ISSN:0975-9646

Pramod Khandare et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (2) , 2014, 1785-1787

Data Hiding Technique Using Steganography

Prof.Pramod Khandare, Pooja Kambale, Prajakta Narnavar , Gauri Galande.Jayshree Narnavar

Deptartment of Information Technology
Shriram Institute of Engineering & Technology (Poly) Paniv
Tal-Malshiras Dist-Solapur
Maharashtra (India)

Abstract:With the explosive growth of internet and the fast communication techniques in recent years the security and the confidentiality of the sensitive data has become of prime and supreme importance and concern. To protect this data from unauthorized access and tampering various methods for data hiding like cryptography, hashing, authentication have been developed and are in practice today. In this paper we will be discussing one such data hiding technique called Steganography. Stegnography is the process of concealing sensitive information in any media to transfer it securely over the underlying unreliable and unsecured communication network. Our paper presents a survey on various data hiding techniques in steganography that are in practice today along with the comparative analysis of these techniques. Data hiding, a form of steganography, embeds data into digital media for the purpose of identification, annotation, and copyright. Several constraints affect this process: the quantity of data to be hidden, the need for invariance of these data under conditions where a "host" signal is subject to distortions, e.g., lossy compression, and the degree to which the data must be immune to interception, modification, or removal by a third party. We explore both traditional and novel techniques for addressing the data-hiding process and evaluate these techniques in light of three applications: copyright protection, tamper proofing, and augmentation data embedding.

Keywords: Data Hiding, Cover Media, Steganography, Steganalysis..

INTRODUCTION

Internet came into existence in the late 1960s and 1970s out of the need to exchange research data among the researchers across different universities and also to enable communication in the battlefield to convey vital information which could prove advantageous in the war situations. Since the inception of the internet, the security and the confidentiality of the sensitive information have been of utmost importance and top priority. The reason for this security and confidentiality is because the underlying communication network over which the transfer of sensitive information is carried out is unreliable and unsecured. Anybody with the proper knowledge and right applications can eavesdrop and learn of the communication and intercept the data transfer which could be very dangerous and even life threatening in some situations.

1.1 PROPERTIES

Security : Security is an important property of the internet. The internet should provide and preserve the confidential and sensitive information that flows through it. The security should be such that only the intended recipient of the information should gain access to it.

Distributed Operation: The internet should be distributed rather than only residing on some centralized server. In the event of the crash the internet should not lose its functionality and continue performing efficiently.

Reliability: Reliable communication is one of the vital properties of the internet. The internet should guarantee the reliable delivery of the information to the intended recipient.

Fault-Tolerance: Fault-tolerance means the ability of the system to operate normally even in the events of failure. Internet should exhibit fault-tolerance so that it keeps on functioning even when there is failure in some part of the internet.

Quality of Service Support: Quality of Service (QoS) is one of the crucial properties in terms of communication. Inter should provide QoS support to various applications and sensitive data and should prioritize them depending on the nature of the data.

Robustness: Internet should be robust in the sense that it should continue functioning normally even in the presence of errors and unexpected situations like invalid input.

1.2 VARIOUS DATA HIDING TECHNIQUES

In this section we will be presenting the survey on various data hiding techniques in steganography to facilitate secure data transmission over the underlying communication network.

1.2.1 Data Hiding Techniques in Still Images

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. 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. 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. Optimized Bit Plane Splicing algorithm to hide the data in the images. This method incorporates a different approach than the traditional bit plane splicing technique. In this approach instead of just hiding the data pixel by pixel and plane by plane, the procedure involves hiding the data based on the intensity of the pixels. The intensity of the pixels in categorized into different ranges and depending on the intensity of the pixel, the number of bits are chosen that will be used to hide data in that particular plane. Also, the bits are hidden randomly in the plane instead of hiding them adjacent to each other and the planes are transmitted sporadically thus making it difficult to guess and intercept the transmitted data.

1.2.2. Data Hiding Techniques in Audio Signals

We proposed two novel methods to transfer secret data over the network by hiding them in the audio signals, thus generating a stego-audio signal.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 [19] 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.

1.2.3 Data Hiding Techniques in IPv4 Header

To securely transmit the data over the network 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.

Approaches that exploit the redundancy in the IPv4 header of the TCP/IP protocol suite to convey the secret message over the communication channel without detection . In the first method, the FLAGS field containing the fragmentation information is used to conceal the data and transmit over the network. In the second technique 16-bit identification field of the header through chaotic mixing and the generation of sequence numbers is used to hide the data and convey the information to the recipient.

1.2.4 Data Hiding Techniques in Video Sequences

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.

1.2.5. Data Hiding Techniques using DNA Sequences

A scheme to enable secure sharing of resource in cloud computing environments. The proposed method employs DNA sequences to hide data. The process consists of two steps. In the first step a DNA sequence is selected and the binary data is converted into this DNA sequence by applying the pairing rules. This step, apart from converting the data also increases the complexity by applying the complementary rules and then indexing the garbled sequence. The second step involves the extraction of the hidden data from the DNA sequence where in exactly a reverse operation is performed to the first step.

2. FEATURES

Data-hiding techniques should be capable of embedding data in a host signal with the following restrictions and features:

1. The host signal should be nonobjectionally degraded and the embedded data should be minimally perceptible. (The goal is for the data to remain *hidden*. As any magician will tell you, it is possible for something to be hidden while it remains in plain sight; you merely keep the person from looking at it. We will use the words *hidden*, *inaudible*, *unperceivable*, and *invisible* to mean that an observer does not notice the presence of the data, even if they are perceptible.)
2. The embedded data should be directly encoded into the media, rather than into a header or wrapper, so that the data remain intact across varying data file formats.
3. The embedded data should be immune to modifications ranging from intentional and intelligent attempts at

removal to anticipated manipulations, e.g., channel noise, filtering, resembling, cropping, encoding, lossy compressing, printing and scanning, Digital-to-analog (D/A) conversion, and analog- to-digital (A/D) conversion, etc.

4. Asymmetrical coding of the embedded data is desirable, since the purpose of data hiding is to keep the data in the host signal, but not necessarily to make the data difficult to access.

5. Error correction coding1 should be used to ensure data integrity. It is inevitable that there will be some degradation to the embedded data when the
host signal is modified.

6. The embedded data should be self-clocking or arbitrarily re-entrant. This ensures that the embedded data can be recovered when only fragments of the host signal are available, e.g., if a sound bite is extracted from an interview, data embedded in the audio segment can be recovered. This feature also facilitates automatic decoding of the hidden data, since there is no need to refer to the original host signal.

3 ALGORITHM

Data hiding algorithm

Input: Video
Output: Stego video

Step 1: Read the input Video
Step 2: Perform frame separation
Step 3: Apply Integer DCT on each 8×8 block.
Step 4: Perform Zigzag Scanning on each 8×8block.
Step 5: Apply Huffman coding to compress the frame.
Step 6: Apply secret key to hide the data.
Step 7: Apply LSB Algorithm to embed data
Step 8: Generate Stego video

Data Extraction algorithm

The extraction algorithm is exactly the reverse. From the stego-image, each pixel with embedded data bit is converted to its corresponding natural decomposition and from the *th p* bit-plane the secret message bit is extracted. Further, all the bits are combined to get the secret message.

Input: Stego video
Output: Hidden data
Step 1: Read Stego video.
Step 2: Perform decoding using IDCT and Inverse Huffman coding.
Step 3: Extract hidden data using ILSB and Secret Key.

D. *Secret key generation algorithm*

Step 1: Take a key which is a prime number
Step2: Generate two prime numbers p, q nearer to given key.
Step3: Calculate n=p*q;
Step 4: Calculate m= (p-1)(q-1).
Step 5: Generate e
Assume e=1; x=1;
While (mod(m,e)==0)
e = e+1;
Step 6: Generate d
Take s=1+x*m;
While (mod(s,e) ~= 0)
x = x+1;
s=1+x*m;
d=s/e;

CONCLUSION

In this paper we discussed about steganography and presented some notable differences between steganography and cryptography. We also surveyed various data hiding techniques in steganography and provided a comparative analysis of these techniques. In the Introduction section we discussed about various security flaws and vulnerabilities in internet. We also discussed about various techniques to enable the secure transfer of data with the help of methods like cryptography, steganography, hashing, and authentication. In the next section we presented various techniques to conceal data in steganography.

REFERENCES:

1. V. Manjula et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (5) , 2012,5097 – 5100.
2. W. Bender, "Data Hiding," News in the Future, MIT Media Laboratory, unpublished lecture notes (1994).
3. Cryptography by Atul Kahate