Adabala Devi Mangatayar *et. al.,* / International Journal of Engineering & Science Research

IMAGE VALIDATION SYSTEM BASED ON FINGERPRINT-IRIS RECOGNITION BY CONVOLUTIONAL NEURAL NETWORK (CNN) MODEL

Adabala Devi Mangatayar
Pg Scholar, Department Of Mca, Dnr College, Bhimavaram, Andhra Pradesh.
K.Rambabu
(Assistant Professor), Master of Computer Applications, DNR college, Bhimavaram, Andhra Pradesh.

***Abstract** One of the main results of the validation system is based on the fingerprint-based iris recognition system and respective technology. The entire biometric process is very much authentic and unique than the other types of recognition system and validation process. This has provided innovative ideas in the daily lives of human beings. The multimodal biometric process has generally applied various types of applications for properly dealing with the appropriate and most significant limitations of the "unimodal biometric system". The entire process has been generally included with the proper sensitivity of noise, the population coverage areas, variability cases of the inter class and intra class issues, vulnerability cases of possible hacking and the non universality criteria. The entire research paper has been mainly focused on the deep learning oriented machine learning system. The fingerprint based iris recognition system to do the proper validation of human beings has been mainly done by convolutional neural network (CNN) technique. In the existing data validation process, the iris recognition system has been mainly done with respect to the "high security protection system with actual fingerprints". The entire paper has been briefly elaborated on the best uniqueness, reliability process and the proper "validity of the iris biometric validation system" for the actual purpose of the person identification).*

I. INTRODUCTION

1.1. Introduction

The biometric process has been mainly used to recognize individual types of physical aspects and features. For this purpose, a tremendous amount of acknowledgement technologies have been generally provided with the actual fingerprint, iris procedures and voice acknowledgement. The biometric mainly deals with the proper technical and technological fields for the body controls and body dimensions. The authentication system is based on the appropriate biometric security system that has increased the actual importance within all countries. The used system has been shown the proper valid and best impressive performance based on all these procedures and aspects. For this purpose, the fingerprint is the only procedure for providing the proper security techniques to provide the true uniqueness and the strong privacy properties of the entire system. The exceptional fingerprint assurance or the proper kind of imprint approval has been mainly insinuating the automated methods and procedures to ensure similarity between the two people fingerprints. The entire chapter has been generally provided with the actual purpose of the fundamental research that is overall dependent on the research objectives and respective research questions. In this chapter, the research framework of the entire study has also been provided. The fundamental research has described all the factors that are responsible for this recognition process.

1.2. Background of the study

In this particular recognition system, the outer and the inner boundaries of the iris area have been mainly detected by the different types of integro differential operators. The real success of the biometric system and the biometric process is totally based on the proper classification and proposed recognition system. The entire process mainly depends on the proper robustness and efficiency of the "feature extraction and classification stages". In this case, most choices of the fingerprint game-planning images have been proposed for the various types of bunch fingerprints in four to five classes between the four types. Among all these four aspects, the primary vital priorities and the initial step are the AFIS. The particular types of the biometric process use the unique certified cations for gathering informative data from the various estimations. This kind of data is very much necessary and essential for the various cases of individual priorities. It still remains important and essential for this recognition system.

The Iris recognition of the entire development of enthusiasm has been found within the sound stage of biometrics for human ID. For the proper discussion of the entire recognition system, there are used the "Bayesian graphical models" match the respective images of such types of tests. Among all the classifiers, "convolution neural networks" have been mainly considered the most robust and straightforward aspects to overcome all the obstacles within this system. This entire research study has been proposed as the "integrated approach to the proper iris recognition validation system" for the retention process of a human fingerprint. *[Referred to Appendix 1]*

1.3. Problem statement

There are various types of problems and significant issues that have been mainly faced by the biometric security system. The central and foremost issue is the **biometric authentication process**, and technologies have been mainly raised in the various types of privacy concerns and security concerns (Hamd & Ahmed, 2018). During the processing time of the biometric data, there is no other option to undo or retrieve the respective information from the damage. For the case of the compromised passwords, anyone can modify it with fingerprint, iris scanner and the ear image effects. So for all these aspects, the simple working performance of the biometrics remains within the security risks and privacy risks. There are various types of problems that have been shown in the different slides of the **iris recognition system**, such as the sensor module, preprocessor module and feature extraction process. All these security and privacy issues can be adequately solved by the appropriate types of technologies and modern and advanced techniques. The security process should also be secured with the help of a strong password and robust system process.
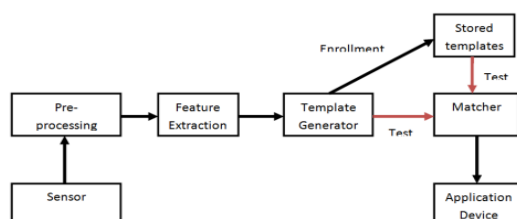

Figure 1: various stages of fingerprint iris recognition process
(Source: Adamu, 2019)

Objectives

With respect to the presented research aims, there have been mainly proposed the correct numbers of research objectives. All these research objectives have been mainly presented as the best outline of the fundamental research. All the research objectives are presented below.

- To represent the proper enhancement of the entire validation system with respect to the appropriate security tools.
- To elaborate the actual uniqueness, good reliability and the appropriate validity of the "iris biometric validation system" that is mainly used for the identification of the human ID.
- To enhance the various processes with the excess security aspects and factors for strengthening the private networks within the system.
- To analyze all types of validating security processes from the various research notes to highlight the most necessary and sufficient categories.

II. LITERATURE SURVEY

The literature review chapter has been mainly provided with a detailed description of the various problems and different types of recognition aspects that has been mainly associated with the entire area of the research study. The fundamental research has been conducted with the help of the different types of research notes of different authors and researchers. The entire process is also evaluated by the brief description of the research from the different online articles, journals and various websites. The fundamental research has been conducted with respect to the in-depth analysis process of the entire validation based recognition system. Including all of these, this particular chapter has also demonstrated the particular models and theories of the proposed topic for evaluating the entire description process. In this part, there are also described the literature gaps that are generally

missing in the existing research notes of various authors.

2.2. Empirical Study

According to the author Alrahawe (2018), a biometric system is one of the safest ways to work with the digital world. Since biometrics such as fingerprints, face, and iris recognition are different for different persons, these are safer compared to any other processes to secure confidential data (Alrahawe, 2018). However, in the olden days, there was a lack of technology for which there was less security provided for any confidential information. With the advancement in technology in recent times, biometric security has been an integral part of any system. Moreover, the author states that these kinds of processes for security in digitalization have become error-free, for which this system is getting implemented in the latest systems (Singh & Kant, 2021). Due to minor errors in the system, this is pretty reliable for security purposes. The biometric system has used various types of recognition processes, among which it also uses the finger-knuckle recognition system.
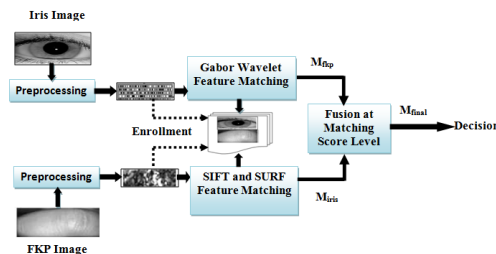

Figure 4: Architecture for fingerprint recognition method
(Source: Alrahawe, 2018)

The knuckle surfaces provide a curved surface to produce the reflection. This is one of the modalities for biometric recognition (Kaur & Garg, 2018). When compared between the biometric security processes, iris recognition is one of the most robust methods since the iris structures vary from person to person. Even an imposter will find it challenging to trick an "iris biometric system". *[Referred to Appendix 2]*
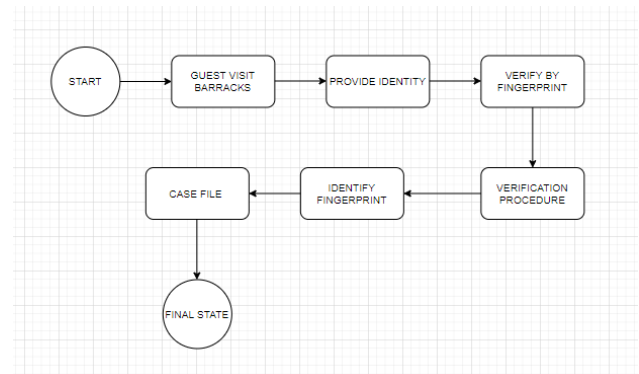

Figure 5: Activity Diagram
(Source: Draw.io)

According to the author Elhoseny (2018), there was a unimodal system for identification and verification processes. However, through the unimodal system, the accuracy was not fully maintained since it failed to meet the proper decision-making criteria. It was found that there was a significant amount of reduction in accuracy while using the unimodal system for verification (Elhoseny, 2018). Thus the multimodal system was introduced. As the multimodal system uses fusion technology, the overall accuracy from the verification was achieved. While comparing the different sorts of modalities, fingerprint and iris always have the highest distinctiveness and permanence. Moreover, they are cost-efficient too, and the speed is relatively higher when compared to any other modalities. While the unimodal system was not totally involved in the decision making concept, the multimodal system covers four different tasks such as acquisition, extracting the feature from the modalities, matching with the actual one and then providing the decisions (La, 2021). The unimodal systems are also used in many cases where less security can be helpful. But for high-security purposes and the sectors that deal with massive amounts of confidential data require multimodal systems.
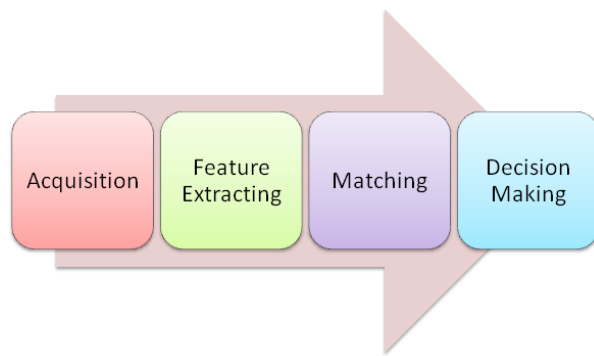
Figure 6: Tasks of Biometric Systems
(Source: Self-created)

According to the author Adamu (2019), the biometric system has been dealt with the particular types of the technical and technological field and department for controlling the entire body dimensioning process. The process has also been stated to have different types of metrics that are directly related to the proper characteristics of the human being (Adamu, 2019). Biometric verification has mainly proposed various types of processors as the accurate method for accessing the complete human body control and human process control. The system has generally dealt with the proper identification and measurement of the individual's process for correctly clustering the various techniques under proper investigation (Regouid *et al.*, 2019). The biometric process is the most unique and contains valuable features and factors to describe all the entities. This particular technology is an excellent addition to the best innovation, and it is very much helpful and necessary for the higher quality business cases that are mainly faced by different types of massive data violation processes. Biometric recognition is a valid and reliable method to verify the real personality of the living person that is totally dependent on physiological qualities and social qualities (Naika, 2018). All these kinds of assumptions are basically constant and irreversible processes without noticeable stress (academia.edu, 2019).

III. PROPOSED METHOD

3.1. Introduction

Biometrics systems have been one of the safest ways to secure and verify any system. In recent times, multimodal biometric techniques are widely implemented in several real-world applications. Due to the lack of validation processes in the unimodal systems, the multimodal biometric system was introduced with the help of deep learning algorithms. The "Convolution Neural Network (CNN)" is nothing but an algorithm that uses deep learning architecture. Validation through biometric systems is evolving day by day and has become a much promising technology that can be used for the identification and authentication of any person. Peer technologies are recently used in the system for solving the validation difficulties through the biometric system. In this part of the research, different analyzing methods will be discussed. For every research work, there is a particular approach which is obtained to reach the final outcomes that will be accomplished in this chapter. Being one of the latest and safest technologies in the history of validation, there are several limitations that are faced while processing the entire task. Some of the systems and software are required to improve so that better services are provided to the clients. So the limitations of the research have also been attached in part. Here the analysis will be done on the basis of the software and technologies that have been used for developing the entire software work. The fingerprint and iris recognition system requires an exemplary user interface as the validation and verification process is given significant priority. Through the wireless communication model, the software work will be done. Deep learning algorithms are another vital part that would be used for this purpose. Through the implementation of the "convolution neural network (CNN)" architecture, reshaping the biometric system would be done.

3.2. Method Outline

This particular research work follows a "Systematic Approach" that helps to reach the actual targets. Though the preliminary stage of the research is more focused on determining the strategies and objectives that will be considered for obtaining the final goals, the central section consists of the software work that involves the "convolution neural network (CNN)" architectural model and RF wireless communication model (Salve *et al.,* 2019). This part of the study helps to outline the proper approaches that would include the software analysis of the system. This paper has been dealt

with the fingerprint and iris recognition system strategies and the problems that are usually faced while implementing the system. Therefore, relevant software and data will be analyzed based on the fingerprint and iris recognition system, and the outcomes will be explained.

In order to achieve the proper validation system through fingerprint and iris recognition system, it is essential to implement the latest and safest technologies in the process. Since the validation system would secure several confidential data, there is a need for an appropriate validation system that will check the authorization process and make decisions accordingly. This is why the research method is a significant part of the chapter that would outline the necessary software for the said venture. In this research, the deep learning algorithm has been an integral part of the overall system. The major three stages are followed for the validation system using fingerprints, such as the preprocessing of the image, extracting the features from the image through the "convolution neural network (CNN)" model and using the classifier (Yadav *et al.,* 2017). This technology provides the designers to work on the system and to decrease the delay that is usually faced while validating. Data from each of the software would be individually collected. Latest technologies such as deep learning algorithms, machine learning concepts and artificial intelligence are viewed as essential fields for developing the validation system (jatit.org, 2017). *[Referred to Appendix 8]*

3.3 Research Approach

The approach is considered as the essential aspect of the methodology chapter that plans the conduction of the research work. The main methods that are generally implemented for developing the validation system would be described here. For any particular research work to complete, different approaches can be followed, such as "Inductive" and "Deductive" approaches (Sameh *et al.,* 2020). However, this particular study follows the deductive approach since the analysis is done on the queries and software from which the outcomes will be achieved. The deductive approach is nothing but the systematic approach where the first priority is given to the research questions based on which the analysis is done, which leads to

gaining appropriate outcomes. The required software would be analyzed using "convolutional neural network (CNN)" architectural models and deep learning techniques. The research work will be carried out on the basis of knowledge on the current validation systems that includes fingerprint and iris recognition.

3.4 Research Design

The research design depicts the processes that a particular research work undergoes. There are mainly two kinds of approaches, such as "Qualitative" and "Quantitative" methodologies. Since this exploration work is a kind of software and technology-related, a different approach is followed purposely (Sharma *et al.,* 2019). For implementing the validation system using the "convolution neural network (CNN)" architecture and models, the software work would be done. The design of the exploration work would be done in a way that it becomes easier for the audience to understand the processes. Moreover, the implementation of wireless communication models, etc., would be demonstrated for obtaining the appropriate validation system.
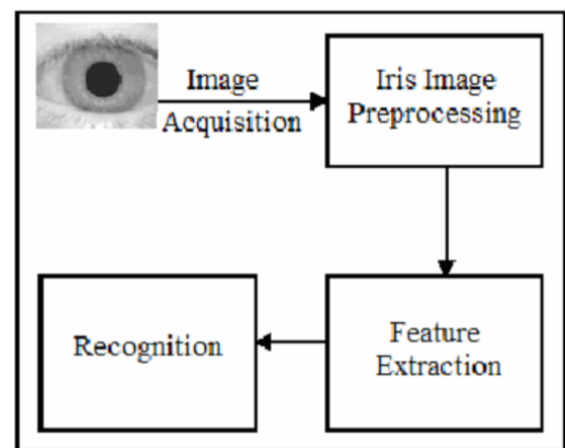

Figure 22: Iris Recognition system methodology

IV.   RESULT

4.4. Generating the Convolutional Neural Network (CNN) Model from the provided dataset
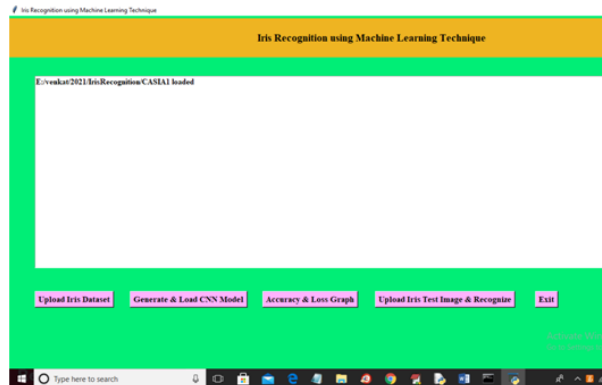

Figure 25: Screenshot of generation of the Convolutional Neural Network (CNN) model
(Source: Provided)

The above figure has been mainly described the loading process of the respective dataset. From this particular dataset the iris image can be easily generated by the "convolutional neural model (CNN)".

4.5. Code for checking the accuracy

The entire code has described the entire process for detecting all the informative data within the "convolutional neural model (CNN)" model. With the help of the process the actual values have been properly generated on the screen in the actual form of graph. In the screen the actual accuracy vs. loss graph has been generated. The predictable value of the curve and the generated accuracy value are 100% correct.

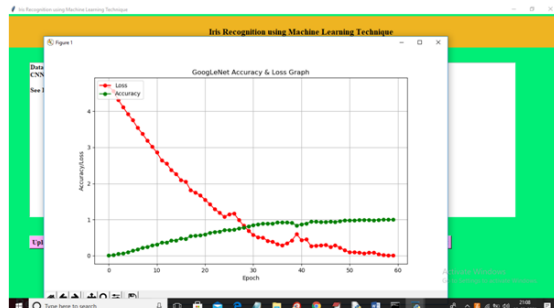## 4.6. Generation of the LOSS Graph and accuracy check

Figure 26: Generation of the LOSS Graph and accuracy check
(Source: Provided)

All the under attached image have been described the actual process of the iris recognition system of all the 108 peoples of the organization. The screenshots are attached below.
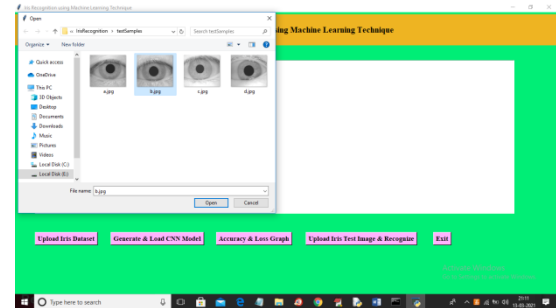

Figure 27: Recognition process
(Source: Provided)

The above figure has been provided the accurate loss graph from the provided dataset and the check the accuracy level through the "convolutional neural model (CNN)". In this case the dotted red line has been represented as the loss value and factors of "convolutional neural model (CNN)". And from the graph it has been properly proved that the iteration loss in the initial cases is greater than 3.9%. But with respect to the increased value of epoch, the loss value has been reduced to the value of zero. In the figure, the green line has been represented with the proper value of accuracy. In the graph, the X-axis has been shown the actual value of epoch and the Y-axis has been shown the proper value of accuracy and respective loss values. With the help of all these values, the system user can be easily able to easily recognize the proper ID from the iris picture through the "convolutional neural model (CNN)" model. The results that have been generally out from the model are totally correct for recognition of human identification.

Adabala Devi Mangatayar *et. al.,* / **International Journal of Engineering & Science Research**
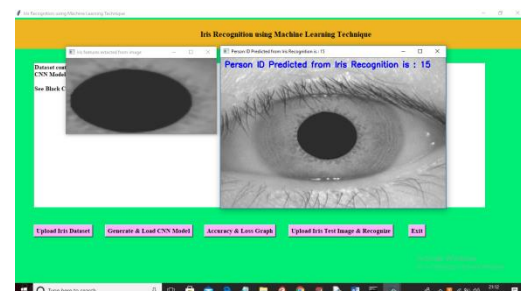
Figure 28: Recognition process
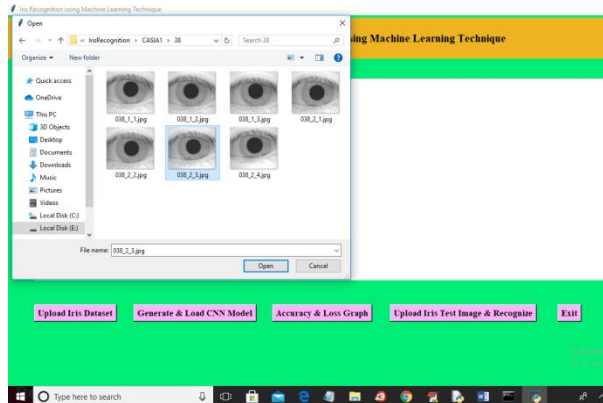(Source: Provided)

Figure 29: Recognition process
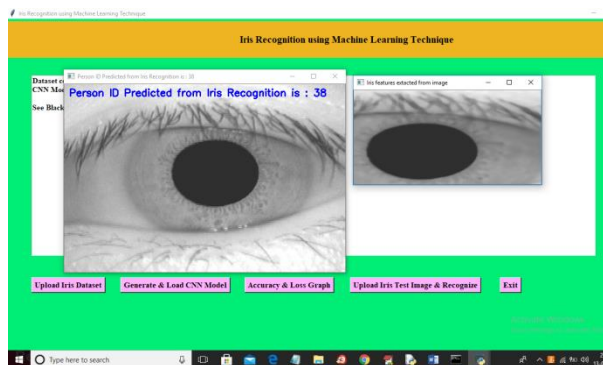(Source: Provided)

Figure 30: Accurate recognition image
(Source: Provided)

With respect to all these screenshots the possible way for getting the accurate iris recognition process of employee can be easily get.
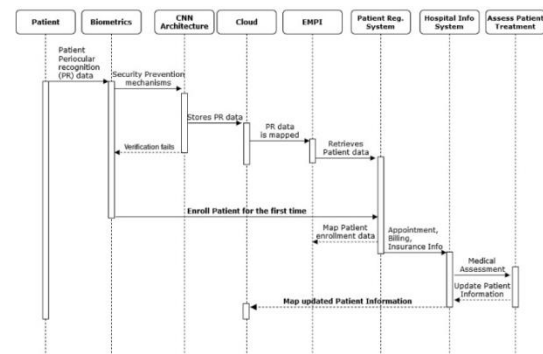

Figure 31: Sequence Diagram
(Source: ars.els-cdn.com)

V. CONCLUSION

This is the final chapter in the assignment that discusses the entire research work and also analyses the software work that has been conducted for obtaining the expected outcomes. This chapter mainly focuses on the expected outcomes, findings and analysis, which will be compared with the actual outcomes. This chapter compares both the actual and expected outcomes. This chapter also discusses the limitations that were faced while conducting the research, as well as. It also provides how this research work can be extended in future. In order to determine the effects of the research and the software study, it is essential to know the fundamental objectives and aims of the study. For conducting the software work, more emphasis has been given on how the implications of different kinds of software and technology will be carried out so that the actual results are achieved. In this particular chapter, the connections between the prime objectives and the results have been built. Future recommendations on the software work will be made so that this research work can be expanded further.

.**REFERENCES**

1. Adamu, A., 2019. Attendance management system using fingerprint and iris biometric. *FUDMA Journal of Sciences (FJS)*, *3*(4), pp.427-433.
2. Akbar, M.J., 2019. A Overview of Spoof Speech Detection for Automatic Speaker Verification.
3. Albakri, G. and Alghowinem, S., 2019. The effectiveness of depth data in liveness face authentication using 3D sensor cameras. *Sensors*, *19*(8), p.1928.
4. Alrahawe, E. A., Humbe, V. T., & Shinde, G. N. An Analysis on Biometric TraitRecognition.

5. Arora, S. and Bhatia, M.P.S., 2018, July. A robust approach for gender recognition using deep learning. In *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)* (pp. 1-6). IEEE.

6. Arteaga Falconi, J.S., 2020. *Towards an Accurate ECG Biometric Authentication System with Low Acquisition Time* (Doctoral dissertation, Université d'Ottawa/University of Ottawa).

7. Ashraf, A. and Vats, I., The Survey of Architecture of Multi-Modal (Fingerprint and Iris Recognition) Biometric Authentication System.

8. Attia, A., Akhtar, Z., Chalabi, N.E., Maza, S. and Chahir, Y., 2020. Deep rule-based classifier for finger knuckle pattern recognition system. *Evolving Systems*, pp.1-15.

9. Cardia Neto, J.B., 2020. 3D face recognition with descriptor images and shallow convolutional neural networks.

10. Cortès Sebastià, G., 2018. *End-to-End photoplethysmography-based biometric authentication system by using deep neural networks* (Bachelor's thesis, Universitat Politècnica de Catalunya).

11. Derman, E., Galdi, C. and Dugelay, J.L., 2017, April. Integrating facial makeup detection into multimodal biometric user verification system. In *2017 5th International Workshop on Biometrics and Forensics (IWBF)* (pp. 1-6). IEEE.

12. Elhoseny, M., Elkhateb, A., Sahlol, A. and Hassanien, A.E., 2018. Multimodal biometric personal identification and verification. In *Advances in Soft Computing and Machine Learning in Image Processing* (pp. 249-276). Springer, Cham.

13. Folorunso, C.O., Asaolu, O.S. and Popoola, O.P., 2019. A Review of Voice-Base Person Identification: State-of-the-Art. *Covenant Journal of Engineering Technology*, *3*(1).

14. Garg, S.N., Vig, R. and Gupta, S., 2017. A Critical Study and Comparative Analysis of Multibiometric Systems using Iris and Fingerprints. *International Journal of Computer Science and Information Security*, *15*(1), p.549.

15. Gogate, G. and Azad, V., Iris Biometric Recognition for Person Identification in Security Society System