iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** V **Month of publication:** May 2023

DOI: https://doi.org/10.22214/ijraset.2023.49548

www.ijraset.com

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

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

Development of an Improved Access Control System using an Enhanced Bimodal Crypto-Biometric System

Rejuaro O. O.[1], Adetunji A. B.[2], Adedeji F.[3], Falohun A. S.[4], Iromini N. A.[5], Adebajo O.O.[6]
[1]*Department of Computer Engineering, Ladoke Akintola University of Technology, Ogbomoso, Nigeria*
[2]*Department of Computer Science, Ladoke Akintola University of Technology, Ogbomoso, Nigeria*
[3]*Department of Computer Science, Leadcity University, Ibadan, Nigeria*
[4]*Department of Computer Engineering, Ladoke Akintola University of Technology, Ogbomoso, Nigeria*
[5]*Department of Computer Engineering, Federal Polytechnic, Offa, Kwara State*
[6]*Department of Computer Engineering, Ladoke Akintola University of Technology, Ogbomoso, Nigeria*

Abstract: ***Recently, biometric was being integrated with cryptography (crypto-biometric system) to alleviate the limitations of the biometric or cryptography system. However, the main shortcoming of cryptography is poorly-chosen or forgotten password while challenges with biometrics include interclass similarities in the feature sets used to represent traits. In this work, a combination of cryptography and bimodal biometric was developed, an Advanced Encryption Standard based Fast Fourier Transform (AES-FFT) was developed and used as the cryptography technique. Hence, an attempt was made to develop an improved access control system using an enhanced bimodal bio-cryptography. Biometric features was extracted from individual face and iris after application of suitable preprocessing techniques for each modality using Principal Component Analysis (PCA) while cryptography key was generated using fused features from the face and iris by Advanced Encryption System based Fast Fourier Transform (AES-FFT). The two captured biometric data at acquisition module via webcam were subjected to appropriate pre-processing and feature extraction module. The features extracted were fused at feature level using weighted average and optimal features were selected using genetic programming (GP). The classification technique used was Support Vector Machine (SVM).***

To supplement the enhancement of the system's integrity, templates and encrypted data were stored in a database. Access to the database was secured with AES-FFT algorithm. Thereafter, an Access Control System was simulated using MATLAB (version R2020b) and evaluated using False Acceptance Rate (FAR), False Rejection Rate (FRR), Equal Error Rate (ERR) and Accuracy. The evaluation results showed that the FAR, FRR, ERR and Accuracy of the fused features using AES-FFT were 1.67, 2.22, 2.78 and 97.92% respectively at 0.76 threshold while for AES, the best values obtained for FAR, FRR, ERR and Accuracy were 3.33, 4.44, 7.90 and 95.83% respectively at same threshold. In view of this, an automated bi-modal crypto-biometric system based on fused iris and face (that is, both face and iris), produced a more reliable accurate and secure system on any repository system as a result of its high accuracy. In other words, the developed AES-FFT technique ensured scalable encrypting capacity, good imperceptibility and security performance, and robustness against various attacks with optimal computational efficiency in terms of its accuracy and time.

Keywords: Encryption, Bio-cryptography, Biometric, Access Control System.

I. INTRODUCTION

Access control in computing is motivated by the need to divulge access to information and available computing resources and services to authorized entities only, through authentication, authorization, and access control. A secure transmission of data for access control system become very important in Information and Communication Technology. A third party can trap data or steal important data stored in a computer. To prevent this, it is advocated to encrypt the messages to provide Information Security (Oluwadamilola *et al*., 2017).

Biometric identification is an emerging technology which gains more attention in recent years. It employs physiological or behavioral characteristics to identify an individual (Richard *et al*., 2007, Omidiora *et al.*, 2015). The combination of biometric data systems and biometrics recognition/identification technologies create the biometric security systems. The biometric security system is a lock and capture mechanism to control access to specific data. In order to access the biometric security system, individuals will need to provide their unique characteristics or traits which will be matched to a database in the system. If there is a match, the locking system will provide access to the data for the user. The locking and capturing system will activate and record information of users who accessed the data (Falohun *et al.*, 2016).

Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. The integration of biometric with cryptography, deals with either cryptographic key release or cryptographic key generation, and is promising in many aspects. Cryptography is the science of using mathematics to encrypt and decrypt data to keep messages secured by transforming intelligible data form (plaintext) into unintelligible form (ciphertext) (Marwa *et al.*, 2016). Cryptography is also a branch of science that define the art of secret writing, and it is a technique in which secret data is changed by its character in such a way that any intruder cannot identify the message. As biometric is directly linked with the owner, it removes the problem of memorizing the cryptographic key and confirms the non-repudiation of users (Jain *et al.*, 2014). The authentication systems which integrate biometric traits with cryptography are called crypto-biometric systems (Hao *et al.* 2006).

In this research, a combination of cryptography and bimodal biometric was developed, an Advanced Encryption Standard based Fast Fourier Transform (AES-FFT) was developed and used as the cryptography technique.

II. RELATED WORKS

Jagadeesan *et al.*, (2010) proposed an efficient approach based on multimodal biometrics (iris and fingerprint) for generating a secure cryptographic key, where the security is further enhanced with the difficulty of factoring large numbers. At first, the features, minutiae points and texture properties are extracted from the iris and fingerprint images respectively. Then, the extracted features are fused at the feature level to obtain the multi-biometric template. Finally, a multi-biometric template is used for generating a 256-bit cryptographic key. For experimentation, the study used the fingerprint images obtained from publicly available sources and the fingerprint images from CASIA Iris Database. The experimental results showed that the generated 256-bit cryptographic key is capable of providing better user authentication and better security.

Wang et al., (2011) proposed a novel multimodal biometric system using face-iris fusion feature. Face feature and iris feature are first extracted respectively and fused in feature-level. However, existing feature level schemes such as sum rule and weighted sum rule are inefficient in complicated condition. In this paper, we adopt an efficient feature-level fusion scheme for iris and face in series. The algorithm normalizes the original features of iris and face using z-score model to eliminate the unbalance in the order of magnitude and the distribution between two different kinds of feature vectors, and then connect the normalized feature vectors in serial rule. The proposed algorithm is tested using CASIA iris database and two face databases (ORL database and Yale database). Experimental results show the effectiveness of the proposed algorithm.

Zuva et al., (2014) proposed using both fingerprint and face for authentication in access system. The study integrated fingerprint and face biometric to improve the performance in access control system. This paper considered restoration of distorted and misaligned fingerprints caused by environmental noise such as oil, wrinkles, dry skin, dirt, displacement etc. The noisy, distorted and/or misaligned fingerprint produced as a 2-D on x-y image, is enhanced and optimized using a hybrid Modified Gabor Filter-Hierarchal Structure Check (MGF-HSC) system model. In face biometric, Fast Principal Component Analysis (FPCA) algorithm was used in which different face conditions (face distortions) such as lighting, blurriness, pose, head orientation and other conditions are addressed. The algorithms used improved the quality of distorted and misaligned fingerprint image. They also improved the recognition accuracy of distorted face during authentication. The results obtained showed that the combination of both fingerprint and face improve the overall performance of biometric authentication system in access control.

Barman *et al.*, (2015) proposed an approach to generate cryptographic key from cancelable fingerprint template of both communicating parties. Cancelable fingerprint templates of both sender and receiver are securely transmitted to each other using a key-based steganography. Both templates are combined with concatenation-based feature level fusion technique and generate a combined template. Elements of combined template are shuffled using shuffle key and hash of the shuffled template generates a unique session key.

In this approach, revocable key for symmetric cryptography is generated from irrevocable fingerprint and privacy of the fingerprints is protected by the cancel able transformation of fingerprint template. Our experimental results show that minimum, average, and maximum Hamming distances between genuine key and impostor's key are 80, 128, and 168 bits, respectively, with 256-bit cryptographic key. This fingerprint-based cryptographic key can be applied in symmetric cryptography where session based unique key is required.

Abuguba *et al.,* (2015) presented an efficient approach to secure cryptographic key generation from iris and face biometric traits. Features extracted from preprocessed face and iris images are fused at the feature level and the multimodal biometric template is constructed from the Gabor filter and Principal Component Analysis outputs. This template is used to generate strong 256-bit cryptographic key. Experiments were performed using iris and face images from CASIA and ORL databases and the efficiency of the proposed approach is confirmed.

Selvarani and Visu (2015) presented personal identification using fingerprint and Iris biometric technology. Usually unimodal biometric techniques are used. Cloud computing provides many resources, very convenient charged service and minimum cost computing. This leads the cloud computing to become the most dominant computing in the recent years. Even though the cloud provide secured service, it also undergoes with some security problem especially form hackers. The existing unimodal bio cryptography techniques often have limitations such as consciousness to noise, intra class consistency, data aspect and other factors. This research study presents personal identification using fingerprint, iris and cryptographic technologies. Combined biometric technology will secure the data from unauthorized users. The purpose of this study is to study the combination of fingerprint and iris and also to include the cryptographic methods to achieve the higher accuracy and more security. The result of this study can overcome some of the limitations of using single biometric technology. The combination of Finger print and Iris form the key for Blowfish algorithm to store the secured data from unauthorized users in cloud environment.

Oluwadamilola *et al.,* (2017) presented combination of cryptography and biometrics; a bimodal biometric cryptosystem, using fingerprint and face as trait for authentication. Subjects' information was encrypted using Advanced Encryption Standard (AES) and biometric templates were stored as Binary Large Object (BLOB) in MYSQL database secured with Message Digest 5 (MD 5) Hashing Algorithm. The system was developed and implemented to operate on one-try, two-try and three-try configurations at varying threshold values. The developed system's performance was evaluated using False Reject Rate (FRR), False Accept Rate (FAR) and Receiver Operating Characteristic Curve (ROC graph) as performance metrics. On ROC graph, three-try configuration gave optimal performance at all threshold values.

Okokpujie *et al.,* (2018) proposed bimodal biometrics (fingerprint and iris) as a means of ensuring the full integrity of the bank's vault system, thus, further reducing the rate of compromise and theft within the bank's vault system. A scanner captures the fingerprint and the iris of authorized users. The images of the fingerprint and iris captured by the scanner are segmented, normalized and made into templates that are stored in a database along with the particulars of the users. The accuracy of the system is measured in terms of sample acquisition error and recognition performance using False Accept Rate (FAR), False Identification Rate (FIR) and False Reject Rate (FRR). The result shows that the proposed system is very effective.

Komal (2019) studied a robust multimodal biometric crypto system, in which two modalities (FKP and face) are used for authentication of a person and one modality (fingerprint) is used for key generation. AES algorithm with fingerprint-based key is used for securing the biometric templates. At authentication time, decision level fusion with AND rule is used for making the final decision. The proposed multimodal biometric crypto system is more robust and secure as compare with other multimodal biometric systems.

Venna and Inampudi (2019) developed a multimodal biometric authentication system (MMBAS) using face, fingerprint and retina images and key generation is also done using these images. Images were pre-processed using adaptive median filtering and Otsu's segmentation algorithm for background subtraction. Then minutiae feature of these images were extracted with the use of Local Binary Pattern (LBP) algorithm and then the feature vectors of face, fingerprint and retina are fused using XOR operation. Later the fused feature vector was used for cryptographic key generation. The evaluation was performed on network security for showing the reliability of the newly introduced approach in terms of Precision, Recall, Accuracy and false rejection rate.

In light of the above reviewed work, Seshadri and Trivedi (2011) described several types of cryptosystems available for biometry applications such as key release, key binding and key generation cryptosystems, most of the researchers majorly focused on key release cryptosystems but paid less attention to key binding cryptosystems, the computational cost of the encryption and decryption

of images as well as the required memory space for the encrypted data. Also, it was discovered that some of these techniques were susceptible to attack and were characterized with visual distortions after authentication. Therefore, this work will adopt an enhanced AES technique which focuses on key binding for encryption and decryption for data security and confidentiality. The scheme that will be used in this study, is targeted at ensuring scalable encrypting capacity, good imperceptibility and security performance, and robustness against various attacks with optimal computational efficiency.

III. METHODOLOGY

The bimodal biometric-cryptography system comprised of quite a few modules to authenticate or verify subjects. The system was divided into two stages; enrolment and authentication as shown in Figure 3.1. In this approach, biometric features were extracted from individual's face and iris after application of histogram equalization for face and iris, iris localization using Hough transform and iris normalization using Daugman's rubber sheet model for each modality. Features were extracted using Principal Component Analysis (PCA) while cryptography key was generated using fused features from the face and iris by Advanced Encryption System based Fast Fourier Transform (AES-FFT). The features extracted were fused at feature level using weighted average and optimal features were selected using genetic programming (GP). Support Vector Machine (SVM) was used to classify the extracted features. To enhance the integrity of the system, templates and encrypted data were stored in a database.
Details of the modules are as follows:

A. Enrolment Stage

Enrolment stage comprised of collection of biometric information (face and iris). At this stage, fused features of face and iris were the means for subject to indicate personal identity for authentication. The dataset used contained 600 iris images and 600 face images, 360 of the iris images and 360 of the face images were used in training the model while 240 of the iris images and 240 of the face images were used to test the model used for authentication. The enrolment stage of the system was made up of the sensor module (enrolment module), pre-processing module, feature extraction module, fusion and feature selection module and encryption and decryption module. At this phase, a webcam device was used to acquire face and iris biometric data of users. Face and iris images of 600 subjects with 3 different samples were captured with a size of 640 by 480 pixels. The two biometric traits were downsized into 128 by 128 pixel without any alteration in the images. All images taken had equal uniform illumination conditions and light color background. The database was populated with 1200 images.

1) Image pre-processing

The preprocessing stage involved enhancement of image by using histogram equalization for face and iris, converting the colored image into grayscale, cropping the image and normalizing of face vectors by computing the average face vector and deducting average face from each face vector. In the case of iris, other pre-preprocessing and segmentation process adopted in this study were iris localization using Hough transform and iris normalization using Daugman's rubber sheet model.

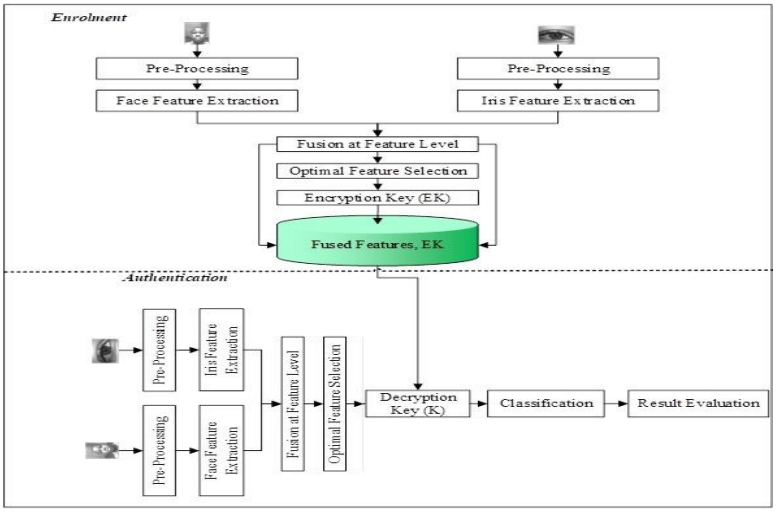


Figure 3.1: Architecture of the developed bimodal biometric cryptography system

2) Feature Extraction Module

Significant collection of basic parameters (face and iris features) that best illustrate the specific array of face and iris expressions were extracted from the pre-processed image of each subset and were used to discriminate between expressions. The extracted face and iris features were encoded and stored as weight vectors for each expression in order to compare it to other expressions in the training dataset. The relevant information was extracted from the variable part of the iris and face such as the coordinates of the pupil and two biometric boundaries. Principal Component Analysis (PCA) was employed in this study to extract features and reduce the dimension sizes of images. The resultant feature representation presents a suitable platform for selecting the optimal feature subsets.

The steps for the PCA algorithm are as follow:

a) Step 1: The normalized training image in the *N*-dimensional space is stored in a vector of size *N*. Let the normalized training face image set,

$$\mathrm{T} = \{X_1, X_2, \ldots, X_N\} \text{ where } T = \{x_1, x_2, x_3, \ldots, x_N\}^{\mathrm{T}} \quad 3.1$$

b) Step 2: Create Eigen space

Each of the normalized training face images is mean centered. This was done by subtracting the mean face image from each of the normalized training images.

$$\bar{X}_i = \bar{X}_i - \bar{X} \quad 3.2$$

Where the average of the training face image set is defined as:

$$\bar{X} = \frac{1}{N}\sum_{i=1}^{N} \bar{X}_i \quad 3.3$$

The training images was combined into a data matrix of size *N* by *P*, where *P* is the number of training images and each column is a single image.

$$\bar{X} = \{\bar{X}_1, \bar{X}_2, \ldots, \bar{X}_p\} \quad 3.4$$

The column vectors are combined into a data matrix which is multiply by its transpose to create a covariance matrix. The covariance is defined as:

$$\Omega = \bar{X}.\bar{X}^T \quad 3.5$$

The eigenvalues and corresponding eigenvectors was computed for the covariance matrix using Jacobian transformation,

$$\Omega V = \Lambda V \quad 3.6$$

Where *V* is the set of eigenvectors associated with the eigenvalues Λ. The eigenvectors $\boldsymbol{Vi \in V}$ are order according to their corresponding eigenvalues $\boldsymbol{\lambda \in \Lambda}$ from high to low with non-zero eigenvalues.

$$\mathrm{V} = \{V_1, V_2, \ldots, V_p\} \quad 3.7$$

c) Step 3: Project Training Images

Each of the centered training images were projected into the Eigen space. The projected training images were computed based on the dot product of the centered training images with each of the ordered eigenvectors denoted as,

$$T_p = V^T \bar{X}_i \quad 3.8$$

The new vectors of the projected images were the feature vectors of the training face images. The feature vector is defined as

$$X_p = \{P_1, P_2, P_3, \ldots, P_m\}^{\mathrm{T}} \quad 3.9$$

d) Step 4: Project Testing Image

The vector of the testing face image $\boldsymbol{Y_s}$ is initially mean centered by subtracting the mean image.

$$\bar{Y} = Y - \bar{X} \quad 3.10$$

The feature vector of the testing image Y_p is obtained by projecting the vector of the mean testing face image $\bar{Y}$ into the Eigen space or the principal components,

$$Y_p = V^T \bar{Y} \quad 3.11$$

The eigenvectors is sorted according to their corresponding eigenvalues from high to low. Then, the eigenvectors corresponding to zero eigenvalues will be discarded while those associated with non-zero eigenvalues were kept. Consequently, the Eigen faceprint is formed.

e) Feature Selection using Genetic Programming

Genetic programming typically starts with a population of randomly generated computer programs composed of the available programmatic ingredients (as provided by the human user in the first and second preparatory steps). Genetic programming iteratively transforms a population of computer programs into a new generation of the population by applying analogs of naturally occurring genetic operations. These operations were applied to individual(s) selected from the population. The individuals were probabilistically selected to participate in the genetic operations based on their fitness (as measured by the fitness measure provided by the human user in the third preparatory step). This Genetic Programming was to select optimal features from the face print and iris extracted features. The procedural steps of genetic programming are as follows:

- Randomly create an initial population (generation 0) of individual computer programs composed of the available functions and terminals.
- Iteratively perform the following sub-steps (called a generation) on the population until the termination criterion is satisfied:
  - Execute each program in the population and ascertain its fitness (explicitly or implicitly) using the problem's fitness measure.
  - Select one or two individual program(s) from the population with a probability based on fitness (with reselection allowed) to participate in the genetic operations in (c).
  - Create new individual program(s) for the population by applying the following genetic operations with specified probabilities:
    i. Reproduction: Copy the selected individual program to the new population.
    ii. Crossover: Create new offspring program(s) for the new population by recombining randomly chosen parts from two selected programs.
    iii. Mutation: Create one new offspring program for the new population by randomly mutating a randomly chosen part of one selected program.
    iv. Architecture-**altering operations:** Choose an architecture altering operation from the available repertoire of such operations and create one new offspring program for the new population by applying the chosen architecture-altering operation to one selected program.
- After the termination criterion is satisfied, the single best program in the population produced during the run (the best-so-far individual) is harvested and designated as the result of the run. If the run is successful, the result may be a solution (or approximate solution) to the problem.

- *Weighted Average Fusion Technique*

The extracted features of face and iris respectively were normalized using the min-max technique. The normalization of both features by the min-max rule are given by equation 3.12 and 3.13:

$$f_{face} = \frac{f'_{face} - \min(f'_{face})}{\max(f'_{face}) - \min(f'_{face})} \quad 3.12$$

$$f_{iris} = \frac{f'_{iris} - \min(f'_{iris})}{\max(f'_{iris}) - \min(f'_{iris})} \quad 3.13$$

Where f'_{face} and f'_{iris} were the features obtained from face and iris respectively, while f_{face} and f_{iris} were the normalized features. Weighted Average (WA) was used to fuse the normalized features. The fused features were achieved using equation 3.14.

$$fit = \sum_{m=1}^{M}\sum_{n=1}^{N} \frac{\omega_1(f_{face}) + \omega_2(f_{iris})}{\omega_1 + \omega_2} \qquad 3.14$$

Where ω_1 is the weight of the *face features* and ω_2 is the weight of the *iris features.*

- *Encryption and Decryption Module*

The biometric information submitted in the database was encrypted using Advanced Encryption Standard with Fast Fourier Transform (AES-FFT) cryptography algorithm. This is to safeguard that subject biometric information is not saved in its original or plain biometric form in other to enhance the system security. AES-FFT algorithm works on the principle of Substitution Permutation network. The AES-FFT cipher was identified as a number of reiterations of transformation rounds that translate the input plaintext into the final output of cipher text. The encryption key was generated from fused face-iris biometric template of each subject. Consequently, the system used a secret and unique key to protect personal data. A set of reverse rounds were applied to transform cipher text back into the original plaintext using the same encryption key. Figure 3.2 expressed the basic structure of AES-FFT.

f) AES

The following steps was used for encryption and decryption:

- Step 1: Derive the set of round keys from the cipher key.
- Step 2: Initialize the state array with the block data (plaintext).
- Step 3: Add the initial round key to the starting state array.
- Step 4: Perform nine rounds of state manipulation.
- Step 5: Perform the tenth and final round of state manipulation.
- Step 6: Copy the final state array out as the encrypted data (cipher text).
- Step 7: Each round of the encryption process requires a series of steps to alter the state of array. These steps involve four types of operations. They are,

SubBytes: This operation is a simple substitution that converts every bite into a different value.
ShiftRows: Each row is rotated to the right by a certain number of bytes.
MixColumns: Each column of the state array is processed separately to produce a new column. The new column replaces the old one.
XorRoundKey: This operation simply takes the existing state array.
Decryption involves reversing all the steps taken in encryption using inverse functions like InvSubBytes, InvShiftRows , InvMixColumns.

g) AES-FFT

Fast Fourier Transform was applied on the image I(x,y) to obtain FFT coefficients of the images. The image features after application contained the real part, imaginary part, and magnitude value and phase angle. FFT is fast and its efficiency was enhanced by real part of the obtained coefficients. The Fast Fourier Transform (FFT) definition is given as

$$C_k = \frac{2}{N}\omega(k)\sum_{n=0}^{N-1} x_n Cos\left(\frac{2n+1}{2N}\pi k\right), \quad 0 \le k \le N-1 \qquad 3.15$$

$$x_k = \sum_{n=0}^{N-1} C_n Cos\left(\frac{2n+1}{2N}\pi k\right), \quad 0 \le n \le N-1 \qquad 3.16$$

FFT was used as modification factor on Shift Row Transformation step and on mix column transformation of AES algorithm. Every other steps of AES algorithm remains the same, except that some modification was made at “ShiftRows” and “MixColumn” level using FFT as enumerated in equation (3.15) and (3.16). The two modification steps are described as follow.

a) *ShiftRows:* If the element of first row and first column is even then first and fourth row remain unchanged and each byte in the second and third row of the state is cyclically shifted right over different number. If the element of first row and first column is odd then first and third row remain unchanged and each byte in the second and fourth row of the state is cyclically shifted right over different number.

b) *MixColumn:* In the mix column the 128-bit arranged as a 4*4 state matrix are operated column by column. The four elements of each column form a five-term polynomial that is multiplied by constant polynomial A(Y) = $\{03\}X^4 + \{01\}X^3 + \{01\}X^2 + \{01\}X + \{02\}$ with module X^5+1 gets the new state matrix. After getting the state matrix from step 1 then interchanging the rows and column of the matrix.

The structure of the AES-FFT is shown in Fig. 3.2.

B. Authentication Stage

At the authentication stage, subject presented his/her face and iris biometric data. Thereafter, preprocessing of the two biometric traits was introduced. Face was acquired and segmentation was employed in case of iris. Then features extracted were fused and optimal features were selected from the fused features and matched with the enrolled data linked. The authentication stage included a section of the enrolment module (Acquisition module, pre-processing module, feature extraction module and fused and feature selection module), matching module that compared optimal features with stored template, and recognition module which determined authentication outcome based on match score. For a subject to be granted access, fused face and iris image must match the enrolled templates at the same time decrypted. The flowchart for the authentication module is shown in Figure 3.3.

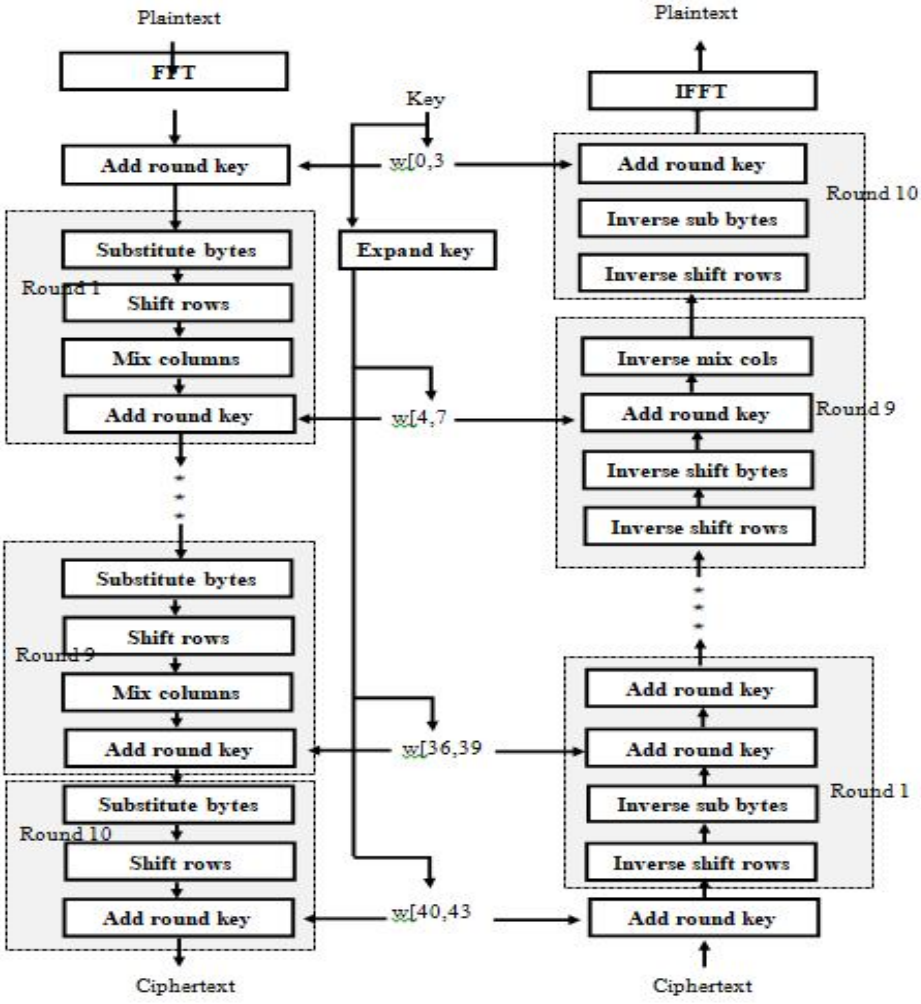


Figure 3.2: The Structure of AES-FFT

1) Classification Module

In this research, support vector machine (SVM) was used for the recognition of fused features. Firstly, the support vector was trained before testing with the matching operation. The optimal selected features of all the images in the data set were the input of the support vector machine.

Support Vector Machine classifier was used after feature selection of the fused features. They involved learning and classifying as supervised. Recognition took place by setting a threshold value for the system. Threshold is a user set value for the authentication system. Threshold is the acceptance or rejection of a bimodal template match which is dependent on the match score falling above or below the threshold.

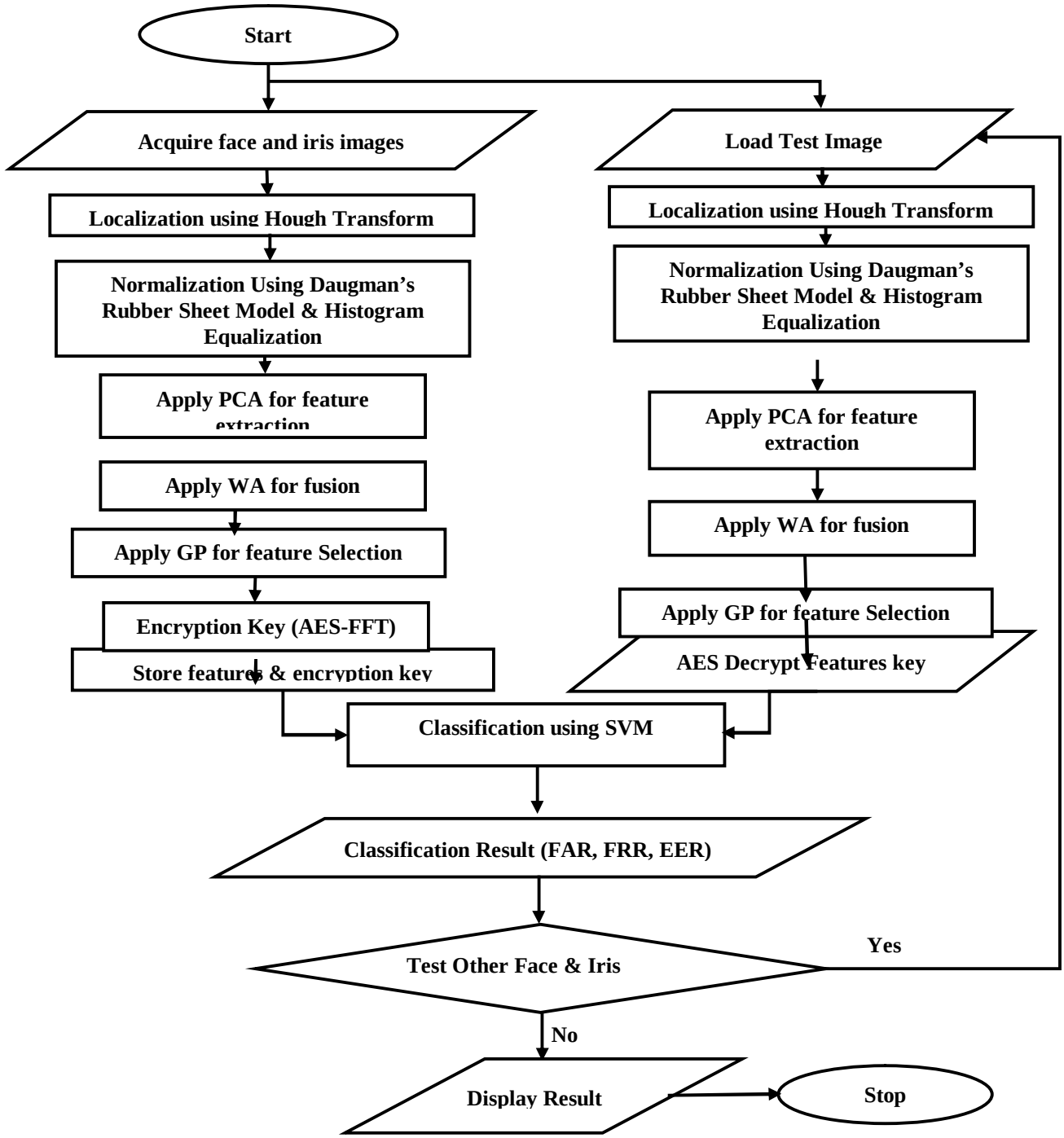


Figure 3.3: Flowchart for authentication module

2) Classification Using SVM

The features achieved using feature selection were classified using SVM. The selected best global position (w_i) of the GP trained the SVM with the detected feature subset mapped by w_i and modelled with the optimized parameters C and σ using equation (3.9).

$$\min \ \frac{1}{2}\|w_i\|^2 + C\sum_{i=1}^{N}\xi_i \qquad Such\ that \quad \sum_{i=1}^{N} w_i x_i \geq \left(\frac{1-\xi_i}{y_i}\right) - b$$

$$i = 1, 2, \ldots, N, \ \xi_i \geq 0, \ i = 1, 2, \ldots, N, \qquad 3.17$$

Equation (3.10) was applied to obtain the final classification of each case:

$$y_i = arg\ max_{k(1\ldots k)}(w_i^T y_i(x_i) + b_i) \qquad 3.18$$

Where *N* is the size of the dataset, *C* is the cost function. I , ξ are the slack variables, x and b is an offset scalar.

C. Performance Evaluation

The performance evaluation was done using recognition accuracy, false acceptance rate (FAR) and false rejection rate (FRR), Equal Error Rate (EER) and computation time.

i. False acceptance rate (FAR): False Acceptance Rate is the percentage of times the system accepts an unauthorized user. FAR describes the rate at which imposters are incorrectly accepted as genuine persons. A false acceptance may lead to damages when matching score established by a biometric system for an imposter satisfies the threshold criteria of matching. FAR which is also sometime referred as False Match Rate (FMR), is given by:

$$FAR = \frac{\text{number of impostors accepted (FP)}}{\text{Total number of imposter comaprisons (TN+FP)}} \times 100\% \qquad 3.19$$

ii. False rejection rate (FRR): False Rejection Rate is the percentage of times the system rejects an authorized user. In other words, FRR is the rate at which a genuine person is correctly rejected as an imposter. FRR is also called as False Non-Match Rate (FNMR). Thus, FRR is given by

$$FRR = \frac{\text{Number of genuine person rejected (FN)}}{\text{Total number of genuine comparism (TP+FN)}} * 100\% \qquad 3.20$$

iii. Recognition Accuracy**:** Recognition Accuracy is used to measure the performance of a verification system and is defined as:

$$Recog\ Accuracy = \frac{(TP+TN)}{(TP+FN)} * 100\% \qquad 3.21$$

IV. RESULTS AND DISCUSSION

A. Evaluation Results (Training)

The dataset used contain 600 iris images and 600 face images, 360 of the iris images and 360 of the face images were used in training the model while 240 of the iris images and 240 of the face images were used to test the model. The training was carried out using AES-FFT and AES with iris, face and later fused iris and face.

1) Results for Iris

Table 4.1 describes the result gotten by the Iris experiment with AES-FFT while Table 4.2 describes the result gotten with AES both at threshold value of 0.2, 0.35, 0.5 and 0.76 with respect to the performance metrics. The results obtained from the tables revealed that at threshold value of 0.76, the introduction of Iris with AES-FFT and AES realized a false acceptance rate of 1.67% and 6.67% respectively, false rejection rate of 3.33% and 7.78% correspondingly and an accuracy of 95.42% and 92.50% at 171.23s and 323.89s respectively. The computation time ranged between 168.89s to 173.60s and 239.72s to 242.92 seconds.

2) Results for Face

Similarly, Table 4.3 and Table 4.4 presents the results obtained by the Face with AES-FFT and AES correspondingly at threshold values of 0.2, 0.35, 0.5 and 0.76 with respect to the performance metrics. The results obtained from table 4.3 reveals that at the threshold value of 0.76, the application of Face with AES-FFT had a false acceptance rate of 3.33%, false rejection rate of 3.33% and accuracy of 96.67% at 222.76 seconds. The table 4.4 also shows that the- computation time ranges between 294.26 to 299.56

seconds. While the results obtained from table 4.4 reveals that at threshold value of 0.76, the application of Face with AES had a false acceptance rate of 6.67%, false rejection rate of 7.22% and accuracy of 92.92% at 297.19 seconds.

3) Results for fused irises and faces

Table 4.5 and 4.6 presents performance evaluation based on recognition accuracy, false acceptance rate and false rejection rate with respect to application of AES-FFT and AES on fused irises and faces. The accuracies generated by fused iris and face were analyzed at threshold values of 0.2, 0.35, 0.5 and 0.76 respectively. Out of all threshold values considered as obtained in Table 4.5 and 4.6, it was noticed that recognition accuracy with introduction of fused irise and face at threshold value 0.76 and above was 97.92% and 95.83% higher in values than other thresholds. Hence, the fused iris and face at 0.76 threshold performed better in accuracy for both tables, but had 1.67% false acceptance rate on table 4.5 and had 3.33% false acceptance rate on table 4.6 then 2.22% false rejection rate on table 4.5 along with a false rejection rate of 4.44% on table 4.6.

Table 4.1: Iris with AES-FFT

TP	FN	FP	TN	FAR(%)	FRR(%)	ACC(%)	Time(sec)	Threshold
177	3	9	51	15.00	1.67	93.33	171.02	0.20
176	4	6	54	10.00	2.22	94.17	173.60	0.35
175	5	3	57	5.00	2.78	95.00	168.89	0.50
174	6	1	59	1.67	3.33	95.42	171.23	0.76

Table 4.2**:** Iris with AES

TP	FN	FP	TN	FAR(%)	FRR(%)	ACC(%)	Time(sec)	Threshold
169	11	11	49	18.33	6.11	90.83	242.89	0.2
168	12	9	51	15.00	6.67	91.25	241.86	0.35
167	13	7	53	11.67	7.22	91.67	239.72	0.5
166	14	4	56	6.67	7.78	92.50	242.92	0.76

Table 4.3: Face with AES-FFT

TP	FN	FP	TN	FAR(%)	FRR(%)	ACC(%)	Time(sec)	Threshold
177	3	11	49	18.33	1.67	94.17	223.76	0.2
176	4	8	52	13.33	2.22	95.00	219.65	0.35
175	5	5	55	8.33	2.78	95.83	223.31	0.5
174	6	2	58	3.33	3.33	96.67	222.76	0.76

Table 4.4: Face with AES

TP	FN	FP	TN	FAR(%)	FRR(%)	ACC(%)	Time(sec)	Threshold
170	10	11	49	18.33	5.56	91.25	299.56	0.2
169	11	9	51	15.00	6.11	91.67	294.87	0.35
168	12	7	53	11.67	6.67	92.08	294.26	0.5
167	13	4	56	6.67	7.22	92.92	297.19	0.76

B. Discussion of Results

The results obtained in Table 4.1, Table 4.2, Table 4.3, Table 4.4, Table 4.5 and Table 4.6 showed the performance of the techniques employed in this research. The results showed that there was significant variation in the performance metrics with increase in threshold value and the best results were obtained at the threshold value of 0.76 across all metrics (False Rejection Rate, False Acceptance Rate and Accuracy) for fused iris and face, iris and face respectively. Therefore, the performance of the developed technique is more dependent on the threshold value. Figure 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10, 4.11, 4.12, 4.13, 4.14 and 4.15 presents the scatter plot of the metrics.

The fused irises and faces gave 97.92%, irises had 95.42% and faces had 96.67% recognition accuracies with AES-FFT respectively, while the fused iris and face gave 95.83%, iris had 92.50% and faces got 92.92% recognition accuracies with AES respectively. It can be inferred from the results based on the performance metrics that AES-FFT applied with irises and faces gave the best result.

Recognition accuracies coupled with False Acceptance Rate generated with fused iris and face with AES-FFT at 0.76 threshold values are as follows: fused iris and face generated 97.92% accuracy at 1.67% FAR, Face had 96.67% accuracy at 3.33% FAR and Iris got 95.42%at 1.67% FAR respectively. While with AES at 0.76 threshold values are as follows: fused iris and face generated 95.83% accuracy at 3.33% FAR, Face had 92.92% accuracy at 6.67% FAR and Iris got 92.50% at 6.67% FAR respectively.

Table 4.5: Fused Irises and faces with AES-FFT Result

TP	FN	FP	TN	FAR(%)	FRR(%)	ACC(%)	Time(sec)	Threshold
179	1	9	51	15.00	0.56	95.83	163.70	0.2
178	2	6	54	10.00	1.11	96.67	169.76	0.35
177	3	3	57	5.00	1.67	97.50	177.14	0.5
176	4	1	59	1.67	2.22	97.92	191.66	0.76

Table 4.6: Fused Irises and faces with AES Result

TP	FN	FP	TN	FAR(%)	FRR(%)	ACC(%)	Time(sec)	Threshold
175	5	9	51	15.00	2.78	94.17	414.53	0.2
174	6	7	53	11.67	3.33	94.58	421.07	0.35
173	7	5	55	8.33	3.89	95.00	421.61	0.5
172	8	2	58	3.33	4.44	95.83	423.77	0.76

Fusion of Iris and Face gave improved results compared to those of Iris separately and Face separately. Patra (2006) carried out a research which showed that multibiometric systems are more secure than unimodal biometric systems (biometric systems that rely on only one trait) mainly due to the presence of multiple data. They discuss how a system uses multiple characteristics for authentication purposes and believe that the use of multiple biometrics makes it much more difficult for an intruder to trick the system. Furthermore, a system that uses two or more user traits ensures a live user is present at the time of data acquisition.

Finally, the aforementioned results were determined based on the optimum threshold value which happened to be selected because of its outstanding performance compared to other threshold values. In view of the above results, fused iris and face with AES-FFT gave more accurate performance due to high number of true positive as well as low number of true negative leading to high accuracy.

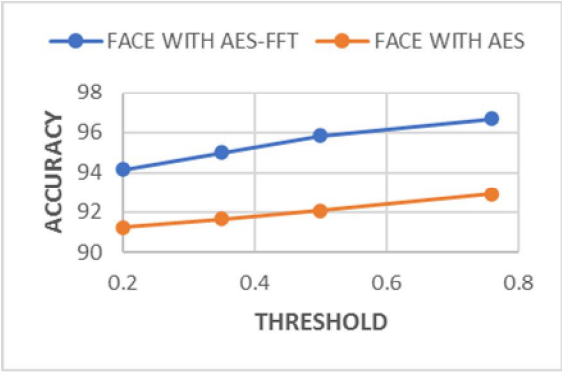
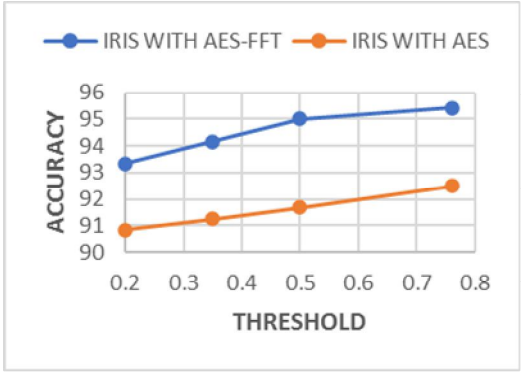


Figure 4.1: Graph showing Accuracy with faces



4.2: Graph showing Accuracy with Iris

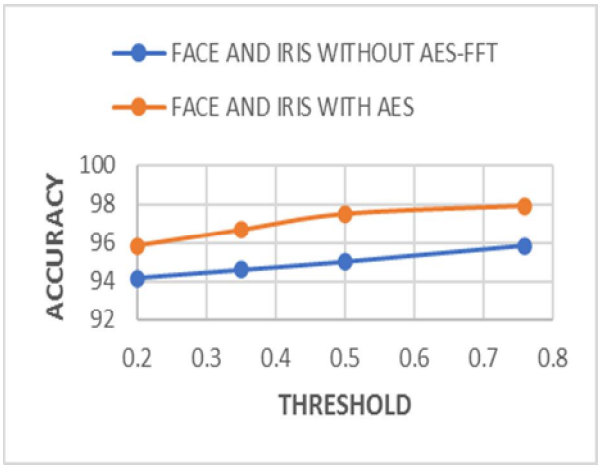


Figure 4.3: Graph showing Accuracy with Face and Iris

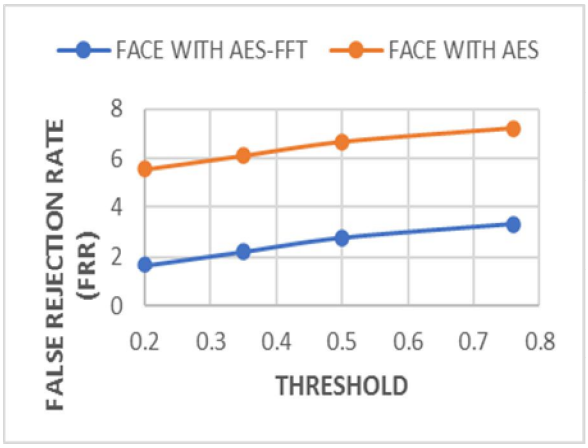


Figure 4.4: Graph showing False rejection rate (FRR) with face4

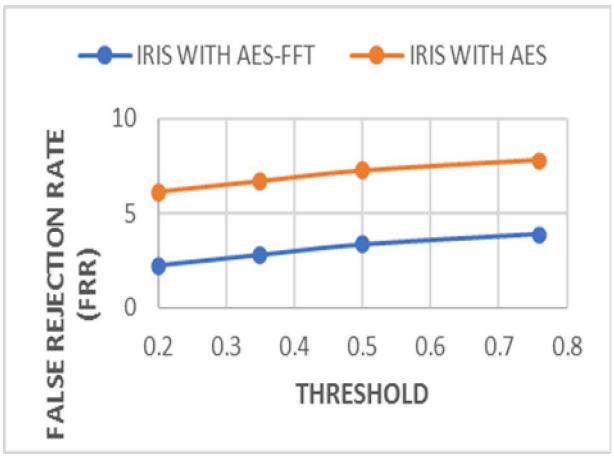


Figure 4.5: Graph showing False rejection rate (FRR) with iris

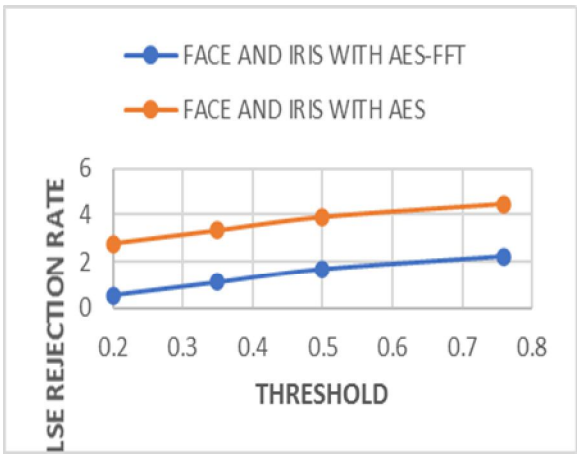


Figure 4.6**:** Graph showing false rejection rate FRR) with face and iris

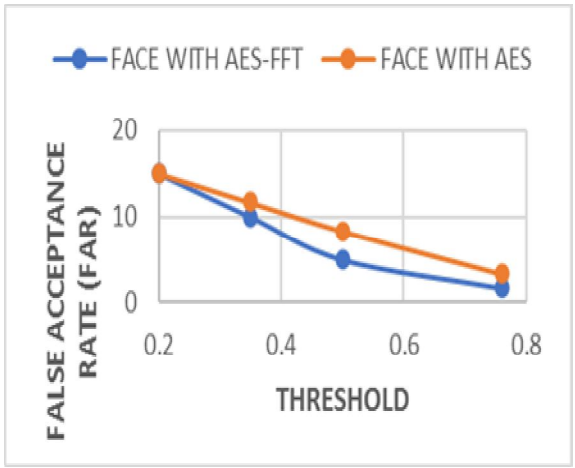


Figure 4.7: Graph showing False Acceptance rate (FAR) with face

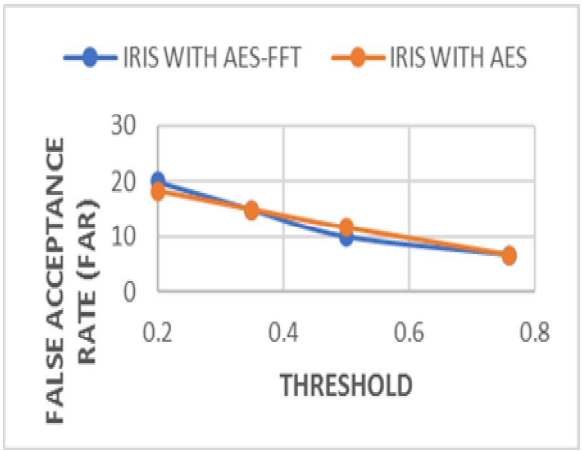


Figure 4.8: Graph showing False Acceptance rate (FAR) with iris

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue V May 2023- Available at www.ijraset.com

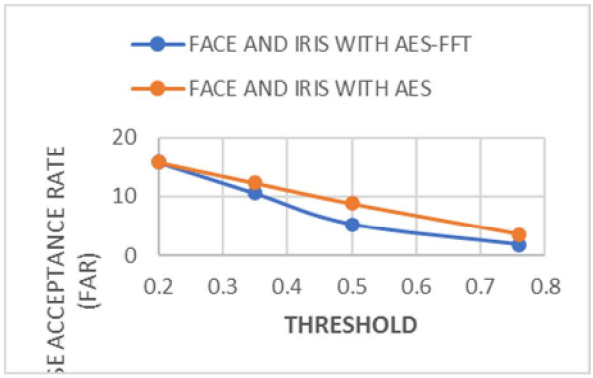


Figure 4.9: Graph showing False Acceptance rate (FAR) with face and iris

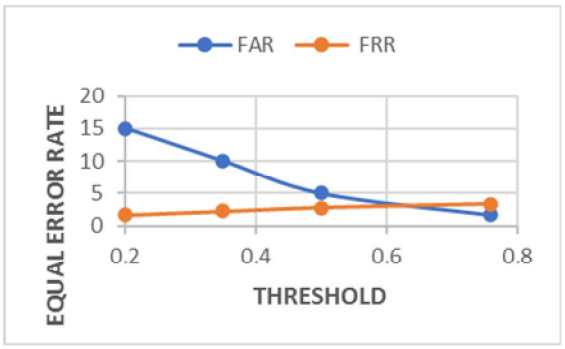


Figure 4.10: Graph showing equal error rate of 2.78 with iris under AES-FFT

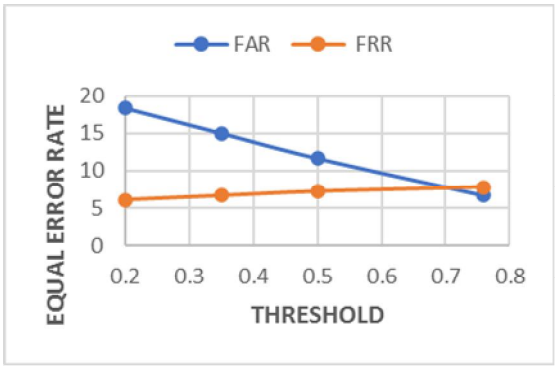


Figure 4.11: Graph showing equal error rate of 7.90 with iris under AES with face under

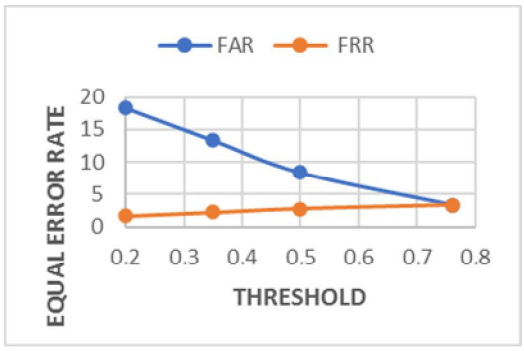


Figure 4.12: Graph showing equal error rate of 3.33 with face and iris under AES-FFT

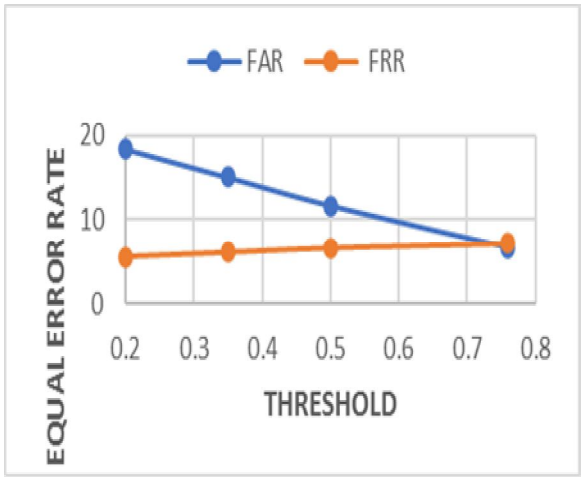


Figure 4.13: Graph showing equal error rate of 6.61 with face under AES

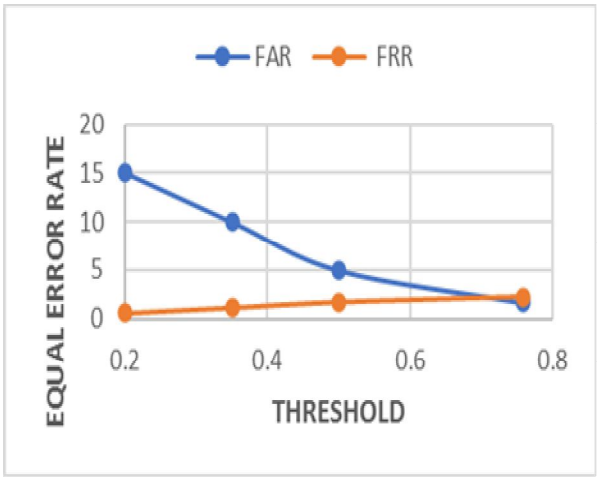


Figure 4.14: Graph showing equal error rate of 2.00 with face and iris under AES-FFT

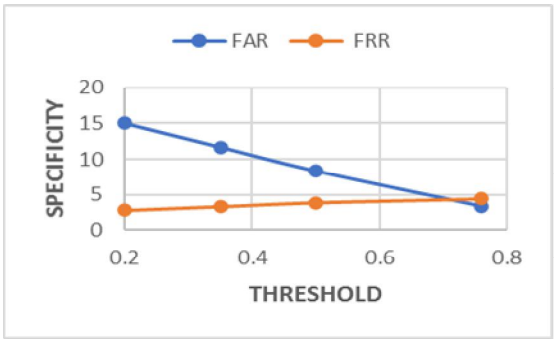


Figure 4.15: Graph showing equal error rate of 4.02 with face andiris under AES

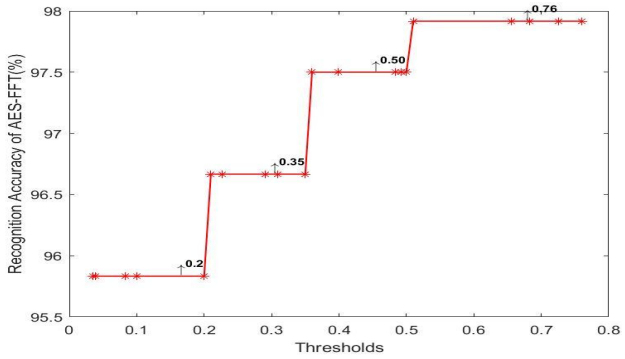


Figure 4.16: Recognition Accuracy of AES-FFT against Thresholds

V. CONCLUSION AND RECOMMENDATION

A. *Conclusion*

This project evaluated the essential features of unimodal (irises and faces) and multi-modal (fused irises and faces) on the performance of multi-modal crypto-biometric system. Three hundred and sixty (360) irises were trained and two hundred and forty (240) irises were used to test the developed technique at different thresholds. The experimental results obtained revealed that the fused irises and faces under AES-FFT encryption technique with SVM classifier gave 98.33% in terms of recognition accuracies, 0.83% false acceptance rate, 97.50% false rejection rate, 99.17% specificity and 32.99s recognition time compare with irises and faces modality. In view of this, an automated bi-modal crypto-biometric system based on fused irises and faces (that is, both faces and irises), would produce a more reliable accurate and secure system on any repository system as a result of its high accuracy. In other words, the developed AES-FFT technique has ensured scalable encrypting capacity, good imperceptibility and security performance, and robustness against various attacks with optimal computational efficiency in terms of its accuracy and time. The techniques developed in this work proved through empirical evidence to be efficient with reduced complexity and robustness against common attacks. It will be applicable to encrypt confidential or personal data. It will eliminate the flaws, vulnerabilities to attack and threats of adulterating digital content. It can also be useful for security purposes in commercial activities which include physical access control, computer network login, door security system, electronic data security and medical records management.

B. *Recommendation*

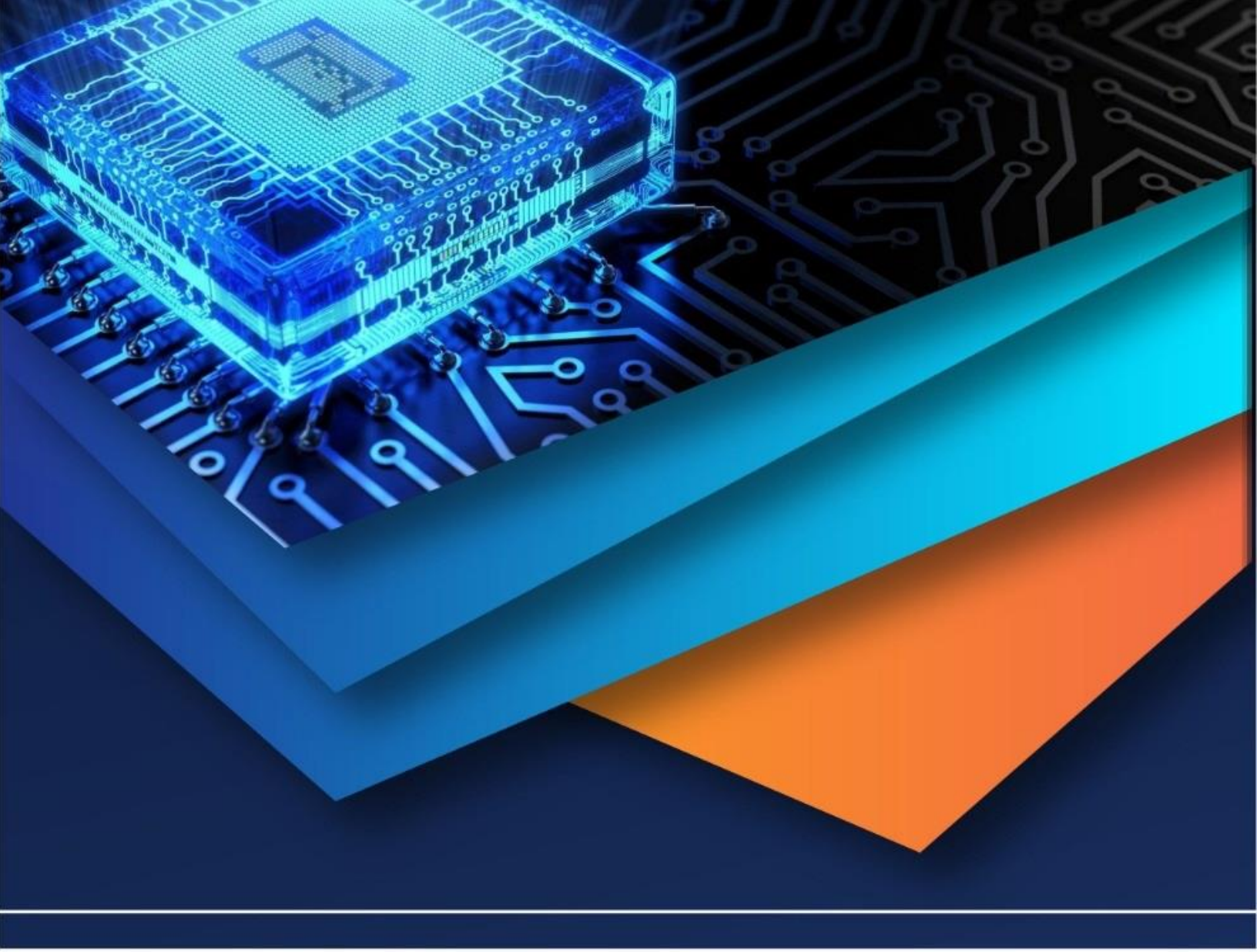
With regards to the performance of the developed technique, SVM based iris system can be used to enhance security challenges in an automated machine such as ATM. It is recommended that: Some evolutionary search algorithm such as Ant Colony Optimization (ACO), Evolutionary Programming (EP), GLCM (GP), Differential Evolution (DE), Artificial Immune Systems (AIS), can be introduced as feature selection techniques in other to aid recognition process. Other Artificial Neural Network techniques could be compared with SVM in other to determine its computational efficiency on iris systems A computer system with higher configuration and capability should be employed in other to handle more datasets because test-running the system with large dataset took a longer time to process.

REFERENCES

[1] Abuguba, S., Milosavljević, M. M., and Maček, N., (2015). An Efficient Approach to Generating Cryptographic Keys from Face and Iris Biometrics Fused at the Feature Level, IJCSNS International Journal for Computer Science and Network Security, vol. 15, no. 6, 6–11.
[2] Al-Shaaby, A. and Alkharobi, T., (2017). Cryptography and Steganography: New Approach. Society for Science and Education, Vol. 5, No. 6. ISSN: 2054-7420.
[3] Amin, M. M, Salleh, S. I., Katmin, M. R. and Shamsuddin, M. Z. (2003). Information Hiding using Steganography. Proceedings on National Conference of Telecommunication Technology (pp. 234 – 238), Shah Alam, Malaysia, IEEE ISBN 0-7803-7773.
[4] Anupriya A. and Sarita S. (2018). A literature review on various recent steganography techniques. International Journal on Future Revolution in Computer Science and Communication Engineering, 4(1), 143-149.
[5] Babu, K. R., Kumar, S. U., and Babu, A. V. (2010). A Survey on cryptography and Steganography methods for information security. International Journal of Computer Applications, 12(3), 13-17.

[6] Barman, S., Samanta, D., & Chattopadhyay, S. (2015). Fingerprint-based crypto-biometric system for network security. EURASIP Journal on Information Security, 2015(1), 3, pp. 2-17.
[7] Benantar, M. (2010). Access Control Systems: Security, Identity Management and Trust Models. IBM Corp, Austin, TX, USA
[8] Boehm, Benedikt (2014) StegExpose: A Tool for Detecting LSB Steganography (Master Thesis).School of Computing, University of Kent, England, 1 - 17.
[9] Bonneau J., Herley P.C., Oorschot V., Stajano F., (2012). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. University of Cambridge Computer Laboratory, Tech Report 817. www.cl.cam.ac.uk/techreports/UCAM-CL-TR-817.html
[10] Bowers M., (2010). Physical Access Control. Bowers Engineering, Randallstown MD.
[11] Chander K., Kaur, P and Chanda A. (2008). Biometric Security using Steganography. International Journal of Security, 2(1), 11 - 18.
[12] Cheddad, A. Condell, K. Curran, K. and Mc Kevitt, P. (2010). Digital Image Steganography: Survey and Analyses of Current Methods. Signal Processing Journal, 90(3), 727 – 752.
[13] Cheng, B., and Titterington D., (1994). Neural networks: a review from a statistical perspective. Statistical Science **9**, no. 1, pp 2–54.
[14] Colores, J., García-Vázquez, M., Ramirez, A., Perez-Meana, H., and Nakano-Miyatake, M. (2013). Video Images Fusion to Improve Iris Recognition Accuracy in Unconstrained Environments. 7914. 114-125. 10.1007/978-3-642-38989-4_12.
[15] Davison, A. (2009). Java Programming Techniques for Games. Java Art. National Academy Press, Newyork, pp. 99.
[16] Deepa, S., and Umarani, R. (2015). A Prototype for Secure Information using Video Steganography. International Journal of Advanced Research in Computer and Communication Engineering, 4(8): 442 – 444.
[17] Deepesh, R. and Bhandari, V. (2013). A Steganography Technique for Hiding Image in an Image using LSB Method for 24 Bit Color Image. International Journal of Computer Applications 64(20), 15 - 19.
[18] Dhiren, R. Patel (2010), "Information Security: Theory and Practice". PHI Learning Private Limited Publisher, New Delhi. 35-117.
[19] Douglas, M., Bailey, K., Leeney, M., & Curran, K. (2018). An overview of steganography techniques applied to the protection of biometric data. Multimedia Tools and Applications, 77(13), 17333-17373.
[20] Eggers, E., Salter, J and Shieneir, W. (2002). A Communication Approach to Image Steganography, Security and Watermarking of Multimedia Contents IV. San Jose, California: Proceedings of SPIE , 22 - 30.
[21] Falohun, A. S., Fenwa, O. D., & Oke, A. O. (2016). An access control system using bimodal biometrics. International Journal of Applied Information Systems, Foundation of Computer Science-FCS, New York, USA, 10(5), 41-47.
[22] Finkenzeller, K., (2003). RFID Handbook Fundamentals and Applications in Contactless Smart Cards and Identification, John Wiley and Sons Ltd.
[23] Fridrich, J. and Goljan, M. (2012). Practical Steganalysis of Digital Images – State of the Art. http://www.ssie.binghamton.edu/fridrich. pp 1 -13.
[24] Gale, A., and Salankar, S., (2015). Performance Analysis on Iris Feature Extraction using PCA, Haar Transform and Block Sum Algorithm. International Journal of Engineering and Advanced Technology (IJEAT). ISSN: 2249 – 8958, Volume -4 Issue -4.
[25] George, J. P., (2012). Development of efficient biometric recognition algorithms based on fingerprint and face. A thesis submitted to the Christ University, pp. 1-9.
[26] Gurney, K., (2004). An introduction to neural networks. University of Sheffield, UCL Press Limited 11 New Fetter Lane London EC4P 4EE.
[27] Gupta, R., Yadav, P., and Kumar, S. (2017). Race identification from facial images using statistical techniques. Journal of Statistics and Management Systems, 20(4), 723-730.
[28] Hao, F., Anderson, R., and Daugman, J. (2006). Combining crypto with biometrics effectively. IEEE transactions on computers, 55(9), 1081-1088.
[29] Jagadeesan, A., Thillaikkarasi, T. and Duraiswamy, D. K., (2010). "Cryptographic Key Generation from Multiple Biometric Modalities: Fusing Minutiae with Iris Feature," Int. J. Comput. Appl., vol. 2, no. 6, 16–26.
[30] Jain, A. K, Ross, A., and Prabhakar, S." (2004). "An introduction to biometric recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14(1): 4–20.
[31] Jain, A. K., Hong, L., and Bolle, R. (1997). On-line fingerprint verification. IEEE Transactionson Pattern Analysis and Machine Intelligence, vol. 19(4): 302-314.
[32] Jain, A. K., Nandakumar, K., and Nagar, A., (2013). Fingerprint Template Protection: In Security and privacy in biometrics. From Theory to Practice, London: Springer, 187–214.
[33] S, Joshna. (2016). Symmetric Key Algorithms: A Comparative Analysis. International Journal of Innovative Research in Computer and Communication Engineering. 4. 15772-15775.
[34] Kaur, J. and Kumar, S (2011)."Study and Analysis of Various Image Steganography Techniques" Proc. International Journal of Computer Science and Technology 2(3), pp. 55 – 64.
[35] Kaur, R., and Sharma, N. (2015). A novel approach to enhance the Security in Vehicular Ad- Hoc Network through Node Authentication using Hash Value and Steganography Schema. Journal of Network Communications and Emerging Technologies (JNCET) www. jncet. org, 2(2):23-29.
[36] Kaur, R., and Singh, T. (2015). Hiding Data in Video Sequences using LSB with Elliptic Curve Cryptography. International Journal of Computer Applications, 117(18): 34-57.
[37] Kaushal, A. and Chaudhary, V. (2013): Secured Image Steganography using Different Transform Domain. International Journal of Computer Applications. 7(2), pp. 24 -28.
[38] Khalid I. R., Arora, K., and Pal, N. (2014). A crypto-steganography: A survey. International Journal of Advanced Computer Science and Application, 5, 149-154.
[39] Komal, C. K., (2019). A Robust Multimodel Biometric Crypto System. International Journal of Recent Technology and Engineering (IJRTE), Volume-8 Issue-2S8, 1953-1961.
[40] Maltoni, D., Maio, D., Jain, A. K., and Prabhakar, S. (2009). "Handbook of fingerprint recognition (2nd ed.). New York: Springer-Verlag.
[41] Marwa, S. E., Aly, A. A., and Omara, F. A. (2016). Data security using cryptography and steganography techniques. IJACSA) International Journal of Advanced Computer Science and Applications, 7(6), 390-397.
[42] McAteer, I., Ibrahim, A., Zheng, G., Yang, W., & Valli, C. (2019). Integration of biometrics and steganography: A comprehensive review. Technologies, 7(2), 34.
[43] Murray Meg C., (2010). Database Security: What Students Need to Know. Journal of Information Technology Education: Innovations in Practice Volume 9.
[44] Nitin Kanzariya, K., and Nimavat Ashish, V. (2013). Comparison of Various Images Steganography Techniques. International Journal of Computer Science and Management Research, 2(1), 1213-1217.

[45] Nithya S., and George P., (2014). **Survey on Asymmetric Key Cryptography Algorithms.** Journal of Advanced Computing and Communication Technologies (ISSN: 2347 - 2804) Volume No. 2 Issue No. 1. niyaa20@yahoo.co.in, georgeprakashraj@yahoo.com
[46] Okokpujie, K. O., Odusami, M., Noma-Osaghae, E., Abayomi-Alli, O., & Oluwawemimo, E. (2018). A Bimodal Biometric Bank Vault Access Control System. International Journal of Mechanical Engineering and Technology (IJMET), 9(9), 596-607
[47] Oluwadamilola, K. O., Ayodeji, A. O., Martins, O. O., Olufunmi, I. S., & Rapheal, O. A. (2017). An improved authentication system using hybrid of biometrics and cryptography. In 2017 IEEE 3rd International Conference on Electro-Technology for National Development (NIGERCON), 457-463.
[48] Omidiora, E. O., Adegoke, B. O, Falohun, S. A. and Ojo, D. A.(2015). Iris Recognition Systems: Technical Overview. International Journal of Research in Engineering and Technology. 3(6): 63-72
[49] Omidiora E.O., Ojo O., Yekini N.A. and Tubi T.O (2012). Analysis, Design and Implementation of Human Fingerprint Patterns System "Towards Age & Gender Determination, Ridge Thickness to Valley Thickness Ratio (RTVTR) & Ridge Count on Gender Detection. International Journal of Advanced Research in Artificial Intelligence (IJARAI), Vol. 1, No. 2, pp: 57-63.
[50] Oppliger, R. (2016). SSL and TLS: Theory and Practice. Artech House.
[51] Prachi P. Sadawarte, P. A. and Tijare (2017). Video data hiding using Video Steganography, International Journal of Advanced Research in Computer and Communication Engineering. 6(2): 305 – 307.
[52] Rahmani, K. I. Arora, K. and Pal, N. (2014). A Crypto-Steganography: A Survey. International Journal of Advanced Computer Science and Applications, (IJACSA) , 5(3), 149-155.
[53] Richard, Y. F. N. and Yong, H. T. (2007). Kai Ming Mok,"An effective segmentation method for iris recognition system", Int.
[54] Ross A. (2009). Multibiometrics. In: Li S.Z., Jain A. (eds) Encyclopedia of Biometrics. Springer, Boston, MA. https://doi.org/10.1007/978-0-387-73003-5_147
[55] Ross A., (2007). An introduction to Multibiometrics. Appeared in the Proc. Of the 15th European Signal Processing Conference (EUSIPCO), Poznan, Poland. arun.ross@mail.wvu.edu, http://www.csee.wvu.edu/˜ross
[56] Sahu, P. and Sinha, S. (2017). Discrete wavelet packet transform based video steganography. International Journal of Mineral Processing and Extractive Metallurgy, 2(1), 7-12.
[57] Salau A. and Jain S. (2019). Feature Extraction: A survey of the Types, Techniques, Applications. 10.1109/ICSC45622.2019.8938371, 158-164.
[58] Samad A. and Hussain S. (2006). Introduction to Fusion Techniques. Rome Air development center, final technical report RACDCTR 81-161.
[59] Selvarani, P., & Visu, P. (2015). Multi-model bio-cryptographic authentication in cloud storage sharing for higher security. Research Journal of Applied Sciences, Engineering and Technology, 11(1), 95-101.2
[60] Seshadri, R., & Trivedi, T. R. (2011). Efficient cryptographic key generation using biometrics. International Journal of Computer Technology and Applications, 2(1), 1-9.
[61] Smith, L., (2002). A tutorial on Principal Components Analysis. Cornell Univ. USA, 51, 52.
[62] Souvik, Roy and P. Venkateswaran (2014). Online payment system using steganography and visual cryptography. In 2014 IEEE Students' Conference on Electrical, Electronics and Computer Science, 1-5.
[63] Suthakar J., Monica E., Annapoorani D. and Richard S. (2014). Study of Image Fusion-Techniques, Method and Applications. International Journal of Computer Science and Mobile Computing ISSN 2320–088X Vol.3 Issue.11 pg.469 – 476.
[64] Suri, S., Joshi, H., Mincoha, V. and Tyagi, A. (2014). Comparative Analysis of Steganography for Coloured Images. International Journal of Computer Sciences and Engineering, 2(4), 180 – 184.
[65] Tharwat, A., (2016). Principal Component Analysis (PCA): An Overview.
[66] Tharwat, A., (2016). Principal component analysis-a tutorial. International Journal of Applied Pattern Recognition. **3**(3) 197-240.
[67] Tutorialspoint (2015). Cryptography Just for Beginners. tutorialspoint Simply Easy Learning. www.tutorialspoint.com.
[68] Venna, S. R., and Inampudi, R. B., (2019). MMBAS-NS: Multimodal Biometric Authentication System and Key Generation Algorithm for Network Security on Mobile Phones. International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-7 Issue-5S2, 189-199.
[69] Verlag S., (1991). Handbook of fingerprint recognition.
[70] Vipula M. W. and Suresh K. (2013). Stegocrypto - A Review of Steganography Techniques using Cryptography. International Journal of Computer Science and Engineering Technology, 4: 423-426.
[71] Walia, E., Jain, P. and Navdeep, A. (2010). An Analysis of LSB and DCT based Steganography, Global Journal of Computer Science and Technology, 10(1), 4 - 8.
[72] Wang, Z., Wang, E., Wang, S., & Ding, Q. (2011). Multimodal Biometric System Using Face- Iris Fusion Feature. JCP, 6(5), 931-938.
[73] Zuva, T., Esan, O. A., & Ngwira, S. M. (2014). Hybridization of bimodal biometrics for access control authentication. International Journal of Future Computer and Communication, 3(6), 444.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY