IJITCE

ISSN 2347- 3657

# International Journal of Information Technology & Computer Engineering

Email : ijitce.editor@gmail.com or editor@ijitce.com

International Journal of
Information Technology & Computer Engineering

ISSN2347–3657

Volume13, Issue 1,2025

# A UNIQUE TECHNIQUE FOR MOBILE IMAGE ENCRYPTION

[1]KAVIDE CHANDU, [2]POOLA KISHORE, [3]GUNDREDDY ANVESH REDDY, [4]KASALA LAKSHMAN REDDY, [5]NALLA LAXMI ANUN, [6]Mrs. N.RADHAMMA, [7]Mr. SUBRAJITH SAHOO,

[12345]Student Department of DS, Narsimha Reddy Engineering College, Maisammaguda (V), Kompally, Secunderabad, Telangana-500100.

[6]Assistant Professor, Department of CSE, Narsimha Reddy Engineering College, Maisammaguda (V), Kompally, Secunderabad, Telangana-500100.

[7]Assistant Professor, Department of Mechanical Engineering, Narsimha Reddy Engineering College, Maisammaguda (V), Kompally, Secunderabad, Telangana-500100.

## Abstract—

Improvements in the realm of mobile apps are on the rise. In addition to their widespread usage on multi-platform mobile devices, Intruders may use comparable technologies to obfuscate their malevolent actions and conceal their identities. Accordingly, safety is paramount. To ensure the safe transfer of sensitive images across mobile nodes, this project prioritizes the use of precautionary encryption and decryption methods such as the PNSR metric and the elliptic curve digital signature algorithm. We will build a defensive app using these algorithms. This project aims to enhance secure transmission by using four distinct tiers of technology. Secret picture selection is the first level. File formats such as jpg and png will be compatible with the hidden image. Using an encryption technique, we encrypt the picture obtained from the first level in the second layer of security. In this case, the PSNR metric is used to quantify the picture quality. The third stage involves identifying the LSB and 3m (Mean, Mean, Mode) of the image in order to conceal the message within the cover image. The last step in security is to compress the resulting stegnographic picture using GZIP. To improve a security procedure, one uses an elliptic curve, which is a digital signature technique. Hence, this is the recommended way to transmit a covert message across critical mobile apps.

**Index Terms—Mobile application, Image Encryption, LSB, 3m,GZIP, Elliptic curve, Digital signature.**

## INTRODUCTION

A collection of technologies that allow users to exchange any kind of data with other devices that aren't physically connected to one another is called "mobile computing." a different one The data may be delivered wirelessly from any location in the globe, to put it simply. To make mobile computing work, you need these three things. They are the software and hardware components of mobile devices that allow users to establish connections. There will be no interruptions in communication thanks to the mobile communication framework's protocols, services, and other components. The primary factor contributing to the success of mobile computing is the portability and continuous internet connectivity of the hardware devices used in this technology [2].

The 1980s saw the beginning of the age of portable computing with the introduction of the first laptop computers. By 1990, thanks to a slew of hardware revisions and improvements, Apple introduced its 640*640 portable computers. Later on, in 1993, the first personal digital assistant (PDA) was introduced, and in 1994, IBM introduced the first smartphone. In the year 2000, smartphones were able to connect to networks. The following year, Apple introduced the iPhone, while Google built the first Android smartphone.

With each new version of the underlying software and hardware, the large variety of mobile computing devices becomes ever more extensive[3-5].

The number of people utilizing these portable computers is growing exponentially as their feature sets become more advanced. More over six billion smartphone subscriptions will be in place worldwide in 2022, and Statista projects that figure will rise by several hundred million in the next years, with the biggest growth anticipated in China, India, and the US[6]. The capacity of mobile phones has been extended, and they are utilized for more than just communication. Many people now utilize their cell phones as if they were personal assistants. Calls, payments, internet purchasing, information collecting, social networking, appointment scheduling, product orders, etc. are all done via these. On the one hand, there is the exponential development of technology, which begs the issue of how secure it really is [7,8]. Each party, the service provider and the endpoint, places equal emphasis on the security aspect. Attention to detail is required at every stage, including the hardware, software, and network components, when it comes to security. The term "hardware security" refers to the practice of safeguarding the actual machine itself against malicious actors. The term "software security" refers to measures taken to ensure the reliability, authenticity, and accessibility of software. In contrast, the goal of network security is to protect the media itself, the network. Data becomes more vulnerable when it is allowed to communicate to another device across a network. Data availability, integrity, and confidentiality are the three main concerns of security. Everyone can benefit from information. You can't just leave it in a network without doing anything; everybody in the network can see it. Within the realm of security, network security has emerged as a key topic. When information is sent from one location to another, it must be transmitted in a secure manner to ensure that it remains secret and is not altered or intercepted while in transit. Consequently, the data should only be sent via a secure channel during transmission. Multiple methods exist for ensuring transmission security. Firewalls, access controls, intrusion detection systems, steganographic methods, and cryptographic approaches may all help us to

## LITERATURE SURVEY

Security Methods for the Internet of Things—Cryptography and Steganography One way to secure data from prying eyes is via the elliptic Galois cryptography protocol.

or change while being transported. The XOR steganography matrix approach is also used with the safe cryptography methodology. The cover picture contains the hidden information thanks to these tactics. To choose the most suitable cover blocks from the picture, it also employs an optimization process known as Adaptive Firefly. The encrypted image's secret message will be safe during transmission over a network when using this technique [9]. B. An Innovative Method for Encrypting Images We will go over four different tiers of security. In order to alter the angles and forms of the hidden picture, the first level of mapping is applied: Conformal Mapping. Level 2 uses encoding methods, where the first level's picture is prepared for RSA encryption and decryption. To conceal the hidden message inside the cover picture, the third level employs the LSB concealing approach. Using the GZIP tool, the final steganographic picture is compressed at the fourth level [10]. (C) Steganography for Internet of Things Data Security

In order to conceal information in an IoT cover signal, this article utilizes a steganographic approach. The process culminates in the generation and transmission of a stenography signal across the IoT. Using low-frequency components of audio cover signals, such as speech and music, rather of high-frequency components, improves signal-to-noise (SNR) ratios. Its greater energy makes it a good medium for embedding data. In order to enhance the stenographic signal and decrease interference caused by hidden information, signal spectra are used. This attenuation results in a 13 dB reduction when compared to the original signal spectrum. For the steganography system to embed data that is resistant to purposeful removal efforts, we used a multi-key combination that takes into account factors including statistical undetectability, steganography signal quality[11], D. Digital Signatures for Data Security

One kind of signature that has found widespread usage in recent years for electronic document signing is the digital signature [12]. This technique is used in the present study. Like a physical signature, an electronic signature verifies the sender's identity and verifies the user's identity. In this article, we will go over the basics of RSA-based digital signature key creation. The process begins with the creation of signature keys and the generation of an RSA key pair using equation

$$ed \equiv 1 \mod \vartheta\ (N) \qquad (1)$$

Euler's totient function is determined by taking the product of two integers e and d, where N is a random, huge prime number. in such case the sender'sN and

$$\sigma \equiv md\ modN \qquad (2)$$

When sending a message, the sender uses the following equation to generate a signature: One subset of permutations is the trapdoor permutation. It has approach is computationally simple while looking ahead, but computationally challenging when looking backward. When the secret key is needed for the signing procedure, a digital signature using trapdoor permutations may be used, which involves doing computations backwards [13].

## OVERVIEW OF THE PROJECT

Many options exist for transmitting data securely. While data is encrypted before being sent to a network, there is still a chance that a when the hacker discovers the key, he may read and change the data. Methods for cautious encryption and decryption algorithms, such as the PNSR metric and the elliptic curve, are the primary emphasis of this system. Secure data transfer of a specific picture between mobile stations is made possible using a digital signature technique. A defensive app will be built using these algorithms. In order to enhance secure transmission, this project will use four distinct technological tiers. Chosen a covert picture is the first step. File formats such as jpg and png will be compatible with the hidden image. Using an encryption technique, we encrypt the picture obtained from the first level in the second layer of security.
The PSNR metric is used to quantify the picture quality in this case. The third stage involves identifying the LSB and utilizing 3m (Mean, Mean, Mode) to conceal the message within the cover image. The last step in ensuring the security of the steganographic picture is to compress it using GZIP. To fortify a safety procedure, one uses an elliptic curve digital signature technique. Hence, this is the recommended way to transmit a secret message across the mobile app's most important apps.

## TECHNOLOGIES PROPOSED

### *Subject: PSNR*

One way to measure the quality of a compressed picture is by looking at its peak signal-to-noise ratio, or PSNR. also a unique picture. The higher the PSNR score, the better the picture quality. In order to gauge the robustness of the cryptosystem, certain performance measures are used. We need knowledge of the MSE value in order to determine the PSNR value. Images' Mean Square Error (MSE) is all it is. The tool is used to *quantify the disparity between two pictures*.

$$MSE \equiv \sum_{M,N} \frac{[I1(m,n) - I2(m,n)]^2}{M * N} \qquad (4)$$

$$PSNR \equiv \log_{10} \frac{R^2}{MSE} \qquad (5)$$

The picture was distorted due to the signal-to-noise ratio. Decibels (dB) are used to measure the PSNR. Cryptography using Elliptic Curves Another kind of asymmetric cryptography is Elliptic Curve Cryptography, or ECC.

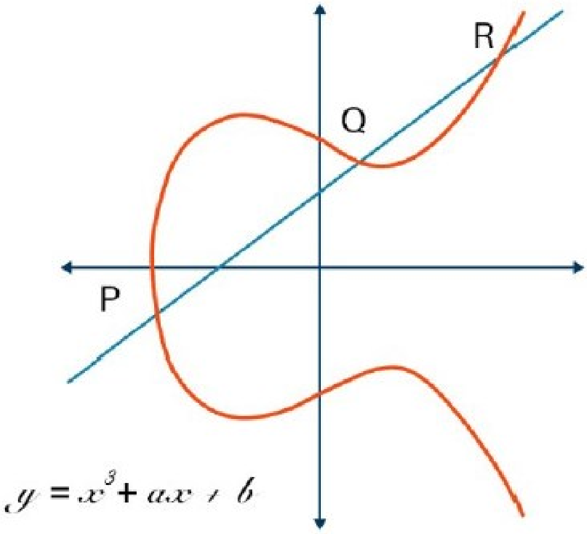

**Fig. 1. Elliptic curve.**

encryption method that entails using a public key for data encryption and a private key for decryption. It is among the strongest forms of encryption. Next up is ECC. encryption using public key technology. An alternate method to RSA is ECC. A mathematical notion derived from an elliptic curve is used to produce the keys. In order to generate keys, the picture depicts an elliptic curve with three randomly selected points P, Q, and R. While other cryptographic approaches use larger keys, ECC uses smaller ones and makes them more complicated, making cracking them mathematically impossible. Here is the representation of an elliptic curve ECC equation:

$$y^2 \equiv^2 + ax + b \qquad (6)$$

Part C: Electronic Identity

Data, software, and other digital documents may have their authenticity confirmed with the use of a digital signature.

reached a level of honesty and reliability. This is being accomplished by use of certain mathematical procedures.

1) To create a digital signature, one must adhere to these steps:

Data is transformed into a message digest when the hash function is applied to it. The digital signature is formed by encrypting this message digest and the sender's private key.

Next, the data is transferred to the recipient accompanied with a digital signature.

The opposite party, the receiver, will get the message digest along with the public key, which is used to decipher the digital signature. Because no one other than the sender has the private key needed to encrypt the hash—and only the sender has the public key—verifying the signature ensures its legitimacy.

- The receiver has now acquired the message digest and may use it to calculate the hash value.
- To make sure the data is intact, we check the hash value before and after transmission. Additionally, time stamps will be appended to the signature. Any changes made to the document after the digital signature is made will render the signature invalid.

## METHODOLOGY PROPOSED

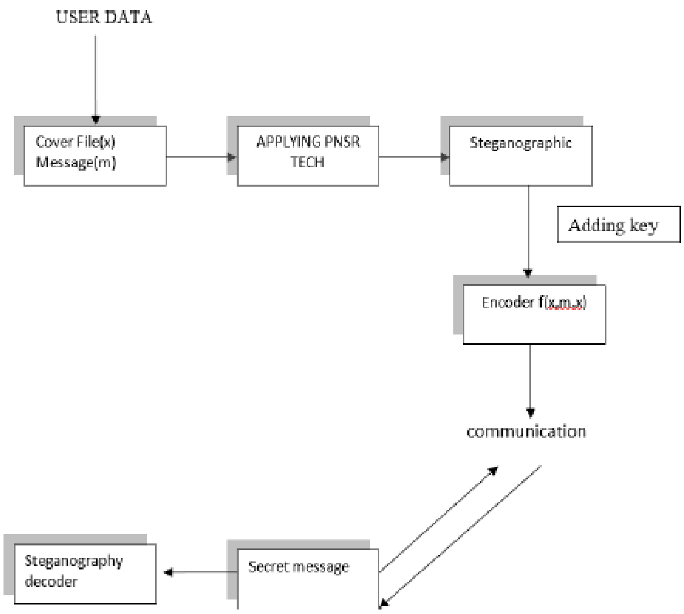

**Fig. 2. Proposed Architecture diagram**

## PROPOSED METHODOLOGY

The suggested solution is mostly concerned with mobile transfer apps that employ the.jpg and.png picture formats during transmission, such as WhatsApp, Telegram, and online shopping.

sent over the internet. We are enhancing the security process by processing these photos using steganography methods and utilizing the PNSR metric, an elliptic curve digital signature methodology. Methods for encryption and decryption algorithms, such as the PNSR metric and the Elliptic curve, are the primary emphasis of this system. Secure data transfer of a specific picture between two mobile stations is made possible using a digital signature technique. Four distinct tiers of technology will be used. Choosing a hidden picture is the first step. File formats such as jpg and png will be compatible with the hidden image. After the first layer of security produces a picture, the second layer encrypts it. Digital signatures are used for encryption in this context. Whenever this online

A document with an electronic signature has already been signed by the sender. The creator of this signature uses their private key, which they keep secret, to make it. The data is then transformed into a hash value using various encryption approaches. Along with the public key, this digital signature is appended to the data before being sent to the recipient. To determine the image's accuracy and quality, the PSNR measure will be used. The higher the PSNR score, the better the picture quality. Level 3 involves locating the least significant bit (LSB) and the three metrics (Mean, Mean, and Mode) of the picture that will be used to conceal the message inside the cover image. In conjunction with a survey, LSB proves to be a more practical method. The last layer of protection is compressing the resulting steganographic picture using GZIP.

## THE CURRENT SETUP

Internet of Things (IoT) applications in the residential and financial sectors are the primary emphasis of this system. As a first line of defense, you may use the Conformal Mapping method. This will change the picture's angle, allowing you to transform the secret image into whatever shape you like. The second stage involves using the RSA technique for encryption and decryption to encode the conformal-mapped picture. Asymmetric key cryptography, such as RSA, is used on the third level, which makes use of the Less Significant Bit (LSB) steganographic approach. The steganographic approach employs this technique to conceal the hidden picture inside its least significant bit values. The last stage is compressing the whole picture using GZIP. One way to tell whether the steganography procedure was successful is to use the peak signal-to-noise (PNSR) metric.

## CONCLUSION

In the realm of unusual picture encryption methods for mobile apps, cryptography network approaches are fully entrenched.Secure transactions are produced via the ECC digital signature. to the data, which will aid in safeguarding data while it is being sent. Elliptic curve cryptography is a new method of encrypting data into message digests, which greatly improves security. By using improved embedding efficiency, the following approach may be used to obtain advanced data concealing capability. It is necessary to know the MSE values in order to determine the PSNR when evaluating performance using parameters and metrics. Lastly, a MAT-LAB simulator is intended to be used to execute all of the aforementioned tasks**.**

## REFERENCES

**[1]. Abdallah, Wasan Khalid, Hadab Hussain, Saba. (2022). A Novel ImageEncryption Approach for IoT Applications. Webology. 19. 1593-1606.10.14704/WEB/V19I1/WEB19107.**

**[2]. Berghel, Hal. (2014). The Future of Digital Money Laundering. Computer.47. 70-75. 10.1109/MC.2014.225.**

**[3]. [5] Pajala, T., Korhonen, P., Malo, P., Sinha, A., Wallenius, J., Dehnokhalaji,A. (2018). Accounting for political opinions, power, and influence:A Voting Advice Application. European Journal of Operational**

**[4]. Research, 266(2), 702-715. https://doi.org/10.1016/j.ejor.2017.09.031**

**[5]. Sher Ali and Syed Babar Ali Rizvi Yousaf Ali Afia Zafar, 2020. ”SurveyPaper On Iot Attacks And Its Prevention Mechanisms,” InformationManagement and Computer Science (IMCS), Zibeline International**

**[6]. Publishing, vol. 3(2), pages 38-41, December.**

**[7]. R. Das and I. Das, ”Secure data transfer in IoT environment: Adoptingboth cryptography and steganography techniques,” 2016 SecondInternational Conference on Research in Computational Intelligence andCommunication Networks (ICRCICN), 2016, pp. 296-301, doi:**

**[8]. 10.1109/ICRCICN.2016.7813674.**

**[9]. R. Montella, M. Ruggieri and S. Kosta, ”A fast, secure, reliable, andresilient data transfer framework for pervasive IoT applications,” IEEEINFOCOM 2018 - IEEE Conference on Computer Communi- cationsWorkshops (INFOCOM WKSHPS), 2018, pp. 710-715, doi:10.1109/INFCOMW.2018.8406884.**

**[10]. Rai, Pooja Gurung, Sandeep Ghose, Mrinal. (2015). Analysis of ImageSteganography Techniques: A Survey. International Journal of ComputerApplications. 114. 11-17. 10.5120/19941-1731.**

**[11]. Khari, Manju Garg, Aditya Gandomi, Amir Gupta, Dr. Rashmi Patan,Rizwan Balamurugan, Balamurugan. (2019). Securing Data in Internet ofThings (IoT) Using Cryptography and Steganography Techniques. IEEETransactions on Systems, Man, and Cybernetics: Systems. PP. 1- 8.10.1109/TSMC.2019.2903785.**

**[12]. S. Janakiraman, V. Raj, K. Thenmozhi and R. Amirtharajan, ”Op- timizedLightweight Image Steganography on Embedded Device via LUTApproach,” 2019 International Conference on Computer Communicationand Informatics (ICCCI), 2019, pp. 1-6, doi: 10.1109/ICCCI.**

**[13]. 2019.8822175.**

**[14]. Janakiraman, S., Raj, V., Thenmozhi, K., Amirtharajan, R. (2019). OptimizedLightweight Image Steganography on Embedded Device via LUTApproach. 2019 International Conference on Computer Communicationand Informatics (ICCCI), 1-6.**

**[15]. Zebari, Dilovan Zeebaree, Diyar Saeed, Jwan Zebari, NechirvanAlzebari,Adel. (2020). Image Steganography Based on Swarm IntelligenceAlgorithms: A Survey. Test Engineering and Mana.**