IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 11, Issue 8, August 2022

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.118

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 8, August 2022||

| DOI:10.15680/IJIRSET.2022.1108099 |

Enhancing Network Security using Digital Image Processing, Cryptography & Steganography

Dewang Mehta1, Thenmozhi T[2], Geerisha Jain[3]

Associate Consultant, Business Technology Solutions at ZS, Pune, Maharashtra, India[1]

Professor, Department of Computer Science Engineering, KGISC Institute of Technology, Coimbatore, India[2]

Software Engineer, Shell India Markets Private Limited, Bengaluru, India[3]

ABSTRACT: Quite often,we communicate exceedingly confidential information over a communication network that we want only the recipient to know. How do we protect such information from malicious attacks? Techniques like steganography, encryption and cryptography can be used to keep our data confidential.But, a combination of these techniques would help us keep our data highly confidential while nullifying the short comings of each of them when used individually. In this paper, we address the problem of security breaches using digital image processing. We know that email service providers sell our data to third party companies for their usage and profits. In today's scenario, security is a major concern while transmitting any information over the network. Security provided by the network is insufficient with the increasing rates of cybercrimes. Therefore, we need to employ other techniques to carefully send our data over the network. In this paper, we explore a number of security techniques that can be combined together to ensure higher levels of security to our data.

KEYWORDS: cryptography, steganography, watermarks, LSB, AES, cryptographic keys, digital signatures

I. INTRODUCTION

In this proposed project, we address the problem of enhancing security of a secret image and secret message that is to be sent over a network, by digitally processing it. We require that the secret image and secret message to be sent to the recipient in such a way that no one else suspects the existence of them. A cover image is used as a decoy in this technique in which the secret image as well as the secret message is embedded. On the sender's side, the secret image is encrypted using AES Algorithm. In this encrypted secret image, the secret message is hidden using LSB Based Image Steganography. Furthermore, the encrypted secret image with the secret text is hidden in the cover image, using LSB Based Image Steganography. The stego image thus obtained is split into 16 parts, indexed and sent to the receiver. On the receiver side, these sub images are fetched one by one and merged based on their index. The encrypted image is obtained from the merged image. Next, we extract the secret text from the LSBs of this encrypted image. Additionally, decryption is performed to extract the original secret image from the encrypted secret image. Thus, the receiver obtains the secret image and the secret message from the cover image.

Paper is organized as follows. Section II describes various algorithms that have been derived earlier with an attempt to curb this network security issue. The flow diagram represents the step of the algorithm. After detection of text, how text region is filled using an Inpainting technique that is given in Section III. Section IV presents experimental results showing results of images tested. Finally, Section V presents conclusion.

II. LITERATURE SURVEY

Septimiu Fabian Mare et al, introduced a new communication system that uses a unique combination of two state cryptographic algorithms i.e. asymmetric RSAand AES with symmetric key cryptography with steganography. The combination of these techniques generates a strong communication system resistant to multiple types of attacks, detection and reverse engineering processes. Our model is built in such a way that it offers a solution to the majority of defects in other stenographic communication systems. [1]

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 8, August 2022||

| DOI:10.15680/IJIRSET.2022.1108099 |

DNA is a medium for communication system for data security since it is a strong security method that achieves maximum protection with low modification rate and high capacity. A new security method can be built by taking theall benefits of DNA based steganography and AES cryptography. This method will provide a double layer security to the secret message. In this technique, the message is encrypted to DNA bases and then AES algorithm is applied on it. This unique methodology provides multi-layer data security to the message. [2]

Utsav Sheth et al., describe a unique technique in which data is hide in an cover image. The lower nibble of each cover image byte is changed so that each nibble contains an input text. The steganography technique used in this implementation increases the data capacity of the cover image and also ensures high level protection. The Java libraries are used for easy implementation. A simple Graphic user interface has been developed using Java's applets and SWING packages. The AES cryptographic technique is further used for improving the data security of the model.[3]
This paper introduces an special technique in which the alice encodes the message using asymmetric cryptographic algorithm. This technique provides double layer protection by encoding the text using multiple algorithms such as Modified Vigenere Cipher algorithm and data is hidden in a cover image using Least Significant Bit steganography. The Least Significant Bit (LSB) is the most commonly implemented algorithms in spatial domain image steganography. At the bob side the secret data message is extracted from the cover image and is then decrypted using different decoding algorthims to extract the original message back. In this paper, G.Prashanti is using Matlab as a simulator to implement the techniques of encryption and steganography. Matlab provide highly computing environment and advanced in built function for image processing.[4]

In this paper, Ammad Ul Isla proposed a unique image stenographic methodology based on most significant bits (MSB) of image pixels. The first bit is used to store the secret bits based on the difference of MSB bit of the cover image and the secret message bit. If the difference of the first bit and secret message is different then the value of bit MSB is changed. The results explain that the given technique ensures significant improvements in signal to noise ratio. Normally, the attackers focus on LSB bits for secret information extraction but the given technique utilizes the MSB bits that are the biggest advantage of this secure algorithm. Also , the given methodology is not only secure, but computationally efficient and fast[5].

In this paper Prof. Beenish Mehboob, compares the various different cryptographic techniques. The main goal of steganography is to hide the data content during the transmission process. The success of stenographic technique depends on the confidentiality and data integrity. The information security also relies on the robustness of the implemented technique. The most commonly used is the Least Significant Bit algorithm for image steganography. We compress the secret information and encode it using the public key of the bob along with the stego key and embed both encrypted messages using a strong algorithm. The output image is obtained by using any stegno algorithm on the information and cover picture and we can saved this out image into different file formats like BMP or PNG. Saving images in these particular formats provides lossless compression during transmission. This paper gives a complete overview on the art of Steganography and gives a unique technique to hide data in a RGB color image [6].

This paper proposes a new methodology of using AES algorithm, to improve the data protection of the hidden information in the two proposed techniques for steganography i.e. the genetic algorithm and path relinking. It also combines the two techniques forming a new hybrid approach that provides the benefits of both the algorithms. It uses the LSB (least significant bits) a substitution algorithm for hiding that enhances the quality of a steno picture. It also improves the possibility of hiding information inside RGB images significantly, increasing the capacity available for storing data by two times when compared to the steganography approach used by gray scale images.Also, all types of digital information from text and compressed files and even the executable programs can be hidden inside the cover image. This increases the scope of various application of the technique for exchanging information across different networks and hiding the data from attackers [7]

Dipti Kapoor Sarmah et al., developed a system where they build a new technique in which Cryptography and Steganography are combined together and implement it as an integrated part along with newly build enhanced security system. In steganography we are using AES algorithm to encode a secret data and a part of the data is hidden in DCT of an image and the rest of the message is used to generate two secret keys which provides multi layer security to this model. [8]The proposed method is summed up by embedding data files into digital media with steganalysis done by Reddy, V. L., Subramanyam et al. [9]

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 8, August 2022||

| DOI:10.15680/IJIRSET.2022.1108099 |

G. G. Rajput et al., focus on image based steganography for hiding data in this paper. He uses LSB technique for embedding text information i.e. secret image in digital RGB color images is proposed. Secret text is encrypted using Least Significant Bits (LSB) of three components of color image namely, red, green and blue (RGB) channels using the angular transformation concept. [10]

Chikouche et al., t reduce the length of hidden message by Deflate algorithm which is a lossless data compression technqiue that combines the LZ77 algorithm and the Huffman algorithm. Another advantage of using this technique is to provide data security the reduced hidden data by AES algorithm. Their experiment results show that the improved approach is most effective compared to existing approaches. [11]

III. METHODOLOGY

The methodology used in this paper is that we have introduced a new secret data communication system that employs the usage of two state-of-the art cryptographic algorithms (RSA through asymmetric keys and AES through symmetric key) along with steganography. The merging of these three techniques generates a robust steganography-based communication system with ability to withstand various types of attacks, their detection and in turn its reverse engineering. This system was designed in a way that offers a solution to the major flaws presented in other stenographic communication systems. [1][12] This paper introduces an algorithm in which the sender encrypts the secret message using a cryptographic algorithm which uses a secret key which is shared between the sender and receiver. This method provides dual security by encrypting the message using different algorithms such as Modified Vigenère Cipher algorithm and data is hidden in an image using LSB or MSB steganography. The Least Significant Bit (LSB) is one of the frequently used techniques in spatial domain image steganography. At the receiver side the message is extracted from the image and is then decoded using various decryption methods to get the original message. In this paper, G.Prashanti is using Matlab as a simulator to implement the techniques of encryption and steganography. Matlab provide highly computing environment and advanced in built function for image processing.[4] The methodology used in this paper is the focus on image based steganography in this paper. An innovative approach established on LSB technique for embedding text data precisely, secret image in digital color images is proposed. Secret text is encoded in Least Significant Bits (LSB) of three components of color image namely, red, green and blue (RGB) channels using the angular transformation concept. [10]

Our project provides all characteristics and features required to develop a secure system:

A. Authentication:The Authentication is the process of recognizing a user's identity. We have developed a login page through which the end user is validated before he can send any message.
B. Confidentiality:Confidentiality means personal data being shared with other individuals that ideally cannot bedivulged to third parties without having a consent of the user. The secret message is encrypted using AES algorithm before transmission, so confidentiality is ensured.
C. Data Integrity:Data security refers to the protection of data against unauthorized access or corruption and is necessary to ensure data integrity. The secret message as well as the secret image are encrypted using cryptographic algorithm AES
D. Non-Repudiation:Nonrepudiation is the guarantee or surety that someone cannot deny something. Generally, non-repudiation denotes the capability to ensure that a party in a certain contract or perhaps a communication cannot deny the authenticity of their signature on a formal document or even the sending of a message that they initiated. In our project, we are putting a digital signature using SHA-1 algorithm to guarantee non- repudiation.
E. Embedding Effectiveness:Likelihood to embed confidential messages effectively in an arbitrary cover
F. Key Exchange:The RSA algorithm can be leveraged for both signing digital signatures and additionally making symmetric key exchange. Here the proposed model is using RSA algorithm for generating the keys for every specified user.
G. Privacy:Privacy guarantees that personal information is collected, processed, preserved, and destroyed legally and justly.
H. Robustness:Capability to detect the confidential message after signal processing operations
I. Security:Secure the cover message and statistically imperceptible model.
J. Stego Key:Combining the secret key with the stenographic algorithm to embed a covert message into a cover Work.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 8, August 2022||

| DOI:10.15680/IJIRSET.2022.1108099 |

Specifications:

- Matlab v15 or above
- Windows 10

Methodology at the sender's end:

• The details of the user are received from the HTML form that is the username and password is accepted
• In case the user is authenticated and has an existing account, then the second page opens.
• The private key, public key, sender's message and decryption of the receiver's message are given as options tothe user.
• The public and private keys are generated through RSA algorithm for each user.
• The secret message of the sender is taken as input and encrypted using AES algorithm to provide confidentiality.
• An image is taken as an input from the user in which the user wants to embed the secret message
• The image is also encrypted using AES algorithm.
• A digital signature is added to the secret message using SHA-1 algorithm using the sender's private key.
• The encrypted and digitally signed secret message is then embedded in the encrypted image using Least Significant Bit algorithm in which the LSB of the pixels of the image are replaced with the secret code.
• The encoded image is then again embedded into another cover image.
• The resulted stego image is then divided into multiple parts (16 to be specific).
• Each part is then separately sent to the recipient.

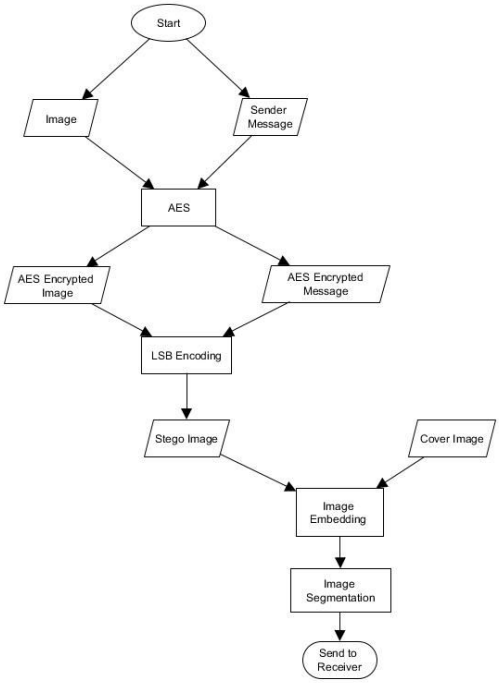

Fig.1 Sender side mechanism

Methodology at the receiver's end:

• On the receiver's end, the sub images are stitched back based on their index values (0 to 15) to regain the original cover image.
• To extract the encrypted image with the encrypted text from the stego cover image, we extract the LSB of all red, green and blue components.
• The encrypted image is then decrypted using the AES decryption algorithm.
• Now, to extract the encrypted text from the image, we again extract the LSB bits of the red, blue and green components.
• The hash is again computed using SHA-1 algorithm using the sender's public key in order to get the encrypted secret message.
• The encrypted text is then decrypted using AES algorithm and hence the receiver can view the secret code.

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 8, August 2022||

| DOI:10.15680/IJIRSET.2022.1108099 |

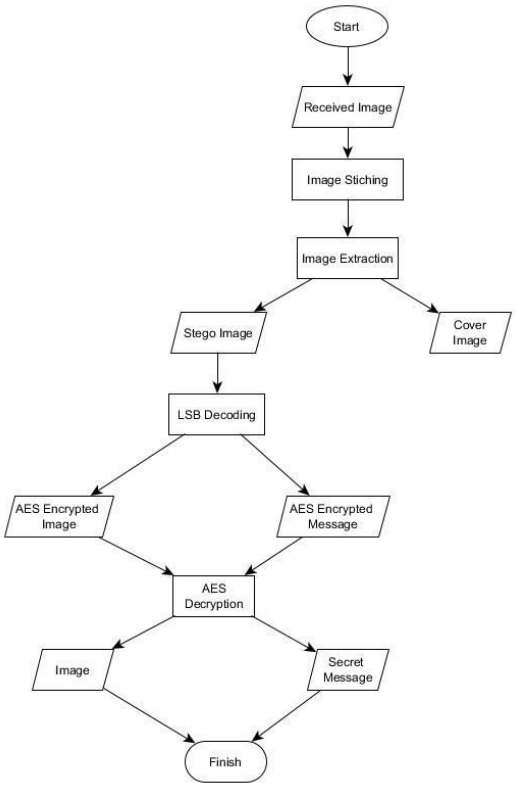

Fig.2 Receiver side mechanism

IV. EXPERIMENTAL RESULTS

Fig.3 Secret Image

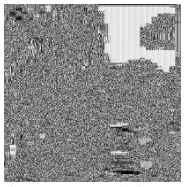

Fig.6 Encrypted image

Fig.4 Secret Image with embedded Text

Fig.7 Cover Image

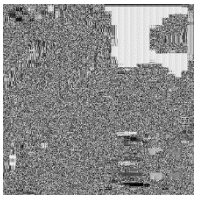

Fig.5 Secret Image with embedded Text

Fig.8 Embedded Cover image

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 8, August 2022||

| DOI:10.15680/IJIRSET.2022.1108099 |

Fig.9 Segmented images at the sender side

Fig.10 Merged image at the receiver side

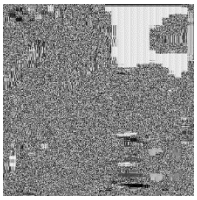

Fig.11 Extracted secret image

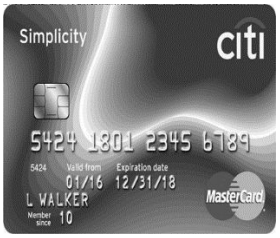

Fig.12 Decrypted Secret image

V. CONCLUSION

The work accomplished throughout this project is summarized with the subsequent points. During this project we have implemented a secure system using the combination of cryptography and Steganography. Steganography, particularly combined with cryptography, may be a powerful tool that allows individuals to speak without the eavesdroppers even knowing that there is some kind of communication. The provided methodology provides acceptable image quality with little distortion within the image. The best advantage of this Crypto/Stegno. System is that the strategy used for encoding, AES, is extremely secure and also the DCT transformation Steganography techniques are very arduous to discover. It additionally shows varied strategy utilized for the smallest amount vital bit relying upon the potency also as encoding standards used.

REFERENCES

[1] Septimiu Fabian Mare et al, Secret data communication system using steganography, AES and RSA, 2011 IEEE 17th International Symposium for Design and Technology in Electronic Packaging (SIITME).

[2] K S Sajisha et al., An encryption based on DNA cryptography and steganography, 2017 International conference of Electronics, Communication and Aerospace Technology (ICECA)

[3] Utsav Sheth et al.,Image steganography using AES encryption and least significant nibble, 2016 International Conference on Communication and Signal Processing (ICCSP)

[4] G.Prashanti" Data Confidentiality Using Steganography and Cryptographic Techniques" 2017 International Conference on circuits Power and Computing Technologies [ICCPCT].

[5] Ammad Ul Isla" An Improved Image Steganography Technique based on MSB using Bit Differencin"the Sixth International Conference on Innovative Computing Technology.

[6] Beenish Mehboob and Rashid Aziz Faruqui "A Stegnography Implementation"2008 IEEE.

[7] Aura Conc" AES Cryptography in Color Image Steganography by Genetic Algorithms" 2015 IEEE.

[8] Dipti Kapoor Sarmah et al.,Proposed System for data hiding using Cryptography and Steganography,

[9] Reddy, V. L., Subramanyam, A., & Reddy, P. C. (2012). Implementation of Least Significant Bit Steganography and statistical steganalysis. Proceedings of the Second17 International Conference on Computational Science, Engineering and Information Technology - CCSEIT

[10] Rajput, G. G., & Chavan, R. (2017). A Novel Approach for Image Steganography based on LSB Technique. Proceedings of the International Conference on Compute and Data Analysis - ICCDA '17. Chikouche, S. L., & Chikouche, N. (2017).

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.118

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details