A Fusion Biometric Authontication based on Fingerprintes and Face Features using PSO and Naïve Bayes

Rupinder sharma[1], Er. Deepinder Kaur[2]
SUSCET, Tangori
(E-mail: rupinder1346@gmail.com)

***Abstract*—** In this era, there are various situations that people need to authenticate themselves. Authentication is a process to determine that someone is really the person that he claimed to be or not. Generally, there are three types of authentication which are something you know, something you have and something you are. Password is an example for something you know. Password is the most common technique used by people to authenticate them. However, password needs a complex combination to make it secure and it is not easy to remember a complex combination. In addition, the example of something you have is taken. Token will generate a random number then people need to input that random number into the system. Next, a system will verify that random number. However, it is not convenient to carry token anywhere as it might be lost or stolen. The last authentication type is something you are. People can authenticate themselves without remembering the complex combination or carry any devices. People only need their own traits to authenticate themselves, for example, their eyes, retina, hand, fingerprint, etc. This authentication method is called biometrics. Biometrics uses physiological or behavioral human traits for authentication purposes. Biometrics authentication has been used in many applications such as e-commerce, access control etc. In this paper, multimodal biometric authentication in light of score level combination of fingerprint and face is proposed. Face and fingerprint is two of the most popular biometric traits and can complement each other for more reliable user authentication. The proposed approach deals with the fusion of fingerprint and face feature using the feature extraction and optimization and classification approaches which is used to increase the genuine authentications in terms of high accuracy rates and less false acceptance rates when both traits of the one individual matches.

Keywords*—*biomatric; fingerprints; PSO; SIFT;

I. INTRODUCTION

Biometrics is the science and technology used for measuring, analyzing the organic data. In information technology, biometrics usually refers for measuring and analyzing human body individuality such as fingerprints, eye retinas and irises, voice patterns, facial patterns, and hand measurements, especially for verification purposes. Biometric is used for extract a feature set from the acquire data, and comparing this set beside to the template set in the database. Biometric fusion can be defined as the use of manifold types of biometric data for improving the recital of biometric systems. An ideal biometric should be unique, universal, and enduring over time that is easy to gauge also cheap in costs, and have high user receipt. No single biometric can fulfill all these requirements simultaneously. For instance, fingerprints and retina are known to be highly unique, but they require dedicated sensors and are not user friendly. On the other hand, voice and facial geometry are not as unique, but they require only a cheap microphone or a camera as a sensor, and they are unobtrusive. Therefore combination of several complementary biometrics can provide higher recognition accuracy than any individual biometric alone [9]. Multimodal biometric systems perform better than Unimodal biometric systems as it removes the limitations of single biometric system. Multimodal biometric system can be constructed using more than one physiological or behavioral characteristic for identification and verification purposes. These types of systems are developed for security purposes in various fields like crime investigation, e-commerce and military purposes. Multimodal biometric system developed using fingerprint, hand geometry, they required the concerned human to make physical contact with a sensing device.

Most of the existing biometric systems developed were based on single biometric features (fingerprint, ear, face, iris and so on). Each biometric trait has its own strength and weakness.

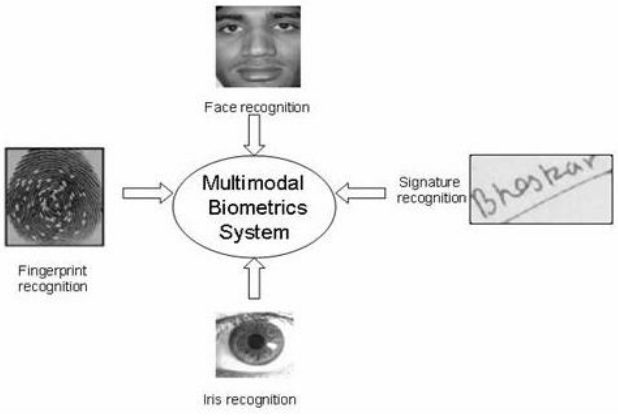

Fig. 1 Biometric Traits

Some of the problem with fingerprint recognition system is fingerprint images have been observed to have poor ridge details. Similarly, face recognition system fails due to variation in facial expression that differ from person to person or due to other parameters. Hence while developing biometric systems the choice of biometric system is important in order to achieve

better performance. Multimodal systems available are face and ear, face and fingerprint, palm print and face, etc. In this proposed work, two unique traits iris and ear are fused to obtain a better performance and high security. [10]

II. EASE OF USE

A. Fusion of Images

Use of multiple biometrics indicators for identifying individuals is known as multimodal biometrics. Evidence obtained from different modalities can be combined by using an effective fusion technique for improving the overall accuracy of the biometrics system, as multimodal biometric system can reduce the FAR/FRR rates and provide more resistance. Multimodal biometric system is more dependable than any other single biometric system. The different Levels of Fusion are [11][12]

- Data-sensor level
- Feature-extraction level
- Matching-score level
- Decision level

The multimodal biometric system can implemented on these fusion schemes to improve the Performance of the system.

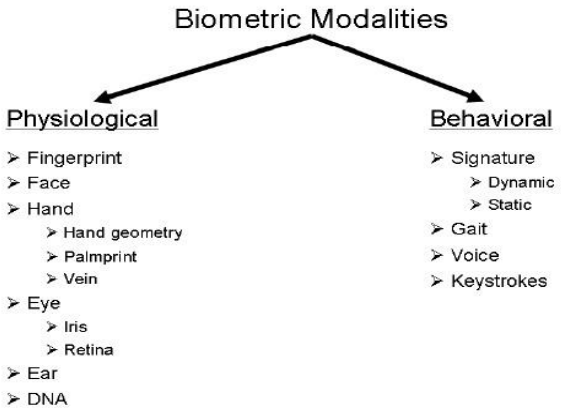

Fig. 2 Different authentication modalities

Usually a classification of the image features is made: physiological that consist of fingerprint, face shape, iris, retina etc. and behavioral i.e. voice, gait, writing style etc. In practice, all verifiers may be considered combinations of physiological and behavioral characteristics due to the interaction mode between the user and the system, which puts its mark over the characteristic. Any physiological or behavioral feature may be used as a biometric verifier as long as it satisfies the following requirements:

- Universality: every person must own characteristic.
- Distinctiveness: two persons having same characteristic does not exist.
- Permanence: the characteristic must be invariant for a time period as long as possible.
- Collectability : It indicates the fact that biometric may be quantitatively measured;
- Performance: refers to the accuracy of the tangible recognition, speed, robustness, as well as the prerequisites for touching a certain level of performance;
- Acceptability – indicates the degree in which the given biometric characteristic is accepted by the users;

Individual character alludes to an arrangement of characteristics like name, government managed savings number, signature and so forth that are connected with a man. Character administration is the procedure of making, keeping up and devastating personalities of people in a populace [1]. A solid character administration framework is earnestly required to battle the pandemic development in fraud and to meet the expanded security prerequisites in a mixed bag of utilizations going from global outskirt intersection to getting to individual data. Setting up (deciding or checking) the character of an individual is called individual acknowledgment or validation and it is a discriminating errand in any personality administration framework. [13] [14]

B. Various types of Biometric system

1) Fingerprints System: Fingerprint authentication systems verify a person's claimed identity from behavioral traits or physiological traits. Biometric system of identification and confirmation provides automatic recognition of an individual based on certain unique features or characteristics possessed by that individual. It takes into consideration the natural features of every single individual for various applications in today's fast growing technical world. Fingerprint systems also help in overcoming the existing problems and limitations in authentication and identification fields and prove efficient and accurate in security related issues. Fingerprint systems can be Unimodal or multimodal. Unimodal fingerprint systems include only one biometric feature at a time for authentication or identification. Unimodal systems may give inaccurate results due to noise, or feature similarity to some extent. Multimodal systems include more than one trait for identification. Multimodal fingerprint system overcomes the limitations of unimodal fingerprint systems such as non-universality, noise in sensed data, spoofing, intra-class variability, inter-class variability [15]. Fingerprint system can be constructed using more than one physiological or behavioral characteristic for identification and verification purposes. These types of systems are developed for security purposes in various fields like crime investigation, e-commerce and military purposes.

In this paper, a unique trait fingerprint is used to obtain a better performance and high security.

- Ear: It has been not proved that the shape of the ear and the structure of the cartilaginous tissue of the pine are unique. The ear recognition approach is based on matching the distance of salient points on the pine from a landmark location on the ear. The appearance of an ear is

not expected to be very distinctive in establishing the identity of a person.

- Face: Face recognition is a non-intrusive method, and facial images are probably the most common biometric characteristic used by humans in today's world to make a personal recognition. The applications of facial recognition range from a static, controlled shot verification to an active, uncontrolled face identification in a cluttered background. It also proves to be a very efficient method as fingerprints and iris. The overall analysis of the face image that represents a face as a weighted grouping of a number of features. Though the verification performance of the face recognition systems are commercially available still they impose a number of restrictions on how the facial images are obtained even sometimes requiring a fixed and simple surrounding or special clarification or quality.
- Iris: Iris is the circular region of the eye that surrounds the pupil and bounded by sclera on either side. The visual textures of an iris are formed during foetus development and stabilize during the first two years of life. The complex iris texture carries very distinctive information like genetical behaviour useful for personal respect. Each iris is unique, like fingerprints. Even the iris of identical twins is different. Iris of left and right of same individual also has difference in its composition. It is very difficult to surgically tamper or alter the texture of the iris. Rather it is easier to detect artificial. Though, the early iris based recognition systems required considerable user sharing technology and was expensive, whereas the newer systems have been converted into more users friendly and cost successful.

2) Vein pattern system: Vein recognition systems largely focus on the vascular patterns of the users hands. As compared to the other biometric systems, the user's veins are situated inside the human body, so not easy to duplicate, thus vein substantiation technology offers high level of precision. Infrared rays emit light that go through the skin of the hand and construct an image of pattern of veins caused by the absorbance of blood vessels. This image is digitized to prepare different biometric templates, which forms the database of the biometric device. Various characters used for developing biometric templates are vessel branch points, breadth of veins and branch angles. The vascular imaging devices can be formed in either contact type or in a non-contact fashion. Non-contact method offers the benefit as compared to contact that it is not essential for the human being to touch the sensor to give the biometric data. It is beneficial in applications where a high degree of cleanliness and hygiene is to be maintained, such as medical functioning room access or where persons are responsive about touching a biometric sensing device [3].

3) Signature Recogniton: Signature is one of the biometric aspects that is used in day to day actions for authorising financial communication, documents, contract etc. In this process, the primary focus is on the visual exterior and texture of the signature. It can be regarded as simple signature comparison. Statically it can be checked by matching the signature with the pre existing signatures. For dynamic signature recognition, users write their signature on a digital tablet which is normally connected to a personal computer for processing and verification, thus real time acquisition of signature can be done [4].

III. LITERATURE REVIEW

R. Snelick et al. (2005) has discussed about the performance of multimodal biometric authentication systems using state-of-the-art Commercial Off-the-Shelf (COTS) fingerprint and face biometric systems on a population approaching 1,000 individuals. The majority of prior studies of multimodal biometrics have been limited to relatively low accuracy, non-COTS systems and populations of a few hundred users. Work is to firstly demonstrating that multimodal fingerprint and face biometric systems can achieve significant accuracy gains over either biometric alone, even when using highly accurate COTS systems on a relatively large-scale population. In addition to examining well-known multimodal methods, new methods of normalization and fusion were introduced which further improve the accuracy.

K. W. Bowyer et al. (2006) has described about the recognition performed by matching models of the three-dimensional shape of the face, either alone or in combination with matching corresponding two-dimensional intensity images. Research trends to date are summarized and challenges confronting the development of more accurate three-dimensional face recognition are identified. These challenges include the need for better sensors, improved recognition algorithms and more rigorous experimental methodology.

R. Jafri et al. (2009) has described that face recognition presents a challenging problem in the field of image analysis and computer vision and as such has received a great deal of attention over the last few years because of its many applications in various domains. Face recognition techniques can be broadly divided into three categories based on the face data acquisition methodology: methods that operate on intensity images; those that deal with video sequences; and those that require other sensory data such as 3D information or infra-red imagery. The author has presented an overview of some of the well-known methods in each of these categories is provided and some of the benefits and drawbacks of the schemes mentioned therein are examined. Furthermore, a discussion outlining the incentive for using face recognition, the applications of this technology and some of the difficulties plaguing current systems with regard to this task has also been provided. The author also mentions some of the most recent algorithms developed for this purpose and attempts to give an idea of the state of the art of face recognition technology.

N. Duta et al. (2009) has discussed about the automated biometric systems which has emerged as a more reliable alternative to the traditional personal identification solutions. The author has presented a survey of the technology used in hand shape-based biometric systems. Firstly reviewed the component modules including the algorithms they employ. Next the discussion of system taxonomies, performance

evaluation methodologies, testing issues and US government evaluations are done.

M. M. Monwar et al. (2009) has discussed various real-world applications, unimodal biometric systems often face significant limitations due to sensitivity to noise, intra class variability, data quality and other factors. Attempts to improve the performance of individual matchers in such situations may not prove to be highly effective. Multi biometric systems seek to alleviate some of these problems by providing multiple pieces of evidence of the same identity. These systems help achieve an increase in performance that may not be possible using a single-biometric indicator. The author has presented an effective fusion scheme that combines information presented by multiple domain experts based on the rank-level fusion integration method. The developed multimodal biometric system possesses a number of unique qualities, starting from utilizing principal component analysis and Fisher's linear discriminant methods for individual matchers (face, ear and signature) identity authentication and utilizing the novel rank-level fusion method in order to consolidate the results obtained from different biometric matchers. The ranks of individual matchers are combined using the highest rank, Borda count and logistic regression approaches. The results indicate that fusion of individual modalities can improve the overall performance of the biometric system, even in the presence of low quality data

J.Y. Cartoux et al. (2013) has described 3D approach for face recognition by segmenting a range image based on principal curvature and finding a plane of bilateral symmetry through the face. This plane is used to normalize for the pose. The methods of matching the profile from the plane of symmetry and of matching the face surface and report 100% recognition for either in a small data set.

R. Subban et al. (2013) has discussed that Fingerprint (FP) serves to identify that the person authenticating is who he/she claims to be. FP identification is popular biometric technique due to the easiness in acquiring, availability of plenty sources for collecting data and their established use. The author has summarized the research work carried out in FP matching techniques, recognition methods and their performance analysis.

K. W. Bowyer (2013) has discussed about the topic of multi-modal biometrics, which has attracted strong interest in recent years. The author has categorized the approach to multi-modal biometrics based on the biometric source, the type of sensing used and the depth of collaborative interaction in the processing. The author also attempts to identify some of the challenges and issues that confront research in multimodal biometrics.

J. Li et al. (2016) has described that the biometrics are a rapidly developing technology that is to identify a person based on his or her physiological or behavioral characteristics. To ensure the correction of authentication, the biometric system must be able to detect and reject the use of a copy of a biometric instead of the live biometric. This function is usually termed "liveness detection". The author has described a new method for live face detection. Using the structure and movement information of live face an effective live face detection algorithm is presented. Compared to existing approaches which concentrate on the measurement of 3D depth information, this method is based on the analysis of Fourier spectra of a single face image or face image sequences. Experimental results show that the proposed method has an encouraging performance.

A. K. Jain et al. (2004) has described that a wide variety of systems require reliable personal recognition schemes to either confirm or determine the identity of an individual requesting their services. The purpose of such schemes is to ensure that the rendered services are accessed only by a legitimate user and not anyone else. Examples of such applications include secure access to buildings, computer systems, laptops, cellular phones and ATMs. In the absence of robust personal recognition schemes, these systems are vulnerable to the wiles of an impostor. Biometric recognition, or simply biometrics, refers to the automatic recognition of individuals based on their physiological and/or behavioral characteristics. By using biometrics it is possible to confirm or establish an individual's identity based on "who she is", rather than by "what she possesses" (e.g., an ID card) or "what she remembers" (e.g., a password). The author has given a brief overview of the field of biometrics and summarizes some of its advantages, disadvantages, strengths, limitations and related privacy concerns.

Y. Wang et al. (2004) has described the Combination of multiple biometrics, which may enhance the performance of personal authentication system in accuracy and reliability. The author compares 13 combination methods in the context of combining the voice print and fingerprint recognition system in two different modes: verification and identification. The experimental results show that Support Vector Machine and the Dempster-Shafer method are superior to other schemes.

R. Govindarajan et al. (2005) has discussed multi biometric systems which utilize the evidence presented by multiple biometric sources (e.g., face and fingerprint, multiple fingers of a user, multiple matchers, etc.) in order to determine or verify the identity of an individual. Information from multiple sources can be consolidated in several distinct levels, including the feature extraction level, match score level and decision level. While fusion at the match score and decision levels has been extensively studied in the literature, fusion at the feature level is a relatively understudied problem. The author has discussed fusion at the feature level in 3 different scenarios: (i) fusion of PCA and LDA coefficients of face (ii) fusion of LDA coefficients corresponding to the R, G, B channels of a face image (iii) fusion of face and hand modalities. Preliminary results are encouraging and help in highlighting the pros and cons of performing fusion at this level. The primary motivation of this work is to demonstrate the viability of such a fusion and to underscore the importance of pursuing further research in this direction.

P. Ambalakata (2005) has described that the biometric based authentication, the science of using physical or behavioral characteristics for identity verification is becoming a security mainstay in many areas. Their utilization as an authentication technology has become widespread from door access to ecommerce especially after the September 11th

terrorist attacks. The author has examined the major forms of known attacks against biometric systems such as Spoofing, Replay attacks and Biometric template database attacks. Biometric systems that use face, fingerprints, iris and retina are used for the study. The methods covered are Liveness detection mechanisms, Challenge-Response systems, Steganography and Watermarking techniques, Multimodal biometrics, Soft biometrics and Cancelable biometrics. Each mechanism is explained in detail. Potentials and weaknesses of the methods are shown and discussed. The effectiveness of the solutions is measured in terms of the various security metrics like cost, amount of effort, practicality, etc. The results of the study indicate that spoofing attacks are a still a major threat to the biometric systems. Liveness detection mechanisms are easily defeated in the case of face and fingerprints, while iris and retina systems are very resistant to spoofing attacks. The systems that use watermarking techniques suffer from the lack of algorithms to deal with image degradation introduced by the watermarks. Although soft biometrics like gender, age, color, race etc can be used to improve the speed of biometric matching through efficient filtering of the database of candidate templates, there exists no real accepted mechanisms for automatic extraction of soft biometric characteristics.

IV. RESEARCH PROBLEM AND FORMULATION

People can authenticate themselves without remembering the complex combination or carry any devices. People only need their own traits to authenticate themselves, for example, their eyes, retina, hand, fingerprint, etc. This authentication method is called biometrics. Biometrics uses physiological or behavioral human traits for authentication purposes. The physiological traits include face, fingerprint, palm, retina and etc. and the behavioral traits include gait, speech, signature and etc. Biometric verification systems confirm a person's requested identity from interactive traits (signature, voice) or physical traits (face, iris, Ear). Multimodal biometric classification overcomes the boundaries of unimodal biometric schemes such as non-universality, noise in detected data, deceiving, intra-class variability, inter-class inconsistency. unimodal biometric systems do not provide sufficient levels of accuracy and security and not even prevent the attacks against data modification and authentication. There has only been limited research done into the application of multimodal biometric systems. Most of the studies have only made on the unimodal systems which are very vulnerable and are having less security. This cannot be accurate enough and might produce very different and distorted results. So an efficient secure approach is needed with high recognition rates and less error rate probabilities. As biometric deals with the authentications based on human traits which will increase the security of the biometric authentication. So the proposed approach deals with the fusion of fingerprint and face feature using the feature extraction and optimization and classification approaches which is used to increase the genuine authentications in terms of high accuracy rates and less false acceptance rates when both traits of the one individual matches.

A. Objectives

To implement a new approach for multimodal biometric using fingerprint and face recognition on score level fusion. The followings objectives are to achieve:

- To study the basics of biometric systems and their processing in terms of image.
- To extract the features for facial imageries using scale invariant feature transform (SIFT) and optimization through PSO for the instance selection
- To perform extraction of minutiae from the fingerprint imageries
- To perform the classification using Naive bias to recognize the right authentications and comparison with the base paper to evaluate the performance in terms of equal error rates, recognition accuracy, false acceptance rate, false rejection rates

V. RESEARCH PROBLEM AND FORMULATION

Biometric system of identification and confirmation provides automatic recognition of an individual based on certain unique features or characteristics possessed by that individual. It takes into consideration the natural features of every single individual for various applications in today's fast growing technical world. Biometric systems also help in overcoming the existing problems and limitations in authentication and identification fields and prove efficient and accurate in security related issues. Various biometric aspects are used for developing such systems like voice, ear, heartbeat, signature, face, fingerprints etc. Iris recognition and fingerprint is measured as one of the most accurate biometric methods available owing to the unique epigenetic patterns of the iris. A system will be developed that can recognize human iris patterns and fingerprint munities analysis of the given samples. Iris has unique genetic combination for every individual that remains same for a long period throughout one's lifetime.

A. Algorithm used

1) Practical Swarm Optimization: Particle Swarm Optimization (PSO) is a simplified algorithm and optimizes the problem in an iterative manner which will provide global best solutions from the number of solutions. It deals with free space search operations over the particle's position and velocity and can seek vast spaces to get best optimize solution. So, PSO is generally considered for the sake of optimization which is popularly known as routing optimization.

For every particle j = 1, ..., swarm do

Set the particle's location with a consistently dispersed random vector Xi

Set the particle's best recognized location to its initial location Pi

If f (Pi) <f (gb) then

1. Update the swarm's finest known position: gb
2. Set the particle's speed: vi

3. While a finishing is not encountered do

For each particle ij= 1, ..., Swarm do

For each measurement d = 1, ..., n do

4. Evaluate fitness function

5. Update the particle's speed: vi, Update the particle's location: xi, Update the best known location: gb

Where gb is the resultant global best optimize solution which is done in the iterative manner.

2) Scale Invariant Feature Transform: To recognize and classify objects efficiently, feature points from objects can be extracted to make a robust feature descriptor or representation of the objects. David Lowe has introduced a technique called Scale Invariant Feature Transform (SIFT) [11] to extract features from images. These features are invariant to scale, rotation, partial illumination and 3D projective transform and they are shown to provide robust matching across a substantial range of affine distortion, change in 3D viewpoint, addition of noise and change in illumination. SIFT features provide a set of features of an object that are not affected by occlusion, clutter and unwanted noise in the image. In addition, SIFT features are highly distinctive in nature which have accomplished correct matching on several pair of feature points with high probability between a large database and a test sample. Following are the four major filtering steps of computation used to generate the set of image feature based on SIFT.

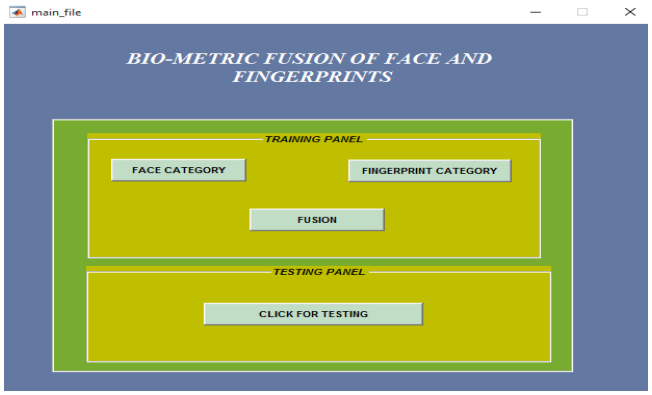

Fig. 3 Main Panel

The above Fig. shows the main panel for the multimodal fusion scenario in which the system deals with the user interface controls for the uploading of the face and fingerprint scenarios

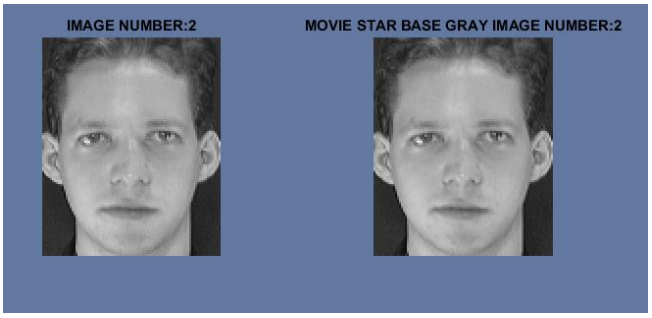

Fig. 4 Original Image Uploading

The above Fig. shows the uploading of the original image of the face and its grey scale image as it is shown in the Fig. in the subplot regions and shows that the matrix dimension of the original image can be in the 3 dimension so it needs to be cover in the grey scale so that it will be converted into 2 dimension to be processed in the efficient manner.

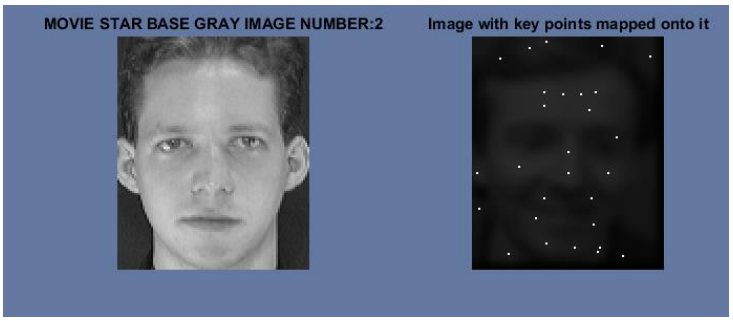

Fig. 5 Feature extraction

The above Fig. shows the feature extraction process using scale invariant feature transform as its one of the main task in the image processing to extract the feature vector using scaling and rotation of the image and it extract the feature vector in terms of the key points of the image

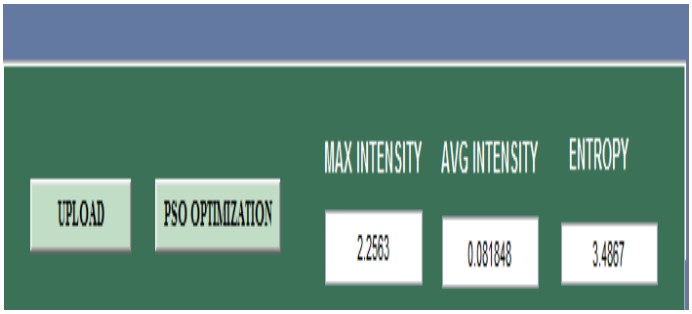

Fig. 6 User interface controls

In the above Fig. we can see that the proposed approach is able to extract the feature of each uploaded image in terms of intensity and entropy of the image which calculated the disorder of the image and shows the user interface controls for the uploaded image.

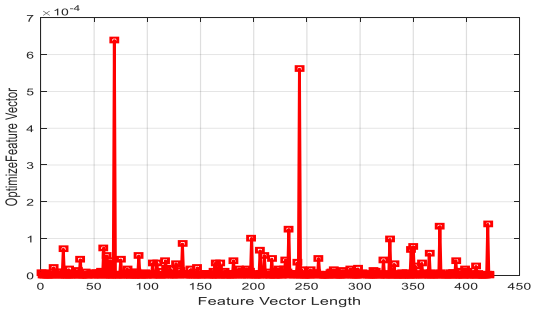

Fig. 7 PSO optimization

The above Fig. shows the optimization process to extract the optimized feature vector which is one of the main tasks in efficient authentications. This is the optimize feature values which are relevant characteristic values to achieve high accuracy of the system.

Fig. 8 Fingerprint

The above Fig. shows the fingerprint uploading scenario and its edge detection to extract the boundaries of the image. The proposed approach is able to achieve edges of the image using canny edge detector

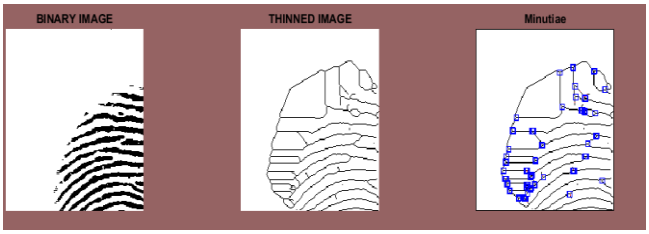

Fig. 9 processing of fingerprints

The above Fig. shows the operation on the fingerprint to extract the ridges and munities of the uploaded current sample to achieve high munities and thinning of the image. First the thinning of the image is done to dilate the image and then the ridges and munities are extracted.

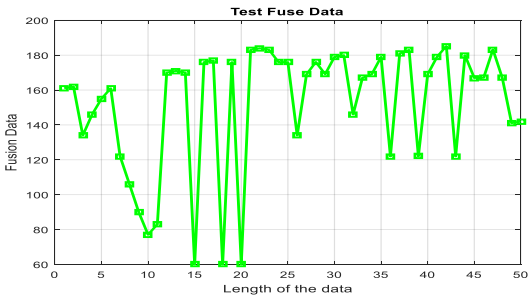

Fig. 10 Fused Data

The above Fig. shows the fusion operation of the feature extracted during the testing phase which shows that the proposed approach is able to fused the both characteristics of the uploaded test sample of the face and fingerprint which is one of the main processes in the classification of the record of the individual in an accurate manner.

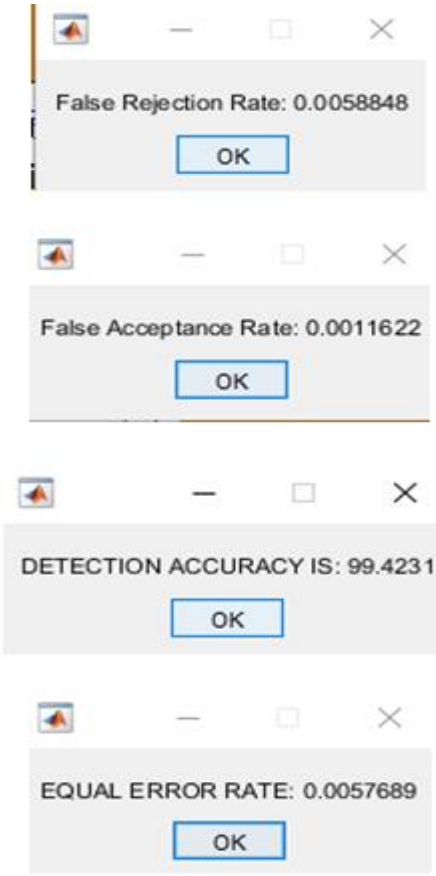

Fig. 11 The performance analysis of the proposed approach

The above Figures show the performance analysis of the proposed approach which is able to achieve high performance in terms of the less error rate probabilities. The evaluation is done in terms of equal error rates which must be low, detection accuracy which must be high, false acceptance rate which also must be low and false rejection rate which must be low for the efficient multimodal authentication of the system

TABLE 1Performance evaluation table

Parameter	Proposed
False acceptance rate	0.0011
False rejection rate	0.0058
Equal error rate	0.00576
Accuracy	99.4231

TABLE 2 Comparison table

Parameter	Proposed	Base
Equal error rate	0.5 %	7 %

CONCLUSION

Biometrics is a science of analyzing and measuring the behavioral and physiological characteristics of human beings. The physical body parts and observable features used for biometric identification are iris , palm print , face, feet, hands, fingers , teeth , ears , retinas, signatures, veins, odors, DNA and voice. Biometric identification provides high level of security by identifying individuals based on anatomic uniqueness. An anatomic uniqueness is a most reliable tool for authentication that cannot be ripped off or lost. A biometric system acquires biometric key from individuals, extracts feature set and recognize the individual based on the extracted feature set. In this modern era, it is a rapidly evolving field with the applications ranging from unlocking the personal device to get entry in any region of world. Biometric systems are being deployed in various common applications including employee attendance system, computer or personal device login, kiosks, airport security, law enforcement, access control and banking transactions etc. Fingerprint based individual authentication systems have recently gain intensive investigate interest due to the untrustworthiness and inconvenience of traditional authentication systems. Fingerprint newly became a vital component of any victorious person identification solutions as biometric character cannot be stolen, shared or even beyond. Among biometric technologies, fingerprint based verification systems bear more compensation than any other biometric technology as it offers an outstanding recognition performance. Fingerprint patterns are invented to be exceptional due to the complexity of the fundamental environmental and genetic processes that influence the generation of fingerprint pattern. Biometrics authentication has been used in many applications such as e-commerce, access control etc. In this research, multimodal biometric authentication in light of score level combination of fingerprint and face is proposed. Face and fingerprint is two of the most popular biometric traits and can complement each other for more reliable user authentication.

REFERENCES

[1] A. K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition 1," IEEE Trans. Circuits Syst. Video Technol., vol. 14, no. 1, pp. 4–20, 2004.

[2] A. Ross and A. Jain, "Information fusion in biometrics," Pattern Recognit. Lett., vol. 24, no. 13, pp. 2115–2125, 2003.

[3] A. Kumar, D. Wong, H. Shen, and A. Jain, "Personal Verification Using Palmprint and Hand Geometry Biometric," Audio- Video-Based Biometric Pers. Authentication, vol. 2688, p. 1060, 2003.

[4] G. Gordon, Face recognition based on depth and curvature features, Computer Vision and Pattern Recognition (CVPR), pp. 108–110, june 1992.

[5] J.Y. Cartoux, J.T. LaPreste, M. Richetin, Face authentication or recognition by profile extraction from range images, in: Proceedings of the Workshop on Interpretation of 3D Scenes, pp. 194–199, 2013.

[6] J.C. Lee, E. Milios, Matching range images of human faces, in: International Conference on Computer Vision, pp. 722–726, 1990.

[7] J. Kittler, M. Hatef, R.P.W. Duin, and J. Matas, "On Combining Classifiers," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 20, no. 3, pp. 226- 239, Mar. 1998.

[8] J. Li, Y. Wang, T. Tan, and A. K. Jain, "<title>Live face detection based on the analysis of Fourier spectra</title>," vol. 5404, pp. 296–303, 2016.

[9] J. Funada, N. Ohta, M. Mizoguchi, T. Temma, K. Nakanishi, A. Murai, T. Sugiuchi, T. Wakabayashi, and Y Yamada, "Feature extraction method for palmprint considering elimination of creases," Proc.14th Intl. Conf. Pattern Recognition., vol. 2, pp. 1849 -1854, Aug. 1998.

[10] J. Chen, C. Zhang, and G. Rong, "Palmprint recognition using crease," Proc. Intl. Conf. Image Process., pp. 234-237, Oct. 2001.

[11] K. W. Bowyer, K. Chang, and P. Flynn, "A survey of approaches and challenges in 3D and multi-modal 3D + 2D face recognition," Comput. Vis. Image Underst., vol. 101, no. 1, pp. 1–15, 2006.

[12] L. Hong and A.K. Jain, "Integrating Faces and Fingerprints for Personal Identification," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 20, no. 12, pp. 1295-1307, Dec. 1998.

[13] M. M. Monwar and M. L. Gavrilova, "Multimodal Biometric System Using Rank-Level Fusion Approach," IEEE Trans. Syst. Man, Cybern. Part B Cybern., vol. 39, no. 4, pp. 867–878, 2009.

[14] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," IBM Syst. J., vol. 40, no. 3, pp. 614–634, 2001.

[15] N. Duta, "A survey of biometric technology based on hand shape," Pattern Recognit., vol. 42, no. 11, pp. 2797–2806, 2009.

[16] N. Duta, A. K. Jain, and Kanti V. Mardia, "Matching of palmprint," Pattern Recognition. Lett., vol. 23, no. 4, pp. 477-485, 2002.

[17] R. Govindarajan and A. Ross, "Feature level fusion using hand and face biometrics," Proc. SPIE - Int. Soc. Opt. Eng., vol. 5779, no. March, pp. 196–204, 2005.

[18] R. Snelick, U. Uludag, A. Mink, M. Indovina, and A. Jain, "Large-scale evaluation of multimodal biometric authentication using state-of-the-art systems," IEEE Trans. Pattern Anal. Mach. Intell., vol. 27, no. 3, pp. 450–455, 2005.

[19] R. Jafri and H. R. Arabnia, "A Survey of Face Recognition Techniques," J. Inf. Process. Syst., vol. 5, no. 2, pp. 41–68, 2009.

[20] R. Subban and D. P. Mankame, "A Study of Biometric Approach Using Fingerprint Recognition," Lect. Notes Softw. Eng., vol. 1, no. 2, pp. 209–213, 2013.

[21] R. Brunelli and D. Falavigna, "Person Identification Using Multiple Cues," IEEE Trans. Pattern Analysis and Machine Intelligence, vol. 17, no. 10, pp. 955- 966, 1995.

[22] S. Ben-Yacoub, Y. Abdeljaoued, and E. Mayoraz, "Fusion of Face and Speech Data for Person Identity Verification," IEEE Trans. Neural Networks, vol. 10, no. 5, pp. 1065-1075, 1999.

[23] V. Matyas and Z. Riha, "Security of biometric authentication systems," 2010 Int. Conf. Comput. Inf. Syst. Ind. Manag. Appl. CISIM 2010, pp. 19–28, 2010.

[24] W. Zhao, R. Chellappa, P. J. Phillips, and A. Rosenfeld, "Face Recognition: A Literature Survey," ACM Comput. Surv., vol. 35, no. 4, pp. 399–458, 2003.

[25] X. Wu, K. Wang, and D. Zhang, "Fuzzy directional energy element based palmprint identification," Proc. ICPR, pp. 689-700, 2002.

Y. Wang and T. Tan, "Combining Fingerprint and Voiceprint Biometrics for Identity Verification : an Experimental Comparison," pp. 663–670, 2004.