International Journal on Recent and Innovation Trends in Computing and Communication
Volume: 4 Issue: 12

ISSN: 2321-8169
54 – 56

Data Hiding using Emoticons

Miss. Madhura A. Bhoi, Miss. Barkha V. Budhwani, Miss. Poonam R. Dhayagode, Miss. Tahurafeeza J. Sayyed, Miss. Pratvina Talele
MIT College of Engineering, Pune.

Abstract: In 21st century Digital communication has become a very essential part of day to day life of every human. It has continuously evolved over the year. It has made communication easier. People can communicate anywhere and anytime large amount of data is transmitted every day, every second. Here data security comes into picture. Each and every individual want their data to be secure and doesn't want it to be used in an unauthorized way. There are various techniques to provide data security such as cryptography and steganography. Cryptography is the science of encompassing the principles and methods of transforming a plain text message into one that is unintelligible and then, that message back to its original form. Steganography is the art and science of hiding information by embedding messages into other messages. Steganography means "Covered Writing" in Greek. Both the techniques have their own limitations; to overcome those limitations, here in this paper, we are combining both the techniques to enhance data security.

*****

I. INTRODUCTION

Data security has become a major concern these days. Communications can be some of the most sensitive messages sent across the network. Hackers these days target a range of important data- from customers' personal information to overall business processes. Therefore, there is a need of a system that secures data communication. Cryptography and steganography are the two concepts used for providing data security. A few key concepts are as follows:

1. **Cryptography**: Cryptography is the science encompassing the principles and methods of transforming a plaintext message into one that is unintelligible, and then that message back to its original form.
2. **Plaintext**: A plaintext is the original message.
3. **Cipher text**: Cipher text is the transformed message produced as output. It depends on plaintext and the key.
4. **Key**: It is some critical information used by the cipher, known only to the sender and the receiver.
5. **Encryption**: It is the process of converting plaintext to cipher text.
6. **Decryption**: It is the process of converting cipher text back to plaintext.

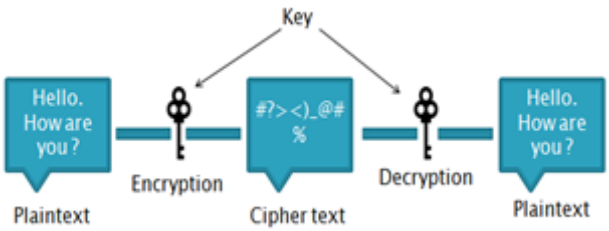

Figure 1: Cryptography.

7. **Steganography**: Steganography is the art and science of hiding information by embedding messages within other, seemingly harmless messages. **Steganography** means "covered writing" in Greek.
8. **Cover/Carrier message**: It is the message within which the original message is embedded.
9. **Stego-text**: It is the message after embedding **original** message within the carrier message.

Figure 2: Steganography

In the proposed system we are combining the benefits of both the techniques.

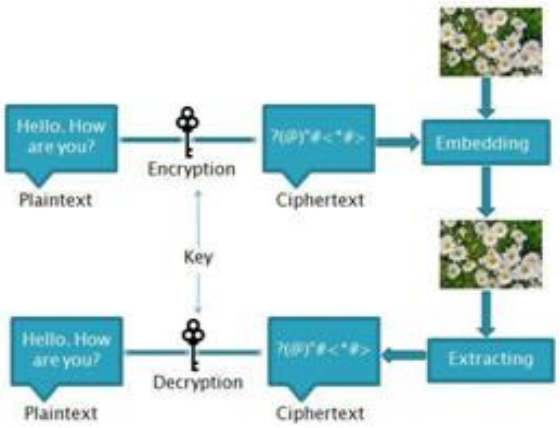

Figure3: Cryptography+Steganography

II. RELATED WORKS

Unlike other steganography approaches, studies on data

hiding in short message service (SMS) are quite limited. The first investigation on SMS steganography was reported by Shirali Shahreza [5], which utilized image as cover media and SMS as carrier to transfer the hidden message to the recipient. In this method, a black and white (B&W) image is used to transfer the hidden message by changing the intensity of pixels. However, low capacity (27 bytes) is the main drawback of the mentioned technique, due to the use of only black and white image rather than using full color.

The study presented in [1] exploited the use of emoticons and lingoes to hide the secret message. But, in this case if the cover media is hampered there is no way to protect the underlining original message.

III. PROPOSED METHOD

In this approach, the emoticons that are frequently typed in chat and SMS, are used as cover media to deliver the data in a hidden manner. The emoticon is a sort of icons that depicts a user's feeling in text mode as shown in figure 5. These icons are widely used, especially in SMS and chat where there is a limitation on the number of characters.

Figure 5: Various emoticons

The illustration of the proposed method depicted in figure 6.

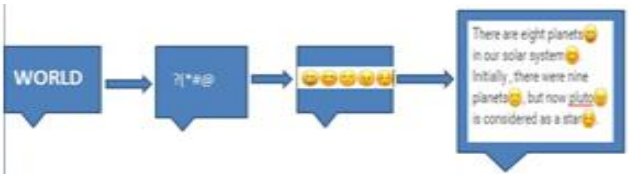

Figure 6: Data hiding system

To start with, first the user has to enter the text. Then the provided text will be encrypted using the public key of the receiver. The encrypted message is then hidden behind the cover media that are the emoticons. Again the emoticons are put into the cover text which finally makes our stego text to be transmitted over the communication channel.

The receiver on the other end receives the stego text. He then first extracts the emoticons from the cover text and then maps the meaning of each emoticon to get the encrypted messages. He then, using he's own private key to decrypts the message to finally get the plain text message.

IV. ADVANTAGES AND LIMITATIONS

The proposed method combines the effects of both cryptography and steganography. In earlier approaches [2,3,4,5] only steganography was used for hiding data , in this case if the cover media is broken or hampered the underlined secret message can be easily accessed in an unauthorized way. Therefore in the proposed system we are first encrypting the text and then hiding it with a cover text so that even if the covered media is hampered or attacked the attacker will be able to see the encrypted data and not the original message.

The combined effects of both the techniques thus maintains the confidentiality of the communication and increases reliability.

It uses public key algorithm. As public key algorithm uses two keys it is difficult to access the data even if attacker gets one of the keys.

The only limitation of proposed system is that it is more suitable only for short secret messages , since each alphabet requires the storage of one emoticon.

V. Conclusion

After studying various approaches and techniques we have come to the conclusion that the communication can be more secure if we combine the effects of both cryptography and steganography. Advantage of the system can be that it provides dual security by first encrypting the data and then hiding it. The only limitation is that it is suitable for short messages. The proposed system can be used in critical situations where the communication mainly takes place through short messages such as defense systems.

References

[1] Vahab Iranmanesh, Ho Jing Wei, Sean Lee Dao-Ming, Olasimbo Ayodeji Arigbabu "On using Emoticons and Lingoes for Hiding Data in SMS", 2015 International Symposium on Technology Management and Emerging Technologies(ISTMET), August 25- 27, 2015, Langkawi, Kedah, Malaysia.

[2] S. Bhattacharyaa, I. Banerjee, and G. Sanyal, "A survey of steganography and steganalysis technique in image, text, audio and video as cover carrier", Journal of global research in computer science, 2(4), 2011.

[3] Chandrakant Badgaiyan, Ashish Kumar Dewangan, hupesh Kumar Pandey, "A SURVEY PAPER ON

SMS BASED STEGANOGRAPHY", International Journal of Advanced Computer and Mathematical Sciences ISSN 2230-9624. Vol 3, Issue 4, 2012, pp 441-445.

[4] I. V. S. Manoj, "Cryptography and steganography", International journal of computer applications, 1(12), 2010.

[5] M. Shirali-Shahreza, "Stealth steganography in SMS", Proceedings of the third IEEE and IFIP International conference on wireless and optical communications networks (WOCN), April, 2006.