A Novel Plausible Deniability Scheme in Secure Steganography

Farshad Amin, Majid Soleimanipour, and Alireza Karimi

Abstract—The goal of steganography is to avoid drawing suspicion to the transmission of a hidden message. If suspicion is raised, steganography may fail. The success of steganography depends on the secrecy of the action. If steganography is detected, the system will fail but data security depends on the robustness of the applied algorithm. In this paper, we propose a novel plausible deniability scheme in steganography by using a diversionary message and encrypt it with a DES-based algorithm. Then, we compress the secret message and encrypt it by the receiver's public key along with the stego key and embed both messages in a carrier using an embedding algorithm. It will be demonstrated how this method can support plausible deniability and is robust against steganalysis.

***Keywords*—**Steganography, Cryptography, Information Hiding.

I. Introduction

STEGANOGRAPHY includes methods of transmitting secret messages through cover mediums or carriers in a way that existence of the embedded message is indistinguishable. Carriers consist of image, audio, text or video and the secret message can be a media such as plain text, encrypted text or any information that we can be displayed as a string of bits.

Steganography is a subset of information hiding and at the time of rapid development of digital technology and universality of Internet has become one of the most interesting fields of data security.

Today, available techniques of information hiding such as image, audio and video steganography have been widely studied. These techniques are designed so that be resistant against steganalysis but most of them do not support plausible deniability under pressure.

II. Previous Work

Plausible deniability has been studied in different context in the literature [4, 7-9]. It was first used in the context of arguments [7]. This technique uses an indirect way of putting forward a reposition such that a target respondent is meant to accept, at the same time putting a defensive shield if in case the responder queries and you don't have a justifiable response. In the context of cryptography, it was first introduced by Canetti [8]. In this work, plausible deniability is defined as: "encryption scheme is deniable if the sender can generate plausible keys and random choices that will satisfy the authority and at the same time keep the past communication private." Canetti [8] defines and constructs various types of deniable encryption schemes. Chun [9] proposed a novel data-hiding methodology similar to invisible ink where a general steganography system and plausibly deniable schemes, are demonstrated.

Potdar [4] used a cipher text as an incomprehensible cover medium. Fig. 1 shows the proposed algorithm.

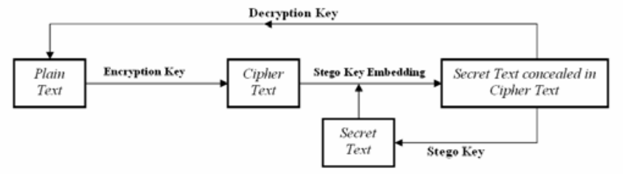


Fig. 1 Block diagram of [4]

For implementation of the proposed method, the following five steps are considered:

Step 1: Construct cipher text as cover medium - Let *m* be the plain text, *E* encryption algorithm, *K* encryption key and m_c cipher text, then:

$$E_K(m) = m_c$$

Step 2: Embed secret message in the cipher text - Let SE be the steganography algorithm, K_S the stego key, *M* the secret message, *SG* the stego object, then:

$$SE_{K_S}(M, m_c) = SG$$

Step 3: Uncover secret message from stego object – Let *SD* be the algorithm for recovering the secret message using the same stego key, then:

$$SD_{K_S}(SG) = M$$

Step 4: Deny secret communications – Reveal encryption key *K* to uncover the cover medium plain text to deny information hiding. Thus:

$$D_K(SG) = \hat{m}$$

Step 5: Verification – Encryption of the resulting text in Step 4 must give the stego object. That is:

$$E_K(\hat{m}) = \hat{m}_c$$

The condition for plausible deniability is:

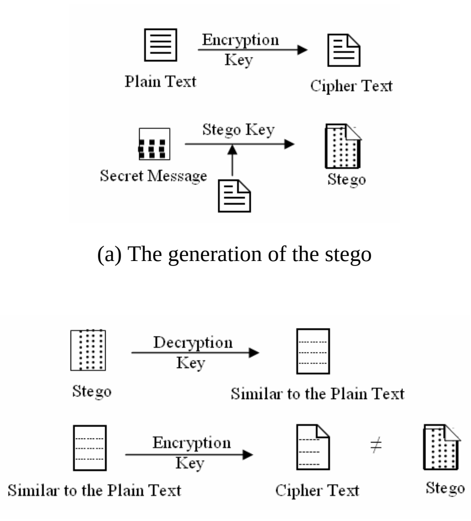
$$\hat{m}_c = SG$$

Farshad Amin is currently with the Computer Engineering Department, University of Sharif, Tehran, Iran (e-mail: f_amin@ce.sharif.edu).

Majid Soleimanipour is currently with the Electrical Engineering Department, University of Sharif, Tehran, Iran (e-mail: soleimanipour@sharif.edu).

Alireza Karimi is with the Iran Telecommunication Research Center, Tehran, Iran (e-mail: emailkarimi@yahoo.com).

The method in [4], shall satisfy this condition, otherwise, deny is not plausible. However, finding a satisfying algorithm is very difficult. A graphical representation of the method is shown in Fig. 2.



(a) The generation of the stego

(b) Not supporting plausible deniability

Fig. 2 Graphical representation of Potdar's method

III. Theoretical Structure of the Proposed Method

In this method, we use a diversionary message and encrypt it with a DES-based algorithm. Then, we encrypt the secret message by the receiver's public key along with the stego key and embed both messages in a carrier using an embedding algorithm. Fig. 3 shows this procedure. We use a cipher text as the carrier, as it is incomprehensible and can provide higher capacity. Thus, if the capacity for hiding the secret message and diversionary message is not an issue, a plain medium is applicable.

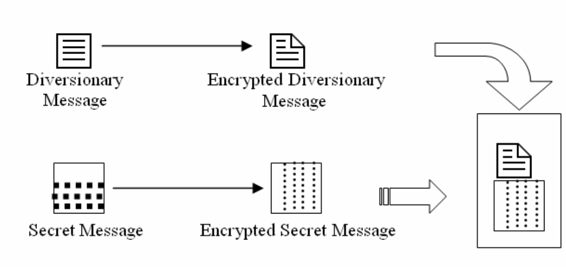


Fig. 3 Proposed Method

Fig. 4 shows the general block diagram of the proposed steganography model.

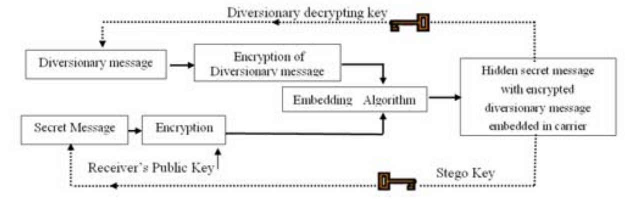


Fig. 4 Block diagram of the proposed method

To increase secrecy and plausible deniability, we also use a diversionary message because firstly people usually do not try to discover the steganographic content in an incomprehensible medium. This will fulfill the aim of steganography that is to avoid drawing suspicion to the secret communication. The third party will try to decrypt but does not obtain any useful information but the intended receiver who has the stego key will have access to the hidden information. Secondly this technique supports plausible deniability, i.e., if the third party doubts about the existence of a secret communication, the diversionary encrypting key can be detected but the stego key will not be detected.

So if the third party has access to the hidden secret message in the encrypted diversionary message, the design of the algorithm is such that he will find the diversionary encrypting key, which leads to the diversionary message.

The receiver using private key and stego key and by decryption and reconstruction of the information will also have access to the secret message.

IV. Mathematical Model

To support plausible deniability, two embedding algorithm along with two different keys are needed. It means that we embed the diversionary message into a media by an algorithm and a distinct key and embed the secret message by an embedding algorithm and another key. Under pressure, the algorithm and the key for the diversionary message can be revealed. This algorithm must be capable of re-generating of the stego. Therefore to implement the system we follow the following steps:

Step1: To encrypt the original and diversionary message, two algorithms are needed. Let m be original message, m_d diversionary message, E and E_d encryption algorithms, K and K_d encryption keys and m_c and m_{cd} the encrypted secret and diversionary message, then:

$$E_K(m) = m_c \quad \text{And} \quad E_{d\,K_d}(m_d) = m_{cd}$$

Step 2: To embed data in the carrier M, we need two steganography algorithms. This step generates the stego object. Let SE_O be steganography algorithm of the secret message, SE_d steganography algorithm of the diversionary message, K_{S_0} the original steganography key, K_{S_d} the diversionary steganography key, SG_O the original stego and SG_d the diversionary stego, then:

$$SE_{OK_{S_O}}(M, m_c) = SG_O$$

$$SE_{dK_{S_d}}(M, m_c) = SG_d$$

Step 3: To detect the embedded data in the stego object, the receiver can use the original stego key and the steganography algorithm (SD_O).

$$SD_{OK_{S_O}}(SG_O) = m_c$$

Under pressure, the diversionary key and steganography algorithm (SD_d) can be uncovered.

$$SD_{d\,K_{Sd}}(SG_d) = m_{cd}$$

Since the diversionary message is also encrypted and is not determined for the third party, the third party will try to decrypt it and this is exactly what keeps him away from the secret message, so the secrecy of the original message is maintained.

If user A is again under pressure, he will give the decryption key of the encrypted message to the third party. Fig. 5 shows this procedure.

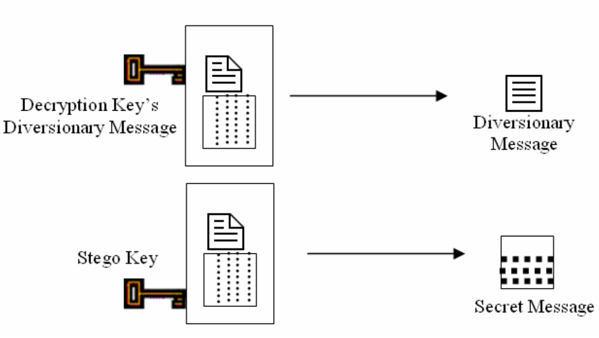


Fig. 5 Support of Plausible Deniability

V. Conclusion

In this paper, we studied a theoretical structure for a steganography method and showed that how using a diversionary message in an incomprehensible medium can provide secrecy and plausible deniability.

This structure can be used both for deception of the third party and for hiding the information. If the existing information in the encrypted message is an arbitrary diversionary message, the third party will be deceived and the main information will not be detected. On the other hand, the sender and receiver can deny existence of any secret communication.

References

[1] Y.H. Yu, C.C. Cheng, Y.C. Hu, “Hiding secret data in image via predictive coding” , Pattern Recognition, Vol. 38, pp 691-705, 2005.

[2] Fisk G., Fisk, M., Papadopoulos, C., Joshua, N., “Eliminating Steganography in Internet Traffic with Active Wardens”, Available:http://citeseer.nj.nec.com/fisk2eliminating.html, 2002

[3] Fabien A.B.P., Anderson R., Kuhn M.,” Information Hiding- A Survey”, in Proceeding of IEEE, pp. 1062-78, 1999.

[4] Potdar V., Chang E., “Visibly Invisible”. Available: http://www.fit.cbs.curtin.edu.au/ceela/docs/index.php, 2004.

[5] Provos N., “Defending against statistical steganalysis”, 10th USENIX Security Symposium, 2001.

[6] Sallee P., “Model-based steganography”, International Workshop on Digital Watermarking, Seoul, Korea, 2003..

[7] Walton D., “Plausible Deniability and Evasion of Burden of Proof”. Available: http://io.uwinnipeg.ca/~walton/96deniability.pdf, 1996.

[8] Canetti R., Dwork C., Naor M., Ostrovsky R.,”Deniable Encryption”, Crypto '97, pp. 90-104, 1997.

[9] Chun-Hsiang Huang, Shang-Chih Chuang, Ja-Ling Wu, ” Digital Invisible Ink and its Applications in Steganography”, Proceeding of the 8th workshop on Multimedia and security, Geneva, Switzerland, pp. 23 – 28, 2006.