A Model of Anonymous Covert Mailing System  
Using Steganographic Scheme

Eiji Kawaguchi*, Hideki Noda*, Michiharu Niimi* and Richard O. Eason**

(*) Kyushu Institute of Technology  **) University of Maine
Kitakyushu, 804-8550 Japan  Orono, Maine 04469-5700 USA
(*) kawaguch@know.comp.kyutech.ac.jp

Abstract
In this paper we show a model of an anonymous covert mailing system for Internet communication. It is the system scheme of an on-going project to develop a real-life secure mailing system in our group. In this system a sender can send a secret message even to a non-acquainted person in an anonymous way. The users of this system are assumed to be members of a closed organization. But it is not primarily limited only to such users. It is a quite easy-to-use system with very cheap cost. This project as of now is at a prototype-developing stage.

1. Introduction
Human beings have long hoped to have a technique to communicate with a distant partner anonymously and covertly. We may be able to realize this hope by using steganography. Modern steganography has a relatively short history because people did not pay much attention to this skill until Internet security became a social concern. Most people did not know what steganography was because they did not have any means to know the meaning. Even today ordinary dictionaries do not contain the word “steganography.” Books on steganography are still very few [1], [2].

In 1997 the authors invented a new steganographic method named “BPCS-Steganography.” The most important feature of this steganography is that it has a very large data hiding capacity [3], [4]. It normally embeds 50% or more of a container image file with information without increasing its size. We made an experimental program (for Windows) and located it on a Web site for free downloading [5]. We also have several introductory Web pages to BPCS-Steganography and its applications [6].

Steganography can be applied to variety of information systems. Some key is used in these systems when it embeds/extracts secret data. One natural application is a secret mailing system [7] that uses a symmetric key. Another application pays attention to the nature of steganography whereby the external data (e.g., visible image data) and the internal data (any hidden information) cannot be separated by any means. We will term this nature as an “inseparability” of the two forms of data.

In the present paper we will show our basic model of an anonymous and covert e-mailing
system. The structure of the present paper is as follows. In Section 2 we will make a short discussion on the problems of an encrypted mailing system. Section 3 describes the scheme of the Anonymous Covert Mailing System. We will show how we can make it a safe system in Section 4. Finally, in Section 5, we show our future schedule to make it a real life system.

2. Problems of an encrypted mailing system

There are two types of cryptography systems: (1) symmetric key systems, and (2) asymmetric key systems.

In a symmetric system a message sender and receiver use a same encoding/decoding key. In this system, however, the sender and the receiver must negotiate on what key they are going to use before they start communication. Such a negotiation must be absolutely secret. They usually use some second channel (e.g., fax or phone). However, the second channels may not be very secure. There is another problem in this situation in that if the sender is not acquainted with the receiver, it is difficult to start the key-negotiation in secret. Further more, the more secure the key system is, the more inconvenient the system usage is.

An asymmetric system uses a public key and a private key system. The public key is open to the public, and it is used for message encoding when a sender is sending a message to the key owner. However, if the public key is counterfeited, this system does not work at all. So, the public key must be guaranteed as authentic. Therefore, this system needs a special authentication bureau, which is an organization that all the people in the world can trust in. In reality, it can only exist if it commercially pays. Therefore, this system is expensive and time consuming for users.

3. A model of an anonymous covert mailing system

The authors’ research group at Kyushu Institute of Technology started to develop a secure and easy-to-use e-mailing system according to the BPCS-Steganography method. We do not intend to develop a new “message reader-and-sender” or “message composer”, but we are developing three system components that make an Anonymous Covert Mailing System (ACMS). A message sender inserts (actually, embeds) a secret message in an envelope using steganography and sends it as an e-mail attachment. The receiver receives the attached envelope and opens it to receive the message. An “envelope” in this system is actually an image file that is a container, vessel, cover, or dummy data in the terminology of steganography. This system can solve all the problems mentioned above.

The following items are the conditions we have set forth in designing the system.

1. The name of the message sender can be anonymous.
2. The message is hidden in the envelope and only the designated receiver can open it.
3. Sender can send a secret message even to an unacquainted person.
4. It is easy to use for both sender and receiver.
5. The system is inexpensive in installing and using.

We expect this ACMS is used in a closed organization (such as in a company), but there are no restrictions for any group (or the general public) to use it.

3.1 Components of the system
ACMS is a steganography application system (or program). It makes use of the inseparability of the external and internal data. The system can be implemented differently according to different programmers or different specifications. Different ACMS' are incompatible in operation with others. In other words, an organization using ACEM must use one single ACMS. However, each member in the organization uses it in a customized way. The customization is made when the user installs it on his/her own computer. In the following description, \( M_i \) denotes a member \( i \), and \( M_j \) denotes a member \( j \).

An ACMS consists of the three following components.

1. Envelope Producer (EP)
2. Message Inserter (MI)
3. Envelope Opener (EO)

We denote \( M_i \)'s ACMS as \( ACMS_i \) (i.e., customized ACMS by \( M_i \)). So, it is described as \( ACMS_i = (EP_i, MI_i, EO_i) \).

\( EP_i \) is a component that produces \( M_i \)'s envelope (\( E_i \)). \( E_i \) is the envelope (actually, an image file) which is used by all other members in the organization when they send a secret message to \( M_i \). \( E_{i0} \) is produced from an original image (\( E_0 \)). \( M_i \) can select it according to his preference. \( E_i \) has both the name and e-mail address of \( M_i \) on the envelope surface (actually, the name and address are "printed" on image \( E_i \)). Fig. 1 illustrates an envelope. It will be placed at an open site in the organization so that anyone can get it freely and use it any time. Or someone may ask \( M_i \) to send it directly to him/her.

\( MI_i \) is the component to insert (i.e., embed according to the steganographic scheme) \( M_i \)'s message into another member's (e.g., \( M_j \))'s envelope (\( E_j \)) when \( M_i \) is sending a secret message (\( Mess_i \)) to \( M_j \). One important function of \( MI_j \) is that it detects a key (\( Key_j \)) that has been hidden in the envelope (\( E_j \)), and uses it when inserting a message (\( Mess_i \)) in \( E_j \).

\( EO_i \) is a component that opens (extracts) \( E_i \)'s "message inserted" envelope \( E_i(Mess_j) \) which \( M_i \) received from someone as an e-mail attachment. The sender (\( M_j \)) of the secret message (\( Mess_j \)) is not known until \( M_i \) opens the envelope by using \( EO_i \).

3.2 Customization of an ACMS

Customization of an ACMS for \( M_i \) takes place in the following way. \( M_i \) first decides a key (\( Key_i \)) when he installs the ACMS onto his computer. Then he types in his name (\( Name_i \)) and e-mail address (\( EAdrs_i \)). \( Key_i \) is secretly hidden (according to a steganographic
method or some other method) in his envelope \( (E_i) \). This \( Key_i \) is eventually transferred to a message sender’s \( MI_j \) in an invisible way. \( Name_i \) and \( EAdrs_i \) are printed out on the envelope surface when \( M_i \) produces \( E_i \) by using \( EP_i \) (cf. Fig. 1). \( Key_i \) is also set to \( EO_i \) at the time of installation. \( Name_i \) and \( EAdrs_i \) are also inserted (actually, embedded) automatically by \( MI_i \) any time \( M_j \) inserts his message \( (Mess_j) \) in another member’s envelope \( (E_j) \). The embedded \( Name_i \) and \( EAdrs_i \) are extracted by a message receiver \( (M_j) \) by \( EO_j \). Fig. 2 illustrates the scheme of this AC-Mailing system.

![Fig. 2 The scheme of the AC-Mailing system.](image)

### 3.3 How it works

When some member \( (M_j) \) wants to send a secret message \( (Mess_j) \) to another member \( (M_i) \), whether they are acquainted or not, \( M_j \) gets (e.g., downloads) the \( M_i \)’s envelope \( (E_i) \), and uses it to insert his message \( (Mess_j) \) by using \( MI_j \). When \( M_j \) tries to insert a message, \( M_i \)’s key \( (Key_i) \) is transferred to \( MI_j \) automatically in an invisible manner, and is actually used. \( M_i \) can send \( E_i(Mess_j) \) directly, or ask someone else to send it to \( M_i \) as an e-mail attachment.

\( M_j \) can be anonymous because no sender’s information is seen on \( E_i(Mess_j) \). \( Mess_j \) is hidden, and only \( M_i \) can see it by opening the envelope. It is not a problem for \( M_j \) and \( M_i \) to be acquainted or not because \( M_j \) can get anyone’s envelope from an open site. ACMS is a very easy-to-use system because users are not bothered by any key handling, as the key is always operated automatically. As ACMS doesn’t need any authorization bureau, this system can be very low cost. All these features overcome the drawbacks of an encrypted mailing system.
system (cf. Section 2).

4. Anti reverse-engineering strategy

This ACMS is secure only if the key is not stolen (i.e., not disclosed by anyone). The location of the hidden key in the envelope is kept secret by the system developer, but some people may be interested in reverse-engineering the execution programs (EP and MI). General techniques to make a program difficult to reverse-engineer include the following.

(1) To make the structure of the program a very tangled one, or a “spaghetti program.”
(2) To make it “manually untraceable” by way of inserting very complicated subprograms.
(3) To set a lot of branches in the program-flow according to non-algorithmic conditions.

One practical method for (3) is to use “time intervals” between two (or more) instructions along a program-flow. In a normal running mode of the computer, the flow branches into a correct direction, but in a reverse-engineering mode the computer speed may be shifted down for tracing and the flow strays into incorrect directions. This confuses the reverse-engineers completely. It is difficult to make a theoretical analysis of how secure the system is, but it is practically safe if the programs are made very carefully.

5. Future schedule

Our project is still at a prototype-implementation stage. The basic system design has already been finalized. We will test and investigate the actual usage of the system within a software company of 700 employees in the Tokyo area. We may also test this system for “inter-organization” use by introducing a “user-group identifying capability” in the system. The final goal of the project is to develop a “world-wide use” version as soon as possible.

References