A Deep Dive Into Iris Recognition: Leveraging Machine Learning For Improved Biometric Security

[1]Mr.Venkata Prasanth Tirupati
[1]Student
Department of Computer Science andEngineering
PSCMR College of Engineering andTechnology
Vijayawada, Andhra Pradesh, India

[2]Mr. Abhiram Valluri
[2]Student
Department of Computer Science and Engineering
PSCMR College of Engineering andTechnology
Vijayawada, Andhra Pradesh,India

[4]Mrs.V.Rama Lakshmi
[4]Associate Professor Department of Computer Science and Engineering
PSCMR College of Engineering andTechnology
Vijayawada, Andhra Pradesh,India

[3]Mr. V. Mani Sai Kiran
[3]Student
Department of Computer Science and Engineering
PSCMR College of Engineering andTechnology
Vijayawada, Andhra Pradesh,India

***Abstract*— The significance of validity, uniqueness, and reliability in the iris biometric validation system for person identification is covered in the study. The validation method is built on iris recognition and fingerprint technology, which is very genuine and distinct from other recognition systems. The shortcomings of the unimodal biometric system are addressed by the multimodal biometric procedure. This procedure considers noise sensitivity, population coverage areas, hacker vulnerability, a variety of intra- and inter-class concerns, and non-universality requirements. The convolutional neural network (CNN) approach, in particular, is the primary emphasis of the paper's deep learning-oriented machine learning system. Using real fingerprints, the fingerprint-based iris recognition technology verifies people's identity for use in high-security protection systems.**

Keywords—— Iris Recognition, FingerPrint Technology, CNN, Deep Learning, Machine Learning.

I. INTRODUCTION

Biometrics are commonly used to identify individuals based on physical characteristics. Various authentication systems, such as fingerprint, iris, and voice recognition, have been widely used. Biometrics focuses on the technical aspects of bodily control and measurement. The authentication system relies on biometric security measures, which are increasingly important in all nations. The system performed wellacross all methods and aspects, demonstrating its validity. Fingerprinting is the only secure method that ensures system uniqueness and anonymity. According to a recent study, hackers target computer infrastructure every 39 seconds on average. This remark implies that security systems are becoming increasingly important. However, simple security measures like login and password are not effective[1]. Many users choose easy-to-guess passwords, PINs, or nicknames. Some people scribble their credentials on credit cards or glue them to computers. This may imply that the user is the weakest link in thecomputer system. The fundamental question is, how can it be altered? The answer to such a situation is simple. Biometrics is a well-recognized solution. Human identification science uses quantifiable features such as fingerprints, iris, retina, and keystroke dynamics to verify individuals. There are three types of features: physiological (related to our body and measurements), behavioral (e.g. signature), and hybrid (combining physiological and behavioral qualities, such as voice). Biometric-based computer security systems eliminate the need for extra passwords since users' measured features serve as actual passwords. Research indicates that iris is a key factor in achieving high accuracy, efficiency, and recognition rates. This feature has almost 250 distinct components. The feature vectors describe human identity. Research has shown that the feature vectors for both eyes of a person (left and right) differ significantly, and this is also true for twins. They each have unique irises (with distinct feature vectors). The most essential aspect is that the iris is difficult to fake. There are only a few research publications that give proof of successful spoofing procedures. However, it must be stated that these works utilized rudimentary iris-based biometric devices. These systems do not account for iris-liveness, making them subject to print attacks. However, collecting high-quality iris samples requires specialized instruments, which is a significant disadvantage. Some circumstances require the aid of a skilled ophthalmologist to finish the procedure. Of course, iris samples may be gathered using cutting- edge smartphones (such as the Apple iPhone 12, Max, or Samsung Galaxy S20+) with high-resolution cameras. However, further support is required. To gather these pictures independently, specialized sensors are available on the market. However, their costs are significant, and some require certain lighting conditions to produce exact, high-quality photographs [2]. There are several methodologies and algorithms for recognizing identities using iris biometrics in the

literature. This quantifiable quality ensures excellent efficiency and precision, leading to a significant quantity of work on the subject. Daugman's algorithm is a key solution [3]. This technique encodes random iris patterns in real-time using a specified distance metric. The vectors are then tested for statistical independence. This is a well-known answer, often contrasted with innovative ideas. This algorithm is also recognized as a standard in other works and systems. Another intriguing algorithm was introduced in [4]. The scientists employed PCA and DWT to extract optimal features from iris images and minimize processing time. The authors said that their method should operate in real-time. This study likewise employed frequencies to characterize the sample, however the results differed from our technique. The authors of the research reported that the algorithm achieved 95.4% accuracy on 100 iris scans. The authors' failure to test their theory on larger samples raises the most pressing concern about their study. The next worthwhile option was given in [5]. This study explores the notion of negative iris recognition. The investigation was conducted using negative iris databases. This effort aims to determine if the protective mechanisms used on iris templates may render them unrecoverable to hackers. Recent systems may not ensure efficiency and accuracy, particularly for bank accounts and sensitive data. This work does not explicitly focus on iris recognition. However, the fundamental purpose of this work is to understand how to safeguard iris feature vectors in databases. When designing iris-based security systems, it's important to include prevention against spoofing. Biometrics systems typically rely on printed pictures for recognition, rather than real samples. It is especially relevant to iris-based systems. This problem is thoroughly explained in [6]. The article suggests that using print attack photos of live iris, contact lenses, or a combination of both can significantly impact false-positive detection by the system. All experiments used the IIIT-WVU iris dataset. The authors proposed a new method to avoid assaults using a deep convolutional neural network. Another intriguing study was described in [7]. The authors of this research provide a revolutionary way to recognize human identities using iris technology. However, they only analyzed low-quality photos. Their approach relies on lifting wavelet transforms. The authors stated their approach can ensure excellent accuracy for the CASIA V1 dataset. However, they did not disclose any findings from other databases. The algorithm's accuracy was calculated in a way that limits the solution's actual efficiency. Using a single database does not ensure consistent solution efficiency and correctness across different sample sets. In the publication [8], the authors proposed a method for calculating the quality of iris images. Poor quality samples have been linked to higher false rejection rates (FRR) and worse system performance (accuracy). The authors suggested their method for assessing iris image quality. The study describes a measure based on statistical properties of local picture intensities, including sign and magnitude. This study is noteworthy because it allows us to pick whether to use a conventional algorithm for iris identification or to enhance image quality through additional phases. Deep learning and machine learning are increasingly being used in biometrics for classifying measurable features. This phrase also applies to the iris. The authors searched several databases (IEEE, Scopus, SpringerLink) for studies on iris-based person recognition using convolutional neural networks [9, 10], support vector machines [11], and deep learning approaches [12, 13]. While these ideas are intriguing, they require large databases and significant computational power to launch. While they can ensure precision and efficiency, it come at a significant expense. Furthermore, such methods are almost hardto implement. It is difficult to implement these solutions on mobile devices like smartphones or wearables.

II. LITERATURE SURVEY

Hung-Min Sun et al. describe Text passwords are the most often used method of user authentication on websites due to their convenience and simplicity. However, passwords are easily stolen and compromised due to various risks and weaknesses. Firstly, people frequently use weak passwords and reuse them across several websites. Reusing passwords can lead to a domino effect, where an attacker can use one compromised password to obtain access to other websites. Second, inputting credentials into untrustworthy computers exposes you to the potential of password theft. Passwords may be stolen using several methods, including phishing, keyloggers, and malware. Our article presents oPass, a user authentication mechanism that uses a user's smartphone and short messaging service to prevent password theft and reuse threats [1].

Priyanshu Gupta et al. suggest This research investigates how print attacks and contact lenses might spoof iris recognition performance, increasing the danger of incorrect identification. The ID iris spoofing database, which has over 4800 iris photographs of more than 100 people with differences induced by contact lenses, sensors, and print assaults, is described. Finally, the article indicates that cost- effective descriptor techniques can aid in the prevention of spoofing assaults [2].

J. Daugman et al. discussed four developments in iris recognition: disciplined approaches for modeling iris borders, Fourier-based methods for addressing off-axis gazing, statistical inference methods for removing eyelashes, and an investigation of score normalization strategies. The statistical results are based on 200 billion iris cross-comparisons collected from 632,500 irises in the UAE database to investigate normalization concerns [3].

Humayan Kabir Rana et al. described Biometric recognition as identifying people based on their unique characteristics or behaviors. Iris is a popular choice because of its stability and complexity. We present a strategy that uses PCA on DWT to extract iris characteristics while reducing runtime. DWT divides an iris picture into four sub-bands, whereas PCA selects the best characteristics from one sub-band. This approach is quite effective for iris classification [4].

Osuma Ouda et al. suggested Biometric template protection solutions are intended to solve security and privacy concerns in biometric-based authentication systems. However, subsequent research has found that the resilience of these strategies against reversibility and linkability attacks is overstated. Negative iris recognition is an iris template protection system that uses negative databases. We provide a thorough security study of this technique, demonstrating that the original iris-code bits can be retrieved using a single protected template. Furthermore, the system is subject to assaults using record multiplicity and lacks unlinkability. Our experiments show that the negative iris recognition technique is vulnerable to reversibility, linkability, and record multiplicity assaults [5].

Arora S et al. described the susceptibility of iris recognition systems to presentation attacks, namely print assaults. The study demonstrates that hackers may trick these systems by utilizing print assault pictures, contact lenses, or a mix of the two. To overcome this issue, the research recommends the usage of deep Convolutional Neural Networks, which can identify such spoofing tactics with high accuracy [6].

Mohammed NF et al. explain This research introduces a new iris identification method that uses the lifting wavelet transform to detect persons from low-quality iris photos. The iris region is confined and transformed into a rectangular rectangle. To generate the iris code, the new technique extracts a collection of features from the lifting wavelet subbands and quantizes two subbands (LH3 and HL3) as well as the average values for the two high-pass filter regions (HH1, HH2). Test findings on the CASIA V1 dataset demonstrate high identification and verification rates[7].

M. Jenadeleh et al. suggested Image quality is critical to the functioning of biometric devices. Obtaining high-quality iris pictures in visible light is a challenge for iris identification systems. Poor-quality iris photos lead to higher false rejection rates and worse system performance. We propose a quick measure for predicting iris image quality using statistical aspects of local image intensities. The rejection of poor-quality iris photos increased the iris recognition system's performance[8].

E. Jalilian et al. described CNNs are effective at tackling artificial vision difficulties such as picture segmentation, but they require a large amount of labeled data, which is both expensive and time-consuming. This work presents two pixel-level domain adaption strategies for training a CNN- based iris segmentation model capable of transferring source database domains to target databases. This eliminates the necessity for target-labeled information. We also show that a particular CNN can be trained for iris segmentation with extremely little training data while achieving optimum segmentation scores [9].

H. Hofbauer et al. suggested CNN-based iris segmentation outperforms previous approaches. However, to use them successfully in a traditional biometric recognition system, the parameterization problem must be solved. We offer a method for parameterizing CNN-based segmentation, allowing it to function as a full segmentation step or noise mask in an iris biometric system. We shall assess both approaches to determine their efficacy [10].

K. Roy et al. explain A support vector machine-based iris recognition system for human identification. The iris/pupil border is determined using Canny's edge detection and the Hough transform, while eyelash recognition is accomplished using a simple thresholding approach. The Gabor wavelet approach is used to extract deterministic characteristics from the altered iris of a person in the form of a template. The collected iris characteristics are placed into a support vector machine (SVM) for classification purposes. Our results show that SVM outperforms an artificial neural network- based classifier [11].

S. Minaee et al. described Iris recognition as a critical topic in security. In this study, we present a deep learning framework for iris recognition based on residual convolutional neural networks. Our model generated encouraging results and outperformed earlier techniques. We also presented a visualization tool for identifying key spots in iris pictures. Our architecture may be applied to various biometric recognition jobs, resulting in a more scalable and accurate solution [12].

S. Arora et al. present a computer vision-based biometric system that employs deep learning to recognize and validate iris pictures. The system extracts information from iris pictures and classifies them into 224 classes using a mix of Convolutional Neural Networks and Softmax Classifiers. Our findings indicate that the choice of hyperparameters and optimizers influences the system's efficiency. However, our technique beats previous ones by obtaining accuracy [13].

III. METHODOLOGY

Biometric systems are an extremely safe and dependable technique of confirming and protecting systems. In recent years, multimodal biometric approaches have gained popularity in real-world applications. This is because unimodal systems lack adequate validation methods. To solve this issue, deep learning methods like the Convolution Neural Network (CNN) have been used to develop multimodal biometric systems. Biometric systems are constantly evolving and provide promising solutions for identifying and authenticating persons. Peer technologies are also being used to overcome any potential validation flaws with the biometric system. This section of the investigation will go over several analytical methodologies. For each study project, a specific strategy is used to get the results that will be presented in this chapter. Despite being one of the most recent and safest validation methods in history, there are a few restrictions to consider when processing the full work. Some systems and software need to be improved to deliver better services to clients. As a result, the study's limitations have been partially attached. The study will be conducted based on the software and technologies utilized to construct the full software activity. Utilizing fingerprint and iris recognition technology is a key element that demands a reliable user interface to guarantee high-quality validation and verification procedures. The

software development procedure will adhere to the wireless communication model, and deep learning algorithms will be employed. Incorporating the convolution neural network (CNN) architecture will transform the biometric system, making it a fundamental part of the methodology section that describes the implementation of the research endeavor. The primary approaches used for designing the validation system will be detailed below. Different methodologies, such as "Inductive" and "Deductive" procedures, can be used to fulfill any specific research project. The above-mentioned study analyzes using a deductive strategy. This implies that the research topics are selected and investigated methodically utilizing the queries and software that will provide the findings. The deductive technique is a dependable and effective way for obtaining appropriate results.The methodology describes the steps that a given research project takes. There are primarily two types of approaches: "qualitative" and "quantitative" procedures. Because this investigation activity is tied to software and technology, a unique approach is used on purpose. The validation system will be built on the "convolution neural network (CNN)" architecture and models. The procedures will be provided in a more understandable format for the audience.Furthermore, the installation of wireless communication models, among other things, would be presented to acquire an adequate validation system. Data gathering is one of the most important components of any research project. Data gathering is critical since the majorityof research is conducted via primary or secondary analysis. The analysis is completed using the collected data. Because this is a software-based research project, the data generated by the program will be used throughout the analytical process. Since the majority of the job is focused on correct validation and decision-making criteria, acquiring information about these scenarios was critical. Furthermore, the linked validation system setup aspects, such as image processing and "convolution neural network (CNN)" models, would be necessary for data collection and storage. However, there are certain limits to this specific research that will be addressed with future upgrades. It emphasizes critical areas such as the design and methodologies of convolution neural networks (CNN), image processing and extraction, decision-making, and so on.

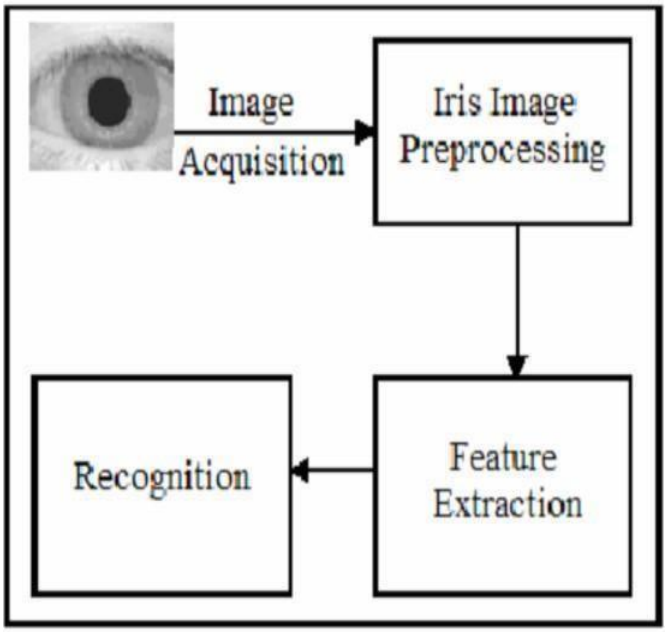


FIG 1: Iris Recognition system methodology

IV. RESULTS AND DISCUSSION.

A. *The Determination of the information using the CASIA IRIS dataset :*

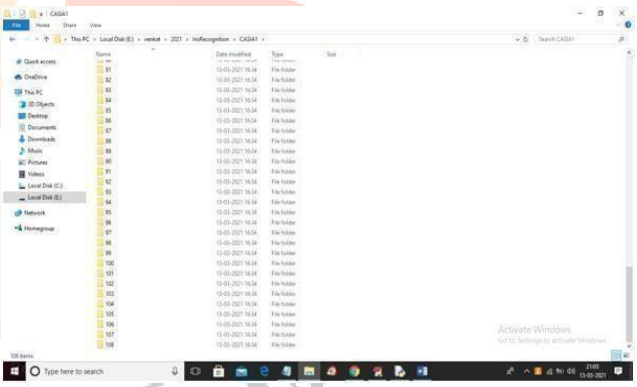


FIG 2. CASIA IRIS Dataset

The aforementioned statistic was included in the dataset along with the user IDs of 108 individuals. It was primarily done to commemorate everyone associated with Iris. The "CASIA iris dataset" was primarily responsible for the implementation. The collection must include specific photos of 108 individuals in the location. Regarding this particular dataset, the system user can attend adequate training on the "convolutional neural network (CNN)" model for all members of the organization. The system user may anticipate and recognize all individuals using this "convolutional neural network (CNN)" model.

B. *Generating the Convolution Neural Network Model from the provided dataset*

The figure below primarily depicts the loading procedure of the corresponding dataset. The "convolutional neural model (CNN)" may simply build an iris picture from this specific dataset.

FIG 3. Generating of Convolution Neural Network (CNN) Model

C. Generation of LOSS Graph and Accuracy Check

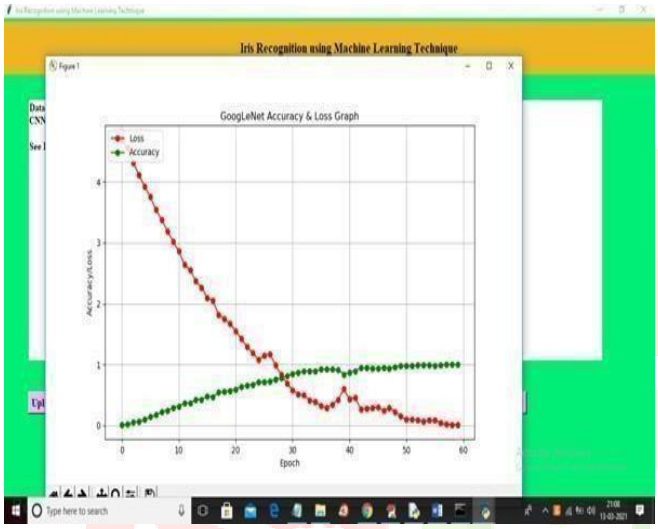
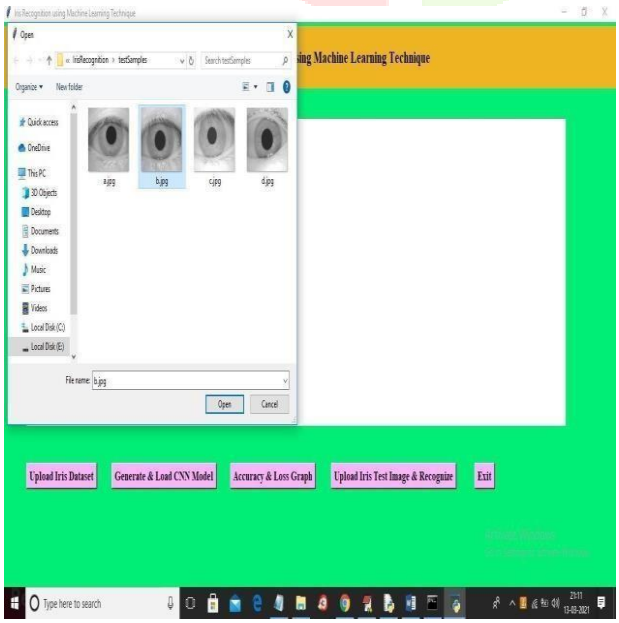
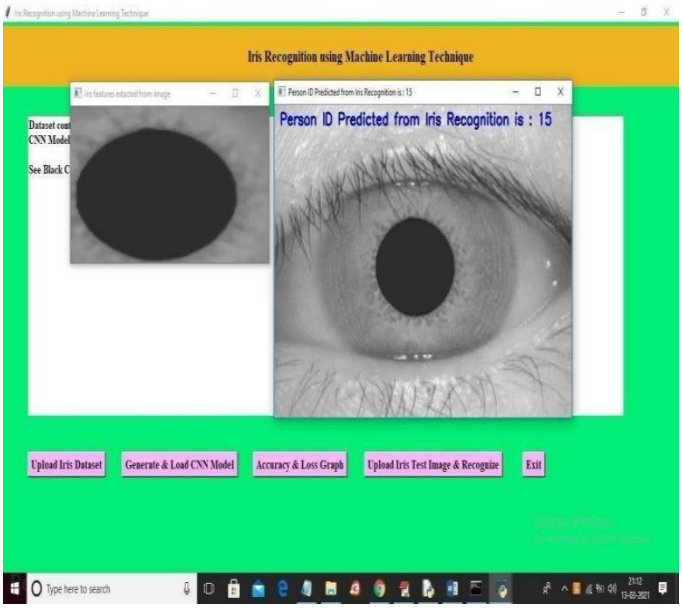


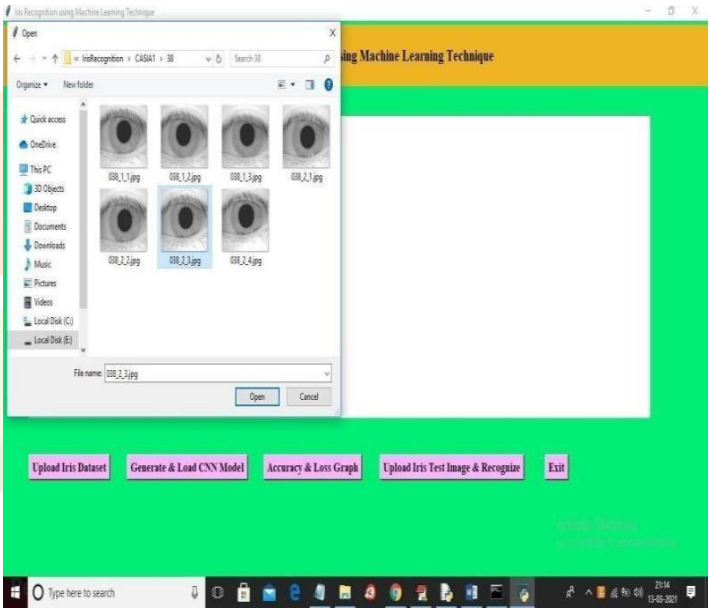
FIG 4. Generation of LOSS graph and Accuracy check



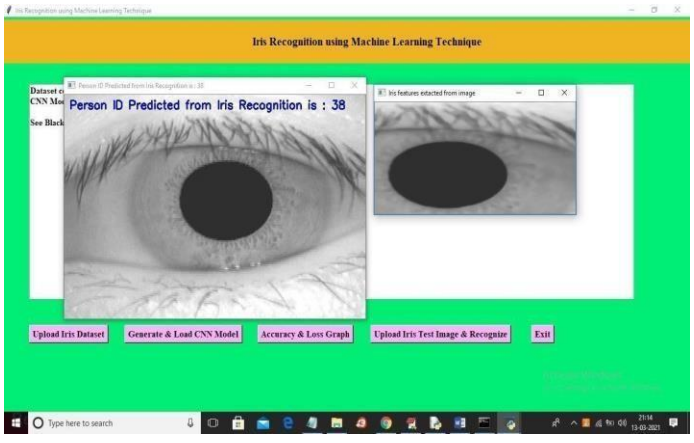
(a)



(b)



(c)



(d)

FIG 5. Recognition Process

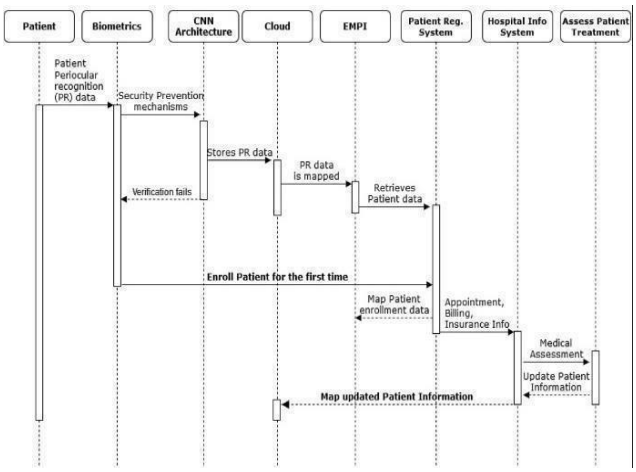


FIG 6. Sequence Diagram

The image above displays an accurate loss graph from the given dataset and evaluates the accuracy level using the "convolutional neural model (CNN)". In this scenario, the dotted red line represents the loss value and factors of the "convolutional neural model (CNN)". The graph shows that the iteration loss in the initial stages is higher than 3.9%. However, as the epoch value increases, the loss value decreases to zero. The green line in the illustrationrepresents the correct accuracy value. The X-axis of the graph displays the epoch value while the Y-axis displays the accuracy value and the corresponding loss values. With these parameters, the system user can easily determine the correct identification from the iris image using the "convolutional neural network (CNN)" model. The model's answers, in general, are accurate for human identification.

V. CONCLUSION

It focuses mostly on the expected outcomes, findings, and analysis, which will be contrasted with the actual results.It contrasts the actual and projected results and examines the limits encountered while doing the research. It also describes how this study effort might be expanded in the future. To assess the impact of the research and software study, it is critical to understand the study's underlying objectives and goals. In software development, greater emphasis is placed on ensuring that the intended results are achieved by considering the consequences of varioussoftware and technology options.

The research has primarily concentrated on creating an iris recognition system that utilizes the "convolution neural networking (CNN)" technique to achieve optimal security goals.To capture all of the needs, the entire technology should be upgraded. The multimodal biometric process is extremely difficult to develop and implement, and the procedure has had a significant impact on overall working performance. In terms of literature evaluation, the described models and theories may accurately and concisely represent all of the system's requirements and relevance. The right useof various types of technologies may be done to create accurate software that is extremely successful for allaudiences.

We suggest that you use a text box to insert a graphic (which is ideally a 300 dpi TIFF or EPS file, with all fonts embedded) because, in an MSW document, this method is somewhat more stable than directly inserting a picture.

To have non-visible rules on your frame, use the MSWord “Format” pull-down menu, select Text Box > Colors and Lines to choose No Fill and No Line.

References

[1] Sun H-M, Chen Y-H, Lin Y-H (2012) oPass: a user authentication protocol resistant to password stealing and password reuse attacks. IEEE Trans Inf Forensics Secur7(2):651–663.

[2] Gupta P, Behera S, Vatsa M, Singh R (2014) On iris spoofng using print attack. In: IEEE 2014 22nd international conference on pattern recognition, Stockholm, Sweden, 24– 28 August 2014. https://doi.org/10.1109/ICPR.2014.296.

[3] iris recognition works. IEEE Trans Circuits Syst Video Technol 14(1):21–30.

[4] Rana HK, Azam MS, Akhtar MR, Qunin JMW, Moni MA (2019) A fast iris recognition system through optimum feature extraction. PeerJ Comput Sci 5:184.

[5] aoui S, Tsumura N (2020) Security evaluation of negative iris recognition. IEICE Trans Inf Syst 103(5):1144–1152.

[6] Arora S, Bhatia MPS (2020) Presentation attack detection for iris recognition using deep learning. Int J Syst Assur Eng Manag. https://doi.org/10.1007/s13198-020- 00948-1.

[7] Mohammed NF, Ali SA, Jawad MJ (2020) Iris recognition system based on lifting wavelet. In: Mallick P, Balas V, Bhoi A, Chae GS (eds) Cognitive informatics and soft computing. Springer Advances in Intelligent Systems and Computing, vol 1040, pp. 245–254. Springer, Berlin.

[8] Jenadeleh M, Pedersen M, Saupe D (2020) Blind quality assessment of iris images acquired in visible light for biometric recognition. Sen.

[9] .Jalilian E, Uhl A, Kwitt R (2017) Domain adaptation forCNN-based iris segmentation. In: IEEE proceedings of 2017 IEEE International Conference of the Biometrics Special Interest Group (BIOSIG), Darmstadt, Germany, September 20–22, 2017. https://doi.org/10.23919/BIOSIG.2017.8053502.

[10] Hofbauer H, Jalilian E, Uhl A (2019) Exploiting superior CNN-based iris segmentation for better recognition accuracy. Pattern Recognit Lett 120:17–23.

[11] Roy K, Bhattacharya P (2006) Iris recognition with support vector machines. In: Zhang D, Jain A (eds) Proceeding advances in biometrics, international conference, ICB 2006, Hong Kong, China, January 5–7, 2006, Springer lecture notes in computer science, vol 3832, pp 486–492. [12] Minaee S, Abdolrashidi A (2019) DeepIris: iris recognition using a deep learning approach. arXiv:1907.09380 [cs.CV].

[13] Arora S, Bhatia M (2018) A computer vision system for iris recognition based on deep learning. In: IEEE proceedings of 2018 IEEE 8th International Advance Computing Conference (ACD), Greater Noida, India, December 14–15, 2018. https://doi.org/10.1109/IADCC.2018.8692114.