A Model of E-Correspondence with Error Correction

Abhishek Shukla
Deptt. of M.C.A.
R.K.G.I. T.,Gzb., U.P.(India) (Research Scholar Singhania University, Raj. INDIA)

Meenu Sahni
Department of Mathematics B.I.T.S Gzb.,U.P.(India) (Research Scholar Mewar University, Raj. INDIA)

Deo Brat Ojha
Deptt. of Mathematics,
R.K.G.I. T., Gzb., U.P.(India),

ABSTRACT

In this paper, we presented a model of e-correspondence with error correction for Internet communication. It is the model of a real-life secure e-correspondence system for any organization. In this model a sender can send a secret message even to a unacquainted person in an anonymous way. The users of this model are assumed to be may or may not be the members of a closed organization.

Keywords

Steganography ; e-correspondence system, Bilinear pairing, Error Correction Code.

1. INTRODUCTION

1.1 The Main Text

Human beings have long hoped to have a technique to communicate with a distant partner anonymously but later on distinctive and must be secure. 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 [6], [7]. The most important feature of this steganography is that it has a very large data hiding capacity [2], [5]. It normally embeds 50% or more of a container image file with information without increasing its size. 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 [8] 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 e-correspondence with error correction system for internet communication. 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, gives the preliminaries. section 4 presents model for our proposed MECC scheme, section 5 concern with components of the model, section 6 provides the process of working.

2. PROBLEMS OF AN ENCRYPTED MAILING SYSTEM

There are two types of cryptography scheme: Symmetric key schemes and asymmetric key schemes.

In a symmetric system a message sender and receiver use a same encryption/decryption key. In this scheme, 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. Furthermore, 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.

3. A MODEL OF E-CORRESPONDENCE WITH ERROR CORRECTION

The authors started to develop a secure and easy-to-use e-correspondence. We do not intend to develop a new “message reader-and-sender” or “message composer”, but we are developing three system components that make a model of e-correspondence with error correction (MECC). 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 may or may not be anonymous, as depends upon their wish.

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 unaccustomed person.

4.It is easy to use for both sender and receiver.

3.1 Customization of an MECC

3.1.1 Bilinear Pairings

Customization of an MECC for a member $(M_{MECC\ I})$ takes place in the following way. $(M_{MECC\ I})$ first decides a key $(Key_{MECC\ I})$ when he installs the MECC onto his computer. Then he types in his name $(Name_{MECC\ I})$ and e-mail address $(\text{Email adr}_{MECC\ I})$. $(Key_{MECC\ I})$ is secretly hidden (according to a steganographic procedure in his envelope $(E_{MECC\ I})$ This $(Key_{MECC\ I})$ is eventually transferred to a message sender's $(MI_{MECC\ II})$ in an invisible way. $(Name_{MECC\ I})$ and $(Name\ adr_{\ MECC\ I})$ are printed out on the envelope surface when $(M_{MECC\ I})$ produces $(E_{MECC\ I})$ by using $(EP_{MECC\ I})$. $(Key_{MECC\ I})$ is also set to $(EO_{MECC\ I})$ at the time of installation. $(Name_{MECC\ I})$ and $(\text{Email adr}_{MECC\ I})$ are also inserted (actually, embedded) automatically by $(MI_{MECC\ I})$ any time $(M_{MECC\ I})$ inserts his message $(Mess._{MECC\ I})$ in another member's envelope $(E_{MECC\ I})$. The embedded $(Name_{MECC\ I})$ and $(\text{Email adr}_{MECC\ I})$ are extracted by a message receiver $(M_{MECC\ II})$ by $(EO_{MECC\ II})$.

3.2 Error Correction Code

A metric space is a set C with a distance function $dist : C \times C \to R^{+} = [0,\infty),$ which obeys the usual properties (symmetric, triangle inequalities, zero distance between equal points).

3.2.1 Definition

Let $C\{0,1\}^{n}$ be a code set which consists of a set of code words c_i of length n. The distance metric between any two code words c_i and c_j in C is defined by $dist(c_i, c_j) = \sum_{r=1}^{n} \left| c_{ir} - c_{jr} \right|, c_i, c_j \in C$.

This is known as Hamming distance [9].

3.2.2 Definition

An error correction function f for a code C is defined as $f(c_j) = \{c_j \mid dist(c_i, c_j) \text{ is the minimum, over } C \setminus \{c_i\}\}.$ Here, $c_j = f(c_i)$ is called the nearest neighbor of c_i .

3.2.3. Definition

The measurement of nearness between two code words c and c' is defined by $\text{nearness}(c, c') = \text{dist}(c, c')/n,$

it is obvious that $0 \le \text{nearness}(c, c') \le 1.$

3.2.4. Definition

The fuzzy membership function for a codeword c' to be equal to a given c is defined as

$$FUZZ(c') = \begin{cases} 0 & if\ nearness(c, c') = z \le z_0 < 1 \\ z & otherwise \end{cases}$$

Let q be a large prime with l bit length. Let G_1 be a cyclic additive group generated by P , whose order is q. Let G_2 be a cyclic multiplicative group of the same order q. A bilinear pairing is a map $\hat{e} : G_1 \times G_1 \to G_2$ with the following properties:

(a)Bilinear: For any $aP, bP \in G_1, \hat{e}(aP, bP) = \hat{e}(P, P)^{ab}$,

where $a, b \in Z_q^{*}$; for any

$P, Q, R \in G_1, \hat{e}(P + Q, R) = \hat{e}(P, R).\hat{e}(P, R)$,

$\hat{e}(P, Q + R) = \hat{e}(P, Q).\hat{e}(P, R)$;

(b) Non-degenerate: Existing $P, Q \in G_1$ such that at $\hat{e}(P, Q) \ne 1$

(c) Co computable: There is an efficient algorithm to compute $\hat{e}(P, Q)$ for all $P, Q \in G_1$.

3.2.5 Gap Diffie-Hellman (GDH) Group

(a) Computational Diffie-Hellman problem (CDHP): Given $aP, bP \in G_1$. For $a, b \in Z_q^{*}$, to compute $abP(ab)$, Decisional Diffie-Hellman problem (DDHP): Given $P, aP, bP, cP \in G_1$ for $a, b, c \in Z_q^{*}$, to decide whether $c = ab \bmod q$, if so, (P, aP, bP, cP) is called a valid Diffie-Hellman quaternion.

3.2.6 Definition

We call G_1 a GDH group if DDHP can be solved in probabilistic polynomial time (PPT) but there is no PPT algorithm to solve CDHP on G1with non-negligible probability. Assume there is a bilinear map $\hat{e}$, then (P, aP, bP, cP) is a valid Diffie-Hellman quaternion $\Leftrightarrow \hat{e}(aP, bP) = \hat{e}(P, cP)$.

3.2.7 Definition

The MECC scheme involves a signer , a limited verifier (the designated recipient of the signature) and a certain third party (usually a Judge). It consists of six algorithms and a specific protocol, is denoted by MECC ={Setup, Private Key Extraction, Signing, Limited, Verifier, Verification, Confirmation Protocol, Conversion, Public Verification}.

4. OUR PROPOSED MECC SCHEME

Our MECC scheme involves a signer A, n limited verifier $B_1, B_2, \dots, B_n$, a Judge J and a PKG.

The group G_1, G_2 , are defined as equivalent to that in section 2. Define three cryptographic hash functions $H_0 : \{0,1\}^* \rightarrow G_1, H_1 : \{0,1\}^* \rightarrow Z_q^*, H_2 : G_2 \rightarrow G_1$. The scheme is described as follows:

(a) Setup: PKG picks a random number $s \in_R Z_q^*$ and sets $P_{pub} = sP$ as the public key. It publishes system parameters $cP = (G_1, G_2, q, P, \hat{e}, H_0, H_1, H_2, P_{pub})$ and keeps s secretly as the master secret key.

(b) Private Key Extraction: User $U(\in \{A, B_1, B_2, ..., B_n, J\})$ submits its identity ID_u to PKG. PKG computes public key $Q_u = H_0(ID_u)$ and privacy key $D_u = s.Q_u$ and sends D_u to $U(\in \{A, B_1, B_2, ..., B_n, J\})$ respectively via a secure channel.

(c) Signing: We use the variant [12] of the ID-based signature scheme given by Yi [10]. Given a message $m \in \{0,1\}^*$ signer A picks a random number $r \in_R Z_q^*$, computes $U = rP, h = H_1(m,U), V = rP_{pub} + hD_A$. Then A designates limited verifier to $B_1, B_2, ..., B_n$ by following computation: $T_1 = H_2(\hat{e}(Q_{B_1}, V)), ..., T_n = H_2(\hat{e}(Q_{B_n}, V))$ and $S_1 = T_1 \oplus V, ..., S_n = T_n \oplus V$ the resulting MECC is $C, m, U, S_1, ...S_n, XOR$

(d) Limited Verifier Verification: Given MVCES $C, m, U, S_1, ...S_n, XOR$, the limited verifier $B_i (i \in \{1, 2, ..., n\})$ compute $t(c), XOR, t(m), t(U), t(S_1), t(S_2), ..., t(S_n)$,

$$h = H_1(m,U), T_i = H_2(\hat{e}(D_{B_i}, U + hQ_A)), C, m, U, S_1, ..., S_n, XOR$$

and B_i checks whether , $\hat{e}(P,V) = \hat{e}(P_{pub}, U + hQ_A)$ holds. The signature is valid if and only if the equation holds, $c' = t(m) \oplus t(U) \oplus t(S_1) \oplus t(S_2) ... \oplus t(S_n)$.

Customization of an MECC for a member $MECC_{first}$ takes place in the following way. $MECC_{first}$ and $MECC_{second}$ complete up to the 4(d) step. Then $MECC_{first}$ types in his name ($NAME_{first}$) and e-mail address ($e-mail_{first}$). Key is secretly hidden (according to a steganographic method or some other method) in $MECC_{first}$ envelope (E_{first}). This Key is eventually transferred to a message sender's MI_{second} in an invisible way. $NAME_{first}$ and $e-mail_{first}$ are printed out on the envelope surface when $MECC_{first}$ produces E_{first} by using EP_{first}. Key is also set to EO_{first} for the initialization. $NAME_{first}$ and $e-mail_{first}$ are also inserted (actually, embedded) automatically by MI_{first} any time $MECC_{first}$ inserts message ($MESSAGE_{first}$) in envelope (E_{second}) The embedded $NAME_{first}$ and $e-mail_{first}$ are extracted by a message receiver ($MECC_{second}$) by EO_{second} .

5. COMPONENTS OF THE E-CORRESPONDENCE

MECC is a steganography application .It makes use of the inseparability of the external and internal data. The E-Correspondence can be implemented differently according to different programmers or different specifications.

MECC consists of the three following components.

1. First to agree with step 4.
2. Envelope Producer (EP)
3. Message Inserter (MI)
4. Envelope Opener (EO)

In this scheme we have two communicating parties first and second. We denote first's MECC as $MECC_{first}$ So, it is described as $MECC_{first} = EP_{first}.MI_{first}.EO_{first}.EP_{first}$ is a component that produces MI_{first} 's envelope E_{first}. E_{first} is the envelope (actually, an image file) which is used by all, when they send a secret message to $MVCES_{\mathbf{first}}$. EO_{first} is produced from an original image EO. $MECC_{first}$ can select it according to his preference. E_{first} has both the name and e-mail address of $MECC_{first}$ on the envelope surface (actually, the name and address are "printed" on image E_{first}). It will be placed at downloadable site, so that anyone can get it freely and use it any time or someone may ask $MECC_{first}$ to send it directly to him/her. MI_{first} is the component to insert (i.e., embedded according to the steganographic scheme) $MECC_{first}$'s message into another member's (e.g., $MECC_{second}$'s envelope (E_{second}) when $MECC_{first}$ is sending a secret message ($MESSAGE_{first}$) to $MECC_{second}$. One important function of MI_{first} is that it detects a key (KEY_{second}) that has been hidden in the envelope (E_{second}), and uses it when inserting a message ($MESSAGE_{first}$) in $MESSAGE_{first}$. EO_{first} is a component that opens (extracts) E_{first} 's "message inserted" envelop E_{first} ($MESSAGE_{second}$) which $MECC_{first}$ received from someone as an e-mail attachment. The sender ($MECC_{second}$ ') of the secret message ($MESSAGE_{second}$) is not known until $MECC_{first}$ opens the envelope by using EO_{first} .

6. WORKING

When some member $(M_{MECC\ II})$ wants to send a secret message $(MESS_{MECC\ II})$ to another member $(M_{MECC\ I})$, whether they are acquainted or not, $(M_{MECC\ II})$ gets (e.g., downloads) the $(M_{MECC\ I})$'s envelope $(E_{MECC\ I})$, and uses it to insert his message $(Mess._{MECC\ II})$ by using $(MI_{MECC\ II})$. When $(M_{MECC\ II})$ tries to insert a message, $(M_{MECC\ I})$'s key $(Key_{MECC\ I})$ is transferred to $(MI_{MECC\ II})$ automatically in an invisible manner, and is actually used. $(M_{MECC\ I})$ can send $(E_{MECC\ I}(M_{MECC\ II}))$ directly, or ask someone else to send, it to $(M_{MECC\ I})$ as an e-mail attachment. $(M_{MECC\ II})$ can be anonymous because no sender's information is seen on $(E_{MECC\ I}(M_{MECC\ II}))$. $(Mess._{MECC\ I})$ is hidden, and only $(M_{MECC\ I})$ can see it by opening the envelope. It is not a problem for $(M_{MECC\ II})$ and $(M_{MECC\ I})$ to be acquainted or not because $(M_{MECC\ II})$ can get anyone's envelope from an open site.

Due to the stymieing channel, there is a chance for the occurrence of error. Let $(M_{MECC\ I})$ get message $(t(c)_{MECC\ II})$ instead of $(c_{MECC\ II})$, where t denote the transmission error. Now, $(M_{MECC\ I})$ apply error correction function on $(t(c)_{MECC\ II})$ and gets $(t(c)_{EEPQC\ \ II})'$. $(M_{MECC\ I})$ check that $dist\{(t(c)_{MECC\ II}), t(c)_{MECC\ II})'\} > 0$, $(M_{MECC\ I})$ will realize that there is an error occur during the transmission. $(M_{MECC\ I})$ apply the error correction function f to $(c_{MECC\ II})' : f((c_{MECC\ II})'$.

Then $(M_{MEEC\ I})$ will compute nearness

$$(t(c_{MECC\ II}), f((c_{MECC\ II})')) = \frac{dist\{t(c_{MECC\ II}), f((c_{MECC\ II})')\}}{n}..$$

$$FUZZ((c_{MECC\ II})') = \left\{\begin{matrix} 0 & if\ nearness(c_{MECC\ II}),(c_{MECC\ II}\ \ )') = z \le z_0 < 1 \\ z & otherwise \end{matrix}\right\}$$

When some member ($MECC_{second}$) wants to send a secret message ($MESSAGE_{second}$) to another member ($MECC_{first}$). and $MECC_{second}$ complete step 4. then $MECC_{second}$ gets (e.g., downloads) the $MECC_{first}$'s envelope (E_{first}), and uses it to insert his message ($MESSAGE_{second}$) by using MI_{second}. When $MECC_{second}$ tries to insert a message, $MECC_{first}$'s key is transferred to MI_{second} automatically in an invisible manner, and is actually used. $MECC_{first}$ can send $E_{first}MESSAGE_{second}$ directly, or ask someone else to send, it to $MECC_{first}$ as an e-mail attachment. $MECC_{second}$ can be anonymous because no sender's information is seen on $E_{first}MESSAGE_{second}$, $MESSAGE_{second}$ is hidden, and only $MECC_{first}$ can see it by opening the envelope. It is not a problem for $MECC_{second}$ and $MECC_{first}$ to be acquainted or not but step 4 is required for authenticity.

REFERENCES

[1] A. Menezes, M. Qu, and S. Vanstone, "Key agree-ment and the need for authentication," in Proceed-ings of PKS'95, pp. 34-42, 1995.

[2] M. Niimi, H. Noda and E. Kawaguchi :"An image embedding in image by a complexity based region segmentation method", Proceedings of International Conf. on Image Processing'97, Vol.3, pp.74-77, Santa Barbara, Oct., 1997.

[3] E. Kawaguchi and R. O. Eason :"Principle and applications of BPCS- Steganography", Proceedings of SPIE: Multimeda Systems and Applications, Vol.3528, pp.464-463, 1998.

[4] L. Law, A. Menezes, M. Qu, J. Solinas, and S. Van- stone, An Efficient Protocol for Authenticated Key Agreement, Technical Report CORR98-05, Department of CO,University of Waterloo, 1998.

[5] E. Kawaguchi,et al: "A concept of digital picture envelope for Internet communication"in Information modeling and knowledge bases X,IOS Press, pp.343-349, 1999.

[6] Stefan Katzenbeisser and Fabien A.P. Petitcolas (eds) :"Information hiding techniques for steganography and digital watermarking", Artech House, 2000.

[7] Neil F. Johnson, Zoran Duric and Sushil Jajodia :"Information Hiding", Kluwer Academic Publishers, 2001.

[8] K. H. Ko, D. H. Choi, M. S. Cho, and J. W. Lee, "New signature scheme using conjugacy problem."(http://eprint.iacr.org/2002/168).

[9] L. Law, A. Menezes, M. Qu, J. Solinas, and S. Van-stone, "An efficient protocol for authenticated key agreement," Design, Codes and Cryptography, vol. 28, no. 2, pp. 119-134, 2003.

[10] Eiji Kawaguchi, Hideki Noda, Michiharu Niimi and Richard O. Eason, A Model of Anonymous Covert Mailing System Using Steganographic Scheme, Information modelling and knowledge bases X,IOS Press, pp.81-85,2003.

[11] X.Yi, An Identity-Based Signature Scheme From the Weil Pairing,IEEE communications letters 7(2),76-78, 2003.

[12] URL http://www.know.comp.kyutech.ac.jp/BPCSe/Dpenv-e/DPENVe- pro_ down. html.

[13] X.Cheng, L.Guo, X.Wang,An Identity-based Mediated Signature Scheme from Bilinear Pairing, International Journal of Network Security,2(1):29-33, 2006. http://isrc.nchu.edu.tw/ijns.

[14] Xiaofeng Wang, Liang Cao, Shangping Wang,Yaling Zhang, ID-Based Convertible Limited (Multi-)Verifier Signature Scheme,2008 International Conference on Computer Science and Software Engineering.774-777.