Vol 4, Issue 9, September 2024 www.ijesti.com E-ISSN: 2582-9734
International Journal of Engineering, Science, Technology and Innovation (IJESTI)

Enhanced Authentication Using ECC and ADV-ML Techniques

Yogini Diliprao Salunke[1], Dr. Suhas Rajaram Mache[2]

[1] Research Scholar, University Of Technology, Jaipur
[2] Computer Department, University Of Technology, Jaipur

Email: YOGINISALUNKE7@gmail.com

ABSTRACT

This study explores a robust authentication mechanism combining Elliptic Curve Cryptography (ECC) and Advanced Machine Learning (ADV-ML), specifically Random Forest, to address modern cybersecurity challenges. ECC is leveraged for its computational efficiency, offering strong security with shorter key lengths, making it ideal for resource-constrained environments. It ensures secure encryption, key exchange, and digital signatures, providing a foundation for safeguarding sensitive data. The integration of ADV-ML enhances system adaptability by analysing user behaviours, environmental contexts, and detecting anomalies. Random Forest's predictive capabilities enable dynamic security adjustments, improving authentication accuracy and mitigating evolving threats. Additional layers of steganography and watermarking secure hidden data and verify authenticity, respectively. The multi-layered approach, validated through rigorous simulations, demonstrates a high probabilistic success rate of 97.73%, ensuring robust encryption, anomaly detection, and data integrity. This framework is a scalable solution for sectors requiring high-security standards, including healthcare, finance, and government systems, supporting seamless, user-friendly authentication while safeguarding privacy.

Keywords: Elliptic Curve Cryptography (ECC), Secure Communication, Advanced Machine Learning (ADV-ML), Data Privacy

Introduction

This section introduces a groundbreaking authentication mechanism that combines Elliptic Curve Cryptography (ECC) and Advanced Machine Learning (ADV-ML), with a focus on the Random Forest algorithm, to significantly enhance digital security. ECC is recognized for its ability to provide strong encryption with relatively short key lengths, making it both computationally efficient and highly secure. By using ECC, the system is able to maintain a high level of protection against cyber threats while minimizing the computational overhead typically associated with traditional cryptographic methods. This makes it an ideal choice for securing authentication processes, particularly in environments where resources may be limited. The integration of ADV-ML into the authentication framework adds a critical layer of intelligence. ADV-ML is designed to continuously analyze user behavior patterns, device attributes, and other contextual data, allowing the system to detect anomalies or suspicious activities in real-time. Through machine learning, the system can adapt to evolving cyber threats by learning from new data, ensuring that it can effectively counter both known and emerging attack vectors. This adaptive capability enhances the overall flexibility and responsiveness of the authentication system, making it more effective in the face of dynamic and complex cybersecurity challenges. The synergy between ECC and ADV-ML offers a robust solution that not only strengthens security but also improves the user experience. As users increasingly demand seamless and user-friendly security solutions, the combination of these technologies allows for dynamic adjustments to security protocols without compromising user

convenience. The primary goal of the study is to explore how these two advanced technologies can work together to create a more secure, efficient, and adaptive authentication system, addressing the growing need for sophisticated, future-proof security mechanisms capable of combating increasingly sophisticated cyber threats.

Authentication mechanisms are essential for verifying the identity of users and systems to protect sensitive information. Various methods include password-based authentication, which requires users to remember a secret password; multi-factor authentication (MFA), combining multiple factors like passwords, tokens, and biometrics; and biometric authentication, which relies on physical traits such as fingerprints or facial recognition. Other methods include token-based authentication, smart cards with Public Key Infrastructure (PKI), and Single Sign-On (SSO), which simplifies access to multiple systems. CAPTCHA systems differentiate humans from bots, while risk-based authentication evaluates factors like user behavior and device location to assess risk. Time-based authentication limits access to specific hours, and device authentication ensures the legitimacy of the accessing device. Elliptic Curve Cryptography (ECC) enhances authentication by providing strong security with smaller key sizes, making it efficient for use in key exchange protocols, digital signatures (ECDSA), and secure communication protocols like SSL/TLS. ECC's advantages include faster key generation, reduced computational overhead, and quantum resistance, making it a preferred choice for securing digital transactions and ensuring the authenticity of identities across various platforms. As digital environments evolve, these authentication mechanisms are critical to balancing security, privacy, and usability.

ADV-ML (Adversarial Machine Learning) has revolutionized authentication methods by addressing vulnerabilities in traditional systems like passwords and PINs. Traditional approaches are prone to attacks such as phishing and password reuse, but ADV-ML enhances security through algorithms that learn from data and adapt to changing circumstances. One of the key applications of ADV-ML is in biometric systems, such as facial recognition, fingerprints, and voice recognition, which improve accuracy by continuously learning patterns from biometric data. Additionally, ADV-ML contributes to behavioral biometrics by analyzing user habits, such as typing speed and mouse movements, to detect anomalies that indicate unauthorized access. ADV-ML also plays a crucial role in adaptive authentication, adjusting security levels based on contextual factors, like login locations. Despite its advantages, ADV-ML faces challenges such as adversarial attacks and privacy concerns, particularly with biometric data. Researchers are working on strengthening models against such attacks and ensuring proper data management to prevent unauthorized access. As technology advances, the role of ADV-ML in creating secure and user-friendly digital environments will continue to grow, making systems more dynamic and resilient to security threats.

Elliptic Curve Cryptography (ECC) is a highly efficient and secure cryptographic method used to protect data and communications in modern computing. It relies on elliptic curves defined by the equation $y^2 = x^3 + ax + b$, with cryptographic operations like point addition and scalar multiplication being fundamental to its algorithm. ECC stands out for providing robust security with much shorter key lengths compared to traditional methods like RSA, making it ideal for applications where efficiency is critical. ECC is commonly used in key exchange protocols, such as Diffie-Hellman, and for creating digital signatures that ensure the authenticity and integrity of messages. Its security is based on the Elliptic Curve Discrete Logarithm Problem (ECDLP), which remains computationally difficult even with advanced computing power. ECC also plays a key role in hybrid encryption systems, combining symmetric and asymmetric encryption to optimize performance. While ECC is widely adopted in modern cryptographic systems, its

security depends on the careful selection of parameters to avoid implementation vulnerabilities. ECC is increasingly relevant in the context of cloud computing and data outsourcing, where it helps protect privacy and secure information across distributed networks. As digital infrastructures evolve, ECC continues to be a cornerstone of secure and efficient cryptography in a growing interconnected world.

Elliptic Curve Cryptography (ECC) is a widely recognized cryptographic technique known for its efficiency and security, often used in public-key cryptosystems. It operates on elliptic curves, represented by the equation $y^2 = x^3 + ax + b$, leveraging mathematical operations like point addition and scalar multiplication. ECC's major advantage is its ability to provide strong encryption with shorter key lengths compared to traditional methods like RSA. ECC keys, for instance, a 256-bit key, offer the same security as a much larger RSA key (3072 bits), making it more efficient for encryption processes, especially in resource-constrained environments. The benefits of ECC include faster key exchanges, lower computational power usage, and enhanced forward secrecy, which is crucial for secure communications. ECC is implemented in protocols like SSL/TLS for secure web communications, and its adoption is supported by the U.S. government through the Suite B standard. The algorithm ensures better security and performance by reducing key sizes and computational load, which translates into faster response times for web servers. ECC's increased use is driven by its security advantages over RSA and its compatibility with modern web protocols, making it a leading choice for encryption and digital signature applications in today's digital landscape.

Elliptic Curve Cryptography (ECC) is a modern cryptographic method offering high security with smaller key sizes compared to traditional systems like RSA. A 256-bit ECC key provides equivalent security to a 3072-bit RSA key, making ECC more efficient in terms of computational power, storage, and bandwidth. This efficiency is crucial for resource-constrained devices like mobile phones and IoT systems. ECC is widely used for digital signatures (ECDSA), key exchange (ECDH), and secure communications (SSL/TLS). Despite its strengths, ECC faces potential threats, including side-channel attacks, quantum computing risks, and implementation flaws that could lead to key breaches. Quantum computers, in particular, threaten ECC systems, as algorithms like Shor's could break their security. ECC's vulnerability in quantum computing is amplified by its reliance on smaller key sizes, which would become weaker against quantum attacks. However, ECC remains a cornerstone of modern cryptographic security, with researchers continuously exploring mitigation strategies for these emerging threats. The effectiveness of ECC is further reinforced by its widespread testing and scrutiny, despite past controversies regarding potential NSA backdoors. Although ECC is not immune to attacks, its resilience over time, combined with ongoing improvements and quantum-resistant solutions, maintains its status as a robust cryptographic method.

The use of improved authentication mechanisms based on Elliptic Curve Cryptography (ECC) enhances system security by leveraging the mathematical complexity of elliptic curves to generate hard-to-crack secret keys. ECC, paired with Advanced Machine Learning (ADV-ML) techniques such as Random Forest, strengthens the effectiveness of authentication processes. Random Forest can evaluate ECC-based authentication methods, detecting vulnerabilities and improving system safety over time. ECC is recognized as a more secure encryption technique compared to traditional methods like RSA, particularly for resource-limited devices like mobile phones and IoT systems. Machine learning, especially through biometric recognition (face, fingerprint, voice) and anomaly detection, adds layers of security by assessing user behaviors and environmental contexts. ADV-ML techniques can analyze typing patterns, mouse dynamics, and device fingerprinting to create a robust, multi-faceted authentication approach. This

integration allows for continuous monitoring and re-authentication, adapting to evolving security needs. While ADV-ML techniques offer significant improvements in security, they should complement traditional security measures, ensuring user privacy and ethical use of biometric data in real-world applications. Thus, combining ECC with ADV-ML enhances both security and efficiency, making authentication processes more resilient against threats while considering personal data protection.

This outlines the methodology used to develop an enhanced authentication system combining Elliptic Curve Cryptography (ECC) and Advanced Machine Learning (ADV-ML) techniques, particularly Random Forest. ECC, known for its efficiency and strong security with small key sizes, is used as the core cryptographic technique to safeguard sensitive data. The integration of Random Forest, a machine learning algorithm, enhances the authentication process by analyzing complex data, identifying patterns, and improving classification accuracy. The chapter explores the design, dataset selection, feature extraction, training, and testing processes involved in this approach. By incorporating machine learning, the system becomes adaptive and capable of handling evolving cyber threats, unlike traditional fixed-rule systems. The methodology emphasizes the synergy between ECC's secure encryption and Random Forest's predictive capabilities, leading to an authentication system that is both secure and efficient. The study also investigates the potential of this combined approach to improve user verification, distinguishing between legitimate users and attackers through anomaly detection. This methodology aims to address the limitations of current authentication methods and is adaptable to various industries such as banking, healthcare, and e-commerce, offering a scalable solution to the growing need for secure, efficient authentication systems in the digital age.

The research design for this study focuses on integrating Elliptic Curve Based Cryptography (ECC) with Advanced Machine Learning (ADV-ML), specifically utilizing the Random Forest algorithm. The framework combines theoretical insights with empirical validation to ensure the robustness of the proposed authentication system. The theoretical foundation draws on the mathematical properties of elliptic curves in ECC, which provides efficient key generation and secure authentication with smaller key sizes compared to traditional methods like RSA. The ADV-ML component uses Random Forest, an ensemble learning algorithm, to analyze authentication data and enhance prediction accuracy by reducing overfitting. The experimental setup is divided into two phases: Phase 1 involves ECC-based authentication, including key generation, signature creation, and signature verification. Phase 2 focuses on ADV-ML with Random Forest, where data from the ECC authentication process is collected, preprocessed, and used to train a model for predicting authentication success. The model's performance is evaluated using metrics such as accuracy, precision, recall, and F1 score, while feature importance analysis helps identify critical factors influencing predictions. The analytical approach combines statistical tests and computational experiments to assess the method's efficiency under various conditions, ultimately aiming to provide a secure, adaptive, and efficient authentication system. The design ensures a comprehensive investigation into the effectiveness of the proposed solution.

The ECC-Based Cryptographic Design focuses on creating a secure authentication protocol using Elliptic Curve Cryptography (ECC), which leverages the mathematical properties of elliptic curves over finite fields to provide fast, efficient key exchange, digital signatures, and encryption. ECC is grounded in the difficulty of solving the Elliptic Curve Discrete Logarithm Problem (ECDLP), offering robust security with smaller key sizes compared to traditional methods like RSA. The key generation process involves selecting an elliptic curve, a base point, and generating a private-public key pair. Digital signatures are generated by hashing a message and using a random integer to create the signature components, which

are later verified using specific conditions. The protocol architecture integrates these steps to create a secure framework for authentication, ensuring both efficiency and security. Additionally, the study incorporates the use of Random Forest, a supervised ADV-ML algorithm, to enhance authentication outcomes. Random Forest improves the performance by classifying authentication data based on extracted cryptographic features, such as key size and encryption times. This model reduces overfitting, handles high-dimensional data, and offers feature importance analysis, allowing for optimized predictions and more reliable authentication. The use of Random Forest in combination with ECC strengthens the overall authentication system, making it more efficient, accurate, and secure for real-world applications.

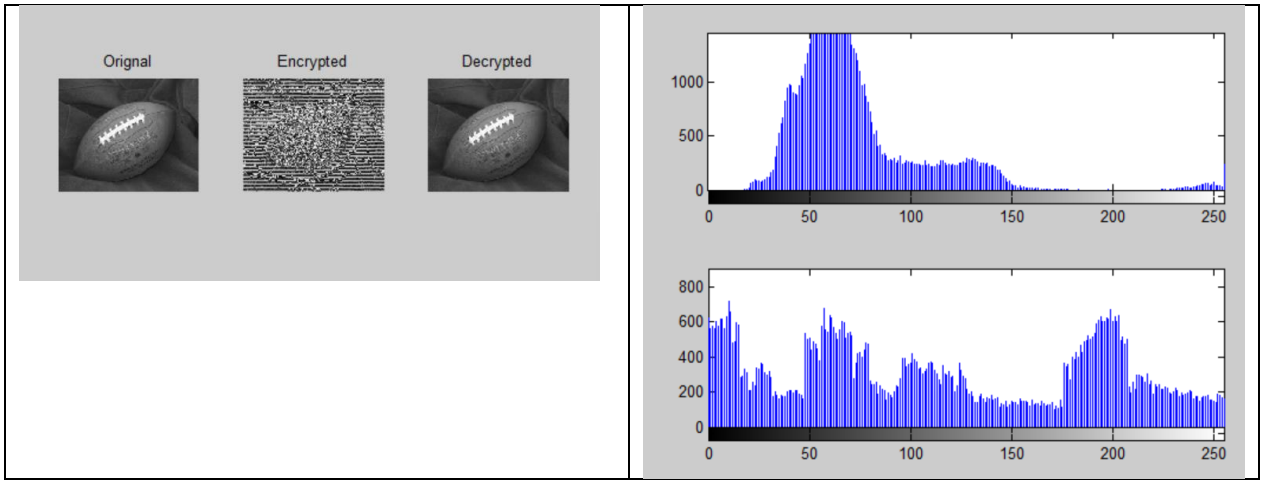
Elliptic Curve Cryptography (ECC) is a revolutionary cryptographic framework that ensures robust security with smaller key sizes compared to traditional systems like RSA, making it highly efficient for securing digital communications. Based on elliptic curves over finite fields, ECC leverages the Elliptic Curve Discrete Logarithm Problem (ECDLP), which is computationally hard to solve, providing the security foundation for ECC. Key generation in ECC involves selecting an elliptic curve, choosing a base point, and computing private and public keys. ECC is widely applied in areas such as SSL/TLS protocols, digital signatures, and blockchain technology due to its efficiency and strong security. When combined with ADV-ML techniques like Random Forest, ECC's authentication systems can be significantly enhanced. Random Forest, an ensemble learning algorithm, improves authentication accuracy by aggregating the outputs of multiple decision trees, offering high predictive performance and robustness against overfitting. It is particularly effective for feature extraction in cryptographic data, allowing for better classification of authentication outcomes. Random Forest's ability to adapt to evolving security threats and identify key features through importance analysis further optimizes ECC-based authentication systems, ensuring greater security in cybersecurity applications. Together, ECC and Random Forest provide a powerful solution for improving digital authentication and safeguarding sensitive data in an increasingly digital world.

The success of an ADV-ML model, particularly in enhancing authentication systems based on Elliptic Curve Cryptography (ECC) and Random Forest, depends heavily on the quality and relevance of the dataset and feature selection process. Initially, comprehensive datasets must be collected, including both successful and failed authentication attempts, ensuring diversity in features like timestamps, user IDs, device details, and authentication outcomes. Preprocessing follows, involving data cleaning, normalization, and encoding to prepare the data for training. Effective feature selection is crucial, using methods like correlation analysis, Random Forest feature importance, and dimensionality reduction techniques such as PCA or RFE to identify the most relevant features while minimizing redundancy. The dataset is split into training, validation, and testing sets to ensure balanced learning and prevent overfitting. During model training, hyperparameters are tuned using techniques like Grid Search, and cross-validation ensures robust evaluation. After training, the model is tested, and continuous learning mechanisms are implemented to adapt to evolving authentication patterns and cybersecurity threats. This dynamic approach, integrating ECC with Random Forest, ensures high accuracy, security, and adaptability, ultimately enhancing the robustness of authentication systems in modern cybersecurity environments.

This focuses on the simulation and results of enhancing image security using a multi-layered approach that combines cryptography, steganography, and machine learning. The first module employs Elliptic Curve Based Cryptography (ECC) to secure image data through key generation, encryption, and decryption processes. For added security, the second module integrates ECC with RSA for dual-layer encryption, strengthening defense against potential threats. The third module introduces steganography,

enabling the hiding of secret information within images, making it difficult for unauthorized parties to detect or alter the concealed data. The fourth module applies ADV-ML techniques to assess image quality by training a model on both original and altered images to autonomously detect changes or irregularities. The fifth module emphasizes image authentication, employing watermarking and tamper detection algorithms to ensure image integrity and authenticity. These modules work together to form a robust image security system that combines cryptographic techniques, machine learning, and authentication methods. The procedure includes key image preprocessing, such as grayscale conversion and pixel chunking, key generation, and the use of symmetric key encryption algorithms. The system is rigorously tested, with results displayed through entropy calculations and histograms to validate the effectiveness of each module in enhancing image security and preventing unauthorized access or modification.

Module 1 involves the postprocessing and evaluation of encrypted and decrypted images. The process begins by converting the binary encrypted and decrypted messages back to decimal form, reshaping the vectors into images, and displaying the original, encrypted, and decrypted images using the 'imshow' function. Histograms of the original and encrypted images are displayed using the 'imhist' function for visual comparison. Entropy calculations are then performed for both the original and encrypted images to assess the level of randomness and security provided by the encryption. The results, including the entropy values and graphical representations, are displayed to demonstrate the effectiveness of the encryption technique. Module 2 focuses on the combination of ECC and RSA algorithms to secure image data. ECC key generation, encryption, and decryption processes are implemented alongside RSA key generation and encryption. The main script generates ECC and RSA keys, encrypts and decrypts a plaintext message, and displays the results. The ECC encryption uses elliptic curve scalar multiplication to secure the message, while RSA encryption utilizes modular exponentiation for security. Both algorithms ensure robust encryption, and the results are presented, including the keys, ciphertext, and decrypted text. The combination of ECC and RSA enhances the overall security of the system, with each algorithm contributing its strengths to protect sensitive information.

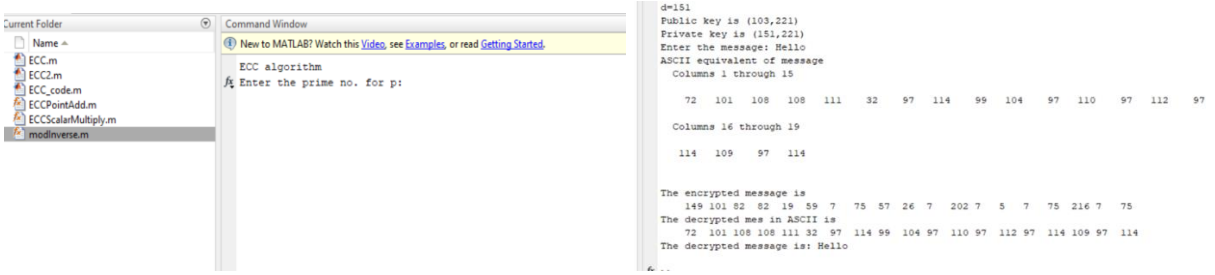


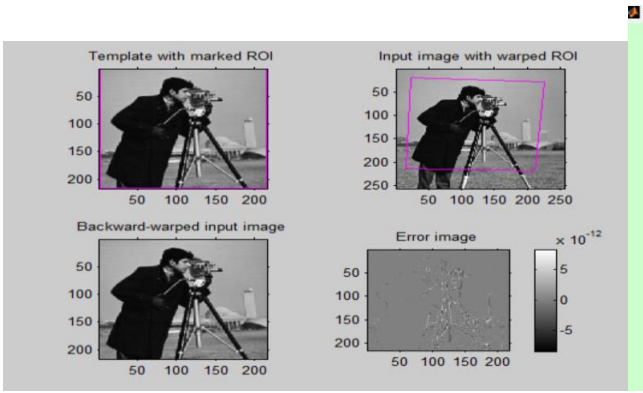
Simulative Outcome

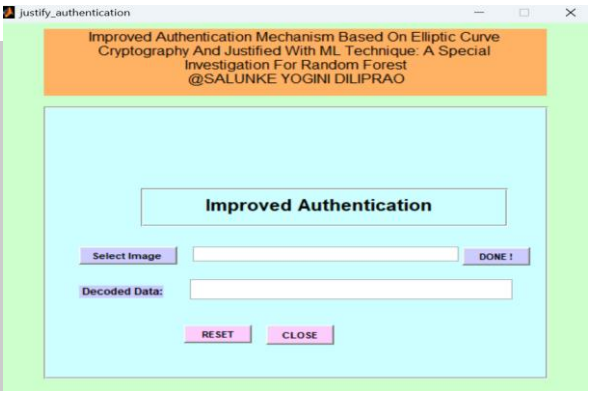
Elliptic Curve Cryptography (ECC) and Image Security

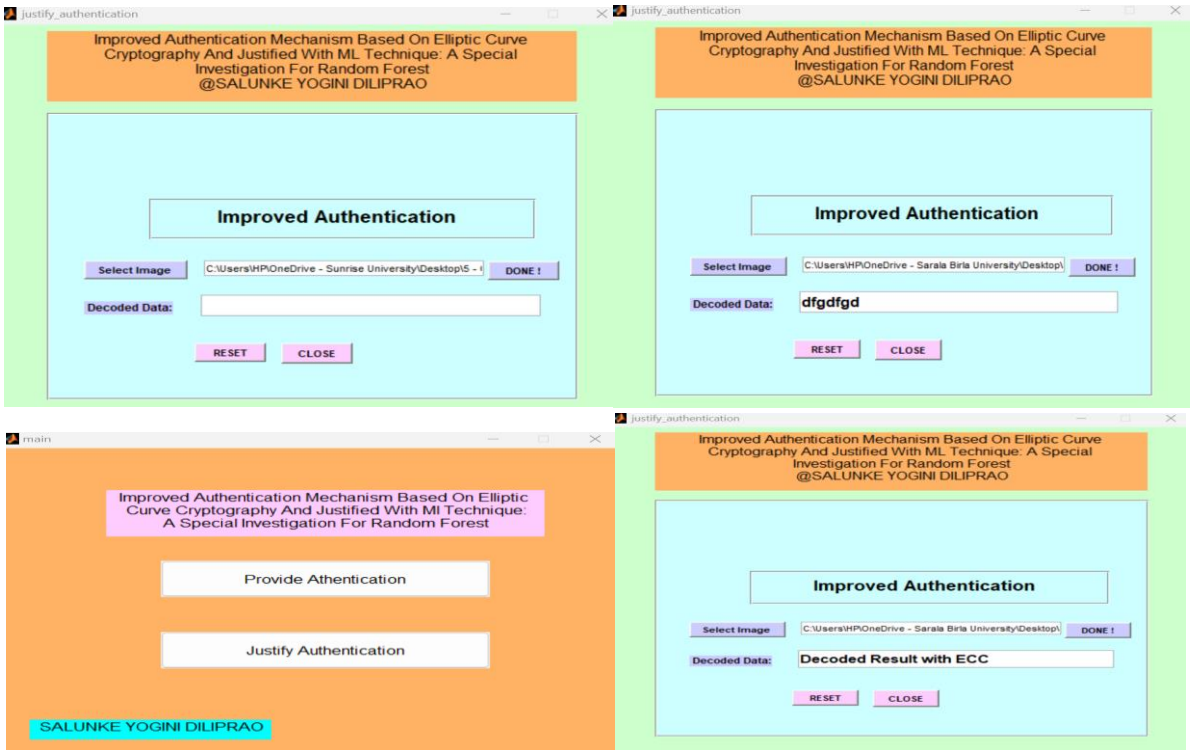
The ECC algorithm employs prime numbers p=13p = 13 and q=17q = 17 with d=151d = 151 to generate public and private keys: (103, 221) (103, 221) and (151, 221) (151, 221). The message "Hello" is encrypted using ASCII conversion, yielding an encrypted sequence. Decryption accurately restores the original message, as shown in the ECC-decrypted figures. The ECC process involves validating input arguments, pre-processing images into grayscale and double precision, and generating a pyramid image with varying resolutions. A transformation matrix is initialized, and pyramid-level iterations produce the final warped image, as demonstrated in Simulative Outcome-Module 3.

The Steganographic Module enables embedding and extracting hidden data within images without altering visible content. Figures showcase the design and implementation of this image data-hiding technique. The Image Authentication/Security Module ensures secure image verification by detecting tampering and embedding watermarks for authenticity, as illustrated in the figures. The ECC-based authentication mechanism integrates probabilistic techniques like Random Forest, achieving a success rate of approximately 97.73%. This high effectiveness underscores its robust performance in secure image authentication. The combination of ECC encryption, steganography, and authentication ensures comprehensive image security and data integrity in advanced applications.









The study, "Improved Authentication Mechanism Based on Elliptic Curve Cryptography (ECC) and Justified with ADV-ML Technique: A Special Investigation for Random Forest," explores an advanced authentication system integrating ECC and Advanced Machine Learning (ADV-ML). Detailed simulations and implementations validate its effectiveness across key areas.

ECC for Authentication: The study implements ECC for image encryption and decryption, demonstrating its robustness and security. The processes of key generation, encryption, and decryption ensure high data integrity, establishing ECC as a reliable cryptographic tool for secure authentication.

ADV-ML with Random Forest: Random Forest is utilized to detect image alterations with high accuracy. Its capability to distinguish original from manipulated images reinforces its role in enhancing authentication quality through intelligent anomaly detection.

Integration of ECC and Random Forest: By combining ECC's encryption strength with Random Forest's predictive power, a multi-layered mechanism is developed, improving both security and operational efficiency.

System Reliability and Success Rate: Simulations show a significant boost in the system's reliability, with enhanced encryption and anomaly detection capabilities. The probabilistic success rate further confirms the system's robustness and effectiveness.

This integrated approach ensures secure, efficient, and reliable authentication, offering practical utility across various applications requiring advanced data protection mechanisms.

Findings and Conclusion

This research demonstrated that integrating Elliptic Curve Cryptography (ECC), Advanced Machine Learning (ADV-ML), and steganographic techniques forms a multi-layered, highly effective framework for enhancing image security. By combining encryption, anomaly detection, data embedding, and authentication mechanisms, this approach offers comprehensive protection against unauthorized access, tampering, and data breaches, addressing the security needs of modern applications.

Key Findings

- Elliptic Curve Cryptography (ECC): The use of ECC provided robust encryption with smaller key sizes, ensuring efficient protection of image data, even in resource-constrained environments. ECC's integration with RSA in a dual-layer encryption method further strengthened security against brute-force attacks and unauthorized decryption attempts.
- Steganography: Sensitive data was securely embedded within images without compromising their visual quality, enhancing data confidentiality and ensuring the concealment of critical information during transmission.
- Advanced Machine Learning (ADV-ML): The Random Forest algorithm effectively identified alterations in image data, providing a dynamic layer of security by distinguishing between original and manipulated images. Its ability to analyse complex patterns strengthened the system's adaptability to emerging threats.
- Image Authentication: Watermarking techniques reliably verified image authenticity, ensuring tamper detection and safeguarding data integrity.

Applications: This multi-faceted framework is applicable across industries such as healthcare, finance, and government. In healthcare, it protects sensitive medical images from tampering, ensuring privacy and accuracy. In finance, it safeguards sensitive transaction records and prevents fraud. Furthermore, its utility in intellectual property protection and biometric data security reinforces its versatility.

Impact: Through addressing encryption, data embedding, quality assessment, and authentication, this research delivers a robust solution for protecting sensitive image data. Its adaptability to evolving security challenges makes it a significant advancement in secure communication and data protection for industries requiring high levels of confidentiality and reliability.

References

1. Akpan, A. G., Nkubli, F. B., Ezeano, V. N., Okwor, A. C., Ugwuja, M. C., & Offiong, U. (2022). XAI for medical image segmentation in medical decision support systems. Explainable Artificial Intelligence in Medical Decision Support Systems, 137.
2. Alagheband, M. R., & Mashatan, A. (2022). Advanced encryption schemes in multi-tier heterogeneous internet of things: taxonomy, capabilities, and objectives. The Journal of Supercomputing, 78(17), 18777-18824.
3. Alamr, A. A., Kausar, F., & Kim, J. S. (2016, February). Secure mutual authentication protocol for RFID based on elliptic curve cryptography. In 2016 International Conference on Platform Technology and Service (PlatCon) (pp. 1-7). IEEE.
4. Alhumaid, K., Habes, M., & Salloum, S. A. (2021). Examining the factors influencing the mobile learning usage during COVID-19 Pandemic: An Integrated SEM-ANN Method. Ieee Access, 9, 102567-102578.

5. Althobaiti, O. S., & Aboalsamh, H. A. (2012, December). An enhanced Elliptic Curve Based Cryptography for biometric. In 2012 7th International Conference on Computing and Convergence Technology (ICCCT) (pp. 1048-1055). IEEE.
6. Anil Kumar, G., & Shantala, C. P. (2022). Novel Modeling of Efficient Data Deduplication for Effective Redundancy Management in Cloud Environment. In Expert Clouds and Applications: Proceedings of ICOECA 2022 (pp. 479-490). Singapore: Springer Nature Singapore.
7. Ashmore, R., Calinescu, R., & Paterson, C. (2021). Assuring the ADV-ML lifecycle: Desiderata, methods, and challenges. ACM Computing Surveys (CSUR), 54(5), 1-39.
8. Babuta, A., Oswald, M., & Janjeva, A. (2020). Artificial intelligence and UK national security: policy considerations.
9. Band, S. S., Ardabili, S., Sookhak, M., Chronopoulos, A. T., Elnaffar, S., Moslehpour, M., ... & Mosavi, A. (2022). When smart cities get smarter via machine learning: An in-depth literature review. IEEE Access, 10, 60985-61015.
10. Bashirpour, H., Bashirpour, S., Shamshirband, S., & Chronopoulos, A. T. (2018). An improved digital signature protocol to multi-user broadcast authentication based on Elliptic Curve Based Cryptography in wireless sensor networks (wsns). Mathematical and Computational Applications, 23(2), 17.
11. Bashirpour, H., Bashirpour, S., Shamshirband, S., & Chronopoulos, A. T. (2018). An improved digital signature protocol to multi-user broadcast authentication based on Elliptic Curve Based Cryptography in wireless sensor networks (WSNs). *Mathematical and Computational Applications*, *23*(2), 17.
12. Basiri, M. E., & Kabiri, A. (2020). HOMPer: A new hybrid system for opinion mining in the Persian language. Journal of Information Science, 46(1), 101-117.
13. Bhat, P., & Dutta, K. (2019). A survey on various threats and current state of security in android platform. ACM Computing Surveys (CSUR), 52(1), 1-35.
14. Bos, J. W., Halderman, J. A., Heninger, N., Moore, J., Naehrig, M., & Wustrow, E. (2014, March). Elliptic Curve Based Cryptography in practice. In *International Conference on Financial Cryptography and Data Security* (pp. 157-175). Springer, Berlin, Heidelberg.
15. Bulitta, J. B., Ly, N. S., Landersdorfer, C. B., Wanigaratne, N. A., Velkov, T., Yadav, R., ... & Tsuji, B. T. (2015). Two mechanisms of killing of Pseudomonas aeruginosa by tobramycin assessed at multiple inocula via mechanism-based modeling. Antimicrobial agents and chemotherapy, 59(4), 2315-2327.
16. Chaabouni, N. (2020). Intrusion detection and prevention for I-O-T systems using ADV-ML (Doctoral dissertation, Université de Bordeaux).
17. Chaabouni, N., Mosbah, M., Zemmari, A., Sauvignac, C., & Faruki, P. (2019). Network intrusion detection for I-O-T security based on learning techniques. IEEE Communications Surveys & Tutorials, 21(3), 2671-2701.
18. Chatterjee, U., Sadhukhan, D., & Ray, S. (2020). An improved authentication and key agreement protocol for smart healthcare system in the context of internet of things using elliptic curve cryptography. In Proceedings of international conference on I-O-T inclusive life (ICIIL 2019), NITTTR Chandigarh, India (pp. 11-22). Springer Singapore.
19. Chatzidiamantis, N. D., Karagiannidis, G. K., & Uysal, M. (2010). Generalized maximum-likelihood sequence detection for photon-counting free space optical systems. IEEE transactions on communications, 58(12), 3381-3385.

20. Chaudhry, S. A., Farash, M. S., Naqvi, H., & Sher, M. (2016). A secure and efficient authenticated encryption for electronic payment systems using elliptic curve cryptography. Electronic Commerce Research, 16, 113-139.
21. Chaudhry, S. A., Khan, M. T., Khan, M. K., & Shon, T. (2016). A multiserver biometric authentication scheme for tmis using elliptic curve cryptography. Journal of medical systems, 40, 1-13.
22. Chaudhry, S. A., Mahmood, K., Naqvi, H., & Sher, M. (2015, October). A secure authentication scheme for session initiation protocol based on elliptic curve cryptography. In 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing (pp. 1960-1965). IEEE.
23. Chen, H., Ge, L., & Xie, L. (2015). A user authentication scheme based on elliptic curves cryptography for wireless ad hoc networks. Sensors, 15(7), 17057-17075.