Journal
IJCSM

Iraqi Journal for Computer Science and Mathematics

Journal Homepage: http://journal.esj.edu.iq/index.php/IJCM
e-ISSN: 2788-7421 p-ISSN: 2958-0544

A Generating Distorted CAPTCHA Images Using a Machine Learning Algorithm

Saba Abdulbaqi Salman [1]*, Yasmin Makki Mohialden [2], Nadia Mahmood Hussien [2]

[1] Department of Computer Science, College of Education, Al-Iraqia University, Baghdad, Iraq.
[2] Department of Computer Science, College of Science, Mustansiriyah University, Baghdad, Iraq.

*Corresponding Author: Saba Abdulbaqi Salman

DOI: https://doi.org/10.52866/ijcsm.2024.05.03.023
Received March 2024; Accepted May 2024; Available online July 2024

ABSTRACT: CAPTCHAs (Completely Automated Public Turing Test to Tell Computers and Humans Apart) have become universal in web security systems to differentiate between automated bots and human users. This research presents a novel approach for generating and classifying distorted CAPTCHA images utilizing machine learning techniques. The process involves developing a random text and rendering it onto an image, introducing distortion for security. The proposed method involves developing CAPTCHA images by combining text rendering and controlled distortion techniques. These images are then utilized to train a random forest classifier for accurate recognition. A Random Forest classifier is employed to recognize the generated CAPTCHA images. Experimental results demonstrate the approach's efficacy in achieving high validation accuracy. The validation accuracy of the classifier demonstrates its effectiveness in deciphering distorted images. Thus addressing the challenge of creating CAPTCHAs that are both human-readable and resistant to automated recognition.

Keywords: CAPTCHA, Random Forest classifier, Security, Machine learning, Recognition, Image distortion.

1. INTRODUCTION

The CAPTCHA is the acronym for the Completely Automated Public Turing Test to Tell Computers and Humans Apart an automated security program algorithm. Initially, the 2003 proposal of Ahn et al. was designed to determine whether a user is a machine or a person. This project aims to generate and administer tests that are easily solvable by humans but challenging for computers. The CAPTCHA generation process involves combining an image with numerous randomly generated characters and then introducing interference noise to distort these characters, thereby increasing the difficulty of computer recognition [1] [2].

CAPTCHAs are extensively utilized as a security measure to prevent automated bots from engaging in malicious website activities. They serve as a safeguard to differentiate between human users and automated bots. Traditional CAPTCHA systems create visually distorted characters that human users can interpret, yet they remain perplexing for machines to comprehend [3].

The three main CAPTCHA recognition techniques are the feature analysis matching method [2], the shape context matching method [3], and the neural network-based method. Chellapilla and Simard discovered that characters may be detected using a neural network if a single character in the CAPTCHA identification image can be segmented thoroughly [5]. A feature segmentation technique based on the Gabor filter was proposed by Gao et al. It extracts the characters' features in the CAPTCHA in four different directions and then utilizes CNN to identify the combination of these features to identify the characters. Most text in CAPTCHA may be realized using this technique [6]. A new RCN model based on depth learning was proposed by George et al. It is a neural network model that mimics the imaging principles of visual nerve cells. The RCN model may efficiently solve CAPTCHA's twist, deformation, and adhesion, which can differentiate distorted and deformed items with a high recognition accuracy ratio [7].

This work aims to enhance CAPTCHA generation and recognition using a combination of random text generation, image rendering, distortion application, and machine learning classification by developing a method for generating CAPTCHA images with controlled distortion. Implement a Random Forest classifier for CAPTCHA recognition. Assess the recognition accuracy of the classifier on distorted images.

This paper focuses on a novel method for generating and classifying CAPTCHA images, enhancing security by creating complex images for computerized algorithms to decipher.

*Corresponding author: author@organization.edu.co

Our contribution is to enhance CAPTCHA generation by improving CAPTCHA security by introducing controlled distortion, making automated recognition challenging. Effective Recognition: Using a Random Forest classifier showcases its effectiveness in recognizing the generated CAPTCHA images.

The novelty of this paper is the proposed approach combines traditional CAPTCHA techniques with machine learning, enhancing generation and recognition. The controlled distortion introduces a new layer of security—this approach applies to online systems requiring robust protection against automated attacks. Examples include account registration, online voting, preventing content scraping, and maintaining user-friendliness.

The main general application fields for online user authentication are: The generated CAPTCHAs can be employed for user authentication during online registrations, login attempts, and other secure interactions. Preventing Automated Attacks: The complex and diverse CAPTCHA images are barriers against automated scripts that abuse online systems or perform malicious activities.

The outline of the paper in Section 2 related work; Section 3 proposed methodology. Section 4 Results and discussion; Section 5 conclusion.

2. LITERATURE REVIEW

2023, The authors of this paper propose a CAPTCHA recognition algorithm based on character segmentation and the Random Forest algorithm. It focuses on recognizing CAPTCHA codes by segmenting characters and using the Random Forest classifier [8].

2020, The authors of this paper introduce an efficient CNN model that uses attached binary images to recognize CAPTCHAs. The proposed model improves recognition accuracy and simplifies the structure of the CAPTCHA recognition system [9].

2020, The authors of this essay examine the safety of images. -based CAPTCHAs against attacks based on machine learning. It explores the effectiveness of optical character recognition (OCR) in recognizing distorted text in CAPTCHA images [10].

2020, The authors combat deep learning's threat to CAPTCHA security by introducing advCAPTCHA, a practical adversarial captcha generation system. This system, deployed on a large-scale online platform, effectively reduces attackers' success rates through novel negative learning techniques. Validation shows its feasibility in practical applications and resilience against diverse attacks. Leveraging user risk analysis, advCAPTCHA adapts by serving potential attackers and refining itself with its responses. It is a significant tool for generating robust captchas, offering real-world solutions and guidance for captcha developers and practitioners [11].

2004, this paper's authors describe distortion estimation techniques for solving visual CAPTCHAs. It focuses explicitly on solving EZ-Gimpy and Gimpy-r CAPTCHAs using object recognition [12].

3. THE PROPOSED METHODOLOGY

New methodologies will encrypt and protect most programs, enabling them to be utilized from anywhere, even without personal computers. Machine learning (ML) is essential for AI. Despite being a subset of AI, machine learning is often called AI owing to its learning and decision-making skills. AI development continued until the late 1970s. Modern business and research depend on machine learning for many companies. It improves hardware and software efficiency using algorithms and neural network models. Machine learning algorithms generate mathematical models using "training data" to make decisions without being explicitly programmed [13] [14] [15]. The suggested approach uses machine learning and security.

The primary goal of this suggested system is to secure user data and information by making it appear as if online user accounts are fully protected and validated before login. The proposed security system comprises two main steps: CAPTCHA image generation and random forest classification.

3.1 THE FIRST STEP, CAPTCHA IMAGE GENERATION

A random text composed of alphanumeric characters is generated as the basis for the CAPTCHA image. The text is solidified onto an image canvas using a chosen font. Controlled distortion is introduced through a noise plot, creating pixel shifts that contribute to image variability. This results in CAPTCHA images that are both human-readable and resistant to automated Recognition.

3.2 RANDOM FOREST CLASSIFICATION

The generated CAPTCHA images are transformed into feature vectors and used as training samples for a random forest classifier. The classifier is trained to associate image features with corresponding CAPTCHA texts, allowing it to recognize and categorize new CAPTCHA instances. In the classification phase, a Random Forest classifier is trained on the generated CAPTCHA images, where the images are flattened to feature vectors and labeled with the corresponding CAPTCHA text.

The proposed method uses the following Python libraries: pillow, numpy, and sklearn(ensemble, model_selection, metrics) for RandomForestClassifier, train_test_split, and accuracy_score. The Block diagram is shown in Figure 1:

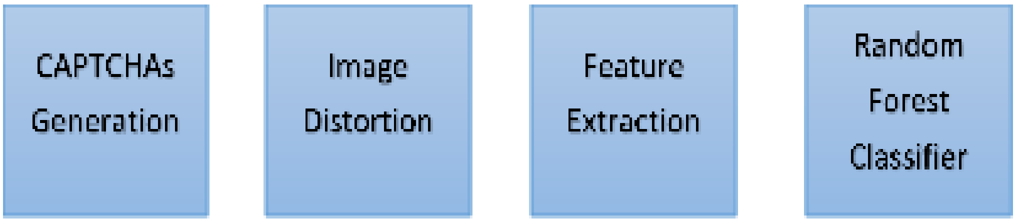


FIGURE 1. - **The block diagram**

The main steps of the algorithm are as follows:

- Generate a random text for the CAPTCH using a pool of characters and numbers.
- Create a distorted image from the text by applying a font file for the results of using TTF, Jazeera.tff. And applying BAUHS93.TTF, and others.
- Apply distortion. We applied a different distortion.
- Generate CAPTCHA images and labels for training.
- Generate training data and split it into training and validation sets.
- Train a Random Forest classifier.
- Validate the classifier on the validation set.

The secure features enable the system to evolve continually by changing the types of fonts and distortions used to generate images.

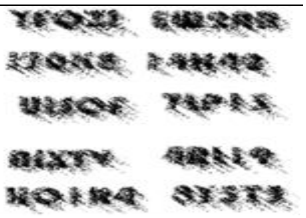
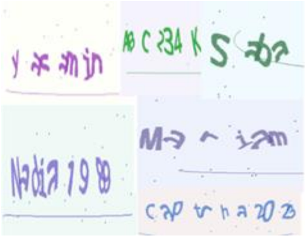
4. RESULTS AND DISCUSSION

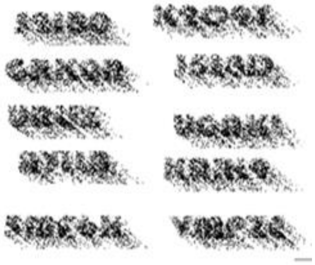
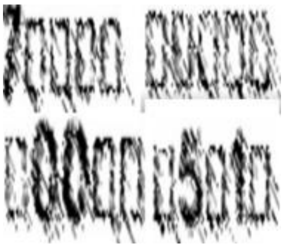
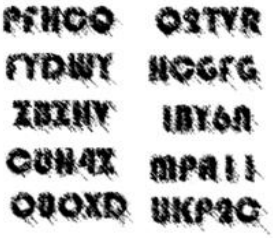
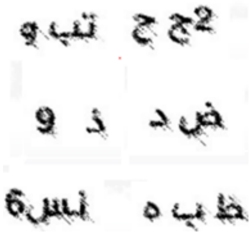
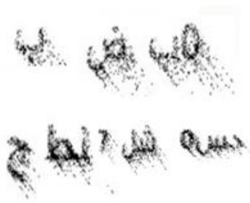
This section will discuss generating and classifying distorted CAPTCHA images using machine learning techniques. This work has been developed for various methods of authentication that state to maintain the utmost security. The model was applied to different fonts with varying degrees of distortion.

And each time, it gave different results. It turned out that the best ratio suitable for English letters and Arabic language was the purest. We also see a sample in the table when distortion values are not determined. Also, we noticed that the time spent generating images based on Arabic text was longer than that spent developing ideas based on English text.

TABLE 1. Shows the results of applying a set of parameters, as shown in the table.

Table 1. - **Result in 1 depending on different distortion value**

The setting for random characters	**a TTF font file used**	**Distortion**	**Generated CAPTCHA images**
'ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789'	BAUHS93.TTF	Selected randomly depending on image (width, height) *5	
	Agency FB.TTF	Selected randomly depending on the image (width, height) without any degree of distortion	

	BAUHS93.TTF	Selected randomly depending on image (width, height) *10	
	jazeera.ttf	Selected randomly depending on image (width, height) *2.5	
'ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789'	BAUHS93.TTF	**Selected randomly depending on image (width, height) *2.5**	
'	**(TTF)أبجد هوز.**	**Selected randomly depending on image (width, height) *2.5**	
أ ب ت ث ج ح خ د ذ ر ز س ش ص ض ط ظ ع غ ''ف ق ك ل م ن ه و ي٠ ١ ٢ ٣ ٤ ٥ ٦ ٧ ٨ ٩	**(TTF)أبجد هوز.**	**Selected randomly depending on image (width, height) *5**	

The Random Forest classifier achieves notable validation accuracy on the generated CAPTCHA images, demonstrating its capability to decipher distorted text successfully. This suggests the viability of utilizing machine learning for CAPTCHA recognition.

5. CONCLUSION

Today, artificial intelligence and machine learning have become the focus of many applications, as they have been adopted in developing the model presented in this paper. The proposed approach demonstrates the successful combination of CAPTCHA generation, controlled distortion, and machine learning-based recognition. The results indicate the potential for increased security and improved human-robot differentiation in online systems. The system is applied in different situations, with and without distortion. Furthermore, it is used for different fonts in Arabic and English. We suggest the same method by generating an audio rather than an image file.

Funding

The author's paper explicitly states that no funding was received from any institution or sponsor.

ACKNOWLEDGEMENT

The authors thank Mustansiriyah University (https://uomustansiriyah.edu.iq/) and Al-Iraqia University in Baghdad, Iraq, for their support in the present work.

.CONFLICTS OF INTEREST

The author would like to express gratitude to the institution for their invaluable support throughout this research project.

REFERENCES

[1] L. V. Ahn, M. Blum, N. J. Hopper, and J. Langford, "CAPTCHA: Using challenging AI problems for security," in Theory and Application of Cryptographic Techniques, Springer, Berlin, Heidelberg, 2003, pp. 294-311.

[2] E. Bursztein, A. Moscicki, C. Fabry, S. Bethard, J. C. Mitchell, and J. Dan, "Easy does it: More usable CAPTCHAs," in Proc. ACM Conf. Comput. Commun. Secur., 2014, pp. 1507-1518.

[3] G. Mori and J. Malik, "Recognizing objects in adversarial clutter: Breaking a visual CAPTCHA," in IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit., vol. 2, 2003, pp. II-II.

[4] S. S. Abdulbaqi, S. Al-Janabi, and A. M. Sagheer, "Security Attacks on E-Voting Systems Using Blockchain," Iraqi J. Comput. Sci. Math., vol. 4, no. 2, pp. 179-188, 2023.

[5] K. Chellapilla and P. Y. Simard, "I use Machine Learning to Break Visual Human Interaction Proofs (HIPs)," in Proc. Int. Conf. Doc. Anal. Recognit., 2004, pp. 265-272.

[6] H. Gao, J. Yan, C. Fang, Z. Zhang, and J. Li, "A Simple Generic Attack on Text CAPTCHAs," in Netw. Distrib. Syst. Secur. Symp. (NDSS), San Diego, CA, Feb. 2016.

[7] D. George et al., "A generative vision model that trains with high data efficiency and breaks text-based CAPTCHAs," Science, vol. 358, no. 6368, eaag2612, 2017.

[8] S. Kong and Y.-C. Chang, "A CAPTCHA Recognition Algorithm Based on Character Segmentation and Random Forest," J. Phys.: Conf. Ser., vol. 2504, no. 1, Art. no. 012036, 2023.

[9] A. Thobhani, M. Gao, A. Hawbani, S. T. M. Ali, and A. Abdussalam, "CAPTCHA Recognition Using Deep Learning with Attached Binary Images," Electronics, vol. 9, no. 9, Art. no. 9, 2020.

[10] F. H. Alqahtani and F. A. Alsulaiman, "Is image-based CAPTCHA secure against attacks based on machine learning? An experimental study," Comput. Secur., vol. 88, 101635, 2020.

[11] C. Shi et al., "Text Captcha Is Dead? A Large Scale Deployment and Empirical Study," in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., 2020.

[12] 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., vol. 2, 2004, pp. II-II.

[13] N. M. Khassaf and S. H. Shaker, "Image Retrieval based Convolutional Neural Network," Al-Mustansiriyah J. Sci., vol. 31, no. 4, pp. 43-54, 2020.

[14] M. S. Mahdi and S. N. Alsaad, "False Matches Removing in Copy-Move Forgery Detection Algorithms," Al-Mustansiriyah J. Sci., vol. 31, no. 1, pp. 47-53, 2020.

[15] G. S. Karam, "Blurred Image Restoration with Unknown Point Spread Function," Al-Mustansiriyah J. Sci., vol. 29, no. 1, pp. 189-194, 2018.