IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-5, May 2019 E-ISSN: 2347-2693

Systematic Evaluation of Existing CAPTCHA Techniques

S.S. Kulkarni[1*], H.S. Fadewar[2]

[1,2]School of Computational Sciences, S. R. T. M. University, Nanded, India

[*]*Corresponding Author sushama.s.kulkarni@gmail.com*

DOI: https://doi.org/10.26438/ijcse/v7i5.13991402 | Available online at: www.ijcseonline.org

Accepted: 23/May/2019, Published: 31/May/2019

***Abstract*—** Continuous evolution of CAPTCHA techniques is necessary to combat modern generation of AI enabled bots. Designing a new CAPTCHA scheme requires a careful review of existing CAPTCHA techniques. But existing reviews of current CAPTCHA techniques lack systematic evaluation of the current trends in CAPTCHA development. Existing reviews focus on mere enlisting of current CAPTCHA schemes in several categories and explaining their working schema. Hence systematic evaluation and analysis of existing CAPTCHA techniques in several categories is necessary. In this paper we highlight the facts and flaws of existing CAPTCHA techniques in order to provide insights for future improvements in current CAPTCHA techniques. We have focused on providing simple and clear understanding of existing CAPTCHA techniques in a systematic way. This will help researchers to overcome the drawbacks of current CAPTCHA schemes and work on improvement of weaker aspects of existing CAPTCHA techniques.

***Keywords*—**CAPTCHA, HCI, Web security, Human Interactive Proof (HIP), Bots

I. INTRODUCTION

CAPTCHA (Completely Automatic Public Turing Test to Tell Computer and Human Apart) is a test to combat bots and allow human users to interact with the given system. CAPTCHAs can be presented in textual, audio, video, image, puzzle or a game format. CAPTCHA test is designed to be easy for human users and difficult for bots.

Construction of CAPTCHAs is based on AI problems. If a CAPTCHA can be solved programmatically it marks scientific progress on a hard AI problem. A problem which cannot be solved by computer programs can be used as CAPTCHA. This indicates that continuous efforts are being made to improve the robustness of CAPTCHAs.

Many reviews of existing CAPTCHA techniques have been performed by several researchers [18]. But in this paper we attempt to gain understanding about current CAPTCHA techniques and find out their flaws through systematic evaluation. This will help CAPTCHA developers to design efficient CAPTCHA tests avoiding the existing drawbacks.

In this paper we have evaluated various categories of CAPTCHA like OCR based CAPTCHA, Non-OCR based CAPTCHA, Cognitive CAPTCHA, Face Detection based CAPTCHA and CAPTCHA as gRaphical Password (CaRP).

Rest of the paper is organized as follows, Section I contains the introduction of CAPTCHA concept, Section II contains the evaluation of OCR based CAPTCHAs, Section III contains evaluation of Non-OCR based CAPTCHAs, Section IV contains evaluation of Cognitive CAPTCHAs, section V contains evaluation of Face Detection based CAPTCHA techniques, Section VI describes evaluation of CAPTCHA as gRaphical Password (CaRP) schemes and Section VII concludes systematic evaluation with future directions.

II. EVALUATION OF OCR BASED CAPTCHAS

OCR-based CAPTCHAs are mainly text-based CAPTCHAs in which the user is shown distorted images of letters and/or digits. User must recognize it in order to pass the CAPTCHA test. OCR-based CAPTCHAs rely on the distortion techniques for preventing bots. Low readability results into increased failure rate for human users. Most of the websites use OCR based CAPTCHAs for preventing bots.

Table 1 shows the evaluation of OCR-based CAPTCHAs.

Table 1. Evaluation of OCR based CAPTCHAs

Facts Found	Flaws Found	Reference
Pessimal Print method artificially lowers the quality of the printed letters to prevent bots [1]	Mori-Malik algorithm and brute-force method is capable of breaking it	A. L. Coates et al., "Pessimal Print: A Reverse Turing Test", 2001
Baffletext method produces words that are not provided in English dictionaries, picture of the word is	Provides low comfort level for human users since use of random letters instead of dictionary words irritates human users	Chew M. et al., "BaffleText: a Human Interactive Proof", 2003

changed with different degrees of ease or difficulty [2]		
Gimpy method uses its word from a dictionary with 850 words [3]	A correlation algorithm correctly identified the word in EZ-Gimpy CAPTCHA 99% of the time and a direct distortion estimation algorithm identified the 4 letters in Gimpy-r CAPTCHA 78% of time	Gabriel Moy et al., "Distortion Estimation Techniques in Solving Visual CAPTCHAs", 2004
Text-based CAPTCHA uses the ability of people to read images of text more reliably than OCR [4]	These CAPTCHAs are becoming more difficult for genuine users, attackers are also getting better at breaking existing CAPTCHAs	Kumar Chellapilla et al., "Building Segmentation Based Human-Friendly Human Interaction Proofs (HIPs)", 2005

Evaluation of OCR based CAPTCHAs indicate that these are the most susceptible CAPTCHA schemes. More complex schemes of OCR CAPTCHAs for preventing bots are being introduced. But complex OCR based CAPTCHAs irritate human user and are difficult as well. Thus researchers must focus on providing ease of use for human users and improving robustness at the same time.

III. EVALUATION OF NON-OCR BASED CAPTCHAS

Non-OCR based CAPTCHAs basically test the audio/video sense capability of a human being. Table 2 shows the evaluation of Non-OCR based CAPTCHAs.

Table 2. Evaluation of Non-OCR based CAPTCHAs

Facts Found	Flaws Found	Reference
Implicit CAPTCHA requires users to make a simple click in specified area of the picture [5]	This CAPTCHA is prone to pattern recognition attack	H.S. Baird et al., "Implicit CAPTCHAs", 2005
Audio CAPTCHA plays a sound, the user must recognize it and type the word [6]	3 different types of widely used audio CAPTCHAs were broken with 71% accuracy	Tam J. et al. "Breaking Audio CAPTCHAs", 2008
Video CAPTCHA requires a user to provide appropriate tag for the video displayed as a CAPTCHA test [7]	Irritates human user because of greater loading time. They are prone to bot attacks which use database replication, Video analysis, etc.	K.A. Kluever et al., "Balancing usability and security in a video CAPTCHA", 2009

Evaluation of Non-OCR based CAPTCHAs indicate that they face pattern recognition and other advanced AI enabled attacks. Audio CAPTCHAs in this category are becoming soft targets. Hence researchers developing a new Non-OCR based CAPTCHA have to implement AI-Hard problems to thwart bots in a more efficient way.

IV. EVALUATION OF COGNITIVE CAPTCHAS

Table 3. Evaluation of Cognitive CAPTCHAs

Facts Found	Flaws Found	Reference
Question-based CAPTCHA assesses skills of a user through a question which can only be answered by a human user [8]	It is a language dependent CAPTCHA	Mohammad Shirali-Shahreza et al., "Question-Based CAPTCHA", 2007
Math CAPTCHA asks user to solve a mathematical equation [9]	Difficulty level of the equation may cause discomfort for a novice human user	C. J. Hernandez-Castro et al., "Pitfalls in CAPTCHA design and implementation: The Math CAPTCHA, a case study", 2010
NLP CAPTCHA makes use of advertisements which are embedded with the challenge for users	It is a language dependent CAPTCHA	http://nlpcaptcha.in/
Game CAPTCHA uses a database of cartoon mini-games that are interesting and supportive for users with accessibility difficulties as well	Gaming bots can solve these CAPTCHAs	http://areyouahuman.com
Move & Select CAPTCHA requests user to move and correctly rearrange the randomly placed pieces of an image and then select events associated with image from a drop down list [10]	It requires high amount of efforts from a human user to solve this CAPTCHA	M. M. Tanvee et al., "Move & Select: 2Layer CAPTCHA Based on Cognitive Psychology for Securing Web Services", 2011
Four-Panel cartoon CAPTCHA required user to rearrange the stages of a funny story in proper order [11]	Some of the humours may not have relevance in different cultures and societies. Hence it has high error proneness.	T. Yamamoto et al., "A Proposal of Four panel cartoon CAPTCHA", 2011
CAPTCHA based on human cognitive factor asked user to choose the desired types of challenge from 5 types of challenges [12]	It allows user to choose specific domain area from given 5 domain areas which could make it easy for bots to gain success with lowered efforts	M. J. M. Chowdhury et al., "CAPTCHA Based on Human Cognitive Factor", 2013
A CAPTCHA utilizing cognitive ability of human through PHP presented user alphanumeric characters hidden within innovative designs and asked user to recognize the presented alphanumeric string [13]	It has less visual clarity thus offers low readability. It is not suitable for blind users	V. Dhaka et al., "Developing a CAPTCHA Utilizing Cognitive Ability of Human through PHP", 2015

Cognitive CAPTCHAs use AI-hard or AI-Complete problems to identify humans and bots apart. In fact, cognitive CAPTCHAs are those which use human cognitive skills like classification, grouping, interpretation, game playing, etc. for preventing bots. But cognitive CAPTCHAs pose an obstacle for people having certain cognitive disabilities. Table 3 shows the evaluation of Cognitive CAPTCHAs.

Evaluation of Cognitive CAPTCHAs highlights that language dependency, cultural sensitivity, necessity of highly complex cognitive skills, visual complexity are major issues encountered by these CAPTCHAs. Hence researchers must consider solving these issues while designing a new cognitive CAPTCHA.

V. EVALUATION OF FACE DETECTION BASED CAPTCHA TECHNIQUES

Face detection based CAPTCHA techniques request user to find human faces in the CAPTCHA image and click the human faces in order to pass the CAPTCHA challenge. Some of the Face detection based CAPTCHAs perform liveness test by requesting user to upload "selfie" picture or video. Table 4 shows the evaluation of Face detection based CAPTCHA techniques.

Table 4. Evaluation of Face Detection based CAPTCHA Techniques

Facts Found	Flaws Found	Reference
FaceDCAPTCHA requested user to click on the real human faces without selecting non-human faces from a set of distorted and occluded real and fake face images on a random background [14]	It is prone to Face Detection Algorithm based attack	G. Goswami et al., "FaceDCAPTCHA: Face Detection based Color Image CAPTCHA", 2014
FATCHA required user to perform some trivial gesture using face or head [15]	It is not acceptable in certain culture to share live videos of female users. Thus it can create accessibility barrier for women in certain cultures	M. De Marsico et al., "FATCHA: biometrics lends tools for CAPTCHAs", 2017
rtCAPTCHA asked user to take a "selfie" video while announcing the answer to the Captcha [16]	It is not acceptable in certain culture to share "selfie" videos of female users. Thus it can create accessibility barrier for women in certain cultures	E. Uzun et al., "rtCaptcha: A Real-Time CAPTCHA Based Liveness Detection System", 2018

Face detection based CAPTCHA techniques are vulnerable to Face detection Algorithm attacks. These CAPTCHAs can pose as accessibility barrier for women users in certain cultures. Thus they can invoke culture sensitive issues. Researchers designing Face detection based CAPTCHA should take care of strength of CAPTCHA along with the accessibility to all genders.

VI. CAPTCHA AS GRAPHICAL PASSWORD (CARP)

One of the evolving techniques is the use of CAPTCHA as gRaphical Password (CaRP). It combines graphical password and CAPTCHA scheme. CaRP uses Captcha-based Password Authentication (CbPA) protocol to prevent online dictionary attacks. CaRP can be classified as:

- Recognition based CaRP
- Recognition-Recall based CaRP

Table 5 and Table 6 shows the evaluation of Recognition based CaRP and Recognition-Recall based CaRP.

Table 5. Evaluation of Recognition based CaRP

Facts Found	Flaws Found	Reference
ClickText requires user to click a sequence of characters which are randomly arranged in set of 33 characters on a 2D space. It authorizes user if password characters are clicked in specified sequence [17]	Random rotation and low spacing between neighbouring characters sometimes lowers the readability of ClickText CAPTCHA	Bin B. Zhu et al., "Captcha as Graphical Passwords-A New Security Primitive Based on Hard AI Problems", 2014
ClickAnimal uses sequence of animal names as password. CAPTCHA is generated by arranging 2D animal images on a cluttered background [17]	It has smaller password space as compared to Click Text CaRP	Bin B. Zhu et al., "Captcha as Graphical Passwords-A New Security Primitive Based on Hard AI Problems", 2014
AnimalGrid is a combination of ClickAnimal and Click A Secret (CAS) schemes [17]	It is difficult to handle for a novice user.	Bin B. Zhu et al., "Captcha as Graphical Passwords-A New Security Primitive Based on Hard AI Problems", 2014

Table 6. Evaluation of Recognition-Recall based CaRP

Facts Found	Flaws Found	Reference
TextPoint requires user to click a sequence of clickable points on a character. Coordinates of user clicked-points are directly sent to authentication server [17]	It is prone to phishing attack	Bin B. Zhu et al., "Captcha as Graphical Passwords-A New Security Primitive Based on Hard AI Problems", 2014
TextPoints4CR each character having multiple clickable points appears only once. Server stores a password for each account [17]	It is prone to phishing attack	Bin B. Zhu et al., "Captcha as Graphical Passwords-A New Security Primitive Based on Hard AI Problems", 2014

Evaluation of CAPTCHA as gRaphical Password (CaRP) schemes indicates that they have issues like low readability, complexity of user interface and high vulnerability to phishing attack. Researchers designing a new CAPTCHA as gRaphical Password (CaRP) scheme must provide user friendly interface and take necessary precautions to avoid phishing attack.

VII. CONCLUSION

Evolution of AI techniques has improved efficiency of bots. Thus necessity of new robust CAPTCHA schemes is growing. Every effort to design a new generation of

CAPTCHA requires a retrospective and through evaluation of existing CAPTCHA techniques. Researchers must avoid flaws of current CAPTCHA techniques while designing a better and efficient CAPTCHA. This paper has evaluated existing CAPTCHAs in various categories like OCR based CAPTCHA, Non-OCR based CAPTCHA, Cognitive CAPTCHA, Face Detection based CAPTCHA and CAPTCHA as gRaphical Password (CaRP). We have summarized the facts found about each of the CAPTCHA under consideration and also highlighted the flaws of these CAPTCHAs. We hope this will provide much needed insights for development of future generation of robust CAPTCHAs.

REFERENCES

[1] A.L. Coates, H. S. Baird and R. J. Faternan, "*Pessimal Print: A Reverse Turing Test*," In the Proceedings of the 6th International Conference on Document Analysis and Recognition, Seattle, WA, **USA**, pp. **1154-1158**, **2001**.

[2] M. Chew and H. S. Baird, "*BaffleText: a Human Interactive Proof*," In the Proceedings of 10th SPIE/IS&T Document Recognition and Retrieval Conference (DRR2003), Santa Clara, CA, **USA**, pp. **305-316**, **2003**.

[3] G. Moy, N. Jones, C. Harkless, and R. Potter, "*Distortion Estimation Techniques in Solving Visual CAPTCHAs*," In the Proceedings of the 2004 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'04), vol. **2**, pp. **23-28**, **2004**.

[4] K. Chellapilla, K. Larson, P. Y. Simard, and M. Czerwinski, "*Building Segmentation Based Human-Friendly Human Interaction Proofs (HIPs)*," In the Proceedings of HIP 2005, Bethlehem, PA, **USA**, pp. **1-26**, May 19-20, **2005**.

[5] H. S. Baird and J. L. Bentley, "*Implicit CAPTCHAs*," In the Proceedings of SPIE/IS&T Conference on Document Recognition and Retrieval XII (DR&R2005), **San Jose**, pp. **191-196**, **2005**.

[6] J. Tam, J. Simsa, S. Hyde, and V. Ahn, "*Breaking Audio CAPTCHAs*," In the Proceedings of 21st International Conference on Neural Information Processing Systems, Vancouver, British Columbia, **Canada**, pp. **1625-1632**, December **2008.**

[7] K.A. Kluever and R. Zanibbi., "*Balancing usability and security in a video CAPTCHA*," In the Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS '09), ACM, New York, NY, **USA**, Article **14**, pp. **1-11**, **2009**.

[8] M. Shirali-Shahreza and S. Shirali-Shahreza, "*Question-Based CAPTCHA*," In the Proceedings of International Conference on Computational Intelligence and Multimedia Applications, Sivakasi, Tamil Nadu, **India**,pp. **54-58**, **2007**.

[9] C. J. Hernandez-Castro and A. Ribagorda, "*Pitfalls in CAPTCHA design and implementation: The Math CAPTCHA, a case study*," Computers & Security, Vol. **29**, No. **1**, pp. **141-157**, **2010**.

[10] M. M. Tanvee, M. T. Nayeem, and M. M. Rafee, "*Move & Select: 2 Layer CAPTCHA Based on Cognitive Psychology for Securing Web Services*," International Journal of Video & Image Processing and Network Security, IJVIPNS/IJENS, Vol. **11**, No. **5**, pp. **917**, **2011**.

[11] T. Yamamoto, T. Suzuki, and M. Nishigaki, "*A Proposal of Four-Panel cartoon CAPTCHA*," In the Proceedings of International Conference on Advanced Information Networking and Applications 2011, Singapore , pp. **159–166**, **2011**.

[12] M. J. M. Chowdhury, N. R. Chakraborty, "*CAPTCHA Based on Human Cognitive Factor*," International Journal of Advanced Computer Science and Applications, Vol. **4**, No. **11**, pp. **144-149**, **2013**.

[13] V. Dhaka, G. Gandhi, "*Developing a CAPTCHA Utilizing Cognitive Ability of Human through PHP*," International Journal of Advanced Networking Applications, Special Issue, pp. **50–54**, **2015**.

[14] G. Goswami, B. M. Powell, M. Vatsa, R. Singh, and A. Noore., "*FaceDCAPTCHA: Face Detection based Color Image CAPTCHA*," Future Generation Computer Systems, Vol. **31**, pp. **59–68**, February **2014**.

[15] M. De Marsico, L. Marchionni, A. Novelli, and M. Oertel, "*FATCHA: biometrics lends tools for CAPTCHAs*," Multimedia Tools Applications, Vol. **76**, No. **4**, pp. **5117-5140**, February **2017**.

[16] E. Uzun, S. P. H. Chung, I. Essa, and W. Lee, "*rtCaptcha: A Real-Time CAPTCHA Based Liveness Detection System*," Network and Distributed Systems Security Symposium (NDSS), San Diego, CA, **USA**, **2018**.

[17] Bin B. Zhu, Jeff Yan, Guanbo Bao, Maowei Yang, and Ning Xu, "*Captcha as Graphical Passwords-A New Security Primitive Based on Hard AI Problems*," IEEE Transactions on Information Forensics and Security, Vol. **9**, No. **6**, pp. **891-904**, June **2014**.

[18] A. Bhalerao, L. Rade, "*A Basic Survey of CAPTCHA :Application and Challenges*", International Journal of Scientific Research in Computer Science and Engineering, Vol. **06**, No. **01**, pp.**1-5**, **2018.**

Authors Profile

Mrs. S. S. Kulkarni pursued Bachelor of Science from S. R. T M. University, India in 2005 and Master of Science from S. R. T M. University, India in year 2007. She has aquired Post Graduate Diploma in Advanced Computing from CDAC, Pune, India in year 2008. She is currently pursuing Ph.D. in School of Computational Sciences, S. R. T M. University, India. She has published several research papers in reputed international journals and conferences including IEEE & Springer and it's also available online. Her main research work focuses on Web Security Algorithms, Accessibilty on web, Human Computer Interaction and CAPTCHA based security. She has 3 years of industrial experience and 1 years of teaching experience.

Dr. H. S. Fadewar pursued Bachelor of Science from Dr. B. A. M. University, India and Master of Science from S. R. T M. University. He has obtained M. Phil. from Y. C. M.O. University and pursued Ph.D. from S. R. T M. University, India. He is currently working as Assistant Professor in School of Computational Sciences, S. R. T M. University, India since 2011. He a life member of The Indian Science Congress Association, Kolkata and International Association of Engineering. He has published more than 40 research papers in reputed international journals and conferences including IEEE, Springer and it's also available online. His main research work focuses on Human Computer Interaction, Data Mining and Biometrics. He has more than 15 years of teaching experience and 10 years of Research Experience.

