ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
Volume 1 Issue 2 September 2011

E-COMMUNICATION TECHNIQUE FOR THE ENVIRONMENT CONTAINING TRANSMISSION ERROR

Meenu Sahni
(Research Scholar Mewar University, Chittorgarh, Rajsthan).
Bhagwati Institute of Technology & Science
U.P.Technical University
Ghaziabad,U.P.(INDIA)

Abhishek Shukla
(Research Scholar Singhania University, Jhunjhunu, Rajsthan).
R.K.G.Institute Of Tehchnology
U.P.Technical University
Ghaziabad,U.P.(INDIA)

Deo Brat Ojha
R.K.G.Institute Of Tehchnology
U.P.Technical University
Ghaziabad,U.P.(INDIA)

Abstract. In this paper, we show E-Communication technique for the environment containing Transmission Error. The main goal of steganography is covert communication. We propose new E-communication technique for security and if any error occurred during the transmission due to teeming channel, it can also be determine and encountered by fuzzy error correction code.

1 Introduction

In wireless communications the channel can be modelled by calculating the reflection off every object in the environment. A sequence of random numbers might also be added into stimulate external interference and/or electronic noise in the receiver.
Steganography is related to hide messages in a cover signal so that they can be retrieved at the receivers end with the help of secret keys. Privacy
Is the main concern by steganography and it ensures the private messages will not be disclosed to illegal users. About steganography [1], [2] and its data hiding capacity [3], [4] ensures that even if the message is intercepted on the network, no one can read it unless either has secret key or legal receiver. Another application pays attention to the nature of steganography whereby the

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
Volume 1 Issue 2 September 2011

external data (e.g. visible image data) and the internal data (any hidden information) cannot be separated by any means. The term is known as "inseparability" of the two forms of data [5], [6], [8], [9], [10], [11], [12].

This paper contains three sections : Section 2 will make a short discussion on the problems of an encrypted mailing system section 3 describes the scheme of the e-mailing system in a braid group using steganographic scheme.

2 Preliminaries

2.1 Braid Group

Emil Artin [7] in 1925 defined Bn, the braid group of index n, using following generators and relations: Consider the generators $\sigma_1, \sigma_2, \ldots\ldots \sigma_n,$ where σ_i represents the braid in which the $(i+1)^{st}$ string crosses over the ith string while all other strings remain uncrossed. The defining relations are

1. $\sigma_i\sigma_j = \sigma_j\sigma_i$ for $|i-j| \geq 2$,

2. $\sigma_i\sigma_j\sigma_i = \sigma_j\sigma_i\sigma_j$ for $|i-j| = 1$

An n-braid has the following geometric interpretation: It is a set of disjoint n-strands all of which are attached to two horizontal bars at the top and at the bottom such that each strands always heads downward as one walks along the strand from the top to the bottom. In this geometric interpretation, each generator σ_i represents the process of swapping the i^{th} strand with the next one (with i^{th} strand going under the $(i+1)^{th}$ one). Two braids are equivalent if one can be deformed to the other continuously in the set of braids. Bn is the set of all equivalence classes of geometric n-braids with a natural group structure. The multiplication ab of two braids a and b is the braid obtained by positioning a on the top of b. The identity e is the braid consisting of n straight vertical strands and the inverse of a is the reflection of a with respect to a horizontal line. So σ^{-1} can be obtained from σ by switching the over-strand and understrand.

$\Delta = (\sigma_1, \sigma_2 \ldots\ldots \sigma_{n-1})(\sigma_1, \sigma_2 \ldots\ldots \sigma_{n-2}) \ldots\ldots (\sigma_1, \sigma_2)(\sigma_1)$ is called the fundamental braid.

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
Volume 1 Issue 2 September 2011

We describe some mathematically hard problems in braid groups. We say that x and y are conjugate if there is an element a such that $y = axa^{-1}$. For $m < n; B_m$ can be considered as a subgroup of Bn generated by σ_1, σ_2 ……. σ_{m-1}.

2.2 Error Correction Code

A metric space is a set C with a detection function dist : C × C → R+ = [0, ∞), which obeys the usual properties 9symmetirc, triangle inequalities, zero distance between equal points) [13], [14].

Definition : Let $C \in (0,1)$ be a code set which consists of a set 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

$$dist(c_i, c_j) = \sum_{r=1}^{n} \left| c_{ir} - c_{jr} \right| \forall c_i, c_j \in C$$

This is known as Hamming distance [15].

Definition : An error correction function f for a code C is defined as

$$f(c_i) = \{\frac{c_j}{dist(c_i, c_j)} = \min C - \{c_i\}\}$$

Here, $c_i = f(c_i)$ is called the nearest neighbour of c_i [13].

Definition : The measurement of nearness between two code words c and c' is defined by $nearness(c, c') = dist(c, c')/n$, it is obvious that $0 \le nearness(c, c') \le 1$ [15].

Definition : The fuzzy membership function for a code word c' to be equal to a given c is defined as [15] –

FUZZ (c')=0 if $nearness(c, c') = z \le z_0 < 1$

= z otherwise.

3 Problems occurred in Encrypted Mailing System

Cryptography scheme are of two types : One is symmetric key schemes and Second one is 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

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
Volume 1 Issue 2 September 2011

negotiate on what key 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 is open to the public and it is used for message encoding when a sender is sending a message to the key owner.
Now, if communication channel is too much busy, noisy or teeming then may or may not be an error occurred. If any error is generated due to noisiness, we should detect and encountered for safe and secure communication either our users are anonymous or within an organization.

4 A model of E-Communication Technique for the Environment Containing Transmission Error(ECTECT)

ECTECT is a steganography application . It makes use of the inseparability of the external and internal data. The system can be implemented differently according to the different programmers or different specifications. Different ECTECT's are incompatible in operation with others.
An ECTECT consists of the three following components :
1. Envelope Producer (EP)
2. Message Inserter (MI)
3. Envelope Opener (EO)
In this scheme, we have two communicating parties first and second. We denote first ECTECT as $ECTECT_I$. So, it is described as $ECTECT_I = EP_I, M_{II}, EO_I$.

EPI is a component that produces MII's envelope EI. EI is the envelope (actually, an image file) which is used by all, when they send a secret message to $ECTECT_I$. EO_I is produced from an original image EO. $ECTECT_I$ can select it according to his preference. EI has both the name and e-mail address of $ECTECT_I$ on the envelope surface (actually, the name and address are "printed" on image E_I). It will be placed at downloadable site, so that anyone can get it freely and use it anytime. Or someone may ask $ECTECT_I$ to send it directly to him / her. M_{II} is the component to insert (i.e. embed according to the steganographic scheme) $ECTECT_I$'s message into another member's (e.g. $EBSS_{II}$)'s envelope (E_{II}) when $ECTECT_I$ is sending a secret message (M_I) to $ECTECT_I$. One important function of M_{II} is that it detects a key (K_{II}) that has been hidden in the envelope (E_{II}), and uses it when inserting a message (M_I) in E_{II}. EO_I is the component that opens (extracts) E_I's "message inserted" envelope E_I (M_{II}) which $ECTECT_I$ received from someone as an e-mail attachment. The sender ($EBSS_{II}$) of the secret message (M_{II}) is not known until $ECTECT_I$ opens the envelope by using EO_I.

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
Volume 1 Issue 2 September 2011

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

4.1 Customization of an ECTECT

The Conjugacy Search Problem (CSP) asks to find a in Braid Group B_n satisfying $y = axa^{-1}$ for some a in B_n, CSP asks to find at least one particular element a like that. It is considered infeasible to solve CSP for sufficiently large braids. The probability for a random conjugate of x to be equal to y is negligible. For B_n, a pair $(x, y) \in B_n \det\times B_n$ is said to be CSP-hard if $x \square y$ and CSP is infeasible for the instance (x, y) .If (x, y) is CSP-hard, so is clearly (y, x) .

In this section we describe A Model of E-Communication Technique for the Environment containing Transmission Error (ECTECT) between two entities sender and receiver, and consider its security. For this scheme, the initial setup known to both sender and receiver is:

We denote by

x Sufficiently complicated x -braid;

$a \in LB_n$: sender's long term private key;

$X_{sender} = axa^{-1}$: sender's long term public key;

$b \in UB_n$: receiver's long term private key;

$X_{receiver} = bxb^{-1}$: receiver's long term public key.

Following the above mentioned notations, we describe the ECTECT below. The protocol works in the following steps.

Sender Receiver

$Y_{sender} = cxc^{-1}$

$\rightarrow$

$K_{receiver} = bX_{sender}b^{-1}$

ISSN (Online) 2249 - 054 X

International Journal of Computing and Corporate Research

Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists

Volume 1 Issue 2 September 2011

$$Y_{recceiver} = K_{receiver} dY_{sender} d^{-1} K^{-1}_{receiver}$$

←

1. Sender choose $c \in LB_n$, computes $Y_{sender} = cxc^{-1}$. If $Y_{sender} = I$ (Identity braid), terminates the protocol run with failure. Otherwise sender sends it to receiver.

2. Upon receiving Y_{sender} Y_{sender} , Receiver choose $d \in UB_n$, computes
$K_{receiver} = bX_{sender} b^{-1}$, and
$Y_{recceiver} = K_{receiver} dY_{sender} d^{-1} K^{-1}_{receiver}$.

3. If $K_{receiver}$ or $Y_{recceiver} = I$, receiver terminates the protocol run with failure. Otherwise receiver sends it to sender.

4. Upon receiving $Y_{recceiver}$, sender computes
$K_{sender} (= K_{receiver}) = aX_{receiver} a^{-1}$ and the shared key $KE_{receiver} = cK^{-1}_{sender} Y_{receiver} K_{sender} c^{-1}$.

5. Receiver also computes the shared key $KEY_{receiver} = dY_{sender} d^{-1}$.

6. In each step 4 and 5, if KEY_{sender} or $KEY_{receiver}$ is I, then the protocol run is terminated with failure.

7. After regular protocol running, Sender and Receiver share the secret $K = KEY_{sender} = KEY_{receiver}$.

Customization of an ECTECT for a member $ECTECT_I$ takes place in the following way. $ECTECT_I$ and $ECTECT_{II}$ first agree to generate a key ($K = KEY_{sender} = KEY_{receiver}$) here sender is $ECTECT_{II}$ and receiver $ECTECT_I$. Then $ECTECT_I$ types in his name ($NAMEECTECT_I$) and e-mail address ($E\text{-}MAILECTEC_I$). Key is secretly hidden (according to a steganographic method) in $ECTECT_I$ envelope ($EECTECT_I$). This Key is eventually transferred to a message sender's $MIECTECT_I$ in an invisible way. $NAMEECTECT_I$ and $E\text{-}MAILECTEC_I$ are printed out on the envelope surface when $ECTECT_I$ produces $EECTECT_I$ by using $EPECTECT_I$. Key is also set to $EOECTECT_I$ for the initialization. $NAMEECTECT_I$ and $E\text{-}MAILECTECT_I$ are

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
Volume 1 Issue 2 September 2011

also inserted (actually, embedded) automatically by $MIECTECT_I$ any time $ECTECT_I$ inserts message ($MESSAGEECTECT_I$) in envelope ($EECTECT_I$). The embedded $NAMEECTECT_I$ and $E\text{-}MAILECTECT_I$ are extracted by a message receiver ($ECTECT_{II}$) by $EOECTECT_{II}$.

5 HOW IT WORKS

When some member ($ECTECT_{II}$) wants to send a secret message ($MESSAGEECTECT_{II}$) to another member ($ECTECT_I$),whether they are acquainted or not, $ECTECT_{II}$ gets (e.g., downloads) the $ECTECT_I$'s envelope ($EECTECT_I$), and uses it to insert his message ($MESSAGEECTECT_{II}$) by using $MIECTECT_{II}$. When $ECTECT_{II}$ tries to insert a message, $ECTECT_I$'s key is transferred to $MIECTECT_{II}$ automatically in an invisible manner, and is actually used. $ECTECT_I$ can send $EECTECT_I$ $MESSAGEECTECT_{II}$ in encrypted form using same key directly, or ask someone else to send, it to $ECTECT_I$ as an e-mail attachment.

$ECTECT_{II}$ can be anonymous because no sender's information is seen on $EECTECT_I$ $MESSAGEECTECT_{II}$. $MESSAGEECTECT_{II}$ is hidden, and only $ECTECT_I$ can see it by opening the envelope. It is not a problem for $ECTECT_{II}$ and $ECTECT_I$ to be acquainted or not because $ECTECT_{II}$ can get anyone's envelope from downloadable site. ECTECT is a very easy-to-use system because users are not bothered by any key handling.

Let $ECTECT_I$ get message ($t(MESSAGEECTECT_{II})$) instead of ($MESSAGEECTECT_{II}$), where t denote the transmission error. Now, $ECTECT_I$ apply error correction function on ($t(MESSAGEECTECT_{II})$) and gets ($t\ (MESSAGEECTECT_{II})'$). $ECTECT_I$ check out

$$dist\ (t(MESSAGEECTECT_{II})), (MESSAGEECTECT_{II})') > 0,$$

$ECTECT_I$ will realize that there is an error occur during the transmission. $ECTECT_I$ apply the error correction function f to $t(MESSAGEECTECT_{II})'$: $f(t(MESSAGEECTECT_{II}))$.
Then ($MESSAGEECTECT_I$) will compute nearness
$(t(MESSAGEECTECT_{II})), t(MESSAGEECTECT_{II})') = dist\ (t(MESSAGEECTECT_{II}))$

$$f(t\ (MESSAGEECTECT_{II})') / n$$

$$FUZZ\ (c') = 0 \text{ if nearness, } t(MESSAGEECTECT_{II})), (t(MESSAGEECTECT_{II})') = z \leq z_o < 1$$

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
Volume 1 Issue 2 September 2011

= z otherwise.

6 Conclusion

ECTECT is a very easy – to – use system because users are not bothered by any key handling, as the key is always operated automatically. As ECTECT doesn't need any authorization bureau, this system can be very low cost. All these features overcome the drawbacks of an encrypted mailing system. Our approach provides the method to remove the error due to stymieing channel through fuzzy approach.

References

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

[2] Neil F. Johnson, Zoran Duric and Sushil Jajodia (2001) "Information Hiding", Kluwer Academic Publishers.

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

[4] E. Kawaguchi and R. O. Eason (1998) "Principle and applications of BPCS-Steganography", Proceedings of SPIE: Multimedia Systems and Applications, Vol.3528, 464-463.

[5]URL:http://www.know.comp.kyutech.ac.jp/BPCSe/Dpenv/DPENVeprodown. html.

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

[7] E. Artin, (1947), "Theory of braids," Annals of Mathematics, vol. 48,101-126.

[8] K.H.KO,S.J.Lee, J.H.Cheon, J.W.Han,J. S. Kang, and C Park, (2000)"New public- key cryptosystem using braid groups," in Advances in Cryptology (Crypto'00),LNCS1880,166-183, Springer-Verlag.

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

ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for Research Scholars, Academicians, Engineers and Scientists
Volume 1 Issue 2 September 2011

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

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

[12] Eiji Kawaguchi, Hideki Noda, Michiharu Niimi and Richard O. Eason, (2003), "A Model of Anonymous bases X", IOS Press, 81-85.

[13] J.P.Pandey, D.B.Ojha, Ajay Sharma, (2009),"Enhance Fuzzy Commitment Scheme: An Approach For Post Quantum Cryptosystem", in Journal of Applied and Theoretical Information Technology, Vol. 9 No. 1, 16-19. V.Pless, (1982),"Introduction to theory of Error Correcting Codes", Wiley , New York.

[14] V.Pless, (1982),"Introduction to theory of Error Correcting Codes", Wiley , New York.

[15] A.A.Al-saggaf, H.S.Acharya,(2007),"A Fuzzy Commitment Scheme", IEEE International Conference on Advances in Computer Vision and Information Technology, 28-30.