

2FA-Securehealth: Strengthening Healthcare Systems With Two-Factor Authentication

Adnan Mazhar Alam¹, Tushar Ghorpade², Ekta Sarda³

¹ Student, Department of Computer Engineering, Ramarao Adik Institute Of Technology, D. Y. Patil Deemed to be University, Nerul, Navi Mumbai 400706.

² Guide, Department of Computer Engineering, Ramarao Adik Institute Of Technology, D. Y. Patil Deemed to be University, Nerul, Navi Mumbai 400706

³ Guide, Department of Computer Engineering, Ramarao Adik Institute Of Technology, D. Y. Patil Deemed to be University, Nerul, Navi Mumbai 400706

Email: ¹ala.adnrt22@dypatil.edu, ²tushar.ghorpade@rait.ac.in, ³ekta.sarda@rait.ac.in

Orchid Id number: ¹<https://orcid.org/0009-0006-4628-889X>

Corresponding Author*: Adnan Mazhar Alam.

Authentication System was unveiled by the efficient computer scientist Ronald Rivest; this was the biggest achievement in the security since the advent of 2FA. Altogether, this innovation developed a strong barrier in the realm of digital security and contributed to the struggle against cyber threats. Two-Factor Authentication (2FA) also known as the two-step verification has therefore evolved as one of the most important security practices for securing access for mobile users. Coupled with threats that are felt online this particular kind of authentication system has a critical role in protecting desirable information from being accessed by unauthorized persons. Since 2FA is a security system that respondents use traditional passwords, KBA, possession-based components such as SMS or OTP, and even complex biometric verifications, it is a strong barrier against hackers and any other unauthorized individuals. Based on the aforementioned points, it would be appropriate to conclude that it is right to claim that the major advantage of implementing 2FA is in attaining a significantly higher level of security than is provided by SHA methods. This added extra layer of security greatly enhances the task of the unauthorized groups to breach the multiple layers of security therefore making 2FA as the gold standard of security in the contemporary society of personal and business protection.

KEYWORDS :- Two Factor Authentication (2FA), Captcha, Multi-Factor Authentication.

1) Introduction:

With constant developments in technology, Two-Factor Authentication (2FA) has turned out to be vital in the protection of any confidential data bearing in mind the case of health related systems. Since cyber-attacks became a common trend and the need of counter measures that would secure sensitive quite the data many clients relied on 2FA technology. Therefore, this paper sets to improve the security structure of 2FA technology by incorporating more sophisticated and advanced cryptographic solutions to protect the enormous patient databases

within the health care systems. The use of two-factor authentication 2FA can be traced back to the “ra/re” Authentication System long developed by Ronald Rivest in the year 1984 and has progressed in fitting other more intricate and safe measures that would be applicable in the modern society.

Traditional means like passwords, CAPTCHAs, and biometrics have proved to have their shortcomings. For example, CAPTCHAs serve their purpose in regard to humans and bots but are in much danger with deep learning abuse [5]. Text-capable CAPTCHAs are widely known to the extent that they are rarely ignored in the current generation of CPUs, but AI masking techniques have made it a repetition. The plus of reviews has been proposed to increase the strength of text data CAPTCHAs against the interference of the HI bots [7], [9]. Furthermore, despite the fact that biometric systems are more secure, they also face problems like imprecision of data and forgery, for example, in unimodal systems [6].

Furthermore, the healthcare sector is more prone to risks of cyber attacks as a result of the confidential nature of patient information. The use of NFC and facial recognition technology in attendance and identification systems has already worked effectively in overcoming the issues of human error, information redundancy, and user-friendly applications [3]. Taking into account these factors, this research aims to learn from such advancements and propose the adoption of a robust and appropriate 2FA algorithm for the healthcare industry that can be implemented via layers of cryptography in transmitting medical information over the communication channels. Utilizing techniques like CAPTCHA and biometric authentication, our objective is to design a powerful real-time access control system that thwarts any cyber threats towards a healthcare information system that seeks to protect all the patients' information [1], [4], [10].

2) Literature Review:

The study proposes a mobile attendance system that integrates Near Field Communication and face recognition technology for security and convenience. In traditional attendance methods and fingerprint recognition such as biometric systems one encounters problems like data reuse problems and finger conditions that cause human errors. Preliminary authentication is done using NFC while Raspberry Pi identifies the student through facial recognition with data stored in the cloud for convenience and flexibility. The methodology involves the use of literature review on attendance systems, near field communication, face authorization, and cloud storage while adopting prototyping model of system development. The purpose of the system is absence of paper and work with it, and it can be useful for real time tracking attendance in education institution along with parent monitoring and management of information flow for faculty members [1]. A new way of boosting CAPTCHA recognition, which deals with the cases when characters in them are wrongly classified as belonging to different classes, is described here. The method proposed introduces a twofold Deep Convolutional Neural Network (DCNN) framework that combines all-class DCNN and confusion-class DCNN. A confusion relationship matrix is built to analyze class confusions whereas set partition algorithm is employed to divide confusion classes into subsets and each subset has its own trained confusing class DCNN. Finally an interactive training and validation algorithm was

used to improve the accuracy of recognition. The results of experiments show that the approach of selective learning can significantly enhance CAPTCHA recognizability, surpassing existing state-of-the-art techniques by 1.4%–39.4% [2]. To tackle the inefficiencies of traditional methods like RFID, NFC and biometric technology have been employed in making a variety of attendance systems. Conventional systems are cumbersome, prone to human error and require significant manual effort. However, while these systems integrated with biometric readings specifically fingerprint identification may provide automation, they are likely to experience problems such as inaccurate readings caused by dirty or wet fingers. Recent developments have seen a combination of mobile devices with NFC and face recognition for improved security as well as fewer mistakes made. For example, an attendance management system that is simplified by ensuring accurate identification via NFC and face authorization which is backed by Raspberry Pi and cloud storage as it reduces paper usage through streamlining attendance management and allows real-time data access. This hybrid approach enhances dependability and efficiency by overcoming limitations of previous methods used in this manner [3]. Stronger security measures, such as complex passwords, CAPTCHA and biometric authentication, have been necessitated in recent years by the rise of cyber-attacks and cyber warfare aimed at safeguarding online platforms and confidential data. But these measures are a big problem for older people; they easily forget hard to remember passwords or go through multifarious authentication processes. Besides, such conditions as cataracts, stroke, and congestive heart failure may hinder the use of biometric authentication leading to false rejections thus posing barriers to accessing important online services like Telehealth. Though Biometric Authentication offers an alternative way of securing our systems it is not without vulnerabilities that may lead to barriers to accessibility among elderly adults especially those with complications in health matters. The aged care sector is among the industries which should give thorough thought about this due to their ever growing aging population [4]. CAPTCHA means Completely Automated Public Turing test to tell Computers and Humans Apart, and it is employed to protect most commercial accounts from malicious bots, and the most common type is the text CAPTCHA. At the same time, improvements have occurred in deep learning methods, which allows for easier penetration of these CAPTCHA systems. Common approaches to attack CAPTCHAs include problems like high algorithmic difficulty, massive sample collection, and manual labeling of images. This paper propose a transfer learning based approach that simplifies the attack and also lower the cost of labeling. Specifically, the current method is to train the model using synthetic samples generated from noise and fine-tuning the model with a few real-world samples; in this way, the attack success rates remain high, which are between 36. undefined Moderate and slight inter-rater agreement of 0.79 and 9% across 25 different online CAPTCHAs . The study also examines how training sample characteristics affect attacks' accuracy, revealing that the dissimilarity between synthetic and real samples is not relevant here, and underlining that transfer learning is important for achieving good performance and decreasing data preparation costs in CAPTCHA attacks [5]. Individuals are authenticated by biometric systems using physical or behavioral attributes, which are referred to as unimodal and multimodal respectively. Noise in the data and imitation attacks are difficulties faced by unimodal systems thereby reducing their accuracy. On the other hand, multimodal systems incorporate various characteristics for better identification and verification. In this article, we examine several unimodal and multimodal approaches noting their pros and cons, recognition steps, architectures, modes of operation,

algorithms as well as fusion techniques. The paper also discusses some limitations that exist in unimodal systems then points out possible directions for future research based on over 200 publications on trends in biometrics from 2011 to 2016 [6]. Bots are putting at risk the dependence of internet users on services such as search engines and email, thereby prompting the use of CAPTCHAs (Completely Automated Public Turing tests) meant to distinguish humans from machines. Even though CAPTCHAs increase security by restricting automatic signups, they still have some weaknesses that can be taken advantage of by those bad programs. This paper explores different types of CAPTCHA available and looks into their merits and demerits in text, image, audio/video and puzzle patterns [7]. CAPTCHAs are developed to facilitate the separation of humans from computers in terms of online security for clarification as finally trusted computers might be too separated from the human input. Nevertheless, conventional text-based CAPTCHAs are difficult to reach and therefore vulnerable to assaults. Recent studies suggest that personalized assessments should use bio-detection functions (BDFs) including colour differentiation and typing rate. This paper examines the shortcomings of current CAPTCHA designs and emphasizes the need for individual customization based on attributes such as color harmony or letter resemblance so as to improve both security and usability [8]. Through the integration of recognition, recall, and cued recall approaches, motion-based CaRP makes it more difficult for those who try to compromise authentication procedures which greatly enhances the security of online systems yet still being user-friendly. So this new way is a better advancement over older CAPTCHA approaches since it has a more robust shield against new risks [9]. Online services expansion brings more vulnerability to different automated attacks in organizations. CAPTCHA is used for distinguishing between human users and bots. This paper presents a novel technique that utilizes custom mouse cursor images and outperforms the existing text and image based CAPTCHAs. Generally, CAPTCHAs are divided into four categories namely: text, audio, image or video; each one having distinct weaknesses such as text recognition confusion or audio file size limitations. Apart from using custom cursors, the proposed approach combines true random number generation (TRNG) to enable users to match between pictures while increasing randomness and making it difficult for machines to attack, The results indicate an increase in the usability as well as the security, and there can also be improvements such as generating images dynamically in future and using drag-and-drop options [10]. CAPTCHA , or Completely Automated Public Turing test to tell Computers and Humans Apart , ensures that responses are generated by human beings rather than bots. This paper gives a puzzle-based CAPTCHA which was developed using HTML, JavaScript , and CSS where users are required to drag and drop images in the right order. The system was developed using an evolutionary prototyping model that comprises of an image collection, processing engine and user interface . Users have to organize images correctly in order to pass but if they fail then another challenge is presented. This approach improves user interaction while at the same time providing strong protection against automation. Simply put, the puzzle based method has the chance to future progressions in terms of high resolution pictures and handheld editing which shows usable yet safe design [11]. Text CAPTCHAs are imperative to avoid cyber intrusions, yet their increasing complexities have made it difficult for commonly used supervised learning methods that depend on large labeled datasets. In order to resolve this issue, the Self-Supervised Multiview CAPTCHA Recognition Model (SSMCR) is proposed based on self-supervised

learning and contrastive loss so as to create efficient representations utilizing restricted labeled data. The model reformulates the recognition task as a multiview problem wherein it generates pseudoviews from original images using a siamese infrastructure with convolutional and recurrent networks' combinations for reliable feature extraction. Through this method, the recognition precision is improved and extensive annotations are no longer needed, hence marking better development in both CAPTCHA security and computer vision [12]. A discussion on what is good about visual or audio CAPTCHAs and what is bad about them has been presented in this assessment. Some weaknesses of visual CAPTCHAs especially those disabled and become vulnerable to OCR attacks are talked about in this document. Based on human physical aspects, image-based CAPTCHAs are suggested to be more secure user-friendly options; their effectiveness and usability are thus put on some balance point. For blind people, indications have been given that computer-coded audio CAPTCHAs can lead to automatic learning problems through segmentation and recognition. In conclusion, it emphasizes that managing CAPTCHA security and accessibility in relation to different categories of users is an ongoing battle [13]. One of the important tasks websites perform is distinguishing between bots and humans, and this is where CAPTCHAs come in. This paper presents a multilingual handwritten CAPTCHA that employs characters in English, Arabic, Spanish and French. The technique improves security against Optical Character Recognition (OCR) attacks through varied samples of handwritings and distortions making it more user-friendly. This approach deals with limitations associated with traditional text based CAPTCHAs while increasing their overall efficiency and accessibility [14]. Biometric systems utilize physiological and behavioral traits for identification and verification, divided into unimodal and multimodal types. Multimodal systems enhance accuracy by addressing unimodal limitations like noise and spoofing. This paper reviews various biometric modalities, detailing the recognition process stages: pre-processing, feature extraction, matching, and decision-making. It explores multimodal architectures, operational modes, fusion methods, and research trends, aiming to identify challenges and improvement opportunities in unimodal systems. Analyzing over 200 publications, the paper provides insights into advancing biometric technologies [15].

2FA-SecureHealth Model

In this unique CAPTCHA system, an added measure of protection is incorporated in the process of verifying the identity of the user. When the user click on the link to expand the CAPTCHA image, a new window immediately appears with a mathematical image that is visible for 3 seconds. It means that a pop-up window will appear, and as soon as one selects a choice, the window will shut down. To advance, the user must type in the correct mathematical content that is shown on the pop-up window. From prior considerations, only after the mathematical image is correctly identified and typed by the user will the user be directed to the dashboard. This method improves the level of security since a person has to recognize and promptly respond to the puzzle or display, and it is difficult for hackers to gain unauthorized access

3) Proposed Methodology:

This section described the details of proposed method named as "SecureHealth", figure 1.0 showing the process of "SecureHealth" was done.

Algorithm :-

Step 1 – Initial from the authentication of the user.

Step 2 – Described 2FA enforces the usage of the captcha-based setup.

Step 3 – If input is successful,

Step 4 – A captcha image containing one or more characters of math equation, or geometric figure, is depicted in a new page for a randomly set time of between 1.5– 2 second this tab, then closes

immediately and the is requested to type the correct name based of the captcha content whether it would be the math problem name if any shape: Circle, etc.

Step 5 – If user type the correct name, they are permitted to the dashboard whereas if they type the wrong name, they didn't get the access.

Step 6 – This security because ID verification goes beyond what is necessary to validate the credentials of a candidate.

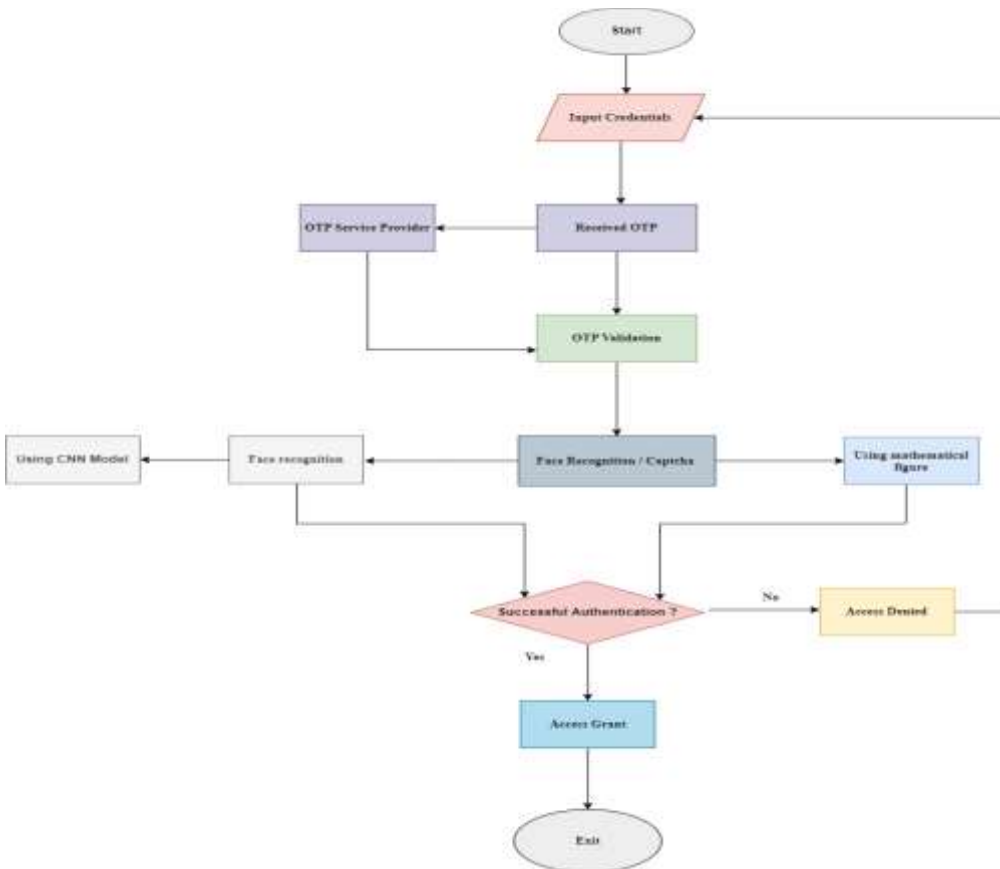


Figure 1.0 Process of 2FA-SecureHealth proposed model

Flowchart In detail review :

1. **Step 1** :- The user attempts to identify and access the system and the process starts.
2. **Steps 2** :- “Input Credentials”.

In the beginning, the user is asked to provide their login details that are a username and a password in order to perform an authentication procedure. This is the most basic level of authentication.

3. **Step 3** :- “Received OTP”:

Once the user has passed the above step and put in their credentials, an exclusive password mainly known as one time password or OTP, is created and forwarded to the user through a service provider carrying such instructions, the most common source being a message, a mail or an app. At this point, the user is required to enter the OTP in order to proceed.

4. **Step 4** :- “OTP Validation”

The system looks at the OTP the end user has entered and determines if it is the same one that was sent. If the OTP is correct, then the procedure continues, OR the subject might be prompted to do it again.

5. **Step 5** :- “Face Recognition / CAPTCHA”.

Here, the user is expected to undergo additional authentication by face recognition or typing a CAPTCHA.

In case the systolic methods are applied, the face of the user will be scanned and compared with the already saved pictures.

In terms of the latter, a user may be presented with some math puzzle or certain shape or anything else that looks non-technical, to prove he corroborates humanity.

6. **Step 6** :- Face Recognition (Optional):

In the event that an individual’s likeness is scanned, a two-dimensional image of the person is digitized and a face recognition technique, possibly based on a CNN algorithm or some other sophisticated technique, is employed. At this stage, the purpose is to confirm that the access system user is indeed the individual matches with the identity profile.

7. **Step 7** :- Using CAPTCHA (Optional):

In a situation that CAPTCHA is used, a user is displayed a circle or square and asked to identify the figure or solve some math problem. The person has to solve it correctly in order to move forward.

8. **Step 8** :- Successful Authentication?

- The system confirming if the user has successfully complete the step involving either face recognition or CAPTCHA.
- In case the authentication turns out to be successful (the face is in the database or compromised CAPTCHA), access is granted.
- If the authentication process is done unsuccessfully, the user is refused access as well.

9. **Step 9** :- Access Granted:

After passing through the authentication procedure, the system allows the user entering the dashboard or using a certain service.

10. **Step 10** :- Access Denied:

If the user fails either face recognition or the CAPTCHA, access is granted, and the user proceeds no further.

11. **Step 11** :- Exit: The process concludes either when access is not granted or when it is granted.

Face Recognition :-

At this stage, we focus on recognizing a face using a Deep Learning technique specifically a neural network with Convolutional layers which has been used frequently for any image-related tasks such as facial verification systems. The methodology of face recognition procedure based on CNN can be explained in several steps which are linked by some mathematical actions which help to distinguish and compare the facial traits of the provided data with the database images.

1. Face Detection and Preprocessing

The first task of face recognition systems then is to collect and prepare facial data from the target input image. The first step before any recognition can occur is to find the face in the image as it requires face detection methods. So, the face image is captured and processed (usually scaled to a fixed image size, made to fit in a gray scale image etc.) in order to provide a standardized input to the CNN model.

2. Feature Extraction via CNN

The CNN model is composed of different layers one of which extracts the desired characteristic from the face image given as an input. The layers of a CNN network include:

Convolutional Layers – these layers perform convolution on the input image with multiple filters (kernels) and derive the local features present in the input logical image. Each filter retake local features like margin, textures, and patterns from the facial insert.

$$(I * K)(x, y) = \sum_i \sum_j I(x-i, y-j) K(i, j)$$

Figure 1 Equation No. 1

Let's assume that I denotes the input image, K – the kernel (or, filter), and (x, y) – spatial coordinates. In this case, the filter is moved along the image to produce a so-called feature map.

Activation Function(ReLU): Thereafter, a non-linearity is introduced by applying an activation function to the output of the convolution generally a ReLU (Rectified Linear Unit) is used. This is useful in making the CNN model capture more complex patterns:

$$f(x) = \max(0, x)$$

Figure 2 Equation No.2

Pooling Layers: In these layers, the feature maps are downsampled in order to lessen their spatial dimensions while keeping vital information intact. One popular type of pooling operation is max-pooling, where the maximum value in a certain area is taken:

$$P_{\max} = \max(F)$$

Figure 3 Equation No. 3

Where F is the feature map, and P_{\max} is the pooled feature.

Fully connected layer: Now it's tapped into the locality features through convolutional layers, and this is flattened up as an input to fully connected layers that actually learn how to combine locality features into a global representation of a face.

Softmax Layer(Classification) Finally, the output of softmax often presents the output of the probability distribution over classes (in that case, everyone whose face is in the database). The recognized face has as the selected class the one with the highest probability

$$p_i = \exp(z_i) / \sum_j \exp(z_j)$$

Figure 4 Equation No. 4

Where θ_i is the probability associated with class c_i and z_i is the output score related to class t_i given by the last fully connected layer.

3. Face Information Grasping and Comparison

Most existing face recognition systems that use CNNs architectures such as FaceNet and DeepFace do not classify images but directly output face embeddings, which is a vector

representation of the face image reduced to a fixed length from a higher dimensional vector space. The system then looks for the resulting embeddings in the database by finding images from the database that have a particular Euclidean distance from the database image.

Creating the Face Embedding: Let I be the input face image. Apply a convolutional neural network that will take this and output an embedding vector $f(I)$. The embedding vector $f(I)$ is indeed the high dimensional vector that is used to represent the image of the face.

$$f(I) \in \mathbb{R}^d$$

Figure 5 Equation No. 5

The parameter 'd' is conventionally identified as being equal to either 128 or 512, defining the amount of dimensions that will be in the embedding space.

Corresponding Faces Using Euclidean Distance: In order to verify the face, the system checks the new embedding $f(I_{new})$ against all stored embeddings $f(I_{stored})$ available in the database by analyzing the distance between two images using Euclidean distance:

$$d(f(I_{new}), f(I_{stored})) = \sqrt{\sum_{i=1}^d (f(I_{new})_i - f(I_{stored})_i)^2}$$

Figure 6 Equation No.6

In the event that the distance is less than a specific limit θ , the system treats the face as verified.

Threshold Criterion :

$$d(f(I_{new}), f(I_{stored})) < \theta$$

Figure 7 Equation 6

In cases where the distance is less than a certain limit, the features of the face will be regarded as being in congruence with the user's face and access will be granted. Conversely, if the distance is greater than the limit, access will be denied.

The Benefits of Employing CNNs in Face Recognition for 2FA.

Precision: CNN's capability to 'see' deep into images and pick out intricate and vague characteristics surpasses regular faces recognition systems.

Substantiveness: One such system employing a CNN is able to complete vast numbers of face recognitions, thus it is appropriate for the systems with a huge people base.

Flexibility: It is less affected by changes in illumination, face pose, facial expression and/or the presence of accessories; hence more reliable than simplistic approaches.

4) Result and Discussion

The main discussions in the future concerning the presented CAPTCHA methodology will be based on considering the factors which will show how effectively introduced CAPTCHA can decrease the number of different sorts of automated attacks, being at the same time

comprehensible for the average user. The major highlighted areas are as follows; The flexibility in difficulty levels. This means that there will be a constant need for refining the system and making sure that it adapts correctly to the balance between security and usability.


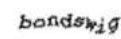


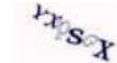

Captcha / Parameters	Sample image	String Length	Limitations
reCAPTCHA by Google		8-10	Distortion, Overlapping, varied fonts
reCAPTCHA by Wikipedia		8-10	Distortion
ReCAPTCHA by Baidu_1		4	Noise lines, Rotation
ReCAPTCHA by Baidu_3		4	Hollowed characters, varied fonts
reCAPTCHA by Microsoft		4-6	Hollowed character, diagonal distribution
2FA-SecureHealth		6	Mathematical image

Table : 1.1 Parameters between existing CAPTCHA and new introduced CAPTCHA

Comparative Analysis of Face recognition using CNN model :

Author / Year	Terminology Used	Dataset	Advantages	Disadvantages
K. Jayanthi, Chitradevi D, Saranya N, S. Anbukkarasi 2023	RCNN framework	Ryerson General media Melody (RAVDESS)	Fast R-CNN detectors sharing the convolutional layer	R-CNN limitations in processing speed and prediction output

Kuupole erubaar ewald 2020	3D facial patch spoof	CASIA- SURF	A new fusion based approach, 3 input modalities IR to detect a real face	Highly cost, complexity
Rong Xie 2019	Small face detection Algorithm	WiderFace	Superior algorithm	Low accuracy, High false positives
Shun-Cheung Lai 2019	SRNet and FNet	CelebA	High-quality image reconstruction	High computational cost, Require large training data
Abdulfattah E. Ba Alawi 2021	DNN model, MobileNetV2	RMFD, SMFD	High accuracy, lightweight, fast interference	High computational cost, low accuracy in details

Table : 1.2 Comparative analysis of Face-recognition**5) Future Scope**

To enhance both security and usability, future enhancements to the CAPTCHA may entail integration of dynamic difficulty levels, making use of machine learning for optimization, as well as incorporation of mobile, voice and multilingual adaptation.

6) Conclusion

Hence, the proposed CAPTCHA methodology enrolls cognitive and temporal components for the new CAPTCHA methodology to enhance the security of authentication. This approach operates on the principle of making the user perform a task in which he or she works with a pop-up, or the image of a mathematical equation for a few seconds, making it hard for bots to mimic the process. The need to complete part of the mathematical content read on the pop-up window and retype it also contributes to security, as it also adds more robustness to the authentication process. This method has the added advantage of improving the efficiency of the CAPTCHA systems and at the same time also the usage level which ultimately leads to greater safety and reliability to the control of the dashboard's access.

7) References:

- 1) A. Gupta, P. Medhi, S. Pandey, P. Kumar, S. Kumar and H. P. Singh, "An efficient multistage security system for user authentication," 2016 International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT), Chennai, India, 2016
- 2) 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.
- 3) S. U. Masruroh, A. Fiade and I. R. Julia, "NFC Based Mobile Attendance System with Facial Authorization on Raspberry Pi and Cloud Server," 2018 6th International Conference on Cyber and IT Service Management (CITSM), Parapat, Indonesia, 2018, pp. 1-6
- 4) M. A. Kowtko, "Biometric authentication for older adults," *IEEE Long Island Systems, Applications and Technology (LISAT) Conference 2014*, Farmingdale, NY, USA, 2014
- 5) P. Wang, H. Gao, Z. Shi, Z. Yuan and J. Hu, "Simple and Easy: Transfer Learning-Based Attacks to Text CAPTCHA," in *IEEE Access*, vol. 8, pp. 59044-59058, 2020
- 6) M. O. Oloyede and G. P. Hancke, "Unimodal and Multimodal Biometric Sensing Systems: A Review," in *IEEE Access*, vol. 4, pp. 7532-7555, 2016
- 7) Y. S. Aljarbou, "Improving of Current CAPTCHA Systems," 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 2019
- 8) N. Nanglae and P. Bhattarakosol, "A Study of Human Bio-detection Function under Text-Based CAPTCHA System," 2012 IEEE/ACIS 11th International Conference on Computer and Information Science, Shanghai, China, 2012
- 9) K. Anjitha and I. K. Rijin, "Captcha as graphical passwords-enhanced with video-based captcha for secure services," 2015 International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), Davangere, India, 2015
- 10) V. A. Thomas and K. Kaur, "Cursor CAPTCHA — Implementing CAPTCHA using mouse cursor," 2013 Tenth International Conference on Wireless and Optical Communications Networks (WOCN), Bhopal, India, 2013
- 11) F. A. B. Hamid Ali and F. B. Karim, "Development of CAPTCHA system based on puzzle," 2014 International Conference on Computer, Communications, and Control Technology (I4CT), Langkawi, Malaysia, 2014
- 12) M. O. Yusuf, D. Srivastava and R. Kushwaha, "Exploring self-supervised learning in Multiview captcha recognition," 2023 IEEE 20th India Council International Conference (INDICON), Hyderabad, India, 2023, pp. 1106-1111, doi: 10.1109/INDICON59947.2023.10440750.
- 13) Saikirthiga and S. Vaithyasubramanian, "Review on development of some strong visual CAPTCHAs and breaking of weak audio CAPTCHAs," 2016 International Conference on Information Communication and Embedded Systems (ICICES), Chennai, India, 2016

- 14) M. H. Aldosari and A. A. Al-Daraiseh, "Strong multilingual CAPTCHA based on handwritten characters," 2016 7th International Conference on Information and Communication Systems (ICICS), Irbid, Jordan, 2016, pp. 239-245, doi: 10.1109/IACS.2016
- 15) Z. Cheng, Z. Wu, Z. Yang, Z. Yang, X. Li and W. Liu, "Reinforced Perturbation Generation for Adversarial Text-based CAPTCHA," 2024 27th International Conference on Computer Supported Cooperative Work in Design (CSCWD), Tianjin, China, 2024