Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2024 SCPE. Volume 25, Issues 2, pp. 1040–1055, DOI 10.12694/scpe.v25i2.2524

SECURESENSE: ENHANCING PERSON VERIFICATION THROUGH MULTIMODAL BIOMETRICS FOR ROBUST AUTHENTICATION

SAMATHA J[*]AND G .MADHAVI[†]

Abstract. Biometrics provide enhanced security and convenience compared to conventional methods of individual authentication. A more robust and effective method of individual authentication has emerged due to recent advancements in multimodal biometrics. Unimodal systems offer lower security and lack the robustness found in multimodal biometric systems. The research paper introduces a novel approach, employing multiple biometric modalities, including face, fingerprint, and iris, to authenticate users in a multimodal biometric system. The paper proposes the ”Secure Sense” framework, which combines multiple biometric modalities to improve person verification accuracy. The proposed system utilizes both web-based and real-time datasets. For the web-based dataset, we employed the Chicago Face dataset for facial data, the MMU1 dataset for iris data, and the SOCOfing dataset for fingerprint data. In real-time data collection, facial data is captured using a Zebronics Zeb-Gem webcam, fingerprint data is obtained using the Mantra MFS scanner, and iris data is collected using the Mantra MIS scanner. In the envisioned system, we introduce an innovative approach that employs a decision-level fusion technique across three unique biometric modalities, resulting in an impressive accuracy rate of approximately 93% across all modalities.

Key words: Biometrics, CNN, Daugman, Decision level fusion, Haar-Caascade, multimodal

1. Introduction. The process of identifying individuals based on their physiological, biological, or behavioral characteristics is known as biometrics[1]. These qualities are unique to each person and do not change more or less throughout life. Biometric security has proven to be an effective tool compared to electronic security. Biometric traits can be either physiological or behavioral traits of humans. This is possible as long as you have the following properties: Integrity, Uniqueness, Lasting Quality, Collectability, Circumvention, Value, Execution. Body type is a factor in physiological biometrics. Fingerprinting is a feature that has been around for over a century. Examples include irises, DNA, palm prints, and hand shapes. Behavioral biometrics relate to human behavior. The main trademarks used are brands that are still widely used today. Keystrokes, gait (the way you walk), and writing style are some additional factors. The ability to speak is one biometric feature that falls into both categories. Choosing the right biometric based on your application is important.

Sensor data is noisy and not universal, and in monomodal biometric systems using a single biometric, there is no fixed representation of the biometric. Discourse, for example, biometric element whose characteristics change radically when a person is affected by a cold or home conditions. Creating a multimodal biometric system that integrates evidence from multiple biometric sources can alleviate some of these problems. Multimodal or multibiometric frameworks use a variety of physiological or social biometric data to record and identify people. An implementation of such a multimodal biometric personal verification framework is presented in this paper.

Some features offer great reliability and accuracy, but no 100% accurate biometrics. With the growing global need for security, there is a clear need for robust automatic person recognition systems. Accuracy of authentication is always of paramount importance when dealing with applications containing sensitive data. thus, facilitating multimodal biometrics. An integrated prototype system that includes different biometric types is called multi-biometric. Combining multimodal biometrics with personality verification can improve the performance of character verification frameworks. Multimodal biometrics can improve false acceptance rate (FAR) performance without reducing the likelihood of access denial by increasing the ability to distinguish between genuine and fraudulent classes[2]. Although there are many challenges in enrolling large populations using a single (unimodal) biometric, identifying unimodal biometrics is highly effective. The main problem with unimodal biometric systems is the fact that no single technology is suitable for all applications. As a result,

[*] Department of CSE, Matrusri Engineering College, JNTUK, India (samathajuluri@gmail.com)

[†] Department of CSE, University College of Engineering, JNTUK, India (madhavi.researchinfo@gmail.com)

the use of multimodal biometric systems overcomes the drawbacks of unimodal biometric systems. Multi-biometrics are widely used all over the world. Various systems require reliable person recognition systems to verify or determine the identity of individuals. These schemes ensure that only authorized users can access the services offered[3]. Examples of such applications include secure access to buildings, computer systems, laptops, mobile phones, and ATMs [4]. These systems are vulnerable to fraudulent schemes in the absence of robust personal recognition engines. Due to unimodal limitations, an authentication scheme based on only one modality may not meet all requirements. Current work is expected to create a bimodal biometric framework using facial, fingerprint, and iris highlights. This is to mitigate the impact of certain obstacles in the unimodal biometric framework.

Robust authentication through multimodal biometrics entails the utilization of multiple biometric factors in conjunction to bolster security during user authentication. This approach offers a range of advantages, including heightened precision, enhanced security, increased resistance to spoofing attacks, and adaptability to varying environmental conditions.

2. Related Works. The multimodal biometric authentication system has been the subject of several proposals and developments. None of the biometrics is 100% accurate, despite the fact that some of the characteristics offer good performance in terms of reliability and accuracy. The authentication accuracy of the system is always the primary concern for applications that involve the flow of confidential information. Because of this fundamental reason, multimodal biometrics should be used [5].

Elhoseny [5] proposed the majority of security frameworks fall into one of these three categories: based on information; What you know, like a PIN, password, or identification, could very well be guessed, ignored, or shared. A token known as "What you have," such as a key or card, is another type; It could be taken, duplicated, or misplaced. The final type is the use of biometrics; what you are, like your face, IRIS, fingerprint, and other characteristics. Biometric identification systems can identify individuals by comparing a template set that is stored in the database to the measured and analyzed physiological or behavioral characteristics. Uni-modular biometric frameworks suffer from certain issues like noise in detected data, incompleteness, parody attacks, intra-class varieties, and similarity between classes. The utilization of a blend of at least two biometric types to further develop a framework's security is known as a multi-modular biometric framework. Models include Iris and fingerprints, to enhance user authentication and security. There are five levels of fusion in multi-modal biometric systems: scale sensor; where, at the feature level, the sensor's raw data are combined; At this level, the features of each user biometric process are combined to form a single feature set or score level; where the final decision, rank level, and match scores from difference matches are combined to show how similar the input and stored templates are to one another; Each selected personality is assigned a position by each biometric subsystem, and the subsystem positions are combined to create a new position for each character and choice level; The last acknowledgment choice is made by consolidating the aftereffects of each biometric subsystem. Multi-biometric systems can be broken down into six distinct groups: diverse sensors; which use a variety of sensors and algorithms to capture biometric characteristics and extract various data; where numerous cases of the equivalent biometric information are handled by various calculations; use numerous examples, different occurrences of the equivalent biometric, for example, left and right irises or pointers; In order to obtain a more comprehensive multi-modal representation of the underlying biometric, multiple samples of the same biometric are taken using the same sensor; hybrid, in which evidence from two or more biometric features is combined; refers to systems that use two or more of the five other categories. This chapter presents a proposed system for fingerprint and iris recognition that is based on minutiae extraction for fingerprint recognition and hamming distance for IRIS Recognition. The proposed system is built with MATLAB 7.8.0.347(R2009a) and makes use of CASIA Iris V1 data for Iris recognition and FVC 2000 and 2002 DB1 A data for fingerprint recognition. It compares the standalone fingerprint recognition system's FAR, FRR, and accuracy metrics with those of the multi-modal biometric system based on Fingerprint and Iris, demonstrating that the multi-modal system's FAR and FRR results are lower and accuracy is higher than those of the standalone fingerprint recognition system [6]. The experiment's findings were based on Iris recognition datasets from CASIA Iris V1 and fingerprint recognition datasets from FVC 2000 and 2002 DB1 A.

The author in [7] explained, Feature Extraction, and Classification are the three distinct phases of this novel biometric image classification approach, which is based on an optimal neural network and presented in this paper. The novel method begins with the procedure of pre-processing the median filter. The element extraction stage, in which different highlights are really separated from biometric pictures, comes straightaway. Shape and surface components like the finger impression and ear include are among the removed highlights. The ONN method does a great job of classifying the images. The sensitivity, specificity, and accuracy of the new method's efficiency metrics, as well as the False Positive Rate, False Negative Rate, and accuracy, are successfully estimated. It breezes through without a hitch with regards to grouping pictures with excellent viability, accomplishing real effectiveness in the errand of characterizing pictures, and delivering energizing outcomes with extraordinary exactness.

The development of sensing and multi-modal communication technologies has resulted in an increase in the complexity of multi-modal biometric recognition (MBR). The presence of biometric data with higher dimensionality and more diverse inputs has also added complexity to MBR. This paper proposes a multi-modal fusion technique system based on the GLCM algorithm's combination of features from fingerprint and iris images. Prior to suggesting the proposed acknowledgment framework, a survey of past investigations on the iris and unique mark was finished. The AND entryway was used to pursue the final choice in the combination method choice. The review's results showed that, in comparison to the KNN classifier's recommended limit of up to 90%, the proposed framework achieved a high accuracy rate. The system's evaluation was based on the FAR, FRR, and total accuracy rate [8].

Application security cannot be guaranteed without authentication. Cloud computing is a model for providing IT-related services to a variety of end users that uses the internet. Cloud services are becoming easier to use over time because they give users a lot of freedom. Also, it raises a few worries in regard to information security. The inherent biological patterns of the multi-modal biometric system enhance the robustness of the authentication mechanism. Because of the caught design, it precisely separates the people from their characteristics. Additionally, this concept can be applied in a variety of ways to strengthen the system, including, among other things, securing health information and the human genetic code for future reference through digital ledger management and EHR management. This work proposes a multi-modal biometric authentication method to increase cloud-based data security. An MD-5 hashing calculation is used to combine the elements removed from a unique finger, iris, and palm print in multiple stages to produce a hash of strings and numbers for a mystery key. The protected data is encrypted with one of three symmetric key encryption algorithms—DES, AES, or Blowfish—using the secret key. AES outperforms the other two algorithms in terms of performance in relation to the strength of the encryption process, while DES takes less time to execute. This model demonstrated its robustness in data security [9] thanks to the fusion of human modalities in the security mechanism.

Paper [5] proposes CNN-based deep learning models for the feature-level fusion of online fingerprints and signatures. At convolution and fully connected layers, early and late feature fusion techniques that combine features from both biometric modalities have been developed. The fingerprint input image has a fixed size of 150 x 150 x 1, and the online signature file is 17 x 17 pixels. The size of the signature was changed to 1 x 17 x 1 before it was sent to the network for online signatures in order to combine the characteristics of an online signature and a fingerprint. Different systems were attempted to consolidate the elements of an internet-based signature and a picture of a unique finger impression. Be that as it may, the width of the web-based mark's component vector, which was set to 1, didn't work on the precision or some other qualities for other assessment measurements for the proposed framework. The problem was solved, and the system's accuracy and values for other evaluation metrics were raised, by adding two zero-padded layers to the signature network. The additional zeros were added, at least at the top, base, left, and right, of the element vector using this zero-cushioning strategy. As a result, the dimensions of the final feature vector increased to 4 x 4. Similarly, the final feature vector for fingerprints was 4 x 4. These features have been concatenated and passed through fully connected layers in order to extract and classify features in a more abstract way. The model was trained and tested using the new data set. With the early fusion scheme, the system was 99.10% percent accurate, and with the late fusion scheme, it was 98.35% accurate. The fusion may also use low-level fingerprint characteristics or level 3 features, such as active sweat pores and ridge contours, in the future to ensure a user's accuracy and liveliness. One of the various biometrics-specific different state-of-the-art cryptography methods may be incorporated into the proposed system in the future to further ensure the fused biometric template's safety.

Paper [6] proposes a useful feature-level fusion method for a multimodal biometric recognition system. We looked at the multimodal biometric, which includes a level combination like an ear and palm impression. The four main steps in our proposed method are preprocessing, feature extraction, optimal feature level fusion, and recognition. The shape highlights were separated utilizing a changed district developing calculation, and the surface elements were extricated utilizing the HMSB administrator. Additionally, we selected the relevant features by employing the optimization technique. For picking the ideal component, we used the OGWO + LQ computation. On the positive, we proposed affirmation, for the affirmation we used the multi-part support vector machine (MKSVM) estimation. Measures like responsiveness, particularity, and precision are used to evaluate the implementation of our proposed strategy. Our proposed strategy outperforms other techniques in terms of awareness, particularity, and precision, as demonstrated by the trial results and similar research. Consequently, the multimodal biometric recognition system can greatly benefit from the efficiency of our suggested method. Individual confirmation demonstrates utilizing convolution brain networks is an effective method for putting a multimodal biometric framework on equipment. Our proposed work's execution on CNN [22] would be a future undertaking.

3. Existing Unimodal based Systems. Unimodal systems are biometric identification systems that use a single biometric trait of the individual for identification and verification[10].

Fingerprint Recognition. During this recognition process, fingerprint features like swirls, arcs, loops, raised patterns, ridges, and other fine details are recorded using ink or a digital scanner to take an image of the fingerprint[11]. Then, we store or process this data with cryptographic algorithms. Particulars can be planned to relative finger positions utilizing a product program, and comparable details data can be looked through in a data set. To speed up the search, images are converted into strings. So, in most cases, the fingerprint image is just a string of characters to compare. By holding their finger on the reader for a few seconds, fingerprint readers enable users to identify or verify an individual. Today, fingerprint readers also check for blood flow and make sure the ridges on the ends of the fingers are where they should be to make sure no fake fingers are used. One of the benefits of this procedure is that it makes use of advanced technology and is easy to use. In addition to supporting the capability of enrolling multiple fingers for enhanced anti-spoofing properties, this method is extremely accurate and stable over time[9]. There are some drawbacks to this method: Contacting the unique finger impression per user can smirch your fingers, which can influence picture quality. The skin type and condition may influence the registered data [28].

Facial Recognition. This identification interaction estimates the whole facial design, like the distance between the eyes, nose, mouth, and the edge of the jaw [12]. Functions are used to create and store templates in the database. A single image is formatted based on facial features and captured with a conventional or video camera during a confirmation or differential verification cycle. This format is then contrasted and the layout of the data set. In the future, only high-performance test procedures will make use of this acknowledgment arrangement. Before authentication, systems today demand that users smile, blink, and move in a humane manner[34]. This is done to stop people from pretending to be part of the system. This framework enjoys the benefit of being inconspicuous. It functions admirably at an insignificant cost as it permits you to remove pictures utilizing normal reconnaissance cameras. Additionally, this strategy can be used covertly in high-security settings like airports. To put it another way, the person is not aware that the picture was taken. The disadvantage is that appearance and the environment can have an impact on facial recognition, which is highly dependent on the quality of the images obtained. This system can cause issues with identical twins and is typically inaccurate. Additionally, it operates secretly, jeopardizing your privacy[13].

Hand Geometry. Utilizing this recognition system is a straightforward but highly accurate process. The user places their hands on a metal surface with guidance pegs to assist in proper hand alignment. The gadget finds out around 90 hand qualities, including length, width, thickness, finger surface region, and palm size. These characteristics can be checked against another template in the database or form a template that is stored in the database. The fact that hand geometry technology has one of the biometrics industry's smallest templates—typically less than 10 bytes—is one of its primary advantages [12]. It likewise has high client mindfulness and is non-nosy. The searcher's relatively large size and low precision are its weaknesses. Children, people whose joints are inflamed, people whose fingers are missing, or people with large hands may find reporting challenging. Now, it is only used for the verification process.

Iris recognition. To identify individuals, this technology looks for characteristics like freckles, furrows, and rings in the colored tissue around the pupil [24]. This is one of the biometric technologies with the highest degree of accuracy. As indicated by a new Silicon.com article, an administration exploration including facial acknowledgment, iris acknowledgment, and unique finger impression acknowledgment found that iris acknowledgment played out the best as a confirmation technique, in spite of the difficult enrolment process. A normal camcorder can be utilized to get a picture of the iris, and it very well may be finished from a more noteworthy distance than with a retinal output. Users of this technology need to work together to get a clear picture. Subsequently, the gadget is planned so that when the client puts his head before it, he can see his iris reflecting in the gadget, demonstrating that an unmistakable picture can be gotten. In order to ensure that the framework is not fooled by a fictitious eye, the device may alter the light that is reflected into the eye and observe the pupil expanding. This framework has the advantage of a high confirmation rate and fraud protection. The iris data are the same for the left and right eyes and do not change as you get older. The disadvantage of this strategy is that it is extremely intrusive; The process of enrolling is somewhat challenging since not everyone is familiar with the system. John Daugman, a Cambridge College scientist, was responsible for a great deal of exploration on iris acknowledgment.

Retinal Recognition. It is a technique for observing the retina's blood vessel pattern, which is said to vary from person to person. Essentially, the retina is comprised of material tissue with various layers close by photoreceptors like cones and shafts. Photoreceptors take in the light rays they emit and turn them into an electrical force that the mind uses to create images. In comparison to the tissue that surrounds the eye, the blood vessels that make up the retina are better able to detect and reflect infrared light. In this way, the gadget utilizes its IR light to enlighten the retina, and when the IR is mirrored, a retina assessment gadget utilizes it to eliminate the remarkable components of the retina utilizing different estimations. The size of the pupil, which controls how much light reaches the retina, affects image quality. The fact that a person's retina stays the same throughout their lifetime is a benefit of this innovation. In comparison to other technologies, it has many distinctive features and a high verification rate. Client anxiety when eyes are filtered from very close distances, the requirement to remove eyeglasses at contact hotspots, and the widespread perception that devices can damage the retina are all obstacles to this strategy. Being patient and cooperative with a lot of customers [27-29].

Signature Recognition. The behavioral part of how we sign names is analyzed by Mark's Acknowledgment. This development is due to direct qualities such as timing, pressure, speed, overall changes, and different stroke paths throughout the stamping. Despite all the characteristics of copy brands being fundamental from the ground up, the nature of their behavior is difficult to copy. This device includes a stylus (or pointer) and a There are special writing tablets that The pen must be used by the customer to sign on to the tablet. This system collects all information about features, creates templates, and stores them in a database. You are required to register for various events to complete valid registration. This method is advantageous because it is a painless device that is well-known and difficult to imitate. The drawback is that the signature should not be too long or too short. A signature that is too long can contain too much behavioral data and make it difficult for the system to find consistent and unique data points. If the signature is too short, there may not be enough data points for the system to create a unique template. Whether you're standing, sitting, or resting your arms, the recording process should take place in the same environment. The structure also tries to modify the client, resulting in signature anomalies [27].

Voice Recognition. Voice originates from the vocal cords. When we try to communicate, the distance between the vocal cords narrows or widens. Thus, increasing expansion with deep breathing and narrowing with exhalation produces an unmistakable sound. Most of the vocal tract consists of the larynx, oropharynx, oral cavity, nasopharynx, and nasal cavity. In this method, users are asked to recite part of a list of texts or numbers using a microphone or phone connected to their computer. A computer receives the user's voice and converts it into digital form. A template is created by saving this format and extracting certain features from it. Statistical profiles are created by comparing multiple samples and identifying various recurrence patterns. As a result, statistical profiles are compared to ensure accuracy. The advantage of this strategy is that existing communication bases or mouthpieces can be used. It is unobtrusive and easy to use. This is a problem because background noise affects the system. Accuracy is very low, as it can be affected by voice adaptation due to aging, disease, alcohol consumption etc [23].

Gait Recognition. Gait recognition is a technology that recognizes people by the unique way they walk. Stride recognition is usually useful for reconnaissance because it tends to be caught without the person's consent. Faking and hiding are also extremely challenging. Energizers like liquor and medications, which make individuals unequal, actual changes brought about by pregnancy, a mishap, weight gain or misfortune, an individual's state of mind, and the garments they wear can all influence walking. Stride acknowledgment should be possible by utilizing typical observation cameras. A portion of the benefits are that it tends to be finished in a good way and minimal expense observation cameras can be utilized. It is difficult to fake and can be affected by the person's background, clothes, and emotions, which are disadvantages [27].

Key stroke Recognition. Because different people type differently on computer keyboards, keystroke detection is necessary. This strategy includes a keyboard or a computer-attached keyboard. When asked to enter a particular word on multiple occasions, the user must meet certain requirements, such as typing correctly. In the event of typos, You must start from scratch. The manner in which an individual sorts, the total composing speed, the time between progressive keystrokes, how long each key is held down, and how frequently an individual presses other keys utilizes the console. The request wherein capitalized letters are placed, for example, the numeric keypad and capability keys, whether the shift key or the letter key is delivered first, and so on., are a few of the extracted characteristics. These characteristics are used to generate a template for a statistical profile of a person's behavioral characteristics. They are advantageous because they are entirely software-based, do not require additional hardware, integrate with other biometrics, and require little training. Another advantage is that you can change the word and make a new template if you change the template for a particular word. This method has one drawback: it doesn't make it easier to remember passwords. In addition, the technology is still in its infancy and has not yet undergone a significant amount of testing.

Hand Vascular Pattern Recognition. The technology uses state-of-the-art recognition algorithms based on the unique veins and capillaries found on the back of the human hand to validate or recognize human users. Vein pattern recognition is based on the concept that the hotter the image, the brighter it becomes during infrared imaging. The colder the object, the darker it appears. So, when you scan your hand with an infrared reader, your vein pattern will appear darker than the surroundings. Everyone's pattern is different. If the image is saved as a personal template, it can be used for verification or identification purposes. The advantage is the high accuracy of this method. Unaffected by harsh environments such as construction sites, military bases, and manufacturing plants [13]. It is also very convenient for users as it requires minimal knowledge of the system. Infrared absorption patterns can be easily compared via optical and DSP techniques to provide a large, robust, and stable base for matching units. This usually requires a lower-resolution IR [27].

3.1. Limitations of Unimodal Systems. The following are the limitations [24] of unimodal systems.

Distortion of the biometric data that was input. Users may be rejected or identified incorrectly as a result of distorted biometric data preventing the alignment process with database templates.

Intra class variations. The biometric information obtained during identity verification may differ from the information used to create the registration format, which may affect verification systems. Biometric forms should show slight differences within the class.

Interclass similarities. Biometric highlights ought to be altogether unique for various individuals and ought to guarantee little similitudes between classes in the component space. Any biometric system can only effectively distinguish a certain number of users. The limitations of the recognizable proof framework cannot be arbitrarily extended to calculus consistent with a fixed set of element vectors.

Non-universality. There should be a lot of variation between classes in the biometric template. It is not always possible to obtain accurate and useful biometric data from users.

Intruder attacks. This type of attack modifies biometric authentication functionality to avoid detection. You could even create a fake biometric design to recognize someone else's personality.

4. Proposed System. In the proposed system, we incorporate three distinct biometric modalities: face, iris, and fingerprint. Our dataset comprises both web-based and real-time data sources. The web-based data includes well-established online datasets, specifically, the Chicago face dataset for face recognition, the MMU1 dataset for iris recognition, and the SOCOfing dataset for fingerprint recognition. In contrast, the real-time dataset is gathered using webcam technology as well as Mantra MIS and MFS scanners. Subsequently, we conduct feature extraction on all these modalities. We employ decision-level fusion techniques to amalgamate these extracted features. Finally, the authentication process is carried out using a Convolutional Neural Network (CNN) algorithm.

4.1. Datasets.

4.1.1. Web Based Dataset.

Face Dataset. The Chicago Face Database was created by Bernd Wittenbrink, Debbie S. Mom, and Joshua Correll at the School of Chicago. It offers standard, high-resolution portraits of men and women whose ethnicities range from 17 to 65. There are a lot of norming data for each model [14-16].

IRIS Dataset. The Multimedia University (MMU1) database contains eye images for the IRIS-based biometric system's training models. Each person's individual IRIS patterns for each eye make it easier to identify them. 46 people's left and right IRIS are represented by 460 images and a few empty files in this dataset. Individual ID and characterization of an IRIS picture in view of a saved information base can be achieved through IRIS division [17].

Fingerprint Dataset. A biometric fingerprint data set produced for scholarly exploration is the Sokoto Coventry Finger Impression Dataset (SOCOFing). SOCOFing is comprised of 6,000 fingerprint images from 600 African subjects. These fingerprint images include synthetically altered versions with three distinct levels of alteration—obliteration, central rotation, and z-cut—as well as distinctive features like labels for gender, hand and finger name, and so forth [18].

4.1.2. Real Time Dataset. We have gathered the real-time dataset for our task, from the students. We have taken ten images, four of each student's face, three images of their fingerprints, and three images of their iris.

The face pictures are gathered utilizing the Zebronics Zeb-Gem Genius webcam. A USB-powered web camera with a 3P lens and clear videos is the Zeb-Crystal Pro. It has night vision, a clip-on design for easy mounting, and a built-in microphone. 30 frames per second, 640 x 480 video resolution, and 1.2 meters of cable. The webcam can be used directly without the need for drivers.

The fingerprint pictures are collected utilizing the Mantra MFS scanner. The MFS100 USB fingerprint sensor is a high-quality option for desktop or network security fingerprint authentication. MFS100 depends on optical detecting innovation which effectively perceives low-quality fingerprints too. MFS100 can be utilized for validation, ID, and check works that let your unique finger impression carry on like computerized passwords that cannot be lost, neglected, or taken. Scratches, impacts, vibration, and electrostatic shock are all prevented by a hard optical sensor. Attachment and play USB 2.0 rapid point of interaction upholds numerous gadgets taking care of. 500 dpi optical finger impression sensor scratch-free sensor surface. supports Windows 7, 8, 10, Vista, Windows 2000, Linux, Windows ME, and Windows 98 SE SDK, Libraries, and Drivers on all platforms. 32-Bit and 64-Bit Support for applications and easy integration into production servers [19]. This scanner needs MFS100 RD service and MFS100 driver to be downloaded.

The Mantra MIS scanner is used to collect the iris images. The Mantra MIS100V2 IRIS Scanner is a powerful and durable iris scanner that has been used in numerous projects and is renowned for its precision. MIS100V2 is an excellent USB IRIS Sensor for IRIS Confirmation to get to the work area or organization security. The Single IRIS Sensor MIS100V2 can be extensively utilized for banking, access control, and identity applications like Aadhaar Authentication. The inbuilt LED indications make it simple to adjust the MIS100V2 quality algorithm, which is able to quickly and easily identify low-quality IRIS images. The MIS100V2's fast auto-capture capabilities are due to its proprietary distance sensing and focus analysis technology. Downloading the MIS100V2 RD service and driver is required for this scanner [20].

4.2. Feature Extraction Techniques.

4.2.1. HAAR-CASCADE API:. Haar Cascade is an algorithm for detecting features in images. A cascade function is trained on a lot of positive and negative images for detection. The algorithm doesn't need a lot of work and can run in real-time. We can train our own cascade function for custom objects like cars, bikes, and animals. Since it just distinguishes the matching shape and size, Haar Outpouring can't be utilized for face acknowledgment. The flowing window and outpouring capability are used in Haar overflow. It makes an effort

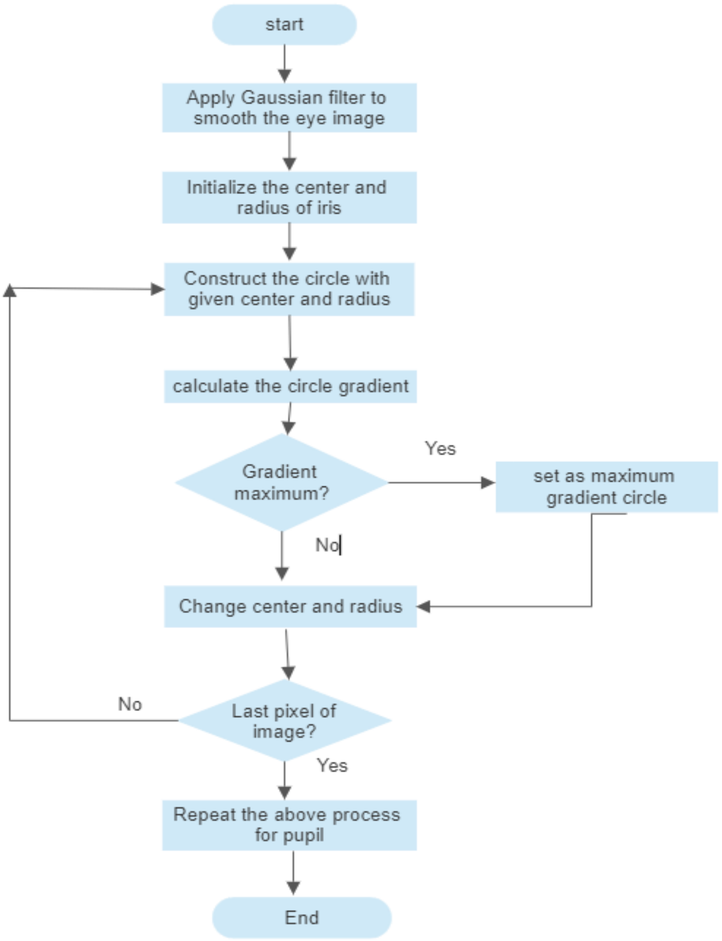
start
Apply Gaussian filter to smooth the eye image
Initialize the center and radius of iris
Construct the circle with given center and radius
calculate the circle gradient
Gradient maximum?
Yes
set as maximum gradient circle
No
Change center and radius
No
Last pixel of image?
Yes
Repeat the above process for pupil
End

Fig. 4.1: Flow chart describing Daugman's method

to identify strengths and weaknesses for each window. Positive if the window is a component of something else; negative in this case. The Haar cascade can be used with a binary classifier. It gives the outpouring windows, which could be a piece of our article, a positive worth. additionally, detrimental to those windows that cannot be a component of our product. The abundance of pre-trained haar cascade files makes implementation extremely simple. We also have the ability to train our very own haar cascade, but for that to work, we need a lot of data. A GitHub repository managed by the OpenCV library contains all of the well-known pre-trained haars cascade files. These documents can be utilized for an assortment of item recognition undertakings, for example, Eye detection, vehicle detection, nose/mouth detection, body detection, and license plate detection are all methods of human face detection [23].

4.2.2. DAUGMAN Algorithm for Iris. The first step is to apply a Gaussian filter to the eye image. This helps in reducing noise and creating a smoother image. Initialize the center and radius of the iris. These parameters will be used as starting points for constructing the iris boundary. Using the initialized center and radius, you create a circle within the eye image. This circle represents the estimated boundary of the iris. Then calculate the gradient along the circle's boundary. This step helps identify edges and patterns in the iris. check if the gradient along the circle is at its maximum. If it is, this circle is considered as the maximum gradient circle, which corresponds to the iris boundary. If not, adjust the center and radius of the circle to refine the boundary estimation. After processing the entire circle, check if reached the last pixel of the image. If not go

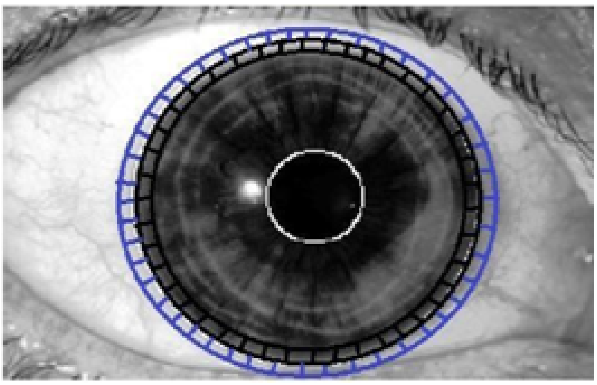

Fig. 4.2: The dark boxed line addresses a one-pixel wide iris line at a specific span 'R' (not to scale) at the middle direction and the blue boxed line addresses one-pixel wide circle at a similar focus coordinate at sweep 'R+1'

back to the step of constructing a circle with the adjusted center and radius, repeating the process for the next region of the iris. Repeat the Above Process for Pupil as shown in Fig 4.1.

4.2.3. DAUGMAN'S Operator. The task is to find the middle directions and the span of the iris and the student and Daugman's condition is utilized for this assignment. The integral of a differential equation is Daugman's theory of border recognition's central focus [23].

$$\max(r, x_0, y_0)\left| G_\sigma(r) * \frac{\partial}{\partial r} \oint_{r,x_0,y_0} \frac{l(x,y)}{2\pi r} ds \right| \tag{4.1}$$

The intensity of the pixel at coordinates (x, y) in the image of an iris is represented by (x, y). r signifies the sweep of different round areas with the middle directions at (x_0, y_0). σ is the Gaussian distribution's standard deviation. A scale sigma Gaussian filter is denoted by the symbol $G_\sigma(r)$. (x_0, y_0) is the accepted focus direction of the iris. The parameters (r, x_0, y_0) specify the circle's contour as s.

The Daugman's operator in Equ. (4.1) is pivotal in improving iris features, ultimately resulting in precise user authentication.

By altering the center (x, y) of the circular contour and the radius (r), the operator seeks the circular path with the greatest change in pixel values. In order to achieve precise localization, the operator is applied iteratively while the smoothing is gradually reduced. On the off chance that the factors x, y and r have a place with the reaches $[0; X]$, $[0; Y][0; R]$ separately, this strategy has the computational intricacy of the request $[X * Y * R]$. As a result, in order to compute the circle parameters using this method, a total of R scans are required at each pixel.

An inquiry over the whole picture (of an eye) is finished, pixel by pixel as depicted in Fig. 4.2. The normalized sum of all circumferential pixel values increases in radius at every pixel. At each degree of expanded span, the contrast between the standardized amounts of pixel power values at neighboring radii circles is noted. That pixel is deemed to be the center iris pixel when, following the entire search, summation, and differentiation portion of the calculation, the greatest variation in the sum of circumferential pixel intensity values exists between two adjacent contours.

4.2.4. 2D Gaussian Filter. In signal processing and electronics, a Gaussian filter is one whose impulse response is a Gaussian function. A Gaussian channel changes the info signal numerically through convolution with a Gaussian capability. According to our hypothesis, the Gaussian smoothing administrator is a 2-D convolution administrator used to smooth eye images to remove noise. The one-layered Gaussian channel has

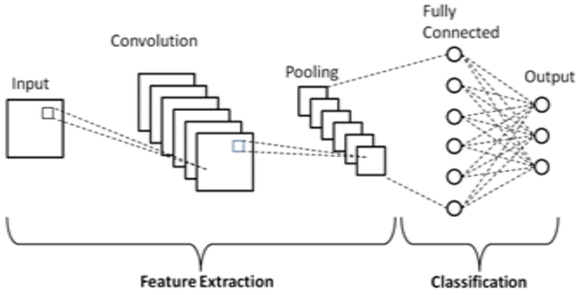

Fig. 4.3: CNN Architecture

a drive response given in Equ. (4.2)

$$g(x, y) = \frac{1}{2\pi\sigma^2} \cdot e^{-\frac{x^2+y^2}{2\sigma^2}} \tag{4.2}$$

where x and y signify the separation from the beginning towards the edges of the channel in the level hub and vertical pivot bearings, separately and σ is the standard deviation of the Gaussian dispersion.

4.2.5. 2D Convolution. In math and useful examination, convolution is a numerical procedure on two capabilities f and g as given in Equ. (4.3), creating a third capability that is ordinarily seen as a changed variant of one of the first capabilities

$$(f * g)(t) = \int_{-\infty}^{\infty} f(r)g(t-r)\,dr \tag{4.3}$$

While the image t is utilized above, it need not address the time-space.

A 2D Gaussian filter is employed to achieve image smoothing or blurring, while a 2D convolution filter serves various image processing functions, including edge detection and feature extraction [33].

4.3. Convolutional Neural Network. CNNs are a subset of Profound Brain Organizations that are appropriate for visual picture examination since they can recognize and group picture highlights. PC vision, regular language handling, picture and video acknowledgment, and clinical picture investigation are only a couple of their many purposes. CNN is useful for image recognition due to its high accuracy. Medical image analysis, phone security, and recommendation systems are just a few of the many uses for image recognition [25]. The term ”Convolution” is used in CNN to refer to the mathematical function of convolution. Convolution is a unique type of linear operation in which two functions are multiplied to create a third function that explains how one function’s shape is altered by another [21]. In layman’s terms, the output is created by multiplying two images that can be represented as matrices in order to extract features from an image [26]. A convolution device for isolating and recognizing the different picture highlights for use in highlight extraction examination. The feature extraction network contains numerous pairs of convolutional or pooling layers. a fully connected layer that, based on the features that were extracted in earlier stages, uses the convolution output to predict the class of the image. This CNN model of component extraction intends to diminish the number of features present in a dataset[21]. It adds new highlights to a current arrangement of elements, to sum up those highlights. There are a number of layers in the CNN architecture diagram.

There are three distinct types of layers in the CNN as depicted in Fig. 4.3 [29] pooling layers, fully connected (FC) layers, and convolutional layers. The stacking of these layers will result in the formation of a CNN architecture. The dropout layer and the activation function are two additional significant parameters that are described below in addition to these three layers [25].

4.3.1. Convolutional layer. The primary layer that is used to distinguish the various highlights from the information pictures is this one. The dot product (MxM) between the parts of the input image that are proportional to the size of the filter is taken by sliding the filter over the image. The Feature map is the output, and it contains information about the image, like its corners and edges. The numerical activity of convolution is completed in this layer between the information picture and a channel of a specific size MxM. Subsequently, this component map is dealt with in various layers to get to know one or two features of the data picture. The CNN convolution layer sends the result to the subsequent layer after applying the convolution operation to the input. Convolutional layers in CNN offer significant advantages because they ensure that the pixel's spatial relationship remains unchanged.

4.3.2. Pooling Layer. A Convolutional Layer is typically followed by a Pooling Layer. This layer's essential goal is to reduce computational expenses by making the convolved include map more modest. This is accomplished by reducing connections between layers and independently working on each component map. There are many different Pooling operations, each with its own set of rules and methods. It basicalley summarizes the features created by a convolution layer. In Max Pooling, the choice of the largest element is made using the feature map. The normal of the components in a picture part of a foreordained size is determined utilizing Normal Pooling. The total sum of the elements in the predefined section is computed using Sum Pooling. The Pooling Layer for the most part fills in as a framework between the Convolutional Layer and the FC Layer. This CNN model makes it easier for the networks to independently recognize the features because it generalizes the features that were extracted by the convolution layer. This also results in a reduction in computation time within a network.

4.3.3. Fully Connected Layer. The Fully Connected (FC) layer, which is used to connect the neurons between two distinct layers, is made up of the weights, biases, and neurons. These layers make up the last few layers in the majority of CNN architectures and come before the output layer. The flattened input image from the layers before it is received by the FC layer. After the vector has been smoothed, it goes through a couple of more FC layers, which are ordinarily where numerical capabilities tasks occur. At this point, the classification process begins. The fact that two completely associated layers will perform better than a single associated layer is the reason why two layers are associated. The amount of human oversight in CNN is reduced by these layers.

4.3.4. Dropout Layer. Overfitting in the preparation dataset is normal when all highlights are associated with the FC layer. When a model performs well on one set of data but fails to perform as well when applied to another set of data, this phenomenon is known as overfitting. To beat this issue, a dropout layer is utilized wherein two or three neurons are dropped from the cerebrum network during the planning process achieving a lessened size of the model. 30% of the hubs leave the brain organization haphazardly after passing a dropout of 0.3. An AI model's exhibition is improved by dropout since it works on the organization and forestalls overfitting. It removes neurons from the neural networks during training.

4.3.5. Activation Functions. Finally, the CNN model's enactment capability is one of its main limitations. They are used to estimate and learn about any kind of constant and intricate connection between the organization's factors. Simply put, it determines which model information should fire in the forward direction and which should not at the end of the network. The organization gains non-linearity accordingly. The ReLU, Softmax, tanH, and Sigmoid capabilities are only a couple of the enactment works that are much of the time used. Each of these capabilities serves a specific purpose. A CNN model typically employs softmax for multi-class classification, while the sigmoid and softmax functions are preferred for binary classification. In layman's terms, a CNN model's enactment capabilities decide if a neuron should be actuated. It comes to a conclusion about whether or not the contribution to the work is necessary to anticipate using numerical tasks.

Fig. 4.4 demonstrates the connections that exist between the various components that are being utilized. They are typically created with the intention of deepening one's comprehension of how the various parts interact with one another to accomplish the objectives.

4.4. Workflow.

4.4.1. Acquisition. The primary module that collects biometric data from individuals is the hardware for biometrics sensor hardware. A camera sensor, for instance, captures images of the face and iris; a fingerprint scanner for fingerprint, and so on. The acquisition of iris and fingerprint images in our project is performed

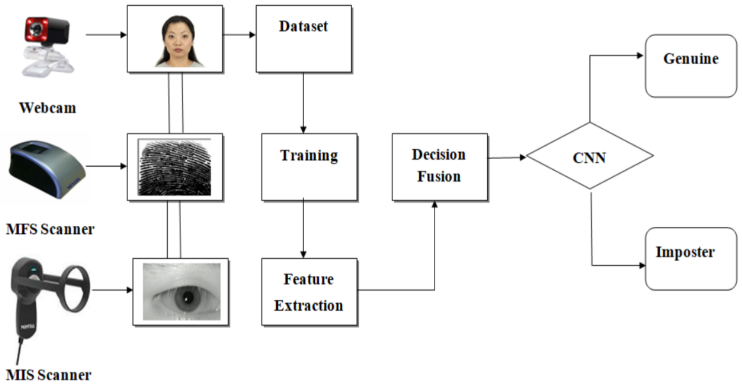

Fig. 4.4: Proposed System

using Mantra devices. We have used an MFS100 scanner for fingerprint acquisition, a MIS100V2 scanner for iris acquisition, and a ZERBRONICS webcam for the face.

4.4.2. Dataset and Training. The project makes use of both real-time and internet-based datasets. Chicago face dataset (CFD-INDIA)[16]. MMU1 iris dataset[17], and Sokoto Coventry Fingerprint Dataset (SOCOFing) [18] make up the internet dataset. The mantra devices and webcam are used to collect the real-time dataset. These datasets are used to train the multimodal system.

4.4.3. Feature extraction. The captured biometric data is pre-processed to remove any additional imperfections or noises, and then it is processed further for the feature extraction procedure, which aims to select biometric features that are most likely to convey an individual's uniqueness.

4.4.4. Preprocessing steps.

Normalization:. The range of pixel intensity values is altered by this procedure. The aim of normalization is to bring the image into a range that is easy to sense. OpenCV involves standardized capability for picture standardization.

Skew Correction:. When scanning or taking a picture of any document, there is a chance that the resulting image may occasionally be slightly skewed. The image's skewness should be corrected in order to improve the algorithm's performance.

Image Scaling. The image should have more than 300 PPI (pixels per inch) for better performance. Thus, assuming that the picture size is under 300 PPI, we really want to increment it. We can involve the Pillow Library in this.

Noise Removal. For smoothing the image, this step removes the small dots and patches that are more intense than the rest of the image. That is simple to accomplish with OpenCV's rapid Nl Means Denoising Colored function.

Thinning and Skeletonization. This step is performed for the manually written text, as various writers utilize different stroke widths to compose. The width of the strokes is uniformized with this step. OpenCV can be used for this.

Gray Scale image. An image moves from other color spaces to gray tones through this process. Between complete black and complete white, the color varies. OpenCV's cvtColor() capability plays out this undertaking without any problem.

Thresholding or Binarization. In this step, any colored image is transformed into a binary image with only black and white as colors. This can be accomplished by establishing a threshold, which is typically half of the 127-pixel range from 0 to 255. On the off chance that pixel esteem is more prominent than the edge, it turns into a white pixel; If not, it will turn into a black pixel. Otsu's Binarization and Versatile Binarization may be a superior choice for deciding the picture explicit limit esteem. The preprocessing steps such as resizing and grey scaling have been applied to the images in the paper.

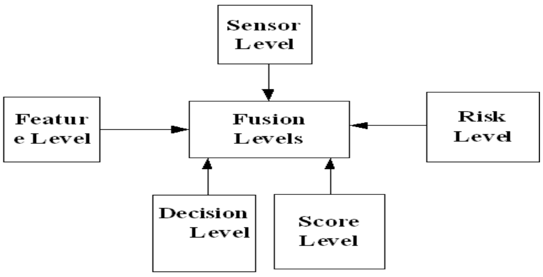

Fig. 4.5: Fusion Levels

Table 5.1: Performance of Algorithms

Algorithm	Performance Metrics		
	Face CNN	Finger CNN	Iris CNN
Accuracy	93.01	93.17	93.2
Precision	88.888	88.235	88.235
Recall	92.592	90.909	92.181
F-Score	92.0	88.235	90.909

4.4.5. Fusion. The fundamental module in the multimodal individual. verification framework is the biometrics block. One generally utilized way to deal with the development of biometrics blocks is joining individual data from various biometric features. There are various approaches to joining biometric highlights sensor level fusion, feature level fusion, decision level fusion, score level fusion, rank level fusion as depicted in Fig 4.5 One type of data fusion is decision fusion, in which the decisions of multiple classifiers decisions are combined into a single decision about the activity that took place in five levels of fusion in multi-modal biometric systems.

Sensor level. where the raw data from the sensor are combined.

Feature level. A single feature set is created at this level by combining features extracted from each user biometric process.

Level score: . where the final decision is made by combining match scores from different matches, which show how similar the input and stored templates are to one another.

Rank Level. Each character is assigned a rank by each biometric subsystem, and the ranks from the subsystems are combined to create an additional rank for identity.

Decision Level. By combining the result of each biometric subsystem, the final recognition decision is made.

In brief, feature-level fusion integrates biometric data or feature vectors, sensor-level fusion combines information from sensors, rank-level fusion considers the ranking of users across individual modalities, score-level fusion amalgamates similarity or matching scores from individual modalities, and decision-level fusion harmonizes the ultimate binary decisions reached by individual modalities.

We have employed decision-level fusion for this paper.

5. Results. Table 5.1 shows the Accuracy, Precision, Recall, and F-SCORE of face, fingerprint, and iris CNN algorithms.

The graphical representation of Table 5.1 is shown in Fig 5.1. The figure reveals the performance of the CNN algorithm on the face, fingerprint, and iris.

In the current system, the prevailing approach predominantly relies on unimodal models, with only a limited representation of multi-modal systems. Specifically, an unimodal face recognition attendance monitoring system [30] has been devised, achieving an accuracy of 87% through the utilization of the MultiTask Cascaded Convolutional Neural Network (MTCNN) and FaceNet.

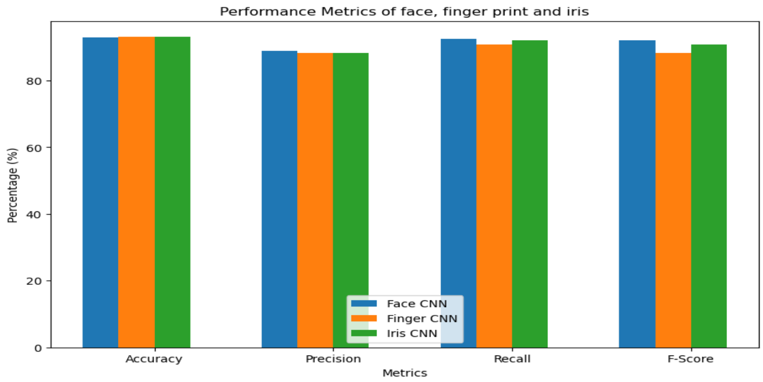

Fig. 5.1: Graphical representation of the performance of all algorithms

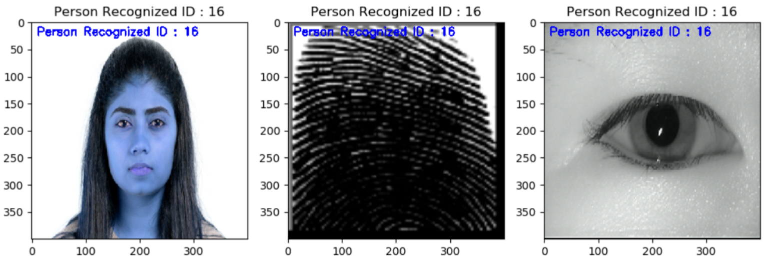
Person Recognized ID : 16
Person Recognized ID : 16
Person Recognized ID : 16
Person Recognized ID : 16
Person Recognized ID : 16
Person Recognized ID : 16
0
50
100
150
200
250
300
350
0
100
200
300

Fig. 5.2: User Prediction

In contrast, another model has adopted a multi-modal approach by integrating both facial and fingerprint biometrics [31], delivering an impressive accuracy of 96.54%. This feat was accomplished by employing the LBPH algorithm for facial recognition and the FLANN algorithm for fingerprint analysis[33]. Additionally, a separate multi-modal system, combining facial and iris recognition techniques through the deployment of the CNN algorithm, has achieved an impressive accuracy rate of 98.33% [34].

In the proposed system, we introduce a novel approach by implementing a decision-level fusion technique across three distinct biometric moralities. This represents a pioneering feature of our system. It's noteworthy that the system's accuracy can be further enhanced through the acquisition of more data and comprehensive training in future applications.

Fig 5.2 illustrates the outcome of user ID prediction achieved by inputting multimodal biometric data such as face, fingerprint, and iris.

6. Conclusion. The sole reason for user authentication is to guarantee that the right individuals have access to the right assets. The first step in protecting data and devices is verifying a user's identity. This paper proposes a robust convolutional neural network-based multimodal verification system to improve the current person verification system's recognition accuracy. Iris, face, and fingerprints are used in the system. Non-universality, spoof attacks, and distinctiveness are just a few of the issues that single-modal biometric systems must deal with. Implementing multimodal biometric systems, which combine multiple biometric features to overcome the difficulties of a unimodal system, can alleviate some of these limitations. The findings indicate that multimodal systems are superior to anyone biometric trait in terms of accuracy. They combine strong security with a high level of convenience.

REFERENCES

[1] Elhoseny, Mohamed, Ahmed Elkhateb, Ahmed Sahlol, and Aboul Ella Hassanien. ”Multimodal biometric personal identification and verification.” Advances in Soft Computing and Machine Learning in Image Processing (2018): 249-276.

[2] Chanukya, Padira SVVN, and T. K. Thivakaran. ”Multimodal biometric cryptosystem for human authentication using fingerprint and ear.” Multimedia Tools and Applications 79 (2020): 659-673.

[3] Mustafa, Ahmed Shamil, Aymen Jalil Abdulelah, and Abdullah Khalid Ahmed. ”Multimodal biometric system iris and fingerprint recognition based on fusion technique.” International Journal of Advanced Science and Technology 29, no. 03 (2020): 7423-7432.

[4] Joseph, Teena, S. A. Kalaiselvan, S. U. Aswathy, R. Radhakrishnan, and A. R. Shamna. ”RETRACTED ARTICLE: A multimodal biometric authentication scheme based on feature fusion for improving security in cloud environment.” Journal of Ambient Intelligence and Humanized Computing 12, no. 6 (2021): 6141-6149.

[5] Leghari, Mehwish, Shahzad Memon, Lachhman Das Dhomeja, Akhtar Hussain Jalbani, and Asghar Ali Chandio. ”Deep feature fusion of fingerprint and online signature for multimodal biometrics.” Computers 10, no. 2 (2021): 21.

[6] Purohit, Himanshu, and Pawan K. Ajmera. ”Optimal feature level fusion for secured human authentication in multimodal biometric system.” Machine Vision and Applications 32 (2021): 1-12.

[7] Wang, Yunhong, Tieniu Tan, and Anil K. Jain. ”Combining face and iris biometrics for identity verification.” In Audio-and Video-Based Biometric Person Authentication: 4th International Conference, AVBPA 2003 Guildford, UK, June 9–11, 2003 Proceedings 4, pp. 805-813. Springer Berlin Heidelberg, 2003.

[8] Maithili, K., V. Vinothkumar, and P. Latha. ”Analyzing the security mechanisms to prevent unauthorized access in cloud and network security.” Journal of Computational and Theoretical Nanoscience 15, no. 6-7 (2018): 2059-2063.

[9] Kirby, Michael, and Lawrence Sirovich. ”Application of the Karhunen-Loeve procedure for the characterization of human faces.” IEEE Transactions on Pattern analysis and Machine intelligence 12, no. 1 (1990): 103-108.

[10] Hong, Lin, and Anil Jain. ”Integrating faces and fingerprints for personal identification.” IEEE transactions on pattern analysis and machine intelligence 20, no. 12 (1998): 1295-1307.

[11] Snelick, Robert, Umut Uludag, Alan Mink, Mike Indovina, and Anil Jain. ”Large-scale evaluation of multimodal biometric authentication using state-of-the-art systems.” IEEE transactions on pattern analysis and machine intelligence 27, no. 3 (2005): 450-455.

[12] Ribaric, Slobodan, and Ivan Fratric. ”A biometric identification system based on eigenpalm and eigenfinger features.” IEEE transactions on pattern analysis and machine intelligence 27, no. 11 (2005): 1698-1709.

[13] Monwar, Md Maruf, and Marina L. Gavrilova. ”Multimodal biometric system using rank-level fusion approach.” IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics) 39, no. 4 (2009): 867-878.

[14] Nagajyothi, Grande, et al. ”High-Speed Low Area 2D FIR Filter Using Vedic Multiplier.” Proceedings of Third International Conference on Advances in Computer Engineering and Communication Systems: ICACECS 2022. Singapore: Springer Nature Singapore, 2023

[15] Ma, Debbie S., Joshua Correll, and Bernd Wittenbrink. ”The Chicago face database: A free stimulus set of faces and norming data.” Behavior research methods 47 (2015): 1122-1135.

[16] Ma, Debbie S., Justin Kantner, and Bernd Wittenbrink. ”Chicago face database: Multiracial expansion.” Behavior Research Methods 53 (2021): 1289-1300.

[17] Lakshmi, Anjana, Bernd Wittenbrink, Joshua Correll, and Debbie S. Ma. ”The India Face Set: International and cultural boundaries impact face impressions and perceptions of category membership.” Frontiers in psychology 12 (2021): 627678.

[18] C. Sarada, V. Dattatreya and K. V. Lakshmi, ”Deep Learning based Breast Image Classification Study for Cancer Detection,” 2023 IEEE International Conference on Integrated Circuits and Communication Systems (ICICACS), Raichur, India, 2023, pp. 01-08

[19] Shehu, Yahaya Isah, Ariel Ruiz-Garcia, Vasile Palade, and Anne James. ”Sokoto coventry fingerprint dataset.” arXiv preprint arXiv:1807.10609 (2018).

[20] C. Ch.Sarada, K. V. . Lakshmi, and M. . Padmavathamma, “MLO Mammogram Pectoral Masking with Ensemble of MSER and Slope Edge Detection and Extensive Pre-Processing”, IJRITCC, vol. 11, no. 3, pp. 135–144, Apr. 2023.

[21] Tripathi, Shashank, Jay Murgi, Kalpana Rai3 Sneha Soni, and Rajdeep Singh. ”A literature survey on multi model bio-metric system.” J. Comput. Technol 10 (2021): 1-5.

[22] Wang, Zijie J., Robert Turko, Omar Shaikh, Haekyu Park, Nilaksh Das, Fred Hohman, Minsuk Kahng, and Duen Horng Polo Chau. ”CNN explainer: learning convolutional neural networks with interactive visualization.” IEEE Transactions on Visualization and Computer Graphics 27, no. 2 (2020): 1396-1406.

[23] Villavisanis, Dillan F., Clifford I. Workman, Daniel Y. Cho, Zachary D. Zapatero, Connor S. Wagner, Jessica D. Blum, Scott P. Bartlett, Jordan W. Swanson, Anjan Chatterjee, and Jesse A. Taylor. ”Associations of facial proportionality, attractiveness, and character traits.” Journal of Craniofacial Surgery 33, no. 5 (2022): 1431-1435.

[24] Saboune, Farah Mohamad Farouk. ”Virtual Reality in Social media marketing will be the new model of advertising and monetization.” In 2022 Ninth International Conference on Social Networks Analysis, Management and Security (SNAMS), pp. 1-7. IEEE, 2022.

[25] Cooney, Ciaran, Raffaella Folli, and Damien Coyle. ”A bimodal deep learning architecture for EEG-fNIRS decoding of overt and imagined speech.” IEEE Transactions on Biomedical Engineering 69, no. 6 (2021): 1983-1994.

[26] Muhammad, Khan, Jamil Ahmad, Zhihan Lv, Paolo Bellavista, Po Yang, and Sung Wook Baik. ”Efficient deep CNN-based fire detection and localization in video surveillance applications.” IEEE Transactions on Systems, Man, and Cybernetics: Systems 49, no. 7 (2018): 1419-1434.

[27] Alaskar, Haya, Abir Hussain, Nourah Al-Aseem, Panos Liatsis, and Dhiya Al-Jumeily. ”Application of convolutional neural networks for automated ulcer detection in wireless capsule endoscopy images.” Sensors 19, no. 6 (2019): 1265.

[28] Vinoth Kumar, V., T. Karthikeyan, P. V. Praveen Sundar, G. Magesh, and J. M. Balajee. ”A quantum approach in lifi security

using quantum key distribution." International Journal of Advanced Science and Technology 29 (2020): 2345-2354.

[29] Mehmood, Asif, and Bishwas Mishra. "A Survey on Various Unimodal Biometric Techniques." Sparklinglight Transactions on Artificial Intelligence and Quantum Computing (STAIQC) 1, no. 1 (2021): 23-35.

[30] Sumalatha, Veluru. "A Study of Fingerprint Patterns in Type II Diabetes." PhD diss., Rajiv Gandhi University of Health Sciences (India), 2017.

[31] Phung, Van Hiep, and Eun Joo Rhee. "A high-accuracy model average ensemble of convolutional neural networks for classification of cloud image patches on small datasets." Applied Sciences 9, no. 21 (2019): 4500.

[32] NagaJyothi, Grande, and Sriadibhatla SriDevi. "Distributed arithmetic architectures for fir filters-a comparative review." In 2017 International conference on wireless communications, signal processing and networking (WiSPNET), pp. 2684-2690. IEEE, 2017.

[33] Rukhiran, Meennapa, Sethapong Wong-In, and Paniti Netinant. "IoT-Based Biometric Recognition Systems in Education for Identity Verification Services: Quality Assessment Approach." IEEE Access 11 (2023): 22767-22787.

[34] Kumar, V. Vinoth, KM Karthick Raghunath, N. Rajesh, Muthukumaran Venkatesan, Rose Bindu Joseph, and N. Thillaiarasu. "Paddy plant disease recognition, risk analysis, and classification using deep convolution neuro-fuzzy network." Journal of Mobile Multimedia (2022): 325-348.

[35] S. T. Ahmed, V. V. Kumar, and J. Kim, "AITel: eHealth Augmented-Intelligence-Based Telemedicine Resource Recommendation Framework for IoT Devices in Smart Cities." IEEE Internet of Things, vol. 10, no. 21, pp. 18461-18468, 1 Nov, 2023, .

Edited by: Polinpapilinho Katina
Special issue on: Scalable Dew Computing for Future Generation IoT systems
Received: Aug 19, 2023
Accepted: Nov 9, 2023