Contents lists available at ScienceDirect

Neurocomputing

journal homepage: www.elsevier.com/locate/neucom

A survey of CAPTCHA technologies to distinguish between human and computer

Xin Xu[a,b,*], Lei Liu[a], Bo Li[a,b]

[a] School of Computer Science and Technology, Wuhan University of Science and Technology, Wuhan 430065, China
[b] Hubei Province Key Laboratory of Intelligent Information Processing and Real-time Industrial System, Wuhan University of Science and Technology, Wuhan 430065, China

ARTICLE INFO

Article history:
Received 6 April 2019
Revised 24 July 2019
Accepted 11 August 2019
Available online xxx

Keywords:
CAPTCHA
Usability
Security

ABSTRACT

CAPTCHA, Completely Automated Public Turing test to tell Computers and Humans Apart, is widely used as a security mechanism to classify human and computer. This security mechanism is based on the Turing Test, which has been conceived to ensure network security. Usability is another fundamental issue, which can avoid human users proceeding tedious and time-consuming operation. CAPTCHA design should consider security and usability simultaneously. This paper provides a review on the development of CAPTCHA technologies for human and computer classification, along with their applications and instantiations. Different from previous CAPTCHA survey, this review discusses the CAPTCHA mechanism from usability and security aspects, therefore attacking (anti-classification) and defending (classification) technologies towards current CAPTCHA are both reviewed. Besides, recent emerging CAPTCHA and the attacking techniques are also introduced in this paper, such as game CAPTCHA, deep learning-based attacking, and etc.

© 2020 Elsevier B.V. All rights reserved.

1. Introduction

CAPTCHA (Completely Automated Public Turing test to Tell Computers and Humans Apart), also called HIPs (Human Interaction Proofs) [1], is a test to classify human users and computer. Typically, these problems are based on hard AI, which most human users can pass, but computer cannot [2]. The idea of CAPTCHA is derived from the Turing test [3], however it is different from Turing test in three folds. Firstly, the generating and scoring of CAPTCHAS are finished by machine automatically; secondly, the purpose of designing CAPTCHA is to identify the difference between human and computer, instead of avoid distinguishing; thirdly, CAPTCHA is a kind of security mechanism, while most Turing tests are used as an indicator to reflect the progress of AI [4]. Therefore, CAPTCHA is usually regarded as a kind of Reverse Turing test for humans and computer classification [5–10].

CAPTCHA technology is involved in many research fields, such as artificial intelligence, network information safety, natural language processing, computer vision, signal processing, and etc. At present, CAPTCHA is mainly used for network security to classify humans and computer, so as to ensure the safety of network applications [11–16], including online voting, email registration, spam mail [17–21], weblog, search engine, chat room [22–24], and distributed denial of service. However, the usability of some existing CAPTCHA is far from satisfactory, human users usually have to face tedious and time-consuming operation [17,25]. According to reports, it takes 10 seconds in average for a human user to identify typical CAPTCHA characters with noise interference. Therefore, CAPTCHA design should consider security and usability simultaneously. As illustrated in Fig. 1, the key points of CAPTCHA design lies in exploring the gap of recognition ability between human users and computer.

This paper provides a review on the development of CAPTCHA technology. The main contributions of this review are in four folds:

1. This paper discusses the CAPTCHA mechanism from usability and security aspects, therefore attacking and defending techniques towards current CAPTCHA are both reviewed;
2. For text CAPTCHA, this paper summarizes the genetic attacking methods towards them, especially adds the deep learning-based attacking techniques;
3. This paper reviews image CAPTCHA using a different type of categories from previous survey, and summarizes typical current image CAPTCHA with good safety;
4. Recent emerging CAPTCHA are also introduced in this paper, such as game CAPTCHA.

[*] Corresponding author at: School of Computer Science and Technology, Wuhan University of Science and Technology, Wuhan 430065, China.
E-mail address: xuxin@wust.edu.cn (X. Xu).

https://doi.org/10.1016/j.neucom.2019.08.109
0925-2312/© 2020 Elsevier B.V. All rights reserved.

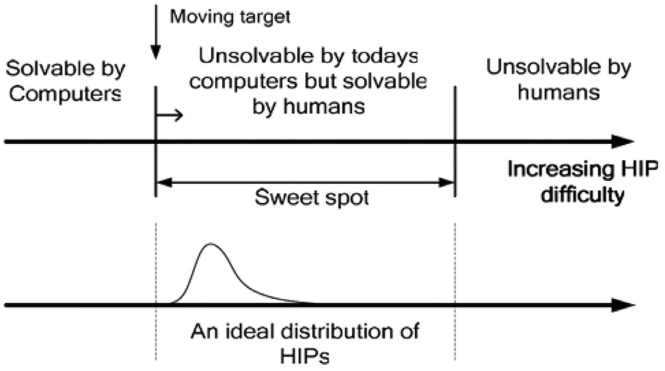

Moving target
Solvable by Computers
Unsolvable by todays computers but solvable by humans
Unsolvable by humans
Sweet spot
Increasing HIP difficulty
An ideal distribution of HIPs

Fig. 1. Using CAPTCHA/HIP for human and computer classification based on their difference in recognition ability [26].

2. Existing CAPTCHA and genetic attacking methods

2.1. Existing CAPTCHA

CAPTCHA [27] can be divided into text CAPTCHA, Image CAPTCHA [28], Sound CAPTCHA [29], and etc. Human users and machines show different recognition capabilities when facing CAPTCHA with different carriers and contents [30]. The characteristics are briefly summarized in Table 1.

Text-based CAPTCHA is simple and the most widely used type of CAPTCHA. It aims to evaluate the difference between human and computer in recognizing character sequence. Text-based CAPTCHA utilizes alphabets with lower & upper cases and digits from zero - nine to formulate a large question pool. Users may have difficulties in identify the correct text or characters like Multiple Fonts, Font size, Blurred Letters, Wave Motion, and etc., when emphasizing more on the security of text-based CAPTCHA. While text-based CAPTCHA is vulnerable to character segmentation attacking and OCR recognition attacking [23], when emphasizing more on its usability aspect.

Image-based CAPTCHA can provide challenge tests to identify the difference between human and computer in understanding image content. Commonly used challenges include image object detection, target recognition, and scene understanding. Because most image CAPTCHAs do not need text inputs, they are suitable to implement on mobile devices with better usability. However, image-based CAPTCHA requires large image pool, as limited input space may easily be attacked by machine learning.

Sound CAPTCHAs are usually developed for the convenience of the visually impaired as a supplement to text and image CAPTCHAs. It is based on the difference in the ability between human and computer in recognizing voice signal. Many portals are equipped with sound CAPTCHAs in text and image CAPTCHAs, and ask user to enter the same words as which are spoken in the audio clip.

2.2. Genetic attacking methods towards CAPTCHA

In general, genetic attacking methods first find the locations of objects to segment them; then, the objects can be recognized. Generally, object segmentation is more difficult than object recognition for machines. For example, there are many OCR (optical character recognition) programs that can effectively identify single characters in a text CAPTCHA, but it is relatively difficult to separate these characters from the CAPTCHA. Generally, a CAPTCHA can be considered to be of high security when the machine's recognition rate for CAPTCHAs is below 0.01%. The basic attack methods, which pertain to CAPTCHA object segmentation and object recognition, are briefly introduced below.

2.2.1. Object Segmentation Attack

The CAPTCHA object segmentation, which occurs after the preprocessing step, is usually combined with the vertical histogram, color filling, snake and other methods. The preprocessing step mainly removes noise interference [31], such as background patterns [32] and connecting arcs [33], to facilitate CAPTCHA object segmentation. An example of connecting arc removal is shown in Fig. 2.

Vertical Histogram: The object segmentation method that is based on the vertical histogram is proposed in Yan et al. [33,38]. The main idea is to segment according to the gray value difference between the object and the connection line, which is shown in Fig. 3.

Colour fill: This method segments according to the connectivity of each object [33]. By traversing the foreground pixels, the main idea is to find all the foreground pixels that are connected to them.

Snake segmentation: This method uses the snaked broken line to segment each object in a CAPTCHA [38]. It is as shown in Fig. 4.

2.2.2. Object recognition attack

Object recognition attacking includes pixel statistics [39], dictionary attacking [39], object recognition attacking [40] and etc.

Pixel Statistics: This method only works if the pixel number of CAPTCHA objects remains the same and the pixel number of each object is different. The pixel statistics result for standardized English characters is shown in Fig. 5.

Dictionary Attack: This method is mainly designed for CAPTCHAs that only use certain characters and have a limited number of character combinations. In addition, it can be used in conjunction with pixel statistics, as shown in Fig. 6.

Object Recognition Attack: This kind of method adopts artificial intelligence algorithms to recognize different CAPTCHA objects. The common attack methods include pattern matching [26], OCR recognition, machine learning [40], etc.

2.2.3. Other CAPTCHA attacking methods

Random guess attack: This kind of attack, which is also called the blind guess attack, is generally used when a CAPTCHA has a small input space and there is no limit to how many attempts a user can make.

Table 1
existing CAPTCHA classification.

Object type	Corresponding hard AI problem	Characteristics
Text-based CAPTCHA	Recognize character sequence	The most widely used type; vulnerable to character segmentation attacking and OCR recognition attacking [23].
Image-based CAPTCHA	Understand image content	Convenient to use; input space is limited and easily be attacked by machine learning.
Sound-based CAPTCHA	Recognize voice signal	Seldom used; usually be regarded as the assist of text-based and image-based CAPTCHA.

Please cite this article as: X. Xu, L. Liu and B. Li, A survey of CAPTCHA technologies to distinguish between human and computer, Neurocomputing, https://doi.org/10.1016/j.neucom.2019.08.109

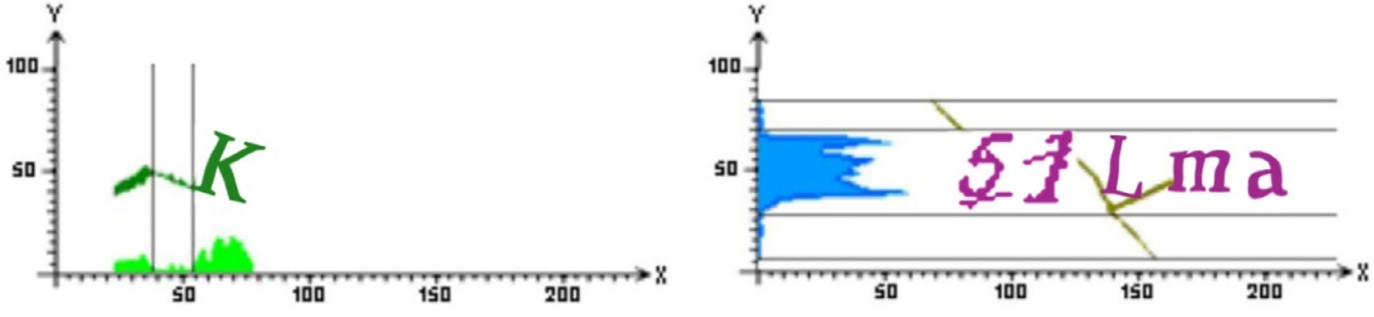


Fig. 2. Using histogram for arcs removal.

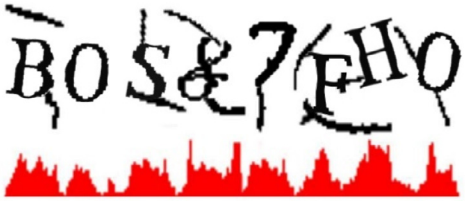


Fig. 3. Vertical histogram segmentation.

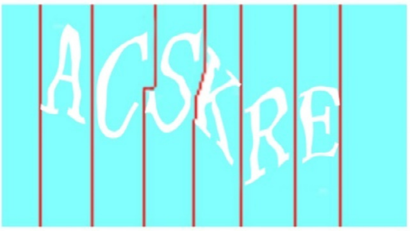
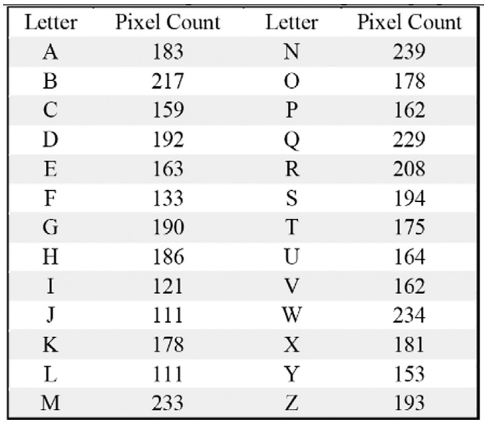
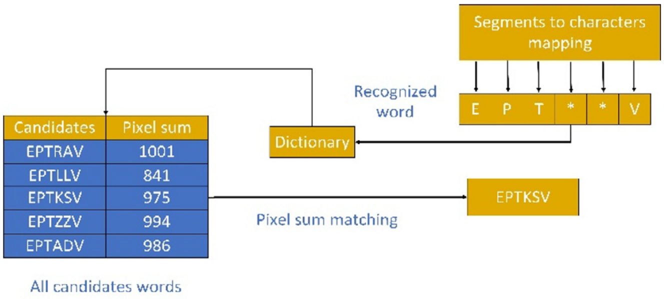


Fig. 4. Snake segmentation.



Letter	Pixel Count	Letter	Pixel Count
A	183	N	239
B	217	O	178
C	159	P	162
D	192	Q	229
E	163	R	208
F	133	S	194
G	190	T	175
H	186	U	164
I	121	V	162
J	111	W	234
K	178	X	181
L	111	Y	153
M	233	Z	193

Fig. 5. Character pixel statistics.



Candidates	Pixel sum
EPTRAV	1001
EPTLLV	841
EPTKSV	975
EPTZZV	994
EPTADV	986

Fig. 6. Dictionary attack.

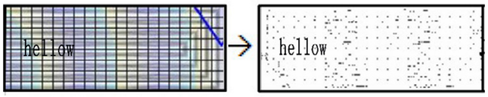


Fig. 7. Remove interference of EZ-Gimpy using preprocessing algorithm.

3. CAPTCHA technology attacking and defending review

Since the idea of the CAPTCHA test was proposed, many kinds of hard AI problems have been designed for human-machine interaction verification by researchers [41,42]. Some CAPTCHA technologies have been widely used, while other CAPTCHA technologies, which are not actually used, are only schematically designed [43,44]. Therefore, while reviewing the attack and defence processes from the perspective of security and usability, this paper pays more attention to CAPTCHA solutions that have been applied in practice at present. However, other schemes are analysed according to their design ideas.

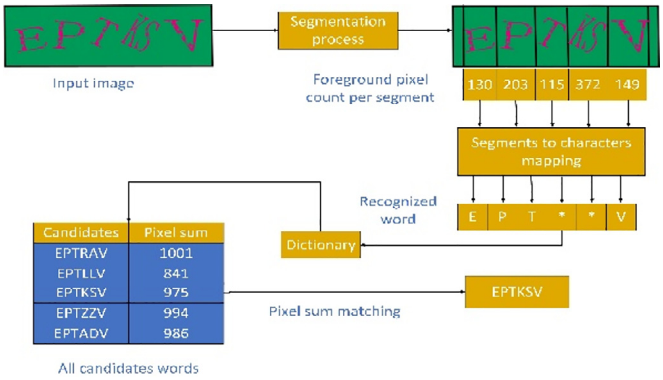
3.1. Text CAPTCHA

The most commonly used CAPTCHA type is the text CAPTCHA [45,47]. The main idea is to defend against malicious bot program attacks based on the differences between humans and machines in their character recognition ability, which has been widely used to guarantee the security of many network applications [33–53].

(1) English words as text

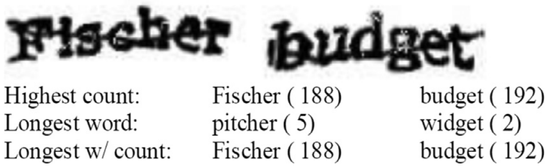
EZ-Gimpy is a kind of text CAPTCHA that was designed by CMU. The text of this CAPTCHA type is comprised of English words [54]. To improve security, EZ-Gimpy adds different types of interference to English words, such as black and white lines, background networks, gradients, blurs, and pixel noise. However, EZ-Gimpy can be easily attacked by using the image preprocessing method. For example, Simard et al. [32] adopted the preprocessing algorithm, which can effectively eliminate these noise interferences [55], as shown in Fig. 7. In addition, because EZ-Gimpy uses English words and has a small input space, it is vulnerable to pattern matching attacks. For instance, Mori et al. [56] used shape matching to recognize an entire English word, and the recognition rate reached 92%. In addition, Moy et al. [42], in which the recognition rate is 99%, structured a template based on a single English character and compared the characters one by one [58].

To enhance the security of a CAPTCHA, another type of interference noise (random trimming [59]) is adopted by CAPTCHAervice.org. However, this kind of interference noise has already been cracked successfully by Yan et al. [38]. As shown in Fig. 8, the single character is segmented based on colour; then it is recognized by using pixel statistics and dictionary attacking and achieves a recognition rate of 94%.



Candidates	Pixel sum
EPTRAV	1001
EPTLLV	841
EPTKSV	975
EPTZZV	994
EPTADV	986

Fig. 8. An attack against CAPTCHAervice.org.



Highest count:	Fischer (188)	budget (192)
Longest word:	pitcher (5)	widget (2)
Longest w/ count:	Fischer (188)	budget (192)

Fig. 9. An attack against reCAPTCHA.

The above CAPTCHA has a small input space, and the used interference noise is easily removed by the existing OCR program [60]. Therefore, this kind of CAPTCHA has low security [46–63], and other similar CAPTCHAs include Gimpy [64] and others.

To enhance the security of CAPTCHA, reCAPTCHA was proposed to select English words from old printed materials or scanned text as CAPTCHA text [65–67]. ReCAPTCHA allows users to recognize two English words in a test in which the English word with the tag is used for human-machine recognition. Then, the authentic human user's input is regarded as a label of another word. First, this approach can defend against the recognition attacks of traditional OCR programs. Second, this method can also effectively increase the input space of the CAPTCHA. However, reCAPTCHA is also cracked by the following tactics. As shown in Fig. 9, Wilkins et al. [68] adopted a preprocessing step to assist the OCR recognition. This method uses a series of corrosion and expansion preprocesses for each character before OCR recognition, which achieves a recognition rate of 17.5%. Starostenko et al. [69] focuses on analysing character directions, folds and other changes in reCAPTCHA and proposes an SVM-based classification to segment and recognize attacks, which has a recognition rate of 94%. In addition, the recognition rate of reCAPTCHA has been further improved through the continuous development of deep learning technology in recent years. For example, Goodfellow et al. [70–73] uses deep convolutional neural networks to integrate object segmentation and object recognition attacks [74,75]. This method has been successfully used for recognizing the street view character text in reCAPTCHA, thus achieving a recognition rate of 99.8%

Using English words as CAPTCHA text has good usability. However, this type of CAPTCHA is vulnerable to be attacked because of its limited space (words).

(2) Random string as text

Another kind of text CAPTCHA uses random strings [76] to expand the solution space, such as Ticketmaster [77]. To improve security, it adds a random angle crossover line to CAPTCHA text. However, it is also hard for Ticketmaster to defend against the previously mentioned attacks against EZ-Gimpy, and the main difference is only in the processing of the random angle crossover line. As shown in Fig. 10, Simard et al. [32] adopts dilution and corrosion operations to remove these crossover lines in CAPTCHA, which can achieve a recognition rate of 4.9%.

Considering that the increasing difficulty of object segmentation can more effectively improve the security [4] of CAPTCHA compared with object recognition, the MSN CAPTCHA randomly adds three different thick connection curves between characters to increase the difficulty of character object segmentation [78]. With respect to the interference of the connection curve, the vertical histogram and color filling methods were used in Yan et al. [33], which is shown in Fig. 11. By combining features [34–37] such as shapes, positions, pixel statistics, etc., the interference in these connection curves can be effectively avoided with a recognition rate of 60%. Nakaguro et al. [79] proposed a multiple interaction-based secondary snake attack method, which can achieve a recognition rate of 83%.

Aiming at Internet banking, Li et al. [80] attacked three types of transaction confirmations and 41 types of text CAPTCHAs for users logging in. This attack is mainly aimed at the interference in the connection lines, noise points and character overlaps that are used in these text CAPTCHAs. Then, a corresponding attack method of image processing and pattern recognition was proposed [81], such as k-means clustering, digital image restoration, morphological image processing, cross-correlation character recognition, image quality evaluation, etc.

Hollow CAPTCHAs attempt to use contour lines to construct the connected hollow characters to improve security and usability. However, Gao et al. [82] proposed an attack method to convert hollow characters to solid characters. As illustrated in Fig. 12, the main idea is to divide the CAPTCHA into multiple parts using color filling and then use the convolutional neural network for recognition. The results show that this attack can achieve a recognition rate of 93% for Tencent's Hollow CAPTCHA.

Using random strings can extend the input space and solution space to some extent. However, because the number of characters is fixed, the available character combinations are still limited; thus, there is still the possibility of attacks using pattern matching. To increase the identification difficulty of a pattern matching algorithm, researchers attempt to use handwriting as the CAPTCHA text to further expand the input space. Thomas et al. [83] and Rusu et al. [84] proposed a handwritten text generation method and added different kinds of interference to prevent OCR program recognition. However, this kind of handwritten CAPTCHA has poor usability, and sometimes it is hard for users to correctly recognize these random strings. Although English words are used as text, the guessed answer is also needed for users, which is shown in Fig. 13.

Considering that using 3D text is a better defence against attacks such as pattern recognition [85–91] than using 2D text, researchers have designed a variety of 3D text CAPTCHAs, including the Super CAPTCHA, 3dcaptcha and Teabag 3D, and some of these CAPTCHAs are actually used by websites. However, in essence, 3D text can be considered as a 2D text pattern with noise interference; therefore, this approach still may be attacked by

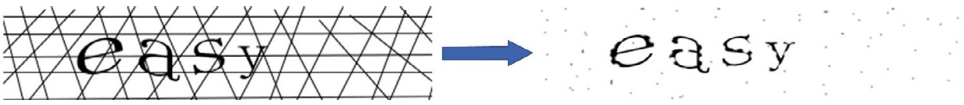


Fig. 10. An attack on Ticketmaster CAPTCHA.

Please cite this article as: X. Xu, L. Liu and B. Li, A survey of CAPTCHA technologies to distinguish between human and computer, Neurocomputing, https://doi.org/10.1016/j.neucom.2019.08.109

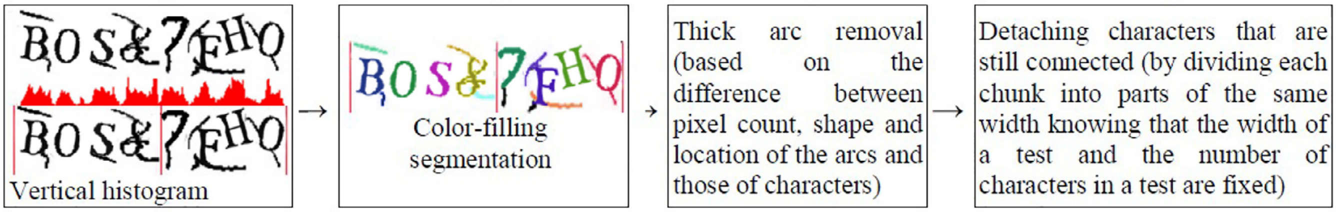

Vertical histogram
Color-filling segmentation
Thick arc removal (based on the difference between pixel count, shape and location of the arcs and those of characters)
Detaching characters that are still connected (by dividing each chunk into parts of the same width knowing that the width of a test and the number of characters in a test are fixed)

Fig. 11. An attack on MSN CAPTCHA.

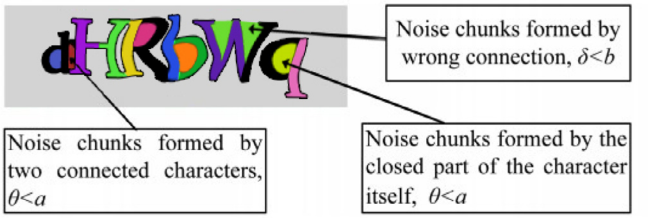

Noise chunks formed by wrong connection, δ<b
Noise chunks formed by two connected characters, θ<a
Noise chunks formed by the closed part of the character itself, θ<a

Fig. 12. Color-filled based CAPTCHA segmentation.

using pattern recognition technology [92–95]. For example, Nguyen et al. conducted pattern recognition attacks on these three-3D text CAPTCHAs and achieved recognition rates of 27%, 58% and 31%, respectively.

In addition, to improve the usability of CAPTCHA, Google proposed a design method based on multi-feature nonlinear combinations. The method uses a variety of features, such as visual features, anti-segmentation features and anti-recognition features. The method also has better usability with defending against attacks such as machine learning and statistical models, which can effectively improve the CAPTCHA recognition rate to 95.3% for users.

(3) Universal text CAPTCHA attack method

As mentioned above, attacks on text CAPTCHAs usually detect the locations of the character objects first and then recognizes each character object separately [96]. This approach includes three steps: preprocessing, character object segmentation and character object recognition.

For machines, character object segmentation is generally more difficult than character object recognition [4,97,98]. Therefore, Bursztein et al. [99] systematically tested 15 kinds of text CAPTCHAs with anti-segmentation features and proposed an attack method named DECAPTCHA. The main idea of DECAPTCHA is to evaluate the robustness of CAPTCHA by creating a toolbox containing different attack and defence algorithms. Therefore, it is also considered as the first universal text CAPTCHA attack method. However, the DECAPTCHA only performs segmentation attacks on character objects, and its performance is not effective on reCAPTCHA. The main reason why reCAPTCHA can defend against DECAPTCHA attacks is that it does not use the aforementioned connected lines but uses a kind of negative kerning (or called character folding) technology [99] to defend against object segmentation attacks, as shown in Fig. 14.

To segment folded characters, Bursztein et al. [100] proposed a universal text CAPTCHA attack method. Considering that the sequential method [101] of the first segmentation and then the recognition is adopted by common CAPTCHA attacks, the current interference should be adjusted using a manual method, which has limited applicability. In view of this, Bursztein et al. [100] adopts the machine learning method to integrate the segmentation and identify attacks, and it can successfully recognize the text CAPTCHAs of Baidu, CNN, eBay, reCAPTCHA, Wikipedia and Yahoo.

Gao et al. used stroke join point segmentation and column segmentation methods to recognize character folding, and the recognition rate of text CAPTCHAs was further improved [102]. In addition, they subsequently tried to follow the strategy of Bursztein et al. [100] to integrate segmentations and identify attacks, and a text CAPTCHA attack method based on Log-Gabor filtering was proposed [103]. This method can recognize the 20 most widely used text CAPTCHAs in 15 seconds (according to the Alexa ranking, https://www.alexa.com/topsites), and achieve a recognition rate of 5%-77%.

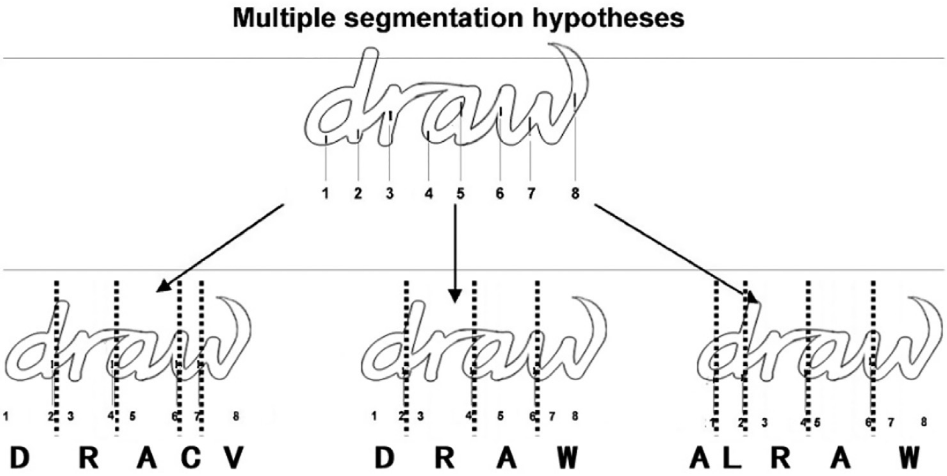


Fig. 13. The uncertainty of handwritten CAPTCHA and various segmentation schemes.

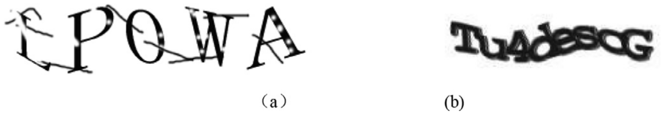
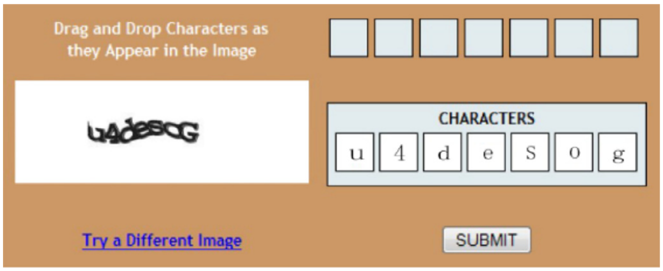


Fig. 14. Defense against object segmentation attacking: (a) connecting line; (b) negative kerning.


Drag and Drop Characters as they Appear in the Image

CHARACTERS

u 4 d e s o g

Fig. 15. Interactive text CAPTCHA.

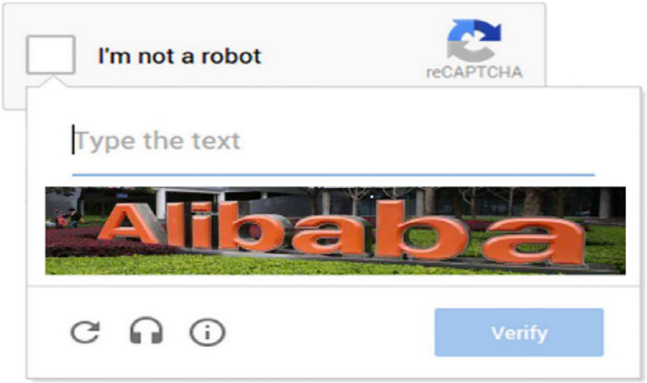


Fig. 16. Google's No CAPTCHA reCAPTCHA.

To defend against the CAPTCHA attack method that is described above, researchers tried to improve the security using more user interaction [104,105]. For example, Desai et al. [106] proposed that human-machine differentiation could be implemented through mouse operations. This interactive text CAPTCHA requires the user to drag characters sequentially to the appropriate white space as instructed, which is shown in Fig. 15 [107–111]. Subsequently, researchers further strengthened the security of interactive text CAPTCHAs from the aspects of defending against third-party attacks [112], increasing the input space [113], etc. For example, as developed by Google, the latest version of No CAPTCHA reCAPTCHA [114] has adopted this interactive method, which is shown in Fig. 16.

(4) Text CAPTCHA design

In summary, researchers have conducted a series of studies on the security and usability of text CAPTCHAs. However, there is still no standard evaluation system so far. Chellapilla et al. tested the usability of text CAPTCHAs for different types of interference [26,77], and Yan et al. evaluated the performance with respect to three aspects: the user recognition rate, response time and satisfaction. Then, they tested the impacts of the interference type, text content and presentation mode on the usability of text CAPTCHAs [25,124]. Thomas et al. also proposed a systematic framework to evaluate the security and usability of text CAPTCHAs [116].

From the development of text CAPTCHAs, different features [117,118] are used to design traditional text CAPTCHAs with respect to security and usability, such as different character styles (word widths, fonts, and directions), random string texts, character folding, etc. However, most existing text CAPTCHAs can be cracked by using simple image processing techniques (such as binarization, dilation, morphological processing, connectivity analysis, etc.) combined with prior knowledge. For example, the No CAPTCHA reCAPTCHA of Google is a kind of text CAPTCHA with good security and usability, but it has also been cracked by the popular deep learning techniques in recent years [119]. In addition, recently, Jaderberg et al. [120] proposed a text detection and recognition method based on current popular end-to-end deep learning. This method can recognize the text in natural scenarios, and so it is also expected to be used to attack text CAPTCHAs.

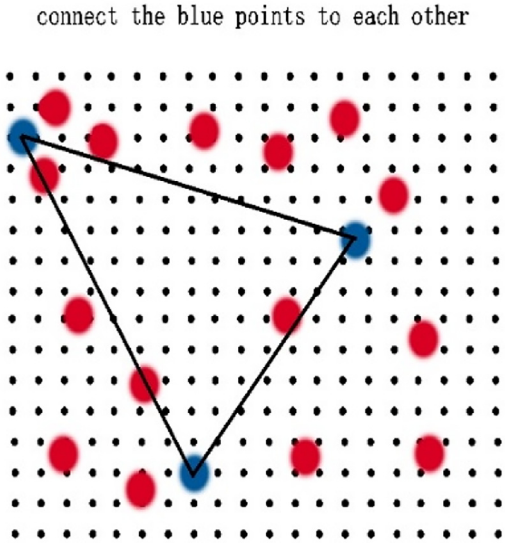

connect the blue points to each other

Fig. 17. Drawing CAPTCHA.

3.2. Image CAPTCHA

As a large number of text CAPTCHAs were successfully cracked, researchers tried to design hard AI problems that were harder than character recognition. By designing problems such as image object detection, target recognition, and scene understanding, image CAPTCHAs have been used to test the differences in human and machine capabilities on these problems and protect against malicious bot program attacks. Most image CAPTCHAs do not need text inputs; thus, they are suitable to implement on mobile devices with better usability [121–123].

3.2.1. Model-based image CAPTCHA

Image CAPTCHAs rely on labelled image data. However, the labour that is required to manually annotate image data is significant, and using network image data makes it difficult to ensure reliable sources. Therefore, researchers attempt to generate image CAPTCHAs based on models. Different 2D/3D models are constructed using image modelling so that a large amount of test image data can be generated by only adjusting the model parameters [124].

A drawing CAPTCHA is a 2D model-based image CAPTCHA [113–127]. As shown in Fig. 17, it first displays points with unique shapes and noises on the screen and then lets the user find and connect them to each other. However, the noise point in a Drawing CAPTCHA is not very similar to the target object point, and so it is vulnerable to object segmentation attacks. For example, Lin et al. [128] made use of the differences between diamond shape points and interference noise points to attack and achieved a recognition rate of 75%.

Please cite this article as: X. Xu, L. Liu and B. Li, A survey of CAPTCHA technologies to distinguish between human and computer, Neurocomputing, https://doi.org/10.1016/j.neucom.2019.08.109

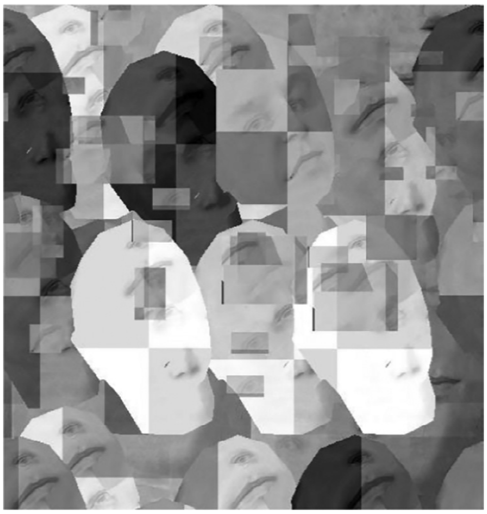


Fig. 18. Artifacial.

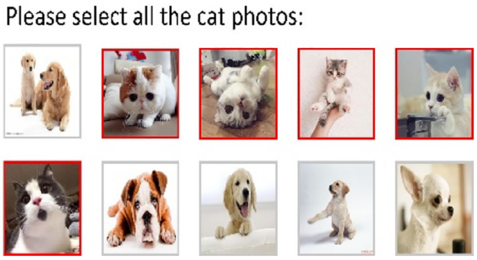


Fig. 19. Asirra CAPTCHA.

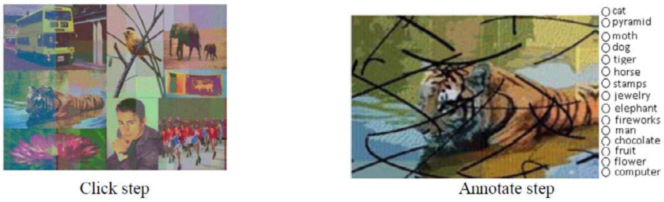


Fig. 20. IMAGINATION CAPTCHA.

Artifacial uses a more complex 2D face model [129,130] to design image CAPTCHAs based on the differences in human facial recognition abilities [131]. Aimed at the low similarity of targets and noises in Drawing CAPTCHAs, face-like noises are introduced into the image background by Artifacial, and the user needs to find the unique face and locate the facial feature points, as shown in Fig. 18. However, existing machine learning algorithms can attack them by training and learning the characteristic differences between the face-like noise and the target face in Artifacial. For example, Zhu et al. [132] reduces the difficulty of segmentation attacks by learning this feature to reduce the noise and achieves a recognition rate of 18%.

Two-dimensional/3D model-based image CAPTCHAs can generate a large amount of test image data by adjusting the model parameters, but this method is vulnerable to attacks such as machine learning and pattern matching.

3.2.2. Database-based image CAPTCHA

Because it is difficult to guarantee the security of an image CAPTCHA based on a 2D/3D model [133–136], researchers build the image database using manual labelling, and the designs of the database-based image CAPTCHA are built according to the differences between humans and machines with respect to their image recognition abilities.

(1) Based on image object recognition

Early database-based image CAPTCHAs mostly recognized generic objects, such as cats, dogs, and human faces. Chew et al. studied the image CAPTCHAs based on object recognition technology and proposed three defensive strategies for its security [137]: an increased database size, a dynamically updated database, and added interference to the image.

Collage is designed based on strategy 1 to distinguish humans from machines by letting users recognize one object in 6 annotation images [138,139]. Because Collage selected 6 labelled images randomly to compose the test data, it can effectively increase the size of the database. However, because the number and positions of the objects in the test image are fixed and there is no noise that is incorporated into the image, Collage is vulnerable to object segmentation and recognition attacks.

Based on strategy 2, Elson and others worked with Petfinder to develop an image CAPTCHA called Asirra [140]. As shown in Fig. 19 [141], users need to recognize the images of cats from 12 images of cats and dogs. To solve the high labour requirements of manual labelling, Asirra uses the image data from Petfinder's website to ensure the scale and dynamic update of the database. Here, Asirra uses multiple choice questions to expand the solution space, thus enhancing the security. Subsequently, Aggarwal et al. [142] further expands the effect of Asirra and ensures the reliability of the data through a large-scale online voting mechanism. However, Asirra is vulnerable to attacks by using image recognition technology, such as Golle et al. [40], which can distinguish cat and dog images in Asirra by simply combining colour and textural features with a recognition rate of 10.3%.

For strategy 3, Datta et al. add noise to the image and design IMAGINATION [143]. As shown in Fig. 20, IMAGINATION first uses division and jitter techniques to generate pseudo boundaries for interferences and then adds interference lines and so on to increase the difficulty of cracking the security. In addition, IMAGINATION uses a cascade structure to expand the solution space. Subsequently, Datta et al. add different kinds of noise (such as brightness changes, quantization noise, and jitter) to IMAGINATION. Furthermore, the effects of the different noises on the human-machine recognition ability were tested [139,144–146]. However, IMAGINATION only requires users to click on the centre area of any image, and even with pseudo boundary interference, it is not difficult for existing image processing algorithms to detect the boundary of only one of the 8 small images. To bypass the low requirements of IMAGINATION, a context-based object recognition attack method was proposed in Zhu et al. [132], and the recognition rate reached 4.95%.

(2) Based on semantic content comprehending

With the development of image recognition technology, the security of image CAPTCHAs based on object recognition is greatly challenged, so researchers sought to design hard AI image processing problems that were more difficult. Considering that the main differences between image CAPTCHAs and text CAPTCHAs are their presentation (image vs. text) and interaction (mouse vs. keyboard), Schryen et al. [147] systematically evaluate the objective indicators, such as the effect and efficiency of these two types of CAPTCHA, as well as the subjective indexes, such as the usability and the degree of satisfaction, and explore the reasons why image CAPTCHAs based on 2D/3D models and object recognition technology are easily attacked by image recognition algorithms. According to their research results, the early image CAPTCHAs based on 2D/3D models and object recognition technology did not make full use of the differences between human and machines using semantic content

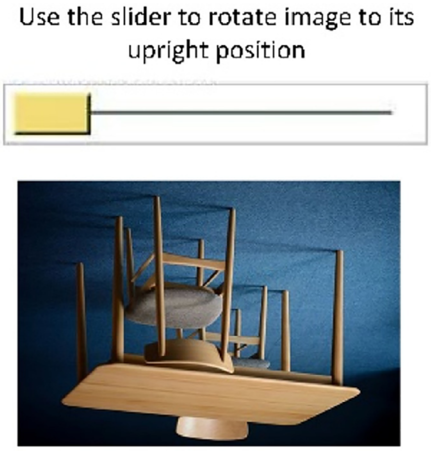


Fig. 21. What's up CAPTCHA.

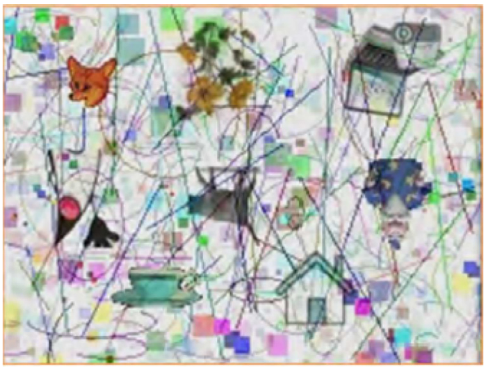


Fig. 22. Image flip CAPTCHA.

and an interactive mode. Therefore, the subsequent design of image CAPTCHAs mainly enhances the security with respect to the semantic content and interactive mode [148].

The directionality of an object is the basic content of image semantics. Gossweiler et al. [149] proposed a kind of What's Up CAPTCHA based on the image direction. As shown in Fig. 21, the user needs to detect the direction of the object in the randomly rotated test image and then uses the scroll bar to rotate the image object to the vertical direction. Banday et al. [150] further adds interference noise to the image and proposes the image Flip CAPTCHA, as shown in Fig. 22. Considering that using a 3D model can better protect against attacks such as pattern recognition than using a 2D model, Ross et al. [151] proposed a sketch 3D model called Sketcha based on direction. As shown in Fig. 23, this CAPTCHA based on object orientation can increase the testing data and improve the requirements of the solution, and the interactive operation using the scroll bar can also increase the difficulty of malicious bot program attacks. However, for symmetric images in the database, it is difficult for users to judge their orientation. By filtering these images manually, inevitably, there are high labour requirements.

SEMAGE is a kind of image CAPTCHA that is based on semantic content matching [152,153]. The user needs to understand the content of each image first and then find the semantic matching objects, such as the semantic matching image circled in Fig. 24. In Matthews et al. [154], multiple image objects are concentrated in one image using IMAGINATION, and the Scene Tagging CAPTCHA based on the relationship between multiple image objects is proposed. Unlike IMAGINATION, this kind of CAPTCHA is based on semantic content matching, and more complex nonlinear image transformation noise is used. As shown in Fig. 25, the user needs to determine the interrelationships between multiple objects in the image and enter the results into the text box.

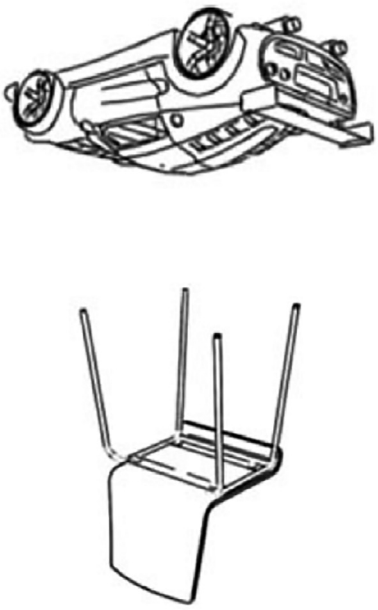


Fig. 23. Sketcha images.

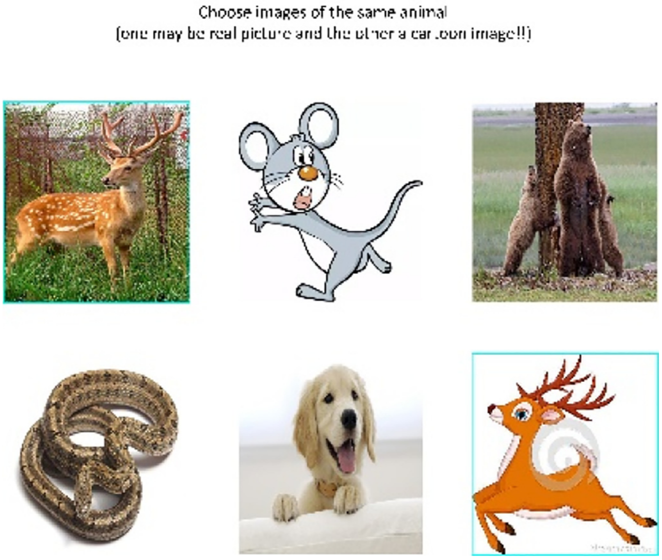

Choose images of the same animal
(one may be real picture and the other a cartoon image!!)

Fig. 24. SEMAGE CAPTCHA.

To reduce the input of the text box and improve the usability of CAPTCHA, Basso et al. [155] proposed a mosaic-based method of human-computer interaction verification, MosaHIP. As shown in Fig. 26, MosaHIP objects are randomly distributed in different locations of Mosaic images and overlaid with other image objects [156]. Users need to drag and drop the descriptive characters onto the corresponding image objects. In addition, the latest version of No CAPTCHA reCAPTCHA [114] that was developed by Google further improves the usability of image CAPTCHAs, as shown in Fig. 27.

However, the security of an image CAPTCHA, which is based on semantic content understanding, also faces the challenge of developing image recognition technology [157,158]. For example, by using deep learning technology that has been popular in recent years, Sivakorn et al. successfully cracked Google's version of No

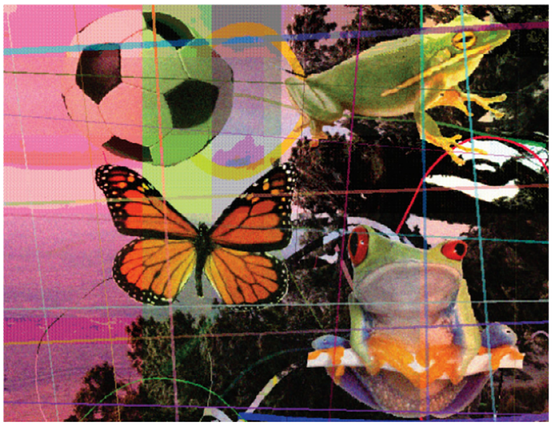
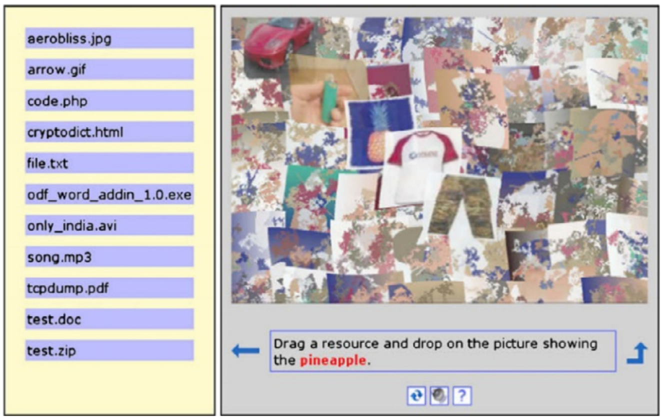


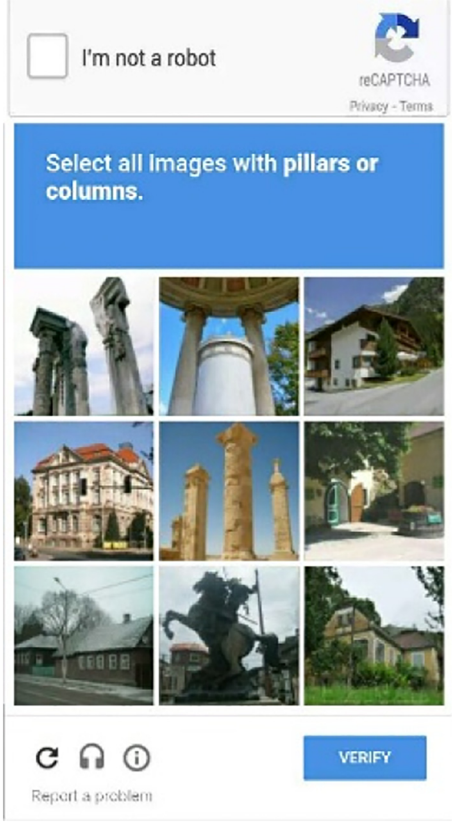
Fig. 25. Scene Tagging CAPTCHA.



aerobliss.jpg
arrow.gif
code.php
cryptodict.html
file.txt
odf_word_addin_1.0.exe
only_india.avi
song.mp3
tcpdump.pdf
test.doc
test.zip

Drag a resource and drop on the picture showing the **pineapple**.

Fig. 26. MosaHIP CAPTCHA.



□ I'm not a robot

Select all images with pillars or columns.

Fig. 27. Google's No CAPTCHA reCAPTCHA.

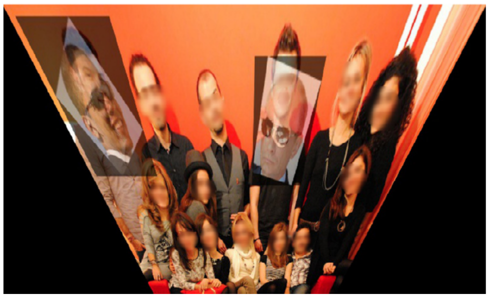


Fig. 28. Face CAPTCHA based on facebook social authentication.

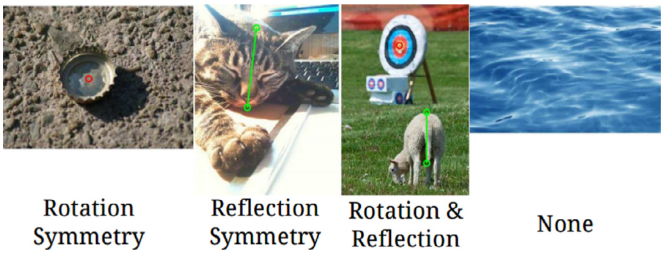


Fig. 29. Symmetry detection-based image CAPTCHA.

CAPTCHA reCAPTCHA. To improve the security of CAPTCHA, Polakis et al. [159] proposed an image selection and transformation method based on Facebook's social authentication to generate image CAPTCHAs [160,161]. In this method, with features such as being unclear, blocked, or from the back, head images of a user's friends are used to defend against the image recognition attacks of bot programs [162–164]. Users can identify their friends from these avatars based on prior knowledge [165–168], as shown in Fig. 28.

However, the security of an image CAPTCHA, which is based on semantic content understanding, also faces the challenge of developing image recognition technology. For example, by using deep learning technology that has been popular in recent years, Sivakorn et al. successfully cracked Google's version of No CAPTCHA reCAPTCHA. To improve the security of CAPTCHA, Polakis et al. proposed an image selection and transformation method based on Facebook's social authentication to generate image CAPTCHAs. In this method, with features such as being unclear, blocked, or from the back, head images of a user's friends are used to defend against the image recognition attacks of bot programs. Users can identify their friends from these avatars based on prior knowledge, as shown in Fig. 28.

To improve image CAPTCHA security, it is necessary to design more difficult hard AI image processing problems. According to the benchmark test results that were provided by CVPR 2011, the existing object recognition algorithms perform poorly in image symmetry detection. In view of this, Funk et al. [134] proposed an image symmetric reCAPTCHA based on symmetric visual perception. As shown in Fig. 29, the symmetric reCAPTCHA is designed based on different human-machine symmetric detection capabilities, which are independent of the object's type, size, shape, orientation, colour, and other image features. The experimental data that are used by a symmetric reCAPTCHA are obtained by 400 users manually annotating 1,200 Microsoft COCO images, with a total of more than 78,000 labelled symmetric image databases. The experimental results show that the symmetric reCAPTCHA has a human-machine recognition rate of over 96%.

In addition, considering that deep learning technology still has difficulty recognizing adversarial examples, Osadchy et al. proposed an image DeepCAPTCHA [170] based on adversarial noise. On the one hand, adversarial noise can effectively defend against the

Please cite this article as: X. Xu, L. Liu and B. Li, A survey of CAPTCHA technologies to distinguish between human and computer, Neurocomputing, https://doi.org/10.1016/j.neucom.2019.08.109

commonly used image preprocessing attacks so it has good security. On the other hand, for users, adversarial noise has imperceptible perturbation characteristics. Therefore, the adversarial examples containing adversarial noise are almost exactly the same as the original image, so DeepCAPTCHA will have better usability than the existing CAPTCHA with interference noise.

In summary, the image CAPTCHA based on semantic content understanding needs to identify most objects in the image, so it can effectively improve the comprehension requirements. Furthermore, the multi-object combination can increase the size of the database. However, these CAPTCHAs rely on image data with annotations, and manual annotations require extensive labour, thus resulting in a limited image database size.

3.3. Sound CAPTCHA

Sound CAPTCHAs are usually used as an aid to text and image CAPTCHAs for the convenience of the visually impaired [171–173]. As shown in Figs. 16 and 27, Google's version of No CAPTCHA reCAPTCHA is equipped with sound CAPTCHAs in text and image CAPTCHAs [174]. Many other portals are also using text and image CAPTCHAs along with sound CAPTCHAs, such as eBay, Yahoo and Microsoft [175,176].

From the perspective of human-computer interaction, the existing sound CAPTCHAs are mainly divided into keyboard inputs [1] and voice retelling [177]. Voice retelling is more usable than keyboard inputs. For example, Von et al. [1] uses spoken CAPTCHAs for the convenience of human users with visual impairments. Shirali-Shahreza et al. [178] further designed HearSay and SeeSay CAPTCHAs on a smartphone app and provided the interaction mode of voice retelling for the visually impaired and visually intact. With respect to the keyboard input method, Bigham et al. [179] add voice playback controls in the input text box for the convenience of the users. Lazar et al. [180] also proposed a real-time voice recognition SoundsRight CAPTCHA based on the differences in the speed of human-computer recognition of sound signals. However, these methods still have limited effects on improving the usability of sound CAPTCHAs, and the way that GPUs are adopted by Xu et al. [181] to improve the recognition speed is also expected to be used to attack SoundsRight CAPTCHAs.

From the perspective of security, sound CAPTCHAs are mainly based on the differences between humans and machines with respect to their sound recognition abilities [182]. Therefore, the existing methods generally improve security by adding interference noise. For example, Kochanski et al. used 18 different kinds of interference noise to protect against bot program attacks [148]. Chan et al. reduce the sound recognition rate of bot programs by adding background noise [183]. Sauer et al. defend against checksum and signature attacks by adding silent states [61]. Soupionis et al. use different voice signals, background noises, and random noises to enhance the security of sound CAPTCHAs, which are used for network voice call verification [184,185].

However, because the human visual system occupies more brain space than the human auditory system, the security of sound CAPTCHAs is weaker than that of text CAPTCHAs and image CAPTCHAs [4,186]. Bursztein et al. attacked the sound CAPTCHAs that are used by the eBay, Authorize, Yahoo and Microsoft websites by analysing the difference between the background noise and target signal, thus reaching 82%, 89%, 45.5% and 49% recognition rates, respectively [175]. This attack is based on low-pass RMS filtering and eliminates the constant background noise and conduct object segmentation. The sound signal corresponds to the position of the remaining wave peak, and finally it can be identified by the classifier.

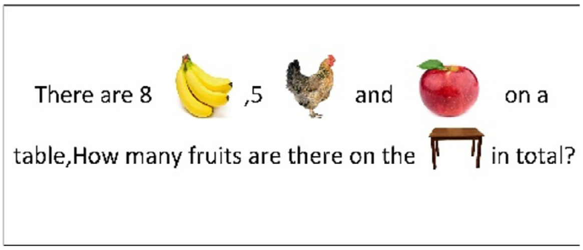

There are 8 ,5 and on a table,How many fruits are there on the in total?

Fig. 30. Question-based CAPTCHA.

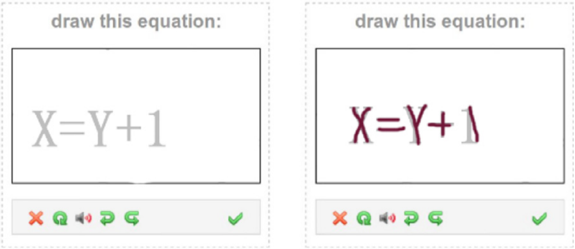


Fig. 31. μcaptcha challenge.

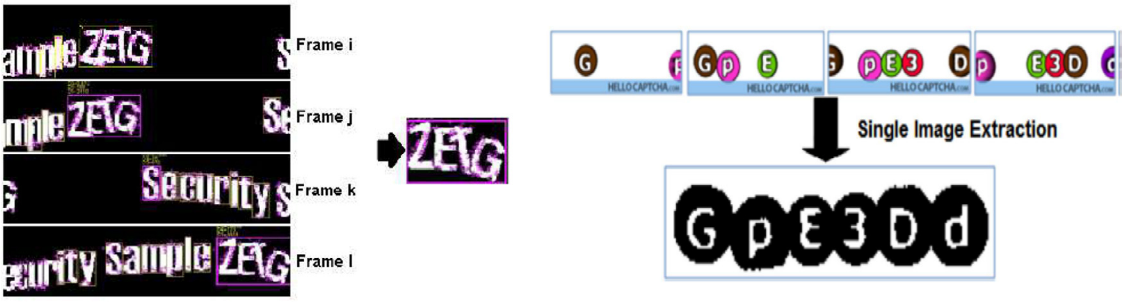
Although the interference noise that used by Google reCAPTCHA, which is better at defending against sound preprocessing attacks, has features similar to sound signals, with the continuous development of machine learning technology in recent years, the security of such sound CAPTCHAs is seriously threatened. For example, Tam et al. use a window with a fixed length to search target audio and identify it by using the peak energy [187]. Based on the three features of extracting the MEL inverse spectral coefficient, the perceptive linear prediction and the correlation spectrum conversion - perceptive linear prediction of the window's audio, Adaboost, SVM and k-NN machine learning [188–190] methods are used to successfully attack the voice CAPTCHAs of Google, Digg and reCAPTCHA, thus reaching 67%, 71% and 45% recognition rates, respectively. Based on the automatic speech recognition method, Meutzner et al. further improved the attack effect on reCAPTCHA [191,192]. This attack method is designed mainly based on the difference in the reverberation tolerance between humans and machines, and it achieves a recognition rate of 62.8%. Subsequently, Meutzner et al. design a sound CAPTCHA [193] based on this difference in human-machine tolerances. However, the security of this sound CAPTCHA will also be greatly challenged with the continuous development of machine learning algorithms [194–196].

3.4. Other types

(1) Math CAPTCHA

Math CAPTCHAs are designed based on the differences in the ability of humans and machines in solving mathematical problems. Such as with the question-based CAPTCHA [197], as shown in Fig. 30, most of the early mathematical CAPTCHAs used basic arithmetic operations (such as addition, subtraction, multiplication, etc.) combined with information such as text and images. Later, researchers successively introduced more complex mathematical operations such as integrations and polynomials, but this also raised the requirements on users' mathematical abilities, so the usability of such mathematical CAPTCHAs is limited. In view of this outcome, the literature proposes a kind of handwritten mathematical sketch called a μcaptcha, which is similar to the drawing CAPTCHA [198]. The μcaptcha does not require a user to have any background in mathematics, but only uses a mouse or touch screen to draw a mathematical formula in the presence of an interference line, as shown in Fig. 31. However, with the continuous development of OCR technology in recent years, the security of mathematical CAPTCHAs also faces great challenges. Hernandez-Castro et al.

Please cite this article as: X. Xu, L. Liu and B. Li, A survey of CAPTCHA technologies to distinguish between human and computer, Neurocomputing, https://doi.org/10.1016/j.neucom.2019.08.109



(a) (b)

Fig. 32. Attacking way of motion CAPTCHA: (a) NUCAPTCHA attacking; (b) HelloCAPTCHA attacking.

[199] proposed a black-box attack method for these mathematical CAPTCHAs, which was mainly designed based on the nonuniformly distributed CAPTCHA parameters (including input parameters, selection functions, distribution of correct answers, etc.).

(2) Motion CAPTCHA

Motion CAPTCHAs are designed on the basis of human and machine ability differences in tasks, such as identifying moving objects, dynamic characters, or video fragments [200–202]. There are relatively few studies on such CAPTCHAs. Currently, NUCAPTCHA1and HelloCAPTCHA2 are widely used. On the one hand, attacks against motion CAPTCHAs are more difficult than text and image CAPTCHAs because the segmentation and identification of dynamic targets is more complex than static targets [203,204]. On the other hand, the attacks for motion CAPTCHAs can also be more accurate because the target will appear in multiple video images.

From the perspective of security analysis, the main idea of attacks against motion CAPTCHAs is to locate key frames from a video to transform a video processing problem into a text or image processing problem. As shown in Fig. 32, Bursztein et al. [205] and Nguyen et al. [206] designed attack methods against NUCAPTCHA and HelloCAPTCHA, thus reaching recognition rates of 83% and 16-100%, respectively. Such attacks are designed primarily for attacking the design flaws in NUCAPTCHA and HelloCAPTCHA, including the significant differences in the text and noise features, fixed character lengths or positions, improper colour usage, video frame lengths, and delay fixations.

Xu et al. further studied the security and usability of NuCaptcha with different noise interferences (such as overlapping characters and emerging images [207]) [181,208]. The results show that the traditional motion CAPTCHA (such as NuCaptcha) is based on detecting persistent or slowly changing targets, which makes it vulnerable to computer vision algorithm attacks, and GPU implementation can even be faster than manual recognition. The emergent CAPTCHA can effectively improve security, as shown in Fig. 33. On the one hand, the single frame image in an emergent captcha lacks enough information for target recognition. On the other hand, the time series changes between video frames also increase the difficulty of the correlation analysis between video frames.

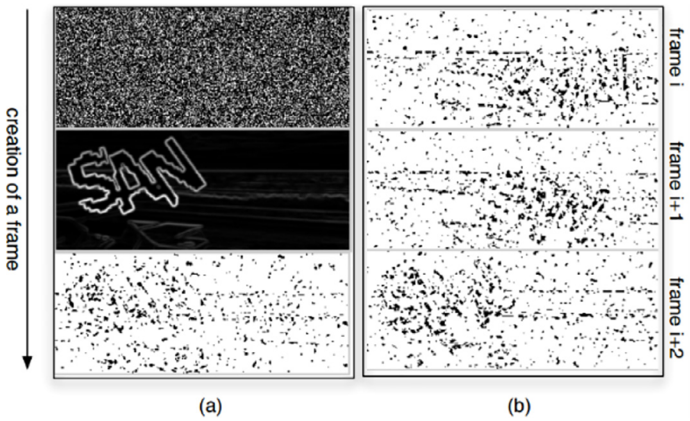
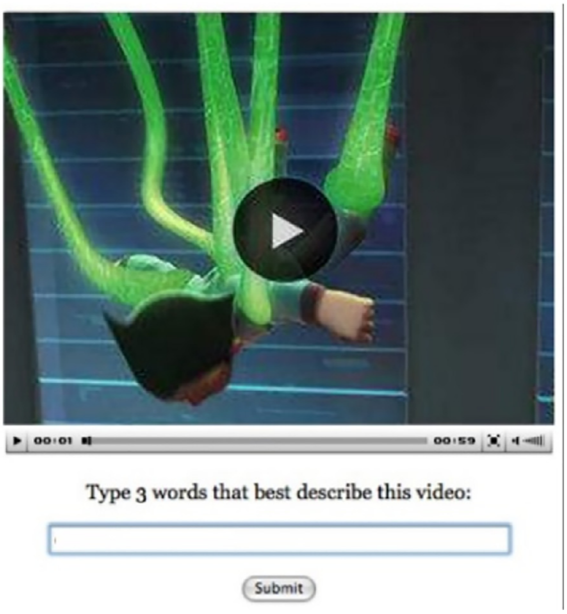


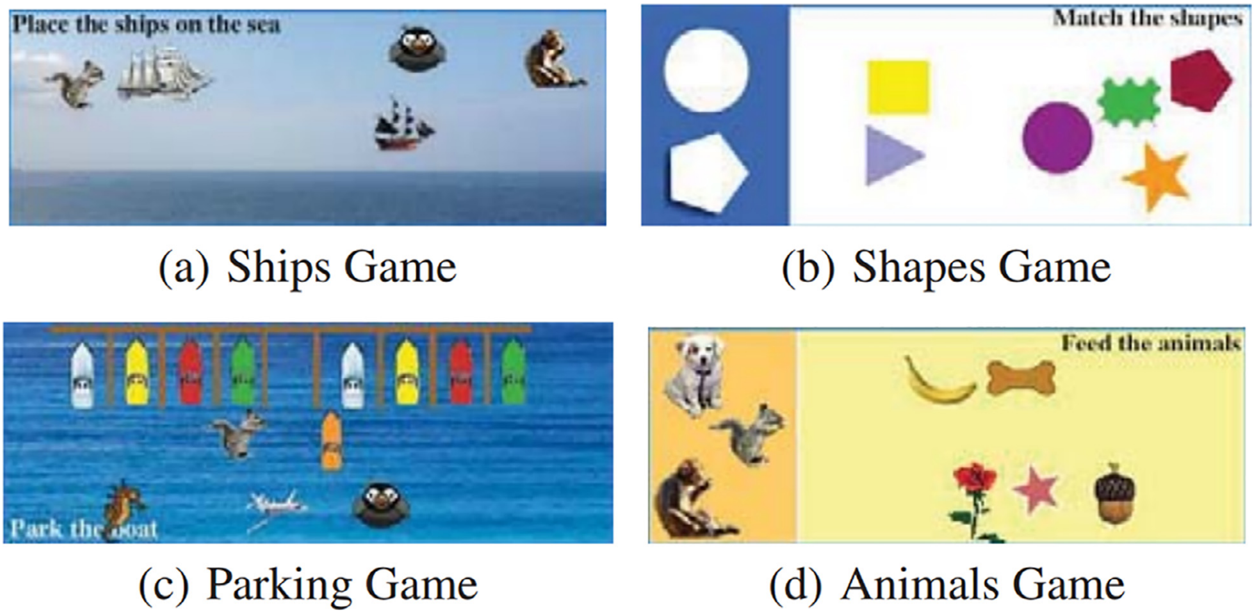
Fig. 33. Emerging CAPTCHA: (a) Top: noisy background frame. Middle: derivative of foreground image. Bottom: singleframe for an Emerging captcha. (b) Successive frames



Type 3 words that best describe this video:

Fig. 34. YouTube video CAPTCHA.

Kluever et al. proposed a video CAPTCHA based on semantic annotations [209]. This kind of CAPTCHA uses YouTube videos with label information. By letting the user describe the video with three words, it can conduct human-machine identification according to the difference in the semantic comprehension ability of humans and machines with respect to videos, as shown in Fig. 34. Since YouTube videos have been provided with label information by the uploader, the size and dynamic update of the video database can be effectively guaranteed. However, this CAPTCHA is vulnerable to the attacking of video preprocessing and video retrieval, and the voice signals in video also provide auxiliary information for attacking [209]. In view of this, Bursztein proposed a scheme to improve the security of motion CAPTCHA by introducing a moving background to confuse the target [205]. However, foreground target detection has long been a research topic in the field of computer vision, and so this scheme may be attacked by video preprocessing and other methods.



(a) Ships Game (b) Shapes Game

(c) Parking Game (d) Animals Game

Fig. 35. DCG CAPTCHA: targets are static, but the objects are dynamic.

(3) Game CAPTCHA

In order to improve the usability of CAPTCHAs, researchers tried to design CAPTCHAs according to the differences between humans and machines when playing games. The goal of the game CAPTCHAs is to allow users to handle CAPTCHAs with ease while effectively defending against malicious bot programs. At present, there are relatively few studies on game CAPTCHAs [29], and the typical example is the dynamic cognitive game (DCG) [210]. As shown in Fig. 35, the DCG CAPTCHA allows human users to interact with a series of dynamic images for human-machine recognition

Mohamed et al. [211] is the first investigation to study the security and usability of the DCG CAPTCHA. According to the experimental results, the DCG CAPTCHA can effectively protect against relay attacks from third parties while providing high usability. However, the DCG CAPTCHA is vulnerable to automatic dictionary attacks. Aiming to address this problem, Emerging Images (EI) [207] technology was utilized in the motion CAPTCHA to effectively defend against automatic dictionary attacks [212]. Recently, with the development of deep reinforcement learning technology, programs have gradually exceeded users' abilities to handle game CAPTCHAs [170]. The security of game CAPTCHAs is also facing great challenges.

3.5. *CAPTCHA performance towards genetic attacking*

In order to evaluation the performance of different CAPTCHA methods, we collect various CAPTCHAs on the web and test their robustness towards genetic attacking methods.

The robustness of a CAPTCHA can be evaluated by investigating its ability to defend the possible attack. As text-based CAPTCHAs is the most commonly used type of CAPTCHA, and is related to most of other CAPTCHA technologies. Many defending strategies may be mentioned in one type of CAPTCHA, but can be applicable to other types as well.

(1) Object segmentation defending

The CAPTCHA object segmentation, which conducts after the preprocessing step, is usually combined with the vertical histogram, color filling, snake and other methods. The preprocessing step mainly removes noise interference, such as background patterns and connecting arcs, to facilitate CAPTCHA object segmentation.

Accordingly, the object segmentation defending of a CAPTCHA can be improved by introducing strategies to the test data to make segmentation harder. Typical method includes applying degradations, e.g. character overlapping, masking operations. Another method is utilizing background clutter, e.g. arcs, variety clutters. Other methods include utilizing different colors, false boundaries, and etc.

(2) Object recognition defending

Although object segmentation influence the attacking of CAPTCHA to a large extent, defending against object recognition can also be designed to improve CAPTCHA robustness.

Object recognition attacking generally includes pixel statistics and dictionary attacking. Accordingly, the object recognition defending of a CAPTCHA can be improved by introducing strategies to the test data to make recognition harder. Typical method utilizes different style/fonts to defend pattern recognition attacks. Another method uses visually similar but semantically different characters/images/audio to confuse pattern recognition techniques. Other methods include using random data, removing or deforming features.

4. Conclusion and future work

In summary, it is generally recognized in the field of network security that CAPTCHA design with both security and usability has become increasingly difficult [170,213]. According to the literature review [4,30,214,215], most of the existing CAPTCHAs use highly differentiated objects in their tests, which are vulnerable to being exploited by programs. Considering that users can more easily identify subtle differences between similar objects than machines [128], current research focuses on using similar objects for man-machine discrimination tests. For example, Google's No CAPTCHA reCAPTCHA [114] takes this approach and provides text, images, and sound CAPTCHAs with good security and usability.

However, No CAPTCHA has actually violated several important CAPTCHA and general security principles in its design. For example, the letter P in CAPTCHA stands for Public, while No CAPTCHA does not expose the internal functions that it uses. Instead, it uses many convoluted Javascript codes to realize the concept of "hidden security". Nevertheless, No CAPTCHA has been cracked by deep learning technology in recent years [119]. In view of this outcome, on the one hand, a few works [114,128,175] that adopt this scheme tend to limit the number of similar objects. On the other hand, with the continuous progress of deep learning technology, the security of such schemes also faces great challenges.

To improve the security of CAPTCHA, the future design of CAPTCHA needs to focus on defence against attacks by algorithms such as deep learning [216]. The purpose of deep learning is to learn multilayer feature representations and abstractions from different types of data, among which the convolution neural network [217–219] has been successfully applied to image classification [220,221] and other tasks since 1989 [222]. In recent years, AlexNet [223] has further improved the architecture of the CNN and significantly improved the classification effect. It has been widely used to train CNNs on GPUs. However, deep learning technology currently is limited when facing hard AI image processing problems, such as symmetry [169] and adversarial examples [170,224]. Therefore, how to design CAPTCHAs with respect to the defects of deep learning is a possible future research direction, such as the work carried out in Osadchy et al. [170].

Acknowledgements

This work was supported by the Natural Science Foundation of China (61602349 and 61572381).

References

[1] L. Von Ahn, M. Blum, J. Langford, Telling humans and computers apart automatically, Commun. ACM (2004) 56–60.
[2] L. Von Ahn, M. Blum, N.J. Hopper, J. Langford, CAPTCHA: Using hard AI problems for security, in: Advances in Cryptology—EUROCRYPT, Springer, 2003, pp. 294–311.
[3] H.S. Baird, A.L. Coates, R.J. Fateman, PessimalPrint: a reverse Turing test, Int. J. Doc. Anal. Recogn. (2003) 158–163.
[4] N. Roshanbin, J. Miller, A survey and analysis of current CAPTCHA approaches, J. Eng. (2013) 1–40.
[5] C. Lu, D.S. Huang, Optimized projections for sparse representation based classification, Neurocomputing (2013) 213–219.
[6] C. Zheng, D.S. Huang, L. Shang, Feature selection in independent component subspace for microarray data classification, Neurocomputing (2006) 2407–2410.
[7] C. Zheng, D.S. Huang, K. Li, G.W Irwin, Z. Sun, MISEP method for Post-Nonlinear Blind Source Separation, Neural Comput. (2007) 2557–2578.
[8] D.S. Huang, S.D. Ma, Linear and nonlinear feedforward neural network classifiers: A comprehensive understanding, J. Intell. Syst. (1999) 1–38.
[9] D.S. Huang, X. Zhao, G. Huang, Y. Cheung, Classifying protein sequences using hydropathy blocks, Pattern Recognit. (2006) 2293–2300.
[10] K. Liu, D.S. Huang, Cancer classification using rotation forest, Comput. Biol. Med. (2008) 601–610.
[11] M. T. Banday and N. A. Shah, "A study of captchas for securing web services," arXiv preprint arXiv:1112.5605, 2011.
[12] O. Longe, A. Robert, U. Onwudebelu, Checking Internet masquerading using multiple CAPTCHA challenge-response systems, in: Proceedings of the 2nd International Conference on Adaptive Science & Technology ICAST, 2009, pp. 244–249.
[13] J. Yan, A.S. El Ahmad, Captcha robustness: A security engineering perspective, Computer (2011) 54–60.
[14] B.S. Saini, A. Bala, A review of bot protection using CAPTCHA for web security, IOSR J. Comput. Eng. (2013) 36–42.
[15] C. Tangmanee, P. Sujarit-apirak, Attitudes towards CAPTCHA: A survey of Thai internet users, J. Global Bus. Manag. (2013) 29.
[16] C. J. Hernández-Castro, D. F. Barrero, and S. Li, An oracle-based attack on CAPTCHAs protected against oracle attacks, arXiv preprint arXiv:1702.03815, 2017.
[17] P. He, Y. Sun, W. Zheng, X. Wen, Filtering short message spam of group sending using CAPTCHA, in: Proceedings of the First International Workshop on Knowledge Discovery and Data Mining WKDD, 2008, pp. 558–561.
[18] C. Zheng, D.S. Huang, Z. Sun, M. Lyu, T. Lok, Nonnegative independent component analysis based on minimizing mutual information technique, Neurocomputing (2006) 878–883.
[19] D.S. Huang, The Study of Data Mining Methods for Gene Expression Profiles, Science Press of China, 2009.
[20] F. Han, D.S. Huang, Improved extreme learning machine for function approximation by encoding a priori information, Neurocomputing (2006) 2369–2373.
[21] F. Han, D.S. Huang, A new constrained learning algorithm for function approximation by encoding a priori information into feedforward neural networks, Neural Comput. Appl. (2008) 433–439.
[22] J. Yan, Bot, cyborg and automated Turing test, in: Proceedings of the International Workshop on Security Protocols, 2006, pp. 190–197.
[23] H.S. Baird, K. Popat, Human interactive proofs and document image analysis, in: Proceedings of the International Workshop on Document Analysis Systems, 2002, pp. 507–518.
[24] Y. Soupionis, G. Tountas, D. Gritzalis, Audio CAPTCHA for SIP-based VoIP, in: Proceedings of the IFIP International Information Security Conference, 2009, pp. 25–38.
[25] J. Yan, A.S. El Ahmad, Usability of CAPTCHAs or usability issues in CAPTCHA design, in: Proceedings of the 4th Symposium on Usable Privacy and Security, 2008, pp. 44–52.
[26] K. Chellapilla, K. Larson, P.Y. Simard, M. Czerwinski, Building segmentation based human-friendly human interaction proofs (HIPs), in: Human Interactive Proofs, Springer, 2005, pp. 1–26.
[27] V.P. Singh, P. Pal, Survey of different types of CAPTCHA, Int. J. Comput. Sci. Inf. Technol. (2014) 2242–2245.
[28] P. Lupkowski, M. Urbanski, SemCAPTCHA—user-friendly alternative for OCR-based CAPTCHA systems, in: Proceedings of the Computer Science and Information Technology, 2008. IMCSIT 2008. International Multiconference on, 2008, pp. 325–329.
[29] P. Golle, N. Ducheneaut, Keeping bots out of online games, in: Proceedings of the ACM SIGCHI International Conference on Advances in Computer Entertainment Technology, 2005, pp. 262–265.
[30] Q. Li, Y. Mao, Z. Wang, A Survey of CAPTCHA Technology, J. Comput. Res. Devel. 49 (3) (2012) 469–480.
[31] L. Shang, D.S. Huang, C. Zheng, Z. Sun, Noise removal using a novel non-negative sparse coding shrinkage technique, Neurocomputing (2006) 874–877.
[32] P. Simard, Using machine learning to break visual human interaction proofs (hips), in: Proceedings of the Advances in Neural Information Processing Systems, 2005, pp. 265–272.
[33] J. Yan, A.S. El Ahmad, A Low-cost Attack on a Microsoft CAPTCHA, in: Proceedings of the 15th ACM Conference on Computer and Communications Security, 2008, pp. 543–554.
[34] Z. Sun, D.S. Huang, Y. Cheung, Extracting nonlinear features for multispectral images by FCMC and KPCA, Digit. Signal Process. (2005) 331–346.
[35] Z. Sun, D.S. Huang, Y. Cheung, J. Liu, G. Huang, Using FCMC, FVS and PCA techniques for feature extraction of multispectral images, IEEE Geosci. Remote Sens. Lett. (2005) 108–112.
[36] Z. Zhao, D.S. Huang, A mended hybrid learning algorithm for radial basis function neural networks to improve generalization capability, Appl. Math. Modell. (2007) 1271–1281.
[37] Z. Zhao, D.S. Huang, Palmprint recognition with 2DPCA+PCA based on modular neural networks, Neurocomputing (2007) 448–454.
[38] J. Yan, A.S. El Ahmad, Breaking visual captchas with naive pattern recognition algorithms, in: Proceedings of the Computer Security Applications Conference ACSAC Twenty-Third Annual, 2007, pp. 279–291.
[39] J. Yan, A.S. El Ahmad, CAPTCHA security: a case study, IEEE Secur. Privacy (2009) 22–28.
[40] P. Golle, Machine learning attacks against the Asirra CAPTCHA, in: Proceedings of the 15th ACM Conference on Computer and Communications Security, 2008, pp. 535–542.
[41] C.A. Fidas, A.G. Voyiatzis, N.M. Avouris, On the necessity of user-friendly CAPTCHA, in: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM, 2011, pp. 2623–2626.
[42] R. Bergmair, S. Katzenbeisser, Towards human interactive proofs in the text-domain, in: Proceedings of the International Conference on Information Security, 2004, pp. 257–267.
[43] K. R. Soumya and R. M. Abraham, A Survey on Different CAPTCHA Techniques, 2014.
[44] Y.-L. Lee, C.-H. Hsu, Usability study of text-based CAPTCHAs, Displays (2011) 81–86.
[45] P.B. Godfrey, Text-based CAPTCHA algorithms, in: Proceedings of the First Workshop on Human Interactive Proofs, 2002, pp. 8–19.
[46] C. Obimbo, A. Halligan, P. De Freitas, CaptchAll: an improvement on the modern text-based CAPTCHA, Procedia Comput. Sci. (2013) 496–501.
[47] Z. Sun, D.S. Huang, C. Zheng, L. Shang, Optimal selection of time lags for temporal blind source separation based on genetic algorithm, Neurocomputing (2006) 884–887.
[48] S. Sharma, N. Seth, Survey of Text CAPTCHA Techniques and Attacks, Int. J. Eng. Trends. Technol. (2015).
[49] A.A. Chandavale, A.M. Sapkal, R.M. Jalnekar, Algorithm to break visual CAPTCHA, in: Proceedings of the 2nd International Conference on Emerging Trends in Engineering and Technology (ICETET), 2009, pp. 258–262.
[50] A.A. Chandavale, A.M. Sapkal, Algorithm for secured online authentication using CAPTCHA, in: Proceedings of the 3rd International Conference on Emerging Trends in Engineering and Technology (ICETET), 2010, pp. 292–297.
[51] H.S. Baird, M. Luk, Protecting Websites with Reading-Based CAPTCHAs, in: Proceedings of the Second International Web Document Analysis Workshop, 2003.
[52] S. Azad, K. Jain, CAPTCHA: Attacks and Weaknesses against OCR technology, Global J. Comput. Sci. Technol. (2013).

[53] X. Ling-Zi, Z. Yi-Chun, A case study of text-based CAPTCHA attacks, in: Proceedings of the International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2012, pp. 121–124.

[54] M. Blum, L. Von Ahn, J. Langford, N. Hopper, The CAPTCHA project, Completely Automatic Public Turing test to Tell Computers and Humans apart,, School of Computer Science, Carnegie-Mellon University, 2000.

[55] R. Beede, Analysis of reCAPTCHA effectiveness, University of Colorado at Boulder, 2010.

[56] G. Mori, J. Malik, Recognizing objects in adversarial clutter: Breaking a visual CAPTCHA, in: Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2003 I-134-I-141.

[57] G. Moy, N. Jones, C. Harkless, R. Potter, Distortion estimation techniques in solving visual CAPTCHAs, in: Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition CVPR, 2004 II-23-II-28.

[58] R.A. Nachar, E. Inaty, P.J. Bonnin, Y. Alayli, Breaking down Captcha using edge corners and fuzzy logic segmentation/recognition technique, Security and Communication Networks (2015) 3995–4012.

[59] T. Converse, CAPTCHA generation as a web service, in: Human Interactive Proofs, Springer, 2005, pp. 82–96.

[60] M. Chew, H.S. Baird, Baffletext: A human interactive proof, in: Proceedings of the Electronic Imaging, 2003, pp. 305–316.

[61] G. Sauer, H. Hochheiser, J. Feng, J. Lazar, Towards a universally usable CAPTCHA, in: Proceedings of the 4th Symposium on Usable Privacy and Security, 2008, p. 1.

[62] A.S. Almazyad, Y. Ahmad, S.A. Kouchay, Multi-modal captcha: A user verification scheme, in: Proceedings of the International Conference on Information Science and Applications (ICISA), 2011, pp. 1–7.

[63] S.B.E. Raj, D. Devassy, J. Jagannivas, A new architecture for the generation of picture based CAPTCHA, in: Proceedings of the 3rd International Conference on Electronics Computer Technology (ICECT), 2011, pp. 67–71.

[64] C. Pope, K. Kaur, Is it human or computer? Defending e-commerce with captchas, IT Profess. (2005) 43–49.

[65] L. Von Ahn, B. Maurer, C. McMillen, D. Abraham, M. Blum, recaptcha: Human-based character recognition via web security measures, Science (2008) 1465–1468.

[66] M. Chew, J.D. Tygar, Collaborative filtering captchas, in: Human Interactive Proofs, Springer, 2005, pp. 66–81.

[67] T. Yamamoto, J.D. Tygar, M. Nishigaki, CAPTCHA using strangeness in machine translation, in: Proceedings of the 24th IEEE International Conference on Advanced Information Networking and Applications (AINA), 2010, pp. 430–437.

[68] J. Wilkins, "Strong captcha guidelines v1. 2," http://bitland.net/captcha.pdf. 2010, p. 8.

[69] O. Starostenko, C. Cruz-Perez, F. Uceda-Ponga, V. Alarcon-Aquino, Breaking text-based CAPTCHAs with variable word and character orientation, Pattern Recognit. (2015) 1101–1112.

[70] I.J. Goodfellow, Y. Bulatov, J. Ibarz, S. Arnoud, V. Shet, Multi-digit number recognition from street view imagery using deep convolutional neural networks, in: Proceedings of the CoRR, 2013 abs/1312.6082.

[71] J. Du, D.S. Huang, G. Zhang, Z. Wang, A novel full structure optimization algorithm for radial basis probabilistic neural networks, Neurocomputing (2006) 592–596.

[72] J. Du, D.S. Huang, X. Wang, X. Gu, Computer-aided plant species identification (CAPSI) based on leaf shape matching technique, Trans. Inst. Meas. Control (2006) 275–284.

[73] J. Du, D.S. Huang, X. Wang, Xiao Gu, Shape recognition based on neural networks trained by differential evolution algorithm, Neurocomputing (2007) 896–903.

[74] K. Liu, R. Zhang, K. Qing, CNN for breaking text-based CAPTCHA with noise, in: Proceedings of the Ninth International Conference on Digital Image Processing (ICDIP 2017), 2017.

[75] J. Hu, W. Ma, A. Khan, L. Liu, Recognizing Character-Matching CAPTCHA Using Convolutional Neural Networks with Triple Loss, in: Proceedings of the International Conference on Knowledge Science, Engineering and Management, 2018, pp. 209–220.

[76] J. Bentley and C. Mallows, CAPTCHA challenge strings: Problems and improvements, in Proceedings of the Document Recognition and Retrieval XIII. 2006, p. 60670H: International Society for Optics and Photonics.

[77] K. Chellapilla, K. Larson, P. Simard, M. Czerwinski, Designing human friendly human interaction proofs (HIPs), in: Proceedings of the SIGCHI Conference on Human factors in Computing Systems, 2005, pp. 711–720.

[78] M. Shirali-Shahreza, Highlighting captcha, in: Proceedings of the Conference on Human System Interactions, 2008, pp. 247–250.

[79] Y. Nakaguro, M.N. Dailey, S. Marukatat, S.S. Makhanov, Defeating line-noise CAPTCHAs with multiple quadratic snakes, Comput. Secur. (2013) 91–110.

[80] S. Li, S. Shah, M. Khan, S.A. Khayam, A.-R. Sadeghi, R. Schmitz, Breaking e-banking CAPTCHAs, in: Proceedings of the 26th Annual Computer Security Applications Conference, 2010, pp. 171–180.

[81] T. Men, Y. Sun, D. Wang, M. Wang, A novel dynamic CAPTCHA based on inverted colors, in: Proceedings of the 2nd International Symposium on Instrumentation and Measurement, Sensor Network and Automation (IMSNA), 2013, pp. 796–799.

[82] H. Gao, W. Wang, J. Qi, X. Wang, X. Liu, J. Yan, The robustness of hollow CAPTCHAs, in: Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, 2013, pp. 1075–1086.

[83] A.O. Thomas, A. Rusu, V. Govindaraju, Synthetic handwritten captchas, Pattern Recognit. 42 (12) (2009) 3365–3373.

[84] A. Rusu, A. Thomas, V. Govindaraju, Generation and use of handwritten CAPTCHAs, Int. J. Document Anal. Recognit. (IJDAR) 13 (1) (2010) 49–64 2010.

[85] D.S. Huang, Systematic Theory of Neural Networks for Pattern Recognition, Publishing House of Electronic Industry of China, 1996.

[86] D.S. Huang, Radial basis probabilistic neural networks: Model and application, Int. J. Pattern Recognit Artif Intell. (1999) 1083–1101.

[87] J.Du D.S.Huang, A constructive hybrid structure optimization methodology for radial basis probabilistic neural networks, IEEE Trans. Neural Netw. (2008) 2099–2115.

[88] D.S. Huang, A constructive approach for finding arbitrary roots of polynomials by neural networks, IEEE Trans. Neural Netw. (2004) 477–491.

[89] D.S. Huang, H. H.S.Ip, Z. Chi, Zeroing polynomials using modified constrained neural network approach, IEEE Trans. Neural Netw. (2005) 721–732.

[90] D.S. Huang, J. Mi, A new constrained independent component analysis method, IEEE Trans. Neural Netw. (2007) 1532–1535.

[91] D.S. Huang, W.B. Zhao, Determining the centers of radial basis probabilistic neural networks by recursive orthogonal least square algorithms, Appl. Math. Comput. (2005) 461–473.

[92] W. Jiang, D.S. Huang, S. Li, Random-walk based solution to triple level stochastic point location problem, IEEE Trans. Cybern. (2016) 1438–1451.

[93] X. Wang, D.S. Huang, H. Xu, An efficient local Chan-Vese model for image segmentation, Pattern Recognit. (2010) 603–618.

[94] X. Wang, D.S. Huang, A novel density-based clustering framework by using level set method, IEEE Trans. Knowl. Data Eng. (2009) 1515–1531.

[95] X. Wang, D.S. Huang, A novel multi-layer level set method for image segmentation, J. Univ. Comput. Sci. (2008) 2428–2452.

[96] X. Xu, J. Zhou, H. Zhang, X. Fu, Chinese Characters Recognition from Screen-Rendered Images Using Inception Deep Learning Architecture, in: Proceedings of the Pacific Rim Conference on Multimedia, 2017, pp. 722–732.

[97] H.S. Baird, M.A. Moll, S.-Y. Wang, ScatterType: A legible but hard-to-segment CAPTCHA, in: Proceedings of the 8th International Conference on Document Analysis and Recognition, 2005, pp. 935–939.

[98] A.S. El Ahmad, J. Yan, L. Marshall, The robustness of a new CAPTCHA, in: Proceedings of the Third European Workshop on System Security, 2010, pp. 36–41.

[99] E. Bursztein, M. Martin, J. Mitchell, Text-based CAPTCHA strengths and weaknesses, in: Proceedings of the 18th ACM Conference on Computer and Communications Security, 2011, pp. 125–138.

[100] E. Bursztein, J. Aigrain, A. Moscicki, J.C. Mitchell, The end is nigh: Generic solving of text-based captchas, in: Proceedings of the 8th USENIX Workshop on Offensive Technologies (WOOT 14), 2014.

[101] J. Zhang, D.S. Huang, T. Lok, M. Lyu, A novel adaptive sequential niche technique for multimodal function optimization, Neurocomputing (2006) 2396–2401.

[102] H. Gao, Robustness of text-based completely automated public turing test to tell computers and humans apart, Inf. Secur. IET 10 (1) (2016) 45–52.

[103] H. Gao, A Simple Generic Attack on Text Captchas, in: Proceedings of the Network and Distributed System Security Symposium (NDSS), San Diego, USA, 2016.

[104] S.D. Bhalani, S. Mishra, A survey on CAPTCHA technique based on drag and drop mouse action, Int. J. Tech. Res. Appl. 3 (2) (2015) 188–189.

[105] D. George, A generative vision model that trains with high data efficiency and breaks text-based CAPTCHAs, Science 358 (6368) (2017) 2612-2017.

[106] A. Desai, P. Patadia, Drag and drop: a better approach to captcha, in: Proceedings of the Annual IEEE India Conference, 2009, pp. 1–4.

[107] A. Gupta, A. Jain, A. Raj, A. Jain, Sequenced tagged captcha: Generation and its analysis, in: Proceedings of the IEEE International Advance Computing Conference IACC, 2009, pp. 1286–1291.

[108] A. Raj, A. Jain, T. Pahwa, A. Jain, Analysis of tagging variants of Sequenced Tagged Captcha (STC), in: Proceedings of the IEEE Toronto International Conference Science and Technology for Humanity (TIC-STH), 2009, pp. 427–432.

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

[110] N.A. Shah, M.T. Banday, Drag and drop image captcha, in: Proceedings of 4th J&K Science Congress 12th to 14th, Srinagar, India, 2008.

[111] A. James, G. George, A. Yeldose, A Survey on Spelling Based CAPTCHA, IJRCCT 3 (3) (2014) 001–007.

[112] Q.-B. Ye, T.-E. Wei, A.B. Jeng, H.-M. Lee, K.-P. Wu, DDIM-CAPTCHA: A Novel Drag-n-Drop Interactive Masking CAPTCHA against the Third Party Human Attacks, in: Proceedings of the Conference on Technologies and Applications of Artificial Intelligence, 2013, pp. 158–163.

[113] N. Roshanbin, J. Miller, ADAMAS: Interweaving unicode and color to enhance CAPTCHA security, Future Generation Comput. Syst. (2016) 289–310.

[114] G. O. S. Blog, "Are you a robot? Introducing “No CAPTCHA reCAPTCHA”," ed, 2014.

[115] T. Tamang, P. Bhattarakosol, Uncover impact factors of text-based CAPTCHA identification, in: Proceedings of the 7th International Conference on Computing and Convergence Technology (ICCCT), 2012, pp. 556–560.

[116] A. Thomas, K. Punera, L. Kennedy, B. Tseng, Y. Chang, Framework for evaluation of text captchas, in: Proceedings of the 22nd International Conference on World Wide Web, 2013, pp. 159–160.

[117] B. Li, C. Wang, D.S. Huang, Supervised feature extraction based on orthogonal discriminant projection, Neurocomputing (2009) 191–196.

[118] B. Li, D.S. Huang, C. Wang, K. Liu, Feature extraction using constrained maximum variance mapping, Pattern Recognit. (2008) 3287–3294.

Please cite this article as: X. Xu, L. Liu and B. Li, A survey of CAPTCHA technologies to distinguish between human and computer, Neurocomputing, https://doi.org/10.1016/j.neucom.2019.08.109

[119] S. Sivakorn, I. Polakis, A.D. Keromytis, I am robot:(deep) learning to break semantic image captchas, in: Proceedings of the IEEE European Symposium on Security and Privacy (EuroS&P), 2016, pp. 388–403.
[120] M. Jaderberg, K. Simonyan, A. Vedaldi, A. Zisserman, Reading text in the wild with convolutional neural networks, Int. J. Comput. Vision 116 (1) (2016) 1–20.
[121] S. Kwon, S. Cha, CAPTCHA-based image annotation, Inf. Process. Lett. (2017) 27–31.
[122] B. Zhu, J. Liu, Q. Li, S. Li, and N. Xu, "Image-based CAPTCHA exploiting context in object recognition," ed: Google Patents, 2013.
[123] P. N. Aleksandrovich, N. I. Alekseevich, V. M. Vladimirovich, N. A. Igorevich, P. V. Borisovna, and N. O. Igorevna, "Image-based captcha system," ed: Google Patents, 2012.
[124] D.S. Huang, W. Jiang, A general CPL-AdS methodology for fixing dynamic parameters in dual environments, IEEE Trans. Syst. (2012) 1489–1500.
[125] M. Shirali-Shahreza, S. Shirali-Shahreza, Drawing captcha, in: Proceedings of the 28th International Conference on Information Technology Interfaces, 2006, pp. 475–480.
[126] A. Karunathilake, B. Balasuriya, R.G. Ragel, User friendly line CAPTCHAs, in: Proceedings of the International Conference on Industrial and Information Systems (ICIIS), 2009, pp. 210–215.
[127] J. Kim, J. Yang, K. Wohn, AgeCAPTCHA: an Image-based CAPTCHA that Annotates Images of Human Faces with their Age Groups, KSII Trans. Int. Inf. Syst. 8 (3) (2014).
[128] R. Lin, S.-Y. Huang, G.B. Bell, Y.-K. Lee, A new CAPTCHA interface design for mobile devices, in: Proceedings of the Twelfth Australasian User Interface Conference-Volume 117, 2011, pp. 3–8.
[129] F. Han, Q. Ling, D.S. Huang, An improved approximation approach incorporating particle swarm optimization and a priori information into neural networks, Neural Comput. Appl. (2010) 255–261.
[130] B. Li, D.S. Huang, Locally linear discriminant embedding: An efficient method for face recognition, Pattern Recognit. (2008) 3813–3821.
[131] Y. Rui, Z. Liu, Artifacial: Automated reverse turing test using facial features, Multimed. Syst. 9 (6) (2004) 493–502.
[132] B.B. Zhu, Attacks and design of image recognition CAPTCHAs, in: Proceedings of the 17th ACM Conference on Computer and Communications Security, 2010, pp. 187–200.
[133] M.E. Hoque, D.J. Russomanno, M. Yeasin, 2d captchas from 3d models, in: Proceedings of the IEEE SoutheastCon, 2006, pp. 165–170.
[134] M. Imsamai, S. Phimoltares, 3D CAPTCHA: A next generation of the CAPTCHA, in: Proceedings of the International Conference on Information Science and Applications (ICISA), 2010, pp. 1–8.
[135] V.D. Nguyen, Y.-W. Chow, W. Susilo, Breaking a 3D-based CAPTCHA scheme, in: Proceedings of the International Conference on Information Security and Cryptology, 2011, pp. 391–405.
[136] S.R. Lang, N. Williams, Impeding CAPTCHA breakers with visual decryption, in: Proceedings of the Eighth Australasian Conference on Information Security-Volume 105, 2010, pp. 39–46.
[137] M. Chew, J.D. Tygar, Image recognition captchas, in: Proceedings of the International Conference on Information Security, 2004, pp. 268–279.
[138] M. Shirali-Shahreza, S. Shirali-Shahreza, Collage captcha, in: Proceedings of the 9th International Symposium on Signal Processing and Its Applications ISSPA, 2007, pp. 1–4.
[139] H. Gao, D. Yao, H. Liu, X. Liu, L. Wang, A novel image based CAPTCHA using jigsaw puzzle, in: Proceedings of the Computational Science and Engineering (CSE), 2010 IEEE 13th International Conference on, 2010, pp. 351–356.
[140] J. Elson, J.R. Douceur, J. Howell, J. Saul, Asirra: a CAPTCHA that exploits interest-aligned manual image categorization, in: Proceedings of the ACM Conference on Computer and Communications Security, 2007, pp. 366–374.
[141] R. Pakdel, N. Ithnin, M. Hashemi, CAPTCHA: a survey of usability features, Res. J. Inf. Technol. 3 (4) (2011) 215–228 2011.
[142] S. Aggarwal, CAPTCHAs with a Purpose, in: Proceedings of the Workshops at the Twenty-Sixth AAAI Conference on Artificial Intelligence, 2012.
[143] R. Datta, J. Li, J.Z. Wang, IMAGINATION: a robust image-based CAPTCHA generation system, in: Proceedings of the 13th Annual ACM International Conference on Multimedia, 2005, pp. 331–334.
[144] R. Datta, J. Li, J.Z. Wang, Exploiting the Human–machine gap in image recognition for designing CAPTCHAs, IEEE Trans. Inf. Forensics Secur. 4 (3) (2009) 504–518.
[145] J.-W. Kim, W.-K. Chung, H.-G. Cho, A new image-based CAPTCHA using the orientation of the polygonally cropped sub-images, Visual Comput. 26 (6) (2010) 1135–1143.
[146] H. Nejati, N.-M. Cheung, R. Sosa, D.C. Koh, DeepCAPTCHA: an image CAPTCHA based on depth perception, in: Proceedings of the 5th ACM Multimedia Systems Conference, ACM, 2014, pp. 81–90.
[147] G. Schryen, G. Wagner, A. Schlegel, Development of two novel face-recognition CAPTCHAs: a security and usability study, Comput. Secur. (2016) 95–116.
[148] D., Brodić, et al., Usability Analysis of the Image and Interactive CAPTCHA via Prediction of the Response Time. 2017.
[149] R. Gossweiler, M. Kamvar, S. Baluja, What's up CAPTCHA?: a CAPTCHA based on image orientation, in: Proceedings of the 18th International Conference on World Wide Web, 2009, pp. 841–850.
[150] M.T. Banday, N.A. Shah, Image flip CAPTCHA, ISC Int. J. Inf. Secur. 1 (2) (2009) 105–123.
[151] S.A. Ross, J.A. Halderman, A. Finkelstein, Sketcha: a CAPTCHA based on Line Drawings of 3D Models, in: Proceedings of the 19th International Conference On World Wide Web, 2010, pp. 821–830.
[152] S. Vikram, Y. Fan, G. Gu, SEMAGE: a new image-based two-factor CAPTCHA, in: Proceedings of the 27th Annual Computer Security Applications Conference, 2011, pp. 237–246.
[153] E. Vimina, A.U. Areekal, Telling computers and humans apart automatically using activity recognition, in: Proceedings of the IEEE International Conference on Systems, Man and Cybernetics SMC, 2009, pp. 4906–4909.
[154] P. Matthews, A. Mantel, C.C. Zou, Scene tagging: image-based CAPTCHA using image composition and object relationships, in: Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, 2010, pp. 345–350.
[155] A. Basso, S. Sicco, Preventing massive automated access to web resources, Comput. Secur. 28 (3) (2009) 174–188.
[156] H.S. Baird, J.L. Bentley, Implicit captchas, in: Proceedings of the Document Recognition and Retrieval XII,, 2005, pp. 191–197.
[157] D. Lopresti, Leveraging the CAPTCHA problem, in: Proceedings of the Human Interactive Proofs, Springer, 2005, pp. 97–110.
[158] G. Goswami, B.M. Powell, M. Vatsa, R. Singh, A. Noore, FaceDCAPTCHA: Face detection based color image CAPTCHA, Future Generat. Comput. Syst. (2014) 59–68.
[159] I. Polakis, Faces in the distorting mirror: Revisiting photo-based social authentication, in: Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, 2014, pp. 501–512.
[160] K. Krol, S. Parkin, M.A. Sasse, I don't like putting my face on the Internet!": An acceptance study of face biometrics as a CAPTCHA replacement, in: Proceedings of the IEEE International Conference on Identity, Security and Behavior Analysis (ISBA), 2016, pp. 1–7.
[161] H. Kwon, Y. Kim, H. Yoon, D. Choi, CAPTCHA image generation systems using generative adversarial networks, IEICE Trans. Inf. Syst. 101 (2) (2018) 543–546.
[162] R. Aadhirai, P.S. Kumar, S. Vishnupriya, Image CAPTCHA: Based on human understanding of real world distances, in: Proceedings of the 4th International Conference on Intelligent Human Computer Interaction (IHCI), 2012, pp. 1–6.
[163] B.M. Powell, G. Goswami, M. Vatsa, R. Singh, A. Noore, fgCAPTCHA: Genetically Optimized Face Image CAPTCHA 5, IEEE Access (2014) 473–484.
[164] P. Liu, J. Shi, L. Wang, L. Guo, An efficient ellipse-shaped blobs detection algorithm for breaking Facebook CAPTCHA, in: Proceedings of the International Conference on Trustworthy Computing and Services, 2012, pp. 420–428.
[165] J. Kim, S. Kim, J. Yang, J.-h. Ryu, K. Wohn, FaceCAPTCHA: a CAPTCHA that identifies the gender of face images unrecognized by existing gender classifiers, Multimed. Tools Appl. 72 (2) (2014) 1215–1237.
[166] H. Gao, L. Lei, X. Zhou, J. Li, X. Liu, The robustness of face-based CAPTCHAs, in: Proceedings of the IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (CIT/IUCC/DASC/PICOM), 2015, pp. 2248–2255.
[167] D. Misra, K. Gaj, Face recognition captchas, in: Proceedings of the Telecommunications AICT-ICIW'06. International Conference on Internet and Web Applications and Services/Advanced International Conference on, 2006 122-122.
[168] J. Mi, D.S. Huang, Bing Wang, Xingjie Zhu, The nearest-farthest subspace classification for face recognition, Neurocomputing (2013) 241–250.
[169] C. Funk, Y. Liu, Symmetry reCAPTCHA, in: Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2016, pp. 5165–5174.
[170] M. Osadchy, J. Hernandez-Castro, S. Gibson, and O. Dunkelman, "No Bot Expects the DeepCAPTCHA! Introducing Immutable Adversarial Examples with Applications to CAPTCHA," Cryptology ePrint Archive: 2016/336, 2016.
[171] S. Choudhary, R. Saroha, Y. Dahiya, S. Choudhary, understanding CAPTCHA: text and audio based CAPTCHA with its applications, Int. J. Adv. Res. Comput. Sci. Softw. Eng. 3 (6) (2013).
[172] F. C. Fisk, S. Ramanathan, M. A. Terry, and M. B. Trevathan, "Advanced audio CAPTCHA," ed: Google Patents. 2013.
[173] J. Holman, J. Lazar, J.H. Feng, J. D'Arcy, Developing usable CAPTCHAs for blind users, in: Proceedings of the 9th international ACM SIGACCESS Conference on Computers and Accessibility, 2007, pp. 245–246.
[174] S. Sano, T. Otsuka, H.G. Okuno, Solving Google's continuous audio CAPTCHA with HMM-based automatic speech recognition, in: Proceedings of the International Workshop on Security, 2013, pp. 36–52.
[175] E. Bursztein, R. Beauxis, H. Paskov, D. Perito, C. Fabry, J. Mitchell, The failure of noise-based non-continuous audio captchas, in: Proceedings of the Security and Privacy (SP), 2011 IEEE Symposium on, 2011, pp. 19–31.
[176] E. Bursztein, S. Bethard, Decaptcha: breaking 75% of eBay audio CAPTCHAs, in: Proceedings of the 3rd USENIX Conference on Offensive Technologies, USENIX Association, 2009, p. 8.
[177] S. Shirali-Shahreza, H. Abolhassani, H. Sameti, M. Hassan, Spoken captcha: A captcha system for blind users, in: Proceedings of the ISECS International Colloquium on Computing, Communication, Control, and Management, IEEE, 2009, pp. 221–224.
[178] S. Shirali-Shahreza, G. Penn, R. Balakrishnan, Y. Ganjali, Seesay and hearsay captcha for mobile interaction, in: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 2013, pp. 2147–2156.
[179] J.P. Bigham, A.C. Cavender, Evaluating existing audio CAPTCHAs and an interface optimized for non-visual use, in: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 2009, pp. 1829–1838.

Please cite this article as: X. Xu, L. Liu and B. Li, A survey of CAPTCHA technologies to distinguish between human and computer, Neurocomputing, https://doi.org/10.1016/j.neucom.2019.08.109

[180] J. Lazar, The SoundsRight CAPTCHA: an improved approach to audio human interaction proofs for blind users, in: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 2012, pp. 2267–2276.
[181] Y. Xu, G. Reynaga, S. Chiasson, J.-M. Frahm, F. Monrose, P.C. van Oorschot, Security analysis and related usability of motion-based captchas: Decoding codewords in motion, IEEE Trans. Dependable Secure Comput. 11 (5) (2014) 480–493.
[182] H. Gao, H. Liu, D. Yao, X. Liu, U. Aickelin, An audio CAPTCHA to distinguish humans from computers, in: Proceedings of the Third International Symposium on Electronic Commerce and Security (ISECS), 2010, pp. 265–269.
[183] T.-Y. Chan, Using a test-to-speech synthesizer to generate a reverse Turing test, in: Proceedings of the 15th IEEE International Conference on Tools with Artificial Intelligence, 2003, pp. 226–232.
[184] Y. Soupionis, D. Gritzalis, Audio CAPTCHA: Existing solutions assessment and a new implementation for VoIP telephony, Comput. Secur. 29 (5) (2010) 603–618.
[185] A. Olalere, J.H. Feng, J. Lazar, T. Brooks, Investigating the effects of sound masking on the use of audio CAPTCHAs, Behav. Inf. Technol. 33 (9) (2014) 919–928.
[186] M. Goto, T. Shirato, R. Uda, Text-based CAPTCHA using phonemic restoration effect and similar sounds, in: Proceedings of the IEEE 38th International Computer Software and Applications Conference Workshops (COMPSACW), 2014, pp. 270–275.
[187] J. Tam, J. Simsa, S. Hyde, L.V. Ahn, Breaking audio captchas, in: Proceedings of the Advances in Neural Information Processing Systems, 2008, pp. 1625–1632.
[188] B. Li, J. Du, X.P. Zhang, Feature extraction using maximum nonparametric margin projection, Neurocomputing 188 (2016) (2016) 225–232.
[189] L.Lei B.Li, X.P. Zhang, Constrained discriminant neighborhood embedding for high dimensional data feature extraction, Neurocomputing 173 (2016) 137–144.
[190] J.Li B.Li, X.P. Zhang, Nonparametric discriminant multi-manifold learning for dimensionality reduction, Neurocomputing 152 (2015) 121–126.
[191] H. Meutzner, V.-H. Nguyen, T. Holz, D. Kolossa, Using automatic speech recognition for attacking acoustic CAPTCHAs: the trade-off between usability and security, in: Proceedings of the 30th Annual Computer Security Applications Conference, 2014, pp. 276–285.
[192] M. Darnstädt, H. Meutzner, D. Kolossa, Reducing the cost of breaking audio captchas by active and semi-supervised learning, in: Proceedings of the 13th International Conference on Machine Learning and Applications (ICMLA), 2014, pp. 67–73.
[193] H. Meutzner, S. Gupta, D. Kolossa, Constructing secure audio captchas by exploiting differences between humans and machines, in: Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, 2015, pp. 2335–2338.
[194] N. Carlini, Hidden voice commands, in: Proceedings of the 25th USENIX Security Symposium (USENIX Security 16), Austin, TX, 2016.
[195] J. Choi, T. Oh, W. Aiken, S.S. Woo, H. Kim, POSTER: I Can't Hear This Because I Am Human: A Novel Design of Audio CAPTCHA System, in: Proceedings of the Asia Conference on Computer and Communications Security, 2018, pp. 833–835.
[196] J. Tam, J. Simsa, D. Huggins-Daines, L. Von Ahn, M. Blum, Improving audio captchas, in: Proceedings of the Symposium On Usable Privacy and Security (SOUPS), 2008.
[197] M. Shirali-Shahreza, S. Shirali-Shahreza, Question-based captcha, in: Proceedings of the International Conference on Conference on Computational Intelligence and Multimedia Applications, 2007, pp. 54–58.
[198] L.A. Leiva, F. Álvaro, μcaptcha: Human Interaction Proofs Tailored to Touch–Capable Devices via Math Handwriting, Int. J. Human Comput. Interact. 31 (7) (2015) 457–471.
[199] C.J. Hernandez-Castro, A. Ribagorda, Pitfalls in CAPTCHA design and implementation: The Math CAPTCHA, a case study, Comput. Secur. 29 (1) (2010) 141–157.
[200] J.-S. Cui, J.-T. Mei, W.-Z. Zhang, X. Wang, D. Zhang, A CAPTCHA implementation based on moving objects recognition problem, in: Proceedings of the International Conference on E-Business and E-Government (ICEE), 2010, pp. 1277–1280.
[201] M. Shirali-Shahreza, S. Shirali-Shahreza, Dynamic captcha, in: Proceedings of the International Symposium on Communications and Information Technologies ISCIT, 2008, pp. 436–440.
[202] B. M. Jakobsson, J. R. Palmer, and G. Maldonado, "Interactive CAPTCHA," ed: Google Patents, 2013.
[203] J. Cui, A 3-layer dynamic CAPTCHA implementation, in: Proceedings of the Second International Workshop on Education Technology and Computer Science, 2010, pp. 23–26.
[204] R. ur Rahman, D.S. Tomar, S. Das, Dynamic image based captcha, in: Proceedings of the International Conference on Communication Systems and Network Technologies (CSNT), 2012, pp. 90–94.
[205] E. Bursztein, "How we broke the NuCaptcha video scheme and what we proposed to fix it," See http://elie.im/blog/security/how-we-broke-the-nucaptcha\-video-scheme-and-what-we-propose-to-fix-it/, Accessed March, 2012.
[206] V.D. Nguyen, Y.-W. Chow, W. Susilo, Breaking an animated CAPTCHA scheme, in: Proceedings of the International Conference on Applied Cryptography and Network Security, 2012, pp. 12–29.
[207] N.J. Mitra, H.-K. Chu, T.-Y. Lee, L. Wolf, H. Yeshurun, D. Cohen-Or, Emerging images, ACM Trans. Graph. (TOG) 28 (5) (2009) 163.
[208] Y. Xu, G. Reynaga, S. Chiasson, J.-M. Frahm, F. Monrose, P. Van Oorschot, Security and usability challenges of moving-object CAPTCHAs: decoding codewords in motion, in: Proceedings of the 21st USENIX Security Symposium (USENIX Security 12), 2012, pp. 49–64.
[209] K.A. Kluever, R. Zanibbi, Balancing usability and security in a video CAPTCHA, in: Proceedings of the 5th Symposium on Usable Privacy and Security, 2009, p. 14.
[210] E. Athanasopoulos, S. Antonatos, Enhanced captchas: Using animation to tell humans and computers apart, in: Proceedings of the IFIP International Conference on Communications and Multimedia Security, 2006, pp. 97–108.
[211] M. Mohamed, A three-way investigation of a game-CAPTCHA: automated attacks, relay attacks and usability, in: Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security, 2014, pp. 195–206.
[212] S. Gao, M. Mohamed, N. Saxena, C. Zhang, Emerging Image Game CAPTCHAs for resisting automated and human-solver relay attacks, in: Proceedings of the 31st Annual Computer Security Applications Conference, 2015, pp. 11–20.
[213] S. Mahato, V.P. Saxena, D. Bhavsar, A Survey of Captcha based Web and Application Security Methods and Techniques, in: Proceedings of the HCTL Open In. J. Technol. Innovat. Res. (IJTIR), 2015 2321-1814.
[214] A. Basso, F. Bergadano, Anti-bot strategies based on human interactive proofs, in: Proceedings of the Handbook of Information and Communication Security, Springer, 2010, pp. 273–291.
[215] J.M.G. Hidalgo, G. Alvarez, Captchas: An artificial intelligence application to web security, Adv. Comput. 83 (1) (2011) 109–181.
[216] M. Tang, H. Gao, Y. Zhang, Y. Liu, P. Zhang, P. Wang, Research on Deep Learning Techniques in Breaking Text-Based Captchas and Designing Image-Based Captcha, IEEE Trans. Inf. Forensics Secur. 13 (10) (2018) 2522–2537.
[217] W. Zhao, D. Huang, J. Du, L. Wang, Genetic optimization of radial basis probabilistic neural networks, Int. J. Pattern Recognit Artif Intell. (2004) 1473–1500.
[218] Z. Zhao, P. Zheng, S. Xu, X. Wu, Object detection with deep learning: a review, IEEE Trans. Neural Netw. Learn. Syst. (2019) accepted.
[219] Z. Zhao, Y. Cheung, H. Hu, X. Wu, Corrupted and Occluded Face Recognition via Cooperative Sparse Representation, Pattern Recognit. (2016) 77–87.
[220] X. Wang, D.S. Huang, J. Du, H. Xu, L. Heutte, Classification of plant leaf images with complicated background, Appl. Math. Comput. (2008) 916–926 2008.
[221] Y. Zhao, D.S. Huang, Completed local binary count for rotation invariant texture classification, IEEE Trans. Image Process. (2012) 4492–4497.
[222] Y. LeCun, Backpropagation applied to handwritten zip code recognition, Neural Comput. 1 (4) (1989) 541–551.
[223] A. Krizhevsky, I. Sutskever, G.E. Hinton, Imagenet classification with deep convolutional neural networks, in: Proceedings of the Advances in Neural Information Processing Systems, 2012, pp. 1097–1105.
[224] C. Szegedy et al., "Intriguing properties of neural networks," arXiv preprint arXiv:1312.6199, 2013.

Xin Xu received the B.Sc. and Ph.D. degree in computer science and engineering from Shanghai Jiao Tong University, China, in 2004 and 2012 respectively. He is an associate professor in the School of Computer Science and Technology, Wuhan University of Science and Technology, Wuhan, China. His current research interests include computer vision, deep learning, and visual surveillance.

Lei Liu is currently working toward the Ph.D. degree at the School of Computer Science and Technology, Wuhan University of Science and Technology, Wuhan, China. His research interests include person re-identification, digital forensics, and visual surveillance.

Bo Li received his M.Sc. and Ph.D. degree in Mechanical and Electronic Engineering from Wuhan University of Technology in 2003, Pattern Recognition and Intelligent System from University of Science and Technology of China in 2008, respectively. Now, he is a professor at School of Computer Science and Technology, Wuhan University of Science and Technology. His research interests include machine learning, pattern recognition, image processing and bioinformatics.

Please cite this article as: X. Xu, L. Liu and B. Li, A survey of CAPTCHA technologies to distinguish between human and computer, Neurocomputing, https://doi.org/10.1016/j.neucom.2019.08.109