CAPTCHA has developed into the most popular utilized standard security measure for preventing automated computer program attacks. In recent years, many attack methods, developed by hackers or researchers, have effectively cracked all common conventional schemes. Some methods, including Invisible reCAPTCHA, have not yet been broken. However, with the introduction of fourth-generation bots accurately mimicking human behavior, a secure CAPTCHA would be hardly designed without additional special devices. Specially, almost all cognitive-based CAPTCHAs with sensor support have not yet been vulnerable to automated attacks. However, they are still compromised to human-assisted relay attacks due to having a limited number of challenges and can be only solved using trusted devices. Table [6](https://jis-eurasipjournals.springeropen.com/articles/10.1186/s13635-022-00134-9#Tab6) lists various recent CAPTCHA attack techniques, with DNN/CNN and ML attack techniques dominating the list.

Text-based CAPTCHAs were the first CAPTCHA scheme and still remain the most popular. Mori and Malik introduced an attack method of shape matching in 2003 to pass Gimpy and EZ-Gimpy CAPTCHAs with an accuracy of 33% and 92%, respectively. The proposed method used a correlation algorithm and a direct distortion estimation algorithm to successfully break EZ-Gimpy with a success rate of 99%. Chellapilla et al. created a highly secure CAPTCHA of anti-segmentation in 2005 after passing various text-based CAPTCHAs with machine learning. In 2008, several anti-segmentation CAPTCHAs, used by Google, Microsoft, and Yahoo, were demonstrated to be able to be cracked by El Ahmad and Yan. Later, other researchers attempted to pass these CAPTCHAs with higher success rates. El Ahmad and Yan also broke Megaupload CAPTCHA with 78% of success. Google researchers used neural networks to break the hardest category of ReCAPTCHA in 2014, with an accuracy of 99.8%. The authors suggested 3D CAPTCHA attack methods without OCR software. In several 3D-based CAPTCHAs, such as 3DCAPTCHA, Teabag 3D, and Super CAPTCHA, they extracted pixels from the characters for automated challenge recognition. Using such a technique, the authors were able to break 3DCAPTCHA, Teabag 3D, and Super CAPTCHA with success rates of 58%, 31%, and 27%, respectively. Furthermore, the same authors were able to pass Teabag 3D by using the 3D textual objects’ side surface information. In the animated-based CAPTCHAs, Nguyen et al. demonstrated how to easily extract information across multiple animated frames by using CL (Catching Line) or PDM (Pixel Delay Map). These methods successfully defeated animated CAPTCHAs such as KillBot Professional, iCAPTCHA, Dracon CAPTCHA, and Atlantis. Due to their vulnerability to segmentation attacks, the same methods were used in to defeat HelloCAPTCHA variants with a success rate ranging from 16 to 100%. NuCaptcha is a segmentation-resistant animated CAPTCHA that works by overlapping and cramming together to counter PDM or CL attack methods. Elie Bursztein separated objects in each frame with a success rate of 90% using an interest points (SIFT algorithm) density evaluation and bounding box shape analysis.

Golle was successful in breaking the Asirra scheme. To accomplish this, SVM (support vector machine) was used to classify cats and dogs with a success rate of 82.7%. Hernandez-Castro et al. suggested a side-channel attack breaking HumanAuth with an accuracy rate of 92%. Facebook image-based CAPTCHA and Google image-based CAPTCHA were bypassed by Sivakorn et al. with success rates of 83.5% and 70.78%, respectively. The authors achieved success rates of 79 and 88% with the new and old variations of reCAPTCHA V2. They also defeated China Railway CAPTCHA and Facebook image CAPTCHA with success rates of 90% and 86%, respectively. Besides, these authors broke different image-based CAPTCHA schemes, including the Tencent CAPTCHA with a success rate of 100%. Convolutional Neural Networks (CNN) was applied to successfully break Avatar CAPTCHA, with a success rate of 99%. Both FaceDCAPTCHA and FR-CAPTCHA were defeated by Gao et al. with success rates of 48% and 23%, respectively. Minteye CAPTCHA was defeated in by utilizing the length of the image’s edges and Sobel operators. The attack method chooses the image with the smallest sum of edges based on the fact that a swirled image takes the longer edges. Hernandez-Castro et al. suggested a low-cost attack using JPEG to measure image continuityUsing this side-channel attack, they successfully broke Capy CAPTCHA, Garb CAPTCHA, and KeyCAPTCHA with success rates of 65.1%, 98.1%, and 20%, respectively.