

Poster: Similarity Assessment Metrics of Hybrid Images for Graphical Password

Madoka Hasegawa Keita Takahashi Shigeo Kato

Graduate School of Engineering, Utsunomiya University

7-1-2 Yoto, Utsunomiya, Tochigi 321-8585, Japan

{madoka@, takahashi @mclaren., kato@ } is.utsunomiya-u.ac.jp

1. INTRODUCTION

In recent years, several graphical password methods have been proposed in which a set of images is employed in place of a password string as the user's key [1]. In terms of memorability, graphical passwords are superior to conventional authentication using random string passwords; however, because the images occupy a large amount of space on the screen, they remain weak against shoulder surfing. To mitigate this risk, unclear images generated by alpha blending, filtering, or hybrid imaging of original images can be used instead.

We focused on the hybrid image method [2] proposed by Oliva et al. as a means of generating unclear images. A hybrid image consists of two images, one of which contains the edge information from a foreground image while the other contains the coarse features of a background image. The visibility of a hybrid image varies depending on the viewing distance, and we proposed to use this property to develop a graphical password system based on the contour of the key image [3]; a legitimate user who is close to the screen will be able to see this, while a shoulder-surfer will not. In this method, the similarity between the key (foreground) image and the background image is important, as the key image may be noticeable to an attacker if the background image is too flat; thus, a method for evaluating image similarity is desired in order to check the suitability of overlaying a background image with a given key image. Although we previously [4] proposed a structural similarity measure based on the speeded-up robust features (SURF) [5], comparisons of subjective impressions to our similarity measure remained ambiguous.

In this paper, we analyze the relationship between subjective impressions and our image similarity assessment method in order to avoid using inappropriate background images in generating a hybrid image for a graphical password. Experimental results show that our similarity measure coincides closely with the subjective visibility of the key image within a hybrid image.

2. GRAPHICAL PASSWORD USING HYBRID IMAGES

Hybrid images combine components with low spatial frequencies within one image with those of high spatial frequencies within another. Figure 1 shows an example that combines a background image of birds with a user's key image of flowers. Interpretation of this image changes depending on the viewing distance, a property that we can utilize for user authentication. In our authentication system, several hybrid images are displayed on the screen. One of the hybrid images consists of the user's key image, i.e., flowers, and a dummy background image, i.e., birds. Other hybrid images are

combinations of two dummy images. A legitimate user should be able to point out the image containing their key and can be authenticated by having the system repeat this challenge and response several times.

In general, a shoulder surfer who stands behind the user cannot recognize the key image within a hybrid image. However, if the background image is too flat, a part of the key image may be noticeable; for example, the flower in the left half of Figure 1 is visible to a certain viewing distance. Therefore, it is important for the graphical password application to evaluate the structural similarity of two images in order to avoid using inappropriate background images.

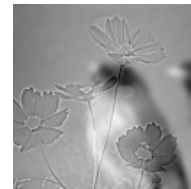


Figure 1 An Example of a Hybrid Image.

3. SIMILARITY ASSESSMENT METHOD

We utilize SURF to detect points of interest and to determine the locations of objects in two images. Based on this, we can define the images' similarity as the overlap in area between objects in the background and foreground images. Figure 2 shows an example of the similarity evaluation process, which consists of the following steps:

Step 1: Apply a high-pass and a low-pass filter to the foreground (I_H) and background (I_L) images, respectively, to obtain the filtered images I'_H and I'_L . The input images and their filtering results are shown in Figures 2 (a)–(d).

Step 2: Detect points of interest from each filtered image using SURF. Figures 2 (e) and (f) show the results of this process, in which the center of each circle corresponds to a point of interest. Here, the radius of each circle is the size of the filter kernel.

Step 3: Generate binary feature maps FM_H and FM_L as shown in Figures 2 (g) and (h). In this process, pixels inside each circle within the SURF output are filled with 1 (white) while the remaining pixels are filled with 0 (black); the resulting white region indicates the location of significant objects in the original image.

Step 4: Obtain a difference image as shown in Figure 2 (i). We define the difference between feature maps as

$$d(x, y) = \begin{cases} 1 & \text{for } FM_H(x, y) = 1 \text{ and } FM_L(x, y) = 0 \\ 0 & \text{others} \end{cases} \quad (1)$$

where (x, y) is the position of a given pixel. This difference measures the area in the foreground that is not covered by

objects in the background, and using this difference measure we can define the similarity S as the ratio of the uncovered area to the total area using

$$S = 1 - \frac{1}{XY} \sum_{y=0}^{Y-1} \sum_{x=0}^{X-1} d(x, y) \quad (2)$$

where X and Y are the width and height of the image, respectively. The value of S will be in the range 0 to 1, and it indicates how appropriate the background image is as a mask to the foreground image.

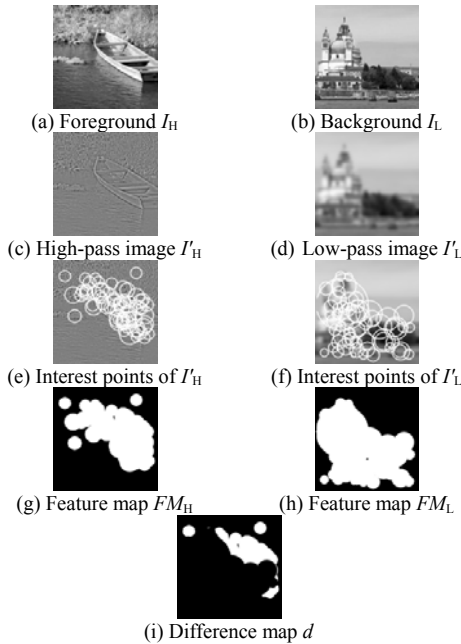


Figure 2 Similarity Evaluation Process.

4. EXPERIMENTAL RESULTS

For several hybrid images, we compared the relationship between the subjective impressions and our image similarity scores. We also measured the structural similarity (SSIM) index [6], which is understood to be an objective similarity score for two images. Figure 3 shows the hybrid images used in this evaluation, each of which contains the same close-up image of armor as the foreground image.

A subjective evaluation was conducted using Scheffe's pairwise comparison method (Ura's variation). Thirty pairs of images

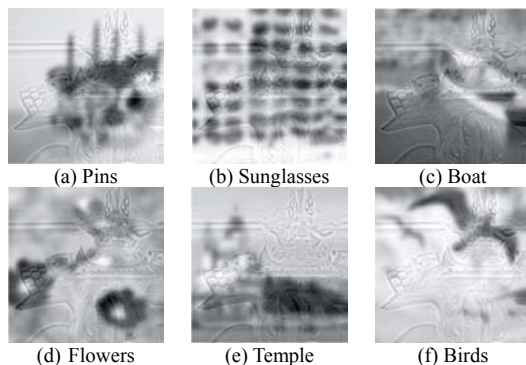


Figure 3 Hybrid Images Used for Evaluation.

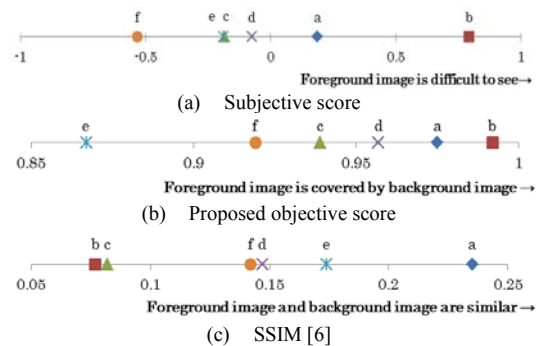


Figure 4 Comparison of Similarity Scores.

were displayed on a monitor one by one and twenty participants were asked to name which image in each pair was more difficult to see the foreground. Figure 4 shows the yardstick diagram for each similarity score, where the letters (a, b, ..., f) correspond to the image index from Figure 3. We can see from Figure 4 that the proposed score mostly coincides with the subjective impression; i.e., images (c), (e), and (f) can be detected as inappropriate images for use in a graphical password that uses hybrid images. By contrast, the SSIM index was not suitable for this purpose.

5. CONCLUSIONS

In this study, we evaluated similarity metrics for automatically choosing hybrid images suitable for use as graphical passwords. Using the SURF features of an image, we defined a measure of similarity between a foreground and background image as the ratio of the area of uncovered objects in the foreground image when overlapped by the background image. We were able to experimentally confirm that our similarity measure coincides with the subjective visibility of a key image in a hybrid image.

6. ACKNOWLEDGMENTS

This work was supported in part by the JSPS Grant-in-Aid for Scientific Research (KAKENHI) No. 25330226.

7. REFERENCES

- [1] X. Suo, Y. Zhu, G. S. Owen, "Graphical Passwords: A Survey," ACSAC '05, pp.463-472, Dec. 2005.
- [2] A. Oliva, A. Torralba, P. G. Schyns, "Hybrid Images," ACM Trans. on Graphics, Vol.25, No.3, pp.527-532, July 2006.
- [3] T. Miyachi, K. Takahashi, M. Hasegawa, Y. Tanaka, S. Kato, "A Study on Memorability and Shoulder-Surfing Robustness of Graphical Password Using DWT-Based Image Blending," PCS2010, pp.134-137, Dec. 2010.
- [4] K. Takahashi, M. Hasegawa, Y. Tanaka, S. Kato, "A Structural Similarity Assessment for Generating Hybrid Images," 45th Asilomar Conference on Signals, Systems, and Computers, pp.240-243, MA8b4-4, Nov. 2011.
- [5] H. Bay, A. Ess, T. Tuytelaars, L. V. Gool, "SURF: Speeded Up Robust Features," Computer Vision and Image Understanding, Vol.110, No.3, pp.346-359, 2008.
- [6] Z. Wang, A. C. Bovik, H. R. Sheikh, E. P. Simoncelli, "Image Quality Assessment: From Error Visibility to Structural Similarity," IEEE Trans. on Image Processing, Vol.13, No.4, pp.600-612, Apr. 2004.