Aesthetic Evaluation of Artforms in RGPM: User's Perspective

Annie O. Egwali, Ph.D.[1*] and Franklyn C. Egwali, Ph.D.[2]

[1] Department of Computer Science, University of Benin, Benin City, Nigeria.
[2] Department of Fine and Applied Arts, University of Benin, Benin City, Nigeria.

E-mail: annie.egwali@uniben.edu*
frankgwali@yahoo.com

ABSTRACT

RGPMs have been used extensively as authenticated proofs and identities. However, users' choices of good or bad passwords are heavily influenced by the design of the artforms embedded in these RGPM. The aesthetics or useful information available in RGPM can aid or hinder users understanding and memorability. The implication is that design choices need to be carefully considered when making usability and security-related modifications to RGPM artforms or user interface. This study therefore evaluates the aesthetic nature of some existing RGPM from the perspective of 274 university students and investigated whether the aesthetics of RGPM have significant impacts on these usability and security factors. This aim is achieved by using a questionnaire based on seventeen aesthetic factors of artforms: balance, contrast, emphasis, form, harmony, line, movement, pattern, plane, point, proportion, rhythm, shape, style, texture, value and variety. The results identify the aesthetic factors that need to be given more consideration when designing RGPM and shows that diverse outlook derived from area of specialization gives different evaluation outcome.

(Keywords: artforms, aesthetics, design choices, usability, security, user interface, recognition-based graphical password models).

INTRODUCTION

For a long time, the fine art disciplines were considered to belong to culture in the most classic sense. Fine arts organizations are a special form of service sector which establish a linkage between nations' cultural heritage and modern life. These art organizations also serve the functions of collection, research and exhibition, as well as education and recreation. Pallud and Straub (2014) pointed out that over time, the role of fine arts has changed significantly for they offer humans several social and experiential benefits, such as life enrichment, avenues for interactions, enjoyment, and learning experiences. However, a gradual shift has been made from the functional definition, where the arts discipline were object-based and focused on acquisition, conservation, communication and exhibition of art, to the purposive definition, which is people-based as applicable in research and exhibitions. Today, fine arts elements have specific constitutions which make them applicable even in the field of computer security, which is ruled by highly security personnel, who seek innovative usable secure forms to secure very sensitive systems.

As users increasingly rely on computer and networking systems for business, personal finance, and investment, coupled with the potential for anonymity afforded by electronic payment systems, fraud through identity theft have become a greater threat. Identity theft which as posited by Paget (2007) is a criminal means of falsifying the identifying information of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable state or local law. Identity theft takes many forms and may be motivated by a desire to steal money, identities, and other secrets for personal gain. Some identity attackers break into applications or operating systems just to show that they can do it—nevertheless, they can cause considerable damage. Because attacks can be automated and replicated, any weakness, no matter how slight, can be exploited (Beardsley, 2005).

According to NCPC (2005), identity theft has a significant negative impact on system users, organizations and the nation. Users whose identities have been stolen can spend months or

years – and thousands of naira – cleaning up the chaos the attackers have made of a good reputation and credit record. Some victims spent an average of 30 hours at a cost of $500 cleaning up after an identity crime. Thus for victims, the cost extends beyond financial losses to non-financial, which include time and reputation, corruption of personal information in corporate and government databases and wrongful arrest; the list goes on and on (Egwali and Odafe, 2012).

Humiliation, anger, and frustration are among the feelings victims experience as they navigate the process of rescuing their identity. The effect of identity attack is so disturbing to individuals, affected organizations and the country in general that there is significant underreporting of the crime. It is, therefore, important to promote practices that can proactively help prevent users' identities. It will be beneficial to protect users by enhancing the authentication model employed in computer systems (Egwali and Odafe, 2012). Identity theft is a growing problem, for the year 2005 had an increase of 890,066, the year 2007 had 1,050,229, at the year 2009 it has an increase of 4,223,370 and still continues to grow (Identity Theft, 2005; Moore and Clayton, 2007; Chiasson, 2009; Egwali and Onibere, 2016).

To secure systems, Paget (2007) recommended both technical and organizational methods to safeguard users' identities, which includes reinforcing user authentication procedures. FDIC (2004) also hypothesize user authentication as a major mitigating technologies. Authentication is the most prevalent approach to reducing the impact of sensitive data compromise and is a key area in security research, which is the determination of whether a user should be allowed access to a given system or resource.

According to Alireza and Angelos (2008), irrespective of the authentication model deployed, it should be adequate to protect against existing attacks and new threats. Wiki (2008) defined authentication in computer security as the process of attempting to verify the digital identity of the sender of a communication such as a request to log in. The sender or principal being authenticated may be a user operating a computer, a computer itself or a computer program.

The most prevalent form of authentication to gain access to computing systems today is via the textual password (TP) models. Some major strengths of the TP are its collectability, cost effectiveness, portability, scalability and it is generally accepted for users are willing to accept the model in their daily lives. Nonetheless TP models have been plagued with usability and security problems. Some security experts have referred to humans as the weakest link in the security chain, because of their inability and/or unwillingness to comply with security protocols (Sasse, et. al., 2001). TP are expected to comply with the following two conflicting protocols (Birget, et al., 2005; Wiedenbeck, et al., 2005; Onibere and Egwali, 2010): (i) passwords should be easy to remember, and the user authentication protocol should be executable quickly and easily by humans; passwords should be secure (i.e., they should look random and should be hard to guess); (ii) they should be changed frequently, and should be different on different accounts of the same user; they should not be written down or stored in plain text.

Adhering to these protocols while choosing and using textual passwords (TPs) are a challenge to humans partly due to the fact that today's users often reuse the same password at many different sites (Corin, et al., 2007; Warsaw, 2003). Under usability studies, findings from earlier studies on TP selection, memorability and usability, conclude that people choose poor TP (Ahmet, et al., 2005; Birget, et al., 2005). A variety of studies (Onibere and Egwali, 2006a) further cited the lack of entropy in users TPs. Users also tend to choose short TP and derive them from personal information that is easily guessable. Users also manage many TPx (Sasse, et al., 2001; Brown, et al., 2004). Moreover, users are unwilling or unable to retain passwords with a large amount of entropy. Consequently users TPs have drawbacks from a usability standpoint, and these usability problems translate directly into security problems which lead to the development and attraction recognition-based graphical password models (RGPM).

RGPM have been introduced as a means to authentication users because they aid users to overcome some of the TP memorability and usability challenges. Artforms embedded in RGPM can be regarded as a medium of artistic expression (Farlex, 2016), and have been used extensively as authenticated proofs and identities (Poole and Le-Phat, 2011). However, users' choices of good or bad passwords are based on the aesthetics available in RGPM images to aid their understanding. Aesthetics, which is the set

of principle concerned with the qualities of appearance, visual appeal, good taste, and beauty and the rules that determine how beautiful or pleasing to the eye an entity is. Aesthetic principles include balance, contrast, emphasis, form, harmony, line, movement, pattern, plane, point, proportion, rhythm, shape, style, texture, value and variety. The implication is that design choices need to be carefully considered when making usability and security-related modifications to RGPM artforms.

RELATED WORKS

A number of studies have been conducted by different researchers on RGPM from the user interface domain. Valentine (1998) conducted a study on PassFaces model utilizing 77 users and discovered that by the third attempt for various intervals of time, which was up to 5 months, login success rate was 72% to 100%. Perrig and Song (1999) conducted a study on Déjà Vu to ascertain its security strength. It was discovered that can counter social engineering attacks due to the use of hash visualization with non-describable abstract images. Déjà Vu usability strength is established from a study conducted, which involves 20 participants (Dhamija and Perrig (2000). Results shows that the password creation time was efficient, for password creation took an average of 45 seconds. The login success rate was 100%. After a week, the success rate was 90% compared to 70% realized with the same group using textual passwords.

Suo, et al. (2005) also carried out a study on Déjà Vu Some and asserted that the password space of textual passwords is much larger than Déjà Vu, consequently, it could not counter guessibility and brute force attacks. It employed a password space of N!/K!(N-K)! (N denotes total set of images and K subset for authentication).

Specifically, a password space has $\binom{N}{M}$ passwords, with N = 25 images in the panel, and M = 5 user password portfolio images. This yields a 53130 ≈ 2^{16} password space with a search time less than 0.5 seconds (Schneier, 1999).

Tari, et al., (2006) compared shoulder-surfing risks between PassFaces, text passwords, and PINs in a lab study and found that because PassFaces used keypad entry rather than a mouse, it was significantly less vulnerable than even text passwords or PINs. It was asserted that if PassFaces uses a keyboard for password entry, then malware attacks would need both a key-logger and screen scraping software to gain enough knowledge for password entry; with regular mouse entry, only a screen scraper was necessary.

Brostoff and Sasse (2003) conducted a study on PassFaces (Real User Corporation, 2001) using 34 users, and found mixed results. They posited that Passfaces password is easier to remember than alphanumeric passwords. Brostoff and Sasse (2003) posits from a user study that PassFaces had only a third of the login failure rate of textual passwords, with about a third the frequency of use. In another study by Dunphy et. al., (2008) on PassFaces using eye-gaze as input in a simulated system (Gong, et al., 1993, Govindarajulu and Madhvanath, 2007), after initial “play” and “enrollment” phases, they found that participants improved in their ability to enter their passwords over time and that login took an average of 20 seconds for passwords consisting of 5 panels of 9 faces.

Valentine (1998) conducted a study on PassFaces model utilizing 77 users and discovered that by the third attempt for various intervals of time, which was up to 5 months, login success rate was 72% to 100%. Brostoff and Sasse (2003) posits from a user study that PassFaces had only a third of the login failure rate of textual passwords, with about a third the frequency of use. Everitt et al. (2009) evaluated PassFaces for multiple password interference in a 5-week study where users received email prompts asking them to log on to 4 different fictitious “accounts” according to different schedules. Those who logged in more frequently and those who practiced each new password individually for several days in succession were more successful at remembering their passwords.

Davis, et al. (2004) conducted a user study on Story and Face (Davis, et al., 2004) models where a panel contained 9 images and a user's password consisted of a sequence of 4 images selected from within this panel. Story passwords had 85% success rate. Participants revealed that they were unlikely to have formulated a story as a memory aid, despite the designers’ intentions; which explains the high number of ordering errors. It was also discovered that the Story model were more varied but still displayed

exploitable patterns based on users choices, indicating that it is likely possible to build an attack dictionary that accounts for these preferences such as differences between male and female choices.

Weinshall and Kirkpatrick (2004) conducted a user study with 9 participants on their model and records a 95% overall login success rate with a good login time of 1.5 to 3 minutes on average. Password creation took 90 seconds to 180 seconds, with users logging on over a period of 10 weeks. Users receive system-assigned portfolios of images and receive extensive training to initially memorize their portfolio since it includes a large number of images (approximately 100), but no times were reported for this initial training phase.

The aforementioned literature summarized, shows that there is an interest in investigating users' perceptions of RGPM as it relates to security and usability issues. However, there is a dearth of sty relating to aesthetics assessment of RGPM.

MATERIALS AND METHODS

The main aim of this study is to evaluate the aesthetic nature of some existing RGPM. The user interface domains of eleven RGPM were uploaded in the website *Info Hub & Center* which can be accessible to respondents at: *http://secure-shield.com*.

The questionnaire is composed of two parts; the first part contains the demographic profile of participants including gender, category, Time spent online and faculties. The second part aims to measure the aesthetic level of twelve RGPM and has standardized 68 statement questionnaires which was categorized into seventeen aesthetic factors namely: balance, contrast, emphasis, form, harmony, line, movement, pattern, plane, point, proportion, rhythm, shape, style, texture, value and variety using a four-point Likert scale ranging from 'strongly disagree = 1' to 'strongly agree = 4'. The questionnaire assesses the website users' perception by asking participants to navigate though the RGPM model interfaces evaluate their aesthetics values and then complete the questionnaire.

Research Model

The website Info Hub & Center which can be accessed at: *http://secure-shield.com*, was uploaded and made assessable to users. The research model consists of independent variable (RGPM artforms) and dependent variable (aesthetic factors). The independent variables includes Déjà Vu (Dhamija and Perrig, 2000), Story (Davis, et al., 2004), Face (Davis, et al., 2004), Hong, et al. (2004) shoulder surfing resistant model, Man, et al. (2003) model, Jansen, et al. (2003) model for mobile devices, Kimwele, et al. (2010) colored graphical passwords model, Passface (Real User Corporation, 2001), Sobrado and Birget (2002) model, Takada and Koike (2003) model, Weinshall Cognitive Authentication Model (Weinshall and Kirkpatrick, 2004) and Bring-Your-Own-Picture (Bianchi, et al., 2015).

The following defined aesthetic factors serve as a guide for evaluating the aesthetic level of RGPM:

Balance: There are three main kinds of visual balance:

- radial, where the design elements radiate out from a center, as in the petals of a daisy or the face of a clock;
- formal (or symmetrical), where the design on one side of a center line is identical to the other side, as in the front view of an animal or a chair;
- informal (or asymmetrical), where the elements of a design are distributed unequally, as in the side view of a teapot.

Contrast: Contrast, the opposite quality to harmony, involves the use of opposing elements, such as clashing colors and shapes, in the same design. Contrast in a design may be more appropriate for a stimulating environment or when impact is wanted, such as in many advertising layouts.

Emphasis: Emphasis refers to placing greater attention to certain areas or objects in a piece of work. It can be created through sudden and abrupt changes in opposing elements. (Example: bright yellow dot in large black area)

Form: Refers to an object's shape and surface qualities giving a 3-dimensional aspect to the object. Examples of surface qualities relate to the materiality; color, texture and finish of the object.

Harmony: A harmonious design is one in which its different elements are in unity with each other for example, its colors may blend together well.

Line: An object with strong "visual movement" tends to be shaped in a way that draws the eye in a certain direction. Its shape or shapes may be asymmetrical, flowing, or dynamic. Objects with less visual movement tend to have more static and symmetrical shapes.

Movement: Refers to the arrangement of parts in a work of art to create a slow to fast action of the eye.

Pattern: A pattern is a repeated design element. Patterns are found on many plants and animals, in nature (for example, leaves and tabby cats) as well as on manufactured products, such as fabrics and wall and floor coverings.

Plane: This is a flat, two-dimensional surface that extends infinitely far. A plane is the two-dimensional analogue of a point (zero dimensions), a line (one dimension) and three-dimensional space. Planes can arise as subspaces of some higher-dimensional space, as with a room's walls extended infinitely far.

Point: This is an entity that has a location in space or on a plane, but has no extent; more generally, an element of some abstract topological space.

Proportion: Proportion has to do with the relationship between different parts of an object or its component pieces (or between those parts and the object as a whole). The proportions of an object made to be used, such as a teapot or a jug may have a functional as well as an aesthetic purpose.

Rhythm: This is related to pattern in that it uses repeating elements, but they may have a stronger quality of movement and be in the form of sequences or series.

Shape: It refers to an object's two-dimensional qualities, anything that has height and width. Shapes define objects, attract attention, communicate ideas and add excitement.

Style: Style is ever-changing and is often subjective. What may be considered ugly or gauche one year may be the height of fashion the next.

Texture: The look and feel of a surface, adds richness and dimension, emphasizes and suggests mood or feeling.

Value: An element of art which refers to the lightness or darkness of a color or tone in a work of art. A full range of values creates the illusion of three dimensions in a two-dimensional work. It also refers to shadows from lightness to darkness.

Variety: It is achieved through diversity and change using different line types, colors, textures and shapes.

Evaluation Metrics

To evaluate the aesthetic level of RGPM from the perspective of students, responses were evaluated according to the following merit point adapted from Webuse evaluation technique which was basically designed to evaluate the usability of websites by means of questionnaire (Priyandari, et al., 2009). The merit values are assigned to participants responses in the following format: 'Strongly Disagree= 1.00', 'Disagree = 2.00', 'Agree = 3.00' and 'Strongly Agree = 4.00'.

The aesthetic point for a factor x, is defined as:

$$x = [\Sigma \text{ (Merit for each question of the factor)}] / [\text{number of questions}]$$

The aesthetic level of the RGPM artforms were determined by using the corresponding merit values from 1.00 to 4.00. The greater the value, the better the aesthetic value from the respondents whereas the lower the value determined lower aesthetic value. Table 1 shows the aesthetic points and the corresponding level for each point. The overall RGPM artforms is the mean value of aesthetic quality points and levels for the 17 factors.

Table 1: Aesthetic Quality Points and Levels.

x (Aesthetic Point)	Aesthetic Level
0 < x < 1.7	Bad
1.7 < x < 2.4	Poor
2.4 < x < 3.5	Good
3.5 < x < 4.0	Excellent

Research Hypotheses

The research predicts that there is significant difference in the aesthetic values of the various RGPM, with the following hypothesis:

H_0: There is no significant difference in the aesthetic values of the various RGPM.

H_1: There is significant difference in the aesthetic values of the various RGPM.

Reliability Analysis

A pilot study was carried out on 50 respondents and the data gathered through the questionnaires were analyzed based on simple statistical techniques using SPSS 17 and Excel. The Cronbach's Alpha value of the questionnaire obtained from the pilot study is 0.851, while the Cronbach's alpha based on standardized Items is 0.877 for 9 items. Ambiguities identified in the pilot study were addressed and minor corrections effected.

Sample Selection

A total of 107 accounts of participants who accessed the site and answered the questionnaire satisfactorily were utilized. The participants in this study were undergraduate and postgraduate fine art students from nine randomly selected institutions in Nigeria: Delta State University, Abraka, Ambrose Alli University, Anambra State University, Bayero University, Federal University of Technology Akure, University of Benin, University of Nigeria, Nsukka, University of Port Harcourt and Cross River State University of Technology. This aim is achieved by using a questionnaire based on the seventeen aesthetic factors of artforms.

RESULTS AND DISCUSSION

Out of the 107 whose questionnaires were accepted, a total number of 69 were 64% are male and 36% were female. 62.3% were undergraduate students and 37.7% were postgraduate students from nine faculties. The summary of the aesthetics evaluation results of the seventeen RGPM aesthetic evaluation of the RGPM is shown in Table 2 and depicted graphically in Figure 1.

Table 2: Aesthetics Evaluation Results of RGPM.

S/N	Factors	Point	Aesthetic Level
1.	Balance	2.454	Good
2.	Contrast	3.698	Excellent
3.	Emphasis	3.540	Excellent
4.	Form	2.459	Good
5.	Harmony	2.427	Good
6.	Line	3.787	Excellent
7.	Movement	2.059	Poor
8.	Pattern	2.122	Poor
9.	Plane	2.407	Good
10.	Point	2.425	Good
11.	Proportion	2.645	Good
12.	Rhythm	2.337	Poor
13.	Shape	3.524	Excellent
14.	Style	2.483	Good
15.	Texture	2.438	Good
16.	Value	2.654	Good
17.	Variety	2.552	Good
Overall Aesthetic Value		2.707	Good

RGPM artforms obtained excellent aesthetic levels in contrast, emphasis line and shape; and good aesthetic level in balance, form,

harmony, plane, point, proportion, style, texture, value and variety. However, movement, pattern and rhythm are poor. Despite the varied factor levels, interestingly the overall aesthetic mean value for the RGPM is 2.707, which is Good on the aesthetic level scale.

CONCLUSION

Over the years, since the adoption of RGPM as authenticated proofs and identities, the aesthetic value of embedded artforms have not been evaluated in order to determine how users' choices of good or bad passwords are heavily influenced by the design of the artforms embedded in these RGPM.

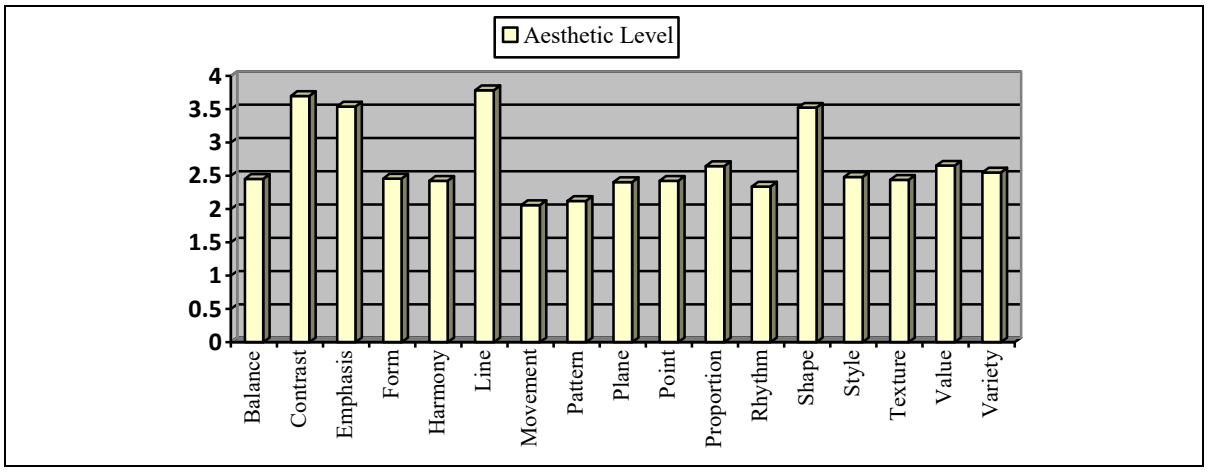

Figure 1: Graphical Representation of the Aesthetics Evaluation Results of RGPM.

This study evaluated the aesthetic nature of twelve existing RGPM artforms using a questionnaire based on the following seventeen aesthetic factors of artforms: balance, contrast, emphasis, form, harmony, line, movement, pattern, plane, point, proportion, rhythm, shape, style, texture, value and variety. The results identify the aesthetic factors that need to be given more consideration when designing RGPM and shows that generally the aesthetic value of RGPM is good when viewed from user's perspective. However, for future work, it will be beneficial to analyze RGPM from other domains and perspectives apart from the direction in existing literature.

REFERENCES

1. Ahmet, E.D., M. Nasir, and J. Birget. 2005. "Modelling User Choice in the PassPoints Graphical Password Scheme". *Proc. Human-Computer Interaction International*.

2. Alireza, P. and S. Angelos. 2008. "Universal Multi-Factor Authentication Using Graphical Passwords". Available at: www.computer.org/portal/web/csdl/doi/10.1109/SITIS.2008.92

3. Beardsley, T. 2005. "Phishing Detection and Prevention Practical Counter-Fraud Solutions". Available at: http://www.planb-security.net/wp/503167-001_PhishingDetectionandPrevention.pdf

4. Bianchi, A., I. Oakley, and H. Kim. 2015. "PassBYOP: Bring Your Own Picture for Securing Graphical Passwords". Available at: http://alsoplantsfly.com/files/2016/Bianchi_Passbyop_IEEE16.pdf

5. Birget, J., D. Hong. and N. Memon. 2005. "Graphical Passwords Based on Robust Discretization". Available at: clam.rutgers.edu/~birget/grPssw/robDiscr.pdf

6. Brostoff, S. and M.A. Sasse. 2003. "Ten Strikes and You're Out: Increasing the Number of Login Attempts can Improve Password Usability". CHI 2003 Workshop on Human-Computer Interaction and Security Systems, Ft. Lauderdale, FL.

7. Brown, A.S., E. Bracken, S. Zoccoli, and K. Douglas. 2004. "Generating and Remembering Passwords". *Applied Cognitive Psychology*. 18(6): 641- 651.

8. Chiasson, S. 2009. "Usable Authentication and Click-based Graphical Passwords". Available at: gradworks.umi.com/NR/47/NR47475.html

9. Corin, R., S. Malladi, J. Alves-Foss, and S. Etalle. 2007. "Guess What? Here is a New Tool that Finds Some New Guessing Attacks (extended abstract)". In: R. Gorrieri and R. Lucchi, editors, IFIP WG 1.7 and ACM SIGPLAN Workshop on Issues in the Theory of Security (WITS), 62–71.

10. Davis, D., F. Monrose, and M.K. Reiter. 2004. "On User Choice in Graphical Password Schemes". Thirteenth Usenix Security Symposium. San Diego, CA. Available at: http://www.usenix.org/events/sec04/tech/davis.html.

11. Dhamija, R. and A. Perrig. 2000. "Deja Vu: A User Study Using Images for Authentication". *Proceedings of 9th USENIX Security Symposium.*, Denver, CO. 45–58. Available at: http://www.usenix.org/publications/library/proceedings/sec2000/dhamija.html.

12. Dunphy, P., J. Nicholson, and P. Olivier. 2008. "Securing Passfaces for Description". In: 4th Symposium on Usable Privacy and Security (SOUPS), July 2008.

13. Egwali, A.O. and E.N. Odafe. 2012. "A Multipurpose Authentication Model for Distance Learning Online Assessment". *Progressio: South African Journal for Open and Distance Learning Practice*. 34(1): 100 – 112.

14. Egwali, A.O. and E.A. Onibere. 2016. "Users Interference from Multimodal Authentication Models". *University of Benin Journal of Science and Technology*. 4(1): 13 – 28.

15. Everitt, K., T. Bragin, J. Fogarty, and T. Fogarty. 2009. "A Comprehensive Study of Frequency, Interference, and Training of Multiple Graphical Passwords". In: ACM Conference on Human Factors in Computing Systems (CHI).

16. Farlex. 2016. "Art Form". *The Free Dictionary*. Available at: http://www.thefreedictionary.com/art+form

17. FDIC. 2004. "Putting an End to Account-Hijacking Identity Theft". Available at: http://www.fdic.gov/consumers/ consumer/idtheftstudy/identity_theft.pdf

18. FTC. 2005. "Identity Theft: Focus of National Consumer Protection Week 2005". Available at: http://www.ftc.gov/opa/2005/02/ncpw05.htm

19. Gong, L., T. Mark, A. Lomas, M. Needham, and J. Saltzer. 1993. "Protecting Poorly Chosen Secrets from Guessing Attacks". *IEEE Journal on Selected Areas in Communications*. 11(5): 648–656.

20. Govindarajulu, N. and S. Madhvanath. 2007. "Password Management using Doodles". In: 9th International Conference on Multimodal Interfaces (ICMI), November 2007.

21. Hong, D., S. Man, B. Hawes, and M. Mathews. 2004. "A Password Scheme Strongly Resistant to Spyware". *Proceedings of International Conference on Security and Management*. Las Vergas, NV.

22. Jansen, W., S. Gavrila, V. Korolev, R. Ayers, and R. Swanstrom. 2003. "Picture Password: A Visual Login Technique for Mobile Device". Available at: http://csrc.nist.gov/publications/nistir/nistir-7030.pdf.

23. Kimwele, M., W. Mwangi, and S. Kimani. 2010. "Strengths of a Colored Graphical Password Scheme". Available at: www.ijric.org/volumes/Vol4/7Vol4.pdf

24. Man, S., D. Hong, and M. Mathews. 2003. "A Shouldersurfing Resistant Graphical Password Scheme". *Proceedings of International Conference on Security and Management*. Las Vegas, NV.

25. Moore, T. and R. Clayton. 2007. "An Empirical Analysis of the Current State of Phishing Attack and Defense". *International Journal of Information Security*. 1(1):69–83. Available at: http://www.cl.cam.ac.uk/ twm29/weis07-phishing.pdf.

26. NCPC. 2005. "Preventing Identity Theft. A Guide for Consumers". Available at: http://www.ncpc.org/cms-upload/prevent/files/IDtheftrev.pdf

27. Onibere, E.A. and A.O. Egwali. 2006. "Modelling the Evaluation of Password Susceptibility in the Key-Pass Authentication Evaluation Model (KAES)". *Nigerian Journal of Computer Literacy*. 7(1): 205 – 214.

28. Onibere, E.A. and A.O. Egwali. 2010. "An Empirical Analysis of Regular and Mnemonic Passwords". *Nigerian Journal of Applied Science*.

29. Paget, F. 2007. "Identity Theft". Available at: http://www.pubblicaamministrazione.net/file/whitepaper/000042.pdf

30. Pallud, J. and D. Straub. 2014. "Effective Website Design for Experience-Influenced Environments: The Case of High Culture Museums". *Information & Management*. 51(3):359 - 373.

31. Perrig, A. and D. Song. 1999. "Hash Visualization: A New Technique to Improve Real World Security". In: International Workshop on Cryptographic Techniques and E-Commerce. 131–138.

32. Poole, D. and S. Le-Phat. 2011. "Digital Transitions and the Impact of New Technology On the Arts". *The Canadian Public Arts Funders (CPAF) Network*.

33. Priyandari, Y., I. Iftadi, and S. Fitriawan. 2009. "Redesigning Website by Considering the Usability Aspects Using Participatory Design". In: 3rd International Seminar on Industrial Engineering and Management. Bali, Indonesia.

34. Real User Corporation. 2001. "The Science Behind Passfaces, Document Revision 2". Real User Corporation, September 2001, <URL: Available at: http://www.realuser.com/published/ScienceBehindPassfaces.pdf

35. Sasse, M.A., S. Brostoff, and D. Weirich. 2001. "Transforming the 'Weakest Link' – A Human/Computer Interaction Approach to Usable and Effective Security". *BT Technical Journal*. 19:122-131.

36. Schneier, B. 1999. “Inside Risks: The Uses and Abuses of Biometrics”. *Communications of the ACM*. 42(8).

37. Sobrado, L. and J.C. Birget. 2002. “Graphical Passwords”. *The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research*. 4: 12-18.

38. Suo, X., Y. Zhu, and G.S. Owen. 2005. “Graphical Passwords: A Survey”. 21st Annual Computer Security Applications Conference (ACSAC'05). 463-472.

39. Takada, T. and H. Koike. 2003. "Awase-E: Image-based Authentication for Mobile Phones using User’s Favorite Images". *Human-Computer Interaction with Mobile Devices and Services*. 2795: 347 – 351.

40. Tari, F., A. Ozok, and S. Holden. 2006. “A Comparison of Perceived and Real Shoulder-Surfing Risks Between Alphanumeric and Graphical Passwords”. *Proceedings of the Second Symposium on Usable Privacy and Security*. Pittsburgh, PA. July 12 – 14, 2006), SOUPS’06, vol 149. ACM, New York, NY, 56 – 66.

41. Valentine, T. 1998. “An Evaluation of the Passface Personal Authentic System. Technical Report. Goldsmiths College University of London: London, UK.

42. Warsaw, P. 2003. Dipartamento di Scienze dell’Informazione Universita di Bologna, Italy. Available at: http://www.cra.org/deivities/hrand.challenghs/securiky/home

43. Weinshall, D. and S. Kirkpatrick. 2004. “Passwords You’ll Never Forget but Can’t Recall”. *Proceedings of Conference on Human Factors in Computing Systems (CHI)*. ACM: Vienna, Austria. 1399-1402.

44. Wiedenbeck, S., J. Waters, J.C. Birget, A. Brodskiy, and N. Memon. 2005. “PassPoints: Design and Longitudinal Evaluation of a Graphical Password System”. *International Journal of Human-Computer Studies*. 63: 102-127.

45. Wikipedia. 2008. “Authentication”. Available at: http://en.wikipedia.org/wiki/Wikipedia: Authentication.

ABOUT THE AUTHORS

Professor (Mrs.) Egwali, Annie Oghenerukevbe, is a Professor of Cyber Security in the Department of Computer Science, Faculty of Physical Sciences. University of Benin, Benin City. Nigeria. Her area of interests includes Network Security, E-commerce, Electronic Marketing and Information Technology, Software Engineering. To date, she has supervised several undergraduate and postgraduate students. She is a member of International Network for Women Engineers and Scientists (INWES), Nigerian Computer Society (NCS) and Third World Organizations of Women Scientists (TWOWS).

Ass. Professor Egwali, Chu Franklyn is an Associate Professor of Sculpture and Environmental Arts at the Department of Fine and Applied Arts of the University of Benin, Nigeria. He holds a BA, MFA degrees in Fine Arts, University of Benin, specializing in Sculpture, Egwali also holds an MA in Art History, Abraka and Ph.D. in Visual Arts from the University of Benin. To date, he has supervised several undergraduate and postgraduate students and has participated in numerous art exhibitions and attended several conferences in the Visual Arts, within Nigeria and internationally.

SUGGESTED CITATION

Egwali, A.O. and F.C. Egwali. 2020. “Aesthetic Evaluation of Artforms in RGPM: User’s Perspective”. *Pacific Journal of Science and Technology*. 21(2): 181-189.

Pacific Journal of Science and Technology