

# CPSC 530 Bit Art Passwords

Bret Shilliday: UCID 30053892: Computer Science  
Zach Brown: UCID 30070355: Computer Science  
Md Mushfiqur Rahman: UCID 30106379: Computer Science  
Oscar Campos: UCID 30057153: Computer Science

## **Table of Contents:**

1. Abstract
2. Introduction and Problem
3. Proposed Work
4. Evaluation
  - a. Memorability
  - b. Frequency of Selection
  - c. Bias in Design
  - d. Security Comparison to Text Based Passwords
  - e. Security Comparison to Graphical Password
  - f. Design Flaws
  - g. Enhancing Security
5. Conclusion

## **Abstract:**

Graphical passwords provide an alternative method for authentication from text-based passphrases. While there have been many proposed methods for graphical passwords, this paper proposes a novel password design using “bit art” which allows users to toggle the state of cells in a grid to form pictures and authenticate. This report provides an overview of the security and usability of our bit art password design compared to text-based passphrases and other graphical passwords through a small scale study where various versions of these passwords were created and results tracked over time. It will also explore potential vulnerabilities of these passwords, as well as recommendations for enhancing security.

*Keywords: Bit Art passwords, authentication, text-based passwords, security, usability, small scale study, vulnerabilities, recommendations, ASCII passwords.*

## **Introduction and Problem:**

Managing control over sensitive data is important however there is often a tradeoff between security and convenience [1]. Currently, the most common form of authentication is through the use of passphrases in the form of text-based passwords. Most of these passwords consist of a unique string of characters that may have certain restrictions bound to them to increase their security.

An alternative to a text-based password is a graphical password, which has the potential to provide greater security while also being easier to memorize [6]. Additionally, text based passwords in practice tend to be composed of the same patterns, words and characters which further degrades their security if a heuristic is used to assist in determining which passwords to attempt first [5].

There has already been extensive research on different types of graphical passwords showing that “most graphical password schemes fall along the descending line, where increased security implies decreased usability” [2]. Despite these findings, we are proposing a novel bit art graphical grid password, to

determine if the design can be a viable substitution to combat the difficulty some users face when creating and then remembering complex text based passwords. Our experiment will explore the usability of our design by looking at the memorability of the password over time and potential bias towards certain designs due to implementation and human nature. We will also attempt to compare our design to character based passwords as well as other popular graphical passwords. Finally we will discuss potential drawbacks, considerations and recommendations for the implementation of our design followed by a suggestion on whether our design is a viable alternative to a traditional passphrase.

### **Proposed Work:**

We have come up with a novel design for a graphical password where the user is prompted with an NxN grid that they can interact with via clicking on the cells. Through this interface, the user can toggle the various cells in order to create a visual image which they can remember and recreate at a later time. These grids can consist of bicolour (black and white) as well as tricolour (red, green, blue and white) cell options. For the bicolour grids, each cell can be easily converted to a binary 0 or 1. For the tricolor grids, the colors can be mapped to a two bit value (00, 01, 10, 11). Using these bit representations, the grid passwords can then be easily converted into a binary number which can be hashed and stored. Below is an example of both types of grids in an 6x6 format:

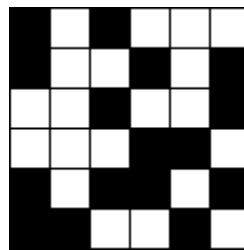


Figure A: 6x6 Bicolour Example

Figure A: This 6x6 grid could be represented in binary as  
101000100101001000110101101110010

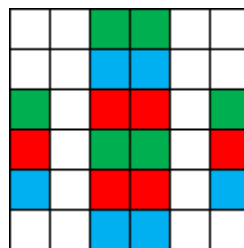


Figure B: 6x6 Tricolour Example

Figure B: This 6x6 grid could be represented in binary as  
000010100000000011110000100001010010010010100001110001010011000011110000

For our experiment, we had each of our group members create a bicolor and tricolor bit art password for 3 different size grids, 6x6, 8x8, 10x10. Each member was free to create anything they wanted without restriction. After the six passwords were created they were set aside until the end of the experiment. Then at intervals of 1 day, 1 week and 1 month, each group member was to recreate their passwords from memory without looking at the original password. Once recreated, the group member could then look at their password to determine where they made mistakes. This would be done by keeping track of the number of correct and incorrect cells to form a correctness percentage.

We also planned in our proposal to determine the equivalent text base password length to each of the proposed grid art designs. Initially, we determined that the best way to do this would be to look at the equivalent number of bits an ASCII encoded password would consist of in comparison to our well defined bit art passwords.

Finally, we wanted to see if some of the same issues that exist in text based passwords such as frequency of characters chosen as well as common patterns can also be found in our designs.

### **Evaluation:**

#### **Memorability:**

After conducting the experiment using the passwords created in Exhibits A, B and C, we first wanted to look at the memorability. As mentioned before, this was done by measuring the number of cells correctly entered (Exhibit D).

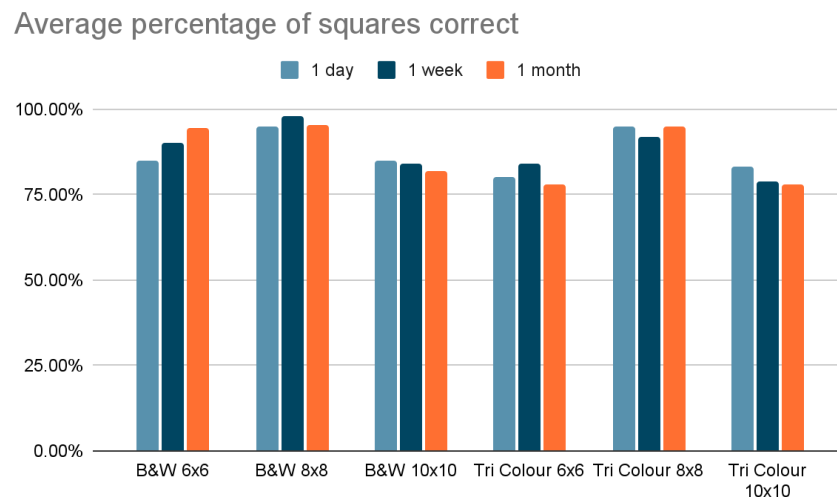


Figure C: Memorability Over Time by Grid

It appears that in both cases, the 10x10 grid was the hardest to remember. Additionally, over time the 10x10 grid became less memorable while the smaller designs did not see the same drop off. Interestingly, it appears that the 8x8 grid was more memorable than the 6x6 grid however this may have been caused by

bias in our limited set of designs. To explore this theory we attempted to look at the frequency of colours chosen as well as recognizable patterns.

### **Frequency of Selection:**

When looking at frequency, we can see that across all sizes and color variations of the grid, approximately two thirds of the cells were untouched. Additionally, for both the 8x8 bicolor, only 25% of the cells were toggled on average which may explain why it performed better than the 6x6 version. Additionally, for the 8x8 tricolour passwords, the colour breakdown was 19.92% red, 7.42% green and 4.69% blue. While users were free to use as many or as few colors as possible, using a tricolor grid as a bicolor grid could potentially make it easier to memorize and represent the first potential bias of bit art passwords. We also found similar results with our 10x10 tricolour grid in that not all colors were used equally.

### **Bias in Design:**

We also identified three other types of bias when evaluating the created passwords. The first was the use of symmetric patterns. As can be seen below, the majority of the passwords incorporated some form of symmetry. This could pose a threat because knowing a portion of the password could reveal the rest.

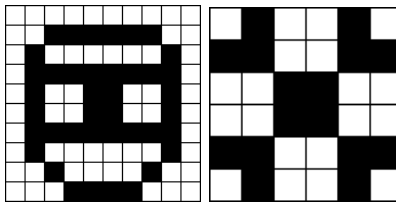


Figure D: Asymmetrical Designs

The second type of bias we identified was the use of drawings. In our dataset, we found that representations of places, or pictures were also commonly present.

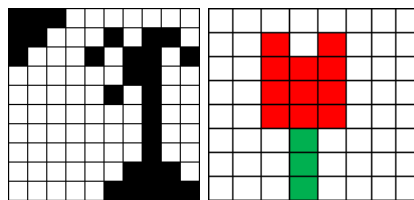


Figure E: Drawing Designs

Finally we noticed a prevalence of personal symbols such as initials. A few examples can be seen with the “BS” and “Z” passwords created by Bret Shilliday and Zach in Figure F.

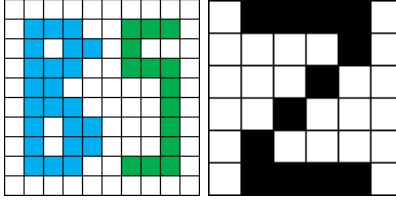


Figure F: Personal Symbol Designs

In almost all cases, one or more of these biases were present such as in the case of the “Canadian Flag”, which is symmetric, represents a real world object and is also personal to the creator.

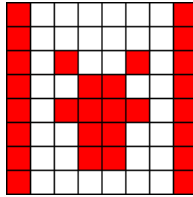


Figure G: Multiple Biases present

#### Security Comparison to Text Based Passwords:

Text-based passwords are typically entered via a keyboard and thus are composed of characters easily accessed via the keyboard. These characters are commonly encoded using the ASCII standard of which there are 95 unique visible characters from which the user is able to select.

Our proposal initially suggested the idea of comparing bit art passwords to text based passwords by finding the number of bits that comprised each bit art password and then dividing that by 8 to get an equivalent ASCII encoding. However we determined that a better solution would be to look at the passwords from the perspective of combinations considering that not all ASCII characters can be easily used when creating a password. As such we devised the following formula:

$$\text{Number of Colour Options Per Cell}^{\text{Number of Cells}} = \text{Possible Text Characters}^{\text{Length of Text Password}}$$

We then assumed that users would be able to use all 95 visible ASCII characters present on a standard keyboard for the possible text characters and substituted each of the values for the respective grids we tested.

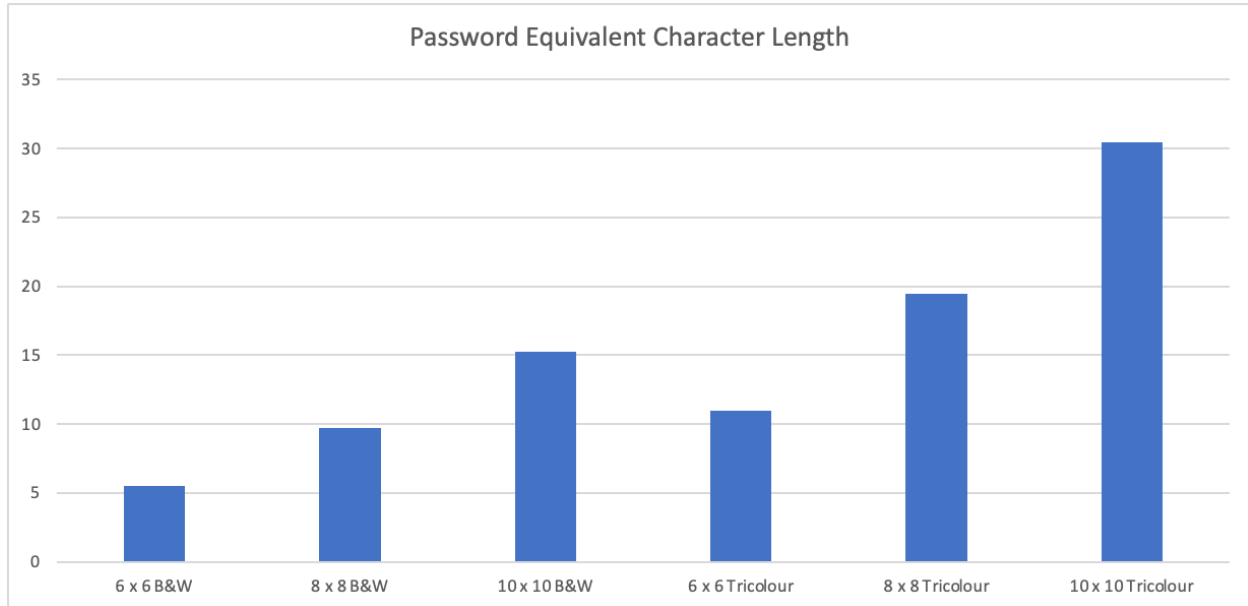


Figure H: Equivalent Text-based Password Length

From there we were able to determine that the password equivalents ranged from ~5.5 characters for the bicolour 6x6 grid to over 30 characters for the tricolour 10x10 grid.

This is relevant as the NIST guidelines state that human generated passwords should be at least 8 characters in length which all but the bicolour 6x6 grid meet.

Additionally, it can be seen that the number of combinations grows logarithmically as expected when increasing the size of the grid for each color variation:

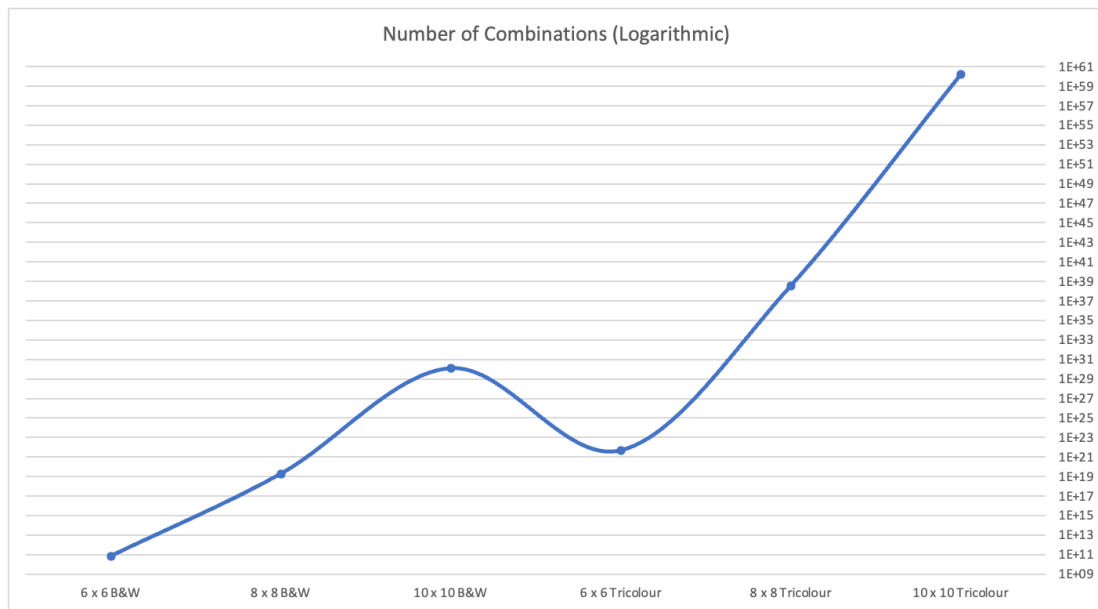


Figure I: Number of Combinations for Grid Variation

## Security Comparison to Graphical Passwords:

As an additional comparison that was not mentioned in our initial proposal we wanted to compare bit art graphical passwords to the three most popular graphical password schemas, Draw-a-Secret (DAS), PassPoint, and finally Android Pattern lock.

Beginning with DAS, a user is provided with an NxN grid to create a secret through strokes which is defined as a continuous path between two grid cells without lifting the “pen/finger”. We can calculate the number of possible combinations with the following equation:

$$4 \times n^2 = \text{possible strokes}$$

Where 4 is the possible directions (North, South, West, East) and n is the size of the grid.

Thus,

- $6 \times 6 \text{ grid} = 4 \times 6^2 = 144 \text{ possible strokes} = \log_2(144) \cong 7 \text{ bits}$
- $8 \times 8 \text{ grid} = 4 \times 8^2 = 256 \text{ possible strokes} = \log_2(256) \cong 8 \text{ bits}$
- $10 \times 10 \text{ grid} = 4 \times 10^2 = 400 \text{ possible strokes} = \log_2(400) \cong 8.64 \text{ bits}$

For PassPoint, users select a sequence of points on an image as their password. The entropy of this system is based on the image size, the number of points selected, and the tolerance for selecting a point. Studies have shown that the average entropy for PassPoint for a 5 point and a 9-pixel tolerance on a 451 x 331 image is around 18 bits of entropy [2].

In the Android pattern lock schema, users connect a sequence of dots on a 3x3 grid to create a pattern. The minimum number of dots that can be connected with this pattern is 4 dots and maximum 9 dots. Its entropy depends on the length and complexity of the pattern with a maximum entropy of approximately 12 bits (approximately 4096 possible combinations). Studies have shown that on average the entropy is much lower, approximately 7-8 bits (128-256 possible combinations), this is because users tend to create much simpler patterns [3].

According to our bit art proposal our lowest grid which is 6x6, black & white, has a maximum of 36 bits of entropy with approximately 68.7 billion combinations. With a total 68.7 billion possible combinations our smallest bit art password can have more entropy according to total possibilities than the three most popular graphical grid passwords (DAS, PassPoint, Android pattern lock) however our bit passwords suffer the same bias towards creating easy and memorable patterns as mentioned above.



## Design Flaws:

Even though our bit design has the potential to offer a more secure alternative to traditional passwords and popular graphical passwords we should consider some of the flaws inherent to our design. As seen before in the evaluation section of this report our team tended to create patterns based on a bias such as symmetric designs, use of images, and tendency to use personal symbols. These biases lead the user to create less complex patterns in order to more easily memorize. This removes randomness of a password creation leading to a less secure password. Additionally, if a user frequently forgets their password, they are more likely to choose a simpler password upon reset which further hinders password security.

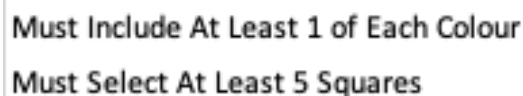
We also did not take into consideration the possible attacks that can be done to recreate and or forge bit art (as well as other types of graphical passwords). The attacks to consider are the following:

1. Smudge Attacks: When users' fingerprints on a touch screen can leak information about the pattern
2. Shoulder Surfing: Observers might still be able to discern and reproduce the pattern if they have a clear view of the user's screen during input
3. Brute Force: Password combinations can still be attempted by trying all combinations of toggled bits
4. Dictionary Attacks: Eventual dictionaries can be built of common graphical passwords to be tried first

While increasing the size of the grid provides more possible combinations and therefore a higher entropy and security, this makes the design less usable. This hinders the ability for the user to navigate and accurately select their password on smaller screens such as smartphones.

## Enhancing Security:

Our initial proposal was focused on the tradeoff between memorability and security however as we discovered common biases within our designs, we have expanded our scope to include suggestions to enhance security of our bit art password design considering the identified flaws. Firstly, complex patterns can be encouraged by providing a minimum requirement for users when creating new bit art passwords. Such requirements can include having a minimum number of cells required to be toggled or a minimum amount of each color in the tricolor grids.



**Must Include At Least 1 of Each Colour**  
**Must Select At Least 5 Squares**

Figure J: Example of Minimum Requirements

Secondly, we suggest that the user be presented with a random grid as a starting point. The objective of this modification is to reduce the amount of white space as noticed was prevalent in the evaluation section and thus providing a less biased password.

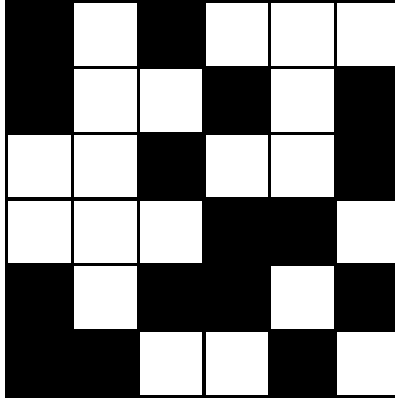


Figure K: Example of Random Starting Grid

Another feature that can be included when creating a bit art password is to provide a password strength checker that accesses the bit art pattern strength. For example the grid could be outlined in green for a secure password, yellow for medium secure password, and red for not-secure. Poor passwords could also be prevented from being submitted. This test could be based off of a test such as the NIST monobit test or other tests based on symmetry or grouping of cells.

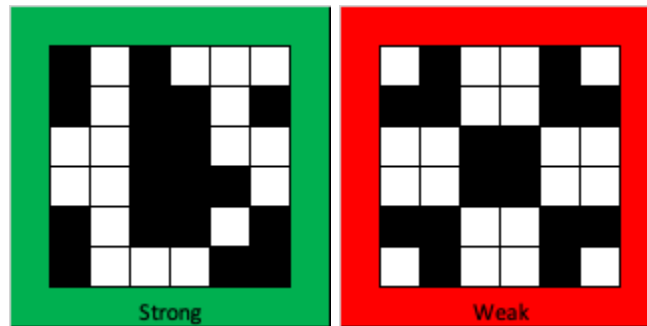


Figure L: Example of Password Strength Indicator

Additionally, another method of identification such as 2FA through SMS, Email or using an authentication application such as Google Authentication, Authy, or Microsoft Authenticator could increase security. Research suggests that using a one time pad access code or authenticator can prevent up to 100% of automated bot attacks, 99% of bulk phishing attacks, and 90% of targeted attacks [4, 5]. By incorporating these enhancements, we can significantly improve the security of our bit art design from common attacks such as shoulder surfing, smudge, brute force and dictionary attacks as mentioned above.

### **Conclusion:**

In conclusion, bit art passwords can be secure and usable when used in conjunction with other security measures. While they are still susceptible to bias in the password creation process and various types of attacks, they can offer a user-friendly alternative for individuals who struggle with traditional text-based passwords. Thus, we recommend this type of password as an alternative to traditional passphrases as well as other popular graphical passwords when implemented with the appropriate enhanced security measures.

## **References:**

- [1]. L. Tam, M. Glassman & M. Vandenwauver (2010) The psychology of password management: a tradeoff between security and convenience, *Behaviour & Information Technology*, 29:3, 233-244, DOI: 10.1080/01449290903121386
- [2]. Chiasson, S., van Oorschot, P. C., & Biddle R. (2007). Graphical passwords: Learning from the First Twelve Years. *ACM Computing surveys*, 44(4), Article 19.
- [3]. Andriotis, P., Tryfonas, T., Oikonomou, G., & Yildiz, C. (2014). A pilot study on the security of pattern screen-lock methods and soft side channel attacks. In *proceedings of the 6th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec '13)*(pp.1-6).ACM.
- [4]: Gassi, P.A., Garcia, M.E., & Fenton, J.L(2017). *Digital Identity Guidelines: Authentication and Lifecycle Management*. National Institute of Standards and Technology. NIST Special Publication 800-63B.
- [5]. Bonneau, J. (2012, May). The science of guessing: analyzing an anonymized corpus of 70 million passwords. In *2012 IEEE symposium on security and privacy* (pp. 538-552). IEEE.
- [6]. De Angeli, A., Coventry, L., Johnson, G., & Renaud, K. (2005). Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems. *International Journal of Human-Computer Studies*, 63(1-2), 128-152.

Appendix:

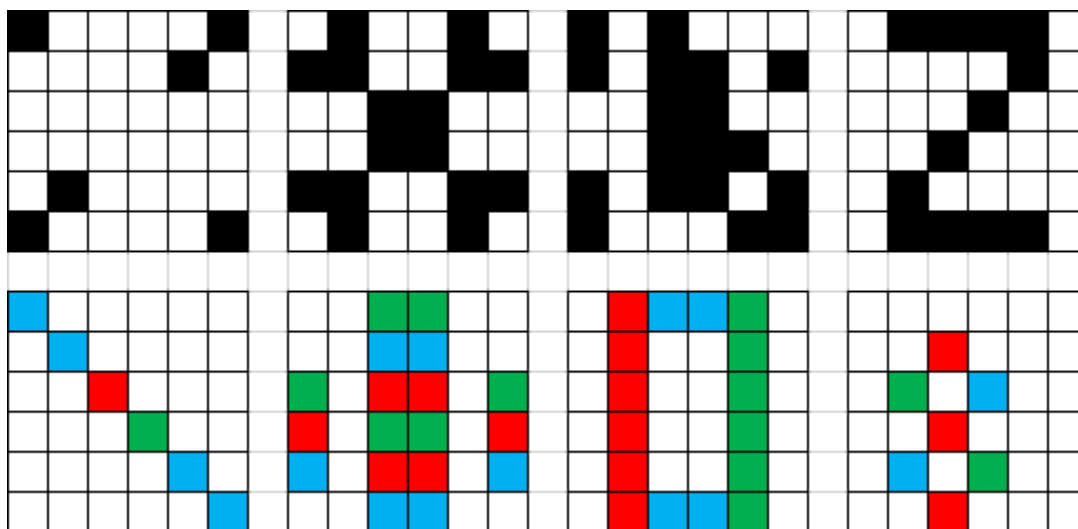


Exhibit A: 6x6 Passwords Created

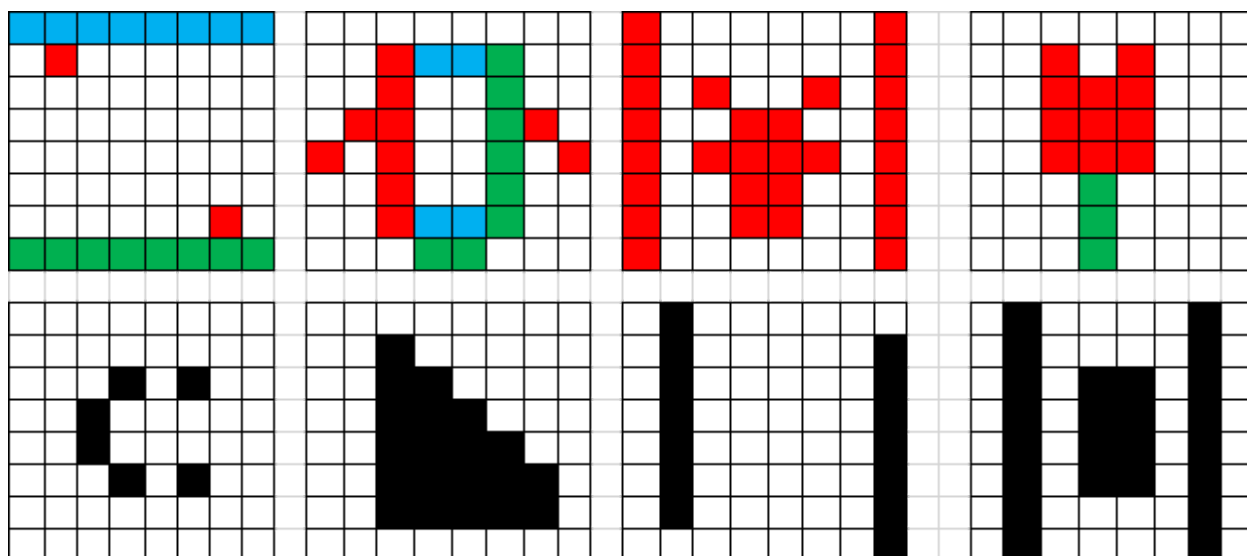


Exhibit B: 8x8 Passwords Created

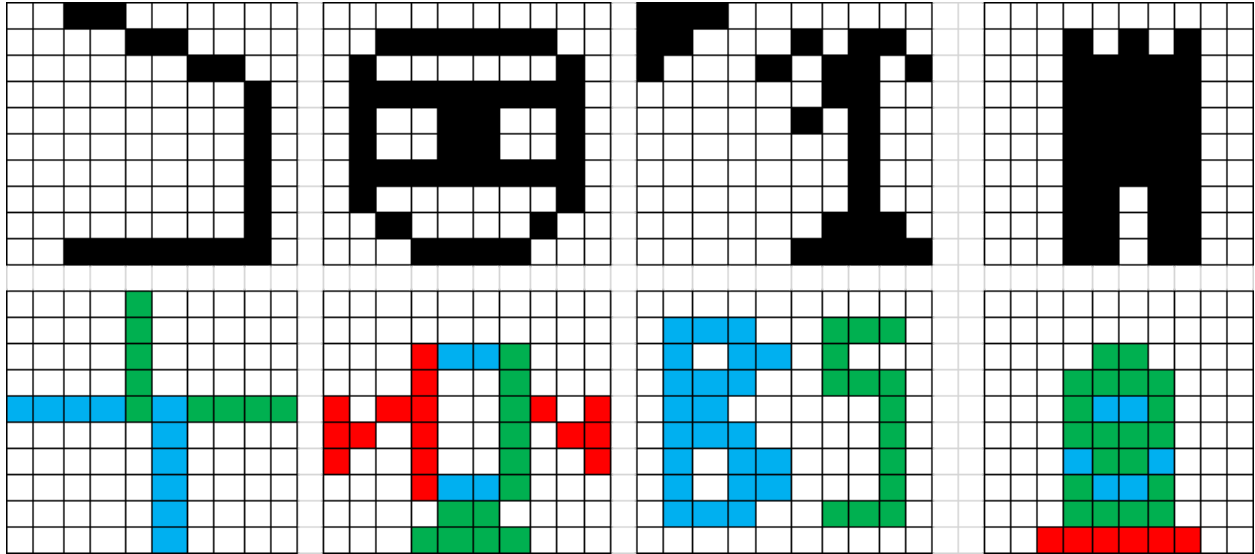


Exhibit C: 10x10 Passwords Created

	Bret	Md	Oscar	Zach	Average	Standard Deviation
1 Day						
Bicolour 6x6	1	1	0.4	1	85.00%	0.30
Bicolour 8x8	1	1	0.8	1	95.00%	0.10
Bicolour 10x8	0.9	1	0.5	1	85.00%	0.24
Tricolour 6x6	0.5	1	0.7	1	80.00%	0.24
Tricolour 8x8	1	1	0.8	1	95.00%	0.10
Tricolur 10x10	0.7	1	0.7	0.94	83.50%	0.16
1 Week						
Bicolour 6x6	1	0.91	0.7	1	90.25%	0.14
Bicolour 8x8	1	0.97	0.95	1	98.00%	0.02
Bicolour 10x8	0.83	0.83	0.7	1	84.00%	0.12
Tricolour 6x6	1	0.6	0.9	0.88	84.50%	0.17
Tricolour 8x8	1	0.8	0.9	1	92.50%	0.10
Tricolur 10x10	0.65	0.7	0.9	0.92	79.25%	0.14
1 Month						
Bicolour 6x6	1	0.83	0.95	1	94.50%	0.08
Bicolour 8x8	1	0.87	0.95	1	95.50%	0.06
Bicolour 10x8	0.73	0.78	0.95	0.81	81.75%	0.09
Tricolour 6x6	0.67	0.58	1	0.88	78.25%	0.19
Tricolour 8x8	1	0.8	1	1	95.00%	0.10
Tricolur 10x10	0.59	0.67	1	0.84	77.50%	0.18

Exhibit D: Cells Memorized Data

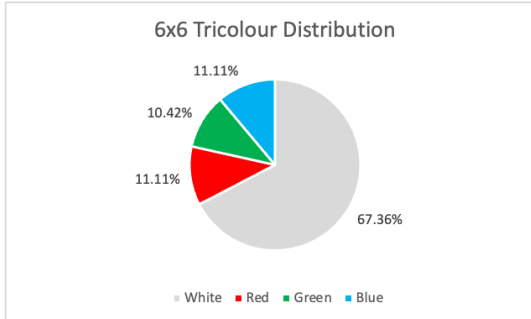
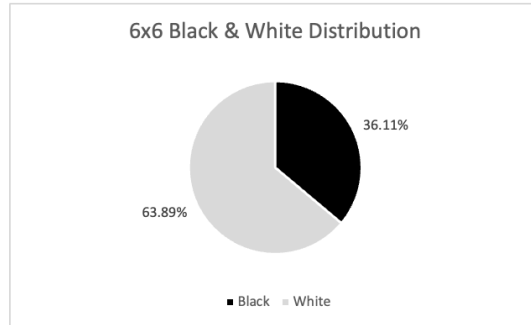


Exhibit E: Color Distribution of 6x6 Created Passwords

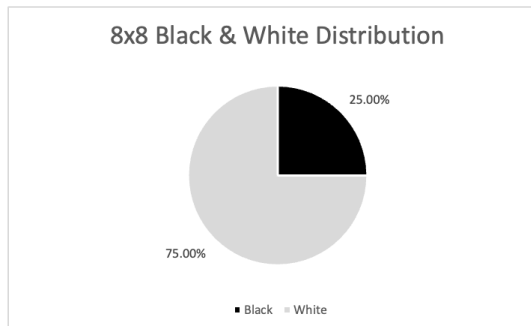
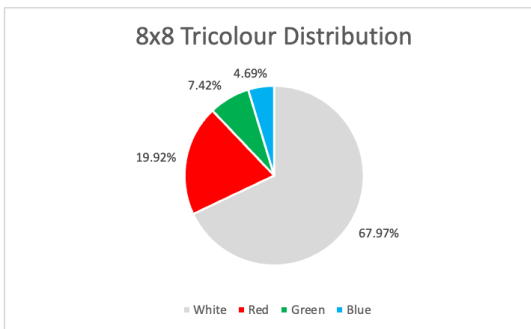


Exhibit F: Color Distribution of 8x8 Created Passwords

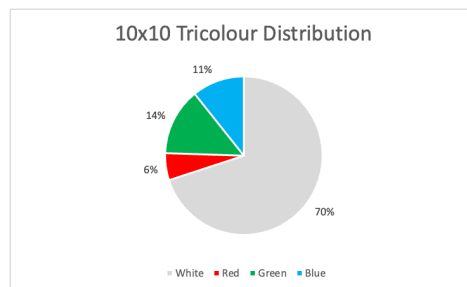
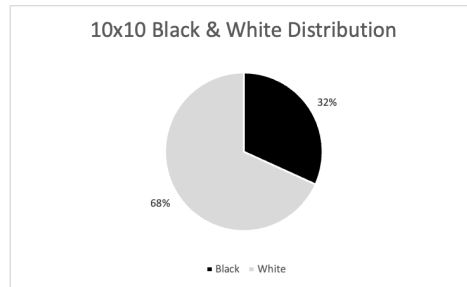


Exhibit G: Color Distribution of 10x10 Created Passwords