International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

ECC with Steganography for Higher Security And Estimation of Image Quality Using Machine Learning

Archana Singh Parmar[1], Dr. Bijendra Singh[2]

[1]Assitant professor TIT&S Bhiwani
[2]Professor BMU Rohtak

ABSTRACT:
As intruders are getting smarter and we want to disguise the fact that anything secret is being transmitted, today's largest challenge when sending data to anyone is to ensure that no one can read our message. So authentication , integrity and confidentiality principals should be achieved to secure our data fully so in this paper we have combined the encryption with steganography and then performed the image quality estimation using machine learning to know the difference between the cover image and processed image .

Keywords: ECC, Stegnography, image quality, machine learning

I. INTRODUCTION

The objective of this research project is to investigate various image cryptography techniques and apply Elliptic Curve Cryptography (ECC) to enhance the security of images. The research aims to explore the effectiveness of ECC in encrypting and decrypting images while ensuring confidentiality and integrity. Additionally, this proposed objective estimate the quality of the recovered images and assess the fidelity of the decryption process compared to the original images. By achieving these objectives, the research aims to provide insights into the robustness and reliability of ECC-based image security methods, contributing to the advancement of image encryption and quality evaluation techniques. Enhancement of image security through the Elliptic Curve Cryptography (ECC) method and estimation of image quality using machine learning is powerful combination to protect and assess the security of images. This research has four major steps to achieve the objective as one is collection of images, second is apply the Elliptic Curve Cryptography (ECC) for Image Security, third is Estimation of Image Quality using Machine Learning as well as the standard parameters and the final forth is Integration of ECC and test images.

2. Elliptic Curve Cryptography (ECC) for Image Security:

ECC is a widely used public-key cryptography method that relies on the difficulty of the elliptic curve discrete logarithm problem for its security. It offers stronger security compared to traditional methods like RSA for the same key length. To enhance image security, we apply ECC in two main ways:

2.1. Encryption: Use ECC to encrypt the image data. The image will be converted into an array of bytes, and ECC used to encrypt this data. The recipient, who possesses the corresponding private key,

decrypt the image and view its content. This ensures that unauthorized individuals cannot access the image without the private key.

2.2. Digital Signature: ECC used to create digital signatures for images. A digital signature provides authentication, integrity, and non-repudiation. The sender generate a digital signature using their private key, and the receiver verify the signature using the sender's public key to ensure the image has not been tampered with and is indeed from the claimed sender.

3. Stegnography for enhanced Security:

Steganographic techniques have been used for centuries. Steganography has been widely used in historical times, especially before cryptographic systems were developed. Secrets can be hidden inside all sorts of cover information. The following formula provides a very generic description of the pieces of the steganographic process:

cover_medium + hidden_data + stego_key = stego_medium

3.1Image Steganography:

The most widely used technique today is hiding of secret messages into a digital image. This steganography technique exploits the weakness of the human visual system (HVS). HVS cannot detect the variation in luminance of color vectors at collection of color pixels. The individual pixels can be represented by their optical higher frequency side of the visual spectrum. A picture can be represented by a characteristics like 'brightness', 'chroma' etc. Each of these characteristics can be digitally expressed in terms of 1s and 0s.

For example: a 24-bit bitmap will have 8 bits, representing each of the three color values (red, green, and blue)at each pixel. If we consider just the blue there will be 2 different values of blue. The difference between 11111111 and 11111110 in the value for blue intensity is likely to be undetectable by the human eye. Hence, if the terminal recipient of the data is nothing but human visual system (HVS) then the Least Significant Bit (LSB) can be used for something else other than color information.

4. Estimation of Image Quality using Machine Learning:

Assessing image quality is essential to ensure that the image content remains intact during encryption and decryption processes. Machine learning algorithms be trained to estimate image quality based on various image quality metrics, such as PSNR (Peak Signal-to-Noise Ratio), SSIM (Structural Similarity Index), and perceptual quality metrics like MSE (Mean Squared Error) and LPIPS (Learned Perceptual Image Patch Similarity).

4.1 Dataset Preparation: Gather a dataset of original images and their encrypted/decrypted versions. we need pairs of images to train the machine learning model to predict the image quality.

4.2 Feature Extraction: Extract relevant features from the images and calculate the image quality metrics mentioned above.

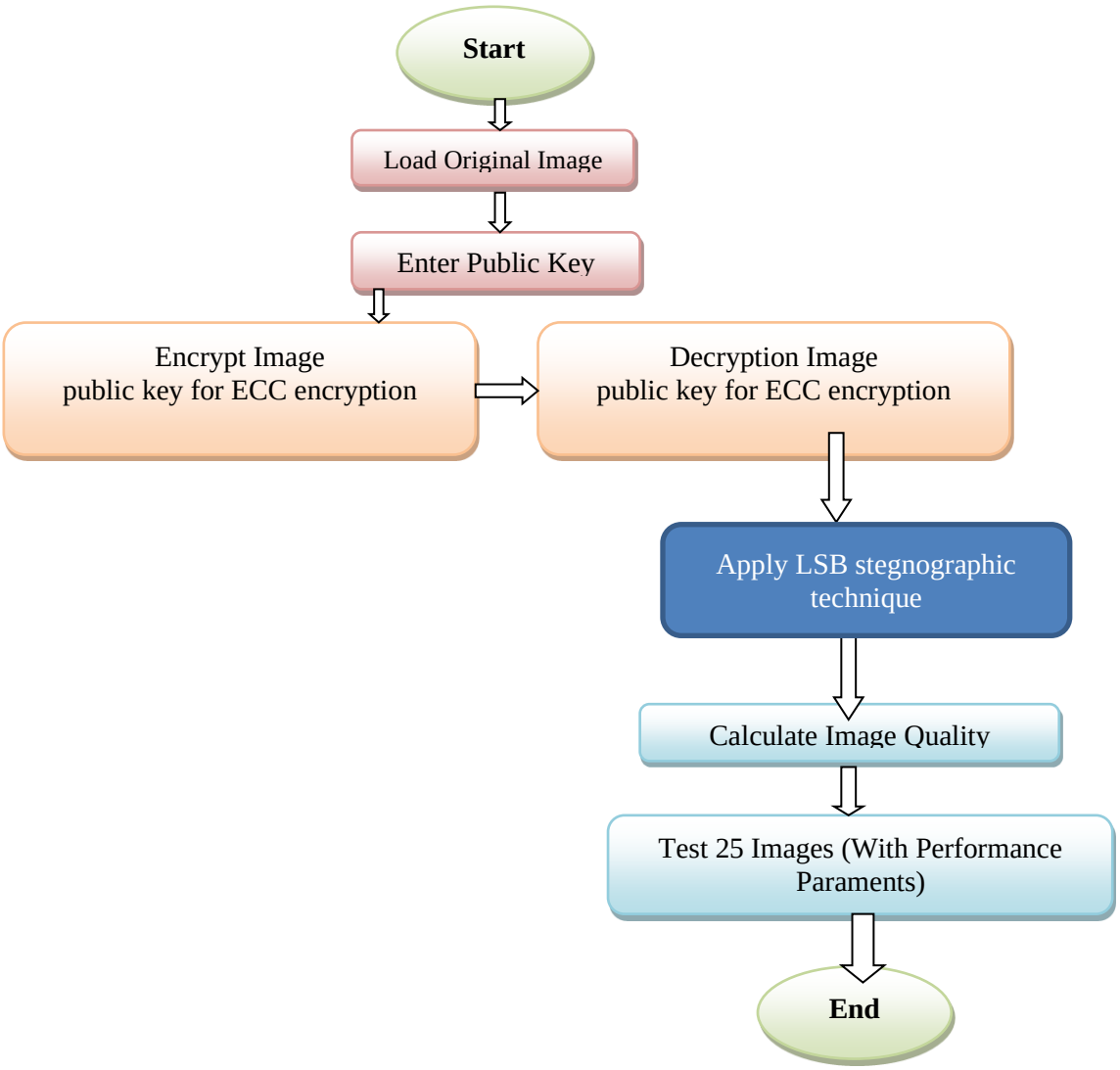
4.3 Model Training: Use supervised machine learning techniques to train a regression model that takes the extracted features as inputs and predicts the image quality metric (e.g., PSNR, SSIM) as the output.

4.4 Model Evaluation: Evaluate the trained model on a separate test dataset to ensure its accuracy in estimating image quality.

5. Integration of ECC with stegnography and test images

- ✓ Select a set of 25 test images to assess the effectiveness of ECC encryption and decryption process.
- ✓ Apply ECC encryption to the test images using the same public keys used in Step 2.
- ✓ Apply LSB stegnographic technique to hide the data
- ✓ Retrieve data at receiver end
- ✓ Decrypt the encrypted test images using the corresponding private keys.
- ✓ Use the trained machine learning model from Step 3 to estimate the image quality of the decrypted test images and compare it with the ground truth data.
- ✓ Analyze the results to assess the security and fidelity of the ECC-based image encryption.

After encrypting an image using ECC,and applied LSB stegnographic technique we use the trained machine learning model to estimate its quality. If the estimated quality falls below a predefined threshold, it might indicate that the image's quality has been significantly affected during the encryption process, potentially due to attacks or incorrect parameters. In such cases, we consider re-encrypting the image or taking necessary corrective actions. By combining ECC for image security, stenographic technique to hide message and machine learning for image quality assessment, we use ensure not only the confidentiality and integrity of the images but also evaluate their fidelity after encryption, providing a comprehensive approach to image security. The integration of ECC (Elliptic Curve Cryptography) in image security involves encrypting the original images using ECC with a public key and then decrypting them with the corresponding private key to restore the images. This process ensures confidentiality and integrity during image transmission or storage. Additionally, a set of 25 test images is used to evaluate the effectiveness of the ECC encryption and decryption process, with image quality metrics such as MSE, PSNR, and SSIM employed to assess the fidelity of the decrypted images compared to their originals.



6. Mathematical model for Image analysis

Assume that we have an original image represented by a two-dimensional matrix "M" of size H x W, where H is the height and W is the width of the image. Each element M(i, j) represents the pixel value at row "i" and column "j."

6.1 mage Encryption using ECC:

The encryption process represented as follows:

C(i, j) = E(M(i, j), PubK)

Above, C(i, j) is the encrypted pixel value, E() is the encryption function, M(i, j) is the original pixel value, and PubK is the public key used for encryption.

Image Decryption using ECC:

The decryption process represented as follows:

M_dec(i, j) = D(C(i, j), PrivK)

Above, M_dec(i, j) is the decrypted pixel value, D() is the decryption function, C(i, j) is the encrypted pixel value, and PrivK is the private key used for decryption.

6.2 Image Quality Estimation using Mathematical Model:

To estimate the image quality, we use a mathematical model that compares the original image "M" with the decrypted image "M_dec" and assigns a quality score "Q" based on the difference between the two images. One common method is Mean Squared Error (MSE), which measures the average squared difference between corresponding pixel values in the two images.

a) MSE = (1 / (H * W)) * ΣΣ((M(i, j) - M_dec(i, j))^2)

Here, MSE represents the Mean Squared Error, H and W are the height and width of the image, and the summation is performed over all pixels in the image.

b) Peak Signal-to-Noise Ratio (PSNR):

PSNR is another metric used for image quality estimation. It measures the ratio between the maximum possible pixel value and the MSE. The higher the PSNR, the better the image quality.

PSNR = 10 * log10((max_pixel_value^2) / MSE)

Above, max_pixel_value represents the maximum possible pixel value in the image (e.g., 255 for an 8-bit grayscale image).

c) Structural Similarity Index (SSIM):

SSIM is a more complex metric that considers structural information, luminance, and contrast of the images. It provides a more perceptually accurate quality assessment.

SSIM = (2 * μ_M * μ_M_dec + C1) * (2 * σ_M_M_dec + C2) / (μ_M^2 + μ_M_dec^2 + C1) * (σ_M^2 + σ_M_dec^2 + C2)

Above, μ_M and μ_M_dec are the means of the original and decrypted images, σ_M and σ_M_dec are the standard deviations, and C1 and C2 are constants to stabilize the division. The summations are calculated over all pixels.

By combining the encryption and decryption processes with ECC and using mathematical formulas to estimate image quality, we analysed the effectiveness of ECC-based encryption while quantifying the quality of decrypted images.

7. Conclusion:

By image quality estimation through different means we want to check the difference between the cover image and stegnographed image , as we are sure that security wise we are gaining strength , now no extruder can know the secret message and even they are not getting our encrypted text , but with these using image estimation technique , information entrphy will be calculated and difference will be noticed between two images so that further improvement can be done .

8. References:

1. Steganography and steganalysis-Robert Krenn, Internet Publication, March 2004
2. http://www.krenn.nl/univ/cry/steg/article.pdf
3. Steganography, http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci213717,00.html
4. Johnson, Neil F., "Steganography", 2000 http://www.jjtc.com/stegdoc/index2.html
5. The WEPIN Store, "Steganography (Hidden Writing)", 1995, http://www.wepin.com/pgp/stego.html
6. Abd EL-Latif, A. A., Abd-El-Atty, B., & Venegas-Andraca, S. E. (2019). A novel image steganography technique based on quantum substitution boxes. *Optics & Laser Technology*, *116*, 92-102.
7. Ahmed, D. E., & Khalifa, O. O. (2014, September). Robust and Secure Image Steganography Based on Elliptic Curve Cryptography. In *2014 International Conference on Computer and Communication Engineering* (pp. 288-291). IEEE.
8. Geethanjali, G., Ashwin, C., Bharath, V. P., Avinash, A., & Hiremath, A. (2021, June). Enhanced Data Encryption in IOT using ECC Cryptography and LSB Steganography. In *2021 International Conference on Design Innovations for 3Cs Compute Communicate Control (ICDI3C)* (pp. 173-177). IEEE.
9. Gladwin, S. J., & Gowthami, P. L. (2020, January). Combined cryptography and steganography for enhanced security in suboptimal images. In *2020 International Conference on Artificial Intelligence and Signal Processing (AISP)* (pp. 1-5). IEEE.
10. Gladwin, S. J., & Gowthami, P. L. (2020, January). Combined cryptography and steganography for enhanced security in suboptimal images. In *2020 International Conference on Artificial Intelligence and Signal Processing (AISP)* (pp. 1-5). IEEE.
11. Gupta, K., & Silakari, S. (2010, November). Performance analysis for image encryption using ecc. In *2010 International Conference on Computational Intelligence and Communication Networks* (pp. 79-82). IEEE.
12. Gupta, K., Silakari, S., Gupta, R., & Khan, S. A. (2009, July). An ethical way of image encryption using ECC. In *2009 First International Conference on Computational Intelligence, Communication Systems and Networks* (pp. 342-345). IEEE.
13. Hu, D., Wang, L., Jiang, W., Zheng, S., & Li, B. (2018). A novel image steganography method via deep convolutional generative adversarial networks. *IEEE Access*, *6*, 38303-38314.
14. 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.
15. 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.
16. Hussain, M., Wahab, A. W. A., Idris, Y. I. B., Ho, A. T., & Jung, K. H. (2018). Image steganography in spatial domain: A survey. *Signal Processing: Image Communication*, *65*, 46-66.
17. Kadhim, I. J., Premaratne, P., Vial, P. J., & Halloran, B. (2019). Comprehensive survey of image steganography: Techniques, Evaluations, and trends in future research. *Neurocomputing*, *335*, 299-326.
18. Liao, X., Yu, Y., Li, B., Li, Z., & Qin, Z. (2019). A new payload partition strategy in color image steganography. *IEEE Transactions on Circuits and Systems for Video Technology*, *30*(3), 685-696.
19. Lu, S. P., Wang, R., Zhong, T., & Rosin, P. L. (2021). Large-capacity image steganography based on

invertible neural networks. In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition* (pp. 10816-10825).

20. Mahalakshmi, U., & Sriram, V. S. (2013). An ECC based multibiometric system for enhancing security. *Indian Journal of Science and Technology*, *6*(4), 1-7.
21. Manjula, Y., & Shivakumar, K. B. (2020). Image Security Implementation and Cryptanalysis using ECC Cryptography, LSB-Watermarking Steganography. *SSAHE-JIR*, 67.
22. Mstafa, R. J., & Elleithy, K. M. (2016). An ECC/DCT-based robust video steganography algorithm for secure data communication. *Journal of Cyber Sec*

Authors Profile

1. IN Store, “Steganography (Hidden Writing)”, 1995, http://www.wepin.com/pgp/stego.html