Vol 6, Issue 6, 2023 **Impact Factor: 5.355** DOI: https://doi.org/10.31426/ijamsr.2023.6.6.6416

IJAMSR

International Journal of
Advanced Multidisciplinary Scientific Research (IJAMSR) ISSN:2581-4281

Use Of Elliptic Curve Cryptography Model for Images Analysis and Stenographic Modelling

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

[1] Research Scholar, Dept. Of Mathematics, Sunrise University, Alwar, Rajasthan
[2] Dept. Of Mathematics, Sunrise University, Alwar, Rajasthan

Email: Gajwinjadhav@Gmail.Com

ABSTRACT

This comprehensive program protects image data from unauthorized access and provides methods for authentication, tamper detection, and image quality assessment using intelligent algorithms. The first module focuses on ECC; a powerful encryption algorithm known for its power in securing digital data. By generating ECC keys, encrypting image data, and using decryption procedures, we have ensured a secure framework for protecting sensitive physical information. This forms the basis of cryptographic security. In the second module, we strengthened image security by introducing a two-layer encryption strategy, which combines ECC with a strong RSA algorithm. This hybrid approach utilized the strengths of both cryptographic techniques, improving encryption strength and resilience against potential attacks. The combination of ECC and RSA creates a formidable defense, making it more challenging for adversaries to compromise the security of encrypted images. Going beyond encryption, the third module delved into steganography, a secret communication technique that hides information within the pixels of an image. By embedding private messages or images within the cover image, we introduce an extra layer of security. This method hides sensitive information and makes it difficult for unauthorized entities to access or manipulate hidden content, thereby improving the overall security posture. In the fourth module, we introduced a quality measurement system based on machine learning. Using advanced algorithms and carefully selected datasets, our system automatically checks image quality. This innovation is important in identifying possible manipulation or modification of images. A machine learning model, trained on a diverse set of images, provides intelligent ways to check the authenticity of visual content, accompanied by cryptographic and steganographic layers of security.

Keywords:* *ECC And RSA Encryption, Steganography, Image Quality Assessment, Machine Learning, Tamper Detection.

1. INTRODUCTION

This study emphasizes the crucial role of images in information display and the need for their secure transmission. It highlights Elliptic Curve Cryptography (ECC) as an excellent choice for encrypting and decrypting images [1-3]. ECC, developed by Neal Koblitz and Victor S. Miller in 1985 and popularized in 2004, is valued for its complexity, which strengthens its security [4-8]. The study concludes that ECC is highly suitable for protecting the privacy and security of transmitted images.

1.1 Image Analysis

Image analysis, also known as computer vision or image recognition, involves computers recognizing features within images [9-15]. It's an extension of text analysis and is becoming increasingly important in fields like medicine, remote sensing, and computer science.

Key Steps in Image Analysis:

1. Pre-processing: Enhancing and normalizing images to ensure high-quality data for further analysis.
2. Feature Extraction: Identifying and quantifying important qualities in images, ranging from basic elements like color and texture to complex structures like patterns and forms [16-20].

Machine Learning in Image Analysis:

The use of machine learning, particularly deep learning models like Convolutional Neural Networks (CNNs), has revolutionized image analysis [21-24]. These algorithms excel in tasks such as image classification, object detection, and segmentation by automatically extracting and interpreting features from images.

Applications:

- Medical Field: Image analysis tools aid in early disease diagnosis, medical problem classification, and treatment planning. These tools improve diagnostic accuracy and efficiency [25-30].
- Forensic Systems: In forensic applications, image analysis supports object detection, tracking, and facial recognition. It's also crucial in the development of autonomous vehicles.

2. LITERATURE REVIEW

Duan et al. (2020), Steganography is a method that may be used to conceal sensitive information inside a picture when it is handled appropriately. Steganography of images is one example of such a technique. picture steganography is a time-honored technology that involves the process of discretely and safely incorporating concealed information into the picture representing the host. As a consequence of this, the payload capacity is almost entirely disregarded, and the Human Vision System (HVS) has to be upgraded in order to enhance the quality of the steganographic picture. Furthermore, as a consequence of this, we describe in this study a novel approach to picture steganography that is based on deep learning and is very effective. Discrete Cosine convert (DCT) is used in order to convert the secret picture, and Elliptic Curve Cryptography (ECC) is utilized in order to encrypt the altered image in order to raise the resistance of the received image to being discovered. The Senet Deep Neural Network, which was designed to improve steganographic capacity and comes equipped with Hiding and Extraction Networks, makes it possible to do steganography and extract full-size images. The results of the experiments demonstrate that this technique is capable of effectively allocating each pixel in the picture in such a way that the relative capacity of steganography approaches 1. Furthermore, the picture that was produced by using this steganography technique has excellent values of Peak Signal-to-Noise Ratio (PSNR) and Structural Similarity Index (SSIM), both of which are equal to or greater than 40 decibels.

Hureib & Gutub (2020), Keeping medical information and records secret and preventing them from being hacked are the goals of the study, which includes techniques to secure sensitive information using encryption and encryption. These tactics are described in the paper. The creation of two layers, one of which use elliptic curve cryptography and the other of which employs picture steganography as a technique of encryption, is essential to accomplishing this goal. As a first phase, the process of encrypting text using ECC is referred to as the first layer. The second layer, on the other hand, refers to the process of concealing the encrypted text inside the picture utilizing steganography images with 1-LSB and 2-LSB as the second step. The use of Elliptic Curve Cryptography (ECC), which is a public key encryption technique that is based on the algebraic structure of elliptic curves over finite fields, seems to be a good alternative for public key. Specifically, this is due to the fact that ECC offers a means for public key encryption. In addition to this, it may be used in a variety of other forms of media, including X-rays, CT scans, and MRI scans, all of which are utilized in the medical recording system as well as in the field. Choosing Image Steganography is a method that is used to prohibit a third party from accessing or quickly locating overlay data, which includes encrypted information. There is another name for this technique, which is picture steganography. When it comes to steganography, the Least Significant Bit technique is an excellent choice since it is a simple steganographic approach with a low degree of complexity. This makes it an interesting option to consider. In this study, we investigate two distinct varieties of steganography, namely 1-LSB and 2-LSB, to determine the distinctions that exist between them and to get a better understanding of the benefits and drawbacks associated with each type. It is possible for any individual, group of individuals, or business to use this strategy in order to conceal and safeguard vital firm information, as well as national secrets, laboratory secrets, and other essential information that characterizes the organizations.

Olaniyi et al. (2015), The difficulty of maintaining the security of information and communication technology (e-voting) has been recognized as the most significant impediment that stands in the way of the widespread use of electronic voting. Previous cryptographic models are susceptible to assault, while modern steno-cryptographic versions are susceptible to modification by an eavesdropper. Secure electronic voting does not possess this vulnerability. Because of these vulnerabilities in the secure electronic voting models that are now in use, there is a potential threat to the secrecy, integrity, and authentication of electronic votes. All of these aspects are essential to the overall success of e-democratic decision-making via electronic voting. The goal of this study is to develop a sophisticated steno-cryptographic model for a safe electronic voting system that can be used in polling stations, online voting settings, and mobile voting environments. This will be done with the intention of increasing the number of people who participate in digital democracy elections and guaranteeing that they are dependable. For the purpose of encrypting the electronic vote, the techniques of Rivest-Sharma-Adleman and Elliptic Curve Cryptography were used. The voter's vote that had been encrypted was decoded and encrypted with the Most Significant Bit (LSB) of the cover location. This was accomplished by using the location concealing information of the modified LSB-Wavelet steganographic technique. Quantitative methods such as Peak Signal to Noise Ratio (PSNR), Signal to Noise Ratio (SNR), Root Mean Square Error (RMSE), and Structural Similarity Index Metrics were used in order to evaluate the picture quality of both the model and the actual object. These measures were used in order to evaluate the quality of the picture (SSIM). The results of the quantitative performance test indicate that the steno-cryptographic model that was developed has the general feature of secure electronic voting. This is an essential characteristic for the supply of trustworthy electronic democratic decision-making. For the purpose of providing electronic voting with a high degree of electoral integrity and political legitimacy, it would be beneficial to apply the idea on a big scale. Real electronic elections will be conducted for the people with the authority of the government, as a result of this development.

Shanthakumari and Malliga (2020), Steganography is an excellent method for concealing the transfer of secret information in order to ensure that it is received by an authorized recipient while still preserving a high degree of security. As a result, this helps avoid breaches in data security. In this day and age, the need of establishing stringent security measures in the field of data transmission has become a tough job owing to the challenges associated to security that are exacerbated by unwanted intrusion. In light of the fact that there are now more data breaches than there have ever been before, the work is made more difficult. The purpose of this presentation is to propose a unique approach that is based on a combination of steganography and encryption methods to embed hidden data in a cover object. Additionally, the presentation intends to get a big capacity for embedding data while maintaining an elevated degree of security. These objectives are going to be accomplished via the use of this presentation. As part of this approach, the Elliptic Curve Cryptography technique is used to encrypt not just the data that is concealed from view but also the data that has been encrypted by using the LSB Inversion algorithm. After that, the cover object is loaded with both sets of encrypted data before being used. The combination of these technologies has been able to effectively meet the standards for a number of essential aspects, including data confidentiality, integrity assurance, capacity, and durability. The construction of these structures is evidence that demonstrates the most effective performance of this steganography technology and the successful execution of it. This brand-new tactic was put through extensive testing on a variety of steganographic assaults, such as visual, histogram, and chi-square analysis. The conclusion that was obtained from the results of the test demonstrated that the mental image offered a tremendous defensive force that was successful in all assaults. Currently, the power of data embedding has attained a high degree of success in comparison to other strategies.

Kaliswaran & Parvees (2020), Over the course of the last few years, there has been a substantial rise in the quantity of digital photos that have been made. As a result, there is a need to ensure the safety of images on the internet in order to communicate confidential information over the network. Because of this, it is necessary to put various image protection measures into effect. The protection of multimedia data is accomplished by the use of cryptography, which has been shown to be an easy and effective way. It is possible to solve the optimization issue that is the process of creating an appropriate key for use in cryptography by using metaheuristic algorithms. This procedure is considered to be a problem. This action is carried out concurrently with the sentence that came before it. As a consequence of this, the primary focus of this investigation is on the creation of a metaheuristic optimization technique that employs cryptographic encryption in order to safeguard photographs. According to this point of view, the objective of this study is to create an efficient hybrid of the Cat Swarm optimization algorithm (CSO) and the fruit fly optimization algorithm (FFO) and ECC for the goal of guaranteeing the safety of images. The CSO-FFO-ECC model is the name given to the model that is produced as a consequence of this combination. Modeling the encryption and decryption processes is accomplished via the use of the ECC technique. Choosing the ideal key for the suggested model is accomplished via the use of a mix of the CSO technique and the FFO algorithm. It is done in this manner in order to cut down on the amount of time that the computer has to spend selecting public and private keys at random. During the process of scanning and extracting pictures, it takes into consideration the "fitness function" as the primary key using PSNR, and it accomplishes both of these tasks. The experimental validation of the CSO-FFO-ECC model is carried out on the data obtained from the benchmark test pictures. a citation is required. An examination of the data is carried out with regard to the peak signal-to-noise ratio (PSNR) and the mean square error (MSE).

3. CONCLUSION

We have developed an advanced image security system that integrates multiple strategies for robust protection. Our approach combines Elliptic Curve Cryptography (ECC) with a two-layer encryption method that includes RSA, enhancing image security against unauthorized access and potential attacks [31-36]. Steganography is also employed to conceal information within image pixels, adding another layer of protection by hiding data in plain sight [37-41]. Furthermore, our system incorporates a machine learning-based quality assessment module that evaluates image integrity, detecting alterations and ensuring authenticity [42-44]. This comprehensive solution not only secures image data but also verifies its quality and authenticity, using sophisticated algorithms to maintain high standards of protection and reliability.

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.
21. Vigila, S. M. C., & Muneeswaran, K. (2012). Nonce Based Elliptic Curve Cryptosystem for Text and Image Applications. Int. J. Netw. Secur., 14(4), 236-242.
22. Bos, J. W., Halderman, J. A., Heninger, N., Moore, J., Naehrig, M., & Wustrow, E. (2014). Elliptic curve cryptography in practice. In Financial Cryptography and Data Security: 18th International Conference, FC 2014, Christ Church, Barbados, March 3-7, 2014, Revised Selected Papers 18 (pp. 157-175). Springer Berlin Heidelberg.
23. CHOUDHARY, M. (2015). ELLIPTIC CURVE CRYPTOGRAPHY ON AN IMAGE (Doctoral dissertation).
24. Pardesi, V., & Khamparia, A. (2015). Encryption/Decryption of X-Ray Images Using Elliptical Curve Cryptography with Issues and Applications. In Emerging ICT for Bridging the Future-Proceedings of the 49th Annual Convention of the Computer Society of India CSI Volume 2 (pp. 357-365). Springer International Publishing.
25. Ponmani, E., Nandhini, E., Karthika, K., & Saravanan, P. (2018). Secured Transmission of a compressed image by using ECC. International Journal of Pure and Applied Mathematics, 119(12), 13387-13396.
26. Rajendran, S., Abilashaa, S., & Doraipandian, M. (2019). Elliptic curve blended cross chaos based secure image communication. Int. J. Recent Technol. Eng., 8, 4481-4.
27. Reyad, O., Kotulski, Z., & Abd-Elhafiez, W. M. (2016). Image encryption using chaos-driven elliptic curve pseudo-random number generators. Appl. Math. Inf. Sci, 10(4), 1283-1292.
28. Chowdhary, C. L., Patel, P. V., Kathrotia, K. J., Attique, M., Perumal, K., & Ijaz, M. F. (2020). Analytical study of hybrid techniques for image encryption and decryption. Sensors, 20(18), 5162.
29. Zhao, Z., & Zhang, X. (2013). ECC-based image encryption using code computing. In Proceedings of the 2012 International Conference on Communication, Electronics and Automation Engineering (pp. 859-865). Springer Berlin Heidelberg.
30. Jinasena, T., Meegama, R., & Marasinghe, R. (2017). Access Control of Medical Images using Elliptic Curve Cryptography through Effective Multi-Key Management in a Mobile Multicasting Environment. Comput. Sci. Eng, 7, 1-7.
31. Rajam, S. T. R., & Kumar, S. B. R. (2015). Enhanced elliptic curve cryptography. Indian Journal of Science and Technology, 8(26), 1-6.
32. Althobaiti, O. S., & Aboalsamh, H. A. (2012, December). An enhanced elliptic curve cryptography for biometric. In 2012 7th International Conference on Computing and Convergence Technology (ICCCT) (pp. 1048-1055). IEEE.
33. Lara-Nino, C. A., Diaz-Perez, A., & Morales-Sandoval, M. (2018). Elliptic curve lightweight cryptography: A survey. IEEE Access, 6, 72514-72550.

34. Prakash, G., & Kannan, M. (2013). ENHANCING SECURITY IN CRYPTOGRAPHIC SMART CARDS THROUGH ELLIPTIC CURVE CRYPTOGRAPHY AND OPTIMIZED MODIFIED MATRIX ENCODING ALGORITHMS. Journal of Theoretical & Applied Information Technology, 58(3).
35. Jagdale, B. N., Bedi, R. K., & Desai, S. (2010). Securing MMS with high performance elliptic curve cryptography. International journal of computer applications, 8(7), 17-20.
36. Almajed, H., Almogren, A., & Alabdulkareem, M. (2020). iTrust—A Trustworthy and Efficient Mapping Scheme in Elliptic Curve Cryptography. Sensors, 20(23), 6841.
37. Singh, R., Chauhan, R., Gunjan, V. K., & Singh, P. (2014). Implementation of elliptic curve cryptography for audio-based application. International Journal of Engineering Research & Technology (IJERT), 3(1), 2210-2214.
38. Sehar, M. (2019). Elliptic Curve Based Multi Secret Image Sharing (Doctoral dissertation, CAPITAL UNIVERSITY).
39. Kalra, S., & Sood, S. K. (2011, July). Elliptic curve cryptography: survey and its security applications. In Proceedings of the international conference on advances in computing and artificial intelligence (pp. 102-106).
40. Sharma, B., & Delhi, R. (2013). Security architecture of cloud computing based on elliptic curve cryptography (ECC). International Journal of Advances in Engineering Sciences, 3(3), 58-61.
41. Duan, X., Guo, D., Liu, N., Li, B., Gou, M., & Qin, C. (2020). A new high-capacity image steganography method combined with image elliptic curve cryptography and deep neural network. *IEEE Access*, *8*, 25777-25788.
42. Olaniyi, O. M., Arulogun, O. T., Omidiora, E. O., & Okediran, O. O. (2015). Enhanced stegano-cryptographic model for secure electronic voting.
43. Shanthakumari, R., & Malliga, S. (2020). Dual layer security of data using LSB inversion image steganography with elliptic curve cryptography encryption algorithm. *Multimedia Tools and Applications*, *79*(5), 3975-3991.
44. Kaliswaran, S., & Parvees, M. M. (2020). An Efficient Hybrid Optimization Algorithm with Elliptic-Curve Cryptography for Image Encryption. *European Journal of Molecular & Clinical Medicine*, *7*(07).