Journal of Information Assurance and Security.
ISSN 1554-1010 Volume 15 (2020) pp. 065-075

The is a revised version of the article presented in the 19th International Conference on Intelligent Systems Design and Applications (ISDA 2019), December 3–5, 2019.

# Visual Password Scheme Using Bag Context Shape Grammars

**Blessing Ogbuokiri**[1] **and Mpho Raborife**[2]

[1]*School of Computer Science and Applied Mathematics, University of the Witwatersrand, Johannesburg, South Africa*
ogbuokiriblessing@gmail.com

[2]*Department of Applied Information Systems, University of Johannesburg, South Africa*
mraborife@uj.ac.za

**Abstract**

In this paper, we implemented the similar images generated by bag context shape grammars as distractors in a prototype visual password scheme. A bag context shape grammar is a shape grammar that uses spatial rules to generate images in a regulated manner. That is, during the generative process, bag context is used as a technique to control when a shape grammar rule should be applied. The prototype visual password scheme is used to measure user experience as to whether users can remember their passwords immediately after enrolment and one week later. This is to ascertain whether the similar images generated using bag context shape grammars are good as a distractor for visual password scheme. The prototype visual password scheme is also built for shoulder surfing and guessing attacks resistance. The outcome of this study shows that bag context shape grammars are good for the generation of similar images as distractors for visual password schemes.

***Keywords***: Visual Password, Formal Language, Shape Grammar, Bag Context Shape Grammar.

## I. Background

Authentication is the process of comparing and verifying the credentials of a user or machine to those on a file or database in computers [1, 2]. The process of giving access to a user is called authorization, while the process of restricting access that is available to users is called privilege. For authentication to take place in computers, users must provide information which is verified for access to be granted. Information can be remembered by recall or recognition [3]. Authentication systems are classified into three factors or methodologies [4]; knowledge factor (e.g., password, personal identification number (PIN)); possession factor (e.g., ATM card, smart card); and an inherent factor (e.g., biometric characteristic, such as a fingerprint, iris, etc.).

Authentication methods that depend on one factor are called single–factor authentication (SFA), which is easier to compromise; while authentication methods that depend on more than one factor are called multi–factor authentication (MFA) which is said to be more difficult to compromise. Further, authentication is categorised into; knowledge factor, possession factor, and inherent factor authentication systems.

### *A. Knowledge Factor Authentication Systems*

This factor relies on what the user knows, which involves the ability of the user to recall or recognize. It is divided into cued recall based, recognition based, recall based, and hybrid systems based. The most popular in use today is recall based [5]. One example of a recall based authentication is passwords (alphanumeric passwords). Passwords are a string of definite length that are made up of a combination of characters, numbers and sometimes special characters. They are SFA based authentication method because they depend on what the user knows only. That is, they do not depend on or a combination of any other factor to work. The challenge of alphanumeric passwords is that they can easily be guessed, eavesdropped, stolen, shoulder surfed and hacked, etc., [6, 7]. Alphanumeric passwords are vulnerable to attacks because a number of people use easy to remember passwords, such as; names of their pet, children, events, models, etc [8]. Secure alphanumeric passwords must be long and with a combination of characters and numbers [9]. Unfortunately, the longer a password is, the more difficult it is to remember or to attack and vice verse.

### *B. Possession Factor Authentication Systems*

This method relies on the items that the user has. That is, the user presents a hardware device or token to gain access. Examples are Automated Teller Machine (ATM) cards, Integrated Campus Management (ICAM) cards, credit/debit cards, smart cards, etc. These cards can be cloned [5]. Possession factor authentication systems are regarded as multifactor authentication methods because they do not only depend on what the user has (the card) but what the

user knows such as Personal Identification Number (PIN). The PIN could also get lost or forgotten by the user, which endangers the users' access [9]. Attacks on possession factor authentication systems can occur in different ways such as phishing, malware or credit card reader skimming [10].

### C. Inherence Factor Authentication Systems

These factors refer to credentials consisting of individual's unique features. It is a multi-factor method because it relies on the biological or physiological features of a user and a hardware device. In Ray [11], individuals' credentials could be obtained from two main technologies; contact metric or contactless metric. A contact metric technology is one that the individual makes contact with a device in order to gain access. Examples are fingerprint scan, dynamic signature verification, etc., [12, 13]. Diseases like Ebola, Corona Virus, etc., could be contacted through this method when an infected person touches the device and a healthy person goes to use the same device. On the other hand, contactless metric technologies are one the user does not make contact with any device but camera or similar devices capture the biological or physiological features [14, 15]. Examples of contactless metric technologies are facial recognition technologies and palm vein access control, etc. The major drawback of this factor is that biometric features change as individuals get old or when they have an accident. Enrolment and storage processes are usually very slow which shows it may only work better with a small number of person [16]. Moreover, they may require expensive equipment to work [17].

Criminals have taken advantage of these authentication problems to impersonate peoples' digital credentials to perpetrate crimes. Globally, more than 556 million people have become victims of these crimes in the last 13 years [18, 19]. According to the United States federal trade commission [20], 40% of initial contacts of most fraud cases were by email, and 20% by Internet websites. In this context, it is estimated that 332,646 victims were affected by financial losses totalling $110 billion dollars [20]. In 2015, it is also estimated that R57.8 million was lost due to unauthorized access to computers in South Africa [21]. In the light of the above, visual passwords have been proposed as a replacement for alphanumeric passwords or biometric authentication systems [22, 23].

## II. Visual Password Schemes

Visual Password Schemes (VPSs) are authentication systems that use images for enrolment and authentication [24–27]. They are classified into recognition or cued recall [26]. VPSs have memory advantages over alphanumeric passwords because passwords are based on pure recall which can easily be forgotten due to human errors [28]. Studies have shown that pictures are recognized with 98 percent accuracy than words and sentences after a long time [21]. According to Shepard [29], seventeen percent recognition error was recorded after viewing 10,000 pictures. This shows that pictures are more easily recalled than passwords [30].

### A. Recognition Based Visual Password Schemes

In Recognition Based Visual Password Schemes (RBVPSs), also known as Cognometric Systems or Searchmetric Systems [11], the user chooses a pass image from a list of distractor or decoy images during enrolment. During authentication, access is granted when the user recognizes the image used for enrolment. Access is granted when the user recognizes and selects the pass image otherwise access is denied [26]. One major example of RBVPSs is the Passfaces. Passfaces are graphical passwords that use faces for enrolment and verification [31]. In this method, a user is allowed to choose four pictures of human faces from a log of human face pictures displayed. During authentication, the system displays nine faces in a three by three grid which consists of one of the faces previously selected by the user during enrolment. If the user clicks on the right image, the process is repeated until the four faces selected during enrolment are verified. At this time access will be granted [31].

One of the challenges of RBVPSs is that image selection and retrieval from an image dataset could slow the entire process [32]. Generally, RBVPSs display few images and one is chosen as the passface (passwords). Attackers may have one out nine chance of guessing image in a set of nine pictures displayed due to the nature of Passfaces method. Moreso, the use of faces for passwords have proven to have very low entropy because people choose faces of celebrities, beautiful people, and relations, etc., making it easily predictable [3]. Furthermore, Townhidi *et al.* [33] developed a cognometrics system which is more secure than passfaces called Secure-Passfaces (S–Passfaces). S–Passfaces is based on three modifications of Passfaces; making keyboard the input method of selecting passwords, creating four pass–images which run concurrently in pairs, allowing users to pick their own pass images for improved memorability [33]. Their test on security and usability of S-Passfaces shows that it was slightly less usable because of the additional security measures compare to Passfaces. Although, users were confident and willing to use the system because of the added security measures.

According to Dhamija and Perrig [32] (in [3]), Hash Visualization Technique (HVT) was used to develop a graphical authentication scheme. This type of scheme allows a user to select some images from randomly generated pictures. Authentication is successful when the user selects the earlier selected image. A major drawback of this system is that picture selection process from the database is tedious and time-consuming.

Wayne *et al.* [34], developed a picture password that uses thumbnail photos which are used to derive passwords. In their work, random character codes are assigned to images which form the passwords. The pictures are presented in $40 \times 40$ pixels, grouped into $5 \times 6$ matrix of elements. Selecting and submitting the correct sequence of thumbnail images authenticates the user to the device. After successful

authentication, the user changes the password by selecting a new theme.

A major reason picture-based passwords are seen as superior to other authentication schemes is that people encode images in their minds in two different ways; by remembering both the visual configuration and a lexical description of the picture, and pictures are stored more comprehensively and with more mental pathways which can be used to retrieve them from memory [24]. According to Renaud and Antonella [24], pictures are classified into three distinct groups as used in authentication:

1. Searchmetric systems: These methods require searching for images in a challenge set. Target images are selected by a variety of input techniques, ranging from direct touch to indirect operation of other interface devices.

2. Locimetric systems: These methods require identification of a series of positions within an image; and

3. Drawmetric systems: These systems require the user to sketch a drawing [24].

### *B. Cued Recall Visual Password Schemes*

Cued Recall Visual Password Schemes (CRVPSs) also called iconmetric systems are methods that provide users with hint so that they can recall their password [11]. It is divided into two sections, namely; reproducing a drawing and repeating a selection [3].

#### *1) Reproduce a Drawing*

Reproduce a drawing is a technique used by Jermyn *et al.* [7] in their work called Draw A Secret (DAS). According to Jermyn, *et al.* [7], users draw their passwords as a simple picture on a two dimensional grid. The system stores the coordinate of the picture in order of drawing. The user redraws the picture during authentication. Access is granted when the coordinates of the new drawing touch the same grid in the same order it was initially drawn.

The security of DAS is low as originally believed [35]. Thorpe and van Oorschot [35], tested brute-force attack using graphical dictionaries they developed on DAS. Their experiment proved that DAS passwords of length 8 or larger on a $5 \times 5$ grid may be less susceptible to dictionary attack than textual passwords. They also observed that space of mirror symmetric graphical passwords is smaller than the DAS passwords space.

Users typically easily recall symmetric images (images that appear the same when flipped, turned or slided) than asymmetric images (images that do not appear the same when flipped, turned or slided), more users may subscribe to symmetric passwords thereby exposing DAS passwords to danger. The size of DAS passwords decreases with few strokes for a fixed password length.

According to Thorpe and Oorschot [35] stroke-count has a serious impact on DAS password space. To improve the security of DAS, Grid Selection method was developed by Thorpe and Oorschot [35]. In their work, the user selects a drawing grid (a rectangular region) in which they enter their password from initially large, fine-grained grid. This is expected to increase DAS passwords space.

Meanwhile, Syukri *et al.* [36] developed a system that allows users to draw their input as a signature with a mouse. During enrolment, the system extracts users' signature area and normalize it. The normalized parameter is stored in the database. For successful authentication to take place, users' signature will be extracted and normalized, then, the system authenticates the signature using geometric average means and a dynamic update of the database. This system eliminated the need to memorize passwords. Although, it is very hard to draw signature with a mouse. The only alternative is to use pen-enabled input device which may be expensive.

#### *2) Repeating a selection*

This method requires a user to select or click on an image a number of times. Examples of this type of system are the graphical passwords system developed using Passlogix [37, 38]. In these systems, boundaries are defined for each image to detect when an image is clicked. During authentication, the user is expected to click on preselected areas of an image in a predefined sequence.

Different approaches have been proposed to improve visual password schemes. Okundaye [5], proposed a tree based visual password scheme. In this work, tree grammars were used to generate syntactic images for visual passwords. Unlike other Passfaces, the similarity of images and human perception of images were obtained with the system.

Rasekgala *et al.* [39, 40] used shape grammars in the design of their visual password schemes. They used shape grammars in the generation of basic shapes under the control of the user. These are similar to the study at hand as they involve the use of grammars in generating images. Unfortunately, they did not use bag context to control the images generated. Other works in regard to Passfaces as summarized in [11] are; cognitive authentication [41], use your illusion [42], visual identification protocol [43, 44], photographic authentication [45], and graphical password with icons/graphical password with icons suggested by the system [46].

To solve some of these challenges identified in visual password schemes like; biased pass image selection as people tend to select faces from their own race or background or attractive faces or the faces of models which makes it prone for guessing attacks, static image representation during enrolment and authentication which makes it easy for shoulder surfing attacks, consumption of large memory space and high bandwidth connection needed for passing images to and from during authentication. The approach of

picture grammars for the generation of abstract images for visual passwords was introduced [23].

## III. Picture Grammars

A picture grammar is an abstract structure with which one can generate a set of images [47]. One form of picture grammars is called shape grammars. A shape grammar uses spatial rules to generate images. The use of shape grammars for image generation does not always produce images in a regulated manner. They generate images without considering the similarity between them. However, research has shown that control can be added to the grammar based image generation process using a technique called bag context [48]. Bag context is a technique used to control the derivation (generation process) of an image. This type of technique, when added to shape grammar rules is called Bag Context Shape Grammars (BCSGs) [49]. BCSGs is a type of shape grammar that generate an infinite number of images in a regulated manner by controlling when a shape grammar rule should be applied during the generation process [49–51].

The essence of this paper is to implement the similar images generated by BCSGs as distractors in a prototype visual password scheme (VPS) [27, 50]. A distractor is an image in a visual password system that diverts the attention of a user from the desired area of focus during login or incorrect image choices that looks similar [23, 50]. The prototype visual password scheme is used to measure user experience as to whether users can remember their passwords immediately after enrolment and one week later. This is to ascertain whether the similar images generated using BCSGs are good as a distractor for a visual password scheme. The prototype visual password scheme is also built for shoulder surfing and guessing attacks resistance. The outcome of this study shows that BCSGs is good for the generation of similar images as distractors for visual password schemes.

The remainder of the paper is organised as follows. Section IV presents the visual password design, followed by the usability study in Section V. In Section VI, we present the performance analysis of the VPS, and finally, Section VII is the conclusion and future work.

## IV. VPS Design

Here, we present the building blocks of the VPS in Section IV-A.

### A. Structure

The VPS is divided into three major parts, namely, enrolment, authentication and the admin. Each part is discussed briefly.

1. **Enrolment:** This part is where the generation of images (distractors or decoy) and the registration of password begins. The generation process is done by the BCSG interpreter that is embedded in the VPS. The BCSG interpreter models shape grammar rules into an image. A user is allowed to select the kind of predefined initial image. Every initial image has its own predefined rules which can generate infinitely different similar images. The system uses the selected initial image as a sample to generate nine distractors using the predefined rules. The nine distractors are randomly displayed on the screen. A user selects the image of choice to use as a password from the randomly displayed images. The system shuffles the images on the screen and requests that the user confirms image selection. The user is asked to supply an identification (ID) number as a means of a unique identifier just in case the user wants to change his password.

   The selected image is converted to a vector using the spatial colour distribution descriptor (SpCD) [52] and stored as an Extensible Markup Language (XML) file. The XML file is a file that defines a set of rules for encoding documents in a format that is both human and machine readable. The initial shape that was used to generate the image and the ID number are also saved.

2. **Authentication:** This part involves the verification of the image password selected by the user. Nine distractors are displayed on the screen. The system uses the saved initial shape in 1. and the appropriate predefined rules to generate the equivalent image distractors generated during enrolment. The nine images are displayed on the screen. One of the nine images must correspond exactly to the image password selected during enrolment.

   When a user selects an image, the system converts it to a vector using SpCD and matches the same with the saved vector in the XML file. Then the system shuffles the images and requests that the user selects another image. This process is repeated three times. If the result of the three attempts are the same, that is, the vector matches the one in the XML file for the three attempts, then access is granted.

   When a user does not remember his or her password, the system requests that the user supplies his ID number inorder to change the password.

3. **Admin:** This part overwrites any account. That is, it can deny or grant access at any time. Next, we present the architecture of the system in diagram (see Section IV-B).

### B. System Architecture

In this section, the system architecture is shown in Fig. 1. The architecture represents how each of the components of the VPS communicates to each other. Next, we discuss the human computer interaction (HCI) design of the VPS.

### C. HCI design

According to cognitive psychology, the way in which humans receive, process and store information, solve problems and acquire skill is very crucial [53]. Research in this area has shown that recognition is easier than recall, as such, humans remember images easily after a long period [53]. In

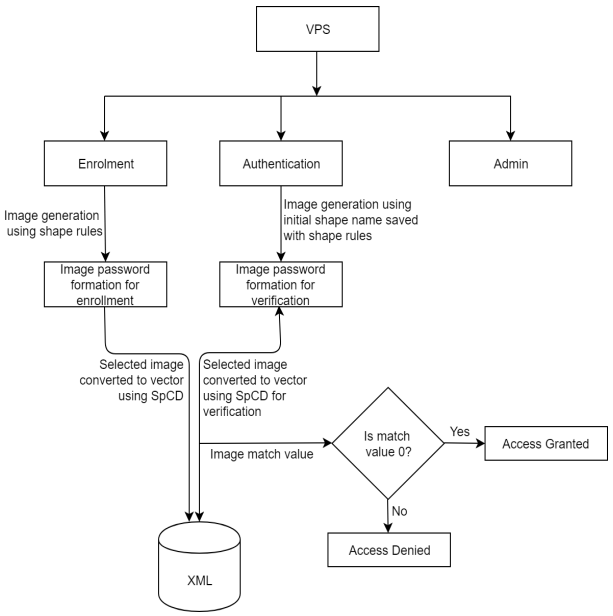


**Figure. 1**: The VPS architecture

order to design an interactive and an easy to use system, our type of VPS interface is designed having in mind the way in which humans receive, process and store information in order enhance recognition of image password [54].

*1) Layout*

The VPS layout is designed based on the International Telecommunication Union (ITU E.1.161) standard and recommendation for the arrangement of a digit, letters, and symbols on the telephone and other devices that can be used for gaining access to a telephone network [55]. The standard number for push buttons are ten digits, 0 to 9. The standard arrangement is 3 x 4 array as shown in Figure 2. The VPS layout was designed to randomly display images on a $3 \times 3$ array. The picture boxes (Image 1 to Image 9) in Figure 3 presented in the 3 x 3 array are mimicked from the push buttons arrangement in Figure 2 leaving out the last row. Each picture box is of size 130 pt x 130 pt. The 3 x 3 array is organised in a (550 pt x 550 pt) frame.

Therefore, during rendering, the system is designed to automatically pick the size of the device screen and displays the frame at the centre of the screen.

| | | |
|---|---|---|
| 1 | 2 | 3 |
| 4 | 5 | 6 |
| 7 | 8 | 9 |
| | 0 | |

**Figure. 2**: Push buttons arrangement

*2) GUI*

Designing the graphic user interface (GUI) is very crucial as the choice of colour, font type, and font size can affect users interest [56]. According to colour psychology [53], the majority of people see blue as their favourite colour. This

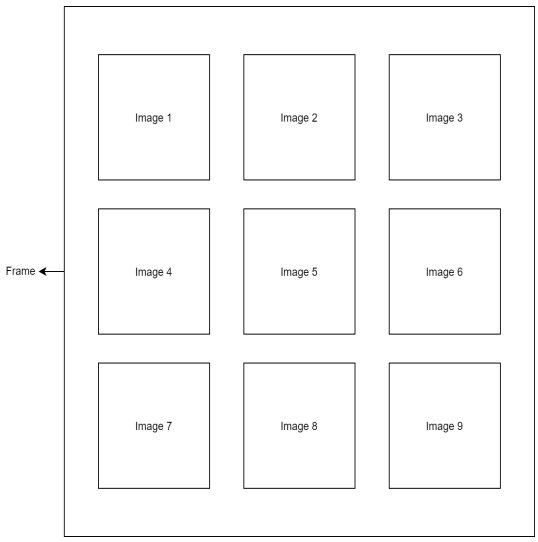


**Figure. 3**: The VPS Layout

is because most colour blind people can see the colour blue and it is associated with nature (e.g. clean water, clear sky, etc.), and more. This motivated our choice of blue as the font colour on a white background. The Sans Serif bolded font size 14 is used to assist users with visual impairments. The Sans Serif font is a category of the font that does not use serif, small lines at the ends of characters.

**Login GUI Design** The login design is where the verification is done (see Figure 4). It is made up of four parts as listed below:

1. Admin – denies and grants access to users at any time.
2. Login frame – holds and displays the nine distractors or decoy images for verification.
3. Create New Password – allows a user to generate and select new image password.
4. Forgot Password – requests users identification number for image password change.
5. Number of Trials – keeps count of login attempts by a user.

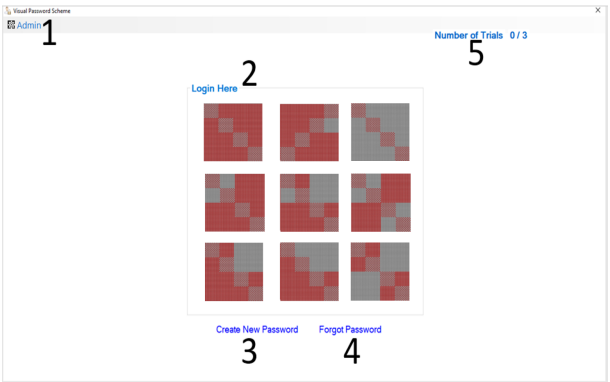


**Figure. 4**: The VPS Login design

**Enrolment GUI Design** This module is made of three major parts, which are listed below:

1. Select Shape – allows a user to choose the type shape he wants to use for the image generation.
2. Image Type – allows the user to choose the type of image he wants to generate using the selected shape.
3. Image Frame – holds the randomly displayed nine distractor images.

### *D. Password Design*

Password formation is done by first, partitioning the picture into 64 ($8 \times 8$) equal blocks. Then, the image is transformed into a 64 coefficient matrix using SpCD. A zigzag scan [57] is performed on the 64 coefficient matrix inorder to reduce it to a vector which is saved for verification (See Figure 5).

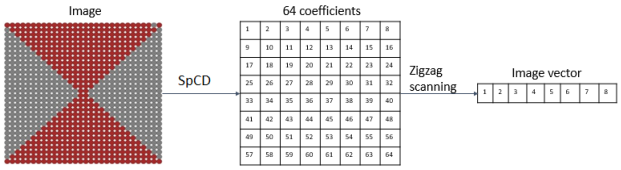


**Figure. 5**: The VPS passwprd formation

### *E. Strength Analysis*

Here, we discuss the ability of the VPS for shoulder surfing and guessing attacks resistance. Shoulder surfing occurs when an attacker learns a user's password by watching the user login. That is, an attacker takes up a position where the user's login details can be seen while he login. The attacker can achieve this aim by watching with the optical eyes, a special camera, video recorder or binocular, etc [58]. Guessing or Brute force attack involves trying every possible combination or trials until the correct password is found [58, 59]. Shoulder surfing and guessing attack resistance have improved significantly over the years [58–60].

To prevent these attacks in our type of VPS, we implemented similar images which act as distractors to the target image, and to the human attacker who observes from a distance. Also, the distractors are randomly displayed at every trial during authentication. This means that the nine images are shuffled when they are displayed on the screen at every trial. The user has to identify the image he selected earlier and select it again. The user has to make three accurate trials for access to be granted. If the user fails at any stage of the three attempts, he will not be notified of the particular stage at which he made the mistake.

Although, large password space contributes largely to the security of a system, which is the main defence against a brute force attack. However, most recognition based graphical passwords tends to have a small password space [61]. This is because picture passwords are mostly used in mobile devices, as such, password space must be limited [61]. An increased password space is not realistic for users [61].

Interestingly, it is more difficult to carry out a brute force attack against visual passwords than alphanumeric passwords [62].

## V. Usability Study

In this section, we look into users ability to remember a password immediately after enrolment and the user's ability to remember the password at least one week later.

### *A. Participants*

A hundred and eleven novice users, who are not familiar with the VPS were trained to use the VPS. The participants were 67 male and 44 female with an average age of 25 years. These set of participants were taken because they are expert computer users who use computers for at least 4 to 5 hours a day, either for personal research or work activities.

### *B. Materials*

Most of the computers used in testing the VPS displayed nine images of equal size in a frame on the center of a screen of standard size. The nine images are randomly displayed at every trial. The system displays the images randomly to determine whether a novice could learn, remember, and select the image password successfully. The time it takes for a successful authentication is recorded by the system.

### *C. Procedure*

The participants were divided into four groups. Each group was trained separately by the researcher. After the initial training and explanation of how the system works and how to identify an image. The researcher demonstrated the system by showing the participants how to create a password and how to log into the computer with the password.

Then, the participants were guided to create their password individually. All the participants created their password successfully. The participants were asked to use the password they created to login into the computer. At this time, the participants were not guided any more. A number of the participants were able to remember their passwords and login successfully, immediately after the enrolment. The time for each successful login was recorded. The participants were interviewed to get their perception of the system.

Furthermore, one week after the enrolment, a follow up was initiated. The participants were reminded to login to determine whether they could still remember their image passwords. The outcome is discussed in Section V-D. The Chi-Square $(\mathrm{X}^2)$ test was used to analyse the association between a participants ability to login to the computer immediately and one week later. That is, if those who successfully login immediately and one week later, did that by chance or they remembered their passwords and vice versa.

**Hypothesis One**

- $\mathrm{H}_0$: The null hypothesis assumes that there is no association between a participants ability to login immediately and one week later,

- $H_1$: The alternative hypothesis claims that there is some association between a participants ability to login immediately and one week later.

### *D. Results*

All participants were able to complete the process of login and authentication. The outcome is grouped and summarised in Table 1 also called observed data. The $X^2$ test is based on a test statistic that measures the divergence of the observed data from the values that would be expected or expected values (see Table 2). The expected value for each cell is generated from the observed data in Table 1 as thus:

$$(\text{row\_total} * \text{column\_total})/\text{n}, \tag{1}$$

where $n$ is the total number of observations in the table. If the expected value for each cell is greater than or equal to 5, then, the $X^2$ is good for the experiment, otherwise, another test statistic will be used. For example, the value in column two, row two of the expected values table (see Table 2) is calculated using Equation 1 to be

$$39 * 46/111 = 16.16216$$

*Table 1*: Observed Data

| | | One week after | | |
|---|---|---|---|---|
| | | **No** | **Yes** | **Total** |
| Immediately | **No** | 24 | 15 | 39 |
| | Yes | 22 | 50 | 72 |
| | **Total** | 46 | 65 | 111 |

*Table 2*: Expected values

| | | One week after | | |
|---|---|---|---|---|
| | | **No** | **Yes** | **Total** |
| Immediately | **No** | 16.16216 | 22.83784 | 39 |
| | Yes | 29.83784 | 42.16216 | 72 |
| | **Total** | 46 | 65 | 111 |

From Table 1, 24 participants are not able to remember their password immediately and one week later, 22 remembered their passwords immediately and forgot it one week later. 15 participants could not remember their password immediately but remembered it one week later, while 50 participants were able to login immediately and also one week later. From the results, there are 72 (64.9%) of the total number of participants who were able to login immediately while 39(35.1%) could not log in immediately.

The results suggest that the majority of the participants were able to log into the system immediately. There were 65(58.6%) of the total number of participants who were able to log into the system one week later successfully and there were 46 (41.4%) of the total number who were not able to log into the system after one week. There was a decrease in the total number of participants who were able to log into the system immediately compared to the total number that logged into the system one week later.
The $X^2$ test statistic is computed using Equation 2.

$$X^2 = \sum_{i}^{k} \frac{(O_i - E_i)^2}{E_i} \tag{2}$$

where the observed value for each cell in Table 1 is denoted by $O_i$, and the expected value for each cell in Table 2 is denoted by $E_i$. The variable $i$ is the specific cell in the table and $k$ represents the total number of cells without the total column or row.

For example, using the Equation 2, we obtain the $X^2$ test statistic as thus

$$\begin{aligned} X^2 &= \frac{(24-16.16216)^2}{16.16216} + \frac{(15-22.83784)^2}{22.83784} + \\ &\quad \frac{(22-29.83784)^2}{29.83784} + \frac{(50-42.16216)^2}{42.16216} \\ &= 3.80096 + 2.86991 + 2.05885 + 1.45703 \\ &= 10.18675 \end{aligned}$$

Then, we proceed to calculate the probability value (p-value) of the $X^2$ test statistic. The p-value helps to support the claim as to whether to accept or reject the $(H_0)$. The p-value is also evidence against the $H_0$. Therefore, $H_0$ is rejected if the p-value is $\leq 0.05$. According to the experiment, the p-value = 0.00156 using the z table.

### *E. Discussion*

The results of the $X^2$ test statistic show that there is a statistically significant ($X^2$ = 10.18675, p-value=0.00156) relationship or association between a participant's ability to log into the system immediately after enrolment and one week later. We, therefore, reject the $H_0$ and accept the alternative hypothesis $H_1$. Hence, there is an association between the two variables. That is to say, those who remembered their passwords immediately and one week later was not by chance.

The odds (odds ratios[1]) of a successful login immediately are 3.64 times the odds of an unsuccessful login. The odds ratio is significant (p-value=0.002) with a confidence interval[2] of (1.61, 8.23).

## VI. Performance Analysis

We tested the VPS performance in terms of its ability to produce the right result at the shortest possible time. We recorded the times it took for 20 successful logins on the machine the application was built and arrived at an average of 12.6 seconds and standard deviation of 3.2671. Then, we compared the times to the average of 20.7 seconds of the 72 successful logins on the different machines with a standard deviation of 8.2619.

[1]The measure of an association between an exposure and an outcome.

[2]Used to estimate the precision of the odds ratio.

The essence is to know if the performance of the system is machine bias. That is, if the performance in terms of time is dependent on the machine or not. The Independent Samples *t* test is used to compare the means of the two independent group of times (seconds) to determine whether there is statistical evidence that the associated time means are significantly different.

**Hypothesis Two**

- $\mathrm{H}_0$: The null hypothesis assumes that the time means are not significally different
- $\mathrm{H}_1$: The alternative hypothesis assumes that there is a signficant difference in the time means.

Therefore, $\mathrm{H}_0$ is rejected if the p-value is $\leq 0.05$.

*A. Result*

The independent *t* test statistic is calculated using the Equation 3.

$$\mathrm{t} = \frac{\bar{\mathrm{X}_1} - \bar{\mathrm{X}_2} - (\mu_1 - \mu_2)}{\mathrm{s_p}\sqrt{\frac{1}{\mathrm{n_1}} + \frac{1}{\mathrm{n_2}}}} \mathrm{s_p} = \sqrt{\frac{(\mathrm{n_1}-1)\mathrm{s_1^2} + (\mathrm{n_2}-1)\mathrm{s_2^2}}{\mathrm{n_1}+\mathrm{n_2}-2}} \tag{3}$$

Where the variables $\bar{X_1}$ = mean of sample 1, $\bar{X_2}$ = mean of sample 2, $\mu_1 - \mu_2$ = difference in the two population means, $s_1^2$ = sample varience of sample 1, $s_2^2$ = sample varience of sample 2, $n_1$ = size of sample 1, and $n_2$ =size of sample 2.

**Note**: Sample 1 is for the main machine, while sample 2 is for different machines. The experiment performed using the Equation 3 showed that the independent *t* test statistic is -4.3195 and the p-value = 0.000004.

*B. Discussion*

The results of the $t$ test statistic show that $t$ = -4.3195 and p-value = 0.000004 using the $t$ table, this implies that, there is a statistically significant difference between the time means. We reject the null hypotheses $\mathrm{H}_0$ and accept the alternative hypotheses $\mathrm{H}_1$. This simply means that the run time of the VPS could be affected by the machine used.

## VII. Conclusion and Future Work

In this paper, we implemented the VPS using the BCSGs generated images. The similar images which act as distractors were randomly displayed to improve shoulder surfing and guessing attacks resistance in the VPS design. The VPS was tested for human usability, which proves that several people could remember their image password after one week. The performance of the VPS in terms of run time was tested. It is also observed that the VPS performance could be affected by the type of machine used. Finally, the findings in this paper suggest that BCSGs is good for the generation of similar images as distractors for visual password schemes.
In the future, if this idea is implemented in a robust software tool, it will find applications in the industry where password security is important.

## Acknowledgements

The authors would like to thank the Department of Science and Technology (DST) and the Council for Scientific and Industrial Research (CSIR) Inter-bursary support programme, South Africa, for funding this research.

## References

[1] M. KOTHAVALE, "Computer security ss3: Biometric authentication [online accessed]. 15.05. 2020," *http://www. cs. bham. ac. uk/~ mdr/teaching/modules03/security/students/SS3/handout/index. html*.

[2] M. Hogan, "Are you who you claim to be?, national institute of standards and technology, international standards organisation," 2003.

[3] X. Suo, Y. Zhu, and G. S. Owen, "Graphical passwords: A survey," in *Computer security applications conference, 21st annual*. IEEE, 2005, pp. 10–pp.

[4] J. Nicholson, "Design of a multi-touch shoulder surfing resilient graphical password," *B. Sc in Information Systems, Newcastle University, Newcastle*, 2009.

[5] B. Okundaye, "A tree grammar-based Visual Password Scheme," Ph.D. dissertation, School of Computer Science and Applied Mathematics, University of the Witwatersrand, Johannesburg, 2015.

[6] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Effects of tolerance and image choice," in *Proceedings of the 2005 Symposium on Usable Privacy and Security*. ACM, 2005, pp. 1–12.

[7] I. Jermyn, A. J. Mayer, F. Monrose, M. K. Reiter, A. D. Rubin *et al.*, "The design and analysis of graphical passwords." in *8th Usenix Security Symposium*, 1999, pp. 1–14.

[8] H. Benko, A. D. Wilson, and P. Baudisch, "Precise selection techniques for multi-touch screens," in *Proceedings of the SIGCHI conference on Human Factors in computing systems*. ACM, 2006, pp. 1263–1272.

[9] F. F. I. E. Council, "Authentication in an Internet banking environment," *Financial Institution Letter, FIL-103-2005. Washington, DC: Federal Deposit Insurance Corporation (FDIC).*, vol. 18, pp. 1–14, 2005.

[10] R. E. Smith, *Elementary information security*. Jones & Bartlett Publishers, 2015, no. 2.

[11] P. P. Ray, "Ray's scheme: graphical password based hybrid authentication system for smart hand held devices," *International journal of computer trends and technology*, vol. 3, pp. 235–241, 2012.

[12] D. Maltoni, D. Maio, A. Jain, and S. Prabhakar, "Handbook of fingerprint recognition springer verlag," *Nu, USA*, 2003.

[13] M. Upmanyu, A. M. Namboodiri, K. Srinathan, and C. Jawahar, "Blind authentication: a secure crypto-biometric verification protocol." *IEEE transactions on information forensics and security*, vol. 5, no. 2, pp. 255–268, 2010.

[14] M. Watanabe, T. Endoh, M. Shiohara, and S. Sasaki, "Palm vein authentication technology and its applications," in *Proceedings of the biometric consortium conference*, 2005, pp. 19–21.

[15] B. Ogbuokiri and M. Agu, "An enhanced authentication system using face and fingerprint technologies," *IOSR Journals (IOSR Journal of Computer Engineering)*, vol. 1, no. 17, pp. 74–84, 2015.

[16] L. O. Gorman, "Comparing passwords, tokens, and biometrics for user authentication," *Proceedings of the IEEE*, vol. 91, no. 12, pp. 2021–2040, 2003.

[17] P. Hunter, "Biometrics latest: one size does not fit all comers," *Computer Fraud & Security, Elsevier*, vol. 2004, no. 8, pp. 7–9, 2004.

[18] M. Kara, "Identity theft in united states of amarica, bureau of justice statistics,us." *Retrieved from http://www.ojp.gov/*, 2015.

[19] D. Rob, "Identity theft victims statistics," *Identity theft and scan prevention services official website, retrieved from http://www.identitytheft.info/victims.aspx*, 2016.

[20] U. F. T. Commission *et al.*, "Consumer sentinel network data book for january–december 2014," 2015.

[21] A. Stander, A. Dunnet, and J. Rizzo, "A survey of computer crime and security in south africa." in *ISSA*, 2009, pp. 217–226.

[22] A. B. Hassanat, "Visual passwords using automatic lip reading," *arXiv preprint arXiv:1409.0924*, 2014.

[23] B. Okundaye, S. Ewert, and I. Sanders, "A novel approach to visual password schemes using tree picture grammars," in *Proceedings of the 2014 PRASA, RobMech and AfLaT International Joint Symposium*, 2014, pp. 247–252.

[24] K. Renaud and A. De Angeli, "Visual passwords: cure-all or snake-oil?" *Communications of the ACM*, vol. 52, no. 12, pp. 135–140, 2009.

[25] K. Revett, *Behavioral biometrics: a remote access approach*. John Wiley & Sons, 2008.

[26] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, "Passpoints: Design and longitudinal evaluation of a graphical password system," *International Journal of Human-Computer Studies*, vol. 63, no. 1, pp. 102–127, 2005.

[27] B. Ogbuokiri and M. Raborife, "Visual password scheme using bag context shape grammars," in *Proceedings of the 19th International Conference on Intelligent Systems Design and Applications*. ISDA 2019, December 3–5, 2019.

[28] D. A. Norman, *The design of everyday things: Revised and expanded edition*. Basic books, New York, 2013.

[29] R. N. Shepard, "Recognition memory for words, sentences, and pictures," *Journal of verbal Learning and verbal Behavior*, vol. 6, no. 1, pp. 156–163, 1967.

[30] A. Paivio, T. B. Rogers, and P. C. Smythe, "Why are pictures easier to recall than words?" *Psychonomic Science*, vol. 11, no. 4, pp. 137–138, 1968.

[31] C. RealUser, "The science behind passfaces," *http://www.realusers.com. Accessed June. 25*, 2016.

[32] R. Dhamija and A. Perrig, "Deja vu-a user study: Using images for authentication." in *USENIX Security Symposium*, vol. 9, 2000, pp. 4–4.

[33] F. Towhidi, M. Masrom, and A. Manaf, "An enhancement on passface graphical password authentication," *J. Basic. Appl. Sci. Res*, vol. 3, no. 2, pp. 135–141, 2013.

[34] W. Jansen, S. Gavrila, V. Korolev, R. Ayers, and R. Swanstrom, "Picture password: a visual login technique for mobile devices," *Citeseer*, 2003.

[35] J. Thorpe and P. C. van Oorschot, "Towards secure design choices for implementing graphical passwords," in *Computer Security Applications Conference, 2004. 20th Annual*. IEEE, 2004, pp. 50–60.

[36] A. F. Syukri, E. Okamoto, and M. Mambo, "A user identification system using signature written with mouse," in *Australasian Conference on Information Security and Privacy*. Springer, 1998, pp. 403–414.

[37] S. M. Kumar and P. Rodrigues, "A roadmap for the comparison of identity management solutions based on state-of-the-art idm taxonomies," in *International Conference on Network Security and Applications*. Springer, 2010, pp. 349–358.

[38] L. D. Paulson, "Taking a graphical approach to the password," *Computer*, vol. 35, no. 7, pp. 19–19, 2002.

[39] M. Rasekgala, I. Sanders, S. Ewert, and T. Fogwill, "Shape grammar model generating secure visual passwords: The move towards completely grammar based images," in *Second International Conference on Advances in Computing, Communication and Information Technology - CCIT 2014*. Birmingham, UK, 2014, pp. 208–214.

[40] M. Rasekgala, S. Ewert, I. Sanders, and T. Fogwill, "Requirements for secure graphical password schemes," in *IST-Africa Conference Proceedings, 2014*. IEEE, 2014, pp. 1–10.

[41] D. Weinshall, "Cognitive authentication schemes safe against spyware," in *2006 IEEE Symposium on Security and Privacy (S&P'06)*. IEEE, 2006, pp. 6–pp.

[42] E. Hayashi, R. Dhamija, N. Christin, and A. Perrig, "Use your illusion: secure authentication usable anywhere," in *Proceedings of the 4th symposium on Usable privacy and security*. ACM, 2008, pp. 35–45.

[43] A. De Angeli, L. Coventry, G. Johnson, and K. Renaud, "Is a picture really worth a thousand words? exploring the feasibility of graphical authentication systems," *International Journal of Human-Computer Studies*, vol. 63, no. 1, pp. 128–152, 2005.

[44] W. Moncur and G. Leplâtre, "Pictures at the atm: exploring the usability of multiple graphical passwords," in *Proceedings of the SIGCHI conference on Human factors in computing systems*. ACM, 2007, pp. 887–894.

[45] T. Pering, M. Sundar, J. Light, and R. Want, "Photographic authentication through untrusted terminals," *IEEE Pervasive Computing*, vol. 2, no. 1, pp. 30–36, 2003.

[46] K. Bicakci, N. B. Atalay, M. Yuceel, H. Gurbaslar, and B. Erdeniz, "Towards usable solutions to graphical password hotspot problem," in *2009 33rd Annual IEEE International Computer Software and Applications Conference*, vol. 2. IEEE, 2009, pp. 318–323.

[47] N. Jingili, S. Ewert, and I. Sanders, "Syntactic generation of similar pictures," in *Obaidat M., Ören T., Rango F. (eds) Simulation and Modeling Methodologies, Technologies and Applications. SIMULTECH 2018*. Springer, Cham, 2020, pp. 153–180.

[48] F. Drewes, C. Du Toit, S. Ewert, B. Van Der Merwe, and A. P. Van Der Walt, "Bag context tree grammars," in *Developments in Language Theory*. Springer, 2006, pp. 226–237.

[49] B. Ogbuokiri and M. Raborife, "Bag context shape grammars," *IAENG International Journal of Computer Science*, vol. 47, no. 1, pp. 75–86, 2020.

[50] ——, "The similarity of images generated by bag context shape grammars," in *Proceedings of the 2020 International SAUPEC/RobMech/PRASA Conference*. Cape Town, 29-31 January, 2020, pp. 1–6.

[51] ——, "Bag context shape grammar implementation: From theory to useable software," *Computer-Aided Design and Applications*, vol. 17, no. 3, pp. 548–574, 2019.

[52] A. C. Savvas, S. B. Yiannis, and L. Mathias, "SpCD - Spatial Color Distribution Descriptor - a fuzzy rule based compact composite descriptor appropriate for hand drawn color sketches retrieval," in *2nd International Conference on Agents and Artificial Intelligence*. Artificial Intelligence, 2010, pp. 58–63, accessible http://hdl.handle.net/11728/10155, [Last accessed 20-September-2018].

[53] R. J. Sternberg and K. Sternberg, *Cognitive Psychology*. Wadsworth, 2011.

[54] C. Katsini, C. Fidas, G. E. Raptis, M. Belk, G. Samaras, and N. Avouris, "Influences of human cognition and visual behavior on password strength during picture password composition," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, ser. CHI '18, no. 87. New York, NY, USA: ACM, 2018, pp. 73–87. [Online]. Available: http://doi.acm.org/10.1145/3173574.3173661

[55] International-Telecommunication-Union, "Series E: Overall network operation, telephone service, service operation and human factors," *Telecommunication Standardization Sector of ITU*, pp. 1–14, 2004.

[56] D. Alan, J. Finaly, G. D. Abowd, and B. Russel, *Human Computer Interaction*. Pearson Prentice Hall, 2004.

[57] A. C. Savvas, S. B. Yiannis, and L. Mathias, "Img(rummager): An interactive content based image retrieval system," in *SISAP '09 Proceedings of the 2009 Second International Workshop on Similarity Search and Applications, Prague, Czech Republic — August 29 - 30*. IEEE Computer Society, 2009, pp. 151–153.

[58] S. Wiedenbeck, J. WatersLeonardo, and S.-C. Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme," in *Proceedings of the working conference on Advanced visual interfaces, AVI 2006, Venezia, Italy, May 23-26*. ACM, 2006, pp. 177–184.

[59] G. Haichang, R. Zhongjie, C. Xiuling, X. Liu, and A. Uwe, "A new graphical password scheme resistant to shoulder-surfing," in *2010 International Conference on Cyberworlds*. IEEE, 2010, pp. 18–23.

[60] A. Awais, A. Muhammad, H. M. Kashif, and T. Ramzan, "Secure graphical password techniques against shoulder surfing and camera based attacks," in *International Journal of Computer Network and Information Security, November 2016*. IEEE, 2016, pp. 11–18.

[61] G. Haichang, L. Xiyang, W. Sidong, L. Honggang, and D. Ruyi, "Design and analysis of a graphical password scheme," in *Fourth International Conference on Innovative Computing, Information and Control*. IEEE, 2009, pp. 675–678.

[62] N. K. Sreelaja and N. K. Sreeja, "An image edge based approach for image password encryption," in *Security Communication Networks 2017*. Wiley Online Library, 2017, p. 5733–5745.

# Author Biographies

**Blessing Ogbuokiri** holds a doctoral degree (PhD) in Computer Science from the School of Computer Science and Applied Mathematics, University of the Witwatersrand, Johannesburg, South Africa, in 2020. His research interests are in the areas of Theory of Computation, Deep Learning for Social Good, Machine Learning, and Computer Vision.

**Mpho Raborife** holds a doctoral degree (PhD) in Computer Science from the School of Computer Science and Applied Mathematics, University of the Witwatersrand, Johannesburg, South Africa, in 2016. She is a senior lecturer at the

Department of Applied Information Systems, University of Johannesburg, South Africa. Her research interests are in the areas of Natural Language Processing and Formal Languages and its applications.