same spatial resolution as the original feature map.

3.2. **Attention mechanism models.** To ensure the effective recovery of target boundary information, Channel Attention (CA) is introduced before feature map fusion. CA aims to enhance the model's performance by weighting the feature maps and filtering out information crucial to the current task. This allows for precise control over different channels, capturing target-related information in a more targeted manner, thus improving generalization performance for unseen data. Figure 3 illustrates the CA module.

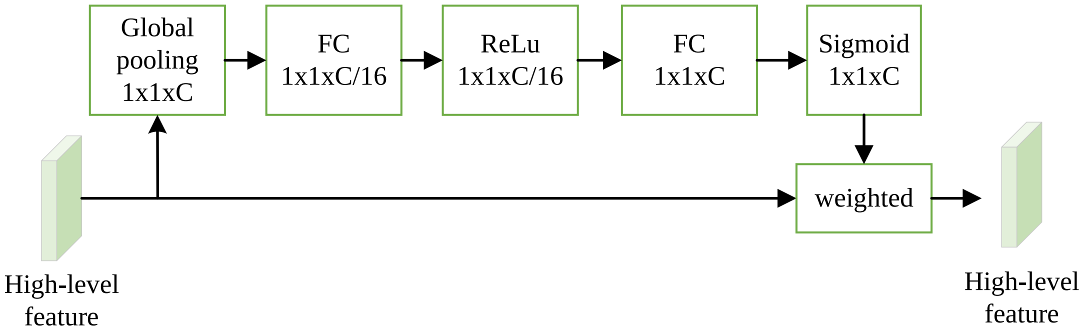


Figure 3. Structure diagram of channel attention

The proposed CA is divided into two parts: compression and activation. The compression part compresses the feature map by global average pooling as shown in Equation (3):

$$z_c = F_{sq}(u_c) = \frac{1}{W \times H} \sum\nolimits_{i=1}^{W} \sum\nolimits_{j=1}^{H} u_c\,(i, j) \tag{3}$$

The symbol $u$ is used to denote a feature map with dimensions $H \times W \times C$, and the total number of channels is denoted by $c$. For each channel $c$ in the feature map, we use $u_c$ to denote the corresponding 2D matrix. For feature map compression, we adopt global average pooling as the compression process to compress the input feature map into a vector, which helps to reduce the dimensionality of the data and makes the subsequent processing more efficient. The correlation between the channels is established and the excitation operation is performed on the feature map to generate a self-learning vector of channel weights, which is shown in Equation (4) for the excitation operation:

$$s = F_{ex}(Z, W) = \sigma\left(g(Z, W)\right) = \sigma\left(W_z \delta(W_1 Z)\right) \tag{4}$$

The excitation operation assigns the obtained channel weights to each channel. Specifically, the channel attention module introduces a fully connected layer to encode the channel dependencies of the obtained compression features $Z$, learns the nonlinear interactions between channels, and introduces a sigmoid function to limit the weights to the range of $(0, 1)$, and finally, multiplies the obtained weights with the input features, assigns weights to its channels, and the obtained outputs can be expressed as (5):

$$X_c = F_{scale}(u_c, s_c) = u_c \cdot s_c \tag{5}$$

The spatial attention module efficiently filters out background information, allowing the network to focus more on foreground regions of interest, This advanced feature filtering ensures that the network has a sharper perception of target-related information. The low-level features are denoted as $\mathrm{U} = \{u^{1,1}, u^{1,2}, \ldots, u^{i\times j}, \ldots, u^{H\times W}\}$, firstly, the low-level features are compressed by the convolution operation to compress the channels of the feature map $\mathrm{U} \in \mathrm{R}^{\mathrm{C}\times H\times W}$, so as to obtain the feature $S \in \mathrm{R}^{H\times W}$, and then, the encoded spatial feature map mapped to $[0, 1]$ is normalized by the Sigmoid operation. The feature map is normalized and finally the output of spatial attention is shown in Equation (6):

$$\mathrm{U}_{SA} = \left\{f(s_{1,1})u^{1,1}, f(s_{1,2})u^{1,2}, \ldots, f(s_{H,W})u^{H\times W}\right\} \tag{6}$$

4. **R-GAN models.** GAN can learn the attacker's strategy and generate pseudo-random sequences that are more difficult to crack. In response to the problem of difficulty in training the GAN model, the generator and discriminator of the GAN model are redesigned to be able to generate pseudo-random sequences in a better way. Figure 4 shows our improved R-GAN model.

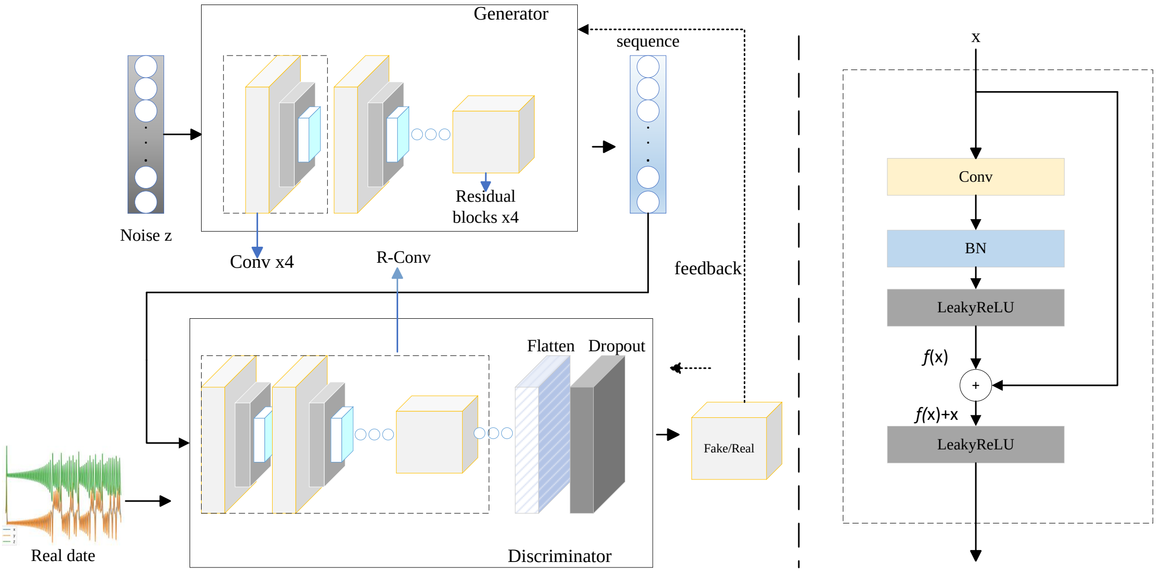


FIGURE 4. R-GAN key generation model

4.1. **Generator network.** During the training of the generator model, we observed the phenomenon of vanishing gradients and loss of information, and designed a new residual module that replaces the neural network with a conv layer, the generator consists of a fully connected layer and four residual convolutional layers, the multilayer structure can be more comprehensive extraction of features, and the addition of the residual network to the generator part can improve the performance of the generation of high-dimensional chaotic sequences effectively. The input is passed directly to the output layer, as depicted on the right side of Figure 4. If no jump connection is added, the input $x$ will be mapped by $f(x)$, to obtain $H(x)$, and the output equation is shown in Formula (7):

$$H(x) = f(x) \tag{7}$$

After adding the hop connection, the output is shown in Equation (8):

$$H(x) = f(x) + x \tag{8}$$

This design has no negative impact, helps accelerate the convergence process of the model, and better captures long-term dependencies and complex nonlinear features in the input sequence.

### 4.2. Discriminator network.

The structure of the discriminator consists of three convolutional layers tasked with feature extraction, identifying, and capturing key features through convolutional operations on the input data. The flat layer's role is to compress the data between the convolutional and fully connected layers, enhancing the efficiency of information transfer. Additionally, to prevent overfitting, a discard layer is introduced to improve generalization ability.

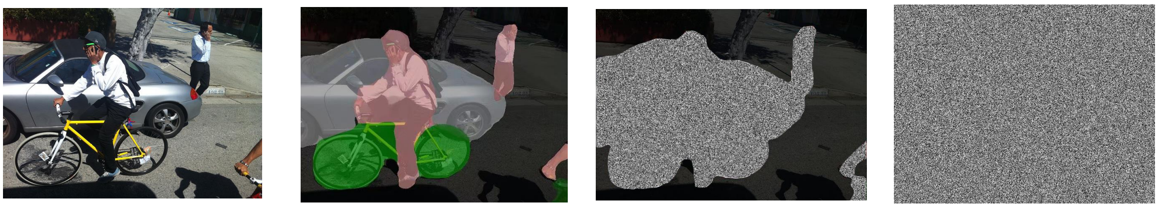
## 5. Image encryption method.

By designing the ADA-DeepLab model, important regions of the image are segmented to extract the portion intended for encryption. The Chen chaotic system is employed as the training set for the GAN key generator, generating diverse pseudo-random sequences. Traversing the segmentation structure with pixel points in the region of interest set as 1 and those in the region of disinterest as 0, the segmented image is combined with the GAN key generation model to create a binary mask using the segmentation structure. The coordinates of pixel points, with 1 in the region of interest and 0 in the region of disinterest, are indexed and saved in an array. A key is selected from the R-GAN model for the encryption algorithm, encrypting the region with pixel points set as 1. The original image's pixel values are replaced with the encrypted values, concealing crucial information from the plaintext image. Subsequently, other compatible pseudo-random sequences from the R-GAN model are chosen as another key to encrypt the remaining regions. The encrypted images of important and background regions are merged, implementing different encryption methods for the entire image to enhance its security. The specific algorithm is outlined in Algorithm 1.

**Algorithm 1** The steps of the image encryption method are as follows

```
Require: Input the plaintext image $P_{h\times w}$, where $h$ represents the height, and $w$ represents the width
Obtain the binary mask, 0 and 1, for the pixel points $x$ in the segmented image using ADA-DeepLab;
R-GAN generates keys by selecting any two keys, $k1$ and $k2$.
if $x$=1 then
    Encryption is applied to all coordinates of pixel point $x$ using key $k1$;
end if
if $x$=0 then
    Encryption is applied to all coordinates of pixel point $x$ using key $k2$;
end if
Replace the pixel values in the original image with the encrypted pixel values to generate the encrypted segmented image.
Ensure: Generate the encrypted image
```

The important region information in the plaintext image is hidden, and the encryption effect is shown in Figure 5.



(a) original image (b) split image (c) Regional encrypted (d) Overall encrypted

FIGURE 5. Image Segmentation Encryption

## 6. Experimental results and analysis.

### 6.1. Experimental data and platforms.

**6.1. Experimental data and platforms.** The configuration of the project covers a number of aspects, specifically, Windows 10, the operating platforms are CUDA 11.2 and CUDNN 8.1 and in terms of the programming environment Python version 3.7.0 and Poarch version 1.9.1, the memory size is 16GB.

PASCAL VOC 2012 dataset: This dataset is a widely used computer vision dataset that contains 20 different object categories covering common objects and scenes including people, animals, and natural environments.

**6.2. Evaluation indicators.** The $mIoU$represents the average intersection on the concatenated set, which is a commonly used evaluation metric in image segmentation tasks and is calculated as shown in (9):

$$mIoU = \frac{1}{k+1} \sum\nolimits_{j=0}^{k} \frac{p_{jj}}{\sum_{i=0}^{k} p_{ji} + \sum_{i=0}^{k} p_{ji} - p_{jj}} \tag{9}$$

Table 1 shows that through experimental proof on the PASCAL VOC 2012 dataset, our proposed ADA-DeepLab algorithm performs better in terms of $mIoU$ compared to other mainstream algorithms, and exhibits a significant increase in accuracy, achieving a satisfactory result of 82.1%, which demonstrates that our algorithm has a stronger performance in dealing with image segmentation tasks.

TABLE 1. Validation results for the PASCAL VOC 2012 dataset

| Method | $mIoU$% |
|---|---|
| EDPNet [21] | 80.8% |
| Im-Deeplabv3+ [22] | 80.6% |
| DPNet [23] | 79.5% |
| SA-FFNet [24] | 76.5% |
| Ours | 82.1% |

**6.3. Key spatiality analysis.** The key space is the set of all possible keys used by the encryption algorithm, which can be expressed as the size of the range of values for all keys in the encryption system. In this paper, we employ the hyperchaotic Chen system as the training set for the GAN key generator. The precision of floating-point numbers under a computer operating system is about $10^{-16}$. Therefore, the key space in this chapter is approximately $2^{460}$, exceeding $2^{100}$. Such a large key space demonstrates the method's ability to resist brute force attacks.

6.4. **Sequence performance testing.** After discussing the image segmentation part we are going to test the keys required for image encryption, in cryptography high quality random numbers are essential for the security of cryptographic algorithms. The NIST 800-22 test is a commonly used method for evaluating and verifying that random number generators satisfy cryptographic requirements. It is therefore used to evaluate the statistical properties of the generated sequence to gain insight into the randomness of the sequence. If the value is less than 0.01, it is considered a failure. According to the test results, the generated pseudo-random sequence passed all the tests, indicating that the sequence is difficult to crack.

Table 2. NIST-800-22 test results

| Statistical Tests | Value | Result |
|---|---|---|
| Cumulative Sums | 0.21713 | Successful |
| Linear Complexity | 0.38572 | Successful |
| Frequency | 0.40162 | Successful |
| Block Frequency Text | 0.39617 | Successful |
| Runs Text | 0.62541 | Successful |
| LongestRun Text | 0.35726 | Successful |
| O T Test-1 | 0.84517 | Successful |
| O T Test-2 | 0.75168 | Successful |
| Rank Text | 0.62713 | Successful |
| DFT Text | 0.32852 | Successful |
| Maurer Test | 0.29635 | Successful |
| Serial testing | 0.11548 | Successful |
| Random Excursions Test-1 | 0.57351 | Successful |
| Random Excursions Test-2 | 0.35274 | Successful |
| Approximate Entropy | 0.80986 | Successful |

6.5. **Correlation analysis.** The correlation coefficient is a statistical measure of the strength and direction of the linear relationship of the image and is calculated as shown in (10)

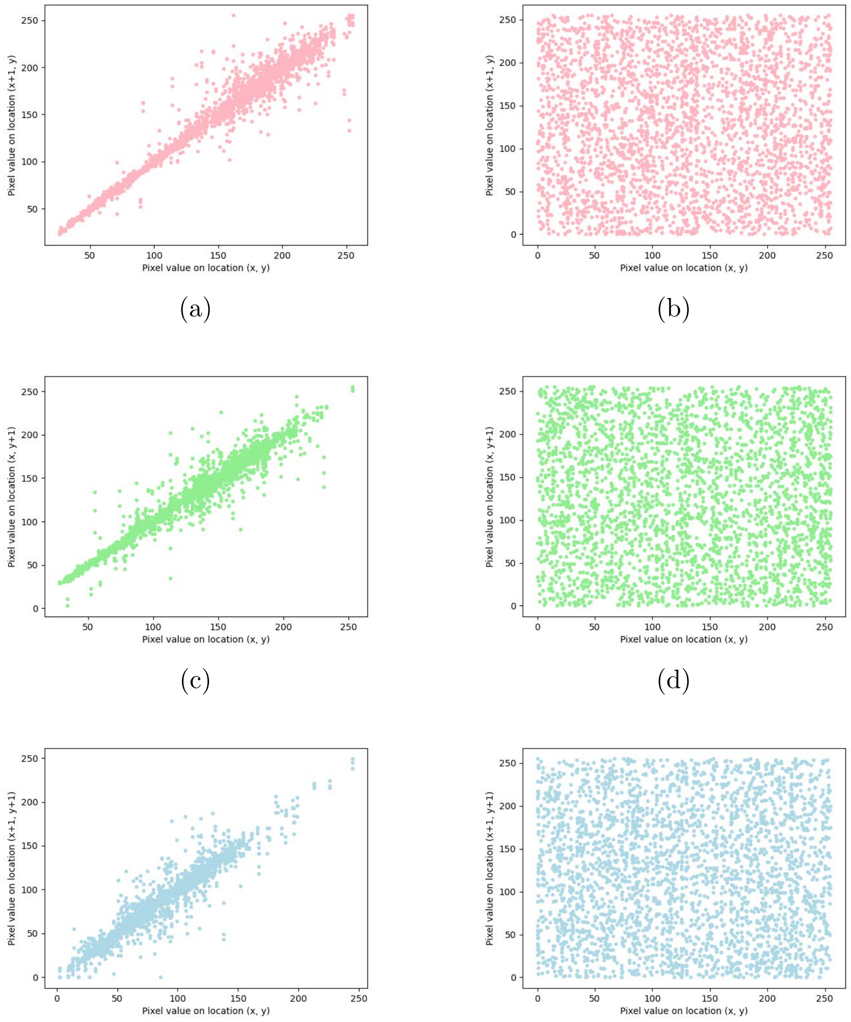
$$\begin{cases} E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \\ D(x) = \frac{1}{N+1}\sum_{i=1}^{N}(x_i - E(x))^2 \\ \operatorname{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)) \\ r_{x,y} = \frac{\operatorname{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \end{cases} \tag{10}$$

Neighboring pixels of digital images have strong correlation, the leakage of a pixel value will threaten the security of the surrounding information at the same time, after the experimental data verification, we can learn from Table 3 that the correlation coefficient of the encrypted neighboring pixels changes from the state of close to 1 to the state of close to 0, which indicates that there is no linear relationship between the two images, and the use of this paper's method compared with the other mainstream methods, the encryption effect of the present paper is better.

Figure 6 represents the distribution of correlation coefficients of Lena image and encrypted image.

Table 3. The correlation coefficient

| Direction | Horizontal | Vertical | Diagonal |
|---|---|---|---|
| Lena Image | 0.9803 | 0.9759 | 0.9704 |
| Ref. [25] | -0.0018 | 0.0041 | -0.0011 |
| Ref. [26] | -0.0447 | 0.0004 | -0.0047 |
| Ref. [27] | 0.0035 | -0.0006 | -0.0074 |
| Ref. [28] | 0.0019 | -0.0015 | -0.0039 |
| Ours | -0.0013 | 0.0003 | -0.0034 |



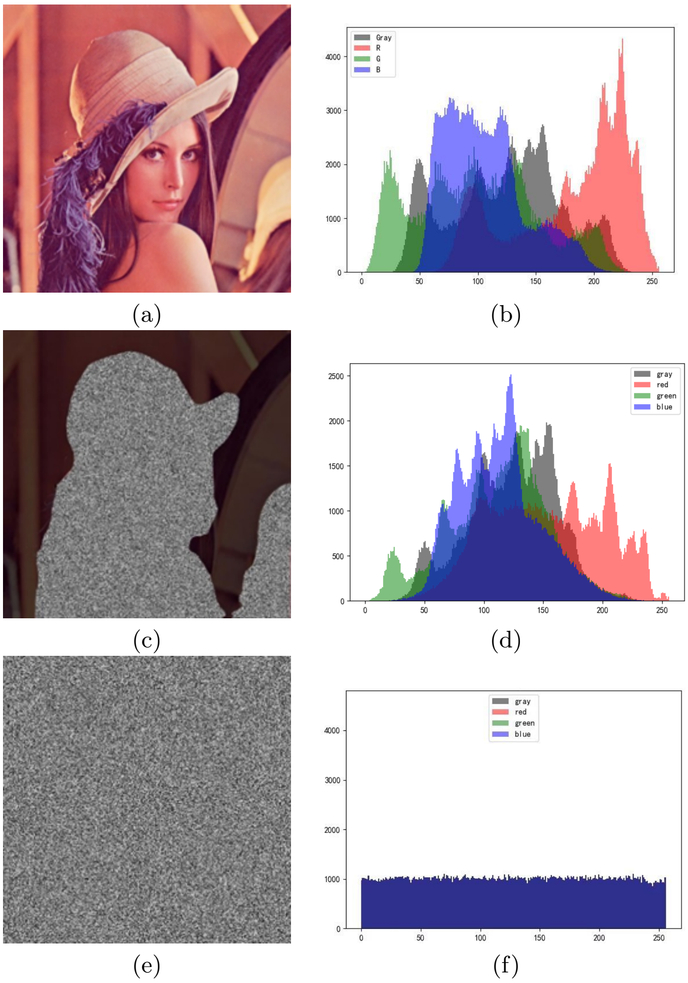
(a) (b)

(c) (d)

(e) (f)

Figure 6. Correlation coefficient graph

6.6. **Histogram analysis.** Histogram analysis examines the frequency distribution of individual values in both plaintext and ciphertext images [29], where certain pixel values may appear more frequently in the plaintext image, forming distinct peaks. In ciphertext images, this frequency distribution may be altered due to the randomness introduced by encryption, and the histogram may exhibit smoother and more uniform characteristics. In Figure 7, the histograms of the Lena image, local encryption, and whole encryption are shown respectively.



(a) (b)

(c) (d)

(e) (f)

FIGURE 7. Correlation coefficient graph

6.7. **Resistance to differential attacks.** Resistance to differential attacks reflects its resistance to differential attacks, which are a common type of attack Password analysis methods. Attackers use differential information in cryptographic algorithms to obtain keys or crack passwords, This article tests $NPCR$ and $UACI$, and the formula of $NPCR$ is shown in (11) :

$$NPCR = \frac{\sum_{i,j} D(i,j)}{M * N} * 100\% \tag{11}$$

$M$denotes the width of the image and $N$ denotes the height of the randomized image, and Equation (12) shows the calculation of $D(i,j)$:

$$D(i,j) = f(x) = \left\{ \begin{array}{l} 1, C_1(i,j) \neq C_2(i,j) \\ 0, otherwise \end{array} \right\} \tag{12}$$

$UACI$ is a metric used to quantify image distortion, and the function of $UACI$ is to provide a single numerical value that can be used to assess the degree of difference between the original image and the distorted image. The calculation formula can therefore be expressed as Equation (13):

$$UACI = \frac{1}{M * N} \frac{\sum (c_1(i,j) - c_2(i,j))}{255} * 100\% \tag{13}$$

We select a random pixel point for Lena image and change its pixel value to get a new image. After obtaining the ciphertext image. Multiple operations are averaged as in Table 4, and finally it is found that even if only small changes are produced, the two encrypted images reflect a great difference.

Table 4. Key sensitivity analysis

| Lena | Ref. [27] | Ref. [26] | Ref. [28] | Ref. [25] | Ours |
|---|---|---|---|---|---|
| $NPCR$ | 0.9961 | 0.9962 | 0.9957 | 0.9962 | 0.9962 |
| $UACI$ | 0.3338 | 0.3355 | 0.3343 | 0.3345 | 0.3344 |

### 6.8. **Information entropy analysis.**

The mathematical definition of information entropy is based on probability, where it is higher when an event has more possible outcomes. Conversely, as we can predict the outcome of an event more accurately, the information entropy decreases. The information entropy of image $x$ is calculated as (14).

$$H(x) = -\sum\nolimits_{i=0}^{n-1} p(x_i)\log_2 p(x_i) \tag{14}$$

The ideal value of information entropy for an image is 7, indicating that the information is well-hidden. From the table, it can be observed that the information entropy of the encrypted portion of the image is close to the ideal value. This suggests that the various key encryption methods generated by R-GAN can effectively conceal information and enhance the confusion of the information.

Table 5. Information Entropy Analysis

| information entropy | Lena |
|---|---|
| Ref. [25] | 79975 |
| Ref. [26] | 79989 |
| Ref. [27] | 79993 |
| Ref. [28] | 79971 |
| Ours | 79993 |

## 7. **Conclusion.**

This paper encrypts the image segmentation part using different key encryption methods. Firstly, to address the issue of a short chaotic period, a key generation model, R-GAN, is introduced. The generator and discriminator are improved to effectively handle the degradation problem of the model training network and the short chaotic period. Secondly, to address the imprecise segmentation of target outlines, a new deformable pyramid module is designed. The introduction of an attention mechanism allows for more nuanced processing of image features, reducing the loss of crucial details. Finally, this paper not only encrypts the entire image but also achieves more refined encryption of sub-image portions. Future work aims to enhance the input chaotic sequences and improve encryption algorithms for better results. Dealing with the segmentation of complex irregular images presents a significant challenge.

## REFERENCES

[1] L. Yang, Y.-C. Chen, and T.-Y. Wu, "Provably secure client-server key management scheme in 5g networks," *Wireless Communications and Mobile Computing*, vol. 2021, pp. 1–14, 2021.

[2] S. K. Farhan Musanna, Deepak Dangwal and V. Malik, "A chaos-based image encryption algorithm based on multiresolution singular value decomposition and a symmetric attractor," *The Imaging Science Journal*, vol. 68, no. 1, pp. 24–40, 2020.

[3] H. Shen, X. Shan, M. Xu, and Z. Tian, "A new chaotic image encryption algorithm based on transversals in a latin square," *Entropy*, vol. 24, no. 11, 2022.

[4] T.-Y. Wu, X. Fan, K.-H. Wang, J.-S. Pan, C.-M. Chen, and J. M.-T. Wu, "Security analysis and improvement of an image encryption scheme based on chaotic tent map." *Journal of Information Hiding and Multimedia Signal Processing*, vol. 9, no. 4, pp. 1050–1057, 2018.

[5] T.-Y. Wu, X. Fan, K.-H. Wang, C.-F. Lai, N. Xiong, and J. M.-T. Wu, "A dna computation-based image encryption scheme for cloud cctv systems," *IEEE Access*, vol. 7, pp. 181 434–181 443, 2019.

[6] M. Akraam, T. Rashid, S. Zafar *et al.*, "A chaos-based image encryption scheme is proposed using multiple chaotic maps," *Mathematical Problems in Engineering*, vol. 2023, 2023.

[7] Y. Huang, L. Huang, Y. Wang, Y. Peng, and F. Yu, "Shape synchronization in driver-response of 4-d chaotic system and its application in image encryption," *IEEE Access*, vol. 8, pp. 135 308–135 319, 2020.

[8] H. Sun, C. Li, J. Zhang, S. Liang, and W. Huang, "Cryptanalysis and improvement of several identity-based authenticated and pairing-free key agreement protocols for iot applications," *Sensors*, vol. 24, no. 1, p. 61, 2023.

[9] S. M. S. Rana, M. J. Uddin, P. Santra, G. Mahapatra *et al.*, "Chaotic dynamics and control of a discrete-time chen system," *Mathematical Problems in Engineering*, vol. 2023, 2023.

[10] L. Wang, Z. Chen, X. Sun, and C. He, "Color image roi encryption algorithm based on a novel 4d hyperchaotic system," *Physica Scripta*, vol. 99, no. 1, p. 015229, 2023.

[11] Q. Natsheh, A. Sălăgean, D. Zhou, and E. Edirisinghe, "Automatic selective encryption of dicom images," *Applied Sciences*, vol. 13, no. 8, p. 4779, 2023.

[12] M. Alsafyani, F. Alhomayani, H. Alsuwat, and E. Alsuwat, "Face image encryption based on feature with optimization using secure crypto general adversarial neural network and optical chaotic map," *Sensors*, vol. 23, no. 3, p. 1415, 2023.

[13] Y. Ma, Y. Peng, and T.-Y. Wu, "Transfer learning model for false positive reduction in lymph node detection via sparse coding and deep learning," *Journal of Intelligent & Fuzzy Systems*, vol. 43, no. 2, pp. 2121–2133, 2022.

[14] Z. Xia, X. Pan, S. Song, L. E. Li, and G. Huang, "Vision transformer with deformable attention," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2022, pp. 4794–4803.

[15] M. Agarwal, S. K. Gupta, and K. Biswas, "Development of a compressed fcn architecture for semantic segmentation using particle swarm optimization," *Neural Computing and Applications*, pp. 1–14, 2023.

[16] A. Norelyaqine, R. Azmi, A. Saadane *et al.*, "Architecture of deep convolutional encoder-decoder networks for building footprint semantic segmentation," *Scientific Programming*, vol. 2023, 2023.

[17] H. Xie, K. Hou, D. Jiang, and W. Ma, "Bust portraits matting based on improved u-net," *Electronics*, vol. 12, no. 6, p. 1378, 2023.

[18] W. Yuan, J. Wang, and W. Xu, "Shift pooling pspnet: rethinking pspnet for building extraction in remote sensing images from entire local feature pooling," *Remote Sensing*, vol. 14, no. 19, p. 4889, 2022.

[19] F. Chen, F. Wu, J. Xu, G. Gao, Q. Ge, and X.-Y. Jing, "Adaptive deformable convolutional network," *Neurocomputing*, vol. 453, pp. 853–864, 2021.

[20] K. Okada, K. Endo, K. Yasuoka, and S. Kurabayashi, "Learned pseudo-random number generator: Wgan-gp for generating statistically robust random numbers," *Plos One*, vol. 18, no. 6, p. e0287025, 2023.

[21] D. Chen, X. Li, F. Hu, P. T. Mathiopoulos, S. Di, M. Sui, and J. Peethambaran, "Edpnet: An encoding–decoding network with pyramidal representation for semantic image segmentation," *Sensors*, vol. 23, no. 6, p. 3205, 2023.

[22] J. He, J. Duan, Z. Yang, J. Ou, X. Ou, S. Yu, M. Xie, Y. Luo, H. Wang, and Q. Jiang, "Method for segmentation of banana crown based on improved deeplabv3+," *Agronomy*, vol. 13, no. 7, p. 1838, 2023.

[23] J. Wang, X. Zhang, T. Yan, and A. Tan, "Dpnet: Dual-pyramid semantic segmentation network based on improved deeplabv3 plus," *Electronics*, vol. 12, no. 14, p. 3161, 2023.

[24] Z. Zhou, Y. Zhou, D. Wang, J. Mu, and H. Zhou, "Self-attention feature fusion network for semantic segmentation," *Neurocomputing*, vol. 453, pp. 50–59, 2021.

[25] Y. Zhang, “A new unified image encryption algorithm based on a lifting transformation and chaos,” *Information Sciences*, vol. 547, pp. 307–327, 2021.

[26] H. Nazir, I. S. Bajwa, S. Abdullah, R. Kazmi, and M. Samiullah, “A color image encryption scheme combining hyperchaos and genetic codes,” *IEEE Access*, vol. 10, pp. 14 480–14 495, 2022.

[27] R. Lin and S. Li, “An image encryption scheme based on lorenz hyperchaotic system and rsa algorithm,” *Security and Communication Networks*, vol. 2021, pp. 1–18, 2021.

[28] S. Alharbi, A. Elsonbaty, A. Elsadany, F. Kamal *et al.*, “Nonlinear dynamics in the coupled fractional-order memristor chaotic system and its application in image encryption,” *Mathematical Problems in Engineering*, vol. 2023, 2023.

[29] T.-Y. Wu, X. Fan, K.-H. Wang, J.-S. Pan, and C.-M. Chen, “Security analysis and improvement on an image encryption algorithm using chebyshev generator,” *Journal of Internet Technology*, vol. 20, no. 1, pp. 13–23, 2019.