

BIOMETRIC AUTHENTICATION SYSTEM USING VISUAL CRYPTOGRAPHY

Vasantha kumari A¹, Mohd.Umar peerzade², Subhralina Nayak³, Bhagya V⁴, Dr.M.senbagavalli ^[5]

^{1,2,3,4} Students, Department of CSE (M.Tech) Alliance University, Bangalore, Karnataka, India

⁵Associate Professor, Department of Information Technology, Alliance University, Bangalore, Karnataka, India

Abstract - in today's era with immense usage of internet and development in the innovation has made development transmission of advanced substance is confronting a significant part in test of security. thus reliably secure component is required to ensure the touchy information and furthermore its confidentiality ought to be guaranteed. The proposed system the utilization of visual cryptography helps in secure transmission of information from sender to recipient in a dependable manner. the fundamental idea behind visual cryptography is to partition mystery pictures into arbitrary offers or random shares and afterward apply them to biometric information, for example, unique mark and iris with the end goal of client validation. in conventional the key that is created can be lost, forgotten or hard to recall in occasions however this paper acquaints a profitable route with manage key age from numerous element extraction from preprocessed finger impression and iris biometric pictures which are intertwined at feature level. Normalized values got from both the vectors are consolidated to frame cryptographic key age. utilizing key produced irregular lattice is shaped and shares are created which is encoded and further confirmed utilizing biometric authorization process at the unscrambling or decryption end henceforth this paper secured application using cryptographic key generation from different biometric modalities of human beings, and iris.

Key Words: Fingerprint, Iris Biometric, Key generation, Cryptography, Encryption, Decryption

1. INTRODUCTION

Visual Cryptography system is a proficient method to improve the data security, which scrambles a secret record or picture by breaking into n quantities of random shares. Pictures can be duplicated by stacking the pictures along with no complex cryptographic strategies. Visual cryptography is arrangement of code and interpret used to cover information into pictures so then it tends to be decoded in the collector end if so the correct key is being used. It is extremely hard to recuperate the first picture at the same time, the two layers of encryption and decoding should be fulfilled really at that time unique information can be

recuperated. In this manner visual cryptography permits secure transmission of mystery pictures. Visual cryptography can be utilized in military application for sending mystery maps, in organizations for sending private model, chart of activities and in financial field for sending marks, passwords, thumb impression and so forth Visual Cryptography conspire was first proposed by Noar and Shamir at Eurocrypt.

The visual cryptography (VC) is presumably the latest framework in which mystery pictures are engraved on the transparencies for an occurrence and they are passed on to n individuals. The essentials thought of visual cryptography communicates a picture is confined into n segments like share 1, share 2... so on. Here picture contains fundamentally two degrees of edification: splendid areas are named with 0.5 and level 0 is used to represent dull locales. With regards to one of the progression, cryptosystem will in general combine both cryptography and biometrics to abuse from the strong reasons for the two fields. In these structures, while the cryptosystem upgrades at high and level up the modifiable security framework, biometric clear the essential to recall passwords or to pass on delicate data. The improved presentation of cryptographic key that is made from biometrics in comprehension to security has gotten a goliath significance among researchers and experimenters. So as the achieve effective insurance from cryptographic attacks a beneficial system is used for confirming cryptographic key age dependent on various modalities like finger impression and iris.

Finger impression include extraction is procured from the finger impression of the client centers around securing, divisional and feature extraction. Thus the framework is liberated from exceptional imprint closeness peril. In like way, iris highlight extraction is done which is extraordinary regardless there age and furthermore individual have their left eye is unique in relation to that of right eye. It basically centers around the iris surface during procurement and afterward followed by division, standardization and coordinating. The two isolated features got are interwoven to manufacture the multimodal biometrics. At computational level blend is refined by strategies for

methodology that are connect, reworking lastly combination. Thus this interaction empowers better client confirmation and security for transmission of information in a dependable way.

2. LITRATURE SURVEY

[1].M.Karolin and T. Meyyappan proposed a system for Secret Multiple Share Creation with Color Images using Visual Cryptography to secure the transmitted images. It makes use of individual's optical action to translate the hidden conveying shares which were overlapped. The complex computations essential in traditional cryptography's disadvantages are compromised by this course of action.

[2]. K. Shankar and P. Eswaran have put forward the RGB Based Multiple Share Creation in Visual Cryptography with Aid of Elliptic Curve Cryptography. On the bases of pixel values this technique is used for creating shares. The pixel values extracted are used in order to put up the multiple shares (share 1, share 2,... share n) and these divisions are classified into blocks. By using the elliptical curve cryptography method the block of shares are encrypted and the same method i.e. ECC is used to decrypt the image which was encrypted.

[3] Gopal D. Dalvi and Dr.D.G.Wakde have putforth method for Facial Images Authentication in Visual Cryptography Using Sterilization Algorithm Unreadable shares in the decryption side is formed by the sterilization algorithm. All indecipherable portions are combined to form authentic depiction. Security is provided for each share key. It is the safest concept for encrypting shares at numerous measure using keys prepositions which one can never decrypt the image.

[4] Annie Daisy V, Vigesh Joe. C and Shinly swarna sugi.s shows An image based authentication technique using visual cryptography scheme In the paper visual cryptographic scheme for sharing confidential image is executed where the computer knowledge is not required for the decryption process as it is easy. In familiar with half toning algorithm encrypted divisions are dissected and the ciphered manifests are concealed in host image then secret image is verified during authentication.

[5] Trupti Patel and Rohit Srivastava proposed a method for A New Technique for Color Share Generation using Visual Cryptography[5].In this paper he proposes a new strategy generating a color band using visual cryptography, wherein it incorporates 3 main components i.e. Red, Green and Blue constituents are drawn out from color bands then gray share creation algorithm is applied to the Red component and then all divisions are combined into Blue, Green components to form colored bits. While in deciphering both Blue, Green components are taken-out from all the portions and combined into Red greyish shares to form Red component. Further all Red, Green and Blue is united to retrieve the

confidential image. Deciphered confidential image has the actual size as that of original confidential image.

[6] Taranpreet Kaur and Manvjeet Kaur proposed a new technique for Cryptographic Key Generation from Multimodal Template using Fuzzy Extractor[6] is one such paper which deals in how to enhance security, using fuzzy extractor the key is brought forth from different traits to improve reliability as well as accuracy of the biometrics. Fuzzy extractor technique is used on different modules like iris and fingerprint in this paper. Basically this is a two pace process, where the key formation stage includes in creation of uniformed random string (key) from multiple modules namely dual fingerprint and iris.

[7]Arpita Sarkar, Binod Kr Singh and Ujjayanta Bhaumik proposed a new scheme RSA Key Generation from Cancelable Fingerprint Biometrics [7]. In this paper it mainly focuses on how strongly cryptosystem key is being bridged with the fingerprint behavioral characteristic of the user and through cancelable fingerprint impression of the user a pair of public and private key is formed for RSA cryptosystem. From the drawn out fingerprint's minute features an asymmetric revocable key is generated and only which can be revoked using shuffling based transformation function applied on all minute locations.

[8] S.Sridevi Sathya Priya, P. Karthigai kumar and N.M. SivaMangai approaches a new scheme for Generation of 128-Bit Blended Key Using AES Algorithm [8]. In this paper using IRIS as well as arbitrary based key in what way generation of 128 bit blended key is fabricated explained in likewise. From IRIS features an IRIS based 128 bit key is formed which is more in-destructive than blended features. The key formed is well masked using arbitrary key forms a blended key using fuzzy commitment scheme up holds the privacy of the system and produced key's randomness is verified and correlated with other randomness of biometrics. The IRIS based biometric key's is 10% less random comparatively to blended keys.

[9] Bharti Kashyap and K. J. Satao proposed a methodology for Implementation of Multimodal Biometrics Cryptosystem for Information Security using Elliptic Curve Cryptography [9]. This paper provides a firm authentication in collaboration with multi biometrics using E.C.C that takes two modules (i) Blended fingerprint impression, facial features, IRIS and digital signatures (ii) In raise of elliptic curve methodology and key's using E.C.C method. In this paper, resizing the biometric features into a fixed size image and it is gray scaled.

[10]Arpita Sarkar and Binod Kr. Singh proposed a Cryptographic Key's Generation from a Cancelable Fingerprint Templates [10]. This paper deals in an ideal way being worked on cancelable fingerprint's impression of the operator and at the recipient end a symmetric key of 128 bit is produced. Eventually the sender and receiver generates canceled template from the impressions of the fingerprint's features and shared among themself for data transmission. Later by obtaining both canceled templates, a combined impression is created and from that combined template cryptosystem key is produced. By this presented approach it confirms the security of the fingerprint's system in use of one

way transformation of original template cancellation, resolves the struggle in storage of key's and key's revoking.

3. PROPOSED SYSTEM METHODOLOGIES

In this stage we examine the current methodology for age of got key from the numerous element extraction of biometrics. The goal of the framework is completed in these 5 phases predominantly:

1. We present Biometric highlight extraction
2. Key extraordinary for a bunch of information
3. Produce picture shares
4. Make encryption and furthermore hope to unscramble same
5. Make GUI for usability

An outlined structure of this scheme is to carry out in 5 different stages is explained below in fig. 1

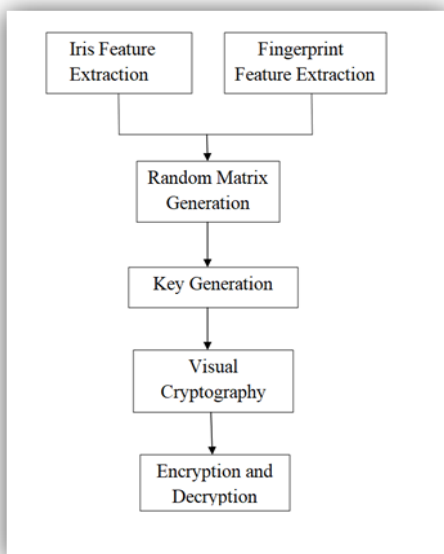


Fig -1: Schematic Structure of the Model

3.1 Fingerprint feature extraction

From the given finger impression format of the client minutia include extraction is done and it is coordinated with the format put away in the information base. The pre-handling stages required for the minutia extraction are

3.2 Image Enhance

Histogram Equalization is a method used to fine tune the image intensities by intensifying the contrast of the captured image. The histeq function compares the flat histogram

present and it results in output image with evenly distributed pixel values spread throughout the range.

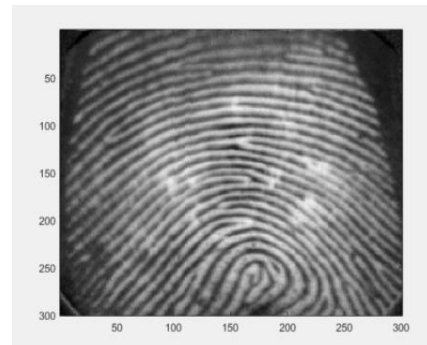


Fig -2: Histogram for Enhancement

3.3 Image Binarization

In this stage the enhanced image is binarized by transforming the gray scale picture into binary image. The fingerprint template while in binarization process produces 1-bit type image, before binarization ridges of fingerprint were usually black, with that of small intensity values are 1 (white ridge) and with the large intensity value it will be 0 i.e., black and white in the background and valleys.

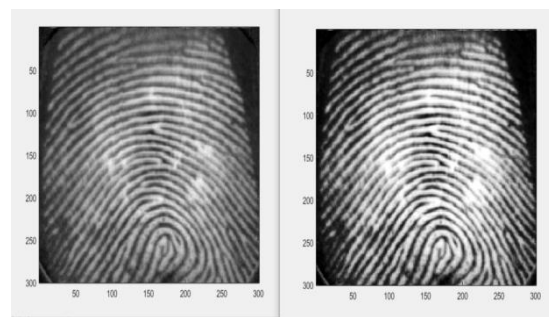


Fig -3: Binarising gray scale image

3.4 Fast Fourier Transform

After Binarization FFT is carried out, this improves the ridges in its appearance, as it cover up the tiny holes present in the ridges. FFT defines phase and magnitude of the ridges, that is how fast the ridges are changing and in which direction it is changing can be noted.

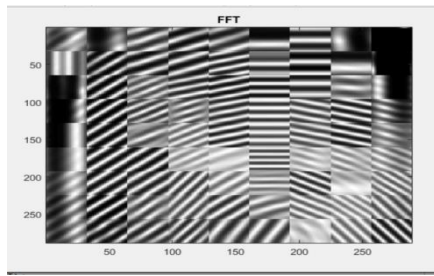


Fig -4: Fast Fourier Transform

3.5 Morphological Operation

Morphological operation is applied to a structural element of an input image creates an output of same size of input image. Morphological operation is a combination of erosion and dilation techniques. Erosion is for shrinking or thins the object in a binary image where as Dilation helps to grow or it thickens the object of the image.



Fig-5: Region of interest

3.6 Feature Extraction

At last the bifurcations, ridge ending and other minutia features are obtained in minutia extraction. A well-known approach called principal curve analysis is being used to distinguish the minutia points of a given template of the user.

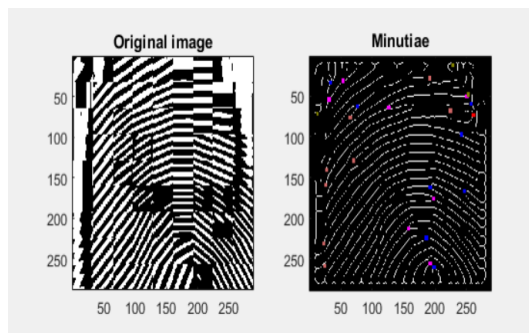


Fig -6: Minutiae Extraction

Standardized Values – After feature extraction is done, the highlighted featured values in each of the preprocessing stages are mapped in the database of size 36*64 single.

	1	2	3	4	5
1	191	28	1	0.0469	
2	53	31	3	2.3205	
3	33	33	3	5.0173	
4	250	50	3	0.0141	
5	31	54	3	1.9458	
6	257	59	3	4.2598	
7	76	63	3	5.7334	
8	126	64	3	2.8080	
9	224	68	1	0.0707	
10	261	73	1	5.4356	
11	65	76	1	2.3768	
12	242	97	3	3.3955	
13	70	129	1	2.4507	
14	27	141	1	1.8708	
15	26	159	1	1.8170	
16	192	162	3	3.2922	
17	246	167	3	3.5933	
18	197	176	3	0.3135	
19	158	213	3	2.5874	
20	196	224	3	6.2041	

Fig -7: Dataset1 of fingerprint feature

4. Iris Feature extraction

Featured points are drawn out from the given input image of the user. Process caught up in preprocessing for template extraction and matching are as follows:

4.1 Image acquisition

Acquisition mainly intended to overcome very low contrast in iris image which is captured and enhance the image quality for further extraction.

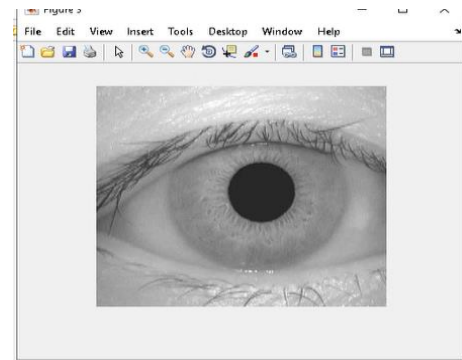


Fig -8: Image Enhancement

4.2 Localization/Normalization

Detects the inner and outer boundaries of pupil region by removing the eyelashes from the eyelid which might be covered at the center region. Normalization is done to process and remove dimensional inconsistency arised due to variation in illumination or improper angle placment while capturing the image

Segmentation

Iris Segmentation is like normalization process performed to remove false and unwanted noise/distortions in the image arised from illumination variations and angle misplacement

while capturing image. Segmentation illustrates all these phases for noise removal is as follows:

- Line coords: It returns x, y coordinate points of the position along with a scale.
- Find line: Using linear hough transform it returns the line coordinates (say x, y) in an image and canny edge detection is used in creating an edge map. Using canny findline top and bottom eyelid is found and line is drawn to represent the points which has sharp and maximum changes in the intensity values.

4.3 Hysthresh

This performs hysteresis threshold of an image and it also finalizes the edge detections by suppressing all other edges which are weak in connecting and not connected to the strong edges.

4.4 Gabor filter

It is used for texture analysis, which extract the significant feature from the normalized iris image and filter the unwanted noise as a result fixed length feature vector is obtained.

4.5 SURF (Speeded Up Robust Features)

Surf plays vital role in iris feature extraction and matching purpose. Surf provides following steps:

- Detects interest points.
- Fix the orientation based on information from a circular region around the point of interest, then erect a square region aligned to the selected orientation and then pull out the surf descriptor from it.
- Finally matching pairs are found by comparing the descriptors obtained from the processed image.

4.6 Minutiae Extraction

The feature is extracted after all the preprocessing stages and the template is matched with the original template cached in the database for authenticate purpose. The computational result found is shown in the image, the green color marking signifies highlighted featured points extracted in the image.

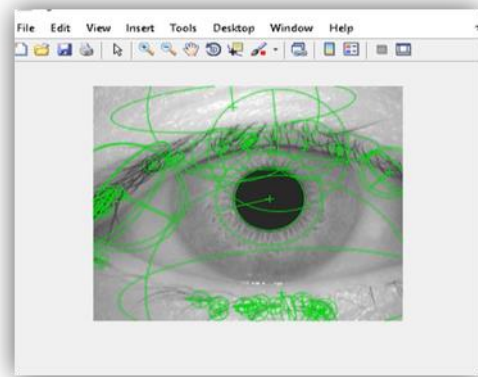


Fig -9: Minutiae Extraction

Standardized Values – After feature extraction is done, the highlighted featured values in each of the preprocessing stages are mapped in the database of size 36*64 single.

1	2	3	4	5	6	7	8	9	10	11
-0.0024	8.9602e-04	0.0008	0.0026	0.0444	-0.0026	0.0537	0.0182	-0.0076	0.0111	0.
0.0029	0.0013	0.0037	0.0021	-0.0120	0.0026	0.0191	0.0198	0.0054	0.0018	0.
-0.0019	0.0030	0.0129	0.0073	0.0205	-0.0250	0.0676	0.0515	-0.0194	-0.0051	0.
0.0055	-0.0014	0.0064	0.0037	-0.0215	-0.0086	0.0447	0.0223	-0.0136	0.0038	0.
0.0039	8.5354e-04	0.0039	0.0012	-0.0243	0.0057	0.1011	0.0484	0.0112	0.0230	0.
-0.0028	7.0656e-05	0.0040	0.0050	-3.0984e-04	-0.0716	0.0247	0.0867	-0.0072	-0.0237	0.
-0.0023	0.0027	0.0049	0.0037	-0.0088	-0.0192	0.0581	0.0395	9.3420e-04	-0.0187	0.
-0.0019	-0.0014	0.0027	0.0030	0.0044	-0.0193	0.0607	0.0679	0.0027	-0.0089	0.
0.0033	-0.0012	0.0067	0.0070	-0.0038	-0.0194	0.0650	0.0503	0.0141	0.0165	0.
-0.0079	-0.0072	0.0081	0.0084	4.1923e-04	0.0325	0.0322	0.0478	0.0302	0.0198	0.
-0.0053	-0.0016	0.0089	0.0056	-0.0217	-0.0408	0.0569	0.0583	0.0224	0.0160	0.
-0.0018	-0.0018	0.0020	0.0022	-0.0232	0.0027	0.0395	0.0220	0.0151	0.0210	0.
-0.0020	-0.0014	0.0022	0.0019	-0.0224	0.0045	0.0396	0.0253	0.0144	0.0241	0.
-0.0042	-7.8810e-04	0.0042	0.0014	0.0142	4.4087e-04	0.0538	0.0094	0.0052	0.0110	0.
0.0027	-5.4680e-04	0.0053	0.0042	-0.0076	-0.0108	0.0341	0.0217	0.0196	-0.0196	0.
-0.0078	-0.0030	0.0086	0.0034	-0.0176	-0.0134	0.0215	0.0215	0.0272	8.7532e-04	0.
0.0019	9.2720e-04	0.0021	9.3072e-04	-0.0160	0.0037	0.0386	0.0195	-0.0049	-0.0086	0.
0.0049	-0.0020	0.0092	0.0048	-0.0041	0.0100	0.0356	0.0256	0.0069	-0.0017	0.
-0.0013	7.7506e-04	0.0027	0.0012	-0.0043	0.0189	0.0719	0.0267	0.0106	0.0196	0.

Fig -10: Dataset 2 of iris feature

5.Key Generation

Key generation is done in two phases i.e., random matrix and key generation with the two dataset values of feature extraction. 3. Extract information required to generate key which is of Alpha numeric format

- Random Matrix- Key is randomly generated by combining both featured values of fingerprint and iris feature extraction. As shown in the below code data1 (fingerprint feature) and data2 (Iris feature) are considered and the zero elements in the dataset obtained from the featured values are removed and then it is filtered for further computation. In X1 the final datasets of both the features are considered i.e., (1:32) and from these vectored values key is generated.

```
data1=features_finger(:);
data2=features_eye(:);
data1(data1==0)=[];
```

```
data2(data2==0)=[];
x1=abs([data1(1:32,:);
```

```
floor(data2(1:32,:)*10000))]
key_gen=x1;
```

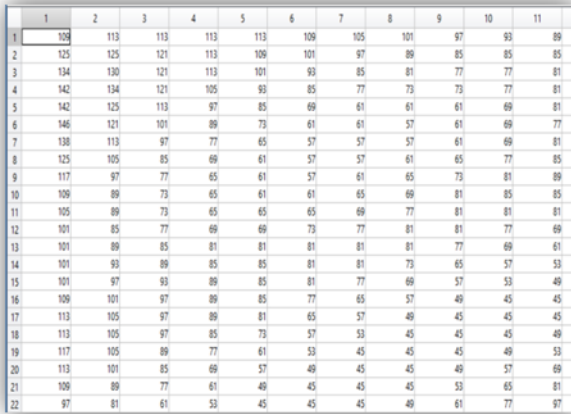


Fig -11: Radom Matrix Generation

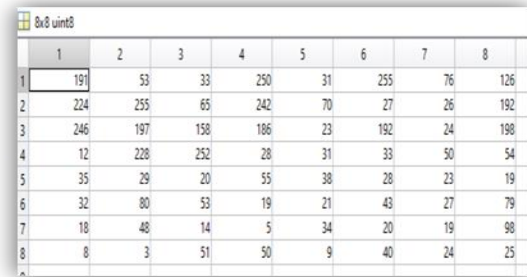


Fig -12: Key generation

Key Generation- By taking into consideration of the highlighted featured values key is generated into 8*8 unit8 matrix format. Unit8 is used as unsigned 8-bit integer and it is the range of the image pixel and images should not exceed that range. The flow of the lines while key generation is as follows:

```
n_r=8; %number of rows needed is 8
n_c=length(key_gen)/n_r;
key=zeros(n_r,n_c);
k=1;
for i=1:n_r % say 1:4
    for j=1:n_c % 1:3
        key(i,j)=key_gen(k);
        k=k+1;
    end
end
key=uint8(key);
m=8; % height of block size
n=8; % width of block size
K=3; % The number of embedding
its in each block.
N_K=2^K; % Binary public keys
Final_key=round(key/2);
```

5.1 Share Creation

Visual cryptography is used for share creation where n number of shares is created into various regions by dividing the image. Using secret sharing scheme the picture is ciphered into n meaningless shares. Information about original image cannot be leaked unless all the shares are obtained. The R, G, B color band pixel values are obtained and the output of that is considered as separate matrix.

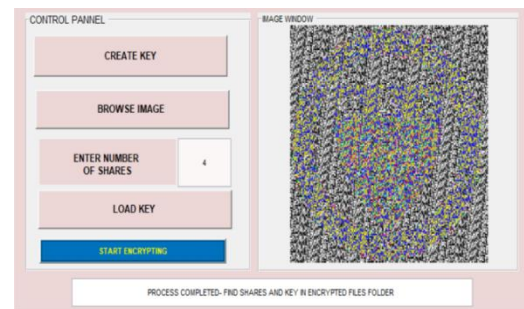


Fig -13: Share formation

5.2 Encryption and Decryption

Original image is divided to n number of R,G,B based color shares before ciphering the data and it finds the no of shares (n) to be formed which is of user specified and key generated is converted into ASCII values are loaded into the system for encryption. By giving the number of shares and loaded key secret image is encrypted and decrypted at the receiver end for retrieving the information. The key generated is used to decrypt the information. Decryption involves 3 steps as follows:

input: Load the data sent over any channel and provide the key and the no of shares to be done in the image.

Step-1: Validate key

Step-2: Decrypt information

Step-3: Display image

output: Image decrypted

A GUI is created to make it user friendly such that user loads image and provides the biometric data so that image is encrypted and similarly on the decryption side same process is followed to decrypt the data. The uniqueness in the project is biometric data being used as a key.

6. Performance Analysis

6.1 Feature Extraction Database

In this approach fingerprint and iris biometrics obtained datasets are stored in the database and obtained in use of generating a cryptographic key.

6.2 Research Setup

The proposed work is being implemented using intel® Core™ i5-7200U processor. It has specification of 2.71 GHZ clock speed in MATLAB (MATLAB 7.0.4) running with Windows 10OS. MATLAB is having many benefits when it is compared with the predictable processor languages (e.g., C, FORTRAN) for deciphering system difficulties. It is also referred as a communicating system in which the elementary data component as an array will not necessitate dimensioning standards. The software package is made available for commercially access since 1984 and it is now being deliberate as a standard implementation at most of the academies and industries over the world.

It is provided with all the built-in set of libraries and procedures that is needed to empower extensive assortment of computation. It includes a very simple to use graphics instructions that helps visualization consequences to retain instantly in no delay in time. Precise applications are composed in parcels is denoted as toolbox. There are various toolboxes used in sign dispensation, emblematic computation, control scheme, imitation, optimize data and in numerous field of practical science and in engineering.

The utmost tools made approachable from the desktop are:

- Command Window
- Command History
- Workspace
- Current Directory
- Help Browser

- Start button
- Command Window: It is majorly used in typing the commands.
- Current Directory: This directory maps the current folders and m-files.
- Workspace: This is used to note program variables and double clicking on a variable helps to see the same in the array editor window.
- Command History: This basically helps in viewing the past commands saved as a full-length hearing using the diary.
- Matlab Help-Browser used in any need of assistance.

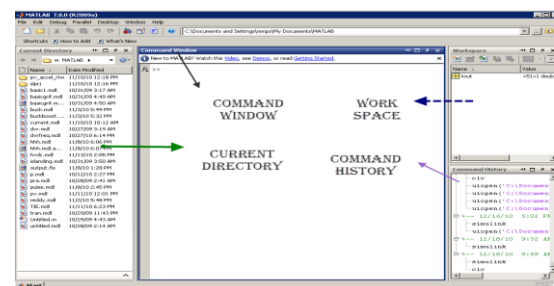


Fig -14: Graphical interface to MATLAB workspace

6.3 Experimental Results:

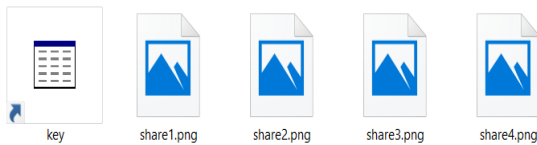
Multiple biometric modalities i.e., fingerprint and iris is loaded from the user as an input and same is provided for encryption that helps to maintain the security in system. In table V, the encrypted shares and the key stored are shown. The stacked image is taken out from the shares of the image and this stacked image is given as input to the decryption to get the original image and without any change in image quality. This methodology is made difficult for cryptographic assaults to obtain the key and retrieve sensitive information.

7. SECURITY ASPECTS

The user provides their original template or raw fingerprint and iris features for cryptographic key generation helps in security of the system as two biometrics are being used which is difficult of place an attack. Key is not generated without any one of the biometric feature and number of shares is user specified that can be changed for user need.

Once the shares are created and the key is shared and is loaded and it is converted into ASCII value and it is stored in the browser as .Mat file as shown in the figure. By the share created using the key generated from multiple biometrics will upheld the privacy and security of the system. Since, key is not

modifiable and it helps to deny all the attacks from cryptographic traits.



Framework issues are more diverse such that the validated users and the mystery passwords have restricted functionalities for all the user's. The outlook of the study is to examine the degree of acceptance of the system by allowing user authentication. This involves in training of user to use the system methodically and be validated. The user must not feel endangered or pressurized by the system in any issues related to GUI instead, they must accept it as a necessity and work on with the help of help browser. User must raise his level of confidence so that he will be capable of making some constructive examination, which is then encouraging, as he is the one who operates with the application and system.

CONCLUSION

In this paper, an ideal methodology is put forth to create a safe cryptographic key for joining different biometric modalities of individual, in order to provide a authenticated security. An efficient system is been carried out to build a cryptographic key depending on the multi-modular biometric (finger and iris) of human being is difficult for a intruder to work on it. The proposed strategy comprises of 3 main modules in particular with biometric template extraction, Multimodal biometric layout and a cryptosystem key generation from normalized values is obtained from feature extraction. At fusion level extracted highlights have been consolidated to get the multi-modal biometric layout. Ultimately, a 256 secured cryptosystem key has been generated. Hence, this paper presents a secured way of transmission of data from sender to receiver without loss of actual quality of data and protects data in a preserved manner.

REFERENCES

- [1] K. Shankar, P. Eswaran, "RGB Based Multiple Share Creation in Visual Cryptography with Aid of Elliptic Curve Cryptography" IEEE, 2017.
- [2] Trupti Pate, Rohit Srivastava. "New Technique for Color Share Generation using Visual Cryptography" IEEE, 2016.
- [3] Basma Ammour, Toufik Bouden, and Larbi Boubchir. "Face-Iris Multimodal Biometric System based on Hybrid Level Fusion"2018.
- [4] Jagadeesan, A. and Dr. K. Duraiswamy. "Secured cryptographic key generation from multimodal Biometrics: Feature level Fusion of Fingerprint and Iris, in International Journal of Computer Science and Information Security"2016.
- [5] L. Jani Anbarasi, G.S. Anadha Mala and D.R.L. Prassana, "Visual Secret Sharing of Color Image Using Extended Asmuth Bloom Technique", Springer, 2016.
- [6] Feng Hao, Ross Anderson, and John Daugman. "Combining crypto with biometrics effectively. IEEE transactions on computers",55(9):1081- 1088.
- [7] Anil K Jain, Karthik Nandakumar, and Abhishek Nagar. "Biometric template security. EURASIP Journal on advances in signal processing", 2008:113.
- [8] Heena M. Patel, Chirag N. Panuwala, Aarohi Vora. "Hybrid Feature level approach for Multi-biometric Cryptosystem", 2016
- [9] Arpita Sarkar, Binod Kr. Singh, "Cryptographic Key Generation From Cancelable Fingerprint Templates",2018
- [10] Arpita Sarkar, Binod Kr Singh."Cancelable Biometric Based Key Generation for Symmetric Cryptography".2018