# Poster: Image Suitability for Graphical Passwords

Mohammad N. Alshehri
Department of Computer Sciences and Cybersecurity
Florida Institute of Technology
Email: malshe012007@my.fit.edu

Heather Crawford
Department of Computer Sciences and Cybersecurity
Florida Institute of Technology
Email: hcrawford@fit.edu

Liam M. Mayron
School of Computing, Informatics, and Decision Systems Engineering
Arizona State University
Email: lmayron@asu.edu

***Abstract*—This work proposes a metric for determining the suitability of guiding images for graphical passwords. This measurement is intended to favor images that encourage users to select memorable, but non-obvious password click points. The metric was developed by analyzing thousands of passwords on a small but varied image database. We found that saliency covered the most frequently clicked portions of an image. Our results show that our model accurately predicts which images will score highest on both memorability and strength, thus providing an indicator as to which images are more suitable as guiding images for graphical passwords.**

## I. Introduction

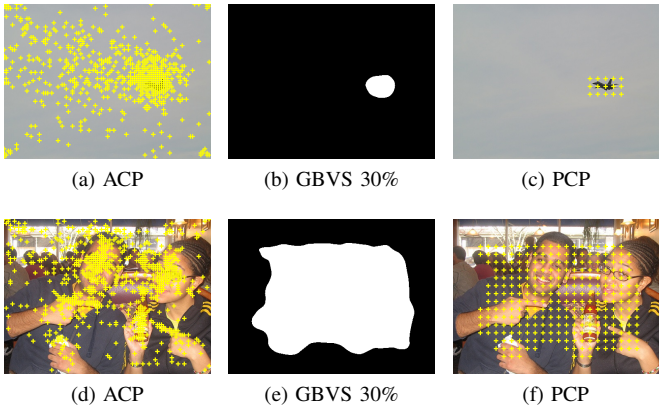
Graphical passwords are appealing due to their potential to improve usability and reduce error rates in comparison to text-based passwords [1]. The selection of the background (guiding) image is critical to the security of the system. An image that is too simple (i.e., as too few "clickable" points) may allow the password be predicted. Past research has focused on analyzing and predicting the locations of user taps - the actions that compose a graphical password [2]–[4]. The user selects several points on a guiding image to initially choose their password, and recalls the same points to authenticate [5]. The hotspots in the guiding image have a higher concentration where users also select click points [6]. Images with significantly more hotspots are selected more frequently when creating graphical passwords [2].

We propose a metric to strengthen graphical passwords before the user makes a single tap. We assess the suitability of a background image in terms of measuring the proportion of hotspots. Our metric incorporates a variety of strategies that have been suggested in the literature, including the relative saliency [2], [4], [7]–[10].

## II. Methodology

Our hypothesis is that the higher the proportion of an image that is covered by a saliency map (as a basis for memorable areas), the higher the entropy of the password for that image (as a basis of strength). To address this hypothesis, we will use the entropy equation to predict the entropy of a click point for a given image.

Training data consists of 15 images [4] originally from the PASCAL Visual Object Classes (VOC) Challenge 2012 dataset [11]. The training data includes more than 10,000 passwords collected from 762 subjects. We used the VOC dataset [11] as our test data, less the 15 images in the training dataset. We used Graph-Based Visual Saliency [12] with a threshold of 30% [9] to compute the visual attention map for the training set images.



(a) ACP (b) GBVS 30% (c) PCP

(d) ACP (e) GBVS 30% (f) PCP

Fig. 1. Samples of the computed saliency, actual and predicted click points

Our calculated salient regions within an image contained the highest percentage of user click points. This implies that the salient regions represent hotspots that attract user attention when looking at an image. As a result, the proportion of saliency maps that covers a given image could be used to measure the image's suitability for use as a guiding image for a graphical password. Having a higher proportion of the image covered by saliency maps leads to a higher number of hotspots, which in turn provides a larger set of points that may be both memorable and secure.

An image is segmented into $19X19$ squares in order to model the predicted click points as the center point of any square that is covered completely or partially by saliency maps as shown in Fig. 1. Predicting the entropy of a click point for an image is an indicator that helps us to accept or reject proportion of saliency maps as a measurement of image suitability. The entropy is defined as measuring the amount of uncertainty in the composition of a password [13] and is measured in bits. In order to test the validity of using the proportion of the image covered by saliency maps to measure the suitability of images, we use the Shannon equation for information content [14]. Fig. 2 shows the process of testing the validity of the model.

The predicted and actual probabilities of a click falling in a given square in the image are used to compute the predicted

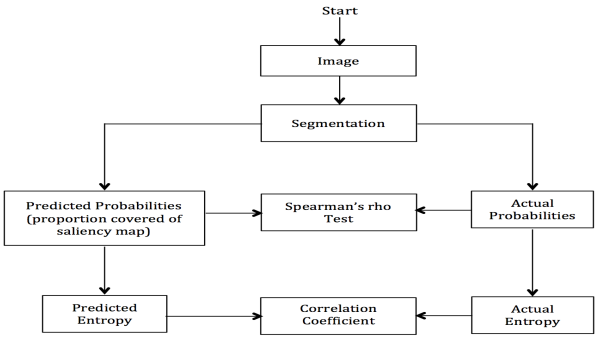



Fig. 2. Process for model validation

and actual entropy of a click point for a square.The average correlation coefficient between predicted and actual entropy is $0.83$ which means there is a high correlation between predicted and actual entropy. There is a positive correlation between the proportion of the image covered by salient regions, and the entropy of a click point in an image. Therefore, there is evidence to support our hypothesis.

## III. Results, discussion, and conclusion

The high degree of correlation between the predicted and actual entropy indicates the effectiveness of using saliency maps to predict the possible memorable areas of an image. The size of the salient areas is positively correlated to the theoretical space of more memorable click points. An image with more salient areas is an image that has more prominent hotspots, supporting our main hypothesis.

Table I shows the rankings of the training dataset images when both predicted entropy and percentage of the image covered by the calculated saliency map are considered. The first column shows the image rankings when sorted according to the percentage of the image covered by the saliency map first, and secondly according to the predicted entropy. The second column shows the image rankings sorted by predicted entropy first, and percentage of the image covered by the saliency map second. The first five images are ranked the same according to both methods of sorting, and that the remainder of the images change in rank by at most one position. This implies that there is very little difference (for this dataset) in one over the other, and that there is evidence of the correlation between these image features.

The model was subsequently applied to a much larger test dataset - 17,097 images. The proportion of the images considered salient in the test dataset ranged from 0.64 (highest) to 0.01 (lowest). The model selected images with greater visual complexity as more appropriate for graphical passwords. These images are more challenging to predict computationally.

In this work, we proposed a strength measurement for background images used to guide suitable image selection for graphical passwords before the user selects their first click point. The measurement can be used to reject simple images (those that are likely to be predicted by computational methods) and encourage the user to select a more complex image that is rich in memorable click points in order to improve the memorability and security of graphical passwords.

TABLE I
Ranking based on proportion covered and predicted entropy

| Rank (saliency, predicted entropy) | Rank (predicted entropy, saliency) | Image | Proportion covered | Predicted entropy |
|---|---|---|---|---|
| 1 | 1 | 11 | 0.47 | 8.01 |
| 2 | 2 | 10 | 0.45 | 7.96 |
| 3 | 3 | 4 | 0.45 | 7.80 |
| 4 | 4 | 9 | 0.45 | 7.80 |
| 5 | 5 | 6 | 0.42 | 7.73 |
| 6 | 7 | 7 | 0.32 | 7.32 |
| 7 | 8 | 15 | 0.3 | 7.44 |
| 8 | 6 | 13 | 0.28 | 7.35 |
| 9 | 10 | 3 | 0.24 | 7.05 |
| 10 | 9 | 8 | 0.23 | 7.07 |
| 11 | 11 | 12 | 0.14 | 6.55 |
| 12 | 13 | 5 | 0.14 | 6.20 |
| 13 | 12 | 14 | 0.13 | 6.31 |
| 14 | 14 | 1 | 0.02 | 3.83 |
| 15 | 15 | 2 | 0.02 | 3.5 |

## References


[1] S. Chiasson, A. Forget, E. Stobert, P. C. van Oorschot, and R. Biddle, "Multiple password interference in text passwords and click-based graphical passwords," in *Proceedings of the 16th ACM conference on Computer and communications security*. ACM, 2009, pp. 500–511.

[2] J. Thorpe and P. C. van Oorschot, "Human-seeded attacks and exploiting hotspots in graphical passwords," in *16th USENIX Security Symposium*, 2007, pp. 103–118.

[3] A. Salehi-Abari, J. Thorpe, and P. C. van Oorschot, "On purely automated attacks and click-based graphical passwords," in *Computer Security Applications Conference, 2008. ACSAC 2008. Annual*. IEEE, 2008, pp. 111–120.

[4] Z. Zhao, G.-J. Ahn, J.-J. Seo, and H. Hu, "On the security of picture gesture authentication," in *Proceedings of the 22nd USENIX conference on Security*. USENIX Association, 2013, pp. 383–398.

[5] I. Irakleous, S. Furnell, P. Dowland, and M. Papadaki, "An experimental comparison of secret-based user authentication technologies," *Information Management & Computer Security*, vol. 10, no. 3, pp. 100–108, 2002.

[6] E. Stobert, S. Chiasson, and R. Biddle, "User-choice patterns in passtiles graphical passwords," in *Annual Computer Security Applications Conference (ACSAC) 2011*, 2011.

[7] D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes." in *USENIX Security Symposium*, vol. 13, 2004, pp. 11–11.

[8] A. E. Dirik, N. Memon, and J.-C. Birget, "Modeling user choice in the passpoints graphical password scheme," in *Proceedings of the 3rd symposium on Usable privacy and security*. ACM, 2007, pp. 20–28.

[9] L. M. Mayron, "A comparison of biologically-inspired methods for unsupervised salient object detection," in *Multimedia and Expo Workshops (ICMEW), 2013 IEEE International Conference on*. IEEE, 2013, pp. 1–4.

[10] L. M. Mayron and M. N. AlShehri, "Evaluating the use of models of visual attention to predict graphical passwords," in *The 52nd Annual ACM Southeast Conference Kennesaw State University, Kennesaw, Georgia*. ACM, 2014.

[11] M. Everingham, L. Van Gool, C. K. I. Williams, J. Winn, and A. Zisserman, "The PASCAL Visual Object Classes (VOC) Challenge," *International Journal of Computer Vision*, vol. 88, no. 2, pp. 303–338, Jun. 2010.

[12] J. Harel, C. Koch, and P. Perona, "Graph-based visual saliency," in *Proceedings of Neural Information Processing Systems (NIPS)*, 2006.

[13] W. E. Burr, D. F. Dodson, and W. T. Polk, *Electronic authentication guideline*. Citeseer, 2004.

[14] C. E. Shannon, "The mathematics theory of communication," *Bell Syst. Tech. J*, vol. 27, pp. 379–423, 1948.