The title of the article is "A Human and Artificial Intelligence Approach to Securely Analyze CAPTCHA Codes". The article discusses CAPTCHA and Human-AI Interaction (HAI) as security mechanisms designed to distinguish between humans and computers. CAPTCHA is a cryptographic protocol that creates tests that are solvable by humans, but difficult for computers, in order to prevent attacks and hacks. HAI investigates the interaction between humans and computers considering usability and security aspects of existing CAPTCHA schemes.

Initial theoretical approaches to distinguish computers from humans, starting with the use of text-based CAPTCHAs on the Internet since 1997, have led to the development of various schemes such as text-based and visual CAPTCHAs. These schemes are used to defend against attacks and hacks based on image processing and machine learning algorithms. CAPTCHAs designed to distinguish between humans and computers have evolved from garbled text to more complex forms, including 3D text and animated text CAPTCHAs. They are designed to make the recognition task more difficult for computer programs and bots, but they also raise privacy and usability concerns for users.

Text CAPTCHAs have become less reliable and have been replaced by images that require the user to perform various actions such as mouse movements, selections, clicks, drawing, slides, or assembling puzzles. For visually impaired users, audio CAPTCHAs have been proposed, such as the audio reCAPTCHA, which requires recognizing numbers in noise. Videos are also used where users must describe the content of the video with text or select a relevant sentence. Cognitive-based CAPTCHA methods that incorporate biometric and physical factors using sensors provide increased security, replacing traditional CAPTCHA methods. Text-based CAPTCHAs such as Gimpy and EZ-Gimpy have been successfully attacked using correlation algorithm, direct distortion estimation algorithm, machine learning, neural networks, and SIFT algorithms, among others. These attacks demonstrated vulnerabilities in various CAPTCHA schemes, with success rates as high as 99%. Research has identified successful attacks against a variety of image-based CAPTCHAs, including HumanAuth, Facebook, Google, reCAPTCHA V2, Tencent, and others. Attack methods include support vector machines (SVMs), side-channel attacks, convolutional neural networks (CNNs), and techniques utilizing image edge length and JPEG compression. These attacks emphasized the vulnerability of CAPTCHA systems to automated hacks. In 2009, Philippe Gollet presented effective attacks on ASIRRA based on the analysis of CAPTCHA features such as font, shape, texture, and color. This image processing method divides photos into cells with texture and color, then fed to support vector machine (SVM) classifiers with a classification success rate of 83%. Experiments using the SVM method and the Decaptcha decoder demonstrated successful attacks on audio CAPTCHAs, including reCAPTCHAs, with success rates ranging from 45% to 85.15%. These attacks included wave file analysis using discrete Fourier transform, supervised learning algorithm, hidden Markov models (HMM), and minimal phonetic mapping. Any biased idea in CAPTCHA design devoid of randomness can be the target of attacks such as side-channel analysis or task categorization. For example, in Teabag, the non-uniform distribution of letter sizes has vulnerability to front-end attacks and back-end detection via pixel correlation. Simple algorithms such as pixel continuity can detect background regions. Megaupload CAPTCHAs that use fixed font and rotation angles become vulnerable to analysis. Some CAPTCHA systems are susceptible to circumvention through the use of previously used session IDs, faulty implementation of response encoding in a URL or form field, and other vulnerabilities such as sending the client a hash of the response. Limited or unevenly distributed task pools and risky methods of communicating with the CAPTCHA server can also pose potential security threats.

CAPTCHA has become the most popular standard security measure to prevent automated computer program attacks. Unlike traditional CAPTCHA schemes, new sensor and behavioral schemes raise privacy concerns such as sending user behavior data, cookies, and sensors to remote servers. This raises security issues and requires attention to user privacy during development. With the rise of automated attacks, distinguishing between humans and bots in CAPTCHA schemes becomes a challenge. To enhance security, additional measures such as evaluating the quality and behavior of the "fluman" need to be implemented. It is also important to distinguish between "fluman" and "fluman-assisted" algorithms and to take measures against relaying attacks. Methods for preventing attacks on fluman farms should also be considered.

To summarize, CAPTCHA is a security scheme where humans and computers compete. In this confrontation, humans rely on the sophistication of artificial intelligence. However, evolving technology allows computers to effectively solve complex artificial intelligence problems, which necessitates continuous improvement of CAPTCHA.