Multimedia based Communication using Sequence Number Field

S. Surwase[1] S. Amane[2] R. Kamble[3] R. Adhav[4] Prof. Pournima More[5]
[1,2,3,4]Student [5]Assistant Professor
[1,2,3,4,5]Department of Computer Engineering
[1,2,3,4,5]G. H. Raisoni College of Engineering and Management, Wagholi, Pune India

Abstract— This document Multimedia Communication using sequence number field is nothing but secret communication within a legitimate communication channel. In Secure Communication two people who are supposed to communicate can communicate by using the some mechanisms which again not a standard communication. This is hidden kind of communication within a communication environment, in legitimate communication where sender and receiver communicate secretly. A previous Secure Communication was unreliable and has low data rate capability. A scheme for secure communication using data compression by the Log operation. The secure data is first compressed using a compression algorithm and then embedded into the edges of the secure image using an arithmetic division operation, Digital signature algorithm and Steganography. Here we are using TCP/IP protocol to send data packets; we are sending our data in the sequence no. field instead of data field to hide the communication.

Key words: AES, Sequence Number Field, Steganography, Digital Signature Algorithm, Compression, Encryption

I. INTRODUCTION

Generally, digital information is an important term in today's world. This digital information can be large in size; most important is this information is in human readable form, so anyone can easily read the data. It provides high possibility of information insecurity. Now days it is important to convert/encrypt the data which is secured or difficult to third party/attacker to understand that information. In network all the data is sent in the form of packets which size of 0-31 bit, so if we want to send large amount of data like 32 bit or more than that we need to compress that data that will reduce the size of data. For the process of compression we use different kind of operations such as arithmetic operation. The output provided by the arithmetic operation is again processed by the digital signature algorithm or steganography. Data hiding is found to be a key to safe communication. Steganography refers to hiding confidential data within an invisible manner. It utilizes digital media such as text, image, audio-video and multimedia so called cover for secret data. Encryption provides secure channels for communicating fields; the encrypted data exists in a unreadable form and may attract the attention of the interceptors to break the secure and secret data. This limitation come in data encryption, calls the communicating entities to use steganography to achieve covertness. The advantage in LSB method is that the large amount of data that can be embedded is more than one in LSB techniques. However most of the LSB techniques are easy to statistical attacks for attacker. Frequency domain techniques offer higher robustness to noise and attacks. This paper presents a data hiding technique that conceals the secure data within the edges of a image of 24 bit of size. The edges of the cover image are identified using the a dynamically generated threshold and can any edge detection algorithm. The secret data is then embedded into the edges of the image in the form of remainder and quotient data using an arithmetic division operation and logical operations.

This document mainly on the secure communication using TCP/IP protocol with Sequence-No field. Here motto to do covert communication is to hide the very existence of communication from attackers. We achieve security for our data transfer by using hidden channel i.e. we are sending our data secretly by using Sequence-No field instead of Data-Field. Generally attacker directly focus on Data-Field to hack the confidential information, but as we are using another mechanism called Sequence-No field to send our secret message or information without any attack. major threat to security in covert channel is trapdoor which is nothing but a non-transparency. Trapdoor is an unintended design within communication whose motto is to leak data or message. Hybrid covert channel is composition of heterogeneous and homogenious covert channels either simultaneously or used at different instant of time.

II. LITERATURE SURVEY

Literature survey is the most important step in software developing process. Before developing the software it is necessary to determine economy, the time factor n company strength. Once these things are stained, next steps are to determine which language and OS can be used for develop the tool. Once the developer start building the tool the developer need large amount of internal and external support. This support can be obtained from senior developer or programmers, from book or from websites. Before build of the system the above consideration are taken into think for developing the propose system.

In this paper[1] the digital era has seen a large growth in technology and we find ourselves commit with the large amounts of data that needs to be shared and accessed with people all over the places in the world. A challenge is posed when data has to be transmitted secretly. This paper presents the secure communication using data compression using log and the arithmetic division operation. The secret data is first compressed using a log operation and then embedded into the edges of the cover image using an edge based algorithm and various other logical operations. Proposed technique gives experimental results indicate that the provides a stego image of good quality. Our Steganography technique also achieves good Structural Similarity Index value as well as a good Peak Signal to Noise Ratio.

In hash based video Steganography [2] deals with hiding secret data or message within a video or image. In this paper, a hash based least significant bit (LSB) technique has been created. A domain technique where the secure information is embedded in the LSB of the image frames. 8 bits of the secure message is divided into 3, 3,2bit and embedded into the RGB pixel values of the cover frames one

by one. A hash based function is used to select the position of insertion secure message or information in LSB bits. The proposed method is analyzed in terms PSNR compared to the original cover image as well as the Mean Square Error (MSE) measured between the original and steganographic files over all video and image frames. An application of the algorithm is illustrated with Audio Video Interleave(AVI) file as a cover media. The results obtained are significant and encouraging. Effort has also been taken to study the steganalysis.

In this paper[3] Steganography is covert communication, which means to hide the very existence of a message from a third person or party. Due to growing need for security of information or message, image Steganography is gaining popularity The important goal of Steganography is to communicate securely in a completely unreadable manner and to avoid leakage the transmission of a hidden data. It is not to keep others from knowing the secured information or message, The data can be visible in basic formats like text,video, audio and Images etc. These forms of data are detectable by human unreadable, and the best solution was Steganography.

In covert channel detection [4] Secret communication using network has always been an area of interest for many peoples. It has only attracted the untrusted parties to communicate with each other secretly and securely but has also attracted the attackers to find ways to finding and leakage the information and use the network in a manner that produce security policies. Secure communication via network has always been an area of interest. It has not only attracted the trusted persions to communicate with each other secretly but has also attracted the attackers to find ways to discover and leakage the message or information and use the network in a manner that security policies. Covert channels are most widely used approaches for secret communication. Number of techniques has been proposed for covert channel detection. This paper covers detecting techniques of the covert channel only is modern way of leaking information and it is difficult to detect such channels.

In Steganography using reversible texture synthesis [5]. We propose a novel approach for Steganography usage a reversible texture synthesis. A texture synthesis process is a very small texture image, which synthesizes a new texture image with a same local appearance and an arbitrary size. We weave the texture synthesis process into steganography to conceal secret information. In contrast to using an existing cover image to hide information, our algorithm deals with the source texture image and embeds secret data through the process of texture synthesis. This allows us to extract the secret data and source texture from a stego synthetic texture. In the last decade many advances have been made in the world of digital media, and much concern has arisen regarding steganography for digital media. Steganography is a separate method of information hiding techniques. It embeds messages into a host medium in order to hide secret messages so as not to arouse malicious by an eavesdropper. A typical Steganography application includes secure communications between two parties those existences is unknown to a possible attacker and whose success depends upon detecting the existence of this communication. In general, the main host medium used in Steganography contains meaningful digital media which are digital image, text, audio, video, 3D model, etc. First, since the size of the cover image is fixed, the more secret messages which are embedded allowed for more image distortion. Consequently, a compromise must be reached between the image quality and the embedding capacity which results in the limited or small size storage capacity provided in any specific cover image. Revoke that image steganalysis is an approach used to detect secret messages hidden in the stego image. A stego image includes some distortion, and regardless of how minute it is, this will interfere with the natural features of the covered image. This leads to the another disadvantage because it is still possible that an image steganalytic algorithm.

In this paper [6] for secrete communication, covert channels or stenographic methods needs to change communication medium unconventionally. Information can be hiding with network protocol as a channel; it is also referred as protocol channel. This initiative now is a part of information hiding research. Covert channels have two types these types are: covert storage and covert timing. In storage covert channel system, sending process alters a particular data item (say, packet headers) and a receiving process simply interprets the altered value of sender's process. On the other hand, in covert timing channel totally depends on the amount of time or order of events (say, packet arrivals, etc.) of sender's process while receiving process simply detects a change in an attribute as well as interprets delay or lack of delay as information.

In High-performance JPEG Steganography in complementary embedding[7] a high-performance JPEG Steganography must be secure enough that needs to resist modern steganalysis. In this document, we resolve a high-performance JPEG steganographic method. The new method acquire the complementary embedding strategy to ignore the detections of several statistical attacks. To show effectiveness of the proposed method, different statistical attacks are generated and used to detect the stego-image that are created by the proposed method. Different JPEG steganographic are also simulated for comparisons with the new implemented method. Experimental results show that the resolve steganographic method has superior performance both in security and capacity, and is practical for the application of covert communication.

III. EXISTING SYSTEM

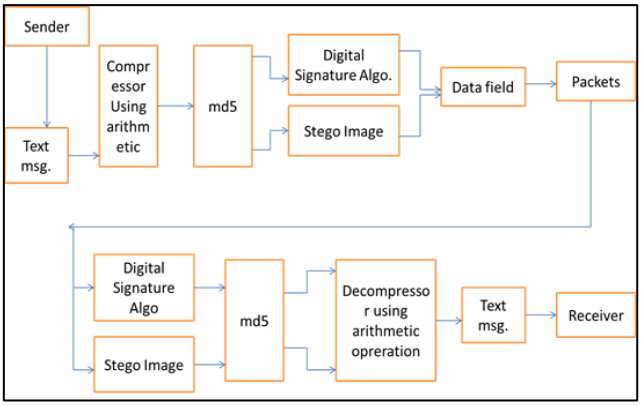

Fig. 1: System Architecture for Multimedia based Communication using sequence number field.

IV. SYSTEM ARCHITECTURE

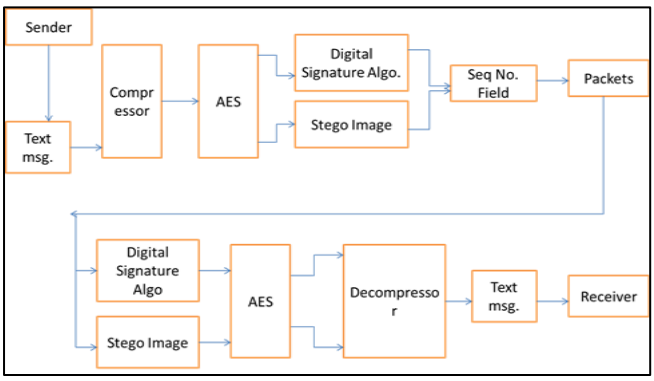

Fig. 2: System Architecture for Multimedia based Communication using sequence number field.

V. RESULTS

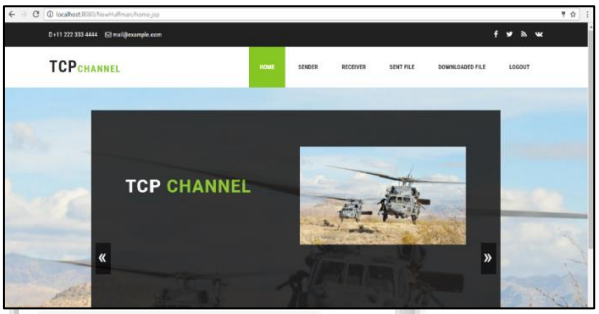

Fig. 3: HomePage

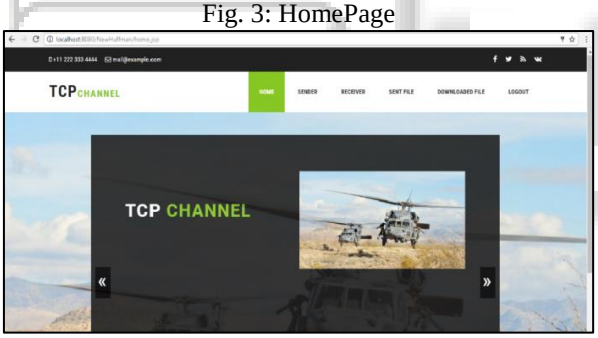

Fig. 4: Registration

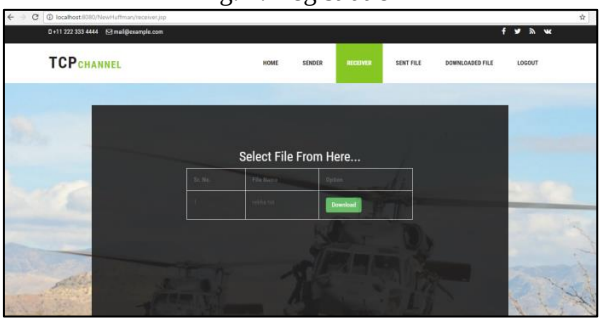

Fig. 5: User Interface for Receiver

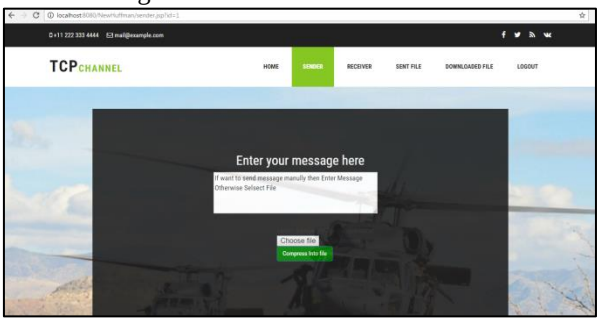

Fig. 6: User Interface for Sender

VI. CONCLUSION AND FUTURE SCOPE

The design and implementation of an multimedia based communication using sequence number field is presented. The design consists of senders and receiver's ip addresses, using those addresses sender/receiver will receive the information. We are using sequence no. field instead of data field thus the security is maintained, Data size is reduced. In proposed system for the compression and decompression of data use the arithmetic operation but that system we use the Log operation for compression and Antilog for decompression. In future the sending/receiving data size is increased.

REFERENCES

[1] Aisha Fernandes, Wilson Jeberson, Covert Communication Using Arithmetic Division Operation, (ICACTA).
[2] Kousik Dasgupta1, J.K. Mandal2 and Paramartha Dutta 2, hash based least significant bit technique (HLSB), International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, No 2, April 2012.
[3] K. Naveen BrahmaTeja1, Dr. G. L. Madhumati 2, K. Rama Koteswara Rao3,Data Hiding Using EDGE Based Steganography, ISSN 2250-2459, Volume 2, Issue 11, November2012 .
[4] S. Zerafshan Gober, Barkha Javed, Nazar Abbas Saq, Covert Channel Detection: A Survey Based Analysis, NUST School of Electrical Engineering and Computer Sciences (SEECS) 2008.
[5] Kuo-Chen Wu and Chung-Ming Wang, Member, IEEE, and Steganography with Revere texture Synthesis, IEEE TOIP, Vol. 24, No. 1, January 2015.
[6] Dhananjay M. Dakhane, Prashant R. Deshmukh, Active warden for TCP Sequence Number base, International Conference on Pervasive Computing (ICPC).
[7] Chiang-Lung Lius, Shiang-Rong Liao, High-performance JPEG Steganography using complementary embedding, Pattern Recognition 41 (2008) 2945 – 2955, ROC Received 12 June 2006; received in revised form 27 April 2007; accepted 3 March 2008

