A PECULIAR IMAGE ENCRYPTION TECHNIQUE FOR MOBILE APPLICATION

1st Krithika R
Network and Communication
SRM Institute of Science and Technology
Chengalpattu,Tamilnadu
kr7193@srmist.edu.in

2nd Dr.J.Godwin ponsam*
Network and Communication
SRM Institute of Science and Technology
Chengalpattu,Tamilnadu
godwinj@srmist.edu.in

2023 International Conference on Computer Communication and Informatics (ICCCI) | 979-8-3503-4821-7/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICCCI56745.2023.10128518

***Abstract*—The upgradation in the field of mobile applications is predominantly increasing. Nowadays mobile applications are used in various platforms on one-handled devices in addition, attackers can use similar technology to anonymize their malicious behaviors and hide their identification of behaviors. Thus, security is important. In this project, we are focusing on the precautionary encryption and decryption algorithms like PNSR metric and Elliptic curve Digital signature algorithm which help us to provide secured transmission of a personal imagebetween the mobile stations. Based on these algorithms a defense application will be developed. There are 4 different levels oftechnology that will be applied in this project which help to improve security transmission. The first level is selecting a secret image. The secret image will support file types like jpg,png. In thesecond level of security, we encode the image that we get from thefirst level using an encryption algorithm. Here the image quality is measured by using PSNR metric, the third level is finding the LSB, along with 3m (Mean,Mean,Mode) of the image to hide the message inside the cover image. Then the obtained stegnographic image is compressed using GZIP is the final security level. An Elliptic curve, a Digital signature algorithm is used to enhancea security process. Therefore, this method is suggested to send a secret message through applications of special importance across the mobile application.**

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

I. Introduction

The term ”mobile computing” refers to a set of technologies that create a setting in which users can share any kind of data with other devices that aren't physically attached to one another [1] To put it simply, the data can be sent from anywhere in the world via wireless transmission. There are three pre-requisites for effective mobile computing. They let users to create connections, and they comprise both the hardware and software of mobile devices. The protocols, services, and other aspects that make up the mobile communication framework ensure that communication flows without any hiccups. The hardware devices used in mobile computing can be taken anywhere and remain linked to the internet, which is the main driving force behind the success of this technology[2]. Beginning with the development of the first laptops in the 1980s, the era of mobile computing was born. Fast forward to 1990, and we have Apple's 640*640 portable computers, made possible bya number of upgrades and changes to the original hardware. It continued with the introduction of the first personal digital assistant (PDA) in 1993 and the first smartphone by IBM in 1994. Connectivity to networks was enabled in smartphones in the 2000s, the first iPhone debuted the following year, and the first Android smartphone was developed the same year. There is a wide range of mobile computing devices available now, each with its own set of features that expands with each new version of the underlying hardware and software[3-5].

As the number of features increases the number of users using these mobile computing devices rises tremendously In 2022, there will be more than six billion smartphone subscriptions globally, and Statista predicts that this number will expand by several hundred million in the next years, with the largest increases expected in China, India, and the United States[6]. Mobile phones are not only been used for communica-tion purposes, but It has also expanded their usage of capacity.Nowadays mobile phones are being used as personal assistants. They are being used for calls, payments, online shopping, gathering information, social media, booking appointments, ordering stuff, etc. With the rise in the tremendous growthof technology on one side, it raises serious questions about security[7,8]. The security factor is equally important to both the service provider end as well as endpoint side. When it comes to security it must be given to all the phases like in hardware part, software part, and network part. Hardware security islike protecting the physical machine from threats and attacks. Software security is something that gives protection to the software by providing integrity, authentication, and availabil- ity. Whereas network security is providing security to thenetwork, the medium. When data is let to transmit to another device through the network, it is more prone to be insecure. The major concern in security is to provide confidentiality, integrity, and availability of data. Information is an asset toall. it cannot be left as it is in a network because anyone using the network can view them. Network security has becomea major concern in the scope of security. A secure data transfer is transferring data from one place to somewhere with the assurance that the data is confidential, not modified or intercepted during transit. So, when the data is transmitted, it should be transmitted in a secure way over a secure channel. There are many ways to secure transmission. We can use various cryptographic techniques, steganographic techniques, firewalls, access control, and Intrusion Detection Systems to

protect the data.

II. LITERATURE SURVEY

A. IoT Security-Cryptography and Steganography Techniques

The elliptic Galois cryptography protocol is presented as a means to encrypt data and prevent its unauthorized disclosure or modification while in transit. In addition to the secure cryptographic technique, The XOR steganography matrix method is implemented. Using these strategies, the secret information is embedded in the cover photo. Similarly, this makes use ofan optimization algorithm called Adaptive Firefly to pick the best possible cover blocks from within the image. Using this method, the secret message in an image will remain secure during network transfer[9].

B. A Novel image encryption technique

Four levels of security are discussed. The first level - Conformal Mapping is applied to the secret image to change the image angles(shapes). Second level incorporates Encoding techniques, where the image obtained from 1st level is set for encryption and decryption using the RSA method. In the Third level – LSB hiding method is used to hide the secret message inside the cover image. In the Fourth level compression of the final steganographic image is generated using GZIP tool[10].

C. Securing IoT Data Using Steganography

This paper employs a steganographic technique for hiding data in an Internet of Things cover signal. After completing this procedure, a stenography signal is produced and transmit- ted via the Internet of Things. Signal-to-noise (SNR) ratiosare improved with the use of low-frequency components of audio cover signals like speech and music as opposed to high-frequency components. Due to its higher energy, it proves to be an effective data-embedding medium. Signal spectra are used to reduce the interference introduced by secret information and improve the quality of the stenographic signal. The attenuation of 13 dB compared to the original signal spectrum is theresult of this attenuation. We used a multi-key combinationto satisfy the steganography system's needs for embedding data against intentional removal attempts, including statistical undetectability, steganography signal quality[11],

D. Data security - Digital Signatures

A digital signature is a kind of signature, that is been used to sign in documents digitally[12]. This method is used in this paper. An electronic signature is like a signature is used to confirm the authenticity of the user i.e., the identity of the signatory who sent the information.In this paper, The digital signature key generation is based on based on RSA is discussed. First signature keys are created and RSA key pair is generated, withequation

$$ed \equiv 1 \mod \vartheta(N) \tag{1}$$

where N - the product of two random unique and large prime numbers, e and d belongs to integers, ϑ is used to determine Euler's totient function. where N and e consist of the sender's public key, and the sender's secret key is contained in d. To sign a message, m, the sender computes a signature equal to the equation

$$\sigma \equiv md \ mod N \tag{2}$$

. To verify the value, in the receiver side, the receiver validates this with the mentioned equation

$$e \equiv m \mod N \tag{3}$$

. A trapdoor permutation is a family of permutations. This method is easy to compute in the forward direction whereas computing is difficult in the reverse direction. Trapdoor permutations can be used for a digital signature where calculations are done in the reverse direction where the secret key is required for signing process[13].

III. OVERVIEW OF THE PROJECT

There are many methods to send data in a secure way. Data while transferred to a network will be in an encrypted format, even though they are encrypted there is a possibility for a hacker to read and modify the data when he finds the key. Here this system is mainly focusing on precautionary encryption and decryption algorithm methods like PNSR metric and Elliptic curve Digital signature algorithm which helps to provide secured data transmission of a particular image between the mobile stations. Based on these algorithms a defense application will be developed. There are 4 different levels of technology that will be applied in this project which help to improve security transmission. The first level is selecting a secret image. The secret image will support file types like jpg, and png. In the second level of security, we encode the image that we get from the first level using an encryption algorithm. Here the image quality is measured by using the PSNR metric, the third level is finding the LSB, along with 3m (Mean,Mean, Mode) to hide the message inside the cover image. Then the obtained steganographic image is compressed using GZIP as the final security level. An Elliptic curve, a Digital signature algorithm is used to enhance a security process.Therefore, this method is suggested to send a secret message through applications of special importance across the mobile application.

IV. TECHNOLOGIES PROPOSED

A. PSNR

Peak signal-to-noise ratio (PSNR) is terminology that helps determine the how good quality between a compressed image and an original image. More the PSNR value, good the quality of the image. These are the performance metrics used to estimate the strength of the cryptosystem. To find the PSNR value we need to know the MSE value. MSE is nothing but Mthe ean Square Error of images. It measures the difference between two images.

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

Where I1 and I2 - given two images M, N - dimensions of the images

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

It is the ratio between signal and noise that distorted the image. The PSNR is measured in decibels (dB)

B. Elliptic Curve Cryptography

Elliptic Curve Cryptography (ECC) is a type of asymmetric cryptographic technique that uses the public key for encrypting the data and a private key to decrypt the encrypted data. It is one of the most powerful cryptography. ECC is the next generation of public key cryptography.ECC is an alternative technique to RSA. The keys are generated by using a mathematical concept from an elliptic curve. The figure mentions the elliptic curve and P,Q,R are the 3 random points taken for key generation purpose. In ECC, The key size is smaller when

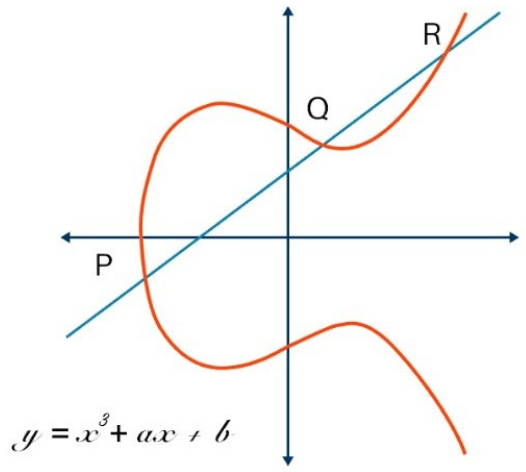

Fig. 1. Elliptic curve.

compared with other cryptographic techniques and ECC makes the key more complex making it mathematically difficult to crack it. An elliptic curve ECC equation is represented as follows,

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

C. Digital Signature

A Digital signature is a technique which is used to validate whether the data, software, or any types of digital document has managed to attain authenticity and integrity. To obtain this, some mathematical techniques are being used.

1) The steps followed in creating a digital signature are :

- When the hash function is applied to data, A message digest will be obtained. this message digest along with the sender's private key is encrypted to form the digital signature.
- Digital signature is then sent to the receiver along with the data transmitted.
- The Receiver on the other side will get the public key with message digest, so with this public key digital signature is decrypted. When the signature is verified, authenticity is assured because only the sender has the private key to encrypt the hash which can further be decrypted using the sender's public key.
- The receiver now has obtained the message digest, so with that message digest hash value is computed.
- Then the hash value obtained before and after data transmission is compared for ensuring integrity. The signature will also be marked with the time stamps along with the signature. If the document is modified after signing, the digital signature will be invalid.

V. Methodology Proposed

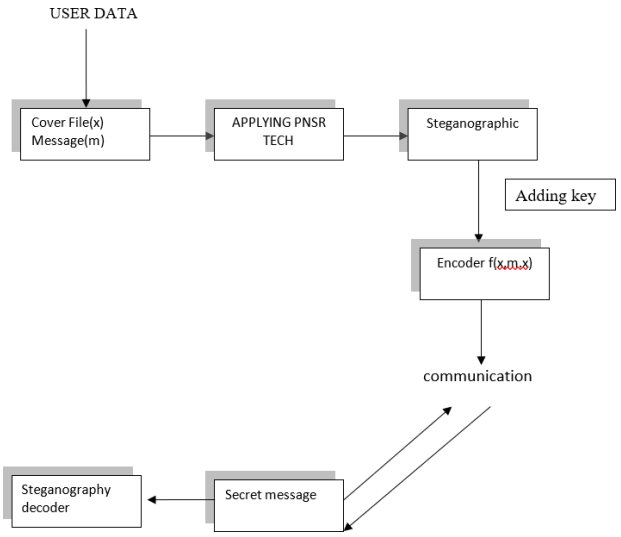

Fig. 2. Proposed Architecture diagram

VI. Proposed Methodology

The proposed system mainly deals with mobile transfer applications like (WhatsApp, telegram,online shopping) that uses image formats of .jpg and .png during the transmission of data into the network. These images are processed with steganography techniques, and we are using the PNSR metric, Elliptic curve Digital signature algorithm to improve the security process. Here this system is mainly focused on encryption and decryption algorithm methods that include the PNSR metric and the Elliptic curve Digital signature algorithm which helps to provide secured data transmission of a particular image during transmission between two mobile stations. Here 4 different levels of technology that will be applied. The first level is selecting a secret image. The secret image will support file types like jpg,png. In the second level of security, encoding of the resulting image from the first level is done. Here, for encryption digital signatures are used. When this digital

signature is used in a document, an electronic signature is been signed by the sender. This signature is created by using the sender's private key and kept safe by the sender. And with help of some cryptographic techniques, the data are converted to some hash value. This digital signature is added to the data and sent to the receiver side along with the public key. PSNR metric will be used to calculate the quality and correctness of the image. More the PSNR value, good the quality ofthe image. In the third level is finding the LSB, along with3m (Mean, Mean, Mode) of the image to hide the message inside the cover image. When undergone with a survey, LSBis found to be a more feasible technique. Then the obtained steganographic image is compressed using GZIP is the final security level.

VII. Existing system

This system mainly focuses on IoT technology in the field is financial, and home applications. By applying the Conformal Mapping technique, the first level of security is implemented, when conformal mapping is done on the secret image, the image angle of the image will be altered, which means the image can be turned to any shape. In the second level, encoding of the resulting image which has gone through conformal mapping is done using the encryption and decryption (RSA) method. RSA cryptographic technique is asymmetric key cryptography while in the third level Less Significant Bit (LSB) steganographic method is used. This method is used to hide the secret image inside the steganographic method in its least significant bit values. In the last level, GZIP is used to compress the entire image. The peak signal-to-noise (PNSR) metric technology is used to find whether the quality of the resulting image was good after the steganography process.

VIII. Conclusion

Cryptography network techniques are immersed in the field of peculiar image encryption techniques for mobile applications. The ECC digital signature generates high levels security to the data which will be helpful in protecting data during transmission. With the novel Elliptic curve cryptography, the data is encrypted into the message digest, so that better security is provided. With the use of enhanced embedding efficiency, advanced data hiding capacity can be achieved if the following methodology is implemented. Performance is evaluated with parameters PSNR metrics, and MSE values should be known to identify PSNR. Finally, all the above- proposed work is planned to be implemented using a MAT- LAB simulator.

References

[1] M. Khari, A. K. Garg, A. H. Gandomi, R. Gupta, R. Patan and B. Balusamy, "Securing Data in Internet of Things (IoT) Using Cryptography and Steganography Techniques," in IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 50, no. 1, pp. 73-80, Jan. 2020, doi: 10.1109/TSMC.2019.2903785.

[2] Hashim, Mohammed Rhaif, Suhad Abdulrazzaq, Ali Hussein Ali, Adnan Taha, Mustafa. (2020). Based on IoT Healthcare Application for Medical Data Authentication: Towards A New Secure Framework Using Steganography. IOP Conference Series: Materials Science and Engineering. 881. 012120. 10.1088/1757-899X/881/1/012120.

[3] Abdallah, Wasan Khalid, Hadab Hussain, Saba. (2022). A Novel Image Encryption Approach for IoT Applications. Webology. 19. 1593-1606. 10.14704/WEB/V19I1/WEB19107.

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

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

[6] Sher Ali and Syed Babar Ali Rizvi Yousaf Ali Afia Zafar, 2020. "Survey Paper On Iot Attacks And Its Prevention Mechanisms," Information Management and Computer Science (IMCS), Zibeline International Publishing, vol. 3(2), pages 38-41, December.

[7] R. Das and I. Das, "Secure data transfer in IoT environment: Adopting both cryptography and steganography techniques," 2016 Second International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN), 2016, pp. 296-301, doi: 10.1109/ICRCICN.2016.7813674.

[8] R. Montella, M. Ruggieri and S. Kosta, "A fast, secure, reliable, and resilient data transfer framework for pervasive IoT applications," IEEE INFOCOM 2018 - IEEE Conference on Computer Communi- cations Workshops (INFOCOM WKSHPS), 2018, pp. 710-715, doi: 10.1109/INFCOMW.2018.8406884.

[9] Rai, Pooja Gurung, Sandeep Ghose, Mrinal. (2015). Analysis of Image Steganography Techniques: A Survey. International Journal of Computer Applications. 114. 11-17. 10.5120/19941-1731.

[10] Khari, Manju Garg, Aditya Gandomi, Amir Gupta, Dr. Rashmi Patan, Rizwan Balamurugan, Balamurugan. (2019). Securing Data in Internet of Things (IoT) Using Cryptography and Steganography Techniques. IEEE Transactions on Systems, Man, and Cybernetics: Systems. PP. 1- 8. 10.1109/TSMC.2019.2903785.

[11] S. Janakiraman, V. Raj, K. Thenmozhi and R. Amirtharajan, "Op- timized Lightweight Image Steganography on Embedded Device via LUT Approach," 2019 International Conference on Computer Communication and Informatics (ICCCI), 2019, pp. 1-6, doi: 10.1109/ICCCI.2019.8822175.

[12] Janakiraman, S., Raj, V., Thenmozhi, K., Amirtharajan, R. (2019). Optimized Lightweight Image Steganography on Embedded Device via LUT Approach. 2019 International Conference on Computer Communication and Informatics (ICCCI), 1-6.

[13] Zebari, Dilovan Zeebaree, Diyar Saeed, Jwan Zebari, Nechirvan Alzebari, Adel. (2020). Image Steganography Based on Swarm Intelligence Algorithms: A Survey. Test Engineering and Management.