

Authentication Using Graphical Password: Effects of Increased Security on Usability

William M. Martin

Aaron G. Cass

March 3, 2018

UNION
COLLEGE



01

Human Computer Interface Security (HCIsec)

02

Password Problem

03

Graphical User Authentication



Select Password Point #1

[Home](#)

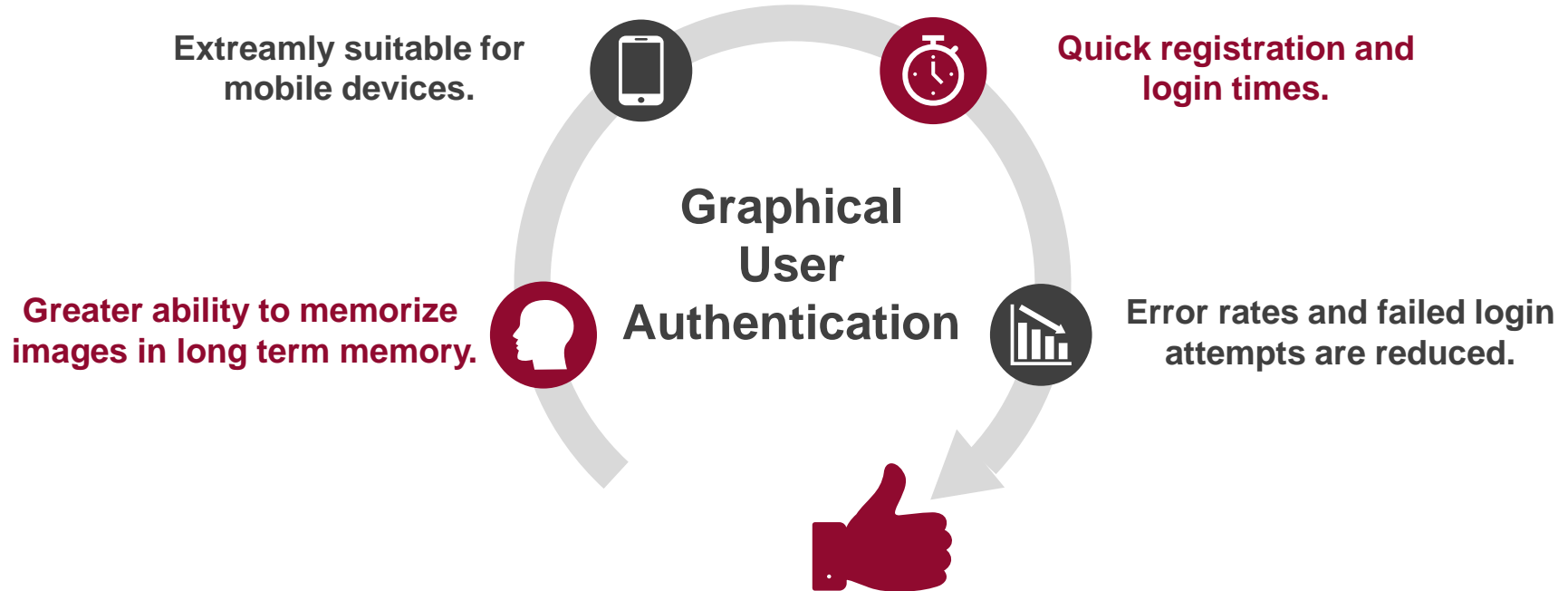
Undo

Log In



Enter your password.

Introduction



Background and Related Work

Brute-Force



Dictionary



Phishing



Spy-Ware



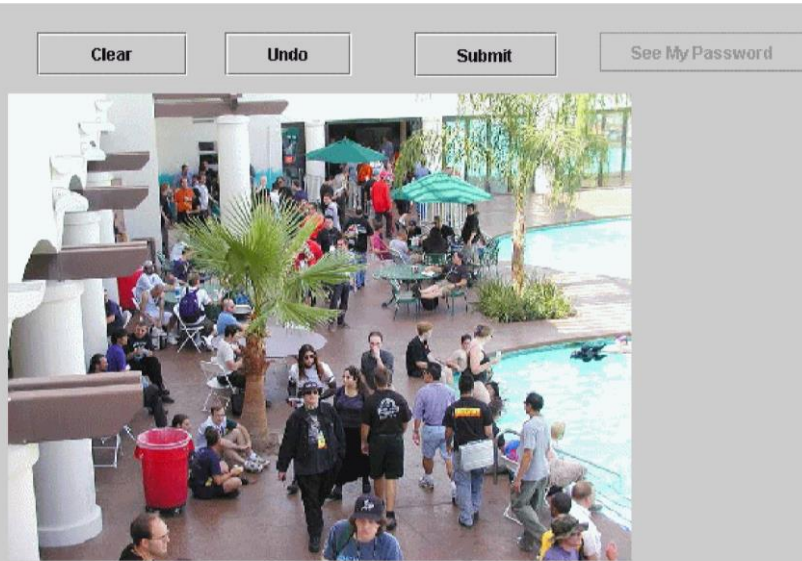
Previous Research states that in many areas, GUA is more secure when compared to alphanumeric authentication.

Background and Related Work

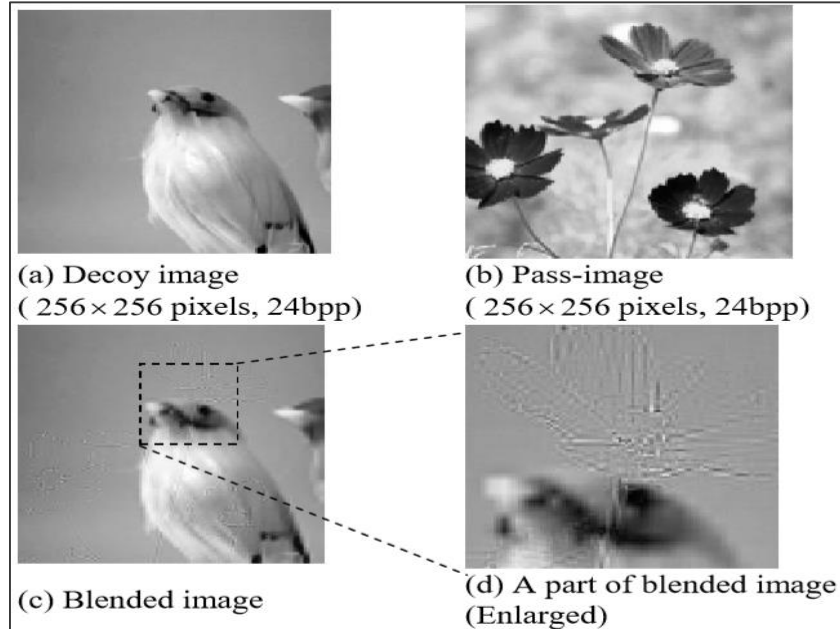
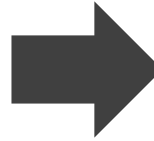


Can a Graphical User Authentication System achieve resilience towards shoulder surfing without lowering usability?

Methods and Design

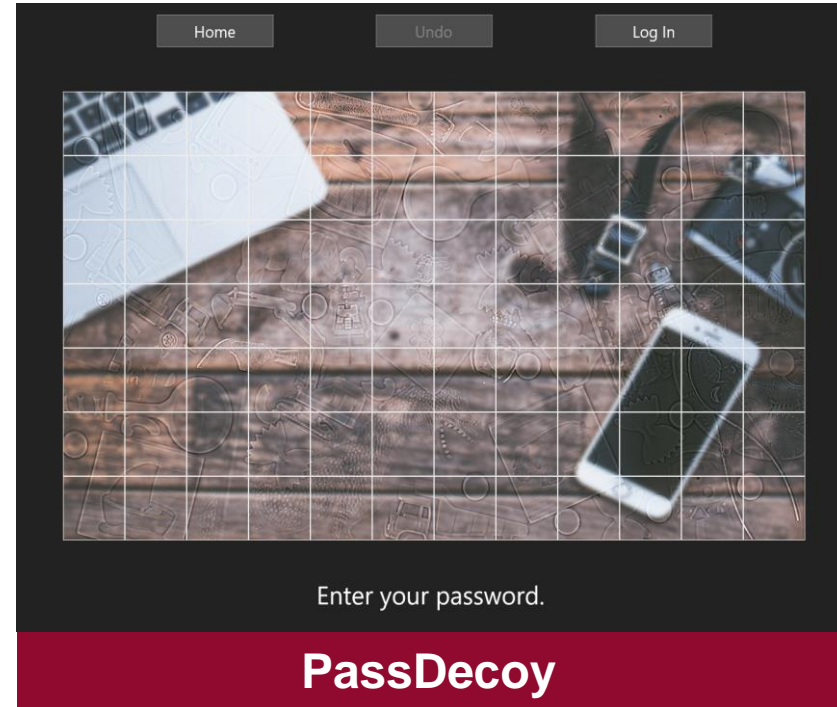
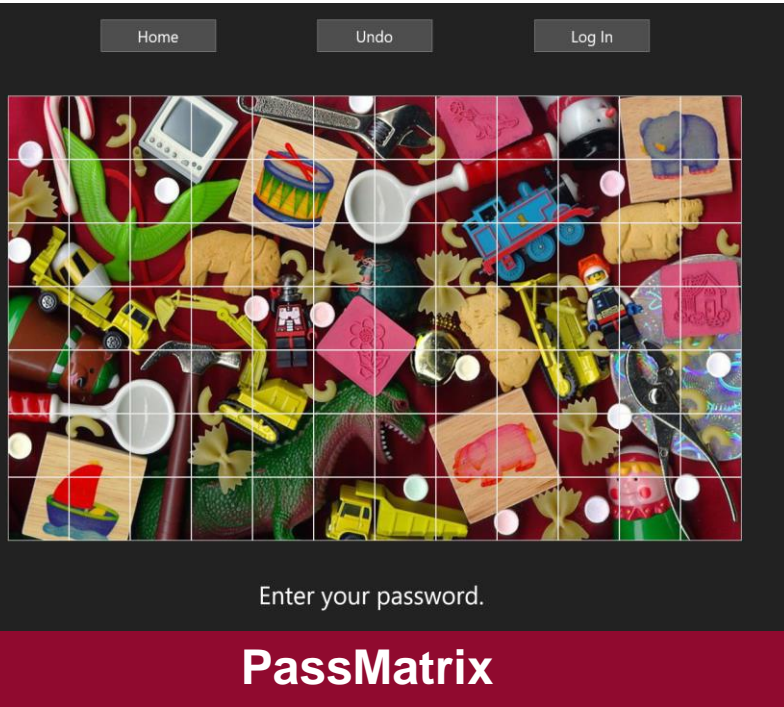


PassPoints



Discrete Wavelet Transform

Methods and Design



Methods and Design

Hybrid Imagery

UNION
COLLEGE



High Frequency - Password Image



Low Frequency - Decoy Image





















Experiments Performed



User Study



20 Participants



Interact with both systems



Test order was randomly administered



Effectiveness

- Number of Failures
- Number of Errors



Efficiency

- Registration Time
- Login Time



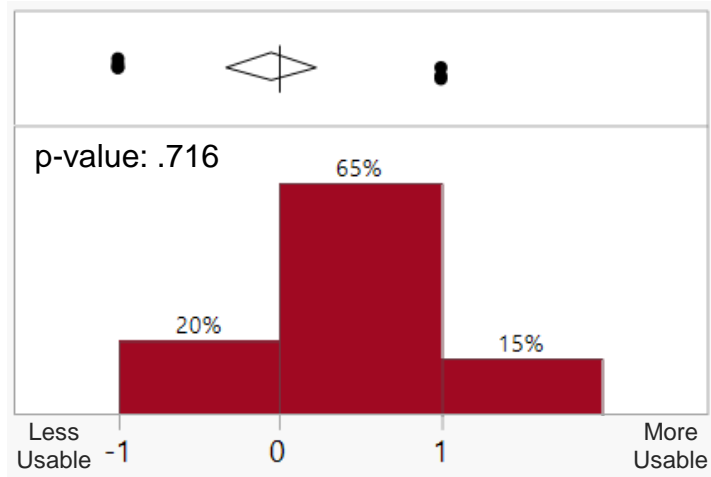
Satisfaction

- 5 question survey
- Likert-Scale Responses

Results

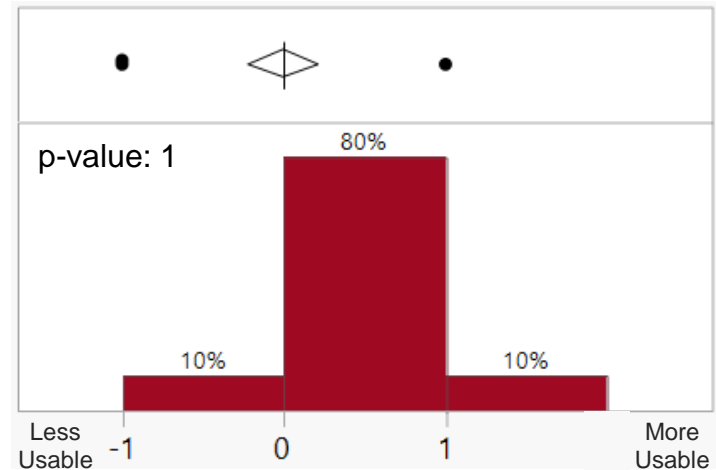
Number of User Errors

There is insufficient evidence to demonstrate that there is a difference between the two systems, if this test was given to a larger group.



Number of Failed Login Attempts

There is insufficient evidence to demonstrate that there is a difference between the two systems, if this test was given to a larger group.

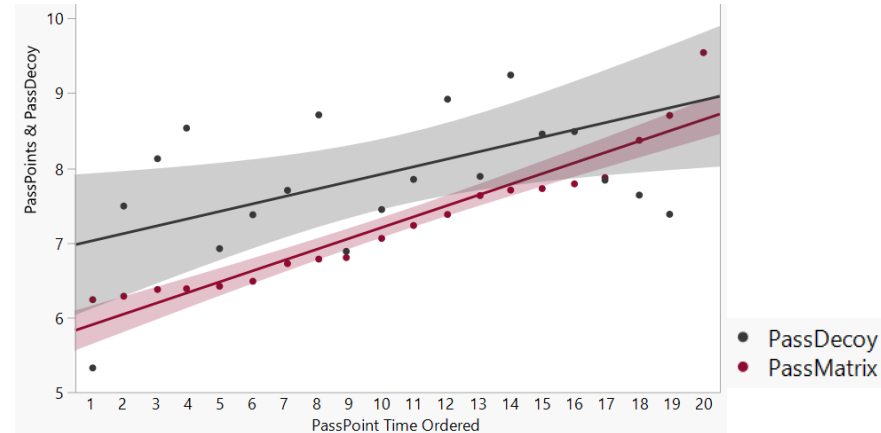
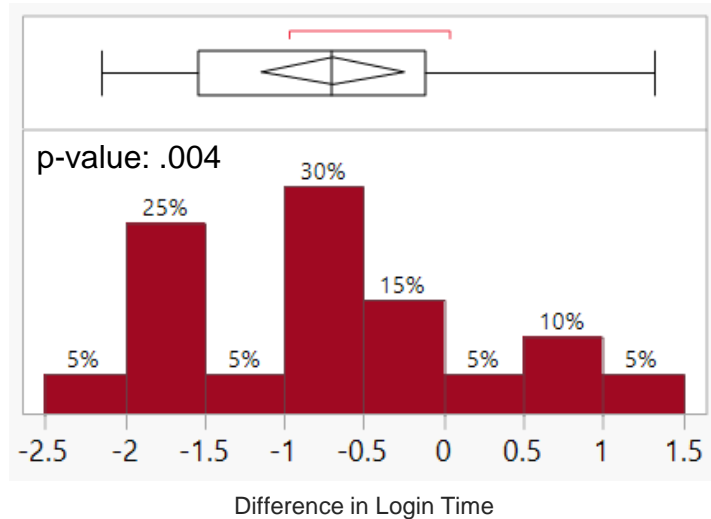


Results

Login Time

There is sufficient evidence to demonstrate that there is a difference between the two systems, if the test was given to a larger group.

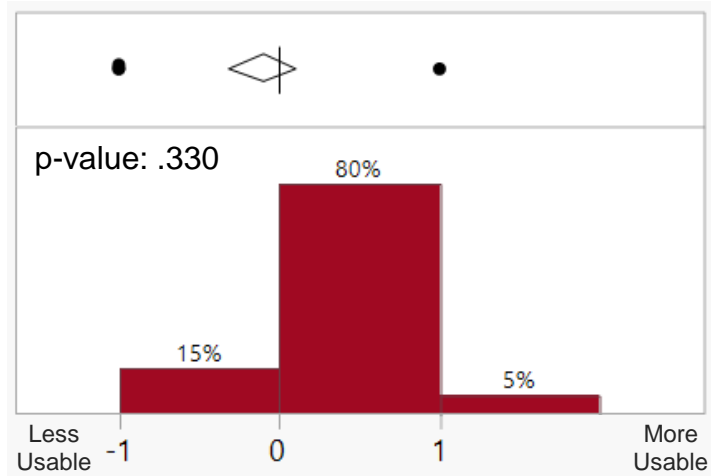
With a confidence of 95%, it can be said that PassDecoy will take users an additional .25 - 1.13 seconds per login attempt.



Results

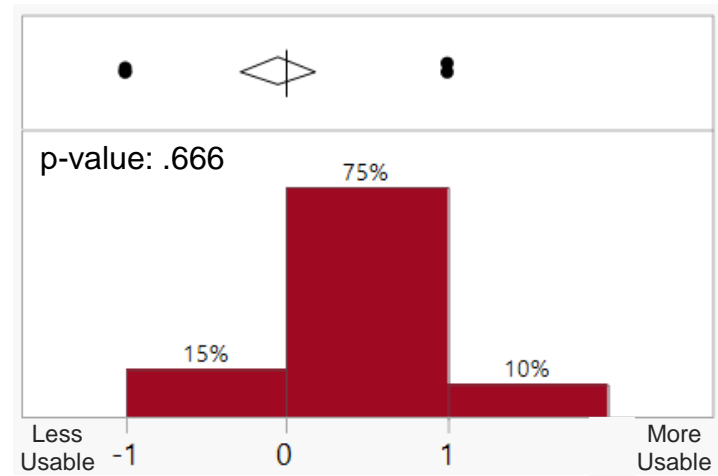
It did not take me long to input my password 3 times.

There is insufficient evidence to demonstrate that there is a difference between the two systems, if this test was given to a larger group.



Once I created my password, I was able to input it correctly.

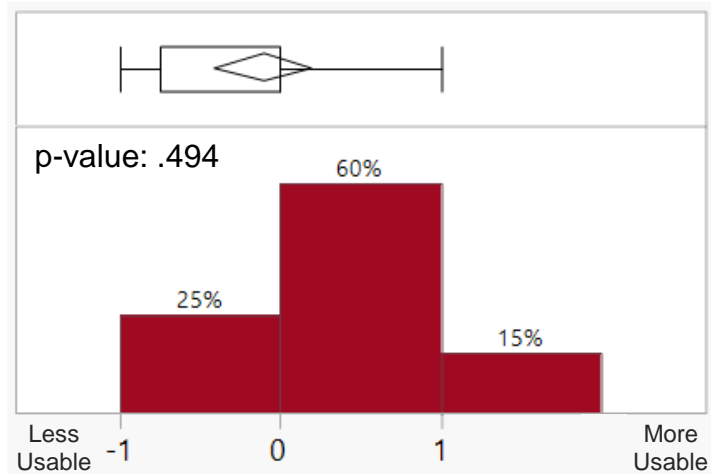
There is insufficient evidence to demonstrate that there is a difference between the two systems, if this test was given to a larger group.



Results

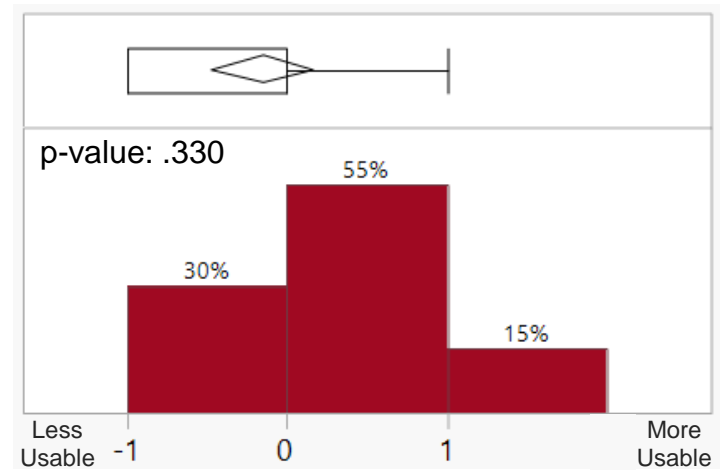
Registering my password was fast.

There is insufficient evidence to demonstrate that there is a difference between the two systems, if this test was given to a larger group.



Inputting my password was easy.

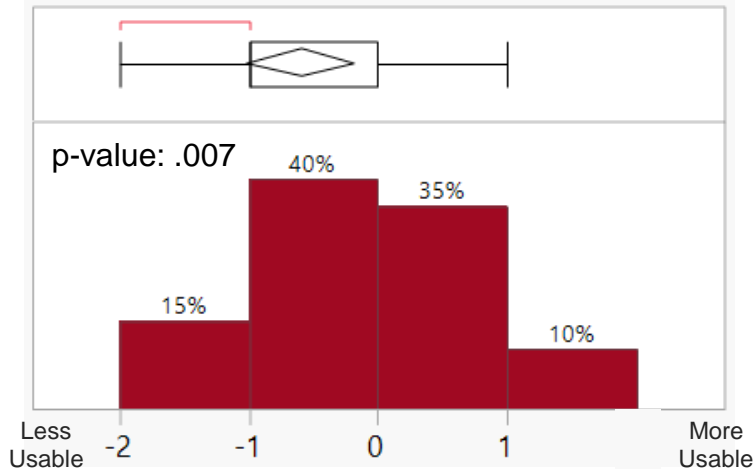
There is insufficient evidence to demonstrate that there is a difference between the two systems, if this test was given to a larger group.



Results

My password images are easy to memorize.

There is sufficient evidence to demonstrate that there is a difference between the two systems, if this test was given to a larger group.



Can a Graphical User Authentication System achieve resilience towards shoulder surfing without lowering usability?

Future Work

01

Remove color from the password image during registration.

02

Test how differences in visual capability effected the results.

03

Conduct additional user tests to see if login time can be reduced through practice.

References

Sonia Chiasson, P. C. Van Oorschot, and Robert Biddle. "Graphical Password Authentication Using Cued Click Points". In: *Proceedings of the 12th European Conference on Research in Computer Security. ESORICS'07*. Dresden, Germany: Springer-Verlag, 2007, pp. 359–374. ISBN: 3-540-74834-2. URL: <http://dl.acm.org/citation.cfm?id=2393847.2393880>.

Elizabeth Stobert et al. "Exploring Usability Effects of Increasing Security in Click-based Graphical Passwords". In: *Proceedings of the 26th Annual Computer Security Applications Conference. ACSAC '10*. Austin, Texas, USA: ACM, 2010, pp. 79–88. ISBN: 978-1-4503-0133-6. DOI: 10.1145/1920261.1920273. URL: <http://doi.acm.org/10.1145/1920261.1920273>.

T. Miyachi et al. "A study on memorability and shoulder-surfing robustness of graphical password using DWT-based image blending". In: *28th Picture Coding Symposium*. Dec. 2010, pp. 134–137. DOI: 10.1109/PCS.2010.5702441.

Fei Ye Haichang Gao Wei Jia and Licheng Ma. "A Survey on the Use of Graphical Passwords in Security". In: *Journal of Software* 8.7 (2013), pp. 1678–1698. URL: <https://pdfs.semanticscholar.org/774c/7ac9d7bd9c73ff16c8b2cc8a21ae08739371.pdf>.