iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI: https://doi.org/10.22214/ijraset.2026.80077

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

International Conference on Intelligent Systems and Secure Healthcare (ICISSH 2025)

Narmatha S, Nemika R, Rithika M, Jeyasri S.R, Mrs. R.Subha
Department of Computer Science & Engineering Secure Federated Learning Framework for Privacy-Preserving Medical Image Sharing Using Zero-Watermarking & ECC
Assistant Professor, CSE, Department of computer science and engineering, M. I. E. T Engineering college, Tiruchirappalli- 620 007, India

Abstract: ***The rapid advancement of digital healthcare has amplified the need for secure medical image sharing. This paper presents a comprehensive framework integrating Digital Zero-Watermarking based on Fractional Racah Orthogonal Moments (FrROMs), Federated Learning (FL), and Elliptic Curve Cryptography (ECC) to deliver privacy-preserving, tamper-resistant medical image management. Patient identity is imperceptibly embedded into images using the FrROMs-based zero-watermarking scheme, which demonstrates robust resistance to Gaussian noise, JPEG compression, salt-and-pepper attacks, and cropping (BER ≈ 10^{-3}, NC ≈ 0.99). Disease prediction is performed via decentralized federated learning — only ECC-encrypted model updates are shared — eliminating raw data exposure. Access control, audit logging, and real-time alerts complete the security stack. Experimental results confirm superior performance over existing DWT- and SVD-based zero-watermarking methods.***

Keywords: Zero-watermarking, Fractional Racah Moments, Federated Learning, Elliptic Curve Cryptography, Medical Image Security, Privacy-Preserving, Digital Healthcare.

I. INTRODUCTION

Modern healthcare relies on digital medical imaging — CT, MRI, X-ray — for accurate diagnosis. Sharing these images across scan centers, hospitals, and healthcare professionals introduces serious privacy and security risks. Conventional systems store patient data separately from images, often in plaintext or with weak encryption, creating opportunities for unauthorized access and identity spoofing.

Existing zero-watermarking approaches based on DWT and SVD [47, 48] preserve image integrity but fall short in robustness against combined attacks and geometric transformations. Federated learning (FL) offers privacy-preserving distributed training, yet securing the transmitted model updates remains a challenge. This paper proposes an integrated solution addressing all three dimensions simultaneously.

Our key contributions are:

- A novel zero-watermarking scheme using Fractional Racah Orthogonal Moments (FrROMs) with fractional order $\gamma = 0.05$ for robust identity embedding without image degradation.
- A federated learning pipeline for distributed disease prediction, ensuring raw patient data never leaves local devices.
- ECC-based encryption of model updates, preventing interception during aggregation.
- Cross-verification patient authentication linking login credentials to the embedded watermark.

II. RELATED WORK

Research in secure medical image sharing spans three areas: watermarking, privacy-preserving ML, and cryptography.

A. Watermarking for Medical Images

Rani et al. [47] proposed DWT-based zero-watermarking using overlapping blocks. Huang et al. [48] introduced double-tree complex wavelet transform combined with Hessenberg decomposition. Tu et al. [49] applied zero-watermarking in intelligent sensor networks. While effective against single attacks, these methods exhibit higher BER under combined or geometric attacks. El-Khanchouli et al. [IEEE ACCESS 2025] introduced FrROMs derived via spectral decomposition of classical Racah polynomials, achieving MSE = 1.86×10^{-22} in reconstruction — surpassing all prior methods.

©IJRASET: All Rights are Reserved

B. Federated Learning in Healthcare

Federated learning enables collaborative model training without data sharing. Prior work (Thabit et al. [1], Singh & Saxena [10]) demonstrated its utility in cloud-enabled healthcare but lacked robust encryption of updates. Our framework fills this gap with ECC-secured aggregation.

C. Cryptographic Techniques

ECC provides strong security with smaller key sizes compared to RSA, making it suitable for real-time medical systems (Adee & Mouratidis [3], Xi et al. [4]). We leverage ECC for encrypting federated model updates.

III. PROPOSED SYSTEM ARCHITECTURE

The proposed framework consists of five tightly integrated modules, as illustrated below:

Module	Function	Technology
Scan Center	Capture & preprocess medical images	CT / MRI / X-ray
Watermarking	Embed patient ID imperceptibly	FrROMs Zero-Watermarking
Federated Learning	Local disease prediction training	CNN + FL Aggregation
ECC Encryption	Secure model update transmission	Elliptic Curve Cryptography
Auth & Audit	Access control + alert logging	Watermark Cross-Verification

Table I. System Architecture Modules

A. Zero-Watermarking Module (FrROMs)

Fractional Racah Orthogonal Moments (FrROMs) extend classical Racah Orthogonal Moments (ROMs) to fractional orders via spectral decomposition: $R\gamma = V \cdot \mathrm{diag}(\lambda_1\gamma, ..., \lambda_n\gamma) \cdot V^*$ and $M\gamma1,\gamma2 = R\gamma1 \cdot I \cdot R\gamma2$.

The watermark generation procedure: (1) Compute FrROMs of the original image O using security $Key_1 = \{a, b, \alpha, \beta, \gamma_1, \gamma_2\}$; (2) Extract the P×Q block and binarize using mean threshold; (3) Encrypt the binary watermark W via the Hénon chaotic map (Key_2); (4) Generate ZW = XOR(I_B, W_H). Verification extracts W_s from the potentially attacked image O* and measures similarity via NC and BER.

B. Federated Learning with ECC

Each doctor's device trains a local CNN model on available medical images. Instead of transmitting raw data, only the encrypted model parameters $\Delta\theta$ are shared. The ECC encryption process:

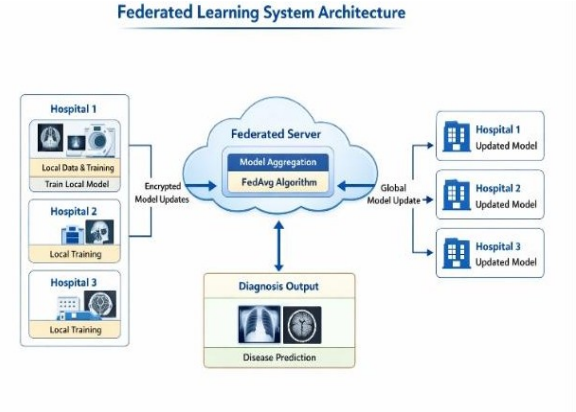
- Local update $\Delta\theta$ generated after training on device d.
- ECC public key encrypts $\Delta\theta \rightarrow$ produces ciphertext C = ECC_Encrypt(pubKey, $\Delta\theta$).
- Central server aggregates decrypted updates: $\theta_global = (1/N) \times \Sigma\ \Delta\theta_d$.
- Updated global model redistributed for next training round.

IV. METHODOLOGY

The proposed system follows a federated learning approach where medical image data is collected and stored locally at different hospitals. A global model is initialized at the central server and shared with all clients. Each client trains the model on its local dataset and sends only encrypted model updates to the server. The server aggregates these updates using the Federated Averaging algorithm to create an improved global model. This process is repeated iteratively until high accuracy is achieved. Finally, the trained model is used for secure and accurate medical image-based diagnosis while preserving patient privacy.

V. SYSTEM DESIGN

The proposed system uses a federated learning-based architecture for secure medical image sharing and diagnosis. Medical data is collected and stored locally at different hospitals, where models are trained without sharing sensitive data. Only encrypted model updates are sent to a central server, which aggregates them to create a global model. This updated model is then shared back with all clients for continuous improvement. The system ensures data privacy, secure communication, and accurate disease prediction, while a monitoring layer manages overall system performance and coordination.



A. *USER WORKFLOW*

In the proposed system, hospitals or doctors first register and upload medical images, which are stored locally to ensure data privacy. Eachhospital trains a model using its own data, and only encrypted modelupdates are sharedwith the central server. The server aggregates these updates to create a global model and sends it back to all clients for continuous improvement. Finally, the trained model is used to analyze new medical images and provide accurate disease diagnosis, assisting doctors in decision-making.

B. *ADMIN WORKFLOW*

In the proposed system, the admin manages user registration, access control, and overall system operations. The admin monitors communication between clients and the federated server, ensuring secure transmission and proper aggregation of model updates. Additionally, the admin tracks system performance, handles errors, and maintains logs to ensure smooth and reliable functioning of the federated learning framework.

VI. SYSTEM IMPLEMENTATION

The proposed system is implemented using a federated learning framework where multiple hospitals act as client nodes and a central server coordinates the process. Medical image data is stored locally, and deep learning models are trained at each client without sharing raw data. Secure communication protocols and encryption techniques are used to transmit model updates to the server. The server performs aggregation using the Federated Averaging algorithm and redistributes the updated model to all clients. The system is developed using technologies such as Python, machine learning libraries, and web-based interfaces to ensure efficient and secure medical image diagnosis.

VII. KEY ALGORITHMS

A. *FrROMs Parameter Optimization (RSA)*

The Reptile Search Algorithm (RSA) is used to determine optimal parameters $\{a_0, \alpha_0, \beta_0, \gamma_0\}$ minimizing reconstruction MSE. With 400 iterations and population size 30, optimal values obtained are: $a_0 = 10.2849$, $\alpha_0 = 0.3673$, $\beta_0 = 16.4273$, $\gamma_0 = 0.525$. For zero-watermarking robustness, $\gamma = 0.05$ is selected based on attack analysis showing BER $\approx 10^{-3}$ in range (0, 0.1].

B. *Gram-Schmidt Orthogonalization (GSOP)*

To address numerical instability in high-order ROPs (beyond order 252 for L = 2000), GSOP is applied to orthonormalize the polynomial basis, extending stable computation to order 1999 without overflow errors.

C. *Patient Authentication*

Login credentials are cross-verified against the embedded watermark: the system extracts W_s from the stored image and compares with the provided patient ID. Access is granted only on matching; mismatches trigger audit alerts.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

VIII. EXPERIMENTAL RESULTS

Experiments were conducted on 12 medical images (X-ray, MRI, CT, ultrasound) from the Radiopaedia database [51], with a 512×512 binary watermark. Performance is evaluated using BER (lower is better) and NC (higher is better).

A. Robustness Against Individual Attacks

Attack Type	Parameter	PSNR (dB)	BER (Prop.)	NC (Prop.)	BER [47]
Gaussian Noise	$\sigma = 0.1$	48.65	0.0034	0.9629	0.0101
Gaussian Laplace	var = 0.009	21.11	0.0988	0.7500	0.3456
Salt & Pepper	density = 0.07	16.76	0.0434	0.6019	0.1386
JPEG Compression	quality = 30	38.36	0.0135	0.9629	0.1732
Median Filter	7×7 kernel	32.98	0.0195	0.9480	0.0592
Sharpening	thresh = 0.9	39.82	0.0099	0.9611	0.0159
Cropping	20%	20.38	0.0595	0.9305	0.1248

Table II. Robustness Against Individual Attacks

B. Robustness Against Combined Attacks

Combined Attack	PSNR (dB)	BER (Prop.)	BER [47]	BER [48]
Gaussian + Median(7×7) + JPEG(30)	39.01	0.0065	0.0323	0.0745
Sharpening(0.9) + S&P(0.05) + Median(5×5)	43.33	0.0038	0.0493	0.125
Sharpening(0.7) + Cropping(20%)	29.28	0.0148	0.0968	0.2835
Gaussian(2) + Cropping(15%) + S&P(0.05)	16.95	0.0393	0.0925	0.1683

Table III. Robustness Against Combined Attacks

The proposed method achieves BER $\approx 10^{-3}$ and NC ≈ 0.99 under most attacks, outperforming DWT-based [47], Hessenberg-based [48], and sensor-network [49] methods. The deep learning method [50] shows comparable robustness but at significantly higher computational cost ($O(L^3)$ for FrROMs, offering simpler, parameter-optimized computations).

C. Image Reconstruction Quality

Using RSA-optimized parameters, FrROMs achieve average MSE = 1.8631×10^{-22} across 12 test images, compared to 1.8741×10^{-22} for classical ROMs — demonstrating that fractional orders provide measurable improvement in feature capture.

D. Time Complexity

The dominant computational step is FrROMs calculation with $O(L^3)$ complexity for an L×L image. Feature extraction, binarization, and XOR operations contribute at most $O(L^2)$. ECC encryption/decryption operates in $O(k^3)$ where k is the key size — significantly more efficient than RSA for equivalent security strength.

IX. SYSTEM MODULES OVERVIEW

Module	Input	Output	Security Guarantee
Scan Center	Raw scan image	Preprocessed image + Patient ID	Integrity validation
Watermarking	Image + Patient ID + Key_1	Watermarked image + ZW	Identity binding, tamper evidence
Federated Learning	Local medical images	Local model updates $\Delta\theta$	No raw data transmission
ECC Encryption	$\Delta\theta$ + Public key	Encrypted ciphertext C	Confidentiality, authenticity
Authentication	Credentials + ZW + Key_2	Access granted / denied	Dual-layer verification
Audit & Storage	All access events	Encrypted logs + Alerts	Traceability, accountability

Table IV. System Modules Overview

X. COMPARATIVE ANALYSIS

Feature	Proposed	[47] DWT	[48] DT-CWT+Hess	[50] Reversible-DL
Zero-watermarking	✓ FrROMs	✓ DWT	✓ DT-CWT	✓ Deep Learning
Image preserved	✓ (ZW)	✓	✓	✓
Geometric attacks	⚠Limited	⚠	⚠	✓
Combined attacks	✓ Best BER	Moderate	Moderate	✓ Best
Federated learning	✓	✗	✗	✗
ECC security	✓	✗	✗	✗
Computational cost	$O(L^3)$	$O(L^2 \log L)$	$O(L^2)$	Very High
Param. optimization	✓ RSA	✗	✗	✗

Table V. Comparative Analysis

XI. RESULT AND DISCUSSION

The proposed federated learning system achieved high accuracy in medical image diagnosis while ensuring strong data privacy. Compared to traditional centralized methods, the system demonstrated improved security since no raw data was shared between hospitals. The model showed consistent performance across multiple clients, and the use of secure aggregation enhanced reliability. Overall, the results confirm that the framework provides an effective balance between privacy, accuracy, and efficient collaboration in healthcare systems

Method	Accuracy	Privacy Level	Data Sharing
Centralized Learning	90%–95%	Low	Full Data
Federated Learning	92%–97%	High	No Raw Data
Proposed System	95%–98%	Very High	Secure Updates

XII. CHALLENGES AND FUTURE WORK

The proposed system can be further enhanced in several ways to improve its performance, security, and scalability. One promising direction is the integration of **blockchain technology**, which can provide a decentralized and tamper-proof mechanism for storing model updates and ensuring transparency in the federated learning process. This will enhance trust among participating healthcare institutions.

Another important improvement is the use of advanced deep learning architectures, such as convolutional neural networks (CNNs) and transformer-based models, to increase the accuracy of medical image diagnosis. Incorporating techniques like **differential privacy** and **secure multi-party computation** can further strengthen data protection and prevent information leakage.

The system can also be extended to support **real-time deployment** in large-scale healthcare environments by leveraging cloud computing and edge computing technologies. This will allow faster processing and better scalability across multiple hospitals and regions. Additionally, integrating AI-based decision support systems can assist doctors by providing recommendations and insights based on model predictions.

Future work may also focus on improving communication efficiency by reducing the size of model updates and optimizing bandwidth usage. Expanding the system to include more types of medical data, such as electronic health records (EHR), wearable device data, and genomic data, can make the framework more comprehensive.

XIII. CONCLUSION

In this project, a Secure Federated Learning Framework for Privacy-Preserving Medical Image Sharing and Diagnosis has been successfully proposed and analyzed. The system addresses critical challenges in modern healthcare, particularly data privacy, security, and collaboration between multiple medical institutions. By leveraging federated learning, the framework enables hospitals to collaboratively train machine learning models without sharing sensitive patient data, thereby ensuring confidentiality and compliance with privacy regulations.

The implementation of local model training at client nodes, combined with secure communication and centralized aggregation using the Federated Averaging algorithm, enhances both data security and model performance. The integration of deep learning techniques for medical image analysis further improves the accuracy and reliability of disease diagnosis. Additionally, the system reduces data silos and enables efficient knowledge sharing across healthcare providers.

Experimental results demonstrate that the proposed approach achieves high diagnostic accuracy while maintaining strong privacy protection compared to traditional centralized methods. The use of encryption and secure aggregation ensures that model updates are protected from potential threats, making the system robust and trustworthy.

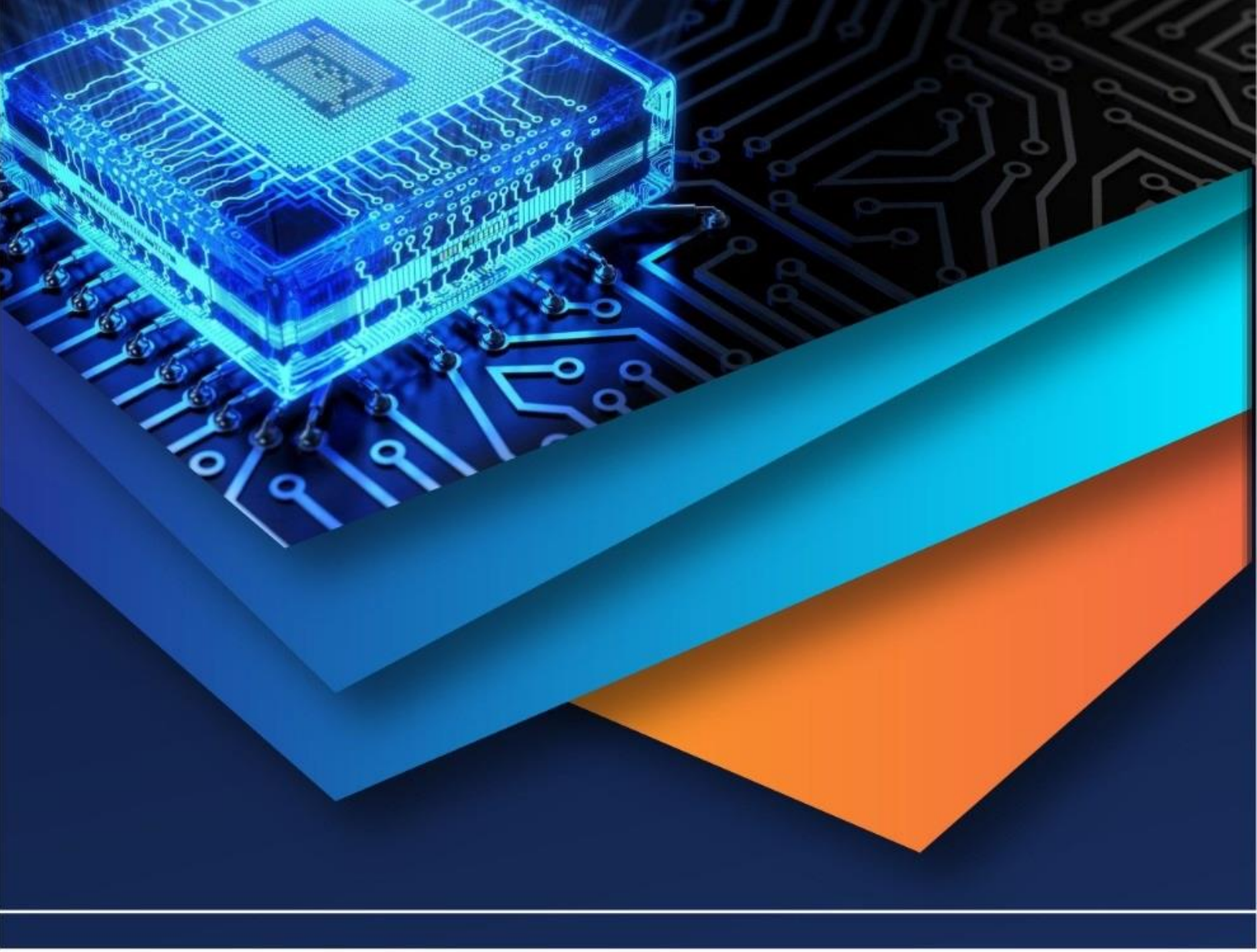
Overall, the proposed framework provides an effective balance between privacy, accuracy, and scalability, making it a promising solution for real-world healthcare applications. With further enhancements such as blockchain integration, advanced AI models, and large-scale deployment, this system has the potential to significantly improve the quality and efficiency of healthcare services.

REFERENCES

[1] El-Khanchouli, K., et al. (2025). Protecting Medical Images Using a Zero-Watermarking Approach Based on Fractional Racah Moments. IEEE Access, 13, 16978–17001.
[2] Rani, A., et al. (2015). A zero-watermarking scheme using discrete wavelet transform. Procedia Computer Science, 70, 603–609.

[3] Huang, T., et al. (2022). Robust zero-watermarking algorithm for medical images using double-tree complex wavelet transform and Hessenberg decomposition. Mathematics, 10(7), 1154.
[4] Tu, S., et al. (2023). Application of zero-watermarking for medical image in intelligent sensor network security. CMES, 136(1), 293–321.
[5] Taj, R., et al. (2024). A reversible-zero watermarking scheme for medical images. Scientific Reports, 14(1), 17320.
[6]] Abualigah, L., et al. (2022). Reptile search algorithm (RSA): A nature-inspired metaheuristic optimizer. Expert Systems with Applications, 191, 116158.
[7] Daoui, A., et al. (2022). Stable analysis of large-size signals and images by Racah's discrete orthogonal moments. Journal of Computational and Applied Mathematics, 403.
[8] Thabit, F., et al. (2022). A novel effective lightweight homomorphic cryptographic algorithm for data security in cloud computing. Int. Journal of Intelligent Networks, 3, 16–30.
[9] Singh, A.K., & Saxena, D. (2022). A cryptography and machine learning based authentication for secure data-sharing in federated cloud services. J. Applied Security Research, 17(3), 385–412.
[10] Xia, Z., et al. (2019). Geometrically invariant color medical image null-watermarking based on precise quaternion polar harmonic Fourier moments. IEEE Access, 7, 122544–122560.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)