IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 2, February 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.379

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1202055 |

Rubik's Encryption Combined with CNN for Biometric Authentication

Manoj V Bhagwath[1], Dr. A. Rengarajan[2]

Student of MCA, Dept. of CS & IT, Jain (Deemed-to-be-University), Bengaluru, India [1]

Professor, Dept. of CS & IT, Jain (Deemed-to-be-University), Bengaluru, India[2]

ABSTRACT: In response to the rapid evolution of technology, safeguarding user data has become paramount, necessitating a robust solution against diverse cyber threats. This research project proposes a comprehensive approach that integrates biometric authentication, specifically iris and fingerprint recognition, with a sophisticated encryption system based on Rubik's Cube and facilitated by Convolutional Neural Networks (CNNs). Biometric authentication establishes an unassailable link between data records and individuals, ensuring heightened accuracy and security. To counter potential threats, the project incorporates a resilient technique known as zero-bit watermarking, embedding minimal information without compromising the original biometric data's size or quality. The integration of Rubik's Cube-based encryption adds an additional layer of complexity to data protection, employing a dynamic and visually intricate encryption algorithm. The amalgamation of iris and fingerprint authentication leverages the unique biological characteristics of individuals, creating a multi-layered security approach. The CNNs play a pivotal role as the backbone for efficient feature extraction and authentication decision-making, enhancing the overall system's accuracy and reliability. This innovative fusion of cryptographic methods and biometric authentication offers a comprehensive solution for safeguarding sensitive information across diverse applications, from secure data storage to fortified communication channels, addressing the evolving landscape of cybersecurity challenges.

KEYWORDS: Biometric authentication, Zero-bit watermarking, Rubik's Cube-based encryption, Convolutional Neural Networks (CNNs), Multi-layered security, Iris and fingerprint recognition.

I. INTRODUCTION

The fundamental objective of biometrics is to automatically differentiate individuals reliably for a specific application by utilizing one or more signals derived from physical or behavioral attributes, such as fingerprints, facial features, iris patterns, voice, palm prints, or handwritten signatures. Biometric technology offers numerous advantages over conventional security methods reliant on information like passwords and pin or physical devices like keys and cards. However, a potential vulnerability arises when adversaries attempt to deceive the system by providing fake physical biometrics. Fingerprint systems, in particular, are susceptible to spoofing using common materials like gelatin, silicone, or wood glue. Consequently, a secure fingerprint system must accurately discern a spoof from an authentic finger. Various fingerprint liveness detection algorithms have been proposed, broadly categorized into hardware and software approaches. In the hardware approach, specific devices are incorporated into the sensor to detect unique properties of a living trait, such as blood pressure, skin distortion, or odor. This study employs the software approach, where fake traits are identified after acquiring the sample with a standard sensor. This enhances data security and uphold data quality. This paper focuses on the implementation of zero-bit watermarking for biometric images to fortify data for authentication purposes. The process primarily includes creating an encrypted unique ID through watermark embedding. The individual's details, represented by the watermark, are stored in the database, while the user receives the generated encrypted ID/master share. During authentication, the user scans the provided master share, initiating the extraction process for the encrypted unique ID. Successful authentication is confirmed if the extracted watermark matches the one stored in the database. The key advantage of sharing the encrypted unique ID is that even if an unauthorized party obtains it, the data remains inaccessible as it is stored in a unique ID format.

In contemporary times, biometric recognition systems find widespread use across various identification sectors, owing to their convenience and robustness in comparison to traditional methods such as passwords. These systems rely on both physiological and behavioral attributes for authentication purposes. Among the various biometric methods, fingerprint recognition stands out as one of the most frequently employed systems due to its high identification accuracy, cost-effectiveness, and applicability to large datasets of images. This has led to its deployment in diverse

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1202055 |

applications like attendance tracking, smartphone identification, forensics, healthcare systems, and banking, among others.

However, despite their advantages, biometric systems, particularly fingerprint recognition, are not immune to malicious attacks. There are two primary types of attacks - direct and indirect. Direct attacks, being more common, do not require prior knowledge and can be executed using simple tools on the sensor device, such as silicon, play-box, or wood glue. In contrast, indirect attacks necessitate in-depth knowledge about the system's modules. The proliferation of attack tools has prompted researchers to focus on developing systems capable of assessing and providing solutions for liveness detection in fingerprint systems. This review explores the recent surge in research documents related to fingerprint biometrics, reflecting the growing interest among researchers in recent years.

II. RESEARCH METHODOLOGY

The innovative zero-bit watermarking technique described in this study capitalizes on the distinct features inherent in an iris image, enabling the generation of a binary pattern without modifying the original image. Notably, this method discreetly embeds watermark bits from a fingerprint image into the segmented iris image of the user, emphasizing the creation of a secure and robust master share. The proposed watermarking algorithm extracts unique features from the iris, integrating them with the fingerprint to construct a binary watermark, resulting in the formation of a distinctive ID. This ID undergoes encryption to produce a master share. The overall watermarking process involves two primary stages: the embedding process, dedicated to generating a unique encrypted ID or master share, and the extraction process, focused on retrieving the fingerprint (watermark image) using the unique encrypted ID (master share).

The research methodology adopted for this study is a systematic and multifaceted approach aimed at developing and validating a novel zero-bit watermarking technique that seamlessly integrates iris and fingerprint features for the establishment of a secure and robust identification system. The first crucial step in our research methodology involves comprehensive data collection. This necessitates the acquisition of a diverse dataset comprising iris and fingerprint images, serving as the foundation for method validation. The collected dataset is pivotal in ensuring the robustness and applicability of the proposed watermarking technique. Upon securing the dataset, the next step is the segmentation of iris images and the extraction of unique features. This process is fundamental in capturing and highlighting the distinctive characteristics of each iris, contributing to the uniqueness of the identification system. The watermark generation process follows, where binary watermarks are created from fingerprint images. Simultaneously, a robust encryption algorithm is developed to safeguard the generated unique ID or master share.

This encryption is crucial in maintaining the security and integrity of the identification system. The embedding process is meticulously designed to discreetly integrate watermark bits into segmented iris images. This phase ensures that the watermarking is seamless and does not compromise the original features of the iris, emphasizing the importance of preserving image quality. Conversely, the extraction process is focused on retrieving watermark images using the unique encrypted ID or master share. This retrieval mechanism is integral to the accurate identification and verification of individuals based on the embedded watermarks. The evaluation stage is comprehensive, assessing the technique's effectiveness in terms of security, robustness, and image quality. Rigorous experiments are conducted using various datasets to validate the proposed watermarking approach under diverse conditions.

Comparative analysis against existing watermarking methods is undertaken to provide insights into the advantages and limitations of the proposed technique. This comparative study aids in positioning the novel approach within the broader context of watermarking technologies. Validation procedures are implemented to ensure the uniqueness and reliability of the generated master share. Rigorous testing protocols are employed to verify the system's accuracy and resilience against potential adversarial attempts. The entire research process, including algorithms, parameters, and results, is meticulously documented for future reference and potential replication. This comprehensive documentation is crucial for transparency, reproducibility, and further advancements in the field of watermarking technologies. Ultimately, the overarching goal of this research methodology is to contribute to the development and validation of an innovative zero-bit watermarking technique that effectively integrates iris and fingerprint features, establishing a secure and robust

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1202055 |

identification system with broad applications across diverse domains.

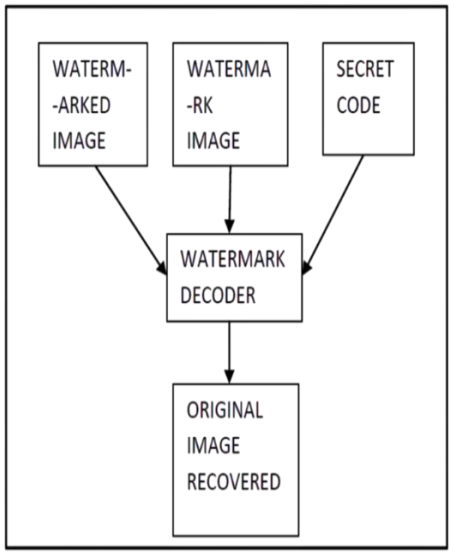
III. BACKGROUND

This research stems from the need for advanced and secure identification systems in various domains. Conventional watermarking techniques may compromise image quality or security. Hence, a novel approach is proposed, integrating iris and fingerprint features in a zero-bit watermarking technique. This aims to establish a secure and robust identification system with applications across diverse fields, addressing limitations of existing watermarking methods. The methodology involves a systematic process from data collection to validation, contributing to advancements in watermarking technologies.

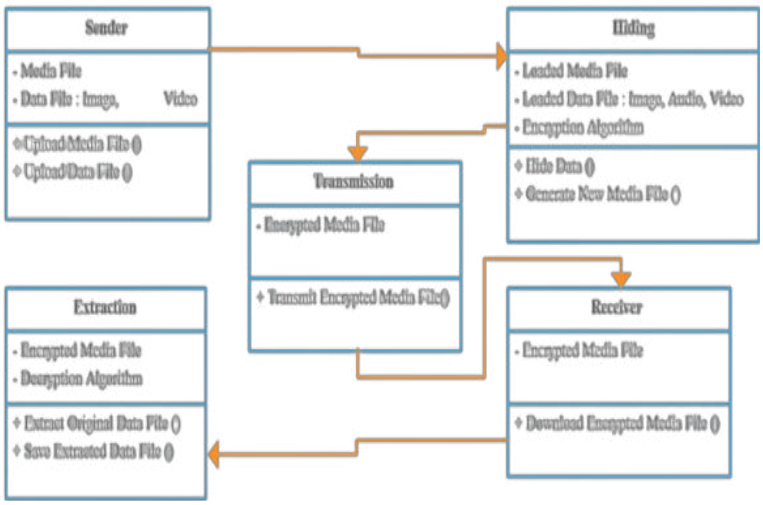
In the contemporary landscape of digital security and biometric identification systems, the demand for innovative and foolproof techniques is ever-growing. Traditional watermarking methods often face challenges related to either compromising image quality or lacking the desired level of security. This research emerges as a response to the limitations of existing watermarking approaches, seeking to develop a novel method that seamlessly integrates iris and fingerprint features. Biometric identification, particularly utilizing iris and fingerprint data, has gained prominence due to its unique and intrinsic characteristics that enhance security measures. Iris images, with their intricate patterns, and fingerprint data, known for its individuality, offer a robust foundation for a secure identification system. However, the integration of these features in a manner that preserves image quality and ensures data security remains a significant challenge. The motivation behind this research is to bridge the gap by proposing a zero-bit watermarking technique that not only maintains the integrity of iris images but also discreetly embeds fingerprint watermark bits for enhanced security. The aim is to create a secure and robust master share, facilitating accurate identification and verification processes. The significance of this research extends to various domains, including but not limited to digital forensics, secure access control, and personal authentication. The potential applications range from law enforcement to secure access to sensitive information, making it a valuable contribution to the broader field of biometric identification and digital security. By combining the distinctive features of iris and fingerprint data in a zero-bit watermarking technique, this research aspires to offer a solution that not only overcomes the limitations of existing methods but also sets a new standard for secure and reliable identification systems. The comprehensive research methodology ensures the validity and applicability of the proposed technique, laying the groundwork for advancements in watermarking technologies with broad implications for diverse industries.

IV. ANALYSIS AND DESIGN

ARCHITECTURE DIAGRAM



CLASS DIAGRAM



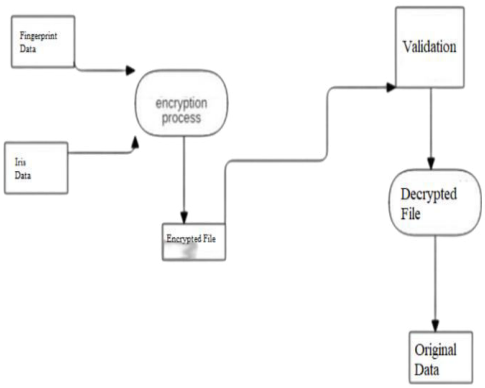
International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

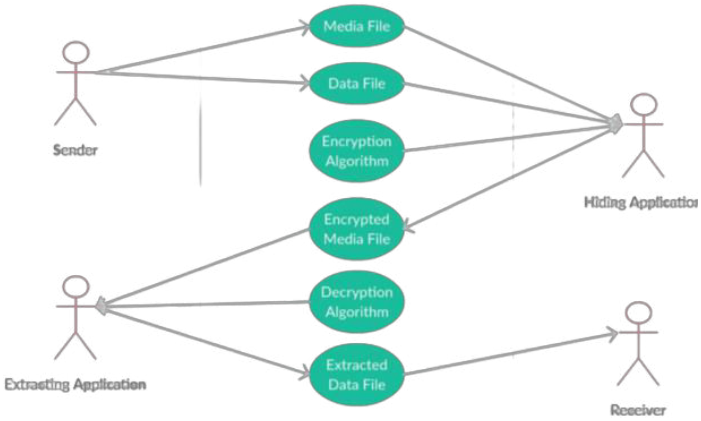
|| Volume 12, Issue 2, February 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1202055 |

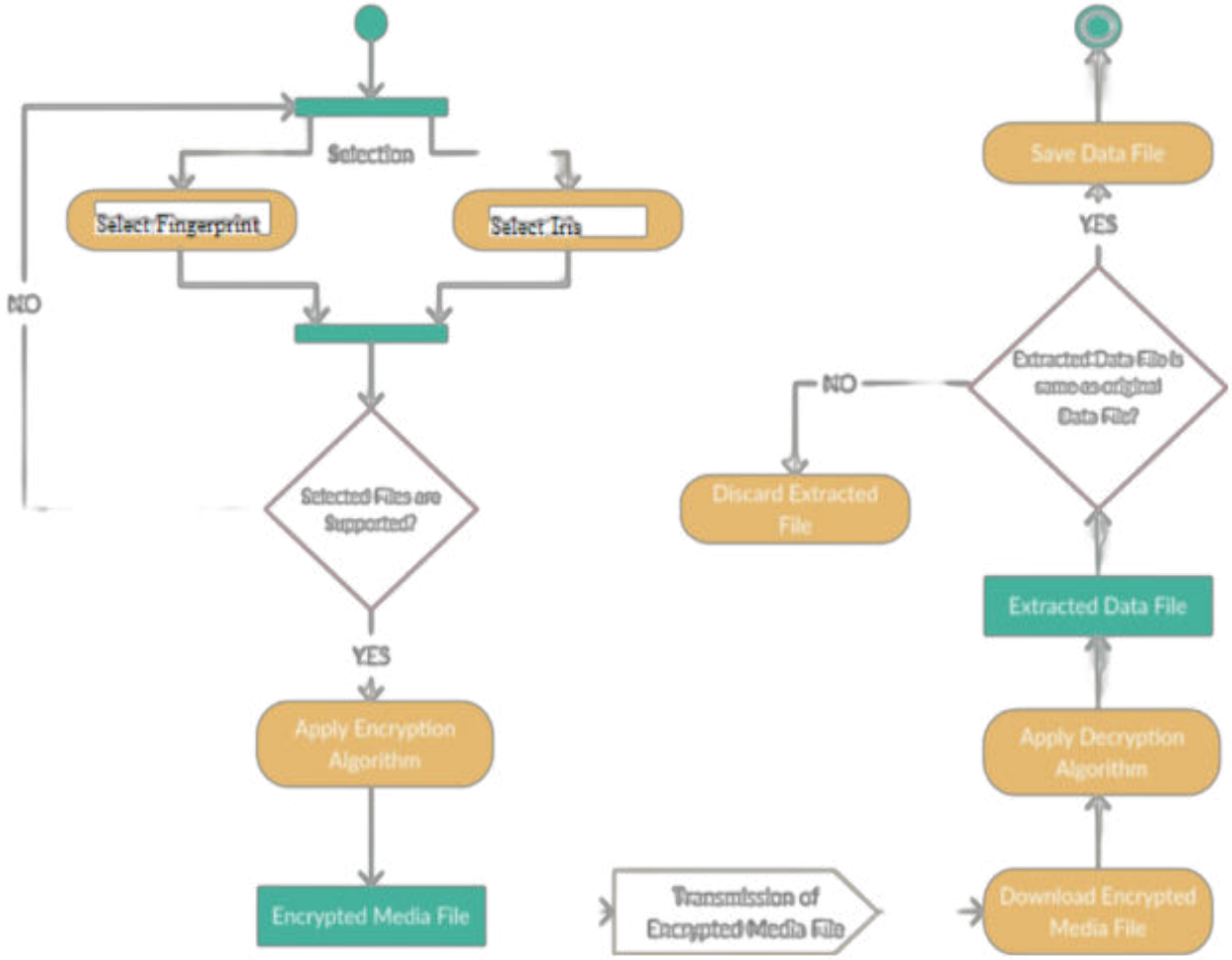
DATA FLOW DIAGRAM



USE CASE DIAGRAM



ACTIVITY DIAGRAM



| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1202055 |

V. TECHNICAL AND ECONOMIC ANALYSIS

From a technical perspective, the proposed zero-bit watermarking technique showcases a promising integration of iris and fingerprint features, leveraging their distinct characteristics. The algorithm's ability to discreetly embed watermark bits into segmented iris images without compromising the original features is noteworthy, emphasizing the preservation of image quality. The methodology involves a systematic approach, from data collection to encryption, ensuring the seamless integration of iris and fingerprint data.

The iris segmentation and feature extraction processes contribute to capturing the uniqueness of individual irises, enhancing the distinctiveness of the identification system. Additionally, the development of a robust encryption algorithm signifies a commitment to security, providing a safeguard against potential threats. The integration of these technical aspects, including compatibility with existing technology and the meticulous preservation of image quality, positions the proposed technique as a technically sound solution for secure identification.

On the economic front, a thorough cost-benefit analysis is essential to assess the viability of implementing the proposed watermarking technique. The economic feasibility of the system involves considerations such as initial development costs, infrastructure requirements, ongoing maintenance expenses, and potential scalability costs. While the integration of iris and fingerprint features suggests advancements in biometric identification, the economic analysis should weigh the benefits of enhanced security and robustness against the associated costs. Furthermore, the potential cost savings resulting from the proposed system's effectiveness in preventing unauthorized access or identity fraud should be factored into the economic assessment. A balanced evaluation of both technical prowess and economic viability is crucial for determining the practicality and potential widespread adoption of the proposed zero-bit watermarking technique in various applications and industries.

VI. CONCLUSION AND FUTURE WORK

In conclusion, this study introduces an innovative zero-bit watermarking technique that leverages the distinctive features inherent in iris images and seamlessly integrates them with fingerprint features to establish a secure and robust identification system. The proposed methodology involves a systematic and multifaceted approach, beginning with comprehensive data collection to build a diverse dataset of iris and fingerprint images. Through segmentation and feature extraction, the uniqueness of each iris is captured, forming the foundation for a distinctive identification system.

The watermark generation process creates binary watermarks from fingerprint images, and a robust encryption algorithm is developed to safeguard the unique ID or master share, ensuring the security and integrity of the identification system. The embedding process discreetly integrates watermark bits into segmented iris images while preserving the original features and image quality. The extraction process focuses on retrieving watermark images using the unique encrypted ID or master share, facilitating accurate identification and verification. The evaluation stage involves rigorous experiments, assessing the technique's effectiveness in terms of security, robustness, and image quality. Comparative analysis against existing watermarking methods provides insights into the proposed technique's advantages and limitations, positioning it within the broader context of watermarking technologies. Validation procedures ensure the uniqueness and reliability of the generated master share, and rigorous testing protocols verify the system's accuracy and resilience against potential adversarial attempts.

Throughout the research process, including algorithms, parameters, and results, meticulous documentation is maintained for transparency, reproducibility, and future advancements in watermarking technologies. The overarching goal is to contribute to the development and validation of an innovative zero-bit watermarking technique that effectively integrates iris and fingerprint features, thereby establishing a secure and robust identification system with broad applications across diverse domains.

ACKNOWLEDGMENT

Dreams do not become realities until a great deal of effort and work ethic is put into them, and no commitment produces fruit in the absence of support and direction. It takes a lot of effort to achieve this aim, and having somebody to advise and assist me is always a blessing.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.379 | Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 2, February 2024 ||

| DOI: 10.15680/IJIRCCE.2024.1202055 |

I'd like to take this time to thank a few people who were instrumental in the completion and execution of this research project. To begin, I want to thank God Almighty for making my attempt a success. I'd want to convey my heartfelt gratitude to the JAIN (Deemed-to-be) University for offering superb facilities and other resources that allowed me to hone my talents. I would like to convey my heartfelt thanks to Dr. A. Rengarajan, the research guide, for his unwavering support and insightful ideas, without which the effective completion of this study would not have been possible.

REFERENCES

[1] Kumar, A., Dwivedi, A., & Dutta, M. K. (2020, February). A zero watermarking approach for biometric image security. In 2020 International Conference on Contemporary Computing and Applications (IC3A) (pp. 53-58). IEEE

[2] Dwivedi, A., Kumar, A., Dutta, M. K., Burget, R., & Myska, V. (2019, July). An efficient and robust zero-bit watermarking technique for biometric image protection. In 2019 42nd International Conference on Telecommunications and Signal Processing (TSP) (pp. 236-240). IEEE.

[3] Mishra, M., Bhattacharya, A., Singh, A., & Dutta, M. K. (2018, February). A lossless model for generation of unique digital code for identification of biometric images. In 2018 4th International Conference on Computational Intelligence & Communication Technology (CICT) (pp. 1-5). IEEE.

[4] Taj, T., & Sarkar, M. (2023). A Survey on Embedding Iris Biometric Watermarking for User Authentication. Cloud Computing and Data Science, 203-211.

[5] Deepika, R., Shambhavi, M., Impana, R., Shishira, A. P., & Krishna, L. (2022, June). Zero-Bit Watermarking Technique for Generation of Unique ID Using Biometric Images. In 2022 2nd International Conference on Intelligent Technologies (CONIT) (pp. 1-4). IEEE.

[6] Swathi, B., & Kumari, T. M. (2017, September). Iris biometric security using watermarking and visual cryptography. In 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI) (pp. 1218-1220). IEEE.

[7] Vashistha, A., & Joshi, A. M. (2016, November). Fingerprint based biometric watermarking architecture using integer DCT. In 2016 IEEE region 10 conference (TENCON) (pp. 2818-2821). IEEE.

[8] Balamurugan, G., Joseph, K. S., & Arulalan, V. (2016, February). An Iris Based Reversible Watermarking system for the security of teleradiology. In 2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave) (pp. 1-6). IEEE.

[9] Abdullah, M. A., Dlay, S. S., Woo, W. L., & Chambers, J. A. (2016). A framework for iris biometrics protection: a marriage between watermarking and visual cryptography. IEEE Access, 4, 10180-10

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.379

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details