JCSE Journal of Computing Science and Engineering

Regular Paper

Journal of Computing Science and Engineering,
Vol. 14, No. 4, December 2020, pp. 163-185

A Systematic Literature Review of Graphical Password Schemes

Tahmina Islam Shammee, Taslima Akter, Muthmainna Mou, Farida Chowdhury*, and Md Sadek Ferdous
Department of Computer Science and Engineering, Shahajalal University of Science and Technology, Sylhet, Bangladesh
{tahminaislamshammee, taslimaakter18989, 276mou}@gmail.com, {farida-cse, sadek-cse}@sust.edu

Abstract

Graphical passwords are an alternative to traditional alphanumeric passwords and can similarly be used to secure online accounts. The widely used alphanumeric passwords have memorability issues and users often find it difficult to memorize a large number of unique passwords. Since 1996, researchers have implemented different graphical password schemes (GPSs) to address such security and usability issues. There are a wide variety of such schemes available. To initiate a study in this domain, it is necessary for a researcher to have a good understanding of the existing research. There are a number of existing review articles, but no systematic literature review (SLR). Additionally, the existing reviews have not covered recent papers. This paper aims to fill in these gaps by reviewing existing GPSs, and intends to address their contributions, limitations, the contexts in which they are used, and the relevant algorithms/techniques. To this end, we conducted an SLR of empirical studies on a number of GPSs published from 1996 to 2019. This article also identifies the security threats that the reviewed schemes are resilient against. A number of schemes have been found to have greater resiliency against different attacks, but not a single scheme is completely resistant to all known attacks.

Category: Privacy and Security

Keywords: Graphical password; Authentication; Recognition scheme; Recall schemes; Cued-recall scheme; Hybrid scheme; Security

I. INTRODUCTION

One of the most important components of any system or web security infrastructure is user authentication. User authentication is the process that allows a device or system to verify the identity of someone who connects to the system's resources. There are several different authentication methods [1], among which, knowledge-based authentication is one of the most popular. There are two types of knowledge-based methods: *alphanumeric* and *graphical* passwords. The former is more widely used as it is easy and inexpensive to implement and familiar to all users. However, alphanumeric passwords have major disadvantages. Because human memory is limited, most users tend to choose simple or short passwords that are easy to remember [2]. This leads to security issues. The alternative is to choose a more secure password that is harder to remember, which results in usability issues. On the other hand, graphical passwords have evolved to leverage the quirks of human memory, as pictures can be remembered more readily than text. Additionally, if the number of possible images is large enough, the password space of a graphical password technique may increase more than that of an alphanumeric password technique and, therefore, use of graphical passwords might offer better resistance to different security attacks [3]. Interest in graphical passwords among researchers has been growing since the method's inception.

Open Access http://dx.doi.org/10.5626/JCSE.2020.14.4.163 http://jcse.kiise.org

Received 07 November 2020; **Accepted** 16 December 2020
*Corresponding Author

 pISSN: 1976-4677 eISSN: 2093-8020

In this article, we present a systematic literature review (SLR) of different kinds of graphical password schemes (GPSs) by analyzing each one's contributions, strengths and limitations. The review was performed by gathering information on existing GPSs proposed between the years 1996 and 2019 and then comparing them by following a set of steps. A number of reviews and surveys of GPS systems have previously been carried out [1, 4-6]. However, existing literature reviews of GPSs are mainly traditional literature reviews that cover research trends and security and usability aspects, whereas we present an SLR that aims to answer various research questions related to GPSs. To the best of our knowledge, there is no existing SLR that focuses on the current state of GPSs along with their contributions, relevant technologies, and other aspects. Also, no useful review papers have been published since 2014. This also motivated our work. In this study, we identify different types of GPSs in a variety of contexts. We also discuss growing trends in GPSs since 1997. GPSs are also reviewed according to their ability to resist different attacks. Structure: Section II presents the research methodology and Section III explains the review planning. Section IV discusses the review process, Section V presents the results of the review, Section VI contains the discussion and Section VII contains the limitations of our study. Finally, we conclude in Section VIII.

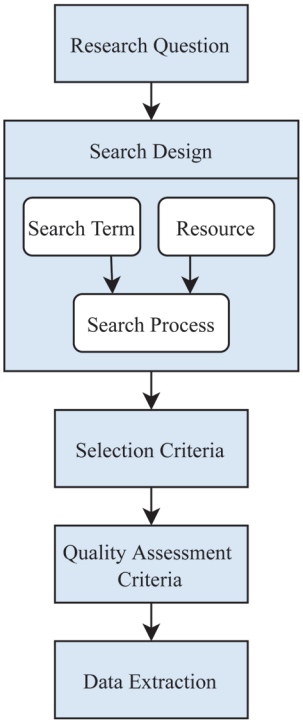

Fig. 1. Review protocol.

II. RESEARCH METHODOLOGY

We have performed a SLR on GPSs following Kitchenham's method [7]. According to this method, we did a good deal of planning first, which included (1) identification of the need for a review, (2) development of a review protocol, (3) development of a set of research questions and (4) review of the protocol by experts. We then conducted a general search following the search protocol/method using different resources (i.e., online databases). Based on the search results, papers were included/excluded according to a few selection criteria. A relevant list of papers were identified. These papers were then reviewed and studied in depth to finally select the papers that were included in this study.

III. PLANNING

This section elaborates on our plans for the SLR. First, we discuss the need for the review (Section III-A) and the development of the review protocol (Section III-B). Then, we present the research questions (Section III-C) and review protocol (Section III-D) for our SLR.

A. The Need for a Systematic Review

The objective of this type of review is to identify as many primary and recognized GPSs as possible from the literature. Furthermore, it attempts to answer the research questions defined in Section III-C using an unbiased search design procedure.

B. Development of the Review Protocol

The developed review protocol is illustrated in Fig. 1. First, we raised some research questions. In the second stage, we designed a search procedure that allowed us to find studies related to the research questions. The search design contains search terms and resources for the subsequent search process. In the third stage, we defined a number of selection criteria that were used to identify the relevant studies. In the fourth stage, we utilized quality assessment criteria to select potential studies. The final stage involved data extraction from the selected studies.

C. Research Questions

We identified five research questions for our SLR, which are given in Table 1.

D. Review Protocol

The review protocol is an important part of the SLR that distinguishes it from traditional reviews. Therefore, it was important that it be reviewed by experts. To ensure

Table 1. Research Questions

	Research question
RQ1	Which are the main Graphical Password Systems (GPSs) that exist in the literature?
RQ2	What are the main contributions and limitations of the GPSs?
RQ3	Which algorithms or techniques are mainly used in GPS?
RQ4	In which contexts the selected schemes are used?
RQ5	Are the GPSs strongly resistant to different attacks?

the credibility and rigorousness of this review process, two supervisors analyzed and reviewed the research plan. The same supervisors also reviewed the final discussion.

IV. METHODS

This section outlines in detail the steps taken to select different studies for our SLR. To this end, we have presented the search design (Section IV-A), study selection (Section IV-B) and, finally, quality assessment (Section IV-C) process.

A. Search Design

The search design consists of finalizing the search terms, search resources and search process; these are described below.

1) Search Terms

In order to search for existing studies, we selected a number of keywords and then created combinations of these keywords using Boolean operators (e.g., AND, OR). The six selected search terms are: *graphical*, *password*, *authentication*, *scheme*, *survey*, and *review*. We used the Boolean operators "AND" and "OR" to connect these terms. The combinations (C) are given below:

- C1: graphical AND password
- C2: graphical AND authentication
- C3: graphical AND (password OR authentication) AND scheme
- C4: graphical AND (password OR authentication) AND survey
- C5: graphical AND (password OR authentication) AND review

2) Search Resources

We conducted the initial search using four well-known electronic databases: Google Scholar (https://scholar.google.co.kr), IEEE Xplorer (https://ieeexplore.ieee.org), ACM Digital Library (http://dl.acm.org), and Springer (https://www.springer.com).

The search terms were used to identify journal papers and conference papers in these databases. The search was conducted in the four databases using only title. Moreover, we restricted our search to papers published in the period from January 1, 1996 to December 31, 2019.

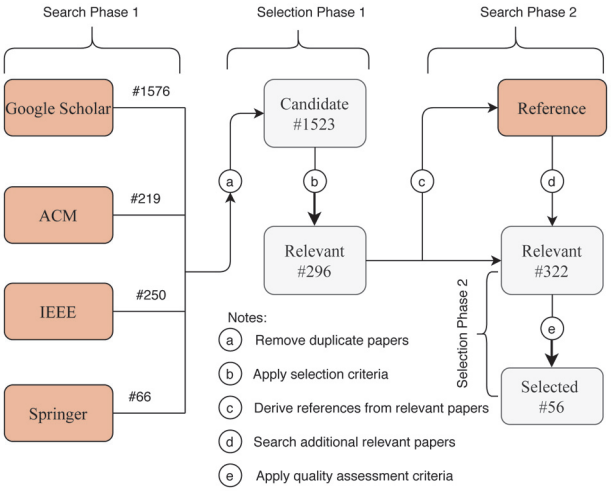

Fig. 2. Search and selection process.

3) Search Process

Following the above steps resulted in identification of a number of papers. We divided the search process into the following two phases:

- Search Phase 1: In this phase, the four electronic databases were searched to construct a set of candidate papers.
- Search Phase 2: In this phase, the reference sections of relevant papers were searched to identify additional relevant papers; if found, these were added to the set.

A total of 322 relevant papers were identified by this search process. Fig. 2 outlines the entire search process.

B. Search Selection

The *search process* resulted in 1,523 candidate papers after removal of duplicate papers. Further filtering was necessary to identify the relevant papers as many candidate papers did not contain information pertinent to the research questions of this review. This was exactly in line with the study selection process. The study selection process consists

Table 2. Selection criteria

Inclusion criteria	Exclusion criteria
Complete graphical password schemes. Papers published within the year range between1996–2019. Papers published in English.	Papers did not contain relevant information. Papers did not publish in any standard conference or journal. Less citation. Biometric schema.

Table 3. Quality assessment questions

	Research question
RQ1	Is the main objective of the paper to deal with graphical password authentication?
RQ2	Does the paper describe a graphical password authentication scheme?
RQ3	Does the paper describe the usability and security of the graphical scheme with an evolution and metric?
RQ4	Has the study clearly reported their findings with results?

of two phases:

- Selection Phase 1: In this phase, papers were selected based on the inclusion and exclusion criteria and only the relevant papers were counted.
- Selection Phase 2: In this phase, we applied the quality assessment criteria to relevant papers, which were identified by search phase 2, to select final papers with acceptable quality.

1) Search Criteria

We defined a number of inclusion and exclusion criteria to filter the candidate papers and selected only those papers with relevance to research questions. The criteria are presented in Table 2.

C. Quality Assessment Criteria

To ensure the quality of each selected paper, we defined some quality assessment questions. The questions are presented in Table 3. We included only those papers with a positive answer for each of the quality assessment questions. By applying this assessment, we finally identified a total of 56 relevant papers for our SLR.

V. RESULTS

In this section, we present the results of our review and answer our research questions.

A. RQ1: What are the Main GPSs That Exist in the Literature?

The existing GPSs can be categorized into four groups: recognition-based, recall-based, cued-recall-based and hybrid-based schemes [8].

1. *Recognition-based*: Recognition-based schemes are also known as *Cognometrics* or *Search Metrics* schemes. In this type of scheme, users identify whether or not they have seen an image before. When creating a password for the first time, a user needs to choose a number of images from a large portfolio of images. During the authentication process, the user must successfully identify his/her password images and distinguish them from other decoy images.
2. *Recall-based*: In a recall-based scheme, also known as a *Drawmetric* scheme, a user creates or selects a secret drawing when registering for the first time and then reproduces the same drawing on a grid or a blank canvas during the authentication stage.
3. *Cued-recall-based*: Cued-recall schemes are also called *locimetric* schemes. These schemes are based on a well-known mnemonic loci method. In these schemes, the user creates different password click points by choosing any point in a specific region in the image. During authentication, a user must successfully identify the chosen password click points in the correct order.
4. *Hybrid*: A hybrid scheme utilizes a combination of two or more different types of GPS or other authentication methods.

In our research findings, among the 56 selected papers, 17 dealt with recognition-based authentication schemes, 13 dealt with recall schemes, 13 discussed cued-recall schemes and, finally, 13 addressed hybrid authentication schemes. This categorization of the selected papers is presented in Table 4.

B. RQ2: What are the Main Contributions and Limitations of the GPSs?

This section presents a descriptive review of several GPS techniques. We highlight their main contributions

Table 4. Graphical Password Schemes

Category	Scheme
Recognition	Deja vu [9], Passfaces [10], Photographic authentication [11], Story [12], VIP [13], CHC [14], Cognitive authentication [15], Use your illusion [16], Color login [17], GPI/GPIS [18], WYSWY [19], SSP [20], LocPass [21], Rodda et al. [22], Evo-pass [23], Por et al. [24, 25], PassApp [26]
Recall	AS [27], BDAS [28], Passdoodles [29], PassShapes [31], Pass-Go [32], YAGP [33], Android screen-unlock [34], Windows 8 password [36], GEAT [37], DRAW-A-PIN [38], RouteMap [39], gRAT [40], TMD [41]
Cued-recall	Blonder [42], Jiminy [43], Inkblot [44], Passpoint [45], Suo [46], CCP [47], PCCP [48], Patra et al. [49], Passmatrix [50], PassBYOP [51], Passblot [52, 53], HapticPoint [54], PassMap [55]
Hybrid	CD-GPS [56], Gokhale and Waghmare [3], Chen et al. [59], Chameleon [60], WIW [61], Wang et al. [62], Passhint [63], Saeed and Umar [64], GOTPass [65], CuedR [67], PCGP [68], TCpC [69], Jumbled PassSteps [70]

and limitations so as to provide a basis on which to answer RQ2. Our findings are presented below.

1) Recognition-Based GPSs

In this review, we analyzed 17 recognition-based GPSs that employ a wide variety of mechanisms.

The *Deja vu* scheme was proposed by Dhamija and Perrig [9]. In this scheme, a challenge set is given that contains both passwords and decoy images. Users need to click the password images to authenticate themselves. The utilization of random art images makes this scheme secure as it is hard to describe these images. *Deja vu* has some drawbacks as well: it uses a single authentication round and the password space is quite low.

The *Passfaces* scheme was proposed by Brostoff and Sasse [10], who were inspired by the reality that humans generally remember faces without any difficulty. To authenticate, users select the pre-selected faces from a grid. This scheme uses multiple authentication rounds. There are some major drawbacks to this scheme, such as biases towards faces and not being secure against shoulder-surfing, brute force and dictionary attacks.

The *Photographic authentication* scheme was proposed by Pering et al. [11] to work with untrusted terminals. To authenticate, a user needs to identify their own personal images from a set of random photographs. It provides memorability since the user uses their personal photographs. People who are not accustomed to taking pictures might find it difficult to use this scheme and end up using a set of easily guessable and less-secure images.

The *Story* scheme, which is similar to the Passfaces scheme, was proposed by Davis et al. [12]. It relies on images of both faces and objects. It uses a single authentication round. By using unique images, it helps to create a story-like feature, which increases memorability. Unfortunately, it is not resilient against shoulder-surfing attacks and guessing attacks.

The VIP scheme, proposed by de Angeli et al. [13], has three varieties, *VIP1*, *VIP2*, and *VIP3*. In VIP1 and VIP2, users need to remember a series of images and enter them in a fixed sequence to authenticate. In VIP3, users can identify images in any order. For security purposes, in case of authentication failure, VIP1 gives three login trials, while VIP2 and VIP3 provide the same visual configuration. The decoy images are changed at each authentication phase, thus making it easy for attackers to recognize the password. It also takes a long time to authenticate compared to alphanumeric PINs.

A recognition-based GPS, *Convex Hull Click* (CHC), was proposed by Wiedenbeck et al. [14]. In this scheme, users must click inside the hull or region created by three pass icons. Each panel includes at least three pass icons. It uses multiple authentication rounds with time-variant responses. Users also do not need to click on the pass icons directly, so it provides more security against shoulder-surfing attacks. However, it is a time-consuming process.

The *Cognitive authentication* method was proposed by Weinshall [15] to provide security against spyware. In this method, the computer sends a sequence of challenges to the user. When users select an image belonging to their portfolio, they proceed downwards or to the right until they reach the bottom or right edge of the panel. Then they identify the label for that specific row or column and, finally, must correctly answer a multiple-choice question that includes the path's correct end points. This procedure is followed for several rounds; the user is authenticated when the probability of random guessing goes under a fixed threshold. This method has a large password size. Training for this method must be done in a secure location for security purposes. The login time is also high for this scheme.

Use *your illusion*, proposed by Hayashi et al. [16], is another recognition-based scheme. To authenticate, the user selects their own distorted images from a set of decoy images. The levels of distortion are high enough that most of the details of the original pictures are concealed. The system locks a device after a few unsuccessful attempts. It has several drawbacks, for example, it uses a fixed edge detection level for all pass and decoy images, and it is not resistant to prolonged observation attacks and spyware attacks.

The *Color login* scheme was proposed by Gao et al. [17]. In it, a user needs to choose some specific color and pass icons. To authenticate, the user needs to choose the

row containing his/her pass icon. This scheme decreases the login time due to the use of background color and provides mild resistance against shoulder-surfing attacks. The security level is chosen by the user, so in some cases, a user may choose a low level of security for convenience.

The *GPI/GPIS* scheme was proposed by Bicakci et al. [18]. In this scheme, users authenticate by selecting six particular icons in a fixed order from a panel of 150 icons. The difference between GPI and GPIS systems lies only in the method of setting passwords. GPI allows user-chosen passwords. GPIS uses system-chosen passwords, though users can rearrange their passwords until they are satisfied. However, this causes the problem of unacceptable login time. Unfortunately, the method does not provide resistance against shoulder-surfing, spyware and phishing attacks.

WYSWYE was proposed by Khot et al. [19]. In this scheme, during the authentication process, a user needs to identify and map a pattern from a large grid onto another grid. The scheme provides time-varied response. It is a complex process and, hence, not suitable for small devices. It is also not resistant to intersection attacks.

SSP, proposed by Wu et al. [20], is somewhat similar to CHC in that it uses the CHC algorithm, but the two differ in several ways. Dynamic moving balls are used to provide security against shoulder-surfing attacks. When one colored dynamic moving ball corresponding to the password moves within the authentication region, the user has to press the space key. This process imposes a memory burden and necessitates more processing time, however, it is resistant to shoulder-surfing attacks.

Yee et al. [21] proposed a recognition-based scheme called *Locpass*. In this scheme, users must memorize the locations of images. During authentication, five types of images are used in a grid. Using these images and a specific method, users need to find the pass location and click on it to get authenticated. Meaningful images are used, so there is no memorability issue. The login time is high compared to other schemes such as Deja vu and Passfaces.

Another scheme similar to Passfaces was proposed by Rodda et al. [22], in which a user needs to enter his/her user name and a grid size. It relies on a multi-round authentication process in which users can select the correct images using a mouse or by entering the position of the image in the grid. It requires a long execution time and exhibits some biases towards faces.

The *Evo Pass* scheme, which is similar to the Use Your Illusion scheme, was proposed by Yu et al. [23]. In this scheme, users must recognize their corresponding pass sketches from a collection of challenge images for authentication. Personal images can be used. It uses pass sketches instead of pass images and the pass sketches evolve periodically. A lock-out policy is used for any instances of authentication failure. The scheme is not resilient to shoulder-surfing attacks and does not utilize the same level of fixed edge detection for all pass and decoy images to provide security against different attacks.

Por et al. [24] introduced a recognition-based scheme based on three digraph substitution rules. In their scheme, users choose two images as pass images and can use only one image to log in during authentication. However, the method is not sufficient to protect against shoulder-surfing attacks. Therefore, the authors proposed another, improved, scheme [25] in which a user is required to click on the pass image shown in the challenge set using digraph substitution rules and pass image feedback. The scheme is strongly resistant to shoulder-surfing attacks using video recorders. However, the improved scheme has some usability issues like memorability and long login time.

In *PassApp*, proposed by Sun et al. [26], the user authenticates by recognizing the apps that are installed on their mobile devices. This eliminates the need for registration. PassApp reduces users' memory burden as they do not need to remember passwords, which greatly enhances usability. It is resistant to one-time shoulder-surfing attacks, but it is vulnerable to dictionary attacks.

Summary: Table 5 summarizes the findings of our reviews of different recognition-based schemes.

2) Recall-Based GPSs

Next, we review recall-based GPSs. For each of the 13 selected schemes, we have highlighted their main contributions and limitations.

Draw-A-Secret (DAS), proposed by Jermyn et al. [27], is the first recall-based graphical password system. In this scheme, users need to draw their password on a 2D (5×5) grid using a stylus or mouse. The drawing consists of one or multiple strokes separated by "pen-ups". Users can draw passwords for as long as they like. Users need to redraw the same password to be authenticated. This method offers a long theoretical space comparable to that of text passwords. It has been shown that, using this scheme, users create symmetric and centered passwords, which might help attackers guess easily.

BDAS, proposed by Dunphy and Yan [28], is an expansion of DAS with an additional background image. It enhances both human memorability and password complexity and reduces the risk of symmetry and central tendency within password images.

Passdoodles [29, 30] is comparable to DAS in that users create a freehand drawing without a visible grid. The drawing consists of at least two pen strokes. The doodle can be drawn in a number of colors. To add variability to the doodles, the system includes different types of pen strokes, pen colors and drawing speeds.

PassShapes, a similar system to Passdoodle, was proposed by Weiss and De Luca [31]. In this system, users need to draw basic geometric shapes made of an arbitrary combination of eight distinctive strokes. PassShapes can be drawn in a number of sizes or in

Table 5. Recognition graphical password schemes

Scheme	Contribution	Limitation
Deja vu [9]	Prevents user from choosing weak password. Use random art images to make it difficult to write down or describe.	Low efficiency (high login time). Not resilient against brute force, guessing and shoulder-surfing attacks. Not time variant response.
Passfaces [10]	Easy to remember and use.	Long execution time. Biasness towards faces (gender, etc.). Not resistant to shoulder-sur ng, brute-force, dictionary, guessing.
Photographic authentication [11]	Use personal photographs thus no memorability issues. Easy to use.	Not suitable for people who do not take pictures regularly and hence, they might not be able to select suitable pictures.
Story [12]	Use images of different types (face, objects, etc.) create a story-like feature thus easy to remember.	Not resistant to shoulder-sur ng and guessing attacks. Ordering errors. Single round authentication system.
VIP [13]	Provides more security. For security purposes in case of authentication failure VIP1 gives three login trials. VIP2, VIP3 provide the same visual configuration.	No variant response. Changing decoy images during each authentication makes it easy for attackers to recognize the password. High login time. Not resistant to shoulder-sur ng, phishing.
CHC [14]	Easy to learn and use. Large password space. Provides security since users never need to click the pass icons directly.	Time consuming
Cognitive [15]	Use machine generated random set of pictures. Large password space. Friendly mechanism.	Need training in secure location. High login time.
Use your illusion [16]	The high level distortion ensures that most details of the original pictures remain obscured. Lock device after a few unsuccessful attempts. Self-chosen images.	All pass and decoy images utilize fixed edge detection level. Exhibits Vulnerability against attacks involving prolonged observation and spyware.
Color login [17]	Interesting game-based and user-friendly interface because of the use of background colors. Use color to decrease login time. The scheme can mitigate intersection and shoulder-surfing attacks up to a certain extent.	The security level is chosen by the user thus it might be possible that a user chooses a low level of security. The security level is chosen by the user thus it might be possible that a user chooses a low level of security.
GPI/GPIS [18]	Large password space. No hotspot problem.	Unsatisfactory login time. Not resistant to shoulder-surfing, spyware, phishing attacks.
WYSWY [19]	One time password. Time variant response.	Complex. Not resistant against intersection attack. Not suitable for small devices like mobile.
SSP [20]	It can provide resiliency against password icons directly compromised. No extra protection is required in the devices.	Imposes memory burden with additional processing time.
LocPass [21]	High memorability No offset mechanism is used to confuse attacker. Meaningful image.	Need training. Long execution time as it needs to follow an algorithm to find out the pass location.
Rodda et al. [22]	Two ways of inputting the password User friendly.	Long execution time. Biasness towards faces.
Evo-pass [23]	User can use personal images. Use pass sketches which provides security. Evolves pass sketches periodically. Roll-back property.	Not resistant to shoulder-sur ng attacks. Since roll back operation is performed locally it takes more storage space.
Por et al. [24, 25]	Need to choose the pass image by using digraph pass image feedback and substitution rules.	Need to learn a specific algorithm (DSR) to use this scheme. Authentication time is long. Hard to remember for using random images.
PassApp [26]	Reduces additional memory burden. Enhances experience of the users	Vulnerable to dictionary attacks

different locations on the screen without use of a visible grid. The shapes are exclusively comprised of straight lines, which makes painting simple and easy, even for non-artistic users. This increases memorability but reduces the password space.

Pass-Go, designed by Tao and Adams [32], was motivated by an expected usability issue of DAS: the difficulty of accurately redrawing something in the exact same position and keeping the strokes off of the grid lines. In this scheme, instead of using grid cells, users use grid intersection points to draw their passwords. Using grid intersections makes it more secure and increases password space. An error tolerance mechanism is used to make it easy for a user to touch an intersecting point.

YAGP, a modification of DAS, was proposed by Gao et al. [33]. In this scheme, users can redraw their password anywhere on the grid canvas. It is a position-free system, like PassShapes. The system adopts partial matching to reduce the limitations for users. However, it is still hard to precisely redraw the same password.

Two commercial items are available that utilize recall-based GPSs. One is *Android screen-unlock* [34], which is a modified version of the Pass-Go scheme [32]. When using Android screen-unlock, the user must draw a pattern by moving his or her finger or stylus over several points in a 3×3 grid. It is sufficient for mobile phones, which mostly are used by a single user and kept in that user's possession. It has very little password space. It has been proven that Android screen-unlock is at risk of smudge attacks [35]. It is also vulnerable to brute force attacks. In the other item, introduced by Microsoft in their Windows 8 OS [36], a user has to draw a set of gestures (any combination) in the image provided by the system. Three types of gestures are used: circles, straight lines, and taps.

GEAT, proposed by Shahzad et al. [37], is a gesture-based authentication scheme. The GEAT scheme initially collects training samples. To this end, the user is asked to create a number of sample gestures (about 15 to 25) on the touch screen of the mobile phone. From those sample gestures, behavioral features, such as device acceleration, finger velocity and stroke time, are extracted and selected. This scheme utilizes a set of 10 predefined gestures from which the user can draw a multi-touch gesture password. It is nearly impossible for an attacker to replicate the gestural behaviors of others through smudge or shoulder-surfing attacks. However, users should be particularly careful to protect their password input from such attacks at the time of training data gathering.

DRAW-A-PIN, an alternative method of entering a PIN, was proposed by Nguyen et al. [38]. In this scheme, a user draws a PIN on the touch screen rather than typing one out. Behavioral biometrics or drawing traits are utilized as an extra characteristic in this scheme. It is a very usable two-factor authentication scheme. It is difficult for attackers to emulate even if they know the PIN. However, the system is vulnerable to imitation attacks and PIN attacks.

RouteMap [39] is a map-based authentication scheme in which users must draw a route on a map which is either with sight or not. Users can draw straight lines between distinctive places, which increases usability. RouteMap provides straightforward guidance for users to create memorable passwords, even when they are making multiple passwords. However, no security analysis of the scheme has yet been reported.

gRAT [40] is similar to Android screen-unlock. In this scheme, a user must draw a pattern using the same set of images as were drawn during the registration phase from a randomized set of images. It provides sufficient security. The randomized algorithm makes this scheme resilient to shoulder-surfing and smudge attacks.

TMD, proposed by Chiang and Chiasson [41], is a multilayered password scheme for touchscreen devices in which a user has to select cells from a 5×7 grid. The selection process must be done in a single motion without lifting the figure. Users can draw a password across multiple layers through a wrap cell, so the password space is larger than that of Android screen-unlock. This scheme also eliminates the fuzzy boundaries problem.

Summary: Our review findings for the selected recall-based schemes are summarized in Table 6.

3) Cued-Recall-Based GPSs

Now we review the selected cued-recall-based GPSs.

The first GPS was a cued-recall-based GPS described by Blonder [42] in 1996. In this scheme, a user clicks on several preregistered locations in an image in the correct sequence to log into a system. It is easier to remember and provides higher security than alphanumeric password schemes. However, it has some disadvantages. For example, it has predefined boundaries and users cannot just click on the image background at random for the predefined area. It is also more vulnerable to shoulder-surfing attacks than alphanumeric password systems.

Jiminy is a cued-recall graphical scheme proposed by Renaud and Smith [43]. To authenticate, a user chooses an image and a color template and places the template on a specific location in the image. Users need to remember the template position within the image instead of remembering their alphanumeric passwords.

Inkblot, proposed by Stubblefield and Simon [44], is similar to a Rorschach inkblot test. In this scheme, users are given a series of inkblots generated by a computer, then they type in the instructed pair of letters (e.g. the first or last letter) from the word/phrase which best describes the inkblot. This instructed pair of letters form the password.

Passpoint, by Wiedenbeck et al. [45], is an extension of Blonder's idea which overcomes some of the main limitations of the latter. Users can use any image, which does not require predefined contrived click regions within

Table 6. Recall graphical password schemes

Scheme	Contribution	Limitation
DAS [27]	Offers a theoretical space comparable with text passwords. User can draw a long password as their wish.	Not resilient to shoulder-surfing and dictionary attacks. Users create symmetric and centered passwords.
BDAS [28]	Reduces the amount of symmetry and centering within password images. Enhances both human memorability and password com plexity.	Not resistant to shoulder-surfing, dictionary attack.
Passdoodles [29]	To add variability, a number of features such as Pen color and different pen strokes are included to the doodles. Large password space.	It is reported that users make mistakes while trying to recall the number, order, or direction of the pen strokes.
PassShapes [31]	PassShapes can be drawn in any location, and in different sizes, on the screen without a visible grid. Increases memorability. Easy and effortless painting.	Reduces the password space vulnerable to shoulder-surfing attack.
Pass-Go [32]	Large password space. Using grid intersection to make it more secure. Error tolerance mechanism is used.	No variant response. Not resistant to dictionary attack, shoulder-surfing attacks.
YAGP [33]	Partial matching is adopted to relax user restrictions. Position-free. Large password space.	Redrawing the password precisely later is hard.
Android screen-unlock [34]	Phones not requiring a high security level, the scheme might be sufficient. Has good usability and provides strong memorability.	Susceptible to smudge attacks, dictionary attacks, brute force attacks. Less password space.
Windows 8 password [36]	Easy to remember, simple to operate.	Susceptible to hotspots and shoulder-surfing attacks.
GEAT [37]	Different data such as the velocity of fingers, the acceleration of the device, and the time of stroke from gestures are extracted.	Users should be careful to protect their password/PIN/pattern input so as to mitigate shoulder-surfing and smudge attacks at the time of training data gathering.
DRAW-A-PIN [38]	Even if the PIN is known, it is difficult for attackers to emulate. Behavioral biometrics. Eyes-free, two-factor. Highly usable.	Vulnerable to PIN attack and imitation attack.
RouteMap [39]	Provides a simple guideline to create memorable passwords and better multiple password memory for users.	Security analyses were not reported.
gRAT [40]	Resistant against shoulder-surfing attack and smudge attack.	It does not provide a completely secure mechanism.
TMD [41]	The password space is increased with layers. Eliminated the fuzzy boundary problem.	It is difficult to draw a pattern using only one line for some users.

a well-marked boundary. During the authentication phase, a user selects five click-points from an image within an (adjustable) tolerance distance in the correct sequence. Even though it utilizes a large password space, it is not resilient against shoulder-surfing attacks and mouse tracking.

Suo [46] proposed a cued-recall scheme based on Passpoint that is resistant to shoulder-surfing attacks and mouse tracking. In this scheme, during authentication, the whole image, except for a small focus area within it, is blurred. The user must indicate whether their click-point is within the focused area. A user inputs 'Y' for yes or 'N' for no, or uses the mouse's right or left button to denote whether the click-point lies within the focused area. One drawback of this scheme is that the authentication process is time-consuming.

Cued Click-Points (CCP) is a cued-recall scheme proposed by Chiasson et al. [47]. It is a combination of Passpoint [45], Passface [10], and Story [12]. To authenticate, from a sequence of images, a user selects a single click-point for each image. This click-point defines the next image to be displayed. The disadvantage of this scheme is that it is susceptible to shoulder-surfing attacks.

Chiasson et al. [48] also designed Persuasive Cued Click-Points (PCCP), in which CCP is utilized as a base system and then a persuasive feature is added. The aim of this addition is to encourage users in selecting more secure and random passwords. It reduces the hotspot

effect, however, it is also susceptible to shoulder-surfing attacks.

Patra et al. [49] implemented a CCP-based GPS with circular tolerance. In this scheme, during authentication, a user must select one click-point on the first two images and two click-points for the third image in sequential order.

Passmatrix was proposed by Hung-Min et al. [50]. In PassMatrix, users need to choose a square for *n* sequential images, instead of *n* squares for one image; the user chooses the number *n*. There are a number of modules in PassMatrix:

- Image Discretization Module, which is used to divide a single image into different squares.
- Login Indicator Generator Module, which is used during the authentication phase to generate a login indicator containing several distinguishable alpha-numeric characters and visual objects, such as colors and icons.
- Axis Control Module to support drag functions for the horizontal and vertical bars.
- Communication Module to ensure connectivity between client devices and the authentication server.
- Password Verification Module, which verifies user-submitted passwords during the authentication phase.
- A back-end database to store user information.

First, the user must create a username during the registration phase, which must be provided to authenticate the user. The login indicator module creates a login indicator which remains visible, and the user uses their hand to touch the screen to draw a circle. The circle can also be delivered by audio feedback. In the next phase, the first-pass image is shown on the screen as a challenge with a horizontal bar as well as a vertical bar. The user must respond to the presented challenge by dragging the bars and aligning the previously selected pass-square with the login indicator. These steps are repeated for all images. Only if the alignments are correct for all images can the user login. No feedback is provided during a wrong entry. The user does not need to directly click on the pass images to login, thus providing more security. This scheme has some limitations, such as the very large login time (since the whole process runs for several rounds), hot-spot problem, etc.

PassBYOP was proposed by Bianchi et al. [51]. Here, a user has to present the image of a physical object to a system camera and then align the image and enter his password as he selects the image locations on live video of the token. Because live video of a physical token is used instead of a digital image, it is hard to login if the user has lost the physical token. This system also requires an extra camera-based device to login with a desktop.

Passblot, proposed by Gupta et al. [52, 53], is a varied version of inkblot. In this scheme, the system shows four randomly selected inkblots from 10 inkblots that were used in the registration phase by that particular user. A strict policy of utilizing different passwords for different sites is implemented, and a one-time password system is provided. The randomly chosen inkblots make it difficult for observers to attack this system by shoulder-surfing. However, after three consecutive login sessions, the system may be susceptible to shoulder-surfing attacks. This is a time-consuming system and some users have found it hard to describe their inkblots.

HapticPoint, proposed by Ratchasan and Wiangsri-panawan [54], extends PassPoints [45] by adding haptic feedback to PassPoints as additional decoy click points. To log in, a user has to select a single click point on the chosen images. During image selection, the user sometimes gets haptic feedback for selecting decoy click points. When the haptic feedback system vibrates, it becomes hard to observe or eavesdrop, so an attacker cannot easily guess the password. Thus, HapticPoint is better than PassPoints at resisting shoulder-surfing attacks.

PassMap is a map-based authentication system proposed by Sun et al. [55] in which the user must select 2 click-points on a large world map. Passwords created using this scheme are user-friendly and easy to memorize. PassMap has better entropy than PassPoints, with an increased cost of attacks. However, it is still susceptible to shoulder-surfing and pattern dictionary attacks. *CPmap* proposed by Meng [56] and *P-GMGP* proposed by Zhou et al. [57] are also map-based authentication systems in which users have to click points on a Google map.

Summary: A summary of our findings about the selected cued-recall systems is presented in Table 7.

4) Hybrid GPS

In this section, we review the selected hybrid GPSs. As before, we highlight the main contributions as well as the limitations of each scheme.

CD-GPS is a click-draw-based scheme proposed by Meng [56]. It is a combination of cued-recall and recall methods that utilizes elements of the PassPoint [45], CCP [47], Story [12], and DAS [27] schemes. During the registration phase, users select a sequence of images from an image pool following a certain order, like a story. Then, the user chooses one or a few other images and draws a secret picture with a series of clicks on the selected images. During the authentication phase, users must select the previously selected images in the correct order as well as reproduce their secret picture in the correct location. This scheme eliminates the hotspot problem in PassPoint as well as the identification and reproduction problems in the draw-based schemes.

Gokhale and Waghmare [3] proposed a shoulder-surfing-resistant scheme which is a modified version of Asraful and Babbar's scheme [58]. This scheme utilizes a combined recognition- and recall-based approach and follows two steps. In the registration phase, users choose a few images from a set of 25 pictures in step 1. In step 2,

Table 7. Cued-recall graphical password schemes

Scheme	Contribution	Limitation
Blonder [42]	Easy to remember than alphanumeric password. More secure than alphanumeric passwords.	Predefined click region so it is easily identifiable. Susceptible to shoulder-surfing attacks.
Jiminy [43]	Only the precise location of the template of the image needs to be remembered. Reduces stress both for end-users and system administrators.	It does not provide a completely secure mechanism.
Inkblot [44]	No advantage for an attacker in guessing a user's password. High in entropy. Large password space.	Non-functional in some environments (like device with tiny screen).
Passpoint [45]	It is flexible because it allows any image to be used Large password space.	Recording the user's mouse motion can be used to reproduce a password. It is difficult to ensure tolerable click points. Vulnerable to shoulder-surfing.
Suo [46]	Resistant to mouse tracking.	Time consuming. Dicult to use. Too few click points can make the scheme easily guessable.
CCP [47]	Gives implicit feedback. No need to remember the order of the image. Reduces the hotspot effects.	Susceptible to shoulder-surfing attacks.
PCCP [48]	Motivates users to choose more random passwords. Reduces the hotspot effects.	Susceptible to shoulder-sur ng attacks.
Passmatrix [49]	It can avoid false accept points as circular tolerance is used. To some extent, memory requirement in the image pool decreases.	Cannot display random images.
Passmatrix [50]	Friendly interface. Variant response. No need to touch password directly. Random login indicator. User can upload images.	Large login time. Hotspot problem. Susceptible to guessing attack and brute force attack. Does not provide any feedback while wrong entry.
PassBYOP [51]	Multifactor authentication system. Less login time.	There needs an extra camera based device to login with desktop. It will be hard to login if the user lost the physical token.
Passblot [52, 53]	A strict policy of utilizing different passwords for different sites is implemented.	After observing three consecutive login sessions, the system may be cracked by shoulder-surfing attacks. Vulnerable to shoulder-sur ng attack, social engineering attack. Time consuming.
HapticPoint [54]	Mitigates dictionary attacks.	Not fully resilient against shoulder-sur ng attacks.
PassMap [55]	User friendly. Provides better entropy than PassPoints. Easy to memorize. Vulnerable to the threat of pattern dictionary attacks.	Susceptible to shoulder-surfing attacks. Vulnerable to the threat of pattern dictionary attacks.

users are shown 3 questions and must choose 3 points to serve as an ROA (region of answer). During authentication, users must select the correct images from the first step and then select the three regions of the pre-selected image in the next step.

A text-based GPS was proposed by Chen et al. [59] in which a user rotates a circle composed of 8 sectors of different colors containing 64 random characters. Rotating the circle allows the user to select his or her pass-color sector, which contains the pass-character of the password. This scheme is resistant to shoulder-surfing attacks and accidental logins.

Chameleon, a text-based GPS, was proposed by Ku et al. [60]. In this scheme, to authenticate, a user must select different pass-characters and the background color of the pass-characters must match the color of his or her pass-color-shape. This scheme is resistant to accidental login attacks and capture attacks.

The *WIW* scheme was proposed by Man et al. [61] to be resistant to shoulder-surfing attacks. During registration, users choose different images, which are considered pass objects. These objects can have many variants, and a unique code is assigned to each variant. During the authentication process, the pass object variants are presented on the screen and the user must provide the unique code related to the variant as well as a code indicating the relative location of the objects in comparison to the eye-pair of the user. This scheme provides time-variant passwords. However, users need to remember the text strings associated with each pass object, which can be difficult.

Wang et al. [62] proposed a scheme based on graphical password- and text-based Captcha. During registration, users select pass images; each image has a system-generated string of letters associated with it. Users also need to select the specific letter positions from these strings of letters. During authentication, users must recognize the pass-images and enter the characters corresponding to the letter positions of each pass-image as selected during registration. The login time is small compared to that of other GPSs. However, this scheme has memorability issues.

In *Passhint*, proposed by Chowdhury et al. [63], users select 4 images with hints for each image. During authentication, users must select the images with the help of the hints (which are present in the login interface). This scheme provides memorability and security against guessing attacks, uses a lockout policy after authentication failure, and has a low login time. However, it has some drawbacks: the registration time is high, it does not use a variant response password system, and it is not resistant to shoulder-surfing attacks.

Saeed and Umar [64] proposed a hybrid scheme that utilizes the concept of dynamic graphics. During registration, users select pass images from a grid, where each image is associated with a 3-digit random code. Users need to remember the order in which they selected the images. The authentication phase consists of two sub-phases: login phase 1 and login phase 2. In login phase 1, a grid of images are given with some colored balls. Users need to remember the colors of the balls associated with their pass images. During phase 2, the same portfolio is given, but the colors of the balls changes every second. When the colors of the balls correspond to their pass images, they must hit the next button within a certain time frame. This process is repeated five times. It is robust and provides memorability, time-variant responses, and a large password space. Since it requires two login phases, the login time is higher. Users also need to click on the images quickly, before the colors change, which can be quite challenging.

In *GOTPass*, proposed by Alsaiari et al. [65], a user sets a unique username and then draws a pattern which was given during the registration period. The user is then presented with a grid that includes pass and decoy images along with an OTP (one-time password) code. The user has to enter the OTP code in a specified way (chosen during registration) to successfully login. Use of a combinations of multilevel authentication mechanisms (graphical + one-time pass) makes this scheme more secure. Also, users do not need to click on pass images directly. However this scheme has several drawbacks: the password space is not large, there are security issues related to storing images in the database, and image storage affects the scheme's performance and increases the registration time. To mitigate some of these limitations, an improved version has also been proposed [66].

The *cuedR* scheme was proposed by Al-Ameen et al. [67]. In it, six portfolios are selected at random by the system and one keyword from each of the selected portfolios is assigned to the user. During the login phase, the user must identify the keywords for each portfolio and enter the key which corresponds to each keyword within a password field. A user will successfully be authenticated only if the user can enter the correct keys for all of the assigned keywords. Different visual, verbal and spatial cues are given to aid users. This scheme provides variant response passwords as well as implicit feedback and also has a large password size. However, its login time is high and the deployment of cuedR requires a good deal of effort.

Chithra and Sathya [68] proposed *PCGP*, in which a user chooses images from an image pool. The images needs to be cropped correctly in the exact ratio as established in the registration process. Finally, each cropped image must be pasted in its pre-specified location. This scheme requires relatively little time to register. It is also sufficiently complex to thwart guessing attacks and password cracking attempts.

TCpC, a text-based graphical authentication system proposed by Matta and Pant [69], requires the user to enter a login ID first. Then the system shows a screen with a (10×10 or 9×11) matrix that contains different characters. The user looks for their required character and chooses either a row or column which contains the character. Then, the user must click any two characters within the selected row or column. This scheme provides a recovery and renewal phase and a limited number of login trials. It requires no costly hardware support. However, it is time-consuming and the user has to remember his text password.

In *Jumbled PassSteps*, proposed by Songcuan and Sison [70], the user must remember the audio output, which includes a random number and a random traversal direction, generated by a one-time grid traversal indicator module. The random number is required during the authentication process. In addition, the user must identify their pass images from a shuffled image pool generated by a grid shuffling module. Using the pass-image as the starting point of the traversal, the user has to click the decoy image which is found by traversal. The process is

Table 8. Hybrid graphical password schemes

Scheme	Contribution	Limitation
CD-GPS [56]	Large password space. Increased entropy.	Authentication time is longer. Hard to remember additional images in an ordered sequence.
Gokhale and Waghmare [3]	Password space is very large.	Two login phases thus takes time.
Chen et al. [59]	Resistant to accidental login. Resistant to shoulder-sur ng attack.	During the registration phase, a secure channel needs to be established by using SSL (Secure Sockets Layer)/TLS (Transport Layer Security).
Chameleon [60]	Resistant to accidental login attacks and capture attacks.	Three login sessions thus takes time.
WIW [61]	Multiple authentication rounds or scenes thus makes it hard to attack. Time-variant password.	Need to remember strings associated with each pass object which is difficult.
Wang et al. [62]	Challenge response algorithm. Login time small compared to other graphical password scheme.	Add memory burden.
Passhint [63]	Memorability. Provides security for guessing attacks Lockout policy after authentication fails. -Small login time.	Registration time is high. Not variant response. Not resistant against shoulder-surfing.
Saeed and Umar [64]	Better memorability. No costly hardware required. Time variant responses. ..... Large password space. Robust.	Need to remember the order. Two login phases thus takes time. User need to quickly click on the images before color changing.
GOTPass [65]	Use one time session password. Multiple authentication mechanisms (graphical and one time pass) combined. ..... No need to click on pass images. Multilevel authentication.	Password space is not long. Need security improvement while storing images in the database which will also affect the performance. High registration time.
CuedR [67]	Provides implicit feedback. Variant response. System assigned password. To help users that they can identify system-assigned keywords difference cues such as visual, verbal, and spatial are used. Large password size.	Deployment of cuedR required more effort. High login time.
PCGP [68]	Increases the felicity of the end user. Less login and registration time More secure.	May not be easy to crop the image for all users.
TCpC [69]	Provides the recovery and renewal phase. User friendly. No costly hardware support. Limited login trials.	Time consuming. User have to remember his text password.
Jumbled PassSteps [70]	Hard to guess even if the login session is observed. Several independent images. Easy to remember.	User needs an earphone or headset to hear the audio. Not suitable for defaced people.

repeated three times. It uses several independent images. The pass-codes are easy to remember and hard to guess, even if the login session is observed. However, a user needs an earphone or headset to hear the audio. Thus, the system is not suitable for deaf people.

Summary: The review findings for the selected hybrid systems are presented in Table 8.

C. RQ3: Which Algorithms/Techniques Are Mainly Used in GPSs?

To answer this question, we examined the specific

algorithms/techniques used in the selected GPSs. Our analysis is presented below.

We observed that, among the 56 selected studies, only 24 schemes used algorithms. Six of the recognition-based schemes used any sort of algorithm. For example, a hashing algorithm is used in the Deja vu scheme [9]. In Evo-pass [23], both hashing and edge detection algorithms are used. On the other hand, the schemes by Por et al. [24] and LocPass [21] use uniform randomization algorithms. The "Use Your Illusion scheme" [16] relies on a non-photorealistic rendering algorithm, whereas PassApp [26] leverages the Monte Carlo method. The remaining 11 recognition-based schemes do not use an algorithm.

In the recall-based GPS category, 7 schemes use algorithms. Both DAS [27] and BDAS [28] use hashing algorithms, whereas GEAT [37] utilizes support vector distribution estimation (SVDE). A number of techniques, such as Levenshtein distance Trend quadrants. TMD [41] uses vector graphics (SVG). DRAW-A-PIN [36] uses linear interpolation, normalization, and dynamic time warping (DTW). Nearest-neighbor classification and the $P algorithm are employed by YAGP [33]. Finally, gRAT [40] leverages a randomized algorithm. The other schemes in this category do not employ any specific algorithms.

Among the 13 cued-recall-based GPSs, 7 use either an algorithm or a certain kind of technology. For example, Inkblot [44], PassPoints [45] and PassMap [55] use hashing algorithms. On the other hand, PCCP [48] employs persuasive technology, Passblot [52, 53] relies on encryption, PassBYOP [51] utilizes the SIFT algorithm and a blob detection algorithm, and HapticPoint [54] leverages a Deep Gaze algorithm. The rest of the schemes in this category do not utilize any algorithm or technology.

In the hybrid GPS category, only 3 schemes use an algorithm. CuedR [67] employs hashing and salt algorithms. PCCG [68] utilizes Gaussian elimination and Cleaves encryption. Finally, Jumbled PassSteps [70] leverages a random grid traversal method. The rest of the hybrid schemes do not employ any specific algorithms.

A summary of the algorithms/techniques utilized by different schemes is presented in Tables 9–12 for the

Table 9. Utilized algorithms/techniques, attack resiliency and considered contexts for recognition GPS

Scheme	Algorithms/techniques	Resilient against	Context
Deja vu [9]	Hash visualization	Dictionary, spyware, social engineering	PDA, ATM, Websites
Passfaces [10]	Not defined	Spyware, social engineering	Not defined
Photographic authentication [11]	Not defined	Replay attacks	Not defined
Story [12]	Not defined	Dictionary attacks	Untrusted terminals
VIP [13]	Not defined	Dictionary, social engineering	Not defined
CHC [14]	Not defined	Shoulder-surfing, guessing, brute-force attack	ATM
Cognitive authentication [15]	Not defined	Dictionary attacks, spyware, shoulder-surfing, brute-force	Not defined
Use your illusion [16]	Non-photorealistic rendering algorithm	Brute force, guessing, social engineering, shoulder-surfing attacks	Computer, insecure networks (internet cafe)
Color login [17]	Not defined	Brute force attack, spyware, dictionary attack	Can be used in web servers, ATM, cellular phones, computer
GPI/GPIS [18]	Not defined	Dictionary attacks	Not defined
WYSWY [19]	Not defined	Shoulder-surfing, brute force attacks	Not defined
SSP [20]	Not defined	Shoulder-surfing, brute force	PC, Desktop
LocPass [21]	Uniform randomization algorithm	Shoulder-surfing, brute force, guessing	Computer
Rodda et al. [22]	Not defined	Spyware, social engineering attacks, shoulder-surfing attacks	Not defined
Evo-pass [23]	Hash, edge detection algorithm	Shoulder-surfing (mild), guessing, dictionary, social engineering, smudge, image harvest attack	Mobile device
Por et al. [24, 25]	Uniform randomization algorithm	Shoulder-surfing, FOA	Not defined
PassApp [26]	Monte Carlo method	Brute force attacks, shoulder-surfing	Mobile device

Table 10. Utilized algorithms/techniques, attack resiliency and considered contexts for recall GPS

Scheme	Algorithms/techniques	Resilient against	Context
DAS [27]	Hashing	Social engineering attack, brute force attack, spyware	PDA
BDAS [28]	Hashing	Social engineering attack, brute force attack, spyware	PDA
Pass-Go [32]	Not defined	Spyware, social engineering, brute force attack	Application environments (web browser) and input devices (PDA, iPhone, etc.)
Passdoodles [29]	Not defined	Social engineering, spyware	Touch screen, touch pad or another pointing device
PassShapes [31]	Not defined	Spyware, social engineering, brute force attack	Touch screen or similar technology
GEAT [37]	Support vector distribution estimation (SVDE)	Smudge attacks, shoulder-surfing attack	Touch screen devices
YAGP [33]	Levenshtein distance, trend quadrants	Shoulder-surfing, brute force attacks	PC
TMD [41]	Vector graphics (SVG)	Not defined	Touch screens, cross platforms or web-based services
DRAW-A-PIN [38]	Linear interpolation, normalization, dynamic time warping (DTW), Nearest-neighbor classification, $P algorithm	Smudge attacks, shoulder-surfing	Touch screen devices
Android screen-unlock [34]	Not defined	Not defined	Android phone
RouteMap [39]	Not defined	Not defined	PC, Mobile
gRAT [40]	Randomized algorithm	Shoulder-surfing attack, Smudge attack	Smartphones
Windows 8 password [36]	Not defined	Not defined	Windows 8

Table 11. Utilized algorithms/techniques, attack resiliency and considered contexts for cued-recall GPS

Scheme	Algorithms/techniques	Resilient against	Context
Blonder [42]	Not defined	Dictionary attack	PC, telecommunications terminal, PDA, an entrance security system, a vehicle ignition control system, etc.
Jiminy [43]	Not defined	Dictionary attack	Not define
Inkblot [44]	Hashing	Not defined	Not define
Passpoint [45]	Hashing, Discretization of image	Dictionary attack, spyware, social engineering	PC
Suo [46]	Not defined	Guessing attack, brute force, dictionary, shoulder-surfing, social engineering	PC
CCP [47]	Not defined	Social engineering	Web
PCCP [48]	Persuasive technology	Dictionary attack	Computer
Passblot [51, 52]	Encryption	Replay attacks, key-logger, dictionary attack, brute force and blind attacks	PC, Smartphone
Patra et al. [49]	Not defined	Not defined	Web login, ATM card application, mobile app
Passmatrix [50]	Not defined	Shoulder-surfing, smudge attack	Laptop, PC, mobile, bank, ATM, web browser
PassBYOP [51]	SIFT algorithm, a blob detection algorithm	Shoulder-surfing, camera based observation, malware guessing	PC, Smartphone
HapticPoint [54]	Deep Gaze algorithm, haptic feedback	Brute force, dictionary	Smartphones
PassMap [55]	Hashing	Brute force attacks	Web

Table 12. Utilized algorithms/techniques, attack resiliency and considered contexts for hybrid GPS

Scheme	Algorithms/techniques	Resilient against	Context
CD-GPS [56]	Not defined	Brute force, shoulder-surfing	Computer
Gokhale and Waghmare [3]	Not defined	Shoulder-surfing, guessing attacks, brute force	Smart phones, PDA, iPod, iPhone
Chen et al. [59]	Not defined	Shoulder-surfing attack	Not defined
Chameleon [60]	Not defined	Capture attack	Not defined
WIW [61]	Not defined	Shoulder-surfing	Not defined
Wang et al. [62]	Not defined	Spyware, replay, brute force attack	Not defined
Passhint [63]	Not defined	Guessing attacks	Not defined
Saeed and Umar [64]	Not defined	Guessing, shoulder-surfing attacks	ATM, access control, cyber cafe, mobile phone
GOTPass [65]	Not defined	Shoulder-surfing (mild resistance), guessing, spyware, dictionary, anti-phishing, replay, intersection	Web based application
CuedR [67]	Salt, hash	Shoulder-surfing (mild resistant), keystroke loggers, brute force, online guessing attack	Bank, email, social networking, e-commerce, university portal
PCGP [68]	Gaussian elimination, cleaves algorithm	Shoulder-surfing, rainbow table attack, social engineering, guessing	Smart devices
TCpC [69]	Not defined	Shoulder-surfing, hidden camera attacks, phishing, key-logger, brute force	PC, smartphone
Jumbled PassSteps [70]	Random grid traversal method	Hotspot, guessing attack, shoulder-surfing attacks	ATM's, desktop, laptop computers

recognition, recall, cued-recall, and hybrid categories, respectively.

D. RQ4: In What Contexts Are the Selected Schemes Used?

GPSs have been deployed in a number of different contexts. Fig. 3 illustrates the various contexts in which different schemes are used as well as the number of contexts considered by different schemes within the four categories.

Within the recognition-based schemes, 8 schemes—CHC [14], Passfaces [10], color login [17], Story [12], GPI/GPIS [18], the scheme by Por et al. [24], LocPass [21], and the scheme by Rodda et al. [22]—have not been mentioned in any particular context. The contexts used in the rest of the works are PDA, computer, ATM, mobile device, ATM and the web. For recall-based schemes, the considered contexts are PDA, computer, ATM, mobile device, other touch-screen devices, ATM and the web.

Within the cued-recall category, 7 schemes are for computers, 5 schemes are applicable to mobile devices and 4 schemes are for use on the web. One scheme (Jiminy [43]) has not been mentioned in any context. For hybrid-based schemes, 5 schemes (WIW [61], Passhint [63], the scheme by Wang et al. [62], Chameleon [60] and the scheme by Chen et al. [59]) have not been mentioned in any context. Most of the schemes in this category are applicable to computers, mobile systems, and the web.

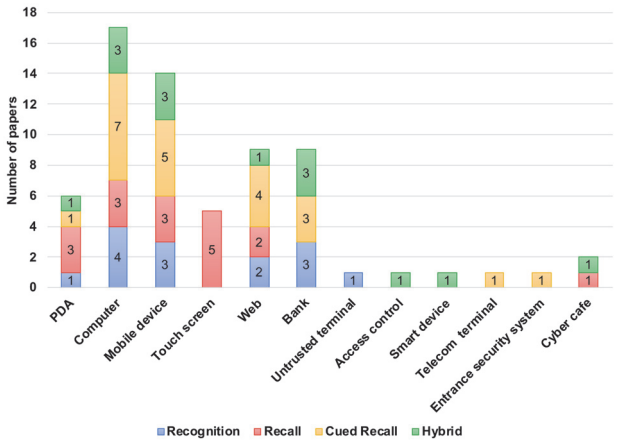

Fig. 3. Contexts used in Graphical password.

As evident in Fig. 3, 14 out of 56 schemes (i.e., 25%) schemes were not mentioned in any particular context, and the majority of contexts that were discussed are computers and mobile devices.

A summary of the contexts considered by different schemes is presented in Tables 9–12 for the recognition, recall, cued-recall, and hybrid categories, respectively.

E. RQ5: Are GPSs strongly resistant to different types of attacks?

To answer this research question, we analyzed the attack resistance capability of the selected schemes. Our findings are presented below.

GPSs aim to provide better security (e.g., larger password space) than alpha-numeric passwords, however, they are still at risk of attacks. Brute force, dictionary, guessing, spyware, shoulder-surfing and social engineering attacks are the current active vectors for graphical authentication environments. Although several studies have suggested that graphical passwords may exhibit greater resiliency against these attacks, no single scheme is completely resistant to all attacks. A summary of the attack resiliency of different schemes is presented in Tables 9–12 for the recognition, recall, cued-recall and hybrid categories, respectively.

In the recognition-based category (Table 9), 10 schemes (CHC [14], use your illusion [16], SSP [20], cognitive authentication [15], Por et al. [24], LocPas [21], Evo-pas [23], Rodda et al. [22], WYSWYE [19], and PassApp [26]) are resistant to shoulder-surfing attacks. On the other hand, 8 schemes (CHC [14], use your illusion [16], SSP [20], color login [17], cognitive authentication [15], the scheme by Por et al. [24], LocPas [21], WYSWYE [19], and PassApp [26]) are resistant to brute force attacks, 4 schemes (CHC [14], use your illusion [16], LocPass [21], and Evo-pass [23]) are resistant to guessing attacks, 7 schemes (Deja vu [9], color login [17], Story [12], VIP [13], GPI/GPIS [18], cognitive authentication [15], and Evo-pass [23]) are resistant to dictionary attacks, 6 schemes (Deja vu [9], Passfaces [10], use your illusion [16], VIP [13], Evo-pass [23], and Rodda et al. [22]) are resistant to engineering attacks and 5 schemes (Deja vu [9], Passfaces [10], color login [17], cognitive authentication [15], and Rodda et al. [22]) are resistant to spyware attacks.

In the recall-based category (Table 10), DAS [27], BDAS [28], Pass-Go [32], and Passdoodles [29] are resistant to social engineering attacks, brute force attacks, and spyware attacks. However, GEAT [37], DRAW-A-PIN [38] and gRAT [40] are resistant to only shoulder-surfing and smudge attacks. Finally, TDM [41], Android screen-unlock [34] and RouteMap [39] have not clearly been shown to be resilient against any type of attack.

In the cued-recall-based category (Table 11), 7 schemes (Blonder [42], Jiminy [43], Passpoint [45], Suo [46], PCCP [48], Passblot [52, 53], and HapticPoint [54]) are resistant to dictionary attacks, 4 schemes (Suo [46], Passblot [52, 53], HapticPoint [54], and PassMap [55]) are resistant to brute force attacks, 3 schemes (Suo [46], Passmatrix [50], and passBOYP [51]) are resistant to shoulder-surfing attacks and 3 schemes (Suo [46], CCP [47], and PCCP [48]) are resistant to social engineering attacks. Inkblot [42] and Patra et al.'s scheme [49] are resistant to guessing attacks.

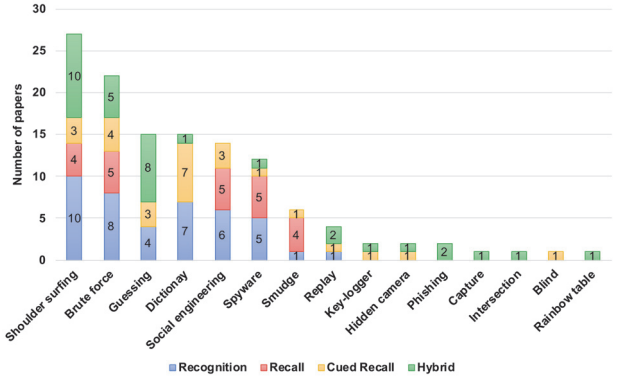

Fig. 4. Graphical password schemes against different attacks.

Among the 12 hybrid schemes (Table 12), 9 (WIW [61], Gokhale and Waghmare [3], CD-GPS [56], GOTPass [65], CuedR [67], PCGP [68], Jumbled PassStep [70], Saeedand Umar [64], Chen et al. [59] and TCpC [69]) are resistant to shoulder-surfing attacks and 5 (Chameleon, CD-GPS, CuedR, the scheme proposed by Wang et al. [62] and TCpC) are resistant to brute force attacks.

Fig. 4 illustrates the different types of attacks that can breach GPSs and the number of schemes in the different categories that are resistant to these attacks.

VI. DISCUSSION

In this section, we provide a brief discussion of our findings about GPSs.

The main challenge in implementing a graphical password authentication system is maintaining the balance between usability and security. In most cases, a particular emphasis on security seems to lead to usability issues like long process time, memorability problems, and so on. Conversely, when a scheme is designed primarily for usability it seems to compromise on security. A harmony arrives when security and usability are emphasized equally. Importantly, users generally attempt to choose a process that takes less time, and graphical password systems are more time-consuming than textual password systems [71]. In some GPSs, users are given a challenge response grid from which to pick a password, e.g., Passfaces [10]. Sometimes users have to complete multiple authentication rounds to login successfully, e.g., CHC [15]. Another important issue with graphical passwords is that they are prone to shoulder-surfing attacks, which needs to be considered. Though a large number of GPSs have been proposed, unfortunately, no single scheme can provide full security against shoulder-surfing attacks.

Also, users have a tendency to think that, so long as they are not a celebrity, no one is going to hack their account. This thinking leads them to construct a weak password with a technique that requires less time and

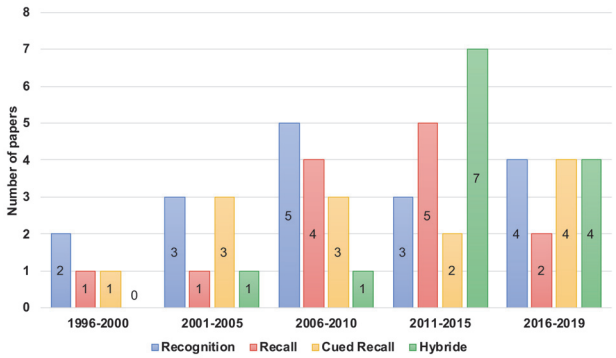

Fig. 5. Graphical password schemes according to publication years.

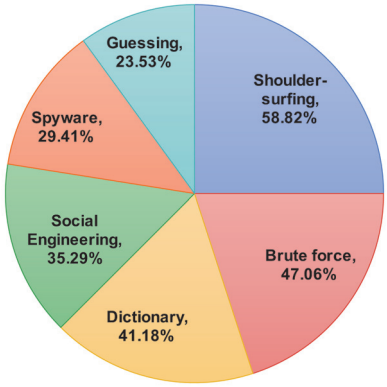

Fig. 6. Resistance against attacks in recognition category.

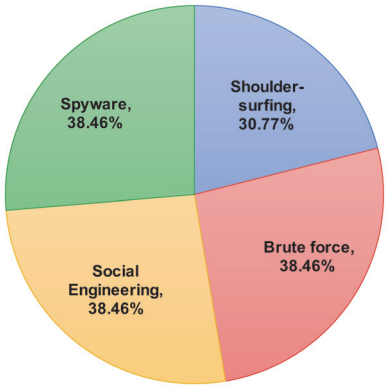

Fig. 7. Resistance against attacks in recrecall category.

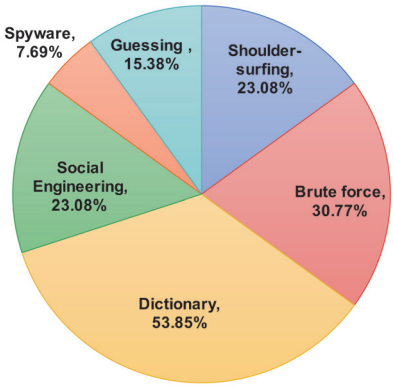

Fig. 8. Resistance against attacks in cued-recall category.

mental energy, as is often seen in text-based password systems. To mitigate these issues in GPSs, the developer and the users need to collaborate with one another. If a developer only emphasizes security while users do not follow any rules when choosing passwords, these issues will never be solved. Users also need to think about their own security. Furthermore, a balance between usability and security must be maintained.

Our review found that a large number of GPSs have been proposed. However, none of these schemes has been widely adopted in the real world. For example, no popular websites, such as social media sites (e.g., Facebook, Instagram and others), have utilized graphical passwords so far. If graphical passwords are widely deployed in different contexts, people will get used to using them.

The idea of a graphical authentication system was introduced in 1996. Since that time, many different graphical authentication systems have been proposed, and the number of new GPSs has gradually increased. To understand this trend, we analyzed the years in which different GPS schemes were introduced. Our analysis is shown in Fig. 5. As shown in Fig. 5, relatively few new graphical authentication systems were introduced from 1996 to 2000 and no hybrid authentication system was developed in that time period. In 2001–2005, the number of GPSs in all categories increased and the first hybrid GPSs were introduced. In 2006–2010, the number of GPSs continued to increase and the number of new recognition-based GPSs reached a maximum. Suddenly, in 2011–2015, the number of hybrid authentication schemes rose drastically, whereas the number of recognition-based GPSs fell. As evident in Fig. 5, in the last 10 years, hybrid schemes have become more popular than other techniques.

Next, we investigated the attack resiliency of schemes in different categories in Figs. 6–9 demonstrate the resiliency of recognition, recall, cued-recall and hybrid schemes, respectively.

As shown in Fig. 6, about 58.82%, 47.06%, 41.18%, 35.29%, 29.41%, and 23.53% of the recognition-based schemes are resistant to shoulder-surfing, brute force, dictionary, social engineering, spyware and guessing attacks, respectively.

Among the recall-based schemes (Fig. 7), 30.77%, 38.46%, 38.46%, and 38.46% are resistant to shoulder-surfing, brute force, social engineering and spyware attacks, respectively. On the other hand, 23.08%, 30.77%, 53.85%, 23.08%, 7.69%, and 15.38% of the cued-recall-

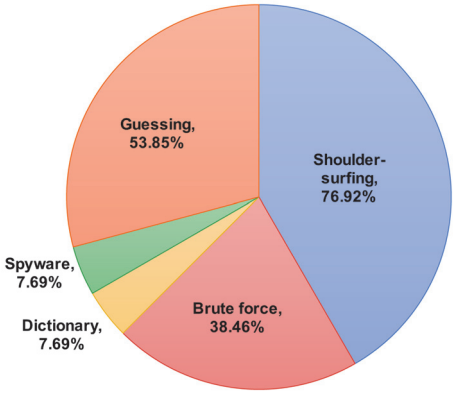

Fig. 9. Resistance against attacks in hybrid category.

based schemes are resistant to shoulder-surfing, brute force, dictionary, social engineering, spyware and guessing attacks, respectively (as shown in Fig. 8).

Finally, 76.92%, 38.46%, 7.69%, 7.69%, and 53.85% of the hybrid schemes are resistant to shoulder- surfing, brute force, dictionary, spyware and guessing attacks, respectively (as illustrated in Fig. 6).

It is evident from our analysis that most of the hybrid schemes are resistant to shoulder-surfing attacks. However, recall-based and hybrid schemes are still vulnerable to dictionary attacks. Though many studies have suggested that various schemes are more resistant to different attacks, no single scheme is completely resistant to all types of attacks.

VII. LIMITATIONS

In this article, we restricted our SLR by applying some selection and quality assessment criteria. Therefore, we may have missed a few schemes that did not meet our selection criteria. Furthermore, some information may be unreliable (e.g., information on resistance to attacks and contributions) as we extracted those data from the original papers, which may include the opinions of the authors.

VIII. CONCLUSION

This SLR aimed to investigate existing GPSs and their contributions, limitations, and challenges. This review identified a total of 1523 candidate papers. After applying a systematic study process and selection criteria, we selected a total of 56 papers. The main findings of this review in relation to the research questions are as follows:

- There has been a great deal of research on GPSs. These schemes can be divided into four categories: Recognition, Recall, Cued-recall, and Hybrid. Among the 56 selected papers, 17 discuss recognition-based authentication schemes, 13 detail recall-based schemes, 13 discuss cued-recall-based schemes and the remaining 13 papers deal with hybrid authentication schemes.
- Our analysis of the selected schemes showed that a wide variety of different algorithms/techniques are used by GPSs, like salt algorithm, hashing, encryption, and so on. We observed that, in the 56 selected studies, only 24 schemes used different algorithms. In the recognition-based category, we found that 6 schemes rely on algorithms. In the recall-based GPS category, 7 schemes use different algorithms. Among the 13 schemes in the cued-recall-based GPS category, 7 use either an algorithm or a technology. Finally, in the hybrid GPS category, only 3 schemes use an algorithm.
- GPSs have been deployed in a number of different contexts. Fourteen out of 56 schemes were not mentioned in any particular context. The majority of considered contexts were computers and mobile devices.
- We also analyzed the attack resiliency of different kinds of GPSs. Among the recognition-based schemes, 10 are resistant to shoulder-surfing attacks, 8 are resistant to brute force attacks, 4 are resistant to guessing attacks, 7 are resistant to dictionary attacks, 6 are resistant to social engineering attacks and 5 are resistant to spyware attacks. Among the recall-based schemes, 4 are resistant to social engineering attacks, brute force attacks and spyware attacks, while 3 are resistant to shoulder-surfing and smudge attacks. In the cued-recall-based category, 7 schemes are resistant to dictionary attacks, 4 are resistant to brute force attacks, 3 are resistant to shoulder-surfing attacks, 3 are resistant to social engineering attacks, and 2 are resistant to guessing attacks. Among the hybrid-based schemes, 9 are resistant to shoulder-surfing attacks and 5 are resistant to brute force attacks.

The main purpose of this SLR is to summarize relevant papers and to explore various different aspects of GPSs. The results of this review could be useful for researchers who wish to analyze the work on different GPSs.

REFERENCES

1. X. Suo, Y. Zhu, and G. S. Owen, "Graphical pass- words: a survey," in *Proceedings of the 21st Annual Computer Security Applications Conference (ACSAC)*, Tucson, AZ, 2005.
2. R. Morris and K. Thompson, "Password security: a case history," *Communications of the ACM*, vol. 22, no. 11, pp. 594-597, 1979.
3. M. A. S. Gokhale and V. S. Waghmare, "The shoulder surfing resistant graphical password authentication technique," *Procedia Computer Science*, vol. 79, pp. 490-498, 2016.
4. R. Biddle, S. Chiasson, and P. C. Van Oorschot, "Graphical

passwords: learning from the first twelve years," *ACM Computing Surveys*, vol. 44, no. 4, pp. 1-41, 2012.
5. M. D. Hafiz, A. H. Abdullah, N. Ithnin, and H. K. Mammi, "Towards identifying usability and security features of graphical password in knowledge based authentication technique," in *Proceedings of 2008 Second Asia International Conference on Modelling & Simulation (AMS)*, Kuala Lumpur, Malaysia, 2008, pp. 396-403.
6. R. Biddle, S. Chiasson, and P. C. Van Oorschot, *Graphical Passwords: Learning from the First Generation*. Ottawa, Canada: School of Computer Science, Carleton University, 2009.
7. B. Kitchenham, "Procedures for performing systematic reviews," Keele University, Keele, UK, *Technical Report SE-0401*, 2004.
8. H. Gao, W. Jia, F. Ye, and L. Ma, "A survey on the use of graphical passwords in security," *Journal of Software*, vol. 8, no. 7, pp. 1678-1698, 2013.
9. R. Dhamija and A. Perrig, "Deja vu: a user study: using images for authentication," in *Proceedings of the 9th USENIX Security Symposium*, Denver, CO, 2000, pp. 45-58.
10. S. Brostoff and M. A. Sasse, "Are passfaces more usable than passwords? A field trial investigation," in *People and computers XIV—Usability or Else!* London, UK: Springer, 2000, pp. 405-424.
11. 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.
12. D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes," in *Proceedings of the 13th USENIX Security Symposium*, San Diego, CA, 2004.
13. 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. 1-2, pp. 128-152, 2005.
14. S. Wiedenbeck, J. Waters, L. Sobrado, and J. C. Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme," in *Proceedings of the Working Conference on Advanced Visual Interfaces*, Venezia, Italy, 2006, pp. 177-184.
15. D. Weinshall, "Cognitive authentication schemes safe against spyware," in *Proceedings of 2006 IEEE Symposium on Security and Privacy*, Berkeley, CA, 2006.
16. 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*, Pittsburgh, PA, 2008, pp. 35-45.
17. H. Gao, X. Liu, R. Dai, S. Wang, and X. Chang, "Analysis and evaluation of the colorlogin graphical password scheme," in *Proceedings of 2009 5th International Conference on Image and Graphics*, Xi'an, China, 2009, pp. 722-727.
18. K. Bicakci, N. B. Atalay, M. Yuceel, H. Gurbaslar, and B. Erdeniz, "Towards usable solutions to graphical password hotspot problem," in *Proceedings of 2009 33rd Annual IEEE International Computer Software and Applications Conference*, Seattle, WA, 2009, pp. 318-323.
19. R. A. Khot, P. Kumaraguru, and K. Srinathan, "WYSWYE: shoulder surfing defense for recognition based graphical passwords," in *Proceedings of the 24th Australian Computer-Human Interaction Conference*, Melbourne, Australia, 2012, pp. 285-294.
20. T. S. Wu, M. L. Lee, H. Y. Lin, and C. Y. Wang, "Shoulder-surfing-proof graphical password authentication scheme," *International Journal of Information Security*, vol. 13, no. 3, pp. 245-254, 2014.
21. L. Yee, L. A. Adebimpe, M. Y. I. Idris, C. S. Khaw, and C. S. Ku, "LocPass: a graphical password method to prevent shoulder-surfing," *Symmetry*, vol. 11, article no. 1252, 2019.
22. V. Rodda, G. R. Kancherla, and B. R. Bobba, "Shoulder-surfing resistant graphical password system for cloud," *International Journal of Applied Engineering Research*, vol. 12, no. 16, pp. 6091-6096, 2017.
23. X. Yu, Z. Wang, Y. Li, L. Li, W. T. Zhu, and L. Song, "EvoPass: evolvable graphical password against shoulder-surfing attacks," *Computers & Security*, vol. 70, pp. 179-198, 2017.
24. L. Y. Por, C. S. Ku, A. Islam, and T. F. Ang, "Graphical password: prevent shoulder-surfing attack using digraph substitution rules," *Frontiers of Computer Science*, vol. 11, no. 6, pp. 1098-1108, 2017.
25. L. Yee, C. S. Ku, and T. F. Ang, "Preventing shoulder-surfing attacks using digraph substitution rules and pass-image output feedback," *Symmetry*, vol. 11, article no. 1087, 2019.
26. H. Sun, K. Wang, X. Li, N. Qin, and Z. Chen, "Passapp: my app is my password!," in *Proceedings of the 17th International Conference on Human- Computer Interaction with Mobile Devices and Services*, Copenhagen, Denmark, 2015, pp. 306-315.
27. I. H. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The design and analysis of graphical passwords," in *Proceedings of the 8th USENIX Security Symposium*, Washington, DC, 1999.
28. P. Dunphy and J. Yan, "Do background images improve 'draw a secret' graphical passwords?," in *Proceedings of the 14th ACM Conference on Computer and Communications Security*, Alexandria, VA, 2007, pp. 36-47.
29. C. Varenhorst, M. Kleek, and L. Rudolph, "Passdoodles: a lightweight authentication method," Research Science Institute, Cambridge, MA, 2004.
30. J. Goldberg, J. Hagman, and V. Sazawal, "Doodling our way to better authentication," in *Proceedings of the Human Factors in Computing Systems (Extended Abstracts)*, Minneapolis, MN, 2002, pp. 868-869.
31. R. Weiss and A. De Luca, "PassShapes: utilizing stroke based authentication to increase password memorability," in *Proceedings of the 5th Nordic Conference on Human-Computer Interaction: Building Bridges*, Lund, Sweden, 2008, pp. 383-392.
32. H. Tao and C. Adams, "Pass-Go: a proposal to improve the usability of graphical passwords," *IJ Network Security*, vol. 7, no. 2, pp. 273-292, 2008.
33. H. Gao, X. Guo, X. Chen, L. Wang, and X. Liu, "YAGP: yet another graphical password strategy," in *Proceedings of 2008 Annual Computer Security Applications Conference (ACSAC)*, Anaheim, CA, 2008, pp. 121-129.
34. [Android Online]. Available: http://android.com
35. A. J. Aviv, K. L. Gibson, E. Mossop, M. Blaze, and J. M.

Smith, "Smudge attacks on smartphone touch screens," *Woot*, vol. 10, pp. 1-7, 2010.
36. Z. Pace, "Window 8: signing in with a picture password," 2011; https://moviesgamesandtech.com/2011/12/17/windows-8-signing-in-with-a-picture-password/.
37. M. Shahzad, A. X. Liu, and A. Samuel, "Secure unlocking of mobile touch screen devices by simple gestures: you can see it but you can not do it," in *Proceedings of the 19th Annual International Conference on Mobile Computing & Networking*, Miami, FL, 2013, pp. 39-50.
38. T. V. Nguyen, N. Sae-Bae, and N. Memon, "DRAW-A-PIN: authentication using finger-drawn PIN on touch devices," *Computers & Security*, vol. 66, pp. 115-128, 2017.
39. W. Meng, "RouteMap: a route and map based graphical password scheme for better multiple password memory," in *Network and System Security*. Cham, Switzerland: Springer, 2015, pp. 147-161.
40. M. A. Khan, I. U. Din, S. U. Jadoon, M. K. Khan, M. Guizani, and K. A. Awan, "g-RAT: a novel graphical randomized authentication technique for consumer smart devices," *IEEE Transactions on Consumer Electronics*, vol. 65, no. 2, pp. 215-223, 2019.
41. H. Y. Chiang and S. Chiasson, "Improving user authentication on mobile devices: a touchscreen graphical password," in *Proceedings of the 15th International Conference on Human-Computer Interaction with Mobile Devices and Services*, Munich, Germany, 2013, pp. 251-260.
42. G. E. Blonder, "Graphical password," US Patent 5559961, Sep 24, 1996,
43. K. Renaud and E. Smith, "Jiminy: helping users to remember their passwords," 2001; http://hdl.handle.net/10500/24759.
44. A. Stubblefield and D. Simon, "Inkblot authentication," Microsoft Corporation, Redmond, WA, *Technical Report MSR-TR-2004-85*, 2004.
45. 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. 1-2, pp. 102-127, 2005.
46. X. Suo, "A design and analysis of graphical password," Master's thesis, Georgia State University, Atlanta, GA, 2006.
47. S. Chiasson, P. C. Van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," in *Computer Security – ESORICS 2007*. Heidelberg, Germany: Springer, 2007, pp. 359-374.
48. S. Chiasson, A. Forget, R. Biddle, and P. V. Oorschot, "Influencing users towards better passwords: persuasive cued click-points," in *Proceedings of People and Computers XXII Culture, Creativity, Interaction (HCI)*, Liverpool, UK, 2008, pp. 121-130.
49. K. Patra, B. Nemade, D. P. Mishra, and P. P. Satapathy, "Cued-click point graphical password using circular tolerance to increase password space and persuasive features," *Procedia Computer Science*, vol. 79, pp. 561-568, 2016.
50. H. M. Sun, S. T. Chen, J. H. Yeh, and C. Y. Cheng, "A shoulder surfing resistant graphical authentication system," *IEEE Transactions on Dependable and Secure Computing*, vol. 15, no. 2, pp. 180-193, 2016.
51. A. Bianchi, I. Oakley, and H. Kim, "PassBYOP: bring your own picture for securing graphical passwords," *IEEE Transactions on Human-Machine Systems*, vol. 46, no. 3, pp. 380-389, 2015.
52. S. Gupta, P. Sabbu, S. Varma, and S. V. Gangashetty, "Passblot: a usable way of authentication scheme to generate one time passwords," in *Advances in Network Security and Applications*. Heidelberg, Germany: Springer, 2011, pp. 374-382.
53. S. Gupta, S. Sahni, P. Sabbu, S. Varma, and S. V. Gangashetty, "Passblot: a highly scalable graphical one time password system," *International Journal of Network Security & Its Applications*, vol. 4, no. 2, p. 201, 2012.
54]T. Ratchasan and R. Wiangsripanawan, "HapticPoints: the extended passpoints graphical password," in *Information Security Applications*. Cham, Switzerland: Springer, 2018, pp. 16-28.
55. H. M. Sun, Y. H. Chen, C. C. Fang, and S. Y. Chang, "PassMap: a map based graphical-password authentication system," in *Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security*, Seoul, Korea, 2012, pp. 99-100.
56. Y. Meng, "Designing click-draw based graphical password scheme for better authentication," in *Proceedings of 2012 IEEE 7th International Conference on Networking, Architecture, and Storage*, Xiamen, China, 2012, pp. 39-48.
57. Z. Zhou, C. N. Yang, Y. Yang, and X. Sun, "Polynomial-based google map graphical password system against shoulder-surfing attacks in cloud environment," *Complexity*, vol. 2019, article no. 2875676, 2019.
58. M. A. Haque and B. Imam, "A new graphical password: combination of recall & recognition based approach," *International Journal of Computer, Electrical, Automation, Control and Information Engineering*, vol. 8, no. 2, pp. 320-324, 2014.
59. Y. L. Chen, W. C. Ku, Y. C. Yeh, and D. M. Liao, "A simple text-based shoulder surfing resistant graphical password scheme," in *Proceedings of 2013 International Symposium on Next-Generation Electronics*, Kaohsiung, Taiwan, 2013, pp. 161-164.
60. W. C. Ku, D. M. Liao, C. J. Chang, and P. J. Qiu, "An enhanced capture attacks resistant text-based graphical password scheme," in *Proceedings of 2014 IEEE/CIC International Conference on Communications in China (ICCC)*, Shanghai, China, 2014, pp. 204-208.
61. S. Man, D. Hong, and M. M. Matthews, "A shoulder-surfing resistant graphical password scheme: WIW," in *Proceedings of the International Conference on Security and Management*, Las Vegas, NV, 2003, pp. 105-111.
62. L. Wang, X. Chang, Z. Ren, H. Gao, X. Liu, and U. Aickelin, "Against spyware using captcha in graphical password scheme," in *Proceedings of 2010 24th IEEE International Conference on Advanced Information Networking and Applications*, Perth, Australia, 2010, pp. 760-767.
63. S. Chowdhury, R. Poet, and L. Mackenzie, "Passhint: memorable and secure authentication," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Toronto, Canada, 2014, pp. 2917-2926.
64. S. Saeed and M. S. Umar, "A hybrid graphical user authentication scheme," in *Proceedings of 2015 Communication, Control and Intelligent Systems (CCIS)*, Mathura, India,

2015, pp. 411-415.
65. H. Alsaiari, M. Papadaki, P. Dowland, and S. Furnell, "Secure graphical one time password (GOTPass): an empirical study," *Information Security Journal: A Global Perspective*, vol. 24, no. 4-6, pp. 207-220, 2015.
66. H. Alsaiari, M. Papadaki, P. Dowland, and S. Furnell, "Graphical one-time password (GOTPass): a usability evaluation," *Information Security Journal: A Global Perspective*, vol. 25, no. 1-3, pp. 94-108, 2016.
67. M. N. Al-Ameen, M. Wright, and S. Scielzo, "Towards making random passwords memorable: leveraging users' cognitive ability through multiple cues," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, Seoul, Korea, 2015, pp. 2315-2324.
68. P. Chithra and K. Sathya, "Pristine PixCaptcha as graphical password for secure eBanking using Gaussian elimination and cleaves algorithm," in *Proceedings of 2018 International Conference on Computer, Communication, and Signal Processing (ICCCSP)*, Chennai, India, 2018, pp. 1-6.
69. P. Matta and B. Pant, "TCpC: a graphical password scheme ensuring authentication for IoT resources," *International Journal of Information Technology*, vol. 12, pp. 699-709, 2020.
70. J. P. Songcuan and A. M. Sison, "Jumbled passsteps: a hotspot guessing attack resistant graphical password authentication scheme based on the modified passmatrix method," in *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy*, Kuala Lumpur, Malaysia, 2019, pp. 55-59.
71. A. V. D. M. Kayem, "Graphical passwords: a discussion," in *Proceedings of 2016 30th International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, Crans-Montana, Switzerland, 2016, pp. 596-600.

Tahmina Islam Shammee

Tahmina Islam Shammee received her B.Sc. in Computer Science and Engineering from Leading University, Sylhet, Bangladesh in 2017. Currently, she is pursuing her M.Sc. in Computer Science and Engineering from Shahjalal University of Science & Technology, Sylhet, Bangladesh. She is also working as a Junior Web Developer in SJ Innovation, Sylhet, Bangladesh. Her research interests include HCI and computer security.

Taslima Akter

Taslima Akter is an undergraduate student of Computer Science and Engineering at Shahjalal University of Science and Technology, Sylhet, Bangladesh. Her research interests are graphical passwords and security.

Muthmainna Mou

Muthmainna Mou is an undergraduate student of Computer Science and Engineering at Shahjalal University of Science and Technology, Sylhet, Bangladesh. Her research interests are graphical passwords and security.

Farida Chowdhury

Farida Chowdhury received her Ph.D. degree in Computer Science from the University of Stirling, U.K., where she investigated the effect of churn in NAT-ed Structured Peer-to-Peer Overlays. She is currently an Associate Professor with the Department of Computer Science and Engineering, Shahjalal University of Science and Technology, Bangladesh. She has published many articles in reputed journals and as book chapters as well as in different conferences and workshops. Her research interests include networking, blockchain, big data, cloud computing, HCI, and security and privacy issues in social networks.

Md Sadek Ferdous

Md Sadek Ferdous received his Ph.D. degree in identity management from the University of Glasgow, UK. He is currently working as an Assistant Professor with the Department of Computer Science and Engineering, Shahjalal University of Science and Technology, Sylhet, Bangladesh. He is also a Research Associate with the Centre for Global Finance and Technology, Imperial College Business School. He has several years of experience of working as a Postdoctoral Researcher in different universities in different European and UK-funded research projects. He has published numerous research articles and book chapters in these domains in different books, journals, conferences, workshops, and symposiums. His current research interests include blockchain, identity management, trust management and security and privacy issues in cloud computing, and social networks.