International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 01 | Jan 2022 www.irjet.net p-ISSN: 2395-0072

A Literature Review on Image Steganography Using AES

Varsha D[1], Soundarya H K[2], Dr. Mohammed Tajuddin[3]

[1]Student, Dept. of Computer Science Engineering, Dayananda Sagar College of Engineering, Karnataka, India
[2]Student, Dept. of Computer Science Engineering, Dayananda Sagar College of Engineering, Karnataka, India
[3]Professor, Dept. of Computer Science Engineering, Dayananda Sagar College of Engineering, Karnataka, India

---

Abstract - *The art of concealing / hiding information or data bits on a cover or carrier file is known as Steganography. We can envisage Steganography being utilized in nearly any sort of file, including image files. Masking information, such as text, photos, or audio files, within other image files is known as Image Steganography. Image steganography enables the communication between one another, secretly and stealthily. To add even more security, the secret message, which is contained within the image file, is encrypted. Data compression is an important aspect of information security since compressed data is more secure and easier to manage. By encrypting data and hiding it from attackers, the primary purpose is to save physical space on storage devices and reduce the time it takes to transport data over the internet. The secret message is then coded and compressed before being combined into the compressed cover image file. The result stego-image is then sent to the receptor where the message is uncompressed, decoded and retrieved. This survey focuses on the methods implemented by authors of several works for hiding and securing the information.*

Key Words: Steganography, Cryptography, Data compression, AES, DWT, Huffman coding, LSB.

1. INTRODUCTION

The two most common security approaches are cryptography and steganography. Cryptography describes the process by which regular text is converted into unintelligible text and back again. The word "cryptography" has been invented utilizing an association of two Greek words, "Krypto" meaning hidden and "graphene" meaning written. Steganography involves the concealment of a message in an alternate message or in a real object. The name "steganography" comes from the Greek word "steganographia," which combines the words "stegano" and "graphia,", which means "covered or concealed" and "writing" respectively. We use the combined encryption and steganography to secure the classified message.

Information in visible form is encoded and decoded utilizing singular secret key in AES, a symmetric key encryption algorithm. The US National Security Agency (NSA) has sanctioned the Advanced Encryption Standard (AES) as the only publicly available encryption solution for safeguarding highly classified secret material. Originally known as Rijndael, AES is the result of the work of Vincent Rijmen and Joan Daemen. Here, the secret message is initially encrypted using AES encryption. Once it has been encrypted, the encoded message is then compressed using Lossless Data Compression, Huffman Coding, and the cover image is compressed using Lossy Image Compression, DWT.

In order to make texts, images and audio files transfer faster and take up less storage space; larger files have to be compressed to make them smaller. Larger files take longer to download or upload over the internet. These issues can be overcome by Compression. Any kind of data can be compressed. Lossy and lossless compression are the two basic forms of compression. To minimise the size of a file, the lossy compression technique removes some of the original data. Once the file has been compressed, the destroyed data cannot be recovered. The Discrete Wavelet Transform (DWT) comes under lossy compression and it is one of the image processing techniques. With the DWT, an image is turned into a series of wavelets, which can be stored much more capably than blocks of pixels. The image is not degraded or altered in any way when using lossless compression. A file can be remodeled exactly as it was when it was first produced because no data is lost during lossless compression. On the other side, lossless compression does not save as much space as lossy compression. Huffman coding is a lossless image compression technology that was developed to avoid code duplication while maintaining image quality. Huffman coding has a number of advantages over other data compression approaches, such as lossless data compression, which can be both effective and inexpensive to apply. The implementation entails the occurrence of all data, which is then ordered ascending. A Huffman tree was created as a result of the approach, which can be used to restore data to its original state after compression.

For the cover media, the Least Significant Bits (LSB) algorithm is used, which replaces the secret message bits with least significant bits and this algorithm is one of the most well-known algorithms in the industry. The human eyes cannot detect this change. It is very fast and simple. LSB steganography is utilised to incorporate the compressed secret message in the compressed cover image. The recipient receives this compressed Stego-Image

after it has been sent over the internet. Here, it is decompressed, extracted and decrypted. Similarly, there are many approaches for hiding and securing the data, which are explored in this survey.

2. LITERATURE SURVEY

A) Arshiya Sajid Ansari, Mohammad Sajid Mohammadi, Mohammad Tanvir Parvez, "A Comparative Study of Recent Steganography Techniques for Multiple Image Formats", (2019)

The paper work concentrates on the process of steganalysis, application and limitations of Steganography. It presents a deliberation on diverse steganography image file formats like JPEG, BMP, PNG and TIFF along with colour models for image formats like CMYK model, RGB model, HSL, HSV, NCS, DCT, DWT, LSB, etc. A modified inspection of the existing models are performed, on the basis of parameters like stego image perceptibility, technical resources and security facet. A souring range of PSNR reading designates fitter quality of stego image. The inspection shows that JPEG (DCT/DWT) algorithms are more unsusceptible to attacks and provide high reluctance to steganalysis. BMP spatial domain techniques have greater capacity but are easily vulnerable to steganography whereas the PNG palette techniques are more reliable and opportune for small size data implementation. Accordingly, Bitmap format is apt for high capacity requirement.

To mediate the secret message, one must opt a suitable blend of steganography method accompanying fit cover image format so that it disallows the captivation of the attacker.

B) Siddharth Singh and Raaghavv Devgon,"Analysis of Encryption and Lossless Compression Techniques for Secure Data Transmission", (2019)

The paper work traverse distinct compression methods and cryptographic techniques. Most applications online uses image or video file for communicating content. Due to restricted bandwidth available, compression methods are pertained, and to guarantee privacy of user encryption is executed. Apt solution is combination of encryption and compression techniques. The paper inspects methodologies in compression technique like Huffman coding, Run length coding, Arithmetic coding and Lempel- Ziv-Welch compression. Lossy compression involve Huffman coding and Discrete Cosine Transformation, whereas Lossless compression comprises of LZW and Run length coding. It also explores various cryptographic techniques like Caser Cipher, Data Encryption Standard and Rivest Cipher. An investigation was done on testing of image compression and encryption algorithm that are classified as: 1) Encryption followed by compression, 2) Compression followed by encryption, 3) Collaboration of encryption and compression.

The result presumed that the finest compression and encryption standards were performed by encryption of image initially followed by compression techniques.

C) Masumeh Damrudi, Kamal Jadidy Aval, "Image Steganography using LSB and encrypted message with AES, RSA, DES, 3DES, and Blowfish", (2019)

The paper examines the cryptographic techniques AES, RSA, DES, 3DES, and Blowfish, as well as the steganography algorithm LSB. The cryptographic algorithms are Java programmes that have been imported into the MATLAB environment. An investigation is done on the mentioned algorithms at the same time and same environment to contrast the discrete factors such as encryption and decryption time, PSNR, SNR, Histogram and MSE. To achieve high security, cryptography and steganography are blended and used. Firstly, using the mentioned algorithms data is encrypted, followed by the secret message embedded using LSB algorithm.

The investigation output led by the survey is that the execution time of RSA is more than other algorithms mentioned.

D) Osama F. AbdelWahab, Aziza I. Hussein, Hesham F. A. Hamed, Hamdy M. Kelash, Ashraf A.M. Khalaf and Hanafy M. Ali, "Hiding data in images using steganography techniques with compression algorithms", (2019)

This paper explores on the steganographic techniques along with compression algorithm. It explains the embedding and extracting algorithm. Here a comparison is done between two different techniques. Firstly, LSB algorithm is used with no encryption and compression. In second technique the secret message is encrypted and LSB is applied with DCT algorithm to transform the image into frequency domain.

From the outcome of the experiment, we come to know that, we need to hide the secret data while minimising its size, enabling more security. MSE and PSNR are used to assess the performance of these two approaches. The result of the experiment shows that using LSB and DCT effectively reduce the number of bytes in file, hence can be transmitted faster and takes less space on a disk.

E) Rashmi Kasodhan and Neetesh Gupta, "A New Approach of Digital Signature Verification based on BioGamal Algorithm", (2019)

Information security consists of aspects like authentication, confidentiality and integrity of data. In order to achieve this digital signature by original sender

and verification by deliberate recipient is crucial. The paper scouts classification of Digital Signature (DS) scheme such as, Direct Digital Signature and Arbitrated digital signature. The experiment approach is done using BioGamal algorithm, which includes DNA, and ElGamal algorithm. ElGamal is asymmetric algorithm used for encryption and decryption whereas DNA is used to generate cipher text. This method intensifies security and reduces time complexity.

Outcome of this experiment shows that, it is 30-40% efficient with respect to playgamal algorithm with encryption/decryption time.

F) Christy Atika Sari, Giovani Ardiansyah, De Rosal Ignatius Moses Setiadi, Eko Hari Rachmawanto, "An improved security and message capacity using AES and Huffman coding on image steganography", (2019)

Cryptography and steganography are two recurrent methods to implement security in information security domain. The paper prospects on methods like Discrete Wavelet Transform (DWT), AES and Huffman coding. The method lodged is combination of AES, Huffman coding and DWT which reduces the total bits in message. Examination of the experiment is done by PSNR and MSE.

The conclusion of the lodged method is that it lays out a good quality stego image with soaring capacity in DWT for steganography by diminishing the total message's bit up to 22.319% from the original message's bit. A good quality stego image is proved by obtaining the median of PSNR result more than 40db that is 46.1788.

G) Nandhini Subramanian, Omar Elharrouss, Somaya Al-Maadeed and Ahmed Bouridane, "Image Steganography: A Review of the Recent Advances", (2021)

This paper recce the recent advances of image steganography. It elucidates the traditional methods like LSB, PVD, DCT and EMD. These methods lead to distortion due to high capacity by encumber the cover image with more pixels for hiding secret message. The paper also explains the CNN based image steganography techniques and GAN steganography. An inspection is done with PSNR value comparison, which gives the output with prime PSNR value 64.7 obtained using cycle GAN. GAN based method uplifts security and hidden capacity. The paper also elaborates on challenges faced, scopes in future, etc.

The paper terminates that deep learning proves prodigious potential in image steganography.

H) Chitra Biswas, Udayan Das Gupta, Md. Mokammel Haque, "An Efficient Algorithm for Confidentiality, Integrity and Authentication Using Hybrid Cryptography and Steganography", (2019)

The paper traverse the distinct streams of cryptography and steganography. It explains the three primitives for steganography algorithms i.e., Security, Capacity and Robust. The proposed algorithm avail steganography and Hybrid cryptography. Firstly, using AES algorithm the message is encrypted and using public key of RSA even the symmetric key is encrypted, which escalates the security. The Hash value of message is engendered using public key of RSA to produce a digital signature. At receiver end, this is used to examine integrity. The message is embedded using LSB technique.

The result of the experiment is that the histogram for both cover image and stego image is identical, hence provides confidentiality, integrity and authentication.

I) Vikas Singhal, Yash Kumar Shukla, Navin Prakash, "Image Steganography embedded with Advance Encryption Standard (AES) securing with SHA-256", (2020)

The paper scouts the amalgam of three methods LSB, AES and SHA256. The proposed method accomplishes the task of securing information. It first hides the data using LSB technique and surfeit the protection of data using cryptographic technique AES-256 as well as the weak point that a hacker could target that is key, it also has been protected via the use of hashing technique SHA256.

The result shows a disguised image, making it non-viable to attract imposters. Hence, proposed system proves high security for classified information and exchanging it with no susceptibility.

J) Mustafa S. Abbas, Suadad S. Mahdi and Shahad A. Hussien, "Security Improvement of Cloud Data Using Hybrid Cryptography and Steganography", (2020)

The paper traverse on the drawback in cloud environment, i.e., security issues of data storage. The proposed algorithm is, initially the data is compressed using LZW algorithm, later hybrid encryption using AES symmetric and RSA asymmetric algorithms is performed. The encrypted data is hidden using LSB technique and hashing algorithm is applied.

Analysis is done using PSNR and SSIM values, which were calculated before and after applying compression technique. The result shows that PSNR values of stego image are better for compressed data when contrasted with non-compressed data.

3. MOTIVATION

The motivation in the back of growing image Steganography methods according to its use in diverse companies to talk among its members, in addition to, it may be used for communication among participants of the army

or intelligence operatives or agents of businesses to cover secret messages or in the subject of espionage. The main purpose of employing Steganography is to avoid attracting attention to the transfer of secret data. If suspicion is raised, then this aim that has been planned to reap the safety of the secret messages, because if the hackers make any changes to the sent message, this observer will try to figure out what data is buried therein.

The main motivations are:

- Protection of digital data and
- Information transferred via the Internet is kept private.

The goals are:

- By encasing the transmitted data in a cover material, the information becomes invisible.
- To improve the information's security and resilience to attackers.
- To achieve the CIA Triad of Information Security (Confidentiality, Integrity, and Authentication).

4. CONCLUSION

From the survey of existing methodologies and the techniques used for hiding the data, it can be seen that we need to use proper combination of techniques for security and efficiency of hiding the important data. Steganography conveys secrets across seemingly harmless covers in an attempt to hide a secret's existence. The employment and applications of digital steganography and its derivatives are increasing exponentially. Although the security of the Least Significant Bit technique is good, we can improve it in several ways by utilising different carriers and different keys for encryption and decryption.

REFERENCES

[1] Ashraf A. M. Khalaf, O. F. Abdel Wahab, A. I. Hussein and H. F. A. Hamed, "Hiding Data Using Efficient Combination of RSA Cryptography, and Compression Steganography Techniques", IEEE Access, volume: 9, Feb 2021.

[2] Arshiya Sajid Ansari, Mohammad Sajid Mohammadi and Mohammad Tanvir Parvez, "A Comparative Study of Recent Steganography Techniques for Multiple Image Formats", I. J. Computer Network and Information Security, 2019, 1, 11-25 Published Online January 2019 in MECS (http://www.mecspress.org/) DOI: 10.5815/ijcnis.2019.01.02

[3] Siddharth Singh and Raaghavv Devgon,"Analysis of Encryption and Lossless Compression Techniques for Secure Data Transmission", 2019 IEEE 4th International Conference on Computer and Communication Systems.

[4] Masumeh Damrudi and Kamal Jadidy Aval, "Image Steganography using LSB and encrypted message with AES, RSA, DES, 3DES, and Blowfish", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-8, Issue-6S3, September 2019.

[5] Osama F. AbdelWahab, Aziza I. Hussein, Hesham F. A. Hamed, Hamdy M. Kelash, Ashraf A.M. Khalaf and Hanafy M. Ali, "Hiding data in images using steganography techniques with compression algorithms", TELKOMNIKA, Vol.17, No.3, June 2019, pp.1168~1175 ISSN: 1693-6930, accredited First Grade by Kemenristekdikti, Decree No: 21/E/KPT/2018 DOI: 10.12928/TELKOMNIKA.v17i3.12230

[6] Rashmi Kasodhan and Neetesh Gupta, "A New Approach of Digital Signature Verification based on BioGamal Algorithm", Proceedings of the Third International Conference on Computing Methodologies and Communication (ICCMC 2019) IEEE Xplore Part Number: CFP19K25-ART; ISBN: 978-1-5386-7808-4

[7] Christy Atika Sari, Giovani Ardiansyah, De Rosal Ignatius Moses Setiadi, Eko Hari Rachmawanto, "An improved security and message capacity using AES and Huffman coding on image steganography", TELKOMNIKA, Vol.17, No.5, October 2019, pp.2400~2409 ISSN: 1693-6930, accredited First Grade by Kemenristekdikti, Decree No: 21/E/KPT/2018 DOI: 10.12928/TELKOMNIKA.v17i5.9570

[8] Nandhini Subramanian, Omar Elharrouss, Somaya Al-Maadeed, and Ahmed Bouridane, "Image Steganography: A Review of the Recent Advances", IEEE Access, volume: 9, Jan 2021

[9] Chitra Biswas, Udayan Das Gupta and Md. Mokammel Haque, "An Efficient Algorithm for Confidentiality, Integrity and Authentication Using Hybrid Cryptography and Steganography", International Conference on Electrical, Computer and Communication Engineering (ECCE), Feb 2019

[10] Vikas Singhal, Yash Kumar Shukla and Navin Prakash, "Image Steganography embedded with Advance Encryption Standard (AES) securing with SHA-256", International Journal of Innovative Technology and

Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-9 Issue-8, June 2020

[11] Mustafa S. Abbas, Suadad S. Mahdi and Shahad A. Hussien, "Security Improvement of Cloud Data Using Hybrid Cryptography and Steganography", 2020 International Conference on Computer Science and Software Engineering (CSASE), Duhok, Kurdistan Region – Iraq

[12]] Junxiu Liu, Jiadong Huang, Yuling Luo, Lvchen Cao, Su Yang, Duqu Wei and Ronglong Zhou, "An Optimized Image Watermarking Method Based on HD and SVD in DWT Domain", IEEE Access, volume: 7, July 2019

[13] Mustafa Cem Kasapbasi, "A New Chaotic Image Steganography Technique Based on Huffman Compression of Turkish Texts and Fractal Encryption With Post-Quantum Security", IEEE Access, volume: 7, Oct 2019

[14] Rashad J. Rasras, Ziad A. AlQadi and Mutaz Rasmi Abu Sara, "A Methodology Based on Steganography and Cryptography to Protect Highly Secure Messages", Engineering, Technology & Applied Science Research, Vol. 9, No. 1, 2019, 3681-3684