

## REVIEW ARTICLE

# A systematic literature review: Integrating deep learning models for visual-based CAPTCHA generation

Qian Wang<sup>1,2</sup>, Shafaf Ibrahim<sup>1</sup>, Zainura Idrus<sup>1,\*</sup>

<sup>1</sup> College of Computing, Informatics and Mathematics, Universiti Teknologi MARA, Shah Alam 40450, Malaysia

<sup>2</sup> Department of Artificial Intelligence, Leshan Vocational & Technical College, Leshan 614000, China

\* Corresponding author: Zainura Idrus, zainura@tmsk.uitm.edu.my

---

## ABSTRACT

The review conducted a systematic literature review (SLR) of the CAPTCHA generation field to analyze the attack resistance and user-friendliness of the existing CAPTCHA generation techniques. The survey reviewed 28 representative papers out of 1363 CAPTCHA generation-related papers from the Scopus academic database, outlining the image-based CAPTCHA generation techniques. The review employed multiple tables and graphs to assess the resistance to attacks and user-friendliness performance of CAPTCHA. The CAPTCHA is produced by using various generation techniques. The review addresses the following research questions: What deep learning generation techniques are employed for image-based CAPTCHA? Should the evaluation of CAPTCHA generation effectiveness prioritize security alone or consider attack resistance and user-friendliness simultaneously? The answers can provide comprehensive help and future work for scholars. The review further proposes possible future research directions, such as integrating various CAPTCHA generation technologies, including image processing techniques, deep learning algorithms, and human cognitive ability models, to generate more challenging CAPTCHA, effectively preventing attacks by robots or malicious software.

**Keywords:** CAPTCHA generation; deep learning; anti-recognition; user-friendliness; cybersecurity

---

## ARTICLE INFO

Received: 17 January 2024  
Accepted: 19 February 2024  
Available online: 7 June 2024

## COPYRIGHT

Copyright © 2024 by author(s).  
*Journal of Autonomous Intelligence* is published by Frontier Scientific Publishing. This work is licensed under the Creative Commons Attribution-NonCommercial 4.0 International License (CC BY-NC 4.0).  
<https://creativecommons.org/licenses/by-nc/4.0/>

## 1. Introduction

The threat of cybercrime has prompted people to pay attention to cybersecurity to protect networks from attacks. Around the world, many universities and scientific research institutions are concerned about cybersecurity. According to data, the cybersecurity market will be worth approximately US \$156.3 billion in 2022 and expands at a compound annual growth rate (CAGR) of 12.5%, reaching US\$403 billion by 2027. In the modern era of cybersecurity, CAPTCHA has emerged as an indispensable safety safeguard. It is extensively employed in web services and applications to prevent malicious attacks and intrusion by automated bots.

Since CAPTCHA was initially introduced by von Ahn in 2000<sup>[1]</sup>, CAPTCHA has become one of the most extensively used internet security measures. Particularly, due to their widespread popularity, simplicity in implementation, and cost-effectiveness. Text-based and image-based CAPTCHA are the two types that are most frequently used<sup>[2]</sup>. By presenting a challenge easier for human users but difficult for automated scripts, CAPTCHA aims to distinguish between programmers and human users<sup>[1,3]</sup>. CAPTCHA has evolved into a crucial security tool for mitigating cybersecurity risks. Besides countering distributed denial-of-service (DDoS) attacks, CAPTCHA

also prevents automated bots from exploiting online services<sup>[4]</sup>. Malicious coders, including hackers, collect CAPTCHA from websites using automated bots or crawling tools, and subsequently crack them which poses threats to websites and user accounts.

In CAPTCHA generation area, traditional image processing methods include add noise, rotation and geographic transformer to the CAPTCHA images<sup>[5,6]</sup>. However, CAPTCHA that is generated by classical image processing cannot defend against the attack of advanced deep learning algorithms. Therefore, it is essential to use advanced techniques to produce robust CAPTCHA. Deep learning technology is an end-to-end technology that performs excellently in many fields, such as medicine, computer science, and biology. Due to its excellent image processing and generalization abilities, deep learning technology is widely used in numerous popular fields, such as image generation<sup>[7]</sup>, image recognition<sup>[8]</sup>, object detection<sup>[9]</sup>, speech emotion recognition<sup>[10]</sup>, epidemic prediction<sup>[11]</sup>, question-and-answer systems<sup>[12]</sup>, and Twitter sentiment analysis<sup>[13]</sup>. Deep learning technology can provide robust solutions to various CAPTCHA generation models, providing a comprehensive reference.

While there exists an extensive body of review articles discussing CAPTCHA attack techniques<sup>[14-18]</sup>, limited attention has been devoted to the analysis of CAPTCHA generation models. Existing research results show that the attack algorithm based on deep learning algorithms designed by researchers can easily break text-based CAPTCHA<sup>[19]</sup>. The latest research<sup>[20]</sup> shows that text-based CAPTCHA has a lower solving time but higher success attack rate than image-based CAPTCHA. Image-based CAPTCHA has a faster response time and is recommended for potential use due to its responsiveness. Therefore, the anti-attack ability of CAPTCHA needs to be enhanced. Research results show that image or image-text CAPTCHA (graphic-based) can protect CAPTCHA and improve its robustness. Researchers<sup>[5]</sup> found that users prefer graphical-based CAPTCHA over text-based CAPTCHAs, despite their complexity. Furthermore, numerous authors employ advanced techniques for synthesizing or generating CAPTCHA, yet there is absence of common benchmarks and the distinctive designs of various CAPTCHA schemes. Thus, it is a challenge to compare the effectiveness of CAPTCHA<sup>[14]</sup>. Notably, the methods employed for CAPTCHA generation strategies lack a systematic and comprehensive analysis. Moreover, resistance to attacks is not the only measure of CAPTCHA performance. Another primary metric is user-friendly performance. Many researchers<sup>[21-23]</sup> only evaluate the attack resistance index of CAPTCHA, while few researchers focus on the user-friendly performance<sup>[24]</sup>.

Addressing the gaps in the literature, this research endeavors to identify gaps and propose research directions for future deep learning CAPTCHA generation technology, particularly image-based CAPTCHA. Through empirical findings, this study focuses on the image-based CAPTCHA generation algorithm and conducts a systematic literature review (SLR). In this study, three main research questions will be studied.

- 1) Deep learning technologies: What deep learning technologies have been utilized in the image-based CAPTCHA generation model?
- 2) Insight into previous studies: When evaluating the effectiveness of CAPTCHA, should both evaluation indicators (resistance index and user-friendly) be considered?
- 3) Future generative technologies and research directions: What will be the future direction of research and development in deep learning generative technologies to accommodate a CHAPTCHA model that is capable of generating anti-attack and user-friendly solutions?

In order to address the three research questions, this paper has been organized as follows: Section 1 briefly introduces the research questions. Section 2 outlines the methodology, providing details on the deep learning techniques and methods used to achieve the objectives. The results of the screening are presented in Section 3, followed by the analysis, discussions, and future work in Section 4. The conclusion is presented in the final section.

## 2. Methodology

### 2.1. Systematic searching strategies

The research is guided by PRISMA (Systematic Reviews and Meta-Analyses), which assists systematic reviewers in clearly stating the review’s purpose, actions taken, and findings<sup>[25]</sup>. CAPTCHA, an acronym with a specific professional meaning, represents Completely Automated Public Turing test to tell Computers and Humans Apart. Researchers used it as a constant expression of reverse tuning test. To conduct a thorough analysis and broaden the scope of the search, this study employed ‘CAPTCHA’ as searching keyword string. As a result, 1363 articles were discovered in the Scopus database (until 2023.12.29).

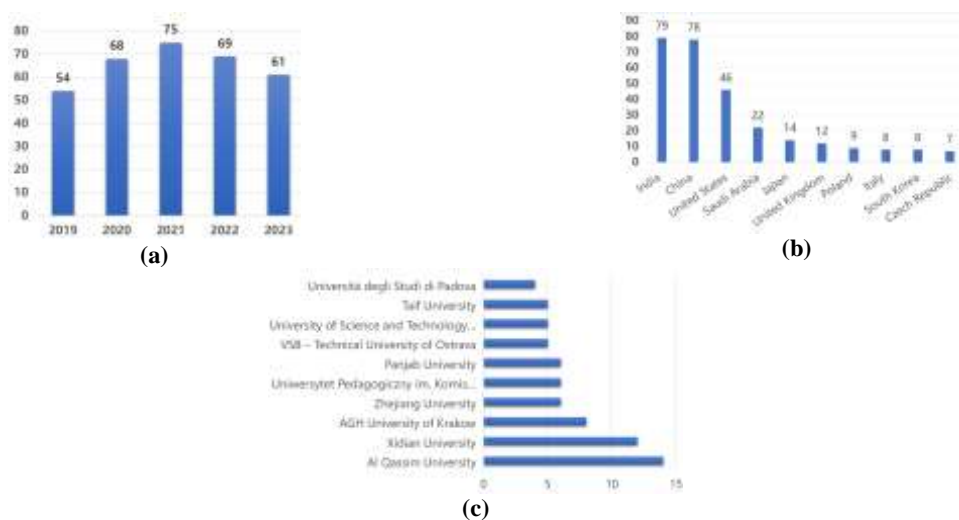
### 2.2. Screening

As the second step of the research, screening plays a crucial role. It systematically examines all literature to filter out any CAPTCHA-related literature that does not meets the standards. The screening process includes an automatic selection function of the database that filters all documents based on specific criteria for purposes, as shown in **Table 1**.

**Table 1.** Inclusion and exclusion criteria.

Criterion	Inclusion	Exclusion
Timeline	2019–2023	2018 and earlier
Language	English	Non-English
Document type	Journal articles and Conference paper	Conference review, erratum, book chapter, book series
Subject area	Computer science, engineering, mathematics	Decision sciences, social science, physics and astronomy and other areas

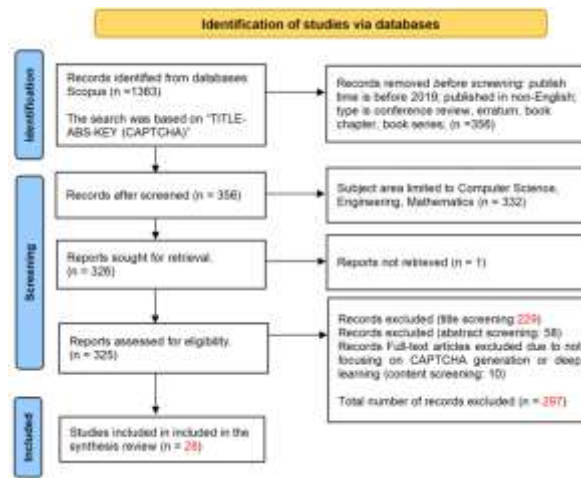
Firstly, to ensure the novelty of the literature, the review excluded publications with a publish date before 2019 and selected a total of 482 research articles from the last five years (2019–2023). To ensure language consistency, non-English papers were excluded from the review. Additionally, to increase the research value of the review, literature containing source types such as conference review, erratum, book chapter, and book series were removed, retaining only conference papers and journal articles. Finally, to ensure that the review was limited to the field of science, the authors restricted the subject area to computer science, engineering, and mathematics, and removed unrelated articles. Following these adjustments, at last 326 qualified articles have been identified for the next stage of review. **Figure 1** indicates the statistical data from Scopus dataset.



**Figure 1.** Statistical data from Scopus dataset. (a) number of articles in the past five years; (b) top 10 countries with the most articles; (c) top 10 research institutes with the most articles.

### 2.3. Eligibility

In the review of the literature, “eligibility” indicates the standards by which studies or other sources are chosen for inclusion. This is to ensure that the sources are relevant as well as appropriate to attain the objectives of the research. The flowchart of the research process is shown in **Figure 2**.

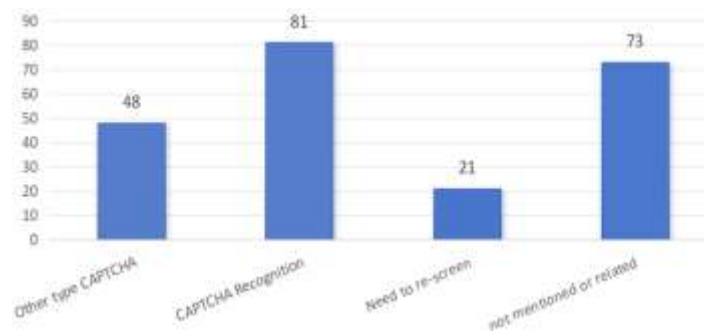


**Figure 2.** Flowchart of the search process.

To make the result accurate, the authors manually examined the records from article title to abstract, and the content of the full text. As an example, articles were removed when their title contains the key words, such as recognition, recognize, crack, solve, solver, animated, audio CAPTCHA. In addition, any reviewed articles were also removed. After the title screening process, a total of 229 articles were eliminated. All the title screen principles are shown in **Table 2**. The authors also analyze the number of these screened articles. The distribution is shown in **Figure 3**.

**Table 2.** Keyword principles of title screen.

Other type CAPTCHA	CAPTCHA recognition	Need to re-screen	NOT mentioned/related
Combined cognitive ability	Attack/Attack against	Challenge-response	Dataset
3D/Animated CAPTCHA	Solver/ Generic Solver	Usability/Robustness	DDoS attack
Games/gestures CAPTCHA	Recognition/recognize	Security, usability	Secret-Key sharing
Bio/ Animated CAPTCHA	Captcha Recognition	Image design	PIN Authentication
Audio/Bundled CAPTCHA	Breaking CAPTCHA	Website protection	Online Banking
Behavioral/Devanagari	Crack/captcha breaking	Enhance/Protect	Education/Hardware
Eye Movements CAPTCHA	Solver for Breaking	challenge-response	-
Swahili/Hindi language	Image identification	-	-
Visually impaired	Attack/Attack against	-	-



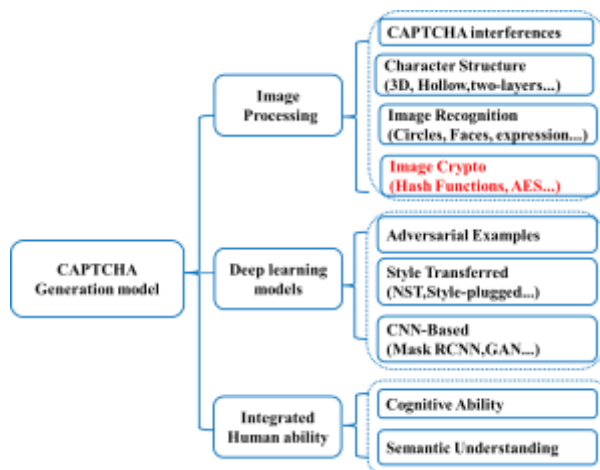
**Figure 3.** Distribution of articles excluded (title screening).

Since the abstract is indicative of the primary work and experimental results, the next screening focuses on it. Articles that do not provide indications of anti-attack and usability evaluations were eliminated. After reviewing the abstracts, a total of 58 articles were removed. Finally, the next step involved a thorough examination of the full text of the articles. During this process, ten records were excluded due to a lack of focus on CAPTCHA generation algorithms and the absence of evaluation indices. The total number of excluded records is 297.

### 3. Results

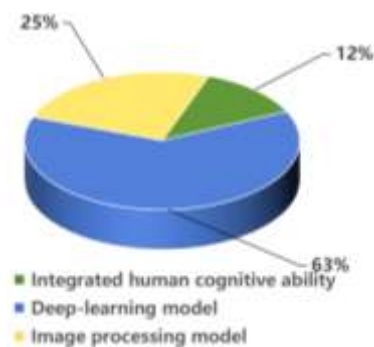
#### 3.1. Overview result

To ensure the security of the image-text CAPTCHA, researchers have employed various security mechanisms. One commonly utilized approach involves the incorporation of perturbations or the transformation of deep learning algorithms. Classical image processing and deep learning algorithms are two important approaches in producing CAPTCHA. Researchers incorporate human cognitive capacities to protect CAPTCHA from the end-to-end attack algorithms. Their study aims to produce both secure and user-friendly CAPTCHA by integrating human cognitive and semantic comprehension skills. Through careful reading, 28 articles highly pertinent to the subject of CAPTCHA were finally use for CAPTCHA generation. **Figure 4** illustrates the categorized subtopics found within these selected articles.



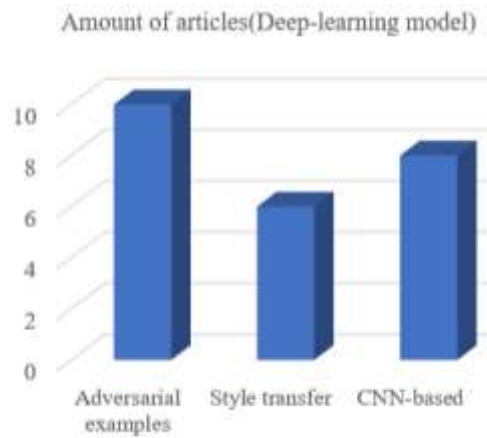
**Figure 4.** CAPTCHA generation techniques.

Among the total 28 research studies examined, eight researchers applied image processing models, while twenty researchers utilized deep learning models. Additionally, four researchers combined human cognitive skills and other deep learning models. After the authors examine the image processing generation models in detail, it was found that two researchers used image crypto technology to improve the security of the CAPTCHA innovatively. **Figure 5** indicates articles distribution chart of CAPTCHA generation models.

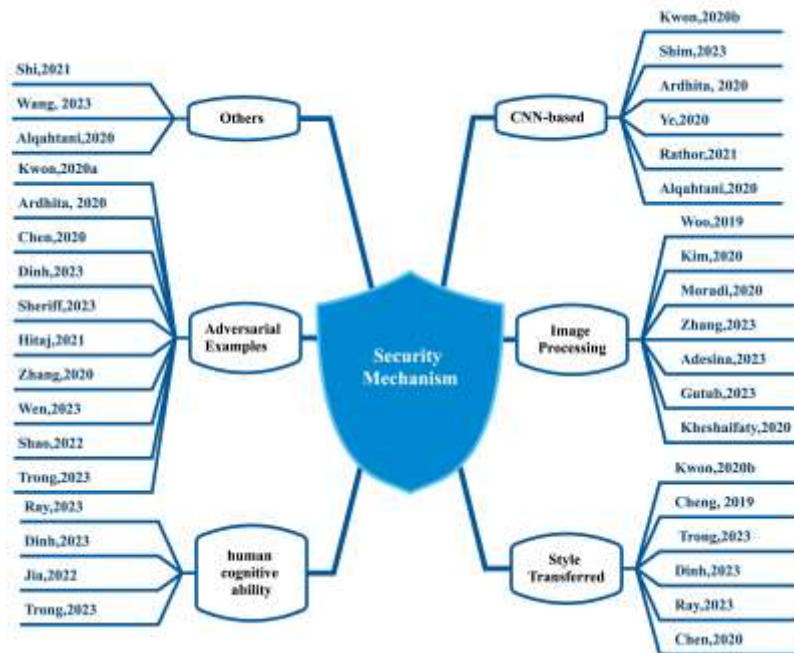


**Figure 5.** Articles distribution chart.

After a comprehensive review of the full text, the authors identified that ten researchers<sup>[8–9,22–29]</sup> employed adversarial examples techniques, constituting half of the total number using deep learning models. Additionally, six researchers<sup>[9,24,30–33]</sup> utilized style transfer models, while eight researchers<sup>[1,7,22,30,34–37]</sup> employed CNN-based methods. Notably, two researchers<sup>[1,37]</sup> adopted a comprehensive technical approach within the CNN-based methods. **Figure 6** illustrates the articles distribution chart of Deep-learning generation models and security mechanisms that were used in CAPTCHA generation models are shown in **Figure 7**.



**Figure 6.** Deep-learning generation models distribution.






**Figure 7.** Security mechanisms that researchers have used in CAPTCHA generation models.

### 3.2. Classical image processing models

Researchers found that using routine image processing techniques such as distortion, diverse colors, varying lengths, multiple fonts, and noisy lines, the production of CAPTCHA can have significant benefits in terms of enhancing online security and preventing automated spam and bots from accessing websites. Classical image processing approaches can integrate interference usage, character structure transformation, and special image recognition. Notably, the researchers proposed that the hash functions can encrypt the CAPTCHA image, providing a handy reference for image-based CAPTCHA generation<sup>[26,27]</sup> (See **Table 3**).

**Table 3.** Classical image processing generation models.

No.	Image processing	Methods	Example	References
1	CAPTCHA interferences	Noisy arcs or lines Diverse colors Variable length multi-fonts		[2] [28] [29] [19]
2	CAPTCHA character structure	3D characters Hollow Character distortion Dots Two-layer		[28,30,31] [32] [33] [29] [32]
3	Special image recognition	overlapping of circles and ovals Face image/Facial expression Other images		[34] [35–37] [20]
4	Image crypto	Hash functions, AES ...	-	[26,27]

### 3.3. Deep learning models

Besides classical image processing models to enhance the security of CAPTCHA, deep learning techniques, particularly Generative Adversarial Networks, provide a powerful tool for CAPTCHA image generation technology, making the generated CAPTCHAs more challenging and secure. In addition to image generation, deep learning technology is widely applied in other emerging areas such as question-answering systems, sentiment analysis, Internet of Things (IoT), object detection, intelligent cities, and cyber-attack predictions, presenting beautiful developments<sup>[12,13,38–42]</sup>. The studies have applied advanced deep learning algorithms, demonstrated attractive research directions and areas, and provided unique contributions to the future applications of deep learning. For instance, Gutub and his esteemed research group<sup>[38]</sup> utilized a CNN-LSTM deep learning model for sentiment analysis of social media Twitter. Also, they<sup>[12]</sup> mentioned that deep learning in question-answering systems is on the rise, pointing out many research directions involving deep learning technology.

While deep learning technology demonstrates strong generalization and excellent performance in many fields, the current research gap lies in identifying specific deep learning algorithms that can be applied in captcha generation algorithm models, along with their respective advantages and disadvantages. We have compiled the following review **Table 4** through analysis and comprehensive reading of 28 selected articles.

Currently, the deep learning technology applied in the CAPTCHA-generating algorithm can be used to produce robust text or image-based CAPTCHA. From **Table 4**, the authors found that Adversarial examples, style transfer, CNN-based algorithms were the main deep-learning CAPTCHA generation techniques. These advanced deep learning techniques are mainly used in image-based CAPTCHA generation models, focusing on image generation. According to the study, image-based CAPTCHA is more popular than text-based CAPTCHA<sup>[5]</sup>. Thus, besides security measurement, the user-friendly performance is also considered in most of the research<sup>[24,33,43–48]</sup>. This indicates the tendency to balance the security and user-friendly in CAPTCHA generation process. However, there still exists issues with identifying an appropriate balance between effectively avoiding attacks and maintaining user-friendliness<sup>[5,49,50]</sup>.

**Table 4.** Overview of the deep learning-based CAPTCHA generation models.

No.	Deep learning techniques	References/Authors, Year	Anti-attack	User-friendly
1	Adversarial examples	[21]	0%,45%	-
2	Adversarial examples	[24]	-	97.5%
3	Adversarial examples	[51]	50% to 99.4%	-
4	Adversarial examples	[52]	17.3%–28.1% (part)	-
5	Adversarial examples	[22]	Multiple data	-
6	Adversarial examples	[43]	Almost 0%	86% to 96.5%
7	Adversarial examples	[53]	√	-
8	Adversarial examples	[23]	√	-
9	Adversarial examples	[44]	lower than one millionth	91.25%
10	Adversarial examples	[45]	√	√
11	Style transfer	[46]	√	Qualitative
12	Style transfer/ NST	[47]	√	√
13	Style transfer/ NST	[45]	√	√
14	Style transfer/ NST	[52]	7.8%–17.3%(part)	-
15	Style transfer	[54]	Multiple data	-
16	Style transfer	[55]	√	-
17	CNN-based/DNN	[46]	3.5% and 3.2%	Qualitative
18	CNN-based/GAN	[56]	-	-
19	CNN-based/GAN	[24]	√	√
20	CNN-based/GAN	[33]	√	√
21	CNN-based/ RCNN	[57]	-	-
22	CNN-based/ ML	[58]	√	-
23	DL/ Integrated	[48]	5.35% to 28.4%	82.2%, 80.4%
24	DL/ Integrated	[14]	√	-

### 3.3.1. Adversarial examples

The concept of Adversarial Examples was first introduced by Szegedy et al. They discovered that introducing perturbation to the pixels of the original samples led to a significant fall in accuracy for deep learning models, including convolutional neural networks<sup>[59]</sup>. By introducing perturbations to the CAPTCHA image, the effectiveness of text-based or image-based CAPTCHA has been successfully enhanced. Ten Researchers that from China, India, United States, Czech Republic, Italy<sup>[21–24,43–45,51–53]</sup> utilized the adversarial examples to enhance the security of image CAPTCHA.

Kwon et al.<sup>[21]</sup> introduced adversarial examples technique for generating CAPTCHA images utilizing the FGSM, I-FGSM, and DeepFool algorithms. The results indicated that the FGSM method yielded a recognition rate of 0%, the I-FGSM method similarly achieved a recognition rate of 0%, while the DeepFool method achieved a recognition rate of 45%. These findings were obtained through experimentation with a Python dataset using TensorFlow as the machine learning library.

Ardhita et al.<sup>[24]</sup> developed a method for synthesizing a robust CAPTCHA generator that is resistant to attacks by image recognition algorithms. Sheriff et al.<sup>[22]</sup> introduced Deep CAPTCHA, a pioneering method in CAPTCHA generation that employs meticulously crafted adversarial noise to deceive deep learning classification models. This method ensured that information could be easily read by humans while also protecting against any efforts to modify or delete it. Their research investigated the domain of CAPTCHA



development, focusing on deep learning techniques, and demonstrated enhanced user-friendliness and security in comparison to conventional CAPTCHA.

Hitaj et al.<sup>[43]</sup> utilized an innovative CAPTCHA system (CAPTURE) that employed adversarial examples to produce CAPTCHA that can be readily solved by humans, while also being very successful at preventing machine learning-based bots from solving them. Shi et al.<sup>[48]</sup> introduced disturbances in the frequency domain instead of the spatial domain. They discovered that the addition in the spatial domain is a localized alteration of the picture, which is delicate. The addition of perturbations in the frequency domain results in a widespread alteration that is difficult to eliminate.

Shao et al.<sup>[44]</sup> developed a novel CAPTCHA system by synthesizing adversarial examples. They produced pseudo-adversarial CAPTCHA and used a transferable adversarial technique specifically for text-based CAPTCHA.

The adversarial examples approach involves introducing perturbations to CAPTCHA pictures to counteract the ability of machine learning systems to accurately recognize them. Nevertheless, the disturbance mechanism may be eradicated by using several removal methods<sup>[60]</sup>.

### 3.3.2. Style transfer generation models

With the deep study of high-quality image production based on deep learning algorithms, researchers concentrated on the CAPTCHA image. Currently, style transfer models like Neural Style Transfer (NST) are often used in the generation model to generate various stylized CAPTCHA images.

A fusion model that integrated adversarial examples and NST model was designed by Dinh and his team<sup>[52]</sup>. Their experimental findings demonstrate that this combined generative model enhances the security of traditional CAPTCHA.

Kwon et al.<sup>[46]</sup> introduced the Style-Plugged-CAPTCHA, integrating styles from other images while preserving the original CAPTCHA's content. The outcomes indicate that this proposed approach diminishes the recognition rate by the DeCAPTCHA system to 3.5% and 3.2% when employing one and two style images, respectively. However, human recognizability is maintained.

Likewise, Cheng et al. employed Neural Style Transfer (NST) to generate two types of CAPTCHA named Font-CAPTCHA and Grid-CAPTCHA<sup>[47]</sup>. Their experimental findings revealed a significant reduction in the success rate of automated attacks with the application of neural style transfer technique. Specifically, the success rate decreased notably, demonstrating a substantial improvement in security measures. The human performance in solving the challenges was commendable, achieving a success rate of 75.04% for Grid-CAPTCHA and 84.49% for Font-CAPTCHA. It is important to note that additional details regarding the sample size, experimental design, and specific percentage reduction would enhance the comprehensiveness of the reported results.

Ray and his team<sup>[54]</sup> designed a Style Matching CAPTCHA (SMC) by using neural-style transfer (NST) to enhance both security and user efficiency. The SMC, assessed with a sample size of 152 people, demonstrated a commendable accuracy rate of 95.61% and a fast reaction time of 6.52 seconds. In contrast, the average accuracy of CNN attacks was a mere 37%.

StyleCAPTCHA was designed by Chen et al.<sup>[55]</sup>. Users were required to distinguish the stylized images that consist of human faces and animal faces. The stylized source material included facial images of humans and animals, with both the primary facial image and the style reference image concealed from the user. As a defense against attacks utilizing deep convolutional networks (DCNs), StyleCAPTCHA changes its style to make it harder for attackers to use Deep Convolutional Networks (DCNs) to classify tasks with different styles.

### 3.3.3. CNN-based generation models

Besides employing adversarial examples and Style transfer generation models, researchers utilize CNN-based model to enhance the performance of CAPTCHA.

Shim et al.<sup>[56]</sup> primarily focus on generating CAPTCHA images of superior quality within a specific timeframe. In their study, they utilize a GAN model to generate novel CAPTCHA images for verification purposes, thereby enhancing the overall security of the CAPTCHA system..

Alqahtani et al.<sup>[58]</sup> explored the effectiveness of image-based CAPTCHA through experiments. They utilized machine learning technologies like classification, and Naïve Bayes to break the CAPTCHA. The system achieved an average accuracy of 85.32%, successfully solving 56.29% of reCAPTCHA challenges.

### 3.4. Integrated human cognitive ability and semantic understanding

To enhance the security and usability of CAPTCHA, it is essential to consider not only the optimization of the generation model but also the integration of human cognitive ability and semantic understanding with deep learning algorithms or image processing algorithms. This approach proves to be highly effective in achieving the desired results.

Jia et al.<sup>[61]</sup> introduced a novel semantic approach for creating CAPTCHA incorporating text and images. This approach considers the phrase’s meaning, the item being shown (in this case, a bird), and its position. To enhance the categorization of CNN, the user’s recognition progress and semantic comprehension are included in the generation of text-image-based CAPTCHA. Their experimental findings revealed that ResNet-50’s ability to categorize the recommended TICS (the CAPTCHA method they presented) achieved an accuracy of just 3.38%.

Ray et al.<sup>[54]</sup> developed a Style Matching CAPTCHA (SMC). They utilized Neural Style Transfer (NST) and human cognitive ability to enhance the performance of CAPTCHA both in security and usability performance. Evaluated with 152 participants, the SMC achieved an impressive accuracy rate of 95.61% and a response time of 6.52 seconds. In contrast, the average CNN attack accuracy was only 37%. The integrated cognitive ability CAPTCHA generation models are shown in **Table 5**.

**Table 5.** Overview of integrated cognitive ability CAPTCHA generation models.

No.	Focus techniques	References/Authors, Year	Anti-attack	User-friendly
1	Combined cognitive ability	[54]	Multiple data	-
2	Combined cognitive ability	[52]	Multiple data	-
3	Semantic understanding	[61]	3.38%	√
4	Combined cognitive ability	[45]	9.3% to 23.5%	72% to 88%

### 3.5. Results analysis

In short, when people design CAPTCHA, two performance indicators, security and user-friendliness should be considered comprehensively. Enhancing human recognition capabilities while defending against recognition by bots is something people should consider. However, most researchers only focus on one of the CAPTCHA performance indicators, ignoring considering them simultaneously for a thorough evaluation.

When generating CAPTCHA, researchers can utilize comprehensive algorithms to guarantee both the security and user-friendliness of CAPTCHA. For instance, adding image background noise or character interference, combined with human cognition or semantic understanding ability, constructs advanced deep learning models. **Table 6** provides a comprehensive summary of the key aspects of secure CAPTCHA generation technologies and the different types of CAPTCHAs they are applied to. The table highlights the deep learning technologies that can be integrated into this context. Future researchers can use these technical

theories to explore and improve CAPTCHA generation methods. Based on the insights from **Table 5**, researchers can develop novel approaches to solve the limitations of existing technologies. Currently, it is challenging to balance security and user-friendliness in CAPTCHA. Therefore, researchers can explore hybrid generative models combining classic image processing and deep learning techniques. These models can consider human semantic understanding and cognitive levels to generate secure and user-friendly CAPTCHA. Alternatively, researchers can also use transformers, attention, GAN, VAE, and other technologies to enhance CAPTCHA’s security and ease of use.

**Table 6.** Summary of secure CAPTCHA generation models and application.

Focus metrics	Strategy	Implementation method	Example	Application CAPTCHA type
Anti-attack	Anti-machine recognition	Add perturbation	Adversarial examples Background interference overlapping images	Image/Image-text Image/Image-text Image/Image-text
		Change character structure	3D, Hollow, Two-layer, distortion...	Text
		Transfer style images	Image style transfer Font style transfer	Image/Image-text Text
Anti-attack User-friendly	Anti-machine recognition Enhance human identification	Add inferences Human cognitive ability	Comprehensive approach	Image-text
User-friendly	Enhance human identification	Image recognition	Dots/ Image encryption Faces/Facial expression User Confirmation (reCAPTCHA)	Text Image/Image-text Image-text
		Semantic understanding	Generate images based on text description	Image-text
		Human cognitive ability	Image-text matching Text-image correlation	Image-text Image-text

## 4. Discussion and future work

Previous studies show that deep learning technology possesses powerful image processing and recognition capabilities in the image field, especially in its application to CAPTCHA generation and recognition. However, practical limitations or drawbacks constrain applying deep learning techniques to CAPTCHA generative models. For instance, adversarial examples technology can “fool” the recognition model, but the disturbance mechanism may be removed by removal methods. In addition, style transfer technology exists in the presence of inaccuracies or distortions in the representation of image content, leading to an inaccurate portrayal of the original content during image generation.

Furthermore, GAN-based generation technology can produce reality images but requires high hardware requirements, and the generation speed is slow. Therefore, researchers should consider the trade-off between image quality and generation speed. Combined human cognitive abilities seem user-friendly, but sometimes the result depends on the number of participants. The more participants, the better the user-friendly performance. One solution is to deploy the CAPTCHA on real-world websites for public testing to obtain authoritative user test data. The disadvantage is that this type of CAPTCHA involves the user’s privacy and security.

Nevertheless, deep learning techniques are still the preferable for CAPTCHA generation tools because of its powerful computing capabilities. Unlike classic image processing technology, which requires manual participation to extract features, deep learning technology can automatically extract features for learning. Therefore, the complexity of deep learning technology models is high. Regarding whether to consider security and usability evaluation indicators, classic image processing generation technology is considered less

simultaneously. In contrast, the generation technology model that combines deep learning and human cognitive abilities considers security and usability evaluation indicators simultaneously (See **Table 7**).

Therefore, integrating classical image processing, deep learning techniques, and human cognitive ability will help improve the performance of future image-based CAPTCHA generation algorithms, thereby improving user-friendliness and resistance to identification. Also, researchers can use emerging technologies such as transformer techniques, natural language processing (NLP), and big language model like ChatGPT to generate CAPTCHA challenges that require users to answer real-time dynamic questions. Furthermore, CAPTCHA challenges can be deployed on the real website to test the user-friendliness authoritatively. In addition, image encryption technology can also be applied in the CAPTCHA generation model to improve the security of CAPTCHA images.

**Table 7.** Evaluation comparison of overall techniques.

Techniques	Computing resources	Features extraction	Model complex	Balance security and usability
Classical image processing	Low	Manual	Simple	Less both consider
Deep learning technique	High	Automatic	Complex	Balance
DL+ human cognitive ability	High	Automatic	Complex	Balance

## 5. Conclusion

This review provides refined reference and guidance for future research in the field of CAPTCHA generation. The authors analyze gaps in existing literature and identifies future research directions by summarizing and evaluating existing research. CAPTCHA generation technology is divided into three major types: classic image processing technology, deep learning technology, and technology combined with human cognitive ability. This survey scientifically screened 1363 referred articles in the past five years and analyzed 28 carefully selected CAPTCHA generation papers. The advantages and disadvantages of different deep learning generation technologies are analyzed in-depth. Among them, integrating deep learning technology and the other two types of technologies can improve the performance of image-based verification code generation algorithms. It performs well in terms of security and user-friendliness indicators.

This survey provides future research directions. When integrating deep learning technology, several factors should be considered to generate attack-resistant and user-friendly CAPTCHA. Firstly, the algorithm should be robust enough to resist brute-force, dictionary, and machine learning-based attacks. Secondly, the generated CAPTCHA should be user-friendly, which means it should be simple and easy to solve for legitimate users. Additionally, the CAPTCHA should be compatible with different devices and platforms, such as mobile phones and tablets.

Regarding future CAPTCHA generative technologies and research directions, there are numerous ongoing developments in this field. One promising direction is using adversarial training to improve the robustness of CAPTCHA against attacks. Another direction is using deep reinforcement learning to generate a more complex and diverse CAPTCHA that is still easy for humans to solve. The use of biometric-based CAPTCHA, such as fingerprint recognition or facial recognition, is also being explored.

## Conflict of interest

The authors declare no conflict of interest.

## References

1. von Ahn L, Blum M, Hopper NJ, Langford J. CAPTCHA: Using hard AI problems for security. In: Proceedings of the Advances in Cryptology—EUROCRYPT 2003: International Conference on the Theory and Applications of

Cryptographic Techniques.

2. von Ahn L, Maurer B, McMillen C, et al. reCAPTCHA: Human-Based Character Recognition via Web Security Measures. *Science*. 2008; 321(5895): 1465-1468. doi: 10.1126/science.1160379
3. Awasthi S, Srivastava AP, Srivastava S, et al. A Comparative Study of Various CAPTCHA Methods for Securing Web Pages. 2019 International Conference on Automation, Computational and Technology Management (ICACTM). Published online April 2019. doi: 10.1109/icactm.2019.8776832
4. Mirkovic J, Reiher P. A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review*. 2004; 34(2): 39–53.
5. Gutub A, Kheshaifaty N. Practicality analysis of utilizing text-based CAPTCHA vs. graphic-based CAPTCHA authentication. *Multimedia Tools and Applications*. 2023; 82(30): 46577-46609. doi: 10.1007/s11042-023-15586-5
6. Zhu BB, Yan J, Guanbo Bao, et al. Captcha as Graphical Passwords—A New Security Primitive Based on Hard AI Problems. *IEEE Transactions on Information Forensics and Security*. 2014; 9(6): 891-904. doi: 10.1109/tifs.2014.2312547
7. Reed S, Akata Z, Yan X, et al. Generative Adversarial Text to Image Synthesis. In: Proceedings of the 33rd International Conference on Machine Learning.
8. Chen C, Li O, Tao D, et al. This Looks Like That: Deep Learning for Interpretable Image Recognition. Available online: <https://proceedings.neurips.cc/paper/2019/hash/adf7ee2dcf142b0e11888e72b43fcb75-Abstract.html> (accessed on 2 December 2023).
9. Deng J, Xuan X, Wang W, et al. A review of research on object detection based on deep learning. *Journal of Physics: Conference Series*. 2020; 1684(1): 012028. doi: 10.1088/1742-6596/1684/1/012028
10. Aouani H, Ayed YB. Speech Emotion Recognition with deep learning. *Procedia Computer Science*. 2020; 176: 251-260. doi: 10.1016/j.procs.2020.08.027
11. Ajagbe SA, Adigun MO. Deep learning techniques for detection and prediction of pandemic diseases: a systematic literature review. *Multimedia Tools and Applications*. 2023; 83(2): 5893-5927. doi: 10.1007/s11042-023-15805-z
12. Roy PK, Saumya S, Singh JP, et al. Analysis of community question-answering issues via machine learning and deep learning: State-of-the-art review. *CAAI Transactions on Intelligence Technology*. 2022; 8(1): 95-117. doi: 10.1049/cit2.12081
13. Altalhi S, Gutub A. A survey on predictions of cyber-attacks utilizing real-time twitter tracing recognition. *Journal of Ambient Intelligence and Humanized Computing*. 2021; 12(11): 10209–10221. doi: 10.1007/s12652-020-02789-z
14. Wang P, Gao H, Guo X, et al. An Experimental Investigation of Text-based CAPTCHA Attacks and Their Robustness. *ACM Computing Surveys*. 2023; 55(9): 1-38. doi: 10.1145/3559754
15. Chandavale AA, Sapkal AM, Jalnekar RM. Algorithm to Break Visual CAPTCHA. 2009 Second International Conference on Emerging Trends in Engineering & Technology. Published online 2009. doi: 10.1109/icetet.2009.24
16. Chew M, Tygar JD. Image recognition captchas. In: *International Conference on Information Security*. Springer; 2004.
17. Wang P, Gao H, Shi Z, et al. Simple and Easy: Transfer Learning-Based Attacks to Text CAPTCHA. *IEEE Access*. 2020; 8: 59044-59058. doi: 10.1109/access.2020.2982945
18. Noury Z, Rezaei M. Deep-CAPTCHA: A deep learning based CAPTCHA solver for vulnerability assessment. Published online 2020. doi: 10.48550/ARXIV.2006.08296
19. Zi Y, Gao H, Cheng Z, et al. An End-to-End Attack on Text CAPTCHAs. *IEEE Transactions on Information Forensics and Security*. 2020; 15: 753-766. doi: 10.1109/tifs.2019.2928622
20. Adesina AO, Ayobioloja PS, Obagbuwa IC, et al. An Improved Text-Based and Image-Based CAPTCHA Based on Solving and Response Time. *CMC-Computers Materials & Continua*. 2023; 74(2).
21. Kwon H, Yoon H, Park KW. Robust CAPTCHA Image Generation Enhanced with Adversarial Example Methods. *IEICE Transactions on Information and Systems*. 2020; E103.D(4): 879-882. doi: 10.1587/transinf.2019edl8194
22. Sheriff M, Mahesh V, S MSH, et al. No Bot Anticipates the Deep Captcha Presenting Disposed Illustrations with Applications to Captcha Generation. In: Proceedings of the 2023 International Conference on Circuit Power and Computing Technologies (ICCPCT).
23. Wen Y. Robust image-based CAPTCHA generation using adversarial attack. Subramanian K, ed. *Third International Conference on Intelligent Computing and Human-Computer Interaction (ICHCI 2022)*. Published online January 13, 2023. doi: 10.1117/12.2655934
24. Ardhita NB, Maulidevi NU. Robust adversarial example as captcha generator. In: Proceedings of the 2020 7th International conference on advance informatics: concepts, theory and applications (ICAICTA).
25. Page MJ, McKenzie JE, Bossuyt PM, et al. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *BMJ*. Published online March 29, 2021: n71. doi: 10.1136/bmj.n71
26. Kheshaifaty N, Gutub A. Preventing multiple accessing attacks via efficient integration of captcha crypto hash functions. *International Journal of Computer Science and Network Security*. 2020; 20(9): 16–28.
27. Kheshaifaty N, Gutub A. Engineering Graphical Captcha and AES Crypto Hash Functions for Secure Online Authentication. *Journal of Engineering Research*. Published online November 10, 2021. doi: 10.36909/jer.13761

28. Ye G. Yet another text captcha solver: A generative adversarial network based approach. In: Proceedings of the 2018 ACM SIGSAC conference on computer and communications security.
29. Kim S, Choi S. DotCHA: An Interactive 3D Text-based CAPTCHA. *Journal of Web Engineering*. 2020. doi: 10.13052/jwe1540-9589.1884
30. Imsamai M, Phimoltares S. 3D CAPTCHA: A Next Generation of the CAPTCHA. 2010 International Conference on Information Science and Applications. Published online 2010. doi: 10.1109/icisa.2010.5480258
31. Woo SS. Design and evaluation of 3D CAPTCHAs. *Computers & Security*. 2019; 82: 49-67. doi: 10.1016/j.cose.2018.12.006
32. Gao H, Yao D, Liu H, et al. A Novel Image Based CAPTCHA Using Jigsaw Puzzle. 2010 13th IEEE International Conference on Computational Science and Engineering. Published online December 2010. doi: 10.1109/cse.2010.53
33. Ye G, Tang Z, Fang D, et al. Using Generative Adversarial Networks to Break and Protect Text Captchas. *ACM Transactions on Privacy and Security*. 2020; 23(2): 1-29. doi: 10.1145/3378446
34. Zhang J, Tsai MY, Kitchat K, et al. A secure annuli CAPTCHA system. *Computers & Security*. 2023; 125: 103025. doi: 10.1016/j.cose.2022.103025
35. Goswami G, Powell BM, Vatsa M, et al. FaceDCAPTCHA: Face detection based color image CAPTCHA. *Future Generation Computer Systems*. 2014; 31: 59-68. doi: 10.1016/j.future.2012.08.013
36. Li X. A new CAPTCHA based on facial expression recognition. In: Proceedings of the Fifth International Conference on Artificial Intelligence and Computer Science (AICS 2023). Available online: <https://www.spiedigitallibrary.org/conference-proceedings-of-spie/12803/128032N/A-new-CAPTCHA-based-on-facial-expression-recognition/10.1117/12.3009229.short> (accessed on 2 December 2023).
37. Moradi M, Keyvanpour MR. A novel CAPTCHA scheme based on facial expression reconstruction. *International Journal of Electronic Business*. 2020; 15(4): 368. doi: 10.1504/ijeb.2020.111061
38. Gutub A, Shambour MK, Abu-Hashem MA. Coronavirus impact on human feelings during 2021 Hajj season via deep learning critical Twitter analysis. *Journal of Engineering Research*. 2023; 11(1): 100001. doi: 10.1016/j.jer.2023.100001
39. Singh A, Satapathy SC, Roy A, et al. AI-Based Mobile Edge Computing for IoT: Applications, Challenges, and Future Scope. *Arabian Journal for Science and Engineering*. 2022; 47(8): 9801-9831. doi: 10.1007/s13369-021-06348-2
40. Sufi FK, Alsulami M, Gutub A. Automating Global Threat-Maps Generation via Advancements of News Sensors and AI. *Arabian Journal for Science and Engineering*. 2022; 48(2): 2455-2472. doi: 10.1007/s13369-022-07250-1
41. Hemalatha J, Sekar M, Kumar C, et al. Towards improving the performance of blind image steganalyzer using third-order SPAM features and ensemble classifier. *Journal of Information Security and Applications*. 2023; 76: 103541. doi: 10.1016/j.jisa.2023.103541
42. Farooqi N, Gutub A, Khozium MO. Smart community challenges: Enabling IoT/M2M technology case study. *Life Science Journal*. 2019; 16(7): 11-17.
43. Hitaj D, Hitaj B, Jajodia S, et al. Capture the Bot: Using Adversarial Examples to Improve CAPTCHA Robustness to Bot Attacks. *IEEE Intelligent Systems*. 2021; 36(5): 104-112. doi: 10.1109/mis.2020.3036156
44. Shao R, Shi Z, Yi J, et al. Robust Text CAPTCHAs Using Adversarial Examples. 2022 IEEE International Conference on Big Data (Big Data). Published online December 17, 2022. doi: 10.1109/bigdata55660.2022.10021100
45. Trong ND, Huong TH, Hoang VT. New Cognitive Deep-Learning CAPTCHA. *Sensors*. 2023; 23(4): 2338. doi: 10.3390/s23042338
46. Kwon H, Yoon H, Park KW. CAPTCHA Image Generation: Two-Step Style-Transfer Learning in Deep Neural Networks. *Sensors*. 2020; 20(5): 1495. doi: 10.3390/s20051495
47. Cheng Z, Gao H, Liu Z, et al. Image-based CAPTCHAs based on neural style transfer. *IET Information Security*. 2019; 13(6): 519-529. doi: 10.1049/iet-ifs.2018.5036
48. Shi C, Xu X, Ji S, et al. Adversarial CAPTCHAs. *IEEE Transactions on Cybernetics*. 2022; 52(7): 6095-6108. doi: 10.1109/tcyb.2021.3071395
49. Chow YW, Susilo W, Thorncharoensri P. CAPTCHA design and security issues. *Advances in Cyber Security: Principles, Techniques, and Applications*; 2019.
50. Tian P, Liao W, Kimbrough T, et al. Generating Adversarial Robust Defensive CAPTCHA (GARD-CAPTCHA) in Convolutional Neural Networks. In: *International Conference on Software Engineering Research and Applications*. Springer; 2022.
51. Chen J, Gao X, Deng R, et al. Generating Adversarial Examples Against Machine Learning-Based Intrusion Detector in Industrial Control Systems. *IEEE Transactions on Dependable and Secure Computing*. 2022; 19(3): 1810-1825. doi: 10.1109/tdsc.2020.3037500
52. Dinh N, Tran-Trung K, Truong Hoang V. Augment CAPTCHA Security Using Adversarial Examples With Neural Style Transfer. *IEEE Access*. 2023; 11: 83553-83561. doi: 10.1109/access.2023.3298442
53. Zhang J, Sang J, Xu K, et al. Robust CAPTCHAs Towards Malicious OCR. *IEEE Transactions on Multimedia*. 2021; 23: 2575-2587. doi: 10.1109/tmm.2020.3013376

54. Ray P, Bera A, Giri D, Bhattacharjee D. Style matching CAPTCHA: Match neural transferred styles to thwart intelligent attacks. *Multimedia Systems*. 2023; 29(4). doi: 10.1007/s00530-023-01075-0
55. Chen H, Jiang B, Chen H. StyleCAPTCHA. *Proceedings of the 2020 ACM-IMS on Foundations of Data Science Conference*. Published online October 18, 2020. doi: 10.1145/3412815.3416895
56. Shim JY, Jung S, Kim J, et al. Stabilized Performance Maximization for GAN-based Real-Time Authentication Image Generation over Internet. *Multimedia Tools and Applications*. Published online July 15, 2023. doi: 10.1007/s11042-023-15885-x
57. Rathor VS, Garg B, Patil M, et al. Security analysis of image CAPTCHA using a mask R-CNN-based attack model. *International Journal of Ad Hoc and Ubiquitous Computing*. 2021; 36(4): 238. doi: 10.1504/ijahuc.2021.114108
58. Alqahtani FH, Alsulaiman FA. Is image-based CAPTCHA secure against attacks based on machine learning? An experimental study. *Computers & Security*. 2020; 88: 101635. doi: 10.1016/j.cose.2019.101635
59. Szegedy C, Zaremba W, Sutskever I, et al. Intriguing properties of neural networks. Published online 2013. doi: 10.48550/ARXIV.1312.6199
60. Alsuhbany SA. A Survey on Adversarial Perturbations and Attacks on CAPTCHAs. *Applied Sciences*. 2023; 13(7): 4602. doi: 10.3390/app13074602
61. Jia X, Xiao J, Wu C. TICS: Text–image-based semantic CAPTCHA synthesis via multi-condition adversarial learning. *The Visual Computer*; 2022.