iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** III **Month of publication:** March 2023

DOI: https://doi.org/10.22214/ijraset.2023.49072

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue III Mar 2023- Available at www.ijraset.com

A Captcha-Based Graphical Password with Strong Password Space and Usability Study

Medha Sapkal[1], Ninaad Sarulkar[2], Kaif shaikh[3], Prathmesh Sarode[4], Prof. A.A Shirode[5]
[1, 2, 3, 4, 5]*Department of Computer Engineering, AISSMS College,RB Motilal Kennedy Rd, Near R.T.O, Railway Officers Colony, Sangamvadi, Pune, Maharashtra 411001*

Abstract: Security for authentication is required to give a superlative secure users' personal information. This paper presents a model of the Graphical password scheme under the impact of security and ease of use for user authentication. We integrate the concept of recognition with re-called and cued- recall based schemes to offer superior security compared to existing schemes. Click Symbols (CS) Alphabet combine into one entity: Alphanumeric (A) and Visual (V) symbols (CS-AV) is Captcha-based password scheme, we integrate it with recall- based n×n grid points, where a user can draw the shape or pattern by the intersection of the grid points as a way to enter a graphical password. Next scheme, the combination of CS-AV with grid cells allows very large password space (2.4 × 10^4 bits of entropy) and provides reasonable usability results by determining an empirical study of memorable password space. Proposed schemes support most applicable platform for input devices and promising strong resistance to shoulder surfing attacks on a mobile device which can be occurred during unlocking (pattern) the smartphone.

Keywords: Captcha security, Captcha-based password, User authentication, Graphical password

I. INTRODUCTION

A fundamental task of information security is the authentication of a legitimate user on the system. Text password is the most common user authentication scheme for desktop or mobile applications, but this scheme has several limitations & drawbacks [1] i.e., while a number of the passwords of per user increases, the forgetting rate of the password also rises [2]. Graphical authentication schemes are alternative of the traditional text password and it has been deeply studied [3]. Graphical password can highly motivate by the fact that humans can remember pictures better than text[3], this assumption is supported by psychological study [4, 5]. Another approach of user authentication is based on biometric traits, either physical or behavioral. These schemes based on biometric trait suffer from the problem of spoofing and need to verify the liveness of distinguish between a real user and a photo or a video [6]. The graphical password can be used as an alternative to biometric systems or aggregate with them.

The main issue of graphical password is shoulder surfing attack to capture the login credential such as during unlocking the smart phone [7], (see at [8-10]). In shoulder surfing attack, the login process can capture by direct observation or with external technical equipment (e.g. camera). Another issue of the text and the graphical password is a low entropy rate of the password space. User can create a strong password at single system, but it is difficult to remember for a long time. Recently, Zhu et al. [11] introduce the CaRP (Captcha as gRaphical Passwords) schemes. CaRP provides the clickable Captcha image and the sequence of clicks on an image is used to generate the graphical password. Most prominent of CaRP is ClickText (CT) and AnimalGrid (AG) schemes. The CT scheme corresponds to a traditional password where the alphabets drawn on a Captcha image and a user set the password by click on the sequence of alphabets. AG consists of animal models and after clicking the animal on an image, it leads to another □× □ grid-cells window wherein a user can choose grid-cells for his/her password.

We inspire from Zhu et al. [11] CaRP scheme and proposed a new password scheme using Alphanumeric (A) and Visual (V) symbols (CS-AV) (we reported it in our previous work [12]) combining with Pass-Go [13] scheme. It opposes the shoulder surfing attacks on mobile devices. We call it "Clicked on Object to Draw a Pattern (CODP)". The CODP scheme chooses an object from CS-AV image and then grid points' window is appeared where the intersection points are used to draw a pattern as like a Pass-Go scheme [13]. The intersection points are same as a pattern used in smartphone. Expected password is a combination of CS-AV objects with intersection points. Another main issue of the graphical password is a low password space. We introduce another novel scheme to overcome this issue by using CS-AV scheme combine with □× □ grid cells' window. We call it as "Click on Object to Select Secrets (COSS)". It is as like GA [11] scheme with addition a user can click on alphabets or objects to select them for password and besides it, proposed COSS scheme uses an object as graphical cue behind □× □ grid- cells to improve the usability measurement.

©IJRASET: All Rights are Reserved

Further, both schemes are based on emoji [14] sign system to measure the password strength that a user can observe and reset his password accordingly. Next, for the security analysis, the password space is measured in entropy bits for both schemes. It shows 58.6 bits and 2.4×10^4 bits of entropy of CODP and COSS schemes, respectively. In contrary, state-of-the-art schemes have shown 43 bits, 40 bits, and 271 bits for pass-points [15], CT [11], and QBP [16] schemes, respectively. The most recent, QBP scheme shows 271 bits password space, which is obtained by integrating secret questions and answers with pattern to enhance the entropy bits. While proposed COSS scheme obtain 2.4×10^4 bits of entropy which is reliable and highestcompare to these state-of-the-art schemes.
In this paper, the empirical study of security and usability of proposed schemes are conducted by following [11, 13, 16] schemes. The remaining paper is organized as followed: Related work is described in Section II. Section III shows our proposed mechanisms, and Sections IV and V explain the empirical study of usability and security issues of our schemes. Section VI concludes the discussion and conclusion.

II. RELATED WORK

A. *Graphical Password*

The graphical password schemes can be classified into three basic categories according to password structure including Recall, Cued-recall, and Recognition-based authentication, the explanation is given in [11].
Recall-based graphical password scheme demands a user to regenerate the same interaction outcome with no cueing. DAS (Draw-A-Secret) is the first recall-based scheme proposed by Jermyn et al. [17], where a user draws a password on a 2D grid. BDAS [18] adds background images into DAS scheme to encourage the user to create a more complex password. Hai Tao [13] introduces a Pass-Go scheme that generates a password and it increases the usability by using grid intersection points. Besides this, recent recall-based graphical password, e.g., Questions-Background Image- Pattern (QBP), is introduced in [16], which is integrated by adding the BDAS and Pass-Go scheme, in result it provides a strong password space. QBP [16] scheme also contains secret questions and answers which integrated with pattern to enhance the entropy bits, while this scheme may take a long time in setting of questions and answers, it's a tedious task. The cued-recall scheme provides the visual cue to a user in memorizing the graphical password. Pass-point [19] is a widely known example of the Cued-recall scheme. Recognition-based graphical password systems develop on a variety of images where a user can generate his/her password by using those certain images. Zhu at el. [11] introduce a novel approach of graphical password called as Captcha as gRaphical Password (CaRP). CaRP schemes are click-based graphical password. It uses alphanumerical characters and 2D animal's models to generate CaRP image, which is built on the Captcha technology. These visual objects appear in the CaRP image and allow a user to input the password. CaRP further sub-categorized into Recognition and Recognition-recall scheme. Recognition–based CaRP called as CT. Recognition-recall is combined tasks of both recognition and cued-recall. It contains both properties of recognition and cued-recall schemes. E.g., AG, wherein 2d animal's models on image covers the recognition part, while grid-cells window indicates cued-recall scheme. Therefore, AG provides an effective password space. However, in AG, auser has to perform an additional dragging task to set his password.

B. *Password Strength*

Password strength can be measured by password entropy [16, 20]. A mathematical definition of entropy in terms of the probability distribution function is:

$$H(x) = -\sum p(X = x) \log_2 p(X = x), \quad (1)$$

where, P(X=x) is the probability that the variable X has the value of x. The entropy is used to determine the difficulty of the password or key [20]. It can be conventionally expressed in bits. If i bits are chosen and 2i are possible values and it is said to have i bits of entropy. If n numbers of characters are chosen from the size of N alphabets in total, then the entropy

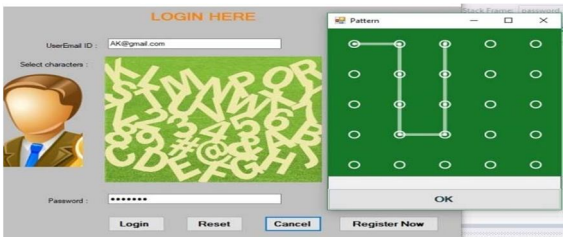


Fig 1. The interface of user authentication of CODP scheme, where English alphabet and digits (0-9) are used as visual objects in CS-AV of the password in a bit is *n*, and the possible value is 2^n. e.g.,

$N = 33$ and $n = 8$; $33^8 = 1.4 \times 10^{12}$, which is equal to $\sim 2^{42}$, which indicates 42 bits of entropy. The general representation of entropy is given by [16, 20]:

$$G = \log_2 (N^r), \quad (2)$$

where, *'N'* is possible objects, *'r'* is selected alphabets for password and *'G'* is bits of entropy.

C. *Text-Based Captcha Security*

Tang M. et al. [21], Wu X. et al. [22], and Zhang J. et al.
illustrated Captcha based security. Tang M. et al. [21] explored the summary of different Text Captchas and their recognition performance by introducing the advanced deep learning techniques in breaking Text-based Captchas, wherein the study of Captchas using large scale characters sets to identify the effect of their algorithms under Captcha attacks. The number of text-based Captchas solely focusing on being segment resistant alone is not enough to guarantee that a Captcha is secure because here may be side-channel attacks that can be used to defeat a Captcha [12, 24]. However, these algorithms only investigate Captcha segment resistant which can lead the bot to identify the Text-Captcha image but they did not conduct any empirical study to break the Captcha as a gRaphical password (CaRP) schemes.

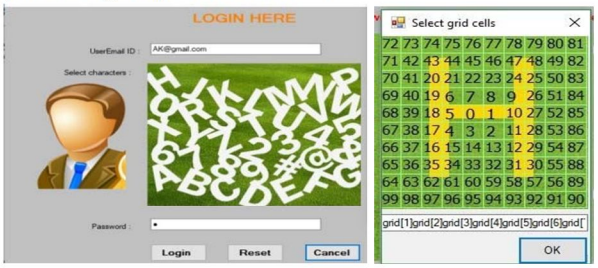
III. PROPOSED SCHEMES

The proposed graphical schemes are integration of the CaRP[11], Pass-Go [13] and BDAS [18] graphical password scheme, which is categorized into two sub-schemes:

1) Clicked on Object to Draw a Pattern (CODP)
2) Click on an Object to Select Secrets (COSS)

A. *CODP Scheme*

It is two steps graphical password scheme, demonstrated in Fig 1. In first step, the image is generated by using CS-AV algorithm [12]. The N number of alphabet symbols are mapped into the image in random sequence by utilizing the common color for each symbol in each attempt. Each symbol is rotated from 30° to -30°, zoomed from 60% to 80%, overlapped up to 3 pixels randomly. In each attempt, each row contains r number of symbols, r= □N / m □ , depending on the number of input symbols N, and m is number of rows. These symbols are mapped into the sine wave format at Captcha image, where the wave amplitude is varied (8 to 15 pixels) in each attempt. In next step, the n×n grid point's window is



(a) (b)

Fig 2. The interface of user authentication of the COSS scheme. (a) Shows the CaRP image contains 33 characters including special characters. (b) grid cells window labelled with 0 to 99, and 'H' is background cue which is selected from CaRP image.

Generated by using as Pass-Go [13] scheme (see Fig 1). It has green background and white circles indicate $n \times n$ grid points wherein a user draws the pattern or shape by connecting these points into one set. The points can be marked in 8 different directions and each point is labeled with an integer number, starting from 1 to n×n, following by row-major order. Any object of CS-AV image can be followed by $n \times n$ grid point'swindow.

B. *COSS Scheme*

COSS is the integration of CS-AV and BDAS [18] schemes, as demonstrated in Fig 2. It is also two steps authentication scheme. In first, the CS-AV scheme is used to generate the CaRP image as it described in (III-A) and in next step, we use n×n grid cells, each cell is used as a secret location and following the BDAS [18], we generate cued- recall for a user, by the object which clicked at CS-AV image is zoomed by 200% and drawn in the background of grid's cell window.

Each grid cell is a label with the number; it starts from 0 and reaches to n×n as following GA [11] scheme pattern. Assume a password, P and P="ABCH 'grid[1]', 'grid[2]',…@D". Each 'grid[.]' replaces with a set of pixels s×s, where 's×s' is the patch of grid cell pixels.

C. Password Setting

In both schemes, a user can generate the graphical password by clicking on the sequence of objects at the CaRP image and by performing a double click on any object at the Captcha image, the user can find a window with n×n grid points for CODP scheme where he/she can draw a shape as a pattern by pen up or by a mouse. Pattern might be started from any points and end with at least 4 counts. The previous points will be considered as the end point if there is no further neighbor point is selected. Each point connects with a neighbor by the straight line. User can't jump to the next point without choosing the current point. A user can reset, cancel or confirm the selected pattern. For example, a graphical password, P="ABC@p<1>p<2>p<7>p<12>p<17>p<18>p<13>p <8>p<3 >DE", with a particular sequence, the points p<·> are shown by white line in Fig 1.

Similarly, for COSS scheme, user need to follow same steps as CODP scheme, only difference is the user need to click on the grid cells instead of drowning pattern. For example, P="ABCH, 'grid[1]', 'grid[2]' 'grid[3], 'grid[4]'", where H is the character which was selected to generate the grid cells window and, e.g., 'grid [1]' is obtained by click on the position at '1' of grid cells window.

D. Registration & Authentication

1) *Registration:* A Client 'C' accesses the Authentication Server 'AS' and requests 'q' to 'AS' and 'AS' responses to 'C' in terms of image. 'C' accepts the challenge and passed it by selecting the password 'p' and reproduced the password as it did in the previous attempts. After that, the password hashed (SHA-256) H(p, salt) corresponding to 'C', 'AS' will save the password associated with client record into the system.
2) *Authentication:* A client will repeat the same password but the 'p'' password will be compared with stored hash password 'p' if both hashed values are equal, the user will successfully access the system.

IV. IMPLEMENTATION OF PROPOSED METHODS

The scheme is implemented in C#.Net, framework and run at the Windows operating system. The application is associated with the SQL server 2012 Database. The user name, ID, selected password and other associated data are saved into the database at 'AS'. For CS-AV image setting, input objects N set as 33, each object is rotated by 30° to -30° degree randomly and drawn on the grassy ground image. Each object covers individual quadratic area. The ground truth of each object is stored in a List. However, each object partially overlapped up to 3 pixels and this overlapped area, boundary, and corner of the object are marked as absent. To reduce the searching cost of click point at the image, the binary search mechanism is used, where clicked location on the image can be traced in $(\log_2 N)$ computation cost, N is number of objects on Captcha image. For the next step; in CODP scheme, the pop-up window is generated with $n \times n$, $n = 5$ grid points. Each point assigned with a number starting from 1 to 25 and stored as ground truth. User can freely drag the mouse in 8 different directions while the selects points are concatenated into an array and sequence of selected points are assigned into a graphical password, *P*. For COSS scheme, instead of grid points, it bases on $n \times n = 100$ grid cells, $n = 10$

In this setting, at first, clicked object at CS-AV image is stored and zoomed with 200% then drawn as the backgroundof the pop-up image as is shown in Fig. 2, a character 'H' with a yellow color. Each cell label with the number, starting from1 to $n \times n$ and it contains $s \times s$ image patch. For each click on a grid cell of COSS scheme will contribute an $(s \times s)$ image patch into the graphical password.

A. Password Strength

To calculate effectiveness of graphical password, the entropy bits, log (Nr) is calculated. For CODP, we use 6 minimum alphanumeric characters and 4 connected points from grid points window, the password strength can be measured as: □ = 58 (which is a combination of 33 alphanumeric characters and 25 grid points), □ = 10, then entropy from equation (2) becomes: 'G', G □ $\log_2(58^{10})$, $G = 10 \times 5.86 = 58.6$ bits.

For COSS scheme, N=133, where, 33 are alphanumeric characters and 100 are grid cells. The estimated entropy bits is: G □ $\log_2$ (13310) = 70.5 entropy bits, by using r=10. It comprises 6 alphanumeric characters and 4 grid cells. Each grid cell labelled with number, thus, it reach to 70.5 entropy bit. To overcome the graphical password space, each grid cell which is a patch of an image with a length of 20 × 20 pixels is used as part of password and for 4 grid cells, 4× 20 × 20 = 1600 pixels in total. If a user selects 4 grid cells in his/her

TABLE I. COMPARISON OF MOST RELEVANT GRAPHICAL PASSWORD SCHEMES, ACCORDING TO PASSWORD SPACE IN BITS

Schemes	DAS (5x5 grid) [17]	BDAS [18]	Passpoints [19]	Pass-Go [13]	QBP [16]	CT [11]	CA[11]	Our CODP	Our COSS
Entropy Bits	57.7	76	43	58	≤271	40	42	58.6	2.4×10^4

Password then COSS scheme password space reaches to 1600+6, where 6 is alphanumeric characters. Then □ = 33 + 100 × 20 × 20 and entropy bits can be calculated as G □ log (40,0331606) , G= 24,540 ≈ 2.45 × 104 bits which shows that COSS provides a very strong graphical password space. The comparative study with state-of-the-art schemes is reported in Table I. The proposed schemes$_2$ have strong entropy bits rate compared to DAS [17], BDAS[18], Passpoints [19], Pass-Go [13], ClickText [11], ClickAnimal(CA)[11], and same as AG [11] schemes.

B. Usability Study

It is a difficult task to assess security in a term of human guessing attacks on the graphical password, our study of the graphical password is based on the survey of proposed schemes. Therefore, for the usability study, 40 volunteers took part of the project. The age of 40 participants were among 21 to 34 and they were familiar with computer equipment's and schemes. Further, at registration phase, proposed system is established to see the password strength, proactively, by applying the emoji-based approach [14] where it shows red, yellow and green strength meter according to weak, normal and strong password respectively. However, meter setting can be tuned on the number of objects on the image, grid points, and several grid cells. We assume a password is considered as strong if it consists of 6 objects or characters, with combination of 4 grid points for CODP and 4 grid cells for COSS scheme, respectively.

1) *Entry Time:* Entry time is measured as authentication time for each participant. The participants were classified as gender and password length for CODP scheme compare for both gender; for a male, the average number of characters select as password is 6.5 and average number of points used is 9.5 whereas for female, the average number of selected objects at image is reached to 6.25, while average points used in drawing pattern is 11.5. For the COSS scheme, we analyzed the grid cells scheme with a cue and without a cue. Cue is an object which appears at back of grid cells and the average number of grid cells selected is 5.5 and without cue the average number of grid cells selected is 5.25. Additionally, time of authentication is calculated for each participant and average time (sec) is shown in Table II which indicates that CODP scheme took less time compare to COSS scheme.
2) *Success Rate:* The success rate is based on the successful login attempts of participants. A participant has a right to try three login attempts to generate the graphical password. The recall of the graphical password is divided into 3 sub-sections for verifications: 1st, 2nd, and 3rd successful attempts and remaining 4th attempt indicating that he is failed to provide the legitimate information. The result of a 4th attempt of each scheme is shown in Table III. It illustrates that CODP has maximum successful rate in first attempt, while COSS

TABLE II. PARTICIPANT'S PASSWORD CREATION TIME FORCODP AND COSS SCHEMES

Methods	Min Time (s)	Max Time (s)	Average Time (s)
CODP	18.20	34.26	27.45
COSS(without cued)	21.40	39.37	31.33
COSS(with cued)	20.23	41.53	29.38

TABLE III. PARTICIPANTS' ATTEMPTS TO ACCESS THE CODPAND COSS SCHEMES

Methods	User attempts on CODP and COSS schemes			
	1st %	2nd %	3rd %	4th /failure %
CODP	43	34	21	2
COSS(with cued)	37	35	22	6

COSS (without cued)	36	37	18	9

TABLE IV. COMPARING DIFFERENT SCHEMES BY THE EASE OFUSE

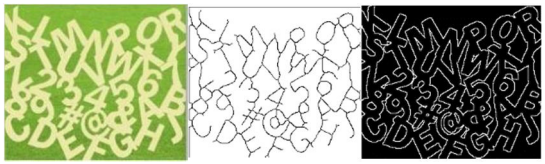
Methods	CODP (%)	COSS (%)	CODP (%)	COSS (%)
	VS. CT [11]		VS. QBP[16]	
Much easier	2.75	1.5	3.5	2.75
Easier	25	10	45	40
Same	55	65	40	35
More difficult	16	20	10	15
ificantly more difficult	1.25	3.5	1.5	7.25

(without cue) has the lowest successful rate in a first attempt but it shows maximum successful rate in a second attempt over CODP and COSS (with cue) scheme. In a third attempt, COSS (with cue) has maximum successful attempts and CODP has the lowest accepted attempts. Similarly, in 4th attempt, COSS (without cue) has maximum failure rate (9%) while CODP scheme has the lowest failure rate (2%).

3) Survey: A survey with 32 participants (discussed in Section IV-B), who was willing to join this section to measure the ease of use of the proposed schemes over existing password schemes. Each participant was to answer the following questions: the proposed schemes are 'much easier' 'easier', 'same', 'more difficult', and 'significantly more difficult" to use than CT [11] and QBP [16] schemes. In Table IV, distributions of the number of answers on respective questions in percent are presented. These results proves that proposed methods have similar difficulty level compare to existing approaches with strong password space.

V. SECURITY ANALYSIS & ATTACKS

There is no comprehensive segmentation solution that can be applied to segment and recognize the individual object on Captcha image with a 100% success rate to date [25]. Fig. 3



(a) Original image (b) Skeleton image (c) Edge detection

Fig 3. Image processing application on CaRP image. (a) CaRP imagecontains alphabets used in CT [14] scheme, (b) Image after skeleton process, (c) indicates edge detection process.

Determines the typical image processing techniques which may use to break or facilitates to break the Captcha images. The CS-AV image is shown in Fig. 3(a). Fig. 3(b) shows the image's skeleton. Skeletonization is a process that is used to thin a shape of image object while preserving the general structure. Since, skeleton thin characters into a single pixel thickness which may be used to identify the geometry of the character. Hence, this information is used to identify the characters. Overlapping the characters with horizontal and vertical neighbor, skeleton scheme does not respond with useful information. For highlight the outlines of overlapping characters, edge detection filters [26, 27] is applied on CS-AV image, but it does not facilitate the task of segmenting the characters. However, the recent research of using deep learning techniques, Tang M. [21] and Gao H. [28] explored widely the Text-Based Captcha attacks and reported the high level of Captcha break results, where the success rate achieved by their attack of the single and two-layer Microsoft Captcha is 50.9% and 65.8% respectively. Gao H. [28] reports success rate was 44.6% of Captcha attack on Microsoft Captcha using Convolutional Neural Networks (CNN). It shows that text- Captcha can be successfully recovered within reliable time. If [21, 28] schemes succeed to break the CaRP Text image, it still needs to facilitate the system to perform the click on it to generate the graphical password, and again a sequence of clicks with a combination of the recall scheme will be significantly difficult for a bot to generate the complete graphical password.

We did a theoretical study on the graphical password. Assume that bot can break Captcha image with a very high success rate, then bot has two choices: 'the password known by a bot' and 'the password unknown by a bot'. In the first situation, the bot must recognize the correct objects and their locations and then place sequence of clicks on them to generate the password. In this scenario, first a bot needs high success rate of objects segmentation which facilitates it to find the characters on CaRP image. Next, to know the password, a bot need the password cracker. Thus, a password cracker is applied to the database associated with participants whom use the CT [11], CODP and COSS scheme, by using a popular password-cracking tool: 'John the Ripper version 1.7.9' [29]. John the Ripper has three operation modes: "Single crack", "wordlist", and "incremental". In our study, the default setting is used of John the Ripper and taking wordlist "password.lst" from [30], which was used in the "wordlist" modes. Operating in "single crack", "wordlist", and "incremental" modes for 24 hours for each scheme, John the Ripper did not find any password of CT[11], CS-AV[12], CODP and COSS schemes. This experiment was conducted using SAMSUNG (Core i5, 2.53 GHz, RAM 4 GB) portable laptop. Thus, this study illustrates that to know the password by a bot is a significantly complex task by using cracker tools. In the second scenario, 'the password unknown by a bot', means bot knows the CaRP image, but it does not has any knowledge of a password string.

Thus, the bot can apply brute force attack by setting all thepossibilities onto the system which is an NP-hard problem.

1) *Shoulder Surfing Attacks*: Shoulder surfing attacks occur when a graphical password is generated in public places or it may observe with technical equipment [9, 10]. Our CODP scheme can defeat in term of varying the location of characters in Captcha image in each attempt and a new challenge will occur which character is selected to process the next window for drawing the pattern and the grid points will not lead by the correct characters for the new image anymore.
2) *Relay attacks and Captcha breaker*: Relay attacks may be executed in different possible ways. Captcha challenge can be relayed to continue the surfing website where the human is hired to solve the Captcha challenges for small payments. For our scheme instead of human, we apply the recent version of Captcha breakers 'GSA and CaptchaSniper" [26, 27] which break simple Captcha containing 6 to 8 characters with very high success rate. GSA Captcha effortlessly analyses and solves the Captcha image. Hence, to identify the characters on the CODP and COSS Captcha images, both GSA and Captcha Sniper programs are applied. The experiments are conducted for 24 hours on several images under the following image processing filters: color detection, auto threshold, scaling, blur effects, sharpening, mask, auto brightness, set contrast, normalize, Skelton, median, remove-objects, and several other filters are automatically applied. Consequently, both software recognize 3.25% characters only, but did not recognize all set of character at any image.

VI. DISCUSSION & CONCLUSION

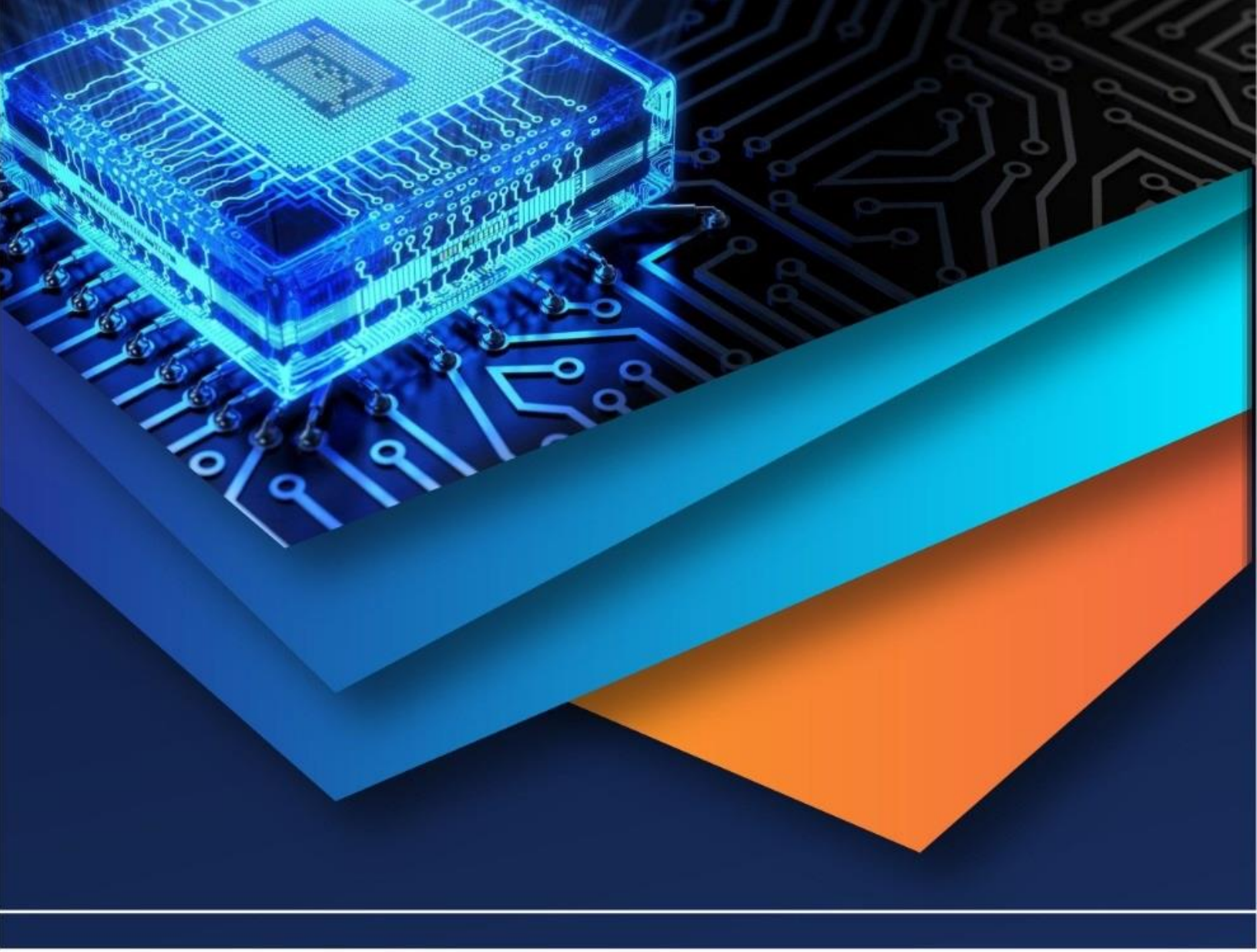
This paper introduces two new graphical passwords schemes: CODP and COSS schemes which can overcome the shoulder surfing attacks, such as unlock the smartphone's pattern and provides a strong password space. The proposed method, CODP and COSS scheme generates 58.5 and 2.45 × 104 entropy bits password space, respectively, while state-of- the-art methods CT [11], CA [11], and QBP [16] entropy bits approach to 40, 42, and 271, respectively. The proposed method shows strongest entropy bits compare to the QBP scheme by obtaining 2.45 × 104 entropy bits. It is because of set of pixels are integrated with alphabets. In contrary, QBP scheme allows to generate 271 bits strong password by using set of questions and answers as part of password which looks a tedious task. In security study, we found that our schemes can be under attack by deep learning techniques which has been only investigated on 2-layers Captcha challenges and it needs a pixel-level labelling to learn the model of Captcha scheme. Nevertheless, it did not investigate the CaRP image particularly.

The future work is to investigate a comprehensive study of CaRP image segmentation or objects recognition on CaRP image and next is to combine the proposed scheme with biometrics systems to enhance the security of spoofing attacks.

REFERENCES

[1] H. Yuan, Y. Han, and J. Hu, "Password memorability and security : empirical results," Int. Comput. Sci. Softw. Eng. Conf. Vol. 4, pp. 25– 31, 2008.
[2] D. R. Pilar, A. Jaeger, C. F. A. Gomes, and L. M. Stein, "Passwords usage and human memory limitations: a survey across age and educational background," PLoS One, vol. 7, no. 12, 2012.
[3] P. Elftmann, "Secure alternatives to authentication mechanisms submitted by," Aachen Univ. Aachen, Ger. Thesis, October 2006, pp. 1–92.
[4] L. Standing, J. Conezio, and R. N. Haber, "Perception and memory for pictures: Single-trial learning of 2500 visual stimuli," Psychon. Sci., vol. 19, no. 2, pp. 73–74, Aug. 1970.
[5] R. N. Shepard, "Recognition memory for words, sentences, and pictures," J. Verbal Learning Verbal Behav., vol. 6, no. 1, pp. 156–163, 1967.
[6] D. C. Garcia and R. L. de Queiroz, "Face-Spoofing 2D-Detection Based on Moiré-Pattern Analysis," in IEEE Transactions on Information Forensics and Security, vol. 10, no. 4, pp. 778-786, April 2015.

[7] F. Schaub, R. Deyhle, and M. Weber, "Password entry usability and shoulder surfing susceptibility on different smartphone platforms," Proc. 11th Int. Conf. Mob. Ubiquitous Multimed. - MUM '12, pp. 1-10,2012.
[8] R. Biddle, S. Chiasson, and P. C. Van Oorschot, "Graphical Passwords: Learning from the first twelve years," ACM Comput. Surv., vol. 44, no.4, p. 41, 2012.
[9] G. Ye et al., "Cracking android pattern lock in five attempts," Proc. 2017Netw. Distrib. Syst. Secur. Symp., no. March, 2017.
[10] V. Venkateswara Rao and A. S. N. Chakravarthy, "Analysis and bypassing of pattern lock in android smartphone," IEEE Int. Conf. Comput. Intell. Comput. Res. ICCIC, pp. 1–3, 2017.
[11] B. B. Zhu, J. Yan, Guanbo Bao, Maowei Yang, and Ning Xu, "Captcha as graphical passwords: a new security primitive based on hard AI problems," IEEE Trans. Inf. Forensics Secur., vol. 9, no. 6, pp. 891–904,2014.
[12] A. Khan, &A. G. Chefranov, "A new secure and usable captcha-based graphical password scheme," In International Symposium on Computer and Information Sciences, Springer, Cham., September, 2018, pp. 150- 157.
[13] H. Tao and C. Adams, "Pass-Go: A proposal to improve the usability ofgraphical passwords," Int. J. Netw. Secur., vol. 7, no. 2, pp. 273–292, 2008.
[14] S. Furnell, W. Khern-am-nuai, R. Esmael, W. Yang, and N. Li, "Enhancing security behaviour by supporting the user," Comput. Secur.,vol. 75, pp. 1–9, 2018.
[15] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system," Int. J. Hum. Comput. Stud., vol. 63, no. 1–2, pp. 102–127, 2005.
[16] B. Togookhuu and J. Zhang, "New graphic password scheme containing questions-background-pattern and implementation," Procedia Comput. Sci., vol. 107, pp. 148–156, 2017.
[17] A. D. Jermyn, I., Mayer, A. J., Monrose, F., Reiter, M. K., & Rubin, "The design and analysis of graphical passwords," Proc. 8th USENIX Secur. Symp. Washingt. D.C. USA, August 23-26, pp. 23–26, 1999.
[18] P. Dunphy and J. Yan, "Do background images improve 'draw a secret' graphical passwords?," Proc. 14th ACM Conf. Comput. Commun. Secur. - CCS '07, pp. 36-47, October 2007.
[19] S. Chiasson, P. C. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," pp. 359–374, 2007.
[20] W. E. Burr, D. F. Dodson, and W. T. Polk, "Electionic authentication guidelines," 800-63 Ver. 1.0 (Withdrawn), June 30, 2004.
[21] M. Tang, H. Gao, Y. Zhang, Y. Liu, P. Zhang, and P. Wang, "Research on deep learning techniques in breaking text-based captchas and designing image-based captcha," IEEE Trans. Inf. Forensics Secur., vol. 13, no. 10, pp. 2522–2537, 2018.
[22] X. Wu, S. Dai, Y. Guo, & H. Fujita, "A machine learning attack against variable-length chinese character captchas," Applied Intelligence, vol. 49, no. 4, pp 1548-1565, 2019.
[23] J. Zhang, X. Hei, & Z. Wang, "Typer vs. captcha: private information based captcha to defend against crowdsourcing human cheating," arXiv preprint arXiv:1904.12542, 2019.
[24] Y. W. Chow, W. Susilo, & P. Thorncharoensri, "Captcha design and security issues," In Advances in Cyber Security: Principles, Techniques, and Applications, Springer, Singapore, pp. 69-92, 2019.
[25] V. D. Nguyen, Y. W. Chow, and W. Susilo, "A captcha scheme based on the identification of character locations," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics),vol. 8434 LNCS, pp. 60–74, 2014.
[26] German Software development and Analytics, "GSA captcha breaker,"2018, https://www.gsa-online.de/en/, accessed 10 October 2018.
[27] Captcha-Sniper, "Captcha sniper," 2018, http://www.captchasniper. com/, accessed 10 October 2018.
[28] H. Gao, M. Tang, Y. Liu, P. Zhang, and X. Liu, "Research on the security of microsoft's two-layer captcha," IEEE Trans. Inf. Forensics Secur., vol. 12, no. 7, pp. 1671–1685, 2017.
[29] John the Ripper Password Cracker, "http://www.openwall.com/john/," accessed 2 January 2019.
[30] Openwall Wordlists Collection, "http://www.openwall.com/wordlists/," accessed 2 January 2019.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)