Zero-bit Watermarking Technique for Generation of Unique Id Using Biometric Images

[1]Varsha D M
Student,
BNMIT, Bangalore
varshadmbhat19@gmail.com

[2]Prof. Divya M S
AssistantProfessor,
BNMIT,Bangalore
divyams@bnmit.in

[3]Varsha R
Student,
BNMIT, Bangalore
Varshamurthy150302@gmail.com

[4]Vibha R Siddheshwar
Student,
BNMIT, Bangalore
Vibha.rs@yahoo.com

Abstract

With the rapid pace of technological growth, it is very important to secure user data. A robust technique which not only secures data but prevents it from various attacks is necessary. Such a technique is proposed within this article. Biometric authentication is one such practice seen today. Contrast to other forms of authentication, biometric recognition provides a strong link between a data record and an individual and it guarantees high level of accuracy and security. But this biometric data can be used by attackers to get illegal access. In order to prevent such acts, a robust technique known as zero-bit watermarking is proposed through this paper.

Keywords: *Biometric Authentication, Zero-bit Watermarking, Singular Value Decomposition, Discrete Wavelet Transform*

1. Introduction

In the digital era, securing user data against unauthorized access is paramount. Traditional authentication methods are often vulnerable to attacks, necessitating more robust security solutions. Biometric authentication offers a strong link between an individual and their data record, enhancing security and accuracy. However, biometric data itself can become a target for attackers seeking illegal access. The challenge lies in protecting biometric data from such threats without compromising the data's integrity. The project aims to address this issue by developing a zero-bit watermarking technique that ensures the security of biometric data used for authentication purposes. To tackle this problem, the project employs a combination of advanced techniques: Zero-bit watermarking, it embeds a unique encrypted ID into biometric images without altering the original image quality.

Biometric Integration which involves integrating unique features from an iris image with a fingerprint to generate a master share for user authentication. Finally, encryption algorithm to secure the watermark within the biometric data, ensuring that even if attackers access the encrypted ID, it remains useless without the corresponding data in the database. These techniques collectively form a robust framework to protect biometric data, ensuring high levels of security and privacy for users.

2. Scope

The zero-bit watermarking technique for biometric images, ensures data security without altering the original image's quality. This technique is crucial in biometrics, where even slight variations can affect identity verification. The proposed method uses Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) to extract unique features from an iris image, creating a master share or unique ID for each user. This ID is encrypted and stored, serving as a robust defense against various image processing attacks. The process involves embedding a watermark into the biometric image and later extracting it for authentication, comparing it with the stored watermark in the database. If the extracted watermark matches the stored one, the user is authenticated. The technique's effectiveness is demonstrated through its resilience to attacks, as shown by experimental results. Future improvements could include alternative watermark storage methods and machine learning algorithms for detecting iris and pupil sizes, enhancing the system's security and efficiency. Zero-bit watermarking thus presents a promising solution for securing biometric data in an increasingly digital world.

3. Objectives

A. Biometric Data Security: The document emphasizes the importance of protecting biometric data, which is highly sensitive and unique to individuals. The proposed technique aims to prevent illegal access and attacks on biometric data1.

B. Zero-bit Watermarking: This innovative method is designed to safeguard biometric images, such as iris or fingerprint data, without altering the original image quality2. It embeds a watermark into the biometric image to create a secure and unique identifier.

C. Unique ID Generation: The process generates a master share or encrypted unique ID by integrating the watermark with the user's biometric data3. This ID is used each time the user needs to authenticate, ensuring a high level of security.

D. Robustness Testing: The technique's robustness is evaluated by performing Bit Error Rate (BER) calculations and Peak Signal-to-Noise Ratio (PSNR) analysis under various simulated attacks, ensuring the system's reliability.

E. Quality Maintenance: While securing biometric data, it's crucial to maintain the integrity and quality of the data. The proposed system ensures that the watermarking process does not degrade the biometric image.

F. System Feasibility: The project's feasibility is analysed in terms of technical requirements, cost-effectiveness, and the potential return on investment. The system is developed using current technology and is economically viable for implementation.

4. Literature Review

Video summarization is a critical task in computer vision and multimedia processing, aimed at condensing lengthy videos into concise representations while preserving essential content and context. Leveraging advancements in deep learning and object detection, recent research has focused on enhancing the efficiency and effectiveness of video summarization techniques. This literature review explores key contributions in this domain, discussing various methodologies, challenges, and opportunities.

Kumar, et al. [1] The proposed algorithm, known as Rubik's cube scrambling with Bit-plane shuffling and Frame rotation (RBF), aims to provide a unique and robust method for encrypting colored images. The algorithm employs a combination of Rubik's cube scrambling, Bit-plane shuffling, and Frame rotation to enhance the security of the encryption process.

Dwivedi, et al. [2] The authors focused on leveraging the success of deep learning in various domains, particularly in image processing, to enhance fingerprint classification methods. Their proposed idea involved the application of deep learning techniques to achieve effective fingerprint classification. However, the authors acknowledged potential drawbacks in their approach, specifically highlighting the need for exploring additional data-augmentation techniques.

M. Mishra et al. [3] The proposed algorithm aims to enhance the security of image encryption by operating at the bit level in three-dimensional space. The key concept revolves around the amalgamation of the Rubik's cube method with bit-level encryption principles, offering a unique and robust approach to the image scrambling process.

A. Swathi and T. M. Kumari [4] A secure biometric authentication approach that leverages Convolutional Neural Networks (CNN) and Q-Gaussian multi-support vector machines (QG-MSVM) with different level fusion of electrocardiogram (ECG) and fingerprint data.

A. Vashistha and A. M. Joshi [5] Introduces an innovative algorithm leveraging a 6D-chaotic system and 2D fractional discrete cosine transform (FrDCT) for the encryption of biometric templates. The proposed method represents a significant advancement in biometric template protection, utilizing the chaotic dynamics of a six-dimensional system along with the spatial-frequency domain transformation capabilities of 2D FrDCT.

G. Balamurugan, et al. [6] The proposed system employs IrisMatch-CNN as both a feature extraction and classification algorithm, emphasizing the integration of machine learning into the embedded environment for enhanced iris verification.

M. A. M. Abdullah et al. [7] Introduces a multimodal iris recognition system that utilizes deep learning techniques with VGG16, DenseNet169, and ResNet50 architectures. The proposed system leverages the combination of convolutional neural networks (CNNs) to enhance the accuracy and reliability of iris recognition by using both the right and left irises.

Lydia Elizabeth et al. [8] provides an in-depth examination of standard watermarking system frameworks and outlines essential requirements employed in the design of watermarking techniques for diverse applications.

The authors conclude their study by reviewing state-of-the-art watermarking techniques and highlighting the efficacy of the Discrete Wavelet Transform (DWT) as a high quality and robust method for image watermarking.

M. K. Dutta, et al. [9] The paper presents a method that focuses on distinguishing specific fingerprint information, including left-right hand classification, sweat-pore classification, scratch classification, and fingers classification, through the application of deep learning techniques.

V. J. Subashini et al. [10] The proposed technique in their work utilizes the Discrete Cosine Transform (DCT) for compact feature extraction in biometric images. The authors conclude by noting a limitation in the applicability of their proposed watermarking scheme

5. Proposed System

We propose a methodology that combines three techniques for biometric data security and authentication: fingerprint and eye classification using CNNs, Rubik's Cube encryption and decryption, and zero-bit watermarking. These techniques aim to protect biometric data from various threats, such as forgery, duplication, tampering, and hacking, by using advanced methods of feature extraction, encryption, and watermarking.

6. Methodology

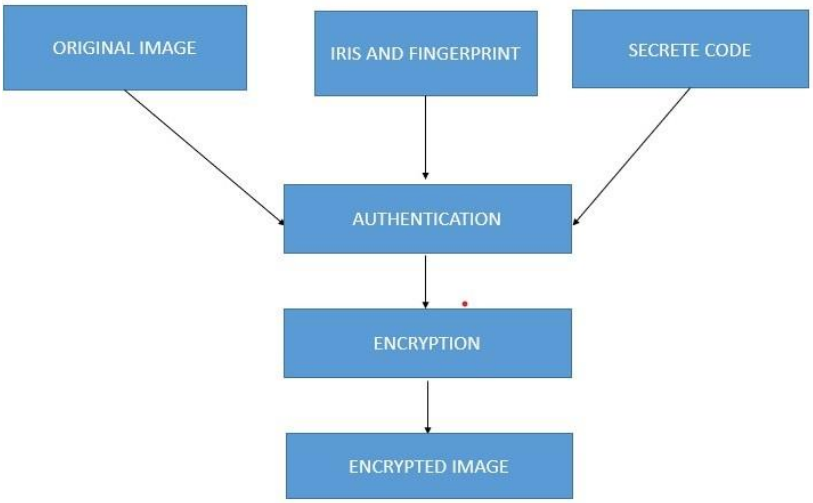

Fig. 1. Work flow of Encryption part of proposed work.

Fingerprint and eye classification using convolutional neural networks (CNN) is a critical biometric authentication task that involves distinguishing between authentic and counterfeit biometric data.

- In this process, CNN models are employed to analyze the unique patterns in real fingerprints and eyes, as well as their corresponding fake counterparts, such as forged fingerprint impressions or fabricated iris images.
- By training on a dataset containing both genuine and fake samples, the CNNs learn to extract discriminative features and make accurate classifications, enhancing security and reliability in biometric authentication systems.

• Rubik's Cube encryption and decryption is a unique and complex cryptographic technique that utilizes the Rubik's Cube puzzle as a key for securing data.
• To encrypt a message, the cube's various layers are manipulated according to a predetermined algorithm, transforming it into a scrambled state.

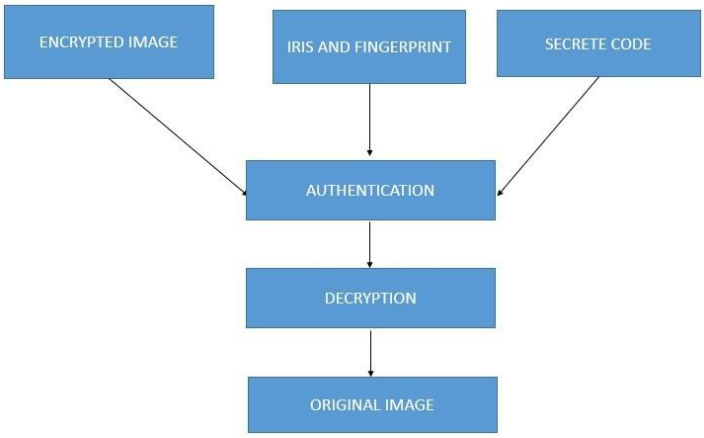

Fig 2. Work flow of Decryption part of proposed work

- The recipient, possessing the same cube and algorithm, can then reverse the process to decipher the original message.
- This method relies on the immense number of possible Rubik's Cube configurations, making it theoretically challenging to break without the precise key, offering a novel approach to encryption and decryption with potential applications in information security. This module focuses on collecting, preprocessing, and managing the dataset used for training and testing the deep learning models. It ensures that the data is diverse, representative, and appropriately processed for model training.

7. Workflow

The workflow of the proposed methodology from the document includes the following key points:

- Data Collection and Preprocessing: The process begins with the collection of biometric images, specifically iris images. These images are then converted to grayscale for further processing.
- Algorithms Used: The methodology employs a series of algorithms at various stages:
  - Canny Edge Detection for edge mapping.
  - Hough Transform for identifying iris and pupil coordinates1.
  - Doughman’s Rubber Sheet Model for normalizing the iris image.

- Discrete Wavelet Transform (DWT) and Singular Value Decomposition (SVD) for feature extraction.
- XOR Encryption for securing the watermark.

- Analysis and Evaluation: The unique features extracted from the iris image are integrated with an encrypted fingerprint to generate a master share. This master share is then used for biometric authentication.
- System Implementation: The system is designed to generate a zero-bit watermarking technique that embeds the watermark into the biometric image without loss of data.
- Testing and Validation: Various test cases are conducted to ensure the system's functionality, such as loading images, data encryption, and decryption.
- Optimization and Fine-Tuning: The system is optimized for accuracy and security, ensuring that the watermarking does not distort the original biometric image and remains robust against image processing attacks

8. Conclusion

The zero-bit watermarking technique does not distort the original image. In biometrics, slightest variation of an image can change the unique identity of the person. Therefore, the proposed method can be preferred for watermarking biometric images as it causes hardly any distortion in the host images. DWT and SVD are used to extract distinct attributes within the algorithm that is proposed. The experimental results indicate that the integration of the watermark is efficiently carried out as the master-share of each image is uniquely generated. The experimental demonstrates that the algorithm proposed is robust against several image processing attacks, as demonstrated by the experimental results. The proposed method stores the encrypted watermarks in a database. An alternative way to store the watermarks can be explored in order to secure the watermarks from attacks. Since the pupil size of the host iris differs from one person to another, a machine learning algorithm can be used to train the model to detect iris and pupil of various size

References

1. *Kumar, A. Dwivedi and M. K. Dutta, "A Zero watermarking Approach for Biometric Image Security,"*
2. *A. Dwivedi, A. Kumar, M. K. Dutta, R. Burget and V. Myska, "An Efficient and Robust Zero-Bit Watermarking Technique for Biometric Image Protection,"*
3. *M. Mishra, A. Bhattacharya, A. Singh and M. K. Dutta, "A Lossless Model for Generation of Unique Digital Code for Identification of Biometric Images,"*
4. *B. Swathi and T. M. Kumari, "Iris biometric security using watermarking and visual cryptography,"*
5. *A. Vashistha and A. M. Joshi, "Fingerprint based biometric watermarking architecture using integer DCT,"*
6. *G. Balamurugan, K. S. Joseph and V. Arulalan, "An Iris Based Reversible Watermarking system for the security of teleradiology,"*

7. *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,"*
8. *GuandeWu,JianzheLin,Claudio T. Silva IntentVizor: Towards Generic Query Guided Interactive Video Summarization.*
9. *Lydia Elizabeth B., Duraipandi C., A. Pratap and Rhymend Uthariaraj V., A grid-based iris biometric watermarking using wavelet transform,"*
10. *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,"*
11. *V. J. Subashini, S. Poornachandra and M. Ramakrishnan, "A fragile watermarking technique for fingerprint protection, "2021 IEEE Recent Advances in Intelligent Computational Systems (RAICS)*