Impact Factor (SJIF): 3.632

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 3, Issue 2, February-2016

Data Hiding and Storing using Steganography

Ekta Chauhan, Khusbu Panchal, Romil Patel

Information Technology, SIE
Information Technology, SIE
Information Technology, SIE

Abstract — In today's world, the communication is the basic necessity of every growing area. Everyone wants the secrecy and safety of their communicating data. The purpose of our project is to hide the message and prevent the detection of hidden message by using Steganography. It maintains secrecy between two communicating parties. Steganography is the practice of hiding private or sensitive information within something that appears to be nothing out to the usual. Steganography is often confused with cryptology because the two are similar in the way that they both are used to protect important information. The difference between two is that steganography involves hiding information so it appears that no information is hidden at all. If a person or persons views the object that the information is hidden inside of he or she will have no idea that there is any hidden information, therefore the person will not attempt to decrypt the information. The most common use of steganography is to hide a file inside another file.

Keywords- Encryption-Decryption, Steganography, Data Storing, Data Hiding, Security, Privacy.

I. INTRODUCTION

In today's world, the communication is the basic necessity of every growing area. Everyone wants the secrecy and safety of their communicating data. In our daily life, we use many secure pathways like internet or telephone for transferring and sharing information, but it's not safe at a certain level. In order to share the information in a concealed manner two techniques could be used. These mechanisms are cryptography and steganography. In cryptography, the message is modified in an encrypted form with the help of encryption key which is known to sender and receiver only. The message cannot be accessed by anyone without using the encryption key. However, the transmission of encrypted message may easily arouse attacker's suspicion, and the encrypted message may thus be intercepted, attacked or decrypted violently. In order to overcome the shortcomings of cryptographic techniques, steganography techniques have been developed. Steganography is the art and science of communicating in such a way that it hides the existence of the communication. Thus, steganography hides the existence of data so that no one can detect its presence. In steganography the process of hiding information content inside any multimedia content like image, audio, video is referred as "Embedding".

Encryption and Decryption

The process of making data unreadable by other humans or computers for the purpose of preventing others from gaining access to the content is known as Encryption. Decryption is the process of taking encrypted text and converting it back into text that human can read and understand.

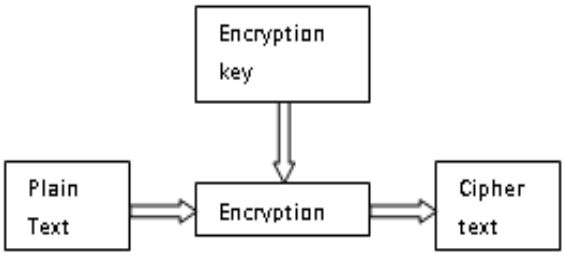

Fig 1: Encryption

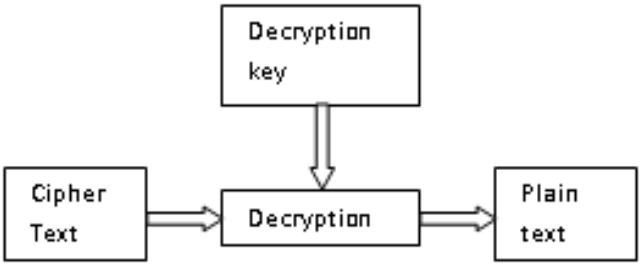

Fig 2: Decryption

II. APPLICATION OF STEGANOGRAPHY

There are many applications for digital steganography of image, including copyright protection, feature tagging, and secret communication. Copyright notice or watermark can embedded inside an image to identify it as intellectual property. If someone attempts to use this image without permission, we can prove by extracting the watermark. In feature tagging, captions, annotations, time stamps, and other descriptive elements can be embedded inside an image. Secret communication does not advertise a covert communication by using steganography. Therefore, it can avoid scrutiny of the sender, message and recipient. This is effective only if the hidden communication is not detected by the others people.

III. BLOWFISH ALGORITHM

Blowfish is a variable-length key, 64-bit block cipher. There are two parts to this algorithm; a part that handles the expansion of the key and a part that handles the encryption of the data

.

KEY EXPANSION IN BLOWFISH ALGORITHM

1. Initialize the P-array and S-boxes.
2. XOR P-array with the key bits. For example, P1 XOR (first 32 bits of key), P2 XOR (second 32 bits of key).
3. Use the above method to encrypt the all-zero string.
4. This new output is now P1 and P2.
5. Encrypt the new P1 and P2 with the modified subkeys.
6. This new output is now P3 and P4.
7. Repeat 521 times in order to calculate new subkeys for the P-array and the four S-boxes.

DATA ENCRYPTION AND DECRYPTION IN BLOWFISH ALGORITHM

Data encryption occurs via a 16-round Feistel network. Each round consists of a key dependent permutation, and a key and data-dependent substitution. All operations are XORs and additions on 32-bit words.

1. The input is 64-bit data element, say x.
2. Divide x into two 32-bit halves. i.e. xL, xR.
3. Perform operations on xL and xR.
4. Now swap xL and xR.
5. After the sixteenth round, swap xL and xR again to undo the last swap.
6. Finally recombine xL and xR to get the cipher text.
7. Decryption is exactly the same as encryption.

IV. FLOW OF PROPOSED SYSTEM

First data will be selected or entered by the user of the system .After that the blowfish encryption algorithm is applied on the selected data to convert that data in unreadable form i.e. the data converts plain text into cipher text. Now to secure that data we choose one image to hide that data behind it. But before that we have to generate one stego image. To convert the image in stego image apply Discrete Wavelet Transform (DWT) algorithm. Finally the data is hidden behind the image. The hidden data can be stored in the folder.

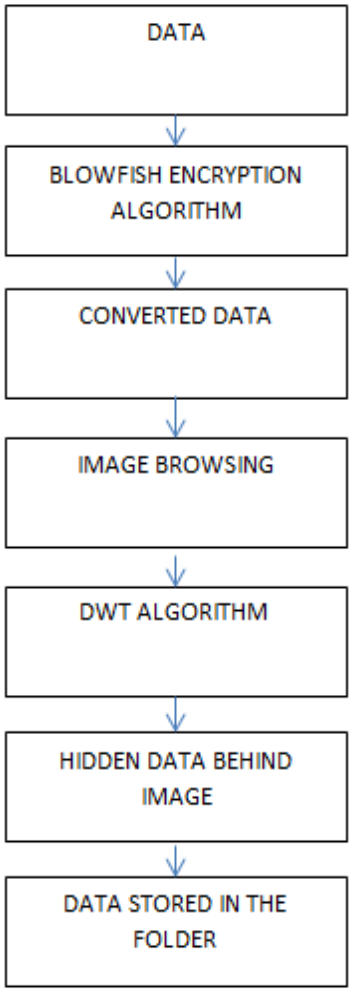

Fig 3: Flow of the proposed system

V. CONCLUSION AND FEATURE SCOPE

In this paper, we explained only encryption and decryption process of the data. In this review paper we implement encryption process. In our future research paper we implement the Discrete Wavelet Transform (DWT) algorithm.

ACKNOWLEDGEMENT

We take this opportunity to express our profound sense of gratitude and respect to all those who helped us through the duration of this project. Firstly, we are extremely grateful to Sigma Institute's, for providing us the excellent working environment to undergo our project. We devote our success in this effort to our project guide for giving us the opportunity to undertake the project and providing crucial feedbacks that influenced us and provide opportunity to undertake the project work in the esteemed concern. We are also deeply thankful to Head of I.T. Department, whose useful suggestion, gentle soothing attitude and right directions helped us a lot to learn in this project and also for her constant encouragement and support throughout the project. Last, but not the least, we would like to extend our profound thanks to all our esteemed colleagues and friends at college level who helped us in the specific areas of this project.

REFERENCES

[1] Moerland, T., "Steganography and Steganalysis", Leiden Institute of Advanced Computing Science, www.liacs.nl/home/ tmoerl/ privtech.pdf.
[2] Silman, J., "Steganography and Steganalysis: An Overview", SANS Institute, 2001.
[3] Jamil, T., "Steganography: The art of hiding information is plain sight", IEEE Potentials, 18:01, 1999.
[4] Wang, H & Wang, S, "Cyber warfare: Steganography vs. Steganalysis", Communications of the ACM, 47:10, October 2004.
[5] Anderson, R.J. & Petitcolas, F.A.P., "On the limits of steganography", IEEE Journal of selected Areas in Communications, May 1998.

[6] Marvel, L.M., Boncelet Jr., C.G. & Retter, C., "Spread Spectrum Steganography", IEEE Transactions on image processing, 8:08, 1999.
[7] Dunbar, B., "Steganographic techniques and their use in an Open-Systems environment", SANS Institute, January 2002.
[8] Artz, D., "Digital Steganography: Hiding Data within Data", IEEE Internet Computing Journal, June 2001.
[9] Simmons, G., "The prisoners problem and the subliminal channel", CRYPTO, 1983 Chandramouli, R., Kharrazi, M. & Memon, N., "Image steganography and Steganalysis: Concepts and Practice", Proceedings of the 2nd International Workshop on Digital Watermarking, October 2003.
[10] Zoran Duric, Sushil Jajodia, Neil Fisher Johnson, "Information Hiding".