

Captcha as Graphical Password Authentication System with IP Blacklisting

Syeatha Merlin Thampy

*Department of Computer Science & Engineering
St. Joseph College of Engineering and Technology Palai,
India*

Syeatha Merlin Thampy

*Department of Computer Science & Engineering
St. Joseph College of Engineering and Technology Palai,
India*

Abstract

Nowadays, authentication is one of the important fields in information security. Strong text-based password could provide certain degree of security level. However, the fact that, those strong passwords are difficult to memorize by the users. Graphical authentication has been proposed as an alternative solution to text-based authentication. Many researches shows that humans can remember images better than text. In recent years, many networks, computer systems and Internet based environments used graphical authentication technique for authentication. But this graphical authentication technique has many limitations. CAPTCHA is a programme that protects website against bots by generating and grading tests that human can pass but current computer program cannot. This paper present a new technology called Captcha as gRaphicalPassword (CaRP). CaRP combines both CAPTCHA and graphical password scheme. CaRP offers protection against dictionary attacks, relay attacks, shoulder surfing attacks. With the rapid development of internet, the number of people who are online also increases tremendously. The misuse and abuse of internet is growing at an alarming rate. Restriction of access is performed by introducing the concept of blacklisting of IP address.

Keywords: Graphical password, brute force attack, dictionary attacks, security, image passwords

I. INTRODUCTION

Graphical password techniques are an alternative to alphanumeric passwords in which users click on images to authenticate themselves rather than using alphanumeric strings. Because of increasing threats or misuses to networked computer systems, there is great need for security innovations system. Security practitioners and researchers have made stalk in protecting systems and individual users' digital assets or sensitive data. Users interact with security technologies either passively or actively. For passive use, users must have understood ability. For active use people must need much more from their security solutions: ease of use, memorability, efficiency, effectiveness and satisfaction.

Authentication is the mechanism of determining whether each user should be allowed access to a particular system or resource. It is a critical area in the field of security research and practice. Alphanumeric passwords are used widely for authentication purpose, but other methods are also available, including biometrics and smart cards for authentication. Many problems that the users have with alphanumeric passwords which are mainly related to memorability of secure passwords or strong password. In an attempt to create more memorable passwords that helps the users, graphical password systems have been invented. In these systems authentication is based on clicking over images rather than typing alphanumeric strings. Several kinds of graphical passwords have been invented.

A graphical password scheme[2] is an authentication system that works by having the user select click points from images, in a specific order, which is presented in a graphical user interface (GUI) to the user. The graphical-password approach is also called graphical user authentication (GUA)[3,4,5]. A graphical password is easy to memorize than a text-based password for most people. Suppose an minimum of 8-character password is necessary to gain entry into a particular computer network. Instead of w8KiJ72c, a user might select images of the earth, the country of France, a white stucco house with arched doorways and red tiles on the roof and so on.

The proposed system introduce a new security primitive based on hard AI problems, namely, a novel family of graphical password systems integrating Captcha technology, which called as CaRP (Captcha as gRaphical Passwords). CaRP is both a Captcha and a graphical password scheme. A CAPTCHA [18] is a program that protects websites against automated actions by generating tests that humans can pass easily but computer programs cannot. The term CAPTCHA (for Completely Automated Public Turing Test To Tell Computers and Humans Apart) was invent in 2000 by Luis von Ahn, Manuel Blum, Nicholas Hopper and John Langford of Carnegie Mellon University[1]. CaRP is click-based graphical passwords, where a sequence of clicks points on an image is used to create a password. Unlike other click-based graphical passwords schemes, images used in CaRP are Captcha challenges, and a new CaRP image is generated for every user's login attempt. CaRP offers protection against online dictionary attacks in the field of web application, which have been for long time a major security threat for various online web services. CaRP also offers protection against relay attacks, an increasing security threat to bypass Captchas protection, where in Captcha challenges are easy to humans to solve[12,13]. CaRP requires solving a Captcha challenge in every user's login. This

impact on usability can be reduced by adapting the CaRP image's difficulty level based on the login history of the user's account and the machine used to log in.

With the rapid development of internet, the number of people who are using web application also increases tremendously. But now a day's, can see that not only growing positive use of internet but also the negative use of it. The misuse and abuse of internet is growing at an alarming rate. This misuse and abuse can be limited using IP blocking. Restriction of access is performed by introducing the concept of blacklisting of IP address. It may be defined as the basic access control mechanism. The blacklisted IP table consists of all IP address whose access has been denied.

II. AUTHENTICATION SYSTEM AND BAD HOST

Authentication is one of the key areas in security research and practice, which determines whether a user should be allowed access to a given system or resource. Traditionally, alphanumeric passwords have been used for authentication. Today other methods, including biometrics and smart, are possible alternatives. However, passwords are likely to remain superior for some time because of drawbacks of reliability, security, or cost of other technologies. In particular, smart cards also need PINs and passwords. Passwords also have drawbacks, most in terms of memorability and security. This has led to a new idea to improve passwords. One such innovation is graphical passwords, i.e. passwords that uses images rather than alphanumeric strings. The underlying idea is that using images will lead to greater memorability to the users and decrease the tendency to choose insecure or weak passwords, which will in turn increase overall password security.

The proposed system introduce a new security primitive based on hard AI problems, namely, a novel family of graphical password systems combining with Captcha technology, which called as CaRP (Captcha as gRaphical Passwords)[14]. CaRP is both a Captcha and a graphical password scheme. A CAPTCHA is a program that protects websites against bots by generating tests that humans can pass but current computer programs cannot. CaRP is click-based graphical passwords, where a sequence of clicks on an image is used to derive a password. Creation of unlimited number of accounts can be limited by IP blacklisting[15]. The dictionary attack and brute force attack can be avoided by limiting the trials at login time. The authentication is done by three levels of password which are text based, CaRP and click points.

A new user initially registers to the system by providing username, email, phone number, text password, CaRP password and click points password. Text based allow user to enter text based, which is minimum of six[6,7] alphanumeric strings. Next level is CaRP where user needs to click correct image specified by the system. Each login or registration time the images are displayed in random sequence. In CaRP password selection, a set of animal image are stored in the database. On registration these stored animal images are displayed in grid form to the user interface randomly. Also the name of the images as in text form shows randomly to each user. Each user at registration time need to select the corresponding animal image as per the displayed text (name of the animal). This image will be the user CaRP password. User need to memorize this selected image for authentication. This correct selection can be done only by a human. While the bots feel this as a difficult task. Hence this reduces automated attacks made by the attackers. If the selection is right, then user need to select click point password. Here user need to click some points (three points) on the selected image as their password. This scheme is flexible to the user because it allows any image to be used, e.g. natural images, paintings, etc. The images could be chosen by the user. The only practical requirement is that the image be intricate and rich enough so that many possible click points are available. Another flexibility is that, do not need artificial predefined click regions with marked boundaries. A user's password consists of any randomly chosen sequence of points in the image. Since an tangled image easily has hundreds of memorable points, not many click points are needed to make a password hard to guess. For example, with five or six click points one can make more passwords than 8-character Unix-style alphanumeric passwords over a standard 64-character alphabet. The authentication process involves the user selecting several points on picture in a particular order. When logging in, the user is supposed to click close to the selected click points, within some (adjustable) tolerance distance. Here only one image is needed for the user to set their password in this level.

At authentication time, user need to provide username, email, text password, CaRP image password and click points password. If this selection is right, then login success. Then the user enter to their own accounts. Each user can store documents to their accounts. The systems provide an option for setting security to the stored documents.

For security reasons, the system should not store passwords explicitly. Users text password, click points were saved in encrypted format using AES-128 encryption algorithm. Advanced Encryption Standard (AES) algorithm is not only for security but also for great speed. The user clicked points at the final level of authentication were saved as (x,y) coordinates in the database.

With the rapid development of internet, the number of people who are online also increases tremendously. The misuse and abuse of internet is growing at an alarming rate. Restriction of access is performed by introducing the concept of blacklisting of IP address. It may be defined as the basic access control mechanism. The blacklisted IP table consists of all IP address whose access has been denied. The blacklisted IP is termed as bad host file. Creation of unlimited number of accounts can be limited by IP blacklisting. The dictionary attack and brute force attack can be avoided by limiting the trials at login time[16,17].

The maximum trial in authentication is limited to three. This limitation is done for avoiding any attacks to the user account. When the maximum trial is reach, the system blocked the users account. Then send a number to the user email account and asked the user to change the CaRP image password. This number can be any digits number. On changing password, system ask the user to enter the number send via the email. If the correct number is enter, then the system allow the user to change the CaRP image

password. Otherwise the system doesn't allow to change the CaRP password. Thus it again reduce the attacks done by the attackers.

III. RESULTS AND DISCUSSIONS

Security-sensitive environments secure their resources against unauthorized access by implementing access control mechanisms. Text based passwords are not secure for such applications. User authentication can be improved by using both text passwords and image passwords. Authentication plays an vital role in protecting resources against unauthorized use. Many authentication procedure exist from simple password based authentication system to costly and computation intensive Biometric authentication systems. But still the most commonly used authentication system is based on text passwords. Text based passwords are not secure enough for several applications that implement security by access control mechanisms.

Authentication based on text based passwords has many pitfalls. A user may have many accounts on different computers. He has to remember several passwords. The general predilection is that an individual may not remember text passwords easily and he may write it down or save it somewhere. This can lead to plagiarize password to gain unauthorized access to a system. If passwords are not very long, they are easy to crack using brute force attacks like trying different passwords (online attack) or by offline attack on the password hash file[8,9,10]. There are many other ways to crack passwords like packet sniffing. On the other hand, if a password is hard to guess, then it is often hard to remember. To address this problem, authentication methods that use pictures as passwords were invented.

Graphical password schemes have been proposed as an alternative to text-based schemes, motivated partially by the fact that humans can easily memorize pictures better than text; many psychological studies supports such assumption. Pictures are generally easier to be memorized or recognized than text. In addition, if the number of possible pictures is large, the possible password space of a graphical password scheme may beat that of text- based schemes and thus offer better resistance to dictionary attacks. Because of these advantages, there is a growing temptation in graphical password. In addition to workstation and web log-in applications, graphical passwords have also been applicable to ATM machines and mobile devices.

The benefits of the proposed system can be analyzed based on three categories: usability, deployability and security.

A. Usability Benefits

- Memorywise-Effort: Users of the scheme have to remember the text password, CaRP password image and three click points on the corresponding image for authentication.
- Nothing-to-Carry: Users do not need to carry an auxiliary physical object (electronic device, mechanical key, piece of paper) to use the scheme.
- Easy-to-Learn: Users who don't know the scheme, can figure it out and learn it without too much trouble, and then easily recall how to use it.
- Efficient-to-Use: The time the user must spend for each authentication is acceptably short. The time required for setting up a new association with a verifier, although possibly longer than that for authentication, is also reasonable.

B. Deployability Benefits

- Negligible-Cost-per-User: The total cost per user of the scheme, adding up the costs at both the prover's end (any devices required) and the verifier's end (any share of the equipment and software required), is negligible. The scheme is feasible for startups with no per-user revenue.
- Server-Compatible: At the verifier's end, the scheme is suited with text-based passwords. Providers don't have to change their existing authentication framework to support the scheme.
- Browser-Compatible: Users don't have to change their client to support the scheme and can expect the scheme to work when using other machines with an up-to-date, standards-compliant web browser and no additional software.

C. Security Benefits

- Resilient-to-Targeted-Impersonation: It is not possible for an acquaintance (or skilled investigator) to impersonate a specific user by misusing knowledge of personal details (birth date, names of relatives etc.).
- Strength of password: Three levels of passwords are using. Text password have minimum of six alphanumeric strings. Next is CaRP password and click points which provide can make more passwords strength than 8-character text password.
- Restriction of account creation: Restriction of access is performed by introducing the concept of blacklisting of IP address. It may be defined as the basic access control mechanism. The blacklisted IP table consists of all IP address whose access has been denied. The blacklisted IP is termed as bad host file. Creation of unlimited number of accounts can be limited by IP blacklisting.
- Online guessing attack: In automated guessing attacks, the trial and error process is executed automatically whereas dictionaries can be constructed manually. Construction of dictionary can be done for text password. But this cannot be applicable for image password and click points password. Probability for trial and error attack is very low because the system contain lots of image set and large password space for click points password

- Human guessing attacks: In human guessing attacks, humans are used to enter the security passwords in the trial and error process. Humans are much slower than computers in mounting guessing attacks. Because of large password space human need to take more time to find out the credentials. So this is a difficult task for human. The large number of trials is limited at login time.

For understanding various aspects of authentication usability of different users a survey was conducted. For this survey participants of 100 students from my college (engineering college) was selected. The questionnaire consist of questions regarding password selection, aid used for remembering password and so on. Among this 100 students, 5 students are selected for interfacing with the proposed system. Feedbacks from these 5 students were noted.

All the participants have online accounts. Table 1 shows different response regarding the password from the 100 participants. All of them have multiple online accounts in the web. Most of them uses text password having easy memorable. Also uses aid for remembering text password. From this response, conclude that most of the users use easy memorable password and use same password for multiple accounts. If the users use complex password, they depend on some aid for remembering the password. Table 2 shows frequency of aid used for remembering password. Most of them use some aid for remembering the password. Graph 1 also shows the same. From this, easily predict that users feel difficulty in remembering text password because of many reasons like having multiple accounts, different passwords, using complex password and so on.

Table – 1

Summary of feedback

<i>QUESTIONS</i>	<i>NUMBERS</i>
<i>Participants having online accounts</i>	<i>100</i>
<i>Having multiple accounts</i>	<i>100</i>
<i>Using text password</i>	<i>100</i>
<i>Using image password</i>	<i>2</i>
<i>Using same password</i>	<i>80</i>
<i>Using different password</i>	<i>20</i>
<i>Using complex password</i>	<i>13</i>
<i>Using aid for remembering password</i>	<i>80</i>

Table – 2

Different aid for remembering password

<i>AID USED</i>	<i>RESPONSE</i>
<i>Write down in personal diary</i>	<i>2</i>
<i>Draft in mail</i>	<i>80</i>
<i>Saving in mobile</i>	<i>40</i>
<i>Saving in laptops/tablets</i>	<i>10</i>
<i>Memory</i>	<i>74</i>
<i>Browser password manager</i>	<i>7</i>

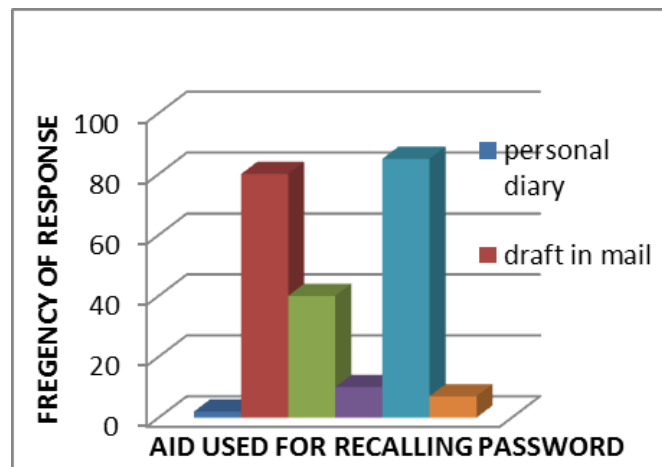


Fig. 1: Graph 1: Aid Used For Recalling Password

The average registration time for CaRP authentication is 126 seconds and for the existing system AnimalGrid is 42 seconds. CaRP take more time for registration because it has three levels of password creation where AnimalGrid have only one level of password. Graph 2, shows average time taken by these two different authentication system.

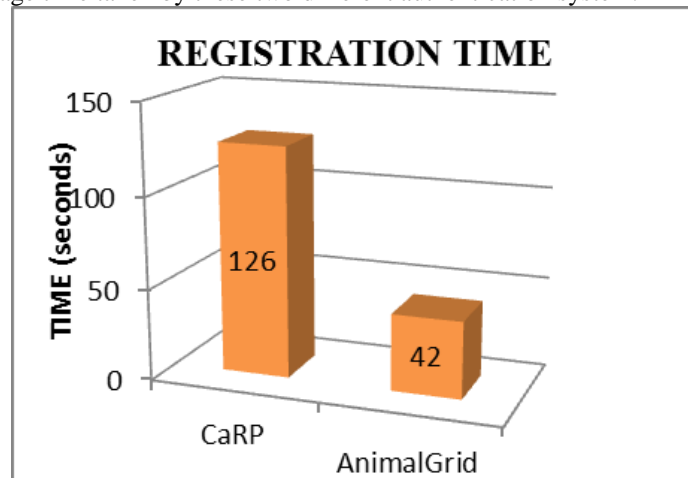


Fig. 2: Graph 2: Average time for registration

The average login time for CaRP authentication is 90 seconds and for the existing system AnimalGrid is 40 seconds. CaRP has three levels of password. So it take more time than AnimalGrid. Graph 3, shows average login time taken by these two different authentication systems.

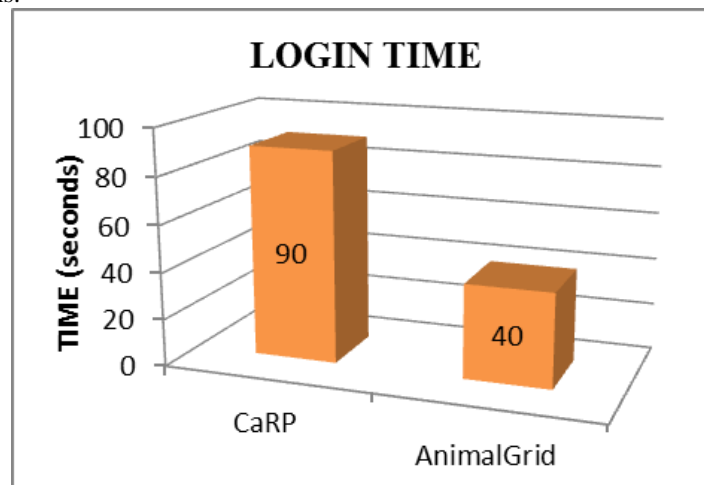


Fig. 3: Graph 3: Average time for login

Table – 3
CaRP authentication feedback

FEEDBACK	RESPONSE
Select correct CaRP password at registration time	5
Select image for click points password	5
Correct clicks at login time	4
IP blocked users	0
More attempt taken for login	1

Table 3 shows CaRP authentication feedback from 5 participants. All users selected CaRP password correctly at registration time, selected an image from their own system and chosen three click points over the image. Among 5 participants four of them selected correct image and click points at login time. Only one had taken more attempts for login. Any one of participants IP address was blocked. Since registration and login was done by human. Humans are easy for selecting CaRP password, but bots feel difficulty in this stage. From this feedback, it is clear that the CaRP authentication is very easy for the user.

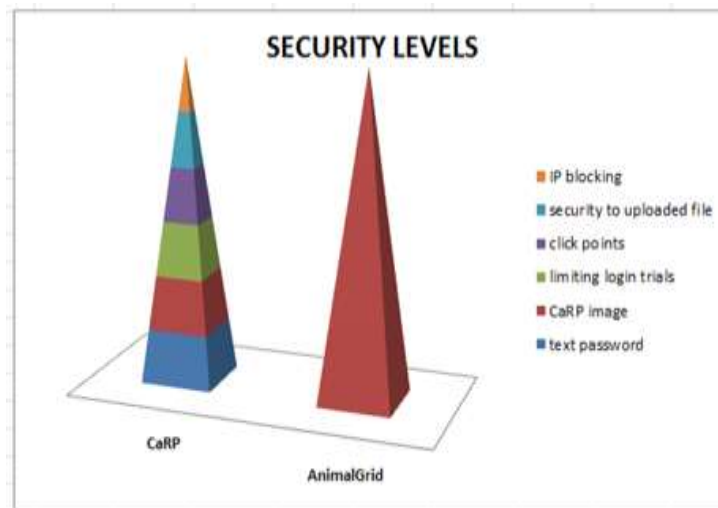


Fig. 4: Graph 4: The number of security levels used

Number of security levels used in CaRP authentication and AnimalGrid is shown in the graph 4. AnimalGrid uses only one level of security, which is setting AnimalGrid password. CaRP authentication uses three levels of passwords: text password, CaRP password and click points password. After entering to users account the system provides an option for setting security to the uploaded/stored documents. The stored documents could only be downloaded by authenticating the click points to the corresponding image. With the rapid development of internet, the number of people who are online also increases tremendously. The misuse and abuse of internet is growing at an alarming rate. Restriction of access is performed by introducing the concept of blacklisting of IP address. It may be defined as the basic access control mechanism. The blacklisted IP table consists of all IP address whose access has been denied. The blacklisted IP is termed as bad host file. Creation of unlimited number of accounts can be limited by IP blacklisting. The dictionary attack and brute force attack can be avoided by limiting the trials at login time. As the number of security level increases, security to the authentication system also increases. Hence CaRP authentication system provide better security than AnimalGrid.

IV. CONCLUSION

Graphical password techniques are an alternative to alphanumeric passwords in which users click on images to authenticate themselves rather than type alphanumeric strings. A CAPTCHA is a program that protects websites against bots by generating some tests that which humans can pass but current computer programs cannot.

The proposed system introduces a new technology called CaRP. CaRP is click-based graphical passwords, where a sequence of clicks on an image is used to derive a password. CaRP integrating both Captcha and graphical password scheme. The notion of CaRP introduces a new family of graphical passwords, which adopts a new approach as a countermeasure for online guessing attacks: a new CaRP image, which is a Captcha challenge, is used for every user's login attempt to make trials of an online guessing attack computationally independent of each other. Unlimited number of account creation can be avoided by IP blacklisting which is the basic access control mechanism. The blocked IP list is termed as bad host file. Brute force and dictionary attack can be mitigated by limiting the trials at login time.

REFERENCES

- [1] VedPrakash Singh, PreetPal, "Survey of Different Types of CAPTCHA", IJCSIT, Vol. 5 (2), 2014, 2242-2245
- [2] R. Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical passwords: Learning from the first twelve years," ACM Comput. Surveys, vol. 44, no. 4, 2012.
- [3] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords," in Proc. 8th USENIX Security Symp., 1999, pp. 1-15.
- [4] S. Chiasson, P. C. van Oorschot, and R. Biddle, "Graphical password authentication using cued click points," in Proc. ESORICS, 2007, pp. 359-374.
- [5] S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot, "Influencing users towards better passwords: Persuasive cued click-points," in Proc. Brit. HCI Group Annu. Conf. People Comput., Culture, Creativity, Interaction, vol. 1, 2008, pp. 121-130.
- [6] R. Dhamija and A. Perrig, "Déjà Vu: A user study using images for authentication," in Proc. 9th USENIX Security, 2000, pp. 1-4.
- [7] A.E. Dirik, N. Memon, and J.-C. Birget, "Modeling user choice in the passpoints graphical password scheme" in Proc. Symp. Usable Privacy Security, 2007, pp. 20-28
- [8] J. Yan and A. S. El Ahmad, "A low-cost attack on a Microsoft CAPTCHA," in Proc. ACM CCS, 2008, pp. 543-554.
- [9] J. Elson, J. R. Douceur, J. Howell, and J. Saul, "Asirra: A CAPTCHA that exploits interest-aligned manual image categorization" in Proc. ACM CCS, 2007
- [10] P. Golle, "Machine learning attacks against the Asirra CAPTCHA," in Proc. ACM CCS, 2008, pp. 535-542.
- [11] G. Mori and J. Malik, "Recognizing objects in adversarial clutter," in Proc. IEEE Comput. Society Conf. Comput. Vis. Pattern Recognit., Jun. 2003, pp. 134-141.
- [12] <http://www.captcha.net>
- [13] <http://www.findexamples.com/5-examples-of-different-types-of-captchas>
- [14] Bin B. Zhu, Je Yan, Guanbo Bao, Maowei Yang, and Ning Xu "Captcha as Graphical Passwords A New Security Primitive Based on Hard AI Problems", IEEE Transaction Information Forensics and Security, vol. 9, no. 6, June 2014.

- [15] Khundrakpam Johnson Singh, Tanmay De “DDOS Attack Detection and Mitigation Technique Based On Http Count and Verification Using CAPTCHA”, in International Conference on Computational Intelligence & Networks, 2015.
- [16] Joseph Bonneau et.al “The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes”, In Proc. IEEE Symp. on Security and Privacy, 2012
- [17] P. C. van Oorschot and S. Stubblebine, “On countering online dictionary attacks with login histories and humans-in-the-loop,” *ACM Trans. Inf. Syst. Security*, vol. 9, no. 3, pp. 235–258, 2006.
- [18] L. von Ahn, M. Blum, N. J. Hopper, and J. Langford, “CAPTCHA: Using hard AI problems for security,” in Proc. Eurocrypt, 2003, pp. 294–311.
- [19] B. B. Zhu et al., “Attacks and design of image recognition CAPTCHAs,” in Proc. ACM CCS, 2010, pp. 187–200.
- [20] G. Moy, N. Jones, C. Harkless, and R. Potter, “Distortion estimation techniques in solving visual CAPTCHAs,” in Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit., Jul. 2004, pp. 23–28.