Original Article

Hybrid Biometric Based Person Identification Using Machine Learning

Venkata Ramana N[1], Dr.S. Anu H Nair[2], Dr.K.P. Sanal Kumar[3]

[1]Research scholar, Department of CSE, Annamalai University, Chidambaram, India
[2]Department of CSE, Annamalai University, Chidambaram, India (Deputed to WPT, Chennai)
[3] PG Department of Computer Science, R. V. Government Arts College, Chengalpattu, India
E-Mail:[1]ramana.9n@gmail.com, [2]anu_jul@yahoo.co.in, [3]sanalprabha@yahoo.co.in
DOI: 10.47750/pnr.2022.13.S08.195

Abstract

When compared to the more traditional methods of authentication, biometric systems offer a much higher level of protection for a wide range of uses (like pin, passwords etc.). Various sectors of modern society can find use for biometric systems. Among these are authentication for computers, attendance tracking for businesses, financial transactions, safeguarding private information, securing access to buildings, and ensuring the safety of travellers at airports. Identifying and verifying individuals via their unique physical and behavioural characteristics is the primary function of the biometric system. Importance of biometric systems in modern society is analysed in this paper. Single-trait biometric user recognition is currently used, but it does not offer sufficient security for critical programmes. Multimodal biometric systems are used to get around these issues. Physical and behavioural characteristics, like fingerprints and DNA, signatures and fingerprints, etc., are all part of a multimodal biometric system's arsenal for authenticating users. In addition to the hard biometric features already mentioned (skin colour, age, height, hair colour, eye colour, gender, etc.), the use of a person's soft biometric traits is becoming increasingly common. While soft biometrics can be used to boost the efficiency of biometric systems that focus on other characteristics, they are not without their own set of drawbacks, such as a lack of permanence and distinctive behaviour. User authentication, security, and performance are all boosted by the work presented in this paper using Machine learning (F-SVM -Fuzzy-Support Vector Machine) model.

Keywords: Biometric, Machine learning, SVM, DNA, FACE.

1. INTRODUCTION

Everyday people in today's digital world are on the lookout for new methods of increasing their personal security, methods which must be more reliable and accurate if they are to be adopted widely. Authenticating a user before granting them access to their files is a routine task for everyone. Applications used for this purpose should restrict access to the data to only those who are authorised to view it. Biometrics is a new system that uses biological characteristics to provide a very high level of security. Biometrics is a method of identification that relies on a person's unique physiological and behavioural traits. This method can be used to help you figure out who you are talking about and what you need to know about them. To protect one's privacy in today's connected world, it's crucial to use a personal authentication method. A certain amount of safety is needed for personal authentication. Any of the three methods presented are viable options for ensuring one's own safety.

- At the ownership level of security, the user gains access to a resource after creating the evidence of ownership. Case in point: a locker key.
- Accessing information at the "Specialized Knowledge" level requires the user to recall a secret phrase or phrase. A username and password are two such examples.
- For authentication at the biometrics level, the user's specific physiological and behavioural characteristics are used.

Examples include fingerprints, retina scans, and keystrokes. Using multiple layers of authentication can improve the efficiency of the whole process. The first two layers of security have many drawbacks and difficulties despite their widespread adoption. Hence, it is possible to misplace the key or forget the passphrase. The first two tiers make use of temporary, unnatural properties because of human error. It's obviously very challenging for the

user to keep track of their possessions at the first two levels, so they're not permanent. However, in the third level, authentication is based on the individual's distinct traits, making forgery impossible. Figure 1 displays some common examples of biometric characteristics. Here The justifications listed below highlight how crucial a biometrics-based authentication system is:

- Biometric data is secure and cannot be lost or destroyed.
- Human physical existence is required for feature access.
- Characteristics of the human body are highly individual.

Ke3y characteristics of biometric features are as follows:

- Individuality: Each person needs their own unique set of characteristics that are associated with their biometric modality.
- Permanent availability; the biometric characteristic must be present in every living person.
- The trait you choose for your deception must be difficult to fake.
- The biometric characteristic must be easily obtained using a sensor, and this implies that it is attainable.
- The biometric feature must be permanent throughout a person's life for it to be used.
- For the biometric trait to be considered "permissible," society must readily accept it.
- The success criterion is that the trait's human-recognition accuracy meets all of the requirements set forth in the applications.

Using these seven criteria, Table 1 below compares and contrasts the various physiological and behavioural biometric techniques. The highest value for an attribute is 1, the next highest value is 2, and the lowest value is 3 in the table.

Table 1 . the range of biometric properties (Three for "low," two for "medium," and one for "high" describe)

Biometrics	Universality	Ubiquity	Durability	Obtainable	Accomplishm	Permissibility	Deception
Face	1	3	2	1	3	1	3
Finger print	2	1	1	2	1	2	1
Hand geometry	2	2	2	1	2	2	2
Keystrokes	3	3	3	2	3	2	2
Hand veins	2	2	2	2	2	2	1
Iris	1	1	1	2	1	3	1
Retinal scan	1	1	2	3	1	3	1
Signature	3	3	3	1	3	1	3
Facial thermograph	1	1	3	1	2	1	1
Odor	1	1	1	3	3	2	3
DNA	1	1	1	3	1	3	3
Gait	2	3	3	1	3	1	2
Ear Canal	2	2	3	2	2	1	2

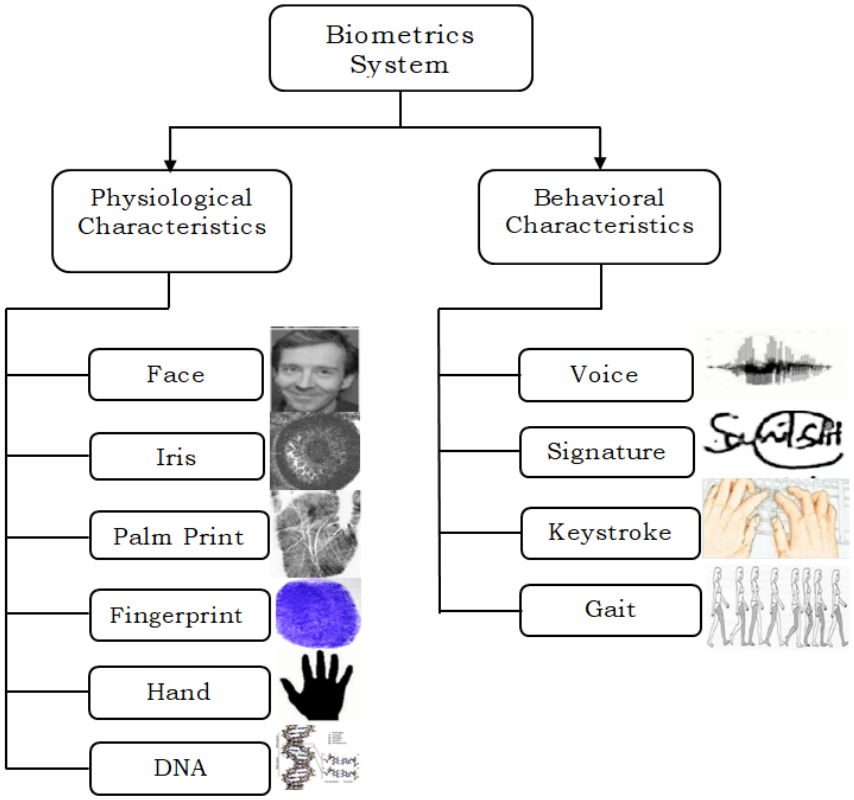

Figure 1. Biological Characteristics; Characteristics

2. LITERATURE SURVEY

For the biometric cryptosystem based on polynomials, [8] a safeguard method has been developed. The biometric data is transformed into Eigen spaces after being subjected to a Gabor filter for pattern extraction, and the mined features are transformed using a Karhunen Loeve (K-L) transform. Projections are made using the transformed features and the randomly generated points, with the help of a polynomial obtained from the key. The ordered sets are made up of both the points and their equivalent projections. A fuzzy vault is formed by connecting ordered sets and chaff points. At decryption time, matching scores are determined by comparing the claimed biometric features to those that were initially deposited. If there are more than a certain number of matched values, then the decoding was successful. The accuracy is tested using three different biometric identifiers: the finger, the palm, and the iris. Fingerprint and palm print security systems [9] have been presented as a model. The features are extracted using a Gabor filter. Using feature level fusion, fingerprint and palm print features are combined into a single biometric. The hammering distance is used for recognition. A multi-biometric system based on fingerprints and ear scans [10] has been developed. To start, an adaptive median filter is applied to both biometric images to get rid of unwanted noise. Fingerprint images are parsed for minute details. The ear image is processed before being fed into an Active Appearance Model (AAM) to mine features. Chaff points are added, and two features are grouped together. The fuzzy vault is built by combining the clustered feature points and the secret key. When verifying a user, we compare their query features to those stored in the safe to determine their identity.

[11] creates a multimodal biometric template security system with a fuzzy vault. Images of fingerprints and irises undergo histogram equalisation as part of the preprocessing stage. Then, the thirteen minute details are extracted, blended, and projected. The projected features and cryptographic key are used to create the fuzzy vault. Features of the query are compared to the vault during decoding. The key will be given out if the matching score is lower than the threshold. Bottom-hat filtering, a straightforward and precise method for mining principal lines from palm prints, was introduced in [12]. Normalization, median filtering, average filters along four prefixed directions like 0, 45, 90, 135; grayscale bottom hat filtering; a combination of bottom hat filtering, binarization, and post processing; and so on are all examples of bottom hat filtering. Biometric cryptosystems can be broken down into two distinct categories, key binding and key generation, depending on the type of auxiliary data they use. As part of the key binding strategy, a cryptographic key is appended to the template in order to acquire the auxiliary data. In the key binding method, recovering the key or original biometric template is an arduous task. The key is reconstructed from the auxiliary information using query features during the verification process. The biometric template is used as the only source of information to generate the helper data used to generate the key.

In [13], the authors introduced a fuzzy vault to safeguard biometric templates. The tiniest details have been meticulously prealigned with the help of a guiding reference point. The alignment method is highly secure

and does not reveal any granular details. To prevent being vulnerable to a correlation attack, the finer points of the prealignment process are quantized. The fuzzy vault cryptosystem is used to implement prealigned fingerprint template matching, and its security is examined in light of various attacks. A cancelable palmprint cryptosystem based on a palm hash code in two dimensions has been developed [14].

The alignment matching problem is at the heart of the palmprint texture encoding challenge. Row-alone and row-co-occurrence fuzzy vaults are related to cancelable palmprint and palmprint texture codes, respectively. 2DPHC Fuzzy Vault is more resistant to brute force, multiple template, key inversion, and heterogeneity attacks. In [15], a process for preparing fingerprint images for use is described. Discrete Fourier Transform (DFT) and histogram equalisation techniques are used to increase the contrast of images. We see progress with the DFT approach. Fuzzy based approach is utilised for securing biometric template by the authors [16]. Features of fingerprint and hand geometry are combined to reduce the spoof attacks on biometric systems. Since biometric templates were kept safe throughout the feature fusion simulation process, the results are encouraging. Equal Error Rate (EER) of 3.3% and improved GAR of 97.3% are both positive indicators of the multi biometric scheme's enhanced performance. Multiple biometric features have been presented in [17] as a template protection method. Preprocessing, feature extraction, feature grouping, feature fusion, and fuzzy vault generation are the five main steps involved. In order to improve performance and pinpoint chaff points, Particle Swarm Optimization (PSO) is used.

3. PROPOSED MODEL

To differentiate between a genuine user and a fake, biometrics take into account a wide range of personal characteristics, both physical and behavioural. Unimodal biometric systems (those based on a single biometric trait) allow for identification but have drawbacks like a high error rate, non-universality, noise in sensed data, etc. Multimodal methods, which use multiple user characteristics for verification, might be able to solve these issues. The performance, accuracy, and security of a multimodal biometric system are superior to those of a single-modal system. When we introduce matching detection with multimodal biometric, we do so with the hope of using it in highly secure contexts like government and financial institutions. This novel method utilises a multimodal approach to define the matching detection technique (which determines whether the enrolled user is live or not). In this part, we show how integrating DNA and fingerprint biometrics with a matching detection technique can boost security and performance.

Intended Schematic To create a more reliable authentication system, it is common practise to use a combination of two biometric traits, such as DNA and fingerprint, in conjunction with matching detection. Accessibility and safety are both improved with this design. The sensor-level fingerprint matching in this method relies on the perspiration method. The physiological perspiration process varies in time as the fingerprint makes contact with the sensor surface. Most sensors (optical, solid-state sensor, etc.) are affected by things like humidity and temperature changes. The presence of perspiration in a given time domain is indicative of the authenticity of the fingerprint sample presented to the sensor. The proposed multimodal approach also makes use of a FSVM detection technique for another biometric trait, DNA. There are always two steps involved in the biometric verification and identification process. A person must first be enrolled, and then they must be authenticated. In our proposed system, new samples are compared to a database of enrolled samples (shown in Fig. 2) that contains a template of DNA and fingerprint traits. As shown in Fig. 3, the authentication phase begins with a sensor-level application of matching detection to determine whether or not a newly captured sample is alive. The given sample is considered "live" if the features extractor module generates a template from the extracted features and sends it to the matcher module for comparison. Once a match has been made between the template and the matcher, a match score is calculated and sent on to the decision module. The match score is used by the decision modules to reach a conclusion. Our cutting-edge method currently employs a fusion of decision-making levels. Fusion is the process of combining the outcomes of both methods into a single output, as shown in table 2. Each and every component of the given architecture model is defined by the given approach's algorithm, which is as follows:

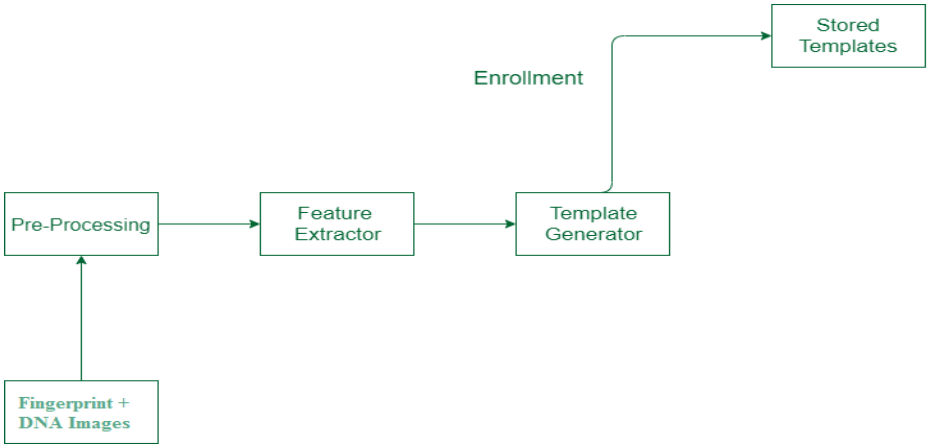

Figure 2. Enrolment Phase

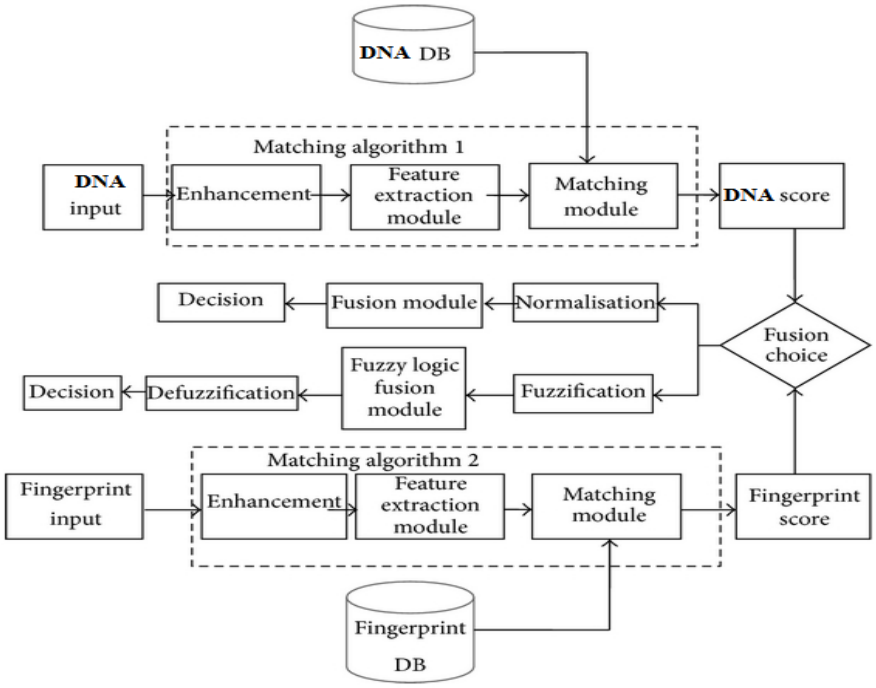

Figure 3. Authentications Phase

Methodology for multimodal biometric authentication with an FSVM algorithm
Step1: DNA and fingerprint samples are presented to the different sensors.
Step2: Matching is checked at sensor level for both modalities

- Fingerprint sample matching is checked by the sensor itself by sensing perspiration.
- DNA matching is checked by capturing user response of eye blinking and smiling DNA through the web camera.

Step3: If both input samples are live then

- Sample sends to feature extractor module Else
- Fake user samples

Step4: Feature extractor modules generate templates individually by extracting their feature set and template send to matcher modules.
Step5: Both matchers match the receiving templates with stored templates in Enrollment phase and generate match score which is a basis for taking a decision by decision module
Step6: Both decision level modules compare match score with the threshold value and provide results for fusion.
If match scores >= threshold value Then Real user
Else Fake user End
Step7: The important thing in this approach is fusion which is done on the results of decision module. Fusion combines decision of both approach and decides whether the person is authorized or not
according to these steps:

- Recognition of person with high threshold value IF fdmr=real AND fcdmr=real THEN Recognize authorized user

ELSE

Recognize unauthorized user

- Recognition of person with normal threshold value

IF fdmr=real AND fcdmr=real OR fdmr=real AND fcdmr=fake OR fdmr= fake AND fcdmr=real THEN

Recognize authorized user ELSE

Recognize unauthorized user

Step8: End

3.1. METHODOLOGY

3.1.1. DATA ACQUISITION

The first stage of any biometric authentication system is the collection of images. Digital cameras, fingerprint scanners, video cameras, low and high resolution cameras, and many others can all be used to obtain the FDNA. Depending on the task at hand, choose a camera. Because of their slow acquisition and subpar image quality, digital cameras aren't a good choice for capturing FDNA samples. For this reason, it is not suitable for use in the here and now. Images with a high resolution are used for forensic purposes while low resolution images are used in commercial settings.

3.1.2. PREPROCESSING

In preprocessing, we eliminate superfluous information, fix distortions, align FDNAs, and crop the region of interest (ROI). Procedures that come before the actual processing are as follows:

- Filtering: use a filter to get rid of the background noise
  - Binarization: use a thresholding technique to change the image into binary form.
  - Boundary tracing: following the FDNA's border to identify significant nodes
- The first step is locating the key points, which can be done with a tangent-based or finger-based method.
  - Define a reference frame for the coordinates: Learn where to cut the FDNA picture and in what orientation.
- First, identify the region of interest (ROI) and then take out the core of the FDNA.

Because of its comprehensive coverage of the FDNA and its one-of-a-kind structure for each individual, the FDNA's central region is used as ROI in numerous systems. There are a number of different approaches that can be used to extract ROIs. To get to the ROI, the central region of the FDNA is oriented and aligned. The FDNA can be oriented in a number of different ways, including the elliptical method, bisector method, and tangent based method.

3.1.3. INFORMATION EXTRACTION BASED ON FEATURES

The features extracted from the ROI will be cropped from the image. We use edge detectors and the FDNA magnitude in our line-based method. In the subspace technique, the coefficient is used as a metric. Principal Component Analysis, Latent Dirichlet Allocation, and Independent Component Analysis are all good examples. A statistical method's efficacy can be improved by taking into account both regional and international factors. Gabor filters are used in the encoding method to obtain phase information on a local scale. shown in figure 3 and figure 4.

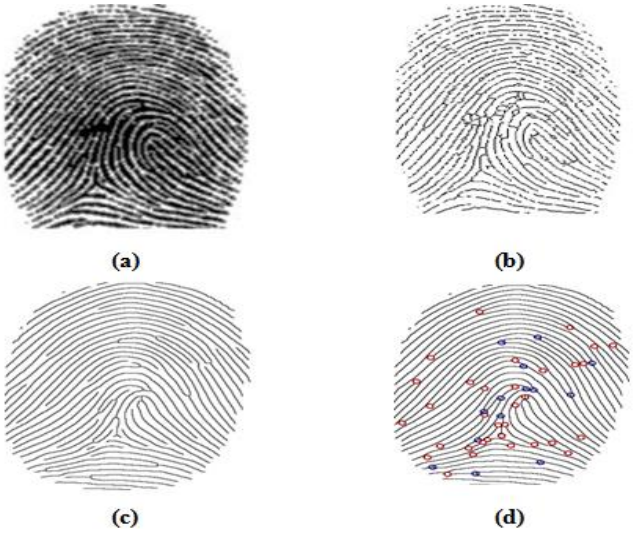

Fig 3: Extraction of Feature from Fingerprint ((a) Preprocessed image (b) After thinning (c) After morphological operation (d) Extracted features)

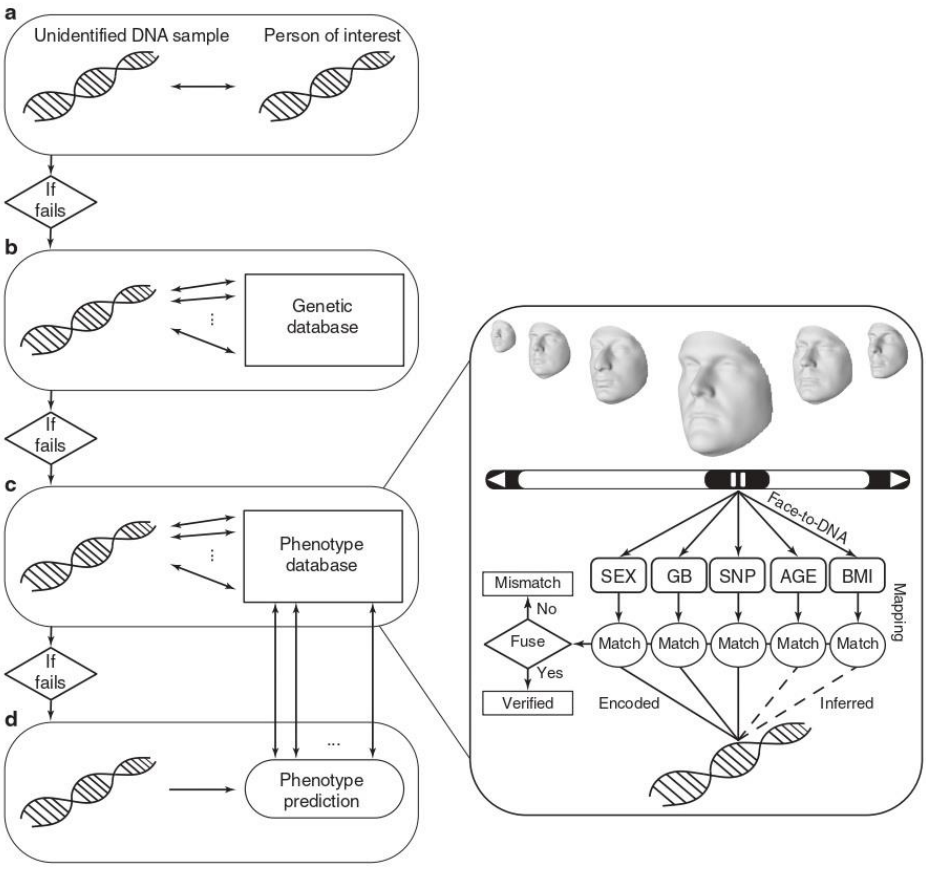

Fig 4: Flowchart of the proposed paradigm in the context of current DNA investigational tools

(a. The initial step in attempting to identify a person from an unidentified DNA sample is to compare it to a database of known DNA samples, b. If a match cannot be made, the same unidentified DNA sample is compared to the genetic profiles of people whose identities are already known, c. If there is another identification problem, our method may be useful. Each face-to-DNA classifier uses a phenotype database to pair a given face with a specific DNA probe based on a number of molecular features, such as sex, genomic background (GB), SNPs, age, and BMI. It is now possible to confirm or reject a DNA profile against a known face by fusing together multiple, per-aspect matching scores to provide an overall score, d. DNA phenotyping could also be used to compare predicted and observed traits, but this would likely just be a last resort before resorting to showing the results to the public in the hopes that someone will recognise the person. However, this capability has not yet been reached with the current state of DNA phenotyping.)

3.1.4. CLASSIFICATION

Functionalities of FDNA are extracted and then stored in a database template following feature extraction. There's something special about each individual template. When an image is submitted as a query for verification or authentication, its features are compared to those in the template. Threshold-based matching scores are used to make the final call on whether or not to accept the image for authentication. To complete the classification process, FSVM Classifiers are created based on the use of similarity, Mahalanobis, Euclidean, and Manhattan distances.

Table 2: The Result of an Intentional Fusion Attempt

Finger Decision Module Result	DNA Decision Module Result	Final Result
Real	Real	Authorized
Real	Fake	Unauthorized
Fake	Real	Unauthorized
Fake	Fake	Unauthorized

The fusion results for the high threshold value are shown in Table 2. If the output of both traits decision modules is "real," the application will treat the user as authorised; otherwise, it will identify them as an unauthorised user and return an appropriate error message. Consequently, this tactic is suitable for highly secure contexts like banking and the military.

The Gains from a More Thoughtful Strategy:

- It is simple to implement the planned multimodal biometric strategy for user authentication. An algorithm is used to detect a match between the DNA and the fingerprint, and then the two sets of data are combined.
- Due to matching detection, the time it took for a fraudulent user to provide a fake trait to the intended multimodal biometric system was reduced. It is important to note that the proposed system does not perform sensor-level authentication of the fraud user through matching detection.
- The intended multimodal biometric approach is more efficient than the traditional single-modal biometric system in a number of ways. When compared to other traits, DNA and fingerprinting are particularly sturdy.
- Safer: The multimodal biometric approach was designed to prevent spoofing, making the system safer overall.
- Using multiple traits for identification, the targeted multimodal biometric approach ensures low false alarm rates and false reject rates, as well as high accuracy.
- The only drawback of the intended multimodal biometric approach is its relative expense; the approach uses a device for matching detection for DNA recognition and fingerprint trait.

4. RESULT AND DISCUSSION

4.1. DATABASE:

DNA and fingerprints are used in a multimodal biometric system for authentication purposes. We used the publicly accessible Indian DNA database, which includes a collection of DNA images captured on the IIT Kanpur campus, for DNA recognition. All the pictures were taken with the subjects standing tall and looking directly into the camera. The data is stored as JPEGs. Each image is 640 pixels wide by 480 pixels high, and it has 256 shades of grey. The CASIA Fingerprint Image Database, Version 5.0, is used for fingerprinting, and it contains 20,000 fingerprint scans from 500 individuals. All 328x356 pixel fingerprint images are stored as 8-bit grayscale BMP files.

B) A LOOK AT THE STRENGTHS AND WEAKNESSES OF MULTIMODAL BIOMETRIC SYSTEMS COMPARED TO THOSE OF A SINGLE BIOMETRIC MODALITY

Improvements in False Acceptance Rate (FAR), False Rejection Rate (FRR), and Accuracy can be seen when using the intended multimodal biometric system. DNA unimodal, fingerprint unimodal, and the intended DNA and fingerprint multimodal biometric system are all evaluated using the FAR and FRR. The FAR and FRR of the intended multimodal system are shown in Table 3. The point where these two curves intersect is the equivalent effectiveness ratio (EER), which also serves as the intended multimodal system's threshold.

Table 3. Examining the effectiveness of the planned multimodal biometric system

System	FAR	FRR	Accuracy
Face	10%	11%	90.65%
Fingerprint	15%	15%	85%

Purposed System (DNA +Fingerprint)	2.25%	1.75%	99%

Fusion results at the typical threshold value are displayed in Table 3. This tactic can be used for software where the priority is on convenience rather than safety. This method can be used for any company's attendance tracking if the outcomes needed to pass a predetermined benchmark.

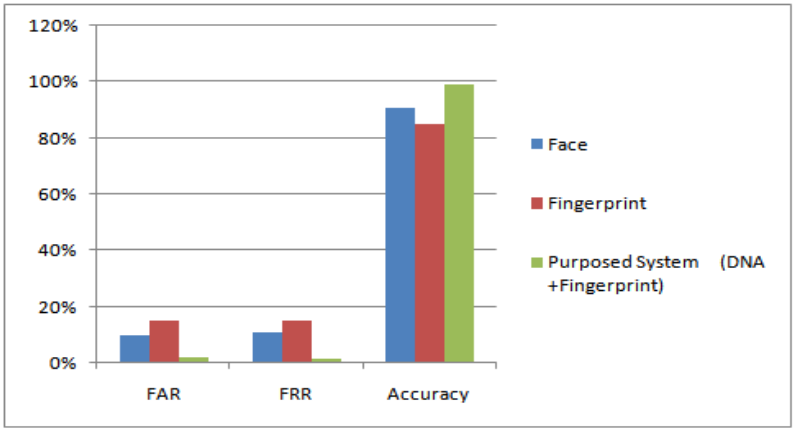

Figure 6. Evaluation of the planned multimodal biometric system by graphical representation

The evaluation of the planned multimodal system is depicted in table 3 and figures 6. The experimental results demonstrate that the multimodal system not only improves upon the accuracy of the individual unimodal systems (to the tune of 96%) but also reduces their error rates (both FAR and FRR). As a result, a FSVM based multimodal biometric system serves the purpose intended more effectively than a unimodal one.

5. CONCLUSION

This part explains how combining DNA and fingerprint biometric traits can strengthen the safety of a biometric system. Similarly, the purposeful method employs matching detection to determine whether or not the specified user is actually present by using FSVM model. Traits like DNA and fingerprints are collected and then checked for a match. If the user is online, the algorithm continues; if not, an invalid or unwelcome one is identified. In the following part, we will see yet another strategy for enhancing the efficiency and safety of biometric systems, this time by incorporating DNA and iris with a soft biometric trait (eye colour).

REFERENCES

1. D. Jyotishi and S. Dandapat, "An ECG Biometric System Using Hierarchical LSTM With Attention Mechanism," in IEEE Sensors Journal, vol. 22, no. 6, pp. 6052-6061, 15 March15, 2022.
2. S. B. Abdullahi et al., "Biometric Information Recognition Using Artificial Intelligence Algorithms: A Performance Comparison," in IEEE Access, vol. 10, pp. 49167-49183, 2022.
3. J. E. Tapia, S. Gonzalez and C. Busch, "Iris Liveness Detection Using a Cascade of Dedicated Deep Learning Networks," in IEEE Transactions on Information Forensics and Security, vol. 17, pp. 42-52, 2022.
4. B. Fatimah, P. Singh, A. Singhal and R. B. Pachori, "Biometric Identification From ECG Signals Using Fourier Decomposition and Machine Learning," in IEEE Transactions on Instrumentation and Measurement, vol. 71, pp. 1-9, 2022, Art no. 4008209.
5. C. Yuan, S. Jiao, X. Sun and Q. M. J. Wu, "MFFFLD: A Multimodal-Feature-Fusion-Based Fingerprint Liveness Detection," in IEEE Transactions on Cognitive and Developmental Systems, vol. 14, no. 2, pp. 648-661, June 2022.
6. M. Hamza, S. Tehsin, H. Karamti and N. S. Alghamdi, "Generation and Detection of Face Morphing Attacks," in IEEE Access, vol. 10, pp. 72557-72576, 2022.
7. D. Girardi, F. Lanubile, N. Novielli and A. Serebrenik, "Emotions and Perceived Productivity of Software Developers at the Workplace," in IEEE Transactions on Software Engineering, vol. 48, no. 9, pp. 3326-3341, 1 Sept. 2022.
8. L. Fei, B. Zhang, Y. Xu, C. Tian, I. Rida and D. Zhang, "Jointly Heterogeneous Palmprint Discriminant Feature Learning," in IEEE Transactions on Neural Networks and Learning Systems, vol. 33, no. 9, pp. 4979-4990, Sept. 2022.
9. H. Geng, Z. Huan, J. Liang, Z. Hou, S. Lv and Y. Wang, "Segmentation and Recognition Model for Complex Action Sequences," in IEEE Sensors Journal, vol. 22, no. 5, pp. 4347-4358, 1 March1, 2022.
10. H. Khalifa, N. A. Zaher, A. S. Abdallah and M. W. Fakhr, "Convolutional Neural Network Based on Diverse Gabor Filters for Deepfake Recognition," in IEEE Access, vol. 10, pp. 22678-22686, 2022.
11. Y. Zhang, M. Liu, F. Yu, T. Zeng and Y. Wang, "An O-Shape Neural Network With Attention Modules to Detect Junctions in Biomedical Images Without Segmentation," in IEEE Journal of Biomedical and Health Informatics, vol. 26, no. 2, pp. 774-785, Feb. 2022.
12. G. Mahfoudi, F. Retraint, F. Morain-Nicolier and M. M. Pic, "Statistical H.264 Double Compression Detection Method Based on DCT Coefficients," in IEEE Access, vol. 10, pp. 4271-4283, 2022.
13. J. Meng, W. -S. Zheng, J. -H. Lai and L. Wang, "Deep Graph Metric Learning for Weakly Supervised Person Re-Identification," in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 44, no. 10, pp. 6074-6093, 1 Oct. 2022.
14. Z. Wei, X. Yang, N. Wang and X. Gao, "RBDF: Reciprocal Bidirectional Framework for Visible Infrared Person Reidentification," in IEEE Transactions on Cybernetics, vol. 52, no. 10, pp. 10988-10998, Oct. 2022.

15. J. Miao, Y. Wu and Y. Yang, "Identifying Visible Parts via Pose Estimation for Occluded Person Re-Identification," in IEEE Transactions on Neural Networks and Learning Systems, vol. 33, no. 9, pp. 4624-4634, Sept. 2022.
16. K. Rzecki and M. Baran, "Application of Elastic Shape Analysis to User Authentication and Identification," in IEEE Transactions on Emerging Topics in Computing, vol. 10, no. 2, pp. 1157-1165, 1 April-June 2022.
17. G. Li and H. Sato, "Sensing In-Air Signature Motions Using Smartwatch: A High-Precision Approach of Behavioral Authentication," in IEEE Access, vol. 10, pp. 57865-57879, 2022.