Research trends on CAPTCHA: A systematic literature

Igbekele Emmanuel O.[1], Adebiyi Ayodele A.[2], Ibikunle Francis A.[3], Adebiyi Marion O.[4], Olugbara O. Oludayo[5]
[1,2,3]Department of Computer Science, Landmark University, Omu-Aran, Nigeria
[4,5]ICT and Society Research Group and Luban Workshop, Durban University of Technology, South Africa

Article Info

Article history:

Received Apr 30, 2020
Revised Apr 13, 2021
Accepted May 3, 2021

Keywords:

CAPTCHA
Convolutionary neural network
Deep convolutionary neural network
Human interaction proofs
Intrusion detection systems
Web services

ABSTRACT

The advent of technology has crept into virtually all sectors and this has culminated in automated processes making use of the Internet in executing various tasks and actions. Web services have now become the trend when it comes to providing solutions to mundane tasks. However, this development comes with the bottleneck of authenticity and intent of users. Providers of these Web services, whether as a platform, as a software or as an Infrastructure use various human interaction proof's (HIPs) to validate authenticity and intent of its users. Completely automated public turing test to tell computer and human apart (CAPTCHA), a form of IDS in web services is advantageous. Research into CAPTCHA can be grouped into two -CAPTCHA development and CAPTCH recognition. Selective learning and convolutionary neural networks (CNN) as well as deep convolutionary neural network (DCNN) have become emerging trends in both the development and recognition of CAPTCHAs. This paper reviews critically over fifty article publications that shows the current trends in the area of the CAPTCHA scheme, its development and recognition mechanisms and the way forward in helping to ensure a robust and yet secure CAPTCHA development in guiding future research endeavor in the subject domain.

Corresponding Author:

Igbekele Emmanuel Olufemi
Department of Computer Science
Landmark University
Km 4 Ipetu, Omu-Aran Road, PMB 1001, Ipetu Road Omu-Aran, Kwara State, Nigeria
Email: igbekele.emmanuel@lmu.edu.ng, emmanuel.igbekele@gmail.com

1. INTRODUCTION

The advent of the Internet has been very advantageous to the society and it has impacted significantly all sectors of the economy [1]. Education, commerce, finance, health, transportation have all migrated from the manual and redundant way of carrying out their day-to-day activities to an automated and integrated process [2], [3]. With this migration comes the quest for accessibility at every point in time irrespective of destination and region. Hence all automated processes are integrated into a common infrastructure called web services and are generally accessed through an infrastructures commonly referred to as service-oriented architecture (SOA) [4]-[6]. Honeypots [7]-[10], intrusion detection systems (IDS) and human interaction proofs (HIPs) are both forms of SOA [11]. While IDS focuses and sensing changes that may occur within a system as a result of external interference, HIPs on the other hand allows a system to ascertain the category to which its users belong when usage is being done over a network [12]. Essentially, this is done over three broad categories viz; to distinguish computer-bots from humans, distinguish a class of humans from another and to distinguish a particular human from another. Independently, virtually all intrusion detection systems (IDS) have been found to be vulnerable to manipulations and attacks in a way and completely automated public turing test to tell computer and human aparts (CAPTCHAs) are no exception. In recent years, for CAPTCHAs, mechanisms such as solving attacks (SA) [13], bypass attacks (BA) [14] and human exploitation attacks (EA) [15] have been used successfully thereby granting access into sensitive data for bot programs [16], [17]. Consequently, the quest to tighten the widening gap between computer programs and humans in strengthening the existing CAPTCHA security mechanisms [18], novel theories have been presented, focusing on the user's response as partial credit. The bottom-line is that there can only be one output for every CAPTCHA response: correct or incorrect. Hence, the reason for the partial credit algorithm (PCA) is that a machine-to-person communication is predominantly important than having just a correct or incorrect response, especially when the efficacy of supplied user information is being considered. This has led to diverse CAPTCHA recognition mechanisms [19]-[21] and therefore brings to fore the emergence of hollow, 3D and machine learning CAPTCHAs [22]. This paper focuses on the various developmental and recognition aspects of CAPTCHA methods that includes its forms, mode of development, vulnerabilities to attacks and its usability. Section 2 presents a theoretical framework and reviews the existing CAPTCHA variances, research strength in the field as well as current trends in CAPTCHA design and recognition. Section 3 provides the method of review while the results of the findings were presented in section 4. Discussion on the results was highlighted in section 5, and section 6 focused on Findings. Section 6 is where we conclude and present future research directions.

2. LITERATURE REVIEW

Intrusion detection systems and security breaches in web applications have over a couple of years now leveraged on CAPTCHAs for detection [23], hence, major research works are being done in this area, some of which will be reviewed in this section. These research works on CAPTCHA have been succinctly divided into two major categories–design (Development) and recognition (Solution). The research work in the area of CAPTCHA design [24] is essentially focused on novel approaches in the development of CAPTCHAs for enhancing system security [25] while the researches in the area of CAPTCHA recognition looks at vulnerabilities in existing and prevalent CAPTCHAs and ways in which they can be exploited [26]. This succinctly promotes development of other novel techniques considering CAPTCHAs have become an integral part of artificial intelligence and an important prerequisite in HCIs. As CAPTCHAs continually became prominent as a class of HIPs, it becomes pertinent to view them in two broad categories–optical and non-optical character recognition (OCR and Non-OCR respectively). The OCR is essentially text-based while the Non-OCR essentially focuses on multimedia (images, audio and video).

2.1. Optical character recognition CAPTCHAs

The optical character recognition CAPTCHAs which instinctively relates to text-based CAPTCHAs is a system that uses a distorted English word that a user is asked to type. When this method was introduced by Andrei Broder and some of his colleagues in 1997, it was used as plain text, without any form of distortion. A text (words, characters, digits) is displayed and a user is expected to type out the word correctly and in order. Gradually, this form of CAPTCHA became easy to solve for computer bots, hence the introduction of distortion to those text images. The advent of distorted word in OCR CAPTCHAs brought a form of relief as it remained easier for users to understand but difficult for bots to recognize using OCR techniques. These text-based CAPTCHAs are presented in the form of an image but embedded in it is a text string relatively difficult to recognize (even for a human) to be identified and orderly re-typed by the user in a text box provided near the CAPTCHA image by the web application. These CAPTCHA variances come under the OCR because by merely looking at them, they are easily solvable by humans. However, computer bot programs have leveraged on this user-friendliness attribute for humans to break most of the OCR CAPTCHAs. In that sense, OCR CAPTCHAs are more easily breakable than Non-OCR CAPTCHAs. The CAPTCHA image is of low quality with different forms of noise and strong degradation applied to it. Examples of OCR CAPTCHAs is presented in the Figure 1.

2.2. Non-optical character recognition CAPTCHAs

The non-optical character recognition CAPTCHAs which translate to image, audio or video-based CAPTCHAs is a system that uses multimedia in the generation and formation of its CAPTCHA. When technological advancement is experienced, it always comes with one or two identifiable setbacks. The most prominent among the major setbacks of OCR CAPTCHAs (vision impairment–human with disabilities) and a few others, Non-OCR CAPTCHA came into play. These CAPTCHAs are powered essentially on speech-recognition and semantic tests in determining users of a system. Semantic CAPTCHAs achieve its secure form by leveraging on the inabilities of machines to answer human-oriented questions. For this kind of CAPTCHAs, users are provided with questions that requires a level of brainwork to provide a solution, and that, in record time too. Questions may revolve around everyday life and activities such as “A sick person is taken to?”, “Fishes live in what?”, forms the baseline for the structure of Semantic CAPTCHAs. However, these kinds of CAPTCHAs are not limited to single-answer questions, often times, questions with more than one answer can be asked.

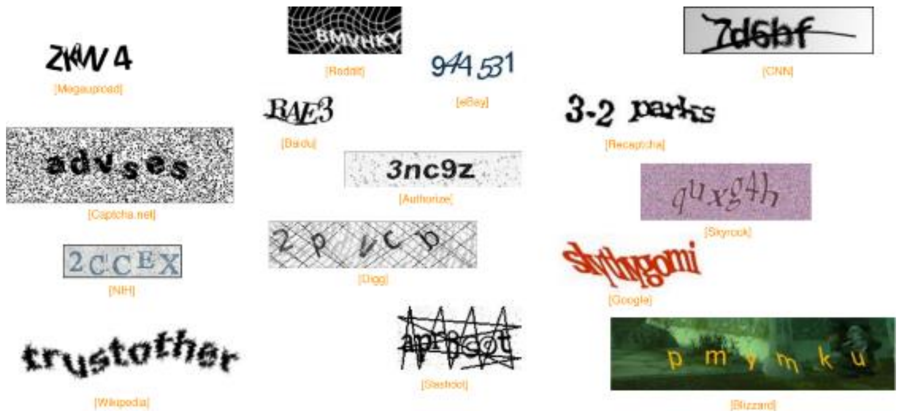


Figure 1. Some examples of popular real-world text-based CAPTCHA schemes [27]

2.3. Related work

Pope and Kaur [28] considered the volume of e-commerce sites in use around the world and thought about CAPTCHAs as a protection mechanism, thereby highlighting the difference between human users and computers programs in their work. In their work which can be classified under CAPTCHA development/design, CAPTCHAs can easily provide a programmable way to discern humans from computers and thereby keeping computer bots away from e-commerce sites and in the process reduce spamming activities. Authors proposed an image composed of pseudorandom letters and numbers placed either in front of an obfuscating background or run through some degradation algorithm to make optical character recognition (OCR) of the final image impractical. This work was at that time a huge success, however, overtime, it has become vulnerable to blind-guessing just as it is with dictionary attacks.

In 2005, Chellapilla and Simard [29] worked on breaking HIPs using machine l learning. In their work which can be classified under CAPTCHA recognition, it was observed that tasks where machine learning algorithms were not as good as Human solutions. Having this in mind, they discovered that machine learning is a very suitable method for detecting recognition tasks, a concept upon which most HIPs are formulated. Thus, they came up with effective HIP (utilized in MSN passport) models which leveraged on challenging character-segmentation tasks to confuse machine learning algorithms.

Shahreza and Shahreza [30] in their work capitalized on the ability of human to be intuitive and to solve mathematical problem to develop CAPTCHAs. In this research which can be categorized under CAPTCHA development, an elementary mathematical problem deployed in form of an image is generated according to a predefined pattern. The entire problem is saved and portrayed to the user in form of an image to be deciphered by user. The solution to this problem hinges on the human intuitive abilities of understanding text of question, detection of question images, understanding the problem, and solving the problem, which is a daring task for a bot program to have all those functionalities. However, this technique is only limited to users with the ability to solve computational problems. Genuine users without prior knowledge of solving elementary mathematical problem will find themselves in the same predicament as bot programs and this defeats the purpose of CAPTCHAs.

In 2008, Kluever [31] made an attempt at using video-tagging (content-based labelling of videos) as a CAPTCHA task for humans to solve. The work which comes under CAPTCHA development extracts videos from public domains (e.g. YouTube) and uses such as CAPTCHA problems. Experiments were conducted with over one hundred and eighty human participants and their responses were analyzed using some metrics. The threshold for passing this CAPTCHA challenge would be an individual successfully providing about three (3) words describing the video just watched. Their work proved to be a huge success at the time considering about 70% to 90% of respondents tagged the video using three words as compared to the 13% success rate of computer bots in tagging same video. A major setback to this work is that a problem is encountered when tag frequency estimates are not publicly available. Also, network distortion can be a major hindrance here.

Hindle *et al.* [32] worked on a CAPTCHA that uses reverse-engineering in its identification and recognition. The authors whose work can be categorized under CAPTCHA recognition, solved real-world CAPTCHAs by using simple available image processing techniques which includes bitmap comparison, thresholding, fill-flood segmentation, dilation, and erosion. This was accomplished through the use of black-box and white-box methodologies for reverse engineering and solving CAPTCHAs. Their model however only focuses on Image-processing CAPTCHAs which makes it vulnerable to bots' program specifically targeted at Image processing.

Banday and Shah [33] also worked on a CAPTCHA design of images that are clickable and can be flipped. The work which falls under the CAPTCVHA development category presented clickable image-based CAPTCHA techniques. The technique presents users with a CAPTCHA image composed of several inter-twined sub-images. The proposed technique grants improved security than that of normal OCR-based techniques, consumes less web page area and improves the user-friendliness of the web page. The model however were found to be defaulting as it has issues relating with distortion and presentation dimension.

Yamamoto *et al.* [34] in their work proposed to capitalize on the ability of humans to identify strangeness as presented in a CAPTCHA. Their research work categorized under CAPTCHA recognition utilized sentences as interpreted and translated by machines in the development of a new CAPTCHA series. SS-CAPTCHA (CAPTCHA using Strangeness in sentences) as depicted performs its function by checking how well humans can distinguish between natural sentences as constructed by humans and those that are generated by machine-translation. In their work, a system randomly presents P natural sentences created by humans (NSs) and Q garbage sentences generated from a natural sentence by a machine translator (GSs) to a user. A combination of both generated sentences (P+Q) sentences are then randomly placed. The quest then is for the user to select the set of natural sentences from the sequence of (P+Q) sentences. A successful selection of all humanly generated sentences certifies the user to be human while one or more errors certifies the user to be a bot program. A major pitfall of this CAPTCHA is that of comprehension of the user. Also, language barrier comes into play here and message translators cannot be an option.

Almazyad *et al.* [35] in their work which can be categorized under CAPTCHA development, proposed a multi-modal CAPTCHA. Most CAPTCHAs largely depends on the ability of enhanced distortion on text images making them unrecognizable to the techniques being utilized in its recognition, and these text-based schemes are in widespread use especially for applications for social networking sites, email generation, eCommerce and other online auction sites. Their work focuses on a new technique to build a CAPTCHA which is multi-modal (picture and text based). An image is being presented on the screen and many text labels layered over it. The task becomes that of the user to match the correct name of the image in context to its text label in the pool that are scattered all over it. Looking at their research, it is extra-work for humans to solve multi-layer CAPTCHA tests, and it can be frustrating for humans when the tests are cumbersome.

Raj *et al.* [36] introduced a new image-based CAPTCHA simply in graphical form. The CAPTCHA has advantages over other text-based CAPTCHAs in that, no malicious program could perform any segmentation, thresholding, shape matching nor random guessing for edge-detection. During its analysis process for security checks, the mechanism showed better results. However, future algorithms were found to break the graphics CAPTCHA.

In 2014, Nguyen [37] worked on systematically investigating the security strength of text-based CAPTCHAs by focusing on text animation (2D, 3D and 4D). In doing this, a tool box was developed with novel algorithms and attacks to help analyze the alternative to the security of design paradigms. In his work which can be categorized under CAPTCHA recognition, he showed that segmentation-resistance, a widely accepted design in the creation of text-based CAPTCHAs, still remains an indispensable design principle that applies to animated CAPTCHAs like 2D, 3D and 4D. Thus, he proposed a segmentation-resistant CAPTCHA scheme that identified both the character and its location. His approach highly enhanced the principle of segmentation-resistance thereby paving the way for the design of more secured and usable CAPTCHAs. However, the work solely focused on strengthening the development of just one kind of CAPTCHA-text-based.

Woo *et al.* [38] in their research work focused more on a special kind of Image CAPTCHA–3D CAPTCHA. Image processing has transformed from plain text to 2D and then to 3D. Prior to their work, previous works had already focused on offline pre-processing techniques in breaking 3D CAPTCHAs. In their work grouped under CAPTCHA development, a novel 3D object-based CAPTCHA scheme was proposed to layer the image to be displayed over a 3D object. The prototype developed was presented as a proof of concept that 3D object-based CAPTCHA scheme is an anti-spam mechanism for websites. Their approach was first to ask a user to decipher the 3D object rotation task, e.g. Sketcha. After this, a user will have to solve the 3D text CAPTCHA. It is believed that 3D text recognition, as well as 3D object rotation, while easy for human to solve is a difficult task for a simple machine to solve accurately. The limitation to this work is that there are so many novel approaches that exposes its vulnerability to state-of-the-art vision programs.

Abinaya *et al.* [39] in their work shed lighter on the important features that distinguish phishing websites from legitimate ones and assess how good rule-based data mining classification techniques are in predicting phishing websites and which classification technique is proven to be more reliable. The authors explored the use of images in the preservation of the privacy of image captcha by segmenting the original image captcha into shares that can then be stored in separate database servers in a way that the real image captcha would only be made available when both segmented images are simultaneously available. In essence, they proposed that the individual sheet images would not necessarily reveal the identity of the real image CAPTCHA. Once the real image captcha is revealed to the user it can be used as the password. A limitation to this work is the fact that either transparent images or layers are required to reveal the information.

Castro *et al.* [40] in their work categorized under CAPTCHA recognition, analyzed Capy CAPTCHA (a text-based and puzzle-based Image CAPTCHA) for existing vulnerabilities from the perception of a computer bot. In their work, a side-channel attack was presented that does not solve either of the recognition challenges. Rather, a low-cost attack was proposed that leverages on the continuity of the image's size and measurement. The major limitation with this design decision is that it is vulnerable to attacks of significant difference between image sizes that are wide apart (say 10pixels apart).

Chen *et al.* [41] focused on CAPTCHA recognition and in their work, they reviewed recent developments in the text-based CAPTCHA recognition field. Also, they proposed a CAPTCHA recognition scheme for text-based CAPTCHAs that utilizes a five-stage mechanism in its operation. The mechanisms includes preprocessing, segmentation, combination, recognition, post-processing amongst others.

Chen *et al.* [42] in their work proposed an attack on hollow CAPTCHA with the aid of merging and accurate-filling. The work which can be categorized as CAPTCHA recognition proposes a framework that supports individual character components through character segmentation that aids classification. The process involves repairing the character contours by a thinning operation and a contour-filling algorithm is then applied to solidify the characters. Segmentation is then introduced to separate the characters and this is closely followed by the utilization of the nearest neighbor algorithm to obtain individual characters void of redundancy. Finally, a convolutionary neural network is introduced to acquire final recognition results. Conclusively, the results from the experiment shows that the proposed method has a higher success rate and a superior efficiency in attack when compared with existing typical attack methods on hollow CAPTCHAs.

Divyashree [43] in his work grouped under CAPTCHA development proposed incorporation of password transmission into the CAPTCHA verification process to aid in determination of the strength of the password especially in certain environment. The Author therefore proposes two unified real-time authentication mechanisms which he named cognitive CAPTCHA and honeypot generation for protecting the information being provided over internet. The significant contribution in his work is the generation of an all-inclusive, non-reusable cognitive CAPTCHA rather than relying on external CAPTCHA services for authentication. The essence of designing cognitive CAPTCHA was to have unrestricted access and control of Image conversion in real-time, and this makes the inclusion of a honeypot trap to give a deviation for the spam bots to get trapped thereby eliminating the robot spams. Honeypots and cognitive CAPTCHA are generated in real-time within the website, risks of relying on CAPTCHA service providers, facing denial of services and bearing its cost are completely eliminated.

Yu and Darling [44] in their work categorized under CAPTCHA recognition, presented a low-cost approach which capitalizes on the operation of open-source libraries for an AI-based chosen-plaintext attack. Samples were generated in large quantities from the Python CAPTCHA open-source libraries in modules and then edited in order to track the character's profile placed in the image. Segmentation then occurs by means of a customized convolutionary neural network (CNN) through peak segmentation. Characters present in the segmented samples were then identified using a process called TensorFlow object detection. The experimental results showed that the proposed TensorFlow object detection merged with convolutionary neural network (TOD+CNN) model could break open-source CAPTCHA libraries and could even go further to break external Claptcha-like CAPTCHAs such as Delta40 benchmark.

Ma *et al.* [45] in their work categorized under CAPTCHA recognition, presented an adaptive median filtering algorithm using divide and conquer that recognizes and breaks CAPTCHA. In their research, they improved efficiency through correlation after the filtering window data was sorted. Next was the adaptive readjustment of the size of the filtering window in order to eliminate the noise density. Superior performance was achieved when compared with the conventional median filters which gives their work an edge. However, one adverse effect of their experiment is that the denoising effect is very poor with images that appear blurry or stroked (examples of that will include Gimppy as well as other 2D, 3D and 4D CAPTCHAs). The effect of the denoising on blurry images causes faulty or wrong recognition. As a recommendation for future work, the Authors planned to further improve the filtering performance under higher noise intensity and severe distortion.

Zhang *et al.* [46] in their work were much more concerned about who is solving a CAPTCHA, a human or a computer bot (which they called a typer). Not only that, but also, when a human is solving, is it intentional or a decoy. In their work which is categorized under CAPTCHA development, it is opined that in modern times, development of CAPTCHAs is being crowdsourced into strange and foreign web applications allowing unsuspecting users (also known as typers) solve the CAPTCHAs for bots unknowingly. The work proposed the introduction of personal (login) information into the CAPTCHA and by extension break the linkup between attackers and the typers. An analysis of the existing CAPTCHA solving mechanism was conducted and this resulted to the introduction of a principle for blocking the typers. The methodology was subsequently tested with two web applications and the resultant effect was the incorporation of a generation algorithm to tolerate human error and in the process complicate matters for typers. While it is a known fact that typers can randomly guess attack albeit at a very low success rate, a legitimate user (human, with intent) would accurately solve same CAPTCHA within seconds.

Recently, in the area of object recognition, the results that has been obtained with the help of DCNN cannot be over-emphasized. Every research work in the area of object recognition has been all about improvement in performance of DCNN. Beginning from Image recognition [47], handwriting recognition [48], face recognition [49] and also CAPTCHA recognition [50]. CNN are neural networks having tied parameters for a range of neurons. Like other neural networks, they are made up of several filtering layers and each layer applies an affine transformation to the vector input followed by an elementwise non-linearity.

However, for convolutional networks, the affine transformation are usually implemented as a discrete convolution in the place of a fully general matrix multiplication which other network uses. This sole attribute of convolutional networks makes them computationally efficient in that it allows them scale to large images and also builds equivariance to translation into the model. DCNN on the other hand has a high performance which is very much dependent on supervised learning of model parameters. Also, considering the fact that DCNN has a low recognition accuracy in confusion class makes it the directional path to tread when it comes to CAPTCHA development.

Chen *et al.* [51] in their work proposed a two-stage DCNN class that allows the integration of both the all-class DCNN and also the confusion class DCNN. In their work, categorized under CAPTCHA recognition, they developed a two-staged deep convolutionary neural network (DCNN) framework that uses selective learning confusion class (SLCC) for Text-based CAPTCHA recognition. Contrary to what exists in other frameworks, their work improved accuracy by equipping confusion class samples on DCNN. In doing this, a confusion relation matrix was constructed that focus attention on relationship between classes as opposed to the number of confusing characters in each class. A set partition algorithm was proposed and this algorithm divided multiple subsets based on confusion relation matrix. The CAPTCHA recognition accuracy of confusion classes was thereby increased by training and validating learning algorithm as proposed.

Results from the experiment shows that compared with the existing methods for CAPTCHA recognition, the proposed method delivered higher success rate than its counterparts. In doing this, they were able to construct a relational class that enhances the relationship between other confusion classes which further made analysis of all-class DCNN possible. Furthermore, partition algorithms that divides confusion class into multiple subsets was introduced, and with these, validating and training interactive learning algorithm was produced. The result of their work was an improved text-based CAPTCHA recognition accuracy by 1.4% to 39.4%.

3. RESEARCH MODEL

Kitchenham and Charters [52] presented a model for carrying out systematic literature review which was adopted alongside the fundamentals towards a seamless conduct of study as presented by Höst and Alagić [53].

3.1. Research question

The focus of this study is to provide an answer to the research question below:

What is the trend of research work and the level of interest that researchers are picking in CAPTCHA design and recognition, with a special review of the latest and most researched issues and category?

In order to aid a definitive answer to this question, a review of current works in literature was carried out.

3.2. Reasons for considering studies in this review in this field

In recent times, the process of gathering relevant information on intrusion detection systems based on diverse literature was topmost on web security. However, the work was finally restricted to the CAPTCHA domains, this is in tandem with the work of [54], [55]. The detailed inclusion and exclusion criteria applied to this review are illustrated in the Table 1.

Table 1. Considerations for inclusion and exclusion in this review

SN	Inclusion Criteria	Exclusion Criteria
1	Articles are within the Computer Science and IT subject area	Publications focusing on intrusion detection systems (because that in itself is a broad topic and can very ambiguous for this review
2	Articles are solely written English Language	Theoretical literatures or critiques
3	Publication year was limited to the 2001 to 2019 range	Non-peer-reviewed journal articles
4	Only publications from journals, conferences and workshops were selected	Web pages related mentions but with insignificant technical information
5	CAPTCHA (design/development or recognition) must be in the article topic	Hypothetical or technical reports and workshops on CAPTCHA
6	Articles that are peer-reviewed and proceedings from conferences	Television commentaries or newspaper reports
7	Previous reviews in the area of CAPTCHA strengths and weaknesses	Editorials that discussed the field with a focus on arguments for research requirement

3.3. Strategies for searching for relevant publications

Diverse steps were considered in the process of gathering literatures. Elsevier, Journal of Science, Researchgate, ScienceDirect, ACM Digital Library, IEEEXplore and SpringerLink were key players in this quest. Search terms were particularly in the following categories of interest: Intrusion detection systems, CAPTCHAs, CAPTCHA development and recognition, and current trends in CAPTCHA. Every of the categories of search terms were used either in isolation or concatenated using the regular Boolean operators “AND” and “OR”. Table 1 as shown below is the systematic literature and information search strategy.

A test for synonyms engaged in the literature was adopted using a selection and combination of keywords and this assisted in covering a variety of latest and relevant publications on CAPTCHA development in CNN. The search terms below were engaged. The following combinations of search terms were applied: CAPTCHA OR CAPTCHA review or intrusion detection systems or CAPTCHA recognition or CAPTCHA development or CAPTCHA literature review or CAPTCHA mechanism or recent works on CAPTCHA or Application of AI techniques in CAPTCHA or CNN in CAPTCHA or DCNN and Information technology or computer science.

4. RESULTS AND DISCUSSION

Initially, this search mechanism utilized above produced a total selection of n=258 publications; out of these, n=173 were chosen from databases (search steps 1 and 2, Table 2). Also, n=25 were selected through open search on websites and establishing contacts with individuals (search steps 3–5, Table 2). In step 1, we took off n=130 articles based on the relevance to the study and consideration of the language of communication, title and deletion of duplicates. The remaining n=128 publications were then reviewed, and a further n=58 got eliminated for not meeting the inclusion criteria as indicated in Table 2.

Table 2. Comparison of common classification techniques [56]

Authors	Decision Trees	Neural Networks	Naïve Bayes	K-Nearest Neighbor	Support Vector Machine
	Quinlan (1979; 1993)	Rosenblatt (1962)	Duda and Hurt (1973)	Cover and Hart (1967)	Vapnik (1995)
Accuracy	√√	√√√	√	√√	√√√√
Learning Speed	√√√	√	√√√√	√√√√	√
Classification Speed	√√√√	√√√√	√√√√	√	√√√√
Tolerance Value	√√√	√	√√√√	√	√√
Tolerance to irrelevant values	√√√	√	√√	√√	√√√√
Tolerance to redundant values	√√	√√	√	√√	√√√
Tolerance to highly interdependent values	√√	√√√	√	√	√√√
Dealing with Discrete or Binary or Continuous attributes	All	Not Discrete	Not Continuous	All	Discrete
Noise tolerance	√√	√√	√√√	√	√√
Dealing with overfitting danger	√√	√	√√√	√√√	√√
Incremental learning attempt	√√	√√√	√√√√	√√√√	√√
Support multi-classification	√√√√	Naturally Extended	Naturally Extended	√√√√	Binary Classifier
Explanation ability, knowledge, transparency, classification	√√√√	√	√√√√	√√	√

The final step of selection had us focusing on the impact of CNN and DCNN on CAPTCHA development and recognition with a comprehensive discussion including all authors, and this led to the inclusion of an additional study from the references list in one of the publications on DCNN. Conclusively, 70 studies were identified to have fulfilled all the established selection criteria and were thereby included in this review.

4.1. Search string

The research scope was never in doubt right from inception with a directional search geared towards the concept, prediction techniques, research gaps, and suggestions. The Research question and choice of words were a direct product of the problem definition, and this is what pointed us to only standard and referred databases [57]. The combination of keywords was essentially to test for titles of articles that are similar and to ensure an in-depth coverage of relevant publications on CAPTCHA design in intrusion detection systems [58]. The different search string combinations are as listed in section 3.3 earlier.

4.2. Purpose of review

This review is an array of research areas focused on intrusion detection systems, employed machine learning techniques, and CAPTCHA development and recognition. Worthy of note is the fact that although CAPTCHA reviews have been regularly carried out, no systematic literature review for current trends in CAPTCHA development and recognition is in existence but rather in CAPTCHA as an IDS or the workability of different types of CAPTCHA. The works of [59]-[61] are on IDS generally using specific approaches but not reviews. CAPTCHA development and recognition using hybrid approaches. In [62], hybrid approaches were employed to solve CAPTCHAs but yet, none is a systematic literature review in that domain to give directions of research. Different algorithmic CAPTCHAs also received attention in various ways based on diverse approaches, [63]. Furthermore, a hybrid approach; and hybrid approaches utilizing Machine Learning concepts like CNN and DCNN in [64], [65]; while [66] is a study on CAPTCHA which also doubles as survey on CAPTCHA development techniques. Review of different kinds of CAPTCHA techniques was done in [67]-[69].

4.3. Research challenges

Bias is a significant challenge when it comes to systematic reviews of literatures. Hence, in ensuring there was no bias in the search categorization, inclusion or exclusion criteria were introduced to help the decision-making process, it was ensured that selected papers were thoroughly scrutinized by each of the collaborating researchers for this work. Table 3 shows details of this. Although, the choice of search strings was strategic in determining the list of papers utilized, a minute change in the strings used for this work would have produced different set of relevant publications from what is presented here. However, our systematic review could still have an element of bias, because the databases consulted, indexed more of the renowned conferences and journals on the subject of machine learning in development and recognition of CAPTCHA; hence, the views of low class publications are ignored. Conclusively, searching further non-English sources will definitely afford a reduction in the possible bias in the study.

From this review, it was observed that a lot of work went into intrusion detection system from 2001 to date. The volume of publications in the domain in the decade at the turn of the millennium was almost doubled between 2011 and 2015, and also having a few review publications for the analysis. Also, there was a consistent increase in the number of publications from 2011, showing more attention in algorithmic infusion into CAPTCHA development using machine learning in the academia. The last few years 2018 and 2019 precisely have witnessed an unprecedented high in publications. Majority of these publications for 2018 and 2019 might not be readily available for analysis; which is evident in the drop in the number of publications accessed. Table 4, 62% of the papers analyzed were from journals; 35% came from conferences while the remaining 3% stems from symposiums and workshops as depicted in Figure 2. The exploration of standard and robust databases afforded us the privilege of ignoring the views of low class publications. Furthermore, our focus was on papers written in only English language. The knowledge presented here therefore does not represent the two aforementioned classes which could have significantly afforded a more robust and in-depth analysis.

Findings of this review having the research questions in mind are as follow:

Research Question - What is the trend of research work and the level of interest that researchers are picking in CAPTCHA design and recognition, with a special review of the latest and most researched issues and category?

It was discovered that the latest works on CAPTCHAs have a few things in common:

- They focus more on either development or recognition of CAPTCHA and;
- Machine Learning and Deep Learning algorithms are the new phase of CAPTCHA.

While the existing literatures have covered IDS, CAPTCHA techniques, selective and deep learning algorithms in the area of CAPTCHA development, and then convolutionary and deep convolutionary neural network (CNN and DCNN) approaches, intrusion detection system is yet to receive adequate attention even though it takes its toll on cybersecurity and how conglomerates, consortiums and organizations fall victim of this anomaly.

Table 3. Information search strategy for literature review

Step	Description	Details
1	Survey of reference lists of relevant publications	A few consulted crucial publications pointed to relevant references
2	Website searches	Visiting sites that have articles related to study
3	Bibliographic Databases	General database
4	Request for information and related texts from colleagues	Establishing contact with colleagues in the academia for required helpful information and pointers to the research
5	Full-text journals	Elsevier, Journal of Science, Researchgate, ScienceDirect, ACM Digital Library, IEEEXplore and SpringerLink
6	Personal mailing requests to authors of impactful publications for full texts, additional information.	Request for full text of publications not available without a particular subscription or payment

Table 4. Yearly distribution of reviewed papers

SN	No.	SN	No.
2001	2	2011	5
2002	0	2012	4
2003	1	2013	3
2004	1	2014	4
2005	3	2015	6
2006	1	2016	4
2007	3	2017	7
2008	4	2018	12
2009	2	2019	5
2010	3	2020	0

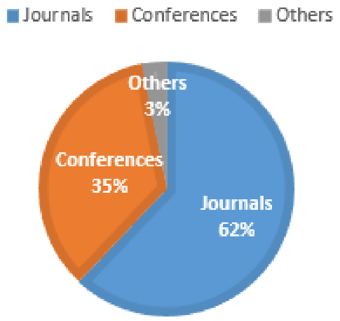


Figure 2. Distribution of article source for literature review

5. CONCLUSION

In this survey paper, a systematic literature review has been carried out on current trends in Intrusion Detection Systems with a focus on CAPTCHA development and recognition, in order to understand the trend of research interests so far in CAPTCHAs in the context of development and recognition based on both the currently researched issues. The articles that aided this survey have highlighted deep learning algorithms and machine learning techniques to both detect and design new forms of CAPTCHA in order to further enhance the security systems of web applications with the engagement of several approaches prominent amongst which is the hybrid techniques. Machine learning and deep learning algorithms, types, forms, and security, accuracy and performance measures are of importance in the review. The survey reveals that although CAPTCHAs as a form of Intrusion detection systems is widely accepted in web applications, its workability, performance, accuracy and security is not only based on the algorithm and mechanism put to use, but also a function of the type of CAPTCHA, data pre-processing, how the hybrid techniques are combined, and several other factors. This paper would guide future researchers in their choice of CAPTCHA development and recognition techniques to use and a pointer to available and possible improvements on some of the existing techniques.

ACKNOWLEDGEMENTS

Deep Aappreciation to my Institution Landmark University for their immense support and enabling environment for research. Profound gratitude to my Supervisor, Prof. Ayodele Adebiyi for his immense support and supervision. Appreciation to Prof. A. E. Okeyinka who ensured I doubled up in preparation for this. Appreciation also goes to Dr. Mrs. Marion Adebiyi who was a readily available listening ear.

REFERENCES

[1] S. W. Smith, “WebALPS : A Survey of E-Commerce Privacy and Security Applications,” ACM SIGecom Exchanges, vol. 2, no. 3, pp. 29-36, Jun. 2001, doi: 10.1145/844324.844329.

[2] M. M. Choudhury, “A study of the significant factors affecting trust in electronic commerce,” Doctoral thesis, Durham University, 2009.

[3] V. Khu-smith, “Enhancing the security of electronic commerce transactions,” Department of Mathematics, Royal Holloway, University of London, England, Jun. 2003 [Online]. Available: http://digirep.rhul.ac.uk/items/e42a99f4-78e1-69a3-87fd-6ac743f828ca/1/.

[4] A. Ansalem Ez and E. Igbekele, “Cloud Computing Research in Nigeria: A Bibliometric and Content Analysis,” *Asian Journal of Scientific Research*, vol. 12, no. 1, pp. 41-53, 2019, doi: 10.3923/ajsr.2019.41.53.

[5] M. S. Soares and J. M. S. França, “Characterization of the Application of Service-Oriented Design Principles in Practice: A Systematic Literature Review,” *Journal of Software*, vol. 11, no. 4, pp. 403-417, Apr. 2016, doi: 10.17706/jsw.11.4.403-417.

[6] M. Endrei, J. Ang, A. Arsanjani, S. Chua, P. Comte, P. Krogdahl *et al*., “Patterns: Service Oriented Architecture and Web Services,” *Redbooks*, Websphere Software, pp. 79-106, 2004.

[7] A. Higgins, “Adaptive Containerised Honeypots for Cyber-Incident Monitoring,” *Integrated Masters in Computer Engineering (M.A.I.),* May 2018 [Online]. Available: https://www.scss.tcd.ie/publications/theses/diss/2018/TCD-SCSS-DISSERTATION-2018-001-ABSTRACT.pdf.

[8] B. Mphago, “Deception in Web Application Honeypots: Case of Glastopf,” *International Journal of Cyber-Security and Digital Forensics*, vol. 6, no. 4, pp. 179–185, 2017, doi: 10.17781/p002304.

[9] N. Nassar and G. Miller, "Method for two dimensional honeypot in a web application," *8th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom)*, 2012, pp. 681-686, doi: 10.4108/icst.collaboratecom.2012.250743.

[10] A. J. Nkwetta, “Honey-System: Design, Implementation and Attack Analysis,” College of Technology, Universityof Buea, Jul. 2018.

[11] W. K. A. Hasan, “A Survey of Current Research on CAPTCHA,” *International Journal of Computer Science and Engineering Survey*, vol. 7, no. 3, pp. 1-21, 2016, doi: 10.5121/ijcses.2016.7301.

[12] N. Sahu and V. Richhariya, “Honeypot: A Survey,” *International Journal of Computer Science and Technology*, vol. 3, no. 4, pp. 858-864, 2012.

[13] C. J. Hernández-Castro, M. D. R-Moreno, D. F. Barrero, and S. Gibson, “Using machine learning to identify common flaws in CAPTCHA design: FunCAPTCHA case analysis,” *Computers and Security*, vol. 70, pp. 744-756, 2017, doi: 10.1016/j.cose.2017.05.005.

[14] E. Bursztein, S. Bethard, C. Fabry, J. C. Mitchell and D. Jurafsky, "How Good Are Humans at Solving CAPTCHAs? A Large Scale Evaluation," *2010 IEEE Symposium on Security and Privacy*, 2010, pp. 399-413, doi: 10.1109/SP.2010.31.

[15] M. Blum, L. A. von Ahn, and J. Langford, “The CAPTCHA Project, Completely Automatic Public Turing Test to Tell Computers and Humans Apart,” Dept. of Computer Science, Carnegie-Mellon Univ, Nov. 2000 [Online]. Available: http://www.captcha.net.

[16] V. Butrimas, “Threat Intelligence Report Cyberattacks Against Ukrainian Ics,” *Report, Threat Intelligence*, 2019.

[17] E. N. Kaur, “Introduction of Cyber Crime and Its Type,” *International Research Journal of Computer Science (IRJCS)*, vol. 5, no. 08, pp. 2014-2018, 2018, doi: 10.26562/IRJCS.2018.AUCS10080.

[18] L. von Han, M. Blum, and J. Langford, “Telling Humans and Computers Apart (Automatically) or How Lazy Cryptographers do AI,” in *Communication of the ACM*, vol. 3, pp. 1-11, 2013.

[19] J. Anil, G. S. Naveli, and S. Bhukya, “Image Based Captcha Generation System,” *International Journal of Pure and Applied Mathematics*, vol. 118, no. 24, pp. 1-9, 2018.

[20] Y. Ba, “Understanding Cybercrime and Developing a Monitoring,” Turku University of Appied Sciences, 2017.

[21] M. T. Banday and N. A. Shah, “A Study of CAPTCHAs for Securing Web Services,” *International Journal of Secure Digital Information Age*, vol. 1, no. 2, pp. 66–74, Dec. 2011.

[22] C. R. Ibekwe, “The Legal Aspects of Cybercrime in Nigeria: An Analysis with the UK Provisions,” University of Stirling, 2015.

[23] N. M. Al-Fannah, "Making defeating CAPTCHAs harder for bots," *2017 Computing Conference*, 2017, pp. 775-782, doi: 10.1109/SAI.2017.8252183.

[24] O. Rajaee, G. S. Large, and J. D. Bastian, “In-Depth Study of CAPTCHA,” Pennsylvania State University, 2017, doi: 10.13140/RG.2.2.17533.97768.

[25] V. Premanand, A. Meiappane, and V. A. V. Arulalan, “Survey on Captcha and its Techniques for BOT Protection,” *International Journal of Computer Applications*, vol. 109, no. 5, pp. 1-4, 2015, doi: 10.5120/19181-0661

[26] M. Moradi and M. Keyvanpour, “CAPTCHA and its Alternatives: A Review,” *Security and Communication Networks*, vol. 8, no. 12, pp. 2135-2156, 2015, doi: 10.1002/sec.1157.

[27] E. Bursztein, M. Martin, and J. C. Mitchell, “Text-based CAPTCHA strengths and weaknesses,” *Proceedings of the ACM Conference on Computer and Communications Security*, 2011, pp. 125-137, doi: 10.1145/2046707.2046724.

[28] C. Pope and Khushpreet Kaur, "Is it human or computer? Defending e-commerce with Captchas," in *IT Professional*, vol. 7, no. 2, pp. 43-49, Jan.-Feb. 2005, doi: 10.1109/MITP.2005.37.

[29] K. Chellapilla and P. Y. Simard, “Using machine learning to break visual human interaction proofs (HIPs),” *Advances in Neural Information Processing Systems*, vol. 17, pp. 265-272, 2005.

[30] M. Shirali-Shahreza and S. Shirali-Shahreza, "Advanced Collage CAPTCHA," *Fifth International Conference on Information Technology: New Generations (itng 2008)*, 2008, pp. 1234-1235, doi: 10.1109/ITNG.2008.12.

[31] K. A. Kluever, “Video CAPTCHAs : usability vs security,” *IEEE Workshop on Image Processing*, pp. 1–4, 2008.

[32] A. Hindle, M. W. Godfrey and R. C. Holt, "Reverse Engineering CAPTCHAs," *2008 15th Working Conference on Reverse Engineering*, 2008, pp. 59-68, doi: 10.1109/WCRE.2008.35.

[33] M. T. Banday and N. A. Shah, “Image Flip CAPTCHA,” *The ISC Int’l Journal of Information Security*, vol. 1, no. 2, pp. 105-123, 2009.

[34] T. Yamamoto, J. D. Tygar and M. Nishigaki, "CAPTCHA Using Strangeness in Machine Translation," *2010 24th IEEE International Conference on Advanced Information Networking and Applications*, 2010, pp. 430-437, doi: 10.1109/AINA.2010.55.

[35] A. S. Almazyad, Y. Ahmad and S. A. Kouchay, "Multi-Modal CAPTCHA: A User Verification Scheme," *2011 International Conference on Information Science and Applications*, 2011, pp. 1-7, doi: 10.1109/ICISA.2011.5772421.

[36] S. B. E. Raj, D. Devassy and J. Jagannivas, "A new architecture for the generation of picture based CAPTCHA," *2011 3rd International Conference on Electronics Computer Technology*, 2011, pp. 67-71, doi: 10.1109/ICECTECH.2011.5942052.

[37] V. D. Nguyen, “Contributions to Text-based CAPTCHA Security,” School of Computer Science and Software Engineering, University of Wollongong, vol. 190, 2014.

[38] S. S. Woo, M. D. Rey, and J. Kim, “3DOC : 3D Object CAPTCHA,” *WWW '14 Companion: Proceedings of the 23rd International Conference on World Wide Web*, 2014, pp. 397-398, doi: 10.1145/2567948.2577300.

[39] R. Abinaya, S. Janani, and P. N. Devi, “Anti-Phishing Image Captcha Validation Scheme using Visual Cryptography,” *International Journal of Scientific Research in Science, Engineering and Technology (IJSRSET)*, vol. 1, no. 2, pp. 86-90, 2015.

[40] C. J. Hernández-Castro, M. D. R-Moreno and D. F. Barrero, "Using JPEG to Measure Image Continuity and Break Capy and Other Puzzle CAPTCHAs," in *IEEE Internet Computing*, vol. 19, no. 6, pp. 46-53, Nov.-Dec. 2015, doi: 10.1109/MIC.2015.127.

[41] J. Chen, X. Luo, Y. Guo, Y. Zhang, and D. Gong, “A Survey on Breaking Technique of Text-Based CAPTCHA,” *Security and Communication Networks*, vol. 2017, pp. 1-15, 2017, doi: 10.1155/2017/6898617.

[42] J. Chen, X. Luo, J. Hu, D. Ye, and D. Gong, “An Attack on Hollow CAPTCHA Using Accurate Filling and Nonredundant Merging,” *IETE Technical Review (Institution of Electronics and Telecommunication Engineers*, vol. 35, no. 1, pp. 106-118, 2018, doi: 10.1080/02564602.2018.1520152.

[43] N. Divyashree, “Secured Conversion and Generation of Cognitive CAPTCHA Implementing Honeypot Technique,” *IOSR Journal of Computer Engineering (IOSR-JCE)*, vol. 20, no. 3, pp. 24-26, 2018, doi: 10.9790/0661-2003012426.

[44] N. Yu and K. Darling, “A Low-Cost Approach to Crack Python CAPTCHAs Using AI-Based Chosen-Plaintext Attack,” *Applied Sciences*, vol. 9, no. 10, 2010, doi: 10.3390/app9102010.

[45] W. Ma, J. Qin, X. Xiang, Y. Tan, Y. Luo, and N. Neal, “Adaptive Median Filtering Algorithm Based on Divide and Conquer and Its Application in CAPTCHA Recognition,” *Computer, Materials and Continua*, vol. 58, no. 3, pp. 665-677, 2019, doi: 10.32604/Cmc.2019.05683.

[46] J. Zhang, X. Hei, and Z. Wang, “Typer vs CAPTCHA : Private information based human cheating,” *Beijing Electronics Science and Technology Institute*, pp. 1-17, 2019.

[47] K. Alex, S. Ilya, and E. H. Geoffrey, “ImageNet Classification with Deep Convolutional Neural Networks,” *Handbook of Approximation Algorithms and Metaheuristics*, vol. 25, pp. 1097-1105, 2007, doi: 10.1201/9781420010749.

[48] D. Ciregan, U. Meier and J. Schmidhuber, "Multi-column deep neural networks for image classification," *IEEE Conf. on Computer Vision and Pattern Recognition*, 2012, pp. 3642-3649, doi: 10.1109/CVPR.2012.6248110.

[49] C. Ding and D. Tao, "Trunk-Branch Ensemble Convolutional Neural Networks for Video-Based Face Recognition," in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 40, no. 4, pp. 1002-1014, doi: 10.1109/TPAMI.2017.2700390.

[50] J. G. Ian, B. Yaroslav, I. Julian, A. Sacha, and S. Vinay, “Multi-digit Number Recognition from Street View Imagery using Deep Convolutional Neural Networks,” *Journal of Astrophysics and Astronomy*, vol. 26, no. 2–3, pp. 231–239, 2005, doi: 10.1007/BF02702331.

[51] J. Chen, X. Luo, Y. Liu, J. Wang and Y. Ma, "Selective Learning Confusion Class for Text-Based CAPTCHA Recognition," in *IEEE Access*, vol. 7, pp. 22246-22259, 2019, doi: 10.1109/ACCESS.2019.2899044.

[52] B. Kitchenham and S. Charters, “Guidelines for performing Systematic Literature Reviews in SE,” Keele University and Durham University Joint Report, pp. 1-44, 2007, doi: 10.1145/1134285.1134500.

[53] M. Höst and A. Oručević-Alagić, “A systematic review of research on open source software in commercial software product development,” *Information and Software Technology*, vol. 53, no. 6, pp. 616-624, 2011, doi: 10.1016/j.infsof.2010.12.009.

[54] S. Jalali and C. Wohlin, "Agile Practices in Global Software Engineering - A Systematic Map," *2010 5th IEEE International Conference on Global Software Engineering*, 2010, pp. 45-54, doi: 10.1109/ICGSE.2010.14.

[55] V. M. Rao and Y. P. Singh, "Decision Tree Induction for Financial Fraud Detection," *Proceeding of the International Conference on Artificial Intelligence in Computer Science and ICT (AICS 2013)*, 2013, pp. 321-328.

[56] H. Bhavsar and A. Ganatra, "A Comparative Study of Training Algorithms for Supervised Machine Learning," *International Journal of Soft Computing and Engineering*, vol. 2, no. 4, pp. 74-81, 2012, doi: 10.1.1.492.6088.

[57] Z. Stapić, E. G. López, A. G. Cabot, L. De M. Ortega, and V. Strahonja, "Performing systematic literature review in software engineering," *Central European Conference on Information and Intelligent Systems*, Shanghai, China, 2012, pp. 441-447, doi: 10.1145/1134285.1134500.

[58] M. Maguire and B. Delahunt, "Doing a Thematic Analysis: A Practical, Step-by-Step," *The All Ireland Journal of Teaching and Learning in Higher Education*, vol. 8, no. 3, p. 3351, 2017.

[59] M. Conti, C. Guarisco, and R. Spolaor, "CAPTCHaStar! a novel CAPTCHA based on interactive shape discovery," *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, Springer, Cham, 2016, pp. 611–628, doi: 10.1007/978-3-319-39555-5_33.

[60] T. Gougeon and P. Lacharme, "How to Break CaptchaStar," *Internatonal Conference on Information Systems Security and Privacy*, pp. 41-51, 2018, doi: 10.5220/0006577600410051.

[61] S. H. Bhandari and S. M. Deshpande, "A Dual Domain Approach for Surface Roughness Evaluation," *International Conference on Computational Intelligence and Multimedia Applications (ICCIMA 2007)*, 2007, pp. 344-348, doi: 10.1109/ICCIMA.2007.308.

[62] B. S. Rachana, S. Dhruthi, R. Swarna, and A. Chandan, "Improved Security Aspects on Microsoft's Two-Layer Captcha," *IJARIIE*, vol. 2, no. 5, pp. 46-52, 2017.

[63] J. Yan and A. S. El Ahmad, "Breaking Visual CAPTCHAs with Naive Pattern Recognition Algorithms," *Twenty-Third Annual Computer Security Applications Conference (ACSAC 2007)*, 2007, pp. 279-291, doi: 10.1109/ACSAC.2007.47.

[64] H. Nejati, N. M. Cheung, R. Sosa, and D. C. I. Koh, "DeepCAPTCHA," *Proceedings of the 5th ACM Multimedia Systems Conference*, 2014, pp. 81-90, doi: 10.1145/2557642.2557653.

[65] S. Sivakorn, I. Polakis and A. D. Keromytis, "I am Robot: (Deep) Learning to Break Semantic Image CAPTCHAs," *2016 IEEE European Symposium on Security and Privacy (EuroS&P)*, 2016, pp. 388-403, doi: 10.1109/EuroSP.2016.37.

[66] M. Subramanyam and V. Priya, "A Study of Captcha Techniques and Development of SUPER Captcha for A Study of Captcha Techniques and Development of SUPER Captcha for Secured Web Transactions," *International Journal of Appkied Engineering Research*, vol. 10, no. 21, pp. 20135-20141, 2015.

[67] V. P. Singh and P. Pal, "Survey of Different Types of CAPTCHA," *International Journal of Computer Science and Information Technologies*, vol. 5, no. 2, pp. 2242-2245, 2014.

[68] D. Brodić, A. Amelio, and R. Janković, "Exploring the influence of CAPTCHA types to the users response time by statistical analysis," *Multimedia Tools and Applications*, vol. 77, no. 10, 2018, doi: 10.1007/s11042-017-4883-7.

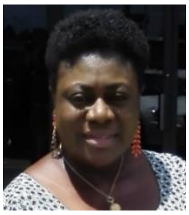
[69] P. P. Doke and S. A. Nagtilak, "A Survey on CAPTCHA as Graphical Password," *International Journal of Science and Research (IJSR)*, vol. 4, no. 12, pp. 2032–2036, 2015, doi: 10.21275/v4i12.nov152436.

BIOGRAPHIES OF AUTHORS

Igbekele Emmanuel O. is a Ph.D research student of Landmark University whose research is focused on Cybersecurity and Service Oriented Architectures. He has been in the Cybersecurity research field since 2012 during his final year as an Undergraduate student. He holds a Bachelor of Science Degree in Computer Science and a Masters Degree in Computer Science at University of Ibadan, Ibadan and the prestigious Covenant University, Ota, Nigeria respectively. He has certifications in Data Virtualization and Cybersecurity.

Adebiyi, Ayodele Ariyo, is a faculty and former Head of Department of Computer and Information Sciences, Covenant University, Ota Nigeria. He is currently the Dean, College of Pure and Applied Sciences at Landmark University, Omu-Aran, Nigeria, a sister University to Covenant University. He holds a B.Sc degree in Computer Science and MBA degree from University of Ilorin, Ilorin, Nigeria in 1996 and 2000 respectively. He had his M.Sc and Ph.D degree in Management Information System (MIS) from Covenant University, Nigeria in 2006 and 2012. His research interests include, application of soft computing techniques in solving real life problems, software engineering and information system research. He has successfully mentored and supervised several postgraduate students at Masters and Ph.D level. He has published widely in local and international reputable journals. He is a member of Nigerian Computer Society (NCS), the Computer Registration Council of Nigeria (CPN) and IEEE member.

Francis Ibikunle is a Professor of Information and Communication Engineering and a long-standing practising engineer of over three decades in the industry and in academic research and teaching experience. He received his Bachelor's degree in Electrical/Electronic Engineering and won a Federal Government scholarship award to study abroad and obtained his Masters and PhD degrees in Information and Telecommunications Engineering. He is currently working at Landmark University, Omu Aran, Nigeria as a Researcher in the Electrical and Information Engineering. Prior to being an academic, he had worked in the industry for 19 years. His work experience and areas of research are in Mobile & Wireless Communications, Internet of Things (IoTs), Artificial Intelligence (AI), Energy Sources and Energy efficiency. He has several publications to his credit in categories of dissertations, chapters in books, journal articles, and conference proceedings. He is an associate editor and editorial board member to many referred international journals. He is a registered member of several professional and academic bodies like the Council for the Regulation of Engineering in Nigeria (COREN); Fellow of the Nigerian Society of Engineers (FNSE), Fellow of Nigerian Institution of Power Engineers (FNIPE).



Marion O. Adebiyi received a BSc. degree in computer science from University of Ilorin, Kwara State, Nigeria in 2000. Her MSc. and Ph.D degree also in computer science, bioinformatics Option from Covenant University, Ota, Nigeria in 2008 and 2014 respectively. She is a senior lecturer in Computer Science Department of Landmark University and Covenant University. She authors two books, over ten chapters and more than 50 articles, with over 25 conferences and workshops. Dr Adebiyi heads the H3Africa projects coordinating Division, and Entomology and Data Management Division of Covenant University Bioinformatics Research (CUBRe) group and her research interests include bioinformatics, genomics, proteomics, and Organism's inter-pathway analysis. From 2002 to 2004, she was a web content developer/ IT Technical Officer at the World Mission Agency, Canaan land Nigeria. Since 2006, she joined Computer and Information Sciences Department of Covenant University as a Graduate Assistant and rose through the ranks to an Assistant Professor in 2008. She is currently a Post-Doctoral Fellow at the Department of Information Technology, Durban University of Technology, Durban. South Africa and Senior lecturer at LMU. She authors two books, more than 50 research articles, and has attended over 45 conferences and workshops. Her research interests include bioinformatics, genomics, proteomics, transcriptomics, and Organism's inter-pathway analysis, she is involved in developing and implementing approaches and methods used in genetics research to associate specific genetic variations with diseases and traits, with interest in Infectious diseases of African populations, pathogens, hosts and vectors. She serves as a reviewer to many peer-review journal outlets. She was the West African President of the Regional Student Group Student Council (WA-RSGSC) of International Society for Computational Biology (ISCB) from 2008-2013, she is currently the Treasurer for African Society for Computational Biology and Bioinformatics (ASBCB) since 2015. The CUBRe group is one of the NIH accredited nodes in Africa, a consortium that has made landmark contributions to genomic research, and generally to development of Bioinformatics within the African region.

Oludayo O. Olugbara received B.Sc. and MSc. degrees in Mathematics and Ph.D. degree in computer science. He became a Junior Research Fellow with the Department of Mathematics, University of Ilorin in 1992. He is a full Professor of Computer Science and Information Technology at the Durban University of Technology in South Africa. He is the author of more than 150 research papers in national and international journals, books, book chapters and conference proceeding articles. He has attended many international conferences throughout the world and chaired some technical sessions. His research interest is in the areas of machine intelligence, mobile computing, image processing and exponential technology for smart city development. He had examined several postgraduate theses, dissertations and assessed research publications for professorial appointments both nationally and internationally. He has graduated over 250 Undergraduates, 29 Master's and 13 Doctorate degree students in computer science and information technology. Professor Olugbara was a recipient of many awards that include the International Federation of Information Processing (IFIP) TC2 sponsored by Microsoft Research Cambridge in 2007 and meritorious research paper award at International Conference on Machine Learning and Data Analysis, organized by the IAENG International Association of Engineers, San Francisco, USA in 2012. He was awarded honorary referee of the Maejo International Journal of Science and Technology, Thailand in 2007-2010 and 2011. In December 2015, he was awarded an outstanding scientist by the Center for Advanced Research and Design of Venus International Foundation in India. He became an established researcher courtesy of the National Research Foundation (NRF) of South Africa rating in 2017. He is a University Scholar at the University of Ilorin, Member of Marquis Whos' Who in the World (USA), Member of the Association for Computing Machinery (ACM, USA), Member of Computer Society of South Africa (CSSA) and other academic associations.