# Do You See What I See?
# The Use of Visual Passwords for Authentication

Marc J. Dupuis
marcjd@uw.edu
University of Washington
Bothell, Washington

Jaynie Shorb
jaynies@uw.edu
University of Washington
Bothell, Washington

James Walker
wjameslwalker@gmail.com
University of Washington
Tacoma, Washington

Fred B. Holt
fb.holt@ritepasswords.com
Rite Passwords
Tacoma, Washington

Michael McIntosh
m.mcintosh@ritepasswords.com
Rite Passwords
Tacoma, Washington

## ABSTRACT

A password is one of the oldest forms of authentication whose popularity has not waned. Passwords are easy to use, inexpensive to deploy, and are familiar by everyone. However, this comes with a cost. Passwords are easy to guess, difficult to remember when they are made complex and unique, and found everywhere on the Dark Web. The security usability paradox suggests that any improvements in security will result in a decrease in usability, and vice versa. In this paper, we examine the feasibility of a visual password system in which a traditional password is used, but with the additional capability of modifying the characters of the password to provide significantly higher levels of entropy.

## CCS CONCEPTS

• **Security and privacy → Graphical / visual passwords**; **Usability in security and privacy**; *Social aspects of security and privacy*.

## KEYWORDS

visual passwords, authentication, color preference, recognition vs. recall, memory, cognition, usability vs. security

**ACM Reference Format:**
Marc J. Dupuis, Jaynie Shorb, James Walker, Fred B. Holt, and Michael McIntosh. 2020. Do You See What I See? The Use of Visual Passwords for Authentication. In *The 21st Annual Conference on Information Technology Education (SIGITE '20), October 7–9, 2020, Virtual Event, USA.* ACM, New York, NY, USA, 4 pages. https://doi.org/10.1145/3368308.3415458

## 1 INTRODUCTION

Passwords became the most accepted way of authenticating users even though they violate the psychological acceptability design principle for protection of information [14]. Psychological acceptability depends on easy to use systems, and although passwords have become familiar to the user, they require a focused effort. The use of passwords is widespread, and users are required to supply passwords through multiple interfaces to many vendors. Password rules added to boost security through complexity has reduced usability. The design goal should be to improve both security and usability rather than trading off one for the other [1]. Although various efforts have been undertaken to encourage the user to create more complex passwords using traditional text-based entry (e.g., [5]), the ability to remember and effectively recall such complex passwords remains problematic. And given that less than one-third of individuals use a password manager [4], we need to continue to explore other possible solutions.

For a password schema that uses color as one of the options, there are five general requirements that must be met. First, the colors that are chosen as part of the password schema must have a roughly equivalent chance of being selected. Otherwise, a false sense of security with respect to perceived improvements in entropy will occur. Second, there must be a significant enough number of colors available to increase the entropy such that implementing such a schema is worth any costs associated with doing so, whether on the implementation side or for the end users. Third, the colors chosen as part of the schema must have enough separation between them for end users to be able to quickly and clearly identify a preferred color and later select that same color without being confused by one that is similar. While the number of color choices available is theoretically over 16 million, this is not realistic if we expect end users to be able to later recognize their preferred choice. Fourth, the colors chosen must be able to be represented consistently enough across different devices and visual displays that they can then be successfully recognized as part of the authentication process. Finally, other options must be available for individuals with visual and other impairments such that entropy is not sacrificed in the process.

The purpose of the current paper is to examine the efficacy of using color as part of a password schema by examining some of these requirements. We do this by reviewing the literature with a particular focus on visual password systems. Next, we discuss the concept of color preference since this will inform any system that uses color as part of its schema. Then, we outline the methods used in this study to assess whether color could be an effective component of a text-based password. Finally, we discuss the results from two surveys and what this may mean going forward.

*SIGITE '20, October 7–9, 2020, Virtual Event, USA*

ACM ISBN 978-1-4503-7045-5/20/10…$15.00
https://doi.org/10.1145/3368308.3415458

## 2 BACKGROUND

### 2.1 Graphical Methods

Graphical methods include any component of a password that is visual rather than composed from data in the ASCII Table. Graphical authentication provides a memorable solution for the user through recognition. Some drawbacks include large database sizes to store images, mouse location clicking inaccuracies, and password collisions for basic shapes. The graphical password methods include alignment, color, and images.

Adding color as an option for passwords, Gao and company generated the ColorLogin schema [8]. ColorLogin allows configuration for the number of rounds (1-3), a number of colors (3-5), and some password icons. A group of pictures arranged in 3 x 3 squares create a 9 x 9 over-all group of icons in each round. The user picks their password icons from the group for each round. A benefit of ColorLogin is that the password entry is faster than other graphical icon methods because the color background allows the user to focus on specific 3 x 3 squares for locating their password icons.

Other approaches have also included color as part of the password schema in conjunction with other components, such as shapes, patterns, and objects [11, 12]. For example, the Random Geometric Graphical Password technique has a set of three geometric shapes, three colors, and five click points [12]. There is a random number that is created to determine the colors and the tracks for the objects to follow. The user picks three shapes and clicks on the image to direct the pattern five times. In another example, association methods are used since they may make memorization easier [11]. The password triplet contains a location, a color, and an object. The method of creating the password includes visualization methods on the location, color, and object which encourages the use of image associations and cues for recall. In yet other another approach incorporating a graphical method for password entry is to have the user doodle their password [9]. Users were allowed to generate a password by doodling a color image.

### 2.2 Color Preferences

Research has been examining the color preferences of individuals for several decades (e.g., [2, 6, 10, 13]). Their research covered areas in advertising, marketing, and even the association of color with shapes and objects. With the large number of studies conducted on colors and color preferences, the focus has often been on the colors red, blue, and green as this is what the cone cells in our retina see.

These colors appear to be the foundation behind the research in trying to understand how they relate to an individual's preference based on human emotions, association to shapes and objects, and individual buying choices. However, there is still little scientific data on how that color can influence or affect a person's reasoning, behavior, or preference. This notion is becoming increasingly important in the digital era. Trying to understand why and how people choose a certain color plays a role in creating websites, web pages, and in the current research, password alterations.

A study of color perception and color working memory (CWM) was conducted with a variety of colors in hue. During the trial, between one and eight colors were shown for study with a delayed period of (100-1500ms). The participants were then instructed to select the color that they viewed during the study period from the circular color ring [7]. After completing the trials, the responses were reviewed. The results showed that there were different colors chosen by the participants than the ones shown during the study period. The assumption was that the individual's memory is imperfect when trying to select different colors in hue.

Without significant studies being conducted on how and why people choose a particular color, it is hard to know what type of colors should be implemented into a new innovated password solution. There was no research found on what will make an end user use a particular color for a password. However, it was shown in previous studies that colors in hue are less likely to be remembered. Based on that study, the assumption would extend that conclusion to the multiple of shaded colors. The realization is people choose colors because that color resembles something that they like or is associated with an object that they like with the same color.

## 3 SURVEY 1: COLOR PREFERENCES

### 3.1 Methods

The goal for this study was to examine how color may be used as part of a broader password schema. We conducted two separate surveys to provide some baseline information on the possible efficacy of using color as part of a broader password schema that also includes other manipulations, such as formatting and orientation.

For each of the surveys, we recruited participants using Amazon's Mechanical Turk (mTurk) platform. Recruitment through mTurk has wide acceptability and several advantages [3], including providing a greater cross-section than a college psychology class consisting of mostly sophomores [15].

In our first survey, we successfully recruited 1,177 participants and compensated them with $0.25 each. Our sample consisted of 644 participants that identified as male (54.7%), 518 that identified as female (44.0%), and 15 (1.3%) participants that did not identify their gender preference. The participants were more highly educated (87.3% had a bachelor's degree or higher) and younger (62.6% were 18-34) than the general population, which is consistent with participants from the mTurk platform [3].

We presented participants with a hypothetical new system that would use color as part of the password. Basically, it would color the characters of the entire password their chosen color. While the system we have discussed in this paper is capable of having each character a different color, it was important that we begin with an assessment of the feasibility of something simpler—the entire password being a single color. Each participant was presented with 14 different color choices in random order. The colors selected were chosen from the 16 HTML colors noted in the HTML 4.0 specification with the exception of black and white, which were both omitted. They were asked to state their preference. The presentation of these colors was done by using the text "password" in various colors. See Figure 1.

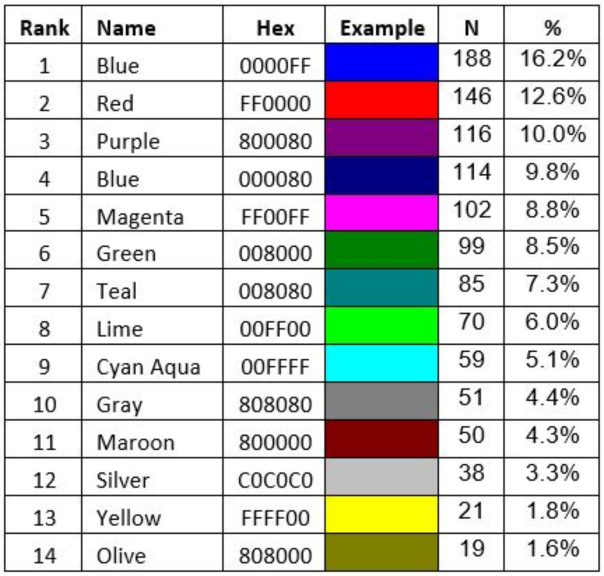
**Figure 1: Password with the Color Blue Used (#0000FF)**

A follow-up question asked them what their color preference would be if their first choice was not available.

## 3.2 Results

There were 1158 responses to the question related to their color preference. And perhaps not too surprisingly, individuals tended to gravitate toward a few colors more than others. In fact, the top three color preferences were chosen by 38.8% of the participants rather than 21.4% if the distribution had been equal. Similarly, the bottom three choices should also represent 21.4% of the choices people made, but instead only represent 6.7%.

In order for color to be as effective as possible to be used as part of a password schema, the distribution of color preferences must be equal among the color choices available to the end user. This is where the theoretical possibilities of such a system conflict with an implementation in the wild. If the implementer of a system knows that the probability of a chosen color is more or less than the 7.14% probability in a system with 14 colors then the would-be adversary would know this as well. While it is not probable that equal distributions will be achieved in a real-world setting, the color palette used must seek to achieve this to the extent possible. The results from the first survey are depicted in Figure 2.



| Rank | Name | Hex | Example | N | % |
|---|---|---|---|---|---|
| 1 | Blue | 0000FF | 🟦 | 188 | 16.2% |
| 2 | Red | FF0000 | 🟥 | 146 | 12.6% |
| 3 | Purple | 800080 | 🟪 | 116 | 10.0% |
| 4 | Blue | 000080 | 🟦 | 114 | 9.8% |
| 5 | Magenta | FF00FF | 🟪 | 102 | 8.8% |
| 6 | Green | 008000 | 🟩 | 99 | 8.5% |
| 7 | Teal | 008080 | 🟩 | 85 | 7.3% |
| 8 | Lime | 00FF00 | 🟩 | 70 | 6.0% |
| 9 | Cyan Aqua | 00FFFF | 🟦 | 59 | 5.1% |
| 10 | Gray | 808080 | ⬛ | 51 | 4.4% |
| 11 | Maroon | 800000 | 🟫 | 50 | 4.3% |
| 12 | Silver | C0C0C0 | ⬜ | 38 | 3.3% |
| 13 | Yellow | FFFF00 | 🟨 | 21 | 1.8% |
| 14 | Olive | 808000 | 🟫 | 19 | 1.6% |

**Figure 2: Color Preference for Password, Survey 1**

Based on these results, we wanted to test the efficacy of a new color palette in achieving a more equal distribution of color preferences from end users. Thus, we conducted a second survey.

# 4 SURVEY 2: REFINEMENT OF COLOR PREFERENCES

In our second survey, we wanted to accomplish three things: 1) Increase the size of the color palette; 2) Obtain a more equal distribution from participants with respect to their color preferences, and 3) Determine how many people would choose color as a modification when having to choose at least three out of five possible modifications.

## 4.1 Methods

As before, we employed mTurk for participant recruitment. Given the more complex nature of this survey, we doubled the compensation being provided. As a result, our sample size was also decreased accordingly. There were 544 completed surveys with 512 usable results. We had 32 participants that failed one or more quality control questions for a 5.9% rejection rate. Participants were compensated with $0.50 each for their time. Out of 512 participants, there was essentially an even split between those that identified as male (255) versus those that identified as female (254) with the remaining participants opting to not select an answer for that question.

We increased the size of the color palette from 14 to 18. In order to minimize the likelihood for compounding the results we obtained, we opted to increase the size only marginally. Additionally, we examined the color choices individuals made from the first survey. We eliminated the top four choices and replaced each one with two similar shades of the same color. The hope was that this would result in a more equal distribution. As before, we provided a hypothetical scenario for our research participants by telling them that we were testing issues related to a possible new password system. We also asked participants to select three out of five possible modification types for their password with color as one possible option.

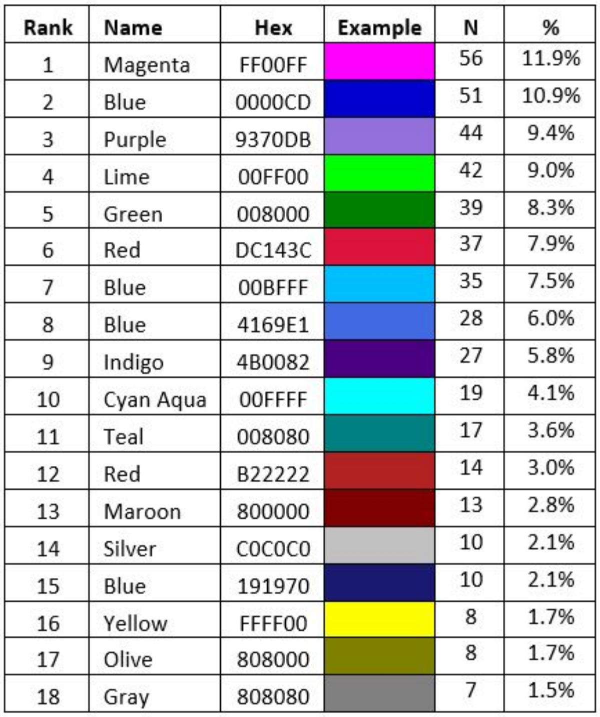
After selecting their preferred password modification types, participants then chose the specific modification for each of the modification types. After completing the first part of the survey, they were asked a series of questions from an unrelated psychological questionnaire. Once they had completed this, they were asked to re-identify the modification types previously chosen and the specific modifications for each type. It was emphasized to them when making the initial selection and then later when recalling their prior selection that they were not quality control questions and they would not be penalized if their response was incorrect.

## 4.2 Results

In the second survey, the top three choices represented 32.2% of all selections. While this number is lower than what was found in the first survey (38.8%), it nonetheless represents a much higher percentage than what we otherwise expect if the distributions were equal. Since we now have 18 colors rather than 14 from survey one, we would expect the top three colors to represent 16.7% of all selections. Our results are almost twice this amount with a different of 15.5 percentage points. This is only marginally better than what was found in survey one (16.9 percentage points). Likewise, the three colors selected the least amount of times represents 4.9% of all selections. These results are depicted in Figure 3.

These participants were also asked to re-identify the specific modification they had selected earlier in the survey. Out of 469 participants, 388 (82.7%) were able to correctly re-identify the color they had previously chosen.

As previously noted, we were curious how many individuals would choose color as a modification if they had to select three out of five possible modification types. Most (91.6%) participants did



| Rank | Name | Hex | Example | N | % |
|---|---|---|---|---|---|
| 1 | Magenta | FF00FF | 🟪 | 56 | 11.9% |
| 2 | Blue | 0000CD | 🟦 | 51 | 10.9% |
| 3 | Purple | 9370DB | 🟪 | 44 | 9.4% |
| 4 | Lime | 00FF00 | 🟩 | 42 | 9.0% |
| 5 | Green | 008000 | 🟩 | 39 | 8.3% |
| 6 | Red | DC143C | 🟥 | 37 | 7.9% |
| 7 | Blue | 00BFFF | 🟦 | 35 | 7.5% |
| 8 | Blue | 4169E1 | 🟦 | 28 | 6.0% |
| 9 | Indigo | 4B0082 | 🟪 | 27 | 5.8% |
| 10 | Cyan Aqua | 00FFFF | 🟦 | 19 | 4.1% |
| 11 | Teal | 008080 | 🟩 | 17 | 3.6% |
| 12 | Red | B22222 | 🟥 | 14 | 3.0% |
| 13 | Maroon | 800000 | 🟫 | 13 | 2.8% |
| 14 | Silver | C0C0C0 | ⬜ | 10 | 2.1% |
| 15 | Blue | 191970 | 🟦 | 10 | 2.1% |
| 16 | Yellow | FFFF00 | 🟨 | 8 | 1.7% |
| 17 | Olive | 808000 | 🟫 | 8 | 1.7% |
| 18 | Gray | 808080 | ⬛ | 7 | 1.5% |

**Figure 3: Color Preference for Password, Survey 2**

choose color as one of their three modification types. Out of 469 participants that chose this as one of their modification types, 99.8% of participants correctly re-identified color as one of the types they had chosen when asked again toward the end of the survey. Only four participants incorrectly identified color as something they had chosen at the beginning of the survey.

# 5 DISCUSSION

## 5.1 Limitations

There are a few limitations worth noting. First, the use of color in any system poses significant challenges for those that are visually impaired, color-blind, or have cognitive limitations that make recognition and recall problematic. The system that was developed includes color as one possible modification out of several others. Thus, this may mitigate the impact for individuals with color-blindness, but not necessarily for those with other impairments.

Second, our data is based on a description of a hypothetical system as presented to individuals completing a survey that were recruited from a crowdsourcing platform. There are issues related to both internal and external validity that cannot be ignored. However, the purpose of this research was to highlight some of the possible benefits and challenges of using color as part of a password schema, as well as some of the considerations that must be taken into account. We believe we accomplished this despite some of the limitations inherent in this research.

Third, color preferences do vary some based on gender. While we did not analyze that specifically in the current study, it is something that must be taken into account before the implementation of such a system. An adversary would likely know the gender of his target. This could make it easier to guess the most likely color choices among even a large color palette.

## 5.2 Future Work

There are several opportunities for additional improvements in the selection of an ideal color palette. While some marginal improvements were made from survey one to survey two, much greater improvements would be needed prior to the implementation of such a system. Similar to distribution problems for the use of color as a modification type, it is expected that these challenges are also present in the other types of modifications. The implications of testing such a system and knowing its limitations is important. A false sense of security through perceived higher levels of entropy based on theoretical considerations alone can be dangerous. Once further refinements have been made based on additional testing such as detailed in this study, it will be important to test the feasibility of this system in real-world experiments and implementations.

# REFERENCES

[1] Robert Biddle, Sonia Chiasson, and P.C. Van Oorschot. 2012. Graphical Passwords: Learning from the First Twelve Years. *ACM Comput. Surv.* 44, 4 (Sep 2012), 19:1–19:41. https://doi.org/10.1145/2333112.2333114

[2] Ines Bramao, Alexandra Reis, Karl Petersson, and Luis Faisca. 2011. The role of color information on object recognition: A review and meta-analysis. *Acta Psychologica* 138 (Jun 2011), 244–253.

[3] Marc Dupuis, Barbara Endicott-Popovsky, and Robert Crossler. 2013. An Analysis of the Use of Amazon's Mechanical Turk for Survey Research in the Cloud. In *International Conference on Cloud Security Management.*

[4] Marc Dupuis, Tamara Geiger, Marshelle Slayton, and Frances Dewing. 2019. The Use and Non-Use of Cybersecurity Tools Among Consumers: Do TheyWant Help?. In *Proceedings of The 20th Annual Conference on Information Technology Education (SIGITE '19).* ACM. https://doi.org/10.1145/3349266.3351419

[5] Marc Dupuis and Faisal Khan. 2018. Effects of peer feedback on password strength. In *2018 APWG Symposium on Electronic Crime Research (eCrime).* IEEE, 1–9. https://doi.org/10.1109/ECRIME.2018.8376210

[6] Andrew Elliot and Markus Maier. 2007. Color and Psychological Functioning. *CURRENT DIRECTIONS IN PSYCHOLOGICAL SCIENCE* 16, 5 (Feb 2007), 250–254.

[7] Jonathan Flombaum and Sarah Allred. 2014. Relating Color Working Memory and Color Perception. *Trends in Cognitive Science* 18, 11 (2014), 562–565.

[8] H. Gao, X. Liu, S. Wang, H. Liu, and R. Dai. 2009. Design and Analysis of a Graphical Password Scheme. In *2009 Fourth International Conference on Innovative Computing, Information and Control (ICICIC).* 675–678. https://doi.org/10.1109/ICICIC.2009.158

[9] Joseph Goldberg, Jennifer Hagman, and Vibha Sazawal. 2002. Doodling Our Way to Better Authentication. In *CHI '02 Extended Abstracts on Human Factors in Computing Systems (CHI EA '02).* ACM, 868–869. https://doi.org/10.1145/506443.506639

[10] Anya Hurlbert and Yazhu Ling. 2007. Biological components of sex differences in color preference. *Current Biology* 17, 16 (2007), R623–R625.

[11] Zhi Li, Qibin Sun, Yong Lian, and D. D. Giusto. 2005. An Association-Based Graphical Password Design Resistant to Shoulder-Surfing Attack. In *2005 IEEE International Conference on Multimedia and Expo.* 245–248. https://doi.org/10.1109/ICME.2005.1521406

[12] P. L. Lin, L. T. Weng, and P. W. Huang. 2008. Graphical Passwords Using Images with Random Tracks of Geometric Shapes. In *2008 Congress on Image and Signal Processing*, Vol. 3. 27–31. https://doi.org/10.1109/CISP.2008.603

[13] Stephen Palmer and Karen Schloss. 2010. An Ecological Valence Theory of Human Color Preference. *National Academy of Sciences* 107, 19 (2010), 8877–8882.

[14] J. H. Saltzer and M. D. Schroeder. 1975. The protection of information in computer systems. *Proc. IEEE* 63, 9 (Sep 1975), 1278–1308. https://doi.org/10.1109/PROC.1975.9939

[15] David O. Sears. 1986. College sophomores in the laboratory: Influences of a narrow data base on social psychology's view of human nature. *Journal of Personality and Social Psychology* 51, 3 (1986), 515.