International Journal of Engineering and Technical Research (IJETR)
ISSN: 2321-0869 (O) 2454-4698 (P) Volume-8, Issue-10, October 2018

Secret Messages in Social Media Using LSB And AES Algorithms

Malavika Prabhakar, Aiswarya Krishnan, Lavanya Nadanasabapathi, Mrinalini Majumdar, D. Saveetha

***Abstract*— With the increase in the popularity associated with the Internet, one of the most crucial factors of computer science and communication lies in ensuring the safeguarding of information. Cryptography is used in order to enhance the confidentiality of data during transmission, and various techniques have been established for the encryption and decryption of data to serve the purpose of hiding the message. However, it does not always suffice to simply hide the contents of a message; there may be times when keeping the very existence of the message hidden becomes necessary and this is where steganography comes in. Steganography refers to a technique in which one hides a secret message (such as a picture, sound, larger text, etc.) inside another larger and much more harmless-looking message in order to obscure the importance of what lies underneath. This paper describes a technique in which the AES encryption algorithm is used for performing cryptography and the LSB algorithm for steganography for the purpose of achieving a greater level of security when sending sensitive information, especially across social media platforms. Java, the programming language, is utilized both for its superior ease of use as well as its various comprehensive libraries.**

***Index Terms*— AES Encryption Algorithm, Cryptography, LSB Algorithm, Steganography**

I. INTRODUCTION

In today's world, social media is deeply entrenched into our lives. Since the increase in the popularity associated with the Internet, one of the most crucial factors of computer science and communication lies in ensuring the safeguarding of information. As the younger generations have made indisputably clear, social networks aren't just used to send out straightforward messages. In fact, they're quite often used as an outlet for sending sensitive information without getting much attention from people around. The problem lies in the fact that despite having an impressive knowledge on the workings of technology and use of social media, users don't understand or appreciate their vulnerability when it comes to safeguarding the data. For a large number of consumers, social media provides a platform to connect with friends and family, share photographs and even to reach out to the public to raise awareness for certain causes.

Users are not privy to the extent of their individual presence and as such, do not think of the consequences of someone unsavory gaining unauthorized access to their account or information. So, they tend to get careless. Any hacker that gains even a little access to your system inherits access to all your contacts. If you were to use a social media platform to comment on movies, books, institutions, restaurants or services, the hacker could utilize this to gain access to your browsing and shopping history.

In order to prevent this from happening, this project aims to provide a technique to hide necessary information inside another larger and harmless looking message, such that a third party cannot identify the presence of the secret message or be able to access it. The technique used is AES encryption to encrypt text files and LSB steganography technique to hide these encrypted text files in the images. This embedded file can then be sent across any social media platform as a harmless looking image. On the receiver side, the message file can be extracted and then decrypted from the cover file to get our original message. This kind of technique can be helpful for frequent users of social networking websites like WhatsApp, Instagram and Facebook, especially for those who need to send sensitive information through such websites.

Malavika Prabhakar, Department of IT, SRM IST, Kancheepuram, India
Aiswarya Krishnan, Department of IT, SRM IST, Kancheepuram, India
Lavanya Nadanasabapathi, Department of IT, SRM IST, Kancheepuram, India
Mrinalini Majumdar, Department of IT, SRM IST, Kancheepuram, India
D. Saveetha, Assistant Professor (O.G), Department of IT, SRM IST, Kancheepuram, India

II. LITERATURE REVIEW

Most social networking sites provide the facility for sharing and uploading media. While people do use social media to share their life moments, they may also choose to send sensitive information via this platform. [1] In March 2013, Ramadhan J. Mstafa and Christian Bach from University of Bridgeport wrote a paper about the different ways of hiding information using different steganography techniques. [2] A Text Steganographic System Based on Word Length Entropy Rate was studied in 2017 to embed data into text documents. [3] The highlight and the difference between their technique and ours, is that we use a simple software which is portable and hence can be used on any platform, and with any type of media instead of just text. Another advantage is that our application can be used by anyone since it isn't very complex. Prior knowledge of java is not a pre-requisite for using this application.

The drawback of using the DES (Data Encryption Standard) algorithm for the cryptography is that its key size of 56 bits is too short for adequate security in this day and age as it can be brute forced quite easily with the right resources. [4] Similarly, the 3DES algorithm is one where DES is basically applied 3 times to the information that is being encrypted. [5] While the encryption key as such is still restricted to 56 bits, the fact that it is applied not just once but 3 times, means that the implementer is given the choice of 3 discrete 56-bit keys, or, even 3 identical keys. While this is a more effective method, certain susceptibilities when applying the same encryption algorithm thrice in succession results in a 168-bit key having a reduction in its security, making it equivalent to that of a

112-bit key and similarly, a 112-bit key having a reduced security equivalent to that of an 80-bit key. In contrast, the AES (Advanced Encryption Standard) algorithm which we use in this project is capable of using different block lengths and key lengths, for instance 128, 192, and 256 bits. This adaptability can result in quicker and additional security of the symmetric block ciphers. As such, AES outperforms 3DES both in software and in hardware.

Factors	AES	3DES	DES
Key Length	128, 192, or 256 bits	(k1,k2 and k3) 168 bits (k1 and k2 is same) 112bits	56 bits
Cipher Type	Symmetric block cipher	Symmetric block cipher	Symmetric block cipher
Block Size	128, 192, or 256 bits	64bits	64 bits
Developed	2000	1978	1977
Cryptanalysis resistance	Strong against differential, truncated differential, linear, interpolation and square attacks	Vulnerable to differential, Brute Force attacker could be analyze plaint text using differential cryptanalysis.	Vulnerable to differential and linear cryptanalysis; weak substitution tables
Security	Considered secure	one only weak which is Exit in DES.	Proven inadequate
Possible Keys	2^{128}, 2^{192}, or 2^{256}	2^{112} or 2^{168}	2^{56}
Possible ASCII printable character keys	95^{16}, 95^{24}, or 95^{32}	95^{14} or 95^{21}	95^{7}
Time required to check all possible keys at 50 billion keys per second**	For a 128-bit key: 5 x 10^{21} years	For a 112-bit key: 800 Days	For a 56-bit key: 400 Days

Fig. 1 Comparison between AES, 3DES and DES [6]

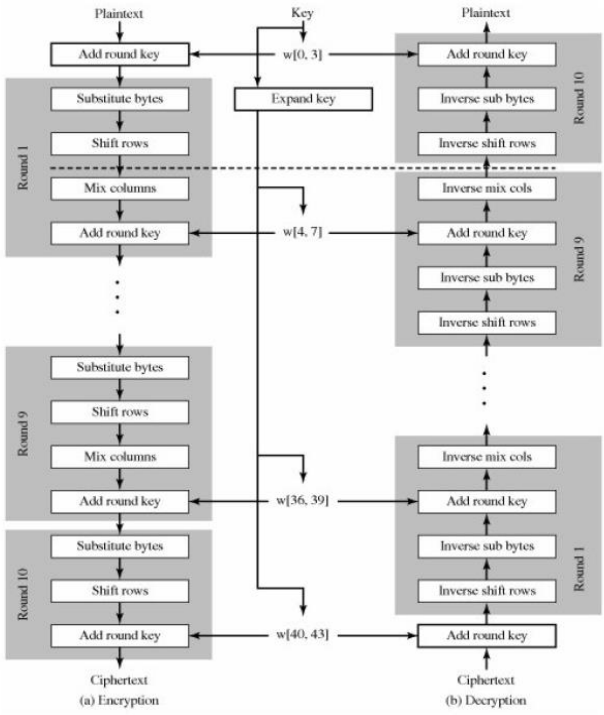

Fig. 2 Working of AES algorithm

As for the steganography side of the project, the Least significant bit (LSB)-based technique is used because, even though it is one of the simplest methods available, it is highly effective. It involves hiding a message within the LSBs of pixel values while avoiding the introduction of distortions which can be detected. [7] Any changes to the LSB value are not detectable to the human eye and hence makes it both easy to implement and serves its purpose well.

III. PROPOSED METHODOLOGY

In order to ensure a higher level of security when sending sensitive information, especially across social media platforms, we propose a model wherein two different techniques are applied. Firstly, cryptography is applied using the AES algorithm in order to convert plaintext into ciphertext that cannot be easily brute-forced. Once this is done, the ciphertext is embedded into a cover image file by applying the technique of steganography and utilizing the LSB algorithm to do so. Finally, the image file embedded with the secret message can be safely transmitted to the intended recipient. Similarly, a reverse of the above steps can be performed in order to extract, decrypt and view the hidden message.

A. AES Algorithm

AES is a popular and widely adopted symmetric encryption algorithm. In using this algorithm, there is a choice regarding the use of a 128-bit key, a 192-bit key or a 256-bit key, resulting in it being stronger and more powerful than the simple 56-bit key used in DES. The AES algorithm uses a substitution-permutation method for creating the encrypted block.

To get a better understanding of how the AES algorithm works, observe the following diagram.

B. LSB Algorithm

LSB refers to the Lowest Significant Bit in the byte value of the pixel of an image. Steganography based on the LSB of an image embeds the secret message in the least significant bits of the cover image's pixel values. This concept of LSB Embedding is very straightforward. It makes use of the fact that the precision level in various image formats is significantly higher than is perceivable by the average human's vision. Hence, a changed image with slight differences in its colors will not be distinguishable from the original image by a person, simply by looking at it. Eight bytes of pixels are required to store one byte of secret data, in the typical LSB technique. However, in the proposed LSB technique, just four bytes of pixels are ample for holding one message byte and the remaining bits in the pixels are not changed.

IV. TESTING

A. Hiding the Secret Message

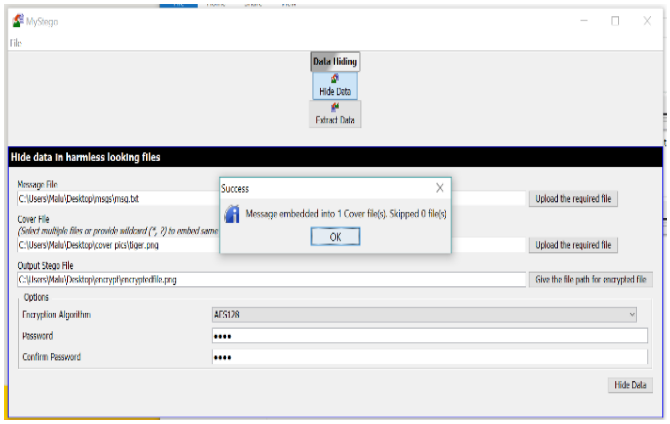

Fig. 3 Enter the data to be hidden and submit details

Fig. 4 The picture has been encrypted, on comparing there is no distortion

B. Extracting the Secret Message:

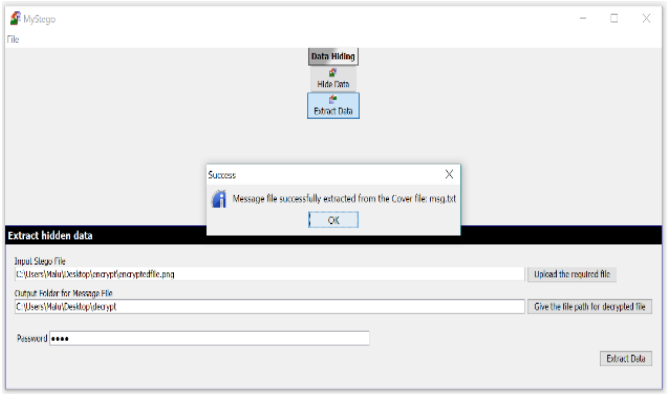

Fig. 5 Enter the output file and extract data

V. FEASIBILITY

The main objective of feasibility is to assess the practicality of the proposed technique. This study includes the operational and economic feasibility of combining steganography and cryptography.

A. Operational Feasibility

i. Reliability:

The package involves one to one connection between the sender and the receiver, thus ensuring confidentiality of the embedded data.

ii. Security:

The application has a dedicated file name and a password, thereby ensuring that unauthorized personnel does not gain access to it.

iii. Portability:

The application is developed in java. This will work on both Linux and Windows operating system. Hence, portability problem will not arise.

iv. Availability:

This software will always be available, meaning that it is not dependent on an internet connection and can be used offline.

B. Economic Feasibility

The application must be built as a stand-alone application. This is required as the encryption and decryption can be done anywhere possible.

VI. FUTURE SCOPE

Since this technique uses steganography as its major part, where you never know if a message is hidden -there is a wide chance for its development in the future on the following basis:

A. Detecting Steganography in Image Files

It can be made possible to identify a simple Steganographic technique by examining the low order bits in the image bytes. However, if the algorithm for steganography is more complex and extends the embedded data across the image in a random way or encrypts the data before embedding, it may not be possible to detect currently, to which solutions can be identified in the future**.**

B. Higher Encoding Density

A logical area of improvement is the ability to hide huge amounts of data with steganography. As steganography is used in crimes like corporate spying, hacking, fraud etc. there will be more demand to hide larger amounts of information. One possible future would be working on large-scale steganography, where large information or data are compressed and stored into smaller files.

C. Printed Media

When the data is embedded in an image and is printed, and then scanned and stored in a file -is it possible to recover the information stored? This might require a special device, and also while in the stages of printing and scanning, devices for allowing inaccuracies which could be considered as a special form of steganography.

D. Resistance to Analysis

As media gets more improved and sophisticated, its resistance to being analysed, or even recognized, will improve. Currently, if steganography media being used is suspected, it is relatively easy to detect it. Once it is detected, the contents could be retrieved which would then be protected only by the strength of the encryption applied to it, if any. In future, further improvement can make steganography undetectable and irretrievable except by those for whom it is intended.

VII. CONCLUSION

In this paper, we proposed a technique involving the combination of the AES algorithm for cryptography and the LSB algorithm for steganography for the purpose of achieving a greater level of security when sending sensitive information across social media platforms. We demonstrated that our system has been designed for simplicity and could be revised with very little effort if such a necessity should arise in the future. It has been observed that the system works with efficiency and also effectively. Its higher user friendliness

may result in others using these documents as a model for developing analogous applications.

REFERENCES

[1] IVAN NECHTA, "STEGANOGRAPHY IN SOCIAL NETWORKS", SIBERIAN SYMPOSIUM ON DATA SCIENCE AND ENGINEERING (SSDSE), JANUARY 2017

[2] Ramadhan J. Mstafa, Christian Bach, "Information Hiding in Images Using Steganography Techniques", Northeast Conference of the American Society for Engineering Education (ASEE), March 2013

[3] Francis Xavier Kofi Akotoye, "A Text Steganographic System Based on Word Length Entropy Rate", **International Journal of Recent Contributions from Engineering, Science & IT (iJES), 2017**

[4] Manoj Kumar Ramaiya, Naveen Hemrajani, Anil Kishore Saxena, "Security Improvisation in Image Steganography Using DES", 3rd IEEE International Advance Computing Conference (IACC), 2013

[5] Praveen Kumar B, Rajaanadan N.S, "Data Encryption and Decryption Using by Triple DES Performance Efficiency Analysis of Cryptosystem", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 4, Issue 3, March 2016

[6] Hamdan. O. Alanazi, B. B. Zaidan, A. A. Zaidan, Hamid A. Jalab, M. Shabbir, Y. Al-Nabhani, "New Comparative Study Between DES, 3DES and AES within Nine Factors", Journal of Computing, Volume 2, Issue 3, March 2010

[7] Champakamala .B.S, Padmini .K, Radhika .D. K, "Least Significant Bit Algorithm for Image Steganography", International Journal of Advanced Computer Technology (IJACT), 2014

AUTHORS

Malavika Prabhakar, 4th Year, B.Tech., Information Technology, SRM Institute of Science and Technology, Kancheepuram, India

Aiswarya Krishnan, 4th Year, B.Tech., Information Technology, SRM Institute of Science and Technology, Kancheepuram, India

Lavanya Nadanasabapathi, 4th Year, B.Tech., Information Technology, SRM Institute of Science and Technology, Kancheepuram, India

Mrinalini Majumdar, 4th Year, B.Tech., Information Technology, SRM Institute of Science and Technology, Kancheepuram, India

Corresponding Author: D. Saveetha, Assistant Professor (O.G), Department of Information Technology, SRM Institute of Science and Technology, Kancheepuram, India Phone: 044-274173000