Data Security in Steganographic Applications using Encryption Algorithms

[1]Prof. Rahul Kadam, [2]Anushree Datta, [3]Poorvi Garg, [4]Taru Uppal, [5]Teril D’Costa

[1]Assistant Professor, [2345]Final Year Students
Department of Computer Science and Business Systems,
Bharati Vidyapeeth (Deemed to be University) College of Engineering, Pune, India

***Abstract*— Steganography is the historic art of hiding confidential information in an inconspicuous manner within other ordinary data. In the olden days, examples of steganography can be seen in murals and other artworks whereas nowadays, it is used to hide secret data inside images or audio files. Cryptography, on the other hand, is the art of sharing data in a reliable way such that only the sender and the receiver can access the original message. Our problem statement is simply: Having previously learned cryptography, how can we as a team improve the process of transmitting data from source to destination using secure data encryption algorithms? Think of steganography as a modern-day solution to secure data transmission using images. The aim of our study is to secure the secret data transmitted using steganography with encryption algorithms and examine the benefits of utilizing these methods in real-life applications. For the purpose of our study, we implemented commonly known encryption algorithms namely AES and RSA to encrypt the plaintext into cipher text and subsequently hide the ciphertext in a digital file through steganography.**

Index Terms: **Steganography, cipher text, AES (Advanced Encryption Standard) cryptography, encryption algorithm**

I. Introduction

With the rapid advancement in technology, it is safe to say that the number of users on the internet and the world wide web (WWW) every day is increasing. With so much data being generated, transmitted, transferred, studied, interpreted, and implemented, it has become a priority for organizations to find a secure way to do so. [1]
For the purpose of data utilization, it is imperative that we transfer data from source to destination on a frequent basis. So, even if most organizations have been able to keep their data secure as long as it is within their network, the security threats increase dramatically when it comes to data transmission. That’s when such confidential information is most at threat. In the modern age, hiding information is the most efficient way to secure data from third parties. Just like invisible ink was used in the olden days to ensure information didn’t leak to undesired sources, today we can use steganography.

Steganography is a method with which we can hide a large amount of information inside an inconspicuous image. Only the sender and receiver of the information have knowledge of existing information, and all other third parties cannot know about it at all.

Our focus with all steganographic techniques is to ensure that the pixels of the image do not get disturbed and don’t give away any signs of having been changed or tampered with in order to hide the secret data. Any distortions made are done in such a way that they remain virtually invisible to the human eye.

II. Literature Review

To improve communication security, many cryptosystems have been presented in the image encryption literature [2]. The proposed algorithm eliminates the step in which the secret key is shared during the encryption process. It is formulated based on symmetric encryption, asymmetric encryption, and steganography theories. The image is encrypted using a symmetric algorithm, then, the secret key is encrypted by means of an asymmetrical algorithm and it is hidden in the ciphered image using the least significant bits steganographic scheme. The analysis results show that while enjoying the faster computation, our method performs close to optimal in terms of accuracy.

Detection of steganography, estimation of message length, and its extraction belong to the field of steganalysis. Steganalysis has recently received a great deal of attention both from law enforcement and the media. In our paper, we classify and review current stego-detection algorithms that can be used to trace popular steganographic products.

We recognize several qualitatively different approaches to practical steganalysis - visual detection, detection based on first-order statistics (histogram analysis), dual statistics methods that use spatial correlations in images and higher-order statistics (RS steganalysis), universal blind detection schemes, and special cases, such as JPEG compatibility steganalysis. [3] [4].

Table 1: Comparative Analysis

Title	Authors	Method	Merits	Limitations	Solutions
Image Encryption Method using Steganographic LSB Method, AES and RSA Algorithm	Abdelkader Moumen and Hocine Sissaoui Year - March 2017	Image Encryption using LSB Method, AES and RSA algorithms	Eliminates sharing of the secret key using steganographic theories, asymmetric encryption, and symmetric encryption.	The computation time of asymmetric encryption is a lot more than that of symmetric encryption. Symmetric encryption is faster but less secure than asymmetric encryption methods.	An algorithm that takes advantage of the computation time of symmetric encryption and the security of asymmetric encryption methods, combining RSA, AES, and LSB method.
Security during Transmission of Data Using Web Steganography	Ahmed Bakhtiyar Uz Zaman Year - May 2018	BMP steganography with IDEA(International Data Encryption Algorithm) approach.	The IDEA algorithm has two layers of security and is very efficient at hiding and embedding data. No distortion is observed in the stego image by the naked eye.	Lossless images have low compression ratio while transmitting over the internet, therefore, are less secure	Use of lossy images (such as BMP/JPEG images) as the cover image in the compression algorithm achieves high compression while maintaining excellent quality, thereby ensuring more security.

III. Methodology

In this project, we study the AES (Advanced Encryption Standard), and LSB (Least Significant Bit) methods of cryptography to implement steganography. [5] Owning and transferring important information by hiding it inside innocent images can be utilized by all industries and individuals. We aim to improve upon existing methods to do so, increase accuracy scores for our model, and conclude the project with a working prototype of software capable of performing steganography.

We used an architectural flowchart to determine the actual working flow of our model and utilized the information, systems, and methodologies already tried and tested from the research papers we sourced that were published within the last few years. With the rapid technological advancement, being on top of the recent developments was a top priority for us.

The system architecture design that we propose is shown in Figure 1.

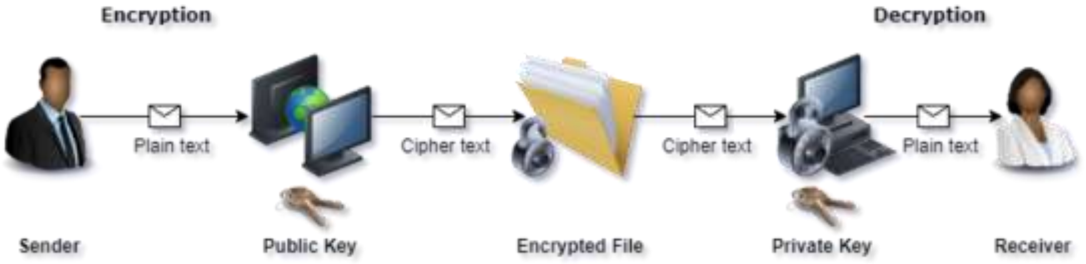

Fig 1. System Architecture Design

IV. Proposed Work

Our proposed work is a pipeline of different libraries and modules in python. We import modules such as PIL, getopt, and sys along with libraries such as crypto, Image, and argv. The script will hide files inside images and save the modified image to disk. It is based on a simple principle that if we change the LSB (Least Significant Bits) of every Pixel, then the change will not be significant and will not be noticed by eyes.

Based on the previous literature we consolidated the following information to do a comparative analysis of previously proposed methods and how we overcome them. For our code, we defined our own set of functions that would help us create a set of keys for both the encryption and decryption processes. Using our imported libraries, we take our RBG images and append (add) our text data in hexadecimal format to ensure that the image remains unaltered to the naked eye.

We would also be careful to include all default case scenarios within our code, so a wrong image input format or wrong key would display a message clearly communicating the mistake to the user and not lead to unprecedented breakages in the code during runtime. For example, if the image the user is trying to decrypt does not have any hidden data, the system should not confuse it with a case of the wrong key. The classification of possible output cases here will be very important to maintain the structural integrity of the steganographic process.

So based on the previous studies, we provide a few solutions to the limitations of their work. We won't use the following to overcome their limitations:

Table 2: Methods and Solutions

Method	Solutions
Image steganography using AES and LSB encryption algorithms	Image extensions .png and .jpeg utilized for steganography Use of Big Endian method along with LSB for improved efficiency of image steganography.

V. Future Scope

For the purpose of this study, we have implemented commonly known encryption algorithms such as RSA and AES to encrypt the plaintext into cipher text and subsequently hide the ciphertext in a digital file through steganography.

Through the combinations of these two techniques, we plan to improve the safety of the data to be transferred and prevent attempts at deciphering the message inside. The aim of our study was to secure the secret data transmitted using steganography with encryption algorithms and examine the benefits of utilizing these methods in real-life applications. Our motivation with this project poses massive future potential. With the recent rise of NFTs, digital artworks, advancements in health, etc. it is inevitable that visual data is the currency of the future. Even patients with copies of their X-rays can have their medical details and history securely hidden within them, without disturbing the quality of the X-ray film itself.

Its significance if implemented is massive: visual data is currency today, and photo identification through reliable authentication is the key to monetizing a secure future. Virtually every industry has an in-built requirement for this, from manufacturing to NFTs. Our project's aim was to create software that could encode sensitive encrypted data files inside images with accuracy and precision.

VI. Conclusion

Our final system is a real-world application of steganography. Our aim with the project was to create a simple way for any average user to be able to hide confidential text data in an unassuming picture and be able to transmit sensitive information without the risk of leakage, and we achieved that using the encryption algorithms we studied as part of our course.Through the course of this project, our team was also able to develop problem-solving skills as we identified, debugged, and improved the efficiency of the execution of the code.

Our objective is to conclude the project with a real-life implementation of our idea that can secure data transmission and guarantee data security in a world where hacking and data leaks are becoming easier as the amount of data keeps increasing while its security seems to become worse.

References

[1] "Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies", OECD Publishing, Paris, OECD (2019)

[2] Mondal, Bhaskar & Priyadarshi, Akash & Nair, Dhanya. (2013). "An Improved Cryptography Scheme for Secure Image Communication". International Journal of Computer Applications. 67. 23-27. 10.5120/11496-7206.

[3] Fridrich, Jessica & Goljan, Miroslav. (2002). "Practical Steganalysis of Digital Images - State of the Art". Proceedings of SPIE - The International Society for Optical Engineering. 4675. 10.1117/12.465263.

[4] Sahu, Aditya Kumar and Sahu, Monalisa. "Digital image steganography and steganalysis: A journey of the past three decades" *Open Computer Science*, vol. 10, no. 1, 2020, pp. 296-342.

[5] Abdullah, Ako. (2017). "Advanced Encryption Standard (AES) Algorithm to Encrypt and Decrypt Data."