International Journal of Advanced Engineering Science and Information Technology (IJAESIT)
ISSN: 2349-3216
Vol.6, No.6, June 2023

Hybrid Cryptography Data Security Tool

[1] Prasannasabhari V
Student of department of CSE
PSNACET
Dindigul, India.
prasannasabhari55@gmail.com

[2] Pradeep S
Student of department of CSE
PSNACET
fDindigul, India.
s.pradeep02112002@gmail.com

[3] Paul Meshach S
Student of department of CSE
PSNACET
Dindigul, India.
pickypercy2000@gmail.com

Abstract — Securing data by encryption and decryption using Cryptography and Steganography techniques. Due to recent developments in steganography analysis, providing security to personal contents, messages, or digital images using steganography has become difficult. By using steganography analysis, one can easily reveal the existence of hidden information in carrier files. This project introduces a novel steganographic approach for securing data of users.The approach introduced in this project makes use of both steganographic as well as cryptographic techniques. In Cryptography we are using AES 128 algorithm and SHA 256 hashing . In Steganography we are using Image Steganography for hiding the data. And we also use the Mutual Authentication process to satisfy all services in Cryptography i.e., Access Control, Confidentiality, Integrity, Authentication. In this way we can maintain the data more securely. Since we use AES algorithm and SHA hashing for securing the data and password respectively and then again on this we perform Steganography to hide the data in an image. Such that any other person cannot access the data present in the Image.

Keywords – Advanced Encryption Standard (AES), Secure Hash Algorithm (SHA), Cryptography, Steganography.

I. INTRODUCTION

Digital communication witnesses a noticeable and continuous development in many applications on the Internet. Hence, secure communication sessions must be provided. The security of data transmitted across a global network has turned into a key factor on the network performance measures. So, the confidentiality and the integrity of data are needed to prevent eavesdroppers from accessing and using transmitted data. Steganography and Cryptography are two important techniques that are used to provide network security.The aim of this project is to develop a new approach to hiding secret information in an image, by taking advantage of benefits of combining cryptography and steganography.

A. CRYPTOGRAPHY

Cryptography is one of the traditional methods used to guarantee the privacy of communication between parties. This method is the art of secret writing, which is used to encrypt the plaintext with a key into ciphertext to be transferred between parties on an insecure channel. Using a valid key, the ciphertext can be decrypted to the original plaintext. Without the knowledge of the key, nobody can retrieve the plaintext. Cryptography plays an essential role in many factors required for secure communication across an insecure channel, like confidentiality, privacy, non- repudiation, key exchange, and authentication.

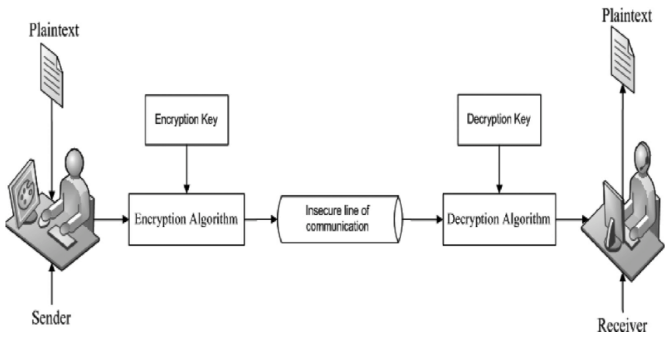

Fig. 1.1 Cryptography as a flow model

B. STEGANOGRAPHY

It can be defined as the science of hiding and communicating data through apparently reliable carriers in an attempt to hide the existence of the data. So, there is no knowledge of the existence of the message in the first place. If a person views the cover where the information is hidden inside, he or she will have no clue that there is any covering data, in this way the individual won't endeavor to decode the data. The secret information can be inserted into the cover media by the stegano system encoder using a certain algorithm. A secret message can be plaintext, an image, ciphertext, or anything which can be represented in the form of a bitstream. After the secret data is embedded in the cover object, the cover object will be called a stegano object. Also the stegano object is sent to the receiver by selecting the suitable channel, where the decoder system is used with the same stegano method for obtaining original information as the sender would like to transfer.

II. RELATED WORK

The Existing System proposed a crypto-watermarking approach based on AES standard encryption algorithm and reversible watermarking data hiding technique to secure medical images. The results proved that the proposed approach achieves both the authenticity and integrity of the images either in the spatial domain or the encrypted domain or both domains.

A. Existing System's Drawbacks

- The conventional encryption methods failed to give the desired result of protecting the data.
- DES is breakable, as the key is 56-bit length.
- The existing Encryption Standard is comparatively slower.

III. THE PROPOSED MECHANISM

In this section, we will discuss a proposed method which combines two different hiding techniques, which are Cryptography and Steganography. In this proposed method first, the message is encrypted by the AES 128 algorithm and the password is encrypted to a key object using SHA 256 hashing function. After that, we use the modified LSB technique to embed the encrypted information in the image. So, this technique combines the features of both cryptography and steganography and provides a high level of security. It is better than either of the techniques used separately. There will be an agreement between users about the key for the concealment algorithm as well as the key for the encryption algorithm or these keys may be exchanged by a secure communication method. Our method starts by encryption first then hides encrypted data.

IV. PERFORMANCE EVALUATION

There are mainly 2 modules in the project "Hybrid Cryptography (Crypto - Stegano) Data security tool" They are:

- Image Cryptography
- Image Steganography

A. Image Cryptography module

Here in Image cryptography, the process of encryption and decryption of a given message and then embedding and extraction of the message takes place. There are two sub modules employed in this module. They are

- Encryption of Image File phase
- Decryption of .enc File phase

1) Encryption of Image File phase

In the encryption stage, we use the SHA 256 Hash function to convert the given password to a hashed key object and then we use the AES 128 algorithm. This technique takes the hashed key object as the key. The Encryption can be done using an image file and with the key object which was generated using the kdf.derive function. Then we will get a file with '.enc' extension, this encrypted file will be used in the decryption of .enc File phase.

Input = Image file (png, jpg and jpeg) + password (hashed key object)

Output = '.enc' file

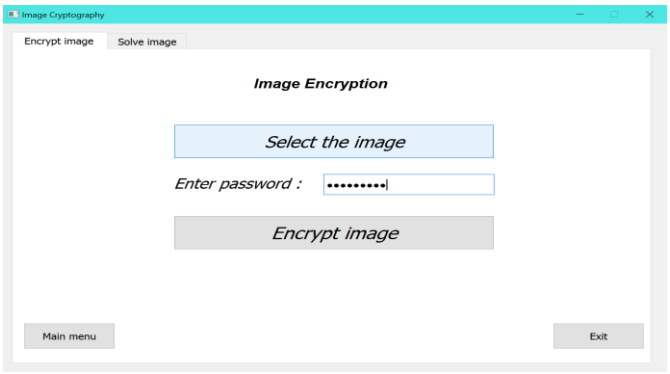

Fig. 4.1 Encryption of Image File phase

2) Decryption of '.enc' File phase

In the decryption stage, we use the '.enc' file which is produced from the encryption stage. We will use the same steps which are used on the Encryption stage. The Decryption can be done using the generated '.enc' file and with the key object which was generated using the kdf.derive function.

Input = '.enc' file + Password (hashed key object).

Output = Solved Image File.

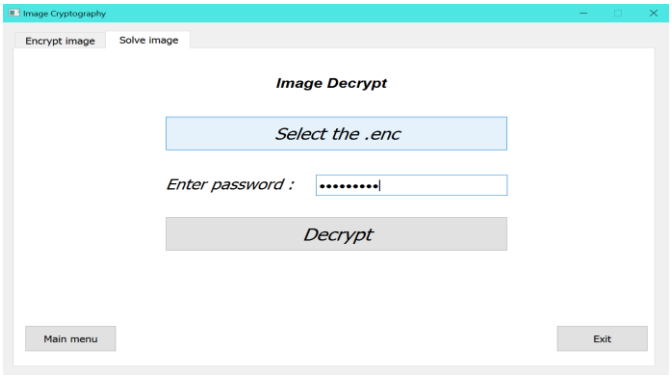

Fig. 4.2 Decryption of '.enc' File phase.

B. Image Steganography module

Here in Image steganography, a certain message is embedded in and extracted from an image file. There are two sub modules employed in this module. They are

- Encryption and Embedding phase
- Decryption and Extracting phase

1) Encryption and Embedding phase

The Encryption and Embedding phase consists of cryptographic and steganography stages. This phase starts with cryptographic then steganography.

a) Cryptography Stage

In the encryption stage, we use the SHA 256 Hash function to convert the given password to a hashed key object and then we use the AES 128 algorithm. This technique takes the hashed key object as the key. The Encryption can be done using the Plain Text and with the key object which was generated using the kdf.derive function. Then we will get a cipher text, this encrypted data will be used in the steganography stage.

Input = Plain text message + Password (hashed key object).

Output = Encrypted Message.

b) Steganography Stage

In the stenography stage, we use LSB (Least Significant Bit) algorithm with some modification to hide information (encrypted data from cryptography stage) inside a cover. In our experiment, we use an image file as cover to present our method. The general LSB method used to hide secret information into an image file; the last bit in each pixel or sample or frame used sequentially to hide one of the binary stream bits Encryption of the cover image.

Input = Encrypted Message + Password (hashed key object) + Cover image.

Output = Stegano - Image.

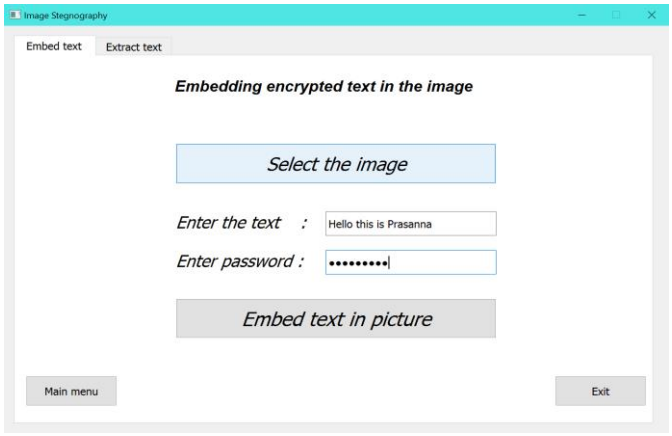

Fig. 4.3 Encryption and Embedding phase

2) Decryption and extracting phase

The decryption phase consists of steganography and cryptography stages. In the decryption phase we will first extract embedded data then decrypt it.

a) Steganography Stage

In the decryption phase, we start with steganography and then with cryptography. We will use the same steps which are used on the Encryption's steganography stage.

Input = Stegano-Image + Password (hashed key object).

Output = Encrypted Message.

b) Cryptography Stage

In the cryptography stage, we use the data which is extracted from the stegano-image file and use . We will use the same steps which are used on the Encryption's cryptography stage. The Decryption can be done using the Extracted Cipher Text and with the key object which was generated using the kdf.derive function.

Input = Encrypted Message + Password (hashed key object).

Output = Solved Plain Text Message

Fig. 4.4 Decryption and Extracting phase

C. Implementation

The implementation of the GUI tool will depend on the platform and programming language used for development. The steps involved in implementing a GUI security tool is illustrated below:

1. Create a graphical user interface for the security tool in python PyQt5 package.
2. Define the style structure of the UI in XML scripting.
3. Implement the core algorithm for cryptography and steganography using predefined functions in the Cryptography and Steganography package.
4. Create access handlers to access message and image fields in the GUI application.
5. Now place the access handlers in appropriate positions and use them to control the GUI application.

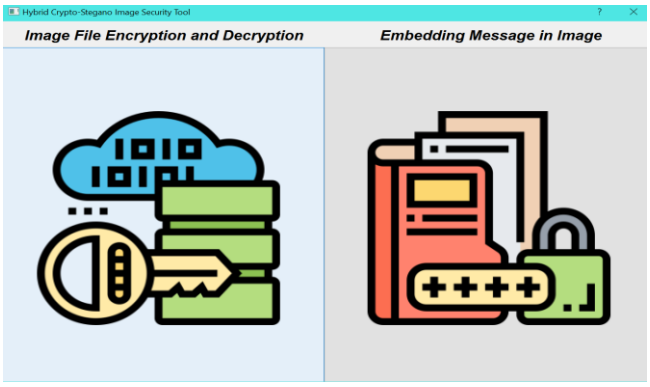

Fig. 5.1 Home Navigation Window

V. CONCLUSION

In this project, we deal with the concepts of security of digital data across the system. This project is designed for combining the steganography and cryptography features for better performance. We performed a new steganography method and combined it with the AES 128 algorithm and SHA 256 hashing. The data is hidden in the image so there will be no chances for the attacker to know that data is being hidden in the image. We performed our method on image by implementing a program written in Python language. The method proposed has proved successful in hiding various types of texts in color images.

We concluded that in our method the Image files and AES are better. Because of their high capacity. This work presents a scheme that can transmit large quantities of secret information and provides secure data confidentiality and integrity between two private parties. Both steganography and cryptography can be woven in this scheme to make the detection more complicated. Any kind of text data can be employed as secret msg. The secret message employing the concept of steganography is sent over the network. In addition, the proposed procedure is simple and easy to implement.

REFERENCES

[1] D. Seth, L. Ramanathan, and A. Pandey, "Security enhancement: Combining cryptography and steganography," International Journal of Computer Applications (0975–8887) Volume, 2010.
[2] H. Abdulzahra, R. AHMAD, and N. M. NOOR, "Combining cryptography and steganography for data hiding in images," ACACOS, Applied Computational Science, pp. 978–960, 2014.
[3] J.V.Karthik and B.V.Reddy, "Authentication of secret information in image steganography," International Journal of Computer Science and Network Security (IJCSNS), vol. 14, no. 6, p. 58, 2014.
[4] M.H.Rajyaguru, "Crystography-combination of cryptography and steganography with rapidly changing keys," International Journal of Emerging Technology and Advanced Engineering, ISSN, pp. 2250–2459, 2012.
[5] Mr.Vikas Tyagi(2012),"Data Hiding in Image Using Least Significant Bit with Cryptography", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 4.
[6] P. R. Ekatpure and R. N. Benkar, "A comparative study of steganography & cryptography" 2013.
[7] M. K. I. Rahmani and N. P. Kamiya Arora, "A crypto-steganography: A survey," International Journal of Advanced Computer Science and Application, vol. 5, pp. 149–154, 2014.
[8] R. Poornimal and J. Iswarya (2013) "An Overview of Digital Image Steganography ", International Journal of Computer Science & Engineering.
[9] R Praveen Kumar, V Hemanth, MShareef, Securing Information Using Steganography, 2013 International Conference on Circuits, Power and Computing Technologies.