ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
*Vol. 2, Issue 5, May 2013*

# STEGNOGRAPHY—"The Art of Hiding Information" A Comparison from Cryptography

**Aparajita, Prof Ajay Rana**

Assistant Professor, Dept. of MCA, Galgotia Institute of Management and Technology/ UPTU, Greater Noida, Uttar Pradesh, India [1]

Program Director, Amity School of Engineering and Technology, Amity University, Uttar Pradesh, India

**Abstract:** Stegnography is about hiding the information whether the hiding thing is an image only. We should encrypt the information before hiding it. Many different formats of files can be used to hide the information but digital files are most widely used because of their frequency on internet. There are varieties of stegnography tools available with their own strength and weaknesses. This paper is a glance and a view at hiding the text in text and hiding the secret information in an image file using various stegnography tools. And will tour the main difference between cryptography and stegnography.

**Keywords:** Stegnograpghy, Cipher text, Plain text, Hiding information, Cryptography.

## I. INTRODUCTION

"We want nothing more than to connect and companies that are connecting us electronically want to know who's saying what, where. As a result, we are more known than ever before". ---- By Prof. Susan Crawfor at Benjamin N. Cardozo School of Law. This is very clear from the statement by Prof, that privacy of the information communication is out most important in today's world. What we share and what we communicate needs to be hided from intruders and people not meant for that information. The biggest reason why intruders gain success in gaining the information is that whatever they acquire is in the form they can easily read and understand. They can use the information to misrepresent someone, can modify it or even can use it to launch an attack. One solution to this problem is, using the techniques of stegnography.
The word stegnography is derived from a Greek word meaning **"covered writing".** Basically it belongs to the class of **"Cryptology",** which includes three techniques in it:

a) **Cryptography:** Science of coding and decoding secret messages.
b) **Stegnography:** The art of hiding information in a way that prevents from detection.
c) **Cryptanalysis:** Breaking cryptosystems or deciphering messages without prior knowledge of the cryptosystems.

**Stegnography:** An art of hiding **THE EXISTENCE** of communication, in contrast to cryptography. Basically it's a method of concealing the information in ways that prevents the detection of hidden information. We should encrypt our information before communicating. By doing this, even if the message is being found, the intruder won't be able to learn what we are trying to send in the message. Stegnography became more important as more people have chosen cyberspace as a mode of sharing the information. It includes an array of secret communication methods that hide the message from being seen or discovered. The development of Stegnography has paralleled the simultaneous growth of **"Cryptanalysis"—** the breaking of ciphers and detecting the steganographic content in the image or text files. Even in the history the kings and the warriors used to use stegnography to hide their messages. Like the kings used to shave the heads of the messenger and then write the message, and let the hairs grow again. Then passing the message without anybody's knowledge and the message will never be traced until the head is shaved off again. Another method, was to write the message with invisible ink and that to by seeing it in mirror, so as to even if someone decode the message through invisible ink, the message won't be understood. The history is filled with more such examples. But, the growing possibilities of modern communications need the special means of security especially on computer network. Consequently, the security of information has become a fundamental issue. Network security is becoming more important as the number of data being exchanged on the internet increases. Therefore, the confidentiality and the data integrity both require to be protected against unauthorized access and use. The result is the explosive growth in the field of information hiding.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
*Vol. 2, Issue 5, May 2013*

Stegnography hides the secret information within the host data set and reliably communicate it to a receiver. The host data set is purposely corrupted, but in a covert way, designed to be visible only to an information analysis. The process of stegnography is to exploit human perception and senses to hide a file inside another file.
Before discussing further we should flip through the concepts and history of cryptography also.

**Cryptography:** It's the study of techniques for secure communication even in the presence of **"adversaries"** (the third party). More generally, it's the art of burring the message in such a way which overcomes the influence of adversaries. Cryptography prior to the modern age was just a story of what might be called Encryption—the conversion of text from a readable state to apparent nonsense.

**Types of cryptography methods:-**

1. **Symmetric:** Here the same key is used to code and decode the message.
2. **Asymmetric:** Mathematical related keys are used to conceal the message.
3. **Hybrid:** combines the strength of both the techniques.

**Methodology:** In the methodology it is depicting different techniques from stegnography as well as from cryptography to hide the information and to describe the difference between both the techniques.
The following are some techniques of Cryptography using which information is being encrypted and then sent to the receiver along with the **"Code"** or the **"Cipher"** text which will be used by the receiver to decrypt the hidden information. Some of them are algorithms which were earlier used to conceal the data, but, not used in today's world. There are basically **two** types of ciphers used.

- **Streamed Based Ciphers:** In this technique one alphabet or text is used at a time to disguise the whole text with a key stream.
- **Block Ciphers:** Dissemble a whole block of message instead of one alphabet or text.

1. **Classical Encryption Technique: -** There are further techniques which come under this series.

   - **Caesar Cipher:** It's on the name of Julius Caesar. Here we use the concept that we add 3 to the individual character and it becomes the key for decoding the message.
     **Example:** Using Caesar Cipher converts the following plain text to cipher text

Plain Text: C R Y P T O G R A P H Y Key=3
Cipher Text: F U B S W R J U D S K B

Plain Text: H E L L O Key=4
Cipher Text: L I P P S

With these examples it's very clear that only one alphabet is being coded at one time. This is the key rule of Caesar Cipher.

- **Monoalphabetic Cipher:** Here a fixed pattern is being decided in advance seeing to which the text is disguised. Like for the following examples we have coded the 26 alphabets with other alphabets but there should no repeation of alphabets.
  **Example:** Using the Monoalphabetic Cipher code the plain text.

Plain Alphabets: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Pattern: F I A E M Z O H L R U B Y S Q C D P X W V T J K G N

Plain Text: O R A C L E

Cipher Text: Q P F A B M

Plain Text: D A T A B A S E

Cipher Text: E F W F I F X M

So according to our pattern we have changed the alphabets accordingly.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
*Vol. 2, Issue 5, May 2013*

- **Polyalphabetic Cipher:** Here we make a table of alphabets in a way that row wise and column wise we write the alphabets and then produce the key for coding the plain text. With this table we are trying to show the basic technique which lies behind the Polyalphabetic cipher. We will write the 26 alphabets in both row and column direction. Inside the table we will start from the first row and write all alphabets row wise below the 26 alphabets written in columns. Then from the second row, as it start from **B** we will start writing from **B** then **C then D** and so on till whole column. But, in the end when we will reach Y in the above column then the alphabets will be finished, so we will start again from **A**. This procedure will be repeated till whole table 26 row wise and 26 column wise alphabets are written. After that we will decide a key for our plain text containing 3 or 4 or 5 as per you like alphabets. The Cartesian product of our first alphabet of plain text with the first alphabet of key will become our **CIPHER ALPHABET** for that particular plain alphabet. Repeat this procedure for the complete plain text till the **CIPHER** is produced. Following is the table depicting the procedure only till **N.**

| | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **A** | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
| **B** | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
| **C** | C | D | E | F | G | H | I | J | K | L | M | N | O | P |
| **D** | D | E | F | G | H | I | J | K | L | M | N | O | P | Q |
| **E** | E | F | G | H | I | J | K | L | M | N | O | P | Q | R |
| **F** | F | G | H | I | J | K | L | M | N | O | P | Q | R | S |
| **G** | G | H | I | J | K | L | M | N | O | P | Q | R | S | T |
| **H** | H | I | J | K | L | M | N | O | P | Q | R | S | T | U |
| **I** | I | J | K | L | M | N | O | P | Q | R | S | T | U | V |
| **J** | J | K | L | M | N | O | P | Q | R | S | T | U | V | W |
| **K** | K | L | M | N | O | P | Q | R | S | T | U | V | W | X |
| **L** | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y |
| **M** | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| **N** | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A |

Now using this table we will conceal the following plain text.

Plain Text: L A C K A F E Key= M A J

To produce the **CIPHER TEXT** we will repeat the 3 alphabets of our key to the plain text. Then we will see in the table where the Cartesian product of the plain text alphabet is and the key alphabet is coming, that particular alphabet will become the **CIPHER** for the plain text alphabet.

Cipher Text: X A L W A O P

Plain Text: H I J A C K Key= ABCD

Cipher Text: H K L D C L

- **Play Fair Cipher:** This is the most important and generally used technique to conceal the text. In this we make a 5*5 matrix, where we write our key first and rest of the alphabets later row wise. The word we use for the key should have no repeated alphabets and it should not contain **I & J** in the key word. The reason behind this is that in the matrix we write these two alphabets together. Now to produce the Cipher text we have four different rules:
  - **a)** If we are going column wise down then we will start from one alphabet after the plain text alphabet.
  - **b)** If we are going column wise up then we will start from one alphabet down the plain text alphabet.
  - **c)** If we are going row wise either left or right we will start one alphabet before the plain text alphabet.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
*Vol. 2, Issue 5, May 2013*

**Example:** Using the play fair cipher solve the following problem:

Plain Text: C O M E T O T H E W I N D O W Key: KEYWORD

Now, we will make a 5*5 matrix, with our key written first and then the rest of alphabet and I&J will be written in one column.

| | | | | |
|---|---|---|---|---|
| K | E | Y | W | O |
| R | D | A | B | C |
| F | G | H | I/J | L |
| M | N | P | Q | S |
| T | U | V | X | Z |

Now, we will calculate the cipher text of each alphabet and will write it together as combined.

Cipher Text: L C N K Z K V F Y O G Q K O

Plain Text: A C C O U N T S Key: FONAMCE

Now, we will again make a 5*5 matrix and follow the above procedure to conceal the plain text to a cipher text.

| | | | | |
|---|---|---|---|---|
| F | O | N | A | M |
| C | E | B | D | G |
| H | I/J | K | L | P |
| Q | R | S | T | U |
| V | W | X | Y | Z |

Cipher Text: C F A P S C U T

- **Hill Cipher:** In this we make 2*2, 3*3, 4*4 matrix to solve our problem. The formula for the calculation of cipher text is:

**Cipher text = [Key * Plain text] MOD 26**

The size of the matrix will determine the way of our formula. Suppose if its 2*2 matrix then we will divide our plain text into groups of two and if 3*3 then in groups of three and so on.

**Example:** Using hill cipher solves the following problems.

Plain Text: M I N I N G Key: [ 2 5

7 8]

Cipher Text: M S O Z E J

The calculation is same as in the formula and because our key is a 2*2 matrix so we will divide the plain text into groups of two and will apply the formula separately to groups for calculating the cipher text.

ISSN: 2319-8753

International Journal of Innovative Research in Science, Engineering and Technology
*Vol. 2, Issue 5, May 2013*

Plain Text: N E T W O R K

Key: [4 2 8
9 1 3
5 7 6]

Cipher Text: E W Z S D Y K

## II. CONCLUSION

From the above survey it is clear that to disguise our plain text we need some technique. In today's world Public Key Cryptography is used to hide the information and it uses the whole block instead of an individual alphabet. There is a lot of future research possible in this field. Stegnography is a really interesting subject and outside of the mainstream cryptography and system administration that most of us deal with day after day. Stegnography can be used for hidden communication. We have explored the limits of stegnography theory and practice, and a comparison to cryptography

## REFERENCES

1. Information hiding: steganography and watermarking—attacks and countermeasures NF Johnson, Z Duric, S Jajodia… - Journal of …, 2001.
2. Performance study of common image steganography and steganalysis techniques M Kharrazi, HT Sencar… - Journal of …, 2006.
3. Information Hiding: **Steganography** and Watermarking-Attacks and ... www.springer.com › Home › Computer Science
   a. Cached
   b. Similar
   c. Share
4. Integrating Classical Encryption with Modern Technique F Saeed, M Rashid - IJCSNS International Journal of Computer, 2010 - paper.ijcsns.org.
5. Call for attack to evaluate the **cryptographic techniques** - CRYPTREC ww.cryptrec.go.jp/english/topics/cryptrec_20101001_callforattack.html.
6. Trends of **Cryptographic Techniques**. sciencelinks.jp › ... › Joho Shori Gakkai Kenkyu Hokoku (2002) by H IMAI - 2002
7. Friedman, William F. (1922). "The index of coincidence and its applications in cryptology". Department of Ciphers. Publ 22. (Geneva, Illinois, USA: Riverbank Laboratories).
8. Shannon, C.E. (1949). "[[Communication Theory of Secrecy Systems]]". Bell System Technical Journal (28-4): 656–715.
9. Shamir, A. (November 1979). "How to share a secret". Communications of the ACM 22 (11): 612–613. doi:10.1145/359168.359176.
10. Kohnfelder, Loren M. (1978). "On the Signature Reblocking Problem in Public Key Cryptography". Communications of the ACM 21 (2): 179