Scientific Research Publishing

Int. J. Communications, Network and System Sciences, 2022, 15, 43-52
https://www.scirp.org/journal/ijcns
ISSN Online: 1913-3723
ISSN Print: 1913-3715

Research on Software Design of Image Copyright Protection in the Field of Education

Yu Huang, Zhengyue Han, Zhenjie Wu, Hanyue Zhang, Rong Wu

Jinan University, Guangzhou, China
Email: angle199421@126.com

How to cite this paper: Huang, Y., Han, Z.Y., Wu, Z.J., Zhang, H.Y. and Wu, R. (2022) Research on Software Design of Image Copyright Protection in the Field of Education. *Int. J. Communications, Network and System Sciences*, **15**, 43-52.
https://doi.org/10.4236/ijcns.2022.154004

Received: January 4, 2022
Accepted: January 18, 2022
Published: April 27, 2022

Abstract

Nowadays, image copyright protection is one of the key points of information security in the field of education. Based on the transient property of human vision, the anti-theft and copyright protection strategies are proposed based on the idea of animation synthesis. In this paper, experiments are designed and compared from multiple perspectives. The results show that the strategy based on animation synthesis can not only ensure the browsing effect of images, but also effectively achieve the purpose of preventing interception via screenshot and protecting the legitimate rights of the original images.

Keywords

Copyright Protection, Image Anti-Theft, Screenshot, Animation Synthesis

1. Introduction

With the rapid development of computer and network technology, more and more data and information involving academia, in the form of pictures, are uploaded to the network. Because of the convenience of storing, copying, modifying and spreading picture information, the network pictures are widely disseminated and easily pirated [1]. Hence, images can easily be copied, modified and redistributed without authorization. However, people's weak awareness of image copyright in the field of education leads to the fact that network images infringement and embezzlement are very common [2].

Taking extracurricular tutoring industry in China as an example, the advertising chart of a certain tutoring course is statistically analyzed. They found that more than 50 percent advertising window or detail images were identical. Apparently, the image copyright protection in the field of education is facing unprecedented piracy threats. Popular websites, platforms on the images of random theft and malicious tampering frequent disputes. Many academic institu-

tions spend much time on avoiding picture theft than creating pictures. There have also been numerous complaints that private images have been intentionally or unintentionally destroyed. Bad consequences are easy to cause the aversion of the originators and lack of creative enthusiasm. Simply relying on legal means is not enough to solve the problem of network picture copyright protection. Technology is indispensable. It is very important to design reasonable technical means to protect the legitimate rights and interests of the picture creators and prevent illegal infringement and embezzlement. It is scientific and significant to maintain the normal order and sustainable development of online community [3].

In order to solve the problem of information security and copyright protection, the academic circle mainly adopts three technologies, including encryption, digital signature and digital watermarking [4]. The consequence of encryption is that raw information cannot be known and accessible to more people through public systems and platforms. And once it is decrypted, it can be copied and spread at will. Digital signatures require additional information and do not allow minor changes to the original information [5]. Digital watermarking makes up for the defects of cryptography. It also makes up for the lack of digital signatures. They fought off many attacks together. Therefore, this is widely used in the field of digital copyright protection [6].

2. Research Status of Anti-Theft Technology for Existing Network Pictures

A number of research institutions and enterprises represented by the United States have supported or carried out related digital watermarking research. They have applied for a number of patents on digital watermarking. In terms of the actual network application, the technical means for the design of image copyright protection mainly include the preprocessing of the image itself before the online public release of the image, that is, the image itself processing protection [7] [8]. Or, when users browse pictures to take some preventive measures can also effectively prevent stolen pictures, that is, picture browsing interference protection.

Image preprocessing includes striking image watermarking and digital image watermarking. Striking image watermarking is the most commonly used method of image copyright protection, which declares the copyright information of the picture by superimposing the eye-catching watermark of the trademark or website on the picture [9]. There are currently two commercial software programs for watermarking, aspjpeg and wsImage. And most users still use Photoshop to process the pictures. Digital watermarking has the advantages of high concealment, easy resistance to tamper, copy, compression, conversion, filtering, repeated addition and other attacks. At present, it has been applied to digital information copyright protection, printed matter anti-counterfeiting, information source traceability and other fields [10]. However, for network images, digital image watermarking is more suitable to prove the copyright of the image. In re-

cent years, some Chinese experts have proposed a Flash embedded image browser. It can effectively resist screenshot, a kind of universal and dangerous stealing method. This was applied to the visual network platform of the industry scientific research special "Research on the prevention and control of invasive alien Species Occidentalis thrips". However, the technology requires user interaction to see the original image, which is not convenient enough.

In general, there have been a lot of studies on copyright protection of pictures, especially in the digital watermarking theory and application has a lot of fruitful achievements. However, in the case of web images, "tracking copyright" may be secondary (digital image watermarking is better for proving copyright). "Preventing users from directly and easily obtaining pictures" is the key problem that image copyright protection should first solve.

3. Design of New Image Anti-Theft Technology

Screenshot capture is the most common method used by clients to obtain images. The picture shows to the user at the same time has created conditions for the user screenshots. At present, the most common protection method for this kind of situation is to cover the eye-catching copyright watermark on the key position of the picture. However, it will affect the full effect of the picture. This has been mentioned above. Therefore, this paper proposes a kind of image theft technology. This does not allow the "original information" of the image to be displayed in the Web browser, nor does it prevent the user from seeing the original image clearly.

The human eye has the property of visual persistence. When a person is looking at an object, the scene disappears from the person's eyes and does not immediately disappear on the retina. She is to keep it for about 1/24 of a second [11] [12]. This provides convenience for our design. It can design an image like a GIF composite frame. At any given moment, what is actually displayed is not the complete picture. But because of the transient nature of vision, the human eye sees the complete picture. Obviously, this particular image format consists of several frames and supports automatic looping. The point of the design is that it would be very difficult for the user to piece together the original image from the screenshot frame by frame. That means it's almost impossible to get a complete picture [13].

The first step is to determine the number of frames for the animation. To achieve the above animation effect, the image needs to be divided into frames. Obviously, the more frames, the better (it's harder to recover from a screenshot). But the price comes with the possibility that the resultant image will flicker. The second step is to determine the block strategy of each frame. According to our hypothesis, at any given moment (equivalent to any frame), there is always a part of the image block that is hidden or blurred. This step needs to determine the segmentation problem of each frame picture. The third step is to determine the operation relationship between each frame. Operation relations can be roughly divided into three types: add, subtract and eliminate. For convenience,

this article uses the elimination type. The fourth step, determine the processing area of each frame block. For the image blocks obtained in the second step, it is necessary to determine which blocks are processed. This makes it easier to get a complete picture at any time (any frame).

4. Experiment Implementation and Improvement

To sum up, on the one hand, the method of adding eye-catching watermarks is limited by such factors as LOGO size, adding position and number of watermarks. On the other hand, digital watermarking does not prevent screenshot. Therefore, the following exploratory experiments are carried out.

- Software support: Ulead GIF Animator, screenshot plug-in
- Experimental principle: visual retention characteristics
- Experiment environment: Microsoft Internet Explorer

- **Experiment 1**

Occlusion effects can be achieved in different ways. Will the white and transparent Settings of the flashing area have a different effect on the final GIF?

Objective: To compare the experimental effect of white area and transparent area.

Experimental process: The original image of the experiment was a JPG file of 400 × 431 (Figure 1). Cross it into four sections like the one on the right. "3/4 of the original picture and 1/4 of the white picture" (Figure 2) and "3/4 of the original picture and 1/4 of the transparent picture" (Figure 3) were used for synchronization experiment.

Turn the four images into GIFs. All set to 50 frames per second. View the final image of a GIF on a web page in IE. Use the screenshot plug-in to verify whether the original image can be successfully captured.

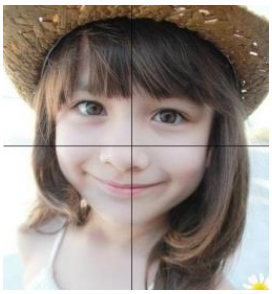

Figure 1. Original image of the experiment.

Figure 2. Original 1/4 white 3/4.

Figure 3. 3/4 Original picture 1/4 transparent.

Experimental results: The above two groups could not successfully intercept the full image, which could meet the condition of visual detachment. However, the difference between transparent and white areas did not affect the viewing effect of the GIF image.

Experimental conclusion: Transparent area occlusion effect and white area occlusion effect is the same in the browser. In other words, transparency does not replace white to reduce the degree of flickering.

- **Experiment 2**

Objective: To compare the effect of white area size on vision.

Experimental process: The original image of the experiment was a JPG file of 400 × 431 (**Figure 1**). Cross it into four sections like the one on the right. "3/4 of the original picture and 1/4 of the white picture" (**Figure 4**) and "1/4 of the original picture and 3/4 of the white picture" (**Figure 5**) were used for synchronous experiments.

GIFs and GIFs were created at 50 frames per second. View the final image of a GIF on a web page in IE. Use the screenshot plug-in to verify whether the original image can be successfully captured.

Experimental results: Comparatively speaking, the effect of "3/4 original picture 3/4 white" is better than that of "1/4 original picture 3/4 white". The reason is that "3/4 original picture and 1/4 white" retains more information about the original picture. The flicker "lost" only a small part.

Conclusion: The more information the original image is retained, the lighter the scintillation effect is. However, when increasing the information of the original picture, pay attention to the white part so that the user can not intercept the complete picture information.

- **Experiment 3**

Objective: To compare the experimental effect of fuzzy area and white area.

Experiment process: The white area of "1/4 white 3/4 original picture" (**Figure 2**) in Experiment 1 was replaced with blur effect (**Figure 6**). Make it into a GIF at 50 frames per second.

Experimental result: the GIF image produced is 282 KB. The screenshot capture tool cannot obtain a complete and clear picture. The image still flickers, but much less so.

Conclusion: Fuzzy effect can provide more information. Since the viewer wants details from the image (especially if the image is used commercially), the image with blurred areas in the screenshot is not enough. Therefore, fuzzy area can also achieve the purpose of preventing screenshots.

Figure 4. Original picture 1/4 white.

Figure 5. 1/4 Original picture 3/4 white.

Figure 6. Blur effect.

- **Experiment 4**

According to experiment 3, fuzzy effect should be selected first. But simply breaking it into four parts could reveal key information about the picture. Therefore, at this stage, the original picture is further divided into 16 parts as follows (Figure 7).

Objective: To compare the experimental effects of 4 plots and 16 plots.

Experimental process: In order to maintain the same amount of information, four 1/16 small blocks need to be blurred here. I'm going to take two diagonals here. The area selected by the dotted line is the fuzzy area (Figure 8). Make it into a GIF at 50 frames per second.

Experimental result: GIF image size is 176KB. Unable to capture a complete and clear full picture. At the same time, the flicker is lighter.

Conclusion: Increasing the number of blocks makes it less likely to "expose" key details during flickering. All things being equal, the more blocks there are, the less exposure there is.

- **Experiment 5**

With the increase of the number of blocks, the number of selected combinations of fuzzy regions increases exponentially. It also presents the choice decision problem of fuzzy region.

Figure 7. 16 subgraph.

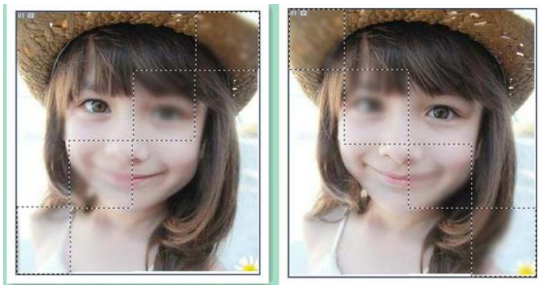

Figure 8. Diagonal blur.

Objective: To change the fuzzy selection strategy and observe the experimental effect

Experimental process: The area selected by the dotted line in the figure below (**Figure 9**) was blurred to make a GIF image of 50 frames per second.

Experimental results: THE GIF image is 288 KB, can not intercept the complete clear picture, flicker slightly.

Conclusion: The facial features of the girl in the original picture were taken as the key information to be obtained. The second message is below the neck. The hat and background are the third information. Therefore, compared with the selection strategy in Experiment 4, this experiment can basically blur the whole graph (except vertices) after one cycle. Always keep key information only half "exposed" at the same time. In experiment 4, the diagonal strategy always exposed most of the secondary information.

- **Experiment 6**

According to experiment 5, different fuzzy regions can achieve different information expression effects. So is the more complex the strategy, the better the corresponding expression effect?

Objective: To observe the effect of the experiment by increasing the complexity of the strategy.

Experimental process: The area selected by the dotted line in the figure below (**Figure 10**) was selected for blurring. Make a GIF at 50 frames per second.

Experimental result: GIF image size is 408 KB. It protects against screenshots. The flicker of the picture is slight.

Conclusion: Scintillation sensation decreased slightly after increasing complexity. But giFs have grown in size. In the picture information expression, it can guarantee the information performance more evenly.

Figure 9. Cross blur.

Figure 10. Rotation blur.

- **Experiment 7**

At this point in the experiment, the choice of strategy presents a problem. If you choose some of the simple loop strategies above, as long as the screener is willing to take more screenshots. They pieced together multiple screenshots to get a complete screenshot. How can this be solved?

Objective: Fuzzy areas were randomly selected (Figure 11) to observe the experimental effect.

Figure 11. Random blur.

Experiment process: make a GIF image at 50 frames per second by randomly selecting the blurred area.

Experimental results: GIF image is 156 KB can resist screenshots, flicker slightly

Conclusion: The random algorithm in this experiment is simulated by selecting irregular rectangular regions with variable number. It takes a lot of effort and time for a screener to get a complete and clear image. At the same time, if the mathematical algorithm is used for random simulation, GIF image size fluctuations are large. This has the potential to "expose" too much critical information at one point.

5. Conclusion and Discussion

Through the combination of increasing the number of blocks, blur processing and random selection of areas, GIF images that can resist the effect of screenshots have been preliminarily obtained, but there is still room for improvement in the following aspects. First, frame setting. If you increase the number of frames per second to 50, the flicker of an image on a picture viewing software can be significantly reduced. But browser plugins don't always support high-frame GIFs. There isn't much difference in the actual performance before and after increasing the number of frames. Secondly, it deals with regional selection strategy. Fuzzy areas are best protected against screenshots by selecting random areas. However, there are several problems such as how to choose the best among many random algorithms, how to determine the key information in the picture, whether different customers will have different information needs and so on. Third, the size of the picture. The larger the number of frames, the larger the number of blocks, and the larger the GIF image size. The result is a longer load time in the browser. Fourth, the user accepts the question. Even if the fuzzy area processing can always feel the flicker, and the user can accept and can accept the degree of flicker. This requires a user survey to be finalized. These problems will be the direction and focus of our work in the next step.

Funding

Supported by the State Key Program of National Social Science of China (Grant No. 16AZD055) and the National Training Programs of Innovation and Entre-

preneurship for Undergraduates (Grant No. 1210559135).

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Qin, Y. (2012) The Application of Computer Application Technology in the Field of Digital Media Copyright Protection. *Silicon*, **21**, 2.

[2] Zhang, X.B. (2011) An Anti-Theft Protection Method for Network Pictures Based on Process Control. *Computer Applications and Software*, No. 7, 294-295.

[3] Hsu, C.T. and Wu, J.L. (1999) Hidden Digital Watermark in Images. *IEEE Transactions on Image Processing*, **8**, 58-68. https://doi.org/10.1109/83.736686

[4] Fan, K.F. (2011) Research on Key Technology and Evaluation Method of Digital Media Content Protection System. Master's Thesis, Xi'an Electronic Technology University, Xi'an, 15-22.

[5] Fridrich, J., Goljan, M. and Memon, N.D. (2000) Further Attacks on Yeung-Mintzer Fragile Watermarking Scheme. *Proceedings of SPIE—The International Society for Optical Engineering*, Vol. 3971, San Jose. https://doi.org/10.1117/12.384997

[6] Sun, J.G., Liang, K. and Xia, S.Z. (2013) Research of Lossless Digital Watermarking Technology. *Applied Mechanics & Materials*, **333-335**, 1219-1223. https://doi.org/10.4028/www.scientific.net/AMM.333-335.1219

[7] Wong, P.W. (1998) A Public Key Watermarking for Image Verification and Authentication. *Proc.ieee Int.conf.image Processing*, **1**, 455-459.

[8] Cox, I.J., Kilian, J., Leighton, T. and Shamoon, T. (1996) A Secure, Robust Watermark for Multimedia. In: Anderson, R., Ed., Information Hiding. IH 1996. *Lecture Notes in Computer Science*, Vol. 1174, Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-61996-8_41

[9] Then, H. (2007) Support Vector Machine and Hyperplanes in Digital Watermark Detection. *TENCON* 2007—2007 *IEEE Region* 10 *Conference IEEE*, Taipei, 30 October-2 November 2007.

[10] Saxena, V. and Gupta, J.P. (2007) Towards Increasing the Robustness of Image Watermarking Scheme against Histogram Equalization Attack. 2007 *IEEE* 15*th Signal Processing and Communications Applications*, Eskisehir, 11-13 June 2007. https://doi.org/10.1109/SIU.2007.4298813

[11] Hua, D., Zhang, J. and Chai, X. (2014) The Design and Implementation of Flash Animation Watermarking. *IEEE Workshop on Electronics IEEE*, Ottawa, 8 May 2014, 489-491.

[12] Deng, H., Jin, S.I. and Wang, G. (2011) Design Method of Digital Watermark Based on Flash Animation. *Computer Programming Skills & Maintenance*, **14**, 99-100.

[13] Sakib, S., Milenkovic, A. and Ray, B. (2020) Flash Watermark: An Anticounterfeiting Technique for NAND Flash Memories. *IEEE Transactions on Electron Devices*, **67**, 4172-4177. https://doi.org/10.1109/TED.2020.3015451