International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

GUI based Multi-Modal Biometrics Authentication

Ms. Gopika S Kumar
Student: Department Of ECE,
BNM Institute of Technology
Bangalore, Karnataka 560070

Ms. Anagha G
Student: Department of ECE
BNM Institute of Technology
Bangalore, Karnataka 560070

Ms. Ananya G A
Student: Department of ECE
BNM Institute of Technology Bangalore,
Karnataka 560070

Mrs. Priya R Sankpal
Asst. Professor:
Department of ECE BNM Institute of Technology
Bangalore, Karnataka 560070

***Abstract*— Security and authentication which are a major concern in this internet era, need to be addressed and one way to achieve this is to use multi-model biometrics. Multi-model biometrics offer more flexibility than unimodal biometrics. In this proposed system, face and retina biometrics are used. We created database comprising of face and retina images belonging to 7 different individuals, extracted their features, fused them together and latter encryption is performed on it. During authentication if the decrypted result of retina and face belong to same individual access is granted or else denied. In this project security is enhanced by adopting encryption of user data.**

Keywords—Retinal and face feature extraction, MultiSVM, Graphic User Interface, Database, Encryption and Decryption.

I. INTRODUCTION

Security mostly refers to protection from hostile attacks. Identity Manipulation can be considered as serious issue of security. Currently, Security of authentication system is facing threats and difficulties. It is found that by ensuring the confidential access to only the authorized user and protecting the privacy of their personal and transactional information, it might limit the influence of harmful attacks. Hence authentication is very important aspect of security. Authentication is act of providing an assertion such as identity of user. Authentication is majorly needed for health sector, business and banks etc. One way of addressing authentication, is the use biometrics. Technically biometrics is defined as measurement and calculation of human body characteristics. Biometrics authentication maybe for identification and access control. In contrast to traditional authentication techniques of using user ID and password, use biometrics authentication, authorization, and accountability.

Biometrics identifier are often grouped into physiological and behavioral biometrics. Physiological biometrics deals with shape of body, such as fingerprint, face, palm veins etc. Behavioral biometrics deals with the person's behavior such as gait and voice. Disadvantages of uni-biometrics has made the authentication process to move towards multi- model biometrics. For increased security and flexibility, the combination of biometrics referred as multi-modal biometrics are used. Applications of biometrics are wide spread ranging from commercial establishments, government sector, health sector, Defense, forensics applications.

II. LITERATURE SURVEY

In Stereo Image Matching method, technological improvements can be seen in area based to feature based matching techniques. Stereo image feature matching uses Harris corner detection algorithm. This algorithm is based on intensity feature matching which controls the strong corners as well as weak corners with the aid of threshold value. In model-based design method, complexity of design can be reduced in contrast to that of the script level design method. Since moment invariant features do not change the property on rotation and variant scale, these features are considered and re beneficial compared to match shifted image pair. This algorithm accepts input images that can be either gray scale or color image, before the processing further, input images pixels are converted to 8-bit gray scale and same resolution is maintained. A 3x3 window is generated using image pixels and partial derivative is employed for computing horizontal and vertical image gradients. Local area feature points are eliminated using threshold operator and if it is less than the chosen value, then middle pixel of the window is termed as corner element. This continued until all the corner elements in the image are identified. Non-maximum suppression is preformed if large number of corners are detected. This avoids confusion in further processing. Upper and lower threshold values are decided based on the type of image. The intensity of corner pixels matched with stereo pair images [1].

In secure audio steganography technique modulo operator is used for hiding target string. Both embedding and extraction process involve two steps which makes this algorithm more robust. Preprocessing involved computing the hexadecimal equivalent of target string by considering four bits at a time. This increases the cover image capacity. Modulo operator used during embedding process reduces distortion and increases imperceptibility. Performance evaluation of algorithm is done by computing SNR and in comparison, to standard LSB and HLLAS techniques. Use of modulo operator has a disadvantage of overlapping during the extraction process.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

This method attempts to reduce the information lost at the receiver side. The cover audio contains the key text as embedded target data. During embedding process, data is pre- processed and hidden using modulo operator.

Preprocessing involves each character of the target string being converted into equivalent corresponding 8 bit ASCII. These are then converted into hexadecimal digits by breaking into 4 bits. The duvet audio is embedded with these hexadecimal digits by adjusting the target samples amplitude canopy. Next the cover audio amplitudes are divided by 16. These amplitude values are compared with the target hexadecimal digits and the duvet audio amplitudes are modified such that the remainder is adequate to the target hexadecimal digits. For performing amplitude adjustment, forward and backward differences are computed. The amplitude values of the hidden information at the receiver side are divided by 16. The resultant hexadecimal digits are converted to their 4-bit binary equivalent. These 4 bits are concatenated to generate the binary string. Decimal equivalent is computed by considering only 7 bits and their corresponding ASCII values are computed as per the length of the target string [2].

Computer vision based automatic classification of fruits is very complex as various fruits will have assorted properties.

Classification using multi-class kernel support vector machine (kSVM) gives accurate and fast classification of fruits. Fruit images are captured using camera, each image background is removed using split-and-merge algorithm. Feature space is composed using the color histogram, texture and shape features extracted from each fruit image. Additionally, Principal component analysis (PCA) is used creating feature space. Winner-Takes-All SVM, Max-Wins-Voting SVM, and Directed Acyclic Graph SVM are used for constructing multi-class SVM. Kernels selected are linear kernel, Homogeneous Polynomial kernel, and Gaussian Radial Basis kernel.

Five-fold stratified cross validation with the condensed feature vectors as input is used for training the SVMs. Combination of color histogram, texture and shape features yield better results than having single feature for the classification of fruits. Use of PCA decreases the features. The experimental results show that effective classification is obtained with the combination of Max-Wins Voting SVM with Gaussian Radial Basis kernel which gives an accuracy of 88.2% [3].

III. PROPOSED SYSTEM

In the proposed Multimodal System, we've chosen Face and Retina because the two biometric traits used for authenticating the identity of an individual. The software used is MATLAB R2014a. GUI is intended employed which for displaying the result. Database is made which is trained with the features of the authenticated people. Face and Retina features are extracted by using Harris Feature detection algorithm which mainly detects the corner/edge features. The extracted Features are the then fused by concatenation and will be hidden in an exceedingly cover image by using Stenography. Decoding of the secret image is finished in similar manner as encoding but in reverse order. The decoded face and eye image will initially be identified to which person they belong to by comparing it with the stored image within the database. We then compare if the extracted Face and Eye image belongs to a same person by using Multi class Support Vector machine (multisvm) method. The proposed system is as shown in Fig *Graphical interface* (GUI): GUI is a computer program generated design for user interface that has graphical elements, such as windows, icons and buttons.

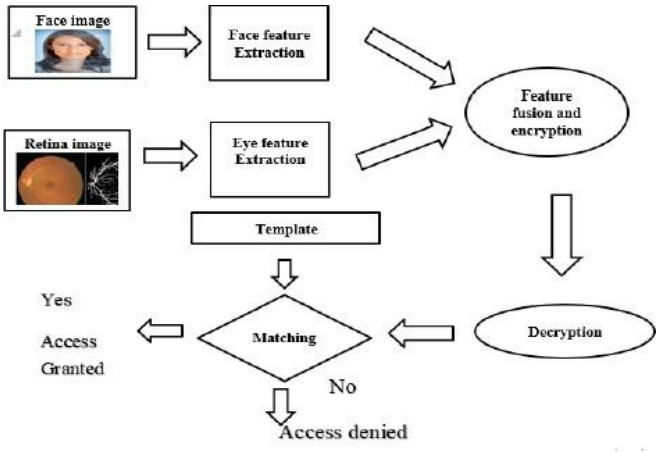

Fig 1: Proposed system block diagram

GUIs provide users with interactive visual feedback about the outcome of each code executed. Multiple programs can be displayed simultaneously using GUI. GUI will be designed in MATLAB by using the command called as guide. There are various tools available which are employed in designing GUI in MATLAB. The three main tools are:

a. Static Text: It's used for adding the title or the other text on the GUI. It contains different parameters that's used for modifying the text for instance font size is employed to define the scale of the text

b. Push button: it's used for creating the press buttons for user interface of the program. The function of every pushbutton depends on the program written for that push button, we have got designed various push buttons, which are used for choosing an image from a folder, Extracting the Features, do encoding, do decoding, authenticate and exit. Push buttons are often labelled with a tag which helps us in identifying a pushbutton and its associated function.

c. Axes: It's a handle which defines on which particular axes the image should get displayed on the GUI.

A. Feature Extraction and Encoding

In the proposed Multimodal System, Face Feature and Retina Feature are extracted by using Harris corner detector. The mathematical operator, Harris corner detector is used to find the features of the image. This operator is used, as it is rotation, scale and illumination variation independent. It also provides an better repeatability when illumination and rotation are changed

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

and hence it is more often applied in stereo matching and image database retrieval.

For Encoding of the information, stenography is adopted, wherein a file, message, image, or video is concealed within another file, message, image, or video. In steganography the intended secret message doesn't attract attention to itself as an object of scrutiny. Here modulo operator is used for hiding the features. The feature extraction and embedding process comprising of two methods provides more robustness strategy. During pre-processing the extracted feature value's binary equivalent is calculated. Modulo operator employed for embedding increased imperceptibility.

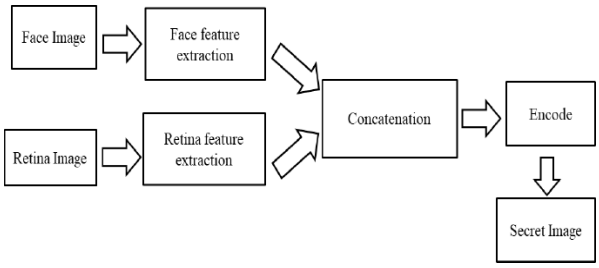

Fig 2: Encoding process flowchart

Encoding Algorithm:

Step1: Global declaration of all push-buttons. Cover image is employed to cover fused features. Using "imread" function filename and path of cover image is stored in a variable, "imshow" display coverage image. Any random image is chosen as cover image.

Step2: Enable next push button. It wants to read face image. Next push button is employed to extract features from face. Using "rgb2gray" Function face image is converted into grayscale and stored. Using "detectharriesfeatures" Function is used detect the corners of face and used to extract features.

Step3: Similarly Enable next push button. It is accustomed read retina image.

Next push button is employed to extract features from face. Using "rgb2gray" Function retinal image is converted into grayscale and stored.

Using "detectharriesfeatures" Function is used detect the corners of retina and used to extract features.

Step4: Both features are fused through concatenation and encrypted then stored behind the duvet cover image.

B. Decoding and Authentication

For Decoding of the information, we've used stenography within the similar way for encoding the information but it in reverse order. For Authentication we've got Multiclass Support Vector Machine(multisvm) technique. Multiclass classification problems (k>2) are generally decomposed into a series of binary problems such that specified quality of SVM are applied in sequence. SVM generally classify data into two classes (match found or mismatch). This algorithm tries seek out match for the given input image with the stored images in the trained database. When a match is found, the person is authenticated and granted the access. If no match is found in the training database, access is denied. Multimodal Biometrics are widely used as it provides High accuracy rate, reliable recognition and enhances the security against vulnerabilities.

Decoding Algorithm:

Step1: Input the Secret key image within which features are hidden.

Step2: Decode the encoded Secret Image by calling user defined function for decryption

Step3: Hidden Face and Retina features are decoded and extracted from Secret image.

Step4: Classification of the extracted features is done by calling user defined function called "multisvm"

Step5: multisvm will provide on which individual does the extracted Face and Retina image belongs to.

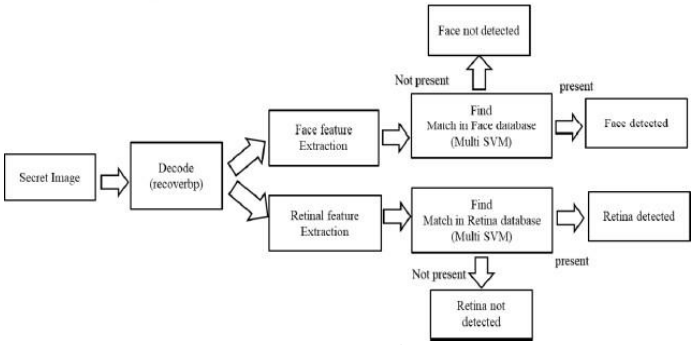

Fig 3: Decoding process flowchart

Encryption Algorithm:

Encryption is done in order to hide the extracted features inside the cover image using modulo o operator-based stenography

Step 1: Cover image, Feature Image and b^{th} bit in which the features are hidden are passed as input. Declare two constants p and h, where p=2^b and h=2^(b-1).

Step 2: Check if total number of pixels required to encrypt(N) is lesser than number of pixels in cover image(S). If its greater(N>S), truncate number of pixels to encrypt to be equal to cover image pixels.

Step 3: Convert cover image matrix to a single row matrix and store result as I1(1*S). Select N pixels from I1 and store result as I2 matrix(1*N).

Step 4: Check if b bit is high in each pixel value of cover Image, if its high make it to zero. Convert each pixel value of extracted Image from decimal to binary, store it as bi matrix. Convert binary values of 0's and 1's to 0's and 8's, store result in b matrix

Step 5: Add each bit of b matrix with each pixel value of I2 matrix and store it as I3 matrix. Convert I3 matrix to the original dimension of cover image and store it as Secret Image.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

Decryption Algorithm:

Decryption is done in extract to hidden features inside the cover image.

Step 1: Recover the features hidden in cover image.

Step 2: Cross-check the Bit number of image where data hidden is passed or not. Default value of Bit b=1 if not passed. Step 3: Check whether number of bits that of decrypted image is less than cover image size or not. Reshape bits into Single Row format and round off. (approx. 31000).

Step 4: Run the for loop for till all pixel values and Check the 4th Bit is High or not and update the empty matrix with 0 or 1. Convert values in the empty matrix from decimal to binary and group them value of 8.

Step 5: Reshape the value and convert back to decimal value. Return the values when function is called.

Multisvm Algorithm:

Step1: Extracted Image, Images stored in database and number of classes are passed as input

Step2: svmtrain is used which is a build in function in MATLAB, that trains the svm classifier with different classes of data present in database

Step3: svmclassify is used which is a build in function in MATLAB, which will compare Extracted Image with Images stored in database and provides output as to which individual does the extracted Face and Retina image belongs to.

Authentication

Step1: check if extracted Features belongs to same person.

Step2: If it belongs to same person, Authentication is successful and access will be granted.

Step3: If it belongs to different individual's, Authentication fails and access is denied.

IV EXPERIMENTAL RESULTS

A. Face feature Extraction.

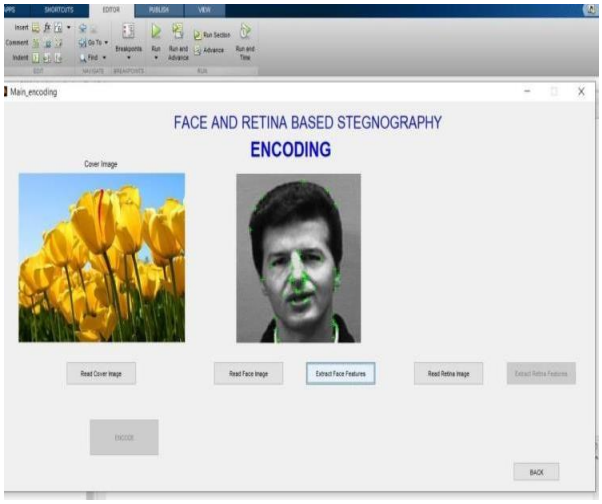

Fig 5: Face features is successfully extracted from given image.

The face image of a person is selected for encoding. Initially the face image can be either color or gray scale image and is converted to gray scale as it reduces storage requirements. Then using next pushbutton, features of face are extracted and stored for encoding.

B. Retina Feature Extraction

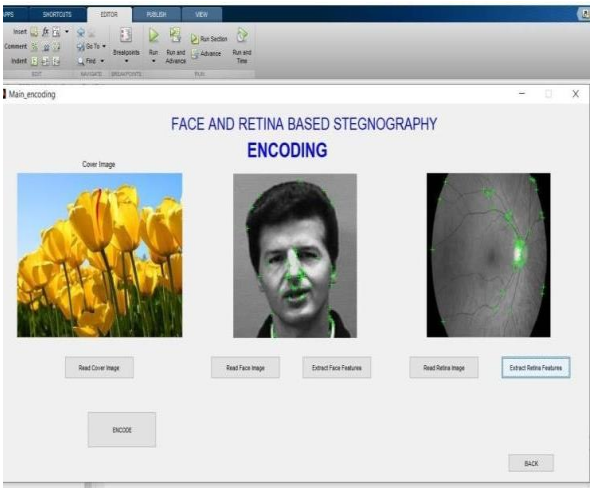

Fig 6: Retina feature extracted.

The retina image of a person is selected for encoding. Initially the retina image can be either color or gray scale image and is converted to gray scale as it reduces storage requirements. Then using next pushbutton, features of retina are extracted and stored for encoding.

C. Encoded Image

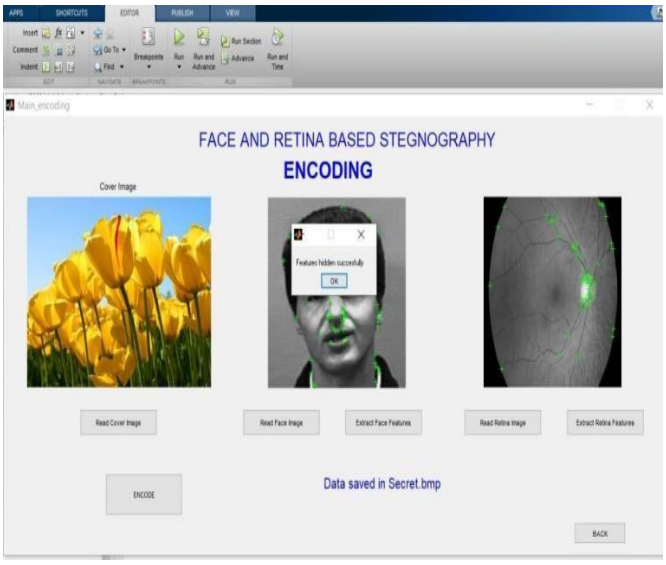

Fig 7: Encoding Successful

The retina and face image are fused using concatenation and encoded and stored in database. Similarly, all the authorized users' biometrics can be saved in database. The fused image is encrypted to avoid manipulations of biometrics data

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

D. Decoded Image

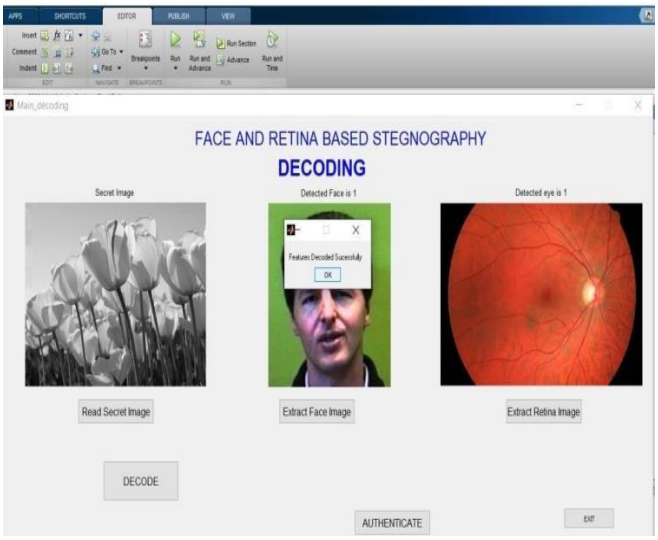

Fig 8: Image decoded successfully

The fused image of the user is decoded and decrypted. Then GUI displays the whether the retina and face image is of the same person or not based on which authentication will be granted.

E. Authentication

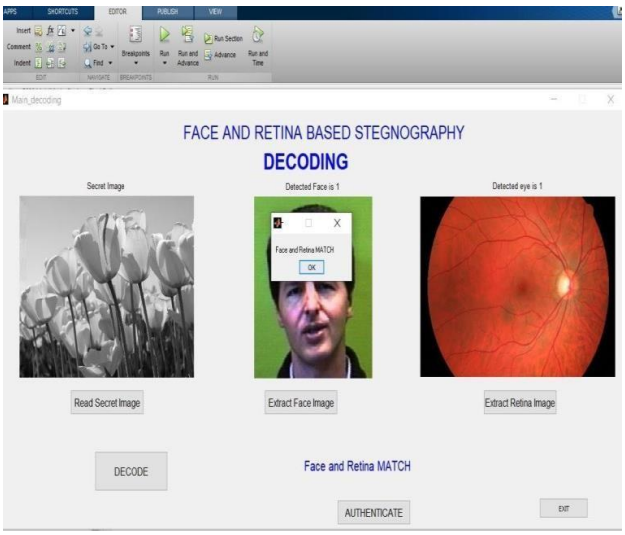

Fig 9: Authentication successful

If the retina and face image belong to the same person and access is granted and displays face and retina match.

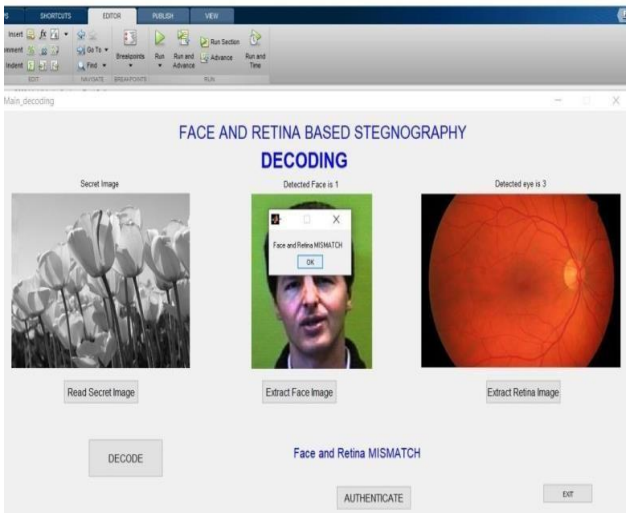

Fig 10: Authentication failed

If the retina and face image belong to two different individuals it shows retina and face mismatch and access is denied.

V. CONCLUSION

The existing Unimodal Biometric system uses single biometric trait for authenticating an individual, its performance gets affected by various parameters such as noisy sensor data, inter class similarities and various vulnerabilities which leads to increased values of False Acceptance Rate (FAR) and False Rejection Rate (FRR). The proposed system of Multi modal Biometric overcomes the drawbacks associated with Unimodal system. Initially the face and Retina Features are extracted by using detect Harris features which is a building function in MATLAB. The extracted Face and Retina Features from an individual is fused by concatenating them. The fused features are hidden in an cover image in order to increase the security of the system by modular based Stenography. The encoded features are then decoded, and compared with the features stored in Database in order to authenticate the individual.

VI. ACKNOWLEDGEMENT

In this project, we have used database containing retina and face images which we obtained from google. Images are purely for academic purposes. The database we used contain seven different individual's face images and their respective retina images. Both retina and face images used are colored images, even gray images can be used as input to the project.

VII. REFERENCES

[1] Komal Shrirang changan and Purushottam G Chilveri "Stereo Image Features Matching Using Harris Corner Detection Algorithm" 2016 ICACDOT, FIT pune.
[2] Biswjita Datta, Souptik Tat and Samir Kumar Bandyopadhyay "Robust High Capacity Audio Stenography using Modulo Operator" 1999 CISP-BEMI
[3] Yudong Zhang and Lenan Wu "Classification of Fruits Using Computer Vision and a Multiclass Support Vector Machine" Sensors 2012, Article I2,12489-12505
[4] R. Parkavi, K.R. Chandeesh Babu, J. Ajeeth Kumar "Multimodal Biometrics for User Authentication" 978-1-5090-2717-0/171 ©2017 IEEE.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 9 Issue 06, June-2020

[5] K. Gunasekara and P Mahalakshmi "Implementation of Multimodal Biometric Authentication Using Soft Computing Techniques"
[6] ISBN No.978-1-4799-3834-6/14 2014 IEEE.
[7] Tanvi Dhingra, Manvjeet Kaur "Fusing Fingerprint and Iris Multimodal Biometrics using Soft Computing Techniques': 2229-3345 2015 IEEE.
[8] Muhammad Saleem P, Dr.T. Senthil Prakash, Ismail PK "Multimodal Biometrics by Integrating Fingerprint and Palmprint For Security ". ISSN (P): 2349-3968, ISSN (O): 2349-3976 IEEE 2015
[9] [8] Ghada Abdelhady1, Mohammed Ismail2, Hussam Elbehiery "Multimodal Biometrics Cryptosystem Using Elliptic Curve" 2014 IEEE.

(This work is licensed under a Creative Commons Attribution 4.0 International License.)