International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 11 Issue: 04 | Apr 2024 www.irjet.net p-ISSN: 2395-0072

Secure Data Transmission Through Steganography using AES Algorithm

Mrs. Rinkal Bari[1], Ms. Saloni Bhosale[2], Tanvi Raut[3], Sanyuti Sankhe[3]

[234]Information Technology, Theem College Of Engineering, Mumbai, India
[1]Professor, Department Of Information Technology, Theem College of Engineering, Boiser, Maharashtra, India

---

Abstract - *Secure Data Transmission Through Steganography using AES Algorithm is the art of hiding the fact that communication is taking place, by hiding information in other information. Different application has different requirements of the steganography techniques used. It may require absolute invisibility of the secret information, while other requires a largest secret message to be hidden. On the other side receiver download the stego image and using the software retrieve the secret text hidden in the stego image. It allows use to choose the bits for replacement from the image then sender select the cover image with the bit replacement choice it helps to generate the secure stego image. It consists of three element cover image which hides the secret image, the secret image and the steganos image which is covered by object with embedded message inside in it. The origin of the term is steganos means secret and graphy means writing. It means hiding one piece of data within another. It is the practice of concealing a file, message, image or video within another files, images, messages or video. This security is available by encrypting the information that is transferred in the image and again encrypting the image that has the data using the AES algorithm. Secure data transmission refers to transfer the data such as confidential information over a secure channel.*

***Key Words*: Steganography; Image; Text; Data Hiding; Information Hiding; Encryption; Decryption; LSB; AES**

1.INTRODUCTION

Ensuring the confidentially and integrity of sensitive information has become crucial in the world of data transfer and communication. Strong and secure procedures to protect data during transmission are becoming more and more important as digital communication spreads. This field of secure data transfer suggests a new method that combines the power of Advanced Encryption Standards AES encryption with the steganography strength. By obscuring the existence of sent data, steganography the practice of hiding information among other seemingly innocent data adds another degree of protection. This means of convert communication improves the data transmission confidentially. Steganography combined with the AES algorithm a popular and extensively used symmetric encryption standard forms a complete solution for protecting confidential data. The Advanced Encryption Standard, chosen for its robustness and efficiency, ensures that even if the hidden information is discovered, its content remains unintelligible without the corresponding decryption key. AES employs a symmetric key block cipher, offering a high level of security and speed suitable for real- time data transmission scenarios. It aims to explore the theoretical underpinnings of combing steganography and AES presenting a detailed analysis of their synergy in achieving secure data transmission. The proposed methodology involves embedding confidential data within cover objects using steganography techniques and subsequently encrypting the composite data using the AES algorithm.

2. LITERATURE SURVEY

Data encryption is the technique for secure sharing of data. These days, hackers employ certain algorithm or other methods to decode the data that senders have encoded. Making ensuring data is hidden from hackers is one technique to guarantee security. In today society people are willing to spend thousands of dollars to guarantee a high-level information security. Hackers are developing with the technology that is used to secure data, as it advances. Data security is crucial in the internet and networking driven world of today. An overview of secure data transmission through steganography using AES algorithm to provide high quality of data security and transfer of data from source to destination. It should be capable of identifying the authorized and unauthorized users. It should be capable of embedding text message into image file, audio, file and video file. By employing various steganographic techniques such as whitespace manipulation, format-based encoding, word-based alterations, or grammar-based modifications, text steganography ensures that the embedded message remains inconspicuous and undetectable to unintended recipients. Text steganography holds significance in scenarios where overt encryption methods may raise suspicion or attract unwanted attention. It provides a discreet means of communication, particularly in contexts where privacy and secrecy are paramount.

2.1 Existing paper

We presented an overview of the steganography it is done to provide secure communication, in present world there is a demand of sending and displaying data in a hidden format especially when the exchange of information and data is taking place publically, and this is the reason because of

which many methods have been proposed for data and information hiding. we use text steganography technique which uses HTML document as the cover medium to hide secret messages. We are using C# .net technology for implementing the technique. Steganography refers to the art and science of hiding secret information in some other media The cover document containing hidden message is called stego- document.[1]

This article presents various types of techniques used by modern digital steganography, as well as the implementation of the least significant bit (LSB) method. The main objective is to develop an application that uses LSB insertion in order to encode data into a cover image. The amount of data that can be hidden into an image depends on the size of the image and the number of least significant bits used for encryption. Hiding information inside images is one of the most popular steganographic techniques used nowadays.[2

The LSB method is the most used method in image steganography. In the LSB method, each bit of the message to be hidden is written to the last bit of a byte of the data that creates the image file. In the LSB method, adding to the last two bits instead of adding to the last bit doubles the amount of data that can be hidden. There are a couple of factors that must be taken into consideration before running the application. The first, and the most important one is the size of the cover image compared to the dimensions of the message that must be hidden. While simple to implement, the LSB hiding method is quite easy to detect. In order for the output stego images to pass steganalysis tests, the application could embed data only in certain regions of the image.[3]

Steganography overview, its demand, advantages, and the techniques involved in it. In this paper there is also an attempt to identify which steganography techniques are more useful what are their requirements and it shows which application will have more compatibility with which steganography technique. To better hide the data in case the message is too small compared to the input image, more complex algorithms can be used. Hidden bits can be dispersed throughout all the image using a unique key that only the sender and the receiver possess. For the encoding part the message is hidden into the least significant bits of a bmp image, thus resulting the stego-image. This image is then given to the decoder to extract the data that has been hidden. Steganography is hiding data into other data. The LSB method is the most used method in image steganography. In the LSB method, each bit of the message to be hidden is written to the last bit of a byte of the data that creates the image file.[4]

2. SYSTEM ARCHITECTURE

A Secure Data Transmission through Steganography using AES Algorithm The system architecture of our project includes various components playing their own specific roles. The main target of the project is the admin panel through which all the activities are managed and recorded. The system architecture includes end user interaction with the system. The admin interface in the system consists of various modules such as sales, billing, customer, staff and inventory. Number of products sold, number of products purchased, the most selling product, the least selling products etc. everything gets updated in the system on regular basis. However, there are often cases when this is not possible, either because you are working for a company that does not allow encrypted emails or perhaps the local government does not approve of encrypted communication. This is one of the cases where Steganography can help hide the encrypted messages, images, keys, secret data, etc. The data stored and transmitted electronically in the world today, it is no surprise that countless methods of protecting such data have evolved. One lesser-known but rapidly growing method is steganography, the art and science of hiding information so that it does not even appear to exist.

3.1 Design

After the requirements have been determined, the necessary specification for the hardware, software, people, data resources, and the information products that will satisfy the functional requirements of the proposed system can be determined. The design will serve as a blue print for the systems and helps to detect these problems before these errors or problems are built into the final system. The design will serve as a blue print for the systems and helps to detect these problems before these errors or problems are built into the final system. With the development of steganographic techniques adapted for each file format, different types of steganalysis methods have also emerged. Due to the increased popularity of digital image steganography, image steganalysis techniques are the most numerous ones. A widely used method involves statistical interpretation. While LSB might not seem 160 very important, it can offer plenty of information regarding the contents of an image.

3.2 Requirement analysis

Requirements analysis is the process of analyzing the information needs of the end users, the organizational environment and any systems presently being used thereby developing the functional requirements of a system that can meet the needs of the users. Also, the requirements should be recorded in a document, email, user interface. The requirements documentation should be referred to throughout the rest of the system development process to ensure the developing project aligns with the needs and requirements.

Hardware Requirement

1. 32-bit color
2. 1024 x 768 pixels

3. 800 x 600
4. 1 GB RAM
5. Laptop / PC/ Desktop

Software Requirement

1. Visual Studio
2. JDK 1.5
3. Any Version of Windows, UNIX

The output of this phase is the project plan, which is the document describing the different aspects of the plan. The project plan is instrumental in driving the development process through the remaining phases.

3.3 Proposed System

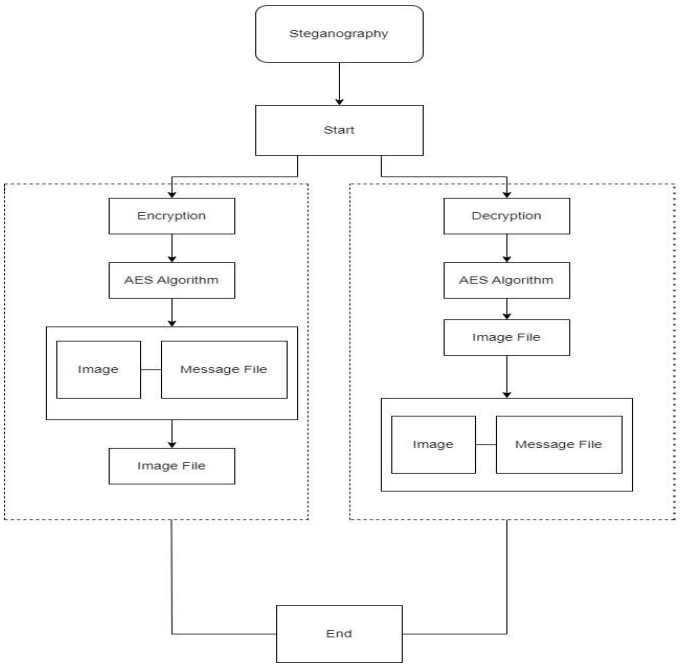

Fig 1. Proposed System of Secure Data Transmission through Steganography using AES Algorithm

To hide file and information the encrypt module is used inside the image in a way such that no one can see that information or file. Only one image file is given in output, and also this module can have any type of image as input. For having the hidden information, the decrypt module is given, as output it extracts the image file and at destination folder two files are given, a hidden file (having hidden message in it) and the original image file. The name and size of file must be stored in a specified place of image before encrypting them.

3.4 System Design

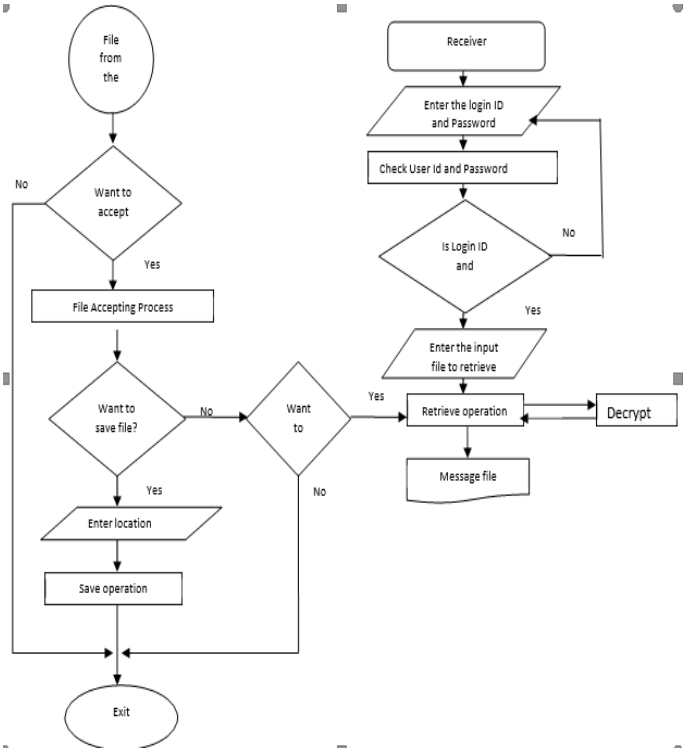

Fig 2. System Flow of Secure Data Transmission Through Steganography using AES Algorithm

A flowchart is a pictureof the separate steps of a process in sequential order. It is a generic tool that can be adaptedfor a wide variety of purposes, and can be used to describe various processes, such as a manufacturing process, an administrative or service process, or a project plan. Use the AES algorithm to encrypt the secret message with a chosen encryption key. This step ensures that the message is secure and cannot be easily read without the decryption key. Examine the cover image to determine where the secret message can be embedded. This could involve analyzing least significant bit (LSB) planes or other techniques to identify suitable locations for embedding. Modify selected pixels in the cover image to embed the binary representation of the encrypted message. This is usually done by altering the LSBs of pixel values to minimize the visual impact on the cover image. Generate the stego image, which is the cover image with the embedded secret message. This flowchart provides a basic overview of steganography using the AES algorithm. Keep in mind that there can be variations and additional steps depending on the specific implementation and requirements of the steganographic system.

4. Results

Effective in our Secure Data Transmission through Steganography using the AES Algorithm results in enhanced data protection when compared to conventional data transfer

methods. A safer way of data hiding is using a publicly available cover source, like a book or a newspaper and using a secret code that contains sequences of three numbers - page, line and character index. This way, the message can only be revealed by having both the secret code and the stego cover. If the message is hidden in such a way that the cover does not arouse suspicion, it will most probably not be discovered. steganography using the AES algorithm offers a secure and efficient method for hiding confidential information within cover images. By encrypting the secret message with AES, the confidentiality of the message is ensured. Therefore, careful consideration and implementation are necessary to achieve robust and secure steganographic communication.

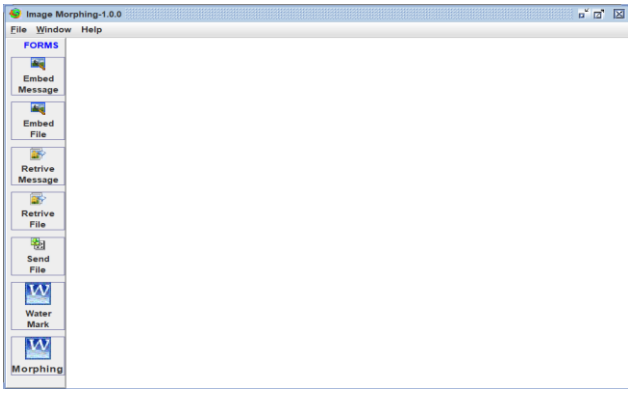

Fig 3. GUI of our model

Describes the GUI system of our project. It contains of Login, Embedded Message, Retrive Message, Water Mark Image.

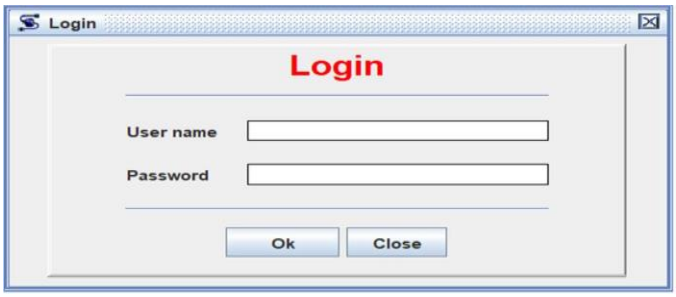

Fig 4. Result for Login

In this user must create her login id to
person to another. The user must provide their personal details to create login id and password. By incorporating these elements into your steganography project's login system, you can ensure secure access control for users, safeguard sensitive data, and mitigate potential security risks

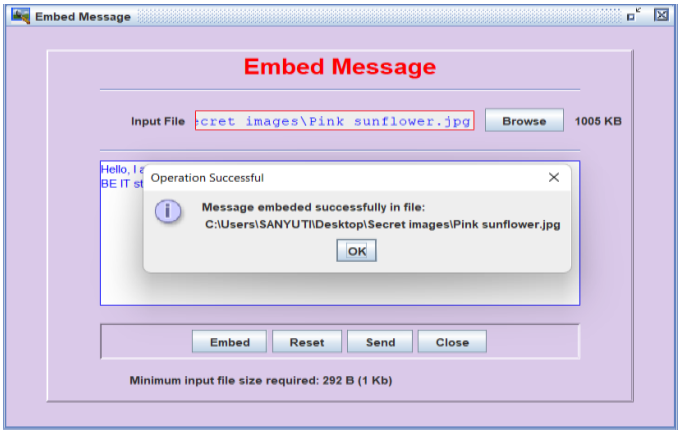

Fig 5. Result for Embed Message

Fig 5. Shows the result of Embed message in which user can embedded the message behind the image. User has to enter the input file and message embedded. If the process is successful, it will show message of message embedded successfully. Obtain the cover image (the image in which the message will be hidden) and the secret message. Select a steganographic technique for embedding the message into the cover image.

Fig 6. Result for Retrive Message

Fig 6. In this result for Retrive message in which user can retrive the message behind the image. User has to enter the input file and it will be embedded. If the message is successful, it will show retrived file successfully. Select the appropriate steganographic extraction technique based on the method used to embed the message.

Fig 7. Result for Water Mark Image

Fig 7 Describes the output of Water Mark Image. If the user has to select input file which is embedded. The embedded process is successful then it will show message, as Embed message completed successfully and it will give the text output. Obtain the original image to be watermarked and the watermark image or text.

Image steganography process:

1. Start: Begin the steganography process.
2. Input Cover Image and Secret Message: Obtain the cover image (the image in which the secret message will be hidden) and the secret message.
3. Choose Steganographic Technique: Select a steganographic technique suitable for hiding the message within the cover image. Common techniques include LSB (Least Significant Bit) substitution, frequency domain techniques (e.g., Discrete Cosine Transform), and spatial domain techniques (e.g., Spatial LSB).
4. Convert Message to Binary: Convert the secret message into binary format. This step is necessary to represent the message in a form suitable for embedding within the image.
5. Analyze Cover Image: Examine the cover image to identify suitable locations for embedding the binary message. These locations should be inconspicuous and unlikely to attract attention.
6. Embed Message into Cover Image: Modify selected elements (such as pixel values or frequency components) of the cover image to embed the binary representation of the secret message. This modification is typically done in a way that minimizes visual distortion and maintains the cover image's appearance.
7. Output Stego Image: Generate the stego image, which is the cover image with the hidden message embedded within it.

Text Steganography Process:

1. Convert Message to Binary (if applicable): If the secret message is in a non-binary format (such as text), convert it into binary format. This step is necessary for certain steganographic techniques that operate on binary data.
2. Analyze Cover Text: Examine the cover text to identify suitable locations for embedding the binary message or modifying the text. These modifications should be inconspicuous and not affect the readability of the text.
3. Embed Message into Cover Text: Embed the binary representation of the secret message into the cover text using the chosen steganographic technique. This may involve inserting additional characters, modifying existing characters, or adjusting formatting elements.

5. CONCLUSIONS

The Secure Data Transmission provides the information to hide private data to cover media that appears to be innocent. Using Steganographic techniques for embedding and AES for encryption, this method guarantees the integrity and confidentially of data being conveyed. Steganography and AES for encryption work together to create a multi-layered defense system against detection and unwanted access. In image Steganography provides a secret method of communication. It includes digital watermarking and hidden messaging. Steganographic technique are becoming increasingly important as technology develops in order to provides safe and dependable communication connections. In text steganography provides a way to communicate covertly by encoding secret messages into otherwise innocent looking text. Overall, text steganography stands as a valuable tool in the arsenal of covert communication techniques, offering a subtle yet potent means of concealing sensitive information within seemingly innocuous text data. Text steganography holds significance in scenarios where overt encryption methods may raise suspicion or attract unwanted attention.

REFERENCES

[1] B. Granthan, "Bitmap Steganography: An introduction,"April1997.

[2] Nurhayati and S.S.Ahmad,"Steganography for inserting message on digital image using aes cryptography algorithm,"2016 4th international Conference on

computer application an journal of electronics and telecommunication 65 2009.

[3] B. Bindu, L. Kamboj, and P. Luthra, "Information Hiding using steganography," Int. J. Adv. Res. Comput. Sci., vol. 9, no. 2, pp

[4] T. Morkel, J.H.P. Eloff and M.S.Olivier "An overview of image Steganography".

[5] N.Provos and P.Honeyman, "Hide and seek: An introduction to steganography," January 2004

[6] J. Krenn, "Steganography and steganalysis," January 2004.