IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 3, Ver. II (May – Jun. 2015), PP 94-98
www.iosrjournals.org

An Architectural Approach of Data Hiding In Images Using Mobile Communication

T.Venkata Satya Vivek*, V.Lakshma Reddy**, Ganta Anil**,
M Rao Batchnaboyina#

** Assistant Professor, Departement of Computer Science & Engineering, PACE Institute of Technology And Sciences.*
***Assistant Professor, Departement of Computer Science & Engineering, PACE Institute of Technology And Sciences.*
#Associate Professor, Departement of Computer Science & Engineering, PACE Institute of Technology And Sciences.

Abstract: *Our paper proposes a new type of technique for retrieving back the hidden information in an images using mobile communications. The usage of mobile communication in this paper is also termed as a step-2 verification on the receiver's side. By using the histogram modification technique the sender is going to embedded the data into an image, and sends it to the receiver. This paper mainly concentrates on the receiver's side to get back the embedded data using mobile communication. In the first section we briefly review the introduction the on data hiding- its previous techniques, applications, and also about reversible data embedding. In the second section we focus on the related work. In the third section we are going to discuss about the proposed methodology for retrieving back the hidden information. The fourth section shows the architecture of the proposed methodology. And the subsequent sections describe a note on security and conclusion.*

Keyword:
Data Hiding
Histogram Modification
Step-2 Verification
Mobile Communication

I. Introduction

With the invent of Computer Networks and Architectures, and ubiquitous broadband services provided by the Internet Service Providers (ISP's), people are capable of surfing on the internet at an acceptable cost. It is also convenient to parties to share the resources and perform commercial activities on the internet. However the hackers might have chance to exploit the servers to dig out a small piece of valuable information, such as credit card numbers, bank account and password details etc. which are supposed to not be exposed to the public. Moreover many chances are there to adversaries to perform man-in-middle-attacks to eavesdrop, falsify data which is transmitted between two parties. Therefore to protect the data from being stolen or illegal way of performing alteration becomes an important issue. Till today many organizations and institutions utilize encryption and decryption techniques to protect data. But the exposure of private key to unwanted means may result in insecurity of the confidential data. With all the above considerations on the other hand, data hiding in images provides an alternative solution to guard against from the illegal activities of the behavior from the adversaries [1].

Data Embedding is a new stegnographic method for embedding the confidential information into a photograph, television signal, or identification card which are termed as a set of host data with small deterioration. Data embedding is traditional problem which has applications in many areas from rigorous mathematics to machine learning and also in data mining, data indexing and security, information retrieval, and multimedia data processing.

Steganography is one such pro-security solution innovation in which the secret data is embedded into an cover image [2]. This way the attacker does not realize that the data is being transmitted since it is hidden to the naked eye and impossible to distinguish from the original media. The data embedding applications can be divided into two (2) groups: a) depending upon the relationship between the embedded image and, b) on the cover image. The relationship between the above two groups of data characterizes different applications. By considering the covert communications, the hidden data may often be irrelevant to the cover media. By considering authentication there may be a chance that the embedded data are closely related to the cover media. In the above specified data embedding applications, the invisibility of an hidden data is an important criteria.

In most of the cases of the data hiding while embedding information or data into an image, the cover media will experience some sort of distortion due to hiding of data. There exists some permanent distortion which has occurred to the cover media even after the hidden data have extracted out. In medical diagnosis and law enforcement applications, it is critical to reverse the marked media back to the original cover image after the hidden data are retrieved for some legal considerations [3]. In the applications of Remote Sensing and High-Energy particle physical experimental investigation, it is also desired that the original cover media can be recovered because of the required high-precision nature. There exists some reversible data hiding techniques which facilitates the immense possibility of applications where to link two sets of data in such a way that the cover media can be losslessly recovered after the hidden data have been extracted out.

II. Related Work

In this section we are going to concentrate on various data hiding techniques in steganography to facilitate secure data transmission over the underlying communication network.

(a)Data Hiding Techniques in Still Images:- Nosrati et al. [4] introduced a method that embeds the secret message in RGB 24 bit color image. This is achieved by applying the concept of the linked list data structures to link the secret messages in the images. First, the secret message that is to be transmitted is embedded in the LSB‟s of 24 bit RGB color space. Next, like the linked list where each node is placed randomly in the memory and every node points to every other node in list, the secret message bytes are embedded in the color image erratically and randomly and every message contains a link or a pointer to the address of the next message in the list. Also, a few bytes of the address of the first secret message are used as the stego-key to authenticate the message. Using this technique makes the retrieval and the detection of the secret message in the image difficult for the attacker.

Kuo et al. [5] [6] [7] [8] presented a reversible technique that is based on the block division to conceal the data in the image. In this approach the cover image is divided into several equal blocks and then the histogram is generated for each of these blocks. Maximum and minimum points are computed for these histograms so that the embedding space can be generated to hide the data at the same time increasing the embedding capacity of the image. A one bit change is used to record the change of the minimum points.

Das et al. have listed different techniques to hide data [9] [10]. The authors have mainly focused on how steganography can be used and combined with cryptography to hide sensitive data. In this approach they have explained and listed various methods like Plaintext Steganography, Still Imagery Steganography, Audio/Video Steganography and IP Datagram Steganography which can be used to hide data. The authors have also elucidated the Steganalysis process which is used to detect if steganography is used for data hiding.

(b)Data Hiding Techniques In Audio Signals:- Kekre et al. proposed two novel methods to transfer secret data over the network by hiding them in the audio signals, thus generating a stego-audio signal [11] [12]. In the first method the authors hide the secret data in the LSB of audio by considering the parity of the sample, i.e. instead of directly replacing the digitized sample of the audio with the secret message, first the parity of the sample is checked and then the secret data is embedded into the LSB. This way it becomes even more difficult for the intruders to guess the bit or the data that is being transmitted. In the second approach, XORing of the LSB‟s is performed. The LSB‟s are XORed and depending on the outcome of this operation and the secret data that is to be implanted, the LSB of the sample data is changed or left unchanged. A different approach is followed by Kondo. Kondo [13] proposed a data hiding algorithm to embed data in stereo audio signals. The algorithm uses polarity of reverberations which is added to the high frequency signals. In this method the high frequency signals are replaced by one middle channel and then the data is embedded. The polarity of reverberations that is added to each channel is performed to adjust the coherence between these channels. The detection of the embedded data is done by employing the correlation between the sum and difference of the stereo signal. Also, original signal is not required to extract the hidden data by using this algorithm.

(c)Data Hiding Techniques In Video Sequences:- Li et al. [14] [15] suggested a data hiding technique based on the video sequences. This method implements an adaptive embedding algorithm to select the embed point where the sensitive data is to be concealed. The scheme functions by adopting 4x4 DCT residual blocks and determining a predefined threshold. The blocks are scanned in an inverse zigzag fashion until the first non-zero coefficient is encountered. The value of this coefficient is compared with predefined threshold and if it is greater than the threshold then that pixel is chosen to embed the data.

(d)Data Hiding Techniques in IPv4 Header:- To securely transmit the data over the network the Vasudevan et al. [16] used the analogy of the jigsaw puzzle. They insinuate to fragment the data into variable sizes instead of fixed size like the jigsaw puzzle and append each fragment of data with a pre-shared message authentication code (MAC) and a sequence number so that the receiver can authenticate and combine the received fragments into a single message. At the sender side every data fragment is prefixed and suffixed with a binary „1‟ and then XOR‟ed with a Random number called the one-time pad and transmitted over the network. When the receiver receives the message it performs the exact opposite process of that to the sender and retrieves the intended message.

Recently, some reversible marking techniques have been reported in the literature. The first method is carried out in the spatial domain. It uses modulo 256 addition (assuming here that eight-bit grayscale images are considered) to embed the hash value of the original image for authentication. In this paper he is using modulo-256 addition to prevent the underflow/overflow and reversibility is achieved.

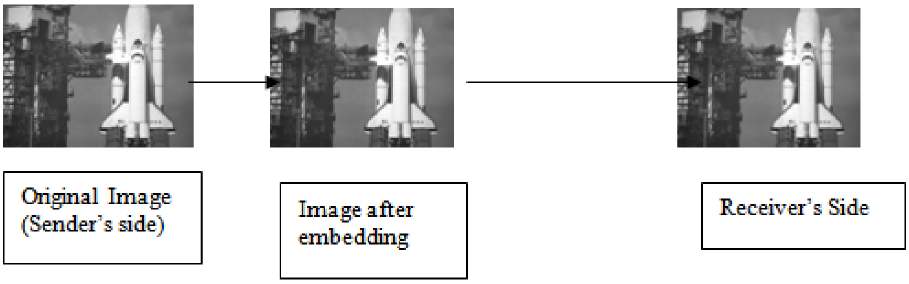
III. Proposed Methodology

The below are the steps showing the proposed methodology of our paper:
Step-1: Select an input image of any size M*N.
Step-2: Apply the Histogram Modification Technique and hide the data into the image.
Step-3: Send the data embedded image to the receiver.
Step-4: The sender has to store some passwords which are of six characters size. In the six characters password the first letter must be a capital letter, and the third letter must be a small letter of the given capital letter; and the remaining characters may be a combination of Numbers and Symbols.
Step-5: Whenever the receiver tries to retrieve the information in an image- he gets a window to enter the mobile number of the receiver. After giving the mobile number he has to click on the "Generate Password" button to get the password to his mobile.
Step-6: When the file opens, the receiver has to extract the hidden data manually which is embedded into the image.

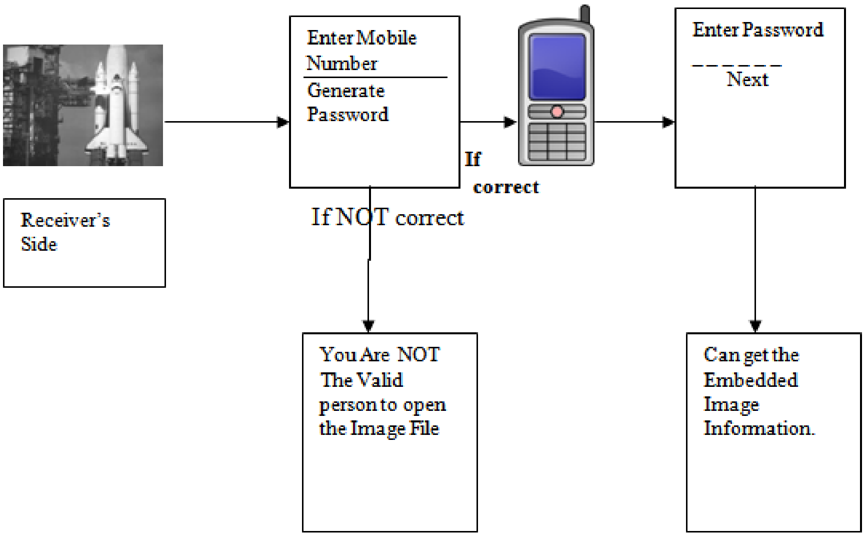
NOTE:- The receiver mobile number is stored in the sender's database. The database checks whether the number is available in the sender's database or not.
*If available, sends the password to that mobile number specified by the receiver.
*If NOT available, sends the message to the receiver that- "You Are Not a Valid Person to Open This File".

IV. Architecture- Proposed Methodology

Sender's Side:-



Receiver's Side:-



V. A Note on Security

In case of using the standard techniques available one could recognize intuitively the information or by any way of using the technique manually. So the use of the Mobile Communication in our paper is to authenticate the receiver (who is trying to retrieve the text from the image) which in-fact increases the security level.

VI. Conclusion

In this Research paper we have used the mobile communication to secure the data by using Histogram Modification technique.

References

[1]. Ching-Yu Yang, WU-Chih HU and Chih-Hung Lin, “Reversible data hiding by Coefficient-bias algorithm”, Journal of Information Hiding And Multimedia Siganl Processing, Volume 1,November 2, April 2010.

[2]. S.Katzenbeisser, F.A.P, Peticolos, “Information Hiding for Steganography and Digital Watermarking” , Artech House, Norwood,MA,2000.

[3]. Zhicheng Ni, Yun-Qing shi, Nirwan Ansari and Wei su, “Reversible Data Hiding”, IEEE Transactions on Circuits And Systems for Video Technology”, Volume 16, No:3, March 2006.

[4]. M.Nosrati, R.Karimi, H.Noratti and A.Nosrati, “Embedding Steg-cover in Cover Images Using Linked List Concepts and LSB Technique”, Journal Of American Science, Volume 7, No.6, 2011,PP.97-100.

[5]. 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 .

[6]. 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.

[7]. 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.

[8]. 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.

[9]. Soumyendu Das, Subhendu Das, Bijoy Bandyopadhyay, Sugata Sanyal, “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.

[10]. Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt, “Digital image steganography: Survey and analysis of current methods”, Journal of Signal Processing, Elsevier, Volume 90, Issue 3, March 2010, pp.727-752.

[11]. H. B. Kekre, Archana Athawale, Archana Athawale, Uttara Athawale, “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.

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

[13]. 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.

[14]. 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.

[15]. 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.

[16]. Rangarajan A. Vasudevan, Sugata Sanyal, 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.

[17]. C. W. Honsinger, P. Jones, M. Rabbani, and J. C. Stoffel, “Lossless Re- covery of an Original Image Containing Embedded Data,” U.S. Patent 6 278 791 B1, Aug. 21, 2001.

Bibliography Of Authors

	T.Venkata Satya Vivek, completed his B.Tech (CSE) from Vishnu Institute Of Technology, Bhimavaram, India and M.Tech(Computer Networks & Security) from KL University, Vijayawada, India. Presently he is working as an Assistant Professor (CSE Department) in PACE Institute of Technology & Sciences. He has published a couple of Research Papers in various International Reputed journals and Conferences. His research interests include Data Hiding Techniques and Cryptography.
	V.Lakshma Reddy, Completed his Master of Computer Applications from Sathyabhama Univesity,Chennai. Presently he is working as Assistant Professor(CSE Department) in PACE Institute of Technology & Sciences. He is having 5 years of Teaching Experience He has published a couple of Research Papers in various International Journals and Conferences. His research areas include Data Mining, Data Warehousing, Cloud Computing, Cryptography.
	M Rao Batchnaboyina, Completed his B.Tech(CSIT) from Jawaharlal Nehru Technological University, Hyderabad and M.Tech(IT) from College of Engineering, GITAM University, Visakhapatnam, India. Presently he is pursuing his PH.D from Acharya Nagarjuna University, Guntur. He is having 8 years of teaching experience. He has published a couple of Research Papers in various International Reputed Journals and Conferences. His research interests include Information Security and Classification in Data Mining.
	Ganta Anil, Completed his B.Tech(IT) from Rao and Naidu Engineering College, Ongole, India and M.Tech(IT) from SRKR Engineering College, Bhimavaram, India. Presently he is working as Assistant Professor (CSE Department) in PACE Institute of Technology and Sciences. He has published a couple of Research Papers in Various International Reputed Journals. His research areas include Image Processing, Data Hiding.