IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, January 2026
Impact Factor: 7.67

Biometric Based Confidential Data Sharing Using Blockchain

Anita S Patil, Sheetal Janthakal, H Srinivas Reddy
Shiva Prasad K, Vinay K S, Dadavali H
CSE-Artificial Intelligence
Ballari Institute of Technology & Management, Bellary, Karnataka, India
anita.bijapur@gmail.com, sjanthakal@gmail.com, seenur027@gmail.com
shivamani00909@gmail.com, vinay974091@gmail.com, ddadavalidadavalih@gmail.com

Abstract: *Protecting sensitive data and ensuring user identity have become top priorities in industries like healthcare, finance, and e-governance in an increasingly linked digital world. Be- cause of their vulnerability to identity theft, phishing, and data breaches, traditional password-based security systems are no longer adequate. A more dependable and user-specific approach to data security is provided by biometric authentication, especially fingerprint recognition. Nevertheless, conventional biomet- ric systems frequently keep information in centralized databases, resulting in single points of failure that, in the case of a breach, could cause irreversible privacy violations.*

This paper presents a safe and effective framework that combines multi-layered encryption, blockchain technology, and fingerprint-based biometric verification to address these prob- lems. To enable distributed embedding of a private message, the suggested system takes a fingerprint image, extracts more than 800 minutiae points, and splits the image into four quadrants. To ensure strong data confidentiality, this message—such as a file key or identity token—is encrypted using triple-layer AES-256 encryption with CBC mode and unique initialization vectors.

The system stores fingerprint cryptographic hashes using Ethereum blockchain technology rather than centralized data repositories, allowing for tamper-proof verification through smart contracts. Blockchain technology lowers the risk of unwanted data access, improves transparency, and offers traceability. In order to guarantee the integrity of embedded data throughout the encryption and decryption processes, a CRC32 checksum mechanism is also used.

This work offers a solid, scalable solution for safe identity verification and encrypted data sharing by fusing biometric uniqueness with cryptographic and decentralized storage tech- niques. The method has potential uses in digital identity systems, financial transactions, healthcare data protection, and secure communications. For wider adoption, future research might look into real-time biometric capture, iris recognition integration, and improved scalability.

Keywords: AES-256 encryption, fingerprint recognition, blockchain technology, decentralized identity, smart contracts, Ethereum, minutiae points, cryptographic hash, CBC mode, CRC32 checksum, data integrity, Web3.py, secure communication, biometric authentication, fingerprint recognition

I. INTRODUCTION

Safeguarding personal information and guaranteeing secure user authentication have become top priorities in many indus- tries, including banking, healthcare, and government systems, as a result of the quick development of digital technologies and online services. Despite being widely used for decades, pass- words and traditional login methods are becoming more and more susceptible to data breaches, social engineering attacks, and hacking. Because many users choose weak credentials or reuse passwords across platforms, cybercriminals can easily target these systems.

Because of their distinct and immutable qualities, biometric authentication techniques have grown in popularity as a means of overcoming these shortcomings. Among these, fingerprint recognition is one of the most useful and

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, January 2026 Impact Factor: 7.67

extensively used biometric methods. It provides cost-effective implementation, high accuracy, and ease of use. Fingerprints are always avail- able to the user and are harder to duplicate or share than pass- words. But even biometric systems have drawbacks, especially when it comes to storing fingerprint data on centralized servers that are still vulnerable to hacking or manipulation.

In this paper, a hybrid security framework that combines fin- gerprint authentication with robust encryption and blockchain- based decentralized storage is presented. Using sophisticated cryptographic techniques, the system encrypts sensitive data, distributes it throughout the fingerprint's spatial zones, and extracts minute details from the fingerprint. To secure the embedded message, such as user credentials or access tokens, a triple-layer AES encryption technique is used. Additionally, the system uses Ethereum smart contracts to store fingerprint- related hashes on a blockchain, reducing the possibility of data alteration or tampering. This guarantees that every interaction is captured on tape and cannot be altered covertly.

A CRC32 checksum is utilized to verify the fingerprint and guarantee data consistency throughout retrieval. This method supports quick and precise verification during user access in addition to improving the system's dependability. This system offers a high level of security appropriate for sensitive applications that require both privacy and trust by combining the advantages of blockchain, encryption, and biometrics. De- centralized storage and real-time biometric verification enable smarter and safer digital interactions, which makes this solu- tion perfect for data protection and next-generation identity management.

II. METHODOLOGY

Our proposed system combines blockchain-based verifica- tion, AES-based encryption, and biometric fingerprint recog- nition to provide a safe way to handle sensitive data and authenticate identities. To guarantee that every element con- tributes to a dependable and impenetrable security framework, the design is organized in a modular fashion. Fingerprint pro- cessing, encryption-based secret embedding, and blockchain integration for decentralized data validation are the key steps in this methodology.

A. Fingerprint Processing

Here, the security framework is set up to start with obtaining a fingerprint image, either directly from a biometric scanner or from a dataset. In order to simplify subsequent analysis and eliminate superfluous visual details, the image is converted to grayscale after it has been captured. While noise filtering techniques eliminate fine distortions and background inter- ference, contrast adjustment techniques are used to highlight ridge structures. After that, the picture is binarized, or turned into black and white, so that the black ridges and white valleys can be easily identified.[1].

(a) Cleaned image (b) Grayscale image

Fig. 1. Preprocessing stages of fingerprint image

The binarized fingerprint is run through a thinning algorithm to improve feature detection. This step makes it easier to extract unique fingerprint features known as minutiae by narrowing the width of ridge lines to a single pixel. The key characteristics used for identity verification are minutiae, which are particular locations where ridges terminate or divide into branches. Only excellent fingerprint samples obtained under ideal lighting and pressure conditions are taken into consideration in order to guarantee accuracy.[3]

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, January 2026
Impact Factor: 7.67

B. Secret Sharing Mechanism

The fundamental concept of the system's security is the use of a unique secret-sharing mechanism to embed data into the fingerprint features. There are three significant sub-stages in this process:

Minutiae Detection

A thorough scan is performed to find legitimate minutiae points after the fingerprint has been thinned. Based on the pattern of nearby pixels, ridge endings and bifurcations are identified using a standard 3x3 pixel window. The orientation and spatial coordinates of every detected minutia are noted. Threshold rules are used to filter out spurious points that arise from noise or irregular pressure during capture in order to increase reliability. A biometric hash is created using the remaining points, which are stored as a feature vector. This hash is generated again during subsequent authentication attempts and serves as a constant reference for encryption.

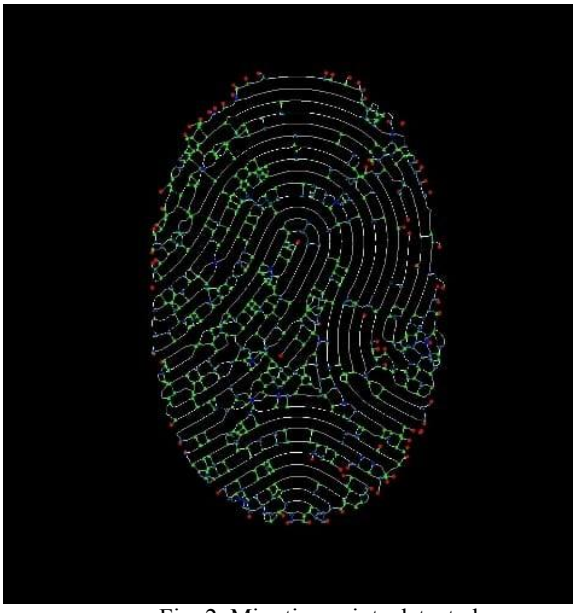

Fig. 2. Minutiae points detected

Quadrant Division

The fingerprint image is separated into four equal quadrants to increase system resilience and add another level of complexity. A subset of minutiae points that are handled independently during the data embedding stage are present in each quadrant. This tactic adds redundancy and resilience by ensuring that the system can still retrieve partial fingerprint information even if only a portion of it is recorded during subsequent use. Additionally, it permits regulated dissemination of encrypted data, enhancing security via fragmentation.

Message Embedding

First, sensitive data is encoded into a binary format, such as private keys, secure tokens, or personal identifiers. Strong data confidentiality is then ensured by encrypting this binary stream in CBC mode using AES-256. Three layers of AES encryption are used to increase security, with a different key and initialization vector (IV) used for each layer. Within each fingerprint quadrant, the resultant ciphertext is divided and embedded throughout the minutiae points.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, January 2026
Impact Factor: 7.67

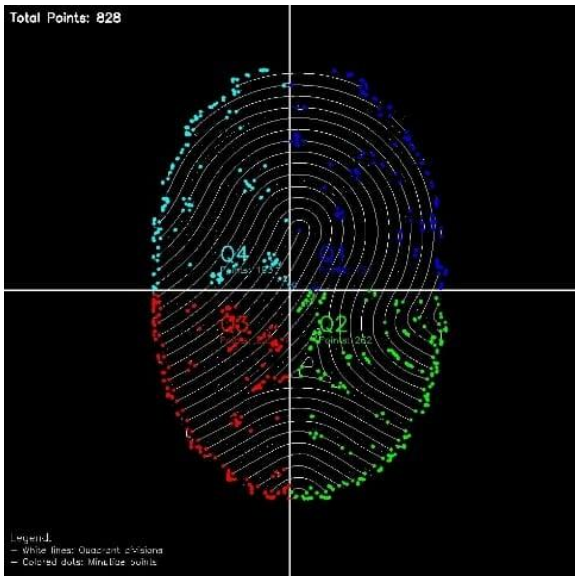

Fig. 3. Quadrant division


Fig. 4. Once after embedding the message

Once after embedding the message

The minutiae coordinates serve as anchor points for the encrypted bits during the embedding process. This indicates that the security of the embedded data is enhanced by the fingerprint's actual location and structure. Without the right fingerprint and processing logic, the message cannot be re- covered by an unauthorized individual. This approach heavily relies on the user's distinct fingerprint since the same biometric hash that was used for encryption must also be used for decryption.

C. Data Verification

The user's fingerprint is scanned once more and processed in the same manner whenever they try to access the protected data. The system reconstructs the biometric hash and re- extracts minute details. It decrypts the embedded

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, January 2026 Impact Factor: 7.67

message using this hash and verifies its authenticity with a CRC32 checksum. This checksum serves as a rapid means of con- firming that the decrypted data has not been tampered with or corrupted. Access is allowed if the fingerprint is legitimate and the decrypted data is identical to the original. Otherwise, attempts at unauthorized access are blocked by the system.

D. Blockchain Integration

The system incorporates blockchain technology to offer tamper-proof, permanent logging of biometric hashes and access metadata. Ganache is used to create and implement a Solidity smart contract on a private Ethereum network. Timestamps, transaction information, and encrypted finger- print hashes are all stored in this contract. Web3.py, a Python library for Ethereum interactions, is used to compare the stored value on the blockchain with the hash currently generated from the user's fingerprint during each authentication.[2] Because blockchain technology is decentralized, even system administrators cannot alter or remove data that has been stored. This feature greatly improves the system's credibility and supports applications that require accountability and audit trails, like secure file storage settings or healthcare systems.

III. REQUIREMENT ANALYSIS

The system is designed using a mix of hardware and software tools, and does used the blockchain technology. The system is built to easily support real-time applications and here we have used the datasets. The method enables a seamless transition between integrating live biometric capture using external sensors and testing with pre-recorded fingerprint datasets.

For the implementation, we have used the standard fingerprint datasets and validated the results. Using these standard datasets, we could easily test the image enhancement, minutiae detection, and encryption reliability under multiple circumstances as they offer a consistent testing environment with a variety of fingerprint samples.

Regarding hardware side, the system is compatible with well-known fingerprint sensors that are best for their accuracy and dependability, such as the R305 or GT-521F32. Microcontrollers like the Arduino Uno, Raspberry Pi, or Nedelcu can readily interface with these sensors. These modules make it possible to scan fingerprints in real time and send data to the processing unit, where it is instantly examined, encrypted, and safely stored.

From the blockchain perspective, Ganache, a program which replicates the Ethereum smart contracts on a developer's computer, is used to implement the system on a local Ethereum blockchain environment. Here Ganache makes it possible to store and retrieve the data on the blockchain and also test transactions safely. A Python-based API, Web3.py, that is used to communicate with these smart contracts. It offers the necessary features for handling transactions, deploying contracts, and application-layer communication with the blockchain.

Solidity, Ethereum's main contract development language, is used to write smart contracts. Only authorized users can conduct transactions on the blockchain thanks to MetaMask, which is used for safe wallet-based interactions and account management. These contracts are in charge of immutably storing fingerprint hash values and related metadata.

Solidity helps to create smart contracts, Ethereum's primary contract development language. Contracts do store the fingerprint hash values and associated metadata in immutable manner. These wallet-based interactions and account management use MetaMask and makes it possible for only authorized users to conduct transactions on the blockchain.

IV. IMPLEMENTATION

Each module is meticulously developed and integrated during the implementation phase, which turns the theoretical design into a functional prototype. To manage the fingerprint, encrypt sensitive data, embed the data, and store verification details on the blockchain, the system is divided into separate phases.

A. Capturing and Preprocessing Fingerprint Images

Either real-time scanning via biometric sensors or the use of publicly accessible fingerprint datasets initiates the fingerprint capture procedure. A number of preprocessing techniques are applied to the resulting image in order to enhance its consistency and clarity. In order to simplify the ridge structure and lower processing overhead, the image is

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, January 2026 Impact Factor: 7.67

first converted to grayscale. After that, normalization techniques are used to create uniformity across samples by adjusting contrast and brightness.

After that, extraneous background textures are eliminated using noise filtering methods like median filtering and Gaussian blurring. Binarization, which transforms the grayscale image into a pure black-and-white format, is done after the image has been cleaned. In order to identify ridge and valley structures, this step is crucial. In order to ensure accuracy in the subsequent feature extraction stage, the image is lastly run through a thinning algorithm that reduces the ridge thickness to a single pixel width.

During this stage, well-known Python libraries for image enhancement and manipulation are used, including scikit-image, OpenCV, and NumPy.

B. Feature Extraction and Quadrant Classification

Following preprocessing, the system uses a sliding window technique to identify fingerprint minutiae, or distinctive features like ridge endings and bifurcations. By examining pixel patterns in a 3x3 neighborhood window, these points are found. Following the identification of legitimate minutiae, their orientation angles and coordinates are stored for later use in a structured format (like JSON).

The centroid of the fingerprint image is used as the reference point to divide it into four quadrants, which gives the data structure and redundancy. Each quadrant's minutiae points are grouped and kept apart. Reliability is increased by this design, which also permits partial fingerprint recognition during verification.

C. AES-Based Secret Embedding

The system then embeds a secret (such as a password, private key, or file location) after processing the fingerprint. The secret is encrypted using AES-256 in CBC mode after first being converted to Base64 format. Three layers of AES encryption are used for increased security, with distinct keys and initialization vectors used at each level.

Following encryption, the ciphertext is separated into smaller segments and allocated to minutiae coordinates in each of the four quadrants. Every component is embedded in a spot that matches a distinct fingerprint characteristic. This implies that without the original fingerprint and the necessary processing steps, even if someone manages to obtain the image, they will not be able to decrypt the embedded message.

The user submits a fingerprint scan for verification, and it goes through the same preprocessing and minutiae extraction procedure. The encrypted data is taken out of the stored locations and the biometric hash is recalculated. The embedded secret is decrypted using the regenerated hash as the decryption key.

A CRC32 checksum is used to verify the authenticity of the data that was retrieved. The system allows access if the decrypted secret matches the anticipated checksum. If not, the authentication attempt is denied, guaranteeing that the data can only be unlocked by a real fingerprint.

The system stores fingerprint-related data on the Ethereum blockchain for final authentication and to guard against tampering. Solidity is used to create a smart contract, and Ganache is used to deploy it on a local blockchain network. This contract creates an unchangeable record of authentication events by storing timestamps and encrypted fingerprint hashes.

The system sends transaction data, retrieves stored hashes for comparison, and establishes a connection to the blockchain via Web3.py. The newly created fingerprint hash and the value stored on the blockchain are compared during user authentication. The system verifies the user's identity and grants access if a match is verified. The system is perfect for sensitive applications needing stringent access control and auditability because of its blockchain-backed structure, which offers transparency and prevents unwanted changes.

V. RESULTS ANALYSIS

Multiple tests were carried out with an emphasis on process- ing time, data embedding quality and encryption performance which helps to evaluate the performance of the designed biometric blockchain system. Some of the important evaluation metrics are Mean Squared Error (MSE), embedding time, and Peak Signal-to-Noise Ratio

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, January 2026
Impact Factor: 7.67

(PSNR). These indicators reveal how well the encrypted data can be embedded into the fingerprint image without degrading the image's aesthetic appeal.

The system exhibits a slight decrease in PSNR values as the secret message lengthens. The fingerprint's usability for authentication is unaffected by the slight deterioration, though. This is to be expected since the original image is being slightly altered by the addition of more data to the fingerprint's minute structure. The PSNR stays within reasonable bounds even at larger payload sizes, guaranteeing that the fingerprint image maintains its structural integrity for precise identification.

Examination of the MSE values were also made using the various message sizes. And there we could find the result that MSE slightly rises with larger messages, as predicted and this is because data embedding causes slight variations in pixel values. The MSE values, however, continue to be low, suggesting that the fingerprint's functional and visual quality is unaffected and that the accuracy of biometric matching is unaffected.

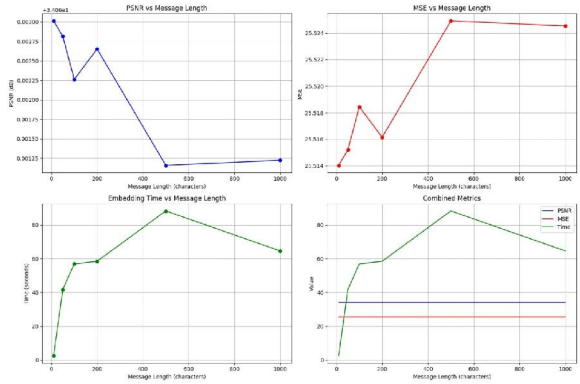

Fig. 5. System Architecture

When the message length is approximately 500 characters, the embedding time peaks in terms of time efficiency. After this, the time gradually drops, indicating that the system stabilizes following the initial overheads. For real-world applications where processing speed consistency is crucial, this behavior is especially helpful.

Once after the data gets retrieved, a CRC32 checksum was calculated to verify its integrity. By this the system can quickly determine whether the decrypted message is identical to the original message to this checksum. This step is crucial and necessary for identifying data corruption or tampering that occurs during storage or transmission.

We do have certain other encryption techniques to assess the performance. AES with triple-layer encryption offered a robust trade-off between processing speed and security among the tested techniques.

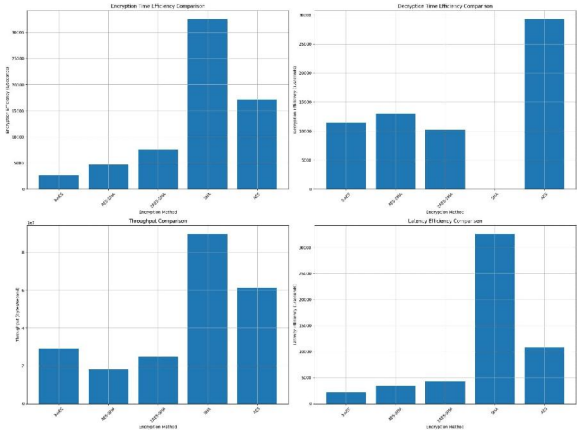

Fig. 6. System Architecture

DOI: 10.48175/IJARSCT-30875

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 2, January 2026 Impact Factor: 7.67

We do use techniques that demonstrate high throughput like SHA, but they also add latency, making them unsuitable for real-time applications. AES and hybrid AES-SHA, on the other hand, demonstrated superior responsiveness and reduced latency, which made them perfect for dynamic environments.

All things considered, the system performed well on all metrics, preserving high security, processing speed, and data integrity. Because of this, it is ideally suited for use in applications that need seamless and safe identity verification.

VI. CONCLUSION

We have used multiple techniques and methods to get an effective result in our project output; by combining fingerprint biometrics with blockchain technology and encryption, this study offers a safe and effective method of identity verification and data protection. By directly embedding encrypted data into the fingerprint's minute details, the system improves on conventional biometric authentication. It also uses decentralized blockchain storage to further secure this data.

We use triple-layer AES encryption to prevent the unauthorized data to embed the data. Ethereum smart contracts record and validate each access event, adding a verifiable, impenetrable layer of security. By enabling real- time authentication with just the user's fingerprint, this hybrid system effectively removes the risks related to centralized storage.

Based on the experimental results, this application is quite against unwanted data access, provides dependable encryption-decryption performance, and preserves image quality. The overall framework's integrity is strengthened by the use of CRC32 checksums, which further ensure that the embedded message is preserved during retrieval.

To add up more, the suggested application provides a solid basis for decentralized data management, encrypted file sharing, and safe digital identity verification. This strategy creates new opportunities for safe communication and user authentication in vital areas like banking, healthcare, and e-governance by fusing biometric uniqueness with strong cryptography and blockchain transparency.

We also thank our peers and colleagues for their consistent support and active cooperation during technical discussions, design reviews, and experimentation phases of this research work. Their constructive suggestions, collaborative spirit, and timely feedback contributed significantly to refining the methodology and improving the overall quality of the results. Finally, we gratefully acknowledge the use of various open-source tools, libraries, frameworks, and publicly available resources, which played a crucial role in the efficient implementation, testing, validation, and performance analysis of the proposed system presented herein successfully.

VII. FUTURE ENHANCEMENT

Although fingerprint-based encryption and blockchain- backed verification provide a high degree of security and dependability, the current system can be enhanced and expanded. Future iterations of the system could incorporate multi-modal biometrics, like fusing fingerprint and iris recognition. By requiring two distinct biometric characteristics, this dual-biometric method would improve authentication and lower the possibility of spoofing or illegal access.

Optimizing the encryption layers for quicker processing without sacrificing security is another possible improvement. Lightweight cryptographic techniques may be taken into consideration in situations where speed is crucial, like mobile applications or low-power embedded systems, even though triple-layer AES encryption offers robust protection.

Another crucial topic for further study is blockchain scalability. Faster and more effective data handling will become more and more necessary as the system expands to accommodate more users and bigger datasets. Using interoperable chains or Layer 2 blockchain solutions could lower processing costs and help handle large transaction volumes.

Lastly, the system may become more cross-platform accessible if it is implemented using a cloud-based architecture. The biometric encryption and verification procedure could be made available as a service to banks, identity verification organizations, and healthcare providers via secure cloud APIs.

By improving the system's performance, security, and adaptability, these improvements hope to make it a practical option for a variety of real-world uses in the years to come.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 2, January 2026
Impact Factor: 7.67

ACKNOWLEDGMENT

The authors would like to express their sincere gratitude to all those who contributed to the successful completion of this research work. We are thankful to our institution for providing the necessary infrastructure and academic environment to carry out this study.

We would like to extend our heartfelt appreciation to our project guide and faculty members for their valuable guidance, continuous encouragement, and constructive feedback throughout the course of this work.

REFERENCES

[1] G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955.

[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[3] I. S. Jacobs and C. P. Bean, "Fine particles, thin films and exchange anisotropy," in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[4] K. Elissa, "Title of paper if known," unpublished.

[5] R. Nicole, "Title of paper with only first word capitalized," J. Name Stand. Abbrev., in press.

[6] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].

[7] M. Young, The Technical Writer's Handbook. Mill Valley, CA: Univer- sity Science, 1989.

[8] Wala'a Essa Al-Ahmadi et al.: "Secure Fingerprint Image Hiding Using DNA-Based Steganography and Cryptography" 2024, PeerJ Computer Science, ISSN: 2376-5992, PP 1–22.

[9] Batool Arif Salim et al.: "AES-Based Image Steganography Integrated with Blockchain for Secure Data Hiding" 2024, Informatica Journal, ISSN: 0350-5596, PP 89–104.

[10] Waheed Rehman et al.: "GAN-Based Image Steganography for Secure and Imperceptible Data Hiding" 2024, arXiv preprint arXiv:2412.00094, PP 1–15.

[11] Yuang Qi et al.: "Provably Secure and Robust Image Steganography Using Autoregressive Image Generation" 2024, arXiv preprint arXiv:2412.12206, PP 1–18.

[12] Youn Kyu Lee et al.: "Securing Biometric Authentication System Using Blockchain" 2021, IEEE Access, ISSN: 2169-3536, PP 1–12.

[13] Harpreet Kaur et al.: "Adaptive Method of Data Hiding using Edge Detection" 2017, International Journal of Computer Applications, ISSN: 0975-8887, PP 25–30.

[14] Anto Merline Manoharan et al.: "Full Parallelism Triple AES Algorithm for Data Encryption" 2021, International Journal of Advanced Computer Science and Applications, ISSN: 2156-5570, PP 112–118.

[15] Tran et al.: "Biometrics-Based Authenticated Key Exchange with Multi-Factor Fuzzy Extractor" 2024, IEEE Transactions on Information Forensics and Security, ISSN: 1556-6013, PP 1–15.