Turkish Journal of Computer and Mathematics Education Vol.12 No. 11 (2021), 2839- 2846
Research Article

Encryption and Decryption of Images based on Steganography and Cryptography Algorithms: A New model

Akhil Verma[a], Amol Gupta[b], Sumit Kumar Suman[c], Md Mustafa Khan[d], Prakash Kumar Sarangi[e]

[a,b,c,d] B.Tech. Student, [e] Assistant Professor
[a,b,c,d,e] School of Computer Science and Engineering, Lovely Professional University, Punjab, India
[a] akhil8685@gmail.com, [b] amolgupta135@gmail.com, [c] sks110498@gmail.com, [d] mustafakntw7@gmail.com, [e] prakash.26183@lpu.co.in

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 10 May 2021

Abstract: Steganography is the art of "hidden writing," and it refers to techniques for concealing knowledge within seemingly innocuous items called "Cover Objects." There are various types of covers for encrypting sensitive information, but photographs are ubiquitous in everyday applications and have a high level of redundancy of representation. As a result, they are appealing candidates for use as cover items. This paper evaluates the LSB algorithm. One of the most well-known steganographic techniques is Least Significant Bit. Embedding with another type of encryption can make it more secure. Many of the scholars suggest the combination of encryption with Steganography adds more obstacles to get cracked. The paper is meant to introduce the concept of LSB with affine cipher encryption technique with the limitations of steganography.

Keywords: Least Significant Bit, Steganography, Affine cipher, Piggybacking

1. Introduction

The last decade has witnessed the expansion in the field of internet; computers and even they have become the major channel of communication that connects the people of the whole world as a single virtual society. As a consequence communities can share their valuable and personal information with each other in which span is no longer a hurdle. Additionally, hidden as well as secure communication is considered as the primary requirement of the people. Through which the field of cyber security is gaining higher success because of the new technologies like steganography,audio-steganography, cryptography, etc. Among all these areas steganography is attaining a great attraction by individuals spawn by the security concern over the internet. Thus, in the idea called as cryptography the message is reshaped in the form of encryption with the help of keys which are known as encryption keys, only the sender and recipient are aware of these public and private keys as the message is not accessed by anyone else without using the key. As there are some flaws for this execution steganography techniques came under process to tame this problem. In such a way the techniques are applied by combining art and science in such a manner that it is able to hide the presence of transmission. In the steganography approach we can hide information content inside any medium of media like images, audio-visuals. On the other side, we may use multiple tracts to assess the success of a steganography scheme. The most important property is statistical undetectability, which indicates how it is to detect the presence of a hidden message. Others are concerned about its range, which refers to the maximum amount of data that can be safely embedded in a job without producing demographically discernible artefacts, and robustness, which refers to the device's ability to resist data extraction.The remaining paper consist of following section Steganography, Literature survey, Our Methodology and Limitations of Steganography.

1.1 Steganography

Steganography is data hidden within data. It means the techniques of camouflaging confidential information within an ordinary file in order to avoid detection. It is an encryption technique which can be used along with cryptography and as an extra-secured practice in which to secure data. Steganography technique can be enforced on images, audio files, and a video file and secure from pirating copyrights materials as well as aiding in unauthorized viewing. The main objectives of this mechanism are to conceal and deceive information. It is a form of clandestine communication in which messages or data are hidden using any medium. It isn't a type of cryptography because it doesn't encrypt data or require the use of a key.

Steganography can be used in a variety of ways to conceal details. One of the most popular methods is to insert data into digital images. We've all become friends with JPEG images, which contain several megabytes of data in the form of pixels.This offers some space for stenographic content to be embedded in digital files. An attacker modifies the least significant bits (LSB) of the data file using stenographic applications and embeds malicious code in the image. The malware will automatically trigger after the target downloads and opens the image file on their device. the malware has now provided the attacker with access to the user's computers and networks. The danger of steganography is that the difference between the original and stenographic images is so

slight that it is impossible to tell the difference with the naked eye. Nowadays, Cyber criminals want to use steganography.

Security researchers discovered a new malware campaign that used Modified Attack Vector (WAV) audio files to mask their malware in recent attacks. The malicious code is thought to have been embedded in the Modified Attack Vector (WAV) audio file using Steganography. Least Significant Bit (LSB), Palette Based Technique, and Safe Cover Selection Technique are some of the techniques used in steganography. In this paper we are focusing on LSB.

2. Literature Survey

Kurak and McHugh , They suggested a process that resembles embedding into the 4 LSBs, are credited with one of the earliest methods to discuss digital steganography(least significant bits) [1]. Image downgrading and contamination, also known as image-based steganography, were investigated.

The method of embedding information into digital content without causing perceptual degradation is known as data hiding [2]. Three well-known strategies for data concealment exist. Watermarking, steganography, and cryptography are the three methods. Covering writing in Greek is known as steganography. It encompasses any procedure that deals with data or data contained inside data.

El-Emam proposed a similar definition, which is used in their study. To hide the data, a bitmap (bmp) image will be used. The pixels will be used to insert data within the image [3]. After that, the pixels of the stego image can be accessed in order to recover the image's secret data. The primary benefit of a steganography algorithm is its straightforward security mechanism. Since the steganographic message is encrypted and hidden inside other harmless sources; it is extremely difficult to detect the message without first understanding its nature and encoding scheme [4].

Contemporary digital technology has shattered confidence in the credibility of visual imagery. They had suggested a security scheme for scanned documents that uses self-embedding techniques to prevent forgery [5]. Not only does the method detect forgery, but it also allows legal or forensics experts to see the original document, even though it has been tampered with. No other security tool can equal the level of assurance that steganography can provide. For electronic patient records, we present a bi-polar multiple-base data hiding LSB embedding technique [7]. The difference in pixel values between an original image and its JPEG counterpart is referred to as a number conversion base.

Nirinjan and Anand also explore patient data concealment in digital images [8] and Li et al. [9]. Images generated using digital technology. As exemplified by the idea of steganography being embedded as part of the normal printing process, Fujitsu3 is developing technology to encrypt data into a printed image that is invisible to the human eye (data) but can be decoded by a mobile phone with a camera.

In this paper, we have divided the entire paper into six sections. Section one describes Introduction to Steganography. Related works we have defined in section two. Our proposed work have described in section three. Some limitations, results, conclusions, and future works have defined in the section four, five and six respectively.

3. Our Methodology

“Data camouflaging sures that the secrecy of data is alive” Hiding data into the binary value without changing the original message and without corrupting the image, this technique is referred to as Steganography. There are various methods of concealing data into other types of data such as hiding of text into voice clip or in video clip or vice versa.

This paper focuses on the method that is least significant bit with the affine cipher encryption technique to make it more secure and to make it less noticeable. In this section, our model divided in to three important sub-sections. In sub-section (i), we have described LSB algorithm with an example how is working. In next sub-section (ii), we have explained the equation of a Affine cipher algorithm. In last sub- section (i.e. Sub-section (iii)), we have presented the details about our model i.e. Stegasis and its design principles. In this sub-section, all input data are process through a pipeline.

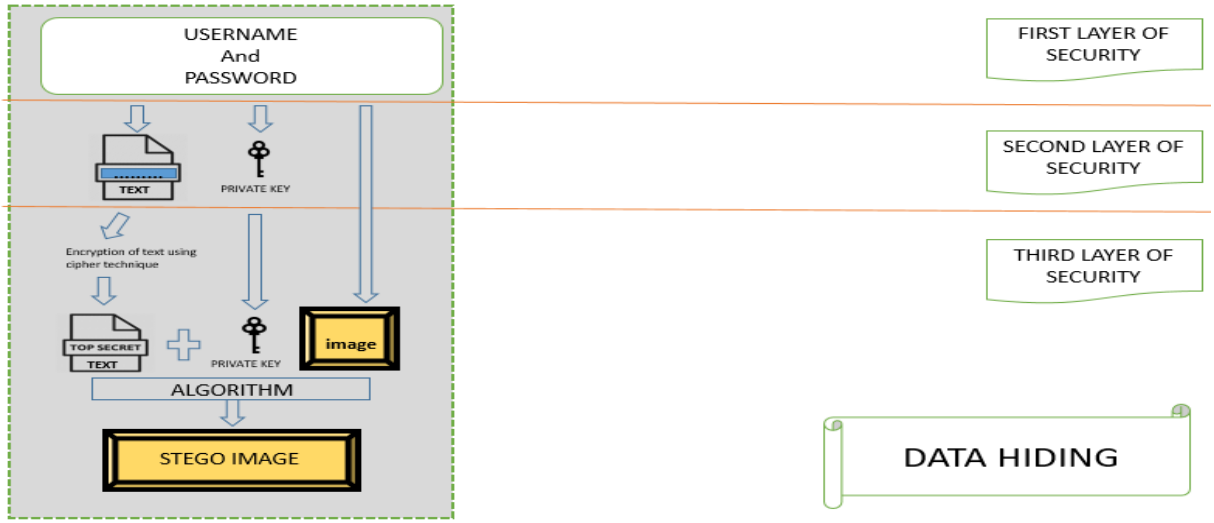

Figure 3.1: Frame work of our model Data Hiding

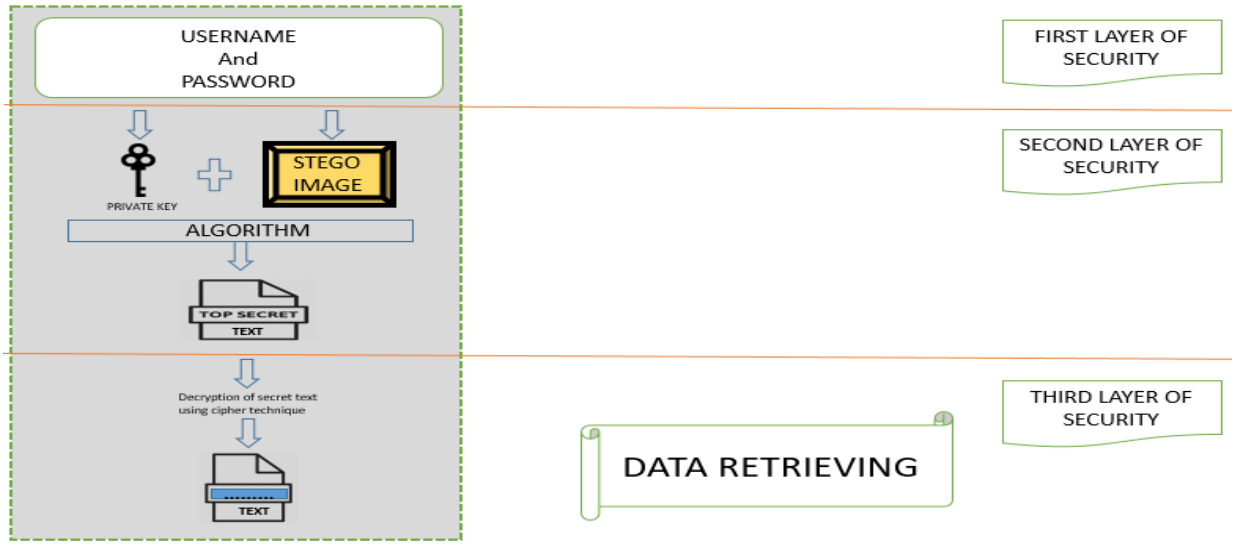

Figure 3.2: Frame work of our model Data Retrieving

3.1: Least Significant Bit (LSB)

In steganography, it is a widely used algorithm. It's a technique for hiding data within the data here we are using image, by replacing the least significant bit of the cover image with the message bits to be protected. It is the lowest number of bits in a binary number series, and it is found on the far right side of the string.

For example, in the binary number (11001101), the least significant bit is 1. Least significant bit first means the least significant bit will arrive first. Example:- the same hexadecimal number 0x12, gain 00010010 in binary representation will arrive as (reversed) sequence 01001000. The 7^{th} bit and $7^{th}+1$ bit of selected pixel are used for hiding data and extraction on the basis of these 2 values. Two bits of message are hidden on each pixel. Reason for using LSB is the visibility of changes after hiding data is very less.

Example:-

Cover data data to be hidden

10011110 10100110

Step1. Select how many bits we are going to use for this encryption.

Note: we can use up to 3 bits. Because an increase in the number of changing bits are leading to an increase in change of image.

Cover data data to be hidden

10011**<u>110</u>** **<u>101</u>**00110

Step2. Take LSB of cover data and MSB of data need to hide and

replace them with each other.

The resultant data is called stego data.

Stego data

10011101

To retrieve the hidden data from stego data all we need to do is reverse the process.

3.2: Affine Cipher

It's a monoalphabetic substitution cipher, which means that each letter of the alphabet has its own numeric value and key (a, b), later encrypted with a mathematical formula that is

N * Key (a) + Key (b) mod 26

Where, N is numerical value of alphabet

3.3: Our Proposed Model Stegasis

Stegasis is an android application which is developed on the basis of the below algorithm (3.3.1). Based on the framework for the app as, we have discussed in fig 3.1 and in fig 3.2. Three levels of protection are used in stegasis.

The first layer includes the user's login information, the second layer requests text using a private key, and then at last the third layer is for hiding that is camouflaging text into the data and retrieving information from the image.

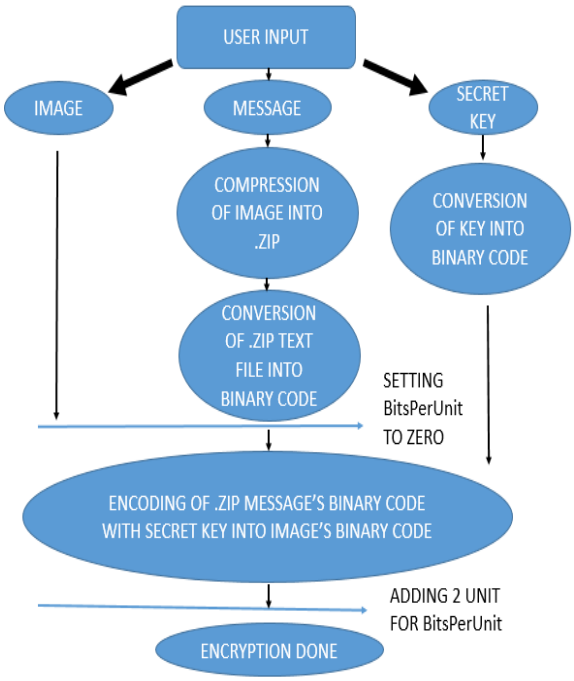

Figure 3.3: Flow diagram of Encryption Interface

In above Fig 3.3, in this section stegasis hides the text into image but before it camouflages, encryption of text into cipher text is done via affine cipher technique to make it more secure. A secret key must be entered here, as it will be required when decoding the picture as shown in the fig 3.4.

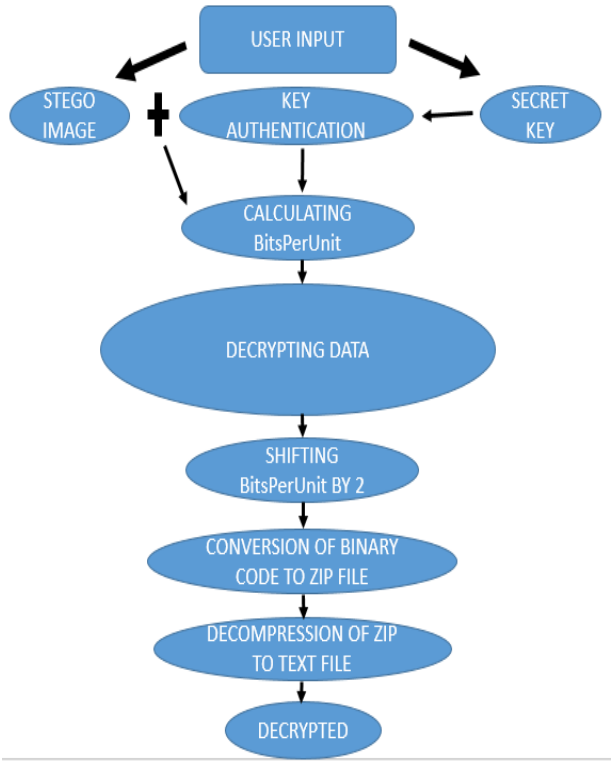

figure 3.4 : Flow diagram of Decryption Interface

The data and the secret key are both embedded in the picture. Users can send created stego images to other users via email without revealing the message hidden within the image. If authorised person wants to read the hidden text then the image must be uploaded on stegasis to reveal the text.

3.3.1: Algorithm to encode data inside image

Input: An image message and a privatekey

Output: Cipher text of image message

Step 1. Input the Image, Message, PrivateKey;

Step 2. Create text file of Message entered;

Step 3. compress text file;

Step 4. conversion of PrivateKey into binary code;

Step 5. conversion of text file into binary code;

Step 6. set of BitsPerUnit to zero;

Step 7. Encoding of Message into binary code;

Step 8. Addition of 2 unit for BitsPerUnit;

Step 9. Encryption is done.

3.3.2: Algorithm to decode data

Input: Cipher text of image message

Output: Decrypted message of image

Step 1. Input of Encrypted Image, PrivateKey;

Step 2. Comparison of PrivateKey;

Step 3. Calculation of BitsPerUnit;

Step 4. Decoding complete binary codes;

Step 5. Shifting of Bits Per unit by 2;

Step 6. Conversion of binary codes to text file;

Step 7. Decompression of text file;

Step 8. Decryption is done.

4. Limitations of Steganography

Message recovery becomes little challenging if the image is compressed or distortion takes place. Let us consider a scenario where Alice decided to share an encrypted image to Bob via any social media where image is first compressed then it is received, throughout this process encrypted data gets distorted, that is Bob won't receive any message.

Figure4.1: Distortion due to compression

Another challenge related to it is that if unauthorised person gathers password by piggybacking or tailgating then it may give access to it. For example suppose if Bob is travelling using public transport with his friend Eve, at that time Alice sent an encrypted photo to Bob in which confidential data is hidden and the key to access it but Eve standing next has seen the password which made data unsecure.

Huge data files which are bigger in size may create suspicion also it is little onerous to write computer programs which can perfectly read hidden data, sometimes it may be impenetrable.

5. Results and working Principle of our model

This paper results in providing the future scope of using steganographic texting which is much more reliable than day to day texting. For example if someone has access to our personal device then the intruder may be able to get all information easily. On the other hand, by using a steganographic approach we can prevent this type of attack, whenever we need to send any important message we can take use of modern technique that is stegasis an application which helps to hide text into image with a key, without the same key decrypting the message is challenging.

5.1 Encryption Interface in Stegasis

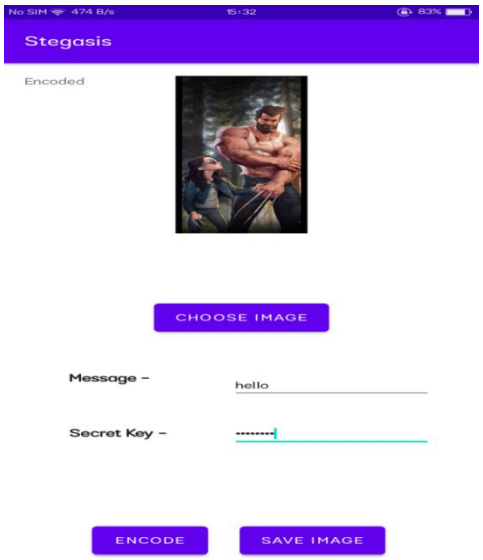

Figure5.1: Input and Encryption Interface in Stegasis

In the above figure 5.1 tells us about the encryption part in which we are supposed to choose an image and enter the secret key as well as we have to enter the message which has to be encoded and after pressing the encoded button a pop-up will appear which tells us that your message is encoded and after that we are supposed to save the image

5.2 Decryption Interface in Stegasis

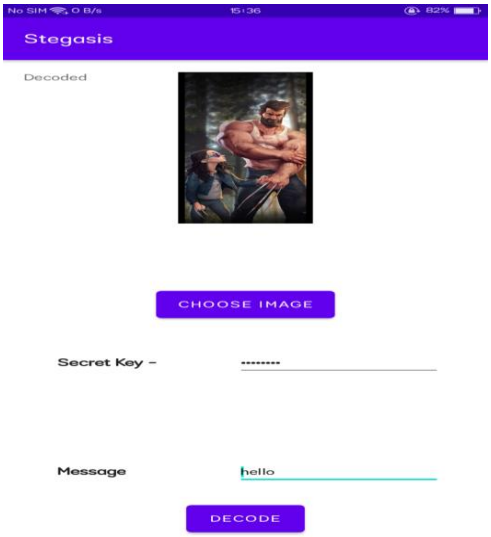

Figure 5.2 : Decryption Interface in Stegasis

In the figure 5.2 displays us that our message is successfully decoded, for that first we have to choose the encoded image from the gallery and then we have to enter the secret key and once we enter the key we have to click on decode and our encoded message will be displayed. Our approach to achieve integrity and confidentiality in texting is by using LSB(least significant bit) algorithm as it results in very few changes in appearance of image which is very difficult to catch with naked eyes.

6. Conclusion and future work

In image-based steganography, we present a novel concept in which variable no bits can be stored in each channel. Our algorithm is based on real-world data. The change in least significant bits of pixel, this method yields a high potential with minimal optical distortions. Experiments show that our algorithm outperforms than other algorithms of a similar kind. Rather than using the same static (fixed) partition scheme for all cover files, select the partition based on the cover media at run time. To evaluate the change, we need to look for irregularities in pixels of image, and try to extract the changed bits which provide us the hidden data.

The change is very difficult to catch with naked eyes. By using this steganographic approach one is able to hide the message even if someone has access to their devices, because no one knows which images are used for which message as the change is invisible through naked eyes. Digital watermarking is where steganographic techniques would most likely be used. Digital watermarks offer a way to monitor who owns what, which is essential for content creators who want to protect their copyrighted works from unauthorized distribution. Steganography could be prohibited by legislation because governments have already claimed that criminals use these techniques to communicate. The following are some examples of how steganography might be used:

i. In the event of a security breach, data is hidden on the network

ii. Peer-to-peer private communications.

iii. To prevent transmission, confidential messages are posted on the internet..

Corrective audio or image data is embedded in case corrosion occurs as a result of a bad link or transmission..

References

1. C. Kurak, J. McHugh, A cautionary note on image downgrading, in: Proceedings of the IEEE 8th Annual Computer Security Applications Conference, 30 November–4 December, 1992, pp. 153–159.
2. M. Chen, N. Memon, E.K. Wong, Data hiding in document images, in: H. Nemati (Ed.). Premier Reference Source–Information Security and Ethics: Concepts, Methodologies, Tools and Applications, New York: Information Science Reference, 2008, pp. 438-450.
3. N.N. El-Emam, Hiding a large amount of data with high security using a steganography algorithm, Journal of Computer Science 3 (2007) 223-232.
4. T. Jahnke, J. Seitz, (2008). An introduction in digital watermarking applications, principles and problems, in: H. Nemati (Ed), Premier Reference Source–Information Security and Ethics: Concepts, Methodologies, Tools and Applications, New York: Information Science Reference, 2008, pp. 554-569.
5. H. Farid, A survey of image forgery detection, IEEE Signal Processing Magazine 26 (2) (2009) 16–25.
6. A. Cheddad, J. Condell, K. Curran, P. Mc Kevitt, A secure and improved self-embedding algorithm to combat digital document forgery, Signal Processing 89 (12) (2009) 2324–2332.
7. S. Miaou, C. Hsu, Y. Tsai, H. Chao, A secure data hiding technique with heterogeneous data-combining capability for electronic patient records, in: Proceedings of the IEEE 22nd Annual EMBS International Conference, Chicago, USA, July 23–28, 2000, pp. 280–283.
8. U.C. Nirinjan, D. Anand, Watermarking medical images with patient information, in: Proceedings of the 20th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, Hong Kong, China, 29 October–1 November 1998, pp. 703–706.
9. Y. Li, C. Li, C. Wei, Protection of mammograms using blind steganography and watermarking, in: Proceedings of the IEEE International Symposium on Information Assurance and Security, 2007, pp. 496–499.