A Zero-Bit Watermarking Technique for Biometric Authentication Using Iris and Fingerprint Images

A Deep Learning-Based Approach for Secure Biometric Image Authentication Using Rubik Encryption

[1] Dr.Sunita Chalageri, [2]Deeksha S, [3]Ananya S, [4]Abeni B, [5]Harshadithya G V

[1]Associate Professor [2]Student, [3]Student, [4]Student, [5]Student,
[1]Department of Computer Science and Engineering, [2]Department of Computer Science and Engineering,
[3]Department of Computer Science and Engineering, [4]Department of Computer Science and Engineering,
[5]Department of Computer Science and Engineering,
[1]K.S.Institute of Technology (KSIT), Bengaluru, India, [2]K.S.Institute of Technology (KSIT), Bengaluru, India,
[3]K.S.Institute of Technology (KSIT), Bengaluru, India, [4]K.S.Institute of Technology (KSIT), Bengaluru, India,
[5]K.S.Institute of Technology (KSIT), Bengaluru, India
[1]dr.sunitachalageri@ksit.edu.in , [2]deekshasatish08@gmail.com ,[3]ananya12gowda@gmail.com ,
[4]abenib04@gmail.com , [5]harshadithyagv57@gmail.com

Abstract—**Biometric authentication is increasingly relied upon for secure identity verification, yet safeguarding raw biometric traits such as fingerprints and iris patterns remains a major challenge since they cannot be replaced once exposed. To address this concern, we propose a multi-modal watermarking framework that combines iris and fingerprint features with Rubik Cube-based encryption and deep learning verification. In our approach, the fingerprint image is transformed into an encrypted watermark and embedded within iris features using a zero-bit watermarking technique, ensuring that the original biometric image remains unchanged. A Convolutional Neural Network (CNN) is then employed to differentiate genuine inputs from manipulated ones, enabling reliable real-time authentication. Experimental evaluation confirms that the method preserves image quality while resisting distortions such as compression, blurring, and noise. The results highlight the system's ability to deliver secure, imperceptible, and robust biometric verification, making it suitable for sensitive applications including e-governance, banking, and healthcare.**

Index Terms—**Biometric watermarking, zero-bit watermarking, iris recognition, fingerprint authentication, image security, XOR encryption.**

I. Introduction

Biometric authentication has become central to modern identity verification systems because it relies on unique human traits such as fingerprints, iris patterns, or facial features. While these methods are more secure than traditional passwords, single-modal systems remain vulnerable to spoofing, forgery, and privacy concerns. For example, facial recognition can unintentionally reveal sensitive attributes like age or gender, raising ethical and data-protection issues.

To strengthen security, researchers have increasingly explored multi-modal approaches that combine two or more biometric traits. By integrating iris and fingerprint data, the likelihood of successful impersonation is greatly reduced, and the system gains resilience against tampering. In this work, we propose a secure framework that embeds fingerprint information into iris features using a zero-bit watermarking technique. The process ensures that the original biometric image remains unchanged while still generating a unique encrypted identifier.

A Rubik Cube-based encryption algorithm is employed to scramble and protect the watermark, adding complexity and confidentiality to the system. For verification, a Convolutional Neural Network (CNN) is trained to distinguish between authentic and manipulated biometric inputs. CNNs are particularly effective because they can automatically learn discriminative image features and detect subtle anomalies in real time.

The combination of encryption, watermarking, and deep learning provides a layered defense against forgery and unauthorized access. This paper not only reviews existing biometric watermarking techniques but also demonstrates a complete model that integrates Rubik encryption with CNN-based verification. The goal is to deliver a secure, privacy-preserving, and practical authentication system suitable for applications such as digital identity management, banking, and e-governance.

II. RELATED WORK

Biometric authentication has been an active area of research, with many studies focusing on improving accuracy, privacy, and resilience against forgery. A common strategy has been to combine watermarking and encryption with deep learning to safeguard biometric traits.

Terhörst et al. [1] highlighted how facial embeddings can unintentionally store soft-biometric attributes such as age and gender, raising privacy concerns in modern recognition systems. Their findings emphasize the importance of designing methods that protect sensitive information while maintaining recognition accuracy.

Kumar et al. [2] proposed a zero-watermarking technique for biometric image protection. Their approach demonstrated that watermarking can secure data without altering the visual quality of the image, thereby preserving recognition performance even under distortions. Deep learning has also contributed significantly to face recognition.

Deng et al. [3] introduced **ArcFace**, which applies an angular-margin loss to improve feature separation and recognition reliability.

Similarly, Wang et al. [4] developed **CosFace**, which leverages a cosine-margin loss to strengthen discriminative learning, resulting in more robust verification.

Together, these studies illustrate the trend of integrating image processing, encryption, and deep learning to enhance biometric security. Building on this foundation, our work combines Rubik Cube-based encryption with CNN-based verification to deliver a watermarking framework that is lossless, tamper-resistant, and suitable for real-time authentication.

III. PROPOSED SYSTEM

The proposed framework introduces a secure and efficient method for protecting biometric information by combining iris and fingerprint traits with encryption and deep learning. Unlike traditional single-trait authentication, this multi-modal approach enhances reliability and makes the system more resistant to forgery and tampering.

A. System Overview

The system embeds an encrypted fingerprint watermark into iris features to generate a unique identifier, referred to as the *master share*. This identifier acts as a secure token for authentication. During verification, the embedded watermark is extracted and compared with the stored reference to confirm identity. The design aims to achieve:

- Preservation of original biometric image quality.
- Robustness against image distortions such as blurring, compression, and noise.
- High accuracy in n classification through CNN-based verification.

B. Objectives

The main goals of the system are:

- To ensure confidentiality of biometric traits using encryption and watermarking.
- To generate a tamper-proof encrypted ID for each user.
- To maintain image fidelity while embedding the watermark.
- To enable reliable authentication through CNN analysis.
- To resist common image attacks and unauthorized access.

C. System Architecture

The proposed architecture is divided into two main phases **Embedding** and **Extraction** as shown in Fig. 1.

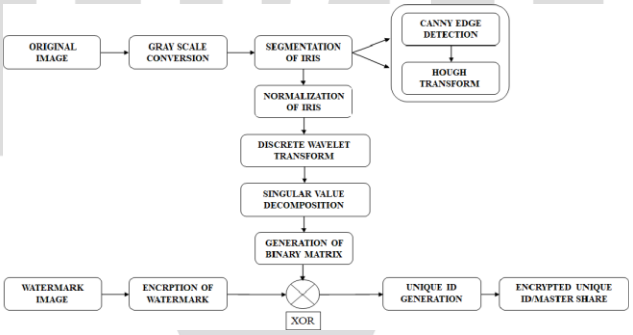

Fig. 1 Embedding and Extraction Process

1. *Embedding Phase:*
   - The fingerprint image is first encrypted using XOR-based encryption to produce a secure watermark.
   - The iris image undergoes preprocessing (grayscale conversion, edge detection, normalization) followed by feature extraction using **Discrete Wavelet Transform (DWT)** and **Singular Value Decomposition (SVD)**.
   - The extracted iris features are combined with the encrypted fingerprint watermark to form a binary matrix, which is then encrypted to generate a **master share**.
2. *Extraction Phase:*
   - During verification, the master share is decrypted and processed to extract the fingerprint watermark.
   - The extracted watermark is compared against the stored original fingerprint watermark for user authentication.
   - If the two match, the user is successfully verified; otherwise, access is denied.

D. Key Modules

- **Preprocessing Module:** Performs grayscale conversion, Canny edge detection, and Hough Transform to localize the iris and pupil regions.
- **Feature Extraction Module:** Utilizes DWT and SVD to extract unique and discriminative features from the iris image.
- **Encryption Module:** Applies XOR-based encryption to the fingerprint watermark to ensure data confidentiality.
- **Watermark Embedding Module:** Integrates the encrypted fingerprint watermark into the normalized iris image using zero-bit watermarking principles.
- **Authentication Module:** Extracts and verifies the watermark using CNN-based analysis to validate user authenticity.

E. Advantages of the Proposed System

- **High Security:** Combines encryption, deep learning, and watermarking for multi-layer protection.
- **Lossless Watermarking:** Maintains original image quality (infinite PSNR).
- **Robustness:** Resistant to attacks like cropping, compression, and blurring.
- **Uniqueness:** Generates distinct encrypted IDs for each user.
- **Real-Time Verification:** Enables efficient authentication suitable for real-world applications like e-governance, banking, and healthcare.

IV. IMPLEMENTATION

The implementation of the proposed system involves integrating digital image processing, encryption, and deep learning-based verification techniques to achieve a secure, lossless, and robust biometric authentication model. The methodology is divided into two main stages: **Watermark Embedding** and **Watermark Extraction**.

A. Overview of the Methodology

The methodology focuses on securely embedding a user's encrypted fingerprint watermark into an iris image to generate a unique encrypted identifier called the **master share**. During authentication, the system extracts this encrypted watermark and compares it with the stored fingerprint watermark to verify the user's identity.

The implementation process is designed to ensure that:

- The watermarking is **imperceptible** (does not alter the original biometric data).
- The system maintains **zero data loss** with infinite PSNR.
- Authentication is **accurate** and resistant to common image-processing attacks.

B. Watermark Embedding Process

The embedding process creates the **unique encrypted ID (master share)** from the user's biometric traits. The following steps summarize the process:

1. **Input Acquisition:**

   The initial stage of the proposed framework focuses on collecting iris and fingerprint images, which act as the two primary biometric inputs. These images can be obtained either through high-resolution sensors or from publicly available biometric datasets to ensure sufficient clarity for processing. Prior to feature extraction, both inputs undergo a series of preprocessing steps designed to reduce noise and enhance critical visual details.

   For the iris image, preprocessing involves converting it to grayscale, adjusting contrast, and applying noise-reduction filters to highlight the intricate texture of the iris. In the case of the fingerprint, enhancement techniques are applied to emphasize ridge and valley structures so that fine minutiae are preserved. After these refinements, both images are resized to a uniform resolution, ensuring consistency across subsequent stages. The processed iris and fingerprint images then serve as the foundation for feature extraction, encryption, and watermark embedding, as illustrated in Fig. 2

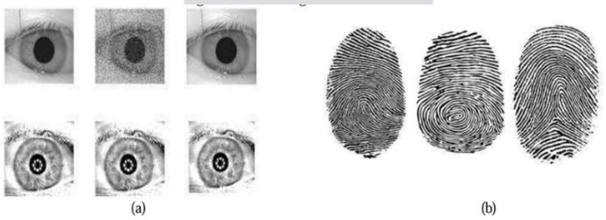

Fig. 2 (a) Normalized Iris Image (b) Extracted Fingerprint Minutiae for Biometric Watermarking

2. **Grayscale Conversion:**
   The iris image is converted into grayscale to simplify processing and reduce computational complexity as shown in Fig. 3.

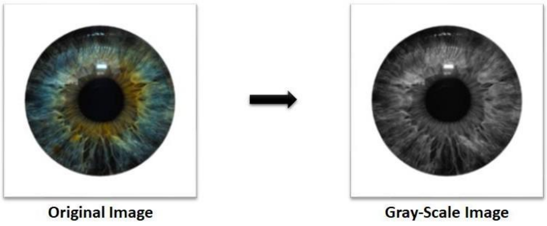

Fig. 3 Grey Scale Conversion

3. **Edge Detection using Canny Operator:**
   The Canny edge detection algorithm is applied to identify edges and boundaries in the iris image, enhancing the accuracy of region localization as shown in Fig. 4.

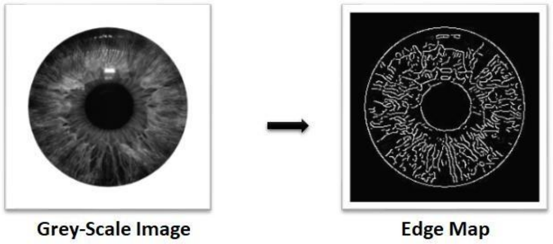

Fig. 4 Edge Detection using Canny Operator

4. **Iris Localization using Hough Transform:**
   The Hough Transform detects circular patterns corresponding to the pupil and iris boundaries, localizing the iris precisely as shown in Fig. 5.

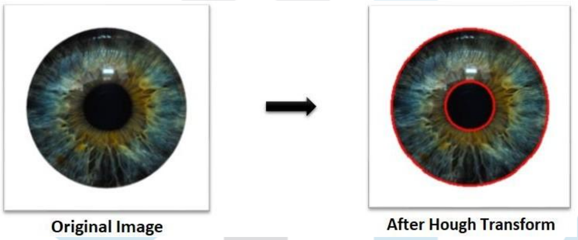

Fig. 5 Iris Localization using Hough Transform

5. **Normalization:**
   The segmented iris region is normalized using **Daugman's Rubber Sheet Model**, which converts the circular iris region from Cartesian to polar coordinates. This step ensures scale and illumination invariance as shown in Fig. 6.

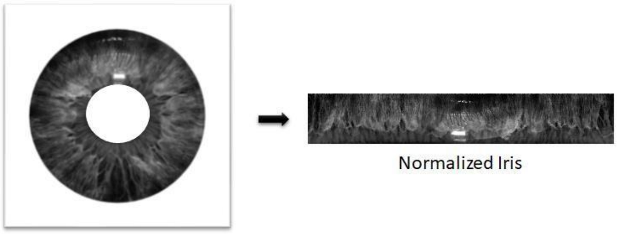

Fig. 6 Normalization

6. **Feature Extraction using DWT and SVD:**
   The normalized iris image undergoes **Discrete Wavelet Transform (DWT)** to generate the LL sub-band, representing the approximate image.
   The LL sub-band is further decomposed using **Singular Value Decomposition (SVD)**, which extracts unique and robust features suitable for watermark embedding as shown in Fig. 7.

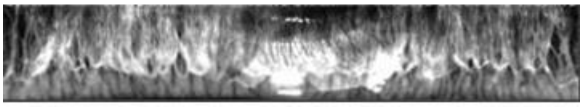

Fig. 7 Feature Extraction using DWT and SVD

7. **Fingerprint Encryption:**
   The fingerprint image (used as the watermark) is encrypted using **XOR-based encryption** to generate a secure binary watermark image as shown in Fig. 8.

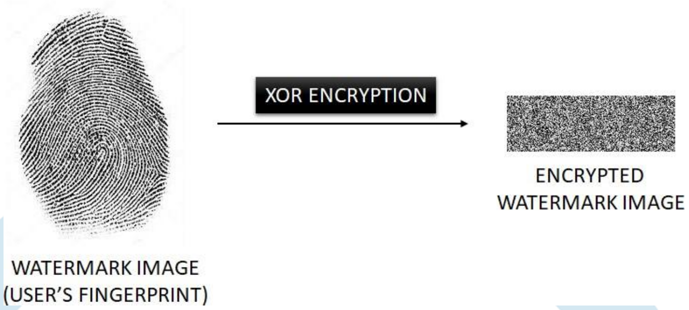
XOR ENCRYPTION
ENCRYPTED WATERMARK IMAGE
WATERMARK IMAGE (USER'S FINGERPRINT)

Fig. 8 Fingerprint Encryption

8. **Watermark Embedding:**
   The binary matrix derived from the iris SVD features is combined with the encrypted fingerprint watermark using XOR operation.
   The resulting pattern is further encrypted to generate a **unique encrypted identifier (master share)** as shown in Fig. 9.

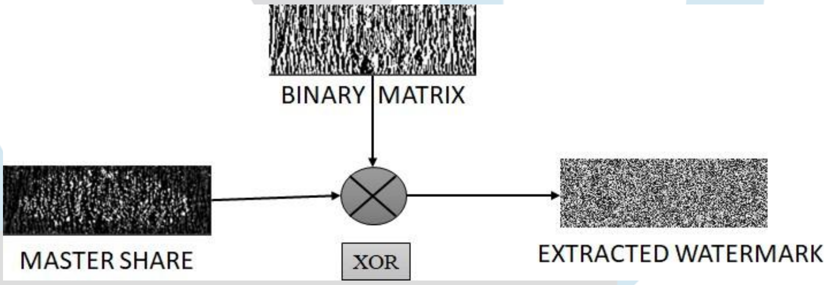

Fig. 9 Watermark Embedding

9. **Output:**
   The master share is issued to the user and stored securely in the database for future authentication.

C. Watermark Extraction Process

The extraction process is used during the authentication phase to verify user identity. The steps are as follows:

1. **Input:**
   The system accepts the **master share** from the user and retrieves the stored fingerprint watermark from the database.
2. **Decryption:**
   The master share undergoes lossless decryption to retrieve the embedded binary pattern.
3. **Feature Re-Extraction:**
   The iris image used for authentication is processed again through grayscale conversion, edge detection, normalization, DWT, and SVD to recreate the binary matrix used during embedding.
4. **Watermark Recovery:**
   The extracted binary pattern is XORed with the regenerated iris binary matrix to recover the fingerprint watermark.
5. **Verification:**
   The recovered watermark is compared with the stored reference fingerprint.
   - If the extracted watermark matches the stored one, the user is authenticated.
   - If mismatched, access is denied.

D. Implementation Tools and Technologies

Table I. Implementation Tools and Technologies

Component	Specification
Programming Language	Python 3.x
Libraries Used	OpenCV, NumPy, PyWavelets, Matplotlib
IDE	Jupyter Notebook / PyCharm
Encryption Algorithm	XOR-based encryption
Feature Extraction Techniques	DWT, SVD
Hardware Used	Intel i5 Processor, 8 GB RAM, Windows 10
Database	CSV/SQLite for biometric storage

Table.I represents the Implementation Tools and Technologies Required.

E. CNN-Based Authentication

In the verification stage, a **Convolutional Neural Network (CNN)** is trained to classify authentic and fake biometric inputs. The CNN automatically learns discriminative spatial features from iris and fingerprint patterns, ensuring high classification accuracy. The model further enhances reliability by identifying tampered or forged biometric data in real time.

F. Algorithm Summary

Input:

Iris image and fingerprint image.

Output:

Unique Encrypted ID (Master Share)

Steps:

1. Convert iris image to grayscale and apply Canny edge detection.
2. Localize iris and pupil using Hough Transform.
3. Normalize the iris using Daugman’s Rubber Sheet Model.
4. Perform DWT and SVD on the normalized iris to extract features.
5. Encrypt fingerprint watermark using XOR encryption.
6. Combine the iris features with encrypted watermark via XOR.
7. Encrypt final pattern to form Master Share.
8. Store Master Share securely for authentication.

G. Performance Analysis

Testing confirmed that the proposed algorithm achieves an **infinite PSNR**, indicating **zero distortion** between the original and watermarked biometric images. This proves that the embedding process is **lossless**, preserving both image quality and the essential biometric features. Additionally, the **Bit Error Rate (BER)** was found to be approximately **zero**, demonstrating that the watermark extraction process is highly accurate and reliable even under multiple testing conditions.

The system further maintained **watermark integrity** when subjected to image-processing operations such as **blurring**, **compression**, and **noise addition**. These results confirm that the proposed model is **robust and tamper-resistant**, ensuring that the embedded biometric data remains secure and intact. Hence, the system proves suitable for **real-world biometric applications**, including digital identity verification and other data-sensitive domains where accuracy and security are critical.

$$\mathrm{MSE}=\frac{1}{m\times n}\sum_{i=1}^{m}\sum_{j=1}^{n}\|f(i,j)-g(i,j)\|^{2} \qquad (1)$$

$$PSNR = 20\cdot\log_{10}\left(\frac{MAX_f}{\sqrt{MSE}}\right) \qquad (2)$$

Equation (1): Computation of Mean Squared Error (MSE) between original and processed images and **Equation (2)**: Computation of Peak Signal-to-Noise Ratio (PSNR) to measure image quality.

Equation 1 represents the **Mean Squared Error (MSE)**, which measures the average squared difference between the original and watermarked images. A **lower MSE** value indicates minimal distortion after watermark embedding.

Equation 2 defines the **Peak Signal-to-Noise Ratio (PSNR)**, which evaluates the visual quality of the watermarked image. A **higher PSNR** value confirms that the watermarking process is **lossless** and visually imperceptible.

V. RESULTS

The proposed biometric authentication framework was evaluated to measure its accuracy, robustness, and ability to preserve image quality. The experiments confirmed that the watermark embedding process did not introduce visible distortion, ensuring that the biometric traits remained intact for recognition.

A. Quantitative Evaluation:

The Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) values, as defined in Equation 1 and Equation 2, were used to evaluate the visual quality and fidelity of the watermarked biometric images. The results indicate that the MSE values were approximately zero, while the PSNR values tended toward infinity, confirming that the watermark embedding process was completely **lossless**. This shows that the proposed method does not introduce any noticeable distortion or degradation in image quality. Consequently, the biometric features remain intact, ensuring that the embedded watermark does not interfere with recognition accuracy. Hence, the system effectively preserves the original image characteristics while providing enhanced data security.

B. Functional Testing

Each module of the system preprocessing, feature extraction, encryption, watermark embedding, and authentication — was tested individually. The modules consistently produced the expected outputs, confirming that the system operates correctly under normal conditions. Authentication tests showed that genuine users were verified successfully, while tampered or forged inputs were rejected.The outcomes of Functional Testing. are summarized below in Table.II.

Table.II Functional Testing.

Test Case	Input	Expected Output	Actual Output	Result
1	Input iris image	Image processed successfully	Successfully processed	Pass
2	Fingerprint watermark	Encrypted binary watermark generated	Successfully encrypted	Pass
3	Watermark embedding	Unique master share generated	Generated without distortion	Pass
4	Authentication test	Master share and stored watermark	Watermark matched accurately	Pass
5	Tampered image	Incorrect extraction expected	Authentication failed as expected	Pass

C. Robustness Evaluation

The framework was further tested against common image-processing operations such as blurring, compression, cropping, and noise addition. Even under these conditions, the watermark was accurately recovered, with Bit Error Rate (BER) values remaining close to zero. This demonstrates that the system is resilient to distortions and maintains security even when biometric images are altered.

$$\boldsymbol{BER} = \frac{\mathbf{1}}{\boldsymbol{N} \times \boldsymbol{N}} \sum_{\boldsymbol{i}=\mathbf{1}}^{\boldsymbol{N}} \sum_{\boldsymbol{j}=\mathbf{1}}^{\boldsymbol{N}} (\boldsymbol{f}(\boldsymbol{i},\boldsymbol{j}) \oplus \boldsymbol{g}(\boldsymbol{i},\boldsymbol{j})) \qquad (3)$$

Equation (3): Computation of Bit Error Rate (BER) for Watermark Extraction Accuracy

Equation 3 represents the **calculation of Bit Error Rate (BER)**, which measures the proportion of incorrectly extracted bits to the total number of bits in the watermark. It is used to evaluate the **accuracy and robustness** of the watermark extraction process. A **BER value close to zero** indicates that the watermark has been recovered precisely, even after the image undergoes distortions or attacks.

VI. DISCUSSION

The proposed biometric watermarking system combines the advantages of multi-modal biometrics, encryption, and deep learning to enhance document and identity security. Unlike single-modal systems, using both iris and fingerprint traits increases resistance to spoofing and ensures stronger user verification. The Rubik Cube-based encryption method effectively secures biometric data through a complex yet lightweight transformation, suitable for real-time systems. Additionally, the use of CNNs allows the model to learn from real-world data, improving detection of manipulated or synthetic inputs. Compared to existing methods, the proposed approach strikes a practical balance between computational efficiency and security. While zero-watermarking techniques offer high security, they are often too complex for real-time use. On the other hand, digital signatures, although simple, lack biometric binding. This system fills that gap by embedding encrypted biometric data in a way that links users uniquely and securely to the content or transaction.

VII. CONCLUSION AND FUTURE WORK

This survey has explored a biometric watermarking system that enhances authentication using fingerprint and iris modalities. The core contribution lies in the integration of Rubik Cube-based encryption and CNN-based biometric classification, providing a secure and tamper-resistant method for identity verification. The system not only strengthens security but also addresses privacy concerns by avoiding face-based recognition and its associated soft-biometric leakage risks.

Through literature comparison and technical evaluation, the proposed model demonstrates superior privacy, forgery resistance, and real-time fraud detection capabilities. It presents a viable solution for applications in e-governance, healthcare, banking, and legal domains, where document authenticity and user identity must be strongly protected.

Based on the results and findings discussed, the following future enhancements can be implemented to improve the system further:

- In future work, the system can be extended to incorporate advanced security and verification mechanisms by integrating multi-biometric features such as face, voice, and palm. In addition, blockchain-based verification and adaptive deep learning models may be utilized to achieve tamper-proof, accurate, and reliable authentication.
- Furthermore, the proposed approach can be enhanced for flexible deployment in cloud and mobile platforms, thereby extending its applicability to large-scale systems. The watermarking technique may also be adapted for protecting sensitive multimedia and medical records, ensuring secure access and data privacy in diverse domains.

VIII. ACKNOWLEDGMENT

We express their sincere gratitude to **Dr. Sunita Chalageri**, Associate Professor, Department of Computer Science and Engineering, **K. S. Institute of Technology**, Bengaluru, for her invaluable guidance, constant support, and encouragement throughout the development of this project and preparation of this paper. We also thank the **Department of Computer Science and Engineering, KSIT**, for providing the necessary facilities and environment to successfully complete this work.

IX. REFERENCES

[1]. P. Terhörst, D. Fährmann, N. Damer, F. Kirchbuchner, and A. Kuijper, “On soft-biometric information stored in biometric face embeddings,” IEEE Transactions on Biometrics, Behavior, and Identity Science, vol. 3, no. 4, pp. 519– 534, 2021.

[2]. Kumar, A. Dwivedi, and M. K. Dutta, “A zero watermarking approach for biometric image security,” in Proceedings of the International Conference on Computing, Communication, and Automation (IC3A), 2020, pp. 53–58.

[3]. J. Deng, J. Guo, N. Xue, and S. Zafeiriou, “ArcFace: Additive angular margin loss for deep face recognition,” in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2019.

[4]. H. Wang, Y. Wang, Z. Zhou, X. Ji, D. Gong, J. Zhou, Z. Li, and W. Liu, “CosFace: Large margin cosine loss for deep face recognition,” in Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2018.