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 12, Issue 4, April 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

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

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204312 |

Multi-Image Steganography Using Advanced Encryption Standard

Supriya Dighe, Namrata Shilimkar, Priti More, Chandan Thombare, Prof.Mrs. Sonal Shirke

Dept of Computer Engineering, Rajgad Dnyanpeeth's Shri Chhatrapati Shivajiraje College of Engineering, Bhor, India

ABSTRACT: Data transfer requires consideration of information security. Due to security issues, sending sensitive data or communications over the internet can be difficult. Typically, we use cryptography to communicate text-based secret communications and hide information. There are so many methods used nowadays to conceal information in any media. The use of steganography is one such method. Using Multi-image steganography to build a secure communication system will stop hackers from meddling with the sender and receiver's communications. The primary method of information concealment is picture steganography, in which the cipher text is included into a cover image that is almost invisible to unauthorised individuals who attempt to see it. Any type of text and picture can serve as the concealed information inside a cover image. Multi-image Steganography is defined conceptually as the action of breaking a secret code into many pieces and embedding each piece into a different cover picture. So, we put out two concepts for image steganography to make it exceedingly difficult for hackers to hide the data. The goal is to develop a safe and secure system, this study suggests using the Least Significant Bit (LSB) Steganography technique with the Advanced Encryption Standard (AES) Cryptography approach.

KEYWORDS : Cyber security, Encryption, Decryption, Security, Cryptography.

I. INTRODUCTION

As a part of information security "Steganography" is a wellknown concept, literally which signifies the meaning "covered writing". Steganography imposes the secret information within a cover object termed as stego-medium to escape detection and to retain the original information with minimum distortion. This stego-medium appears like a non-secret file in the network and manages to avoid drawing the attention towards itself as a content of security.

secret-information + cover-medium = stego-medium

Steganography used extensively for secure communication. The schemes used at this age are the physical process of Steganography. In modern digital steganography information is first encrypted. Then using an embedding algorithm in the transport layer encrypted information is embedded with the cover medium and transmitted over the network. Both cryptography and steganography provide data confidentiality and authenticity. In contrast to cryptography which focuses on keeping the message secret while the existence of secret message may tempt the attacker whereas Steganography hides a message aside from very existence of secret information. Cryptography ensures privacy of message and structure of the message alter whereas steganography ensures the secrecy of message and the structure of message does not alter. Steganography may use in conjunction with cryptography by concealing the existence of the ciphered text so that the information is more secure.

II. RELATED WORKS

AES

AES (Advanced Encryption Standard) It was necessary to replace DES as its key size is very small. With the growth of computer power, it is considered a threat to the full attack of search keys. DES triples were designed to solve this issue, however were discovered be slow. This is where AES starts to shine, which is found to be 6x times faster than Triple-DES. The most well-liked and prevalent accepted algorithm for symmetric encryption that can be achieved today is the Advanced Encryption Standard (AES). Unlike DES, in AES the quantity of cycles varies and is subject to the crucial length. AES works on using 128-bit keys, 192-bit keys, and 256-bit keys having 10,12 and 14 rounds respectively. In Modern cryptography, AES is well-liked and backed by hardware and software. To date, no effective crypto-analytic attacks on AES have included detected. Additionally, AES has an inherently flexible key length, allowing a level of 'future assurance' against the advancement of the capacity for perform key searches. There have 20 years since the

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204312 |

launch of the AES but has not yet adopted any knownattack right now, which is why it can safely be known as the unbreakable global standard of encryption.

Modes of AES Algorithm

1.ECB (Electronic Code Book):
It is the simplest mode among all. It divides the plaintext message block from size 128 bits. The blocks are then encryptedusing the same key and algorithm. Hence, it generates the same cipher text for the same block every time. It is regarded as weakness and therefore it is advised that not to use ECB for encryption

2.CBC (Cipher Block Chaining):
CBC (Cipher Block Chaining) operation method for block ciphers uses an Initialization Vector (IV) to improve encryption. The IV serves as the starting point for the chain of XOR operations that link the plaintext blocks together in the ciphertext.

3. CFB (Cipher FeedBack):
CFB can serve as a stream cipher. It encrypts the initialization vector (IV) first and then XOR with the plaintext to produce the cipher text. Then it encrypts the text in the cypher next plaintext block. In this mode, decryption can be performed in a parallel manner but encryption cannot be performed in a parallel manner.

4. OFB (Output FeedBack)
In OFB mode, the encryption process begins by encrypting the IV using the block cipher, and then XORing the resulting ciphertext with the first plaintext block to produce the first ciphertext block. This ciphertext block follow fed back into the block cipher to produce a new keystream block, which is XORed with the next plaintext block to produce the next ciphertext block.

Steganography
Steganography is the technique for hiding data and aims to hide data in a manner such that any eavesdropper cannot observe any changes in the original media. Steganography is a data encryption method and aims to encrypt the data in a manner such that any listener can see the changes in the original media. This is typically referring to the method of concealing existence of contact data. It hides information facts. It is a procedure for transferring data secretly from one digital medium to another before recovering it later.Any type of text and picture can be generate the concealed information inside a cover image. Multi-image Steganography is defined as conceptually as the action of breaking a secret code into many pieces and embedding each piece into a different cover picture. So, we put out two concepts for image steganography to make it exceedingly difficult for hackers to hide the data. To generate a safe and secure system, this study suggests using the Least Significant Bit (LSB) Steganography technique with the Advanced Encryption Standard (AES). Cryptography approach.

Text to image/ Image Steganography A digital picture is the most secure way to carry sensitive information through the internet using steganography. The picture is captured using the camera, the light of the camera will sense the object which should be captured, and it will be displayed on the screen of the camera. Image is the combination of the pixels; the resolution of the picture depends upon the pixel. Pixel is the minute area of illumination on a display screen. Human eyes cannot sense the pixels in the image. Pixel is made of three components. Three components of the pixel are Red, Green and Blue (R, G and B). Each pixel has a depth of 24 bits which is 3 bytes. Each component is of size one byte. Any color is formed by the combination of these three components. The byte value varies from 0 to 255. The color will be displayed based on the value of the bits, 0 is the darkest and 255 is the brightest. The size of the picture is given in the pixels, for example, the size of the picture is 600*450, and then the image is the combination of 2,70,000 pixels. pixel is made of three components which of each component is the size of 8 bits, for example, 11111111 00000000 00000000 is the pixel bits then the pixel will red in color. Depending upon the RGB values the pixel color will be changed. The hidden message that must be included inside the image is converted into the bits depending on their ASCII value. Then these data bits will be stored in the image based on the steganographic technique used. Steganography is related to a variety of high technology where data is hidden into an image file. This is possible to replacing redundant bits of less important in the original data.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 12, Issue 4, April 2023 ||

| DOI:10.15680/IJIRSET.2023.1204312 |

III. PROPOSED SYSTEM

Multiple private keys, you're the system can support many secret images to be hidden within a single cover image, while also making sure that only authorized users who possess the proper private key can access each hidden image. This adds an additional layer of security to the steganography process, as it prevent access by unauthorised users the hidden images even if they are able to detect that steganography is being used.
Additionally, it's worth noting that your system's approach of not disclosing information about other hidden images when one image is accessed is also a useful security feature. This ensures that even if one of the hidden images is compromised, the remaining images will still be protected and not disclosed to unauthorized users.
Overall, your proposed system appears to provide enhanced security and privacy for multi-image steganography, which could be useful in a variety of applications where sensitive images need to be transmitted or stored securely.

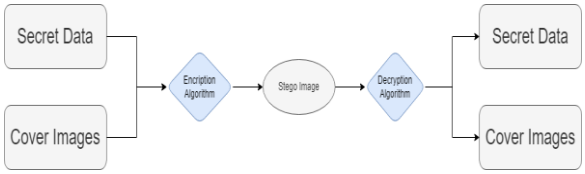

Fig. Flow of the System

IV. CONCLUSION

In this age of civilization exchanging data for communication through the network is an integral part of every organization and every sector of society. Our proposed algorithm is to secure this communication with a secure communication system by creating a distributed connection. This algorithm imposed an encrypted text that has undergone encryption using the AES algorithm within a JPEG image and then the image file is sent over the network i.e. we combine the concept about Cryptography and Steganography making an illusion to the hacker that the sender sends an unsuspicious media file to the receiver. As an image file appears in network as an innocent media file so this doesn't attract the hacker as the content of security.

REFERENCES

1. Abhishek Das, Japsimar Singh Wahi, Mansi Anand, Yugant Rana. "Multi-Image Steganography Using Deep Neural Networks".
2. Vajiheh Sabeti, Shadrokh Samavi, Mojtaba Mahdavi,ShahramShirani,"Steganalysis of Pixel-Value Differencing Steganographic Method"
3. Vojtech Holub*, Jessica Fridrich and Tomáš Denemark,"A Universal distortion function for steganography in an arbitrary domain"
4. Vojtˇech Holub and Jessica Fridrich,":Designing Steganographic Distortion using Directional Filters".
5. Po-Yueh Chen* and Hung-Ju Lin,"A DWT Based Approach for Image Steganography".
6. Taha M.S." Combination of Steganography and Cryptography".
7. Utsav Sheth, Shiva Saxena. "Image Stegonography using AES encryption algorithm".
8. Md Ahamand, Md Abdullah. "Comparison of encryption algorithm for multimedia".
9. M. Pitchaiah, Philemon Daniel, Praveen. "Implementation of advanced encryption standard algorithm".
10. Behrouz Forouzan. "Cryptography and network security".

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.423

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