ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 6, June 2015

Providing security to Online Shopping using credit cards through Text Steganography Techniques

Sumathy Kingslin [1], Vidhya Saraswathi. V [2]

Associate Professor, PG and Research Department of Computer Science,
Quaid E Millath Government College for Women, Chennai, India [1]

M.Phil. Research Scholar, PG and Research Department of Computer Science,
Quaid E Millath Government College for Women, Chennai, India [2]

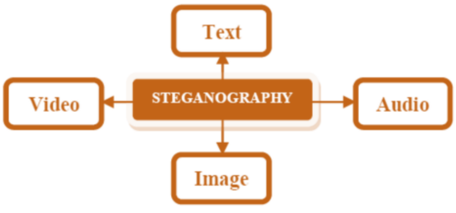
Abstract: Maintaining the security of the secret information has been a great challenge. Communication shared through Internet, draws the attention of third parties, hackers and crackers, which may cause attempts to break and expose the unusual messages. Steganography is a promising region which is used for secured data transmission over any public media. In this paper, a text steganography procedure has been planned with the help of techniques: English based text steganography and word mapping technique applied in the online shopping area using credit card transaction. This would help the user credentials and the transaction page in a safe and secure way for the users. Accuracy as a factor, also captured the encryption time measured before and after encrypting the information.

Keywords: Hackers, Crackers, Encryption, English based text steganography, Word mapping technique.

I. INTRODUCTION

Steganography is derived from a finding by Johannes Trithemus (1462-1516) entitled ‘Steganographia‘, meaning ‚covered writing‘. Steganography is the art and science of hiding a message within a message without drawing any suspicion to others so that the message can only be detected by its intended recipient. Cryptography and Steganography are ways of secure data transfer over the Internet. Cryptography scrambles a message to conceal its contents; steganography conceals the existence of a message [11].

Steganography can be classified into image, text, audio and video steganography depending on the cover media used to embed secret data



Types of Steganography

The advantage of using steganography is to conceal information. The transmission of messages is transparent to any given viewer. Messages can be concealed in different formats that are undetectable and unreadable to the human eye. Steganographic technologies are very important in Internet privacy today. With the use of steganography and encryption, corporations, governments, and law enforcement agencies can communicate secretly [6].

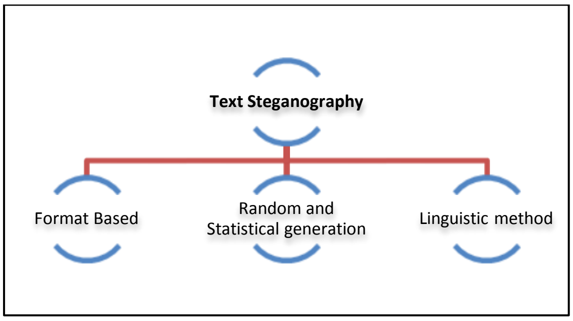
The Basic features of data hiding algorithms are:

- Embedding capacity
- Invisibility
- Robustness
- Un-detectability [12].

TEXT STEGANOGRAPHY

Text steganography involves anything like changing the format of an existing text, changing words within a text, generating random character sequences. Due to deficiency of redundant information which is present in image, audio or a video file, text steganography is believed to be the trickiest technique. In text documents, we can hide information by introducing changes in the structure of the document without making a notable change in the concerned output. Unperceivable changes can be made to an image or an audio file, but, in text files, even an additional letter or punctuation can be marked by a casual reader. Storing text file require less memory and its faster as well as easier communication makes it preferable to other types of steganographic methods [7].

Text steganography can be broadly classified into three types: Format based Random and Statistical generation, Linguistic methods.



DOI 10.17148/IJARCCE.2015.4624

Format based method
Format-based methods usually modify existing text for hiding the steganographic text. Insertion of spaces or non-displayed characters, careful errors tinny throughout the text and resizing of fonts are some of the many format-based methods used in text steganography [10].

As we know, many of the techniques been in text steganography, for implementation of thesis word mapping technique is introduced to provide two way secure data which encrypts a secret message using genetic operator crossover and then embeds the resulting cipher text, taking two bits at a time, in a cover file by inserting blank spaces between words of even or odd length using a certain mapping technique. The embedding positions are saved in another file and transmitted to the receiver along with the stego object [11] [5].

Random and Statistical generation
This avoid comparison with a known plaintext, steganographers often resort to generating their own cover texts. Character sequences method hide the information within character sequences.

Linguistic method
The affluence of electronic documented information available in the world as well as the exertion of serious linguistic analysis makes this an interesting medium for steganographic information hiding [10].

II. RELATED WORKS

The properties of a sentence and the redundant feature characters used in Indian languages, a secret message is hidden into an innocent cover file containing Indian texts. Likewise, the same was implemented for Persia and Arabic languages. Hindi letters and its diacritics and numerical code are used in [1] for hiding message into Hindi text. generating a random sequence of characters or words, specific information can be hidden in sequence [9] but it often results in meaningless words or sentence which can be easily traceable. By altering the features of a text information is hidden in text [1].

The technique used in this paper is a particular code called Vedic numerical code used in deciphering Sanskrit text. For applying the Vedic code to the English alphabet, frequency of letters in English vocabulary [1] is used as the basis of assigning numbers to the letters in the English alphabet. No discrimination is made for assigning coding number to vowels and consonants as compared to [2].

Each letter in the alphabet is assigned a number in the range of 0 to 15 based on the frequency of the letters. Encoding and decoding techniques are applied based on the few steps involved in deriving the output as a secret data. Each letter in the secret message is represented by its ASCII code and obtained ASCII code is expressed in 8 bit binary number. The 8 bit binary number is then divided into two 4 bit parts. Each 4 bit part, representing a number in the range 0 to 15, is then used to choose corresponding suitable letters. The reverse process is applied for decoding the information [3] [4].

EBT technique can be used in any of the areas for secure purpose. To provide another level of protection in the real time usage, other technique is also implemented.

III. PROPOSED WORK

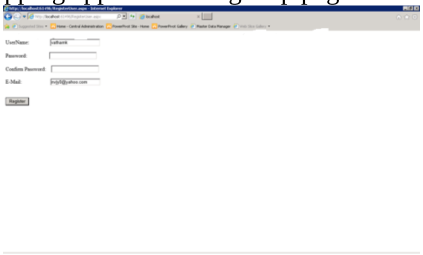
Data loss, hackers, crackers, insecurity, etc. are mostly involved in the web based activities (i.e. banking, shopping, utility payments, etc.). In this paper, safe and secure communication from sender to receiver is protected using the text steganography. Online shopping, which is the vast usage by the customers in today's world has some challenges in the security concerns [9].

To avoid the issues, the user credentials of the customers and the transaction page, i.e. the payment page has been protected through the text steganography techniques. Online shopping using the credit card is the briefly involved data to have the clarity of the information security. An English based text steganography (EBT) technique for the encryption and decryption is used in the shopping environment. The random sentence generator is implemented using the concept of the mnemonic generator. To have another level secure protection, the encrypted data has been done by the word mapping technique.

IV. EXPERIMENT RESULTS

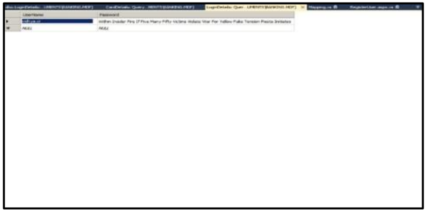
Implementation of online shopping using credit cards in a secured term using text steganography technique resulted in an efficient way.

This technique is used in the user login credentials for online shopping application- Sign Up page:



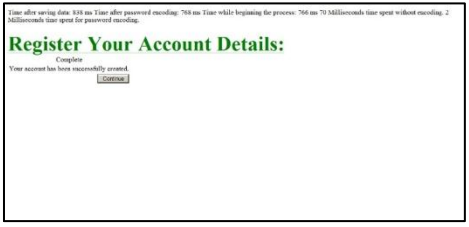
UserName: vathank
Password:
Confirm Password:
E-Mail: rvjy0@yahoo.com

Backend data shown in the signup module after the technique implemented will be in the meaningful sentence:


LoginDetails: Query...(BANKING.MDF)
CardDetails: Query...(BANKING.MDF)
LoginDetails: Quer...(BANKING.MDF)
Mapping.cs
RegisterUser.aspx.cs

	UserName	Password
▶	[illegible]	Within Insider Fire 17 Five Many Fifty Victims Wasabi War For Yellow Fake Tension Fiesta Initiates
*	NULL	NULL

Also, this resulted the time frame taken for before and after encryption technique:



Time after saving data: 838 ms Time after password encoding: 768 ms Time while beginning the process: 766 ms 70 Milliseconds time spent without encoding. 2 Milliseconds time spent for password encoding.

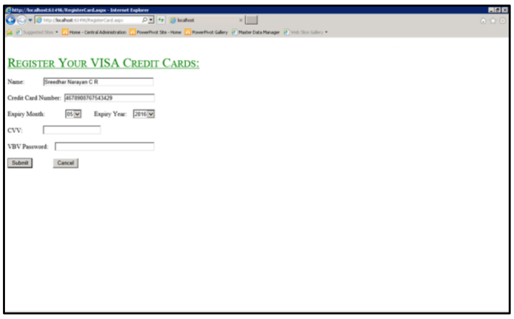
Register Your Account Details:

Complete

Your account has been successfully created.

DOI 10.17148/IJARCCE.2015.4624

Online shopping- transaction page needed a strong secure page, while the transaction is done through credit cards. So, the text steganography techniques is also implemented in VBV and CVV password to be strong enough defeat for hackers in the user registration transaction page:


http://localhost:61496/RegisterCard.aspx - Internet Explorer

REGISTER YOUR VISA CREDIT CARDS:

Name: Sreedhar Narayan C R

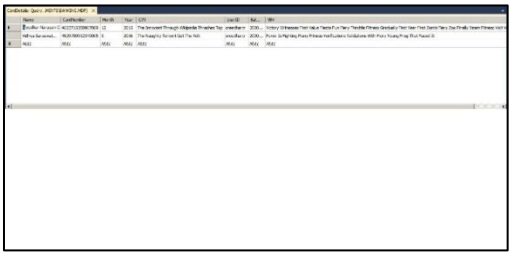
Credit Card Number: 4678900767543429

Expiry Month: 05 Expiry Year: 2016

CVV:

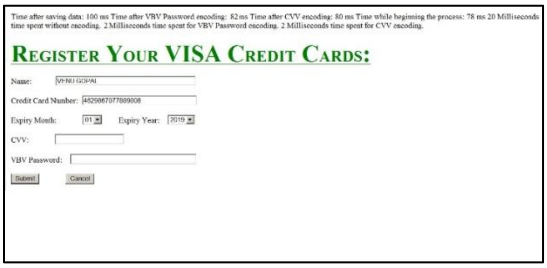
VBV Password:

Techniques implemented in the backend data for both CVV and VBV passwords:


CardDetails: Query...MENTS\BANKING.MDF)

Name	CardNumber	Month	Year	CVV	UserID	Sal...	VBV
Sreedhar Narayan C	[illegible]	12	2015	The Innocent Through Wikipedia Thrashes Top	sreedharcr	2030...	Victory Witnesses First Value Fiesta Fun Fiery Throttle Fitness Gradually First Year First Zombi Fiery Zoo Finally Team Fitness Visit V
Vidhya Saraswat...	[illegible]	5	2016	The Naughty Servant Got The Silk	sreedharcr	2030...	Power Is Fighting Plenty Fitness Horticulture Solidations With Fiery Young Frog That Faced It
NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL

Time taken for the encryption is also provided for the accuracy and data consistency.


Time after saving data: 100 ms Time after VBV Password encoding: 82ms Time after CVV encoding: 80 ms Time while beginning the process: 78 ms 20 Milliseconds time spent without encoding. 2 Milliseconds time spent for VBV Password encoding. 2 Milliseconds time spent for CVV encoding.

REGISTER YOUR VISA CREDIT CARDS:

Name: VENU GOPAL

Credit Card Number: 4629867077889008

Expiry Month: 01 Expiry Year: 2019

CVV:

VBV Password:

Users who use the credit cards for shopping through internet, can have a stress-free and at ease implementation.

V. CONCLUSION

Today's world is dependent on Internet for all the bank transactions, shopping, trading etc. for the ease and comfort zone. But on the other hand, hackers and crackers takes an advantage of finding out the loop holes and defeats the data and information. To avoid such situations, plain text of security is needed. This can be facilitated through text steganography techniques. Data integrity and confidentiality can be in a secured data for all the trends using credit cards.

In future, these trends and techniques can be implemented in other cards as well for the transaction and also for all trends and applications.

REFERENCES

[1] Souvik Roya,*, P.Venkateswaran, "A Text based Steganography Technique with Indian Root", International Conference on Computational Intelligence: Modeling Techniques and Applications (CIMTA) 2013, Procedia Technology 10 (2013) 167 – 171.

[2] Surapaneni Pujitha*, B Veera Mallu**, " SMS Based Mobile Banking", International Journal of Engineering Trends and Technology (IJETT) - Volume4Issue4- April 2013.

[3] Indradip Banerjee, Souvik Bhattacharyya, "A Procedure of Text Steganography Using Indian Regional Language", I. J. Computer Network and Information Security, 2012, 8, 65-73.

[4] Khan Farhan Rafat and Muhammad Sher, "Indiscernible Communication through ASCII Text Document/File (Communication in Veil)", IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 4, No 2, July 2013

[5] S.Changder, N. C. Debnath, D.Ghosh, "A Greedy Approach to Text Steganography using Properties of Sentences", Proceedings of the 2011 Eighth International Conference on Information Technology(ITNG 2011), ISBN: 978-0-7695-4367-3, pp. 30-35, Las Vegas, NV, USA.

[6] F. A. P. Petitcolas, R.J. Anderson, and M. G. Kuhn, "Information hiding- a survey," In *Proceedings of IEEE*, vol.87, pp. 1062-1078, 1999.

[7] L. Y. Por, and B. Delina, "Information hiding- a new approach in text steganography," *7th WSEAS Int. Conf. on Applied Computer and Applied Computational Science*, 2008, pp. 689-695.

[8] M. Khairullah, "A novel text steganography system in cricket match scorecard," *Int. Journal of Applications*, vol.21, pp. 43-47, 2011.

[9] Walter Bender, Daniel Gruhl, Norishige Morimoto, A. Lu, "Techniques for Data Hiding", IBM Systems Journal, Vol. 35, 1996.

[10] Kalavathi Alla, Dr. R. Siva Rama Prasad, "An Evolution of Hindi Text Steganography", Proceding of Sixth International Conference on Information Technology, pp. 1577-1578, Las Vegas, NV, 2009.

[11] Monika Agarwal, "text steganographic approaches: a comparison" International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.1, January 2013, PDPM-IIITDM, Jabalpur, India.

[12] W. Bender, D. Gruhl, N. Morimoto, and A. Lu, "Techniques for data hiding," IBM Systems, Journal, vol.35, pp. 313-336, 1996.

BIOGRAPHIES

Sumathy Kingslin has completed her Post Graduation from Bharathidasan University and M.Phil from Mother Teresa Women's University, Kodaikanal. She has a rich experience of 21 years of teaching and 11 years of research. Her areas of interests are Information Security, network security and Steganography. She is currently working on Steganography.

Vidhya Saraswathi received her B.Sc. degree in Computer Science and MCA Degree from Affiliated to Madras University, India. Her areas of interest are Text Steganography and network security.

DOI 10.17148/IJARCCE.2015.4624