

# Hash Visualization in User Authentication

Rachna Dhamija

School of Information Management and Systems  
University of California, Berkeley  
Berkeley, CA 94720-4600  
rachna@acm.org

## ABSTRACT

Although research in security has made tremendous progress over the past few years, most security systems still suffer by failing to account for human factors. People are slow and unreliable at processing long and meaningless strings, yet many security applications depend on this skill. For example, a major problem in user authentication is that people have difficulties in choosing and memorizing secure passwords. In this paper, we have investigated how the usability and security of user authentication systems can be improved by replacing text strings with structured images.

## Keywords

Security, passwords, authentication, user interface

## INTRODUCTION

Authentication schemes based on passwords have a number of shortcomings. Passwords that are simple or that have some meaning to the user are easier to remember, but are more vulnerable to attack. Passwords that are complex and arbitrary are more secure, but are difficult to remember. Since users can only remember a limited number of passwords, they tend to write them down or will use similar or even identical passwords for different purposes.

One approach to improve user authentication systems is to replace the precise recall of a password or PIN with the recognition of a previously seen image, a skill in which humans are remarkably proficient [2,3].

## A PROTOTYPE IMAGE AUTHENTICATION SYSTEM

We have prototyped a user authentication system that utilizes “visual hashes” in place of text based passwords. One proposed hash visualization algorithm is *Random Art*, a technique that converts meaningless strings into abstract structured images [1].

Instead of having to memorize a password, the user is able to create an image “portfolio”, by selecting some desired number of images, which he must memorize for future recognition. During authentication, the user is presented with a different set of images, some of which are from the

portfolio and others which are chosen randomly. To login, the user must correctly identify all of his or her portfolio images. Another variation on this idea uses a fixed database of real photographs instead of Random Art images.

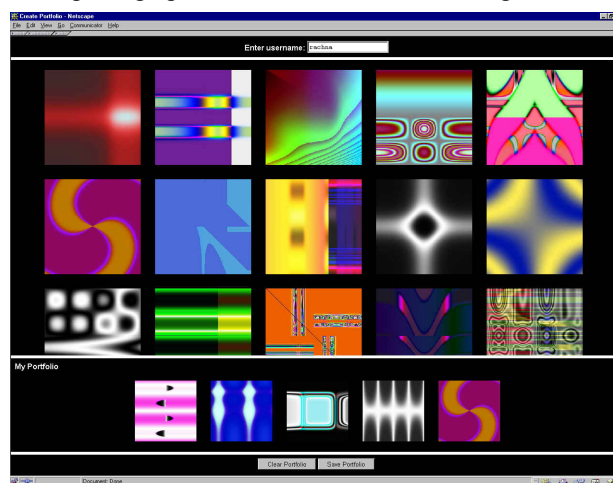


Figure 1. Random Art Portfolio Creation Screen

## Security of Image Authentication

The security of image authentication will depend on how many images are in the user's portfolio and how many the user is presented with. Suppose that the portfolio contains  $P$  images and that for authentication, the system presents a total of  $T$  images. This gives us  $T!/[(T-P)! P!]$  possible combinations. For example, a 4 digit credit card PIN that is four digits long results in 10,000 possible combinations. To achieve an equivalent result with images, we could use  $P=5$  and  $T=20$  which gives us 15,504 possible combinations. The optimal combination of  $P$  and  $T$  will depend on the level of security and performance time desired.

One security advantage of images, especially of Random Art images, is that they are harder to write down and to share with others than passwords and PINs. A vulnerability of this system is that an attacker might try to discover the image portfolio by making repeated login attempts and taking the intersection of images that are presented. Such attacks need to be taken into consideration during system design.

## USER STUDY

We conducted a user study to compare the prototype image authentication system to traditional text based authentication systems. Two types of image portfolios were

compared, using Random Art images and photographs. Twenty participants (11 males and 9 females) were selected to be representative of the general population of computer users.

Participants were first asked to create a four digit PIN and a six character password, both which they believed to be secure and that they had never used before. Participants also created two types of image portfolios, one consisting of five Random Art images and another consisting of five photographs. During portfolio creation, users were presented with the same set of one hundred images to choose from, although the image order was randomized.

Participants then had to authenticate using all four techniques. To authenticate using image portfolios, users had to select their five portfolio images, which were randomly interspersed with twenty other images they had never seen before. Participants were asked to login again using all four techniques after one week.

**Task Completion Time**

It took longer for users to create image portfolios and to login with them compared to passwords and PINS. Photo portfolios took longer to create than Random Art portfolios, but it took slightly longer for users to login with the Random Art portfolios. This suggests that people can recognize photographic images more quickly than abstract images. Figure 2 shows the average times for successfully completed tasks.

	PIN	Password	Art	Photo
<b>Create (session1)</b>	15	25	45	60
<b>Login (session1)</b>	15	18	32	27
<b>Login (session2)</b>	27	24	36	31

Figure 2. Average seconds to create/login

	PIN	Password	Art	Photo
<b>session 1</b>	5% (1)	5% (1)	0	0
<b>session 2</b>	35% (7)	30% (6)	10% (2)	5% (1)

Figure 3: % Failed logins (# failed logins/20 participants)

**Number and Severity of Errors**

A number of minor and major errors were made with PINs, passwords and portfolios. It is interesting to note that during the first session all users were able to recover from their errors and login successfully with portfolios, but this was not always the case with PINs and passwords, no matter how long or how many login attempts were made. Even after one week, the number of unrecoverable errors made with images was far lower than that of passwords and PINs. If more secure password and PIN restrictions were imposed, we suspect that the number of failed logins in those categories would increase.

**Qualitative Results**

It's easier than it looks: Although some users remarked that they would never be able to remember their portfolios, all

were very surprised by the fact that they could in fact recognize their images and at how quickly the selection took place.

Text vs. images: The majority of users reported that image portfolios were easier to remember than PINs and passwords, especially after 1 week, and that they would use such a system if they were confident that it was secure and if image selection times were improved.

Random Art vs. photos: Users tended to select photographic images based on a theme or something that had personal meaning to them. There was much more variation in the Random Art images chosen among users compared to the photographs.

**DISCUSSION , CONCLUSIONS & FUTURE WORK**

Image portfolio creation and login times must be reduced in order for such a system to be convenient for users. One improvement would be to reduce image size to minimize the need for scrolling, which occupied a significant portion of the task completion time.

To strengthen the system against an intersection attack, the interface can be divided into a number of screens. A user will be required to determine if any of his or her portfolio images is present in order to proceed to the following screen.

Results indicate that image authentication systems have potential applications, especially where text input is hard (e.g., PDAs or ATMs), for infrequently used passwords or in situations where passwords must be frequently changed. Because the error recovery rate was significantly higher for images compared to passwords and PINS, such a system may be useful in environments where high availability of a password is paramount and where the inability to easily communicate passwords to others is desired.

By taking advantage of the input capabilities of Random Art, users could be allowed to create images and then be asked to recognize or to recreate their images to authenticate. Hash visualization techniques may also be applicable to other security applications that depend on a user's ability to process large strings.

**ACKNOWLEDGMENTS**

I would like to thank James Landay, J.D. Tygar, Adrian Perrig and Dawn Song for their input in this project.

**REFERENCES**

1. Perrig, A. and Song, D. Hash Visualization: A New Technique to Improve Real-World Security, in *Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce*
2. Standing, L. Learning 10,000 pictures. *Quarterly Journal of Experimental Psychology*, 25:207-222, 1973.
3. Standing, L., Conezio, J., and Haber, R.N. Perception and memory for pictures: Single-trial learning of 2500 visual stimuli. *Psychonomic Science*, 19(2):73-74, 1970.