2011 International Conference on Information and Electronics Engineering
IPCSIT vol.6 (2011) © (2011) IACSIT Press, Singapore

ASSYMETRIC KEY STEGANOGRAPHY

Debrup Banerjee

NIT-DURGAPUR

Abstract. Information security is an important area of research and study that is gaining importance with passage of time. The main objective of information security is to secure the information from all kinds of threats and attacks. Many kinds of techniques have been invented to secure the information and the most popular among them is cryptography [1]. Although in cryptography [1]the text is sent to the destination in a very secured form as many coding techniques are used to encrypt the text, if an interceptor intercepts the secret message he will get the message in coded format which he will not be able to decrypt without knowing the key used to encrypt the message, but he will guess that
something unusual is happening between the sender and the receiver. Hence a new technique Steganography [2][3] as in [2] [3] has been discovered where the messages or information sent will not attract to themselves, to messengers, or to recipients .But recently it has been found out that there are also some ways to detect the secret message from the cipher meaningful text encrypted by Steganography [2][3]. Hence in this paper, a new approach has been adopted to build a more powerful model of text Steganography [2][3] by asymmetric key approach which specifies sending of numerical digits as keys in meaningful form to protect the secret message. .

Keywords. Cryptography , steganography , encryption , decryption.

1. INTRODUCTION

Steganography [2][3] is a process that involves hiding a message in an appropriate carrier for example an image or an audio file. In these cases the objective is not to make it difficult to read the message as cryptography [1]does, it is to hide the existence of the message in thefirst place possibly to protect the courier.But it has been found out that steganography [2][3] have got some disadvantages. Hence in this thesis a new approach have been thought of to eliminate the disadvantages of steganography [2][3] and get a more secured steganographic model.

2. RELATED WORKS

2.1. TEXT STEGANOGRAPHY TECHNIQUES

Some researches on hiding information in texts have been performed. Here are some of the previous research works.

- Particular characters in words

  Hiding information can be performed by selecting characters in certain words. In the simplest form, the first words in a paragraph are selected in such a manner, that by placing the first characters of the words side by side we can extract the information

- Line or Word shifting

  Shifting text lines vertically and words horizontally may help in hiding some Information. This method shifts line up or down with a fixed space Say (0.03inch) and modifies the distance between words according to the hidden Information but when the text is Electronically rewritten or modified, there is a great possibility for the hidden Text to be destroyed.

- Adding extra white spaces or abbreviations

Space steganography [2][3] hides information by adding extra white spaces between words, Or at end of lines. This technique can be used with any text and does not reveal the secrecy to the normal reader. However its capacity and robustness is low. It cannot hide too much information within text and some electronics text editors automatically

remove extra white spaces.

3. EXPLANATION WITH EXAMPLE

3.1. SENDER SITE

ENCYPTION

- Secret Message :- DO IT

- Intermediate Cover text: - GO TO.

- Public key obtained :- 301153

  Explanation: - In the secret message, "DO IT" the alphabet D after incrementing by 3 alphabets, gets substituted by G and a mapping from D to G is obtained. In the secret message, "DO IT" second alphabet O is mapped to O in the intermediate cover text and so, the second position digit in Public key in Step 3 is 0. The same reason for number 11 and 5 which is obtained after incrementation and decrementation of the next alphabets, and 3 which is the rightmost digit in the public key is the

  position which signifies the 3RD digit of the public key which is 1 which is not a unit digit , while decrypting 1 should be taken as 11 and the whole public key 301153 should be broken into decimal places 3,0,11,5,3 otherwise the decryption[6] process will be very hard if this position is not known.

- Real Cover message to be sent: - RAMS'S ID NUMBER IS 301153 AND HE WILL GO TO OFFICE FROM TOMMOROW.

- 2nd. Public key obtained from the above message is 81023

  Explanation: - First decimal place of the 2nd. Public key (81023) = 8 signifies the position where the secret message is embedded. In step 5, the word GO is placed after 8 words. The next two digits 10 signify that the secret message is up to the 10th. word. The fourth digit of the second Public key (that is, 2) specifies that two digits 10 will be separated from 8 to know the actual positions of the encrypted intermediate text. Last place in the 2nd public key = 3 which signifies the place in the intermediate text where the alphabet is decremented but not incremented.

- Normal text to send this 2nd public key:-SHYAM'S ID NUMBER IS 81023 AND HE WILL BE RESIGNING FROM OFFICE TOMMOROW.

- Finally the two cover texts (the real cover text and the normal cover text) are to be sent one after the other to the receiver via any means. But the original secret message is embedded only in the real cover text and the normal cover text is passed only to send the 2nd public key which will be hashed with the 1st. public key to give the actual secret message to the receiver.

3.2. RECEIVER SITE

DECRYPTION

- The Receiver will get two numbers. One is 301153 and the other is 81023

- The only thing which is used as private key in this algorithm is the meaning which each place of the digits signifies of the two public key received by the receiver. The two public keys are known only to the receiver and the sender.

- Now, the Receiver shall first apply 301153 and 81023 to the final cover text. The cover text is: RAMS'S ID NUMBER IS 301153 AND HE WILL GO TO OFFICE
  FROM TOMMOROW.

- To separate the intermediate cover text from the final cover text, the Receiver will first use the 2nd. Public key, that is, 81023 and extracts the sentence; “GO TO” from the final cover text.

- Then, the Receiver shall separate the 1st. Public key according to the units and tens digit. For example, 301153 is separated as (3 and 0) and (11 and 5) because the last digit which is 3 is used to separate 11 from the other unit digits as the 3 signifies the position where we get a 10’s digit.

- Now, from the 2nd. Public key, the User checks which digit among these
increments and which one decrements the alphabets and then finally, by applying the values of the digits 3,0,11,5 to the intermediate Cover Text “GO TO”, the Receiver shall get the Secret message “DO IT”.

4. CONCLUSION

The process discussed in the thesis is a bit complex. So, some future works need to be done to make this process much more secure and a bit simpler for the end users to use but that should not be at the cost of security. The aim is to finally develop or find out a cryptographic method which encrypts a very large decimal digit into a very small decimal digit and decrypting the original digit from the small decimal digit, which shall help the sender to build a meaningful sentence based on the number of digits available.

5. ACKNOWLEGDMENT

I want to thank sincerely my project guide Mr. Souvik Bhattacharya during my btech course who helped me a lot to clear my basics regarding study of steganography [2][3].

6. REFERENCES

[1] Cryptography – Wikipedia, http://en.wikipidea.org/wiki/Cryptography

[2] Steganography - wikipidea, http://en.wikipidea.org/wiki/Steganography

[3] A history of steganography - Fabien Petitcolas

[4] A novel Arabic text steganographic method - Adnan Abdul-Aziz Gutub, and Manal Mohammad Fattani, □http://www.waset.org□

[5] Image segmentation and steganography - Mamta juneja and Parvinder Singh Sandhu

[6] Simple Encrytion - Decryption Algorithm - Majid Al-Qdah,, Lin Yi Hui.
http://www.cscjournals.org/csc/manuscript/Journals/IJCSS/Volume1/Issue1/IJCS