iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** VI **Month of publication:** June 2017

DOI:

www.ijraset.com

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

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Multi-Mode Detection and Identification of Biometric Using Multilevel Scaler SVM

P Appala Naidu[1], Dr. CH GVN Prasad[2]
[1] *Research Scholar, Rayalaseema University, Kurnool, AP, India,*
[2]*HOD, Dept. of CSE, SICET, JNTU-H, , Hyderabad, India.*

Abstract: ***the face, iris and fingerprint are most promising biometric authentication system that can be identify and analysis a person as their unique features that can be quickly extracted during the recognition process. to ensure the actual presence of a real legitimate trait in difference to a fake self-pretended synthetic or reconstructed sample is aimportant problem in biometric verification, which needs the development of new and efficient protection measures. biometric systems are susceptible to spoofing attack. a dependable and efficient remedy is needed to attack the epidemic growth in identity theft. the biometric system deals with non-ideal scenarios such as blurred images, reflections etc. which are faked by others. due to this image quality assessment approaches to implement fake detection method in multimodal biometric systems. image quality assessment approach is used to prepare the feature vector which contains quality parameters such as blur level, color diversity, reflection, error rate, noise rate, similarity values and so on. then implement multi level support vector machine classification algorithm to detect fake biometrics by storing these features as vectors in database.***
keywords: multimodal biometrics, image quality, spoofing attack, fake detection, feature vector.

I. INTRODUCTION

Biometric is epidemically growing technology for automated acknowledgment or authentication of the uniqueness of a person using distinctive physical or behavioral characteristics such as fingerprints, face, iris, retina, voice, hand geometry and signature etc. To ascertain a personnel identity biometric relies on - who you are or what you do, as conflicting to what you remember -such as a PIN number or secrete keyword or what you use -such as an ID card. However, significant advances have been realized in biometrics, several spoofing techniques have been established to deceive the biometric systems, and the protection of such systems against attacks is still an open problem.

So , the direct or spoofing attacks have provoked the biometric community to study the liabilities in contradiction of this type of duplicitous action with respect to fingerprint, the face, the signature, or even the bearing and multimodal tactics. Spoofing attacks arise when a person tries to masquerade as someone else faking the biometrics data that are confined by the acquisition sensor in an attempt to avoid a biometric system and thereby ahead an illegal access and advantages. Some type of falsely created artifact e.g. gummy finger, printed iris image, face mask, photograph, audiovisual, 3d Model or imitate the behavior of the actual user like a gait, signature, key stroke dynamics,voice id and etc. are used by the imposter to fake the biometric scheme. Consequently, there is an accumulative essential to detect such efforts of attacks to biometric systems. Liveness detection is one of the existing countermeasures in contradiction of spoofing attack. It aims at physiological signs of being in biometric illustration such as eye blinking, face expression changes, mouth movements, finger skin sweat, blood pressure, particular replication properties of the eye etc. by accumulating exceptional sensors to biometric system. Use of multimodal system is another beneficial countermeasure in contradiction of spoofing attack. Combining face or iris or fingerprint recognition by means of other biometric modalities such as bearing and language is perception of multimodal system. So that multimodal systems are basically trickier to spoof than uni-modal systems. Multimodal systems are more complex than the single modal systems. The multimodal biometrics system illustrated in fig 1.

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

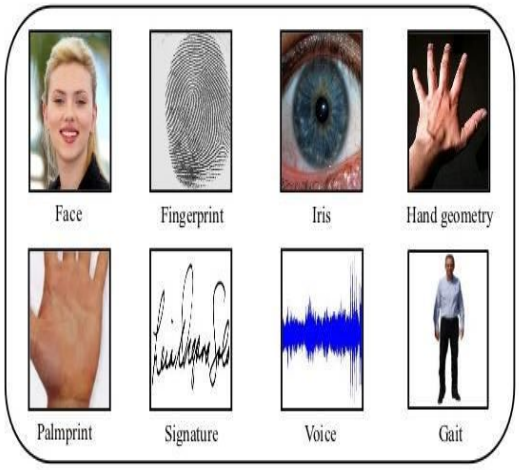


Fig. 1 Multimodal Biometric system

Therefore, there is an increasing need to detect such attempts of attacks to biometric systems. In addition to spoofing attacks, there are other ways to attack system. If an intruder has to access the system has access to scores of the recognition system, the user can easily circumvent the system. However, this type of attack is more difficult to be performed. As the acquisition sensor is the most vulnerable part, any user has easy access to this part of the system that makes spoofing attack techniques have become more attractive for intruders.

II. RELATED WORK

S.Prabhakar,S.Pankanti et.al [1] proposed a novel parameterization using quality events which is verified on a thoroughliveness detection system. Image quality can be assessed by measuring one of the following properties: frame strength, ridge continuity, veracity of the ridge-valley structure, ridge clarity, or estimated authentication performance when using the appearance at hand. A number of information are used to measure these properties: (i)angle information provided by the direction field,(ii) pixel intensity of thegray-scale image, (iii)Gabor filters, which represent another implementation of the direction angle, and power spectrum. (iv) Fingerprint quality can be assessed either examining the image in a holistic method, or combining the quality from local non-overlapped blocks of the image.

J. Galbally, et.al [2] studies two cases for attack detection in faces. The first case study examines the efficiency of the Bayesian-based hill-climbing attack on an Eigen face-based system. The second study employs the previously found optimal configuration to attack a GMM Parts-based system. By using the same optimal configuration between studies we can determine if the performance of the attack is highly dependent on the values of the parameters selected.

K. A. Nixon, V. Aimale, and R. K. Rowe [5] presented liveness detection solutions for great importance in the biometric field as they help to prevent direct attacks those accepted out by means of synthetic traits, and very difficult to detect), improving this mode of level of the security provided to the user.

K. Jain, K. Nandakumar, and A. Nagar [3] introduced a publicly existing database, procedures and a typical technique to guesstimate counter measures to spoofing attacks in face recognition systems. There seems to survive no consensus on best practices and techniques to be situated on attack exposure using non-intrusive systems. The number of publications on the subject is little. A missing key to this puzzle is the absence of typical databases to test counter-measures, trailed by a set of protocols to evaluate performance and allow for objective comparison.

J. Galbally, F. Alonso-Fernandez, J. Fierrez, and J. Ortega-Garcia [4] proposed the image reconstruction approach exploits the evidence stored in the pattern to recreatean accurate image by guessing several aspects of the original unknown fingerprint through four processing steps. The attacking scenario measured in this work supposes that only the mandatory evidence stored in a Impression Particulars Record of the ISO template is available.

L. Best-Rowden, H. Han, C. Otto, B. Klare, and A. K. Jain[6] implement face quality actions to determine when the fusion of resource sources will help boost identification accuracy. The quality actions are also used to assign weights to altered media sources in fusion schemes.

As per Wenxiong Kang, Xiaopeng Chen, QiuxiaWub[7]based on finger images, the local binary pattern algorithm was used to extract features and then match the fingerprints and finger veins, whereas oriented FAST and Rotated BRIEF algorithm was applied for knuckle prints. Finally, score-level fusion was performed on the matching results from the above three finger biometrics. In Ying Xu, FeiLuo, Yi-KuiZhai and Jun-Ying Gan [8], a multimodal biometric recognition using iris and facial images was discussed. Contour let transform and two dimensional principal component analyses were used here to extract the iris features and the facial features respectively, and a feature vector was formed by the combination of the iris and facial features. A fixed random vector is used to improve the recognition efficiency. The efficiency of sum rule-based and support vector machine based score level fusion were effectively used in fingerprint identification and detection was deliberated in Shi-Jinn Horng, Yuan-Hsin Chen [9]. Three biometric characteristics i.e. fingerprints, faces, and finger veins, were taken into consideration for the purpose of the investigation. The diminution of high-scores effect normalization obtained from min-max normalization technique is used for formulating vigorous normalization systems by the authors.

ShubhangiSapkal [10] have smartly developed a novel level synthesis method to fine tune population coverage and scale down spoofing that possess the quality of flexibility to error forbearance of various mono-modal biometric techniques. This method was intended as an access management system necessitating the enhanced safety in permitting access to significant data. Poh. N et.al [11] have proficiently proposed a technique to mechanically validate the uniqueness of an individual by way of biometrics, employing face and fingerprint. They established the fact that the superior performing fusion algorithms were those that make the utmost use of the mechanically mined biometric trait quality calculated with a view to detect the utmost possible biometric mechanism from which the query biometric data was obtained.

The hand print recognition has been deliberated in [12], based on the statistical processing of the hand vein patterns. The hand vein database has been prepared under practical conditions by going through different procedures. Here, the feature extraction is implemented by the combination of geometric and appearance-based techniques and the recognition is implemented by distance metrics .A bank of Gabor filters was used for feature extraction infeng Yang, Yihua Shi [13] of finger print images, from which fingerprint codes were generated using the local and global features. In Meng. Z and Gu.X [14], Palm-dorsal vein recognition method based on histogram of local Gabor phase XOR Pattern has been suggested and they have used chi-square distance measure for recognition. The modified two directional linear discriminant analyses were proposed by Lee [15] for personal verification approach using palm vein patterns. Here A minimum distance classifier is used for user identification. Based on these proposals the vein based biometrics provides improved security and so cannot be spoofed in an easy way. Hence, the hand vein biometrics such as finger vein, palm vein and dorsal vein of the hand are used in our proposed system for multimodal biometric recognition.

A. Image Distortion Analysis Based Face Spoofing Detection

Biometrics provides tools and techniques based on behavior, physical and chemical traits to recognize humans in an automatic and a unique manner. The most common signs are face, fingerprint, voice, iris, hand vein, hand geometry, signature, and DNA. Due to the latest pattern recognition techniques applied to face recognition, biometric systems based on facial characteristics have been largely applied to problems, including user access control, surveillance and criminal identification. At the same time that significant advances have been achieved in biometrics, several spoofing techniques have been developed to deceive the biometric systems, and the security of such systems against attacks is still an open problem.

Spoofing attacks occur when a user tries to access the data by falsifying the biometrics data which is captured by the acquisition sensor in an attempt to circumvent a biometric system and so, Security is main concern for today's scenario. As part of this most of the highlevel organizations uses lot of security systems based on thumb, voice, face, iris, etc, but are not so reliable.image distortion analysis divided into two stages.

Even if any stage is split incorrectly, unofficial entry will be identified. Existing framework analyzed image distortion analysis approach to identify the fake faces. IDA includes specular reflection, chromatic moment, and blurriness and color diversity.

Specular Reflection Features analyze illumination of the images.Reflection Features analyze illumination of the images. Then blurriness is measured by differentiating the actual input image with its blurred version. Then convert the normalized facial image from the RGB space into the HSV (Hue, Saturation, and Value) space and then calculate the mean, deviation, and skewness of each channel as a chromatic feature and finally analyzes color reproduction loss in given input images. Feature vectors are then fed into multiple SVM classifiers. The proposed scheme is to achieve a more stable face spoof detection performance.

B. Fingerprint Recognition System

Every fingerprint of each person is considered to be distinctive, Even the Twins also contain different fingerprint. Fingerprint recognition is the most conventional biometric recognition method. Fingerprints impressions have been used from long time for identifying individuals. Fingerprints contain of ridges and furrows on the surface of a fingertip. Generally attackers attack on fingerprint recognition system by detain real fingerprint, then they make fake fingerprint using silicon, gelatin and playdoh and try to access the system. The following are various finger print datasets as shown in figure 3.

Fig.2 Fingerprint datasets

C. IRIS Recognition System

Iris recognition is another biometric reorganization system for authenticating user's w.r.t to accessing data in a secure manner. Here video images of the irises of an individual's eyes, whose multifaceted random patterns are distinct and can be seen from some distance, are taken for identifying users. Iris cameras perform detection of a person's identity by combining the computer vision, statistical inference, pattern recognition and optics.

The iris of an individual person is unique and no two are the same i.e. each one is distinctive. An attack on the iris is not so easy but how to attack on the system is as shown below. To create a fake iris is of three steps

1) Novel images are capture for a better quality

2) They are printed on a dissertation using a Commercial printe

3) Printed images are presented at the iris sensor.

The iris datasets are gathered from CASIA database and then images in fig. 3.

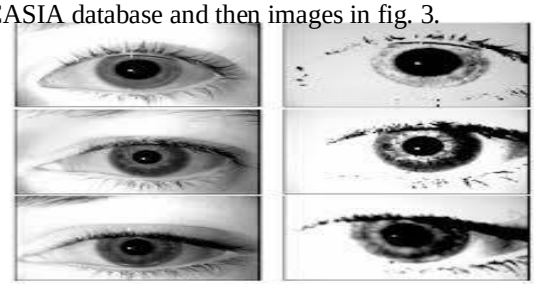


Fig. 3 IRIS datasets

D. Face Recognition System

The most popular acceptable biometrics is Face recognition, because it is one of the most general methods of persons employ in their visual interactions and acquisition of faces. The face acknowledgment systems make different among the contextual and the face. It is most substantial when the system has to categorize a face within a multitude. The system then creates use of a person's facial features – its valleys and heights and milestones and indulgences these as lumps that can be equated and planned in contradiction of those which are stored in the system's database.

There are about 100 lumpsen circling the face print that makes use of the system and this includes the eye socket depth, jaw line length, distance between the eyes, cheekbone shape, and the size of the nose. It is very challenging to develop this recognition technique which can recognize the effects of facial expressions, age, slight variations in the imaging environment.

Attack on the face recognition system is shown in the following figure in that figure fake and genuine image are shown and that

Volume 5 Issue VI, June 2017
ISSN: 2321-9653

images are discover out due to different method of face recognition. In face recognition system fake users attack on system by detaining the picture to the mobile devices or camera. And try to authenticate. Possible scenarios in face database in fig 4.

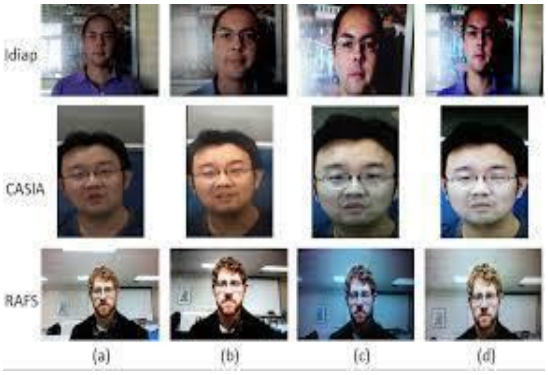


Fig. 4 Face datasets

E. Multimodal Biometric System Using Image Quality Assessment

To ensure the genuine presence of a real rightful trait in difference to a fake self-manufactured imitation or recreated sample is a major trouble in biometric verification, which requires the improvement of new and effective security measures. Background to fingerprint detection describes the biometric use of fingerprints scanning is also done by biometric tools. The objective of proposed system is to enhance the security of biometric recognition frameworks, by adding liveness assessment in a speedy, user friendly and non-intrusive manner, through the use of image quality assessment. Image quality assessment divided into full reference and no reference methods as shown in fig.5.

Full-reference (FR) IQA methods rely on the accessibility of a clean undistorted reference image to estimate the quality of the test sample. Full reference IQA contains three types of measurements such as error sensitivity measures, structural likeness measures and information theoretic measures. No-Reference IQ Measures does not require of a reference sample to regulate the quality level of an image. This measurement contains such as distortion measures, training based measures and natural scene statistics measures. Then implement image fusion approach to

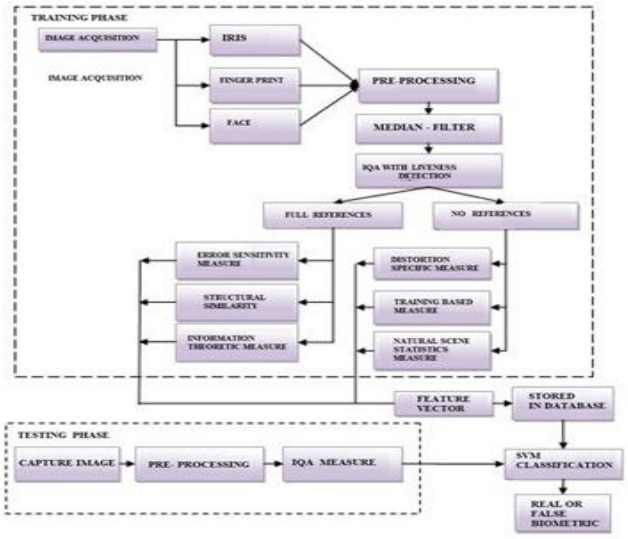


Fig.5 Image Quality Assessment Methods

combine all biometric features that includes iris, face and fingerprint features and finally QDA based classification technique can be implement to finalize the accuracy of the object match. The algorithm shown uses SVM –Sheralt Transformation and Inverse Transformation technique to find the accurate match of the object.

1) Input data sets

2) Perform SVM-Sheralt Transformation

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

3) Check for scale invariant
4) Perform mapping with match identification
a) Check For Like hood Base Function
b) CheckScaler-Sheralt Invert Transformation
5) If True
a) Match Is AccurateEls
b) Match Is Not Accurate

III. PROPOSED METHOD

Biometric recognition has the advantage of being reliable and secure for authentication purposes. Multi-biometrics uses more than one trait and overcomes the draw backs of using single modality. It improves security, but choosing the right modality and techniques involved, is of utmost importance. Thumb, Iris and face objects of the human are used here as the biometric modalities. The proposed technique employs Shearlet transform and SIFT for feature extraction and the fusion is carried out using maximum likelihood ratio-based technique. The block diagram of the proposed technique is given in Fig. 6.

A. Formation of feature set

In order to generate the required feature set, the input vein images of hands are transformed using Shearlet transform and Scale-invariant feature transform.

B. Shearlet Transformation

he Shearlet is an affine system with a single generating mother Shearlet function parameterized by a scaling, shear, and translation parameter. The Shearlet transform thus overcomes this drawback while retaining most aspects of the mathematical framework of wavelets. Shearlet has the properties that the

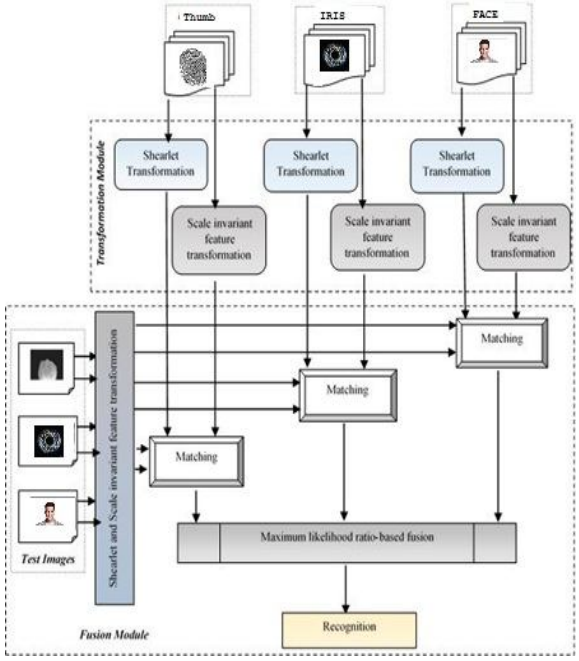


Fig.6 Block diagram of Proposed System

associated system forms an affine system and the transform can be regarded as matrix coefficients of a unitary representation of a special group. Shearlet can be represented as

$\Psi_{a,s,t}(x) = a^{-3/4}\,\Psi((D_{a,s}\text{-}1(x\text{-}t))$

Where $D_{a,s}$=[a,$-a^{1/2}$ s; 0, $a^{1/2}$]..... (1)

Where, *a* is a scaling parameter, *s* is a shear
Parameter and *t* is a translation parameter.
The mother Shearlet function □ is defined as

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

$\Psi(\xi_1, \xi_2) = \Psi(\xi_1)\ \Psi(\xi_2)$..... ….. (2)

Where, $\square_1$ is a wavelet and $\square_2$ is a bump function. The associated continuous Shearletscalertransform depends on the scaling, shear and translation parameters and is defined by

$$ST[f(a,s,t)] = f, \Psi_{a,s,t} \text{..... (3)}$$

This transform can also be regarded as matrix coefficients of the unitary representation:

$$\sigma(a,s,t)(\Psi)(x) = \Psi_{a,s,t}(x) = a^{-\frac{3}{4}}\Psi\left(D_{a,s} - 1(x-t)\right) \text{... (4)}$$

Let the input of Thumb, Iris and Face Images be represented as

$$T = \{t_1, t_2, t_3, \ldots\ldots t_n\},$$
$$I = \{i_1, i_2, i_3, \ldots\ldots i_n\}, and$$
$$F = \{f_1, f_2, f_3, \ldots\ldots f_n\} \text{.....(5)}$$

Here, *n* is the number of images. Then the Shearlet transformed Thumb, Iris, and Face images can be represented by

$$ST = \{st_1, st_2, st_3, \ldots\ldots st_n\}$$
$$SI = \{si_1, si_2, si_3, \ldots\ldots si_n\} and$$
$$SF = \{sf_1, sf_2, sf_3, \ldots\ldots sf_n\} \text{.....(6)}$$

A. Scale-Invariant Feature Transformation

Scale-invariant feature transform (SIFT) is a step by step procedure to identify and delineate the local features in images. There are mainly four steps involved in SIFT algorithm namely scale space extreme detection, key point localization, orientation assignment, key point descriptor and key point matching.

Scale-space extrema detection is employed to detect larger corners using larger windows. Here, Laplacian of Gaussian (LoG) is found for the image with various scaling parameter values (θ). LoG acts as a blob detector which detects blobs in various sizes. As LoG is a little costly, SIFT algorithm uses Difference of Gaussians which is an approximation of LoG. Difference of Gaussian (DoG) is obtained as the difference of Gaussian blurring of an image with two different θ and $k\theta$. Once this DoG is found, images are searched for local extrema over scale and space.

Once potential key points locations are found, they have to be refined to get more accurate results in the key point localization. If the intensity at this extrema is less than a threshold value, it is rejected so as to eliminate low contrast key points. Similarly, edge threshold is used to remove low edge key points. These processes would rise to retain of strong interest points.

The SIFT transformed images of Thumb, Iris and Face images can be represented by

$$FT = \{ft_1, ft_2, ft_3, \ldots\ldots ft_n\}$$
$$FI = \{fi_1, fi_2, fi_3, \ldots\ldots fi_n\} and$$
$$FF = \{ff_1, ff_2, ff_3, \ldots\ldots ff_n\} \text{.....(7)}$$

B. Maximum Likelihood Ratio-based Fusion and Recognition

The feature set obtained from the transformations are matched and fused for recognition. Initially, images of hand Thumb, Iris and face are transformed using the above transforms and stored in the database. The database (DB) would consist of both the Shearlet and the SIFT transformed images.

$$DB = \{ST, SI, SF, FT, FI, FF\} \text{.....(8)}$$

Where

$$ST = \{st_1, st_2, st_3, \ldots\ldots st_n\}$$
$$SI = \{si_1, si_2, si_3, \ldots\ldots si_n\}$$
$$SF = \{sf_1, sf_2, sf_3, \ldots\ldots sf_n\}$$
$$FT = \{ft_1, ft_2, ft_3, \ldots\ldots ft_n\}$$
$$FI = \{fi_1, fi_2, fi_3, \ldots\ldots fi_n\}$$
$$FF = \{ff_1, ff_2, ff_3, \ldots\ldots ff_n\}$$

Subsequently, the matching score is compared to the test input images and those in the database. The test images are represented by

Volume 5 Issue VI, June 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

$T = \{T_{test,} I_{test,}, F_{test,}\}$ .....(9)

The transformed images are represented as:

$T^* = \{st_{test,} si_{test,}, sf_{test,} ft_{test,} fi_{test,} ff_{test}\}$ .....(10)

These features are compared with those in the database using the Euclidean distance measure which gives the matching score. If the Euclidean distance between the test image and that of the data base image is less than the threshold set, then the images are said to be in a matched condition. Suppose the Euclidean distance between images Im_1 *and* Im_2 is represented by *dis* and the threshold set is represented as d_{thr}.

If $dis < d_{thr,}$ then Im_1 *and* Im_2 are in matched condition.

Each of the images are matched with the database image and then matching scores of all images are discovered. Then the fusion process is carried out with the use of maximum likelihood ratio based on fusion matching score.it is basically a density based score fusion which requires explicit estimation of genuine and impostor match score densities. Each comparison of the test image with that in the database would yield a matching score and for the fusion process each of the matching scores are taken into consideration.it is supposed that total of m matching is carried out, to get the matching score vector given by

$SV = \{sv_1, sv_2, sv_3 \ldots\ldots sv_n\}$ .....(11)

Let the conditional joint densities of the M match scores for the genuine and impostor classes be represented by *Ge(sv) and Ip(sv).* The respective class of genuine or impostor is assigned by analyzing the score vector and Gaussian mixture model is employed for finding out the score densities.

Let the M-variant Gaussian density be represented as *g(sv;μ,c),* where μ is the mean vector and *c* is the covariance matrix .the estimates obtained can be represented as $\hat{Ge}(sv)$ and $\hat{Ip}(sv)$ then the maximum likelihood ratio is given by

$$L(sv) = \frac{\hat{Ge}(sv)}{\hat{Ip}(sv)} \text{.....(12)}$$

The matching score vector SV is assigned to genuine class,

if L (SV) > decision threshold or assigned to impostor class.

if L (SV) ≤ decision threshold, The decision threshold is determined based on the specified False Acceptance Rate (FAR).

The performance of the system is measured using False Fake Rate and False Genuine Rate. Compare to existing system, our work provide reduced number of FFR and FGR. The graphical representation is in fig 7.

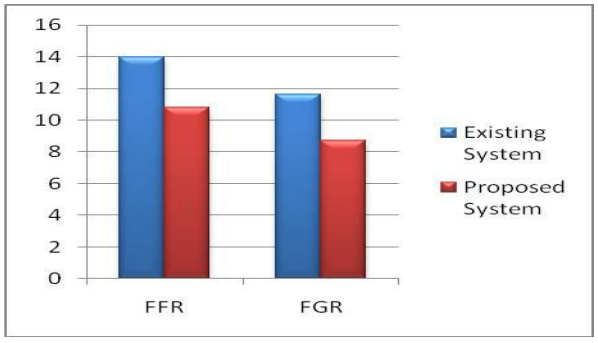


Fig. 7 Performance evaluation

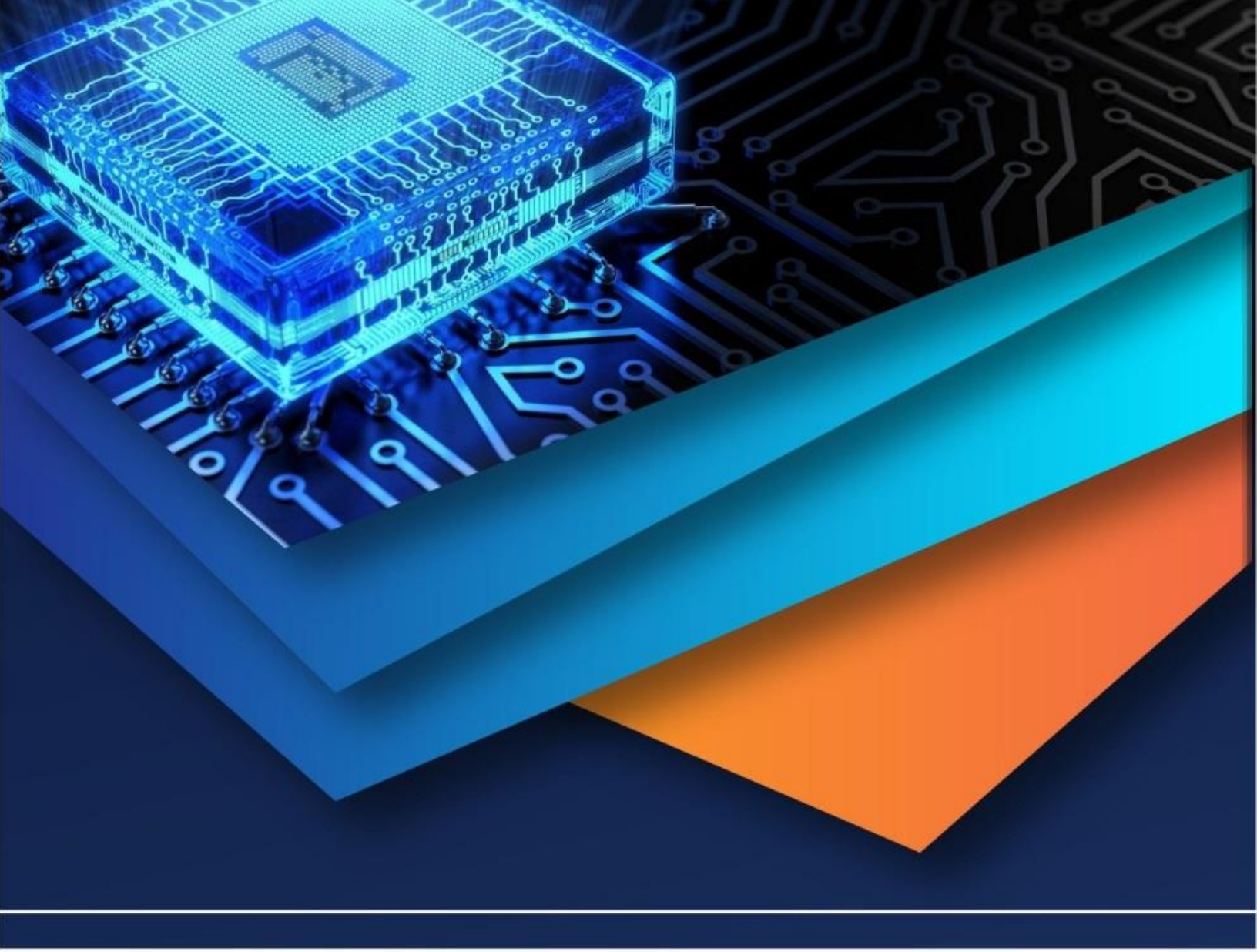
IV. CONCLUSION

Image quality assessment is used to detect the fake biometrics. Due to Image quality dimensions, it is simple to find out real and fake users because fake identities often have some different features than original it always enclosed different luminance and color levels, general artifacts, extent of evidence, and magnitude of sharpness, found in both type of images, natural appearance or structural distortions. Multi- Biometric system is challenging system. It is more secure than uni-biometric system. This technique can analyze multi modal biometric system with image fusion approach. Implement image fusion approach to combine both biometrics (fingerprint and iris, iris and face, face and fingerprint). So we can implement image SVM Scalar technique to fuse all biometric features as in one image format. This method is used to improve security in database level. The dynamic IQA is a very

promising technique in making recognition system more robust against fake based spoofing attempts to provide alert system to intimate mobile message to person who are authorized by the system.

REFERENCES

[1] S. Prabhakar, S. Pankanti, and A. K. Jain "Biometric recognition: Security and privacy concerns," IEEE Security Privacy, vol. 1, no. 2, pp. 33–42, Mar./Apr. 2013.
[2] J. Galbally, C. McCool, J. Fierrez, S. Marcel, and J.Ortega-Garcia, "On the vulnerability of face verification systems to hill-climbing attacks," Pattern Recognition., vol. 43, no. 3, pp. 1027–1038, 2014.
[3] K. Jain, K. Nandakumar, and A. Nagar,"Biometric template security," EURASIP J. Adv. ignal Process., vol. 2008, pp. 113–129, Jan. 2014.
[4] J. Galbally, F. Alonso-Fernandez, J. Fierrez, and J.Ortega-Garcia, "A high performance fingerprint liveness detection method based on quality related features," Future Generat. Comput. Syst., vol. 28, no. 1, pp. 311–321, 2015.
[5] K. A.Nixon, V. Aimale and R.K.Rowe, "Spoof detection schemes," Handbook of Biometrics. New York, NY, USA: Springer Verlag, 2008, pp. 403–423.
[6] L. Best-Rowden, H. Han, C. Otto, B. Klare, and A. K. Jain, "Unconstrained face recognition: Identifying a person of interest from a media collection," IEEE Trans. Inf. Forensics Security, vol. 9, no. 12, pp. 2144–2157, Dec 2015.
[7] Wenxiong Kang, Xiaopeng Chen, QiuxiaWub: The Biometric Recognition on Contactless Multi-Spectrum Finger Images, Infrared Physics & Technology, Vol. 68, 2015, pp. 19-27
[8] Ying Xu, FeiLuo, Yi-KuiZhai and Jun-Ying Gan: Joint Iris and Facial Recognition Based on Feature Vol. 12, No. 6,, 2015
[9] Shi-Jinn Horng, Yuan-Hsin Chen, Ray-Shine Run, Rong-Jian Chen, Jui-Lin Lai and Sentosal, K. O: An Improved Score Level Fusion in Multimodal Biometric Systems, Parallel and Distributed Computing, Applications and Technologies, 2009, pp. 239-246
[10] ShubhangiSapkal: Data Level Fusion for Multi Biometric System using Face and Finger, International Journal of Advanced Research of Computer Science and Electronics Engineering, Vol. 1, No. 2, 2012
[11] Poh. N: Benchmarking Quality-Dependent and Cost-Sensitive Score-Level Multimodal Biometric Fusion Algorithms, Information Forensics and Security, Vol. 4, No. 4, 2009, pp. 849-866
[12] Yuksel, A., Akarun, L. and Sankur, B: Hand Vein Biometry Based on Geometry and Appearance Methods, IET Computer Vision, Special Issue: Future Trends in Biometric Processing, Vol. 5, No. 6, 2011, pp. 398-406
[13] Jinfeng Yang, Yihua Shi, Jinli Yang: Personal Identification Based on Finger-Vein Features, Computers in Human Behavior, Vol. 27, 2011, pp. 1565-1570
[14] Meng. Z and Gu.X: Palm-Dorsal Vein Recognition Method Based on Histogram of Local Gabor Phase XOR Pattern with second Identification, Journal of Signal Processing Systems, Vol. 73, No. 1, 2013, pp. 101-107
[15] Lee, Y, P: Palm Vein Recognition Based on a Modified (2D)2 LDA, International journal of Signal Image and video processing.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY