New CAPTCHA Approach for Securing Online Social Network and Web Pages Using Extended Finite Automata

Menna M.Elblky
Computer Science Department
Faculty of Computers and Information
Menoufia University
Shebin Elkom, Egypt
Mennaahmed453@gmail.com

Medhat A. Tawfeek
Computer Science Department
Faculty of Computers and Information
Menoufia University
Shebin Elkom, Egypt
medhattaw@yahoo.com

Hamdy M. Mousa
Computer Science Department
Faculty of Computers and Information
Menoufia University
Shebin Elkom, Egypt
hamdimmm@hotmail.com

***Abstract*—Today computer and the internet play an important role in our daily life. We have shown highly remarkable of automated behavior that is criminal in violation of terms of services such as auto sharing or send friend request. SO, CAPTCHA is used for protecting webpages against automated programs which are called bots. It is providing challenge response tests that determine whether or not the users are human or bot. It contains various contorted letters that are difficult for attacker's bots, but easy for humans. Since there are a lot of services on the internet, for example (email, social network, search engine) which allow users to register, during registration, some attackers write malicious programs that make website resources damaged by making automated software which is called (Bots). Many research developed more techniques to prevent accessing web resources by spammers. This paper introduces a new mechanism of CAPTCHA approach using extended finite automata (XFA) for securing web pages and online social networks against a new breed of bots. The XFA CAPTCHA is a CAPTCHA based on image which generates its tests using the automata Graph technique. The result of our research evidence that the mechanism of XFA CAPTCHA is effective in terms of security and usability respectively. As a result of that, it improved the rate of efficiency by 97.8%, the time for solving is around 20 seconds, and the value the probability of success rate for speculation attack is decreased to 1.03% in average. When compared to other CAPTCHAs, the XFA CAPTCHA is a strong competitor in terms of security and usability function.**

***Keywords*—**CAPTCHA, Extended finite automata, BOTS, Security, System usability scale, Effectiveness, Efficiency

I. Introduction

Some internet resources and services are attacked by Bots, which are automated programs [1]. Bots can perform behaviors like humans with no method to distinguish them from human action. It can run a series of scripts that perform (good/Malicious) tasks that can be completed on the internet that don't require human interaction. In the past, online social network applications, for example, hacking email accounts by using a combination of password and Facebook become hacked by social bots. To prevent all of this, we use CAPTCHA (Completely Automated Public Turing Test to Tell Computers and Human Apart) [2] to protect emails and other webpages. CAPTCHA is a challenge response technique which provides a test that is difficult to answer by bots and it is easy to answer by users. There are several CAPTCHA techniques that can be divided into CAPTCHA based on Text [3,4,5], CAPTCHA based on Image [6,7,8], CAPTCHA based on video or CAPTCHA based on audio [9]. Designers of CAPTCHA must equilibrium between two major factors: The Usability to validation of participants and the Robustness versus the spammer. In this paper, we intend to develop a new technique of CAPTCHA known as XFA CAPTCHA for protecting webpages and online social networks against harm attacks. XFA which augments traditional finite state automata (FSA) with a finite scratch memory used to remember various types of information relevant to the progress of signature matching. Since an XFA is an FSA augmented with finite scratch memory, it still recognizes a regular language, albeit more efficiently than an FSA. Our technique is relayed on the functionality of the extended finite automata (XFA) Graph approach as a common automata type for developing the tests of XFA CAPTCHA [7]. The rest of this paper is organized as Section II presents the related works, Section III presents our proposed XFA CAPTCHA mechanism, Section IV presents the

evaluation and experimental results, Section VII formulates the Conclusion of this work.

II- REALTED WORK

In this section, we will spotlight on various types of CAPTCHA which rely on non-optical character recognition (non OCR) and optical character recognition (OCR) based [11]. This part is not proposed to be a comprehensive study of all research. We spilt CAPTCHAs into two parts, cross ponding to their proficiency required to answer them: 1-based on text, when text detection is required, and 2-based on image, the ability of the user to detect pictures. Nowadays, Google introduced no CAPTCHA, a system that uses an advanced risk analysis, back-end that considers the engagement of the user and requires the user to enter either a text or an image defy [12].

A. CAPTCHA based on text

Show an obscure word included in a picture, and tells the participant to indicate and write it, often appears in a text box. Baird et al. [13] In 2002, the earlier CAPTCHA based on text was introduced. Many other researchers worked on this type of design after the first suggestion. After this first suggestion, many other researchers worked on this type of design. Many researchers spot light on progress in the flexibility versus automated hackers [14,15]. Recently, CAPTCHA based on text has been more used [16]. We introduce two examples of CAPTCHA based on text, as CAPTCHA Star [40], does not require using a keyboard to type their answer: ICAPTCHA [17] and DDIM-CAPTCHA [18]. The researchers of ICAPTCHA [19] spotlight on their efforts to avoid the relay attacks [20]: for example, when a spammer uses an external paid person for solving the CAPTCHA. This CAPTCHA is based on text to calculate and analyze the interactions that the user do while solving the test. I CAPTCHA asking the user with a traditional obscure word. For every word, the user has to use a series of obscure letters to form her or his answer. I CAPTCHA validation works on two level fronts. The first one, the validation of the answer, distinguishes between a genuine user and an automated script. The second one, the time interleaves after pressing any button UN masks the user's legality from external users. Although, considering this kind of UN masking weak, because of the cumin of the network connection can affect the calculation of the interspersion times. I CAPTCHA shows the participant a little set of electing characters that compose the answers of the test. However, this technique improves usability while also raising the average of threatened attacks that Optical Character Recognition (OCR) application. The design of CAPTCHA presented by Ye et al. [21] (Which is called a DDIM - CAPTCHA) includes obscure terms such as traditional CAPTCHA based on text. The major distinct from the other design by the participant can answer a test: by asking the participant to write the solution, this type of CAPTCHA requests the participant to select the right character from a group of characters into a "box of solution". Letters in a grouping of Characters are overlapped to each other, so the participant must fixed react to the group of characters to pick the character she/he wants. However, re-CAPTCHA [22] is the most popular type that is based on text. A- Usability features: The first execution of CAPTCHA based on text has a short time for completion and a rising success rate for legality users. The prescript to answer a CAPTCHA based on text is easier to understand. Actually, they don't need any knowledge of the participant, anticipate the ability to read and use a keyboard to write the solution, anticipate for particular designs an example, I CAPTCHA [19]. However, typing the solution with a keyboard wears away the CAPTCHA usability on a smartphone. B-Attacks: The most common way to automatically answer CAPTCHA based on text by using Optical Character Recognition software. Designers of CAPTCHA and spammers took part in a combat of intelligence. This combat drive to make enhancement of Optical Character Recognition software, however, making Optical Character Recognition more effective bluster [23] to CAPTCHA based on text. A relay attack is another different effective approach to answering CAPTCHA: some organizations use time of real-person labor to answer CAPTCHAs [24]. This type has a high success rate [25]. The attack strategies versus CAPTCHA are based on text. It can be divided into:

1) send the test to paid persons that can answer it
2) If the solution is a word of sense, use software for optical character recognition with the combination of a dictionary.
3) Use optical character recognition software on a single character respectively.
4) Word segmentation, in order to guess a single picture for each letter.
5) Removing line which can be added as a delphinium to the process of segmentation.
6) Filling the space within each letter, to enhance the effectiveness of optical character recognition.
7) Repairing letters outline by repair cracked lines. This technique affects analyzing spaces between pixels. The Spammer integrates a pair or more of these attack mechanisms to reach a high rate of success. Designers of CAPTCHA respond to

these attacks with many improvements to relieve their effectiveness.

This type of CAPTCHA that is used to protect web pages and Online Social Networks versus spammers. We will introduce some mechanisms which are able to attack, for example an algorithm based on shape recognition [20], an algorithm based on image segmentation [25]. Various CAPTCHA mechanisms have been proposed for protecting resources and web pages from spammers based on novel designs.

B. *CAPTCHA based on image*

Asking the user to observe picture or to react with objects displayed on screen to detect the answer. Dislike CAPTCHA based on text, every CAPTCHA based on image has a different design from each other. So, CAPTCHA which appears to the participant at first time requires more tension to know how it works. Research proves that CAPTCHA depends on image are highly estimated by participants [27]. Actually, CAPTCHA depends on image had a higher rate of success and they have little quarreler than CAPTCHA depends on text [28]. We divided CAPTCHA based on image into three subcategories: motion, static and interactive. One of the delegates static CAPTCHA depend on image was Asirra [11]. Asirra asks the participant to differentiate between dogs and cats, from several different pictures picked from web page example of Asirra shown in figure 1. Another type is a Collage [29]: it needs to press in a given image, through 6 pictures. Deep CAPTCHA [28] asks the participant to arrange six 3d models of objects in the real world according to their size. Other designer spot light on CAPTCHA that depend on video other than static picture recognition. Such as, Motion CAPTCHA [30] by choosing a random video from a database, then asking the user to distinguish through performance done by the person in the video. For example, YouTube Videos CAPTCHA [31, 32]. Another type Play Thru [33] asks the participant to answer a generated mini-game. These kinds of games seek to select shapes on their right spots.

c) *Features of usability*

Since CAPTCHAs based on image have various types, so usability may be changed according to their design. CAPTCHA based on image does not need to use a keyboard. Because of this, users of smartphones and tablets like CAPTCHA based on image over CAPTCHA based on text [34, 35]. Game-based CAPTCHAs [23,25,26] is a new approach that is designed to be more easy to understand and simpler than other types of CAPTCHA. It quarrels the participant to answer easy games, for example CAPTCHA Star [28,29], and GISCH CAPTCHA [41,42]. The VIKAS server generates CAPTCHAs characters of a variable length containing alphanumeric characters. The CAPTCHA verification stores the key generated by the server throw using the key position of the virtual key. Without using noise and distortion make it easy to solve by bots, example of VIKAS shown in figure2 [46,47]. The Hear Act CAPTCHA audio-based, where users are required to listen to a voice with background noise and then identify and type the numbers or words that are read [47]. CAPTCHA based on Gesture [43] is a new generation of another type that is provided on smart phones and Tablets, such as, Srinivas et al in [44], developed a hand CAPTCHA based on gesture mechanism which requires recognition function and matching of pattern. Another type of CAPTCHA is Four-Dimensional Usability Investigation of Image CAPTCHA [45]. Their method depends on the usability for every design factor evaluated by four parts: effectiveness, eye tracking, efficiency, and satisfaction. The problem with it is the smallest number of users that use its only 37 users and it is made in a laboratory that is different from real-life scenes example, shown in figure 3. Another type of CAPTCHA based on human imagination is 3D CAPTCHA [48]. Table1 compares the speculation success rate of attacks in other CAPTCHA types.

Figure 1:example of Asirra CAPTCHA

Figure 2:example of VIKAS CAPTCHA

Figure 3: Image CAPTCHA employs a 3×3

Table 1:compare speculation rate of other CAPTCHA types

Mechanism of CAPTCHA	Probability success rate of Speculation Attack
Collage-CAPTCHA	16.60%
Deep-CAPTCHA	20.00%
Motion-CAPTCHA	25.00%
Video-CAPTCHA	30.00%
Jigsaw-CAPTCHA	6.66%
CAPTCHAStar!	9.00%
Videop-CAPTCHA	2,68%

III. THE PROPOSED XFA CAPTCHA

This part, will present a new generation of CAPTCHA which is called XFA CAPTCHA, a new mechanism for securing web pages versus spammers. The main functionality of the CAPTCHA based on XFA relay on two strategies:

1) The XFA automata Graph that is used to generate CAPTCHA's tests [7].
2) Clickable CAPTCHA [35,37]

We use these two types in order to improve the semantics of our new generation of CAPTCHA's test versus types of Bots. The main mechanism of this CAPTCHA is increasing level of satisfaction and usability for the participant. Whereas, security enhancement versus Bots. In the following, we prepare an overview of our design, architecture and methodology of the mechanism of our proposed XFA CAPTCHA. The XFA CAPTCHA architecture includes two important parts:

1) XFA CAPTCHA Generator: in this phase, the CAPTCHA system randomly gets the puzzle of our XFA CAPTCHA from the Database expecting a secure online service or social activities.
2) The Verification XFA CAPTCHA: In this phase, the system of CAPTCHA verifies and validates the selected answer, which sorts words that can be predicted from the XFA automata graph. The input answer is compared with the right answers in the Database displayed in Figure 4.

The main function of XFA CAPTCHA design relays on a very important strategy in automata which is called extended finite automata [7]. We use the finite automata graph in our designs to generate letters from different languages. In our proposed CAPTCHA, the user must follow arrows in order to select the correct answer. To make it more difficult for spammers (bots), the user must click on three buttons that contain the right answer to pass the test only in three minutes, not more. If the user clicks on wrong answer the CAPTCHA will change automatically to another one. However, when the user selects only one or two answers, the CAPTCHA will change to another one shown in figures 5,6,7.

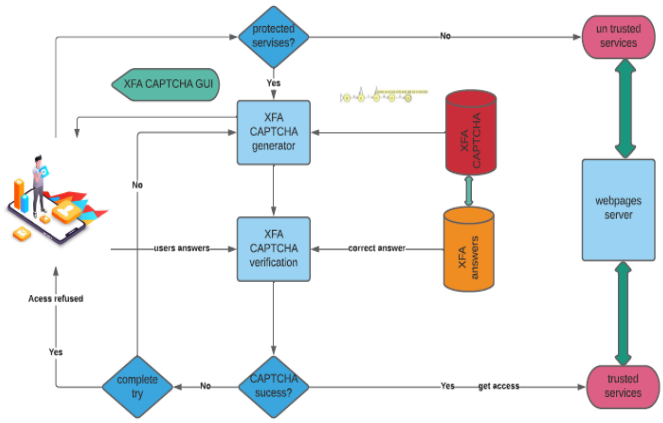

Figure 4: XFA CAPTCHA Architecture

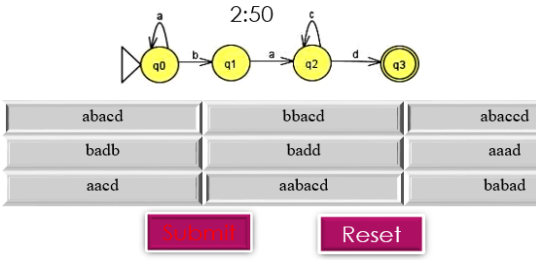

Figure 5: proposed XFA CAPTCHA

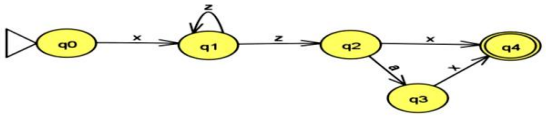

Figure 6: XFA CAPTCHA with four state

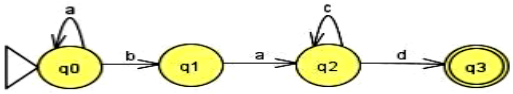

Figure 7: another example of XFA CAPTCHA of three state

IV. EVALUATION OF EXPERIMENTAL RESULTS

For each proposed system of CAPTCHA we must measure its security, usability [38] to

participants and robustness versus bots [39]. Good CAPTCHA must balance between robustness and usability [49,50].

A. *XFA CAPTCHA Implementation*

The algorithm used to generate new XFA CAPTCHA for every login user attempt is as follows: -

Step 1: **Start.**

Step 2: **For** all users Ui enter user name, email, age.

Step 3: Computer generates XFA CAPTCHA for registered user.

Step 4: The user will select the correct three answers according to XFA CAPTCHA.

Step 5: If the user selects the wrong answer, click erases.

Step 6: User clicks on the submit button.

Step 7: **If** the answers are correct **then**

The user passes the test.

Step 8: **Else**

The user can solve another test again.

Step 10: **End for.**

B. *Calculate usability*

In order to measure the evaluation of XFA CAPTCHA on webpages by calculating the usability, we selected nine CAPTCHA challenges (Q1, Q2, Q3, Q4, Q5, Q6, Q7, Q8, and Q9). A group of 255 participants are selected randomly. Chosen participants are divided into staff members, different learning levels and ages, students to solve our proposed CAPTCHA. We rated users into three groups according to their learning levels: intermediate education (70 users within ages between14-18), higher education (110 users within ages between19-26), and University graduated (75 users within ages between27-55). We invited the users through a public link to our research that we publish on the internet. Our research analyzed by taking into consideration the standard: ISO/IEC 9126-4 strategy to metrics of usability [41], which exhorts the usability must be calculated based on three factors; Satisfaction, Efficiency and Effectiveness.

1- *Effectiveness:* can be evaluated by calculating the Completion Rate of our CAPTCHA's challenges. It can be measured by allocating variable one if the participant can answer the CAPTCHA challenge and zero if the participant cannot answer. It can be evaluated as in (1).

$$effictiveness = \left(\frac{SU}{N}\right) \times 100 \qquad (1)$$

Whereas the SU represent the overall number of felicitous users who solved the CAPTCHA challenge, and N represents an overall participant number.

2- *Efficiency:* for the system of CAPTCHA is calculated according to Solve our proposed CAPTCHA in a given period of time. So, the total relative effectiveness using the time ratio taken by the participant who passes the test successfully according to the overall time taken by all participants. Can be evaluated as in 2.

$$Efficiency = \frac{\sum_{i=1}^{R}\sum_{j=1}^{N} n_{ij}\, t_{ij}}{\sum_{i=1}^{R}\sum_{j=1}^{N} t_{ij}} \times 100 \qquad (2)$$

Whereas, (R) is the number of all participants, (N)represents all numbers of CAPTCHA challenges, (nij) represents the result of answering CAPTCHA, the identifier (j)represents tests by participant (i); if the participant passes the challenge successfully, then (nij) will be one, if the user can't pass the test, then the value of (nij) will be zero, and (tij) storing spent time of the participant (i) to finish the task (j).

3- *Satisfaction:* can be calculated by representing some questions to a group of users. This makes it difficult to evaluate the perception of the users of simplicity of using the system to be measured. In this research, we used SUS (System Usability Scale) [44] which includes ten challenges about the perception of users of XFA CAPTCHA. A forty different participants divided into three categorized groups (intermediate education, Higher education and University graduated) respectively have been asked. The answers of users are classified into value one which means strongly disagree to value five which mean completely agree, then we clench the algorithm for calculating satisfaction quadrate to System Usability Scale (SUS). These results establish that XFA CAPTCHA has perfect satisfaction for participants, like the score curve of SUS is greater than the stringent satisfaction limits, which is sixty-eight according to the measure of system usability scale. Our results to measure

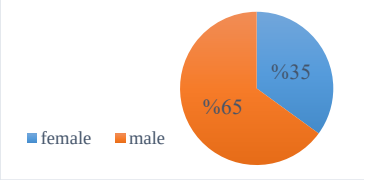

Figure 8: gender percentage

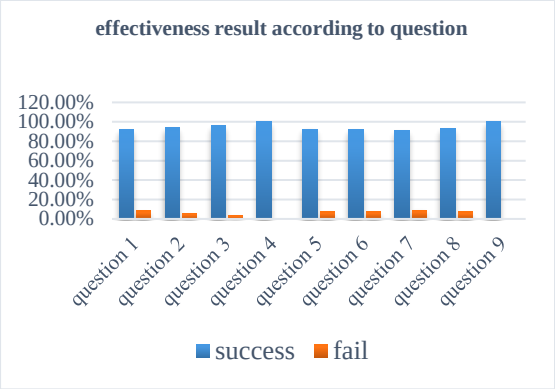

Figure9: effectiveness of XFA CAPTCHA

Figure10:RE-Efficiency for XFA CAPTCHA test

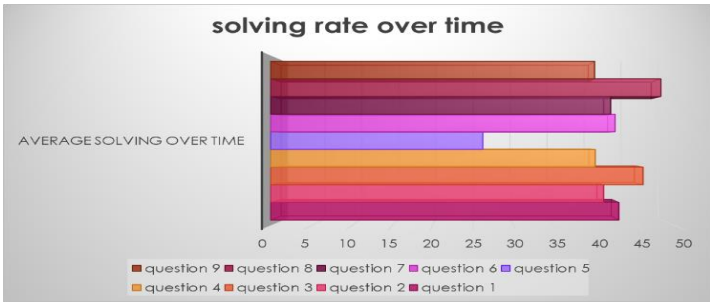

Figure 11: Average solving rate over time for XFA CAPTCHA

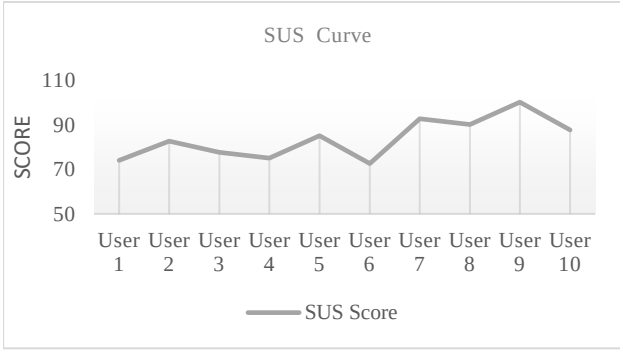

Figure 12: system usability scale for XFA CAPTCHA

effectiveness, satisfaction, ratio for solving time and efficiency of the XFA CAPTCHA are drawn in figures 8,9,10,11,12 respectively. Comparison between XFA CAPTCHA and other types shown in table 2.

Table 2: comparison between our CAPTCHA and others

	Effectiveness	**Efficiency**	**Satisfaction**
A Captcha-Based Graphical Password with Strong Password Space and Usability Study	success rate 1st:37% 2nd:35% 3rd:21% Fail:6%	Not calculated	Not calculated
Necklace CAPTCHA	Success rate 95.6% Fail:4.4	93.33%	Higher than 68
Four demission investigation CAPTCHA [45]	Success rate 92.03% fail 7.97%	-	higher
XFA CAPTCHA	Success: 94.99% Fail: 5.01%	97.8	92.5%

C. Security and Robustness Evaluation

The strength and weakness of any type of the system of CAPTCHA are calculated by how extremely the speculation of CAPTCHA can be solved by a spammer. Because of this challenge, we represent the toughness of XFA CAPTCHA versus speculation of attacking using the Binomial Distribution function as in 3.

$$p(x) = \frac{N!}{X!(N-X)!} P^X Q^{N-X} \qquad (3)$$

Whereas N represent number of all words that can be provided for solving automata of XFA CAPTCHA, X represents the number of correct words that represent the solution of the test, P represents the probability of passing the test, and Q equal to (1-P) which represent the probability of failed in any test. Each result is evaluated from calculating the Binomial Distributed Function for the nine XFA graphs of the XFA CAPTCHA is shown in Figure 13,

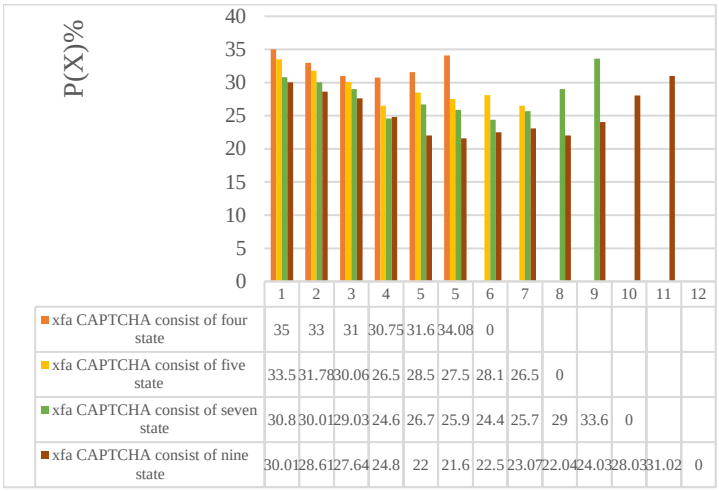

Figure 13: speculation of correct answer for XFA CAPTCHA

The amount in the yellow column shows the smallest number of speculation spam the level of probability for every XFA CAPTCHA graph. However, the Binomial Distributed function is used to measure the probability of correct answers of a given word of the XFA CAPTCHA model. It is necessary to arrange every word in the correct position. For example, bots aren't defying to guess words of the answer of different any CAPTCHA, However the challenge of sorting every word in the correct order to solve the CAPTCHA tests. So we must change the Binomial Distributed Function P(X) to normalize the function NP(X) as in 4. Reaching the equilibrium between security and usability of XFA CAPTCHA requires defy access to predict three words for passing the CAPTCHA challenge shown in table 1. We compared the results between XFA CAPTCHA and other types of CAPTCHA approaches according to the toughness and speculation attack passing probability is shown in Table 1.

$$NP(X) = \frac{P(X)}{X!} \quad (4)$$

VII. CONCLUSIONS

We present a generic mechanism for converting regular CAPTCHA based on text into image and clickable CAPTCHA. Our user, study shows that our XFA CAPTCHA can be solved faster than other types. However, XFA CAPTCHA doesn't rely on a static database of images. The security of our XFA CAPTCHA is reducible to the security of CAPTCHA based on text. Which is wasted time. Indeed, users were able to successfully solve rate up to 97. 8%and system usability scale, 92.5%. Finally, the majority of the users who solved the challenge in our contribution preferred XFA CAPTCHA rather than other types of CAPTCHA.

REFERENCE:

[1] B. Alessandro, and F. Bergadano. "Anti-bot strategies based on human interactive proofs." Handbook of Information and Communication Security. Springer Berlin Heidelberg, 2010, PP: 273-291.

[2] S. Kanika, and R. S. Chadha. "Captcha Generation for Secure Web Services." International Journal of Engineering and Innovative Technology (IJEIT), Volume 2, Issue 10, April 2013.

[3] Usmani, Atiya, et al. "New Text-Based User Authentication Scheme Using CAPTCHA." Information and Communication Technology for Competitive Strategies. Springer, Singapore, 2019. 313-322.

[4] E.Bursztein, , M.Martin, ,and J.Mitchell, (2011, October)."Text-Based CAPTCHA Strengths and Weaknesses". In Proceedings of the 18th ACM conference on Computer and communications security (pp.125-138)

[5] H. Gao, H.Liu, D.Yao, X. Liu, ,and U. Aickelin, "An audio CAPTCHA to distinguish humans from computers." Electronic Commerce and Security (ISECS), 2010 Third International Symposium on. IEEE, 2010.

[6] Anju Bala and Baljit Singh Saini, "A Review of Bot Protection using CAPTCHA for Web Security,"(IOSR-JCE) IOSR Journal of Computer Engineering, Volume 8, Issue 6 (Jan. - Feb. 2013), 36- 42. .

[7] Smith, Randy, Cristian Estan, and Somesh Jha. "XFA: Faster signature matching with extended automata." 2008 IEEE Symposium on Security and Privacy (sp 2008). IEEE, 2008.

[8] Chen, Jun, et al. "A Survey on Breaking Technique of Text-Based CAPTCHA. " Security and Communication Networks 2017 (2017).

[9]Introducing "NoCAPTCHA reCAPTCHA". googleonlinesecurity. blogspot.co.uk/2014/12/are-you-robot-introducing-no-captcha.html, Dec. 2014.

[10] H. S. Baird, A. L. Coates, and R. J. Fateman. Pessimalprint: a reverse turing test. International Journal on Document Analysis and Recognition, 5(2-3):158–163, 2003.

[11] 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.

[12] 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.

[13] E. Bursztein, M. Martin, and J. Mitchell. Text-based CAPTCHA strengths and weaknesses. In Proceedings of the 18th Conference on Computer and communications security, pages 125–138. ACM, 2011.

[14] H. D. Truong, C. F. Turner, and C. C. Zou. iCAPTCHA: the next generation of CAPTCHA designed to defend against 3rd party human attacks. In Proceedings of the International Conference on Communications (ICC), pages 1–6. IEEE, 2011.

[15] Q.-B. Ye, T.-E. Wei, A. B. Jeng, H.-M. Lee, and K.-P. Wu. DDIMCAPTCHA: A novel drag-n-drop interactive masking CAPTCHA against the third party human attacks. In Proceedings of the Conference on Technologies and Applications of Artificial Intelligence (TAAI), pages 158–163. IEEE, 2013

[16] M. Motoyama, K. Levchenko, C. Kanich, D. McCoy, G. M. Voelker, and S. Savage. Re: Captchas-understanding captcha-solving services in an economic context. In Proceedings of the USENIX Security Symposium, volume 10, page 3, 2010.

[17] Akrout, Ismail, Amal Feriani, and Mohamed Akrout. "Hacking google recaptcha v3 using reinforcement learning." arXiv preprint arXiv:1903.01003 (2019).
[18] H. Gao, D. Yao, H. Liu, X. Liu, and L. Wang. A novel image based CAPTCHA using jigsaw puzzle. In Proceedings of the 13th International Conference on Computational Science and Engineering (CSE), pages 351–356. IEEE, 2010.
[19] H. Nejati, N.-M. Cheung, R. Sosa, and D. C. Koh. DeepCAPTCHA: an image CAPTCHA based on depth perception. In Proceedings of the 5th Multimedia Systems Conference, pages 81 90. ACM, 2014.
[20] K. A. Kluever and R. Zanibbi. Balancing usability and security in a video CAPTCHA. In Proceedings of the 5th Symposium on Usable Privacy and Security, page 14. ACM, 2009.
[21] Usuzaki, Shotaro, et al. "Interactive Video CAPTCHA for Better Resistance to Automated Attack." 2018 Eleventh International Conference on Mobile Computing and Ubiquitous Network (ICMU). IEEE, 2018
[22] AreYouAHuman - game based CAPTCHAs. http://areyouahuman.com, June 2013.
[23] G. Reynaga and S. Chiasson. The usability of CAPTCHAs on smartphones. In Proceedings of the International Conference on Security and Cryptography (SECRYPT), pages 427–434, 2013.
[35] R. Pakdel , N. Ithnin , M. Hashemi , CAPTCHA: a survey of usability features, Res. J. Inf. Technol. 3 (4) (2011) 215–228 2011
[24] Greene, Mecheal. Large scale captcha survey. Diss. University of Delaware, 2018.
[25] Chow, Yang-Wai, Willy Susilo, and Pairat Thorncharoensri. "CAPTCHA Design and Security Issues." Advances in Cyber Security: Principles, Techniques, and Applications. Springer, Singapore, 2019. 69-92.
[26] A. S. El Ahmad, J. Yan, and L. Marshall. The robustness of a new captcha. In Proceedings of the Third European Workshop on System Security, pages 36–41. ACM, 2010
[27] C. A. Fidas, A. G. Voyiatzis, and N. M. Avouris. On the necessity of user-friendly CAPTCHA. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, pages 2623
[28] Siripitakchai, Apichai, Suphakant Phimoltares, and Atchara Mahaweerawat. "EYE CAPTCHA: An enhanced CAPTCHA using eye movement." 2017 3rd IEEE International Conference on Computer and Communications (ICCC). IEEE, 2017.
[29] Agrawal, Vani, et al. "Web Security Using User Authentication Methodologies: CAPTCHA, OTP and User Behaviour Authentication." OTP and User Behaviour Authentication (January 6, 2019) (2019).
[30] H. Gao, D. Yao, H. Liu, X. Liu, and L. Wang. A novel image based CAPTCHA using jigsaw puzzle. In Proceedings of the 13th International Conference on Computational Science and Engineering (CSE), pages 351–356. IEEE, 2010.
[31] S. GlobalStats. Canvas (basic support). http://caniuse.com/#feat=canvas, june 2021.
[32] Yu, Junnan, Xuna Ma, and Ting Han. "Four-Dimensional Usability Investigation of Image CAPTCHA." arXiv preprint arXiv:1612.01067 (2016).
[33] Ranjith, G., et al. "Machine learning methods for the classification of gliomas: Initial results using features extracted from MR spectroscopy." The neuroradiology journal 28.2 (2015): 106-111.
[34] Abraham, Jean Marie, et al. "Organizational Costs and Benefits of a Health System Quality Improvement Intervention to Increase Aspirin Use for Primary Prevention of Heart Attack and Stroke." American Journal of Medical Quality (2020): 1062860620962572.
[35] Lorenzi, David, et al. "Towards designing robust CAPTCHAs." Journal of Computer Security Preprint (2018): 1-30.
[36] R. Kosara, C. G. Healey, V. Interrante, D. H. Laidlaw, and C. Ware. User studies: Why, how, and when? Computer Graphics and Applications, 23(4):20–25, 2003.
[37] C. J. Coit, S. Staniford, and J. McAlerney. Towards faster patternmatching for intrusion detection or exceeding the speed of Snort. In 2nd DARPA Information Survivability Conference and Exposition, June 2001
[38] J. Yan and A.S. El Ahmad, "Usability of CAPTCHAs, Or Usability Issues in CAPTCHA Design," Proc. 4th Symp. Usable Privacy and Security (SOUPS 08), ACM Press, 2008, pp. 44-52.
[39] J. Yan, A. S. El Ahmad, "Captcha Robustness: a Security Engineering Perspective ", Computer, vol.44, no. 2, pp. 54-60, February 2011, doi:10.1109/MC.2010.275.
[40] A.A. Chandavale, and A. Sapkal. (2012). Security Analysis of CAPTCHA. In Recent Trends in Computer Networks and Distributed Systems Security (pp. 97-109). Springer Berlin Heidelberg
[41] J. Mifsud " Usability Metrics A Guide To Quantify The Usability Of Any System" (online), http://usabilitygeek.com/usability-metrics-a-guideto-quantify-system-usability/, july 1, 2021, (access: 1 july 2021)
[32] H. Nejati,N.M. Cheung, R. Sosa, and D.C. Koh, (2014, March). DeepCAPTCHA: an image CAPTCHA based on depth perception. In Proceedings of the 5th ACM Multimedia Systems Conference, ACM, (pp. 81-90).
[43] Hasan, Walid Khalifa Abdullah. "A survey of current research on captcha." Int. J. Comput. Sci. Eng. Surv.(IJCSES) 7.3 (2016): 141-157.
[44] Nouri, Zahra, and Mahdi Rezaei. "Deep-CAPTCHA: a deep learning based CAPTCHA solver for vulnerability assessment." Available at SSRN 3633354 (2020).
[45] Li, Xiang, et al. "vrCAPTCHA: Exploring CAPTCHA Designs in Virtual Reality." Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems. 2021.
[46] Rao, Kameswara, Kavya Sri, and Gnana Sai. "A novel video CAPTCHA technique to prevent BOT attacks." Procedia Computer Science 85 (2016): 236-240.
[47] Vaithyasubramanian, S., D. Lalitha, and C. K. Kirubhashankar. "Enhancing website security against bots, spam and web attacks using l CAPTCHA." International Journal of Computers and Applications (2019): 1-7.
[48] P. Golle. Machine learning attacks against the asirra CAPTCHA. In Proceedings of the 15th Conference on Computer and communications security, pages 535–542. ACM, 2008
[49] A.A. Chandavale, and A. Sapkal. (2012). Security Analysis of CAPTCHA. In Recent Trends in Computer Networks and Distributed Systems Security (pp. 97-109). Springer Berlin Heidelberg
[50] J. Mifsud " Usability Metrics A Guide To Quantify The Usability Of Any System" (online), http://usabilitygeek.com/usability-metrics-a-guideto-quantify-system-usability/, july 1, 2021, (access: 1 july 2021)