Volume 1, No. 4, November 2010

Journal of Global Research in Computer Science

ISSN-2229-371X

RESEARCH PAPER

Available Online at www.jgrcs.info

ERROR LESS E-MESSAGING APPROACH USING DOUBLE- EHDES

Ramveer Singh[1*],Awakash Mishra[2], Akshay Tyagi[3] and Deo Brat Ojha[4]

[*1](Research Scholar Singhania University, Jhunjhunu, Rajsthan)
Department of Information Technology, R. K. G. Institute of Technology, Gzb., U.P.(India)
ramveersingh_rana@yahoo.co.in
[2](Research Scholar Singhania University, Jhunjhunu, Rajsthan)
Department of M.C.A, Raj Kumar Goel Engineering College, Ghaziabad, U.P.,INDIA
awakashmishra@gmail.com
[3](Research Scholar Mewar University, Chittorgarh, Rajasthan))
Gradute School of Business & Administration, Greater Noida, U.P., INDIA
akshaytyagi@airtelmail.in
[4]Deptt. Of mathematics, R. K. G. Institute of Technology, Gzb., U.P.(India),
deobratojha@rediffmail.com

Abstract: In this paper, we are introducing an effective and important approach of e-messaging system for transmission with high security and error free using double EHDES. This approach provides a high level of secure mailing scheme for any organization over the internetto communicate a secret error free e-message between anonymous communicators as well as within an organization.

Keywords: Message, EHDES, Double EHDES, Steganography, Covert Mailing System, Fuzzy Error Correcting Code.

INTRODUCTION

Steganography has a relatively short history; even today ordinary dictionaries do not contain the word "steganography". Books on steganography are still very few [1], [2]. The most important feature of this steganography is that it has a very large data hiding capacity [3], [4]. 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 [5], [6] 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 this current paper, we will show an example of a mixed scheme of steganography and cryptography are Secure E-Messaging Scheme Using Symmetric Key Encryption – Double EHDES with method of error correction, which are an anonymous and covert e-mailing system with complete security [10].

Present paper is as follows. In Section 2, we describes the method of error correction with scheme of double enhanced data encryption standard (D-EHDES).In Section 3 we will show a secure messaging scheme using symmetric key. How we can make it a safe system in Section 4. Finally, section 5 is conclusion.

PRELIMINERIES

The amount of transfer messaging has increased rapidly on the Internet. Cryptography is a branch of applied mathematics that aims to add security in the ciphers of any kind of messages. Cryptography algorithms use encryption keys, which are the elements that turn a general encryption algorithm into a specific method of encryption. The data integrity aims to verify the validity of data contained in a given document. [7]

Double EHDES

Double EHDES is an arrangement or cascading of EHDES and its working just like a EHDES but two times. In Enhanced Data Encryption Standard (EHDES) [8, 9], we breaks block of message and follow these three phases: 1. Key Generation. 2. Encryption.
3. Decryption.

Key Generation

In this phase, EHDES generates the n different keys ($K_{new1,}$ $K_{new2,}$ K_{new3}............... $K_{new\ n}$) to apply a function F on Initial key k and a random number (N_{RNG}), for every block of message (M_1, M_2, M_3 ...M_n).

Encryption on Input Data

Message breaks in 64 Bit n blocks of plain text.

$$\mathbf{M = \{M_1, M_2, M_3,..................,M_n\}}$$

Now, we encrypt our message {M_1, M_2, M_3,..................,M_n} blocks by each new generated key $K_{new1,}$ $K_{new2,}$ K_{new3}...............$K_{new\ n}$.

Decryption on Input Cipher

Decryption is the reverse process of encryption. For decryption, we also used the same key which is used in encryption. On the receiver side, the user also generate the same new key $K_{new\ i}$ for each block of cipher and generate plain text through decryption process of data encryption standard.

Error Correction Code

A metric space is a set C with a distance function dist : $C \times C \rightarrow R^+ = [0, \infty)$, which obeys the usual properties(symmetric, triangle inequalities, zero distance between equal points)[11,12].

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

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

This is known as Hamming distance [13].

Definition: An error correction function f for a code C is defined as $f(c_i) = \{c_j / dist(c_i, c_j) \text{ is the minimum, over } C - \{c_i\}\}$. Here, $c_j = f(c_i)$ is called the nearest neighbor of c_i [11].

Definition: The measurement of nearness between two code words c and c' is defined by $\text{nearness}(c, c') = dist(c, c')/n$, it is obvious that $0 \le \text{nearness}(c, c') \le 1$ [13].

Definition: The fuzzy membership function for a codeword c' to be equal to a given c is defined as[13]

$$FUZZ(c') = 0 \qquad \text{if nearness}(c, c') = z \le z_0 < 1$$
$$= z \qquad \text{otherwise}$$

A MODEL OF PROTECTED COMMUNICATION ACAPCD-E

A Competent Approach for Protected Communication with Double EHDES (ACAPCD-E) is a steganography application program with cryptography. In the following description,$M_{E_{ACAPCD-E^I}}$, denotes a member *of ACAPCD-E 1* , and $M_{E_{ACAPCD-E^2}}$,denotes a member of *ACAPCD-E 2* .

An ACAPCD-E consists of the three following components.

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

We denote$M_{E_{ACAPCD-E^I}}$'s ACAPCD-E as $ACAPCD-E_I$(i.e., customized ACAPCD-E by$M_{E_{ACAPCD-E^I}}$. So, it is described as $M_{E_{ACAPCD-E^I}} = (EP_{E_{ACAPCD-E^I}}, MI_{E_{ACAPCD-E^I}}, EO_{E_{ACAPCD-E^I}})$. $EP_{E_{ACAPCD-E^I}}$ is a component that produces $M_{E_{ACAPCD-E^I}}$'s envelope $(E_{E_{ACAPCD-E^I}})$ $and a f = \sum_{i=1}^{n} i$. $E_{E_{ACAPCD-E^I}}$ is the envelope (actually, an image file) which is used by all other members in the organization when they send a secret message to $M_{E_{ACAPCD-E^I}}$. $(EO_{E_{ACAPCD-E^I}})$ is produced from an original image $(EO\ \ )$. $M_{E_{ACAPCD-E^I}}$ can select it according to his preference. $(E_{E_{ACAPCD-E^I}})$ has both the name and e-mail address of $M_{E_{ACAPCD-E^I}}$on the envelope surface (actually, the name and address are "printed" on image $(E_{E_{ACAPCD-E^I}})$. It will be placed with function f at an open site in the organization so that anyone can get it freely and use it any time. Or someone may ask $M_{E_{ACAPCD-E^I}}$to send it directly to him/her. $(MI_{E_{ACAPCD-E^I}})$is the component to insert (i.e., embed according to the stegnographic scheme) $M_{E_{ACAPCD-E^I}}$'s message into another member's (e.g., $M_{E_{ACAPCD-E^2}}$)'s envelope $(E_{E_{ACAPCD-E^2}})$ when $M_{E_{ACAPCD-E^1}}$is sending a secret message $(Mess._{E_{ACAPCD-E^1}})$ to $(M_{E_{ACAPCD-E^2}})$. One important function of $M_{E_{ACAPCD-E^1}}$ is that it detects a key $(Key_{E_{ACAPCD-E^1}})$ that has been hidden in the envelope$(E_{E_{ACAPCD-E^2}})$, and uses it when inserting a message $(Mess._{E_{ACAPCD-E^1}})$ in $(E_{E_{ACAPCD-E^2}})$. $(EO_{E_{ACAPCD-E^1}})$ is a component that opens (extracts) $(E_{E_{ACAPCD-E^1}})$'s "message inserted" envelope $(E_{E_{ACAPCD-E^1}}(Mess._{E_{ACAPCD-E^2}}))$ which $M_{E_{ACAPCD-E^1}}$received from someone as an e-mail attachment. The sender $(M_{E_{ACAPCD-E^2}})$ of the secret message $(Mess._{E_{ACAPCD-E^2}})$is not known until $M_{E_{ACAPCD-E^1}}$opens the envelope by using$(EO_{E_{ACAPCD-E^1}})$.

CUSTOMIZATION OF AN ACAPCD-E

Customization of an ACAPCD-E for member $(M_{E_{ACAPCD-E^1}})$ takes place in the following way. $(M_{E_{ACAPCD-E^1}})$, first decides a key $(Key_{E_{ACAPCD-E^1}})$ with $f = \sum_{i=1}^{n} i$ where i is a positive integer, when he/she installs the ACAPCD-E onto his computer. Let us suppose $E_{ACAPCD-E}2$ try to communicate at any time t, then he/she picks up a number randomly form i. Now, ACAPCD-E generates$f_t = \sum_{i=1}^{n-1} i$. Let $R = f - f_t$, ACAPCD-E generate a key $(Key_{E_{ACAPCD-E^1}})$ with the help of R using Double EHDES key generation process. Then he types in his name $(Name_{E_{ACAPCD-E^1}})$ and e-mail address $(Emailadr_{E_{ACAPCD-E^1}})$. $(Key_{E_{ACAPCD-E^1}})$ is secretly hidden (according to a steganographic procedure in his envelope

$(E_{E_{ACAPCD-E}1})$.This $(Key_{E_{ACAPCD-E}1})$is eventually transferred to a message sender's $(MI_{E_{ACAPCD-E}2})$ in an invisible way. $(Name_{E_{ACAPCD-E}1})$ and $(Emailadr_{E_{ACAPCD-E}1})$ are printed out on the envelope surface when $(M_{E_{ACAPCD-E}1})$ produces $(E_{E_{ACAPCD-E}1})$ by using $(EP_{E_{ACAPCD-E}1})$. $(Key_{E_{ACAPCD-E}1})$ is also set to $(EO_{E_{ACAPCD-E}1})$, when communicators wish to start the communication. $(Name_{E_{ACAPCD-E}1})$ and $(Emailadr_{E_{ACAPCD-E}1})$are also inserted (actually, embedded) automatically by $(MI_{E_{ACAPCD-E}1})$ any time $(M_{E_{ACAPCD-E}1})$ inserts his message $(Mess._{E_{ACAPCD-E}1})$ in another member's envelope $(E_{E_{ACAPCD-E}2})$. The embedded $(Name_{E_{ACAPCD-E}1})$and $(Emailadr_{E_{ACAPCD-E}1})$are extracted by a message receiver $(M_{E_{ACAPCD-E}2})$by $(EO_{E_{ACAPCD-E}2})$.

How it works

When some member $(M_{E_{ACAPCD-E}2})$ wants to send a secret message $(Mess._{E_{ACAPCD-E}2})$ to another member $(M_{E_{ACAPCD-E}1})$, whether they are acquainted or not, $(M_{E_{ACAPCD-E}2})$ gets (e.g., downloads) the $(M_{E_{ACAPCD-E}1})$'s envelope $(E_{E_{ACAPCD-E}1})$, and uses it to insert his message $(Mess._{E_{ACAPCD-E}2})$ by using $(MI_{E_{ACAPCD-E}2})$. When $(M_{E_{ACAPCD-E}2})$tries to insert a message, $(M_{E_{ACAPCD-E}1})$'s key $(Key_{E_{ACAPCD-E}1})$ is transferred to $(MI_{E_{ACAPCD-E}2})$automatically in an invisible manner, and is actually used. $(M_{SES_{EHDES}I})$ can send $(E_{E_{ACAPCD-E}1}(M_{E_{ACAPCD-E}2}))$directly, or ask someone else to send it to $(M_{E_{ACAPCD-E}1})$ as an e-mail attachment with using encryption process of Double EHDES.$(M_{E_{ACAPCD-E}2})$can be anonymous because no sender's information is seen on$(E_{E_{ACAPCD-E}1}(M_{E_{ACAPCD-E}2}))$. $(Mess._{E_{ACAPCD-E}2})$is hidden, and only $(M_{E_{ACAPCD-E}1})$can see it by opening the envelope. It is not a problem for $(M_{E_{ACAPCD-E}2})$and $(M_{E_{ACAPCD-E}1})$to be acquainted or not because $(M_{E_{ACAPCD-E}2})$can get anyone's envelope from an open site.

Error Correction

Receiver check that $dist(t(c)c') > 0$, he will realize that there is an error occur during the transmission. Receiver apply the error correction function f to $c' : f(c)$.

Then receiver will compute nearness

$$(t(c), f(c')) = dist(t(c)f(c'))/n$$

$$FUZZ(c') = 0 \qquad \text{if nearness}(c,c') = z \le z_0 < 1$$
$$= z \qquad \text{otherwise}$$

STEP	***ENTITY***	***PROCESS***
1.	ACAPCD-E 1	A. Generate an envelope$E_{ACAPCD-E}1$. B. Upload an envelope $E_{ACAPCD-E}1$ and X (set of positive integer) with$f = \sum_{i=1}^{n} i$. C. Name $Name_{ACAPCD-E}1$and Email address $Emailadr_{ACAPCD-E}1$ print on envelope$E_{ACAPCD-E}1$'s surface and key $Key_{ACAPCD-E}1$ is hiding using stegnohraphic function in the envelope$E_{ACAPCD-E}1$.
2.	ACAPCD-E 1	Choose any number i randomly fromX.
3.	Downloadable Site Function	A. Calculate $f_t = \sum_{i=1}^{n-1} i$ and$R = f - f_t$. B. Send R to$ACAPCD - E1$.
4.	Downloadable Site Function	A. Moderate key $Key_{ACAPCD-E}1$ using EHDES key process. B. Update key$Key_{ACAPCD-E}1$.
5.	ACAPCD-E 2	Download envelope$E_{ACAPCD-E}1$.
6.	ACAPCD-E 2	A. Picked out key $Key_{ACAPCD-E}1$ from envelope$E_{ACAPCD-E}1$. B. Insert message $Mess._{ACAPCD-E}$ 2 in the envelope$E_{ACAPCD-E}1$. C. Encrypt the envelope contains message($E_{ACAPCD-E}1$ ($Mess._{ACAPCD-E}$ 2))using Double EHDES with key $Key_{ACAPCD-E}1$.
7.	ACAPCD-E 2	Send envelope contains message($E_{ACAPCD-E}1$ ($Mess._{ACAPCD-E}$ 2)) to$ACAPCD - E1$.
8.	ACAPCD-E 1	A. Receive envelope contains message($E_{ACAPCD-E}1$ ($Mess._{ACAPCD-E}$ 2)). B. Decrypt the envelope contains message($E_{ACAPCD-E}1$ ($Mess._{ACAPCD-E}$ 2))using Double EHDES with key $Key_{ACAPCD-E}1$. C. Separate message$Mess._{ACAPCD-E}$ 2 from the envelope$E_{ACAPCD-E}1$. D. Check fuzzy distance, if

		any error occurred, encountered it. E. Read messageMess.$_{ACAPCD-E}$ 2.

CONCLUSION

ACAPCD-E is a very easy-to-use and error free system because users are not bothered by any key handling, as the key is always operated automatically. As ACAPCD-E doesn't need any authorization bureau, this system can be very low cost. All these features overcome the drawbacks of an encrypted mailing system.

REFERENCES

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

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

[3] 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.

[4] 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.

[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] 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.

[7] Diego F. de Carvalho, Rafael Chies, Andre P. Freire, Luciana A. F. Martimiano and Rudinei Goularte, "Video Steganography for Confidential Documents: Integrity, Privacy and Version Control" , *University of Sao Paulo – ICMC, Sao Carlos, SP, Brazil, State University of Maringa, Computing Department,* Maringa, PR, Brazil.

[8] Ramveer Singh , Awakash Mishra and D.B.Ojha "An Instinctive Approach for Secure Communication – Enhanced Data Encryption Standard (EHDES)" *International journal of computer science and Information technology,* , Vol. 1 (4) , 2010, 264-267.

[9] D.B. Ojha, Ramveer Singh, Ajay Sharma, Awakash Mishra and Swati Garg "An Innovative Approach to Enhance the Security of Data Encryption Scheme*" International Journal of Computer Theory and Engineering*, Vol. 2,No. 3, June, 2010,1793-8201.

[10] G. Lo-varco,W. Puech, and M. Dumas. "Dct-based watermarking method using error correction codes", In ICAPR'03, International Conference on Advances inPattern Recognition, Calcutta, India, pages 347–350, 2003.

[11] J.P.Pandey, D.B.Ojha, Ajay Sharma, "Enhance Fuzzy Commitment Scheme: An Approach For Post Quantum Cryptosystem", in Journal of Applied and Theoretical Information Technology, (pp 16-19) Vol. 9, No. 1, Nov. 2009.

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

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

AUTHORS

Ramveer Singh, Bachelor of Engineering from Dr. B.R. Ambedkaruniversity, Agra (U.P.), INDIA in 2003. Master of Technology from V.M.R.F. Deemed University, Salem (T.N.), INDIA in 2007. PersuingPh.D from Singhania University, Jhunjhunu, Rajsthan, INDIA. The major field of study is Cryptography and network security. He has more than eight year experience in teaching and research as ASSOCIATE PROFESSOR. He is working at Raj Kumar Goel Institute of Technology, Ghaziabad (U.P.), INDIA. The current research area is Cryptography and Network security. Mr. Singh is the member of LMCSI, LMIAENG, LMIACSIT, LMCSTA. He is the author/co-author of more than 17 publications in International/National journals and conferences.

Awakash Mishra, Master of Computer Application from Uttar Pradesh Technical University, Lucknow (U.P.), INDIA in 2007. PersuingPh.D from Singhania University, Jhunjhunu, Rajsthan, INDIA. He has more than four year experience in teaching and research as LECTURER. He is working at Raj Kumar Goel Engineering College, Ghaziabad (U.P.), INDIA. The current research area is Symmetric Key Cryptography.

AkshayTyagi, PersuingPh.D from MewarUniversity, Chittorgarh, Rajsthan, INDIA. He has more than five year experience in teaching and research as LECTURER. He is working at Gradute School of Business & Administration, Greater Noida, U.P., INDIA. The current research area is Cryptography& fuzzy commitment scheme.

Dr. Deo Brat Ojha, Ph.D from Department of Applied Mathematics, Institute of Technology, Banaras Hindu University, Varansi (U.P.), INDIA in 2004. His research field is Optimization Techniques, Functional Analysis & Cryptography. He has more than Six year teaching & more than eight year research experience. He is working as a Professor at Raj Kumar Goel Institute of Technology, Ghaziabad (U.P.), INDIA.Dr. Ojha is the member of Mathematical Society Banaras Hindu University, LMIAENG, LMIACSIT. He is the author/co-author of more than 50 publications in International/National journals and conferences.

