Multimodal Image Fusion in Biometric Authentication

Uma Maheshwari[*1], Kalpanaka Silingam[2]

[1,2]Hindusthan Institute of Technology, Coimbatore, India

Email: umamaheshwari@hit.edu.in[1] ; kalpanakasilingam81@gmail.com[2]

Abstract

During this study, a unique multimodal biometric system was constructed. This system incorporated a variety of unimodal biometric inputs, including fingerprints, palmprints, knuckle prints, and retina images. The multimodal system generated the fused template via feature-level fusion, which combined several different biometric characteristics. The Gabor filter extracted the features from the various biometric aspects. The fusion of the extracted information from the fingerprint, knuckle print, palmprint, and retina into a single template, which was then saved in the database for authentication, resulted in a reduction in both the spatial and temporal complexity of the process. A novel technique for safeguarding fingerprint privacy has been developed to contribute to the study. This system integrates the unique fingerprints of the thumb, index finger, and middle finger into a single new template. It was suggested that the Fixed-Size Template (FEFST) technique may be used might develop a novel strategy for the extraction of fingerprint features. From each of the fingerprints, the minute locations of the ridge end and ridge bifurcations as well as their orientations relative to the reference points were retrieved. The primary template was derived from the fingerprint that included the greatest number of ridge ends. For the purpose of generating the combined minutiae template, the templates of the other two fingerprints were incorporated into this template. The merged minutiae template that was developed was then saved in a database so that registration could take place. During the authentication process, the system received the three query fingerprints, and those fingerprints were compared to the previously saved template.

Keywords: wavelet-based image fusion; sum absolute difference; hazy images; Kalman filter.

1. Introduction

The method of identifying humans in a one-of-a-kind manner based on their physiological or behavioral features is known as biometrics. Physiological features are either directly or indirectly inferred by a person's genes and may or may not be modified by their surroundings. [1] Other behavioral characteristics include cognitive biometrics. The use of biometrics ensures safety by providing additional verification and identification options. Verification refers to the process of determining how an individual may be specifically recognized by analyzing one or more differentiating biological characteristics. It performs a comparison of 1:1 matching and confirms a claimed identity using a single template, while identification is performed using 1:N matching, which implies that numerous comparisons are conducted by validating an input template with the whole database in order to determine a person's true identity. It takes more time since it checks with the complete database, and it has the characteristics of a centralized database in nature, such as being static, high-risk, covert, and physiological. Traditional means of identifying a person may be broken down into two categories: those that involve something you know, like a password or a PIN, and those that use something you have, like a key, a smart card, or a token. However, a biometric identify a person based on one of their physical characteristics. Traditional measures such as having anything in your possession or using knowledge-based ways might be readily guessed by fraudsters

Doi: https://doi.org/10.54216/FPA.010203
Received: February 14, 2020 Accepted: April 18, 2020

due to the fact that around one-quarter of individuals seem to write their PIN on their ATM card, in addition to other considerations. It is estimated that yearly identity fraud losses in the United States alone amount to $3 billion in fraudulent ATM withdrawals, $1 billion in fraudulent credit card transactions, and $1 billion in illicit [2] usage of cellular phones.

Figure 1: Database Images

The poll that was just presented makes it very clear that the direction of future developments will be determined by biometric technology, as well as the relevance of this developing field in relation to the rest of the globe. Even while numerous security [3] systems make use of biometric technology, there is not a single biometrical characteristic that can fulfill all of the performance criteria that are necessary for practical systems. In order to increase the degree of security present in identification and verification systems on numerous fronts, multimodal biometric technology has been developed and implemented. There is a pressing need for the development of enhanced algorithms for human recognition, in addition to the creation of fresh paradigms and protocols. A multimodal biometric system is one that incorporates more than two different biometric identifiers in order to increase the system's overall performance. The usage of a certain biometric identification is contingent on a number of characteristics, including universality, permanence, one-of-a-kindness, measurability, performance, circumvention, collectability, acceptability, and the requirements of the situation. These kinds of traits are referred to as biometrics [4].

1.1 Application

It may be used for everything from simple day-to-day tasks to more complex border-crossing applications. Having faith in the reliability of these electronic transactions is critical to the sustained expansion of the global economy. The use of biometrics, [5] either on its own or in conjunction with other technologies such as smart cards, encryption keys, and digital signatures, is destined to become ubiquitous in almost every facet of the economy as well as our everyday lives. Authenticating a person's identity via the use of biometric data is becoming not only more practical but also noticeably more accurate than conventional approaches. It is possible to use it for verification and identification in several modes.

1.2 Needs of study

Emerging technologies like biometrics have great potential as security solutions, and they will play an important role in the effort to keep the globe secure. Utilizing IDs that are based on biometric characteristics may help to enhance access control in sensitive locations. The traditional means of identification, such as using a password, are plagued by the problem of easily forgotten words, and the cost that is incurred each year as a result of forgotten or hacked passwords [6] is quite

Doi: https://doi.org/10.54216/FPA.010203
Received: February 14, 2020 Accepted: April 18, 2020

significant. Therefore, there is a very strong demand for various types of security systems. A multimodal biometric system is required in order to alleviate issues with conventional biometric systems and unimodal biometric systems. In addition, there are no restrictions placed on the apps' scopes. It is possible to deploy it in everything from home access devices to equipment that crosses borders fraudulently. The procedure of doing this study is broken down into many steps, including preprocessing, matching, fusion, normalization, and optimization. The need for the procedures that are used at each step will be discussed in the next paragraph. The database template is kept inside the system, where it may be accessed in order to serve as verification input. The database is compiled using data from a number of sensors, which allows the picture to be preprocessed before the matching process. Localization and normalizing are the two procedures that make up the preprocessing processes for images.

The preprocessing steps for each biometric characteristic are executed in a unique manner. Iris, Finger Print, and Finger Vein Analysis are Combined in This Research Work Iris, Finger Print, and Finger Vein Analysis are Combined in This Research Work Each of the three distinct characteristics calls for a unique approach to the preprocessing stage [7]. The three distinct characteristics each have their own matching method that has been implemented. The recognition system is responsible for generating the scores. Fusion approaches play a crucial part in boosting precision. Different scores may be derived from each biometric characteristic. After the scores have been normalized, they need to be combined. The score is made uniform by the process of normalization, which also prepares the score for fusion. The accuracy and performance of the system may both be improved thanks to normalization's contributions. For the purpose of fusion, a strategy that combines the Genetic Algorithm and Particle Swarm Optimization is utilized to achieve strong authentication systems. A literature review, an understanding of the contributions made by a variety of writers, and a significant amount of work are put out in order to determine where the next generation is and what the world requires from technology. In this area, current research trends are assessed, and the suggested work is planned in accordance with those findings. At each and every level of this research project, the ideas and procedures that are used are geared toward the development of an innovative authentication system that improves accuracy, security, robustness, and reliability. Metrics such as False Acceptance Rate, False Rejection Rate, Equal Error Rate, and Accuracy are used in the performance evaluation process. The SDUMLA-HMT Database provides an assessment of this body of research. It is a chimeric database, which indicates that all of the multimodal biometric features came from the same 106 people as the genuine database.

2 Related Work

After resizing and rotating the picture to compensate for the deviations of hand, [8] retrieved geometrical characteristics from the image. For the purpose of authentication, [9] employed hierarchical characteristics that incorporate both geometries (the length and breadth of fingers) and form (the length of fingertip areas and their locations) in various proportions. It is necessary to separate the fingers from one another in order to get a whole hand form. For the purpose of hand alignment, landmark points, such as fingertip points and valley points, are used rather than guiding pins. After drawing the contour and locating the minimum and maximum points, the next step is to locate the reference point, which is the midpoint of the line that joins the second and third valley points, and the reference axis. Landmark points may then be acquired (line joining the middle fingertip and reference point). The alignment of hand photographs with varying attitudes is accomplished by tilting the reference axis vertically. The influence of differences in hand location is reduced in their technique, which also has the advantages of being more practical and user-friendly [10]. As feature vectors, the lengths of five fingers, the widths of four fingers at two different locations, and the shapes of three different areas of the middle fingertip are employed. The implementation of hierarchical recognition consists of splitting all of the retrieved characteristics into two groups.

In the [11], an ellipse was first utilized to approximate the binarized form of the hand, and then the moments of the binary hand were used to determine which ellipse was the best match. The rotation of the hand is determined by the angle formed by the main axis of this ellipse. After that, geometrical features are calculated using the aligned contour as a starting point. The acquired

Doi: https://doi.org/10.54216/FPA.010203
Received: February 14, 2020 Accepted: April 18, 2020

picture was preprocessed by [12] who did so by transforming the colored image into a binary image. The MATLAB function known as 'in the filter' is used to eliminate noise that is caused by the effects of lightning in the background. The widths of the fingers (the widths of the first four fingers are measured at three different points, and the width of the thumb is measured at two different points), the heights of all of the fingers and the thumb, and two different measurements of palm size are used to compute the feature vector.

[13] retrieved fifteen attributes of users' right hands, some of which include the diameter, area, and breadth of the users' fingers. The database has 500 photographs at a resolution of 120 dpi, each depicting one of fifty different persons. A threshold value of 0.25 is used during the conversion of grayscale pictures to binary images. In order to get rid of noise, morphological procedures and filtering are carried out, and a canny edge detector is used to locate contour. Finding valley points is the initial step in the process of extracting feature points. The characteristics of seven of each person's photographs are utilized as a template, and the feature vectors from the other three images are used for the exam. There are a total of ten images for each individual.

[14] mention that contactless hands are also employed by certain researchers for the purpose of human identification. [14] revealed that by using an infrared illumination device together with the hand's 34 geometric characteristics, they were able to achieve a recognition rate of 96.23% with just 1.85% of FAR on a database with 100 users (60 photos for each user). The majority of geometrical characteristics, such as fingertips and valleys, are computed with the assistance of landmark points. [15] performed an analysis on the dependability of the hand's geometric characteristics, and they came up with a total of 403 features. In the end, features were developed via the use of a combination of the genetic algorithm (GA) and the local discriminative analysis (LDA). 4.51% EER was found over the whole IITD sample (137 subjects).

[16] came up with the idea for an automated recognition approach that is based on hand geometry and does not need feature extraction prior to identification. This method was offered. For the purpose of pattern authentication, a neural network that is based on regression is utilized. During the preprocessing step, the only action that is taken is to resize the images. Middle fingers are extracted utilizing morphological procedures [17] and it is discovered that recognition accuracy rates are higher for dilated fingers as compared to unchanging thinning margins of various finger pictures. This is the case regardless of the kind of finger image. The purpose of this article is to describe a variety of hand geometry-based feature extraction techniques and the findings that were produced from them in the relevant literature. In the next part, we will talk about algorithms that extract features based on hand form.

Over the course of the last several decades, many sorts of biometric characteristics have been the subject of in-depth investigation. In the past, researchers have developed and researched various methods, such as palm printing [18].

In addition, since it is simple to implement and is widely accepted by the general public, identity verification using hand biometric identifiers is garnering an increasing amount of interest among the community of biometrics researchers. Noisy data and intra-class variability are two of the most significant challenges that unimodal systems must overcome [19]. The development of multimodal biometric systems is one possible solution to these kinds of difficulties. Due to the independence of various modalities, such as fingerprints, hand geometry, palm prints, and more, hand-based multimodal biometric systems are garnering greater attention.

[20] integrated fingerprints and hand geometry at the match score level and generated a simplified multivariate polynomial model. They divided the hand into six parts using morphological operators as the basis for the approaches. These regions correspond to the fingers and palm in relation to the forearm. In addition to this, they used high-order Zernike moments to depict the geometrical specifics of each part of the hand. The verification process involves fusing each second over 101

Doi: https://doi.org/10.54216/FPA.010203
Received: February 14, 2020 Accepted: April 18, 2020

individuals, and it has attained a genuine acceptance rate of more than 96% while having a false acceptance rate of under 1%. The characteristics that are included are a two-dimensional palm print, a three-dimensional palm print, hand geometry, and finger texture. The authors do not take into account the form of the hand, despite the fact that this is an essential characteristic for hand-based biometric systems. Obtaining an EER of 2.3% requires an increased amount of computational time and resources.

2.1 *Problem Statement*

The following issues will be addressed as a result of the results of the literature review:

1) The significance of landmark points in the majority of geometry-based schemes is quite important since these locations are included in the computation of features. Fingertips and finger valleys are examples of landmark points. It is important that the landmark points remain the same regardless of whether they are rotated, translated, or scaled. When compared to geometry-based algorithms, the performance of the unimodal hand shape-based algorithms that have been described in the research literature is superior. The exploration and analysis of form characteristics for the development of unimodal hand shape biometrics are now being carried out. All of the currently available shape-based characteristics fall into one of three categories: global, signature, or spectral.

2) If the users do not comply and put their hands in the wrong positions on the acquisition equipment, the hand shape characteristics may change. Because unimodal algorithms rely on just one kind of biometric information, such as simply hand geometry or hand shape, they are unable to offer the necessary resilience for use in applications that need a high level of security. Therefore, a method for feature extraction that takes into account more than one hand characteristic should be the focus.

3 Proposed Work

In the study that is being suggested, multimodal biometrics approaches, including face, iris, and fingerprint-based innovative pattern matching are discussed. In order to have a better outcome from this suggested study, there are four procedures that need to be taken. These phases are called pre-processing, precise feature extraction, multimodal biometric pattern development, and pattern matching. Thirdly, Kernel Fisher Discriminant Analysis (KFDA) is proposed for selecting features from the images. First, the image pre-processing is done by Histogram Equalization (HE), then various feature extraction approaches are proposed to extract features from the face, finger, and iris, and finally, KFDA is proposed for selecting features from the images.
As a consequence of this, in order to produce the multi-biometric pattern, the extracted features are combined with one another at the level of the match score by use of a density-based score level fusion. Following this step, the fused score is utilized to generate a strong 16-bit key. The key matching is then carried out with the help of Learning Vector Quantization (LVQ). The fundamental flow diagram of the multimodal biometric system is shown in figure 2.

Doi: https://doi.org/10.54216/FPA.010203
Received: February 14, 2020 Accepted: April 18, 2020

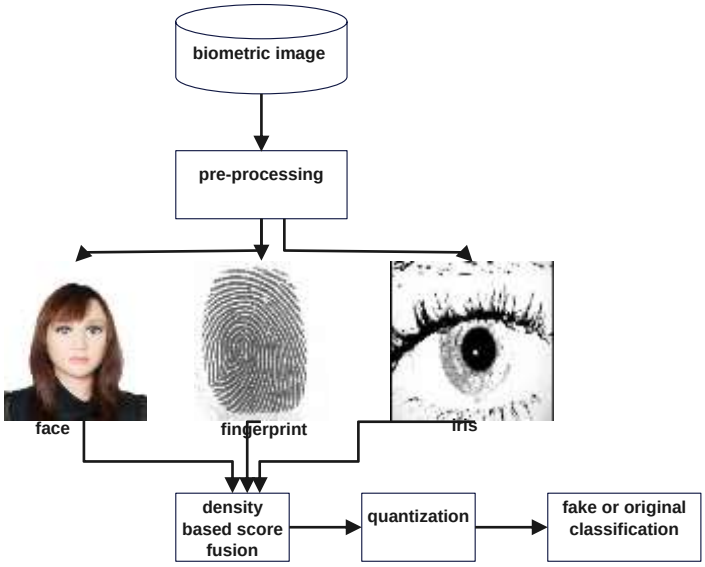

Figure 2: Block Diagram

3.1 Histogram Equalization (HE)

Images of the participant's fingerprints, irises, and faces are used as inputs in this highly awaited research project. Histogram Equalization (HE), which is short for "histogram equalisation," is used to improve the input photos. In the past, this technique for enhancing picture contrast was used successfully to both man-made images and natural scenes. The results were quite positive. HE is a process that modifies the distribution of grayscale value in a picture such that it is consistent throughout. The following formula, which may be represented in mathematical notation: s = T (r). The letter 'r' may be reconstructed from the letter's' using an inverse transformation, as shown in the equation.:

$$r = T^{-1}(s) \quad (1)$$

$$K_0 = round\ (\frac{C_i(2^k-1)}{w.h}) \quad (2)$$

3.2 Fingerprint feature extraction

The following procedures are required in order to extract minute details from a picture of a fingerprint.

The histogram equalisation technique is used in order to bring about an improvement in the contrast of the picture. Utilizing this method does not result in any changes to the picture values that are represented in the matrix x(m, n). Alternately, it displays shifts in the colours of the map that are related to the elements whose values are included in the matrix x(m, n). As a result, this technique has an inclination to consistently employ all of the colours that are available over the whole dynamic range (black to white).

(ii) To convert an 8-bit grayscale fingerprint picture into a 1-bit image via binarization, which is almost equivalent to setting the value verge. There are two possible values, which are 0 and 1. The hills are shown by the number 0, and the valleys are indicated by the value 1. When this method is used to fingerprint photos, the result of the procedure is that the valleys and rides are coloured white and black, respectively. The rides are darker than the valleys.

Doi: https://doi.org/10.54216/FPA.010203
Received: February 14, 2020 Accepted: April 18, 2020

(iii) In order to continue processing, the width of the fingerprint was reduced by a procedure known as "thinning," and the resulting data does not include any information about the fingerprint pictures. The process of thinning may be accomplished with the help of a variety of different algorithms. However, when compared to other algorithms, the Zhang-Suen ones provide superior outcomes in terms of reliability, speed, and outcome in the deletion.
(iv) A minutiae extraction approach is used so that the location of the termination and bifurcations may be determined. The 3x3 matrix is used for the creation of the fingerprint pictures. In this 3x3 matrix, the value of the pixel in the centre is 1, and the values of the pixel closest to the edges are expected to identify the termination and bifurcations.
(v) A technique for the elimination of bogus minutiae is implemented, and it is used to get rid of the fault minutiae. After getting rid of the unneeded elements, adjust the distance to D. Following completion of this procedure, the distance between a termination and bifurcation, as well as the distance between two terminations, as well as the distance between two bifurcations, is less than D.
(vi) Determine an area of interest by drawing a conclusion about the picture that was acquired in the phase before this one.

$$Min\, f = F_{ctr} + P_{cns} \qquad (3)$$

were, $F_{ct} = F_T / \sum_{h=1}^{H} \sum_{i=1}^{N} \Psi_{it}$

$$\sum_{h=1}^{H} \quad \sum_{i=1}^{N} \quad \Psi_{i\,ih} = F_{Tm} \quad / F_{Tm} \qquad (4)$$

F_{Tmax} is the total fuel cost when $P_{it} = P_{imax}$ and F_{Tmin} is the fusion authentication when $P_{ih} = P_{imin}$

$$P_{cns} = \left\{ \sum_{h=1}^{H} \quad \left(P_{Dmd,h} + P_{Lss,h} - \left(\sum_{i=1}^{N} \quad P_{ih} + \sum_{j=1}^{m} \quad w_{jh} \right) \right)^2 \right\} \qquad (5)$$

$$T_x(a_i) = \sum_{y<xi}^{i-1} \quad P(y) + \frac{1}{2} P(xi) \qquad (6)$$

$$len^{(n)} = len^{(n-1)} + \left(union^{\,(n-1)} - len^{(n-1)} \right) F_x(x_n - 1) \qquad (7)$$

$$union^{\,(n)} = len^{(n-1)} + \left(union^{\,(n-1)} - len^{(n-1)} \right) F_x(x_n) \qquad (8)$$

If mid-point is used in the equation, the Tag function will be

$$T_x(a_i) = \frac{\left(en^{\,(n)} + unin^{(n)} \right)}{2} \qquad (9)$$

When used on their own, the derived characteristics from the speech signal based on spectral estimation cannot always perform accurate identification. This is particularly true when there is external noise present and variable environmental conditions. Additional feature components are included into the identification process in order to make it more robust and dependable. This is accomplished by capitalizing on other, previously unknown aspects of the noise sources. The fact that the Cepstrum is a homomorphic transformation, in which the output is a superposition of the input signals, is one of the most essential characteristics of this mathematical operator. The slowly changing section of a waveform, also known as the filter or spectral envelope, and the quickly variable part of a waveform, also known as the source or harmonic structure, make up the spectrum of a waveform. The filter and the spectral envelope are both subsets of the spectrum. Using an anagram of the term "spectrum," which is "Cepstrum," it is possible to accomplish the separation of these two components. It is argued that the Cepstrum lies in the quefrency domain, which is an anagram of the word frequency. The Cepstrum is defined as the inverse Fourier transform of the log magnitude Fourier spectrum of the signal. The cepstral values are kept as discrete components that are referred to as the cepstral coefficients. The amplitude of the nth component along the quefrency axis is the value of the nth cepstral coefficient.

Doi: https://doi.org/10.54216/FPA.010203
Received: February 14, 2020 Accepted: April 18, 2020

4 Experimental Results and Analysis

For the purpose of calculating the performance, both the suggested and current approaches have been carried out on the working platform of MATLAB 2013. NIST Special Database 301 is the source for the collection of fingerprints.

The FERET database has been used to compile the photos of people's faces. Following that, an iris database is compiled with the help of the Institute of Automation at the Chinese Academy of Sciences (CASIA-Iris-Lamp). The CASIA-IrisV3 database includes a total of 22,035 iris photographs, which were collected from more than 700 individuals. Under near-infrared light, each iris picture is a JPEG file with a grayscale level of 8 bits, and it was captured.

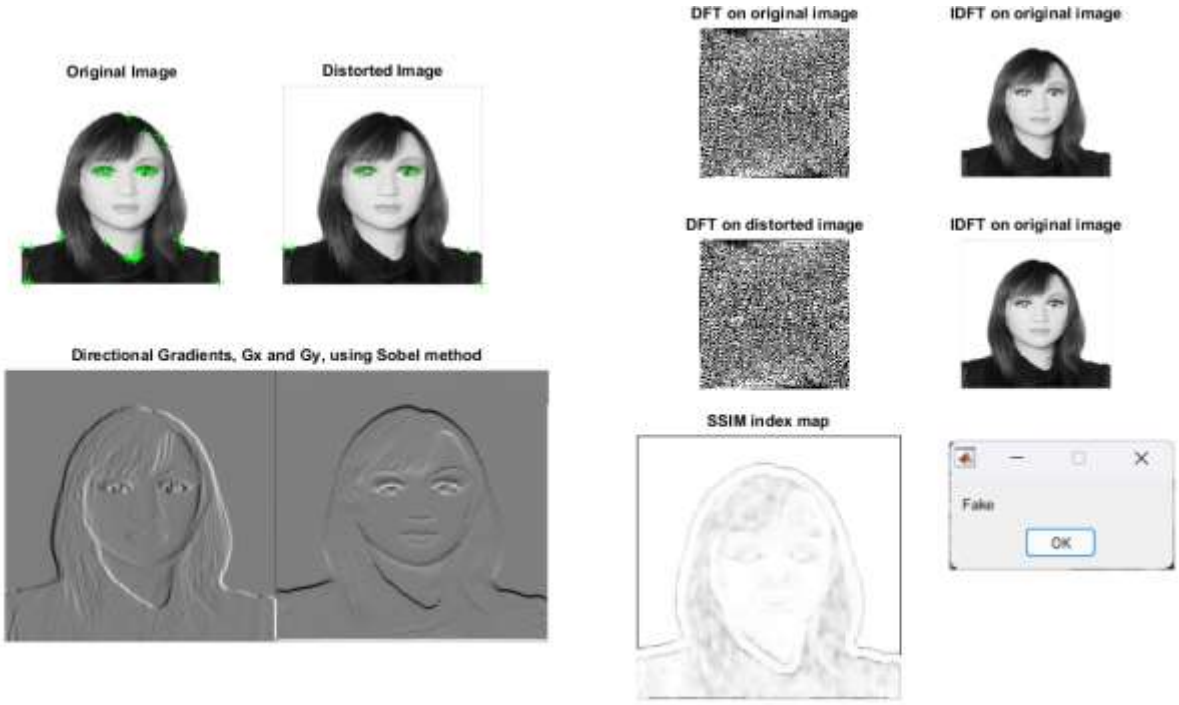

Figure 3 :Face images results

The face input image sample and feature extraction results obtained are shown in figures 3.

Doi: https://doi.org/10.54216/FPA.010203
Received: February 14, 2020 Accepted: April 18, 2020

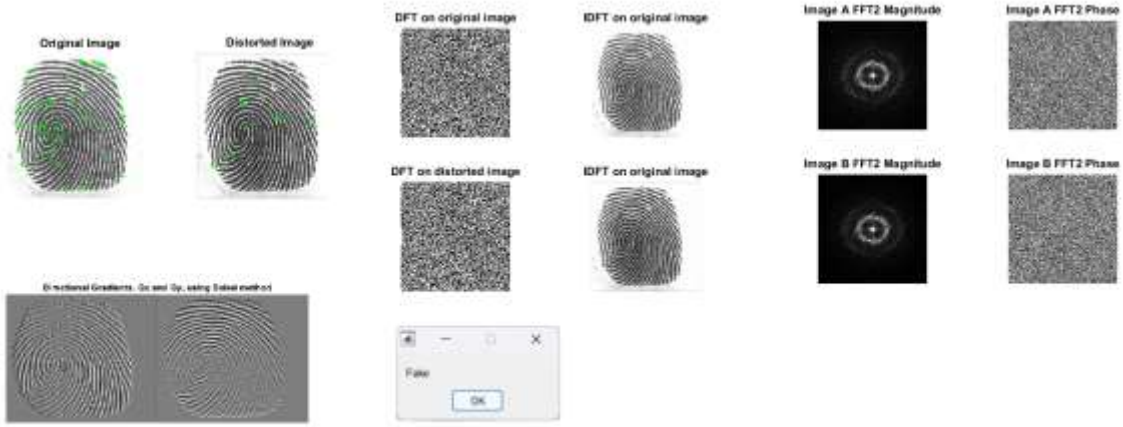

Figure 4:Fingerprint image results

The fingerprint input image sample and feature extraction results obtained are shown in the figure 4.

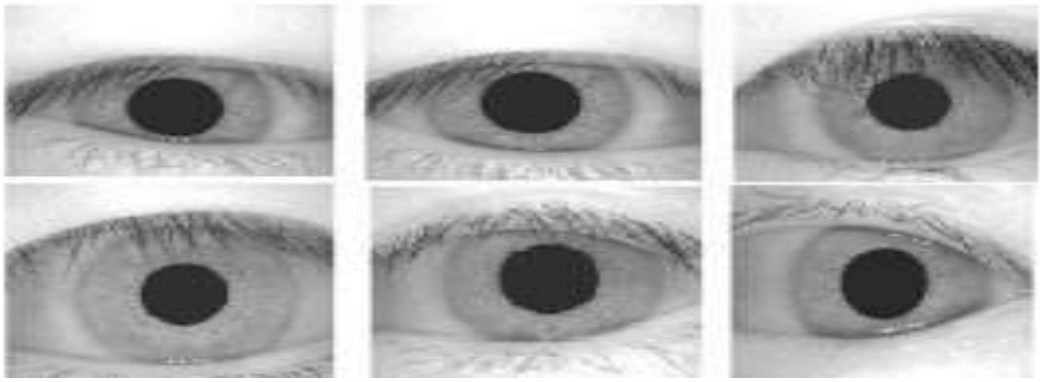

Figure 5 : Input images

Figure 6:Iris results

Doi: https://doi.org/10.54216/FPA.010203
Received: February 14, 2020 Accepted: April 18, 2020

The iris input image sample and histogram results obtained are shown in Figures 5 and 6 respectively.

Performance Analysis

The main concern of the proposed research work also focuses on increasing the security where there are lots of performance measures found to evaluate it.

The performance measures considered in this work are precision, recall, accuracy and f-measure which is represented in table 1.and 2.

Table 1: Performance Analysis

IMAGES	ACCURACY	SENSITIVITY	SPECIFICITY	RECALL	F-SCORE
Set 1	96.32	74.36	89.24	78.23	89.47
Set 2	94.23	65.89	86.23	86.12	86.24
Set 3	91.45	75.65	87.12	86.12	84.65
Set 4	92.34	64.23	89.65	74.56	86.45
Set 5	93.78	74.23	84.35	78.98	89.23

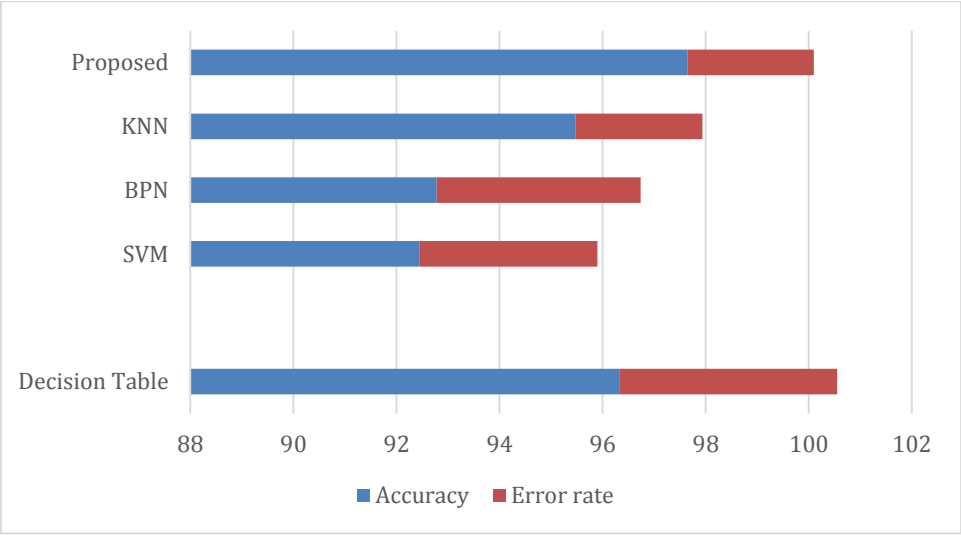

Figure 7: Precision results comparison vs. Recognition methods

Doi: https://doi.org/10.54216/FPA.010203
Received: February 14, 2020 Accepted: April 18, 2020

In terms of accuracy, a comparison is made between the recently introduced LVQ-based face recognition technique and the SVM, ANFIS, and HMM-PSO-based recognition systems that are already in use. It was determined, based on figure 7, that the suggested LVQ-based recognition system achieves 91.2% percent accuracy, while the current SVM, ANFIS, and HMM-PSO-based recognition techniques achieve 88.41%, 90%, and 91% precision, respectively.

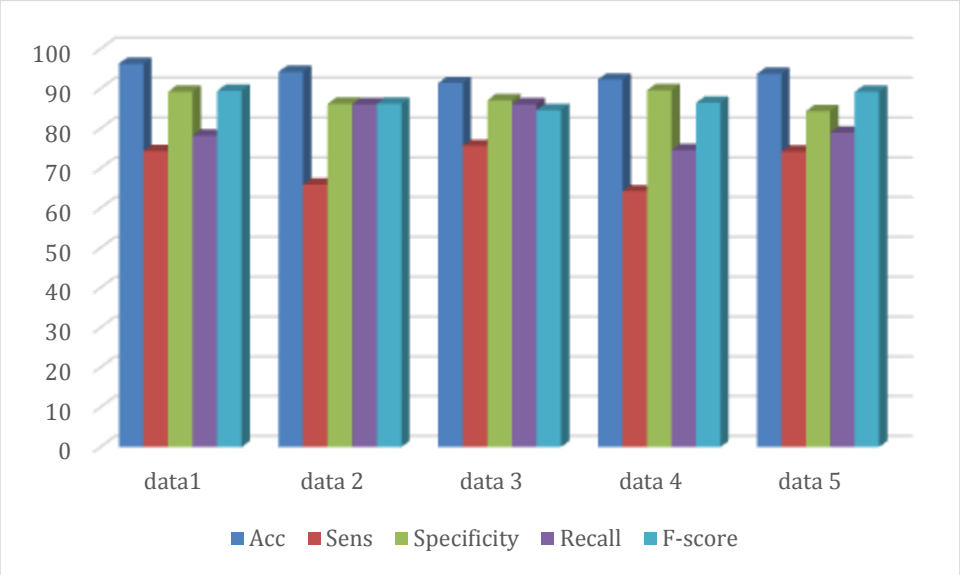

Figure 8: Recall results comparison vs. Recognition methods

Figure 8 illustrates a comparison of the recall of the proposed LVQ-based face recognition strategy with the recall of the current SVM, ANFIS, and HMM-PSO-based recognition systems. The findings of the experiments indicate that the LVQ-based face recognition strategy suggested obtains 88% percent recall, whereas the current SVM, ANFIS, and HMM-PSO-based recognition algorithms achieve 79.58%, 85.01%, and 87.01 correspondingly.

5. Conclusion

In modern times, it is possible to identify, verify, and detect humans through the use of bio recognition technology that is based on multimodal biometrics. This technology has been rapidly developed, and its primary purpose is to ensure the safety of the authentication process used by industries and organisations. At the moment, fingerprints and facial scans are the primary factors used by the vast majority of the successful commercial biometric systems. The multimodal biometrics approaches, namely a face, fingerprint, and smile-based algorithm, are going to be explained in this study that is going to be suggested.

In this initial body of work, an ANFIS classifier-based face recognition system for normal faces is presented. As an input, the unprocessed picture of the face is used. On the input picture, a method known as "robust illumination normalisation" is used in order to enhance the rate of recognition achieved. The next step is to extract from the face the LBP, Gabor, and Phase Congruency characteristics. In order to combine the previously collected characteristics and generate keys, the Z score level fusion process is carried out. The ANFIS classifier is used to do facial recognition on the pictures of the faces based on the key findings. On the other hand, it does not yield reliable identification results when applied to colour face pictures.

The second body of work focused on constructing an effective model for face recognition that used a method known as Hidden Markov Model with Particle Swarm Optimization (HMM-PSO). In the work that has been presented, an Alpha-trimmed mean filter is used to perform preliminary

Doi: https://doi.org/10.54216/FPA.010203
Received: February 14, 2020 Accepted: April 18, 2020

processing on a colour face picture. The Singular Value Decomposition (SVD) technique is used to extract face characteristics from the picture that has been pre-processed and then choose those features. After then, a procedure known as score level fusion is performed in order to combine the scores. At long last, an HMM-PSO technique is used in order to carry out template key pattern matching. The findings of the experiments indicate that the suggested system produces superior performance when compared with the KNN, SVM, and ANFIS methods that are already in use.

A multimodal-based biometric identification system that incorporates the face, iris, and fingerprint was built by a third party as part of an effort to enhance the level of security. In the work that is being offered, the input picture is first improved with the help of Histogram Equalization (HE). Following that, the facial images, finger prints, and iris characteristics that are minutely detailed are retrieved. Kernel Fisher Discriminant Analysis is the method that is used in the process of feature selection (KFDA). In order to merge the characteristics of many modes, density-based score level fusion is carried out. Following this step, the fused score is utilised to generate a strong 16-bit key. In the last step, the key pattern matching is carried out with the help of Learning Vector Quantization, also known as LVQ. The findings of the experiments indicate that the suggested system is capable of achieving superior performance in comparison to the KNN, SVM, ANFIS, and HMM-PSO methods that are already in use.

Funding: "This research received no external funding"

Conflicts of Interest: "The authors declare no conflict of interest."

References

[1] Ratha, N. K., Connell, J. H., & Bolle, R. M. (2001). Enhancing security and privacy in biometrics-based authentication systems. IBM systems Journal, 40(3), 614-634

[2] Wayman, J., Jain, A., Maltoni, D., & Maio, D. (2005). An introduction to biometric authentication systems. Biometric Systems, 1-20

[3] Jain, A. K., Ross, A., & Pankanti, S. (2006). Biometrics: a tool for information security. IEEE transactions on information forensics and security, 1(2), 125-143

[4] Jain, A. K., & Nandakumar, K. (2012). Biometric Authentication: System Security and User Privacy. IEEE Computer, 45(11), 87-92

[5] Scarfo, P. (2013). Achieving assured authentication in the digital age. Biometric Technology Today, 2013(9), 9-11

[6] Hossain, S. M. E., & Chetty, G. (2011). Human Identity Verification by Using Physiological and Behavioural Biometric Traits. International Journal of Bioscience, Biochemistry and Bioinformatics, 1(3), 199

[7] Alsaadi, I. M. (2015). Physiological Biometric Authentication Systems, Advantages, Disadvantages And Future Development: A Review. International Journal of Scientific & Technology Research, 4(8), 285-289

[8] Gamassi, M., Lazzaroni, M., Misino, M., Piuri, V., Sana, D., & Scotti, F. (2005). Quality assessment of biometric systems: a comprehensive perspective based on accuracy and performance measurement. IEEE Transactions on Instrumentation and Measurement, 54(4), 1489-1496

[9] Lourde, M., & Khosla, D. (2010). Fingerprint Identification in Biometric SecuritySystems. International Journal of Computer and Electrical Engineering, 2(5), 852

[10] Hashad, F. G., Halim, T. M., Diab, S. M., Sallam, B. M., & El-Samie, F. A. (2010). Fingerprint recognition using mel-frequency cepstral coefficients. Pattern Recognition and Image Analysis, 20(3), 360-369

[11] Akram, M. U., Tariq, A., Khan, S. A., & Nasir, S. (2008). Fingerprint image: pre-and post-processing. International Journal of Biometrics, 1(1), 63-80 145

[12] Sarfraz, M. S., & Hellwich, O. (2008). An efficient front-end facial pose estimation system for face recognition. Pattern Recognition and Image Analysis, 18(3), 434-441

Doi: https://doi.org/10.54216/FPA.010203
Received: February 14, 2020 Accepted: April 18, 2020

[13] Turk, M. A., & Pentland, A. P. (1991). Face recognition using eigenfaces. IEEE Conference on Computer Vision and Pattern Recognition, pp. 586-591

[14] Wright, J., Yang, A. Y., Ganesh, A., Sastry, S. S., & Ma, Y. (2009). Robust face recognition via sparse representation. IEEE transactions on pattern analysis and machine intelligence, 31(2), 210-227

[15] Zhao, W., Chellappa, R., Phillips, P. J., & Rosenfeld, A. (2003). Face recognition: A literature survey. ACM computing surveys (CSUR), 35(4), 399-458

[16] Jain, A. K., & Li, S. Z. (2011). Handbook of face recognition. New York: springer

[17] Ross, A., & Jain, A. K. (2004). Multimodal biometrics: An overview. IEEE Signal Processing Conference, pp. 1221-1224.

[18] Snelick, R., Uludag, U., Mink, A., Indovina, M., & Jain, A. (2005). Large-scale evaluation of multimodal biometric authentication using state-of-the-art systems. IEEE transactions on pattern analysis and machine intelligence, 27(3), 450-455

[19] ud Din, M. (2011). Data Acquisition System For Fingerprint Ultrasonic Imaging Devic

[20] Jayasree, P. S., & Kumar, P. (2013). A fast novel algorithm for salt and pepper impulse noise removal using B-Splines for finger print forensic images. IEEE International Conference on Image Information Processing, pp. 427-431

Doi: https://doi.org/10.54216/FPA.010203
Received: February 14, 2020 Accepted: April 18, 2020