An Appraisal of Artform as Usable Design Elements of RGPM

Franklyn Egwali, Ph.D.[1]; Annie Egwali, Ph.D.[2*]; and John Ogene, Ph.D.[1]

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

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

ABSTRACT

One application area of artforms is in recognition-based graphical password models (RGPM) found in the user authentication domain of computer systems and handheld devices. This paper studies the correlating artistic design elements of artforms and usable design elements of RGPM in computer security. The probability of occurrence of each correlating element was used to establish some RGPM level of efficacy and deviation from standardized artform design principles. Finally, each model's probability efficacy is ranked and compared with existing ranking based on usable design characteristics of RGPM in computer security. Results show that two models, the Color Password Model and Shield-2 Model performed above average with Shield-2 having a probability of 91% efficiency which is 27% improvement over previous models with high efficacy. Furthermore, this result from an artistic perspective, support past research studies from security and usability perspectives. This shows that there is a correlation between artforms in the art domain and RGPM artforms in computer security.

(Keywords: artform, security, graphical password, design elements, authenticate)

INTRODUCTION

An artform is defined as an activity or the specific shape, or quality of a piece of artistic expression. An artform is often influenced by the media used, that is its formal qualities (i.e., the constraints and limitations of the medium used) which determines its form that does not relate to the objectives of the artist or the audience feedbacks of the audience (Farlex, 2016). Two main design principles: Aesthetics and Function embedded in an artform, has a direct effect on intended users and viewers.

Aesthetics contains rules that define the beauty or attractiveness of an entity to the eye. It comprises qualities relating to the appearance, taste, beauty and visual appeal. Its design characteristics which include shape, pattern, texture, color, proportion, rhythm, form, style, finish, point, line, plane, harmony, contrast, balance and movement (New Zealand Qualifications Authority, 2016).

Function deals with the purpose and use of a work of art (SPARKed, 2014). It addresses how an artform performs for its intended use or user. Functional characteristics include safety, strength, efficiency, stability, durability, cost, fitness for purpose, reliability, construction, user-friendliness, and optimization. Over the years artforms have played significant role in different fields and technologies: in forensic studies, social networks, law enforcement, e-books publishing, gaming, social media, film and video production and in securing systems, where artforms in form of images are used as authenticated proofs and identities (Poole and Le-Phat, 2011).

To authenticate into computer systems in a secured way, users are to comply with two fundamental requirements, namely (a) created passwords should be easy to remember and (b) passwords should be secure (Birget, et al., 2005; Wiedenbeck, et al., 2005). Although ubiquitous, textual passwords have lots of drawbacks from a usability perspective. This has resulted in the proposal and deployment of several other authentication models. A major authentication model presently found in computer systems and handheld devices is the graphical password model that have been proposed as a possible alternative to textual passwords, motivated partially by the fact that humans can remember pictures better than text.

Graphical password models make use of diverse composition of artform interfaces that may have a positive or negative effect on user's ability to remember their generated passwords. This may or may not users meet up with the two fundamental authentication model requirements. Xiaoyuan (2006) asserted that the main design issue for recognition-based models are how to make it easier for users to remember and recognize the artforms. While that of recall-based methods is the reliability and accuracy of user input recognition. This study focuses on recognition-based graphical password models (RGPM) because several studies show that the login success rates for recognition-based models ranged from 90 to 100% (Real User Corporation, 2001; Valentine, 1998; Brosto and Sasse, 2000; Tari, et al., 2006), while for recall-based models, it ranged from 55 to 90% (Wiedenbeck, et al., 2005; Birget, et al., 2005). Studies further revealed that user acceptance level for recognition-based models are higher because of the level of satisfaction (Suo, et al., 2005).

It was also asserted that allowing users to choose their own artforms may lead to high memorability, but at the same time may result in artforms with poor security characteristics (Wiedenbeck, et al., 2005a). However, we posit that the design nature of recognition-based graphical models has an enormous direct effect on a system security level even within the context of 'secure human behaviors'. Presently, there is a dearth of research in this area of study. To establish our assertion, the design principles of artforms were correlated with that of recognition-based graphical models and the focus was on related design principles.

RGPM

Authentication in computer security is defined 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 (Wiki, 2008). According to Alireza and Angelos (2008), irrespective of the authentication model deployed, it should be usable and secure enough to protect the user against existing attacks and new threats. Many choices exist for authenticating users into secure computing systems one of which is the RGPM which present as grids, artforms of everyday natural scenes that include artforms, icons, written signature and symbols. This characteristic according to Picture Superiority Effect Theory (Nelson, et. al., 1976) makes graphical concepts more likely to be recognized and remembered than words. Results from a user study showed that 90% of all participants using graphic password models succeeded in the authentication using this technique, while only 70% succeeded using text-based passwords and PINS (Perrig and Song, 1999).

Also, Psychological studies that are well researched and documented posit that the human brain has the ability to process and recall imagery far more than the ability to remember text (Dhamija and Perrig 2000; Sobrado and Birget, 2002). Other psychological researches on artforms have shown that people can remember detailed visual information in natural scenes (Miller, 1996) and that the content, effect, and coherent organization of art pieces influence the ability to remember an art shape (Bradley, et al., 2000; Mandler and Ritchey 1977; Biederman, et al., 1973). Although the user still has to remember a certain combination, the likelihood of forgetting passwords and needing to write them down is eliminated (Wiedenbeck, et al., 2005).

MATERIALS AND METHODS

To analyze the effect of artforms in computer security, two studies are carried out: (1) a quantitative approach on literature was employed to derive the corpus of design element of artforms that relates to usable design RGPMs characteristics metrics. (2) Using these design elements as a scale, an evaluation of the efficacy of the artforms on each RGPM under study is performed using probability semantics. We denote the fact that a design element is evident in a model by one (1) or zero (0), otherwise. (3) Finally each model's probability efficacy is ranked and compared with existing ranking based on usability and security characteristics (Onibere and Egwali, 2011).

RESULTS AND DISCUSSION

Table 1 shows the quantitative approach on literature, employed to derive the corpus of design element of artforms that relates to graphical password models usability and design characteristics metrics.

Table 1: Common Design Element that Relates Artforms and Computer Security Design Characteristics.

Generic Art Form			Graphical Password Artforms		
Design Principles	**Definition**	**Related Elements**		**Definition**	**Characteristic Metrics**
		Element	**Element**		
Function (Collingwoo 1980; Kennick and Kennick, 1979)	The likelihood that a product or system will continue to do its job.	Reliability	Reliability	The likelihood that a product or system will continue to do its job.	**Usability** (Scheuermann et al., 2002; Behzad et al., 2008; De Angeli et al., 2005; Dhamija and Perrig, 2000; Wiedenbeck et al., 2005; Zhi et al., 2005; ISO, 2009)
	Describe how well a product works in the situation it was designed for and how well it meets the needs of its intended end-users.	Fitness for Purpose	Real Applicability	Describe how well a product works in the situation it was designed for.	
	The degree to which it is easy to use.	User-friendliness	User friendly	The degree to which it is easy to use.	
	Often used in relation to a situation where work is productive, with minimum wasted effort or expense.	Efficiency	Efficiency	Defined in terms of the system utilization in real world;	
	A balance between construction and its cost.	Cost	Cost-Effectiveness	There must be a balance between the cost of implementation and the security measures.	**Design** (Cornel de Jong (2008; Jansen et al., 2003, Jain et al., 1999; Clarke, 1994; Jain et al, 2004)
	Products, systems, and environments designed to as safe as is practically possible to use.	Safety	Safety	Systems designed to be as safe as possible to use.	
Aesthetics (New Zealand Qualifications Authority, 2016; Shiner, 2003; Zangwill, 999).	1. Symmetrical- formal, divided in half same 2. Asymmetrical- informal, divided in half not same 3. Radial- circular, design starts from center > out	Balance	Balance	1. Symmetrical- formal, divided in half same 2. Asymmetrical- informal, divided in half not same 3. Radial- circular, design	
	"Visual movement" - the arrangement of parts in a work of art to create a slow to fast action of the eye.	Movement	Randomization	Conveyable password interface	
	A pattern is a repeated design element.	Pattern	Pattern	Repeated design element.	
	Repeated objects in a regular or irregular rhythm:	Rhythm	Rhythm	Repeating elements in a sequences or series.	
	Emphasizing certain areas to stands out and get noticed first. Emphasis influences choices of colour, value, size shape etc.	Emphasis	Emphasis	Placing greater attention to certain areas or objects in a piece of work.	

Eleven elements and corresponding characteristics metrics were identified. Using the resultant corpus of elements as a scale, an evaluation of the efficacy of the artforms on each of the following recognition-based authentication model was performed.

Déjà Vu (Dhamija and Perrig, 2000) model is based on recognition of computer-generated art shapes (see Figure 1). They implemented the recognition-based model using hash visualization with non-describable abstract art piece. The login is accomplished in one round where the user simultaneously sees 15 artforms displayed on the screen, five of which are the user's password artforms and the remaining 20 are decoy artforms. To be authenticated the user must click on all five password artforms.

The reliability of the model is uncertain, for although it met its memorability standard, it did not satisfy all the usability issues and has cease to be in operation. Studies revealed that the process of selecting a set of pictures from the picture database was tedious and time consuming for users and that it did not fully counter the setbacks of textual passwords it intended to replace (Dhamija and Perrig, 2000; Suo, et al., 2005).

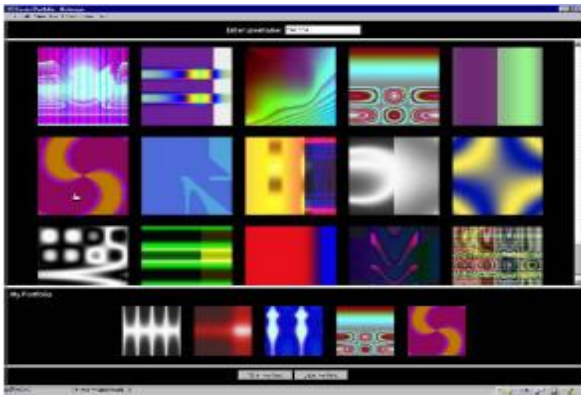


Figure 1: Deja Vu (Dhamija and Perrig, 2000)

However, the model was user-friendly. The system was efficient, for instance the password creation time took an average of 45 seconds and the login success rate was 100%. It was cost effective and safe to use. In terms of balance, it was asymmetrical, no pattern or regular rhythm and no emphasis was placed on certain areas to influence users' choices.

Figure 2: Passfaces Model.
(Real User Corporation, 2001)

Passfaces (Real User Corporation, 2001) consists of a 3x3 grid with nine faces (see Figure 2). To register, a user creates a password by choosing four artforms of human faces from a database of faces. To log in subsequently, the user observes a 3x3 grid with nine faces, consisting of one face previously chosen and eight faces acting as baits. The user must click on a previously recognized chosen face and repeat this process four times consecutively, by recognizing and clicking on the initial four faces selected to complete the authentication process. If all four faces are accurately identified, the system logs the user into the system. The reliability of the model is uncertain, users log in less frequently with the model than with textual passwords because the login process took too long. Brosto and Sasse (2000) conducted a study with 34 users and found mixed results. The model did serve it intended purpose. The model was user-friendly. The system was efficient for users made fewer login errors (95% success rate). It was cost effective and safe to use. In terms of balance, it was asymmetrical and there is no form of visual movement. No pattern or regular rhythm and no emphasis were placed on certain areas to influence users' choices.

Figure 3: Challenge-Response Model
(Man et al., 2003)

In Challenge-response Authentication Model (Man et al., 2003), to register, a user selects a number of artforms as pass-objects; each pass-object has several variants and each variant is assigned a set of unique codes (see Figure 3). During authentication, the user is challenged with several scenes. The pass-objects, which are randomly generated, are displayed on the screen with about 400 to 500 decoy objects. The user has to type in a string of textual characters with the unique codes corresponding to the pass-object variants present in the scene as well as a code indicating the relative location of the pass-objects in reference to a pair of eyes.

The model was not reliable. The log in process can be slow because distinguishing 3 or 4 objects from such an image set was cumbersome. Studies revealed that the model did serve it intended purpose. The model was not user-friendly, for it still requires users to memorize the alphanumeric code for each pass-object variant. For example, if there are 4 pictures each with 4 variants, then each user must memorize 16 codes. The system was efficient for users. It was cost effective and safe to use. In terms of balance, it was asymmetrical. There was visual

movement, for pass-objects were always randomly generated. There were no patterns or regular rhythm and no emphasis was placed on certain areas to influence users' choices.

Figure 4: Weinshall's (Weinshall and Kirkpatrick, 2004)

Weinshall Cognitive Authentication Model (Weinshall and Kirkpatrick, 2004) consists of a portfolio of artforms (see Figure 4). To register, a user must move through a screen from the top-left corner of the panel of artforms. If the user stands on a picture from his or her portfolio then they move down; otherwise they move right. When the bottom edge of the panel is reached, the user identifies the corresponding label for that row or column. The system then presents a multiple-choice question and expects the user to verify the label for the exact endpoint of the path. Later, the user performs several rounds of the same sequence of steps and the system verifies through cumulative probability that the users' answers were not based on chance. At the end of the rounds, the system authenticates the user if the cumulative choices from the round exceed the accepted threshold.

The model was very reliable for after three months, users in their study were still able to recognize over 90% of the artforms in the training. The model served it intended purpose. It was not user-friendly but was efficient for users**.** It was cost effective and safe to use. In terms of balance, it was asymmetrical. There was no form of visual movement. No pattern or regular rhythm and no emphasis was placed on certain areas to influence users' choices.

Figure 5: Picture Password (Jansen et al., 2003)

Picture Password for mobile devices (Jansen et al., 2003) consisted of predefined theme, such as 'seashore', 'kitten' and so on designed. To create a password, a user is required to select a predefined theme which consists of thumbnail photos. The user then selects a sequence of thumbnail photos as a password (see Figure 5). To gain entry to the system, the user needs to recognize and identify the thumbnail photos in the same order as in the registration stage. The model was very reliable, served it intended purpose and was user-friendly. The system was efficient for users. It was cost effective and safe to use. It was asymmetrical. There was no form of visual movement, pattern or regular rhythm. No emphasis was placed on certain areas to influence users' choices.

Figure 6: Story Model. (Davis et al, 2004).

In Story model (Davis et al., 2004) users select a sequence of artforms for their portfolio through storytelling. A panel had 9 artforms and a password involved selecting a sequence of 4 art shapes from this panel. To log in, users are presented with one panel of artforms and they must identify their portfolio art piece from among

decoys (see Figure 6). Artforms in their user study contained everyday objects, places, or people. The model was reliable, it served its intended purpose and was user-friendly. However, the model was not efficient for users as user choices displayed exploitable patterns such as differences between male and female choices. It was cost effective and safe to use. It was asymmetrical. There was no form of visual movement No pattern or regular rhythm and no emphasis was placed on certain areas to influence users' choices.

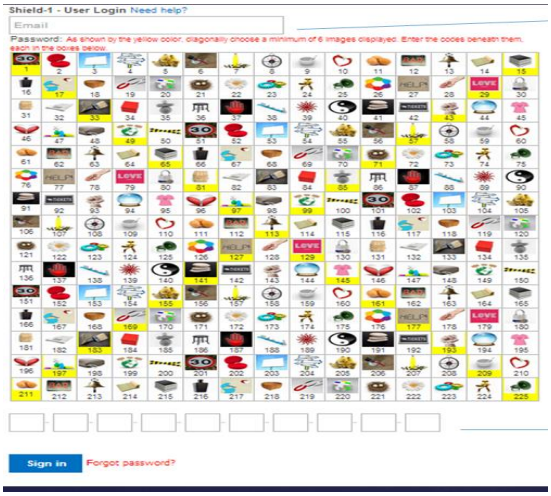
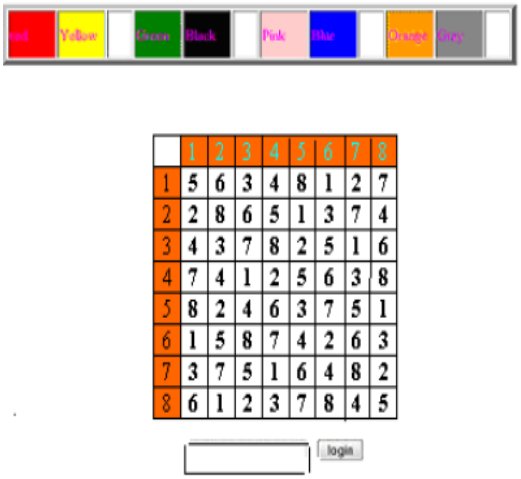


Figure 7: Shield-2 Model (Egwali and Onibere, 2015)

In Shield-2 Model (Egwali and Onibere, 2015) to register, a user must enter his/her full name, e-mail address and type into the available text boxes, artform codes from the artform set diagonally (see Figure 7). A user's password must not be less than six (6) and greater than ten (10). Subsequently to login, the same procedure as in the registration phase is followed. Results from a laboratory study of 31 and a field study revealed that the model was very reliable and served it intended purpose. It was user-friendly and efficient for users. It was cost effective and safe to use. In terms of balance, it was asymmetrical. There was a form of visual movement as artforms were randomly generated, each time the interface is uploaded. There were repeated design elements**,** regular rhythm and emphasis was placed on certain areas using color to influence users' choices.



	1	2	3	4	5	6	7	8
1	5	6	3	4	8	1	2	7
2	2	8	6	5	1	3	7	4
3	4	3	7	8	2	5	1	6
4	7	4	1	2	5	6	3	8
5	8	2	4	6	3	7	5	1
6	1	5	8	7	4	2	6	3
7	3	7	5	1	6	4	8	2
8	6	1	2	3	7	8	4	5

Figure 8: Color Password (Kimwele et al., 2010)

Kimwele et al., (2010) proposed a model which emphasizes on the use of colored graphical passwords as an alternative to textual passwords in order to aid users memory (see figure 8). The model was very reliable, served it intended purpose and was user-friendly. The system was efficient for users. It was cost effective and safe to use. It was asymmetrical. There was no form of visual movement. No pattern or regular rhythm and emphasis was placed on certain areas to influence users' choices.

Figure 9: Face Model. (Davis et al, 2004).

In Face model (Davis et al., 2004), the password is a collection of faces, each selected from a distinct set of n > 1 faces. To choose a password, four successive 3 × 3 grids containing randomly chosen images is displayed before the user who is expected to select one image from the grid as an element of his or her password.

During the authentication phase, the same sets of images are shown to the user, but with randomly permuted images. Displayed images are unique and do not appear more than once for a given user. The model was not very reliable, did not serve it intended purpose, and was not user-friendly. The system was not efficient for users. However, it was cost effective and safe to use. It was asymmetrical. There was no form of visual movement. No pattern or regular rhythm and no emphasis were placed on certain areas to influence users' choices.

The fact that a design elements / characteristic metric is evident in a model is denoted by one (1) and zero (0) otherwise as shown in Table 2. Using probability semantics, the level of efficiency of the individual authentication models under consideration is next determine.

Let ***Dc***=Total derives corpus of design elements / characteristics metrics,

Dv= Déjà Vu Model,

Pf = Passface Model,

CR= Challenge-Response Model,

MA = Multiple Authentication Models,

Pp= Picture Password Model,

Sm =Story Model,

S-2 = Shield-2 Model,

Cp = Color Password Model

and ***Fc*** = Face Model,.

Since ***Dc*** = 11

Probability of ***Dv*** is defined as: P(***Dv***) = $\frac{\text{Number of design elements in } Dv}{\text{Total derives corpus of design elements}} = \frac{4}{11} = 0.37$ (1)
with efficacy result of 37.0%

Similarly,

Probability of ***Pf*** is defined as: P(***Pf***) = $\frac{\text{Number of design elements in } Pf}{\text{Total derives corpus of design elements}} = \frac{5}{11} = 0.04$ (2)
with efficacy result of 4.0%

Probability of ***SR*** is defined as: P(***CR***) = $\frac{\text{Number of design elements in } SR}{\text{Total derives corpus of design elements}} = \frac{5}{11} = 0.04$ (3)
with efficacy result of 4.0%

Probability of ***MA*** is defined as: P(***MA***) = $\frac{\text{Number of design elements in } MA}{\text{Total derives corpus of design elements}} = \frac{5}{11} = 0.04$ (5)
with efficacy result of 4.0%

Probability of ***Pp*** is defined as: P(***Pp***) = $\frac{\text{Number of design elements in } Pp}{\text{Total derives corpus of design elements}} = \frac{6}{11} = 0.55$ (6)
with efficacy result of 55.0%

Probability of ***Sm*** is defined as: P(***Sm***) = $\frac{\text{Number of design elements in } Sm}{\text{Total derives corpus of design elements}} = \frac{5}{11} = 0.04$ (7)
with efficacy result of 4.0%

Probability of ***S-2***is defined as: P(***S-2***) = $\frac{\text{Number of design elements in } S-2}{\text{Total derives corpus of design elements}} = \frac{10}{11} = 0.91$(8)
with efficacy result of 91.0%.

Probability of ***Cp*** is defined as: P(***Cp***) = $\frac{\text{Number of design elements in } Cp}{\text{Total derives corpus of design elements}} = \frac{7}{11} = 0.64$ (9)
with efficacy result of 64.0%

Probability of ***Fc*** is defined as: P(***Fc***) = $\frac{\text{Number of design elements in } Sm}{\text{Total derives corpus of design elements}} = \frac{5}{11} = 0.04$ (10)
with efficacy result of 4.0%

The fact that a design elements / characteristic metric is evident in a model is denoted by one (1) and zero (0) otherwise as shown in Table 2.

It is evident that most recognition-based graphical passwords models fail to meet up with design standards from artistic, usability and memorability perspective. Due to the fact that most of these models depend on a subset of the entire design elements and characteristics, the overall performance of the system is affected. By isolating these design elements / characteristic metrics from an artistic point of view, the Color Password Model and Shield-2 Model performed above average with Shield-2 having a probability of 91% efficiency which is 27% improvement over past models with high efficacy.

Table 2: Design Elements Evaluation of Recognition-based Graphical Passwords Artforms.

S/N	Recognition-based Models	Re	Fp	Uf	Eff	C	S	B	M	P	R	E	Total
1.	Shield-2 Model	1	1	1	1	1	1	0	1	1	1	1	10
2.	Color Password Model	1	1	1	1	1	1	0	0	0	0	1	7
3.	Picture Password Model	1	1	1	1	1	1	0	0	0	0	0	6
4.	Story Model	1	1	1	0	1	1	0	0	0	0	0	5
5.	Multiple authentication Models	1	1	0	1	1	1	0	0	0	0	0	5
6.	Face Model	1	1	1	0	1	1	0	0	0	0	0	5
7.	Challenge-response Authentication Model	0	1	0	1	1	1	0	1	0	0	0	5
8.	Passfaces Model	0	1	1	1	1	1	0	0	0	0	0	5
9.	Déjà Vu Model	0	0	1	1	1	1	0	0	0	0	0	4

Where *Re* = Reliability, Fp = Fitness for Purpose, Uf = User-friendly, Eff = Efficient, C= Cost, S = Safety, B = Balance, M = Movement, P = Pattern, R = Rhythm and E = Emphasis

Table 3: Previous Evaluation of Recognition-based Graphical Passwords **(**Onibere and Egwali, 2011).

S/N	Recognition-Based Models	NI	EM	MU	TS	EU		EC	EL	CR	CI	RA	ReA	Total
						M	K							
1	Shield-2 (Egwali and Onibere, 2015)	1	1	1	1	1		1	1	1	1	1	1	11
2	Multiple authentication models.Weinshall & Kirkpatrick (2006)	1	0	1	1		1	1	1	1	1	1	0	9
3	Challenge-response Authentication (Man *et al.* 2003),	0	1	0	1		1	1	1	1	1	0	1	8
4	Story. Davis et al (10)	1	1	1	0	1		1	1	0	1	0	1	8
5	Face. Davis et al (10)	1	1	1	0	1		1	1	0	1	0	1	8
6	Passface (Real User Corporation, 2001; Dunphy, et. al., 2008; Tari, et. al., 2006)	1	1	0	1	1		1	1	0	0	1	0	7
7	Graphic Password. Sobrado and Birget (2002)	0	1	0	0	1		1	1	1	1	1	0	7
8	Déjà Vu. by Dhamija et al (2000)	0	0	0	1	1		1	1	0	0	1	0	5

Where *NI* = Nice Interface, *EM* = Easy to Memorize, *MU* = Meaningful (Understandable), *TS* = Training simple, *M* = Mouse, *K* = keyboard, *EC* = Easy to Create, *EU* = Easy to use, *EL* = Easy to Learn (Simple Steps), *CR* = Challenge Response, *CI* = Conveyable Image, *RA* = Reliability and Accuracy, and *ReA* = Real Applicability

Table 4: Ranking of Present and Past Studies^.

Recognition-Based Models	Ranking-1[+]	Ranking-2^
Shield-2 Model	10	5
Color Password Model	7	-
Picture Password Model	6	-
Story Model	5	3
Multiple authentication Models	5	4
Face Model	5	3
Challenge-response Authentication Model	5	3
Passfaces Model	5	2
Déjà Vu Model	4	1

*Present study [+] and Past Study^*

Results from this study, although from an artistic perspective, support part of a past research studies conducted on Shield-2 model (see Tabled 3 and 4) presently deployed online at: http://secure-shield.com from security and usability perspectives (Onibere and Egwali, 2011; 2010; Egwali and Onibere, 2015). This shows that there is a correlation between artforms in the art domain and artforms in computer security.

CONCLUSIONS

This study is limited to the analysis of artforms in RGPM that are gaining their way into many computing systems and handheld devices. Although users are often blamed for security breaches, in this work we focused on the design principles of artforms and analyze its relationship with the design nature of the user interface of RGPM. We further focused on usability and design issues. From this empirical work, by means of probabilistic semantics we identified design elements from an artistic perspective that are applicable to address the usability and design issues affecting recognition-based models. We further applied these design elements on some existing models to establish their feasibility in improving future models, at the end it was found that using the principles of art was effective and reliable in graphical password efficiency.

REFERENCES

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

2. Behzad, M., O. Mauricio, and E. Abdulmotaleb. 2008. “Novel Shoulder-Surfing Resistant Haptic-based Graphical Password”. Available at: http://lsc.univ-evry.fr/~eurohaptics/upload/cd/papers/f119.pdf

3. Biederman, I., A.L. Glass, and E.W. Stacy. 1973. “Searching for Objects in Real World Scenes”. *Journal of Experimental Psychology*. 97: 22-27.

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

5. Bradley, M. M., M.K. Grenwald, M.C. Petry, and P.J. Lang. 2000. “Remembering Pictures: Pleasure and Arousal in Memory”. *Journal of Experimental Psychology*. 81(2): 379-390. Symposium. Denver, CO, USA. Available at: http://www.usenix.org/publications/library/proceedings/sec2000/dhamija.html.

6. Clarke, R. 1994. “Human Identification in Information Systems: Management Challenges and Public Policy Issues”. *Information Technology & People*. 7(4): 6-37.

7. Collingwood, R.G. 1980. *The Principles of Art*. Wollheim, op. cit. 1: 36–43.

8. 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.

9. Cornel de Jong. 2008. “Online Authentication Methods. Evaluate the Strength of Online Authentication Methods”. Available at: http://www.usenix.org/events/upsec08/tech/full_papers.html

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

11. De Angeli, A., L. Coventry, G. Johnson, and K. Renaud. 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.

12. Dhamija, R. and A. Perrig. 2000. "Deja Vu: A User Study Using Images for Authentication". In: *Proceedings of9th USENIX Security Symposium*. Denver, CO. p 45–58. Available at: http://www.usenix.org/publications/library/proceedings/sec2000/dhamija.html.

13. Egwali, A.O. and E.A. Onibere. 2015. “Users Interference from Multimodal Authentication Models”. *University of Benin Journal*.

14. Fabian, M. and R. Aviel. 1997. “Keystroke Dynamics as a Biometric for Authentication”. Available at: http://www.cs.jhu.edu/~fabian/papers/fgcs.pdf

15. Farlex. 2016. “Artform”. *The Free Dictionary*. Available at: http://www.thefreedictionary.com/art+form

16. ISO. 2009. “ISO-International Organization for Standardization”. Available at: http://www.iso.org/iso/catalogue_detail.htm?csnumber=1688.

17. Jain, A., R. Bolle, and S. Pankanti. 1999. “Introduction to Biometrics”. In: Jain, A.K., et al. (eds.). *Biometrics: Personal Identification in Networked Society*. Springer: Boston, MA. 1- 41.

18. Jain, A.K., A. Ross and S. Prabhakar. 2004. “An Introduction to Biometric Recognition”. *IEEE Transactions on Circuits and Systems for Video Technology*. 14(1): 4 – 20.

19. 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

20. Kennick, W. and W.E. Kennick. 1979. *Art and Philosophy: Readings in Aesthetics.* St. Martin's Press: New York, NY. p. 89. ISBN 0-312-05391-6

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

22. Man, S., D. Hong, and M. Mathews. 2003. "A Shoulder Surfing Resistant Graphical Password Scheme". *Proceedings of International Conference on Security and Management*. Las Vegas, NV. 89-103.

23. Mandler, J.M. and G.H. Ritchey. 1977. "Long-Term Memory for Pictures". *Journal o Experimental Psychology: Human Learning and Memory*. 3: 386-396.

24. Matsumoto, T., H. Matsumoto, K. Yamada, and S. Hoshino. 2002. "Impact of Artificial Gummy Fingers on Fingerprint Systems". *Proceedings of SPIE, Optical Security and Counterfeit Deterrence Techniques*. IV: 8577.

25. Miller, G.A. 1996. "The Magical Number Seven, Plus or Minus Two: Some Limits on our Capacity for Processing Information". *The Psychological Review*. 63: 81-97.

26. Nelson, D.L., U.S. Reed, and J.R. Walling. 1976. "Pictorial Superiority Effect". *Journal of Experimental Psychology: Human Learning & Memory*. 2: 523-528.

27. New Zealand Qualifications Authority. 2016. "Design and Visual Communications (Graphics) Glossary". Available at: http://www.nzqa.govt.nz/qualifications-standards/qualifications/ncea/subjects/graphics-dvc/glossary/

28. O'Gorman, L. 2003. "Comparing Passwords, Tokens, and Biometrics for User Authentication". *Proceedings of the IEEE*. 91(12): 27 - 35.

29. Onibere, E.A. and A.O. Egwali. 2006. "Analyzing Factors Affecting User Password Practices: A Survey". *Nigerian Journal of Computer Literacy*. 7(1): 80 – 98.

30. Onibere, E.A. and A.O. Egwali. 2010a. "Enhancing Authentication Models Characteristic Metrics via Probability Modeling". *Journal of the Nigerian Association of Mathematical Physics*.

31. Onibere, E.A. and A.O. Egwali. 2010. "Design and Implementation of Shield: A Hybrid Authentication Model". *Journal of Institute of Mathematics and Computer Sciences*. 21(3): 419-433.

32. Onibere, E.A. and A.O. Egwali. 2011. "Enhancing Authentication Models Characteristic Metrics via Probability Modeling". *Journal of the Nigerian Association of Mathematical Physics*. 18: 395 – 400. Indexed in AJOL.

33. 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.

34. 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*.

35. Putte, T. and J. Keuning. 2000. "Biometrical Fingerprint Recognition: Don't Get Your Fingers Burned". *Proc. IFIP TC8/WG8.8, Fourth Working Conf. Smart Card Research and Adv. App.* 289-303.

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

37. Scheuermann, D.M., S. Schwiderski-Grosche, and B. Struif. 2002. "Usability of Bometrics in Relation to Electronic Signature". EU-Study 502533/8, Darmstadt, Germany. http://www.sit.fraunhofer.de/english/SICA/sica_projects/project_pdfs/eubiosig.pdf

38. Shiner. 2003. *The Invention of Art: A Cultural History*. University of Chicago Press: Chicago, IL. p. 3. ISBN 978-0-226-75342-3

39. Sobrado, L. and J.C. Birget. 2002. "Graphical Passwords". T*he Rutgers Scholar, An Electronic Bulletin for Undergraduate Research*. 4: 12-18.

40. Suo, X., Y. Zhu, and G.S. Owen. 2005. "Graphical Passwords: A Survey". 21st Annual Computer Security Applications Conference (ACSAC'05). (2005). p 463-472. Available at: http://www.acsac.org/2005/papers/89.pdf

41. 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: Springer-Verlag GmbH. pp. 347 - 351.

42. 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.

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

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

45. 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.

46. 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.

47. Wiedenbeck, S., J. Waters, J. Birget, A. Brodskiy, and N. Memon. 2005a. "Authentication Using Graphical Passwords Effects of Tolerance and Image Choice:. Available at: http://portal.acm.org/citation.cfm?id=1073001.1073002

48. Wikipedia. 2008: "Authentication". Available at: http://en.wikipedia.org/wiki/Wikipedia: Authentication.

49. Xiaoyuan, S. 2006. "A Design and Analysis of Graphical Password". Available at: http://digitalarchive.gsu.edu/cgi/viewcontent.cgi?article=1026&context=cs_theses

50. Zangwill, N. 1999. "Feasible Aesthetic Formalism". *Nous*. pp. 610-629.

51. Zhi, L., S. Qibin, L. Yong, and D. Giusto. 2005. "An Association-Based Graphical Password Design Resistant to Shoulder-Surfing Attack". Available at: ieeexplore.ieee.org/iel5/10203/32544/01521406.pdf

ABOUT THE AUTHORS

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.

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).

Professor Ogene, John, is a Professor of Graphics and Art History in the Department of Fine and Applied Art, University of Benin, Nigeria. He holds a BA, University of Nigeria, Nsukka , MFA degree from University of Benin and a Ph.D. in Art History from Delta State University, Abraka, Nigeria. 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, F., A. Egwali, and J. Ogene. 2020. "An Appraisal of Artform as Usable Design Elements of RGPM". *Pacific Journal of Science and Technology*. 21(2):170-180.

Pacific Journal of Science and Technology