Comprehensive Image Security: ECC, RSA, Steganography, ML Quality, and Authentication System

Gajanan Rajaram Jadhav[1], Dr. Vinod Kumar[2]

[1]Research Scholar
[2]Department Of Mathematics
[1,2]sunrise University

Abstract

Our image security initiative has developed a robust system through a multifaceted approach, integrating Elliptic Curve Cryptography (ECC), two-layer encryption, steganography, machine-based quality estimation, and image authentication. The first module utilizes ECC for its strong encryption capabilities, securing sensitive image data through key generation, encryption, and decryption. The second module enhances security with a two-layer encryption combining ECC and RSA, leveraging both algorithms to fortify encryption strength and resilience. The third module incorporates steganography, embedding secret information within image pixels to add an extra layer of protection. The fourth module features a machine learning-based quality assessment system, which detects image manipulation by analysing quality metrics with advanced algorithms. Lastly, the fifth module focuses on image authentication through watermarking and tamper detection, ensuring the integrity and authenticity of images. The integrated system offers a seamless user experience with an intuitive interface for encryption, decryption, and other functions. Rigorous testing and deployment have confirmed its reliability and adaptability. As technology evolves, this advanced image security system will continue to address emerging digital security challenges and maintain the confidentiality, integrity, and authenticity of digital information across various industries.

Keywords: Elliptic Curve Cryptography, two-layer encryption, steganography, machine learning, watermarking.

INTRODUCTION

This research highlights the very important function that pictures play in the display of information as well as the need of ensuring that image transmission is safe. Elliptic Curve Cryptography (ECC), which was created in 1985 by Neal Koblitz and Victor S. Miller and gained significant awareness around the year 2004, is emphasized as an excellent option. The exponential complexity of ECC's solution to the elliptic curve discrete logarithmic issue is its greatest strength. As a result, it offers superior security for picture encryption and decryption in comparison to other cryptographic approaches [1]. In its conclusion, the research reaffirms the relevance and dependability of ECC in modern applications, therefore establishing it as a preferable option for preserving the secrecy and security of pictures that are transferred.

Image analysis: Image analysis, which is frequently referred to as "computer vision" or image recognition, is the ability of computers to identify qualities that are included inside an image. There is another name for image analysis, which is "computer vision." Text analysis was the first step in the development of social media analytics, and it continues to be the major emphasis of this field today [2]. On the other hand, image analysis is becoming an increasingly important area within the discipline of computer science. An extension of the qualities of text analysis, picture analysis is the application of such characteristics to visual content. The same purpose is performed by image analysis when it is applied to the examination of social media information. Through the use of the same classification algorithms, it is possible to do analysis on photographs [3]. It is possible for object recognition to display all of the posts that include images of a computer, rather than requiring us to go through all of the posts that contain the word "computer."

The topic of image analysis is a multidisciplinary one that involves a wide range of methods and procedures with the purpose of extracting meaningful information from visual data. Image analysis has become more important in a variety of fields, including medicine, computer vision, remote sensing, and others. This is due to the ever-changing environment of technology and data science, which has led to an increase in the significance of image analysis. The use of complex algorithms and computational approaches is required in this all-encompassing subject in order to analyze, comprehend, and gain insights from pictures [4-8]. These images may be photos, medical scans, satellite imagery, or any other visual representation.

Pre-processing procedures are often the first step in the process of image analysis. During these processes, pictures are improved, normalized, and prepared for further analysis. It is essential to complete these preliminary procedures in order to guarantee that the ensuing algorithms will function on high-quality data that is devoid of any distortions or noise. After the pre-processing step, the feature extraction step is very important since it involves locating and quantifying the key qualities that are present in the photos. A wide variety of features might be present, ranging from basic components such as color and texture to more intricate structures such as forms and patterns [9-14].

The incorporation of machine learning strategies is one of the most important developments in the field of image analysis. Machine learning algorithms, and deep learning models in particular, have shown exceptional performance in a variety of tasks, including image identification, object detection, and segmentation. When it comes to image analysis, Convolutional Neural Networks (CNNs), which are a sort of deep learning architecture, have gained a lot of popularity owing to their capacity to automatically generate hierarchical representations of features straight from the input.

The influence has had a revolutionary effect on the field of medical image analysis throughout this time. A paradigm change has occurred in a number of medical professions, including pathology, radiology, and others, as a result of the development of image analysis tools. Computer-aided diagnostic (CAD) systems, which are enabled by image analysis, provide assistance to medical practitioners in the early identification of diseases, the categorization of medical problems, and the planning of therapy [15-17]. Not only can the use of artificial intelligence into medical imaging increase diagnosis accuracy, but it also improves efficiency, which enables medical professionals to concentrate on more intricate elements of patient care.

In addition to its use in the medical field, image analysis is also an essential component of computer vision applications. Object detection and tracking, autonomous cars, and face recognition systems are just a few examples of the ways in which image analysis algorithms contribute to applications in the real world. Image analysis is a technique that is used in the field of remote sensing and satellite photography to aid environmental monitoring, disaster management, and urban planning [18]. The adaptability and effectiveness of image analysis in tackling difficult issues across a variety of fields is shown by these applications.\

RESEARCH METHODOLOGY

Research Methodology: For the purpose of enhancing the safety of pictures, the purpose of this research project is to examine a variety of image cryptography algorithms and to implement Elliptic Curve Cryptography (ECC). The purpose of this study is to investigate the efficacy of ECC in encrypting and decrypting pictures while maintaining their integrity and secrecy. In addition, this suggested goal evaluates the integrity of the decryption process in comparison to the original photographs and provides an evaluation of the quality of the recovered images. It is the goal of this study to achieve these goals in order to give insights into the resilience and dependability of Encased picture security approaches, therefore contributing to the progress of techniques for image encryption and quality assessment. A strong combination that may be used to secure and evaluate the security of pictures is the enhancement of image security via the use of the Elliptic Curve Cryptography (ECC) technology and the evaluation of image quality through the use of machine learning methodology. In order to accomplish the goal of this research, there are four major steps that must be taken. The first step is the collection of images, the second step is the application of elliptic curve cryptography (ECC) for image security, the third step is the estimation of image quality using machine learning in addition to the standard parameters, and the fourth step is the integration of ECC and test images [19-20]. The steganography procedure should next be carried out utilizing the Secure cover selection method.

SIMULATION AND RESULT

The Elliptic Curve Cryptography (ECC) technique is used in the first module of this study. This complete strategy to improving picture security is being investigated. The use of this cryptographic method guarantees the security of the encryption and decryption operations, hence protecting the data images. The ECC procedure encompasses key creation, encryption, and decryption, which demonstrates its effectiveness in protecting sensitive information from unauthorized access.

In order to strengthen picture security, the second module employs a dual-layer encryption technique that combines ECC and RSA technologies. This combination strengthens the encryption, which guarantees a robust protection against any prospective dangers that may arise with the future. inside the third lesson, a steganographic technique is presented, which may be used to conceal information inside photographs and then retrieve it later. In order to give an extra degree of protection, this module conceals data under a cover picture. This makes it difficult for unauthorized entities to discover or change anything that is disguised.

The fourth module makes use of machine learning methods in order to estimate the quality of the product. After training a model on a dataset consisting of both the original and altered photos, the system is able to independently evaluate image quality, recognizing any changes or irregularities that may have occurred. In order to improve image security, this intelligent quality assessment brings a fresh and original perspective to the table

Image authentication is the primary emphasis of the fifth module, which also includes identification of tampering and watermarking processes. Through the incorporation of one-of-a-kind watermarks and the use of tamper detection algorithms, the system guarantees the authenticity of photographs, hence allowing users to verify material in a dependable manner. This comprehensive strategy combines the power of cryptography, the intelligence of machine learning, and authentication procedures to provide a strong solution for the advancement of picture security.

PROCEDURE

Elliptic Curve Cryptography (ECC)

- Generate ECC keys (private and public) for image encryption.
- Implement ECC encryption and decryption procedures.
- Execute the ECC algorithm on image data, securing it against unauthorized access.

Dual-Layer Encryption (ECC + RSA)

- Combine ECC with RSA for enhanced encryption.
- Generate RSA keys and integrate them with ECC for dual-layer security.
- Implement RSA encryption and decryption to complement ECC.

Steganography

- Develop a steganographic algorithm for hiding information within images.
- Embed a secret message or image into the cover image using the steganographic technique.
- Implement extraction methods to retrieve the hidden content.

Machine Learning for Quality Estimation

- Create a dataset with original and manipulated images.
- Train a machine learning model to distinguish between original and altered images.
- Implement the model to autonomously assess image quality.

Image Authentication

- Incorporate watermarking techniques to uniquely mark each image.
- Develop tamper detection mechanisms to identify any unauthorized alterations.
- Implement authentication verification processes to ensure image integrity.

Integration and Testing

- Integrate all modules into a cohesive image security system.
- Conduct comprehensive testing to validate the effectiveness of each module and their interactions.

User Interface (UI) Development

- Design a user-friendly interface for easy interaction with the image security system.
- Include features for key input, encryption/decryption, steganography, and quality assessment.

pseudo-code

```
// Preprocessing
Load the image (football.jpg)
Convert the image to grayscale if it is a color image
Scale the image to 8-pixel chunks, each pixel represented by 8 bits
Convert the image data to binary
// Key Generation
Set the hexadecimal key: hex_key = '133457799bbcdff1'
Convert the hexadecimal key to binary: bin_key = Hex2Bin(hex_key)
Generate sub-keys: [K1, K2, K3, K4, K5] = SF_Key_Gen(bin_key)
// Encryption and Decryption
for each 8-bit chunk in the binary image data
Encrypt the chunk using sub-keys: cipher = SF_Encrypt(chunk, K1, K2, K3, K4, K5)
Decrypt the cipher using sub-keys: plaintext = SF_Decryption(cipher, K1, K2, K3, K4, K5)
Store the original, encrypted, and decrypted messages
// Postprocessing
If padding is used, remove the padding from the messages
Reshape the vectors into images: Orignal, Encrypted, Decrypted
// Display Results
Display the original, encrypted, and decrypted images using imshow
Display histograms of the original and encrypted images using imhist
// Entropy Calculation
Calculate the entropy of the original and encrypted images
// Display Entropy Results
The entropy values that were generated for both the original and encrypted photos should be shown.
```

In order to offer a high-level overview of the functionality of the MATLAB code, this pseudo-code is described. Specifically, it presupposes that the functions Hex2Bin, SF_Key_Gen, SF_Encrypt, SF_Decrypt, Scalling, convert2bin, Binary2Dec, and imhist are adequately implemented in other places.

CONCLUSION

In the course of our efforts to improve picture security by using a diverse strategy, we have developed a system that is both resilient and comprehensive. The combination of Elliptic Curve Cryptography (ECC), dual-layer encryption, steganography, quality estimate based on machine learning, and picture authentication procedures has resulted in the creation of a complex defensive mechanism that can protect against a wide range of security threats. This all-encompassing solution not only protects picture data from being accessed by unauthorized parties, but it also facilitates the verification of authenticity, the detection of tampering, and the evaluation of image quality via the use of sophisticated algorithms. In the first lesson, the emphasis was placed on ECC, which is a robust encryption method that is well-known for its effectiveness in protecting digital data. The generation of ECC keys, the encryption of picture data, and the implementation of decryption procedures were the means by which we secured the security of a framework for the protection of sensitive visual information. This established a baseline for cryptographic security, which set the groundwork for additional advancements to be implemented thereafter. Through the implementation of a dual-layer encryption method, which included the combination of ECC and the robust RSA algorithm, we were able to strengthen the security of images in the second module. With the help of this hybrid method, the capabilities of both cryptographic approaches were harnessed, which resulted in an additional enhancement of the encryption strength and resistance against prospective assaults. The combination of Elliptic Curve Cryptography (ECC) and Random Number Generator (RSA) resulted in the creation of a robust defense, which made it very difficult for attackers to crack the encrypted pictures' security.

REFERENCES

1. Singh, L. D., & Singh, K. M. (2015). Image encryption using elliptic curve cryptography. Procedia Computer Science, 54, 472-481.
2. Zhang, X., & Wang, X. (2018). Digital image encryption algorithm based on elliptic curve public cryptosystem. IEEE Access, 6, 70025-70034.
3. Kumar, N., Triwedi, P., & Rathore, P. S. (2017). An Adaptive Approach for image adaptive watermarking using Elliptical curve cryptography (ECC). In ICITKM (pp. 89-92).
4. Kolhekar, M., & Jadhav, A. (2011). Implementation of elliptic curve cryptography on text and image. International Journal of Enterprise Computing and Business Systems, 1(2), 1-13.
5. Hureib, E. S., & Gutub, A. A. (2020). Enhancing medical data security via combining elliptic curve cryptography and image steganography. Int. J. Comput. Sci. Netw. Secur.(IJCSNS), 20(8), 1-8.
6. Tawalbeh, L. A., Mowafi, M., & Aljoby, W. (2013). Use of elliptic curve cryptography for multimedia encryption. IET Information Security, 7(2), 67-74.
7. Astya, P., Singh, B., & Chauhan, D. (2014, October). Image encryption and decryption using elliptic curve cryptography. In proceedings oN IJARSE (Vol. 3, No. 10).
8. Gupta, N., Kundu, V., Kurra, N., Sharma, S., & Pal, B. (2015, January). Elliptic curve cryptography for ciphering images. In 2015 International Conference on Electrical, Electronics, Signals, Communication and Optimization (EESCO).
9. Rajvir, C., Satapathy, S., Rajkumar, S., & Ramanathan, L. (2020). Image encryption using modified elliptic curve cryptography and Hill cipher. In Smart Intelligent Computing and Applications: Proceedings of the Third International Conference on Smart Computing and Informatics, Volume 1 (pp. 675-683). Springer Singapore.
10. Arun, C., Basha, S. H., Sivakumar, D. L., Rizwan, M. M., & Kumar, M. P. (2020). Secured Image Transmission Using Elliptic Curve Cryptography (ECC).
11. Li, L., Abd El-Latif, A. A., & Niu, X. (2012). Elliptic curve ElGamal based homomorphic image encryption scheme for sharing secret images. Signal Processing, 92(4), 1069-1078.
12. Nagaraj, S., Raju, G. S. V. P., & Rao, K. K. (2015). Image encryption using elliptic curve cryptograhy and matrix. Procedia Computer Science, 48, 276-281.
13. Gupta, N., & Vyas, R. R. (2017). Image encryption using elliptic curve cryptography. International Journal of Innovation & Advancement in Computer Science, 6(9).
14. Nagaraj, S., & Raju, G. S. V. P. (2015). Image security using ECC approach. Indian Journal of Science and Technology, 8(26), 1-5.
15. Hureib, E. S. B., & Gutub, A. A. (2020). Enhancing medical data security via combining elliptic curve cryptography with 1-LSB and 2-LSB image steganography. International J Comp Sci Network Security (IJCSNS), 20(12), 232-241.
16. Reyad, O., Khalifa, H. S., & Kharabsheh, R. (2019). Image pixel permutation operation based on elliptic curve cryptography. J. Appl. Math. Inf. Sci, 13(S1), 183-189.
17. Yin, S., Liu, J., & Teng, L. (2020). Improved Elliptic Curve Cryptography with Homomorphic Encryption for Medical Image Encryption. Int. J. Netw. Secur., 22(3), 419-424.
18. Khoirom, M. S., Laiphrakpam, D. S., & Themrichon, T. (2018). Cryptanalysis of multimedia encryption using elliptic curve cryptography. Optik, 168, 370-375.
19. Goon, S., Pal, D., Dihidar, S., Nath, S., & Mondal, A. (2018). ENHANCED VISUAL CRYPTOGRAPHY NETWORK (EVCN) FOR SECURED DATA TRANSMISSION COMBINING DES AND ELLIPTIC CURVE CRYPTOGRAPHY. Computer.
20. Reyad, O., & Kotulski, Z. (2015). Image encryption using koblitz's encoding and new mapping method based on elliptic curve random number generator. In Multimedia Communications, Services and Security: 8th International Conference, MCSS 2015, Kraków, Poland, November 24, 2015. Proceedings 8 (pp. 34-45). Springer International Publishing.