IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.12 ⁜ Vol. 10, Issue 2, February 2023

DOI: 10.17148/IARJSET.2023.10216

Information Security Using biometric watermarking

Dheemanth G[1], DeviPrasad N[2],Kalyan Chowdary B[3],Kottala Saivenkat Suchith[4]

Department of Computer Science & Engineering, KSIT, Bengaluru, India[1]

Department of Computer Science & Engineering, KSIT, Bengaluru, India[2]

Department of Computer Science & Engineering, KSIT, Bengaluru, India[3]

Department of Computer Science & Engineering, KSIT, Bengaluru, India[4]

Abstract: Safety is a major concern in our lives today. Whether within an organization or in a restricted area; With the growing need for security measures in everyday life, biometrics has become a hot topic of research targeting its potential value in personal identification. This is because biometric systems are classified as more secure than other security systems. This paper focuses on iris and fingerprint as one of the best biometric features for identity management. Iris recognition possesses properties that make it a quintessential biometric system. The point of this venture is to distinguish an individual without a blunder, burning through less time, and keep away from mistakes in confined regions. The recognition of Iris for dealing with Indian weapons is the most powerful innovation related to the security of our country. The method used for fingerprint authentication divides the identification into stages and eliminates many fake fingerprints at different stages. This saves a lot of time by maintaining a high recognition rate. Although Minutiae-based technology is widely used, it is difficult to extract features if the fingerprint image quality is poor. This paper aims to understand how the characteristics of fingerprints can be inferred. Significant advances in this field show that iris and fingerprint biometrics still require fast, real-time, reliable, and powerful algorithms for higher recognition.

Keywords: CNN(Convolutional Neural Networks), deep neural network, drowsiness, python, Iris, Hough Transform, Daugman Method, Fingerprint, Minutiae, Image Processing.

I. INTRODUCTION

Biometric is a reliable, secure authentication tool where controlled access is given by identifying the individual using the physiological or behavioral characters [5]. Physiological properties are contained in the physical parts of the body such as fingerprints, fingerprints, iris, face, DNA, the shape of the hand, retina, etc. The behavioral characteristics of the are based on human actions such as (voice recognition, key scan, signature scan). The commonly used physiological characters are iris, signature, voice, fingerprint, DNA, and Iris is a significant piece of the natural eye. The two eyes have autonomous and uncorrelated iris designs [1,2]. No two irises of a person are alike; Indeed, the indistinguishable twins have distinctive iris designs [7]. Even though the irises of a similar individual appear to be comparative yet they contain exceptional examples [6]. Irisis a slim, roundabout design in the eye that is an ensured interior organ, hence it's anything but influenced by natural variables. Iris acknowledgment is an interaction of perceiving an individual dependent on textures and patterns in an iris [4]. It is a strategy for biometric confirmation in which the highlights of the iris of an individual eye are extricated. The Iris acknowledgment framework gets the picture, extricates the iris region to decide the extraordinary texture for distinctive identification during the check interaction, and matches it with the database made during the enrolment cycle. It is quite possibly the most exceptional and dependable quick access biometric framework. Iris acknowledgment is a promising arrangement because of its dependability, soundness, uniqueness, and wide scope of utilizations [5].

The fingerprint is one of the most common authentication methods for its accuracy, low cost, and varied applications used to identify people. The fingerprint identification system stores a set of fingerprints in its database, then it tries to identify a fingerprint by matching it with the fingerprints already existing in the database. All different applicable methods for

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.12 ⁜ Vol. 10, Issue 2, February 2023

DOI: 10.17148/IARJSET.2023.10216

fingerprint recognition attempt to reach the proper accuracy and speed. The effectiveness of the fingerprint recognition system is well established in terms of uniqueness and permanence.

The main motive of our project is to ensure data security and maintain the quality of data. This paper deals with zero-bit watermarking of the biometric images in order to secure the data for the sake of authentication. It mainly involves generation of an encrypted unique ID by embedding the watermark. The watermark which is the person's details is being stored in the database while the generated encrypted ID/master share is given to the user. Every time, the user has to scan the master share which is given to him. The encrypted unique ID undergoes the process of extraction in order to extract the watermark. If the extracted watermark matches with the watermark stored in the database then we can say that the user is successfully authenticated. The advantage of sharing the encrypted unique ID is that even if the attacker gets the encrypted unique ID, it is useless to him because the data is stored in the form of unique ID

II. PROBLEM STATEMENT

The project's major goal is to develop a zero-bit watermarking method that will solve the issue of biometric data security without compromising biometric data.

• To create a master share that is delivered to the user by extracting distinguishing features from the initial iris image and combining them with the fingerprint, which serves as the watermark within the embedding method.

• The user's master share and iris are both scanned in order to extract the watermark for identification.

• To build an authentication protocol that verifies a user based on a successful match between the extracted watermark and the watermark stored in the database.

• To evaluate the effectiveness of the method described below, multiple attacks are made, and the results of the BER calculation are tabulated.

• PSNR analysis is carried out to demonstrate the distortion effect on the host iris picture.

III. TERMINOLOGIES

BIOMETRICS:

Biometrics refers to a person's behavioural and physical traits. It is employed in digital watermarking to clearly establish a private, enhancing the effectiveness of watermarking in copyright protection and digital content authentication.

BIOMETRIC AUTHENTICATION:

Biometric authentication is that the method of confirmative a user using his biometric information. a robust link is generated between {a data a knowledge an information} record and a personal and it ensures clarity and data security. however these biometric data will be employed by intruders to urge unlawful access. so as to stop this biometric watermarking is critical.

BIOMETRIC WATERMARKING:

Biometric watermarking is necessary to secure biometric data and shield it from various threats. The use of zero bit watermarking is one such method. Generation of a digital pattern from the unique features of the host picture without affecting the quality of the host picture is known as zero bit watermarking. For the process of extracting separate characteristics from the host iris picture various techniques are involved which are explained further.

GRAY SCALE CONVERSION:

The image read from the user is a colour image. In order to process the image further a gray scale image is required. Hence gray scale conversion is performed on the iris image. Gray scale image is obtained as the output of this step

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.12 ⁜ Vol. 10, Issue 2, February 2023

DOI: 10.17148/IARJSET.2023.10216

CANNY EDGE DETECTION:

It is an algorithm that is used to detect edges in images. The process of detection involves various steps.
The procedures involved in canny edge detection are:

1. **Noise cancellation**: Image noise affects the edge detection on a large scale. The Gaussian filter is used to eliminate this noise.

2. **Gradient Calculation**: The gradient of the image detects the direction and picture element intensity.

$$K_x = \begin{pmatrix} -1 & 0 & 1 \\ -2 & 0 & 2 \\ -1 & 0 & 1 \end{pmatrix}, K_y = \begin{pmatrix} 1 & 2 & 1 \\ 0 & 0 & 0 \\ -1 & -2 & -1 \end{pmatrix}.$$

VERTICAL AND HORIZONTAL SOEL FILTER

$$|G| = \sqrt{I_x^2 + I_y^2},$$
$$\theta(x, y) = arctan\left(\frac{I_y}{I_x}\right)$$

GRADIENT CALCULATION FORMULA

3. **Non-Highest filtering**: The result from the prior stage contains edges that are both thick and thin. This action lessens the impact of the thick ones.

4. **Double Thresholding**: Three types of pixels are identified using double thresholding: strong, weak, and irrelevant pixels. The result is a picture with just two pixels of intensity information.

5. **Edge Tracking by Hysteresis**: If the pixels around them are strong pixels, weak pixels will become strong ones.

HOUGH TRANSFORM:

In order to recognise shapes like lines, circles etc, in an picture, a feature extraction algorithm such as Hough transform can be used. By applying this step iris and pupil can be localized.

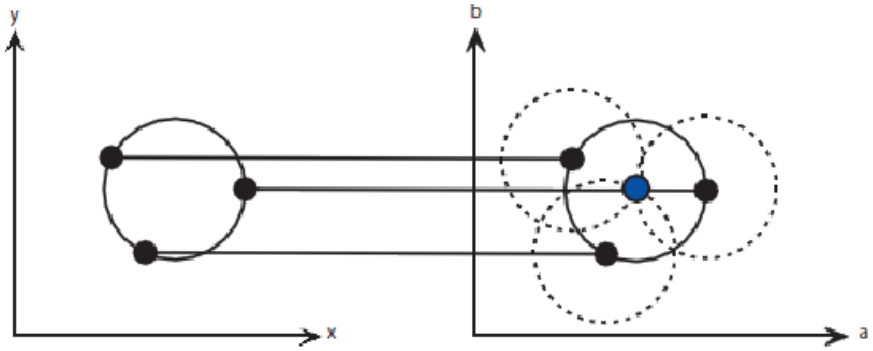
It is a transformation from (x, y) to (a, b) plane. The points present on the circumference of the
circle in the (x, y) plane when mapped to the (a, b) plane gets transformed into centres of distinct circles. After transforming all the points on the circumference to (a, b) plane, the distinct circles in the (a, b) plane meet at a single point. This single point will be the centre of the circle in the (x, y) plane.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.12 ⁜ Vol. 10, Issue 2, February 2023

DOI: 10.17148/IARJSET.2023.10216



IV. METHODOLOGY

The zero-bit steganographic technique creates a binary pattern without sterilising the original image by using the distinguishing characteristics of an associated iris image. The aforementioned method incorporates watermark bits from the user's fingerprint image into their segmented iris image. The technique places a lot of emphasis on creating a master share that is solid and secure. The unique characteristic that is derived from the iris as part of the algorithmic watermarking plan is combined with the binary watermark fingerprint to create the unique ID that is encoded to create a master share.
The two key steps of the watermarking procedure are:

- Embedding Process: This procedure is used to create a special encrypted ID or master share.
- Extraction Process: This procedure entails removing the fingerprint (watermark picture) using a special encrypted ID (master share).

Algorithm for Embedding the Watermark:

This paper focuses on extraction of distinct features from the biometric iris image and imprinting the watermark image in it. To begin with, an iris image is read and grey scale conversion of the same is performed. Segmentation of the iris region and pupil region is to be done. To perform this, Canny Edge Detector is used. It helps to obtain an edge map which is given as input to the Hough Transform. The Hough Transform identifies the iris and pupil coordinates. The next step involves Normalization of the segmented iris image. This is accomplished with the help of Daughman's Rubber Sheet Model. The normalized iris image undergoes decomposition in two levels. To start with, Discrete Wavelet Transform (DWT) is applied on the normalized iris and the LL band is generated. LL band contains the approximate information of the original image. On applying image processing attacks, the change in the pixel value is minimum in the LL band as compared to the other three bands. The next level decomposition is performed using Singular Value Decomposition (SVD). This step mainly ensures the extraction of unique features from the iris as SVD values are always unique. The LL band is divided into non- overlapping blocks of size N*N and SVD is applied on each of the blocks. A resultant matrix is generated such that it contains the first singular values from the diagonal matrices of all the blocks. Furthermore, a binary matrix is created by comparing the successive values of the resultant matrix row-wise. This binary matrix is combined with the encrypted watermark which is the encrypted fingerprint image of the user in order to generate a unique pattern. Encryption is performed on the unique pattern to create a master share. The output of the embedding process is the master share which is given to the user as an ID for further use.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.12 ⁜ Vol. 10, Issue 2, February 2023

DOI: 10.17148/IARJSET.2023.10216

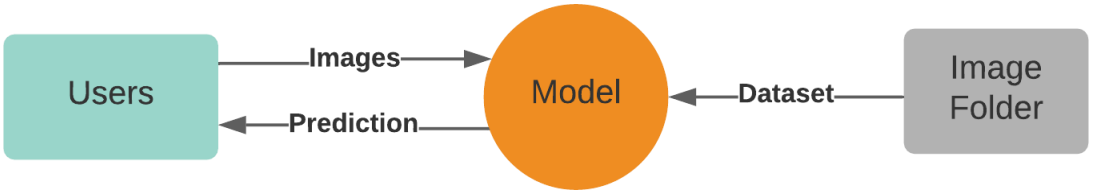
V. DATAFLOW DIAGRAM

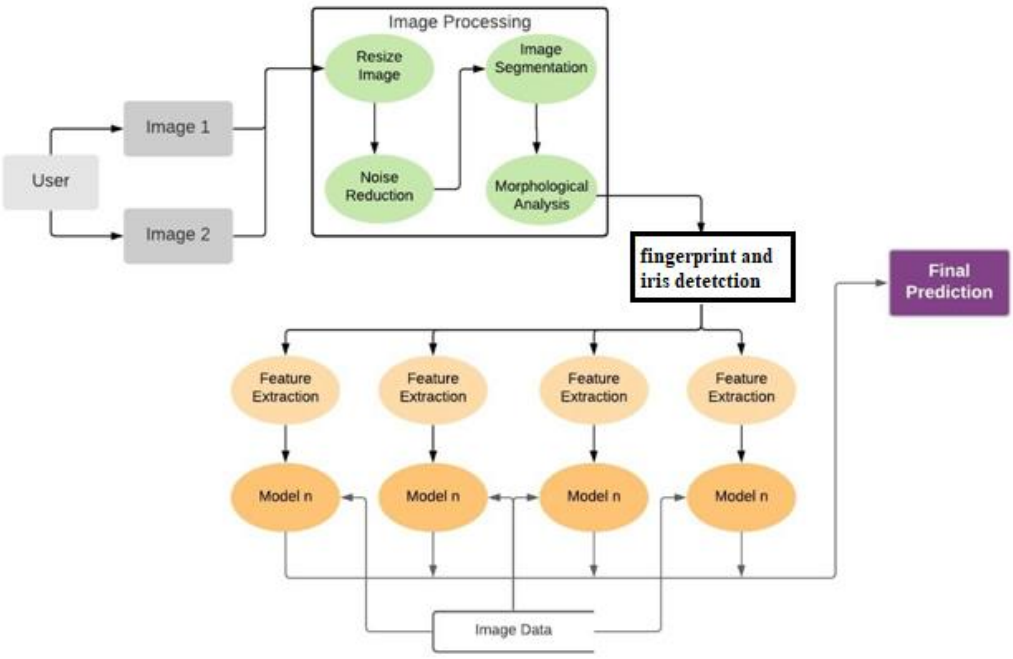
An associate degree data system's knowledge flow is graphically represented by a data flowchart. DFD can be employed quickly during analysis and is very helpful in comprehending a system.

The movement of information through a system is depicted by a data flowchart. It considers a system to be a device that converts inputs into desired outputs. Information can typically withstand a number of changes before it becomes the output in intricate systems, which won't accomplish this transformation in a single step.

Users may visualise how the system will function, what it will be able to accomplish, and how it will be enforced with the use of a knowledge flowchart. To make comparisons and create a more cost-effective system, recent system DFDs may be taken into consideration and compared with a brand-new system DFD.

Data flow diagrams can be used to give the top user a physical map of where the information input will go, ultimately serving as a control over the system's overall structure..





A use-case analysis is used to construct a specific kind of behavioural diagram known as a use case diagram. Its purpose is to present a graphic summary of the functionality a system offers in terms of the actors, their objectives (referred to as use cases), and any interdependencies between those use cases.

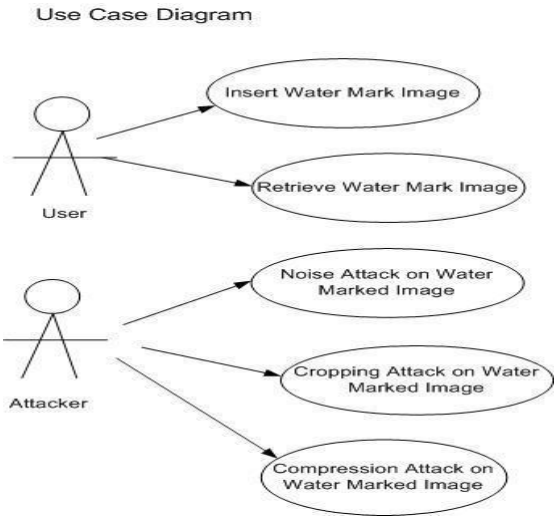
IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

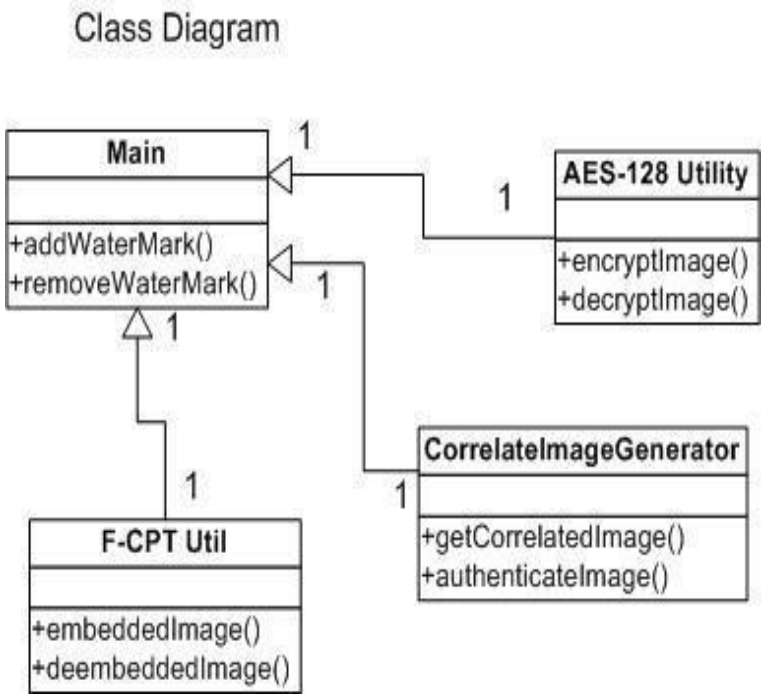
ISO 3297:2007 Certified ⁜ Impact Factor 7.12 ⁜ Vol. 10, Issue 2, February 2023

DOI: 10.17148/IARJSET.2023.10216

A chain diagram in the Unified Modeling Language (UML) is a type of interaction diagram that demonstrates how and in which direction processes interact with one another. It is a chart's hypotheses. The following sequence diagrams



In the Unified Modeling Language (UML) a type of static structure diagram that is known as class diagram that defines the structure of a framework by presenting the elements of system's classes and the connections of classeswith each other. The class diagram is shown below.



VI. CONCLUSION

Zero-bit watermarking is a method doesn't skew the original picture. Even the smallest deviation of a picture will amendment the distinctive identity of the person. Therefore, the planned technique are often most well-liked to watermark biometric data pictures because It hardly distorts at all within the guest image. DWT and SVD square measure wont to extract distinct attributes inside the algorithmic rule that's planned. The research results demonstrate that the watermark

DOI: 10.17148/IARJSET.2023.10216

mixing proceeds quickly since each image's master share is created in an unambiguous manner. The experimental demonstrates that the algorithmic rule planned is strong against many image process threats, as shown by the experimental findings. The intended method keeps the encrypted watermarks during a data transfer. another thanks to store the watermarks are often explored so as to prevent assaults on the watermarks. The host iris's pupil size varies from person to person because, a machine learning algorithmic rule are often wont to train the model to discover pupil and iris of assorted size. Data flow diagrams are often wont to give the top user with a physical plan of wherever the information they input, ultimately as an impression upon the structure of the complete system.

REFERENCES

A. Kumar, A. Dwivedi and M. K. Dutta, "A Zero watermarking Approach for Biometric Image Security," 2020 International Conference on Contemporary Computing and Applications (IC3A), 2020, pp. 53-58,
doi: 10.1109/IC3A48958.2020.233268.

A. Dwivedi, A. Kumar, M. K. Dutta, R. Burget and V. Myska, "An Efficient and Robust Zero-Bit Watermarking Technique for Biometric Image Protection," 2019 42nd International Conference on Telecommunications and Signal Processing (TSP), Budapest, Hungary, 2019, pp. 236-240.
doi:10.1109/TSP.2019.8768881

M. Mishra, A. Bhattacharya, A. Singh and M. K. Dutta, "A Lossless Model for Generation of Unique Digital Code for Identification of Biometric Images," 2018 4th International Conference on Computational Intelligence & Communication Technology (CICT), Ghaziabad,2018, pp.1-5.
doi:10.1109/CIACT.2018.8480297

B. Swathi and T. M. Kumari, "Iris biometric security using watermarking and visual cryptography," 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), Chennai, 2017, pp. 1218-1220.
doi: 10.1109/ICPCSI.2017.8391904

A. Vashistha and A. M. Joshi, "Fingerprint based biometric watermarking architecture using integer DCT," 2016 IEEE Region 10 Conference (TENCON), Singapore, 2016, pp. 2818-2821,
doi: 10.1109/TENCON.2016.7848556.

G. Balamurugan, K. S. Joseph and V. Arulalan, "An Iris Based Reversible Watermarking system for the security of teleradiology," 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave), Coimbatore, 2016, pp. 1-6.
doi: 10.1109/STARTUP.2016.7583937

M. A. M. Abdullah, S. S. Dlay, W. L. Woo and J. A. Chambers, "A Framework for Iris Biometrics Protection: A Marriage Between Watermarking and Visual Cryptography," in IEEE Access, vol. 4, pp. 10180-10193, 2016.
doi: 10.1109/ACCESS.2016.2623905

Lydia Elizabeth B., Duraipandi C., A. Pratap and Rhymend Uthariaraj V., A grid- based iris biometric watermarking using wavelet transform," 2014
International Conference on Recent Trends in Information Technology, Chennai, 2014, pp. 1-6.
doi:10.1109/ICRTIT.2014.6996169

M. K. Dutta, A. Singh, R. Burget, H. Atassi, A. Choudhary and K.
M. Soni, Generation of biometric based unique digital watermark from iris image," 2013 36th International Conference on Telecommunications and Signal Processing (TSP), Rome, 2013, pp. 685-689,
doi: 10.1109/TSP.2013.6614024

V. J. Subashini, S. Poornachandra and M. Ramakrishnan, "A fragile watermarking technique for fingerprint protection, "2013 IEEE Recent Advances in Intelligent Computational Systems (RAICS), Trivandrum, 2013, pp.322-326,
doi: 10.1109/RAICS.2013.6745495

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified ⁜ Impact Factor 7.12 ⁜ Vol. 10, Issue 2, February 2023

DOI: 10.17148/IARJSET.2023.10216

M. R. M. Isa and S. Aljareh, "Biometric image protection based on discrete cosine transform watermarking technique," 2012 International Conference on Engineering and Technology (ICET), Cairo, 2012, pp. 1-5.
doi: 10.1109/ICEngTechnol.2012.6396130

Feng Wen-ge and Liu Lei, "SVD and DWT zero-bit watermarking algorithm," 2010 2nd International Asia Conference on Informatics in Control, Automation and Robotics (CAR 2010), 2010, pp. 361-364,
doi: 10.1109/CAR.2010.5456709.