iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** VI **Month of publication:** June 2023

DOI: https://doi.org/10.22214/ijraset.2023.53443

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VI Jun 2023- Available at www.ijraset.com

Fusion Biometric Recognition Using CNN and LSTM Algorithms

Mrs. V. Bhuvaneshwari[1], S. Sanyogita[2], M. Shalini[3], S. Snega[4], V. Veena[5]
[1]*M. Tech, Assistant Professor/CSE*
[2, 3, 4, 5]*Final Year /CSE*
Achariya College of Engineering Technology, Puducherry

Abstract: ***The automatic identification of people using their unique physical characteristics for security purposes is known as biometrics. Biometric authentication has a significant difficulty that calls for the development of more efficient methods in order to confirm the actual presence of a true legitimate trait as opposed to a fake self-manufactured synthetic or reconstructed sample. Recent developments in machine learning, computer vision, and pattern recognition have accelerated the development of the biometric recognition technology. The suggested approach intends to strengthen the security of biometric recognition frameworks by introducing two authentication. Each modality faces a unique set of difficulties. When practical, adults were used to evaluate the performance of technology and software created for infants. The type of biometric recognition technology will determine how accurate it is the effectiveness of the algorithm, the biometric trait used, and the calibre of the data collected. The recommended method beats earlier state-of-the-art approaches, and extra biometric data reveals extremely valuable information that may be used to quite efficiently discriminate actual features from fake ones.***
Index Terms: Fingerprint, Iris, CNN, LSTM, Biometrics, Authentication

I. INTRODUCTION

The goal of biometric recognition is to identify people based on their distinctive physiological or behavioral traits. Biometric recognition is a significant area of research in the fields of computer vision and machine learning. Long short-term memory (LSTM) algorithms and convolutional neural networks (CNNs) have become effective tools for biometric recognition tasks in recent years. The accuracy, reliability, and effectiveness of biometric recognition systems have significantly increased as a result of the integration of these algorithms. This project's goal is to investigate the application of CNN and LSTM algorithms for biometric recognition and create an efficient system for identifying and confirming people using their biometric data. Deep learning techniques will be used to create the suggested system, using big biometric data sets, It is a method of identifying people that makes use of observable biological or behavioral traits, such as fingerprints, face features, iris, and retinal patterns. It provides a dependable and precise technique for confirming a person's identity and significantly improves the security of numerous applications. Biometric information about individuals should be safeguarded, and suitable security measures should be put in place to prevent its unauthorized use. Systems for adult biometric recognition have many applications, including fraud prevention, identification verification, and access control. However, privacy and security issues are also brought up by biometric identification. There are dangers associated with biometric data breaches and potential misuse.

II. RELATED WORKS

J. Daugman [1] presented the findings of 9.1 million comparisons between eye photos from trials conducted in Britain, the USA, Japan, and Korea, this study also discusses the iris recognition algorithms. Additionally, it is preferable for recognition judgements to be based on characteristics that have high complexity or randomness, stability over the course of the individual's life, and very little genetic penetrance (such that genetically identical or related individuals would still be identifiable). The pattern of the iris in either eye is a phenotypic face feature that possesses these characteristics. Iris patterns have an information density (population entropy) of roughly 3.4 bits per square millimeter when scanned at distances up to a meter, and their complexity ranges from about 266 independent degrees of freedom. The decision environment that results from using iris patterns to identify people has a decidability index of roughly d'= 11. H. Proença [2] suggests a method for iris recognition that makes use of structural pattern analysis techniques. In the suggested method, the iris region's features are extracted using Gabor filters and local binary patterns (LBP), and then the iris structure is analyzed using structural descriptors including junctions, cross points, and bifurcations. A support vector machine (SVM) classifier is then used to categorize the retrieved features.

The proposed method was tested against a collection of iris images and outperformed existing cutting-edge iris identification techniques in terms of recognition accuracy. The robustness of the suggested technique against noise and occlusions in the iris region is also covered in the research. The outcomes of this research show how well the suggested method for iris recognition works and illustrate the possibilities of structural pattern analysis.

An innovative method for iris detection on mobile devices is presented by Kang & Park [3]. The suggested method makes use of many iris photos taken using various mobile devices and fuses the results from each image's scoring. In order to choose the best quality iris photos and toss out the ones with low quality, the authors also present a quality assessment approach. A dataset of iris photos taken using mobile devices is used to test the proposed method, and the findings demonstrate that it works better than other cutting-edge iris identification techniques for mobile devices. A likelihood ratio-based method for combining biometric scores is suggested in the publication "Likelihood ratio-based biometric score fusion" by Nandakumar et al. [4]. The suggested method involves calculating a likelihood ratio for each biometric score, which contrasts the probability that the score belongs to the target user with the probability that it belongs to a fraudster. The final choice score is then calculated by weighting the likelihood ratios together. The authors also suggest a technique based on maximum likelihood estimation to calculate the weights of the sum rule. The results demonstrate that the suggested methodology outperforms other cutting-edge score fusion techniques. The proposed strategy is tested on a dataset comprising fingerprint and face recognition scores. Wiggin and Ericson [5] published a research titled "Contactless Fingerprint Technologies Assessment" that evaluates contactless fingerprint technologies for biometric identification. The research discusses the many market-available contactless fingerprint technologies, including optical, capacitive, and multispectral ones. The writers compare each technology's performance in terms of accuracy, speed, and dependability as well as its benefits and drawbacks. The research also contains a thorough investigation of the variables, such as skin quality and image quality, that affect the effectiveness of contactless fingerprint technology. The authors also cover the possible uses of contactless fingerprint technologies in access control, law enforcement, and border control. In-depth research on fingerprint image quality and its effects on biometric recognition systems is presented in the publication "Fingerprint Image Quality" by Tabassi et al. [6]. In addition to describing the numerous types of fingerprint image quality metrics that can be used to evaluate the quality of fingerprint images, the paper includes a thorough analysis of the several aspects that affect fingerprint image quality, including skin condition, and finger location. The authors also explore the connection between the effectiveness of biometric recognition systems and the quality of fingerprint photos, emphasizing the significance of high-quality fingerprint photographs for accurate and dependable recognition. The paper offers suggestions for the creation of new standards and guidelines for fingerprint image quality as well as an evaluation of the current.

A. Disadvantages

Cross-Matching mistakes: When a biometric system is used to identify a person, cross-matching mistakes are a possibility, particularly in large datasets. A mismatch between a person's biometric data and another person's record could result in identity theft and other possible security or legal problems.

III. EXISTING SYSTEM

The iris pattern, the outer ear shape, and the fingerprint were the three biometric modalities selected. Following an evaluation based on seven criteria for desirable biometric characteristics—universality, uniqueness, permanence, collectability, performance, acceptability, and resistance to circumvention—the modalities were selected. In this section, we review the three biometrics' applications for adults, the literature study into their usage for children, and the problems that still need to be resolved before these technologies may be adopted for the biometric identification of children.

A. IRIS

Iris recognition has performed incredibly well in adult individuals under varied imaging circumstances. It should be noted that these findings depend heavily on the subjects' participation, making it challenging to apply to young children. Researchers have begun looking into iris recognition for kids, though, thanks to recent developments in imaging technologies and iris recognition algorithms.

B. Fingerprint

The cut-off age is up for debate, however it is clear that scanners intended for adults do not function on minors. Uhl and Wild, a Dutch government research, and the US National Institute of Justice all set the age at which adult scanners are useless for children at 3 years, 4 years, and 6 years, respectively.

IV. PROPSED SYSTEM

An alternative strategy was selected after considering comparable work. The chosen methods are explained below, and further technical information is supplied in the subsections that follow. For adults, the iris module is well-established. However, the algorithms that are now in use in the literature were created for adults, and as a result, they make the implicit assumption that the subjects whose irises are being collected will cooperate fully. Young children, however, are unable to comprehend and adhere to directions. They are uncooperative and frequently fail to make the necessary direct eye contact with the acquisition camera. In order to successfully segment and capture the iris pattern from adults, modifications to the preprocessing algorithms had to be implemented while using the hardware and comparison algorithms that were already in place. The Fingerprint module is also well established for adults. However, there currently exists no commercially available solutions for children. At the time of embarking on the endeavor of collecting Fingerprints from adults, we determined that a higher resolution was required, compared to existing devices which were detailed in the literature. Additionally, all reported devices were contact-based. We decided on a contact-less approach, to overcome the challenges.

A. Advantages

Enhanced Security: Since biometric traits are exclusive to each person, they are challenging to copy or fake. When compared to more conventional security measures like passwords or ID cards, which can be misplaced, stolen, or shared, biometric recognition systems offer a better level of protection.

V. ARCHITECTURE

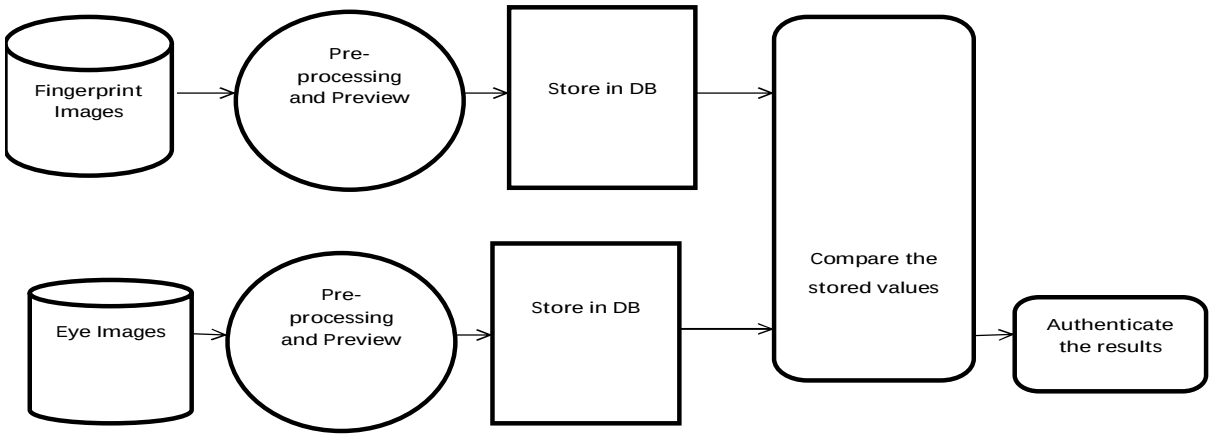


Fig.V.1 Architecture Diagram

VI. METHODOLOGY

A. Overview Of Matlab

A high-performance language for technical computing is called MATLAB. In a simple-to-use environment, it mixes computing, visualization, and programming while expressing issues and solutions using well-known mathematical notation. Common usage comprise,

- Scientific and engineering graphics
- Math and computation
- Algorithm development
- Data gathering
- Modelling, simulation, and prototyping
- Data analysis, exploration, and visualisation
- Data analysis, exploration, and visualisation.

A simple data element in the interactive system MATLAB is an array that doesn't need to be dimensioned. In comparison to the time it would take to build a programme in a scalar non-interactive language like C or Fortran, this enables you to solve a variety of technical computing problems, particularly those using matrix and vector formulations. Matrix Laboratory is the abbreviation for the word.

B. Input Design

The information system and the user are connected through the input design. The evolving specification is included the computer to read data from a written or printed document, or it can happen when users type the data directly into the system. and processes for data preparation and those stages are necessary to transform transaction data in to a usable form for processing. The input process is designed with an eye towards minimising the quantity of input necessary, minimising errors, minimising delays, minimising extra stages, and maintaining a straightforward workflow. The input is made in such a way that it offers security, usability, and privacy preservation. Input Design took into account the following:

1) What information should be provided as input?
2) How should the data be organised or coded?
3) The conversation to direct the operating staff's input-giving.

Guidelines for creating input validations and what to do in case of error occurs.

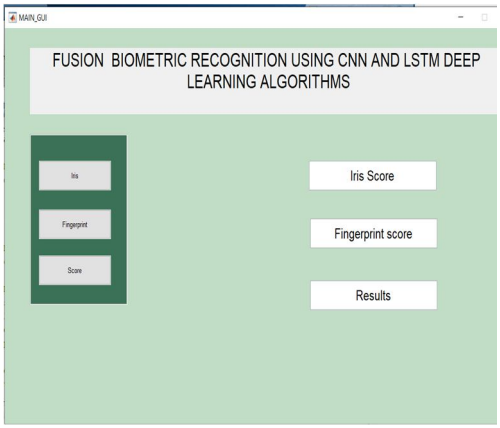


Figure VI.1 Input Screen

C. Preprocessing And Postprocessing Images

For preprocessing and postprocessing activities, Image Processing Toolbox offers reference-standard methods that address common system issues such interfering noise, limited dynamic range, out-of-focus optics, and the variation in color representation between input and output devices. By adjusting a picture's colors or intensities, you can use image enhancement techniques in picture Processing Toolbox to improve the signal-to-noise ratio and highlight visual features. Histogram equalization is something you can do.

• Practice stretching with decorrelation
• Adjust dynamic range. Perform linear, median, or adaptive filtering. Modify the gamma value. The toolbox consists of specialized filtering algorithms and a generalized multidimensional filtering function that performs convolution, correlation, and handling integer image types with different boundary-padding choices. For creating and using your own linear filters, predefined filters and functions are provided.

Figure VI. 2 Iris Preprocessing

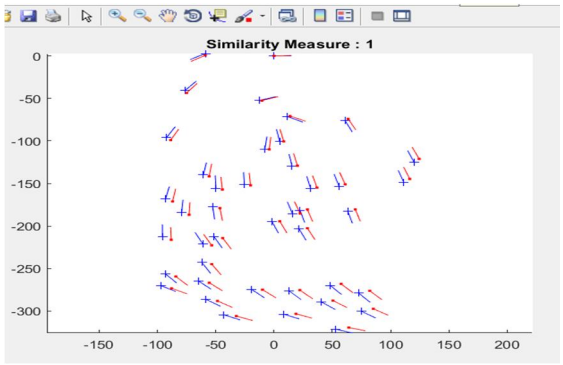


Figure VI. 3 Fingerprint Preprocessing

D. Analyzing Images

Image Processing Toolbox provides a comprehensive suite of reference-standard algorithms and graphical tools for image analysis tasks such as statistical analysis, feature extraction, and property measurement. Statistical functions let you analyze the general characteristics of an image by:

1) Computing the mean or standard deviation
2) Determining the intensity values along a line segment
3) Displaying an image histogram
4) Plotting a profile of intensity value Edge-detection algorithms let you identify object boundaries in an image. These algorithms include the Sobel, Prewitt, Roberts, Canny, and Laplacian of Gaussian methods. The powerful Canny method can detect true weak edges without being "fooled" by noise. Image segmentation algorithms determine region boundaries in an image.

You can explore many different approaches to image segmentation, including automatic thresholding, edge-based methods, and morphology-based methods such as the watershed transform, often used to segment touching objects. Morphological operators enable you to detect edges, enhance contrast, remove noise, segment an image into regions, thin regions, or perform skeletonization on regions. Morphological functions in Image Processing Toolbox include:

a) Erosion and dilation
b) Opening and closing
c) Labeling of connected components
d) Watershed segmentation
e) Reconstruction

E. Working With Large Images

Some images are so large that they are difficult to process and display with standard methods. Image Processing Toolbox provides specific workflows for working with larger images than otherwise possible. Without loading a large image entirely into memory, you can create a reduced-resolution data set (R-Set) that divides an image into spatial tiles and resamples the image at different resolution levels. This workflow improves performance in image display and navigation. You can use a block processing workflow to apply a function to each distinct block of a large image, which significantly reduces memory use. An additional option for working with large images is to use the Parallel Computing Toolbox. All the tool boxes were previously explained.

F. Output Design

A quality output is one that shows the information clearly and complies with the end user's needs. Any system's outputs are how processing results are transmitted to users and other systems. It is decided during output design how information will be displaced for immediate demand as well as the hard copy output. It is the user's most crucial and direct source of information. Efficient and intelligent output design enhances the system's ability to assist users in making decisions.

1) It is important to design computer output in an organised, well-thought-out manner. The correct output must be created, and each output component must be created so that users may utilise the system successfully and easily. When analysing computer-generated output, one should pinpoint the precise output that is required to satisfy the specifications.
2) Decide on how to convey the information.

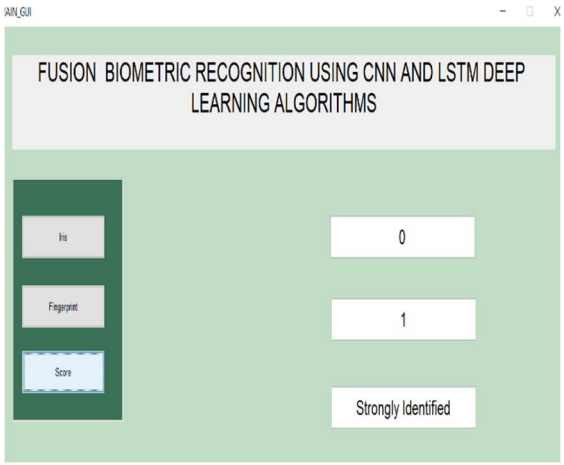


Figure VI. 4 Output Result

VII. CONCLUSION

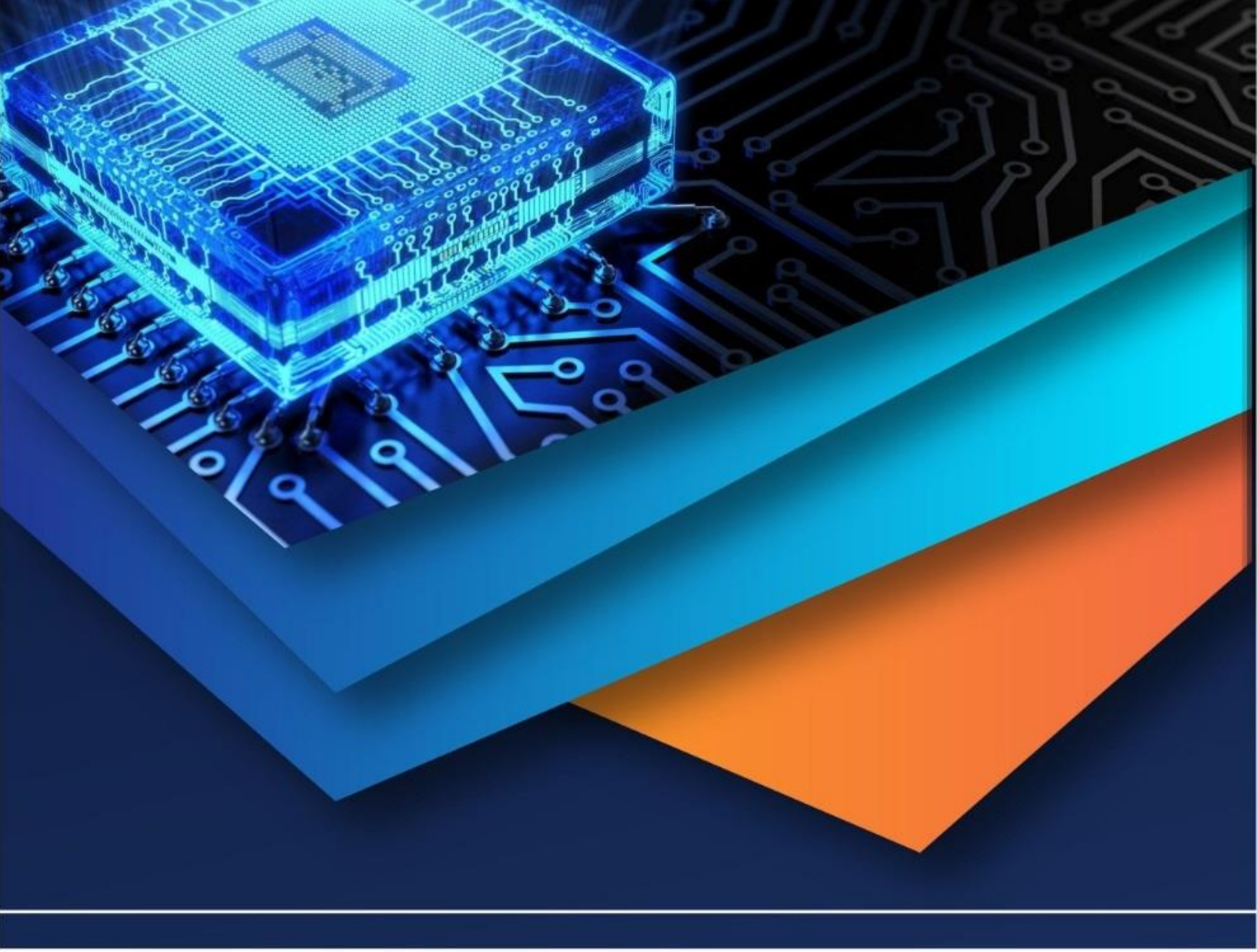
Finally, it should be noted that biometric recognition systems have grown in popularity and significance across a number of industries, including security, identity verification, and access control. These systems leverage unique physical or behavioral characteristics, such as fingerprints, iris patterns, face features, or voiceprints, to reliably identify individuals.

The use of biometric recognition technologies has brought about a number of advantages. First of all, because biometric characteristics are challenging to copy or forge, they provide a higher level of security than more conventional authentication techniques like passwords or ID cards. By doing this, the dangers of identity theft and unauthorized access are reduced. Second, by removing the need to carry physical credentials or memorize passwords, biometric systems offer convenience and efficiency. Users can quickly authenticate by displaying their biometric characteristics, which results in faster procedures and improved security.

Systems for biometric recognition do have some difficulties, though. Privacy difficulties emerge because biometric data is sensitive. To prevent misuse or unauthorized access, stringent security precautions must be taken during the transmission and storage of biometric data. A biometric system's accuracy and dependability can also be impacted by the caliber of the biometric samples used, the system's architecture, and environmental factors. Continuous research and development are necessary to raise accuracy rates and lower rejection or acceptance rates due to error. In spite of these challenges, biometric recognition technologies have proven effective in a variety of settings, including border control, banking, and healthcare. We may anticipate more developments in biometric algorithms, sensor technologies, and system integration as technology progresses, which will result in even more dependable and secure biometric recognition solutions. Overall, biometric recognition systems provide a potential way to increase convenience and security in many different areas, and their continuous development and use will probably influence the direction of authentication and identification systems in the future.

REFERENCES

[1] J. Daugman, ‘‘Probing the uniqueness and randomness of iriscodes: Results from 200 billion iris pair comparisons,’’ Proc. IEEE, vol. 94, no. 11, pp. 1927–1935, Nov. 2006.
[2] J. Daugman, ‘‘Recognising persons by their iris patterns,’’ in Advances in Biometric Person Authentication. Springer, 2005, pp. 5–25.
[3] R. P. Wildes, J. C. Asmuth, G. L. Green, S. C. Hsu, R. J. Kolczynski, J. R. Matey, and S. E. McBride, ‘‘A system for automated iris recognition,’’ in Proc. IEEE Workshop Appl. Comput. Vis., Dec. 1994, pp. 121–128.
[4] H. Proença, ‘‘An iris recognition approach through structural pattern analysis methods,’’ Expert Syst., vol. 27, no. 1, pp. 6–16, Feb. 20.
[5] B. J. Kang and K. R. Park, ‘‘A new multi-unit iris authentication based on quality assessment and score level fusion for mobile phones,’’ Mach. Vis. Appl., vol. 21, no. 4, pp. 541–553, Jun. 2010.
[6] K. Nandakumar, Y. Chen, S. C. Dass, and A. K. Jain, ‘‘Likelihood ratiobased biometric score fusion,’’ IEEE Trans. Pattern Anal. Mach. Intell., vol. 30, no. 2, pp. 342–347, Feb. 2008.
[7] P. Wiggin and L. Ericson, ‘‘Contactless fingerprint technologies assessment,’’ Nat. Criminal Justice Reference Service, ManTech Int. Corp., Fairmont, WV, USA, Tech. Rep., 2014.
[8] B. C. Stanton, M. F. Theofanos, S. M. Furman, and P. J. Grother, ‘‘Usability testing of a contactless fingerprint device: Part 2,’’ NIST, Gaithersburg, MD, USA, Tech. Rep. NISTIR 8158, 2016.
[9] J. Daugman, ‘‘How iris recognition works,’’ in The Essential Guide to Image Processing. Amsterdam, The Netherlands: Elsevier, 2009, pp. 715–739.
[10] E. Tabassi, C. Wilson, and C. Watson, ‘‘Fingerprint image quality,’’ Nat. Inst. Sci. Technol., Gaithersburg, MD, USA, Tech. Rep. 7151, 2004.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY