International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER SSRN

IJIEMR Transactions, online available on 4th Sept 2019. Link :http://www.ijiemr.org/downloads.php?vol=Volume-08&issue=ISSUE-09

Title QUANTUM CRYPTOGRAPHY AND SUPPORT VECTOR MACHINE BASED MULTI-MODAL BIOMETRIC IDENTIFICATION SYSTEM FOR HIGH-SECURITY APPLICATION

Volume 08, Issue 09, Pages: 101–112.

Paper Authors

K.VASAVI,MD.AYESHA BEGUM, S.SOWMYA

ABIT

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

QUANTUM CRYPTOGRAPHY AND SUPPORT VECTOR MACHINE BASED MULTI-MODAL BIOMETRIC IDENTIFICATION SYSTEM FOR HIGH-SECURITY APPLICATION

[1]K.VASAVI,[2]MD.AYESHA BEGUM, [3]S.SOWMYA
[1]Assistant Professor, Department of ECE,ABIT
[2,3]IVB.TECH year student Department of ECE, ABIT
[1]karnati.vasavi@gmail.com, [2]ayeshabegum1242@gmail.com

Abstract:
The main aim of this paper givesmultilevel identification in biometric system.Multi Modal Biometric is the usage of multiple biometric indicators by personal identification systems for identifying the individuals.Multi Modal authentication provides more level of authentication than UniModel Biometrics which uses only one biometric data like Face or Palmprint or Iris.In this paper,a new high secured Face,Fingerprint and Iris based Multi Model Biometric System is introduce which is named as Quantum Cryptography-Support Vector Machine-MultiModal Biometric System(QC-SVM-MMBS).To improve the database security in this QC-SVM-MMBS system Quantum cryptography technique Support Vector Machine Algorithm has been used. By using this QC-SVM-MMBSsystem which provide much better performance in the terms of False Acceptance Ratio(FAR),False RejectionRatio(FRR)accuracy,Execution Time,Error Rate,Recall(R) ,False Negative(FN),False Positive(FP),Precision(P),True Positive(TP) and True Negative(TN).

Keywords: Multi Modal Biometric, Database Security,Quantum Cryptography,Support Vector Machine algorithm and Accuracy.

Introduction:

Biometric Systems are used in the identification process instead of tokens like ID CARDS,and knowledge systems like PASSWORDS.Generally, Biometric system working in the principle of measuring the biological characters and testing the biological Characterssuch as Hands,Fingers,Feet,Iris,Face,Retinas,teeth,ears, Veins,Signatures,Voices,Typing styles, Odors,gaits,DNA,etc,. of individuals.The verification and identifications of the individuals are performed by biometric sensing and processing.The merit on the biometric system is the users do not require remembering the passwords or carrying the tokens to access the certain information.One more advantage is Biometric characteristics are cannot be forgotten or lost.To improve the accuracy and security the Biometric Systems use an individual human body characteristicswhich do not normally change over –time.For testing the biological features,this database is used to identify the individual feature to improve security.Actually,Biometric systems are of two types:One is UniModel Biometricsystems(UM-BS) contains only one Biometric characteristics and MM-BS contains Multiple biometric characteristics .Here we are using the method

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

called Quantum cryptography and SVM based MM-BIS for high security application.Quantum cryptography is nothing but a key distribution which is mostly used to ensure the confidentiality of information transmitted between two parties usually called Alice and Bob,to protect the confidentiality of biometric system,Alice and Bob agree on a common,yet secret,piece of information called a key.The key to successful MM-BS is an effective fusion method which is essential to fuse, the information given by multiple domain experts.In a given problem domain, the preprocessed set of experts is determined by fusion and then an appropriate function is fused optimally which is shown by individual experts.The Fusion process in quantum cryptography combines two distinct entities into new whole entities. Here we are using FLF technique to combine the FI-FLF-MM-BS system extracted feature values. In Quantum cryptography method we are using SVM algorithm.SVM algorithm can perform eitherlinear and non-linear classification.

The major contribution of the paper is started as:

- ✓ The features taken from face, Iris and palm images are detected using BEMD.This kind of technique provides two features such as local phase and Amplitude.
- ✓ The security over the MM-BS is introduced by Support Vector Machine(SVM).This kind of cryptography technique is improves the confidentiality and for unauthorized users (i.e.,hackers) it is difficult to access the information from Biometric systems.
- ✓ The matching of this MM-BS is performed by error correcting code based SVM.

Literature Survey:

Gandhimathi Amrithalingam and G.Radhamani has presented the chaff point based Fuzzy vault to hide the secret key within the biometric data(face and ear).The shape and texture features of face and ear are extracted by using the Modified Region Growing and Local Gabor XOR patter respectively.The new chaff point feature vector is combined with the shape and texture feature vectors to create the chaff points.Here,the PSO is used for finding the optimal locations of feature vectors.In PSO the particles are defined as the extracted feature locations and best location to create the chaff point is to choose depend on the fitness values.

V. Sireesha and S.R.K. Reddy has introduced the two levels of fusion in an Iris and Finger print images for the Biometric authentication.The features of Iris and fingerprint are extracted by feature extraction module which has modified LDP and Gabor based features.There are two levels of fusions are used such as SLF and FLF and these techniques are used for fusing the features of Iris and Finger print.Here FLF used glowworm swam optimization(PSO) for short listing the optimal features. The recognition accuracy of FLF-GSO-MM and SLF-PSO-MM was only 90% and 85% respectively.

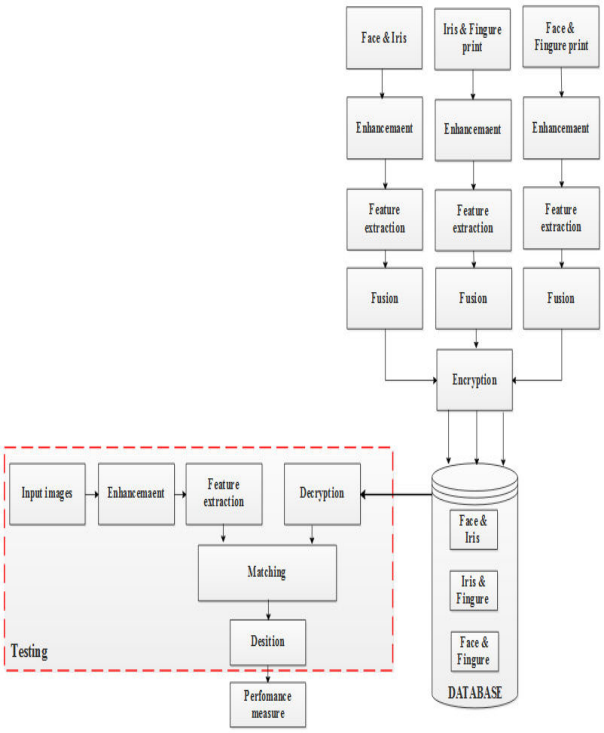
M.S.AslanZ.Hailat,T.K. Alafif and X.W.Chen presented the auto encoder(AE) in multi channel Multi –modal feature learning for face recognition to integrate the Alternating Direction Method of Multipliers(ADMM).The AE was used to paralyze/distribute the optimization tasks by dividing the energy consumption in to several; sub-bands.A number of samples are required in the Convolutional Neutral Network(CNN) to avoid overfitting,which is more complex.

A.Jagadeesan,T.Thillaikkarsai and K.Duraiswamy has presented a multimodal biometrics(Iris and Finger print) for generating

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

a secure cryptographic key.First,the minutiae pointsand texture properties identified from the Iris and Finger print respectively.Then a 256-bit with secure cryptographic key was produced by fusing the extracted features and this key used in BIS.Security of the BIS is good as well as it gives better accuracy. Low level cryptographic techniques have been used in this biometric systems.

PROPOSED METHODOLOGY:



The block diagram of QC-SVM-MMBS is shown in figure(1)

GIVEN INPUT IMAGE:

We are giving the input to the biometric system like any biological characters Face, Iris, Palm(any two combinations).

IMAGE PRE-PROCESSING:

In this proposed method,three different biometric traits are used for recognition purpose and the captured images are shown in figure:2 face,iris,palm images are get from the database.Here,the Laplacian of Gaussian filter is utilized to enhance the image.

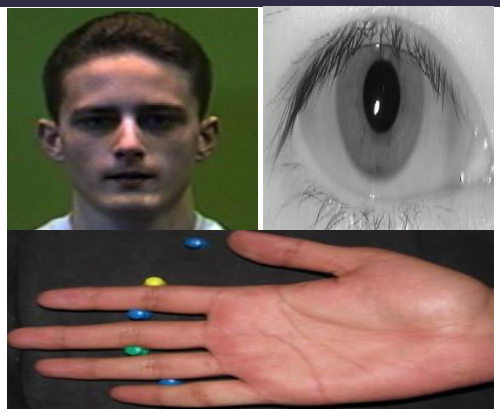


figure:2:Face,Iris,Palm

FEATURE EXTRACTION:

Enhanced image features are extracted in this section, Bidirectional Empirical Mode Decomposition(BEMD) feature value extraction is used for Iris feature detection, minutiae method is used for finger feature detection.

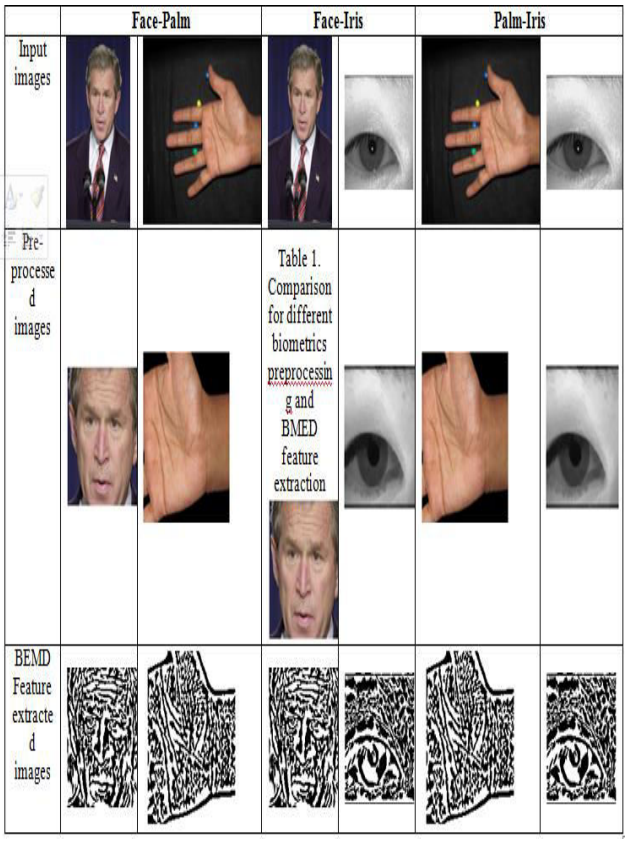


Figure:3: physical feature extraction face,iris,palm.

EMPIRICALMODE DECOMPOSITIONFEATURE EXTRACTION:

Empirical Mode Decomposition was extended from Empirical Mode

Decomposition. BEMD has been used in many fields. But in the field facial expression recognition system only few has been used.BEMD decomposes a complicated data in to a finite number components called the IMF's(Intrinsic Mode Function).An IMF should follow the two conditions

1. Number of extrema and zero crossings must either be equal to zero or differ by atmost one.
2. Mean value of envelop defined by local maxima and local minima should be zero.

The IMF's are obtained by process called shifting process. This process extract the local extrema for eachIMF.BEMD is suitable for non linear and no stationary data.

FUSION:

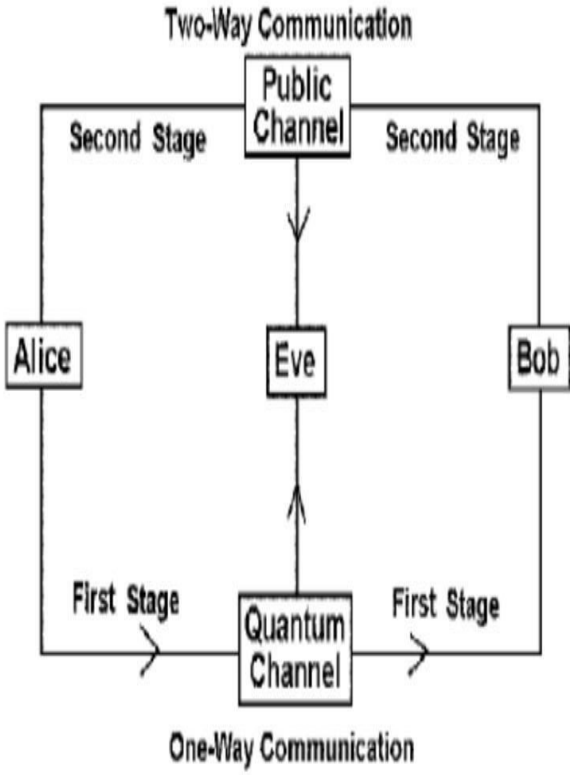
The feature extracted value are combined by the fusion process,which combines two distinct entities into new whole entities .In this FI-FLF-MMBS system extracted feature values are combined by the FLF technique.

QUANTUM CRYPTOGRAPHY:

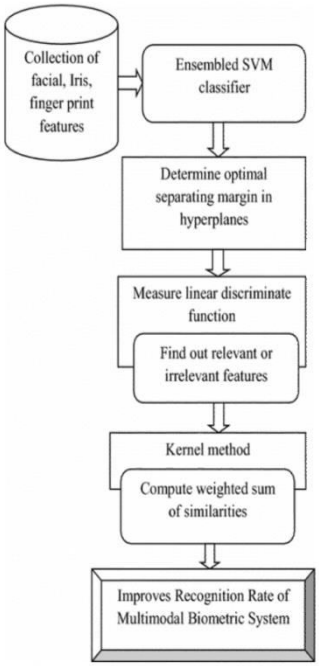
Quantum cryptography is the recent technique that can be used to guard the confidentiality of information transmitted between two devices, which is usually known as Alice and Bob,to protect the confidentiality of biometric system, Alice and Bob,who are commonly agreed in secret piece of information called as "key". By utilizing the behavior of photonswhich are also called as elementary particles. By combining the data with the key, no observer (or) hacker can see the information without knowing the key. This process is known as Encryption. It is difficult to unaccountable the information without knowing the secret key. To decrypt the data, the recipient uses the copy of the key. This is a reverse process to Encryption called as Decryption process.In the transmission time ,we should send the chain with two links. The chain involves the Quantum Distribution key and the Encrypted algorithm. If one of these two links is broken then the whole chain is compromised. Hence, we have to consider the strength of both links. QKD depends on the laws of quantum mechanics. Those are having a strange properties, with the nice result of making the spying discovered. An intruder was believed as Eve, tries to hack the key, intruder will be detected. The authorized parties will then discard the key, while no important information transmitted yet. If no tapping is noticed, the confidentiality of the distributed key is assured formally. The second link of the chain, the encryption algorithm must also have strong properties. As we discussed above the confidentiality of data is surely assured if the encryption key is as long as the message to transmit and is not reused for successive messages. This is where QKD is specifically useful. As it can administer long it is as frequently as wanted by Alice and Bob.QC is a process that uses quantum physics to fix the distribution of symmetric encryption keys. A more accurate name for it is" Quantum Key Distribution". It works by sending elementary particles like "photons" which comes from light, over an optical link.The Heisenberg uncertainty principles specified in quantum physics observation causes normal state. This is used to confirm the reliability of the Distributed Keys.It should be combined to One-Time pad encryption to achieve obvious protection. In practice, this would force strong restrictions on the obtainable bandwidth due to the fact that the key distribution rate of Quantum Key Distribution is usually 1,000 to 10,000 times lower than conventional optical communication. In practice, Quantum Key Distribution is combined with the conventional symmetric encryption, and used to often refresh encryption keys. A security solution is as protected as its weakest link and in network encryption, the

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

current weakest link is the key distribution based on PKC. As its name says, Quantum Key Distribution is used to distribute encryption keys, whose security is based on quantum physics and it is guaranteed for the long-term.
QKD solutions currently consists of key distribution appliances combined with link Encryptor[1].



SVM ALGORITHM CLASSIFICATION:



SVM supervises with associated learning algorithm which can analyze the data and extract patterns used for categorization and regression analysis.This SVM algorithm can also be used to linear and non- linear categorization.A set of training examples are taken from the training data for supervised learning. In any example we are having both input value and predicted output value. The training data is analyzed by supervised learning algorithm to get the predicted correct output categorization for the given set of data input. For example, teacher teaches student to identify the Papaya and Banana. By giving some features of those fruits then can easily identify them. When student sees Papaya or Banana he can easily identifies the difference between those fruits. The things based on his learning from his teacher, this is known as“supervised learning”. He can only make the difference between the Papaya and Banana. If he was given by a new thing, He cannot make sense of the features of other things.
The boundary of a linear classifier is the width. The length of the boundary can be increased before striking the data points of different category. Having the highest boundary between

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

the data sets, the line is secure. Support Vectors are defined as the data points which lie on the boundary line. To separate the two categories, we have to find the hyper plane. By using specific mathematical formulas, SVM cam perform thid by taking a set of points and dividing them using different applications. We can find the positive and negative hyper planes by using the above method. To find the hyper plane by following mathematical formulas are used.

(p.q)+r=+1(for positive) ----(1)

(p.q)+r=-1(for Negative) ----(2)

- **NON-LINEARLY SEPARABLE DATA IN SVM:**

We cannot separate Non-linear separable plane,data or input in an input space which cannot be separated with a linear Hyper plane. By using specific type of kernel,we can map all the points or to attributes space,to separate the Non-linear data on a plane. By using a curvy hyper plane we can separate the points in the attributes space and we can map points in the input space. It

φ(ω,ε)=1/2($\sum_{i=0}^{l}$ εi^{k})------(4)

ω.ω ¿+c¿

s.t.$yi = w.((x_i) - b \geq 1 - Ɛ$

and i=1,2,3….l

Types of kernel

1.Polynomial kernel with width d

K(x,y)=(x^{T} y+1)^{d}------(5)

2.Radial basis function kernel with width s

-¿|x-y|=V¿2/**(2σ))**

K(x,y)$^{¿}$=exp ¿ -----(6)

Recall (R)

Recall is the ratio between the amount of TP to the combination of TP and FN and the equation for the equation (7).

(p.q)+r=0(for Hyper) -----(3)

From the above equations by taking linear algebra ‘p’ and ‘r’ can be calculated.We get the formthat contains the results for ‘p’ and ‘r’ with boundary of2/2√(k.k)¯¯.The boundary is calculated as shown below.

Margin=2/2√k.k¯¯

This SVM algorithm model is used to classify the new data. The different classifications are categorized by taking the new upcoming data which is taken from the calculated boundary values.

will find the data sets which are not as simple as we’ll be have. Some of the points which are not correctly classified,those points are far from the classes or points mix together in a convolution or checkered patterns. Many researches have searched for the solution to acquip the problem of incorrect classification error using SVM algorithm. The following is minimized to create a soft-margin Hyper plane.

$$R = \frac{TP}{TP+FN} \quad (7)$$

Precision (P)

Precision is the ratio between the sum of TP and TN to the sum of TP, TN, FP and FN. This precision is also named as Positive Predictive (PP) value. The mathematical equation for Precision is given in the following equation. 8.

$$P = \frac{TP+TN}{TP+TN+FP+FN} \quad (8)$$

False measure

False measure or balanced F-score is the ratio between the harmonic mean of precision (P) and recall (R) to the sum of precision and recall, it is given in the following equation (9).

$$FM = \frac{2.R.P}{R+P} \quad (9)$$

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

Sensitivity (S_e)

Sensitivity (S_e) is also called as TP rate and it is a basic property of image processing, it is calculated by using equation (10).

$$S_e = \frac{TP}{TP+TN} \quad (10)$$

Performance	True Positive(TP)	True Negative (TN)	False Positive(FP)	False Negative (FN)	False Acceptance Ratio(FAR)	False Rejection Ration(FRR)
Face - Palm	2	17	1	0	0.0556	0.5
Face -Iris	1	18	0	1	0	0
Palm - Iris	2	16	2	0	0.1111	1

Specificity(S_p)

The negative characteristics of this FEP-RSA-MM is calculated by specificity (S_p), it is also named as TN rate. The mathematical equitation for S_p is shown in (11).

$$S_p = \frac{TN}{TN+TP} \quad (11)$$

Accuracy (A)

The computation of closeness between the input image and trained database. Quantity of the image is accurately represented by using the following equation (14).

$$A = \frac{TP+TN}{TP+FP+TN+FN} \quad (14)$$

Gmean

The harmonic mean of TP, TN, FP and FN is defined as the Gmean, it is also named as geometric mean. The following equation (15) represents the G-measure.

$$TP_{rate} = \frac{TP}{P}$$

$$TN_{rate} = \frac{TN}{P}$$

$$G_{mean} = \sqrt{TP_{rate} TN_{rate}} \quad (15)$$

False acceptance ratio (FAR) :

The FAR is the measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user.

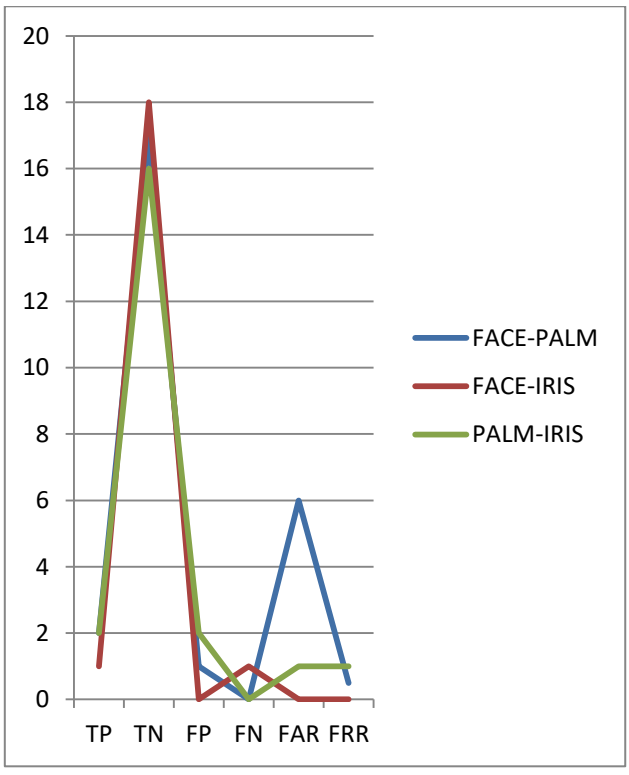
$$FAR = \frac{FP}{FP+TN} (12)$$

False Rejection Ratio (FRR)

FRR is the measure of the likelihood that the BSS will incorrectly reject an access attempt by an authorized user. The equation for FRR is given in the following equation (13).

$$FRR = \frac{FP}{TP+FN} (13$$

Table 2. QC-SVM-MMBS method performance



GRAPH FOR THE TABLE:2

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

RESULTS AND DISCUSSION:

The QC-SVM-MMBS system was analyzed with the help of MATLAB 2017b and the work was done by I_7 system with 8GB RAM. This QC-SVM-MMBS system developed with the biometric features of palm, face and iris to enhance the security of the desired system. The performance of the QC-SVM-MMBS system was evaluated in terms of Recall, Precision, False Measure, Sensitivity, specificity, Accuracy, False Rejection Ratio, False acceptance ratio and geometric mean.

There are three different biometric combinations are used in this QC-SVM-MMBS system such as Face & Iris, Face & Palm and Iris & Palm. From thesecombinations, the features are extracted by BMED. In QC-SVM-MMBS system, the specific person is identified by anyone biometric combination of same person. Initially, two images were taken from one person to extract the biometrics of 6 images. Totally 60 images of 10 people (20 images for face, 20 images for palm and 20 images for iris) were extracted and trained by QC-SVM-MMBS and it was stored in the database. Testing was performed by using 30 images of 10 people (10 images for face, 10 images for palm and 10 images for iris). The generation of database and testing is defined as follows.

In QC-SVM-MMBS training, three different data bases for three different combinations like Face & Iris, Face & Palm and Iris & Palm were generated. Here, the database generation of Face&Palm are explained in details. Hence, there are 20 face images and palm images were taken separately. The preprocessed image of face presented in Figure.5.a, and this preprocessed image is converted into grayscale. Then the image is reshaped at the size of 128□128, it is shown in Figure.5.b. After that the BEMD algorithm extracts the features from the respective face image is shown in Figure.5.c. Likewise, the palm segmentation is used in the palm images that is shown in Figure.6.a. The preprocessing of palm images is achieved by converting the RGB to grayscale images and the features are extracted by BEMD algorithm that is shown in Fig. 6.b and Fig. 6.c

Figure.5a. Input image, b. Preprocessed image, c. BEMD feature extraction

(a) (b) (c)

respectively. These two features (face and palm features) are fused by the feature level fusion (data fusion). QC encryption takes place on the fusion images, then it is encrypted and stored in the data base. Beside the QC-SVM-MM testing is performed, in that one image is taken and it is converted from RGB to grayscale. BEMD is used for extracting features from the images. Before performing the matching progress, the images from the database are decrypted by using qc. By using the decrypted features and individual features, the identification of a specific person is performed with the help of matching.

Figure.6.a. Input image, b. Preprocessed image, c. BEMD feature extraction

Iris,Face & palm and Iris & Palm. BEMD feature extraction and Data fusion of testing is same like the QC-SVM-MMBS training. Based on the correlation function, the similarity between the specific person to the database images are discovered.

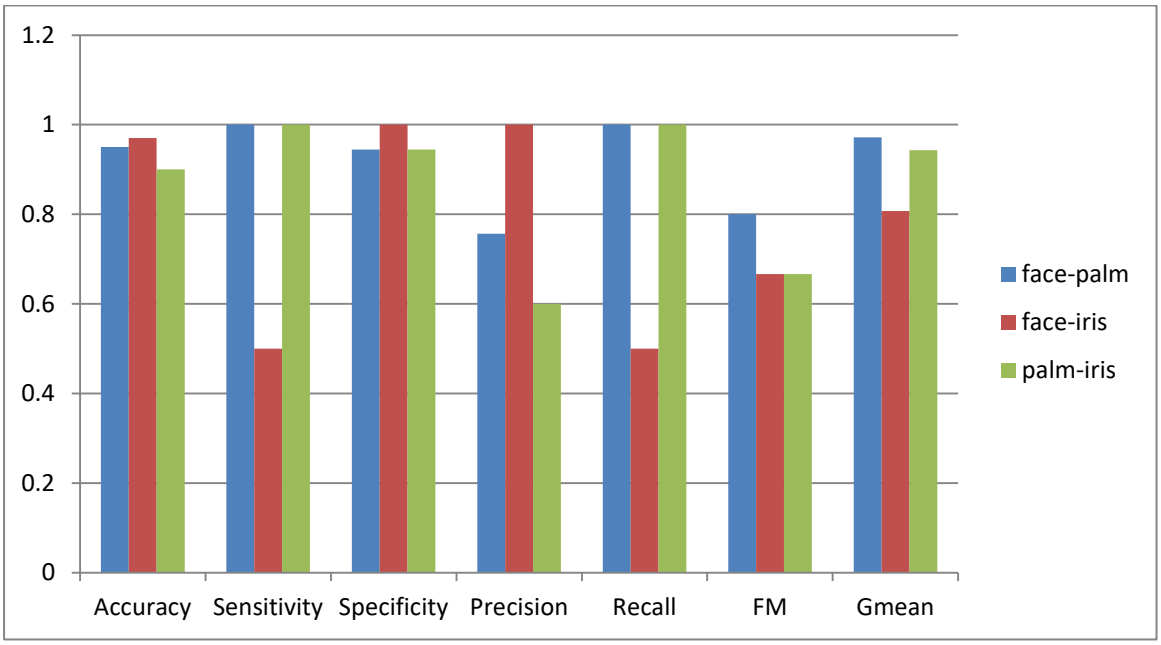
International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

The extracted BEMD features of the face and palm images are combined by feature level fusion, that is shown in the following. These fusion values of face and palm are encrypted by QC encryption and it is stored in the database.

The input images which are used in the training is taken as input to the testing section. Testing also takes three different combinations such as Face and

Table2:. QC-SVM-MMBS method performance

Performance	Accuracy	Sensitivity	Specificity	Precision	Recall	False Measure	G-mean
Face- Palm	0.9500	1.0000	0.9444	0.7567	1.0000	0.8000	0.9718
Face-Iris	0.9700	0.5000	1.0000	1.0000	0.5000	0.6667	0.8071
Palm - Iris	0.9000	1.0000	0.9432	0.6000	1.0000	0.6667	0.9428



Performance	TP	TN	FP	FN	FAR	FRR
Face-Palm	2	17	1	0	0.0556	0.5
Face-Iris	1	18	0	1	0	0
Palm - Iris	2	17	1	0	0.1111	0.5

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

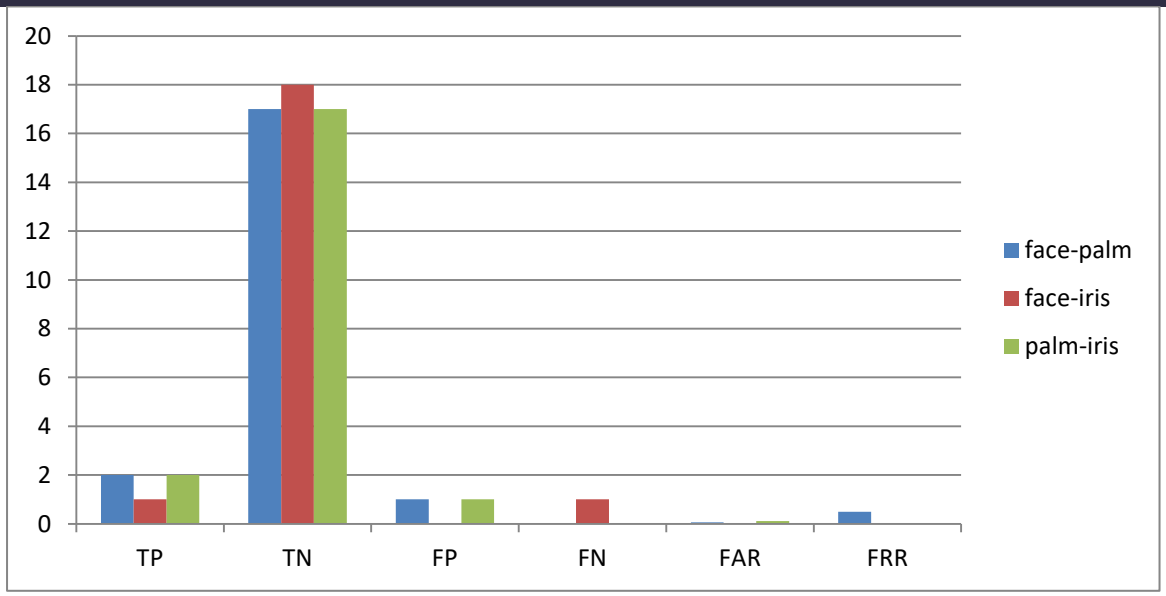
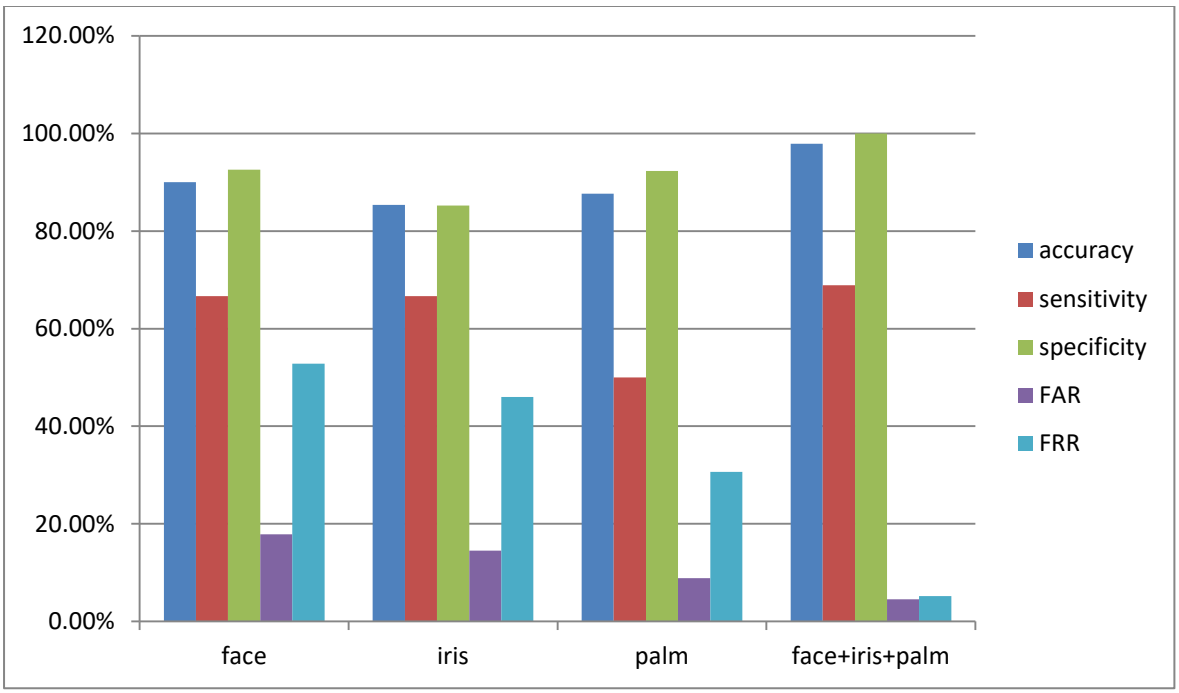


TABLE:4: PERFORMANCE ANALYSIS OF THE PROPOSED METHOD

Performance parameters	Face	Iris	Palm	Face+ Iris+ Palm
Accuracy	90.00%	85.33%	87.67%	97.87%
Sensitivity	66.67%	66.67%	50.00%	68.87%
Specificity	92.59%	85.19%	92.31%	100%
FAR	17.86%	14.54%	8.90%	4.56%
FRR	52.82%	45.98%	30.67%	5.23%

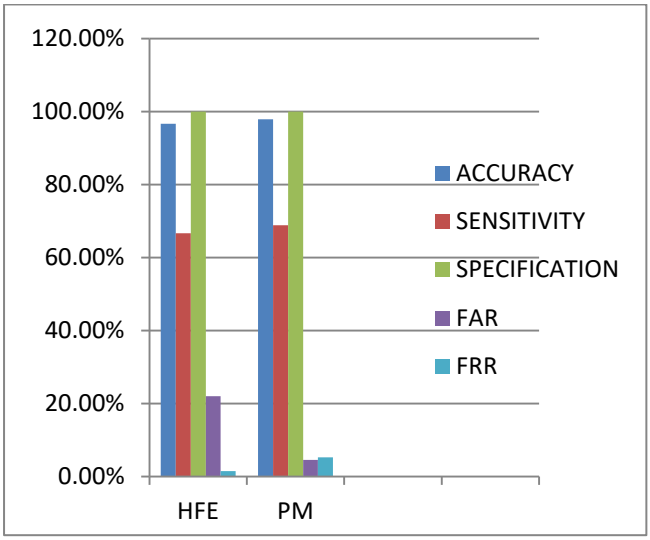


Comparative analysis of the QC-SVM-MMBS method

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COMPARATIVE ANALYSIS OF THE PROPOSED METHODS:

PERFORMANCE PARAMETERS	HFE-DCLM-MMBS	PROPOSED METHOD
ACCURACY	96.67%	**97.87%**
SENSITIVITY	66.67%	**68.87%**
SPECIFICITY	100%	**100%**
FAR	22%	**4.56%**
FRR	1.5%	**5.23%**



CONCLUSION:

The great achievement in Biometric systems is considered as Quantum Cryptography for the purpose of High-security and Accuracy. This is based on QKD. This helps in error reduction and increase the Accuracy rate. When compared to other Cryptographic techniques Quantum Cryptography is Accurate and Reliable. Hence this is used highly now-a-days.

REFERENCES:

[1] https://www.idquantique.com/quantum-safe-security/overview/qkd-technology/?gclid=Cj0KCQjwy97qBRDoARIsAITONTJ8MR9g80tbkcivHTUccas0trbxL4IV51tQzMYFMCv_Der1B6WXyD8aAK9NEALw_wcB

Amirthalingam, Gandhimathi, "New chaff point based fuzzy vault for multimodal biometric cryptosystem using particle swarm optimization 28.4 (2016): 381-394.

V.Sireesha, and S.R.K Reddy "Two levels fusion based Multi-Modal Biometric authentication using Iris and finger print modalities", International Journal of Intelligent Engineering and Systems,Vol.9,No.3,pp.21-35,2016.

M.S. Aslan, Z. Hailat, T.K. Alafif, and X.W. Chen, "Multi-channel multi-modal feature learning for face recognition",*Pattern Recognition Letters*,Vol.85,pp.79-83, 2017.

A. Jagadeesan, T. Thillaikkarsai, and K. Duraiswamy, "Cryptographic key generation from multiple biometric modalities: Fusing minutiae with iris feature",*International Journal of Computer Applications*,Vol.2, No.6,pp.16-26, 2010.

M.S.M. Asaari, S.A. Suandi, and B.A. Rosdi, "Fusion of band limited phase only correlation and width centroid contour distance for finger-based biometrics",*Expert Systems with Applications*,Vol.41, No.7,pp.3367-3382

Nagar, Abhishek, Karthik Nandakumar, and Anil K. Jain. "Multibiometric cryptosystems based on feature-level fusion." IEEE transactions on information forensics and security 7.1 (2012): 255-268.

Mai, Guangcan, Meng-Hui Lim, and Pong C. Yuen. "Binary feature fusion for discriminative and secure multi-biometric cryptosystems." Image and Vision Computing 58 (2017): 254-265.

Palandurkar, Ashish P., Pragati N. Patil, and Yogesh C. Bhute. "Cryptosystem based Multimodal Biometrics Template Security."International Conference on Quality Up-gradation in Engineering, Science and Technology (ICQUEST-2014), pp. 16-20, 2014.

Muthukumar, A., C. Kasthuri, and S. Kannan. "Multimodal biometric authentication using particle swarm optimization algorithm with fingerprint and iris." ICTACT journal on image and video processing 2.3 (2012): 369-374.

Sheena, S., and Sheena Mathew. "MULTIMODAL BIOMETRIC AUTHENTICATION: SECURED ENCRYPTION OF IRIS USING FINGERPRINT ID."International Journal on Cryptography and Information Security (IJCIS), Vol. 6, No. 3/4, pp. 39-46, December 2016.

M. Soltane, N. Doghmane, and N. Guersi, “Face and speech based multi-modal biometric authentication”.

D. Vaidya, Sheetal Pawar, Madhuri A. Joshi, A. M. Sapkal, S. Kar, “Feature level fusion of palmprint and palm vein for personal authentication based on Entrophy technique”,*International Journal on Electronics and communication Technology*, Vol.5, No.spl-1, pp.53-57, 2014

.

S.F. Bahgat, S. Ghoniemy, and M. Alotaibi, “Proposed multimodal palm veins-face biometric authentication”,2013.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org