International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 12 | Dec 2022 www.irjet.net p-ISSN: 2395-0072

Review on: Combination of Cryptography and Steganography for Secure File Transfer Over Internet

Aishwarya Patni[1], Sakshi Kulkarni[2], Prachi Patel[3], Manali Satav[4], Nilam Jadhav[5]

[1]*Student, Department of Information Technology, Dr. D. Y. Patil Institute OF Technology, Pimpri, Pune, Maharashtra, India*
[2]*Student, Department of Information Technology, Dr. D. Y. Patil Institute OF Technology, Pimpri, Pune, Maharashtra, India*
[3]*Student, Department of Information Technology, Dr. D. Y. Patil Institute OF Technology, Pimpri, Pune, Maharashtra, India*
[4]*Student, Department of Information Technology, Dr. D. Y. Patil Institute OF Technology, Pimpri, Pune, Maharashtra, India*
[5]*Assistant Professor, Department of Information Technology, Dr. D. Y. Patil Institute OF Technology, Pimpri, Pune, Maharashtra, India*

Abstract - *In today's world, file transfer over the internet is not secure. The main reason for this insecurity is the presence of a third party. To avoid this, the concept of cryptography is used. In cryptography, the data is converted into an unreadable format known as cipher text. This cipher text can be decrypted only by an authorized person. However, the problem with cryptography is that the data is in an unreadable format, so the sender and the receiver must have the same key to decrypt the data. If the key is lost, then the data cannot be decrypted. To overcome this problem, the concept of steganography is used. In steganography, the data is hidden in some other file. The file in which the data is hidden is known as the carrier file. The carrier file can be an image, audio, video, etc. The advantage of steganography is that the data is hidden in another file, so even if the carrier file is intercepted, the data cannot be decrypted. So, if we combine the concept of steganography and cryptography, we can achieve a more secure file transfer over the internet. In this method, first, the data is encrypted using a key. Then this encrypted data is hidden in a carrier file. So, even if the carrier file is intercepted, the data cannot be decrypted without the key.*

Key Words: steganography, cryptography, asymmetrical, secure, cloud storage, rsa, aes, lsb

1. INTRODUCTION

Data security has become a significant concern for individuals and organizations in recent years. The proliferation of sensitive information stored on computers and transmitted over networks has made data security a critical issue. One of the most effective ways to protect data is to use a combination of steganography and cryptography. Steganography is the practice of hiding information in plain sight. In data security, steganography can be used to conceal the contents of a file or message within another file or message. Cryptography is the practice of secure communication in the presence of third parties. In data security, cryptography can be used to encrypt the contents of a file or message, making it unreadable by anyone who does not have the key to decrypt it.

Using a combination of steganography and cryptography can be an effective way to secure data. The data can be encrypted using cryptography, and then the encrypted data can be hidden using steganography. This two-step process makes it much more difficult for attackers to obtain the data, as they first need to decrypt and locate the hidden data. There are several different ways to combine steganography and cryptography. One common approach is to use a tool that supports both methods. This allows the data to be encrypted and hidden with a single tool, making the process more efficient. Another approach is to use two separate tools, one for each method. This can be more secure, as it makes it more difficult for an attacker to obtain the encryption key and the location of the hidden data. However, this approach can be more challenging to manage, requiring two different tools. Combining steganography and cryptography can be an effective way to secure data. Using both methods, the data can be hidden and encrypted, making it much more difficult for an attacker to obtain the data.

2. LITERATURE SURVEY

[1] Vishnu S Babu, Prof. Helen K J (2015): This article has reviewed various cryptography and steganography method combinations. They were dealing with image-based steganography, and, according to their research, reducing image quality degradation is the main task to improve security. Their comparison suggested that DWT-based steganography with AES encryption can provide better security because this method can retain image quality.

[2] Aiswarya.s, Gomathi.r: According to this article, AES is the most widely used cryptography technique. It encrypts data in blocks, using a large block size. The author also believes that, for steganography purposes, a video is the best choice for a cover file. This is because video generally has a larger capacity to embed data than images or audio files. Spatial domain and transform domain techniques are used to embed the secret data.

[3] Surbhi Singla, Anju Bala (2018): This article provides an overview of a study and critical analysis of cloud computing security parameters and techniques, focusing on cryptography and steganography. The analysis shows that cryptography and steganography can be used to overcome some of the common security risks associated with cloud computing.

[4] Natasha Taneja, Dr. Prinima Gupta (2015): This article suggests combining Cryptography and Steganography will be the best choice as it will maximize security, ensure data integrity, and provide more authentication and privacy.

[5] Shashikant Singh, Seema Yadav, Ankur Raj, Priya Gupta (2018): In this article, the authors have done an analysis of the Global Journal of Computer Science and Technology Volume XIII Issue IV Version I 13 () Year 013 2 F © 2013 Global Journals Inc. (U.S.) A Review of Comparison Techniques of Image Steganography LSB, DCT & DWT methods. The author has successfully implemented these methods and delivered the results. The paper also compares the MSE and PSNR of the different methods. Furthermore, the paper presents a background discussion and implementation of the significant algorithms of steganography deployed in digital images.

[6] Surbhi D. Tiwari, Prof. Krunal J. Panchal (2017): This article has surveyed various types of audio steganography techniques, each with its advantages and disadvantages, providing a comprehensive overview of state of the art in audio steganography. The author concludes that the various audio steganography techniques expand the application possibilities and requirements to provide hiding capacity, a high level of data security, data embedding rate, data extraction rate, and various other factors.

[7] S. Joseph Gladwin, Pasumarthi Lakshmi Gowthami (2020): In this article, the author has used a combined elliptic curve cryptography algorithm with the Hill cipher to encrypt text, which reduces computation overhead. The author then applied DCT to the secret image and embedded 40% of the resulting DCT coefficients into the base image.

[8] Rina Mishra, Praveen Bhanodiya (2015): According to the articles, the authors has found that the problem with cryptography and steganography techniques is that they both require a large amount of space to hide confidential data. To solve this problem, the author suggests that data compression measures should be taken along with both techniques. Compression can be performed on the secret message or cover image before embedding. However, the LSB technique is the most widely used, but it has many drawbacks, such as degrading the image's quality and creating suspicions. So, the author suggests that embedding on the edge area is a better option for data hiding. Because changes in the edge are not easily identifiable, and a massive amount of data can be stored without being detected.

[9] Krishna Chaitanya Nunna, Ramakalavathi Marapareddy (2020): This article concluded that using crypto steganography can achieve two levels of security. There will be no third-party interruption by using this technique because no one can even know that data is embedded into the image, as no noise will be created in the cover image. It provides a high level of integrity and confidentiality of messages.

[10] Kamred Udham Singh (2014): This article discusses audio steganography, the process of hiding data in digital audio signals. They state that the frequency domain is preferred over the temporal domain for data embedding and that music signals are better covered in capacity, inaudibility, and Undetectability. They conclude that the flexible nature of audio file formats and signals makes them good and practical mediums for steganography.

[11] Mohammed Abdul Majeed, Rossilawati Sulaiman, Zarina Shukur, and Mohammad Kamrul Hasan: This article demonstrates both increasing the capacity factor in the format-based method and increasing security in linguistic steganography are still popular topics in text steganography.

[12] Mehdi Hussain, Mureed Hussain (2013): Different proposed techniques in this article have been critically analyzed by the authors, which show that the image's visual quality degrades when the confidential data is increased up to a specific limit using LSB-based methods. Many embedding techniques can be broken or show indications of alteration of the image by careful analysis of the statistical properties of noise or perceptual analysis.

[13] Challa Aksharasree, Dr. B. Indira Reddy (2018): In this article, concepts of cryptography steganography and their applications in securing digital data across the network is studied, and a survey of modern techniques which combined steganography and cryptography is presented.

[14] Souma Pal, Prof. Samir Kumar Bandyopadhyay (2016): In this article, the authors only discuss the Neural Network method (N.N.), and their performance is evaluated on four criteria: the number of secret images, pixel expansion, image format, and type of share generated.

[15] Jayaram P, Ranganatha H R, Anupama H S (2011): The author of this article concludes that audio data hiding techniques can have several uses beyond covert communication or deniable data storage, such as information tracing, fingerprinting, and tamper detection.

3. SECURE FILE TRANSFER SYSTEM USING A COMBINATION OF CRYPTORAPHY AND STEGANORAPHY

3.1. Proposed System

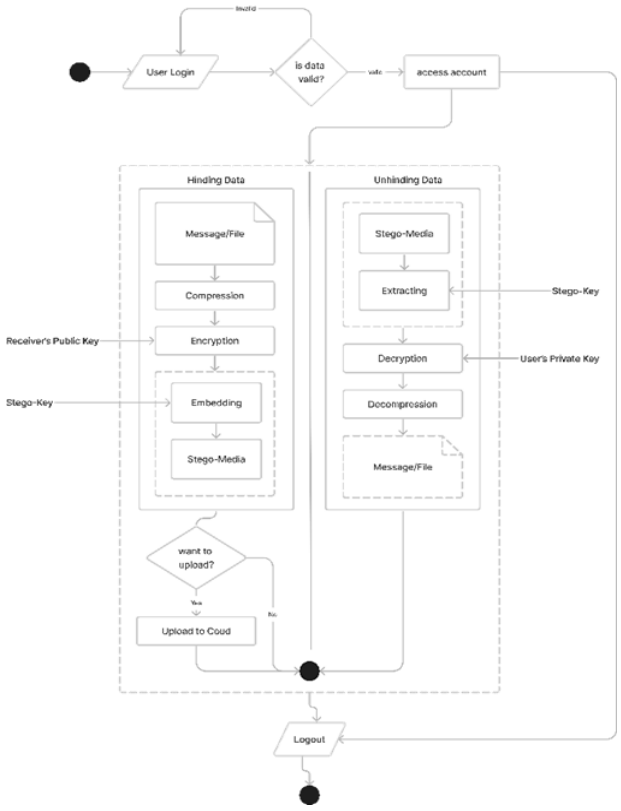

Fig -1: Flow Chart

The flow of the proposed system

1. Users can create an account using his/her data or can log in using existing credentials.

2. After login, the user can either hide data into a file (using a combination of cryptography and steganography) or unhide data from the hidden file using the proposed system.

3. If the user chooses to hide data, then he/she can upload that resulting stego-file (in which the data is hidden) to cloud storage so that the user can share the file link with the receiver.

4. This system will use asymmetric cryptography as the default method, which means files/data can be encrypted using the receiver's public key, known to everyone, and decrypted using the receiver's private key, which is only known to the receiver.

The sole purpose of this system is to make private/confidential data sharing secure using two-layered security like cryptography and steganography. This system consists of 4 modules: authentication, asymmetrical cryptography, steganography, and cloud storage.

1. Authentication: This proposed system is an android application. At the very beginning of opening the application user will be asked to enter credentials to log in, in case the user is a new user who can register/signup.

2. Asymmetrical Cryptography: The data hiding consists of two stages; this is the first of them, the user will be asked to enter the receiver's public key to encrypt the data/file.

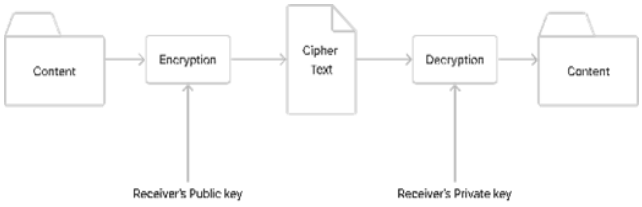

Fig -2: Asymmetrical Cryptography

3. Steganography: This is the second stage of hiding data; the user will be asked for the file type and file to hide data into it.

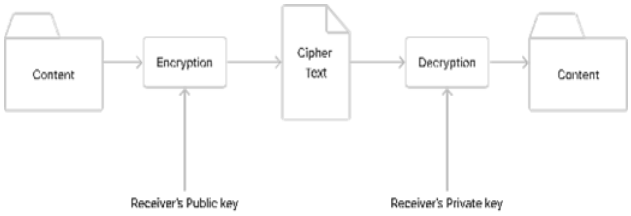

Fig -3: Steganography

4. Cloud Storage: The resultant file will be stored in the device's local storage and uploaded to the cloud storage if the user permits.

3.2 Algorithmic Survey

3.2.1 Cryptography Algorithms

A. DES Algorithm

The Data Encryption Standard (DES) is a now-outdated standard for the encryption of electronic data. It was a symmetric-key algorithm invented in the early 1970s at IBM. DES used a 56-bit key for encryption, which is now considered too small. DES can be cracked using brute force attack. DES has been superseded by the more secure Advanced Encryption Standard (AES) algorithm. [1,2,13]

B. AES Algorithm

Advanced Encryption Standard (AES) is a standard for the encryption of electronic data. The U.S. government developed AES in 1997 and now uses it worldwide. AES is a symmetric-key algorithm, meaning both the sender and the receiver use the same key. This AES standard specifies the Rijndael algorithm, a symmetric block cipher that can process data blocks of 128 bits using key sizes of 128, 192, and 256 bits. The input, the output, and the cipher key are used in Rijndael. It takes an input and output of a block size of only 128 bits. [1,2,13]

C. RSA Algorithm

RSA is one of the earliest public-key cryptosystems widely used for securing data transmission. RSA was first described in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman of the Massachusetts Institute of Technology. In RSA encryption, the key used for encryption is public, while the key used for decryption is kept secret. RSA is based on factorizing two large prime numbers. The public and private key-generation algorithm is the most complex part of RSA cryptography. We can generate two large prime numbers, x and y, using the Rabin-Miller primality test algorithm. A modulus is calculated by multiplying x and y. This number is used by public and private keys and provides the link between them. Its length is called the key length. [1,13]

D. DSA Algorithm

The DSA algorithm is more complicated than the RSA algorithm. In DSA, data is encrypted with a public key and sealed with a digital signature. On the receiving side, the signature is opened by an authorized person, and the data is decrypted with a private key. [2]

E. Elliptic Curve Cryptography (ECC)

ECC is based on the principle of discrete logarithms, which allows for smaller key sizes while providing the same level of security as RSA with larger key sizes. [2]

3.2.2 Steganography Techniques

Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video. The word steganography combines the Greek words steganos (στεγανός), meaning "covered, concealed, or protected", and graphein (γράφειν), meaning "writing". Steganography is often used to conceal secret messages in an image or audio file, but messages can also be concealed in other files. Many carrier file formats can be used, including images, audio, video, and text files. [1]

There are the following types of steganography:

A. Text Steganography

The private data is hidden in the text cover file in binary format without degrading the quality of the text file. [1]

B. Image Steganography

The image is first converted into binary form; then, the private data is hidden in the selected pixel using spatial domain or transform domain techniques. [1]

C. Audio Steganography

The private data is hidden using different steganography techniques in the audio cover file. Audio is converted into the binary form, and the private data is hidden in selected bit positions to produce the stego audio file.

D. Video Steganography

In this video, the secret data is hidden in the frames and audio of the video. Compared to other techniques, steganography provides more security because it has a larger capacity to hide private data. It is also difficult to process a video for steganography, making it a more secure technique. [1]

Different techniques of steganography:

1. LSB Method: The LSB method is the most widely used spatial domain technique. The first bit on the right side is known as the LSB bit. This method alters the least significant bit of the selected pixel/bit by the confidential data. [2,5,6,9,11,13,14,15]

2. Pixel Value Differencing Method: For the selected consecutive pixels, the difference is calculated. Based on the difference, confidential data is embedded using the LSB method. [2]

3. Most significant bit Method: In this method, the leftmost (MSB) bit is altered by the confidential data. The leftmost bit is the MSB, which contains a high pixel resolution. [2]

4. Quantization Index Modulation (QIM) The QIM method is a multi-bit embedding technique that uses the principle of M-ary amplitude modulation for embedding multi-bits. [2].

5. Discrete Cosine Transform: DCT can integrate information well. DCT changes an image from the time domain into the frequency domain and finds the redundant bits. [2,13]

6. Discrete wavelet Transform (DWT): A wavelet is a small wave that can hide data in transform coefficients of an audio signal or image pixel. This technique is known as the wavelet technique. [2,6,10,13,14]

7. Echo Hiding: Echo hiding embeds secret data into audio signals by introducing a short echo to the host signal. [6,10,14,15]

8. Phase coding: In this method, the initial phase of the audio segment is replaced with the reference phase of the secret message. [6,10,14,15]

9. Tone insertion: This technique relies on auditory masking. Psychoacoustical or auditory masking is where a stronger tone renders a weaker tone inaudible in the presence of another louder sound. [6,10,14]

10. Format-based: It encodes secret information by physically formatting a space that alters words horizontally, lines vertically, and the distance between words. [17]

11. Random and statistical base: This method creates cover text by analyzing the statistical properties of text, such as character and word sequences. It then uses these patterns to generate cover text in natural language. [17]

12. Linguistic method: The algorithm relies on the grammatical structure of the text as well as the meaning of words to encode the message. It first checks that the sentence structure is correct and then assigns values to words that have the same meaning as the words in the secret message. These values are then used to hide the message in the cover text. [17]

4. CONCLUSIONS

This paper proposes a system for secure file transfer over the internet that includes two security layers: cryptography and steganography; as per the survey, various cryptography and steganography techniques can be used with different file types, such as images, audio, video, and text. This paper suggests using LSB steganography as it is widely used and most effective, and asymmetric cryptography in place of symmetric cryptography provides more security.

REFERENCES

[1] D. Vishnu S Babu, Prof. Helen K J, "A Study On Combined Cryptography And Steganography", International Journal Of Research Studies In Computer Science And Engineering (Ijrscse) Volume 2, Issue 5, May 2015, Pp 45-49 Issn 2349-4840 (Print) & Issn 2349-4859 (Online)

[2] Aiswarya.s, Gomathi.r, "Review On Cryptography And Steganography Techniques In Video"

[3] Surbhi Singla, Anju Bala, "A Review: Cryptography And Steganography Algorithm For Cloud Computing", Proceedings Of The 2nd International Conference On Inventive Communication And Computational Technologies (Icicct 2018)

[4] Natasha Taneja, Dr. Prinima Gupta, "A Blend Of Cryptography And Steganography", International Journal Of Advanced Technology In Engineering And Science, Volume No 03, Special Issue No. 01, March 2015

[5] Shashikant Singh, Seema Yadav, Ankur Raj, Priya Gupta, "A Survey Paper On Different Steganography Techniques", Proceedings On International Conference On Emerging Trends In Expert Applications & Security (2018), Volume 2, 2018, Pages 103-108

[6] Surbhi D. Tiwari, Prof. Krunal J. Panchal, "A Survey On Audio Steganography With It "s Techniques", Vol-3 Issue-6 2017, Ijariie-issn(O)-2395-4396

[7] S. Joseph Gladwin, Pasumarthi Lakshmi Gowthami, "Combined Cryptography And Steganography For Enhanced Security In Suboptimal Images", 2020 International Conference On Artificial Intelligence And Signal Processing (Aisp)

[8] Rina Mishra, Praveen Bhanodiya, "A Review On Steganography And Cryptography", 2015 International Conference On Advances In Computer Engineering And Applications (Icacea)

[9] Krishna Chaitanya Nunna, Ramakalavathi Marapareddy, "Secure Data Transfer Through Internet Using Cryptography And Image Steganography", Ieee Southeastcon 2020,

[10] Kamred Udham Singh, "A Survey On Audio Steganography Approaches", International Journal Of Computer Applications (0975 – 8887) Volume 95– No. 14, June 2014

[11] Mohammed Abdul Majeed, Rossilawati Sulaiman, Zarina Shukur And Mohammad Kamrul Hasan, "A Review On Text Steganography Techniques"

[12] Mehdi Hussain, Mureed Hussain, "A Survey Of Image Steganography Techniques", International Journal Of Advanced Science And Technology Vol. 54, May, 2013

[13] Challa Aksharasree, Dr. B. Indira Reddy, "Role Of Cryptography And Steganography In Securing Digital Information: A Review", © 2018 Ijcrt, Volume 6, Issue 2 April 2018. Issn: 2320-2882

[14] Souma Pal, Prof.samir Kumar Bandyopadhyay, "Various Methods Of Video Steganography", International Journal Of Information Research And Review Vol. 03, Issue, 06, Pp. 2569-2573, June, 2016

[15] Jayaram P, Ranganatha H R, Anupama H S, "Information Hiding Using Audio Steganography – A Survey", The International Journal Of Multimedia & Its Applications (Ijma) Vol.3, No.3, August 2011

[16] Shivani Sharma, Dr. Avadhesh Gupta, Munesh Chandra Trivedi, Virendra Kumar Yadav, "Analysis Of Different Text Steganography Techniques : A Survey", 2016 Second International Conference On Computational Intelligence & Communication Technology

[17] Dhiral G.parghi, Krunal Panchal, Survey On Securing Data Using Text Steganography & Cryptography, Ijariie-issn(O)-2395-4396