Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 12, No. 2, (2021),
ISSN : **1906-9685**

GRAPHICAL PASSWORDS AS CAPTCHA: ANOTHER SECURITY MEASURE BASED ON HARD AI PROBLEMS

[#1]**Mrs.VUMMENTHALA MAMATHA,** *Assistant Professor*
[#2]**Mr.VANGAPALLI RAVITEJA,** *Assistant Professor*
Department of Computer Science and Engineering,
SREE CHAITANYA INSTITUTE OF TECHNOLOGICAL SCIENCES, KARIMNAGAR, TS.

ABSTRACT: Many security primitives are based on hard mathematical problems. Using hard AI problems for security is emerging as an exciting new paradigm, buthas been under-explored. In this paper, we present a new security primitive based on hard AI problems, namely, a novel family of graphical password systems built on top of Captcha technology, which we call Captcha as graphical passwords (CaRP). CaRP is both a Captcha and a graphical password scheme. CaRP addresses a number of securityproblems altogether, such as online guessing attacks, relay attacks, and, if combined with dual-view technologies, shoulder-surfing attacks. Notably, a CaRP password can be found only probabilistically by automatic online guessing attacks even if the password is in the search set. CaRP also offers a novel approach to address the well-known image hotspot problem in popular graphical password systems, such as Pass Points, that often leads to weak password choices. CaRP is not a panacea, but it offers reasonable security and usability and appears to fit well with some practical applications for improving online security.

Keywords: CaRp, captcha

---

1. INTRODUCTION

One of the key goals in the realm of security is the development of cryptographic primitives based on computationally tough and complex mathematical problems. The integer factorization problem is prioritized by both the RSA public-key cryptosystem and the Rabin encryption. Numerous cryptographic systems, including elliptic curve cryptography, Diffie-Hellman key exchange, and ElGamal encryption, rely on the discrete logarithm problem. The use of tough artificial intelligence (AI) tasks for security, as proposed in the aforementioned literature, is an exciting and creative paradigm. One of the most famous breakthroughs within this paradigm is Captcha, a utility used to discriminate between human and machine users. This is accomplished by giving a job, usually in the form of a conundrum, that is difficult for computers to answer yet simple for people. Captcha has become a typical Internet security tool for preventing automated bots from accessing online email and other services.

Captcha as graphical passwords

A New Way to Thwart Guessing Attacks

A password that is examined and determined to be incorrect after a failed attempt is identified as an incorrect guess and is barred from use in further tries in the event of a guessing attack. The probability of accurately predicting an unknown password drops as the number of attempts grows, increasing the likelihood of uncovering the true password. Let S represent the collection of password approximations made before to each trial, P represent the password being searched, T represent a trial, Tn represent the next trial, and p(T =) indicate the likelihood that will be attempted in trial T. Let En represent the set of password approximations that have been tried over all trials, including the current one (Tn). The password for the nth try (Tn) is chosen from a supplied collection.

S. If $\rho \in S$, then we have

$$p(T = \rho | T_1 = \rho, \ldots, T_{n-1} = \rho) > p(T = \rho), (1)$$

and $E_n \to S$ with $n \to |S|$. (2)

$$p(T = \rho | T_1 = \rho, \ldots, T_{n-1} = \rho) \to 1 \ |$$

where |S| denotes the set S's cardinality. according to the equation. If the password is in the set S, it will always be found within the first |S| attempts. If the password is not found in set S, the set will be thoroughly checked after |S| attempts. The hypothesised password is reviewed in each iteration of the experiment to discover if it is, in fact, the correct password. Each cycle produces consistent results. To defend against automated guessing attacks, Countermeasure against Randomized Passwords (CaRP) employs a novel method. The goal of this project is to answer the following mathematical equation:

$$p(T = \rho | T1, \ldots, Tn-1) = p(T = \rho), \quad \forall n \ (3)$$

An automatic guesswork attack is observed in relation to a computational security concern. the equation. Each trial is computationally distinct from the others, as indicated by the notation (3). The number of prior trials has no effect on the probability of discovering the password in the current trial.

CaRP: An Overview

It is proved in the context of CaRP that a unique image is generated for each authentication attempt, regardless of whether it is made by the same user. To construct a CaRP image, the CaRP approach employs a range of visual components, including alphabetic characters and visually related animals. This graphic represents a Captcha challenge. CaRP images are distinct from Captcha images in that they must include every visible letter of the alphabet in order for users to enter any password. Captcha photos, on the other hand, do not require this. Several Captcha approaches, as listed below, can be transformed into CaRP systems.

Converting Captcha to CaRP

Any visual Captcha system that relies on the recognition of a large number of specific item categories can theoretically be transformed into a CaRP. All text-based Captcha approaches and the great majority of IRCs meet this condition. IRC systems that rely on a single, predetermined category of objects can be expanded to encompass a greater variety of objects, transforming them into more complete CaRPs. In fact, converting a specific Captcha scheme to a CaRP scheme usually necessitates a case-by-case examination.

User Authentication With CaRP Schemes

CaRP schemes, like previous graphical passwords, are assumed to be used in conjunction with additional security measures, such as the establishment of secure channels between clients and the authentication server using Transport Layer Security (TLS). In terms of user authentication, the following is a typical way for implementing CaRP systems. With each user ID, the authentication server, also known as AS, keeps a salt value, denoted by s, and a hash value, denoted by H(, s). It is critical to remember that, as stated by the asterisk, the server does not retain the account's password. A CaRP password is a collection of visual item IDs or interactive locations connected with visual objects that the user has chosen. The Authentication System (AS) generates a Captcha Recognition Protocol (CaRP) image in response to a login request, records the spatial information of the objects in the image, and then transmits the image to the user for password verification by clicking. The coordinates of the chosen sites are recorded and sent to AS.

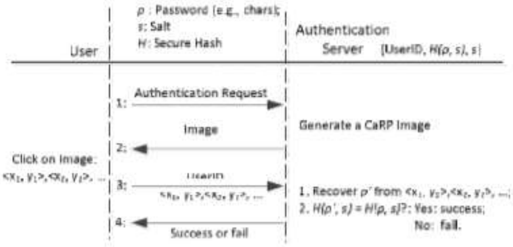


Fig. 1. A flowchart depicting the basic stages of the CaRP authentication process..

The user identity (ID) is necessary for authentication. As is in charge of mapping the coordinates gained onto the CaRP picture. The sites where the user clicked on the image are assigned a sequence of visual object IDs, or interactive points of visual objects, by AS. These IDs are associated with the areas where the user clicked. AS computes the hash value of _ using the account's salt and then compares the result to the previously stored hash value of the account. The authentication operation is regarded successful when it is discovered that the two hash values are equal. The preceding procedure, represented in Figure 1, is known as the basic CaRP authentication. The text of the user is already academic in nature.

2. RECOGNITION-BASED CaRP

A password is defined in this CaRP as a

collection of visual components that fit within an alphabetic framework. Conventional recognition-based graphical passwords suggest that CaRP can access a wide range of visual items. This paper shows two recognition-based Context-aware Role-based Access Control (CaRP) systems, followed by a third variation.

Click Text

Click Text is a text-based Captcha-based Computer-Aided Random Pattern (CaRP) recognition system. Visually complex characters are not included in the alphabet. For example, the presence of the letter O and the digit 0 in the same CaRP image may generate confusion and necessitate the removal of one of these symbols from the alphabet. A Click Text password is a series of alphanumeric characters, such as = AB#9CD87. The authentication server uses the ground truth to determine the characters associated with the user's clicked points. In the context of Click Text pictures, characters can be arranged randomly.

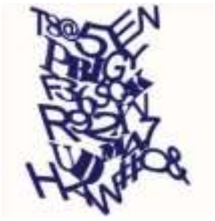


Fig.2. a written representation with a 33-character clickable graphic in addition to it.

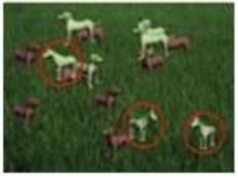
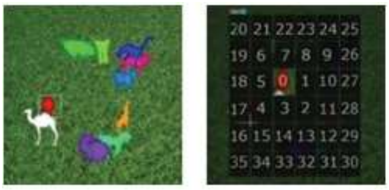


Fig.3. Equine specimens, primarily horses, are on display at the Captcha Zoo and are easily identifiable by their red surroundings..



20	21	22	23	24	25
19	6	7	8	9	26
18	5	0	1	10	27
17	4	3	2	11	28
16	15	14	13	12	29
35	34	33	32	31	30

Image 4. The Click Animal image, which is a picture of an animal, is displayed on the left side of the screen. The red turkey's bounding rectangle acts as the boundary for the 6 by 6 grid on the right side. That is, two-dimensional space. In contrast, text-based Captcha challenges require characters to be typed sequentially and are often sorted from left to right. The figure. Figure 2 depicts an image of the 33-letter Click Text alphabet. When entering a password, the user selects the image that matches to each character in their password in the same sequential order, such as A.

B, #, 9, C, D, 8, and then 7 for password ρ= AB#9CD87.

Click Animal

Captcha technology is used by the Captcha Zoo to generate two-dimensional images of animals from three-dimensional models of horses and dogs. These images are set against a visually appealing background and include a variety of textures, colors, lighting, and places. The user successfully interacts with each horse in the challenge image by clicking on it, proving that they are capable of passing the test. Figure. It is clear that all of the horses in the example are surrounded by the color red.

Animal Grid

The amount of similar fauna is significantly lesser when compared to the abundance of traits that can be observed. The Click Animal interface features a smaller alphabet than the Click Text interface, resulting in a smaller password field. To properly repel human guessing attempts, the CaRP system must have a large password space. The password space for Animal Grid can be extended by combining it with a grid-based graphical password system, where the grid's dimensions depend on the size of the selected animal.

Before entering a password, a Click Animal image appears. After selecting an animal, a picture of a grid with n × n dimensions is displayed. The size of each grid cell correspond to the bounding rectangle enclosing the chosen animal. A label is assigned to each grid-cell to guide users in their identification process. The figure. Figure 4's 6 x 6 grid reveals the presence of a red turkey in the left image. The number chosen was four.

After identifying the bounding rectangle of the chosen animal, an image is generated and shown. In this image, each grid cell corresponds to the size of the detected bounding rectangle, resulting in a nn grid. If the grid image exceeds or falls short of the user's seeing capability, it is proportionally changed to an appropriate size. The user then selects a sequence of grid cells ranging from zero to many that correspond to the grid cells after the first animal in her password. The user then returns to the Click Animal image. In the above scenario, the user selects a point within grid-cell_2_ before selecting a point within grid-cell_1_.

A grid cell pair. The recorded data is made up of the user-selected locations on the grid picture's coordinates, which are obtained from the original image without the use of any scale procedures. The preceding procedure is continued until the user has

3. RECOGNITION-RECALL CaRP

In the context of recognition-recall CaRP, a password is defined as a collection of invariant points derived from objects. An object, such as the letter A, has an invariant point, which is a specific point that has a constant relative positioning across several manifestations of the item, such as different typefaces. This feature allows humans to correctly identify and distinguish the object regardless of how it appears in computer-aided identification and processing (CaRP) images. The next section describes Text Point, a CaRP technique for recognition and recall that use a character alphabet. Following that is a variation designed for challenge-response authentication.

Text Points

Characters' points are unchangeable. Figure. The letter A has five distinct invariant points that can be used as reliable recognition and memory signals. An item's internal point is defined as a position that is further from the entity's nearest boundary than a predetermined limit. When selecting clickable points, the distance between any two clickable points within a character must be more than a predetermined threshold. This is critical in order to clearly identify the clickable locations and avoid overlapping tolerance regions on CaRP images. It is also critical to evaluate variation. For example, if the focal point of a stroke segment within one character has already been determined, it is advisable to avoid selecting the focal point of a comparable stroke segment within another character. As an alternative, it is prudent to choose

Text Points 4CR

During the authentication procedure in the exposed CaRP systems, the coordinates of user-clicked locations are immediately provided to the authentication server. In the event of complicated protocols, such as a challenge-response authentication protocol, the authentication server receives a response. Points can be changed to adhere to challenge-response authentication. This variant is referred to as

Image Generation.

The topic under consideration is picture production. The process for creating a TextPoints4CR image is the same as for creating a Text Points image. The aforementioned procedure is then utilized to ensure that each clickable point is put at least as far away from the grid-cell boundaries as possible. The graphic comprises every clickable region, which is marked by the symbol set _. The distance between each location inside the context of _ is computed.

Authentication.

Authentication. When the user enters a password, the selected point is replaced with the appropriate grid cell. If the click errors are within the range of, it can be presumed that each point the user clicks will correspond to the same grid-cell as the initial password point. As a result, the grid cell sequence generated from user-selected points is the same as the sequence generated by the authentication server using the previously saved password for the account. The aforementioned sequence is the shared secret utilized by both parties in a challenge-response authentication technique.

4. SECURITY ANALYSIS

Security of Underlying Captcha

The challenge of computational intractability in the recognition of objects in CaRP images is a basic component of the CaRP framework. Prior studies on Captcha security were largely case studies of single individuals or employed an approximative methodology. There is no theoretical security paradigm in place yet. Object segmentation is widely recognised as a computationally difficult and combinatorially complex task in modern text Captcha algorithms. The size N of the Captcha alphabet and the relationship between the complexity of object segmentation, denoted as C, and the number M of items in a challenge are both polynomial and exponential, respectively. This relationship is theoretically represented as $C = MP(N)$, where $P()$ is a polynomial function with a parameter greater than one. A CaRP image is typically 30P(N)/(10P(N)), which is approximately 20 times the size of the Captcha challenge. A Captcha challenge typically consists of a 6 to 10 letter sequence.

Automatic Online Guessing Attacks

If we exclude the odds that are regarded minor, the CaRP system, which includes a CPA-secure Captcha, contains the following characteristics: The contradiction approach can be used to prove the initial assertion. Assume the aforementioned feature does not exist, implying that an internal object-point on picture A is strongly dependent on an internal object-point on image B. An opponent could leverage the trust to perform a targeted-pixel attack. Image A is used during the learning phase to learn information about the object covered by point.

Human Guessing Attacks

In human guessing attacks, human agents are utilized to enter passwords through trial and error. It has been shown that when it comes to guessing attacks, people do substantially poorer than computers. According to this formula, the theoretical password space for 8-character passwords for Click Text, which has a 33-character alphabet, is around 338 240. The password space for Click Animal, which has a 10-animal alphabet, is around 108 226. Finally, the password space for Animal Grid, which combines Click Animal with 6 6 grids, is around 10 467 242.

Relay Attacks

Relay attacks can be carried out in a variety of ways. Captcha issues may lead to a busy website that has been hacked or operated by opponents. This allows human users to collaborate to solve difficulties, allowing for continuous internet surfing. As an alternative, these difficulties could be delegated to sweatshops where workers are paid to answer Captcha riddles. Is it possible to launch relay attacks against Context-aware Role-based Access Control (CaRP)?

Shoulder-Surfing Attacks

Graphical passwords are more vulnerable when typed in public settings such as bank ATMs due to the risk of shoulder-surfing assaults. The Car Registration Plate (CaRP) technology is now vulnerable to shoulder-surfer attacks. However, when paired with the previously mentioned dual-view technology, CaRP has the ability to successfully thwart shoulder-surfing attacks.

5. EMPIRICAL EVALUATIONS

Implementations

Click Text and Animal Grid were developed using the ASP.NET framework. The Click Text solution made use of a commercially available configurable text Captcha engine that was previously utilized by Microsoft.

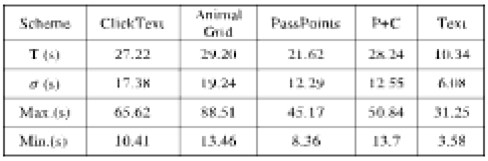
Uppercase letters are the only ones accepted by the Captcha engine. As a consequence, 33 characters were picked in order to conduct usability testing. This selection included capital letters, minus I, J, O, and Z, as well as numerals, minus 0 and 1, and three special characters, namely #, @, and &. Each image utilized in the study was set up to be 400 by 400 pixels in size. The figure. The image in Figure 2 in Section IV-A was made utilizing the above-mentioned technique..

Experimental Results

For each scheme, Table I displays the average login time, sample standard deviation, maximum login time, and minimum login time. The term usability refers to the ease with which a product or system can be used. These figures were derived from the successful login attempts of the 40 participants. Pass Points took slightly longer to login than Click Text, Animal Grid, or P + C, but all three took the same amount of time.

TABLE I

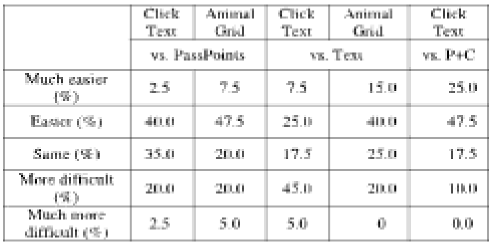
The average (T), sample standard deviation (), and maximum value are three statistical measures that can be used to describe the length of time it takes to log in for various approaches. Furthermore, it is critical to consider the minimum value.



Scheme	ClickText	Animal Grid	PassPoints	P+C	Text
T (s)	27.22	29.20	21.62	28.24	10.34
σ (s)	17.38	19.24	12.29	12.55	6.08
Max.(s)	65.62	88.51	45.17	50.84	31.25
Min.(s)	10.41	13.46	8.36	13.7	3.58

TABLE II

A COMPARISON OF THE USABILITY OF DIFFERENT STRATEGIES



	Click Text	Animal Grid	Click Text	Animal Grid	Click Text
	vs. PassPoints		vs. Text		vs. P+C
Much easier (%)	2.5	7.5	7.5	15.0	25.0
Easier (%)	40.0	47.5	25.0	40.0	47.5
Same (%)	35.0	20.0	17.5	25.0	17.5
More difficult (%)	20.0	20.0	45.0	20.0	10.0
Much more difficult (%)	2.5	5.0	5.0	0	0.0

6. CONCLUSION

CaRP integrates a graphical password system with a CAPTCHA. CaRP methods are classified into two types: recognition-based CaRP and recognition-recall CaRP. As previously stated, recognition-based CaRP is independent of any particular CAPTCHA method. When a particular CAPTCHA method is successfully hacked, it is common for a follow-up, improved scheme to be designed and implemented; this scheme is sometimes referred to as a CaRP scheme. CaRP offers commendable qualities in terms of security, usability, and practical applications, indicating that it has much room for advancement. CaRP's usability can be improved by using images with varying degrees of difficulty that are picked based on the user's login history and the device used to log in.

REFERENCES

1. R. Biddle, S. Chiasson, and P. C. van Oorschot, Graphical passwords: Learning from the firsttwelve years, ACM Comput. Surveys, vol. 44, no. 4, 2012.
2. The Science Behind Passfaces [Online]. Available: http://www.realuser.com/published/ScienceBehindPassfaces.pdf (2012, Feb).
3. Jermyn, A. Mayer, F. Monrose, M. Reiter, and Rubin, The design and analysis of graphical passwords, in Proc. 8th USENIX Security Symp.,1999, pp. 1–15.
4. H. Tao and C. Adams, Pass-Go: A proposal to improve the usability of graphical passwords, Int. J. Netw. Security, vol. 7, no. 2, pp. 273–292, 2008. S. Wieden beck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, Pass Points: Design and longitudinal evaluation of a graphical password system, Int. J. HCI, vol. 63, pp. 102–127, Jul. 2005.