A Brief study on Steganography techniques

Kavitha K J, Pushpalatha O

Asst Prof, Department of ECE, JIT, Davanagere, Karnataka, India

Abstract**—** *As there is a lot of advancement in the field of internet or communication technology, we have various means of storing, accessing and distribution of the data in the digital format. Due to the rapid advancement in this field has also introduced many challenges to the researchers to provide security to the information which is transmitted over the network. The digital information circulating over the network also includes the medical information. In order to provide security, confidentiality and integrity, the steganographic techniques can be employed. In the section 1, it gives the introduction about available hiding techniques; the section 2 explains the various steganography properties, the section 3 gives the types of steganographic techniques, the section 4 gives the applications of steganography, the section 5 gives the quality parameters to be measured for medical information, and the section 6 gives the steganographic algorithms available. Finally the section 7 concludes that to prevent unauthorized access steganography is the suitable technique.*

Keywords**— *Steganography, security, integrity.***

I. INTRODUCTION

Nowadays the technology has rationally developed so that controlling and dealing out of secret data are done on internet because of the common usage of internet. The information needs to be transmitted or exchanged over the Internet for many purposes. In some cases we may need to keep the information confidentially. In such cases if we directly transmit the information, it may be misused by the hackers and may be used for illegal purpose. To avoid such cases security can be provided for the information in three ways [13].

1. Cryptography
2. Steganography
3. Water marking

Each technique is discussed in brief:

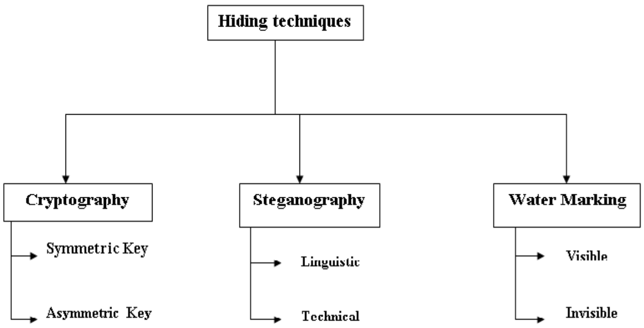

Fig.1: Hiding Techniques

Cryptography which is also called as cryptology is actually derived from Greek word kryptos means that "hidden, secret".

Cryptography [3] can be defined as a technique of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it or in other words we can define it as a secret writing or encoding of messages in secret code and decoding of the information only by the authorized persons.

Cryptography may again classify as:

1. Symmetric Key Cryptography
2. Asymmetric Key Cryptography

Steganography is pronounced STEHG-uh-NAH-gruhf-ee, from Greek *steganos*, or "covered," and *graphie*, or "writing". It is defined as "hiding of a secret message within a usual message and the removal of it at its target" [4]. Steganography is used to hide an encoded message so that no one doubts it exists. Ideally, anyone glance over our data will fail to know it contains translated data.

Steganography can also be classified as:

1. Linguistic
2. Technical which includes audio, text, video and image.

Water marking is a technique of hiding the information in a cover image. This technique may be used to verify the authenticity, integrity or in other words can be used to show the owner ship [5]. The digital watermark can be broadly classified in to two types:

- Visible watermark

- Invisible watermark

Among the above three hiding techniques, steganography plays an important role in providing the security to the information which is exchanged over internet. The steganography can be implemented as shown below:

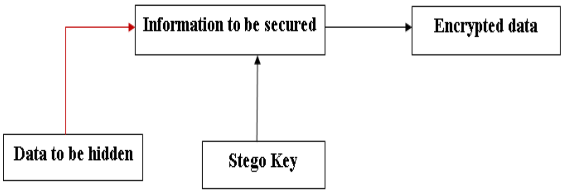

Fig.2: Steganography process

II. PROPERTIES OF STEGANOGRAPHY

The following are the some of the key properties of steganography method which will motivate many of us to use this technique for protecting the information [1].

Imperceptibility: Imperceptibility is the property in which, it is very difficult to distinguish between the original and the steganographic image or information.

Data Payload capacity: This parameter defines the amount of secret data or number of bits that can be inserted in the message without [9] degrading the quality of the image.

Robustness: It is the parameter used to measure the degree of withstanding the ability to avoid the destroying of the embedded information without affecting the quality of the cover image.

III. TYPES OF STEGANOGRAPHIC TECHNIQUES

The techniques used to embed the information can be broadly classified under two categories:

Spatial domain: It is also called substitution method. In this steganographic technique, the data that is to be hidden is directly embedded in the pixels of the image. Least significant bit (LSB) [7 & 8] method is the most popularly used spatial domain technique in which it substitutes the least significant bit of original pixel with the message bit and the human eye will not be able to detect the hidden information in the message. Many other spatial domain methods are also available such as Code word grouping – palette generation algorithm, Adaptive Steganography, Steganography Algorithm using Pattern Matching with External Hardware, Pixel Indicator etc.

Transform domain: this technique is also called frequency domain technique. In this technique, first the information or the message is converted into frequency domain [11] and then in to the transformed image, a confidential data can be hidden.

In order to perform the conversion from time domain in to frequency domain, various techniques are available such as DCT, DWT, and DFT etc. Among all the techniques, DWT yields better results.

IV. APPLICATIONS OF STEGANOGRAPHY

Nowadays Steganography is widely used in many applications. Some of the applications are listed below:

- Private communication and secret data storing
- Security for data modification
- Access control system for digital content sharing
- And many others

Historically, steganography provides the following:

- Potential capability to hide the presence of private data
- Very hard to detect the hidden or embedded data
- Improving the secrecy of the encoded data

In the field of communication, if we want to transmit some confidential data, then the first step is to select some dummy message depending on the size of the data that is to be embedded. Later the confidential data can be embedded in the dummy message using some encryption algorithms along with the key generated. Later to extract the confidential data, the extraction program can be used with the help of the same key which was generated during the process of embedding.

The data that is to be embedded is fragile in most of the cases, it means that the embedded data can be altered or undergoes modification [10] by the unauthorized parties. If it is altered or modified, it is easily detected by the extraction program.

Nowadays the digital information is becoming more popular as it can be easily transmitted to many of the receivers over the internet with free charges. In some case the information that we need to transmit is very valuable, in that case simply transmitting the information may be accessed by illegal people and lead to the misuse of the information. Especially in case of legal cases, the protection of information is very important. In such cases, we can issue a special “access key” in order to extract the information at the receiver side which is possible with the help of steganographic techniques.

Among all the above applications, Medical information transformation [2] is one of the important applications which are playing an important role nowadays.

When the higher diagnosis is required from a specialist who might be at some remote places, in such cases, the information or the image needs to be transmitted over the internet. The transmitted information may be misused by some unauthorized persons. In order to avoid such possibilities, we can employ steganographic techniques to protect the information. While applying the technique, care should be taken to see that the information or the image should undergo degradation because a small change in the information or image may lead to the misdiagnosis which may result in the disastrous result.

Nowadays most of the researchers working on color images and videos using steganographic techniques. And also work is going on 3D images also.

V. QUALITY METRICS

Some of the quality parameters have to be used in order to evaluate the quality of the images. The below paragraph gives the metrics that are usually used to measure the quality of the images after embedding the information into the image.

- Peak signal to Noise ration
- Structural similarity index
- Mean
- Median
- Bit error rate
- Correlation coefficient

VI. STEGANOGRAPHIC ALGORITHMS

The various algorithms are available to perform the steganographic process. Some of them are listed below [12]:

Advanced Encryption Standard: The Advanced Encryption Standard abbreviated as AES is a symmetric block cipher [6] which is first used by the U.S. government in order to protect classified information and is implemented in software and hardware throughout the world to encrypt sensitive data.

It was introduced in the year 1997 as a successor of Data encryption standard DES.

International Data Encryption Algorithm: It is abbreviated as IDEA which was developed first by Zurich, Switzerland. This algorithm uses a block cipher with 128-bit key and is considered to be very secure.

SEED: It is a symmetric encryption algorithm developed by Korea Information Security Agency (KISA) and a group of experts, in the year 1998. The input/output block size of SEED is 128-bit and the key length is also 128-bit. A 128-bit input is divided into two 64-bit blocks and the right 64-bit block is an input to the round function with a 64-bit sub key generated from the key scheduling.

Cipher algorithm: It is a mathematical formula which is designed specifically to ambiguous the value and content of data. Most valuable cipher algorithms use a key as part of the formula. This key is used to encrypt the data, and either that key or a complementary key is needed to decrypt the data back to a useful form.

VII. CONCLUSION

In the above article we have seen there are many hiding techniques available. One of them is steganography technique which is widely used. And also we have seen some of the algorithms. Using steganography with other techniques, secureness can be increased for images/information.

VIII. ACKNOWLEDGMENT

We thank our family members, friends and colleagues for their support in preparing the paper.

REFERENCES

[1] B. Saha and S. Sharma, “Steganographic Techniques of Data Hiding Using Digital Images (Review Paper),” *Defence Science Journal*, vol. 62, no. 1, pp. 11–18, Jan. 2012.

[2] P. Kamal and M. Punjab, “Review of Different Steganographic techniques on Medical images regarding their efficiency,” vol. 4, 2005.

[3] A. J. Raphael, “Cryptography and Steganography – A Survey,” vol. 2, no. 3, pp. 626–630.

[4] R. A. Sampaio and M. P. Jackowski, “Assessment of Steganographic Methods in Medical Imaging,” 1985.

[5] H. V. D. B. Sc, “Available Online at www.jgrcs.info Steganography , Cryptography , Watermarking : A Comparative Study,” vol. 3, no. 12, pp. 2010–2012, 2012.

[6] D. K. Sarmah and N. Bajpai, “Proposed System for data hiding using Cryptography and Steganography,” pp. 1–8.

[7] M. T. Student, “A SECURE DATA EMBEDDING TECHNIQUE IN IMAGE STEGANOGRAPHY FOR MEDICAL IMAGES,” vol. 3, no. 8, pp. 7753–7756, 2014.

[8] V. Pandey, "International Journal of Advanced Research in Computer Science and Software Engineering Secure Medical Image Transmission using Combined Approach of Data-hiding , Encryption and Steganography," vol. 2, no. 12, pp. 54–57, 2012.

[9] P. Mortazavian, M. Jahangiri, E. Fatemizadeh, G. Y. Av, A. Blv, and P. Sq, " Proceedings of fourth IASTED International conferece", Spain,"A LOW-DEGRADATION STEGANOGRAPHY MODEL," pp. 914–920, 2004.

[10] C. P. Sumathi, T. Santanam, and G. Umamaheswari, "A Study of Various Steganographic Techniques Used for Information Hiding," vol. 4, no. 6, pp. 9–25, 2013.

[11] R. Doshi, P. Jain, and L. Gupta, "Steganography and Its Applications in Security," vol. 2, no. 6, pp. 4634–4638, 2012.

[12] M. Umamaheswari, "Analysis of Different Steganographic Algorithms for Secured Data Hiding," vol. 10, no. 8, pp. 154–160, 2010.

[13] C. Science and S. Engineering, "An Overview of Different Type of Data Hiding Scheme in Image using Steganographic Techniques," vol. 4, no. 1, pp. 746–751, 2014.