IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2019.DOI

A Secure Hybrid Authentication Scheme using PassPoints and Press Touch Code

SAIFUL AZAD[1,2], NOOR ELYA AFIQAH CHE NORDIN[1], NUR NADHIRAH AB RASUL[1], MUFTI MAHMUD[3], (Senior Member, IEEE), KAMAL Z. ZAMLI[1], (Senior Member, IEEE)

[1]University Malaysia Pahang, Gambang 26300, Kuantan, Pahang, Malaysia
[2]IBM Centre of Excellence, UMP, Gambang 26300, Kuantan, Pahang, Malaysia
[3]Department of Computing & Technology, Nottingham Trent University, NG11 8NS, Nottingham, UK

Corresponding author : Mufti Mahmud (e-mail : mufti.mahmud@{gmail.com,ntu.ac.uk}).

ABSTRACT With the increasing capabilities of smart devices, keeping them secure has become a major concern. To mitigate that concern, over the last few years, several new classes of authentication schemes have been proposed. Graphical Authentication (GA) is one of those classes and is the focus of this paper. The GA schemes are more popular and preferable for smart devices due to their : heavily graphics-oriented nature, higher memorability over text-based schemes, and no additional hardware requirement. However, most of these GA schemes are unable to resist several prominent attacks, namely shoulder surfing, smudge, and brute force. Therefore, in this paper, a new hybrid authentication scheme is proposed which seamlessly integrates two independent yet popular authentication schemes — Passpoints and Press Touch Code or PTC. The purpose of this new scheme is to ensure a higher level of security by resisting those prominent attacks. The proposed scheme is implemented on the Android operating system and is tested on Huawei P9 plus device, a pressure sensitivity screen enabled device, which is compulsory for the PTC scheme. The performance of the proposed technique is evaluated for security, functionality, and usability. When it is compared with other similar schemes, it outperforms the existing schemes.

INDEX TERMS Authentication schemes, Graphical authentication schemes, Hybrid authentication schemes, Locimetric schemes, PassPoints, Press touch code.

I. INTRODUCTION

AUTHENTICATION is the most common access control method that is applied in almost all digital and computing devices. Generally, the process of authentication involves in acquisition of data from the users and comparing them with the data that are saved in the local database or in the remote authentication server. If the data are matched, the process is deemed complete and the user is given access to the system; otherwise, the user is required to repeat the process until the number of maximum attempt is reached. At the beginning of its introduction, it was a word or a string of characters. However, with the enhancement of smart device technologies, several new classes of authentication schemes have been proposed.

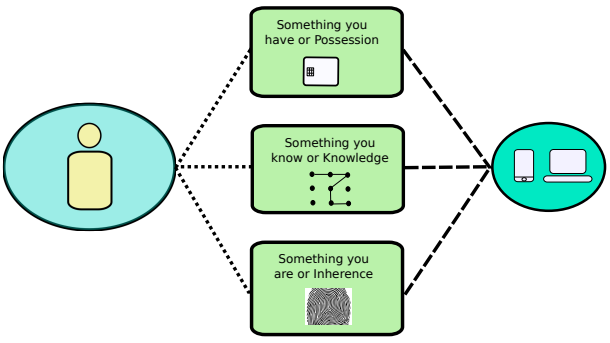

FIGURE 1: The factors that are considered for controlling the access of the smart devices are illustrated.

According to a blog article published by Pearson IT Certification [1], authentication schemes are based on the following three factors, namely (i) something you have or possession (token/smartcard), (ii) something you know or knowledge (PIN, password), and (iii) something you are or inherence (biometric). These factors are also illustrated in Figure 1 along with an example for each factor. Among these three, the most popular one is the second factor, i.e.,

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2948977, IEEE Access

something you know — also known as password-based authentication schemes. Again, these schemes can be further classified as Text-based Authentication (TA) schemes and Graphical Authentication (GA) schemes. However, for the TA schemes, memorability always remains a big concern; and hence, many users tend to choose smaller lengths or weak texts as passwords. Here, the matter of the fact is that when a weak password is chosen to facilitate memorability, it offers lower or no security due to its vulnerability towards many attacks including guessing and brute force.

Conversely, for smart devices, GA schemes are more preferable over TA schemes due to their heavily graphic-oriented nature [2]. In addition, it has been proven by several psychological studies [3] that human can recall visual images easily than texts or alphanumeric characters. Again, no additional hardware is required for operating many of these schemes. However, most of the existing GA schemes are not resilient to three prominent attacks [4], namely shoulder surfing [5], smudge [6], and brute force [2]. In case of the shoulder surfing attack, an attacker can obtain information, such as personal identification numbers (PINs), passwords, and other confidential data by looking over the victim's shoulder. In case of the smudge attack, an attacker relies on the oily residues that are left behind by the user's finger(s) from the last authentication session. And, a brute force attack consists of an attacker systematically checking all possible passwords and passphrases until the match is found. To tackle these attacks, there is a need of a secure GA scheme; and hence, it still remains an important topic to investigate. Therefore, in this paper, a new hybrid GA scheme is proposed. The notable contributions of this work are summarized as :

- — A new hybrid authentication scheme is proposed integrating a locimetric scheme, namely PassPoints with the press touch code to tackle three prominent attacks, namely shoulder surfing, brute force, and smudge.
- — A technique for the seamless integration of both the schemes is introduced.
- — An extensive analysis on the security of the proposed technique is performed including formulations to discover the theoretical password space of the proposed technique.

The rest of the paper is organized as follows. In Section II, most relevant schemes to the proposed technique are reviewed to identify their limitations and to establish the necessity of proposing a new authentication scheme. The proposed technique is elaborated in Section III along with its registration and authentication procedures. It is evaluated in Section IV to discover the effectiveness of the proposed technique. This paper ends with a concluding remark in Section V.

II. RELATED WORKS

Since the proposed technique is a hybrid graphical scheme that combines the PassPoints — a locimetric scheme — with the Press Touch Code (PTC), this section discusses only similar approaches. Note that locimetric schemes are click-based GA schemes where pre-registered target points are necessary to be identified from an individual image as a process of authentication [7]. The evaluation of these schemes starts with the Blonder scheme [8] — the maiden GA scheme.

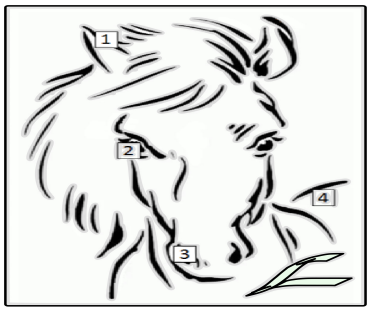

FIGURE 2: An example of Blonder authentication scheme where boxes with the numbers represent the sequence of clicks.

In Blonder scheme, a user is required to click on several pre-selected areas (or on tag regions) of a pre-decided graphical image chronologically as a password. An example of this scheme is delineated in Figure 2 where the sequence of clicks are presented with numbers. A user would be given access only if the click-points and their chronological orders are matched with that of the registered credentials. This scheme has several advantages over TA schemes, such as higher memorability since images are easier to recall, specifically images with personal meaning [9]) and large password space, e.g., in an image of $3\ in \times 5\ in$ with one-quarter inch square ($6\ mm \times 6\ mm$) click points — it offers 13.6 million possible combinations for a selection of just 3 click points in the correct chronological order. However, generally there remains only limited number of click points in an image (perhaps a few dozens in an image [10]) and they are readily identifiable. Therefore, only those images must be chosen that contain adequate number of click points for ensuring higher security. Again, this scheme offers low resilience against the shoulder surfing attack. It also suffers from the hot-points selection problem, where some click-points are selected more than others by the users.

With the advancement of the technologies, several other similar schemes are proposed, such as PassPoints [11], V-Go [12], PassMap [13], and so on. Among them, in the proposed scheme, PassPoints has been chosen to integrate with the PTC due to : i) human being can remember click-points more precisely over texts, which alleviate the memorability issue of the users and ii) it provides a larger password space; and thus, can tackle the brute force attack and guessing attack. Note that PassPoints is an enhancement of the Blonder's technique where a password is represented by numerous clicks on a single picture. However, unlike its predecessor, a user is not restricted to any predefined boundaries and s/he

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2948977, IEEE Access

has the freedom to click at any place on an image. In addition, a password is translated to a cryptographical hash accounting a tolerance region around the choices [14]. A legitimate click must remain within the tolerance boundary. For improved security, the fundamental prerequisite of selecting an image is that it must be a virtually reach image with numerous potentially memorable click points [15]. However, it is still vulnerable to several prominent attacks including shoulder surfing and smudge.

On the other hand, PTC [4] is a new screen size independent authentication scheme that utilizes the press touch or 3-D display capabilities of various Pressure Sensitivity Screen (PSS) enabled smart devices. Here, a password is formed by pressing on a screen forcefully; and hence, the name. The number of forced presses is later discovered from a large number of press values employing the press detection algorithm, which is considered as a PTC value. To increase the password space of the PTC, in [4], it is incorporated with a 2×2 grid cells. In oppose to the simple PTC, this Multi-PTC with grid allows users to provide their PTCs on these grid cells. Although, it has the resilience against the smudge attack — thanks to the scheme that permits a user to visit a cell multiple times. However, its resilience against the shoulder surfing attack is fair as long as the distance between the user and the attacker is not within the vicinity of 0.5m [4]. Again, from an investigation in [4], it has been reported that despite of supporting visit of many grid cell in the Multi-PTC with grid; generally, the users preferred visiting limited number of cells (mostly 4 cells or less). Consequently, its resilience against the brute force attack is challenged.

Among the existing schemes, most comparable to the PTC scheme are knock code [16], vibration code [2], vibration and pattern code [2], and TinyLock [17]. Here, in knock code — which comes with almost all the recent LG devices — a credential is generated using the knocks on a 2×2 grid cells. One of the major drawbacks of this scheme is its vulnerability towards the shoulder surfing attack as reported in [4]. Moreover, it offers a limited password space which is comparable to PIN, and hence, susceptible to the brute force attack. On the other hand, the vibration code utilizes the vibrations of the existing smart devices to generate codes. Since vibration is a sense-based technique, it can resist shoulder surfing attack. However, due to its limited password space even lower than the knock code, it is susceptible to the brute force attack. Again, to increase the password space, another variant of the vibration code is proposed, called vibration and pattern code, which integrates a 2×2 grid cells to draw patterns. The major limitation of this scheme is that it spends a considerably longer duration for authentication. As reported in [4], the average authentication duration using this scheme lies between 4 seconds to 10 seconds.

A variant of the Android Pattern lock is proposed, named TinyLock, to resist the smudge attack and the shoulder surfing attack up to a certain extent. In oppose to its predecessor, tiny grid cells are utilized to generate credentials, and hence, the name. However, it is still susceptible to the brute force attack and experiences fat finger problem. Therefore, proposing a secure authentication scheme still remains an important area of research to investigate.

Here, it is noteworthy to mention that the authentication scheme that is proposed in this paper is not a multi-factor authentication scheme where a user is granted access only after successfully presenting two or more pieces of evidences or factors among possession, knowledge, and inherence, which are mentioned in Section I. The justification of our selection is that most of the multi-factor authentication schemes take longer time in authentication due to presenting two or more different pieces of evidences, and hence, is not suitable for the systems that required frequent access like smart devices. Instead, our proposed scheme is a hybrid scheme like a few of the other schemes that are already proposed.

In [18], a hybrid textual authentication scheme is proposed that is suitable for Personal Digital Assistants (PDAs). This scheme utilizes grid cells for generating passwords. Although, the authors claim that it is resilience against the shoulder surfing, dictionary, and brute force attacks; however, no detail user study is reported to support the claim. Again, since this scheme is based on textual authentication, it is, to some extent, vulnerable to the shoulder surfing attack. Another hybrid authentication scheme is proposed in [19], which is based on shape and text where shapes of strokes are provided as origin passwords followed by text passwords. However, this scheme has several security and usability issues. For instance, due to lack of adaptability, generally users prefer simple or weak strokes, and thus, facilitating attackers to break the password with minimum efforts. Again, the password registration step of this scheme is vulnerable to several attacks as users have to tell the original shapes and strokes to the system. One more similar authentication scheme combining text and image is proposed in [20] with objectives of improving password space and memorability. However, since text and image are both vulnerable to the shoulder surfing attack, the proposed scheme is also vulnerable to the shoulder surfing attack along with others.

Therefore, more advanced authentication schemes are required to improve the security of the smart devices. One such scheme is proposed in this paper that seamlessly integrates the PassPoints and PTC schemes, called Passpoints with PTC or P3TC scheme.

III. PROPOSED SCHEME

As mentioned earlier, in the proposed technique, we integrate the PassPoints — a locimetric scheme — and the PTC to conjoin their advantages for defending three prominent attacks that are mentioned in Section I. Additionally, the PTC has the ability of defending the shoulder surfing attack up to a certain extent and the smudge attack. Again, the PassPoints offers a large password space, and the integration of these two schemes produces even a larger password space, which makes it difficult for the brute force attack to break the password. Another advantage that the proposed technique inherits from its predecessor — PassPoints — is its increased

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2948977, IEEE Access

1	2	3	4	5		m
m+1	m+2	m+3	m+4	m+5	• • •	2m
2m+1	2m+2	2m+3	2m+4	2m+5		3m
3m+1	3m+2	3m+3	3m+4	3m+5		4m
4m+1	4m+2	4m+3	4m+4	4m+5		5m
5m+1	5m+2	5m+3	5m+4	5m+5		6m
6m+1	6m+2	6m+3	6m+4	6m+5		7m
					• • •	
						nm

FIGURE 3: Grid cells on a smart device display. A number is assigned to each cell, which can be found employing Eq. 1.

memorability as it has been reported in [21] is that a human can recognize 98.5% images accurately even after 60 minutes delay.

The detail discussion of the proposed scheme is mentioned below. For better understanding, the entire discussion is divided into four parts : i) PassPoints, ii) Press Touch Code, iii) Seamless Integration, and iv) Registration and Authentication.

A. PASSPOINTS

In the proposed scheme, a background image needs to be selected to facilitate integrating the PassPoints with it. A user has to select a number of points, also known as click-points, P from that image. Generally, a point, p, where $p \in P$ of a smart device screen is represented using the Cartesian coordinate, i.e., (x, y), where x represents the horizontal and y represents the vertical coordinates. Here, x coordinate is a number of pixels along the horizontal axis of a display starting from the pixel (pixel 0) on the extreme left of the screen and y coordinate is a number of pixels along the vertical axis of a display starting from the pixel (pixel 0) at the top of the screen. Together, the x and y coordinates locate a specific pixel location on the screen. However, since pixels are very tiny, it is difficult to repeat a selection precisely. Therefore, in the proposed scheme, the entire display screen is divided into several grid cells, which are numbered incrementally from the top-left to the bottom-right. These grid cells can be displayed with solid lines or can be hidden from the user. Here, it is noteworthy to mention that p_i contains the given number of the cell, not the coordinates. The value of p_i is determined as follows :

$$p_i = \left\lceil \frac{x}{\frac{\gamma_x}{m}} \right\rceil + \left\lfloor \frac{y}{\frac{\gamma_y}{n}} \right\rfloor \times m \qquad (1)$$

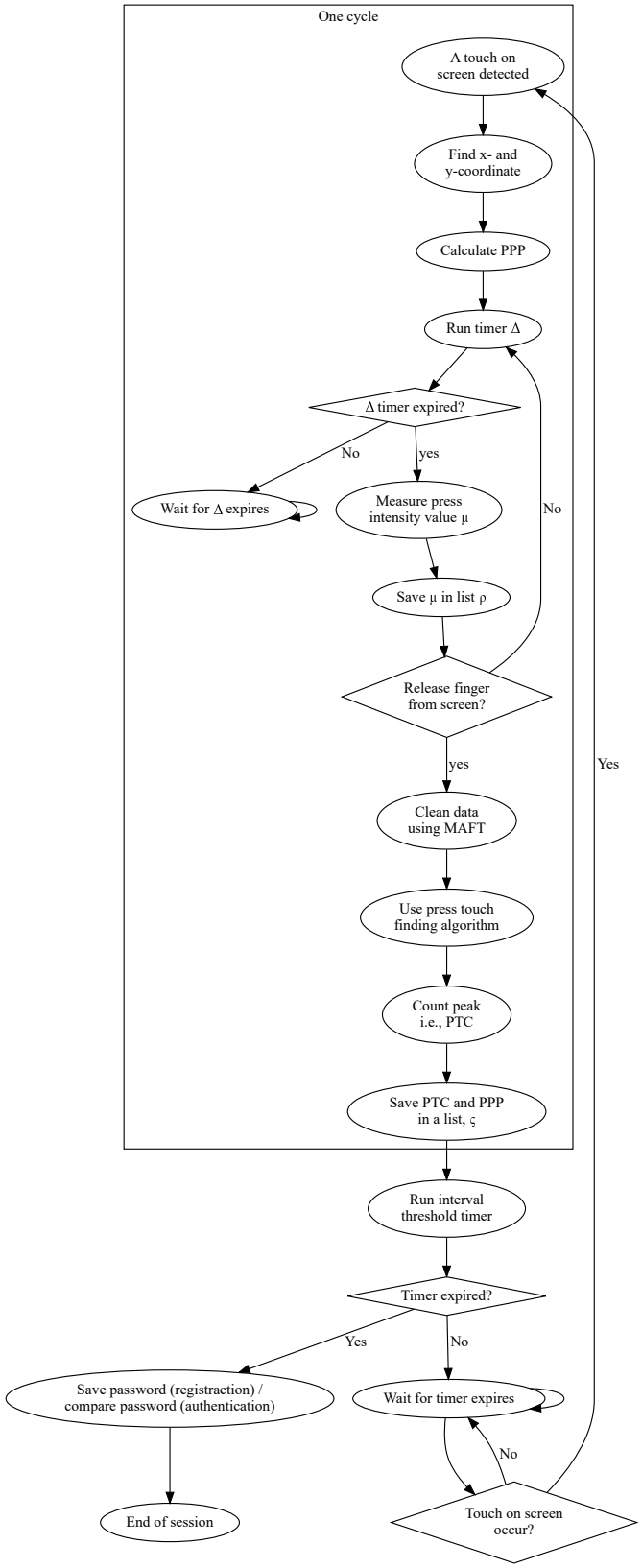

FIGURE 4: The steps that are involved in the proposed scheme.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2948977, IEEE Access

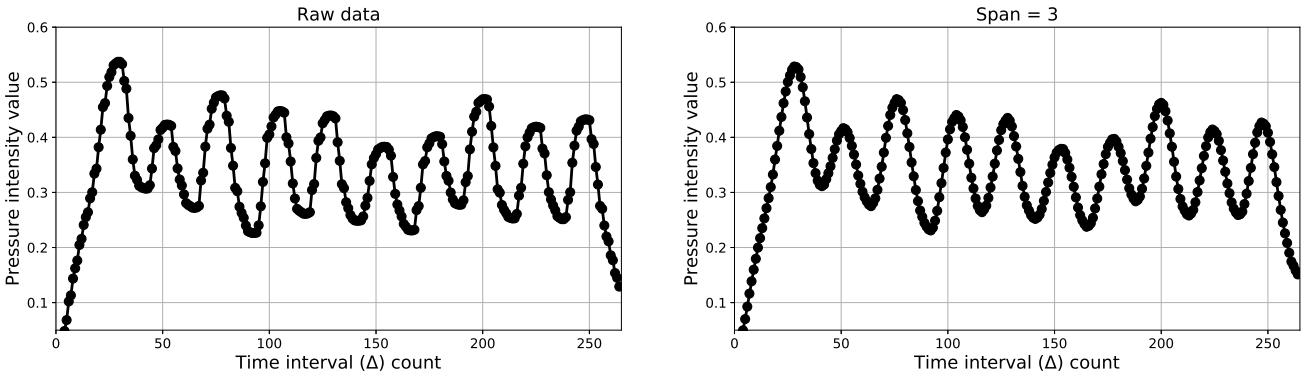

FIGURE 5: An acquired raw data and its smoothed variant for the span of 3 .

where, γ_x and γ_y are the number of pixels of a display horizontally and vertically, respectively; also known as, resolution of that display. Number of horizontal grid cells are denoted by m and number of vertical grid cells are denoted by n. Hence, $\frac{\gamma_x}{m}$ and $\frac{\gamma_y}{n}$ are the span of each cell horizontally and vertically, respectively. A user is allowed (and also suggested) to select multiple cells during a registration session following a timing constraints. According to which, the epoch of two consecutive touches must be less than a fixed time, called interval threshold. Conversely, it would be considered as the end of the registration or authentication session, which is detailed later in Section III-D.

B. PRESS TOUCH CODE

For PTC, a user needs to press on the screen forcefully without releasing the touch. Note that when a user placed his/her finger on the screen, the intensity of the touch at time t_i, μ_{t_i}, is recorded by the PSS enabled devices. It is performed in every δ time (a very short time) by the system itself. However, in the proposed technique, a system call is performed in every Δ time, where $\Delta \geq \delta$, to receive the last press value and stored it in a list, ρ. It is done in this manner since it has been observed that the consecutive μ values are not significantly different if they are acquired after every δ time interval. This process continues until the session finished event is occurred, i.e., release touch from the screen.

Once the finish event occurs, the PTC is calculated from the μ values in ρ using the procedure that is mentioned in [4]. In brief, at first, the data in ρ are cleaned using the Moving Average Filtering Technique (MAFT) technique [22]. For which, the following equation is employed :

$$\mu'_{t_i} = \frac{1}{2N+1}\left(\mu_{(t_i+N)} + \mu_{(t_i+N-1)} + ... + \mu_{(t_i-N)}\right) \tag{2}$$

where μ'_{t_i} is the press intensity value for the i-th data point after the smoothing process, N is the number of neighboring data points on either side of μ_{t_i}, and $2N+1$ is the span. It has been argued in [4] that span = 3 smoothes the data considerably enough for performing the press finding task (see Fig. 5); otherwise, it sometimes flattens the peaks and hence, makes the presses undetected.

Once the data are cleaned, the Press Touch Finding Algorithm (PTFA) or peak finding algorithm that is mentioned in [4] is employed. Note that the PTFA is a brute force technique that endeavor to discover the peaks among the cleaned μ values. The justification of employing a brute force technique here is that it is simple to implement and the number of stored press values in ρ are limited. Here, the PTFA algorithm makes a simple assumption in finding the peaks is that if any press intensity value, μ'_{t_i} is greater than its adjacent neighbors, it is a peak (see equation 3).

$$\mu'_{t_{i-1}} < \mu'_{t_i} > \mu'_{t_{i+1}} \tag{3}$$

Every time a peak is discovered, the PTC is increased by 1 which was initialized as 0 before starting the cycle. When all the peaks are discovered, it is considered as the PTC and stored in a list. For instance, in Fig. 5, since there are 10 peaks, PTC for this sequence is 10. Later, during the authentication process, the user (who registered this PTC) has to recall that value and has to provide the same number of force presses on the screen. Therefore, this scheme falls under knowledge-based authentication scheme.

C. SEAMLESS INTEGRATION

For integrating both the schemes seamlessly, the subsequent technique is introduced. As mentioned earlier in Section III-A, in PassPoints, clicks are given in several points as credentials. However, in the proposed technique, a PTC needs to be provided in every selected point instead of a click; and thus, both the schemes blend seamlessly. Since these points are not anymore click-points, let us call these Points as PTC Providing Points or PPPs, $P = \{p_1, p_2, ..., p_n\}$, where p_i is a PPP and n is the number of selected PPPs in a credential.

Once a PPP is selected, a user needs to provide the PTC of his/her choice by pressing forcefully on the screen without releasing the touch. Note that a release of the touch event is considered as the end of one cycle. The next cycle must begin

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2948977, IEEE Access

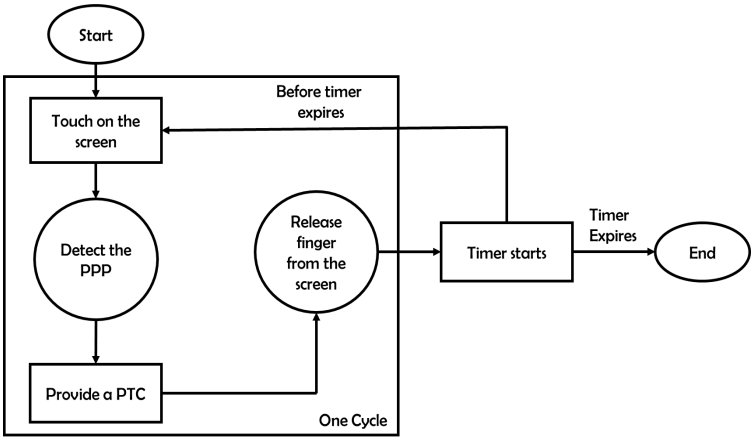

FIGURE 6: The steps for registration or authentication of the proposed scheme. Steps that comprised a cycle are enclosed within a rectangle.

before the interval threshold expires; otherwise, is considered as the end of the session. Following this procedure, a user can select a number of PPPs on the screen and can provide various PTCs in those locations.

At the end of every cycle including session ending cycle, the PTC value is calculated using the procedure that is mentioned earlier in Section III-B and stored in ζ along with their PPPs employing a $2-$tuple data structure, $< PTC, PPP >$. All the aforementioned steps of the proposed scheme are illustrated in Fig. 4. When the session end event occurs, the values in ζ are stored in the system in case of registration process or are compared with registered (or stored) values in case of authentication process, which are discussed in details in the subsequent section.

D. REGISTRATION & AUTHENTICATION

Similar to most of the password-based authentication schemes, at first, a password needs to be registered. Afterwards, that password needs to be recalled every later time during the authentication session. Note that the registration session starts immediately after a user touches on a PPP on the display with a finger and this PPP is denoted as p_0. Then the user is required to provide a PTC at the current PPP by pressing forcefully a desired number of times. Now, this concludes one cycle, such that at p_0, the user registers a PTC ϕ_0. Once such a cycle is finished, the user can release touch from the screen and can start the next cycle before interval threshold expires. Otherwise, the registration session will be terminated. For attaining resilience against the brute force attack, many similar cycles must be repeated at various PPPs $(p_1, p_2, ..., p_n)$ with various PTC values $(\phi_1, \phi_2, ..., \phi_n)$. A recommendation for suitable number of repetitions is noted in Section IV-A. All PPPs along with their respective PTC values are stored in ζ for future reference.

During the authentication session, the similar procedure is repeated in the process of recalling the registered password. Let us assume that a set of PPPs is chosen and their respective PTC are provided by the user following the similar procedure like the registration process. These pairs of data are temporarily stored in ζ'. After the end of the session, ζ' is compared with ζ, and the access to a system will be granted only when they are found identical. For that, all the PPPs and their respective PTC values in ζ' must be identical and exist in the correct sequence as in ζ. In other words, the access would be granted if and only if the following conditions are satisfied :

$$\forall(p_i, \phi_i)\,[(p_i \in \zeta \iff p_i \in \zeta') \,\&\, (\phi_i \in \zeta \iff \phi_i \in \zeta')]$$

If the above condition is not met, the authentication is deemed unsuccessful. In this case, an on-screen error message will be displayed and the user will be asked to retry for an allowed number of sessions set by a maximum threshold.

IV. EVALUATION

For finding out the performance of the proposed authentication scheme, it is implemented on the Android Operating System and is tested on a Huawei P9 Plus device — which is a PST enabled device. Note that the developed application also can be run on other Android based smart devices that satisfies the specification requirement; especially, the requirement of the PST. It should be noted that the proposed scheme can also be implemented in any other operating systems, such as the iOS, if the hardware requirements are satisfied, which has been kept out of the scope of the current work.

Generally, any authentication scheme must take three important requirements into account, namely security, functionality, and usability. In this section, we demonstrate how the proposed scheme satisfies those requirements. In addition, the proposed scheme is also compared with other relevant schemes to demonstrate its superior performance.

A. SECURITY ANALYSIS

The security of the proposed technique is analyzed with respect to its resilience against three most prominent attacks, namely shoulder surfing, brute force, and smudge as in [4].

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2948977, IEEE Access

Picture Resolution (ς)	Region Size	Password Space (log_2)								
		2	3	4	5	6	7	8	9	10
640×480	30×30	8.4	16.8	25.3	33.7	42.1	50.5	58.9	67.3	75.7
	50×50	6.9	13.9	20.8	27.8	6 34.7	41.7	48.6	55.6	62.5
	80×80	5.6	11.2	16.8	22.4	28.0	33.6	39.2	44.7	50.3
1024×768	30×30	9.8	19.5	29.3	39.1	48.9	58.6	68.4	78.2	87.9
	50×50	8.3	16.6	24.9	33.2	41.5	49.8	58.1	66.4	74.7
	80×80	6.9	13.9	20.8	27.8	34.7	41.7	48.6	55.6	62.5

TABLE 1: Password spaces of the PassPoints scheme according to various region sizes and picture resolutions.

1) Shoulder Surfing Attack :

Most locimetric schemes are unable to tackle the shoulder surfing attack; and the PassPoints is no exception. However, the proposed technique inherits a certain level of resilience against this attack due to incorporating the PTC. As demonstrated using an in-lab experiments in [4], presses are seldom recognized from a mid range distance (2 to 3 m) and hard to recognize from a long range distance ($>$ 3 m) . It also has been demonstrated that there is negligible or no defence against the shoulder surfing attack when the distance is near ($<$ 0.5 m). Note that the experiment in [4] is performed on 105 male and female participants of different demographics and all the feedbacks of the participants are noted down and analyzed later.

2) Brute Force Attack :

In the brute force attack, an attacker systematically checks all possible passwords until the correct one is found; however, it becomes infeasible when the password space is large. Therefore, the authentication schemes that offer a large password space are relatively resilient against the brute force attack than the ones with smaller password space.

In the proposed hybrid scheme, the integration of PassPoint technique ensures a large password space which is even further increased by using PTC. For instance, assuming ξ is the number of cells on the screen, which could be found as :

$$\xi = \frac{\gamma_x \times \gamma_y}{\chi_x \times \chi_y} \tag{4}$$

where, γ_x and γ_y are same as Equation 1 and χ_x and χ_y are the number of pixels of a cell horizontally and vertically, respectively. If a user selects λ number of PPPs, then a theoretical password space, τ_{loci} of the choice can be calculated as [23] :

$$\tau_{loci} = \sum_{i=1}^{\lambda} \xi^i \tag{5}$$

The password space for various picture resolutions, ς using the PassPoints scheme are noted with respect to three region sizes in Table 1.

In addition to the above password space, the proposed technique would have other password space from the PTC. If the maximum allowable PTC is ϱ_{max}, then τ_{PTC} for a single cycle can be calculated as :

$$\tau_{PTC} = \sum_{j=1}^{\varrho_{max}} j \tag{6}$$

Hence, the total password space of the proposed scheme could be found as :

$$\tau = \sum_{i=1}^{\lambda} \left(\xi \times \sum_{j=1}^{\varrho_{max}} j \right)^i \tag{7}$$

The theoretical password spaces for various λ values are stated in Table 2. As it can be seen from the table is that the password space is higher when ξ and the number of cycles are higher. For instance, the highest password space is achieved for screen resolution : 1024×768, region size : 30×30, and number of cycles : 5, which is 77.76. In the table, the number of years to break passwords for various combinations are also stated. In this case, all assumptions that are taken into account are analogous to [24]. Here, a modern computer is considered, which takes 1.7×10^{-6} seconds per password or 588235 passwords per second to break. Following this, the highest time that would require to break the password is for 1024×768 screen resolution, 30×30 region size, and 5 cycles, which is 6910797047.92 years. It is noteworthy to mention that if they would have been calculated using GPU or 3D card, the breaking time could have been reduced to 50-100 times. Conversely, if it would have been tried with a supercomputer, a password can be broken 100000 - 150000 faster than the personal computers.

3) Smudge Attack :

The smudge attack becomes possible due to oily residues or smudges that remain on the screen or on the surface of the device as a side effect of proving a password. It has been demonstrated in [6] is that it is possible to discover the password after accumulating and analyzing these oily residues for around 92% cases partially and 68% cases fully. To tackle this attack, in the proposed scheme, a user is permitted to visit the same grid cells multiple times. Again, since the number of presses is given in a single PPP for the PTC, it rules out all possibilities of breaking the password using the smudge attack.

B. FUNCTIONALITY EVALUATION

The proposed authentication scheme spends a lower time for registration and authentication with respect to several similar techniques. For instance, VAP code [2] offers the resilience against the shoulder surfing, brute force and smudge attacks; however, it spends a longer time in registration

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2948977, IEEE Access

Cycles (λ)	Screen Resolution (ς)	Region Size	Password Space (log_2)	Break Time (yr)
1	640×480	30×30	14.2	5.06e-10
		80×80	11.36	7.12e-11
	1024×768	30×30	15.55	1.3e-9
		80×80	12.72	1.82e-10
2	640×480	30×30	28.39	9.5e-6
		80×80	0.0004	1.88e-7
	1024×768	30×30	31.10	6.23e-5
		80×80	25.45	1.23e-6
3	640×480	30×30	42.59	0.18
		80×80	34.1	0.0005
	1024×768	30×30	46.65	3.0
		80×80	38.17	0.008
4	640×480	30×30	56.79	3348.12
		80×80	45.46	1.31
	1024×768	30×30	62.21	143796.0
		80×80	50.89	56.24
5	640×480	30×30	70.98	62855373.30
		80×80	56.83	3457.77
	1024×768	30×30	77.76	6910797047.92
		80×80	63.61	380098.40

TABLE 2: Password spaces and password break time in years of the proposed scheme according to various number of cycles, screen resolutions, and region sizes.

as well as in authentication. As reported in [4], it takes a duration between 4 seconds to 10 seconds for registration and authentication. Conversely, since the presses are provided without moving the finger, it takes a short time both in registration and authentication.

C. USABILITY EVALUATION

Although, a number of authentication schemes have been proposed to date; however, many of them are unable to draw user attentions due to several reasons including complicated in terms of usage and hard to remember. However, in case of the proposed technique, it can be assumed that the users would be able to remember the password easily, which is explained below with the support of adequate evidences. Among the two integrating techniques, the PassPoints employs images and as explained earlier in Section I, human being can remember images more accurately than texts. However, complicacy may arise due to the PTC. Again, the PTC is similar to remembering digits. A human being can remember 4 to 6 digits comfortably. For that reason, this range is utilized as Personal Identification Number (PIN) for authenticating an ATM card holder, which is necessary for various activities related to bank account including withdrawal and deposit of money through ATMs. In the proposed technique, even a password with 5 cycles (equivalent to 5 digits) offers a huge password space that can resist the brute force attack as could be seen in Table 2. In addition, the proposed scheme does not incorporate any complicated mechanism for authentication. It only relies on two simple mechanisms, namely selecting PPPs and giving PTCs on those locations. Hence, it can be argued that the proposed scheme is easy to remember and easy to use.

To uphold our aforementioned claims, a survey has been conducted on 25 male and female participants of various demographics. Here, we would like to mention that the survey was designed in such a way that it did not violate any regulation of the university's Ethics Review Board. Prior to the survey, a written consent has been taken from the participants, where it was mentioned that his/her usability experience would be logged. To keep the participants anonymous, only limited personal information was acquired so that later on it is possible to track back to them. Hence, we can say that all the data are anonymous data and no further treatment is required to de-identified them. The following tasks were performed while conducting the survey :

- Since the proposed scheme is a new scheme, it was introduced to the participants to make them familiar with the scheme as well as to the system. A brief demonstration of registration and authentication has been given, and other relevant aspects were also mentioned.
- Afterwards, the participants were asked to register their passwords according to the instructions stated in Section III-D.
- Later on, after a considerable amount of waiting time, they were asked to authenticate following the instructions in Section III-D. The users were given chances for three times for unsuccessful attempts. Here, it is noteworthy to mention that the participants kept patience and tried multiple times until they succeed. Therefore, we are grateful to all the participants.
- The participants were asked a number of questions after completion of the registration and the authentication session to acquire their feedbacks on the proposed scheme.

The results that are acquired from the participants are plotted in Figure 7. As it can be seen from the figure is that all 100% participants were successfully able to register and authenticate within the minimum number of attempts, which proves that this scheme is easy to use. Again, 80% of the participants were able to successfully authenticate in their first

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2019.2948977, IEEE Access

Attack(s) / `Function(s)`	Authentication Schemes						
	PIN	AN	APL	VAP	PTC	KC	P3TC
Brute Force (A)	H	L	H	M	M	M	L
Shoulder Surfing (A)	H	H	H	L	M	H	M
Smudge (A)	L	L	H	L	L	L	L
`Short Authentication Time (F)`	Y	Y	Y	N	Y	Y	Y

Legends : L – Low, M – Medium, H – High, Y – Yes, N – No, A – Attack, F – Function

TABLE 3: Comparison of the proposed technique with other similar techniques. Here, attack(s) are typed in the *italic font* and function(s) are typed in `typewriter font`.

Criterion	Cycles / Lengths	Authentication Schemes									
		PIN	AN	APL	VAP	PTC	KC	P3TC			
								640 × 480		1024 × 768	
								30 × 30	80 × 80	30 × 30	80 × 80
Password Space (log_2)	5	16.60	38.84	12.80	24.95	24.95	24.95	70.98	56.83	77.76	63.61
	8	26.58	62.14	17.10	39.81	39.81	39.81	113.57	90.93	124.42	101.78
Break Time (yr)	5	2.7e-9	0.013	1.93e-10	8.73e-7	8.73e-7	8.73e-7	62.86e+6	3457.77	68.11e+8	38.01e+4
	8	2.7e-6	13.75e+4	3.79e-9	0.03	0.03	0.03	4.16e+20	63.62e+12	7.67e+23	1.17e+17

TABLE 4: Theoretical password space of various compared schemes and their tentative break time.

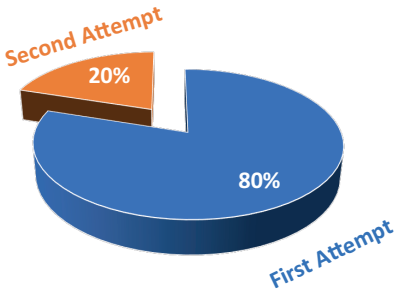

FIGURE 7: The survey results on discovering the memorability of the proposed technique.

attempt; whereas, 20% of them required two attempts, and none of them required three or more attempts to authenticate. Even though, it is a new scheme, the participants were able to authenticate with minimum number of attempts. It shows that the proposed scheme is easy to remember and easy to use.

D. COMPARISON WITH OTHER SIMILAR SCHEMES

To discover the effectiveness of the proposed scheme (PassPoints with PTC or P3TC), it is compared with other prominent similar schemes, such as Personal Identification Number (PIN) [25], Alpha Numeric (AN) [26], Android Pattern Lock (APL) [27], VAP code, PTC, and Knock Code (KC) [28]. Again, in the comparison, three prominent attacks, namely brute force, shoulder surfing, and smudge and one function, namely short authentication time are taken into account.

The performance of all the considered schemes with respect to a function as well as the aforementioned attacks are listed in Table 3. In this table, the vulnerabilities of the compared schemes for various attacks are specified with the terms : high (H), moderate (M), and low (L). On the other hand, for the function, only yes (Y) or no (N) are specified in the table to indicate its presence or absence in a scheme. Again, to support our observations for the brute force attack, we have calculated the theoretical password space and the probable break time for all the compared schemes as shown in Table 4. For PIN and AN, the prior is calculated using the equation : i^l, where i is the number of elements and l is the length. In this paper, for PIN and AN, $i = 10$ (for digits) and $i = 218$ (for extended ASCII printable characters) are taken into consideration, respectively. For the other compared techniques, they are acquired from [2] and/or [4]. Again, for the proposed scheme, it is calculated using Eq. 7. The password break time for all the compared schemes along with the proposed technique that are reported in Table 4 are computed considering the assumptions that are asserted in Section IV-A2.

As could be seen in Table 4, PIN and APL offer short password spaces requiring a very short time to break. Hence, they are highly vulnerable to the brute force attack, which is also noted in Table 3. For instance, a 5-digit PIN number offers a password space of around 16.60 in log_2 scale; whereas, in case of APL, the maximum number of combinations that can be received is 12.80 for the similar scale. For these schemes, the brute force attack would take relatively short times to break, which are — 2.7e−09 (for PIN) and 1.93e−10 (for APL) years. Conversely, VAP, PTC, and KC schemes are moderately vulnerable due to offering a considerably larger password space over PIN and APL schemes. However, AN offers a large password space when the password length is considerably long, e.g., it is 62.14 for the password length of 8. For such a password space, a brute force attack would take 13.75e+04 years to break the password; and hence, its vulnerability towards brute force attack is low. Similar to AN, since the password space of P3TC is considerably high, its resilience against the brute force attack is also high; and hence, the vulnerability is low. However, between

these duo, the P3TC attains a higher password space with considerably limited number of cycles (see Table 4). For instance, the theoretical password space of P3TC for 5 cycles are comparable to that of AN for the password length of 8.

In case of the shoulder surfing attack, as can be seen from the table that PIN, AN, APL, and KC schemes are vulnerable to the shoulder surfing attack since an attacker can attain a password by looking over the shoulder or by capturing video of the session from a certain angel or by performing other relevant tasks. However, VAP code offers a high resistance against this attack due to utilizing vibrations for authentication, which is a sense-based technique. The person, who is sensing the screen or in touch of the phone, would only be able to feel the vibrations, and hence, would be able to break the password. Among the remaining compared techniques, as mentioned in Section IV-A, PTC offers a moderate resistance against this attack. In case of the proposed technique, though the PassPoints component is vulnerable to this attack, the integration of the PTC component makes it attain moderate resistance against the attack.

Again, in case of the smudge attack, except APL, other compared techniques offer higher resilience against this attack. It can be easily tackled by allowing repetition of a certain action(s) like allowing characters to repeat multiple times (like PIN and AN) or allowing grids to visit multiple times (like VAP, PTC, and KC), and so on. However, in APL, since the visit of the grid cells are restricted, an attacker can break the password with a minimum effort.

If we analyze the compared schemes with respect to various attacks, we would find that VAP and P3TC are contending similar with equal number of L and M. VAP offers low vulnerability in case of shoulder surfing and smudge; and moderate vulnerability in case of brute force attacks. Conversely, P3TC offers low vulnerability for brute force attack and smudge attack; and moderate for shoulder surfing attack. However, P3TC wins the comparison when short authentication time function is taken into account. Except the VAP scheme, all the schemes offer short authentication time. On the other hand, in case of VAP, it takes a considerably long time due to long inter-vibration interval. Otherwise, it is difficult to distinctly identify a vibration.

V. CONCLUSION

In this paper, a new hybrid graphical authentication scheme is proposed which seamlessly combines PassPoints and PTC schemes together. Here, the former scheme increases the memorability of the scheme as well as provide a large theoretical password space. Additionally, integration of the PTC further enlarges the password space alongside assisting in defending shoulder surfing attack. Again, due to its large password space, the proposed scheme attains resilience against the brute force attack and visiting a cell multiple times helps to defend the smudge attack. For testing the proposed scheme, it is implemented on the Android operating system, and throughout this entire process, Huwawei P9 device is utilized, which is a PSS enabled device. The performance of the proposed scheme is identified with respect to security, functionality, and usability. It is also compared with other similar techniques and the proposed scheme demonstrates its superiority over those schemes.

ACKNOWLEDGEMENTS

This work has been supported in part by the FRGS project under Grant No. FRGS/1/2019/ICT04/UMP/02/1 (or RDU1901109) and by the RDU project under Grant No. RDU1703100.

Références

[1] D. Gibson, "Understanding the Three Factors of Authentication," Jun. 2011. [Online]. Available : http ://www.pearsonitcertification.com/articles/article.aspx ?p=1718488

[2] S. Azad, M. Rahman, M. S. A. N. Ranak, B. M. F. K. Ruhee, N. N. Nisa, N. Kabir et al., "Vap code : A secure graphical password for smart devices," Computers & Electrical Engineering, vol. 59, pp. 99–110, 2017.

[3] S. Kostromina and D. Gnedykh, "Students' psychological characteristics as factor of effective acquisition of visual information in e-learning," in Proc. of Procedia - Social and Behavioral Sciences, 2016, pp. 34–41.

[4] M. S. Ranak, S. Azad, N. N. H. B. M. N. Nor, and K. Z. Zamli, "Press touch code : A finger press based screen size independent authentication scheme for smart devices," PLoS ONE, vol. 12, no. 10, 2017.

[5] W. Goucher, "Look behind you : The dangers of shoulder surfing," Computer Fraud & Security, vol. 2011, no. 11, pp. 17–20, 2011.

[6] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge attacks on smartphone touch screens," in Proc. of 4th USENIX Workshop on Offensive Technologies, 2010.

[7] P. Biocco and M. Anwar, "Grid authentication : A memorability and user sentiment study," in Lecture Notes in Computer Science, vol. 11594. Springer, 2019.

[8] G. E. Blonder, "Graphical password, us patent 5559961," 1996.

[9] H. Gao, W. Jia, F. Ye, and L. Ma, "A survey on the use of graphical passwords in security." JSW, vol. 8, no. 7, pp. 1678–1698, 2013.

[10] A. H. Lashkari, R. Saleh, F. Towhidi, and S. Farmand, "A complete comparison on pure and cued recall-based graphical user authentication algorithms," in Computer and Electrical Engineering, 2009. ICCEE'09. Second International Conference on, vol. 1. IEEE, 2009, pp. 527–532.

[11] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "Passpoints : Design and longitudinal evaluation of a graphical password-system," International journal of human-computer studies, vol. 63, no. 1, pp. 102–127, 2005.

[12] "Passlogix v-go sso." [Online]. Available : https ://www.scmagazine.com/review/passlogix-v-go-sso/

[13] O. Osunade, I. A. Oloyede, and T. O. Azeez, "Graphical user authentication system resistant to shoulder surfing attack," Advances in Research, vol. 19, no. 4, 2019.

[14] J.-C. Birget, D. Hong, and N. D. Memon, "Robust discretization, with an application to graphical passwords." IACR Cryptology ePrint Archive, vol. 2003, p. 168, 2003.

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

[16] M. Nagatomo, K. Watanabe, K. Aburada, N. Okazaki, and M. Park, "Personal identification with any shift : Authentication method for smartwatches having shouldersurfing resistance," IEICE Communications Express, vol. 1, no. 6, 2019.

[17] L. Yang, Y. Zhi, T. Wei, ShuiYu, and J. Ma, "Inference attack in android activity based on program fingerprint," Journal of Network and Computer Applications, vol. 127, no. 1, 2019.

[18] M. Sreelatha, M. Shashi, M. Anirudh, M. Ahamer, and V. M. Kumar, "Authentication schemes for session passwords using color and images," International Journal of Network Security & Its Applications, vol. 3, no. 3, pp. 111âĂŞ–119, 2011.

[19] Y. Zhang, F. Monrose, and M. K. Reiter, "The security of modern password expiration : An algorithmic framework and empirical analysis," in Proc. of 17th ACM conference on Computer and communications security, 2010, pp. 176–186.

[20] I. Mackie and M. YÄśldÄśrÄśm, "A novel hybrid password authentication scheme based on text and image," in Proc. of IFIP Annual Conference on Data and Applications Security and Privacy, 2018.

[21] O. Adebola, N. Ithnin, M. Z. jali, and N. Akosu, "Graphical password schemes design : Enhancing memorability features using autobiographical memories," Journal of Theoretical and Applied Information Technology, vol. 53, no. 1, pp. 124–130, 2013.

[22] N. Ahmed and K. Rao, Orthogonal transforms for digital signal processing, 1st ed. Springer Science & Business Media, 2012, vol. 1.

[23] 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, 2013.

[24] "Calculating password complexity." [Online]. Available : https ://thycotic.force.com/support/s/article/Calculating-Password-Complexity

[25] S. J. Murdoch, R. Anderson, S. R. Drimer, and M. Bond, "Chip and pin is broken," in Proc. of IEEE Symposium on Security and Privacy, 2011.

[26] A. Nayak and R. Bansode, "Analysis of knowledge based authentication system using persuasive cued click points," in Proc. of Procedia Computer Science, 2016.

[27] R. Biddle, S. Chiasson, and P. C. V. O. PCV, "Graphical passwords : Learning from the first twelve years," ACM Computing Surveys, vol. 44, no. 4, 2012.

[28] LG Corporation, "Knock code," Korean Patent 10-1404234, 2014.