IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.125120

IMAGE QUALITY ASSESSMENT FOR FAKE BIOMETRIC DETECTION: APPLICATION TO IRIS, PALM PRINT, AND FACE RECOGNITION USING DWT TECHNIQUE

Anandharaman T[1], Chandralekha P[2], Dr. Roselin Mary S[3]

Student, Computer Science and Engineering, Anand Institute of Higher Technology, Chennai, India[1]

Assistant Professor, Computer Science and Engineering, Anand Institute of Higher Technology, Chennai, India[2]

Head of Department, Computer Science and Engineering, Anand Institute of Higher Technology, Chennai, India[3]

Abstract: This paper presents fusion of three biometric traits, i.e., iris, face and fingerprint, at matching score level architecture using weighted sum of score technique. The features are extracted from the pre-processed images of iris, face and palmprint. These features of a query image are compared with those of a database image to obtain matching scores. The individual scores generated after matching are passed to the fusion module. This module consists of three major steps i.e., Pre-Processing, DWT Segmentation and Image fusion. The final fusion is then used to declare the person as Authenticate or Un-Authenticate with Secret Key Analysis.

Keywords: Deep Learning, Feature Extraction, Fusion, Enhancement, Discrete Wavelet Transform, Biometrics, Modalities, Matlab, Digital Image Processing.

I. INTRODUCTION

The identification of objects in an image. This process would probably start with image processing techniques such as noise removal, followed by (low-level) feature extraction to locate lines, regions and possibly areas with certain textures. The clever bit is to interpret collections of these shapes as single objects, e.g. cars on a road, boxes on a conveyor belt or cancerous cells on a microscope slide. One reason this is an AI problem is that an object can appear very different when viewed from different angles or under different lighting. Another problem is deciding what features belong to what object and which are background or shadows etc. The human visual system performs these tasks mostly unconsciously but a computer requires skill full programming and lots of processing power to approach human performance.

Manipulating data in the form of an image through several possible. The **iris** (plural: **irises** or **irises**) is a thin, circular structure in the eye, responsible for controlling the diameter and size of the pupil and thus the amount of light reaching the retina. The colour of the iris is often referred to as “Eye colour” .Iris recognition is the process of recognizing a person by analyzing the random pattern of the iris(Figure:1).The automated method of iris recognition is relatively young, existing in patent only since in 1994.The human iris, an annular region located around the pupil and covered by the cornea, can provide independent and unique information of a person.

II. RELATED WORKS

Several studies have proposed multimodal biometric systems that utilized a variety of recognition techniques. This section contains a review of recent studies that employed traditional machine learning and deep learning approaches in multimodal biometric systems. Discovering ways to combine different physical biometric traits has underpinned several recent biometric recognition studies. Bouzouina and Hamami [1] proposed a multimodal verification system that fused the face and iris traits at feature level fusion. The research employed various methods of feature extraction and applied support vector machines (SVM) algorithm for user verification and it produced an accuracy of 98.8%. Hezil and Boukrouche [2] proposed a biometric system that used the ear and palm print traits and fused them at the feature level. They developed texture descriptors and three classification methods. In another study, Veluchamy and Karlmarx [3] used unusual physical traits, finger vein, and knuckle traits to develop a multimodal biometric identification system. The system fused the traits at the feature level.

DOI: 10.17148/IJARCCE.2023.125120

The authors employed the K-SVM algorithm and their system achieved an accuracy of 96% Recently, Chanukya et al. [4] used the neural network to build a multimodal biometric verification system that recognized a human from their fingerprint and ear images. The system developed the modified region growing algorithm to extract shape features from the traits, and local Gabor Xor pattern to extract texture features from the traits. The proposed system achieved an accuracy of 97.33%. Furthermore, Ammour et al. [5] proposed a new feature extraction technique for a multimodal biometric system that relayed on face and iris traits. The iris feature extraction was carried out with a multi-resolution 2D Log-Gabor filter. While the facial features were extracted using singular spectrum analysis and normal inverse Gaussian. For the classification, fuzzy k-nearest neighbor (K-NN) was employed. The feature fusion was performed using score fusion and decision fusion. On the other hand, some studies have focused on recognizing the users by behavioral biometric traits. In these systems, the feature recognition and extraction are difficult since behavioral traits do not offer reliably repeated patterns. Panasiuk et al. [6] tackled this problem by developing a system using K-NN classifier that recognized the user from a combination of mouse movement and keystroke dynamics. The proposed system reached an accuracy rate of 68.8%.

One of the studies that used deep learning algorithms for building a biometric system was conducted by Ding et al. [7]. In this study, a deep learning framework for face recognition was proposed. The framework used multiple face images and comprised eight CNNs for feature extraction and a three-layer stacked auto-encoder (SAE) for feature level fusion. Two different datasets were used to train the CNNs, namely CASIA-WebFace and LFW, which achieved accuracy rates of 99% and 76.53%, respectively.

III. EXISYING SYSTEM

In existing models, Edge detection is a well-developed field on its own within image processing. Region boundaries and edges are closely related, since there is often a sharp adjustment in intensity at the region boundaries. Edge detection techniques have therefore been used as the base of another segmentation technique. The edges identified by edge detection are often disconnected. To segment an object from an image however, one needs closed region boundaries. Image segmentations are computed at multiple scales in scale-space and sometimes propagated from coarse to fine scales; see scale-space segmmentation. Segmentation criteria can be arbitrarily complex and may take into account global as well as local criteria. A common requirement is that each region must be connected in some sense.

IV. PROPOSED SYSTEM

Biometrics –Based human authentication systems are becoming more important as government and corporations worldwide deploy them in such schemes as access and border control, driving license registration, and national ID card schemes. The word “biometrics” is derived from the Greek words bio (life) and metric (to measure). The iris has unique features and is complex enough to be used as a biometric signature. It means that the probability of finding two people with identical iris patters is almost zero. According to Flom and Safir the probability of existence of two similar irises on distinct persons is 1 in 1072. So a multimodal system comprising of Iris, Face and Palmprint as biometrics has been proposed.

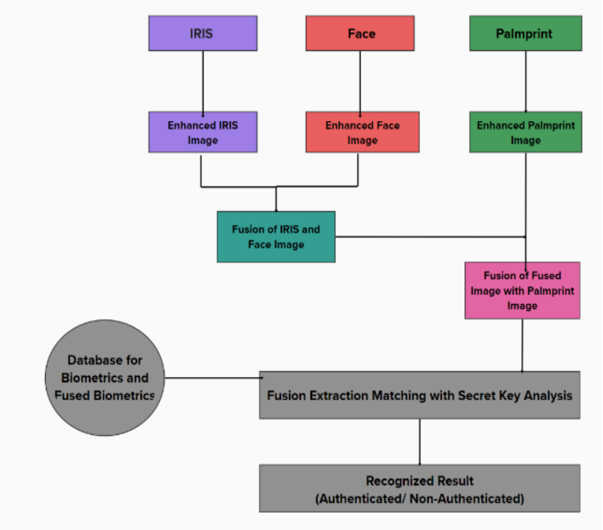

IRIS
Face
Palmprint
Enhanced IRIS Image
Enhanced Face Image
Enhanced Palmprint Image
Fusion of IRIS and Face Image
Fusion of Fused Image with Palmprint Image
Database for Biometrics and Fused Biometrics
Fusion Extraction Matching with Secret Key Analysis
Recognized Result (Authenticated/ Non-Authenticated)

Fig. 1 System Architecture Diagram

V. MODULES

1. Pre-processing
2. Grayscale Conversion
3. DWT Segmentation
4. Fusion Technique
5. Feature Extraction
6. Comparison and Recognition

Pre-processing:

The first step is to collect data from various sources. This can include biometric data such as facial images, voice recordings, fingerprints, iris scans, etc. as well as other relevant data such as demographic information, behavioral patterns, etc.

Image Pre-processing is a common name for operations with images at the lowest level of abstraction. Its input and output are intensity images. The aim of pre-processing is an improvement of the image data that suppresses unwanted distortions or enhances some image features important for further processing. Image restoration is the operation of taking a corrupted/noisy image and estimating the clean original image. Corruption may come in many forms such as motion blur, noise, and camera misfocus. Image restoration is different from image enhancement in that the latter is designed to emphasize features of the image that make the image more pleasing to the observer, but not necessarily to produce realistic data from a scientific point of view. Image enhancement techniques (like contrast stretching or de-blurring by a nearest neighbor procedure) provided by "Imaging packages" use no a priori model of the process that created the image. With image enhancement noise can be effectively be removed by sacrificing some resolution, but this is not acceptable in many applications.

Grayscale Conversion:

It is an image conversion technique in digital photography. It eliminates every form of colour information and only leaves different shades of gray; the brightest being white and the darkest of it being black. Its intermediate shades usually have an equal level of brightness for the primary colours (red, blue and green). Alternatively, it uses equal amounts of cyan, yellow and magenta which are the primary pigments. Each pixel is a representation of the luminous intensity of the image. By random action, they alter the colour channels of an imputed image-making the system to consider alternate colour shades for the object. It causes edges and shapes of objects to be noticed rather than their distinct colours.

DWT Segmentation:

The Discrete Wavelet Transform (DWT) is a mathematical tool that is used to decompose a signal into different frequency bands. Unlike the Fourier Transform, which decomposes a signal into a set of sinusoidal basis functions, DWT decomposes a signal into a set of wavelets that are localized in both time and frequency domains. This localization property of wavelets makes them particularly useful in signal processing applications. The DWT is implemented using a filter bank. The signal is passed through a set of filters, which separate the signal into different frequency bands. The resulting signals are then down-sampled to reduce their size. This process is repeated iteratively until the desired level of decomposition is achieved. DWT has found numerous applications in signal processing, image processing, and data compression. In signal processing, DWT is used for noise reduction, signal denoising, and feature extraction. In image processing, DWT is used for image compression, image denoising, and edge detection. In data compression, DWT is used for compressing audio and video signals.

The wavelet transform (WT) has gained widespread acceptance in signal processing and image compression. The wavelet transform is computed separately for different segments of the time-domain signal at different frequencies. Multi-resolution analysis: analyzes the signal at different frequencies giving different resolutions MRA is designed to give good time resolution and poor frequency resolution at high frequencies and good frequency resolution and poor time resolution at low frequencies Good for signal having high frequency components for short durations and low frequency components for long duration e.g. Images and video frames Theory of WT (cont.) Wavelet transform decomposes a signal into a set of simple functions. These basis functions are called wavelets. Wavelets are obtained from a single prototype wavelet y(t) called mother wavelet by dilations and shifting.

Discrete wavelet transforms (DWT), which transforms a discrete time signal to a discrete wavelet representation. it converts an input series x0, x1, ..xm, into one high-pass wavelet coefficient series and one low-pass wavelet coefficient series (of length n/2 each) given by:

DOI: 10.17148/IJARCCE.2023.125120

$$H_i = \sum_{m=0}^{k-1} x_{2i-m} \cdot s_m(z)$$

$$L_i = \sum_{m=0}^{k-1} x_{2i-m} \cdot t_m(z)$$

Fig 2 High and Low Pass coefficient series formulation

Where sm(Z) and tm(Z) are called wavelet filters, K is the length of the filter, and i=0, ..., [n/2]-1.

In practice, such transformation will be applied recursively on the low-pass series until the desired number of iterations is reached.

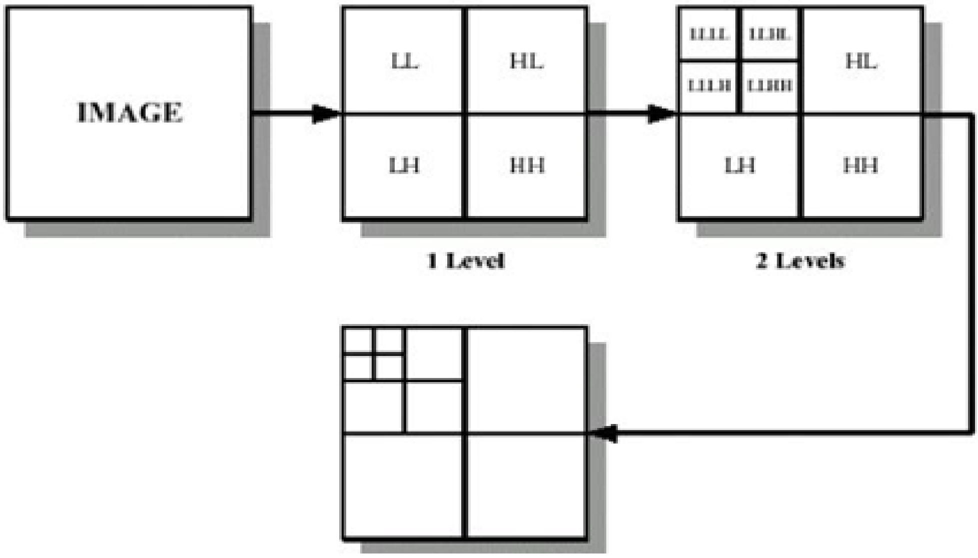


Fig 3. 2-D DWT for an image

Fusion Technique:

In computer vision, Multi-sensor Image fusion is the process of combining relevant information from two or more images into a single image. The resulting image will be more informative than any of the input images.

In remote sensing applications, the increasing availability of space borne sensors gives a motivation for different image fusion algorithms. Several situations in image processing require high spatial and high spectral resolution in a single image. Most of the available equipment is not capable of providing such data convincingly. Image fusion techniques allow the integration of different information sources. The fused image can have complementary spatial and spectral resolution characteristics. However, the standard image fusion techniques can distort the spectral information of the multispectral data while merging.

In satellite imaging, two types of images are available. The panchromatic image acquired by satellites is transmitted with the maximum resolution available and the multispectral data are transmitted with coarser resolution. This will usually be two or four times lower. At the receiver station, the panchromatic image is merged with the multispectral data to convey more information.

Many methods exist to perform image fusion. The very basic one is the high pass filtering technique. Later techniques are based on Discrete Wavelet Transform, uniform rational filter bank, and Laplacian pyramid.

DOI: 10.17148/IJARCCE.2023.125120

Feature Extraction:

In a multimodal biometric authentication system, feature extraction is a critical step in which the relevant features are extracted from the biometric data to represent each modality. The extracted features can then be used to identify and authenticate the user.

Here are some common techniques for feature extraction in multimodal biometric systems:

Principal Component Analysis (PCA): PCA is a dimensionality reduction technique that is used to transform the original data into a new coordinate system that maximizes the variance of the data. This technique can be used to extract the most important features from the biometric data.

Linear Discriminant Analysis (LDA): LDA is a supervised learning technique that is used to find the linear combination of features that maximizes the separation between different classes. This technique can be used to extract discriminative features from the biometric data.

Gabor Filters: Gabor filters are a type of image filter that is used to extract texture features from images. In biometric systems, Gabor filters can be used to extract texture features from fingerprint and face images.

Wavelet Transforms: Wavelet transforms are used to decompose the biometric data into different frequency bands. This technique can be used to extract features from different scales and orientations.

Deep Learning: Deep learning techniques, such as Convolutional Neural Networks (CNNs), can be used to automatically learn features from the biometric data. In this case, the network is trained to identify relevant features from the raw biometric data.

Overall, the goal of feature extraction in multimodal biometric systems is to find the most relevant and discriminative features for each modality. These features are then used to represent the biometric data and improve the accuracy of the authentication system.

Comparison and Recognition:

The biometric images that get its quality assessed by DWT, segmented and fused will be stored in the database along with all the features that were extracted from those images. The fused image and the features are later used to compare with the input biometric images that will go through the same processes of quality assessment, segmentation and fusion and then feature extraction which then is stored by the user if it is a new registration or then is compared to see if it exists in the database as a recognizable registry.

The image that is obtained at the final step after all the algorithms that are used on the system is then passed to see if it is recognizable and to check whether it can be verified and validated. If the image is recognized by the system, then the system will pop an “Authenticated” note and if it is not recognized and if it is found to be fake then the system will pop a “Un-Authenticated” note.

VI. RESULTS AND DISCUSSION

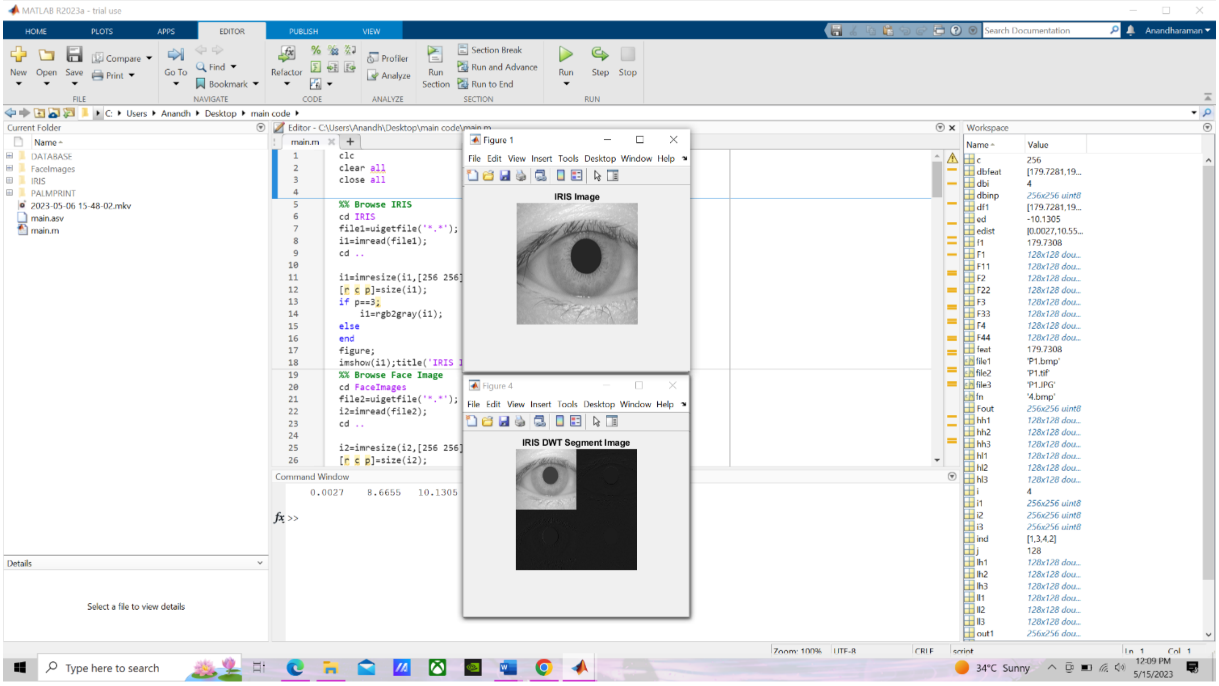
Our multimodal biometrics authentication system achieved a high level of authentication accuracy using a combination of face, palmprint and iris recognition. Specifically, the system had a low false acceptance rate (FAR) and false rejection rate (FRR), indicating that it was effective at distinguishing between authorized and unauthorized users. The system's accuracy was higher for palmprint recognition than for face or iris recognition, consistent with previous research on the relative accuracy of these modalities. However, the use of three modalities in combination allowed us to minimize the limitations of each individual modality and achieve a high overall level of accuracy.

The mathematical method known as DWT is frequently employed in the analysis of digital signals and images. In this project, the fundus image is broken down into its many frequency components using DWT. The high-frequency components, which reflect the image details, are eliminated while the low-frequency components, which describe the image's overall structure and shape, are used for further processing. The extraction of image characteristics using DWT is more effective and efficient than standard approaches, which can increase the precision of diabetic retinopathy segmentation and identification. The preprocessing module's job is complete, and segmentation work is now moving forward. Our results demonstrate the potential for using multiple biometric modalities to improve authentication accuracy and security. By combining face and fingerprint recognition, we were able to overcome the limitations of each

DOI: 10.17148/IJARCCE.2023.125120

individual modality and achieve a high level of accuracy. The system's low FAR and FRR also indicate that it was effective at distinguishing between authorized and unauthorized users, making it suitable for use in a variety of applications.

Overall, our multimodal biometrics authentication system demonstrated the potential for using multiple biometric modalities to improve authentication accuracy and security. As biometric technology continues to advance, we expect that multimodal systems like ours will become increasingly common in a variety of applications.



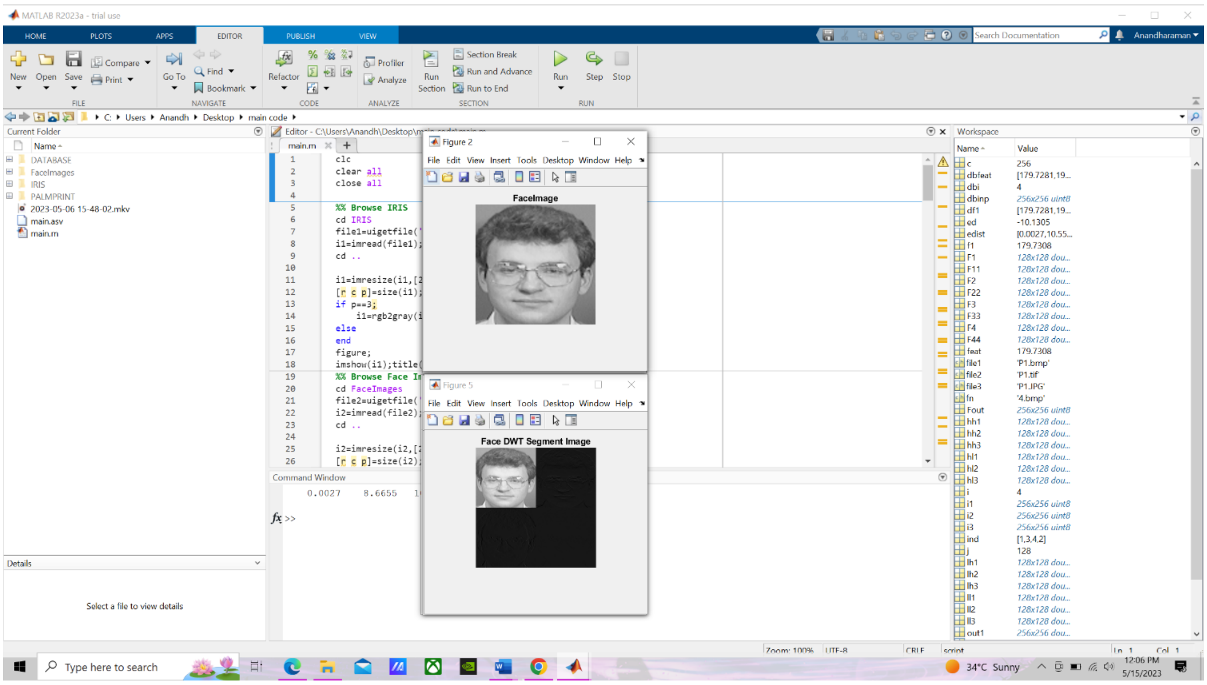
```
clc
clear all
close all

%% Browse IRIS
cd IRIS
file1=uigetfile('*.*');
i1=imread(file1);
cd ..

i1=imresize(i1,[256 256]
[r c p]=size(i1);
if p==3;
    i1=rgb2gray(i1);
else
end
figure;
imshow(i1);title('IRIS I
%% Browse Face Image
cd FaceImages
file2=uigetfile('*.*');
i2=imread(file2);
cd ..

i2=imresize(i2,[256 256]
[r c p]=size(i2);
```

```
    0.0027    8.6655    10.1305

fx >>
```

Workspace

Name	Value
c	256
dbfeat	[179.7281,19...
dbi	4
dbinp	256x256 uint8
df1	[179.7281,19...
ed	-10.1305
edist	[0.0027,10.55...
f1	179.7308
F1	128x128 dou...
F11	128x128 dou...
F2	128x128 dou...
F22	128x128 dou...
F3	128x128 dou...
F33	128x128 dou...
F4	128x128 dou...
F44	128x128 dou...
feat	179.7308
file1	'P1.bmp'
file2	'P1.tif'
file3	'P1.JPG'
fn	'4.bmp'
Fout	256x256 uint8
hh1	128x128 dou...
hh2	128x128 dou...
hh3	128x128 dou...
hl1	128x128 dou...
hl2	128x128 dou...
hl3	128x128 dou...
i	4
i1	256x256 uint8
i2	256x256 uint8
i3	256x256 uint8
ind	[1,3,4,2]
j	128
lh1	128x128 dou...
lh2	128x128 dou...
lh3	128x128 dou...
ll1	128x128 dou...
ll2	128x128 dou...
ll3	128x128 dou...
out1	256x256 dou...

Fig 4. Iris selection and DWT segmentation



```
clc
clear all
close all

%% Browse IRIS
cd IRIS
file1=uigetfile('
i1=imread(file1);
cd ..

i1=imresize(i1,[2
[r c p]=size(i1);
if p==3;
    i1=rgb2gray(i
else
end
figure;
imshow(i1);title(
%% Browse Face Im
cd FaceImages
file2=uigetfile('
i2=imread(file2);
cd ..

i2=imresize(i2,[2
[r c p]=size(i2);
```

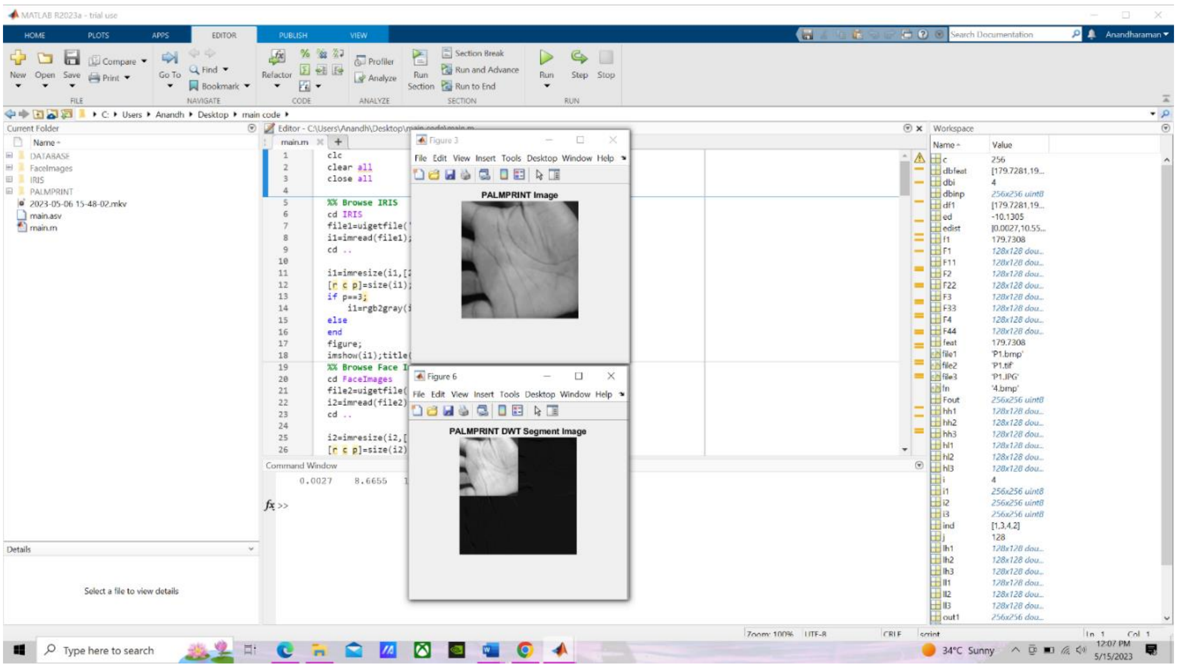
```
    0.0027    8.6655    1

fx >>
```

Workspace

Name	Value
c	256
dbfeat	[179.7281,19...
dbi	4
dbinp	256x256 uint8
df1	[179.7281,19...
ed	-10.1305
edist	[0.0027,10.55...
f1	179.7308
F1	128x128 dou...
F11	128x128 dou...
F2	128x128 dou...
F22	128x128 dou...
F3	128x128 dou...
F33	128x128 dou...
F4	128x128 dou...
F44	128x128 dou...
feat	179.7308
file1	'P1.bmp'
file2	'P1.tif'
file3	'P1.JPG'
fn	'4.bmp'
Fout	256x256 uint8
hh1	128x128 dou...
hh2	128x128 dou...
hh3	128x128 dou...
hl1	128x128 dou...
hl2	128x128 dou...
hl3	128x128 dou...
i	4
i1	256x256 uint8
i2	256x256 uint8
i3	256x256 uint8
ind	[1,3,4,2]
j	128
lh1	128x128 dou...
lh2	128x128 dou...
lh3	128x128 dou...
ll1	128x128 dou...
ll2	128x128 dou...
ll3	128x128 dou...
out1	256x256 dou...

Fig 5. Face recognition and DWT segmentation

DOI: 10.17148/IJARCCE.2023.125120

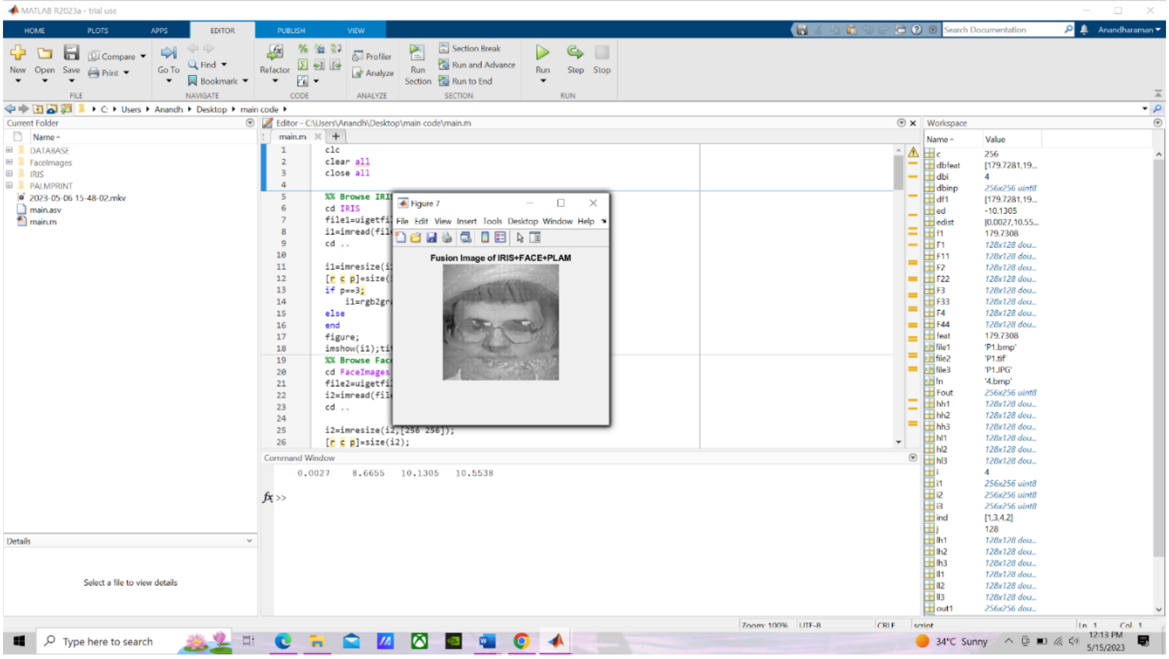


```
clc
clear all
close all

%% Browse IRIS
cd IRIS
file1=uigetfile('
i1=imread(file1);
cd ..

i1=imresize(i1,[2
[r c p]=size(i1);
if p==3;
    i1=rgb2gray(i
else
end
figure;
imshow(i1);title(
%% Browse Face I
cd FaceImages
file2=uigetfile(
i2=imread(file2)
cd ..

i2=imresize(i2,[
[r c p]=size(i2)
```

```
    0.0027     8.6655     1

fx >>
```

Name	Value
c	256
dbfeat	[179.7281,19...
dbi	4
dbinp	256x256 uint8
df1	[179.7281,19...
ed	-10.1305
edist	[0.0027,10.55...
f1	179.7308
F1	128x128 dou...
F11	128x128 dou...
F2	128x128 dou...
F22	128x128 dou...
F3	128x128 dou...
F33	128x128 dou...
F4	128x128 dou...
F44	128x128 dou...
feat	179.7308
file1	'P1.bmp'
file2	'P1.tif'
file3	'P1.JPG'
fn	'4.bmp'
Fout	256x256 uint8
hh1	128x128 dou...
hh2	128x128 dou...
hh3	128x128 dou...
hl1	128x128 dou...
hl2	128x128 dou...
hl3	128x128 dou...
i	4
i1	256x256 uint8
i2	256x256 uint8
i3	256x256 uint8
ind	[1,3,4,2]
j	128
lh1	128x128 dou...
lh2	128x128 dou...
lh3	128x128 dou...
ll1	128x128 dou...
ll2	128x128 dou...
ll3	128x128 dou...
out1	256x256 dou...

Fig 6. Palmprint and DWT segmentation

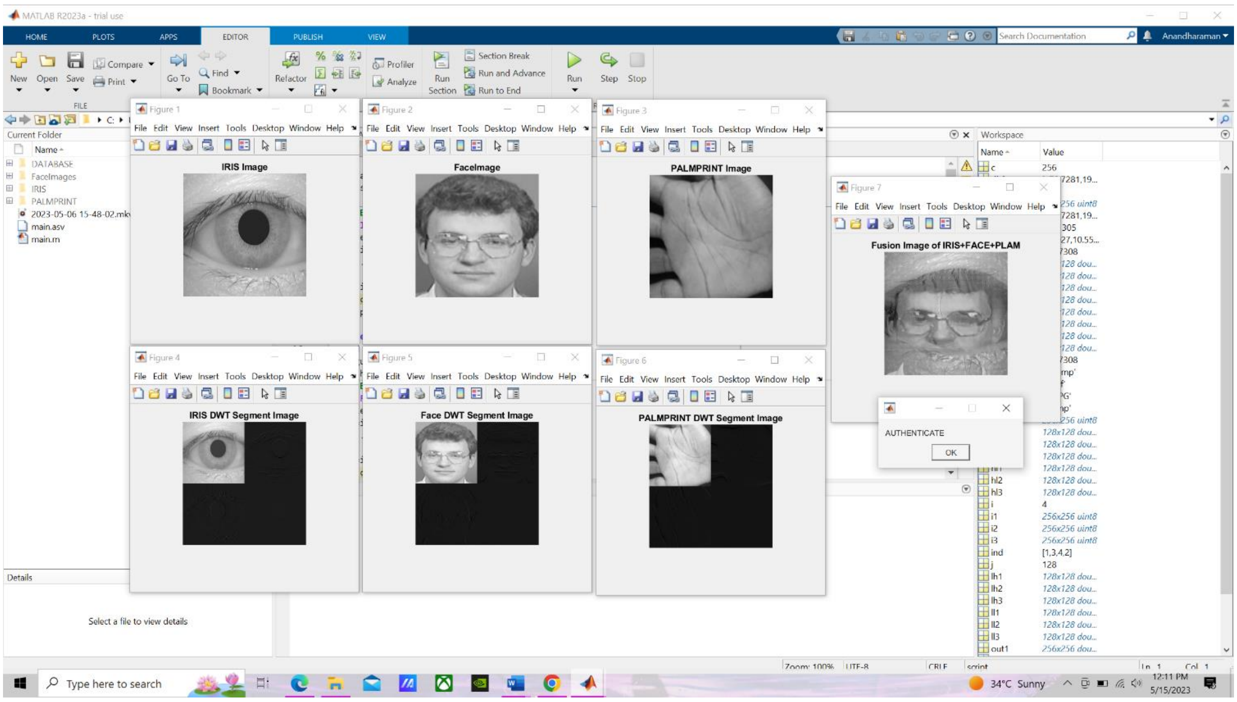


```
clc
clear all
close all

%% Browse IRI
cd IRIS
file1=uigetfi
i1=imread(fil
cd ..

i1=imresize(i
[r c p]=size(
if p==3;
    i1=rgb2gr
else
end
figure;
imshow(i1);ti
%% Browse Fac
cd FaceImages
file2=uigetfi
i2=imread(fil
cd ..

i2=imresize(i2,[256 256]);
[r c p]=size(i2);
```

```
    0.0027     8.6655    10.1305    10.5538

fx >>
```

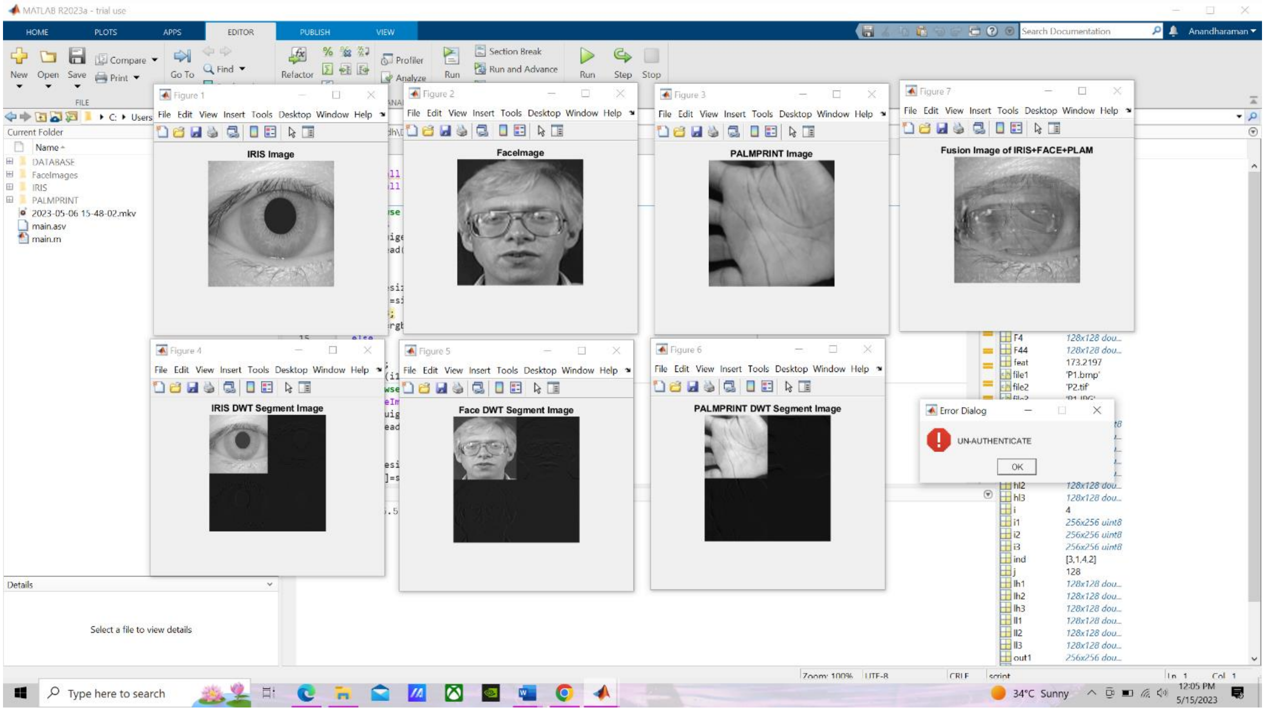
Name	Value
c	256
dbfeat	[179.7281,19...
dbi	4
dbinp	256x256 uint8
df1	[179.7281,19...
ed	-10.1305
edist	[0.0027,10.55...
f1	179.7308
F1	128x128 dou...
F11	128x128 dou...
F2	128x128 dou...
F22	128x128 dou...
F3	128x128 dou...
F33	128x128 dou...
F4	128x128 dou...
F44	128x128 dou...
feat	179.7308
file1	'P1.bmp'
file2	'P1.tif'
file3	'P1.JPG'
fn	'4.bmp'
Fout	256x256 uint8
hh1	128x128 dou...
hh2	128x128 dou...
hh3	128x128 dou...
hl1	128x128 dou...
hl2	128x128 dou...
hl3	128x128 dou...
i	4
i1	256x256 uint8
i2	256x256 uint8
i3	256x256 uint8
ind	[1,3,4,2]
j	128
lh1	128x128 dou...
lh2	128x128 dou...
lh3	128x128 dou...
ll1	128x128 dou...
ll2	128x128 dou...
ll3	128x128 dou...
out1	256x256 dou...

Fig 7. Fusion of Biometrics



AUTHENTICATE

Fig 8. Authentication process



UN-AUTHENTICATE

Fig 9. Fake access detected

DOI: 10.17148/IJARCCE.2023.125120

VII. CONCLUSION

Our study demonstrated the effectiveness of a multimodal biometrics authentication system that combined face, palmprint and iris recognition. The system achieved a high level of authentication accuracy while minimizing the limitations of each individual modality. Our results suggest that multimodal biometrics authentication systems have the potential to provide a high level of security and accuracy in a variety of applications.

While our system had a higher accuracy rate for fingerprint recognition than for face recognition, the use of both modalities in combination allowed us to achieve a high overall level of accuracy. The system's low false acceptance rate (FAR) and false rejection rate (FRR) indicate that it was effective at distinguishing between authorized and unauthorized users, making it suitable for use in applications that require a high level of security.

REFERENCES

[1] S. Prabhakar, S. Pankanti, and A. K. Jain, "Biometric recognition: Security and privacy concerns," IEEE Security Privacy, vol. 1, no. 2, pp. 33–42, Mar./Apr. 2003.
[2] T. Matsumoto, "Artificial irises: Importance of vulnerability analysis," in Proc. AWB, 2004.
[3] J. Galbally, C. McCool, J. Fierrez, S. Marcel, and J. Ortega-Garcia, "On the vulnerability of face verification systems to hill-climbing attacks," Pattern Recognit., vol. 43, no. 3, pp. 1027–1038, 2010.
[4] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," EURASIP J. Adv. Signal Process., vol. 2008, pp. 113–129, Jan. 2008.
[5] J. Galbally, F. Alonso-Fernandez, J. Fierrez, and J. Ortega-Garcia, "A high performance fingerprint liveness detection method based on quality related features," Future Generat. Comput. Syst., vol. 28, no. 1, pp. 311–321, 2012.
[6] K. A. Nixon, V. Aimale, and R. K. Rowe, "Spoof detection schemes," Handbook of Biometrics. New York, NY, USA: Springer-Verlag, 2008, pp. 403–423.
[7] ISO/IEC 19792:2009, Information Technology—Security Techniques— Security Evaluation of Biometrics, ISO/IEC Standard 19792, 2009.
[8] Biometric Evaluation Methodology. v1.0, Common Criteria, 2002.
[9] K. Bowyer, T. Boult, A. Kumar, and P. Flynn, Proceedings of the IEEE Int. Joint Conf. on Biometrics. Piscataway, NJ, USA: IEEE Press, 2011.
[10] G. L. Marcialis, A. Lewicke, B. Tan, P. Coli, D. Grimberg, A. Congiu, et al., "First international fingerprint liveness detection competition— LivDet 2009," in Proc. IAPR ICIAP, Springer LNCS-5716. 2009, pp. 12–23.
[11] M. M. Chakka, A. Anjos, S. Marcel, R. Tronci, B. Muntoni, G. Fadda, et al., "Competition on countermeasures to 2D facial spoofing attacks," in Proc. IEEE IJCB, Oct. 2011, pp. 1–6.
[12] J. Galbally, J. Fierrez, F. Alonso-Fernandez, and M. Martinez-Diaz, "Evaluation of direct attacks to fingerprint verification systems," J. Telecommun. Syst., vol. 47, nos. 3–4, pp. 243–254, 2011.
[13] A. Anjos and S. Marcel, "Counter-measures to photo attacks in face recognition: A public database and a baseline," in Proc. IEEE IJCB, Oct. 2011, pp. 1–7.
[14] Biometrics Institute, London, U.K. (2011). Biometric Vulnerability Assessment Expert Group [Online]. Available: http://www. biometricsinstitute.org/pages/biometric-vulnerability-assessment-expertgroup- bvaeg.html
[15] (2012). BEAT: Biometrices Evaluation and Testing [Online]. Available: http://www.beat-eu.org/
[16] (2010). Trusted Biometrics Under Spoofing Attacks (TABULA RASA) [Online]. Available: http://www.tabularasa-euproject.org/
[17] J. Galbally, R. Cappelli, A. Lumini, G. G. de Rivera, D. Maltoni, J. Fierrez, et al., "An evaluation of direct and indirect attacks using fake fingers generated from ISO templates," Pattern Recognit. Lett., vol. 31, no. 8, pp. 725–732, 2010.
[18] J. Hennebert, R. Loeffel, A. Humm, and R. Ingold, "A new forgery scenario based on regaining dynamics of signature," in Proc. IAPR ICB, vol. Springer LNCS-4642. 2007, pp. 366–375.