A PECULIAR IMAGE ENCRYPTION TECHNIQUE FOR MOBILE APPLICATION

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 mali- cious 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.

**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 im- age 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.

**Proposed system**

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 secu- rity 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.

**SYSTEM SPECIFICATION:**

**HARDWARE REQUIREMENTS:**

* **System :** Intel i7
* **Hard Disk :** 1 TB.
* **Monitor** : 14’ Colour Monitor.
* **Mouse :** Optical Mouse.
* **Ram :** 8GB.

**SOFTWARE REQUIREMENTS:**

* **Operating system :** Windows 10.
* **Coding Language :** Python.
* **Front-End :** Html. CSS
* **Designing :** Html,css,javascript.
* **Data Base :** SQLite.

**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 Cryptogra- phy 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.