ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

A SURVEY OF DIFFERENT TYPE OF DATA HIDING TECHNIQUES AND ITS IMPORTANCE

A.SURESH Assistant Professor, Sri Ramakrishna Institute of Technology, Coimbatore

By the explosive growth of internet and digital communication in recent years the need of security and the confidentiality of the data has becomes the importance parameters, for achieve effecting data transmission. To protect the data from illegal access and safe data communications needs the data hiding techniques like stenography, cryptography, watermarking and hashing have been developed and are in practices today. In this paper will be covering one such data hiding techniques called steganography. Steganography is the process of masking sensitive data in any media to transfer it in secure way over the underlying unreliable and unsafe communication networks. The paper presents a study of different data hiding techniques in steganography that are in practice today world.

Key words: Data Hiding, Cover Media, Steganography, Steganoanlysis

INTRODUCTION

Internet came in the year of 1960s and 1970s which enables communication to the defense to take vital data exchange and also the essential data has been exchange in between the researcher across the diverse universities. Since the origin of the internet, the security, integrity and confidentiality of the sensitive data have been most importance attribute for message passing.

The reason for the security, integrity and confidentiality is become the primary need of communication over the network which transfer sensitive data is carried out in untrustworthy and unsafe. Anyone with the knowledge to snoop our applications and communications, they may capture the data transfer which could be very risky. Ideally the communication network and the routing protocols should expose the following properties

Distributed Operation: The internet message sharing must be distributed rather than only be located in centralized form servers. In crash ofinternet would not lose its functionality and efficiencies during the application processes.

Reliability:Reliable communication is one of the active properties of the internet. The internet must provide assurance for delivery the reliable data to the intended recipient.

Security: Security is a most significant property of the internet data sharing. The internet would provide the security, confidential and sensitive data that flows through it. The security must be provided only the intended recipient those who are going to share the data.

Quality of Service Support: Quality of Service (QoS) is one of the dynamic properties in terms of media communication. In the base of QoS support to various applications and sensitive data transfer and it should prioritize the conditional of the nature of the message transfer.

Robustness:Internet must be robust in the nature of continue functionality, normally even in the existence of errors and unpredicted situations like syntax, invalid input of information. The internet must be robust to tolerate the error.

Fault-Tolerance: Fault-tolerance represents the capability of the system to operate normally even in the fault or failure of any events. Internet should show the fault-tolerance so that it keep on functioning even it may get any unreliable fault, it may occur at some part of the internet.

All the above mentioned properties are worst and cannot be practically implemented in the structure and functioning of the internet as it includes may networks, that may have different structures : like Wired, Wireless, Adhoc, pervasive, ubiquitous computing and also various mobility models[1][2][3][4][5]. One such property that should not be assured in the security of internet.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

Due to the incapability for providing the security, and various vulnerabilities exist in the internet of network that can be exploited and gives rise to various security attacks. Most common security attacks are listed below

1. Man in the Middle attack: In this attack, the eavesdropper makes self-regulating connections with the two parties across the intra-network making them useful trust that they are communicating secretly, when in fact the entire channel communication is controlled and seized by the eavesdropper.

2. TrafficAnalysis: In this analysis the attacker pays attention to the conversation on the communication between the two parties without valid connection between them and they attempt to learn the information that could be shared between them.

3. Impersonation of Spoofing: The main goal of this attack is to take the identity of the person and stimulus the sender that it is communicating with the intended recipient.

Steganography may sometimes wrongly confuse with cryptography, but there are some important and unique differences are existing between them. In some situation the steganography is referred often as cryptography, because the cryptography converse (likes cipher text to plain text and plain text to cipher text) may guess the eavesdropper and they may employ some decryption techniques to gather the hidden information. Also, cryptography techniques frequently require high processing power to perform any kind of encryption and decryption which may cause the serious errors in small devices that have more struggles to handle the enough computing resources to perform cryptography.

On the differing, steganography is the form of concealing the sensitive data in any cover media like image and multimedia across the network. This way the attacker does not grasp that the data is to be transmitted from sender to receiver. Since it is hidden content to the normal visible eye and also it is impossible to isolate from original media content.

Steganography involves five valid steps

1. Which select the cover media for embed the data
2. Now collect the secret data for concealing into the cover media
3. Need a process – Stegano to hide the sensitive data
4. Need the process to inverse the hidden data.
5. May use an optional key or password to authenticate hidden data

II. DATA HIDING TECHNIQUES IN DIFFENENT FORMS

A.Data Hiding Techniques in imagesKuo et al. [7] [8] [9] [10] represents a reversible data hiding techniques that are based on the block separation to conceal the image data. In this paper the cover image is split or shared into number of equal block images and then the histogram is created for each of these separated blocks. Maximum and the minimum points of histogram graphs can be identified so that the inserting space of location map is to be created for hiding the secret data, which increase the embedding capacity of the image. A one bit change must to record in this method, either it may be maximum or minimum.

Nosrati et al. [6] introduced techniques that insert the sensitive message in RGB 24 bit color image. This is achieved by connecting the concept of the doubly linked list data structures to tie the sensitive data in the images. First, the selected sensitive data are to be embedding to the Least Significant Bit plane of 24 bit RGB color space. Next the data structures format of linked list in which each node is placed randomly in the physical memory and each node points connect to other nodes in the list, the selected sensitive or secret data bytes are inserted in the color image randomly and every message data which contains a link and as

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

well as address pointer to connect next message data and also, a few bytes of the address of the first secret data are used as the stego-key to validate and authenticate the our secret message. Using this technique will generate the recovery and the finding of the secret message data in the image which will be most challenging task for the attacker to find the information.

Das et al. have listed various techniques to hide message data [11] [12]. The authors has mainly focusing on how the stegano – image can be used with cryptography to hide confidential data. In this approach they have vital role to perform the listed operation 1. Convert plaintext steganography, 2. Convert Image steganography 3. Convert Audio-Video Steganography and 4. IP based Datagram steganography. This could be used to conceal the sensitive data. The authors has also explained the analysis of stegano images which is used to detect the embedded data.

Naseem et al. [13] represent an Optimized Bit Plane Splicing algorithm to conceal the data in the images. In this approach insteadjust conceal the data pixel by pixel, they may process the level by level for hiding the intensity data pixels. The intensity of the pixels are classified into various ranges, the number of bits are embedded will be used to hide data in the particular bit plane. And also, the bits are hidden randomly in the bit plane instead of conceal them nearby to each otherand finally the level plane are transmitted periodically thus it makes too difficult guess and interrupt the transmitted data

1) Data hiding Techniques in Semi fragile Image

Zhicheng Ni, Yun Q. [29] Shi, Nirwan Ansari, and Wei Su, Qibin Sun, and Xiao Lin,. The hidden data can be extracted correctly after the alternation and compression has been made applied. But the host image is always suffering from overflow and underflow problem. In this method is gives robust against high quality JPEG compression, and Modulo-256 addition algorithms is used to resolve the overflow and underflow problems. The gray scale value of some pixels in the marked image exceeds the sometime upper bound(above 255) or it may goes lower bound(below 0). The resultant will be truncation of image values, it will violate the data hiding properties. The proposed Robust lossless data hiding – that is the spatial domain based on patch work theory is used to eliminate the salt and pepper noise and also it get high signal and low PSNR ratio. So this paper introduce the BCH(Bose-Chadhuri-Hocquenghem) Error correction code (ECC) and permutation scheme is utilized to eliminate the salt and pepper noise.

The authors have shown the discriminating bit embedding process based on the pixel group' content, that may employ to achieve the lossless and robustness. The Embed bit 0 in the closure group point threshold along with error correction code is used. Embed bit 1 in the right or left shift of the closure group threshold with error correction code is also used.

2) Data hiding Techniques using Vector Quantization Technique

Jiann-Der Lee a, Yaw-Hwang Chiou a Jing-Ming Guob[30]. The main objectives in the earlier approach are low embedding capacity and high noise rate. Vector Quantization (VQ) is a block-coding technique that the block of data are quantized instead of convert pixel by pixel levels. The Vector Quantization allows the modeling of probability density functions by distributing the vectors. It works based on the dividing set of point into cluster level, which has approximately same number of closest point can be group to them. Each group is representing the k-means centroid point. In general terms as code book, the code books are used to hide the cluster of data in particular bit plane.

3)Data Hiding Techniques in Audio Signals

Kekre et al. [17] [18]. It proposed the two novel approaches to transfer secret data in and over the network for hiding the audio signals; the Stego-audio signal is the first method in which the authors hide

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

the secret data in LSB (least significant bit). The audio is seeing the parity of the sample, that is instead of directly substituting the digitized data sample the audio with the secret data message are employed to sub suits, the parity of every sample have been checked and the secret data message is embedded into the LSB plane. This way it has provides harder to the intruder to attack the hidden data being send. In the second method, XOR-ing of the LSB's is performed. The LSB's are XORed and depending on the result of this process and the secret information can be embedded, still the LSB of the sample data field is left unchaged.

Kondo [19] proposed next data hiding method algorithm forinserting data in stereo type audio signals. The algorithm uses division of impacts and it's added to the high frequency signals. In this approach the high frequency signals are exchanged by one medium channel and then the data are inserted in between them. The polarity of impacts is gives each channel may perform coherence. The detection of the embedding data is collected by employing the sum and difference of the stereo type signal. Also the original messages are not mandatory to withdraw the hidden data without importance causes.

5) Data Hiding Techniques in Video Sequences

34. Li et al. [25] [26] advised a data hiding technique based on the video sequences. This technique implements an adaptive embedding algorithm for selecting the embed point where the sensitive data is to be hidden from the intruders. The scheme functions by accepting 4x4 DCT residual blocks and used to determining a predefined threshold. The blocks are to be perused in an inverse zigzag fashion until the first none zero coefficients is met. The pixel value of this coefficient is associated with this predefined threshold and it‟s greater than the threshold pixel is chosen to embed the data.

III. CONCLUSION

In the above areas discussed about the steganography and presented some distinguished differences between steganography and cryptography. And also we measured different kind of data hiding techniques in steganography, cryptography, robustness and lossless images

In earlier part we discuss about different form of security defects and susceptibilities in the internet. And also we discussed the various kindsof techniques to activate the secure transferring data with the help of steganography, cryptography, robustness, and lossless methods

REFERENCES

[1] BhavyeshDivecha, Ajith Abraham, CrinaGrosan and SugataSanyal, "Analysis of Dynamic Source Routing and Destination-Sequenced Distance-Vector Protocols for Different Mobility models", First Asia International Conference on Modeling and Simulation, AMS2007, 27-30 March, 2007, Phuket, Thailand. Publisher: IEEE Press, pp. 224-229.

[2] S. Gowrishankar, S. Sarkar, T.G.Basavaraju, "Simulation Based Performance Comparison of Community Model, GFMM, RPGM, Manhattan Model and RWP-SS Mobility Models in MANET," First International Conference on Networks and Communications (NETCOM '09), 27-29 Dec. 2009, pp.408-413.

[3] Jonghyun Kim, VinaySridhara, Stephan Bohacek, "Realistic mobility simulation of urban mesh networks", Journal of Ad Hoc Networks, Vol. 7, Issue 2, March 2009, Publisher: Elsevier, pp. 411-430.

[4] Liu Tie-yuan, Chang Liang, GuTian-long, "Analyzing the Impact of Entity Mobility Models on the Performance of Routing Protocols in the MANET", 3rd International Conference on Genetic and Evolutionary Computing, 14-17 Oct. 2009, pp.56-59.

M.F. Sjaugi, M. Othman, M.F.A. Rasid, "Mobility models towards the performance of geographical-based route maintenance strategy in DSR", IEEE International Symposium on Information Technology, ITsim 2008 , Vol. 3, 26-28 Aug. 2008, pp. 1-5.

[6] M. Nosrati, R. Karimi, H. Nosrati, and A. Nosrati, "Embedding stego-text in cover images using linked

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

list concepts and LSB technique", Journal of American Science, Vol. 7, No. 6, 2011, pp. 97-100.

[7] Wen-Chung Kuo, Dong-Jin Jiang, Yu-Chih Huang, "A Reversible Data Hiding Scheme Based on Block Division", Congress on Image and Signal Processing, Vol. 1, 27-30 May 2008, pp. 365-369

[8] Yih-Chuan Lin, Tzung-Shian Li, Yao-Tang Chang, Chuen-Ching Wang, Wen-Tzu Chen, "A Subsampling and Interpolation Technique for Reversible Histogram Shift Data Hiding", Image and Signal Processing, Lecture Notes in Computer Science, Vol. 6134, 2010, Publisher: Springer Berlin/Heidelberg, pp. 384-393.

[9] Chyuan-Huei Thomas Yang, Chun-Hao Hsu, "A High Quality Reversible Data Hiding Method Using Interpolation Technique," IEEE Fifth International Conference on Information Assurance and Security, Vol. 2, 18-20 Aug. 2009, pp. 603-606.

[10] Che-Wei Lee and Wen-Hsiang Tsai, "A Lossless Data Hiding Method by Histogram Shifting Based on an Adaptive Block Division Scheme", Pattern Recognition and Machine Vision, River Publishers, Aalborg, Denmark, pp. 1–14.

[11] Soumyendu Das, Subhendu Das, BijoyBandyopadhyay, SugataSanyal, "Steganography and Steganalysis: Different Approaches", International Journal of Computers, Information Technology and Engineering (IJCITAE), Vol. 2, No 1, June, 2008, Serial Publications, pp. 1-11.

[12] M. Naseem, Ibrahim M. Hussain, M. Kamran Khan, Aisha Ajmal, "An Optimum Modified Bit Plane Splicing LSB Algorithm for Secret Data Hiding", International Journal of Computer Applications, Vol. 29, No. 12, 2011. Foundation of Computer Science, New York, USA, pp. 36-43.

[13] Ming Sun Fu and O.C. Au, "Data hiding watermarking for halftone images", IEEE Transactions on Image Processing, Vol.11, No. 4, Apr. 2002, pp.477-484.

[14] Soo-Chang Pei and J.M. Guo, "Hybrid pixel-based data hiding and block-based watermarking for error-diffused halftone images", IEEE Transactions on Circuits and Systems for Video Technology, Vol.13, No. 8, Aug. 2003, pp. 867- 884.

[15] SandipanDey, Ajith Abraham, SugataSanyal, "An LSB Data Hiding Technique Using Prime Numbers", IEEE Third International Symposium on Information Assurance and Security, Manchester, United Kingdom, IEEE Computer Society press, USA, 29-31 Aug. 2007, pp.101-106.

[16] H. B. Kekre, ArchanaAthawale, ArchanaAthawale, UttaraAthawale, "Information Hiding in Audio Signals", International Journal of Computer Applications IJCA, Vol. 7, No. 9, Foundation of Computer Science, New York, USA, pp. 14-19.

[17] B. Santhi, G. Radhika and S. RuthraReka, "Information Security using Audio Steganography-A Survey", Research Journal of Applied Sciences, Engineering and Technology, Vol. 4, No. 14, pp. 2255-2258.

[18] K. Kondo, "A Data Hiding Method for Stereo Audio Signals Using the Polarity of the Inter-Channel Decorrelator", IEEE Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, IIH-MSP'09. 12-14 Sept. 2009, pp.86-89.

[19] Rangarajan A. Vasudevan, SugataSanyal, Ajith Abraham, Dharma P. Agrawal, "Jigsaw-based secure data transfer over computer networks", Proceedings of International Conference on Information Technology: Coding and Computing, Las Vegas, Nevada, Vol. 1, 5-7 April 2004, pp. 2- 6.

[20] Kamran Ahsan, DeepaKundur, "Practical data hiding in TCP/IP", Proceedings of ACM Workshop on Multimedia Security, Vol. 2002, pp. 7-19.

[21] Steven J. Murdoch and Stephen Lewis, "Embedding covert channels into TCP/IP", Information Hiding, Lecture Notes in Computer Science, vol. 3727, Springer Berlin / Heidelberg, 2005, pp. 247-261.

[22] Sebastian Zander, Grenville Armitage, and Philip Branch, "A survey of covert channels and countermeasures in computer network protocols", IEEE Communications Surveys & Tutorials, Vol. 9, No. 3, 2007, pp. 44-57.

[23] WojciechMazurczyk and Krzysztof Szczypiorski, "Steganography of VoIP streams", On the Move to Meaningful Internet Systems, OTM 2008, Springer, Vol. 5332, pp. 1001-1018.

[24] Yu Li, He-xin Chen, Yan Zhao, "A new method of data hiding based on H.264 encoded video sequences", IEEE 10th International Conference on Signal Processing(ICSP), 24-28 Oct. 2010, pp. 1833-1836.

[25] Xiaoyin Qi, Xiaoni Li, Mianshu Chen, Hexin Chen, "Research on CAVLC audio-video synchronization coding approach based on H.264", IEEE International Conference on Uncertainty Reasoning and Knowledge Engineering (URKE), Vol. 2, 4-7 Aug. 2011, pp.123-126.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 20, April 2016

[26] Mohammad Reza Abbasy, BharanidharanShanmugam, "Enabling Data Hiding for Resource Sharing in Cloud Computing Environments Based on DNA Sequences", IEEE World Congress on Services (SERVICES), 4-9 July 2011, pp. 385-390.

[27] H.J. Shiu, K.L. Ng, J.F. Fang, R.C.T. Lee, C.H. Huang, "Data hiding methods based upon DNA sequences", Information Sciences, Elsevier, Vol. 180, Issue 11, 1 June 2010, pp. 2196-2208.

[28] Zhicheng Ni, Yun Q. Shi, Fellow, IEEE, Nirwan Ansari, Senior Member, IEEE, Wei Su, Senior Member, IEEE, Qibin Sun, and Xiao Lin, Senior Member, IEEERobust Lossless Image Data Hiding designed for Semi-Fragile Image Authentication ieee Transactions On Circuits and Systems for Video Technology, vol. 18, no. 4, april 2008

[29] Jiann-Der Lee a, Yaw-Hwang Chiou a, Jing-Ming Guo b, Lossless data hiding for VQ indices based on neighboring correlation Contents lists available at SciVerseScienceDirect Information Sciencesjournalhomepage: www.elsevier.com/locate/ins