Data Hiding In Digital Image Using MD5 and DES

Harsimranjeet Kaur

1Research Fellow, Department of Computer Science and Engineering, Desh Bhagat University, Mandi Gobindgarh, Punjab
2Assistant Professor, Department of Computer Science and Engineering, Desh Bhagat University, Mandi Gobindgarh, Punjab

Abstract: Steganography is the process of invisible communication this is accomplished through hiding information behind the image thus hiding the existence of the communicated information. The problems occur is to study the Pixel Group Trace Model-Based Quantitative Steganalysis for Multiple Least-Significant Bits Steganography and need to compare the results in terms of PSNR, MSE with the implementation of Cryptography Technique. The hiding data is encrypted using MD5 and DES then combining of data into the cover image is done using MLSB. We are implementing this by using MATLAB.

Keywords: MD5, DES, PSNR, MSE

1. Introduction

Encryption is a way to increase the security of a message or file by scrambling the contents so that it can be read only by someone who has the right encryption key to unscramble it.

Encryption, by itself, can protect the confidentiality of messages, but other techniques are still needed to protect the integrity and authenticity of a message; for example, verification of a message authentication codes (MAC) or a digital signature. Standards for cryptographic software and hardware to perform encryption are widely available, but successfully using encryption to ensure security may be a challenging problem. A single slip-up in system design or execution can allow successful attacks. Sometimes an adversary can obtain unencrypted information without directly undoing the encryption. Digital signature and encryption must be applied to the cipher text when it is created to avoid tampering; otherwise any node between the sender and the encryption agent could potentially tamper with it. Encrypting at the time of creation is only secure if the encryption device itself has not been tampered with this.

1.2 Message verification

Encryption, by itself, can protect the confidentiality of messages, but other techniques are still needed to protect the integrity and authenticity of a message; for example, verification of a message authentication codes (MAC) or a digital signature. Standards for cryptographic software and hardware to perform encryption are widely available, but successfully using encryption to ensure security may be a challenging problem. A single slip-up in system design or execution can allow successful attacks. Sometimes an adversary can obtain unencrypted information without directly undoing the encryption. Digital signature and encryption must be applied to the cipher text when it is created to avoid tampering; otherwise any node between the sender and the encryption agent could potentially tamper with it. Encrypting at the time of creation is only secure if the encryption device itself has not been tampered with this.
1.3.2 Asymmetric methods

Asymmetric encryption, or public-key cryptography, is different than the previous method because it uses two keys for encryption or decryption. With this method, a public key is freely available to everyone and is used to encrypt messages, and a different, private key is used by the recipient to decrypt messages.

![Encryption Public-Key (Asymmetric)](image)

Two keys are used in asymmetric cipher a public and a private one. The public one is available for everyone, but the private one is known only by the owner. When the message is encrypted with the public key, only the corresponding private key can decrypt it. The private key can’t be learned from the public one.

1.3.3 Steganography

Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. The word steganography is derived from the Greek words “stegos” meaning “cover” and “grafia” meaning “writing defining it as “covered writing”. In image steganography the information is hidden exclusively in images. The idea and practice of hiding information has a long history. In *Histories* the Greek historian Herodotus writes of a nobleman, Histaeus, who needed to communicate with his son-in-law in Greece. He shaved the head of one of his most trusted slaves and tattooed the message onto the slave’s scalp. When the slave’s hair grew back the slave was dispatched with the hidden message [2]. In the Second World War the Microdot technique was developed by the Germans. Information, especially photographs, was reduced in size until it was the size of a typed period. Extremely difficult to detect, a normal cover message was sent over an insecure channel with one of the periods on the paper containing hidden information.

1.3.4 MD5 (Algorithm Used)

The MD5 message-digest algorithm is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32 digit hexadecimal number. MD5 has been utilized in a wide variety of cryptographic applications, and is also commonly used to verify data integrity. MD5 was designed by Ron Rivets in 1991 to replace an earlier hash function, MD4. The source code in RFC 1321 contains a “by attribution” RSA license. MD5 processes a variable-length message into a fixed-length output of 128 bits. The input message is broken up into chunks of 512-bit blocks (sixteen 32-bit words); the message is padded so that its length is divisible by 512. The padding works as follows: first a single bit, 1, is appended to the end of the message. This is followed by as many zeros as are required to bring the length of the message up to 64 bits less than a multiple of 512. The remaining bits are filled up with 64 bits representing the length of the original message, modulo 2^64. The main MD5 algorithm operates on a 128-bit state, divided into four 32-bit words, denoted A, B, C and D. These are initialized to certain fixed constants. The main algorithm then uses each 512-bit message block in turn to modify the state. The processing of a message block consists of four similar stages, termed *rounds*; each round is composed of 16 similar operations based on a non-linear function F, modular addition, and left rotation. Figure 1 illustrates one operation within a round. There are four possible functions F; a different one is used in each round:

\[
F(B, C, D) = (B \land C) \lor (\neg B \land D)
\]

\[
G(B, C, D) = (B \land D) \lor (C \land \neg D)
\]

\[
H(B, C, D) = B \oplus C \oplus D
\]

\[
I(B, C, D) = C \oplus (B \lor \neg D)
\]

Denote the XOR, AND, OR and NOT operations respectively.

MD5 which stands for *Message Digest* algorithm 5 is a widely used cryptographic hash function that was invented by Ronald Rivets in 1991. The idea behind this algorithm is to take up a random data (text or binary) as an input and generate a fixed size “hash value” as the output. The input data can be of any size or length, but the output “hash value” size is always fixed. Here is an example of MD5 Hash function at work:

2. Related Work

Yang et al. [1] presented a pixel group trace model for analyzing the multiple least-significant bits (MLSB) steganography. Based on this model and some statistical characteristics of images, two quantitative steganalysis methods are proposed for two typical MLSB steganography paradigms. The pixel group trace model simulates the MLSB embedding by exclusive or operation, and traces the transition relationship among the possible structures of the pixel group’s value by some trace pixel group subsets. Then, the estimation equations of embedding ratio are derived from the transition probability matrix among trace subsets.
and the symmetry of regular and singular pixel group sets. Finally, a series of experimental results for the case of triple pixel group show that the proposed steganalysis methods can estimate the low embedding ratio with smaller error, especially, for some cases, the interquartile range of the estimation errors is smaller than the best one of the others by more than 45%.

Amirtharajan et al. [2] using one component case: here we have 3 ways to determine the bits * 3 ways to decide the component R, G or B: this results in 9 cases. Using two component case: here we have 3 ways to determine the bits * 3 ways to decide the component RG, RG or GB. This results in 9 cases. Using three component case: here we have 3 ways to determine the bits * one way to decide the component which is RGB. This results in 3 cases. The average capacity ratio is around 1/7 or 14% of the original cover media size. The secret data is scattered throughout the whole image. Also, extracting the secret data without the knowledge of seeds is almost impossible. The capacity of the triple technique is higher than the previous techniques.

Tiwari et al. [3] that most of the data hiding methods in image steganography used a technique utilizing the Least Significant Bits (LSB) of the pixels, i.e. the LSB of each pixel is replaced to hide bits of the secret message. This, normally, produce changes in the cover media but with no significant effect. All the LSBs of pixels of cover image can be used for hiding the secret bits. The hidden information can easily be uncovered using many known statistical steganalysis techniques, such as the X2 that can detect the concealed data inside the image with its original size.

Lili Yu et al [4] “The Application of Hybrid Encryption Algorithm in Software Security” Because of the defect of only the single data encryption and the use of famous encryption algorithm, which was not improved in traditional methods of the registration process, a combined encryption algorithm is proposed in this thesis. That is, the algorithm security is greatly improved, through researching several famous data encryption algorithms, and improving some data encryption algorithms, and arranging encryption algorithms in some order. Finally, the combined encryption algorithm is successfully made by using the initial encryption algorithm, Micro Gerard encryption algorithm and the famous Base64 encryption algorithm. That is, in accordance with the order of the initial encryption algorithm, the improved Micro Gerard encryption algorithm and the famous Base64 encryption algorithm, the user's information is gradually encrypted, and the algorithm security is greatly enhanced.

Zhang Yun-Peng et al [5] “Digital image encryption algorithm based on chaos and improved DES ” In recent years, encryption technology has been developed quickly and many image encryption methods have been put forward. Chaos based image encryption technique is a new encryption technique for images. It utilizes chaos random sequence to encrypt image, which is an efficient way to deal with the intractable problem of fast and highly secure image encryption. However, the chaos based image encryption technique has some deficiencies, such as the limited accuracy problem. This paper researches on the chaotic encryption, DES encryption and a combination of image encryption algorithm, and simulate these algorithms, through analysis of the algorithm to find the gaps. And on this basis, the algorithm has been improved.

Xiaozhong Pan et al [6] “Multiclass detect of current steganographic methods for JPEG format based re-steganography” The aim of this paper is to properly classify various stego images of JPEG to their own steganographic methods. Although some Multiclass Detection methods had been previously published by the authors, they all had various limitations and disadvantages. First, models of some detect methods are too complicated, and their process are too fuzzy. Second, the performance of some detect methods could decline when the embed rate minis. Based on re-steganography, the detection of this paper's algorithm extracts 109-dimensions features and trains SVM multiclassifiers to classify all kinds of stego images and cover images with very high precisions (approximately 100%). Not only the model is very simple, but the performance is all the same excellent when the embed rate minis.

Marwaha et al. [7] in the multimedia stegano cryptic system, the message will first be encrypted using public key encryption algorithm, and then this encrypted data will be hidden into an image file thus accomplishing both data encoding and hiding. The multimedia data will be used to provide the cover for the information. Each color in the multimedia data when considered as an element in an arrangement of 3D matrix with R, G and B as axis can be used to write a cipher (encoded message) on a 3D space. The method which we will use to map the data is a block or a grid cipher. This cipher will contain the data which will be mapped in a 3-D matrix form where the x-axis can be for R (red), y-axis can be for G (green) and z-axis can be for B (blue). Embedding data into an image often changes the color frequencies in a predictable way and also gives redundancy in formats like bmp. To remove this predictability, we will embed the cipher in the image in an encrypted form using a reference database instead of direct bit variations. Also only jpeg image will be used as it reflects the least impact of steganography. Cryptographic algorithms generally need a reference table which aids the conversion of a small block of data into another block (may not be a block of data in the original content).

3. Proposed Work

Problem Formulation: It has been already explained that the Steganography is the art and science of invisible communication. This is accomplished through hiding information behind the image, thus hiding the existence of the communicated information. Our first problem is to study the Pixel Group Trace Model-Based Quantitative Steganalysis for Multiple Least-Significant Bits Steganography and need to compare the results in terms of PSNR, MSE with the implementation of Cryptography Technique. The secret data is encrypted using MD5 and DES then embedding of data into the cover image is done using MLSB. In the result we will get the stego image. The data will be first encrypted and then kept behind the image this is how we are going to hide our data.
3.1 Objectives

- To propose Enhanced Data Hiding Scheme using hybrid MD5 & DES Schemes.
- To implement security using MLSB embedding.
- Prevent from unauthorized access on confidential data.
- To get least image distortion.
- To have more data security using cryptography and steganography.

3.2 Flow of Work

![Flowchart Image]

Our first problem is to study the Pixel Group Trace Model-Based Quantitative Steganalysis for Multiple Least-Significant Bits Steganography. In this work, firstly an input image or secret image is taken on which encryption is done using MD5 or DES (Data Encryption Standard). This encrypted data is hired by embedding using MLSB (Multiple Least-Significant Bits) behind the cover image. After that, we will get our required stego image which needs to be decrypted for the original image. The data will be first encrypted and then kept behind the image this is how we are going to hide our data. Finally, we will compare the results in terms of PSNR, MSE with the implementation of Cryptography Technique.

4. Results and Discussion

![Graph Image 1]

Figure 1: This Graph is use to represent Encoding.

![Graph Image 2]

Figure 2: This Graph is use to represent Load Image.

![Graph Image 3]

Figure 3: This Graph is use to represent MD 5 Encryption.

![Graph Image 4]

Figure 4: This Graph is use to represent Cover Image.

![Graph Image 5]

Figure 5: This Graph is use to represent Secret Image.
Figure 6: This Graph is use to recover image if we lost our image by mistake.

Figure 7: This graph is use to Save Image.

Figure 8: This Graph is use to Select Steganography in release phase.

Figure 9: This is use to enter Private Key.

Figure 10: This is use to represent Decode Image.

Figure 11: This is use to represent Complete Parameters.

5. Conclusion and Future Work

Encryption is a way to enhance the security of a message or file by scrambling the contents so that it can be read only by someone who has the right encryption key to unscramble it. Steganography is the art and science of invisible communication. This is accomplished through hiding information in other information, thus hiding the existence of the communicated information. In this first of all we doing encoding after that we load a image after that we use MD5 Encryption algorithm to improve the security. Then we select a cover image and also select a secret image. Save the cover and secret image. We use the Stegography in release phase to make better our system and to improve the security. After that we enter the Private Key and decode the image. In last we got four parameters i.e PSNR, MSE, EPI, CORELATION. On the basis of these parameters we conclude that the performance of our system is better. In future we can improve the performance of our system various security algorithms like HOOSC, Some other Key Generation Methods.

References


