International Journal for Housing Science and Its Applications
Publish August 10, 2025. Volume 46, Issue 4 Pages 539-549

https://doi.org/10.70517/ijhsa46448

The Application of Digital Art Animation Elements in the Design of Network Security Publicity Platforms

Mo Wang[1,*]
[1] Digital Art and Design, HeBei Vocational College of Arts and Crafts, Baoding, Hebei, 071000, China
Corresponding authors: (e-mail: wangmo1119@163.com).

Abstract In order to enhance the public's awareness of network security, innovative educational means are particularly important. Combining digital art and animation elements as the carrier of network security propaganda, and utilizing advanced technologies such as style migration and self-attention mechanism, a network security propaganda platform with fun and interactivity can be designed so as to improve the dissemination effect of the platform and user participation. This paper proposes a design method of network security publicity platform based on digital art animation elements. The animation elements are extracted by style migration technology, and the generator and discriminator structures are optimized by combining the self-attention mechanism to achieve high-quality animation image generation. The evaluation metrics used include PSNR and SSIM, and the experimental results show that compared with the traditional GAN model, the improved AnimeGANv2-Self-Attention model significantly improves the image stylization effect, with a 1.39% increase in PSNR and a 2.99% increase in SSIM value. In addition, the cybersecurity publicity platform designed in this paper combines animation elements and cybersecurity education, which has a high degree of user attraction and participation. By analyzing the actual user data, the difference between the experimental group and the control group in terms of publicity effect is significant, indicating that the platform is more effective than traditional publicity means in enhancing cybersecurity awareness.

Index Terms Digital art, animation elements, style migration, self-attention mechanism, network security publicity, platform design

I. Introduction

Chinese government cybersecurity publicity platforms, mainly relying on the portals of government departments at all levels [1]. Through a survey of 28 major provincial and municipal cybersecurity publicity platforms in China, it was found that about 90% of the provincial and municipal government platforms in China have relevant cybersecurity publicity content, but only about 50% of the website content is systematic, while 40% of the platform content has not yet been categorized and divided into modules, and there is only a relatively small number of interconnections and echoes between the contents [2], [3]. In terms of presentation, 45% of the websites surveyed only have text descriptions as a form of education, 40% of the websites only have text and pictures in two forms, and only 5% of the websites have more than three forms of education: text, pictures and videos [4]. The above survey results show that China's network security publicity form is relatively single, and lacks a certain degree of attraction.

Developed countries attach great importance to the construction of network security publicity platform [5]. The publicity website of the U.S. National Cyber Security Administration fully embodies systematic, professional, open and modular [6]. The form has elements such as text, pictures, animation, video, etc., and there is a random questionnaire for feedback after accepting the visit, so as to improve the operation of the platform [7]-[9]. The French cybersecurity platform is an open resource platform that not only provides rich cybersecurity education resources, but also aims to provide a platform for the majority of cybersecurity educators to design cybersecurity education programs, allowing for individualized design and providing many successful cybersecurity education cases for reference [10], [11]. The platform is clearly categorized and detailed, with abundant resources and detailed information in the form of text, pictures, animation, video and other elements, and provides the URLs of cooperative websites to enrich the content.

In Mainland China, however, governments around the world do not pay enough attention to the construction of network security publicity platforms, and some places have established publicity platforms, but the content is outdated and slow to be updated, or although they are involved in network publicity, they do not form a systematic and continuous, resulting in the current network security publicity is insufficient and the effectiveness of the platform is not significant [12]-[14]. Therefore, building a unified network security publicity platform for different groups is an

important means to improve and perfect the current methods, approaches and work level of network security publicity and education, and an inevitable way to adapt to the new situation of the rapid arrival of the motorized society and the new environmental needs [15].

With the popularization of the Internet and the acceleration of the informationization process, the problem of network security has become increasingly serious, with the emergence of network fraud, data leakage, virus attacks and other problems, which have brought great trouble to society and individuals. Especially with the wide application of smart devices and the Internet of Things, the ways of cyber-attacks have become more and more complicated, and the challenges of cyber security have increased. Traditional means of cybersecurity publicity mostly rely on static forms such as video and text, which are difficult to effectively attract users' attention and have limited educational effects. Therefore, innovative ways of cybersecurity education have become a top priority.

In recent years, digital art and animation elements are widely used in various educational and publicity fields because of their high expressiveness and attractiveness. As a relaxing and interesting form, animation can effectively attract the interest of young people and make them more receptive to relevant knowledge. Incorporating animation elements into the network security publicity platform can not only improve user participation, but also stimulate users' learning motivation through fun and entertainment.

The goal of this study is to extract digital art animation elements based on the style migration technique and optimize the quality of the generated images by combining the self-attention mechanism to design a network security publicity platform integrating publicity, education and interaction. In order to achieve this goal, this paper adopts innovative technical means in the design process, including the improved AnimeGANv2 model, which incorporates the self-attention mechanism to improve the quality of the generated images. At the same time, the platform also integrates a variety of functional modules, such as data query, case direct, legal assistance, etc., in order to enhance the practical applicability and educational effect of the platform.

II. Network Security Publicity Platform Based on Animation Elements

II. A.Extraction of digital art animation elements based on style migration

This subsection introduces the network structure and loss function of the style migration-based digital art anime element extraction model.In the digital art anime element extraction task, the model needs to accurately recognize the anime elements in order to be able to generate realistic digital art anime elements. In this paper, the AnimeGANv2 model is improved, including the adjustment of the network structure of the generator and discriminator, and the addition of auxiliary classifiers to achieve better image style migration effects.

II. A. 1) Generator network structure

AnimeGANv2 is an upgrade of the first generation of AnimeGAN, which mainly solves the problem of high frequency artifacts in anime images. The improvement measure is to prevent artifacts by using layer normalized LN of features. With LN, different channels in the feature map have the same distribution of feature attributes, effectively preventing the generation of local noise. Compared with the original AnimeGAN, AnimeGANv2 is easier to train, while the number of parameters of the generator network is reduced by about half. The discriminators used by the two models are basically the same, and the only difference lies in the use of the normalization method. For the generator of the AnimeGANv2 model, it is actually a symmetric encoder network containing two modules: standard convolution, inverse residual block, and up and down sampling. There is no need to design a normalization layer because the last convolutional layer has a convolutional kernel size of 1 × 1 and mainly follows tanh for training, and only four IRBs are used for the network of AnimeGAN with the aim of reducing the training effort [16], [17]. In this paper, based on the AnimeGANv2 model, a self-attention mechanism is added to the generator and discriminator respectively, and an auxiliary classifier without fully connected layers is added to the generator to improve the feature extraction of the model. The optimized structure is shown in Fig. 1.

First, the input raw anime image is downsampled using the encoder module and then the feature map is obtained by encoding the features with self-attention mechanism through the inverse residual block. Next, the feature map with attention is up-sampled using the decoder module and fed into it, and finally the anime elements are extracted in the form of generation, where the auxiliary classifier part of the model classifies the feature map obtained after the self-attention mechanism using an auxiliary classifier consisting of convolution and pooling without fully connected layers, and calculates the loss on the classification result. Where the input anime image size is 256×256. The self-Attention in the table represents the feature map after the self-attention mechanism module, which carries spatial self-attention weights and remains invariant in shape.

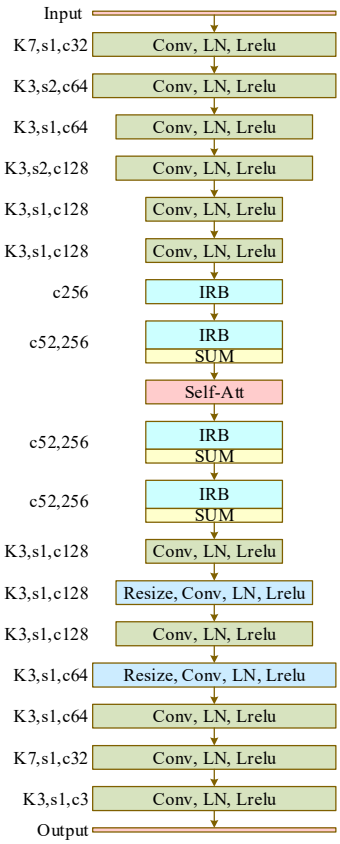

Figure 1: The model generator network structure in this paper

II. A. 2) Discriminator network structure

Similarly we still add Self-Attention mechanism in the discriminator, so that the Self-Attention mechanism module guides the network to know which region of the image to recognize the authenticity of the image. The design and composition of the discriminator is shown in Figure 2. The initial image size of the discriminator input is 256×256, and all the normalization in this network uses the layer normalization method.Adding the Self-attention mechanism module in the discriminator network can get the feature map with the attention weight, which enhances the model's focus on the key regions and thus improves the effect of the extraction of the elements of the digital animation.

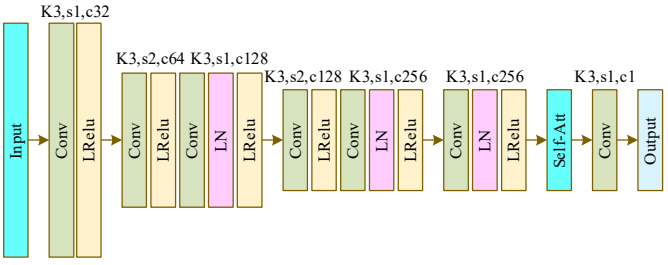

Figure 2: Discriminator network structure

II. A. 3) Loss function

In order to allow the generator to learn the anime features well, so as to better transform real-world images into target anime style images, the loss function in this paper is basically the same as that of the AnimcGANv2 model, except for the addition of a new auxiliary classifier loss. The network uses a total of six loss functions for training, which are grayscale adversarial loss L_{adv}, content loss L_{con}, grayscale style loss L_{gra}, color reconstruction loss L_{col}, adversarial loss for promoting edges, and auxiliary classifier loss L_{aux}. Remember that the reality domain image $S_{data}(p)=\{p_i \mid i=1,\cdots,N\}\subset P$, and the anime domain image $S_{data}(a)=\{a_i \mid i=1,\cdots,M\}\subset A$, where N and

M are the number of photographs in the reality image dataset and the anime image dataset respectively Quantity. In order to remove the color interference, so the anime images are converted to grayscale images, the grayscale image domain is $S_{data}(x)=\{x_i \mid i=1,\cdots,M\}\subset X$, and the color image a_i in $S_{data}(x)$ is converted to grayscale image x_{io}. Remove the image edges in the color anime image $S_{data}(a)$ to construct the data domain $S_{data}(e)=\{e_i \mid i=1,\cdots,M\}\subset E$. In order to avoid the influence of the image color in $S_{data}(e)$ on the color of the generated image, the image in $S_{data}(e)$ is also processed as a grayscale image, i.e., $S_{data}(y)$. The total loss function formula of the model is shown in (1):

$$\begin{aligned}L(G,D)=&w_{adv}L_{adv}(G,D)+w_{con}L_{con}(G,D)\\&+w_{gra}L_{gra}(G,D)+w_{col}L_{col}(G,D)+w_{aux}L_{aux}(G,D)\end{aligned}\tag{1}$$

The adversarial loss uses a least squares loss function, which can generate high-quality images as well as improve the stability of model training, and $L_{adv}(G,D)$ is the adversarial loss; $L_{con}(G,D)$ is content loss; $L_{gra}(G,D)$ is grayscale style loss; $L_{col}(G,D)$ is the color reconstruction loss and $L_{aux}(G,D)$ is the auxiliary classifier loss. w_{adv}, w_{con}, w_{gra}, w_{col}, and w_{aux} are the loss weights used to balance the five losses. In this paper the weights of the loss function are debugged continuously and the finalized weight parameters are $w_{adv}=60$, $w_{con}=10$, $w_{gra}=20$, $w_{col}=50$, and $w_{aux}=0.5$, which achieves a good balance between the image style and the image content. In the generator, least squares loss function, content loss function, grayscale loss function, color reconstruction loss function and auxiliary classifier loss function are used as loss functions. Among them, the content loss function and grayscale style loss function utilize the pre-trained VGG19 network as a perceptual network to extract high-level semantic features from the image. The formula is shown in (2):

$$\begin{aligned}&L_{con}(G,D)=E_{P_i\sim S_{data}(p)}\left[\left\|VGG_I(p_i)-VGG_I(G(p_i))\right\|_1\right]\\&L_{gra}(G,D)=E_{P_i\sim S_{data}(p)}\\&E_{x_i\sim S_{data}(x)}\left[\left\|Gram\left(VGG_I\left(G\left(p_i\right)\right)\right)-Gram\left(VGG_I\left(x_i\right)\right)\right\|_1\right]\end{aligned}\tag{2}$$

where VGG and Gram represent the Gram matrix using VGG network layer and features respectively, p_i is the input real image, $G(p_i)$ is the image generated by the generator, x_i is the grayscale image, and the content loss $L_{con}(G,D)$ and the color loss $L_{col}(G,D)$ are computed using L1 coefficient regularization. Regarding the color extraction and conversion, the RGB channels are first converted to YUV channels, and then different loss calculation methods are used for different channels as shown in equation (3) below:

$$\begin{aligned}L_{col}(G,D)=&E_{p_i\sim S_{data}(p)}\left[\left\|Y(G(P_i))-Y(p_i)\right\|_1\right.\\&\left.+\left\|U(G(P_i))-U(p_i)\right\|_H+\left\|V(G(P_i))-V(p_i)\right\|_H\right]\end{aligned}\tag{3}$$

The Y channel uses the L1 loss function, the U and V channels use the Huber loss function. The loss function of the auxiliary classifier uses the cross-entropy loss function. The cross-entropy loss function is a commonly used classification loss function that analyzes the accuracy of the predictive model. In the model, the auxiliary classifier is used to provide additional classification information that helps the generator to produce more accurate images. The specific formula for the auxiliary classifier loss is shown in (4):

$$L_{aux}(X_i,Y_i)=-w_i[y_i\log x_i+(1-y_i)\log(1-x_i)]\tag{4}$$

where X_i represents the final output of the model, Y_i represents the classification labels, and the final generator loss function $L(G)$ can be expressed as (5):

$$\begin{aligned}L(G)=&w_{adv}E_{P_i\sim S_{data}(p)}[(G(p_i)-1)^2]+w_{con}L_{con}(G,D)\\&+w_{gra}L_{gra}(G,D)+w_{col}L_{col}(G,D)+w_{aux}L_{aux}(G,D)\end{aligned}\tag{5}$$

where p_i is the input real image and $L_{aux}(G,D)$ is the auxiliary classifier loss, the discriminator improves the edge clarity of the generated image by promoting the adversarial loss of the edges, and a novel grayscale adversarial

loss is used to avoid that the generated image is presented as a grayscale image. Therefore, the loss function of the discriminator is represented by the following equation (6):

$$L(D) = w_{adv}[E_{a_i \sim S_{data}(a)}[(D(a_i)-1)^2] + E_{p_i \sim S_{data}(p)}[(D(G(p_i)))^2] + E_{x_i \sim S_{data}(x)}[(D(x_i))^2] + 0.1E_{y_i \sim S_{data}(y)}[(D(y_i))^2]] \quad (6)$$

where $E_{a_i \sim S_{data}(a)}\left[\left(D(a_i)-1\right)^2\right]$ and $E_{p_i \sim S_{data}(p)}\left[\left(D\left(G(p_i)\right)\right)^2\right]$ denotes the discriminator adversarial loss obtained by placing the real style image and the generator-generated image into the discriminator, respectively, and $E_{X_i \sim S_{data}}\left[\left(D\left(X_i\right)\right)^2\right]$ denotes the gray scale loss, $0.1 \times E_{y_i \sim S_{data}(y)}\left[\left(D\left(y_i\right)\right)^2\right]$ denotes the object boundary loss, and 0.1 is used to adjust the boundary so that it is not too strong.

Since the generative adversarial network model is highly nonlinear, optimization after random initialization can easily fall into suboptimal local minima. In order to accelerate the convergence speed of the generative adversarial network, the generator is pre-trained with two epochs and the learning rate is set to 0.0001. In the formal training of the generator and the discriminator, the learning rate is set to 0.00001 and 0.00005, the training period is 100, the batch size is 5, and the optimizer uses Adam.

II. B.Cybersecurity awareness platform design

Comedy stars Zhao Benshan, Pan Changjiang, Huang Hong, Guo Da, Song Dandan, Cai Ming, etc. are portrayed as cyber security propaganda in the form of animation characters, which enhances fun and entertainment and better mobilizes the attention of the educated. Art as a means to design live images and scenes in a light-hearted, humorous and witty way to demonstrate the requirements of each chapter, section and article of the network security propaganda, and at the same time, insert network security accidents over the years (preferably coupled with the video and photographs at the time) can enhance its authenticity and sense of scene. So that people in front of the vivid, graphic images to receive information, accept the security knowledge. In this regard, based on the extraction of digital art animation elements based on style migration, the corresponding software development technology can be utilized to complete the design task of the network security publicity platform.

II. B. 1) Platform key technologies

The network security publicity platform adopts distributed network architecture, utilizes Oracle database, builds multiple distributed database servers and establishes different data interfaces respectively, realizes the effective combination of animation elements and network security education, and promotes the design of network security publicity platform.

(1) Distributed Network Architecture

Distributed network structure is interconnected by nodes with multiple terminals distributed in different locations, nodes are connected to each other, and data can be transmitted by multiple paths [18], [19]. As the network security publicity platform is a communication and interactive platform integrating publicity and learning, the amount of resources carried will be more, so that when a large number of resources are accessed by a large number of network users, it will cause a large server burden, which may lead to slow access by users, and even cause system paralysis by overloading the server. Therefore, the system architecture adopts a fully distributed structure, which can, under the premise of guaranteeing the data security , can realize the effective combination of multifaceted animation elements and network security education, and ensure the accuracy and integrity of data.

(2) Database Technology

The platform adopts Oracle as the database for system development, and exchanges data between the platform and the platform in the way of data interface; Oracle is a large-scale relational database based on advanced structured query language (SQL), which manipulates a large number of regular data collections in a language that facilitates logical management; Oracle database is the most widely used database management system in the world at present. Oracle database is the most widely used database management system in the world, as a general database system, it has complete data management functions. As a relational database, it is a complete relational product. As a distributed database, it realizes the distributed processing function.

(3) Data interface and transmission

The network platform deploys a total platform and several provincial platforms respectively, builds independent servers in the total platform and provincial platforms, realizes the respective management and maintenance in each province, and the total platform carries out the data statistics and summarization, and the data interface and transmission of the platform are as follows: the total platform transmits the information, resources and other data in real-time to the provincial platforms by means of data sending and reads the required data from the provincial

platforms for the total platform to summarize statistics and display. The total platform transmits information, resources and other data to the provincial platforms in real time by means of data issuance, and regularly reads the required data from the provincial platforms for the total platform to summarize and display. The provincial platform realizes the sharing of local resources by calling the interface provided by the general platform, shares high-quality resources to the general platform and other provincial platforms, and completes the sharing of data.

II. B. 2) Functional Design Ideas for Cybersecurity Publicity Platforms

With the prevalence of network fraud is not less than the rapid iteration, through a variety of ways and platforms, vigorously publicize the means and methods of fraud prevention, and actively carry out a variety of activities to strengthen security education, combat network fraud, and safeguard the rights and interests of users. Form-rich activities can achieve better results in a short period of time, but have less effect on the long-term publicity of network security. Relevant departments and organizations are also actively exploring the creation of cybersecurity publicity platforms. “Money Shield, jointly developed by the State Council and Alibaba Group, is an “anti-fraud weapon” for combating new types of network crimes, and is a technical platform that specializes in solving the security of users' funds and preventing the leakage of information, and has built a security technology protection network for ordinary people. Tencent cell phone butler, WeChat public number “network fraud prevention” platform also played a role in the protection of Internet users. Nowadays, the means of criminals are even more dazzling, the script closely follow the social hotspots, fraud tools to push the new, the words directly hit the weakness of human nature, so that it is difficult to guard against. Innovative design and build a new platform for network fraud prevention education, explore new ways is imminent. For this reason, based on the style migration of digital art animation elements extracted on the basis of the use of the corresponding software development technology to develop a network security propaganda platform, integration of animation security education resources, focusing on breakthroughs, to provide instant communication and sharing platforms, greatly improving the preventive awareness and warning effect.

Through interviews, field understanding, questionnaire research, network resources collation and other forms, comprehensive research on students' network security ideology, especially to understand the user's cognitive degree and prevention level of network fraud. At the same time, the research understands the ways and methods of network safety education that users are happy to accept and love, so as to lay a solid foundation for the design and implementation of the new platform. Based on the preliminary research and user needs, combined with the need to prevent and deal with network fraud, it is planned to design five functional modules, which will be continuously supplemented and improved in the implementation process.

(1) Data Query

Integration of network resource databases and related information provided by the police, a variety of fraudulent phone calls, websites, bank cards and other related fraud information content sorting and database, the user can be the first time to query the search to confirm the authenticity of the information and fraud records, to help the user to identify, and to take precautions in advance.

(2) Information Express

The latest information related to network fraud in the form of animation fast delivery, including new means of fraud, new situations and fraud prevention strategies and techniques, to increase the user's interest in reading.

(3) Cases

For network fraud cases, especially the victimization of user groups to track cases, presented in a timely manner in the APP platform, in order to warn.

(4) Legal Aid

Present commonly used alarm phone numbers and reporting channels, to provide timely help for users who suffer from network fraud.

(5) Communication and Sharing

Provide users with a platform for communication and sharing, and can also add friends and other ways to carry out friendly interaction, increase the user stickiness of the platform, and further improve the effect of network security publicity.

III. Analysis of cybersecurity awareness platforms

III. A. Analysis of the extraction effect of anime elements

III. A. 1) Experimental environment

All the experiments in this paper were conducted under Windows 8 operating system, CUDA version 12.2, Cudnn version 7.5.9, hardware platform GeForce NVIDIA 4080Ti GPU, and environment configuration Python4.2 and TensorFlow2.6.

III. A. 2) Data setup

The network needs to be trained in such a way that the weighted sum of the set loss function is kept decreasing. The style images are used in the WikiArt dataset, which contains paintings by 195 different artists, the dataset has 42,129 images for training and 10,628 images for testing, and five style images are used in this experiment for this study.

III. A. 3) Evaluation indicators

This experiment uses 2 metrics, PSNR and SSIM, to quantitatively evaluate the effect of extracting digital art animation elements based on style migration. The details are as follows:

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}\left[I(i,j) - K(i,j)\right]^2 \tag{7}$$

$$PSNR = 10 * \log_{10}\left(\frac{MAX_I^2}{MSE}\right) \tag{8}$$

where I is the original image, K is the generated image, m and n are the width and height of the image respectively, and MAX_j is the maximum value in the image.

SSIM is a metric used to evaluate the similarity of two images, and its calculation process includes three aspects: brightness, contrast and structure, which are closely related to the perceived quality of the image, and its value is between 0 and 1. The larger value indicates that the output image is more similar to the content image, i.e., the better the quality of the output image. By calculating the SSIM value of two images, the degree of their similarity can be assessed to determine the effectiveness of image stylization. The calculation formula is as follows:

$$SSIM(x,y) = \frac{\left(2\mu_x\mu_y + c_1\right)\left(\sigma_{xy} + c_2\right)}{\left(\mu_x^2 + \mu_y^2 + c_1\right)\left(\sigma_x^2 + \sigma_y^2 + c_2\right)} \tag{9}$$

where μ_x and μ_y represent the mean values of x and y, σ_x, σ_y represent the standard deviation of x, y, and σ_{xy} represent the covariance of x and y, respectively.

III. A. 4) Analysis of results

Firstly, the loss functions of different models (GAN, AnimeGANv2, AnimeGANv2-Self-Attention) are analyzed, and the results of the model loss functions are shown in Table 1. The data in the table shows that the loss value of this paper's model is the smallest regardless of the kind of image, which indicates that this paper's model can well extract the digital animation elements in the image, and the element loss reaches within a reasonable range.

Table 1: The result of the model loss function

Image	GAN	AnimeGANv2	Ours
Architecture	0.402	0.394	0.075
Car	0.275	0.384	0.065
Plant	0.476	0.348	0.094
Water	0.437	0.111	0.069
Mountain	0.391	0.467	0.097
People	0.402	0.394	0.075

Secondly the PSNR values under different models are compared and as shown in Table 2, all the three models (GAN, AnimeGANv2, AnimeGANv2-Self-Attention) have the highest values of PSNR when dealing with anime images of architecture. The GAN method and the AnimeGANv2 method have the lowest values of PSNR on the images of faces, while the AnimeGANv2-Self-Attention algorithm has the lowest value of PSNR on water images. Overall, the AnimeGANv2-Self-Attention algorithm has relatively high PSNR values after stylization on all species, and the PSNR of the images generated by the AnimeGANv2-Self-Attention algorithm is improved by 1.39% as compared to the AnimeGANv2 algorithm. The results of the PSNR evaluations are given in the table below:

Table 2: PSNR under different methods

Image	GAN	AnimeGANv2	Ours
Architecture	13.3246	13.2387	14.0126
Car	12.1852	12.1806	12.3598
Plant	13.2357	12.2786	13.4195
Water	12.1952	12.1912	12.2982
Mountain	13.1787	13.2081	13.4251
People	12.1185	12.0914	12.3137

Then the SSIM values of each species under different models were compared, as shown in Table 3, all three models still have the highest values of SSIM when dealing with house images, the GAN method and AnimeGAN method have the lowest values of SSIM on face images, in general, the SSIM values of AnimeGANv2 method after stylization on each species are relatively high, compared with the GAN method Compared to GAN method, AnimeGANv2-Self-Attention method generates images with 2.99% improvement in SSIM. The SSIM evaluation results are given in the table below:

Table 3: SSIM under different methods

Image	GAN	AnimeGANv2	Ours
Architecture	0.5133	0.5028	0.5336
Car	0.4207	0.4104	0.4304
Plant	0.4216	0.4234	0.4342
Water	0.3806	0.3846	0.3923
Mountain	0.4236	0.4303	0.4431
People	0.3642	0.3536	0.3806

Finally, in order to verify the effectiveness of the modules proposed in this paper, each module is added to the base network individually for training in this section. Research method Based on the original GAN model, three sets of experiments were designed and compared the two improvement schemes of introducing Anime and Self-Attention mechanism respectively, A denotes the introduction of Anime, B denotes the Self-Attention mechanism, and Ours denotes the model that incorporates all the modules proposed in this chapter, and the image reconstruction model was computed to reconstruct the image and the SSIM and PSNR values of the input image, respectively. As shown in Table 4, the introduction of Anime and can greatly improve the SSIM and PSNR indexes, and similarly, the introduction of Self-Attention mechanism can improve the SSIM and PSNR indexes by a small margin, and the results show that the introduction of the above modules can more effectively extract the elements of digital art animation in the medium image, and provide effective elemental support for the design of the following cybersecurity publicity platform.

Table 4: Ablation experiment

Method	SSIM	PSNR
GAN	0.4113	13.1875
AnimeGANv2	0.4148	13.2913
GAN-Self-Attention	0.4201	13.4017
AnimeGANv2-Self-Attention	0.4232	13.4816

III. B. Platform performance analysis and application analysis

III. B. 1) Platform performance benchmarking analysis

Performance benchmarking is a method of evaluating the performance of a platform or a component under a specific load scenario, the core of which is to measure key metrics such as response time and resource utilization under different load conditions. Its core lies in measuring key metrics such as response time, throughput and resource utilization of the platform under different load scenarios to comprehensively reflect the performance status of the platform.JMeter is an open source tool for performance testing and load testing, mainly used to evaluate the performance of web applications. It can simulate a variety of load types, such as the number of concurrent users, throughput and response time, in order to test the performance of the system under different conditions. the JMeter client simulator is located on the server configuration is the same as the cluster server configuration, the client

simulator is designed to simulate the high-concurrency multi-user access requests, through the JMeter test plan to the test system's Web server to send HTTP requests, and thus obtain the platform performance data. The client simulator is designed to send HTTP requests to the web server of the system under test through the JMeter test plan under high concurrency. The performance data collection module is responsible for collecting the performance data of the system under test under workload, covering hardware resources, business, database and cluster metrics.

During the benchmarking process, a variety of objective metrics are collected to measure the performance of the network security awareness platform. For better metrics, this paper also considers two types of subjective metrics: Apdex (Application Performance Index) and QoS (Quality of Service), which are described below:

The calculation rule of Apdex is as follows: if the response time is less than or equal to T, the user is satisfied and scores 1. If the response time is between T and T4, the user considers it tolerable and scores 0.5. If the response time is more than T4, the user is not satisfied and scores 0. The formula is shown in equation (10):

$$Apdex_i = \frac{\left(SatisfiedCount + 0.5 \times ToleratingCount\right)}{TotalSamples} \tag{10}$$

where $SatisfiedCount$ represents the number of samples with which the user is satisfied, $ToleratingCount$ refers to the number of samples with which the user is tolerant, and $TotalSamples$ represents the total number of samples.

In addition to response time, the utilization of CPU, memory and other resources should be considered comprehensively when evaluating application performance. In this paper, we develop a performance evaluation system based on the Apdex index for cybersecurity awareness platforms. Different satisfaction intervals are defined for four important system resources, namely memory, network, CPU and disk, as shown in Table 5. Combining the definitions of satisfaction intervals for different indexes in Table 5, Equation (11) is utilized in order to quantitatively evaluate the state of resource utilization, thus reflecting the overall performance of the application platform more comprehensively.

Table 5: Definition of satisfaction intervals for different indicators

Status	Memory utilization rate	Network utilization rate	CPU utilization	Disk utilization rate
Satisfied	0~0.5	0~0.5	0~0.5	0~0.5
Tolerating	0.5~0.8	0.5~0.8	0.5~0.8	0.5~0.8
Frustrated	0.9~1	0.9~1	0.9~1	0.9~1

Quality of Service (QoS) is a measure of the performance of a system, service or network to assess the level of quality of the service it delivers, which can be an important attribute of concern for cybersecurity awareness platforms, and the assessment of performance strengths and weaknesses needs to be closely linked to QoS indicators. In this paper, average throughput and average response time are selected as the main evaluation indexes of QoS, and the 90th percentile response delay is introduced to fully cover the tail-end effect. In the benchmark test, it is assumed that the realized average throughput is $rps(P)$, the average response time is $Lat_{avg}(P)$, and the 90th percentile response time is $Lat_{P90}(P)$. In order to weigh these indicators comprehensively, this paper defines the quality of service (QoS) of the platform as a composite indicator, which is shown in Equation (11):

$$Q(P) = \frac{rps(P)}{\mu^* Lat_{avg}(P) + (1-\mu) * Lat_{P90}(P)} \tag{11}$$

In the formula, μ is used as a weighting factor for response time, which is used to balance the weights of the two indexes of average response time and 90th percentile response time in the evaluation of the strategy, to ensure a comprehensive consideration of service quality. During the operation of the experimental platform, the occurrence of request errors will seriously interfere with the user's operating experience, in view of this, when constructing the performance evaluation system of the network security publicity platform, particular attention is paid to the error rate as a key indicator, and the specific performance evaluation index formula is shown in equation (12):

$$P - score = \lambda\left(\sum Apdex_i\right)/i + \lambda Q(P) + Error(1-2\lambda) \tag{12}$$

where P-score performance score, $Apdex_i$ contains response time, CPU resource utilization, memory utilization, and disk utilization, and λ is a weighting factor, which assigns weights to $Apdex$, QoS, and error rate.

Three physical servers are used to build the Kubernetes cluster, and one node is deployed on each server, which are Master, Node1, and Node2.The JMeter test server is one physical server, which is used to simulate the concurrent requests of the users by JMeter, and the basic data and file resources are imported by Python scripts into EasyLab's database and the server. The workload contains 14 types of tasks, the workload data and JMeter test plan are imported to the corresponding server, the number of threads is set to 500, i.e., up to 500 virtual users make requests at the same time, and the platform performance benchmarking analysis is shown in Table 6. Based on the knowledge of the evaluation index data, it can be seen that the platform's five functional module index values are all lower than 0.5, indicating that users are satisfied with the performance of this paper's cybersecurity education platform.

Table 6: Platform performance benchmark test analysis

Functional module	Apdex	QoS	P-score
Data query	0.293	0.281	0.471
Information Express	0.365	0.259	0.358
Case Report	0.387	0.248	0.298
Legal aid	0.426	0.202	0.427
Exchange and share	0.358	0.254	0.373
Total	0.366	0.249	0.385

III. B. 2) Analysis of platform applications

The 800 people in C district were selected as the object of this study and divided into experimental group and control group, the experimental group used the systematic experimental intervention of this paper, and the control group used the traditional propaganda videos, posters, leaflets, SMS and other ways to publicize the network security. The Liket scale in the questionnaire was used to obtain the quantitative values of the three dimensions of the publicity effect (views X1, retweets X2, likes X3), and the multifactor t-test was performed to analyze the research data obtained by using the SPSS statistical analysis software as shown in Table 7, which is aimed at verifying the effectiveness of the application of this paper's network security publicity platform. The data performance in the table shows that there is a significant difference between the control group and the experimental group in the three dimensions of the publicity effect, i.e., compared with the traditional propaganda video, posters, leaflets, SMS and other ways of network security publicity, the publicity effect of the platform in this paper is more excellent, which can improve the user's awareness of network security.

Table 7: Multi-factor t-test analysis

Dimension	N	Control group		Experimental group		T-Value	P-Value
		Mean	SD	Mean	SD		
X1	400	2.842	0.342	3.921	0.381	4.241	0.002
X2	400	2.769	0.413	3.998	0.392	1.709	0.005
X3	400	2.947	0.394	4.027	0.407	3.453	0.003

IV. Conclusion

The cyber security publicity platform based on digital art animation elements designed in this paper successfully integrates the style migration technique with the self-attention mechanism, and significantly improves the extraction effect of animation elements through the improved AnimeGANv2 model. The experimental results show that compared with the traditional GAN model, the PSNR and SSIM metrics are improved by 1.39% and 2.99%, respectively, after using the AnimeGANv2-Self-Attention model. The design of the platform not only improves the fun and interactivity of cybersecurity education, but also greatly enhances the practicality of the platform through the integration of multi-module functions.

Based on the analysis of user participation data, there is a significant difference between the experimental group and the control group in terms of publicity effect, indicating that the platform is more effective than traditional means in raising users' awareness of network security. Through user feedback and data analysis, all functional modules of the platform show good user acceptance and participation, further proving its effectiveness in practical application.

References

[1] Chałubińska-Jentkiewicz, K., & Hoffman, I. (2022). Online Platforms in the Cybersecurity System. First published in 2022 by, 3.

[2] Liu, C. (2014). Research on the construction of saas-based network publicity support platform. Applied Mechanics and Materials, 543, 3280-3285.
[3] Chen, M. (2021, February). Research on Optimization and Integration of Computer Information Technology and Government Affairs Publicity. In Journal of Physics: Conference Series (Vol. 1744, No. 3, p. 032181). IOP Publishing.
[4] Liu, M., & Liu, L. (2025). Can China's publicity departments build people's trust by building platform government? Evidence from social media in public health emergencies. Chinese Public Administration Review, 16(2), 104-118.
[5] Pham, H. C., Brennan, L., Parker, L., Phan-Le, N. T., Ulhaq, I., Nkhoma, M. Z., & Nhat Nguyen, M. (2019). Enhancing cyber security behavior: an internal social marketing approach. Information & Computer Security, 28(2), 133-159.
[6] Kumar, R., Kumar, P., & Kumar, V. (2022). Network security issue and privacy on online social media platform: case study. AAYAM: AKGIM Journal of Management, 12(2), 96-103.
[7] Trim, P. R., & Lee, Y. I. (2019). The role of B2B marketers in increasing cyber security awareness and influencing behavioural change. Industrial Marketing Management, 83, 224-238.
[8] White, J. (2016). Cyber Threats and Cyber Security: National Security Issues, Policy and Strategies. Global Security Studies, 7(4).
[9] Trim, P. R., & Lee, Y. I. (2024). Advances in Cybersecurity: Challenges and Solutions. Applied Sciences, 14(10), 4300.
[10] Verma, A., Surendra, R., Reddy, B. S., Chawla, P., & Soni, K. (2021, March). Cyber security in digital sector. In 2021 international conference on artificial intelligence and smart systems (ICAIS) (pp. 703-710). IEEE.
[11] Dickerson, S., Apeh, E., & Ollis, G. (2020, November). Contextualised cyber security awareness approach for online romance fraud. In 2020 7th International Conference on Behavioural and Social Computing (BESC) (pp. 1-6). IEEE.
[12] Guo, H., & Tınmaz, H. (2023). A survey on college students' cybersecurity awareness and education from the perspective of China. Journal for the Education of Gifted Young Scientists, 11(3), 351-367.
[13] Zhang-Kennedy, L., & Chiasson, S. (2021). A systematic review of multimedia tools for cybersecurity awareness and education. ACM Computing Surveys (CSUR), 54(1), 1-39.
[14] Erendor, M. E., & Yildirim, M. (2022). Cybersecurity awareness in online education: A case study analysis. Ieee Access, 10, 52319-52335.
[15] Shillair, R., Esteve-González, P., Dutton, W. H., Creese, S., Nagyfejeo, E., & von Solms, B. (2022). Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise. Computers & Security, 119, 102756.
[16] Li Xiong,Zhang Jiye & Liu Yazhi. (2022). Speech driven facial animation generation based on GAN. Displays,74,
[17] Zhi Qiao & Takashi Kanai. (2021). A GAN-based temporally stable shading model for fast animation of photorealistic hair. Computational Visual Media,7(1),1-12.
[18] Chen Scarlett,Wu Zhe & Christofides Panagiotis D. (2021). Cyber-security of centralized, decentralized, and distributed control-detector architectures for nonlinear processes. Chemical Engineering Research and Design,165,25-39.
[19] Anonymous. (2009). Tufin Technologies: Tufin Technologies Delivers on the vision of Security Lifecycle Management with Tufin Security Suite (TSS) 5.0; TSS' distributed deployment architecture, new workflow GUI and Tufin Open Platform API's provide organisations with an automated, flexible, and highly robust platform to create, monitor, manage and audit network security policies. M2 Presswire,