2010 3rd International Conference on Computer and Electrical Engineering (ICCEE 2010)
IPCSIT vol. 53 (2012) © (2012) IACSIT Press, Singapore
DOI: 10.7763/IPCSIT.2012.V53.No.2.93

An Improved Mosaic Graphic Algorithm for Human-Computer Identification

GAO Cai-yun[1+], CAO Tian-jie[1] and ZHU Ai-chun[2]

[1]Department of Computer Science, China University of Mining and Technology

Xuzhou, China

[2]Department of Information and Electrical Engineering, China University of Mining and Technology

Xuzhou, China

Abstract—Most of the existing verification code is text-based, but this kind of verification code is not so safe with the development of robot technology. Therefore, an improved human-computer identification algorithm that is based on the mosaic-image is presented. It shows that some small meaningful images are placed on a big background one that is formed by a number of meaningless images which are made by meaningful ones color, and the meaningful ones should be identified. Because the robots have limitation in the identification and separation of images, human users can easily identify these pictures, but robots can not do it. Thus it can distinguish between humans and robots. It can be used against Denial of Service, password guessing and a large number of downloads and so on.

Keywords-component; formatting; style; styling; insert

1. Introduction

With the continuous development of network technology, web services become widespread and more and more network activity need for human-computer interaction to complete. The robot can imitate human being to accomplish various network activities which are only allowed by humans, and they are faster than Human being. They can continuous access Web resources, which will results in denial of service attacks. Therefore an effective method is needed to implement the friendly interaction between human being and computers, and robot can not imitate. Currently, the most famous technology on distinguishing human and robot is Completely Automated Public Turing Test to Tell Computers and Human Apart [1]. Turing is the first scholar of studying machine intelligence [2]. He determines machine intelligence through a test which is named Turing Test. CAPTCHA can be simply divided into three categories [3-5]: text-based validation code, images-based verification code and voice-based verification code. CAPTCHA can be used widely such as preventing violent attacks, preventing mass spam, preventing web spiders and so on.

2. Basso and Sicco' s Human-Computer Identification Algorithm

Currently, the most effective method which can distinguish human being and robots is the CAPTCHAs, and most CAPTCHAs are text-based. However, as the progress of computer vision and pattern recognition, this kind of text-based HIPs are not as effective as before, and it is more vulnerable for some specific attacks. Recently, some new technology can breach several of the most common CAPTCHAs in the Internet in a very high efficiency. So, with the development of computer vision technology, computers become more and more

[+] Corresponding author.
E-mail address: gcy5388581@163.com

fast, and attacks are more and more sophisticated. So this kind of text-based HIPs will soon be completely invalid, and the new technology must be generated.

At present, the computer can not do many tasks that relate with vision, but these tasks are easier for humans such as understanding the world or apperceiving an image. So we can design a new method to distinguish between humans and robots through this side.

2.1. Algorithm Description

Basso and Sicco proposed a human-computer identification algorithm in 2008, which is named MosaHIP (Mosaic-based Human Interactive Proof) [6]. It uses some of the difficulties on the implementation of existing computer:

(1) Image segmentation in the interest area with a complex context;

(2) Identification of specific concepts under the chaos background;

(3) Image match with specific transformation applied to an image.

Basic idea of MosaHIP is to mosaics images. It uses many small and overlapping images to make up a large image. These small images are divided into two categories: one is the real and meaningful images; the other is meaningless images. In both images, there is only a small part of the first image, and others belong to the second category. The meaningful images are needed to be identified by users. They are pseudo-randomly placed in patchwork images and they overlap each other. Therefore, it is not easy for the computer to identify them. The rest of the images are generated by the random color of color histogram form the meaningful images. The effects which are randomly generated by graphics or lines are added to these images. They are used to generate the chaotic background in order to enable robot difficult to identify the meaningful images.

MosaHIP is divided into two types: the first is as shown in Fig. 1 which displays the “concept-based” MosaHIP test; the second is as shown in Fig. 2 which is the “topmost” MosaHIP test.

Algorithm describes as follows: N meaningful images are selected from the database of pictures. They are zoomed, rotated and done a certain transparency. Then the images are placed on a large image, and the next image overlap 1/4 part with the foregoing one. According to certain rules, the color gradient of the new image is calculated. In accordance with the color gradient, meaningless images are made up by drawing a variety of graphics and lines. The meaningless images are similar with the meaningful ones in size. Then the meaningless ones are placed on another big image one by one until the big one is covered fully. They are also overlap. The last is to make the first large image coincide with the second one.

2.2. Algorithm Analysis

Algorithm proposed by Basso and Sicco although can distinguish between, computers and humans in a certain extent, there are still some drawbacks in it: First, there is an error in the description of the algorithm. In the fourth step, the algorithm is “Determine the positioning location within the area of I_{j-1}, then divide I_{j-1} into 4 quadrants of equal size and place I_j within the borders of a randomly chosen quadrant, overlapping only that one”. In this step, there is 25 percent that the I_{j-1} is completely covered.

In addition, there are some security flaws in the algorithm: 1) whether "concept-based" MosaHIP and “topmost” MosaHIP, there is always a meaningful image which is not being covered. Through some methods, such as segmentation through edge detection [7, 8], segmentation through threshold [9] and so on, there will be a shadow of regular graphic in the processed image. For "concept-based" MosaHIP, the robots, through the shadows, can find the general location of meaningful images to narrow the search. For the "topmost" MosaHIP, the shadow is the needed meaning image. So the robots can recognize this image into the system to execute various attacks. 2) When a new meaningful image is placed, it will overlap 1/4 part of the previous image. Regardless of the order of meaningful images and the position relative, there is regular in the position of the meaningful images opposite to the placement of meaningless images, which makes easier to identify the meaningful image by robots.

Fig. 1: “concept-based” MosaHIP

Fig. 2: “topmost” MosaHIP

3. An Improved Mosaic Graphic Algorithm for Human-Computer Identification

According to the inadequacies of the previous algorithms, an improved algorithm is proposed:

3.1. The Tmproved Human-Computer Algorithm

Here is improved algorithm according to one proposed by Basso and Sicco:

(Step 1)

- Select n images from the database of pictures P and add them to the set of real pictures R = $\{I_1, \ldots, I_n\}$.

- IF the test is concept-based, randomly choose a reference image $I_r \in R$ and retrieve its category G_r;

ELSE, $I_r = I_n$.

(Step 2) For each image $I_j \in R$:

- Randomly choose a scaling factor S_j, with $S_{MIN} \leqslant S_j \leqslant S_{MAX}$, and apply a scaling function to Ij reducing it by S_j.

- Determine whether it has to be rotated and randomly choose the rotation angle $\odot_j$, with $\odot_{MIN} \leqslant \odot_j \leqslant \odot_{MAX}$. Then rotate I_j by $\odot_j$.

- Determine the percentage of transparency to apply to I_j, by randomly selecting a transparency factor T_j, with $0 \leqslant T_j \leqslant T_{MAX}$. Then, apply the transparency function to I_j, if T_j != 0.

(Step 3)

- Create the composite image c of size m by n with transparent background.

- Randomly select a starting location on the image c and position $I_1 \in R$ on c. Make sure that I_1 does not exceed the boundary of c.

- IF $I_1 = I_r$, save the top-left and bottom-right coordinates of I_1 in set D.

(Step 4) For each image $I_j \in R$, with $2 \leqslant j \leqslant n$:

- Determine the positioning location within the area of I_{j-1}, so that I_j only partially overlaps I_{j-1}. For this purpose, divide the I_{j-1} image into 4 quadrants of equal size and randomly select a quadrant, according to the direction of the quadrant, select a new region which is smaller than the previous one. The size of this new region area is greater than or equal 70 percent of the previous one. Then place I_j within the borders of this new region, overlapping I_{j-1} and ensure that it does not cover I_{j-2};

- IF the test is concept-based, I_j must not overlap any previously placed picture I_k, with $1 \leqslant k \leqslant j$.

- IF $I_j = I_r$, save the top-left and bottom-right coordinates of I_j in set D.

(Step 5)

- Compute the color histogram of image c, hist(c).

- Create the background image b of size m by n.

- Fill b with a color gradient between colors randomly chosen in sets RGB_h and RGB_l, where RGB_h contains the k most frequent colors in hist(c) and RGB_l the leftovers.

(Step 6)

- Create a fake image f similar in size to real images and fill its background with a color gradient between randomly chosen colors from RGB_h and RGB_l.

- Draw on f various shapes and lines of colors chosen from RGB_h.

- Randomly change the pixel color of some areas of f using colors from RGB_l.

- IF the test is concept-based, divide the I_1 image into 4 quadrants of equal size and randomly select a quadrant, according to the direction of the quadrant, select a new region which is smaller than the previous one. The size of this new region area is greater than or equal 70 percent of the previous one. Then place f within the borders of this new region, overlapping I_1 and ensure that it does not cover I_1;

- IF the test is topmot, divide the image into 4 quadrants of equal size and randomly select a quadrant, according to the direction of the quadrant, select a new region which is smaller than the previous one. The size of this new region area is greater than or equal 70 percent of the previous one. Then place f within the borders of this new region, overlapping I_n and ensure that it does not cover I_n;

(Step 7)

- Add f to the background image b, starting from the top-left corner.

- Repeat (Step 7) until b is completely covered with fake images.

(Step 8) Reduce the number of colors of image b by applying the Floyd-Steinberg dithering algorithm.

(Step 9) Overlap the composite image c to the background image b. Since c has a transparent background, now b contains both real and fake images.

(Step 10) Apply a distortion function (with pseudo-randomly chosen input parameters) on the image b.

(Step 11)

- Return the image b and the coordinates set D.

- IF the test is concept-based, also return the category Gr.

The improved MosaHIP images are as shown in Fig.3 and Fig.4.

The algorithm is improved in step (4) and (6). For step (4), this improved algorithm makes each meaningful image cover a random area of the previous image, but it does not interfere with the recognition of human. In (6), for the meaningful image which does not covered, the improved algorithm uses a meaningless image to overlap with the meaningful one to enhance the security of the algorithm.

Fig. 3: "concept-based" MosaHIP

Fig. 4: "topmost" MosaHI

3.2. The Tmproved Algorithm Analysis

In computer vision and image retrieval area, the mosaic images can effectively resist attacks such as content extraction and identification, which threaten the algorithm. In the proposed method, a specific content is accessed only when the visual challenge is passed. This is possible only understanding the concept

expressed by a generic image. However, even using the latest technology in the field of robot vision, modern computers can not understand the context of the generic images. In general, pattern recognition in the complex context or identification some concept in a large range and segmenting an image to extract its internal components is a great challenge to the computer program.

Defects in the algorithm proposed by Basso and Sicco have been improved in the given algorithm. For the first defect, in accordance with the laws of meaningful images, it places a meaningless image on the meaningful one which is not covered to make the meaningful image partially covered. For the second defect, when the meaningful images are placed, the size of covered region is not only 1/4, but also it is a random number which is greater than or equal 70 percent and less than 100 percent of the previous image which is one of the divided 4 quadrant. The improved algorithm not only makes human recognize the image easier, but also the laws of the meaningful images which are need to be recognized is similar with the meaningless ones. To the attackers, they can not recognize meaningful image which is needed through the method such as segmentation through edge detection [7, 8], segmentation through threshold [9] and so on.

1) Resistance to segmentation through edge detection

Image segmentation in a particular area is required in order to distinguish the meaningful images form the false ones. A method which can achieve this task is edge detection algorithm, which may delineate the outline of the sub-images of mosaic images. The purpose of separation profile is to quickly reduce the number of image data and simplify the subsequent steps.

The application of an edge detection algorithm can reduce the amount of information present in the MosaHIP image and extract relevant features of each sub-image. But in the algorithm, the number of connected components within the resulting image is still very high and the connected components between meaningful images and meaningless ones are similar, which does not allow to easily detecting the shapes.

2) Resistance to shape matching

Because of overlapping, it is difficult to isolate the meaningful images from the sub-images in MosaHIP. In addition, rotation, scaling and transparency functions are taken to the images, which results an increased difficulty in performing shape matching.

Further measure to reduce the automatic identification is through Floyd-Steinberg dithering algorithm to reduce the color. This step ensures that the task of automatically determining image borders remains challenging, and human recognition abilities still allow a correct identification of single sub-image.

3) Resistance to segmentation through threshold

"Threshold" provides a simple and convenient method to separate different areas of the image. The segmentation process is due to the different intensities of colors between the foreground and background regions of an image. The method compares an intensity of color with the intensity of each pixel. If the pixel intensity is above the threshold, this pixel is set to white. If it is low, the pixel is set to black.

By using the "threshold" method, the mosaic image is not easy to be divided. It selects colors from the image histogram. In fact, it is impossible by comparing the pixel intensity with a specific threshold to distinguish between meaningful and meaningless images, because, the color of meaningful image is common image and there are meaningless image content in the mosaic.

4) Resistance to random guessing

A simple attack for algorithm involves randomly guessing the position of the meaningful image. It can be called "blind attack". Given the area of mosaic image is $m \times n$, and the area that blind attack attempts to locate is $x \times y$, with $x<m$ and $y<n$. Supposed each pixel in the mosaic image have the same chance of being selected to position the reference image. So the chance can be computed:

$$P = A / S = (x \times y) / (m \times n) \quad (1)$$

where A is the area of the reference image and S is the area of the mosaic image.

If the area of meaningful image is between 65 and 70 pixels and P is 4.1%, then the area of mosaic image is close to 110,000 pixels which are about 400×275 pixels. Given the area of mosaic image is 400×400 pixels, then P is only 2.8%.

Although 2.8% is quite low, if time is sufficient, robots still can fully download the protected resources. So it can temporarily lock IP address of possible attacker to solve this problem. The time of lock can increase in the form of index based on the number of accessing failures until it reaches a maximum.

4. Application of Improved Algorithm

MosaHIP image can be used as graphics verification code. It can be used in any applications which need human-computer recognition, such as registration, login, recovering password, downloading resource and so on.

1) User registration

Registration of most web sites only needs to input the registration. These sites could easily be attacked by doing a large number of registrations. A large number of registrations can be used to send ads or to send illegal messages. It also can easily cause a denial of service attack. Using this algorithm, users must do human-computer recognition to recognize the meaningful image before registering. If users are right, they are allowed to register information. Else they are wrong, they can not do anything.

2) User login

General system's login page just need enter user name and password. So it is very easy for robots to carry out password guessing. Once the hacker has known the system password, they can imitate the legit users to do something that may do harm to the legit users. Using this algorithm, users must do human-computer recognition to recognize the meaningful image before logging. If users are right, they are allowed to enter into sites. Else they are wrong, they can do nothing.

3) Recovering password

You forgot your password. When you need to find it, you just need to fill the "problem for prompting password" and "Question Answers". They are both set in registering. Robots can guess the "problem for prompting password" and "Question Answers" to gain the password. So they can easily enter the system to carry out acts of sabotaging system security, such as malicious download, sending malicious information and so on. In order to prevent robots guessing, users can use this algorithm. Before filling the needed information, users need to do human-computer recognition to recognize the meaningful image. If users are correct, they can find their passwords, else they can not.

4) Downloading resource

The websites for downloading resource we usually visit can be divided into two categories: 1) Only when the users successfully log in, they can download the resource; 2) It does not need to login that the users can download resource directly. This algorithm is applied to these two ways. 1) Before logging on, users need to do human-computer recognition. If they are successful, they are the right users to download the resource, else they can not; 2) In order to prevent a large number of downloading by robots, users need to take human-computer recognition before downloading. If they are correct, they can directly download resource, else they can do nothing. Using the algorithm, system can prevent from large number of downloading.

5. Conclusion

This paper first describes the human-computer algorithm proposed by Basso and Sicco. According to the inadequacies of the algorithm, an improved mosaic-based human-computer recognition algorithm is proposed. The algorithm makes the whole image without the laws. So the robots can not recognize the correct meaningful image, so that the robot can not carry out sabotage activities.

6. Acknowledgment

This research is supported by the Jiangsu Provincial Natural Science Foundation of China (No.BK2007035).

7. References

[1] M. Blum, L. von Ahn, J. Langford, The CAPACHA Project, “Completely Automatic Public Turing Test to tell Computer and Humans Apart”[J], www.captcha.net, Dept. of Carnegie-Mellon University, November, 2000.

[2] A. Turing. Computing Machinery and Intelligence Mind[J], 1950, 59(236): 433-460.

[3] C. Pope, K. Kaur. Is It Human or Computer? Defending E-Commerce with CAPTCHAS Mind[C], 2005, 7(2): 43-49.

[4] S. Shirali-Shahreza, A. Movaghar. A New Anti-Spam Protocol Using CAPTCHA[J]. In: IEEE International Conference on Networking, Sensing and Control Piscataway[C], NJ, United States: Institude of Electrical and Electronics Engineers Computer Society, 2007. 234-238.

[5] I. Fisher, T. Herfet. Visual CAPTCHA for Document Authenntication[J]. In: IEEE 8th Workshop on Multimedia Signal Processing Piscataway[C], NJ, United States: Institute of Electrical and Electronics Engineers Computer Society, 2006. 471-474.

[6] Alessandro Basso, Stefano Sicco, Preventing massive automated access to Web resources[J], 2008.

[7] J. Canny, A computational approach to edge detection[J], IEEE Trans. Pattern Anal. Mach. Intell. 8(6) (1986) 679-698.

[8] R. Gonzalez, R. Woods, Digital Image Processing[J], 1992, pp. 679-698.

[9] R. Fisher, S. Perkins, A. Walker, E. Wolfart, Hypermedia Iamge Processing Reference[J], 2004.