A Survey Analysis of Recognition-Based Graphical Password Art-form Design Attributes

Annie O. Egwali, Ph.D.* **and John B. Odetayo, M.Sc.**

Department of Computer Science, Faculty of Physical Sciences, University of Benin, PMB 1154, Benin City, Nigeria.

E-mail: annie.egwali@uniben.edu*

ABSTRACT

Over the current century, recognition-based graphical password models (RGPM) that embed art-forms in their interfaces have been designed to enable users to comply with fundamental usability and security requirements, yet users still find it a challenge to comply with these requirements. Though some studies have centered on humans as the weakest link in the security chain, recent assertions from the literature have shown that the choice of art-forms in graphical password models and allowing users to choose their own art-forms or click point within an art-form during authentication can have a direct effect on a system's usability and security level.

This study is a literature survey on RGPM. The occurrence of some important design attributes relating to RGPM are analyzed in order to determine unique design attributes that can be used as a framework to measure the quality RGPM from designers' perspective. Our result shows that there exist 80 art-form design attributes that can be used as a framework to measure the quality of art-forms in RGPM.

(Keywords: graphical password models, art-forms, interfaces, design, usability, security, authentication)

INTRODUCTION

Implementation of access control policies and standards often involve the identification of appropriate authentication mechanisms and the adopted access control mechanism is directly related to the criticality of the system being protected (Li, et al., 2009). Current authentication techniques can be divided into three main areas: knowledge-based, token-based, and biometric-based authentication. They can also be based on single factor models, two-factor models, or multifactor models. According to Denning and MacDoran (1996), it can also be classified based on where the user is located (location-based authentication). For some decades, authentication via the textual password model has been widely incorporated as part of access control for most systems. Textual or alphanumeric password falls under the domain of knowledge-based authenticating systems. In recent decades, the pervasive nature of the conventional textual passwords, which involves a combination of username and password (or PIN), has been declining because of usability and security challenges (Kucken and Newell, 2004). These alphanumeric passwords which are based on pure recall are a real challenge for users, for recognition memory is better than unaided recall (Norman, 1988).

In an attempt to create more secure and memorable passwords, Graphical Password Models, which involves the use of art-forms have been developed. Graphical or Art-form-based Authentication Models are classified into recognition-based, cued-recall-based, and pure-recall-based models. In Recognition-based Graphical Password Models (RGPM), a user is provided with art-form(s) and has to decide by clicking on the region(s) that match the registration choice(s). The decision is binary: either the art-form is known (recognized) or not known (Suo, et al., 2005). In pure-recall, a user has to draw an art-form or signature without any hints (De Angeli, et al., 2005) while in cued recall, users have to recall a password, but the system offers a framework of hints, context and cues that help the users reproduce their passwords or help them make the reproduction more accurate (Wiedenbeck, et al., 2005).

Presently, there is a dearth of literature on attributes determining important RGPM product from designers' perspective. Moreover, determining software product quality from a designer's perspective is tedious as software qualities vary based on usage. As studies on RGPM continue to increase through research, there is need for an evaluation method from the designers' perspective. Furthermore, within the context of 'secure or insecure human behaviors' the effect of the function and aesthetics of the art-forms in RGPM based on qualities as it relates to art-forms designs, have not really been taken into consideration as it affects usability and security.

DESIGN ISSUES OF RGPM ARTFORMS

An art-form can be defined as an activity or the specific shape, or quality of a piece of artistic work that can be regarded as a medium of artistic expression (Farlex, 2016). It can be seen as any medium regarded as having systematized rules, procedures, or formulations. To address usability and security issues in computing systems, art-forms have been used extensively as authenticated proofs and identities (Poole and Le-Phat, 2011). Sasse, et al. (2001) and Adam and Sasse (1999) affirmed that users' choices of good or bad passwords are based on the useful information available to aid their understanding. They believed that the existing password system models have not done enough in this aspect to assist the users in choosing strong passwords. They faulted an opinion of users' inability to know and remember good password and indifferent concern about security when using art-forms in recognition-based graphical passwords as factors responsible for users choosing bad passwords.

Wiedenbeck, et al. (2005) affirmed that many art-forms are almost certainly usable but a main goal in graphical password model (GPM) should be to avoid bad art-forms that will perplex memory. So many art-forms lack adequate incorporation of usability principles that is why Conlan and Tarasewich (2006) also registered their objection to the popular opinion that the users of the authentication systems are solely responsible for the choices of weak and immemorable passwords. They asserted this view to be inadequate in their work. They believed that most Password System Mechanisms designs do not follow the basic Human-Computer Interaction principles, and this has been responsible for the flaws in textual password mechanisms as opposed to the argument been adopted by major organizations such as Microsoft (Ilett, 2004) and RSA Security (CRU4A, 2018). Anap, et al. (2016) also posits that the implementation problems in GPM are due to the difficulty in design of the password art-forms that are memorable and secure and in providing a large enough password space. Wiedenbeck, et al. (2005) and Elftmann (2006) asserted that the nature of the art-forms used in a system may have a large effect on people's ability to remember their click points but that allowing users to choose their own art-forms may lead to high memorability for an individual, but at the same time may result in art-forms with poor security characteristics. Conlan and Tarasewich (2006) stressed the need for current password system models to adequately incorporate usability principles into their design as evaluated through findings (Sasse, et al., 2001; Adam and Sasse, 1999).

As asserted by Oorschot and Thorpe (2004a), since the deployment of GPM thus far, there is lack of knowledge of 'good' art-form distribution users are likely to select from that will be both usable and secure. According to Wiedenbeck, et al. (2005), studies show that some art-forms perform more poorly than others yet specific criteria for a "good" art-form are not known, and may only be exposed through research or practical experience. A study conducted by Wiedenbeck, et al. (2005) showed a high correlation between memory accuracy and tolerance in use.

Memory accuracy for GPM is strongly reduced if smaller tolerance is used whereas the reverse is the case for a large variety of art-forms (Suo, et al., 2005). Oorschot and Thorpe (2004a) also affirmed that if the number of possible pictures is sufficiently large, and the diversity of picture-based passwords can be captured, graphical passwords may be less susceptible to having weak password subspaces and offer better security. However, studies reveal that five factors (i.e., types of art-forms, nature of the art-forms, racial bias, attractiveness and security) affect RGPM success with respect to usability and security. Thorpe and Oorschot (2007) revealed that visual authentication success is dependent on the type of art-forms that a RGPM uses as well as how the art-forms are encoded and then retrieved when required.

Elftmann (2006) stated that the nature of the art-forms used in a system may have a large effect on people's ability to remember their click points but also compromise security. Studies of characteristics of art-forms exist but are limited (Wiedenbeck, et al., 2005), and are not highly directive for our purposes. Some research studies have investigated art-form memorability in the context of free recall of art-forms, others in the context of recognition memory. These studies do not give us sufficient guidance about the nature or characteristics of recognition-based art-forms. Wiedenbeck, et al. (2005) observed that some art-forms perform more poorly than others and further hypothesize that although research from psychology helps, unfortunately limited knowledge about the relationship of art-forms content and memory makes choosing password art-forms an art rather than a science. Wiedenbeck, et al. (2005) specified five types of bad art-forms that should be avoided: art-forms with few memorable click points, incomprehensible scenes, art-forms with little color or low contrast, abstract art-forms, art-forms with a swirls of colors or other abstraction as used in Déjà Vu (Dhamija and Perrig, 2000) and art-forms associated with the GPM user that may be memorable but guessable.

According to Renaud and De Angeli (2009), the suitability of an art-form for use in authentication can be associated with three prime aspects. The first relates to how clear the art-form is to the user, and the second is how memorable it is (i.e., how easy it is for the user to recall it). Thirdly it relates to the complexity and therefore security level of the art-form. From this finding it can be depicted that the second factor (memorability) and the third factor (security) are dependent on the clarity of the art-form used. Moreover, the well combination of the qualities of art-forms determines the clarity of the art-form.

Also as posited by Dirik (2007), a major goal for studies on GPM is to determine through research, art-forms that will enables us to predict the entropy of user click points a priori (if they lead to low entropy), designs to counter attacks. Jackson (2006) further mentioned that degradation of color in the art-form is one of the possible attempts to mitigate attack in RGPM. Furthermore, coherent art-forms have been found to be more memorable than jumbled ones (Biederman, et al., 1973; Mandler and Ritchey, 1977). Further studies also show that individuals are better able to recognize faces of people from their own race than faces of people from other races (Walker and Tanaka, 2003; Meissner and Brigham, 2001). As asserted by Luce (1974) and Malpass (1992), there is a purported “race-effect” which raises the question of whether users would favor members of their own race when selecting art-forms to construct their passwords. Another study by Norman (1998) makes indication to the race-effect, but makes no reference to any effect it might have on password choice. However a study conducted on twenty users affirmed the fact that users selected the art-forms of individuals they can relate personally to, from similar race as themselves (Birget, et al., 2005).

Suo, et al. (2005) also affirmed the fact that the more attractive the face the more chances of it being chosen. Studies on attractiveness show that across cultures, people tend to agree about the attractiveness of individuals. The expression “beauty is in the eye of the beholder,” has been proved false (Langlois, et al., 2000). Davis, et al. (2004) revealed that art-forms containing graphical password schemes like Face, raises the question of what influence general perceptions of beauty (e.g., facial symmetry, youthfulness, averageness). Therefore, given these a priori perceptions, it is evident that users are more inclined to choose the most attractive art-forms when constructing their passwords. As asserted by Suo, (2006) art-form security is an important design consideration for RGPM. According to Lashkari, et al. (2009), existing literature on RGPM resistance to attacks are limited.

Wiedenbeck, et al. (2005) recommended more research to be done to unearth specific requirements for designing better art-forms in RGPM. Dirik, et al. (2007) suggested further experiments test for different types of art-forms. Bianchi et al. (2015) include the use of a more extensive investigation of alternative technique in place of a single feature extraction technique as used in their work, and formal evaluation to determine the feasibility and robustness of RGPM across different devices and in different environmental conditions. Furthermore, they called for more works to be done to confirm the usability and security of these approaches.

Salehi-Abari, et al. (2008) in their work were uncertain if art-form processing measures can effectively filter out art-forms that are more prone to exploits, for they believe that users are obligated to use all kinds of complex techniques to search for a workaround and as posited by Wiedenbeck, et al. (2005a), complexity depends on the user of the technique. They further asserted that the best way to establish the fact that it is not the art-forms in GPM that is resulting in users compromising systems, is to study in details the effect of the application of design principles in art-forms and to make use of diverse composition of art-form interfaces that may have a positive or negative effect on user's ability to remember their generated passwords. This will enable the assessment of the effect of these art-forms in terms of usability and security. It, thus, established that user choice is heavily influenced by the design of the art-forms. The implication is that design choices need to be carefully considered when making usability and security-related modifications to RGPM art-forms or user interface. Presently, there is no study on the design qualities that should be used for the overall assessment of RGPM art-forms and the technique to measure the generic quality assessment. Due to this breach, security personnel and computer software designers cannot justify large investment in authenticating models that satisfies usability and security even within the context of 'secure' or 'insecure' human behaviors.

Thorpe and Oorschot (2007) also recommended user studies to examine if altering parameters (e.g., pixel sizes of art-forms, tolerance settings, number of click-points) will yield a system with acceptable usability and security simultaneously. They posited that more works needed to be done to determine more popular spots on chosen art-forms after preliminary screening by applying proactive measures as evaluated in their work. Wiedenbeck, et al. (2005) show that the user attention is influenced by both high-level (i.e. art-form content and memory feedback (Osberger and Maeder, 1998)) and low-level factors (i.e. basic geometric and physical art-form features, such as contrast (Yarbus, 1967; Elias and Sherwin, 1984), especially if there is a high contrast between the region's color and the background color, size, shape, color, motion, location, foreground and object category (i.e. studies shows that users generally focus on people in a scene, and in particular on the eyes, mouth and hands) (Patrick- et al., 2004; Yarbus, 1967).

RELATED WORKS

Over the years, different RGPM have been proposed and studies conducted. Déjà Vu (Dhamija and Perrig, 2000) put forward a system based on recognition of computer generated images, which uses hash visualization with non-describable abstract images (Perrig and Song, 1999). To be authenticated the user must click on all five password images and not click on any of the decoy images. The process of selecting a set of pictures from the picture database was tedious and time consuming for the user.

Davis, et al. (2004) designed a RGPM namely: Face. Their aim was to study the impacts of user choices on the security of graphical password schemes. Their lab study consists of dataset collected during the a semester from a set of students in which each student was indiscriminately assigned to either of two graphical password schemes (Face and Story (Davis, et al., 2004)) to access their grades, homework, homework solutions, course reading materials. The analysis of the results of the experiments indicates that both users and the design employed are responsible for the results gotten. The faces chosen by users in the Face scheme were highly biased by the race of the user, also the gender and appealingness of the faces also exert influences on the password choices. Both male and female participants selected female faces far more often than male faces, and then picked attractive ones more often than not. As a result of this, they advised against the use of a Passfaces-like system that permits user choice of the password, without some means to mitigate the dramatic effects of attraction and race that their study measures. Suggested alternatives for mitigating this threat includes prohibiting or limiting user choice of passwords and educating users on better approaches to select passwords, or to select art-forms less prone to these types of biases.

Davis, et al., 2004 also developed Story that was user-tested along with the Face model in a field study where a panel contained 9 images. A user's password consisted of a sequence of 4 images selected from within this panel. 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.

Wiedenbeck, et al. (2005) evaluated Passpoint model with human users by studying two issues: the effect of tolerance or margin of error in clicking on the password points and the effect of the art-forms used in the password system. Their lab studies made use of Passpoint graphical password model with tolerance (20 x 20pixels) using four different art-forms. Results in the tolerance study shows that participants were quite successful using tolerance 20 x 20 pixels but accurate memory for the password was strongly reduced when using a small tolerance (10 x 10 pixels) around the user's password points. Suo, et al. (2005) also asserted that memory accuracy for GPM is strongly reduced if smaller tolerance is used whereas the reverse is the case for a large variety of art-forms.

Wiedenbeck, et al. (2006) proposed the Convex Hull Click (CHC) that is resistant to shoulder-surfing, even while a human observer or a video camera records the login. The CHC scheme allows a user to prove knowledge of the graphical password safely in an insecure location because users never have to click directly on their password art-forms. A lab study was conducted to evaluate the password scheme in terms of accuracy, efficiency, memorability, and user satisfaction. The result of the study showed that the CHC scheme was easy to learn and remember. More than half of the participants made no error in entering their password ten times consecutively. The participants who entered incorrect passwords were nearly correct having only one incorrect click in the five rows. The study also revealed that to improve the login in time faster rearrangement of icons between challenges was necessary, including more pass-icons in the password window; and improve elements that slowed down the user to make the security settings more realistic.

Chiasson, et al. (2007) studied how user interface could affect the security of the authentication system using three click-based graphical password schemes, namely PassPoints, Cued Click-Points (CCP) and Persuasive Cued Click-Points (PCCP) passwords, as a function of the different user interfaces (art-forms) presented by these schemes. They presumed that the designs of the user interfaces of authentication systems influence users' choices of passwords and may encourage either secure or insecure behavior. The main objective of their work was to study the differences in users' choices of passwords using the three models. Among many findings, the result of their experiments reveal that the design of the user interfaces in RGPM impacts on whether users select their click-points in predictable patterns and that the security of passwords can be improved through interface design choices (art-forms). From their results, they noted that design choices which subtly alter user selection of passwords cannot be made naively because they may weaken security. These design choices may lead users to employ coping mechanisms, may makes it too easy to make insecure choices, or may make the insecure option most logical or most convenient from a user's perspective. This means user interface design decisions may sway user behavior, sometimes towards less secure behavior.

Jackson (2006) reviewed related works on GPM and further designed a prototype that could be used to test the possibility of art-form-based authentication being the main security method of the future. The prototype consists of three interfaces which are a picture- based, a facial picture-based and a story-based. He conducted five different experiments to test the memorability, usability and security of the prototype. The results of the experiments indicated that the memorability levels of the three interfaces were slightly below 90%. The best memorable interfaces among the three were the Story-Based and Picture-Based interfaces. He asserted that the Story-based was the best among the three interfaces in term of memorability. He justified this outcome based on the fewer number of passwords to be recalled in Story-based interface compared to other interfaces. Though, in Picture-based interface, some subjects with lesser number of passwords still had difficulty in remembering them.

The success of high memorability in Story-based was attributed to the methodology users adopt to create passwords appealing to themselves. It was noted that Facial picture-based interface scored the least among the three in term of memorability but yet the most secure. It was affirmed that the Picture-based interface is a sensible middle ground between the usability and security. With the prevailing threat of Brute force Attacks on Story-based interface it was noted that more works needed to be done on the security of Artform-based password system. It was concluded that the Story-based Interface promised to be a reliable art-form-based interface of the future with the increase of available selections, and inclusion of more selection tabs.

Dirik, et al. (2007) examined a PassPoint system of graphical password and conducted an experiment to identify the most likely regions for users to click in order to create graphical passwords in the PassPoints system. They went further to develop a model that would help to determine the likely click points in the graphical password for a given art-form. This model could help to predict the measure of the security of a click point of a chosen art-form used in a graphical password and could also help to design automatic dictionary attack and to rule out art-forms with low entropy. They conducted lab study with two fixed test art-forms and compared them. The art-forms were the flying birds' art-form and the walking people art-form. The flying bird art-form was simple and not to good for the PassPoints system because it has very small clickable points while the walking people art-form has larger clickable points. The results of the study shows that users click points compared to the prediction by the model have 80% and 71% accuracy for flying bird art-form and people art-form respectively. The results further showed that the people art-form was better than the bird art-form as a choice art-form in a PassPoints graphical password system. Finally they suggested further experiments test of the model for different types of art-forms.

Salehi-Abari, et al. (2008) improved on the model of Itti, et al. (1998) and showed how it relates to user-selected recognition-based graphical passwords. They focused on the purely automated techniques for guessing attacks. They evaluated various methods for the automated attacks against RBGM based on click-order-patterns. They aimed at identifying attractive points users are likely to select by using art-form processing method. They formed hypothesis on the fact that users tend to click on particular points in a click-point-patterns in order to enable them to remember their passwords easily, and that users prefer some certain points based on how attracted they are to the points. Thus, their automated technique combines click-order-patterns with visual attention models. Their results show that automated attacks, which are easier to arrange than human seeded attacks, are more scalable to systems that use multiple art-forms and posed a significant threat. Importantly, they noted that the attack results are art-form-dependent.

Conlan and Tarasewich (2006) looked in the direction of the impacts of the design of most password selection mechanisms (PSMs) on the security of systems. They evaluated the challenges of password selection and memorability by exploring PSMs with new interface approaches with an aim to develop frameworks and designs that will aid users to select both secure and memorable passwords. They identified two usability problems facing current textual password mechanisms as the gulf of execution and the gulf of evaluation. They defined the gulf of execution as problems arising because the user does not know how to choose good passwords while the gulf of evaluation reflects when the user does not receive appropriate feedback while selecting a password. Thus, in their research, they focused on improving the gulf of evaluation in PSMs. They highlighted three basic considerations when integrating a feedback mechanism into PSMs. The first is when the feedback should come in – either when password has been submitted or as the password is being typed (dynamically). The second is what type of feedback to provide – this can be textual feedback, progress bar, or an avatar, etc. The final consideration is what algorithm to use to analyze the password quality.

Perrig and Song (1999) designed a RGPM and studied the effects of human factors in current security challenges and attributed the failure to the inability of the system to make a provision for human limitations. They examined two human limiting factors which are the difficulty of people when comparing meaningless string and when memorizing strong passwords and PINs. They based the scheme on the fact that humans are very good at identifying geometrical shapes, patterns, and colors, and compared two art-forms efficiently in the case of root key validation (Boynton and Boss, 1971; Williams, 1966; Reynolds et al., 1972), and in the case of user authentication, people are extremely efficient at recognizing previously seen art-forms (Card, 1999; Boff, et al., 1986). Their methodology includes the use of random art for automatic generation of artistic art-forms. Results show that the security schemes needed to account for human factors by making adequate provisions for human limitation. The prototype developed complimented human limitation in comparing meaningless string and memorizing strong passwords/PINs by converting them to structured art-forms which has been proved to be very good in this aspect. However, in their work, not all art-forms generated were usable or improve the security of the system (Wiedenbeck, et al., 2005). They suggested more works on user study to evaluate users' perceptions of generated art-forms, and how to generate recognizable art-forms.

Tari, et al. (2006) explore whether the advantage of high memorability in GPM necessarily leads to risks of shoulder-surfing. They access the real and perceived vulnerability to shoulder-surfing of two configurations of graphical password: Passfaces (mouse vs keyboard data entry), compared to non-dictionary and dictionary passwords. The lab study involved 20 participants who were asked to explore the real and perceived vulnerability of four configurations of authentication systems. Findings showed that despite the common belief that non-dictionary passwords are the most secure type of password-based authentication, it is in fact the most vulnerable configuration to shoulder-surfing.

Coming from the background of many research literatures that largely focus on the usability of Click-based graphical password schemes using a single background art-form (e.g., PassPoints), Thorpe and Oorschot (2004a) argued that the security of RGPM has received little attention. They believed that the issue of the security of RGPM remains largely unaddressed. They claimed that the effect of hotspots has been downplayed. Thus, they examined the security of RGPM, including the effects of different background art-forms, and strategies for guessing user passwords. They focused on a security analysis of an implementation with the same parameters as used in a recent PassPoints publication (Wiedenbeck, et al., 2005). They conducted empirical studies and confirmed the existence of hot-spots and showed that some art-forms are more prone to hot-spotting than others.

Chiasson, et al. (2008) explored the semantic structure of RBGM to identify the common modalities the schemes take and to show how the same kind of scheme could work with alternative interaction modalities for greater accessibility. They examined the different forms of click-based GPM, they found out that they all rely on the same procedures which are visual presentation as output and fine motor control of a pointing device as input. These identified procedures can also be viewed as presentation step and selection step respectively. Having identified the essential structures of the recognition graphical password schemes, they considered using alternative procedures within the same structure. They proposed playing audio sequence (such as a piece of music) and select time-points using a simple keystroke or mouse-click. They stated that these two alternative modalities collectively represent the structure of a click-based graphical password system, but without the need to use either visual display or fine motor control for pointing. They evaluated the proposed scheme and explored the consequences for security and usability. By their findings they affirmed that authentication systems could be designed and implemented independently from any particular form. They suggested possibilities, in the future, of designing an authentication model where users may select modalities suitable to their particular states. They concluded that modality independent authentication is a reasonable concept, but that great care is needed because the modalities employed in implementation will affect both usability and security.

Komanduri and Hutchings (2008) carried out a research into performances, in terms of memorability, usability and security, of Picture-based password scheme and character-based password by maintaining high level of entropy under some certain conditions which include unordered input tasks and ordered input tasks. The main aim of their research was to use pictures to produce memorable, high-entropy password systems. The results of their lab study showed that the memorability of the picture passwords and character passwords were 100% and 67%, respectively.

In contrast, the memorability of both picture and character passwords, in serial order, were 67% and 50%, respectively. These results suggested that ordered passwords of this level are too difficult to remember. Finally, they suggested more research works into user insecure behaviors and unordered randomly-assigned passwords. Towhidi and Masrom (2009) reviewed some of RGPM by identifying their loopholes and security challenges. In addition, they surveyed usability requirements from ISO and other previous works on GPs to form their usability model. Furthermore, security threats related to the sampled RGPM were analyzed to make a comparison table among RGPM based on ISO usability attributes and Attack Patterns. The lab study involved 8 RGPM which includes Passfaces, Déjà vu, Triangle, Movable Frame, Picture password, Man, Story, and Jetafida. They evaluated 3 ISO standards that described usability features in details (ISO 9241, ISO 9126 and ISO 13407) to draw a usability comparison table for the RGPM. Their usability comparison table included reliability, accuracy, easy to use, easy to learn, easy to create, meaningful, memorability and nice interface. They noted that 'pleasant art-form' is a meaningful item that should be included in the usability feature of RIBPM.

Table 1: Artform Design Parameters.

Authors	Design Parameters		Attributes
Suo et. al. 2005; Onibere and Egwali, 2011; Clarke, 1994; Newham, 1995; Jain and Uludag, 2003; Jain et al, 2004	1) Acceptability		High level Attributes
New Zealand Qualifications Authority, 2016 Meissner and Brigham, 2001; Birget et al, 2005; Onibere and Egwali, 2010; Dirik et al, 2007.	Aesthetics	2) Balance	
		3) Color	
		4) Contrast	
		5) Emphasis	
		6) Environment	
		7) Finish	
		8) Form	
		9) Harmony	
		10) Line	
		11) Movement	
		12) Pattern	
		13) Plane	
		14) Point	
		15) Proportion	
		16) Rhythm	
		17) Shape	
		18) Style	
		19) Texture	
		20) Unity / Harmony	
		21) Value	
		22) Variety	
	Function	23) Construction (And Its Cost)	
		24) Optimization,	
		25) User-Friendliness,	
		26) Fitness For Purpose.	
		27) Reliability,	
		28) Ergonomic Fit,	
		29) Strength,	
		30) Durability,	
		31) Efficiency,	
		32) Safety And Stability	
		33) Stability,	
Dhamija and Perrig, 2000; Onibere and Egwali (2010; 2011); Suo et al, 2005; Osberger and Maeder, 1998	34) Speed		
Davis et al, 2004; Oorschot and Thorpe, 2004a; Walker and Tanaka, 2003	35) Unbiased content		
Davis et al, 2004	36) Unpredictable patterns		
Conlan and Tarasewich (2006)	37) Appropriate feedback		
Perrig and Song, 1999; Egwali and Odafe, 2012; Tari et al., 2006)	38) Recognizable art-forms.		
Suo et. al. 2005; Onibere and Egwali, 2011	39) Meaningful 40) Acceptability 41) Training Simple 42) Easy to Use 43) Easy to Create 44) Easy to Learn 45) Performance		
Clarke, 1994; Newham, 1995; Jain and Uludag, 2003; Jain et al, 2004	46) Permanence		
	47) Collectability 48) Universality 49) Randomized		
	Strength	50) Brute Force Resistance,	
		51) Dictionary Resistance,	

Blonder, 1996; Davis et al, 2004; Dhamija and Perrig, 2000; Suo et. al. 2005; Onibere and Egwali, 2011		52) Replay Resistance	
		53) Nice Interface, 54) Easy to Memorize, 55) Conveyable Image, 56) Efficiency 57) Replaceability 58) Collectability 59) Reusable 60) Non comprisable Hot-spots	
	Effectiveness	61) Reliability	
		62) Accuracy	
Chiasson et al, 2007; Chiasson et al, 2008		63) Natural selection pattern	
Wiedenbeck et al, 2006; Onibere and Egwali, 2010; Wiedenbeck et al, 2005		64) Faster rearrangement 65) Ample color set 66) Large tolerance 67) High contrast	Low-Level Attributes
Jackson, 2006; Wiedenbeck et al, 2006; Oorschot and Thorpe, 2004a		68) Large selection base	
Salehi-Abari et al, 2008; Egwali and Enabulele, 2015		69) Scalable	
Suo et al, 2005; Osberger and Maeder, 1998.		70) Available	
Thorpe and Oorschot (2004a)		71) Non comprisable Hot-spots	
Komanduri and Hutchings (2008)		72) Unordered art-form	
Onibere and Egwali, 2010; English (2014)		73) Pleasant art-form	
Oorschot and Thorpe, 2004a; Suo et al, 2005; Davis et al, 2004	Attractiveness	74) Facial symmetry 75) Youthfulness 76) Averageness	
Biederman et al, 1973; Mandler and Ritchey, 1977		77) Coherent	
Onibere and Egwali, 2011; Clarke, 1994; Newham, 1995; Jain and Uludag, 2003; Jain et al, 2004		78) Cost Effective	
Onibere and Egwali, 2011; Egwali and Enabulele, 2015		79) Portable	
		80) Simplicity	

English (2014) posited that the analysis of the security of RGPM have been inconsistent and proposed a metric that allows the security of RGPM to be measured and compared in terms of resistance to four identified attacks, namely random guessing, guessing based on category bias (semantic guessing), frequency attacks, and shoulder surfing attacks. Yet there was no in-depth study as to what attributes make RGPM tested in their work insecure against some attacks.

PROPOSED RGPM DESIGN FRAMEWORK

The following Table 1 contains the occurrence of significant art-form design attributes relating to RGPM isolated from literature. Eighty art-form design attributes were isolated and defined. They are classified into High Level and Low Level attributes and can be used as a framework to measure the quality of RGPM from designers' perspective.

The following are some of the attributes defined from the design perspective with definition gotten from literature as it relates art-form designs in RGPM.

Aesthetics: It 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.

Acceptability: Acceptance level is high when the authentication process does not have any effect whatsoever on the physic of the user or be obtrusive in any way.

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.

Point: Centre of interest in a composition. Visual elements and principles are used to direct the viewer's eye to this point.

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. There are different types of rhythm: Regular-Example: 9s9s9s9s9s9; Irregular-Example: qqeeqqeyyy

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 most often related to aesthetics rather than function. 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.

Unity: All the elements look like they belong together. This helps determine how many elements you use and how you use them.

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.

Universality*:* This denotes that the authenticating characteristic is available to everyone.

Available: The system should be accessible from a number of machines that can in general only be expected to have standard available tools, like standalone systems or in particular a web browser.

Collectability: This indicates that the characteristic can be measured quantitatively.

Conveyable Image: This indicates that the authentication interface contents should be moveable and flexible

Cost Effective: The deployment cost should be insignificantly when compared to other technological solutions and there must be a balance between the cost of implementation and the security measures

Reliability: The probability that a system, including all hardware, firmware, and software, will satisfactorily perform the task for which it was designed or intended, for a specified time and in a specified environment

Accuracy*:* This denotes the degree of closeness of a user's authenticating characteristics measurement of quality and quantity to the true value.

Easy to Create: Authenticating credentials must be easy to create by users.

Easy to Learn: It denotes how easy it is for users to accomplish the authenticating procedure the first time they encounter the design.

Easy to Memorize, Users should be able to return to the authentication model and easily remember how to reestablish the process***.***

Easy to Use: The process of enrollment, training and authentication in the authentication mechanism should be easy and fast. The ideal solution should be based on something the user already knows or does, and should not be overwhelmingly technical.

Efficiency: Efficiency is defined in terms of the system utilization in real world.

Speed: The rate at which the system responds to a user's authenticating commands should be fast enough.

Functional/Function principles - Relate to the operation and the construction of the object i.e. what makes it work.

Replay Resistance: This refers to the system's ability to counteract replaying fraudulent techniques.

Scalable: The degree to which a product or system can be adapted for different or evolving hardware, software or other operational or usage environments.

Simplicity: The design does not use unnecessary complexity.

Reusable: This addresses credential reuse after expiration

Replaceability: This is the degree to which a product can replace another specified software product for the same purpose in the same environment.

Portability: The system should perform on multiple platforms.

Meaningful: The whole authenticating process should be meaningful such that the whole process is related with previous knowledge.

Performance: It refers to the achievable identification accuracy, the resource requirements to achieve acceptable identification accuracy, and the working or environmental factors that affect the identification accuracy.

Permanence: Permanence attribute should be sufficiently invariant (with respect to the matching criterion) over a period of time.

Randomized: The authenticating interface should not follow a deterministic pattern, but follow an evolution described by probability distributions.

Nice Interface: The authenticating interfaces need to be attractive and captivating for all age ranges to utilize.

Strength: The strength of an object or product is determined by its ability to withstand pressures or forces.

Durability is the ability of a product or material to last in a given environment and to stand up to wear. Durability is a relative concept; our expectations of a product's durability depend on a variety of social, economic, and legal factors, such as how and where it is used, how much we pay for it, and the kind of guarantee it comes with. For some objects or materials, their durability will depend on their strength; for others, flexibility or fitness for purpose will be the key factor.

Efficiency: The term is more often used in relation to a situation where work is productive, with minimum wasted effort or expense.

Safety and Stability: Products, systems, and environments must be designed so that they are as safe as is practically possible to use. In many instances, designs have been adapted to make them safer for particular users.

Reliability: It is the likelihood that a product or system will continue to do its job. The design of a product and the components used in it influence its reliability.

Ergonomics: Ergonomics relates to the whole working environment, but an important focus is often the size and shape of objects. Designing objects that take account of people's size and shape requires the use of sets of standardized body measurements called anthropometric data, which can vary from country to country. These measurements are incorporated into the design of objects that will be used by many people, such as spectacles, cups, and public seating.

User-friendliness: The user-friendliness of a product, environment, or system is the degree to which it is easy to use.

Fitness for purpose: It depends on accurate design specifications; it describes how well a product works in the situation it was designed for and how well it meets the needs of its intended end-users.

CONCLUSION

In this work, we posit that in order to support memorize ability and be secured; the very nature of art-forms in RGPM has an enormous direct effect on a system usability and security level even within the context of 'secure or insecure human behaviors. Although users are often blame for security breaches, in this work we focus on the design principles of art-forms and analyze its relationship with the design nature of the user interface domain of systems using RGPM as our case study. From this literature review we identified 80 design attributes that are applicable to address the design issues affecting RGPM. We intend to further apply these design attributes on some existing models to establish their feasibility in measuring and improving future RGPM.

REFERENCES

1. Adams, A., and M.A. Sasse. 1999. “Users are not the Enemy”. *Communications of the ACM*. 42(12): 40-46.

2. Alley, T. and M. Cunningham. 1991. “Averaged Faces are Attractive, but very Attractive Faces are Not Average”. *Psychological Science*. 2:123-125.

3. Anap, A.B., A,A, Nibe, and V.S. Tamboli. 2016. “Secure Graphical Password Requirements”. Available at: https://www.ijraset.com/fileserve.php?FID=4053.

4. Ballard, L., F. Monrose, and D. Lopresti. 2006. “Biometric Authentication Revisited: Understanding the Impact of Wolves in Sheep’s Clothing”. In:15th Annual USENIX Security Symposium. 29–41.

5. Besnard, D. and B. Arief. 2004. “Computer Security Impaired by Legitimate Wsers”. Available at: https://hal.archives-ouvertes.fr/hal-00691818/document.

6. 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.

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

8. Birget, J., D. Hong, and N. Memon. 2005. “Graphical Passwords Based on Robust

Discretization". Available at: clam.rutgers.edu/~birget/grPssw/robDiscr.pdf

9. Boff, K.R., L. Kaufman, and P. James. 1986. *Thomas: Handbook of Perception and Human Performance*. John Wiley and Sons: New York, NY.

10. Bonneau, J., C. Herley, P.C. van Oorschot, and F. Stajano. 2012. "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes". *Proc. IEEE Symp. Security Privacy*. 553–567.

11. Borges, M.A., M.A. Stepnowsky, and L.H. Holt. 1977. "Recall and Recognition of Words and Pictures by Adults and Children". *Bulletin of the Psychonomic Society*. 9(2):113-114.

12. Boynton, R.M. and D.E. Boss. 1971. "The Effect of Background Luminance and Contrast upon Visual Search Performance". *Illuminating Engineering*. 66:173-186.

13. Bradley, M.M., M.K. Grenwald, M.C. Petry, and P.J. Lang. 1992. "Remembering Pictures: Pleasure and Arousal in Memory". *Journal of Experimental Psychology*. 81(2):379-390.

14. Brostoff, S. and M.A. Sasse. 2000. "Are Passfaces more Usable than Passwords? A Field Trial Investigation". *Proceedings of Human Computer Interaction 2000*. Sunderland, UK.

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

16. Chiasson, S., R. Biddle, and P. van Oorschot. 2007. "A Second Look at the Usability of Click-Based Graphical Passwords". *Proc. 3rd Symp. Usable Privacy Security*. 1–12.

17. Chiasson, S., A. Forget, R. Biddle, and P.C. van Oorschot. 2008. "User Interface Design Affects Security: Patterns in Click-Based Graphical Passwords". Available at: https://cups.cs.cmu.edu/~aforget/Chiasson_IntJInfSecDec2009_Patterns.pdf.

18. Conlan, R.M. and P. Tarasewich. 2006. "Improving Interface Designs to Help Users Choose Better Passwords". Available at: https://www.embracetherandom.com/changePasswordUIStudy/Improving%20Interface%2Designs%20To%20Help%20Users%20Choose%20Better%20Passwords.pdf.

19. Coventry, L., A. De Angeli, and G. Johnson. 2003. "Usability and Biometric Verification at the ATM Interface". *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.* (CHI'03). Fort Lauderdale, FL. April 5-10, 2003. ACM Press: New York, NY. 153-160.

20. CRU4A. 2018. "Passwords vs. Strong Authentication". RSA Security. Available at: http://tinyurl.com/cru4a.

21. Davis, D., F. Monrose, and M.K. Reiter. 2004. "On User Choice in Graphical Password Schemes". Available at: http://www.usenix.org/events/sec04/tech/full_papers/davis/davis_html/index.html.

22. 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.

23. De Angeli, A., M. Coutts, L. Conventry, D. Cameron, G.I. Johnson, and M. Fisher. 2002. "VIP: A Visual Approach to User Authentication". *Proceedings of the Working Conference on Advanced Visual Interfaces (AVI 2002)*. ACM Press: New York, NY. 316-23.

24. Denning, D. and P. Macdoran. 1996. "Location-Based Authentication: Grounding Cyberspace for better Security". *Computer Fraud Security*.12-16.

25. Dhamija, R. 2000. "Hash Visualization in User Authentication". Available at: http://people.ischool.berkeley.edu/~rachna/papers/hash_visualization.pdf.

26. Dhamija, R. and A. Perrig. 2000. "Déjà Vu: A User Study using Images for Authentication". Available at: http://www.usenix.org/publications/library/proceedings/sec2000/full_papers/dhamija/dhamija_html/index.html.

27. Dirik A.E., N. Memon, and J. Birget. 2007. "Modeling User Choice in the PassPoints Graphical Password Scheme". Available at: https://isis.poly.edu/memon/pdf/2007_modeling%20user.pdf.

28. 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.

29. Egwali, A.O. and M. Enabulele Iguosaduwa. 2015. "A Multi-Factor Student Assessment Methodology". *The Pacific Journal of Science and Technology*. 16(1):192 – 200.

30. Elftmann, P. 2006. "Secure Alternatives to Password-Based Authentication Mechanisms". Available at:

https://pdfs.semanticscholar.org/2266/946ed016ea407935216b5ed8117f21ab8da6.pdf.

31. Elias, G., G. Sherwin, and J. Wise. 1984. “Eye Movements while Viewing NTSC Format Television". SMPTE Psychophysics Subcommittee, white paper.

32. English, R. 2014. “Modelling the Security of Recognition-Based Graphical Passwords”. Available at: https://pdfs.semanticscholar.org/a17c/8c3c9da41e5541f8b53b57ed233067f74a6f.pdf.

33. Ensor, B., M. Bennett, and E. Giovannini. 2004. “How Consumers Remember Passwords”. Forrester Research.

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

35. Feingold, A. 1992. “Good-Looking People are not what we Think”. *Psychological Bulletin*. 111:304-341.

36. Fieldmeier, D.C. and P.R. Karn. 1990. “Unix Password Security – Ten Years Later”. Available at: https://pdfs.semanticscholar.org/0924/358924ea433ce5ba5b4dc9fc769ed7afacf6.pdf.

37. Gehringer, E. 2002. “Choosing Passwords: Security and Human Factors”. *ISTAS’02*. 2002, 39-373.

38. Gips, J. 1999. “Computer Implementation of Shape Grammars”. Available at: http://www.shapegrammar.org/implement.pdf.

39. Hlywa, M., R. Biddle, and A. Patrick. 2011. “Facing the Facts about Image Type in Recognition based Graphical Passwords”. *Proceedings of the 27th Annual Computer Security Applications Conference*. 36:149–158.

40. Hollingsworth, A. and J.S. Henderson. 2002. “Accurate Visual Memory for Previously Attended Objects in Natural Scenes”. *Journal of Experimental Psychology – Human Percpetion and Performance*. 28:113-136.

41. Ilett, D. 2004. “Gates: Passwords passé”. *CNET News.com*. Nov. 16. Available at: http://tinyurl.com/bcqt5.

42. Itti, L., C. Koch, and E. Niebur. 1998. “A Model of Saliency-Based Visual Attention for Rapid Scene Analysis”. *IEEE Trans. PAMI*. 20(11):1254–1259.

43. Jackson, L. 2006. “Analysis of Image-Based Authentication and its Role in Security Systems of the Future”. Available at: http://www.soc.napier.ac.uk/~bill/lee2006.pdf.

44. Kaige. 2002. “Fun Password Facts Revisited”. *2600: The Hacker’s Quarterly*. 19(3).

45. Klein, D.V. 1999. “Foiling the Cracker: A Survey of, and Improvements to, Password Security”. 2nd USENIX Security Workshop. 5-14.

46. Komanduri, S. and D.R. Hutchings. 2008. “Order and Entropy in Picture Passwords”. *Proceedings of Graphics Interface, Canadian Information Processing Society*.

47. Kucken, M. and A. Newell. 2004. “Fingerprint Formation”. *Journal of Theoretical Biology*. 235 (2005):71–83.

48. Langlois, J., L. Kalakanis, A. Rubenstein, A. Larson, M. Hallam, and M. Smoot. 2000. “Maxims and Myths of Beauty: A Meta-Analytic and Theoretical Review”. *Psychological Bulletin*. 126:390–423.

49. Lashkari, A.H., O.B. Zakaria, S. Farmad, and R. Saleh. 2009. “Shoulder Surfing Attack in Graphical Password Authentication”. Available at: https://pdfs.semanticscholar.org/a7e3/02754e8e66cf15bb84a1e75322ab6e16c5de.pdf.

50. Li, N., Q. Wang, W. Qardaji, E. Bertino, R. Rao, J. Lobo, and D. Lin. 2009. “Access Control Policy Combining: Theory meets Practice”. In: *SACMAT '09: Proceedings of the 14th ACM Symposium on Access Control Models and Technologies*. 135-144. ISBN 978-1-60558-537-6. doi: http://doi.acm.org/10.1145/1542207.1542229.

51. Luce, T. 1974. “Blacks, Whites and Yellows: They all look alike to me”. *Psychology Today*. 8:105–108.

52. Malpass, R.S. 1992. “They all look alike to me”. *The Undaunted Psychologist*. 74-88. McGraw-Hill: New York, NY.

53. Mandler, J.M. and G.H. Ritchey. 1977. “Long-Term Memory for Pictures”. *Journal of Experimental Psychology: Human Learning and Memory*. 3:386-396.

54. Meissner, C. and J. Brigham. 2001. “Thirty Years of Investigation the Own-Race Advantage in Memory for Faces: A Meta-Analytic Review”. *Psychology, Public Policy & Law*. 7: 3-35.

55. Morris, R. and K. Thompson. 1979. “Password Security: A Case Study”. *CACM 22*. 594-597.

56. Nelson, D.L., U.S. Reed, and J.R. Walling. 1977. “Picture Superiority Effect”. *Journal of*

Experimental Psychology: Human Learning and Memory. 3:485-497.

57. Norman, D.A. 1988. *The Design of Everyday Things*. Basic Books: New York, NY.

58. 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. Journal of Institute of Mathematics & Computer Sciences*. Institute of Mathematics & Computer Sciences:. Kolkata, India. 21(3): 419-433.

59. 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.

60. Onibere, E.A. and A.O. Egwali. 2011. "Evaluating the Security Risks of System Using Hidden Markov Models". *Journal of the Nigerian Association of Mathematical Physics*. 18:401– 06. Indexed in AJOL.

61. Osberger, W. and A.J. Maeder. 1998. "Automatic Identification of Perceptually Important Regions in an Image". *Proc.14th International Conference on Pattern Recognition*.

62. Patrick, A.S., A.C. Long, and S. Flinn. 2003. "HCI and Security Systems". *Proceedings of the CHI 2004*. 1056-1057, ACM Press: New York, NY.

63. Perrig, A. and D. Song. 1999. "Hash Visualization: A New Technique to Improve Real World Security". *International Workshop on Cryptographic Techniques and Ecommerce*. 131–8.

64. 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.

65. Renaud, K. and A. De Angeli. 2009. "Visual Passwords". *Communications of the ACM*. 52:135.

66. Reynolds, R.E., R.M. White, and R.L. Hilgendorf. 1972. "Detection and Recognition of Colored Signal Lights". *Human Factors*. 14:227-236.

67. Salehi-Abari, A., J. Thorpe, and P.C. van Oorschot. 2008. "On Purely Automated Attacks and Click-Based Graphical Passwords". Available at: http://www.cs.toronto.edu/~abari/papers/passpoints_acsac08.pdf.

68. 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.

69. Shepard, R.N. 1967. "Recognition Memory for Words, Sentences, and Pictures". *Journal of Verbal Learning and Verbal Behavior*. 6:156-163.

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

71. Tari, F., A. Ozok, and S. Holden. 2006. "A Comparison of Perceived and Real Shoulder-Surfing Risks Between Alphanumeric and Image-Based Passwords". *Proceedings of the Second Symposium on Usable Privacy and Security*. Pittsburgh, PA. July 12 – 14, 2006, SOUPS'06. 149:56-66. ACM, New York, NY.

72. Thorpe, J. and P.C. van Oorschot. 2004a. "Graphical Dictionaries and the Memorable Space of Image-Based Passwords". *Proceedings of the 13th USENIX Security Symposium*. 9-13. San Diego, CA.

73. Thorpe, J. and P.C. van Oorschot. 2007. "Human-Seeded Attacks and Exploiting Hot-Spots in Graphical Passwords". Available at: https://www.ccsl.carleton.ca/paper-archive/usenix07.hotspots.pdf.

74. Thorpe, J. and P.C. van Oorschot. 2007. "Towards Secure Design Choices for Implementing Image-Based Passwords". Available: http://www.acsac.org/2004/papers/48.pdf.

75. Towhidi, F. and M. Masrom. 2009. "A Survey on Recognition-Based Graphical User Authentication Algorithms". Available at: https://pdfs.semanticscholar.org/6a43/395921cb2deeb5295a330a3c737d5d837b65.pdf.

76. Walker, P. and W. Tanaka. 2003. "An Encoding Advantage for Own-Race versus Other-Race Faces". *Perception*. 23:1117-1125.

77. Walther, D. and C. Koch. 2006. "Special Issue: Modeling Attention to Salient Proto-Objects". *Neural Network*. 19(9):1395–1407.

78. Weirich, D. and M.A. Sasse. 2001. "Pretty Good Persuasion: A First Step towards Effective Password Security in the Real World". *Proc. NSPW'01*. Cloudcroft, NM. 137-143.

79. 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.

80. Wiedenbeck, S., J. Waters, J. Birget, A. Brodskiy, and N. Memon. 2005a. “Authentication Using Image-based passwords Effects of Tolerance and Image Choice”. Available at: http://portal.acm.org/citation.cfm?id=1073001.1073002.

81. Wiedenbeck, S., J. Waters, J. Birget, A. Brodskiy, and N. Memon. 2005c. “PassPoints: Design and Longitudinal Evaluation of a Graphical Password System”. *International Journal of Human-Computer Studies*. 63:1-2.

82. Williams, L.G. 1966. “The Effect of Target Specification on Objects Fixated during Visual Search. *Perception and Psychophysics*. 1:315-318.

83. Wixted, T.J. 2004. “The Psychology and Neuroscience of Forgetting”. *Annual Review of Psychology*. 55:235-236.

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

85. Yan, J., A. Blackwell, R. Anderson, and A. Grant. 2000. “The Memorability and Security of Passwords – Some Empirical Results [Online]”. Available: http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-500.pdf. [Accessed 14 August 2008].

86. Yarbus, A. 1967. *Eye Movements and Vision*. Plenum Press: New York, NY.

87. Zhao, J., Y. Shimazu, K. Ohta, R. Hayasaka, and Y. Matsushita. 1996. “An Outstandingness Oriented Image Segmentation and its Application". *ISSPA.* 45-48.

ABOUT THE AUTHORS

Annie Egwali is an Associate Professor in the Department of Computer Science, at the Faculty of Physical Sciences, University of Benin. Benin City. Nigeria. She holds a Ph.D. degree in Software Engineering from the University of Benin. She is a member of the Nigeria Computer Society (NCS), Institute of Electrical and Electronics Engineers (IEEE), International Network for Women Engineers and Scientists (INWES), Third World Organizations of Women Scientists (TWOWS), National Association for the Advancement of Knowledge (NAFAK), and Nigerian Association of Educationists for National Development (NAEND). Her areas of interest include information technology, software engineering, E-commerce, fuzzy systems, software, and network security. To date, she has supervised several undergraduate and postgraduate students.

John Odetayo, holds an M.Sc. degree in Software Engineering in the Department of Computer Science, at the Faculty of Physical Sciences, University of Benin. Benin City. Nigeria. He is currently undertaking Ph.D. research on network security.

SUGGESTED CITATION

Egwali, A.O. and J.B. Odetayo. 2018. “A Survey Analysis of Recognition-Based Graphical Password Art-form Design Attributes”. *Pacific Journal of Science and Technology*. 19(2):58-73.

Pacific Journal of Science and Technology