VIKAS: a new virtual keyboard-based simple and efficient text CAPTCHA verification scheme

Ankit Thakkar*

Department of Information Technology,
Institute of Technology,
Nirma University,
Ahmedabad – 382 481, Gujarat, India
Email: ankit.thakkar@nirmauni.ac.in
*Corresponding author

Kajol Patel

Department of Computer Engineering,
Institute of Technology,
Nirma University,
Ahmedabad – 382 481, Gujarat, India
Email: 15MCEI21@nirmauni.ac.in

Abstract: Nowadays online transactions are becoming ubiquitous that must be protected from bots using different techniques, and CAPTCHA is one of them. Text-CAPTCHA preferred due to its simplicity amongst different types of CAPTCHAs. Text-CAPTCHA can be strengthened by adding some distortion to prevent bot-attacks but cause usability issues for humans. This results in multiple attempts by a user to gain access to the required service and may give frustration to the user. Hence, there is a need to design CAPTCHA which is easy for humans to recognise but difficult for bots. This paper proposes virtual keyboard-based simple and efficient text-CAPTCHA verification scheme (VIKAS) that makes CAPTCHA verification easy for humans but difficult for bots. VIKAS uses simple text-CAPTCHA and verifies the same using positions of the keys pressed by the user using an image-based virtual keyboard. VIKAS is sustainable against segmentation scheme, replay attacks and possible attacks with keyloggers.

Keywords: completely automated public Turing test to tell computers and humans apart; CAPTCHA; virtual keyboard; bots; position-based verification; response time analysis.

Reference to this paper should be made as follows: Thakkar, A. and Patel, K. (2020) 'VIKAS: a new virtual keyboard-based simple and efficient text CAPTCHA verification scheme', *Int. J. Information and Computer Security*, Vol. 12, No. 1, pp.90–105.

Biographical notes: Ankit Thakkar is working as an Associate Professor in the Information Technology Department at Institute of Technology, Nirma University. He received his BE in Computer Engineering from the North Gujarat University, MTech and PhD in Computer Science and Engineering from the Nirma University in 2002, 2009 and 2014, respectively. His research interests

include computational intelligence techniques, wireless sensor networks, and image processing. He is an Associate Editor for the *Swarm and Evolutionary Journal* of Elsevier. He has several papers to his credit and guiding three PhD scholars. He received a gold medal for securing the highest CPI during the MTech.

Kajol Patel completed her MTech in Computer Science and Engineering (Information and Network Security) from the Institute of Technology, Nirma University during year 2017.

This paper is a revised and expanded version of a paper entitled 'A simple and efficient text-based CAPTCHA verification scheme using virtual keyboard' presented at International Conference on Information and Communication Technology for Intelligent Systems (ICTIS-2017), Ahmedabad, Gujarat, India, 25–26 March 2017.

1 Introduction

The growth of online transactions are increasing day-by-day (Meola, 2017) with the growth and development of technologies, the internet (Statista, 2017) and web services. An attacker can have monetary benefit from an unauthorised accessing account of any user by guessing the password of the account through automated programs called bots. This can be avoided by using a completely automated public Turing test to tell computers and humans apart (CAPTCHA). CAPTCHA is a challenge-response test that differentiates humans from machine or computers. This CAPTCHA test is used in many applications such as to prevent spamming of comments on blogs; to protect website registration; to prevent creation of junk e-mails; to prevent automated polling by machines; to secure online transactions; to make fair use of free content downloading services; preventing dictionary and phishing attacks; etc. (CAPTCHA, 2017; Steeves and Snyder, 2009; Banday and Shah, 2011). The websites that do not use CAPTCHA, allows spammers and malicious automated bots to spread junk e-mails and grab thousands of free e-mail accounts (El Ahmad et al., 2010). These security threats may put forth legal liability and can harm the credibility of the organisation as well as shake the trust of the users. Almost all malicious soft agents automate the misuse of web resources that degrades the quality of service for genuine user (Fidas et al., 2011). Google, Yahoo, and Microsoft have deployed their own CAPTCHAs for years to protect their services against e-mail spam by making it challenging for spammers to generate free e-mail accounts (Yan and El Ahmad, 2011).

CAPTCHAs can be classified as text-based, image-based and audio-based CAPTCHA (Gao et al., 2017). Text-based CAPTCHA uses English letters and Hindu-Arabic numeral which is distorted using obfuscation techniques that make it easy for humans to recognise but may be difficult for bots to identify. Text-based CAPTCHAs are widely used (Bursztein e al., 2011) because of the simplicity of its working principle: Identification of text characters by a human. However, the usability of CAPTCHAs is affected by distorted text characters as these distorted characters are very difficult (or sometimes impossible) for humans to identify. This results in multiple attempts by the user to gain access to the required service. This results in frustration to the users (Yan and El Ahmad, 2008b).

The systems based on CAPTCHA has been subjected to many attacks that seek to compromise their efficiency. Many attacks are performed to recognise the characters in CAPTCHA using different types of techniques such as machine learning, shape context matching method, object recognition algorithms, Gabor filter-based techniques to name a few (Yan and El Ahmad, 2011; Mori and Malik, 2003; Chellapilla and Simard, 2004; Yan, 2016). This put forth the requirements of designing of a complex text CAPTCHA by adding a larger amount of distortion and noise. However, this complex text CAPTCHA makes it difficult for the human to pass the test in a single attempt. This results in multiple attempts which are frustrating to the users (Yan and El Ahmad, 2008b; Gafni and Nagar, 2016). Hence, there is a need to design a text CAPTCHA which is difficult for the bots and easy for humans to pass the CAPTCHA test.

1.1 Major contributions

The major contributions of the paper can be summarised as follows:

- This paper proposes *vi*rtual *k*eybo*a*rd-based simple and efficient text CAPTCHA verification *s*cheme named VIKAS that eliminates the use of input box to receive CAPTCHA response. The proposed approach VIKAS is an extension of the work presented in Patel and Thakkar (2018).
- The effectiveness of the VIKAS (uses a handwritten virtual keyboard) is tested with most recent work presented in Patel and Thakkar (2018) that uses ordinary (or normal) virtual keyboard.
- Response time analysis is presented that can be useful to differentiate between human and machine in future
- The proposed approach has been verified by taking exhaustive inputs from different users having different technical backgrounds and having age between 20 years to 50 years.
- The proposed approach is also statistically verified.

2 Related work

Text-CAPTCHAs have been widely used to defend against malicious programs. There are numerous techniques available for breaking text-CAPTCHAs and many attacks have been proposed. In Mori and Malik (2003) have proposed an approach for breaking Gimpy and EZ-Gimpy CAPTCHA. The main disadvantage of the Gimpy version of CAPTCHA was that it uses actual words rather than random strings. So, by examining the pattern of strings and using Gimpy's dictionary, the algorithm was designed to identify the actual words. In Moy et al. (2004) presented a correlation algorithm that matches the whole object to break EZ-Gimpy CAPTCHAs. The proposed approach has achieved a success rate of 99%.

In Yan and El Ahmad (2008a) presented new segmentation techniques to crack a number of text-CAPTCHAs including Microsoft CAPTCHA. Microsoft CAPTCHA uses a string of fixed character length to generate CAPTCHA that weakens the strength of the CAPTCHA. In addition to that distortion leads to usability issues of the CAPTCHA. The Microsoft CAPTCHA was broken by a simple segmentation attack with a success rate of 90%.

A leading online delivery and storage website named Megaupload deployed a new captcha. In El Ahmad et al. (2010) examined the security of this captcha and were able to break the CAPTCHA using automated segmentation attack with a success rate of 78%.

In the studies Naor (1996) have discussed Turing test-based verification scheme which is easy for the humans but difficult for bots. The protocol suffers from three round operation instead of a single round Naor (1996). A text-based CAPTCHA using phonemic restoration effect and similar pronunciation with an Asian accent is proposed in Goto et al. (2014). This approach cannot hide the first and last characters of the question and number of hidden characters in the question are capped to 34%. Effect of gender and educational background on the process of text CAPTCHA verification have been studied in Tamang and Bhattarakosol (2012). A multi-model CAPTCHA (Almazyad et al., 2011) consisting of an image which is labeled with a set of cursive text labels. In order to pass the human verification test, the user has to correctly identify the image by selecting the correct label correspond to the image rendered on the screen. A set of non-English pronounceable words used by BaffleText (Chew and Baird, 2003) to avoid dictionary attacks.

Automated handwritten CAPTCHA generation system is proposed in Ramaiah et al. (2014). This approach adds distortion and noise to the Sigma-Lognormal representation of a handwritten word. However, the proposed approach has the disadvantage of using pre-written words for the CAPTCHA generation. In Rusu and Govindaraju (2004), authors have proposed hand-written CAPTCHAs scheme as character recognition, word segmentation, and letter segmentation problem and shown that such problems are difficult to break in handwritten text compared to machine printed text.

A high-profile segmentation-resistant CAPTCHA scheme was designed and deployed in MSN's hotmail registration system (Simard et al., 2003). The algorithm presented in Simard et al. (2003) is based on the assumption that segmentation is difficult than the recognition. A low-cost attack on Microsoft CAPTCHA was demonstrated in Yan and El Ahmad (2008a) with a segmentation success rate of more than 90%.

With the help of the case study, different types of attacks on text CAPTCHA is demonstrated in Xiao and Zhang (2012). In addition to that, various suggestions were given to increase the difficulty in breaking text CAPTCHAs (Xiao and Zhang, 2012). In Lu et al. (2015) have proposed a method to segment connected characters. However, the accuracy of this new segmentation method decreases, if characters are seriously distorted (Lu et al., 2015).

A novel approach for automatic segmentation and recognition of the overlapped characters is proposed in Starostenko et al. (2015). The approach has achieved average segmentation rate up to 82% for reCAPTCHA 2011. In Fidas et al. (2011) have conducted a survey and shown that CAPTCHAs are difficult for humans to solve.

Most of the text-based CAPTCHAs are cracked by using machine learning techniques due to which more distortion and noise is added to make CAPTCHA complex. This kind of complexity affects usability and robustness of CAPTCHA because users have to make multiple attempts to gain access to the web service or website. This may give frustration to the user and reduce the interest of the user towards using a particular web service. A study has been carried out to investigate users' experiences and attitudes with different types of CAPTCHA tests (Gafni and Nagar, 2016). It is also suggested that the CAPTCHA test should be such that it protects web services from bots and not to exhaust persons with the difficult and confusing test.

Text CAPTCHAs is the most popular due to its simplicity. However, there is a need to increase security without compromising user experience. In this paper, virtual

keyboard-based simple and efficient text CAPTCHA verification scheme VIKAS is proposed. The proposed approach VIKAS makes difficult for bots to break the CAPTCHA and easy for humans to recognise the CAPTCHA characters. VIKAS is developed by considering future directions presented in Patel and Thakkar (2018).

VIKAS uses a hand-written virtual keyboard. Hence, character recognition, word segmentation, and letter segmentation problem are difficult for the proposed approach (Rusu and Govindaraju, 2004). In addition, the use of the virtual keyboard helps to avoid personal data interception (Kaspersky, 2013). It also provides protection against spyware and spoofing attacks (Agarwal et al., 2011). The virtual keyboard is printed with handwritten characters wherein each character is taken from the set of 55 samples. This makes difficult for a machine to recognise the character of a text-CAPTCHA.

The rest of the paper is organised as follows: proposed approach VIKAS is discussed in Section 3, testing and evaluation of the proposed approach along with response time analysis and a statistical test are presented in Section 4, and concluding remarks and future directions are given in Section 5.

3 VIKAS: virtual keyboard-based simple and efficient text CAPTCHA verification scheme

A bot attack can be reduced by increasing complexity of the text CAPTCHA. At the same time, complex text CAPTCHA can result in multiple attempts by the humans that may result in loss of interest to access required website/web service. Instead of adding noise to make complex CAPTCHA, the proposed approach VIKAS secures the response of the CAPTCHA challenge. VIKAS achieves this by eliminating the input box to receive the response of the CAPTCHA challenge. This is because almost all approaches found in the literature use a text box to receive the response of the CAPTCHA challenge either from human or bots. Few approaches in the literature have developed efficient segmentation and recognition technique to perform various attacks on text CAPTCHA. The proposed approach VIKAS has eliminated the use of text box to receive CAPTCHA response. Also, the response received from the client machine consists of the positions of the key pressed rather key value itself. Hence, the segmentation and recognition techniques fail for the proposed approach.

VIKAS uses the text CAPTCHA which is easy for humans to read and recognise. An example of the text CAPTCHA used by VIKAS is shown in Figure 2.

The working principle of the proposed approach is shown in Figure 1. A server generates a CAPTCHA string of a variable length consisting of alphanumeric letters. The server generates key positions of virtual keyboard and stores this positions for the verification of the CAPTCHA response as discussed later in this section. The use of virtual keyboard protects CAPTCHA string from keyloggers and spyware. The proposed approach VIKAS assumes homogenous screen size and resolutions for clients and server. The virtual keyboard will be rendered at the same position on the client machine as the server. The keys of the virtual keyboard are initialised with the handwritten alphanumeric letters which are randomly selected from the Chars74K dataset (de Campos, 2012). The use of handwritten characters makes the test between humans and computer more stringent. Humans have knowledge of handwritten characters and can recognise them easily than bots.

Figure 1 The working principle of the proposed approach (see online version for colours)

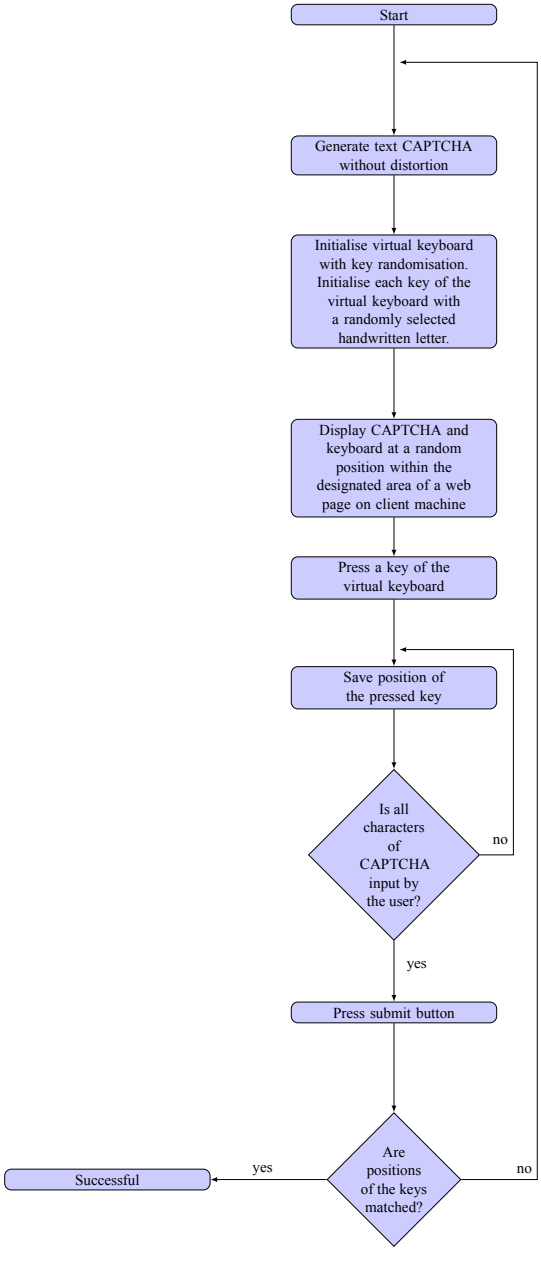
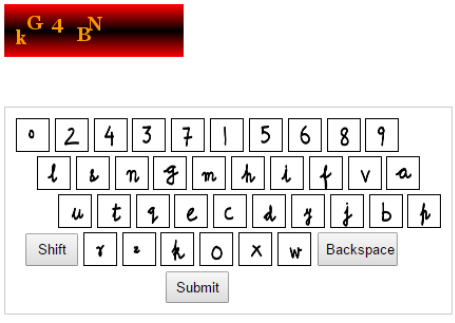
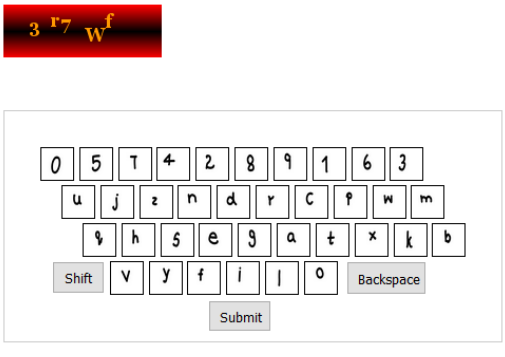


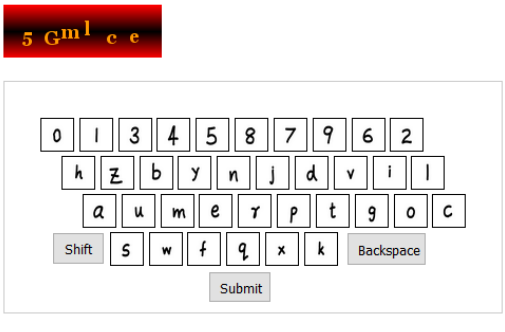
Figure 2 Different CAPTCHAs with the proposed approach, (a) CAPTCHA and handwritten virtual keyboard (b) CAPTCHA and handwritten virtual keyboard (c) CAPTCHA and handwritten virtual keyboard (d) CAPTCHA and handwritten virtual keyboard (e) CAPTCHA and handwritten virtual keyboard (see online version for colours)



(a)

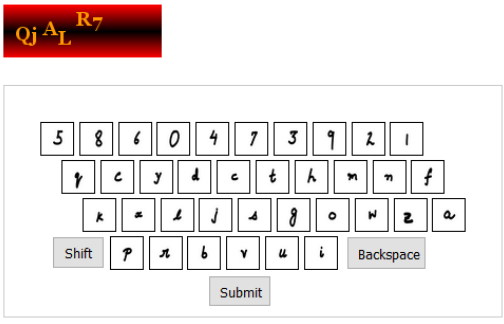


(b)



(c)

Figure 2 Different CAPTCHAs with the proposed approach, (a) CAPTCHA and handwritten virtual keyboard (b) CAPTCHA and handwritten virtual keyboard (c) CAPTCHA and handwritten virtual keyboard (d) CAPTCHA and handwritten virtual keyboard (e) CAPTCHA and handwritten virtual keyboard (continued) (see online version for colours)



(d)

(e)

The user on the client machine presses required keys one by one using the virtual keyboard until the user inputs all characters of the given text CAPTCHA. The positions of the keys are recorded as the user presses the keys. The stored key positions are communicated to the server as a response to CAPTCHA challenge when the user clicks on the submit button of the virtual keyboard. The server fetches the key positions of the CAPTCHA and compares it with the key positions received from the client. The user is granted access to the required service if key positions are matched, otherwise, a new CAPTCHA challenge is given to the user. The key position comparison process protects CAPTCHA from the segmentation and recognition techniques used to perform attacks using bots. A usability status for each and every CAPTCHA is also maintained on the server to protect CAPTCHA test from the replay attacks.

4 Testing and evaluation

The proposed approach generates variable-length text CAPTCHA without much noise so that users can easily recognise the text of the CAPTCHA. A sequence of text-CAPTCHA is shown in Figure 2. The server initialises the keys of the virtual keyboard using English handwritten characters randomly selected from Chars74K dataset (de Campos, 2012). The dataset consists of 64 classes (0–9, A–Z, a–z), 7,705 characters obtained from natural scenes, 3,410 handwritten characters and 62,992 synthesised characters from computer fonts de Campos (2012). This approach uses only handwritten characters from the Chars74K dataset that includes 55 sample per class. The proposed approach renders CAPTCHA and virtual keyboard at any place within the designated area as decided by the server.

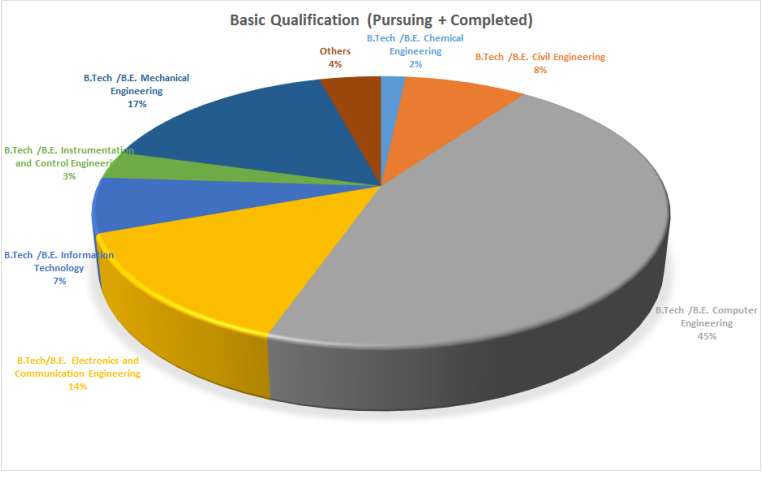
To verify the effectiveness of the proposed approach VIKAS, a total of 121 users are randomly selected. The selected users are faculty members, staff members, and students from different engineering backgrounds. Student users are pursuing their BTech, MTech or PhD in different engineering disciplines. The selected users are of age group between 20–50 years. The user distribution based on basic qualification, age group, and average usage of computers per week is shown in Figures 3–5, respectively. The size of each user group (in percentage) as per the basic qualification is between 2% to 45%. There are 78% users with an age group of 20–29, 17% users with an age group of 30–39, and 5% users are of an age between 40–49 years. The average computer usage per week (in hours) is shown in Figure 5. The average usage of computer per week (in hours) is in the range from one hour to forty hours per week, and more than 40 hours per week. The range is grouped with a bin size of five hours. The percentage of user distribution as per the average usage of computer is between 4% to 23%. Each user has responded with three to five CAPTCHAs. The results of the CAPTCHA verification process along with the time taken by the user to respond to CAPTCHA challenge is recorded. This response time is used to compute average response time taken by the user to input a single CAPTCHA letter. The same set of users is asked to repeat the entire process of CAPTCHA verification using the approach presented in Patel and Thakkar (2018). The approach presented in Patel and Thakkar (2018) uses a normal virtual keyboard and it is always available at the same designated place. One such CAPTCHA is shown in Figure 6. The proposed approach VIKAS differs from the approach presented in Patel and Thakkar (2018) by three ways:

1 VIKAS initialises keys of virtual keyboard with handwritten character data set while the approach presented in Patel and Thakkar (2018) uses normal virtual keyboard

2 VIKAS renders CAPTCHA and virtual keyboard at any place within the designated place while the approach presented in Patel and Thakkar (2018) renders virtual keyboard at the same designated place.

3 Response time analysis is carried out in this paper for VIKAS, the approach presented in Patel and Thakkar (2018) and the time taken by the machine to segment and recognise letters of the CAPTCHA using Tesseract Smith (2007).

Figure 3 User distribution as per the basic qualification (see online version for colours)



Boxplot (Krzywinski and Altman, 2014) is used to make the comparison of the response time and it is shown in Figure 7. It can be concluded that machine takes very less time to segment and recognise a single character of the CAPTCHA as compared to the average time taken by humans to recognise the character and input the same using virtual keyboard. This is because the CAPTCHA letters are simple and free from noise and distortion. It can also be concluded that human takes more time to input a single character using hand-written virtual keyboard compared to the normal virtual keyboard. This is because every time the user has to work with different handwritten characters that are positioned at different places requires a greater amount of recognition time.

Wilcoxon signed-rank test (Lowry, 2014) is performed on response time to statistically show that user takes different time to input a CAPTCHA response with VIKAS and the one presented in Patel and Thakkar (2018). The test concludes that the average time taken to input a letter with the hand-written virtual keyboard is significantly higher than the normal virtual keyboard as the p-value is less than 0.0001.

We have also analysed the result as per the user distribution [the highest qualification, age group, and average usage of computer per week (in hours)]. The average response time for different user groups as per the highest qualification, age group, and average usage of computer per week (in hours) is shown in Figures 8–10, respectively. It can be observed from the results that the time required to enter the CAPTCHA using a hand-written virtual keyboard is higher than that of the approach proposed in Patel and Thakkar (2018) for all the three types of user distributions. This is because of the virtual keyboard uses different placement of the characters along with different types of characters. The results are also consistent with the results presented for all users without any classification.

Figure 4 Agewise user distribution (see online version for colours)

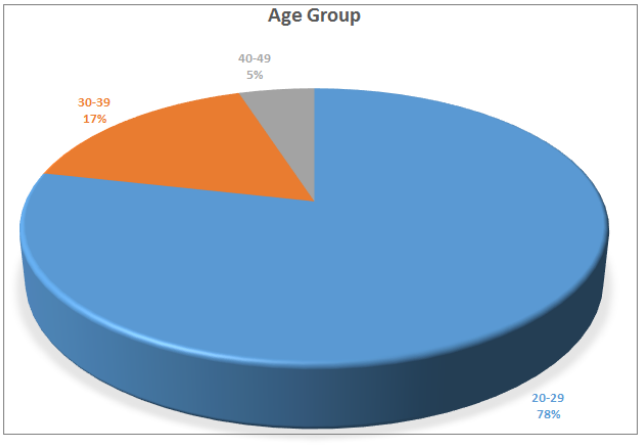


Figure 5 User distribution as per the usege of computer per week (in hours) (see online version for colours)

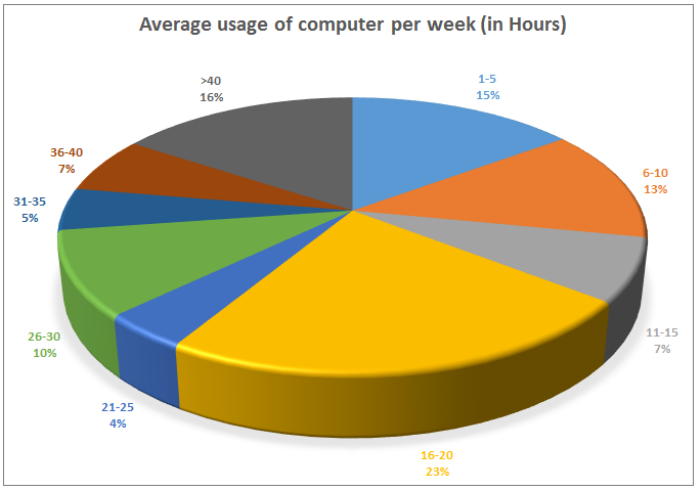


Figure 6 CAPTCHA and normal virtual keyboard (see online version for colours)

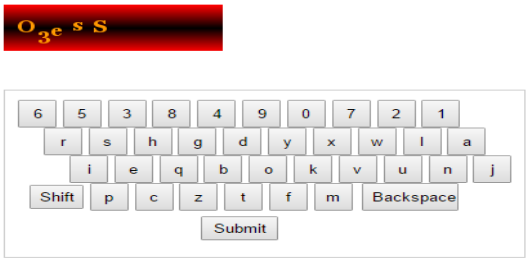


Figure 7 Average response time of VIKAS and approach proposed in Patel and Thakkar (2018) to input a single letter of CAPCHA alongwith average time taken by machine to decode a single CAPTCHA letter

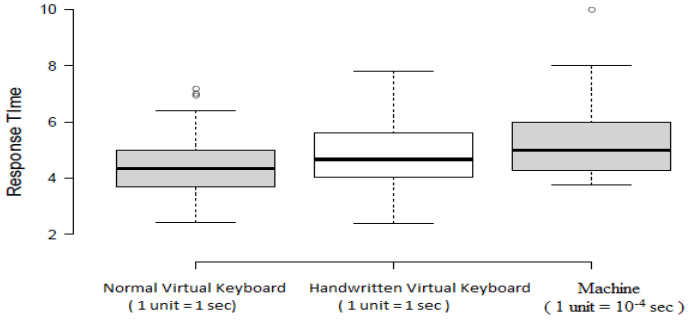


Figure 8 Average response time for different user groups as per the highest qualification (see online version for colours)

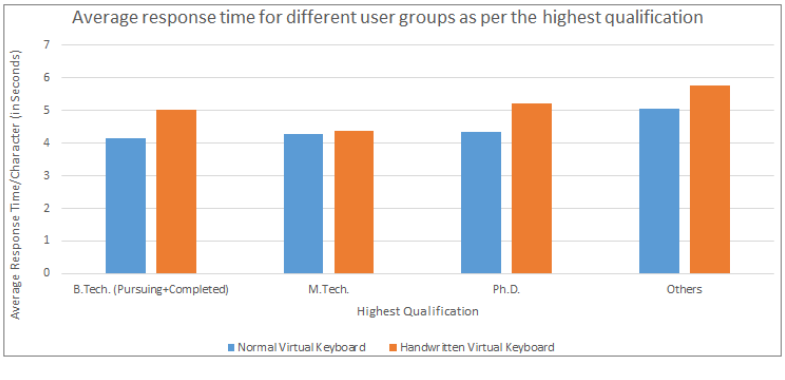


Figure 9 Average response time for different age groups (see online version for colours)

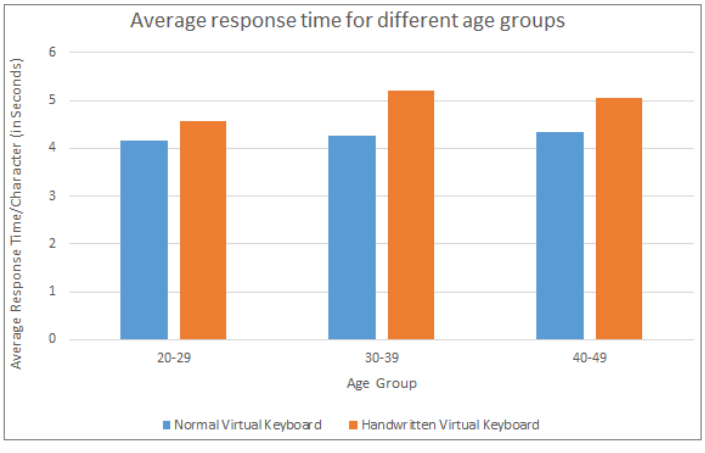
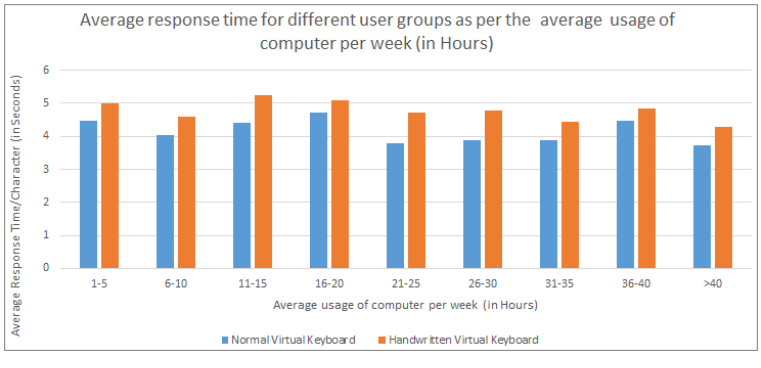


Figure 10 Average response time for different user groups as per the average usage of computer per week (in hours) (see online version for colours)



5 Concluding remarks and future directions

Web applications use CAPTCHA to protect systems from malicious bot attacks and differentiates humans from machines. This paper presented a virtual keyboard-based approach named VIKAS that effectively differentiates between human and machine. The proposed approach uses text CAPTCHA without noise and distortion that makes easy for human and machine to read. At the same time, VIKAS makes it difficult for bots to crack the CAPTCHA as the proposed approach has eliminated the use of text box to input CAPTCHA response. VIKAS also protects from different types of attacks performed by keyloggers

and spyware as it uses a handwritten virtual keyboard that can be rendered at any position within the designated area. It also protects from replay attack as the status of the CAPTCHA is maintained on the server. The proposed approach compares the position of the letters received as CAPTCHA response with the position of the letters of the CAPTCHA challenge generated on the server. The statistical significance of the proposed approach is also ensured by comparing it with the most recent approach.

In the future, the proposed approach can be designed to work with heterogeneous screen sizes, i.e., client and server use different screen sizes and/or resolution. This is one of the future directions of the proposed approach. The second future directions could be the design of a system using machine learning approach that can differentiate between user and bots on the basis of the response time taken by the human/machine to submit the CAPTCHA response. The third future direction is to analyse the effect of true random numbers on the proposed approach VIKAS.

References

Almazyad, A.S., Ahmad, Y. and Kouchay, S.A. (2011) 'Multi-modal captcha: a user verification scheme', in *2011 International Conference on Information Science and Applications (ICISA)*, IEEE, pp.1–7.

Agarwal, M., Mehra, M., Pawar, R. and Shah, D. (2011) 'Secure authentication using dynamic virtual keyboard layout', in *Proceedings of the International Conference and Workshop on Emerging Trends in Technology*, ACM, pp.288–291.

Bursztein, E., Martin, M. and Mitchell, J. (2011) 'Text-based CAPTCHA strengths and weaknesses', in *Proceedings of the 18th ACM conference on Computer and communications security*, ACM, pp.125–138.

Banday, M.T. and Shah, N.A. (2011) 'A study of CAPTCHAs for securing web services', *arXiv preprint arXiv:1112.5605*.

CAPTCHA (2017) *The Official CAPTCHA Site* [online] http://www.captcha.net/ (accessed 16 August 2017).

Chew, M. and Baird, H.S. (2003) 'Baffletext: a human interactive proof', in *International Society for Optics and Photonics, Electronic Imaging*, pp.305–316.

Chellapilla, K. and Simard, P.Y. (2004) 'Using machine learning to break visual human interaction proofs (HIPs)', in *NIPS*, pp.265–272.

de Campos, T. (2012) *The Chars74K Dataset: Character Recognition in Natural Images*, University of Surrey, Guildford, Surrey, UK.

El Ahmad, A.S., Yan, J. and Marshall, L. (2010) 'The robustness of a new CAPTCHA', in *Proceedings of the Third European Workshop on System Security*, ACM, pp.36–41.

Fidas, C.A., Voyiatzis, A.G. and Avouris, N.M. (2011) 'On the necessity of user-friendly CAPTCHA', in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ACM, pp.2623–2626.

Gafni, R. and Nagar, I. (2016) 'CAPTCHA – security affecting user experience', *Issues in Informing Science and Information Technology*, Vol. 13, pp.63–77.

Goto, M., Shirato, T. and Uda, R. (2014) 'Text-based CAPTCHA using phonemic restoration effect and similar pronunciation with an Asian accent', in *2014 17th International Conference on Network-Based Information Systems (NBiS)*, IEEE, pp.517–524.

Gao, H., Tang, M., Liu, Y., Zhang, P. and Liu, X. (2017) 'Research on the security of Microsoft's two-layer CAPTCHA', *IEEE Transactions on Information Forensics and Security*, Vol. 12, No. 7, pp.1671–1685.

Krzywinski, M. and Altman, N. (2014) 'Points of significance: visualizing samples with box plots', *Nature Methods*, Vol. 11, No. 2, pp.119–120.

Kaspersky (2013) *How and Why you Should Use the Virtual Keyboard?* [online] https://www.kaspersky.com/blog/how-and-why-you-should-use-the-virtual-keyboard/3040/ (accessed 5 August 2018).

Lowry, R. (2014) *Concepts and Applications of Inferential Statistics*.

Lu, P., Shan, L., Li, J. and Liu, X. (2015) 'A new segmentation method for connected characters in CAPTCHA', in *2015 International Conference on Control, Automation and Information Sciences (ICCAIS)*, IEEE, pp.128–131.

Meola, A. (2017) *E-Commerce and Online Payment Technologies Overview and Trends* [online] http://www.businessinsider.com/ecommerce-payment-technologies-overview-trends-2016-10?IR=T (accessed 16 August 2017).

Moy, G., Jones, N., Harkless, C. and Potter, R. (2004) 'Distortion estimation techniques in solving visual CAPTCHAs', in *Proceedings of the 2004 IEEE Computer Society Conference on Computer Vision and Pattern Recognition, CVPR 2004*, IEEE, Vol. 2, p.2.

Mori, G. and Malik, J. (2003) 'Recognizing objects in adversarial clutter: Breaking a visual CAPTCHA', in *Proceedings 2003 IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, IEEE, Vol. 1, p.1.

Naor, M. (1996) *Verification of a Human in the Loop or Identification via the Turing Test*, Unpublished draft [online] http://www.wisdom.weizmann.ac.il/~naor/PAPERS/human.pdf (accessed 16 August 2018).

Patel, K. and Thakkar, A. (2018) 'A simple and efficient text-based CAPTCHA verification scheme using virtual keyboard', in Satapathy, S. and Joshi, A. (Eds.) *Information and Communication Technology for Intelligent Systems (ICTIS 2017) – Volume 2. ICTIS 2017. Smart Innovation, Systems and Technologies*, Vol. 84, Springer, Cham.

Rusu, A. and Govindaraju, V. (2004) 'Handwritten CAPTCHA: using the difference in the abilities of humans and machines in reading handwritten words', in *Ninth International Workshop on Frontiers in Handwriting Recognition, IWFHR-9 2004*, IEEE, pp.226–231.

Ramaiah, C., Plamondonm, R. and Govindaraju, V. (2014) 'A Sigma-Lognormal model for handwritten text CAPTCHA generation', in *2014 22nd International Conference on Pattern Recognition (ICPR)*, IEEE, pp.250–255.

Starostenko, O., Cruz-Perez, C., Uceda-Ponga, F. and Alarcon-Aquino, V. (2015) 'Breaking text-based CAPTCHAs with variable word and character orientation', *Pattern Recognition*, Vol. 48, No. 4, pp.1101–1112.

Smith, R. (2007) 'An overview of the Tesseract OCR engine', in *Ninth International Conference on Document Analysis and Recognition, ICDAR*, IEEE, Vol. 2, pp.629–633.

Steeves, D.J. and Snyder, M.W. (2009) *Secure Online Transactions using a CAPTCHA Image as a Watermark*, 21 July, US Patent 7,565,330.

Simard, P.Y., Szeliski, R., Benaloh, J., Couvreur, J. and Calinov, I. (2003) 'Using character recognition and segmentation to tell computer from humans', in *Proceedings Seventh International Conference on Document Analysis and Recognition*, IEEE, pp.418–423.

Statista (2017) *Number of Internet Users Worldwide 2005–2017*. https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/ (accessed 16 August 2017).

Tamang, T. and Bhattarakosol, P. (2012) 'Uncover impact factors of text-based CAPTCHA identification', in *2012 7th International Conference on Computing and Convergence Technology (ICCCT)*, IEEE, pp.556–560.

Xiao, L-Z. and Zhang, Y-C. (2012) 'A case study of text-based CAPTCHA attacks', in *2012 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, IEEE, pp.121–124.

Yan, J. (2016) *A Simple Generic Attack on Text CAPTCHAS.*

Yan, J. and El Ahmad, A.S. (2008a) 'A Low-cost Attack on a Microsoft CAPTCHA', in *Proceedings of the 15th ACM Conference on Computer and Communications Security*, ACM, pp.543–554.

Yan, J. and El Ahmad, A.S. (2008b) 'Usability of CAPTCHAs or usability issues in CAPTCHA design', in *Proceedings of the 4th Symposium on Usable Privacy and Security*, ACM, pp.44–52.

Yan, J. and El Ahmad, A.S. (2011) 'Captcha robustness: a security engineering perspective', *Computer*, Vol. 44, No. 2, pp.54–60.