Volume: 5 Issue: IV Month of publication: April 2017

DOI: http://doi.org/10.22214/ijraset.2017.4160

Graphical Cipher Ratification System

Balika J Chelliah[1], Shreyas HM[2], Aishwarya KS[3]
[1]*Assistant Professor,* [2,3]*Student, Department of Computer Science and Engineering*
SRM University, Chennai, India

Abstract: Graphical Cipher Ratification System is a new graphical password strategy for common terminals that restores the passive digital models commonly used in graphical password systems with materialized tokens, in the form of digital images shown on device such as a smart phone. Users lay forward these images to a system and then input their password as a chain of options on live display of the token. Unique characteristics are taken from these options and used as the cipher. We lay forward three practicability studies of Graphical Cipher Ratification System exploring its authenticity, benefit, and protection against supervision. The authentication study shows that picture-characterized based passwords are noticeable and recommends necessary system attributes. Passwords should contain seven characteristics, 40% of which must analytically match the ones stored on a reliable server in order to be identical. The work completion time and error rates have to be 7.5 seconds and 9%, largely proportionate with the previous graphical password systems which use unchanging digital pictures. Lastly, the security research highlights Graphical Cipher Ratification System's resistance to inspection attack. Thus, three types of attacks such as shoulder surfing, camera-based surveillance or dictionary attacks will fail to record or notice the user's password. These results imply that Graphical Cipher Ratification System promises security while controlling the benefits of the present graphical password strategy.

Index Terms—Graphical cipher, Ratification, digital images, shoulder surfing, surveillance, dictionary attacks

I. INTRODUCTION

Protected access to data establishes present day systems and services. We preserve our interactions, financial data, official documents, and personal files secured by lending identity information and then validating to that identity. Text passwords as well as personal identification numbers (PINs) are the main authentication method [5] as they are not complex and can be set up on systems such as public terminals, or mobile devices. However, difficult passwords can be forgotten easily [13] and are also subject to security problems. This is a major issue since an average user has 25 online accounts protected with up to six contrasting passwords [12] and showing a significant memory burden. To handle this problem, individuals take up insecure coping strategies such as repetition of passwords across systems, making a note of the passwords, or simply forgetting them completely [1]. To ensure that such issues are eased, researchers are looking at them carefully while putting forward and suggesting *graphical password* schemes [3], [4] that depend on input such as picking portions of a picture. These systems have been displayed to enhance memorability without disturbing input time and error rates [16] by also maintaining great resistance to brute force as well as guessing attacks [3].

However, graphical passwords have their issues. One such issue is their sensitivity to intelligent guessing [5], [6], [23] and shoulder-surfing attacks [22]. These attacks are valid since the portions of images that are chosen by the users as password items are easy for an attacker to notice by intruding over shoulders or through camera surveillance to record input and are also comparatively predictable [20], [23]. This issue is notably ambiguous as the image details for graphical password systems are saved on ratification servers [3] and easily shown to attackers as an acknowledgement to input of readily available user identity information [19].

In accordance to this issue, we exhibit a new point-click graphical password system, *Graphical Cipher Ratification System* that expands resistance to observation attack by pairing the user's password to a picture or graphical object. This is accomplished by making use of live display of a token, such as a photograph that the user uploads or picks from the server. We state that attackers will find it difficult to capture useful photocopy of this content because of the connection among the various pictures and the redirection involved if an incorrect sequence is brought in. We demonstrate an implementation for the strategy based on image features and a demonstration of its capacity through three practicability studies covering: 1) the reliability and robustness of feature based input; 2) participant task performance times and error rates using Graphical Cipher Ratification System; and 3) the security against observation attack.

II. RELATED WORK

Graphical cipher systems are knowledge-based verification techniques that influence peoples' ability to remember and identify visual information more easily than alphanumeric information [15]. Based on studies, there are three broad types of graphical ciphers: recall-based schemes based on drawing shapes on screen, recognition-based schemes based on selecting known items from large sets of options, and cued-recall schemes based on choosing sections of already selected Images [3], [10]. Cued-recall schemes are considered as multifactor authentication, as it is associated to Graphical Cipher Ratification System and its combination of a token, or something you have, on which a password, or something you know, is entered.

A. Cued-Recall Password Schemes

Cued-recall password schemes include users picking portions on one or more pictures. A primary example is Pass Points [21]. At the time of login, users are presented with an already selected image, and they type a password by clicking on a sequence of places on the image. Verification is successful if the *XY* coordinates of these clicks are equal to a previously saved set of cipher points. A longitudinal research resulted in login times of 8.78–24.25 seconds and a failed ratification rate of 7–13%.

Cued-recall graphical passwords are subjected to certain disadvantages. For example, users typically choose *hotspots* [20], locations on an image that are largely distinct and are also predictable to hackers. In Microsoft Windows 8 graphical password system, the most common password includes an image of a person and clicking three times on the face, where one of the selection points was an eye. In this case, the cued-click points (CCP) [7] system presents a series of images and permits users to choose only a single point per image, decreasing the need to select common hotspots. Interpretation of this method led to authentication times in the range of 7–8 seconds and success rates of about 90–96%.

Another major problem with *Cued-recall* systems is observation, as password click-points can be noted by attackers after viewing a single authentication process [3]. Protecting against surveillance attack for graphical password systems is difficult. User manipulations such as decreasing text size of the mouse cursor or decreasing resolution of the image may offer some security, but have not been verified. One exception is a variant of Cued Click Points that uses eye-tracking technique [11] for input. But this created a huge impact on the performance of the system: login times increased from 47.1 to 64.3s and only 67% of the users successfully authenticated on their first attempt. Although this technique assures security, it is comparatively slow and causes errors.

B. Multifactor Authentication Schemes

Multifactor authentication [18], based on sequence of two or more separate processes, can increase security. In actual multifactor authentication schemes, physical tokens are used to generate and save personal data for user authentication. For example, mobile phones can be used as the hardware token for one-time password generation. Dodson *et al.* [9] suggested a challenge-response authentication system which involves a user snapping a picture of a QR code with a mobile device. The data from this marker generated encrypted data that were used during login. While these tools offer increased security, they are sensitive to certain dangerous types of attack, such as

Man-in-the-Middle schemes that alter messages transmitted between a user and a system [2].

Graphical Cipher Ratification System is a multifactor authentication system—both a digital token and a password are required for authentication. Graphical Cipher Ratification System differs from previous approaches in three ways. Firstly, like the CCP system, it offers a variation by not only allowing just a single point per image but also redirection of next image in the sequence if a choice proves to be incorrect. Also, any complex image or object can be used as a Graphical Cipher Ratification System token. Secondly, the two authentication factors are tightly paired, with the cipher factor taking a certain tolerance level into consideration as per user's wish. We state that this close relationship will make the technique easy to understand. Finally, we also suggest that these physical tokens will be resistant to Man-in-the-Middle schemes as attackers will face significant hurdles in terms of capturing sequences with enough detail to support successful hacks.

III. OVERVIEW

Graphical passwords are made more secure against intelligent guessing and shoulder-surfing attacks [19], [21]. We state that these weaknesses stem from the ease with which both cipher details and cipher canvases can be observed or, in the case of canvases, directly accessed from a server. Graphical cipher ratification system tackles this problem by introducing a mapping facility into the ratification process. This way, the system changes a graphical cipher, which is a single factor authentication procedure, to a more secure multifactor authentication mechanism. We prove that this makes the ratification system *Resilient-to-Internal-Observation* [5], that is, hackers cannot portray like a user by just replicating input on the authentication device or by over-hearing the interaction between the ratification device and verification system. The ratification takes place as follows. Assuming users have already created a cipher sequence, ratification is done by users identifying themselves at an appropriate terminal. For example, systems such as door locks at workplaces may accept all users are valid, while a user ID might be used on a public computer, and higher security applications, such as a bank ATM, will depend on a physical token such as an ATM card. This system could be combined into any of these schemes. Secondly, they can click on the image locations that correspond to their cipher. We argue this raises the resistance of Graphical Cipher Ratification System to attacks based on password surveillance and guessing as hackers need to have a user's access to the terminal as well as the required knowledge.

IV. IMPLEMENTATION

The prototype of the Android module is built on a 11.4-cm-wide x 20-cm-long x 0.87-cm-high Asus Nexus 7 tablet with a resolution of 1920 x 1200 pixels placed on a platform for support.

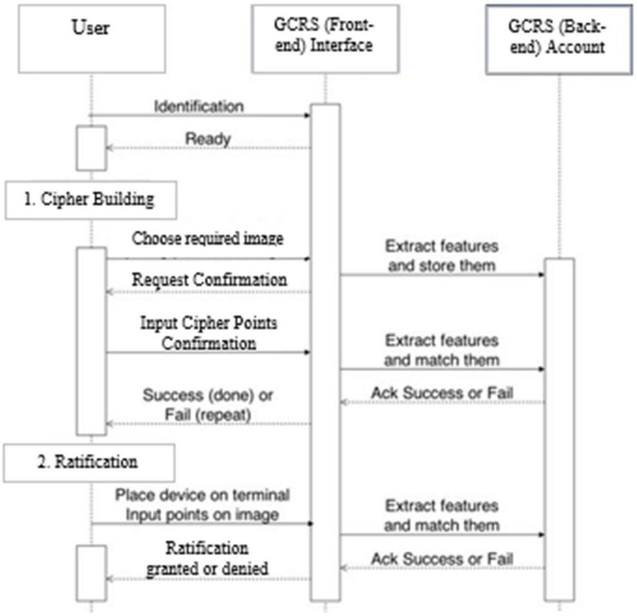
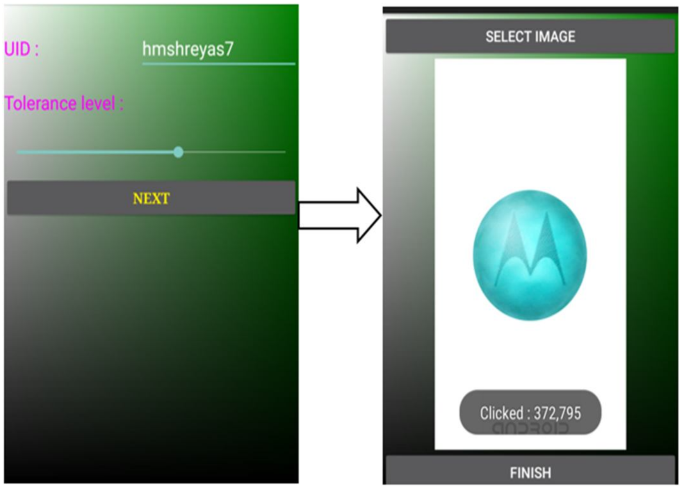

User
GCRS (Front-end) Interface
GCRS (Back-end) Account
Identification
Ready
1. Cipher Building
Choose required image
Extract features and store them
Request Confirmation
Input Cipher Points Confirmation
Extract features and match them
Ack Success or Fail
Success (done) or Fail (repeat)
2. Ratification
Place device on terminal Input points on image
Extract features and match them
Ratification granted or denied
Ack Success or Fail

Fig. 1. Sequence diagram showing the steps involved in creating a graphical cipher for the first time (1. Cipher Building) and when attempting to ratify (2. Ratification).


UID : hmshreyas7

Tolerance level :

Clicked : 372,795

Fig. 2. Overview of the Graphical Cipher Ratification System along with input selections for creating the necessary cipher sequence

The Graphical Cipher Ratification System interface and image feed are shown on the tablet that is connected to the server with the required database and mounted on the surface of the desk.

All input is made through the Nexus touchscreen. Specifically, as illustrated in in Fig. 2, users make selections by tapping the screen to visually highlight 70 x70 pixel (approximately 1.5 cm^2) portions of the displayed image and release to select it. Once an image portion is selected, it is stored as a cipher item and displayed as feedback to the user at the base of the screen, showing the chosen coordinates as a form of reference to let the user know that the click was registered correctly. Users must input a total of four items and then press a finish button in order to enter a complete cipher.

In existing graphical cipher systems [21], the ciphers are represented as the *XY* image coordinates of finger selections alone and do not take proper consideration of the tolerance levels and the image that appears next in the sequence. Some other systems attempt to take a physical image introduced by the user to make the orientation immaterial, taking the image portion itself through image processing. Although this works, manually carrying the necessary photograph or graphical object is neither convenient nor safe in certain circumstances. Maintenance of necessary images on a secure server while storing them apart and mapping them during the time of ratification, yielded very good results.

The matching phase involved reducing the Euclidean distance between the sets of points in the original and entered cipher objects. Subsequently, a threshold on the percentage of matching features was used to determine whether the entered password matched the original. Lower threshold levels result in a lenient cipher system, whereas higher levels are stricter. This process hinges on the fact that the initial image has a mapping to the user ID, the correct set of coordinates, the next image in sequence if the point is correct and the random image to be shown if incorrect. Further images are not mapped to the user ID and instead to the previous image, which would thus require infiltrating different parts of the server to gain any form of access to the overall cipher sequence.

V. EVALUATION

A. Reliability Study

This study assessed the reliability of the Graphical Cipher Ratification System in order to determine suitable thresholds for the equality of two cipher items in terms of the minimum number of image features they should possess and the percentage of image features that should match. As variations in tokens are inevitable with the Graphical Cipher Ratification System's setup, we also explored the robustness of the system in the case of repeated images with different point selections.

1) Materials: Five source images were selected based on the image categories with highest success rate in prior work [6]. They depicted people, food, tiny objects, and random text. These images were displayed on a Motorola Moto G5 Plus mobile phone with a screen resolution of 1920 x 1080 pixels and each image was preprocessed to match this screen resolution. The required points were chosen in an initial study where seven users (aged between 20 and 25 years) chose four cipher items on the selected images and processed them into the Graphical Cipher Ratification System six times. We chose distinguished points from among the selections—either those that were picked most of the time or, if there was significant variation in the areas selected, one of the items arbitrarily. An example of some of the images used in the study can be seen.

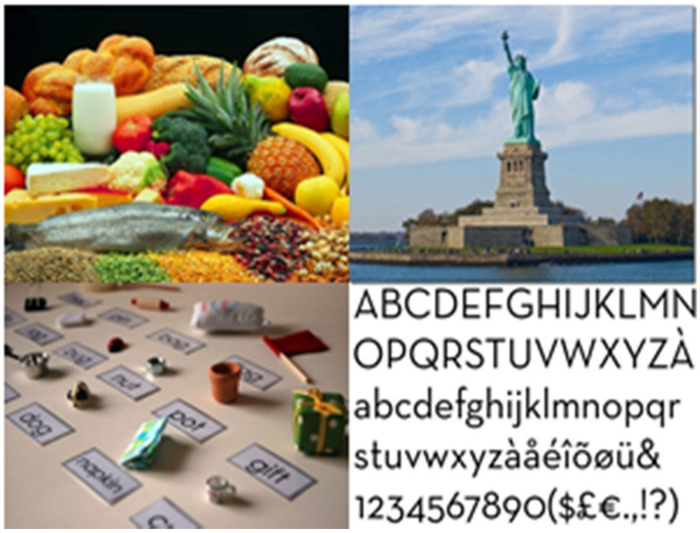


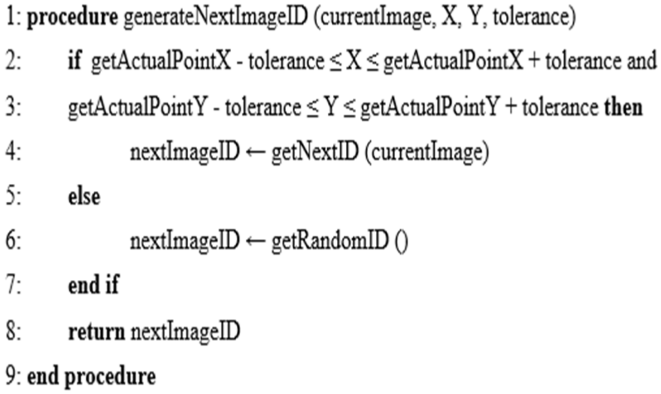
Fig. 5. Sample images used for the testing among participants, each with distinguishable features for selection of cipher sequence

The experiment involved users selecting these chosen points in order. The use of pre-defined and clearly noticeable selection points ensured the results were not affected by issues such as difficulty in remembering.

2) Participants: We recruited 20 volunteers from SRM University, Ramapuram campus. They were a mix of students and staff, aged between 20 and 35 years (Mean: 24, SD: 3.75). None were security experts or significantly enlightened in the area of security research.

3) Procedure: For each of the five chosen images, each user completed a set of 10 input trials which involved selecting the clearly noticeable points in a certain predetermined order. Each user experienced the five images in a random order, and the first trial with each image was used as a reference for matching input in the following nine trials. During each attempt, the user also tried to select multiple points for the same image, repeat images while varying points and make two identical trials to ensure consistency is preserved. In such attempts, the final point of selection would be the only one considered for any given image, the repetition of images would not lead to any confusion in the mapping process since the points chosen are independent of the previous selection, and consistency is maintained by showing that the if identical selections are made throughout, the results would be the same. For any selection, the user gets a feedback indicating the point that has been chosen to confirm the selection and give an idea of the location. Prior to being given the access to make such selections, participants needed to complete the cataloging of the user IDs that they wanted along with the preferred tolerance levels. In doing so, it was possible to verify that only a unique user ID could be picked and the violation of this would pop an error message.

In case of variations in the tolerance levels, it pointed the degrees to which the system would cooperate showing that less tolerance offered stricter validation processes and the opposite was also true. In total, this study took into account 3000 valid selection events—20 participants x5 images x10 trials x 3 selection items.



```
procedure generateNextImageID (currentImage, X, Y, tolerance)
    if getActualPointX - tolerance ≤ X ≤ getActualPointX + tolerance and
    getActualPointY - tolerance ≤ Y ≤ getActualPointY + tolerance then
        nextImageID ← getNextID (currentImage)
    else
        nextImageID ← getRandomID ()
    end if
    return nextImageID
end procedure
```

Fig. 6. Algorithm for generating the ID of the next image to be displayed to the user for continuing the ratification phase.

For each selection, we logged time, the variations in selection, and the matching distances from actual points.

4) Results: The mean completion time was 11.4s (SD: 1.3), and the average matching failure rate was 56.3% (SD: 9.2). The failure rate may seem high but it is due to the fact that when the tolerance level is kept low, a lot of attempts would lead to incorrect cipher sequences. This is why the failure rate is a bit higher than 50%, showing that a little more than half of our participants opted to try the system out with lower tolerance levels, making it harder to exactly pick the right point for the ratification process to be successful. It was also noted that people trying intentionally to pick multiple points in a particular graphical cipher object, found that only when they selected the final point, they were able to get through the ratification phase successfully. Users also experienced cases where selecting an incorrect point automatically redirected them to an image that they did not choose during cataloging. This was verified thoroughly once the users exchanged their devices with others and tested this particular aspect.

B. Usability Evaluation

The second research in this paper examines user performance with Graphical Cipher Ratification System in terms of entry times and error rates for comparison with previous graphical password system strategies. Users in this research authenticated in two conditions: a *private image* of their own choice and an image provided by the system (*public image*).

1) Participants: About 20 participants finished this study, aged between 19 and 33 years (mean 23, SD: 3.6). They were students, teachers, and professionals, chosen arbitrarily in SRM University through emails to message boards, and word of mouth. Participants considered themselves as new computer users (eight), little experienced users (ten), and advanced users (two). No participant was an expert in security research. Participants were screened to make sure all owned a mobile phone and had saved personal images in itsmemory.

2) Materials: The *public* image depicted a group of miniature objects together. To acquire images for the *private* image condition, users were asked to select a personal ratification image in advance.

They were given specific requirements: the image should be of high resolution and not to include large monochrome regions such as white walls which would make most of the areas of the image indistinguishable. Graphical cipher objects chosen by the participants included pictures of eatables (5), people (5), tourist spots (5), dolls and miniature objects (3), and text (2). All selected images met system requirements in terms of visual richness of the contents.

3) Method and Measures: All participants finished both public and private image conditions in a fully balanced design—half of them sensed the private image condition followed by the public condition and the other half *vice versa*. All sessions happened in a quiet room using the system terminal and the Asus Nexus 7 tablet mounted on it. Graphical Cipher Ratification System was configured with a tolerance level of 6 and users were briefed about the system and its mechanism. They then finished a census form followed by the two required experimental conditions. The two conditions followed the same structure. Each started with the *cataloging phase* in which the user set a four-item cipher by choosing points on the displayed graphical cipher object. If any cipher did not have a chosen point, users were not allowed to pick the next one in the required sequence.

At any point, a user could press a reset button to clear the present selection and restart without any penalty. After the four items were chosen, the user re-entered the cipher. If he or she was not able to do so, the system followed the typical practice for bank passwords and needed users to start once again and create a new cipher. After users successfully generated a cipher, they proceeded to the *ratification phase* where they verified the information that they had entered during *cataloging.*

In general, it could be seen that the use of private images boosted the chances of a cipher with greater security when the participants took turns and exchanged devices in order to see if anyone could break into another's account. There was no doubt that this would be the case since the public or sample images provided could be accessed by anyone and everyone and ultimately there would be certain points in those images that would appear to be the most likely to be picked. In the case of private or user-specific images, however, the chances of intelligently guessing the most likely spot is a lot harder as there could be something special or significant that only the user knows about if he or she chooses to pick an image with that kind of value.

These aspects were confirmed by the participants themselves when they described them by stating that the pictures of tourist spots had very few distinguishable and memorable spots, making the selection of cipher locations difficult. Many users also noted that though they found it was easier to select locations from their private images, still sometimes they are confused while selecting points with visually identical locations in their images. Finally, participants acknowledged that the selection of their private image was important and that their viewpoint towards the security and usability of the system is somewhat reflected in these choices

TABLE I
RESULTS OF THE USABILITY STUDY

	System image	User image
Median catalog time (s)	8.1 (5.4)	8.6 (2.8)
Median ratification time (s)	7.4 (2.7)	7.7 (2.2)
Cipher creation success rate	100%	100%
Successful login within 3 trials	100%	100%
Successful login at first trial	100%	83%
Successful login at second trial	–	100%
Total resets	7 / 85	8 / 92
Mean error items (in failed access)	1.8 / 4	2.2 / 4
Mean match (successful)	73.4% (6.6)	78.3% (5.4)
Mean match (fail)	26% (21.7)	12% (14.5)

Fig. 7: Various factors in comparing the usability of both system and user images

C. Security Analysis

This category contributes a security analysis of the Graphical Cipher Ratification system. We developed a threat model for this ratification system that is based on vectors, including attacks such as shoulder surfing, surveillance, dictionary attacks. We examine theft and guessing attacks theoretically and describe a study to assess flexibility to the three different types of observation.

1) Theft: While Graphical Cipher Ratification system cannot prevent theft, its close pairing of a token to a cipher does provide benefits. Unlike many kinds of ratification tokens (e.g., door entry cards), physical possession is not enough to crack the system, which means, attackers must also gain access to the cipher. This way, the system offers advantages over token based systems, including attacks such as shoulder surfing, surveillance, dictionary attacks and those based on secure device pairing over visual channels [14], [17]. There are also three advantages conferred by using a token presented on a mobile device. First, hackers must unlock the mobile device to get the token, probably facing an additional and unrelated security scheme. Second, they must recognize the precise token image. Third, users could perhaps use software to remotely erase a token from a stolen device. This paper states that the relative ease with which users would be able to hide their system password images provides a measure of protection against attacks based on token theft over and above that present in more traditional token based strategies.

2) Educated Guessing or Brute Force Attacks: From a security point of view, cued-recall graphical passwords have practical password spaces comparable to four or five digit PINs [3]. Data from the study suggest that this system has a similarly sized cipher space hinting that each Graphical Cipher Ratification System selection has a viable radius of 35 pixels (0.74cm), denoting a valid selection area of 0.55 cm^2, a figure very close to that used in benchmark systems such as the 0.53cm^2 used in PassPoints. Over a four-item PIN, this leads to a total available cipher space of ~log2 (220.4^4), a figure largely exceeding that of a four-digit numerical PIN [3].

We recognize that these figures are optimistically high and denote a theoretical maximum—in reality, only a group of the possible hotspots are likely to be selected.

We also note that in contrast with other graphical cipher schemes, this system's use of a token makes guessing attacks insufficient if used alone. They must be combined with theft or observation in order to also bring in either the user's token or a highly trustworthy copy. We argue that this increases the security of Graphical Cipher Ratification system relative to previous approaches.

3) Observation: Cued-recall graphical passwords are susceptible to surveillance attacks. A single observation can be enough to reveal a password to a passerby [21]. Reflecting the importance of this vector, a surveillance attack was staged on the Graphical Cipher Ratification system to experimentally assess the system's tolerance to this type of threat. Three types of observation were taken into consideration: shoulder-surfing, camera attack, and an attack based on malware that takes over the system terminal and records the image shown on the screen and the coordinates of the input points chosen by the user. This last attack denoted a worst case scenario. A significant and extensive man-in-the-middle attack related to using the system camera to glance not only on the cipher items entered, but also a copy of the picture they are entered on. We conducted a practical study to analyze the tolerance of Graphical Cipher Ratification system to these vectors using the system configuration inferred from the system feasibility study: ciphers comprising of four items, each with a minimum of seven distinguishable features and a tolerance above 6.

4) Security Study: A representative of our research group posed as an intelligent security conscious victim and repeatedly entered two ciphers in two different points of attack. The first involved the use of a *public* system assigned image representing a crowd of people, as in [6], while the second concerned the use of a *private* personally chosen image, in this case a bowl of fruits. We state that the public plot imitates the case of the usual cued-recall graphical passwords, where the images used for verification are stored on a server and revealed at ratification time. On the other hand, the private scenario looks at whether there is an extra security value in the system's support for personally selected and maintained user-owned pictures.

a) Participants: Three attackers finished this study, a typical size of participant pool for this type of experiment [8]. They were all graduates from SRM University mastering in computer security. None was otherwise involved with this research, and each attacked Graphical Cipher Ratification System in both public and private cases.

b) Procedure: The order of the plots was randomly assigned to each participant, and there was a 30-min interval between attempts to hack each scenario. While attempting to hack each scenario, participants performed a series of three sophisticated attacks: 1) shoulder-surfing 2) camera attack 3) malware combined with camera attack. For each type of attack, participants were asked to spend at least 10 min trying to validate and continue cracking the same scenario. If all three attempts flopped, they moved on to the next attack.

During the shoulder-surfing phase, attackers stood near the victim (within 1.5 m) during three successful ratification trials. Taking notes was encouraged. In this camera stage, attackers were given an HD video recording showing a close-up of the entire ratification mechanism, including cipher item entry and a clear picture of the device displaying the graphical object. The video was taken without visual hindrance from less than 1 m away from the user with an HDR-HC3 HDV 1080i camera. Hackers were able to use any tools they needed during the attacks. In the public image condition, they were automatically given the ratification image, while in the private condition, they were able to make use of Internet searches and any image processing tools they required to find, treat, create, or alter the source image and chosen points observed and captured during the process of attacking. In total, each participant spent about 3 hours to complete the experiment.

c) Measures: We considered the number of ciphers hacked and the relative percentage in the matching: These two measures denote how well the hackers were able to reproduce the user's choices and sequence. The higher the numbers, the firmer the attacks. We also distributed a census for the attackers to indicate on a ten-item Likert scale how tough they felt the attack was and how well they self-assessed their operation. Finally, in the next study interview, we asked them to explain their process.

d) Results: A single examination was enough for all three attackers to hack the public image password. In fact, they were able to do so fast and confidently in less than 10 seconds and with a matching percentage of 64%. In the self-reported census, the attack was proved to be easy (2.3 SD:2.3) and the hackers' performance to be convincing (8.3 SD:2.8). They stated that they entered the cipher after the shoulder-surfing attack. One attacker hinted he or she had taken notes.

With private images, the shoulder-surfing observation was totally unsuccessful. Although attackers spent between 10 and 30 min attempting to find different ways to crack it, they were unable to verify within the given trials, and none of the characteristics could be matched. Attackers proclaimed the task to be difficult (10, SD:0) and their operation to be low (3.6, SD: 4.6).

The camera attack was also ineffective, but two hackers were able to compromise a single cipher item. This attack took more time (15–45 minutes) because attackers obtained frames from the HD footage when the device was facing the camera. The attack was reported to be slightly difficult (7, SD:1.1) and performance to be relatively less (4, SD:2.5).

The malware and camera attack was the most effective—it denotes a worst-case scenario. Two hackers were able to compromise two of the cipher items. This attack took nearly the same time as the camera attack and was not considered to be easier (7.6 SD:0.5) although it concluded in modest improvements to self- reports of performance (5.2 SD:0.5).

Attacks on Graphical Cipher Ratification system took substantial time and effort and yielded a low success rate—although several items were successfully entered, no attacker managed to crack a full system cipher. This result demonstrates the increased security of the system approach against observation. It is particularly compelling as, although the attackers were partially able to hack the cipher, the threat model used in the malware attack was very generous in the type and nature of the data provided. This suggests Graphical Cipher Ratification system would exhibit a very high resistance to observation if deployed in a real-world setting.

VI. CONCLUSION

We presented three verifiable examinations of the Graphical Cipher Ratification System. In the first, we established the feasibility of using image features as cipher items in terms of their unique coordinates and the reliability with which they can be entered. In the second, we established basic user performance data while operating Graphical Cipher Ratification System: Ratification took a median of 7.7s, and although error data was unevenly distributed, mean rates were 9%. Finally, in the third study, we examined security and established that the use of an external graphical cipher object increases the tolerance to observation attack without sacrificing any security measures against other vectors such as intelligent guessing or brute force. These results compare well with earlier work such as PassPoints [21], which yielded mean ratification times of 8.78–24.25s and 1.55–2.75 failed ratification attempts prior to successfully entering a cipher. Similarly, Chiasson *et al.* [6] present a lab study of click-point-based graphical ciphers using multiple images and report a median ratification time of 7s and an error rate of 6%.

In summary, this paper proposed improving the security of graphical cipher systems by integrating live display of a graphical object that a user picks. It first demonstrates the concept by building and testing a fully operational prototype. It then shows that user performance is equivalent to that found in standard graphical cipher systems through a usability study focusing on task time, error rate, and subjective workload. Finally, a security study shows that the system significantly increases resistance to shoulder-surfing attacks in comparison to existing graphical cipher schemes [3], [11], [21]. We argue that this paper demonstrates that the Graphical Cipher Ratification System conserves the beneficial properties of graphical ciphers while increasing their security.

REFERENCES

[1] Adams and M. Sasse, "Users are not the enemy," *Commun. ACM*, vol. 42, pp. 40–46, 1999

[2] M. Adham, A. Azodi, Y. Desmedt, and I. Karaolis, "How to attack two- factor authentication internet banking," in *Proc. 17th Int.* Conf.

Financial Cryptography, 2013, pp. 322–328

[3] R. Biddle, S. Chiasson, and P. van Oorschot, "Graphical passwords: Learn- ing from the first twelve years," ACM Comput. Surveys vol. 44, no. 4, p. 19, 2012

[4] G. E. Blonder, "Graphical passwords," U.S. Patent 5 559 961, 1996.

[5] J. Bonneau, C. Herley, P. C. van Oorschot, and F. Stajano, "The quest to replace passwords: A framework for comparative evaluation of web authentication schemes," in Proc. IEEE Symp. Security Privacy, 2012, pp. 553–567

[6] S. Chiasson, R. Biddle, and P. van Oorschot, "A second look at the usability of click-based graphical passwords," in Proc. 3rd Symp. Usable Privacy Security, 2007, pp. 1–1

[7] S. Chiasson, P. C. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," in Proc. 12th Eur. Symp. Res. Comput. Security, 2007, pp. 359–37

[8] A. De Luca, E. von Zezschwitz, N. D. H. Nguyen, M. Maurer, E. Rubegni, M. P. Scipioni, and M. Langheinrich, "Back-of-device authentication on smartphones," in Proc. SIGCHI Conf. Human Factors Comput. Syst., 2013, pp. 2389–239

[9] B. Dodson, D. Sengupta, D. Boneh, and M. S. Lam, "Secure, consumer- friendly web authentication and payments with a phone," in Proc. 2nd Int. ICST Conf. Mobile Comput., Appl., Serv., 2010, pp. 17–3

[10] K. M. Everitt, T. Bragin, J. Fogarty, and T. Kohno, "A comprehensive study of frequency, interference, and training of multiple graphical passwords," in Proc. SIGCHI Conf. Human Factors Comput. Syst., 2009, pp. 889–89

[11] A. Forget, S. Chiasson, and R. Biddle, "Shoulder-surfing resistance with eye-gaze entry in cued-recall graphical passwords," in Proc. SIGCHI Conf. Human Factors Comput. Syst., 2010 pp. 1107–1110.

[12] D. Florencio and C. Herley, "A large-scale study of web password habits," in Proc. 16th Int. Conf. World Wide Web, 2007, pp. 657–666.

[13] H. Kim and J. Huh, "Pin selection policies: Are they really effective?" Comput. Security, vol. 31, no. 4, pp. 484–496, 2012.

[14] J. M. McCune, A. Perrig, and M. K. Reiter, "Seeing-is-believing: Using camera phones for human verifiable authentication," Int. J. Security Netw., vol. 4, no. 1/2, pp. 43–56, Feb. 2009.

[15] D. Nelson, V. Reed, and J. Walling, "Pictorial superiority effect," J. Exp. Psychol.: Human Learning Memory, vol. 2, no. 5, pp. 523–528, 1976. B K. Renaud and A. De Angeli, "My password is here! An investigation into visuo-spatial authentication mechanisms," Interacting Comput., vol. 16, pp. 1017–1041, 2004.

[16] N. Saxena, J. E. Ekberg, K. Kostiainen, and N. Asokan, "Secure device pairing based on a visual channel (short paper)," in Proc. IEEE Symp. Security Privacy, 2006, pp. 306–313.

[17] B. Schneier, "Two-factor authentication: Too little, too late," Commun. ACM, vol. 48, no. 4, p. 136, 2005.

[18] F. Tari, A. Ozok, and S. Holden, "A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords," in Proc. 2nd Symp. Usable Privacy Security, 2006, pp. 56–66.

[19] J. Thorpe and P. van Oorschot, "Human-seeded attacks and exploiting hot- spots in graphical passwords," in Proc. USENIX Security Symp., 2007, p. 8.

[20] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "Passpoints: Design and longitudinal evaluation of a graphical password sys- tem," Int. J. Human-Comput. Stud., vol. 63, no. 1/2, pp. 102–127, 2005.

[21] S. Wiedenbeck, J. Waters, L. Sobrado, and J. Birget, "Design and evalua- tion of a shoulder-surfing resistant graphical password scheme," in Proc. Working Conf. Adv. Visual Interfaces, 2006, pp. 177–184.

[22] Z. Zhao and G. J. Ahn, "On the security of picture gesture authentication," in Proc. 22nd USENIX Security Symp., 2013, pp. 383–398.