INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 1)
Available online at www.ijariit.com

Application of the Hash Function on Secret Message and Provide it Security with the Help of Invisible ASCII Character Replacement Technology

Swati Dandekar
Dr. D. Y. Patil Institute of Technology, Pimpri, Pune, Maharashtra
swaticdandekar@gmail.com

Dr. Jyoti Rao
Dr. D. Y. Patil Institute of Technology, Pimpri, Pune, Maharashtra
joyti.aswale@gmail.com

Abstract: Most widely used technique over the internet for communication is the text-document exchange. This text document may contain valuable data or some general information of any kind. If this text document contains some important information and if gets hacked than they may change information about it or may misuse that information. Because of all these reasons we need some technique for information hiding within a text document while communication over the internet. Although there is lots of text based information hiding techniques present and proposed by many authors but these techniques have some drawbacks such as poor robustness, lower embedding rate, and semantic clutter. Due to all these flaws in the existing system many time the information is hacked or extracted by the interceptors. To mitigates all these drawbacks of existing system or techniques we proposed a new technique based on the hash function and the invisible ASCII character replacement method. In this approach, we first find the binary formatted information which is added by even numbers of 1's for even parity, after that the space character in every carrier is replaced by SOH with the help of some replacement algorithm. In the third stage, a hash value is generated. At last the hash value is compared with the encoded secrete information.

Keywords: Text-based information Hiding; Invisible Character Replacement; Hash Function; Information Security.

I. INTRODUCTION

Due to the tremendous and fast growth of the internet in recent years, it becomes the most efficient and reliable way of communication. Most widely used technique over the internet for communication is the text-document exchange. As this technique has some challenges while transmitting text valuable data over a public network while communication. Many times this information is hacked by some interceptor so there is lots of need to safely transmit the information over the internet. In order to provide reliable and secure communication over the internet through text documents many techniques and algorithms are proposed like, MAC, SHA, RSA, AES and so on. The data encrypted by such method comes with the code complexity and these techniques follow some format while encryption so it comes easy for the eavesdropper to find the correct decryption technique and extract information from it. To overcome all these techniques we proposed a novel text-based information hiding technique called secrete information hiding techniques based on hash function and invisible ASCII character replacement.

Generally, there are two information hiding methods called digital watermarking and stenography. In this approach, we consider stenography for the information hiding. Stenography is a method in which the information such as audio, video, images or text information is hiding into another file, message, audio, video or text file. In this method emails, messages, audio, video files are used as a carrier to transmit the secret information within this files. Stenography is further classified into two types, multimedia stenography, and text-based stenography. As lots of space available in multimedia stenography, this technique is robust and very useful for the data transmission over the internet. On the other hand, less space, low embedding rate and easy identification of the secret information in text-based stenography very little work has been done on the text-based stenography technique. Because most of the communication is done through text there are lots of challenges in the area to improve the text-based stenography technique. So we have considered text-based stenography as a study to overcome the disadvantages of text-based stenography.

A text-based information hiding method is consisting of two types the format-based information hiding mechanism and the content-based information hiding mechanism. A format based text hiding method carries the secret information by adjusting the font size, line space, word space, word count and so on. Though this method is rarely used as there are changes in font size chances of information loss are increases. Another method is called content-based information hiding method. This method is based on syntax, semantic and statistical properties of natural language.

In this approach, we first find the binary formatted information which is added to even numbers of 1's for even parity, after that the space character in every carrier is replaced by SOH with the help of some replacement algorithm. In the third stage, a hash value is generated. At last the hash value is compared with the encoded secret information.

II. SECURITY CHALLENGES

As most of the data sent over the internet are in text format. Most of the time this data contains some valuable data. If such file or data get hacked by hackers or some unauthorized person, than that information may get change or used in wrong way, therefore, it is necessary to provide the security for the data sends over the internet. There is a number of techniques exists currently which is used for secrete information hiding in text document but having some drawbacks such as code complexity and these techniques follow some format while encryption so it comes easy for the eavesdropper to find the correct decryption technique and extract information from it.

III. METHEDOLOGY

To overcome all the challenges and to successfully send the secret information without getting hacked we proposed a new approach called ASCHII character replacement technique for data hiding in a text document. In this, we first find the segmentation of text document and add a parity bit to binary converted secrete information. After the even party done on secrete information, a secret information hiding process is done on the text carrier document. In this hiding process, each encoded binary secretes information is replaced by the ASCHII character of the carrier text which is done by some replacement algorithm. After that, a hash value is generated. At last the hash value is compared with the encoded secret information.

IV. REVIEW OF LITRATURE SURVEY

In this section we present the different approach and techniques given by different authors regarding information hiding to send text information over the internet is as follow:

H. Krawczyk, M. Bellare, and R. Canetti in [1] proposed an HMAC technique called Keyed-Hashing for Message Authentication. In this approach, they have described a mechanism for message authentication using cryptographic hash functions. A message is sent between two parties that share a secret type of information in order to legalize the transmission of information between these parties. They also mention that the HMAC can be used with any cryptographic techniques such as MD5 and SHA-1. It also generates a secret value for calculation and verification of the message authentication values.

[2] Specifies a new function which is based on SHA-1 and SHA-2 approach caller SHA-3 i.e. Secure Hash Algorithm 3. A hash function is a function which works on binary data with fixed output length. The SHA-3 also provides the KECCAK-p family of mathematical permutations, including the permutation that underlies KECCAK. SHA-3 consists of four cryptographic hash function and two extendable-output functions.

ADVANCED ENCRYPTION STANDARD stand for AES given by Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology. AES based on the Rijndael techniques. The essential processing element used in AES algorithm is a byte. The input, output and Cipher Key bit series are developed as arrays of bytes so as to form by isolating these series into groups of eight adjacent bits to form arrays of bytes [3].

A novel encryption method which publically reveals the secret encryption key which does not require to reveal the decryption key is proposed in [4] R.L. Rivest, A. Shamir, and L. Adleman. This method gives the practical implementation of concept “public-key cryptosystem," which is based on the concepts given by Diffie and Hellman. The message encrypted in this method is divided into M which is then extend to power e publicly specified a range. Then the result is divided into two large secret prime number p and q by publically shared product n.

A theoretical presentation of information hiding techniques is given by Pierre Moulin and Joseph A. O'Sullivan in [5]. In this paper, they formalized some points and evaluate the hiding capacity which related to reliable transmission of secretes information. They also specify the basic rules for the quantities such as information hiding rates, acceptable distortion level for information hider and attacker.

A Digital Image Watermarking via Adaptive Log Texturisation technique is given by Mehran Andalibi and Damon M. Chandler [6]. In this paper, they present a new algorithm for invisible grayscale logo watermarking which operates on the basis of texturization of logo. They first separate the crowd image into poor and good texture parts. After that, the good texture region is transformed into a similar texture using Arnold transform and poorly texture is rotated through the lossless rotation. And at the end, each region is embedded via standard wavelet-based embedding scheme.

In this paper author, NIELS PROVOS AND PETER HONEYMAN introduces a Hide and Seek method. In this, they discuss the existing steganographic systems and there recent research in detecting them using numerical steganalysis. They also present current study and converse the sensible application of detection algorithms and the mechanisms for getting around them. Although steganography is allocable to all kind of data objects in this approach they accepted only JPEG images as these images do not get that much visually affected by steganography.

An algorithm called Text Information Hiding based on replacement techniques is given in [8]. In this algorithm, they proposed a well-organized information hiding technique through replacement concept. They gave that any word in text information is replaced by any meaning full similar conception, including synonym, homonym or special character which keeps the meaning of the sentence same as previous.

An improved algorithm for information hiding based on features of Arabic text: A Unicode approach is given by A.A. Mohamed in [9]. In Arabic, there is a group of six letters written isolated in a text. They use isolated letters as hidden key in Arabic text written in Unicode format. The replacement techniques search for such a letters in words for the replacement of carrier text document.

Nearly all of the accessible stenographic method is not capable to examine highly substitution based linguistic steganography methods which preserve the syntactic and semantic correctness of cover texts. A novel steganalysis approach against substitution-based linguistic steganography based on context clusters is proposed by Peng Meng in [10]. In this approach, they set up context clusters to estimation the context strength and illustrate how to use the information of context strength values to differentiate between usual texts and stego texts. At the end, they also proposed steganalysis technique for synonym substitution-based linguistic steganography.

V. CONCLUSION

Here in this paper, we proposed a new approach for secure text base hiding method based on the combination of hash code and invisible ASCII character replacement technology. The experimental shows that the algorithm gives a good result for the complex type of documents. This algorithm shows that it does not require a Unicode table to extract the information which eliminates the risk of attackers. The result shows that it contains low noise as compared to other methods. The experimental results also show that the proposed algorithm is feasible, effective and reliable. The experimental results also show that as here we consider one space in each sentence it rarely affects the carrier text which also eliminates the attacker's risk.

VI. ACKNOWLADGEMENT

I would like to take this opportunity to express my thanks to my guide Dr. Jyoti Rao for her esteemed guidance and encouragement. Her guidance always helps me to succeed in this work. I am also very grateful for her guidance and comments while designing part of my research paper and learnt many things under her leadership.

REFERENCES

1. Hugo Krawczyk, Mihir Bellare, Ran Canetti. HMAC: Keyed-Hashing for Message Authentication. RFC 2104, February 1997.
2. SHA-3Standard: Permutation-Based Hash and Extendable-Output Functions, FIPS PUB 202. National Institute of Standards and Technology (NIST). August 2015.
3. AES-The official Advanced Encryption Standard, FIPS PUB 197. Computer Security Resource Center. National Institute of Standards and Technology (NIST). Retrieved 26 March 2015.
4. Ronald L. Rivest, Adi Shamir, Leonard M. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM (Association for Computing Machinery) 26(1), 1983, pp. 96–99.
5. Pierre Moulin, Joseph A. O'Sullivan. Information-theoretic analysis of information hiding. IEEE Transactions on Information Theory, 49(3), 2003 pp563-593.
6. Mehran Andalibi, Damon M. Chandler. Digital Image Watermarking via Adaptive Logo Texturisation. IEEE Transactions on Image Processing, 24(12), 2015, pp.1-15.

7. Niels Provos, Peter Honeyman. Hide and seek: an introduction to steganography. IEEE Security & Privacy, 1(3), 2003, pp.32–44.
8 Gongshen Liu, Xiaoyun Ding, Bo Su, Meng Kui. A Text Information Hiding Algorithm Based on Alternatives. Journal of Software, 8(8), 2013, pp.2072-2079.
9. AA Mohamed. An improved algorithm for information hiding based on features of Arabic text: A Unicode approach. Egyptian Informatics Journal, 15(2), 2014, pp.79-87.
10. Peng Meng. Research on Linguistic Steganography and Steganalysis. Ph. D. dissertation, University of Science and Technology (China), 2012.
11. AA Mohamed. An improved algorithm for information hiding based on features of Arabic text: A Unicode approach. Egyptian Informatics Journal, 15(2), 2014, pp.79-87.
12. Peng Meng. Research on Linguistic Steganography and Steganalysis. Ph. D. dissertation, University of Science and Technology (China), 2012.
13. Ryan Stutsman, Christian Grothoff, Mikhail Atallah. Lost in just the translation. In: Proceedings of the 2006 ACM Symposium on Applied Computing (SAC'06), Dijon, France, April 2006, pp 338-345.
14. Chao Chen, Shuozhong Wang, and Xinpeng Zhang. Information hiding in text using typesetting tools with stego-encoding. In: Proceedings of the First International Conference on Innovative Computing, Information and Control (ICICIC ’06), Washington, DC, USA, 2006, pp. 459–462.
15. Xin-guang Sui, Hui Luo. A Steganalysis Method Based on the Distribution of Space Characters. In: Proceedings of 4th International Conference on Communications, Circuits, and Systems. Guilin, China, 2006, pp 54-56.