Steganography with Encrypting Secret Message via Cryptography

[1]Chitranshu Jain, [2]Aishwarya Rai, [3]Anupriya Singh, [4]Dhananjay Gupta, [5]Jayesh Surana,
[1,2,3,4]Students, [5]Assistant Professor
Department of Information Technology
Shri Vaishnav Institute of Technology & Science, Indore, India

---

Abstract **- While transferring the data among the users the confidentiality and privacy should be maintained. The digitally shared data between the users should be converted to some unreadable format which will not be tampered by the intruders. To meet these requirements the technique Steganography can be used. In this technique we use different mediums to hide the data that are text, images, audio, video etc. This paper is focusing on encrypting secret message with the help of symmetric algorithm then hide this encrypt secret message in cover medium like audio, video, images etc. As all we know that data in steganography hides in clear form, so if stego object get captured by any intruder. We lost the confidentiality of the data. Also, now days detection of steganography is not remains that difficult. Many tools and techniques are capable which can detect messages. To provide more security to data, we introduce the concept that encrypt secret message with cryptographic algorithm**.

IndexTerms

- Cover File: It is a file in which hidden information will be stored.
- Stego Medium: Medium through which the information is hidden.
- Message: The data to be hidden or extracted

I. INTRODUCTION

Steganography is a technique use to hide a secret information in such a way that someone unable to find the presence of the information. The term "Steganography" is a combination of two Greek words "Steganos + Graphy". The meaning of steganos is covered or secrete and the graphy means writing or drawing. Hence the covered writing is also called as steganography. The main goal of steganography is to hide the information using some covered media. In case of cryptography the user can able to see the contents of message but can't comprehend the information. On the other hand, in steganography the existence of information will not be noticed by viewer because it is embedded inside some medium. This medium is also called as carrier or cover object. It may be an image, video, texts, sound or any music file.

II HISTORY OF STEGANOGRAPHY:

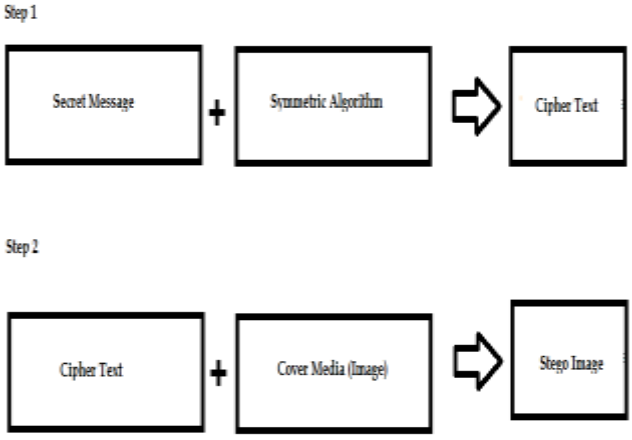
Invisible ink can be applied to a writing surface with a specialty stamp, fountain pen, toothpick, calligraphy pen, or even a finger dipped in the liquid. Once dry, the written surface looks as if it were blank, with a similar texture and reflectivity as the surrounding surface. The sender writes the message with invisible ink and after some sometime written message get disappeared, and seen only when this paper comes under some specific light.

III.PROBLEM DOMAIN:

Now days, providing security to data plays very important role. In steganography hidden message are of plain text. So if any intruder got cover file. They can easily obtain the data with the help of steganography tool and data is in clear form. Hence, we lost privacy of data.

IV.IDEA:

Don't hide the secret data directly. First, encrypt data with symmetric cryptography algorithm, after that hide this data in cover medium.



V. ALGORITHM:

Blowfish is a symmetric block cipher that can be effectively used for encryption and safeguarding of data. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for securing data. Blowfish was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms. Blowfish is unpatented and license-free, and is available free for all uses. Blowfish Algorithm is a Feistel Network, iterating a simple encryption function 16 times. The block size is 64 bits, and the key can be any length up to 448 bits. Although there is complex initialization phase required before any encryption can take place, the actual encryption of data is very efficient on large microprocessors

VI.CONCLUSION:

Due to heavy requirement of information it is necessary to keep the data safe for future references, the data and the usage can be done but at other side there can be certain issues like intruders, man-in-middle attack which makes the digital transmission to be careful, the approach with respect the image steganography is useful if the user wants the data to be hidden but in certain way making it confidentiality property is followed. The approach can be very useful for the person who can be known to the system and works around the things which might require the confidentiality to be followed, the approach is one of the alternatives so as the data is hidden using some JPEG or BMP images which may be useful in hiding the data very easily. Also, in any case stego file got captured by bad guy. It is completely useless because data is encrypted.

VII. References:

[1] Sneha Bansod and Gunjan Bhure, Data Encryption by Image Steganography
[2] Arvind Kumar Km. Pooja, Steganography- A Data Hiding Technique, International Journal of Computer Applications (0975 – 8887) Volume 9– No.7, November 2010
[3] MUHALIM MOHAMED AMIN , SUBARIAH IBRAHIM ,MAZLEENA SALLEH ,MOHD ROZI KATMIN INFORMATION HIDING USING STEGANOGRAPHY
[4] Mehdi Kharrazi, Husrev T. Sencar, and Nasir Memon, Image Steganography: Concepts and Practice
[5] KK Ravi Ayappa, STEGANOGRAPHY -INFORMATION HIDING FOR SECURE COMMUNICATION


IJEDR