ORIGINAL RESEARCH PAPER

Engineering

Volume - 7 | Issue - 4 | April-2017 | ISSN - 2249-555X | IF : 4.894 | IC Value : 79.96

CRYPTOSTEGANOGRAPHY: A MULTILAYER SECURITY DATA HIDING

KEYWORDS: Cryptography, Steganography, Cipher, Encryption, Decryption.

Neha Swami
Department of Information Technology, DYPCOE, Akurdi, Pune

Priyanka Patil
Department of Information Technology, DYPCOE, Akurdi, Pune

Priyanka Pawar
Department of Information Technology, DYPCOE, Akurdi, Pune

Smita Patil
Department of Information Technology, DYPCOE, Akurdi, Pune

ABSTRACT There are two different techniques, both Cryptography and steganography used to cipher or hide information or data in processing communication. Cryptography means, the message sends in an unreadable form in order to only the receiver can understand and read the encrypted text. Such as, in steganographic system, data is cover up by using different media file like text, image, audio, video, file. This paper has main goal to improve a new method of hiding a secret message in different media, by exploiting the benefits of combining cryptography and steganography. A new encryption method by using steganography and cryptography used in this paper for improve the security and improve the quality of service.

INTRODUCTION

One of the reasons why the attackers become successful in intrusion is that they have an opportunity to read and comprise most of the information from the system. A new method based on the combination of both Cryptography and Steganography is necessary which overcome each other's weaknesses and make difficult for the intruders to attack or swipe sensitive information is being proposed.

Cryptography is the study of various techniques used for secure communication by applying some cryptographic algorithms in the presence of third parties or attacker [11].

Steganography is the study of concealing information in digital media through the methods of embedding hidden messages while only the sender and the intended receiver(s) can detect the existence of the messages [1].

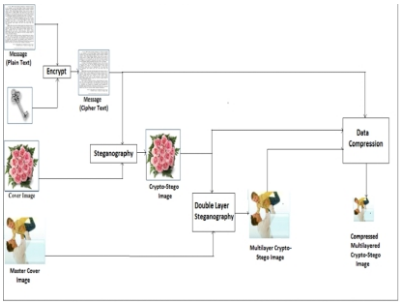

Figure 1:The basic working of a Multilayer security data hiding encoder

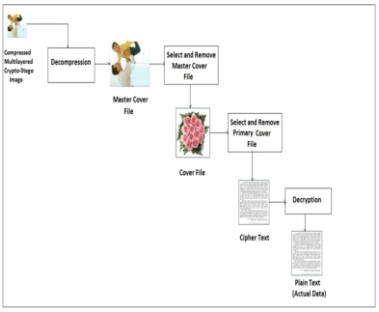

Figure 2:The basic working of a Multilayer security data hiding decoder

APPLICATIONS :

1.Confidential communication and hidden data storage:
The "secrecy of the embedded data is imperative in this area. Historically, steganography have been addressed in this area. Steganography provides us with:

(A) Potential capability to hide the in processed confidential data
(B) Hardiness of detecting the embedded data
(C) Increasing the secrecy of the encrypted data.

2.Protection of data amendment :
We take advantage of the slenderness of the embedded data in this application area. We assurances in the Home Page that "the embedded data can rather be delicate than be very sturdy." Actually, embedded data are frangible in most steganography programs. Particularly, Qtech Hide & View program embeds data in an extremely frangible manner.

CASE STUDY

The personal identity number (PIN) that must be entered into an automated teller machine (ATM), along with a bankcard to confirm that the card is being used by an owner, may either be stored in the bank's computers in a cipher form or be encrypted on the card itself. The conversion used in this type of cryptography is called one-way means it is easy to compute a cipher given the bank's cipher key and the customer's PIN but computationally impractical to compute the plaintext PIN from the cipher, even though the key is known.

CONCLUSIONS

A new high capacity and highly secure data hiding has been presented. The master cover file is most essential for providing more data security as multi-layer Steganography including Cryptography provide a wide range of data security. The experimental results carried out show that the system produces a good quality stego images for a fairly huge amount of payload. The two layer security mixed with high capacity and good transparency make the proposed system a very good user system for convert communications.

REFERENCES:

[1] HoWon Kim, Member, IEEE, and Sunggu Lee, Member, IEEE, "Design and Implementation of a Private and Public Key Crypto Processor and Application to a Security System". In IEEE Transactions on Consumer Electronics, Vol. 50, No. 1, FEBRUARY 2004.
[2] Alvaro Martn, Guillermo Sapiro, and Gadiel Seroussi, Fellow, IEEE., "Is Image Steganography Natural?",In IEEE Transaction On Image Processing, VOL. 14, NO. 12, DECEMBER 2005,
[3] Jessica Fridrich, Miroslav Goljan, Petr Lisonek, and David Soukal, "Writing on Wet Paper", In IEEE Transactions On Signal Processing, VOL. 53, NO. 10, OCTOBER 2005.
[4] Jamshed Hasan, "Security Issues of IEEE 802.16 (WiMAX)", Originally published in the Proceedings of 4th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, 5th December, 2006