Hindawi
Security and Communication Networks
Volume 2022, Article ID 9834541, 1 page
https://doi.org/10.1155/2022/9834541

*Retraction*

# Retracted: Antileakage Technology of Computer Video Information Encryption Based on Digital Information Method

**Security and Communication Networks**

Received 10 November 2022; Accepted 10 November 2022; Published 17 November 2022



*Security and Communication Networks* has retracted the article titled "Antileakage Technology of Computer Video Information Encryption Based on Digital Information Method" [1] due to concerns that the peer review process has been compromised.

Following an investigation conducted by the Hindawi Research Integrity team [2], significant concerns were identified with the peer reviewers assigned to this article; the investigation has concluded that the peer review process was compromised. We therefore can no longer trust the peer review process, and the article is being retracted with the agreement of the Chief Editor.

## References

[1] H. Sun, H. Jiao, and K. Lu, "Antileakage Technology of Computer Video Information Encryption Based on Digital Information Method," *Security and Communication Networks*, vol. 2022, Article ID 3576562, 10 pages, 2022.

[2] L. Ferguson, "Advancing Research Integrity Collaboratively and with Vigour," 2022, https://www.hindawi.com/post/advancing-research-integrity-collaboratively-and-vigour/.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 3576562, 10 pages
https://doi.org/10.1155/2022/3576562





*Research Article*

# Antileakage Technology of Computer Video Information Encryption Based on Digital Information Method

**Hua Sun,[1] Huihua Jiao ,[2] and Kai Lu[3]**

[1]*College of Electronics Engineering and Computer Science, Qiongtai Normal University, Haikou 571127, Hainan, China*
[2]*Inetwork and Educational Technology Center, Qiongtai Normal University, Haikou 571127, Hainan, China*
[3]*Department of Public Safety Technology, Hainan Vocational College of Political Science and Law, Haikou 570100, Hainan, China*

Correspondence should be addressed to Huihua Jiao; jhh@mail.qtnu.edu.cn

Received 29 March 2022; Revised 11 May 2022; Accepted 25 May 2022; Published 14 June 2022

Academic Editor: Mohammad Ayoub Khan



In order to better realize and ensure the security performance of network information itself, various possible risks must be prevented in advance, and a more reliable operation environment must be created as much as possible. A research study on computer video information encryption and antileakage technology based on the digital information method is proposed. Through the research on the working principle of computer display systems, this paper analyzes the common leakage sources. On this basis, it analyzes how to protect the electromagnetic wave leaked from the computer display system. Finally, it is proposed that the protective measure adopted in this paper is (transient electronic pulse emission survey technology, tempest) technology; that is, the image is processed at the source of image information to reduce the electromagnetic radiation of useful information. The corresponding digital filter is designed by fir, and the combined filtering of digital filter and analog filter is applied to eliminate the inherent disadvantage of periodic fluctuation of insertion loss of the digital filter. The research results show that the receiver before filtering can receive video images at multiple frequency points such as 20 MHz, 160 MHz, 220 MHz, 250 MHz, 270 MHz, 290 MHz, and 340 MHz, while the receiver after filtering can only receive video images at two frequency points of 20 MHz and 250 MHz, but it cannot recognize the words in the figure, and its effect is very obvious. It verifies the correctness and effectiveness of the theoretical analysis in this paper.

## 1. Introduction

Today's society is a highly information-based society, and the speed of information change and dissemination is also very fast. At the same time, various information systems are also emerging. The computer display system plays the role of information display and dissemination in the dissemination of information. In the process of information dissemination, information leakage and the acquisition of leaked information have become the biggest potential safety hazard in the process of information dissemination. Information security is also an issue that has been continuously studied for many years [1]. In order to solve the problem of information security, people have also made a lot of efforts, such as adding a firewall and information encryption. At the same time, it also produces the corresponding identity encryption system and so on. After many security mechanisms used by computers, the computer system seems safe [2]. However, in the process of computer use, a large amount of information radiation will be generated. The radiated electromagnetic wave can carry useful information in the computer transmission content. Through interception equipment such as interception receivers, it is easy to intercept the radiated electromagnetic information and restore the original information. Information protection technology (tempest) can be divided into hardware protection technology and software protection technology. Hardware protection technology usually refers to adding shielding or filtering equipment to the hardware equipment of computer systems to reduce the electromagnetic radiation of computer systems and

prevent information leakage. Software protection refers to encrypting image and video information through software processing. In information transmission, due to the different types of signals transmitted by computer display systems, including analog video signals and digital video signals, we need to take different electromagnetic leakage protection measures. For the same video signal, character image and noncharacter image will show different characteristics in the selection of antileakage methods due to their different bandwidth. For the image information after antileakage processing, how to evaluate the image quality of antileakage processing is also a problem to be solved.

Access to digital information: direct access to information and indirect access to information. Direct access to information: direct contact with things through human sensory organs to make the impression of the appearance and characteristics of things in the brain. For example, practical activities include social production, labor practice, and participation in various scientific experiments. The visiting activities include observing various phenomena in nature and society [3, 4]. Indirect access to information: identify and mine the information hidden behind the image with scientific analysis and research methods. For example, people-to-people communication, access to books and materials, radio and television, film and television materials, electronic books, etc. At present, there are four main factors affecting the security of computer network information data. First, the problem of Internet vulnerabilities; at this stage, the computer network operating system supports multiple platforms and projects to operate at the same time. Different projects can be carried out on the host receiving data packets at the same time. In all kinds of information and data transmission, once there is a weak link in the Internet working system, there will be Internet vulnerabilities, which will be extremely vulnerable to hackers. Second, the problem of computer virus infringement: with the continuous development and innovation of science and technology, the types of computer viruses are also constantly updated, and it is easy to attach to a program or file. Once the file carries a virus and is shared and opened by the computer, it will directly lead to the computer being infringed by the virus, and then the user information data will be destroyed. Third, the problem of service equipment data leakage: each computer system will have a certain degree of design deficiency. Once the system fails to deal with the error in time, the attacker will steal the user information and data through the system design defect, and the service equipment data will be leaked. Fourth, the problem of illegal intrusion is mainly that some criminals on the Internet use the user login name or instructions to invade the user's system terminal, generally steal or falsely use the trusted host or user to enter the electronic computer system, and use the way of stealing IP address to invade the terminal to steal network information [5, 6]. Figure 1 shows the antileakage technology of computer video information encryption.

## 2. Literature Review

Tempest technology is a processing technology for the safety protection of the electromagnetic environment. This technology mainly includes a series of technologies for analyzing and studying the sensitive information carried in the electromagnetic leakage signal, testing and receiving, intercepting and restoring, and leakage protection. Tempest is a general term in the field of information security [7]. Soft tempest technology refers to the relevant processing of electromagnetic information through computer software according to image processing technology, so as to reduce radiation, suppress high-frequency components, and achieve the purpose of preventing electromagnetic leakage. Hao and others proposed a computer video information leakage protection method based on digital filtering, determined the constraints of character bandwidth and image readability on digital filtering, designed a digital filter to meet the requirements by using fir, and applied an analog filter to suppress the periodicity of the digital filter. Finally, some important conclusions are obtained through the test [8]. Pan and others proposed a video information leakage prevention method based on dithering and image fusion, that is, by dithering the camouflage information, increasing its high-frequency component, and superimposing it with the useful information without dithering [9]. Park and others proposed a password based on oblique tent mapping. These cryptosystems generate chaotic binary sequences to encrypt the plaintext bit by bit. However, they cannot avoid floating-point data operation, which is affected by the word length of the computer, which makes encryption and decryption dependent on the computer. In other words, if the computer word length of the sender and the receiver is different, because of the initial value sensitivity of chaos, the decryption process will lose synchronization with the encryption [10]. Li and others believe that for a complete computer display system, the information leakage of this part can be restrained to a certain extent by strengthening the computer host to shield the electromagnetic radiation emitted by its motherboard and graphics card. In the connection between the graphics card and the display device, the cable with a certain shielding performance can also be used to suppress the radiation leakage in the process of signal transmission [11]. Luo and others proposed that MEMS has the characteristics of small volume, lightweight, low energy consumption, and stable performance. The maturity of relevant technologies is conducive to mass production. It also has the characteristics of small inertia, high resonance frequency, short response time, high technical content of achievements, and high added value of products. Therefore, it has a wide range of application fields and prospects [12]. According to the electromagnetic theory and information interception theory, Jeong and others stated that the higher the frequency corresponding to the signal carrying useful information, the greater the field strength at the same length of video cable and at the same interception distance, and the greater the possibility of interception [13]. Zhao and others set information encryption and decryption as the same key, which is simple and practical. In the process of practical application, users must do a good job in the transmission and storage of a single key. If the key is obtained by others, it will directly damage their own information and data security [14]. Mathews and others studied the image fusion algorithm of useful information and camouflage dithering information

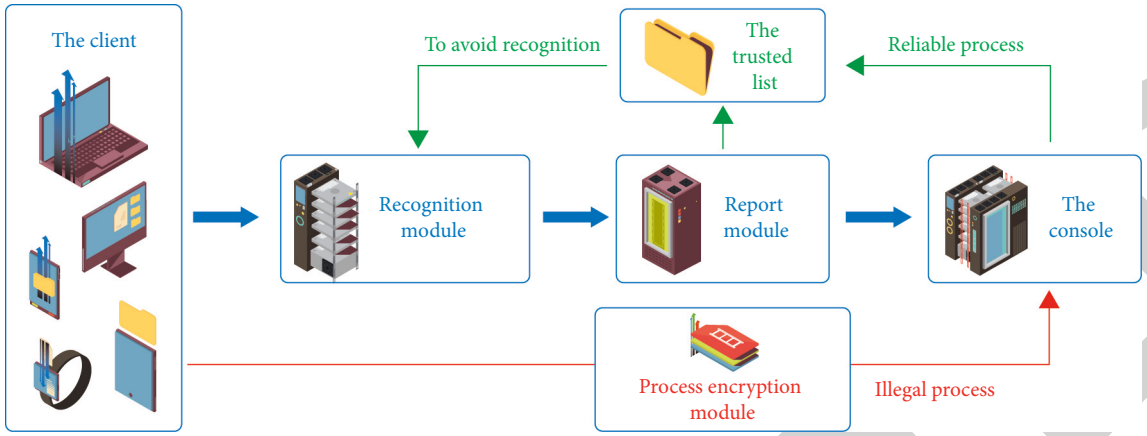


Figure 1: Computer video information encryption and antileakage technology.

and verified the expected conclusion that "fusing camouflage dithering information image and useful information image can make the interceptor only intercept camouflage information at a certain interception distance, but not useful information" [15].

Based on this research, this paper proposes a research on the antileakage technology of computer video information encryption based on the digital information method. Through the research on the mechanism and antiradiation method of computer video information electromagnetic radiation and the antileakage method simulation of different kinds of image information, this paper studies the antileakage method suitable for analog and digital image information. Secondly, by comparing different image quality evaluation standards, the appropriate image quality evaluation standards for different image types before and after antileakage processing are analyzed. Finally, the simulation software of computer video information leakage prevention is realized, which can guide the hardware design of video information leakage prevention. Finally, the whole research process is summarized.

## 3. Research Methods

### 3.1. Principle and Method of Digital Information Leakage Prevention in Video Information

*3.1.1. Digital Signal Interception Principle.* The waveform of the digital signal includes high and low levels and rise and fall times. An ideal digital signal $s(T)$ can be expressed as the delay superposition of rectangular waves in the time domain. Its power spectral density $s(\omega)$ is also the superposition of countless signals after different phase shifts. In addition to the main lobe, there are many side lobes. The energy of each lobe decreases gradually with the increase of frequency. According to the electromagnetic field theory, the radiation efficiency of the same radiation source increases with the increase of frequency. As long as the interceptor tunes the receiver to a high-end lobe of the $S(T)$ spectrum, it can play the role of band-pass filtering [16].

*3.1.2. Spectrum Spread Antiinformation Leakage Technology.* As long as the interception receiver receives one lobe of the original video signal, the signal can be reproduced by means of detection, amplitude limiting, shaping, and amplification. After experimental observation, the waveform characteristics can be received when the bandwidth of the receiver reaches 60% of the lobe of the original video signal. Therefore, if the spectrum of the video signal is expanded, so that the intercepting receiver cannot obtain all the waveform information, the effect of information leakage prevention can be achieved. If the spectrum lobes of the original video signal are very narrow, the receiving bandwidth of the interception receiver will easily reach more than 60%, so as to intercept the video information. If the spectrum of the original video signal is widened by processing, it is difficult for the interception receiver to receive all the information of one lobe, ensuring the security of the information [17].

According to the theory of signal and system, when the two signals are convoluted in the frequency domain, the spectrum width of the signal is equal to that of the broadband signal. For video signals, as long as the spectrum bandwidth of a similar noise signal is much higher than the original video signal, the spectrum of video signals can be expanded through signal processing to prevent information leakage. White noise is an ideal spectrum spread signal. Its power spectral density is constant and has uniform characteristics in an infinite frequency band. However, in signal processing, the autocorrelation function and power spectral density of white noise, which have ideal spectral characteristics, do not exist in fact. Using "0" and "1" to form a random sequence, the probability of two symbols is close to the same. This sequence has an autocorrelation function similar to the white noise signal, so the white noise can be approximated. A pseudorandom sequence is often used in the random analysis; that is, it is not a real random sequence, but a sequence with a long period and the characteristics of a random sequence. Its algorithm is widely used because it is easier to implement than a random sequence. When the period of the pseudorandom sequence is large, the spectral characteristics of its autocorrelation function and power spectral density can be approximated as white noise. For digital video signals, the pseudorandom sequence can be XORed with the original video data to spread the spectrum and reduce the signal-to-noise ratio, so as to improve the security of information transmission.

*3.1.3. Leakage Characteristics of Video Information Display.* If the information displayed by the computer display device changes slowly in a certain period of time, it is easier for the interceptor to obtain useful information, which shows that the leakage of video information is also related to the content displayed by the display device. This characteristic of slow change is particularly obvious when displaying text information because text information is mostly displayed in black and white or other color combinations with high contrast for visual effect, the high and low changes of the digital signal are obvious, and the change of display content is less [18]. The refresh frequency of mainstream LCD displays on the market is basically fixed at 60 Hz, which is more helpful for interceptors to distinguish the refresh signal of display equipment from the useful information displayed. Therefore, the digital signal of text information is more dangerous, which is easy to cause information leakage. For text information, the signal waveforms corresponding to horizontal and vertical strokes are different. If the word "one" is displayed in black on a white background, the corresponding line will contain a long string of black pixel information. In the digital signal, each black pixel will be represented by three ways of "00000000." Therefore, this line of video information will contain a lot of symbols "0." Accordingly, if the word "1" is displayed, the black pixels in a line will be less than the white pixels, while the white pixels are represented by three channels of "11111111;" this line of video information will contain a lot of symbols "1." It can be seen that the ideal video signal is a periodic rectangular wave. The difference is that when a line of video information contains more horizontal strokes, the duration of the low-level signal waveform in the time domain is longer. On the contrary, the high level corresponding to the vertical stroke lasts for a long time. The rectangular wave signal is shown in Figure 2.

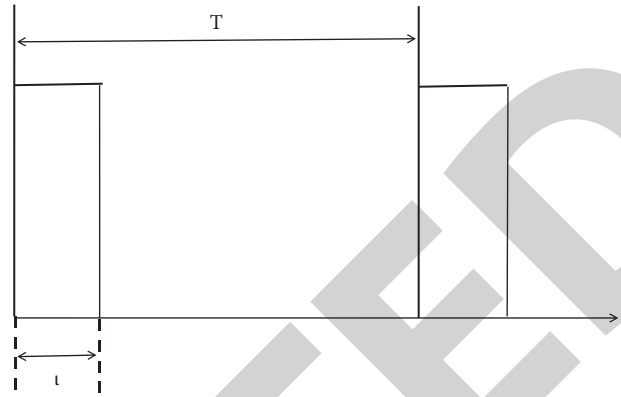


Figure 2: Periodic rectangular wave.

### 3.2. Design of Video Information Leakage Prevention Method

*3.2.1. Design of Antileakage Method of Analog Video Information.* In the analog image signal, the low-frequency component usually represents the area where the brightness value or gray value changes slowly, that is, the flat area in the image. The high-frequency component usually represents the area where the brightness value or gray value in the image changes significantly. It usually refers to the edge, contour, or area that can reflect the image information in the image. The detail part of the image is usually the high-frequency component of the image. For the interception receiver, the high-frequency component is often easier to be intercepted. For those who intend to steal information, intercepting high-frequency components can restore the original image information. Therefore, in the antileakage processing of the image, suppress the high-frequency component as much as possible, or confuse each other by changing the high-frequency component and increasing the camouflage high-frequency component, so as to achieve the antileakage processing of analog video information. Therefore, this paper introduces two antileakage methods for analog video information, namely, FIR digital filtering and image fusion technology based on dithering pseudoemission [19, 20]. These two antileakage technologies are briefly introduced below.

*(1) FIR Digital Filter.* Filters are divided into traditional analog filters and digital filters. A digital filter uses a filter composed of an addition device, multiplication device, delay device, etc. It can be implemented using integrated hardware or computer software. The parameters are easy to modify and the cost is relatively low. The analog filter uses the traditional circuit, which is composed of resistance, inductance, capacitance, and operational amplifier. Once the circuit is designed, it is not easy to change. Therefore, the change cost is high and the use is not easy. Therefore, in the selection and design of the filter, we use the digital filter. There are two kinds of digital filters: one is FIR digital filter and the other is IIR digital filter.

FIR digital filter is a finite length unit response filter, which means that its impulse response is limited. IIR is the infinite unit impulse response. The difference between fir and IIR is that fir has strict linear phase characteristics, while IIR's linear phase characteristics are difficult to control. In the process of image information transmission, we need strict phase characteristics to make the image transmission process not distorted. Therefore, in the selection of digital filters, FIR digital filter is selected in this paper. Therefore, this article mainly introduces the design of the FIR digital filter. The design methods of the FIR digital filter include the window function method and frequency sampling method. The window function method is relatively simple, and there are specific closure formulas to follow. The window function method is used to design FIR digital filter.

The basic principle of designing a digital filter by the FIR window function method is as follows.

When the transfer function $H_d(e^{jw})$ is known, the unit impulse response $h_d(n)$ is

$$H_d(n) = \frac{1}{2\pi} \int_{-\pi}^{\pi} \left(e^{jw}\right) e^{jwn} \mathrm{d}w. \tag{1}$$

In general, the unit impulse response of the ideal filter is infinite. The way to obtain the finite impulse response is to

modify $h_d(n)$ with the finite weighted sequence window function $w(n)$, intercept part of it, and generate a new $h(n)$:

$$h(n) = h_d(n)w(n). \tag{2}$$

The finite sequence $h(n)$ is used to replace the original unit impulse response $h_d(n)$, and the output image function response is obtained by convolution with the input function of the original image. In the design of a digital filter, the periodicity and aliasing of filter insertion loss must also be eliminated. (1) Periodicity: the unit impulse response of the ideal low-pass digital filter corresponds to a set of discrete quantities, which is equivalent to sampling in the time domain [21]. Let $x_a(t)$ be the signal after $x_a(t)$ sampling, as shown in formulas (3) and (4).

Time domain:

$$x_a(t) = \sum_{n=-\infty}^{\infty} x_a(nT)\delta(t - nT). \tag{3}$$

Frequency domain:

$$x_a(t)(j\Omega) = \frac{1}{T}\sum_{k=-\infty}^{k=\infty} x_a(j\Omega - jk\Omega_s), \tag{4}$$

where $x_a(j\Omega)$ is the Fourier transform of $x_a(t)$. It can be seen from (4) that time domain sampling corresponds to periodic continuation in the frequency domain, resulting in passband at periodic high frequency so that high-frequency signal can pass through.

*(2) Image Fusion Technology Based on Dithering Pseudoemission.* When dealing with the leakage prevention of analog video information, the basic idea is to suppress the high-frequency components in the image. Another method is to increase the camouflage high-frequency component. Therefore, image fusion based on dithering pseudoemission is to form interfering high-frequency information by adding camouflage high-frequency components, so as to protect the original information. A specific description of the algorithm: we call the camouflaged image a leak image and the image that needs to be camouflaged as the original image. The final goal we want to achieve is to fuse the two images and overlay them [22] and ensure that the superimposed image is not easy to be detected. Here, assuming that $C_{xy}$ is the pixel value of the original image at the screen $x$ and $y$, and $E_{xy}$ is the pixel value of the leaked image at the screen $x$ and $y$, the pixel value of the fused image is (5):

$$S_{x,y,c} = \left(\alpha \cdot C_{x,y,c}^{\gamma} + \beta \cdot \mathrm{E}_{x,y} \cdot d_{x,y}|_n\right)^{1/\gamma}, \tag{5}$$

where $d_{x,y}|n = (-1)^{y+|x/n|}$ is the jitter function. $0 < \alpha < 0.5$ is the reduction coefficient of information pixel value, and $\beta$ is the jitter coefficient of camouflage information, where $\alpha + \beta = 1$. Parameter $r$ is usually between 1.0 and 2.0.

*3.2.2. Design of Antileakage Method of Digital Video Information.* For the antileakage processing method of digital video information, the motherboard adopts parallel signal transmission when transmitting video information to the graphics card through the bus. When changing the digital video information, we need to change the internal coding mode of video information, so as to broaden the spectrum and change the high-frequency component. The summary continues the previous research results. For digital video information, random scrambling and complementary scrambling are used to process the original information, so as to change the image spectrum and prevent it from being intercepted and received.

(1) Random scrambling: during the transmission of digital video information, the signal is transmitted by three 8-bit parallel data lines. Therefore, each *R*, *G*, and *B* component is transmitted in the form of an 8-bit binary code. Random scrambling is to randomly scramble the digital codes on some bits on the basis of digital codes and replace them with pseudorandom codes. The codes replaced by pseudorandom sequences are expressed as random sequences in the time domain and random spectrum in the frequency domain. After such processing, useful information can be effectively protected. In the existing research, the research results believe that for random scrambling, the high-order digital coding has a great impact on the visual effect of the image and believe that the random scrambling with more than five scrambling bits from the low order can ensure that the processed image information is safe.

(2) Complementary scrambling: complementary scrambling is developed on the basis of random scrambling. It mainly combines the visual effect of human eyes on the basis of random scrambling. When human eyes look at objects and images, there will be a short visual stay effect. Complementary scrambling makes use of this to add and subtract pseudorandom sequences in the last four bits of binary coding of digital signals. Previous studies can also prove that the addition and subtraction of complementary scrambling bits for the last four bits can ensure the scrambling effect. Since the previous frame image is added with pseudorandom sequence and the latter frame image is subtracted with pseudorandom sequence, it has little impact on vision as a whole, which is the effect of hybrid complementarity. After complementary scrambling of the original image, the overall time domain and frequency domain are changed, which can also achieve the purpose of protecting the useful information of the image [23–25].

### 3.3. Analysis of Image Leakage Prevention Features before and after Video Processing

*3.3.1. Research on Digital Filtering of Character Image.* When displaying images on the computer screen, the screen resolution and refresh rate are closely related to the image display. For the screen with a resolution of $1024 * 768$, that is, each horizontal line contains 1024 pixels, a total of 768 lines. That is, the number of rows scanned is 768. Refresh

rate refers to the number of times the screen is refreshed per second. The higher the refresh rate, the more stable the image is, so the refresh rate is also called field frequency. The screen resolution and refresh rate determine the size of the signal point frequency. If the screen resolution is $m \times n$ and the refresh rate is $r$, the size of the point frequency $f$ of the signal is shown in

$$f = m \times n \times r \times 1.277. \quad (6)$$

According to the existing research, the point frequency bandwidth width of the character image is determined according to the vertical stroke of the image. Assuming that the screen resolution is $1013 * 657$ and the refresh rate is 65 MHz, the point frequency under this condition is 67.4 MHz according to the computer display monitor timing VESA and the standards given in the industry standards and guidelines. After practical verification, it is concluded that the number of points and pixels occupied by vertical strokes of characters with different font sizes determine the radiation bandwidth. Assuming that the font size is size 4, its radiation bandwidth is 77.4/17 = 3.3 MHz. According to the conclusions of previous studies, if 25% of the spectrum component in the character radiation bandwidth can be suppressed (the remaining spectrum range is the safe bandwidth), the video information corresponding to the character cannot be reproduced. Different character sizes affect the signal bandwidth. Therefore, for character images, the antileakage method of digital filtering is mainly studied.

Taking typical characters as an example, the characteristics of character images after antileakage processing are analyzed. The resolution of the screen is $1366 * 768$ and the refresh rate is 60 Hz. According to the VESA standard and display timing standard, the point frequency corresponding to the screen resolution and refresh rate is 85.5 MHz. The reason why the dot frequency is not directly calculated by multiplying the screen resolution and refresh rate is that the screen resolution and refresh rate only represent the part displayed on the screen. In the internal processing of the computer, it is obviously more complex, and there are some areas that are not displayed on the screen. When considering the point frequency, we take the way of finding the VESA standard. Because the pixel value occupied by the vertical stroke of font size 4 is 29, the radiation bandwidth of the character size 4 is 85.5 MHz = 29 = 2.93 MHz. According to previous studies, if the spectrum of 30% of the character bandwidth is suppressed, the video information corresponding to the character cannot be reproduced. The security bandwidth of the four characters is 2.93 MHz × 0.7 = 2.05 MH. Therefore, the security bandwidth of our image design is 2 MHz. Select the drawing base window and set the order to 64. Next, do antileakage simulation processing for the character image information [25].

Digital filtering: take the points of the image in the order of rows and columns, and draw the $R$, $G$, and $B$ of each pixel separately to obtain the following time domain diagram. The time domain diagram can be obtained by the Fourier transform. According to the safety bandwidth of No. 2 character of 2 MHz, the software is used to filter it. The time domain diagram and frequency domain diagram before and after filtering are shown in Figures 3 and 4.

It can be seen from the image that the values of $R$, $G$, and $B$ are the same for black-and-white characters. Enlarge the value of the R component to see that the time domain amplitude of the black-and-white character image is between 255 and 0. Beat the cycle. But the visual quality of the image is sacrificed. Next, the author tested 3 MHz, 6 MHz, and 10 MHz cut-off frequencies. When the cut-off frequency increases, the visual effect will be improved, but the security of the spectrum will be sacrificed. The spectral correlation coefficient after filtering is 0.8832.

Filter the black background picture under the condition of the same screen resolution and refresh rate. The simulation results of filtering are shown in Figures 5 and 6.

The correlation analysis of the spectrum before and after processing shows that the correlation coefficient is 0.8901.

## 4. Result Discussion

Using the filter designed by the above filter parameters and the analog filter with a cut-off frequency of 80 MHz, the test system is established. Due to the strict linear phase of the FIR filter, the filtered image distortion is small, but the whole image has a certain time delay, and the readability of the image is still very good. Figures 7 and 8 are the radiation spectra measured in the frequency range of 10 MHz~30 MHz for the images before and after filtering, respectively.

As can be seen from Figure 8, due to the large spatial coupling of high frequency, the filtering effect is reduced, and the corresponding radiation suppression effect is only 15~20 dB. The frequency range of the image reception and reproduction test is 20~500 MHz. Through test and comparison, it can be seen that the receiver before filtering can receive video images at multiple frequency points such as 20 MHz, 160 MHz, 220 MHz, 250 MHz, 270 MHz, 290 MHz, and 340 MHz, while the receiver after filtering can only receive video images at two frequency points of 20 MHz and 250 MHz but can not recognize the words in the figure, and its effect is very obvious. The reason is that the 20 MHz frequency point is lower than the cut-off frequency of the filter, and the filter does not work; The reception of the 250 MHz frequency point is mainly caused by the periodicity of insertion loss of the digital filter. Although an analog filter is added to the test, its filtering performance decreases with the increase of frequency.

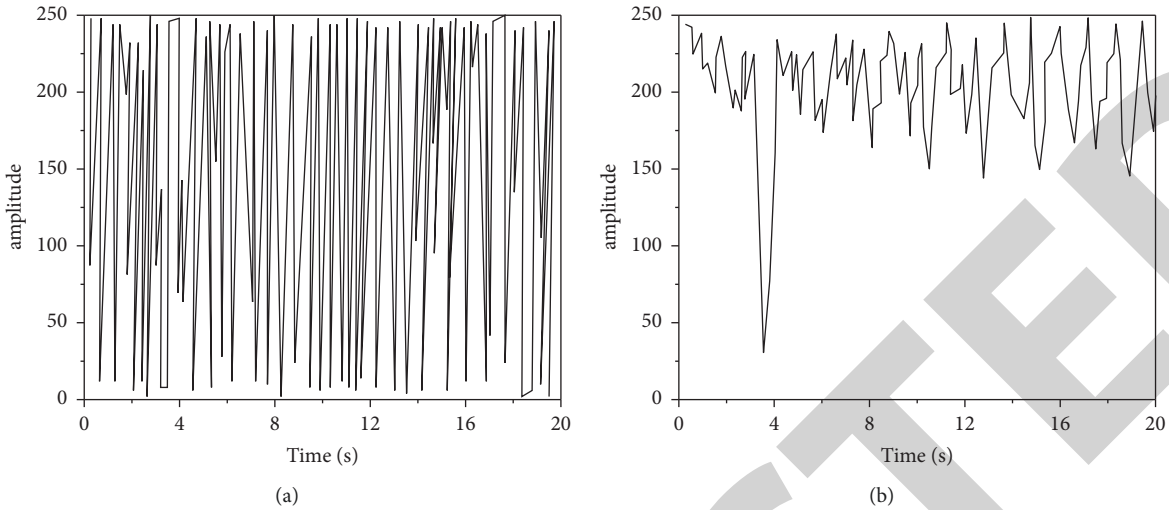


Figure 3: Time domain map before and after white bottom image processing in a digital filtering simulation experiment. (a) R-route time domain information of the original image. (b) The R time domain information after filtering.

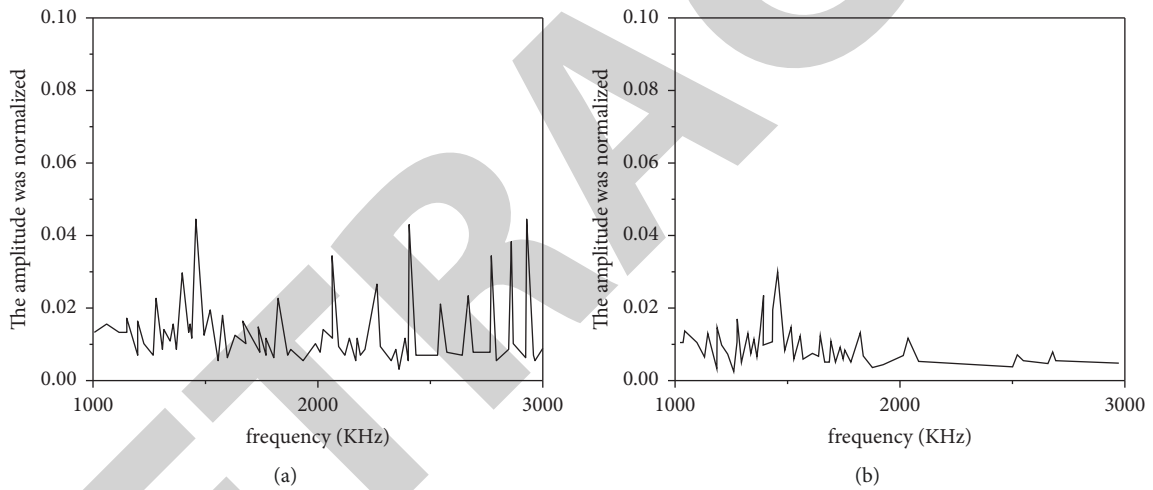


Figure 4: Frequency domain diagram before and after white background image processing in a digital filtering simulation experiment. (a) The R-route frequency domain information of the original image. (b) The R-frequency domain information after filtering.

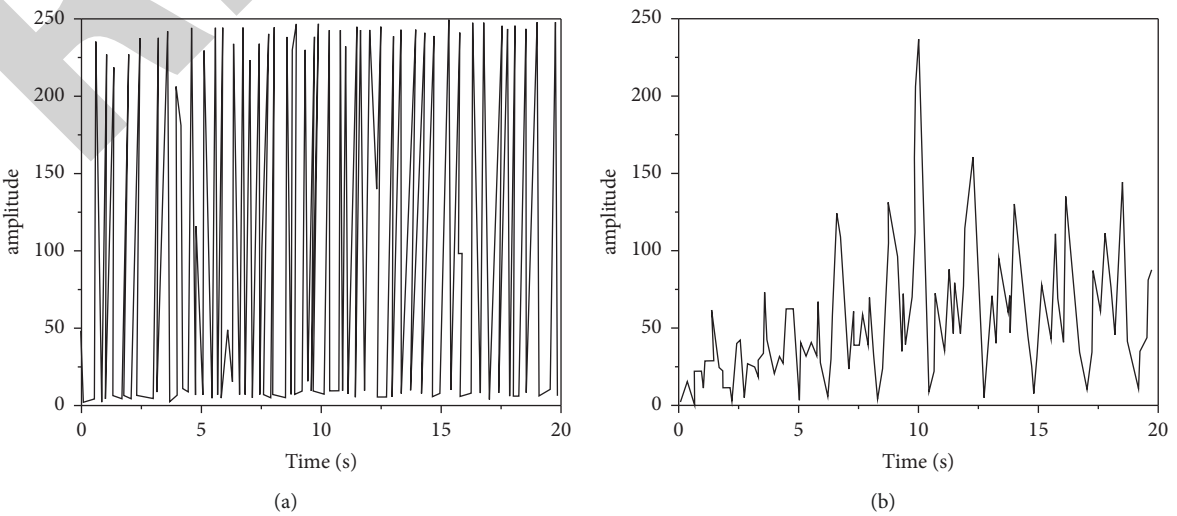


Figure 5: Time domain diagram of black background image before and after filtering in a digital filtering simulation experiment. (a) R-route time domain information of the original image. (b) The R time domain information after filtering.

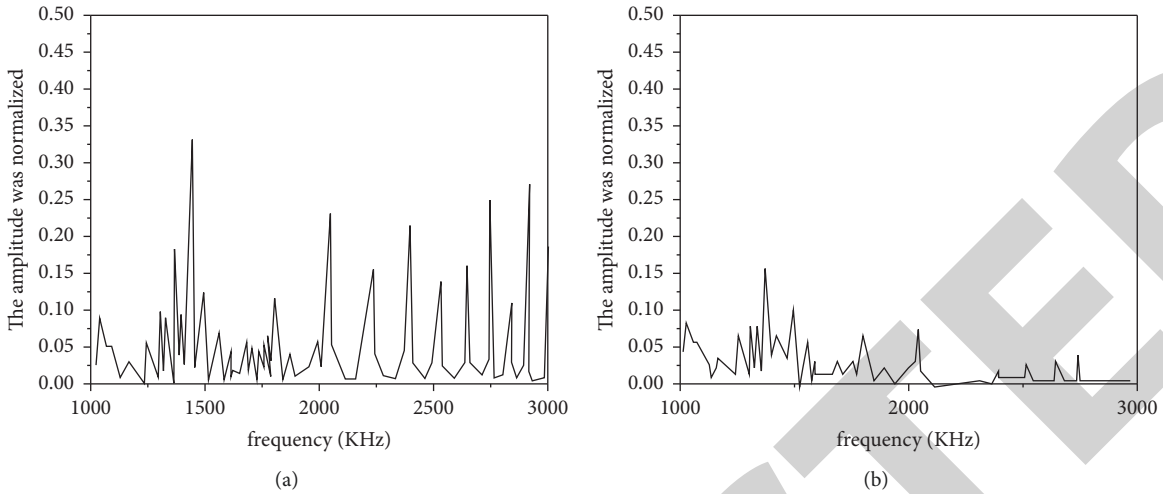


Figure 6: Frequency domain diagram of black background image before and after filtering in a digital filtering simulation experiment. (a) The R-route frequency domain information of the original image. (b) The R-frequency domain information after filtering.

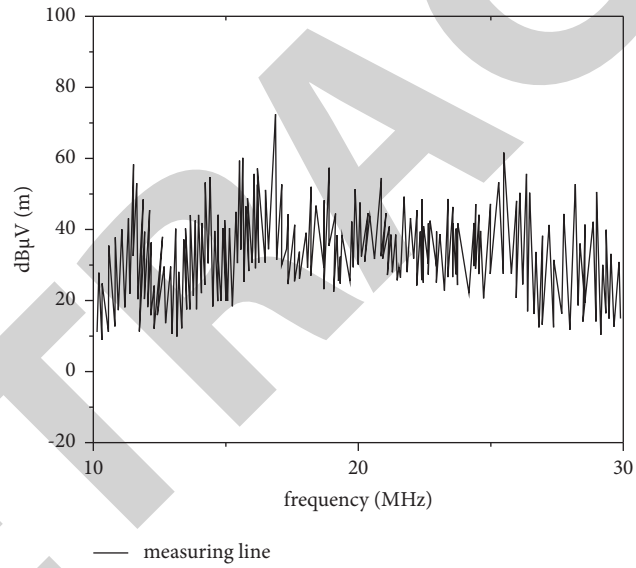


Figure 7: Spectrum received before filtering.

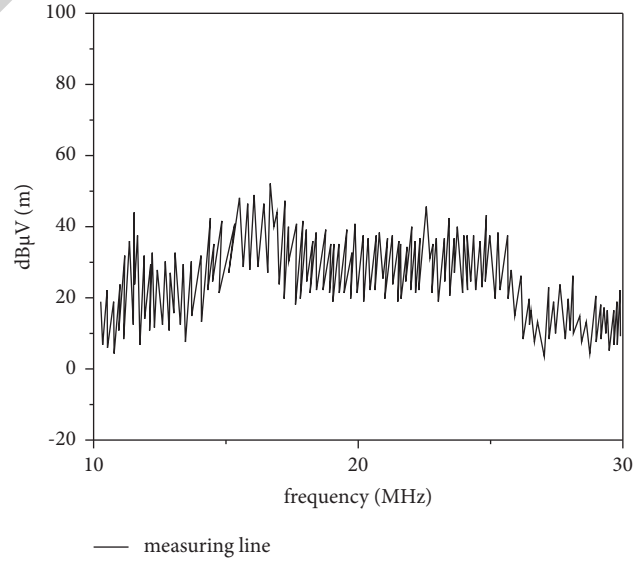


Figure 8: Received spectrum after filtering.

## 5. Conclusion

With the continuous development and innovation of modern science and technology, computer network communication technology not only provides great convenience for people's daily work and life but also poses a greater challenge to the security protection performance of user information and data. Therefore, in order to ensure the long-term and stable development of computer network communication and the security of user information and data, we must pay attention to improving the security and encryption level of computer information and data, so as to ensure that our own information and data are not stolen by others. This paper makes an in-depth study on the digital filtering method of computer video information leakage prevention in theory, determines the constraint conditions and constraint criteria of character bandwidth and image readability for digital filtering, and applies the combined filtering of digital filter and analog filter to eliminate the inherent disadvantage of periodic fluctuation of insertion loss of the digital filter. Finally, the analysis results are verified by experiments, and some conclusions with important application values are obtained.

## Data Availability

No data were used to support this study.

## Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this article.

## Acknowledgments

This work was supported by the Hainan Provincial Natural Science Foundation of China (Grant no. 621RC1082) and the Scientific Research Project of Colleges and Universities in Hainan Province (Grant no. Hnky2021ZD-26, Research on Key Technologies of Student Credit Investigation and Certificate Deposit Based on Blockchain).

## References

[1] J. Wu, Z. Liu, S. Yuan, J. Cai, and X. Hu, "Source term estimation of natural gas leakage in utility tunnel by combining cfd and bayesian inference method," *Journal of Loss Prevention in the Process Industries*, vol. 68, no. 1, pp. 104328–104332, 2020.

[2] J. Chen, Y. Gong, T.-H. Jiang, A.-X. Pan, S. H. Wang, and Z.-G. Yang, "Failure analysis on abnormal leakage of tp321 stainless steel pipe of medium temperature shifting gas in hydrogen production system," *Engineering Failure Analysis*, vol. 125, no. 11, pp. 105413–105416, 2021.

[3] Y. Hao, Y. Wu, J. Jiang et al., "The method for leakage detection of urban natural gas pipeline based on the improved ita and alo," *Journal of Loss Prevention in the Process Industries*, vol. 71, no. 4, pp. 104506–104560, 2021.

[4] M. Li, Y. Song, X. Zhang, Y. Chen, and C. Tang, "A review of implant intra-body communication," *Journal of Beijing Institute of Technology (Social Sciences Edition)*, vol. 31, no. 1, pp. 1–29, 2022.

[5] A. Ueda, A. Ozawa, Y. Kusakabe et al., "Geochemical monitoring of deionized seawater injected underground during construction of an lpg rock cavern in namikata, Japan, for the safety water curtain system," *Environmental Earth Sciences*, vol. 80, no. 22, pp. 744–826, 2021.

[6] Q. Jia, G. Fu, X. Xie, S. Hu, Y. Wu, and J. Li, "Lpg leakage and explosion accident analysis based on a new saa method," *Journal of Loss Prevention in the Process Industries*, vol. 71, no. 5, pp. 104467–104471, 2021.

[7] W. Jin, A. Sankoh, Y. Dong, Z.-Q. Zhong, R. P. Giddings, and M. O'Sullivan, "Hybrid ssb ofdm-digital filter multiple access pons," *Journal of Lightwave Technology*, vol. 38, no. 8, pp. 2095–2105, 2020.

[8] H. Hao, Q.-Y. Zhao, L.-D. Kong, S. Chen, H. Wang, and Y.-H. Huang, "Improved pulse discrimination for a superconducting series nanowire detector by applying a digital matched filter," *Applied Physics Letters*, vol. 119, no. 23, pp. 232601–232605, 2021.

[9] L. Pan, Y. Wu, W. Wang, Y. Wei, and Y. Yang, "A flexible high-selectivity single-layer coplanar waveguide bandpass filter using interdigital spoof surface plasmon polaritons of bow-tie cells," *IEEE Transactions on Plasma Science*, vol. 48, no. 10, pp. 3582–3588, 2020.

[10] Y. Park, D.-H. Moon, and G. Heo, "Digital implementation methods for grid synchronization using an integrated filter," *Journal of Power Electronics*, vol. 20, no. 5, pp. 1261–1272, 2020.

[11] H. Li, Y. Yang, Y. Dai, S. Yu, and Y. Xiang, "Achieving secure and efficient dynamic searchable symmetric encryption over medical cloud data," *IEEE Transactions on Cloud Computing*, vol. 8, no. 2, pp. 484–494, 2020.

[12] T. Luo, T. Zhou, and J. Qu, "Lifetime division multiplexing by multilevel encryption algorithm," *ACS Nano*, vol. 15, no. 4, pp. 6257–6265, 2021.

[13] B.-G. Jeong, T.-Y. Youn, N.-S. Jho, and S. U. Shin, "Blockchain-based data sharing and trading model for the connected car," *Sensors*, vol. 20, no. 11, p. 3141, 2020.

[14] R. Zhao, Y. Zhang, X. Xiao, X. Ye, and R. Lan, "TPE2: three-pixel exact thumbnail-preserving image encryption," *Signal Processing*, vol. 183, no. 6, pp. 108019–108022, 2021.

[15] M. Mathews, "Using bit flips as a source of randomness in cubesat communication encryption," *Acta Astronautica*, vol. 179, no. 4, pp. 546–549, 2021.

[16] A. Shankar, P. Pandiaraja, K. Sumathi, T. Stephan, and P. Sharma, "Privacy preserving e-voting cloud system based on id based encryption," *Peer-to-Peer Networking and Applications*, vol. 14, no. 4, pp. 2399–2409, 2021.

[17] B. Chen, L. Wu, H. Wang, L. Zhou, and D. He, "A blockchain-based searchable public-key encryption with forward and backward privacy for cloud-assisted vehicular social networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 5813–5825, 2020.

[18] M. Koziol, "New encryption strategy passes early test: ghost polarization harnesses ultrafast fluctuations that occur in a light wave," *IEEE Spectrum*, vol. 57, no. 7, p. 11, 2020.

[19] Y. Zhou, J. Guo, and F. Li, "Certificateless public key encryption with cryptographic reverse firewalls," *Journal of Systems Architecture*, vol. 109, no. 3, pp. 101754–101759, 2020.

[20] L. Yang, B. Yang, and C. Xiang, "Quantum public-key encryption schemes based on conjugate coding," *Quantum Information Processing*, vol. 19, no. 11, pp. 415-416, 2020.

[21] A. K. Singh and C. Kumar, "Encryption-then-compression-based copyright protection scheme for e-governance," *IT Professional*, vol. 22, no. 2, pp. 45–52, 2020.
[22] M. Rasori, P. Perazzo, and G. Dini, "A lightweight and scalable attribute-based encryption system for smart cities," *Computer Communications*, vol. 149, pp. 78–89, 2020.
[23] Z. Li, S. Ling, C. Xing, and S. L. Yeo, "On the bounded distance decoding problem for lattices constructed and their cryptographic applications," *IEEE Transactions on Information Theory*, vol. 66, no. 4, pp. 2588–2598, 2020.
[24] L. Guo, Z. Li, W.-C. Yau, and S.-Y. Tan, "A decryptable attribute-based keyword search scheme on ehealth cloud in internet of things platforms," *IEEE Access*, vol. 8, no. 99, pp. 26107–26118, 2020.
[25] L. Chen, M. Liu, Z. Wang, and Z. Dai, "A structure evolution-based design for stable iir digital filters using amecodes algorithm," *Soft Computing*, vol. 24, no. 7, pp. 5151–5163, 2020.