Australian Journal of Basic and Applied Sciences, 9(11) May 2015, Pages: 635-639

ISSN:1991-8178

Australian Journal of Basic and Applied Sciences

Journal home page: www.ajbasweb.com

Enhanced image Steganography using Steg analysis Algorithm for Secured Communication in Network

Chokkalingam SP, Sankaran S, Krishnan A

Department of Computer Science Engineering Saveetha School of Engineering, Saveetha University

ARTICLE INFO

Article history:
Received 12 March 2015
Accepted 28 April 2015
Available online 1 June 2015

Keywords:
Steganography, Chat Communication, Security, LSB,Hidden Communication

ABSTRACT

The term 'Steganography' describes the method of hiding cognitive content in another mediumto avoid detection by the intruders. There are many ways to hide information inside an image,audio/video, document etc. But Image Steganography has its own advantages and is most popular amongthe others. Covert communication is taking place by encrypting the information to be protected. Theintended receiver will decrypt the information using the tool. This paper implements security usingSteganography with the basis of text embedded into image and transferring it. Using the concept ofsteganography we develop a chat application. In this end user identifies an image, which is going to act asthe carrier of data. The data is selected and then to achieve greater speed of transmission the data file andimage file are compressed and sent. Prior to this the data is embedded into the image and then sent. If theimage is hacked or interpreted by a third party user will open up in any image previewed but notdisplaying the data. This protects the data from being invisible and hence be secure during transmission.The user in the receiving end uses another piece of code to retrieve the data from the image.

© 2015 AENSI Publisher All rights reserved.

To Cite This Article: Chokkalingam SP, Sankaran S, Krishnan A, Enhanced image Steganography using Steg analysis Algorithm for Secured Communication in Network. ***Aust. J. Basic & Appl. Sci.,*** *9(11): 635-639, 2015*

INTRODUCTION

One of the reasons that intruders can be successful is the most of the information they acquire from a system is in a form that they can read and comprehend. Intruders may reveal the information to others, modify it tomisrepresent an individual or organization, or use it to launch an attack. One solution to this problem is, throughthe use of steganography. Steganography is a technique of hiding information in digital media. In contrast tocryptography, it is not to keep others from knowing the hidden information but it is to keep others from thinkingthat the information even exists.

Steganography become more important as more people join the cyberspace revolution. Steganography is the artof concealing information in ways that prevents the detection of hidden messages. Steganography include anarray of secret communication methods that hide the message from being seen or discovered.Due to advances in ICT, most of information is kept electronically. Consequently, the security of information has become a fundamental issue. Besides cryptography, steganography can be employed to secure information.In cryptography, the message or encrypted message is embedded in a digital host before passing it through thenetwork, thus the existence of the message is unknown. Besides hiding data for confidentiality, this approach ofinformation hiding can be extended to copyright protection for digital media: audio, video and images.The growing possibilities of modern communications need the special means of security especially on computernetwork. The network security is becoming more important as the number of data being exchanged on theinternet increases. Therefore, the confidentiality and data integrity are requires to protect against unauthorizedaccess and use. This has resulted in an explosive growth of the field of information hiding.Steganography hide the secrete message within the host data set and presence imperceptible and is tobe reliably communicated to a receiver. The host data set is purposely corrupted, but in a covert way, designedto be invisible to information.

Existing system:

The existing systems use cryptography techniques for transmitting data in network. Cryptography hides thecontents of a secrete message from a malicious people. The term is most often

Corresponding Author: Chokkalingam SP, Department of Computer Science Engineering Saveetha School of Engineering, Saveetha University
E-Mail: cho_mas@yahoo.com.co

associated with scramblingplaintext into cipher text (a process called encryption), then back again (known as decryption). In cryptography,the system is broken when the attacker can read the secret message.

Proposed system:

To overcome the disadvantages of the existing system Steganography is used. Steganography is the practice ofhiding private or sensitive information within something that appears to be nothing out to the usual.Steganography is often confused with cryptology because the two are similar in the way that they both are usedto protect important information. The difference between two is that steganography involves hiding informationso it appears that no information is hidden at all. If a person or persons views the object that the information ishidden inside of he or she will have no idea that there is any hidden information, therefore the person will notattempt to decrypt the information. Using the concept of steganography a chat application is implemented forsecure communication.

System features:

The Chat application would provide with the following features:

- Creating an Account: The user gives his personal information, chooses a User ID and a password of his ownchoice. The database on the server side is updated after this.
- Login and Logout: These functions indicate the availability or non-availability of the user.
- Instant Messaging: This is a regular feature of any chat. This chat application would also provide this featurebetween multiple users.
- Transferring files: The chat application would also have to transfer files between the users.

System architecture:

Steganography application:

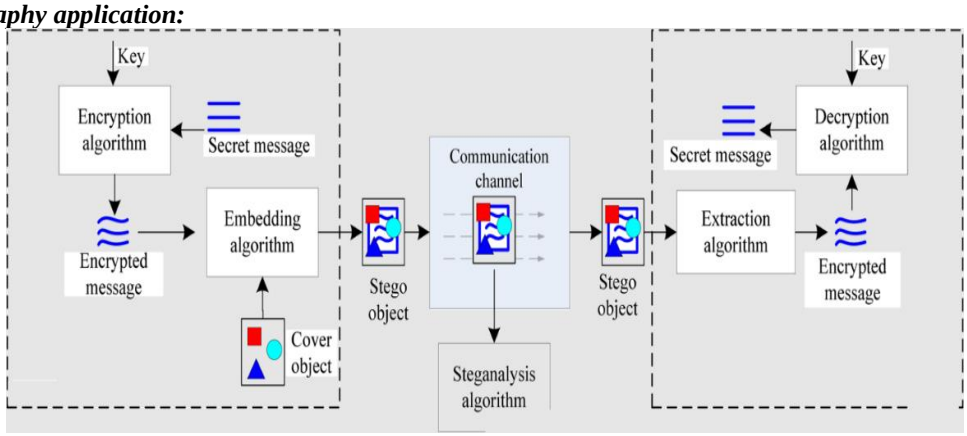

Fig. 1: Architecture of the Steganography Application,

Chat application:

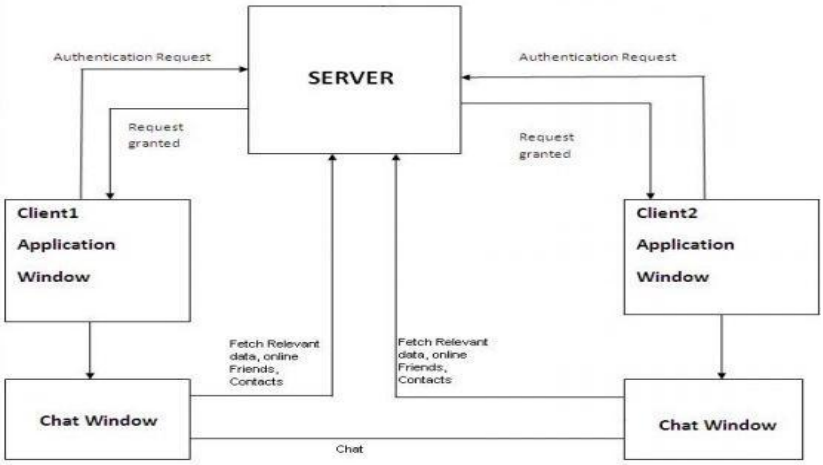

Fig. 2: Architecture of the Chat Application.

Steganography system requires any type of image file and the information or message that is to be hidden. It has two modules encrypt and decrypt. Microsoft.Net framework prepares a huge amount of tool and options for programmers that they simples programming. One of .Net tools for pictures and images is auto converting most types of pictures to BMP format. The algorithm used for Encryption and Decryption in this application provides using several layers lieu of using only LSB layer of image. Writing data starts from last layer (1st or LSB layer); because significant of this layer is least and every upper layer has doubled significant from its down layer. So every step wego to upper layer image quality decreases and image retouching transpires.

The chat application would be accomplished on a Server-Client Architecture within a LAN. The client–server model of computing is a distributed application that partitions tasks or workloads between the providers of aresource or service, called servers, and service requesters, called clients. The Server Side would be acontinuously running service listening to the different Clients asking its services. The chat application would beinstalled on every communicating client. A Database of users would be maintained by the Server. When client logins to the application,the Server authenticates the client,once the user is authenticated theIP address of the client is registered to the Server and it sends the list of online user friends and other relevantdata to the Client. When the user wishes to chat to some other user, his IP address along with a Port addresswould be sent to the other user and vice versa. Thus a connection would be established and the two client PCswould be able to chat together.

System description:

Image steganalysis:

Algorithms for image steganalysis are primarily of two types: Specific and Generic. The Specific approach represents a class of image steganalysis techniques that very much depend on the underlying steganographic algorithm used and have a high success rate for detecting the presence of the secret message if the message is hidden with the algorithm for which the techniques are meant for. The Generic approach represents a class of image steganalysis techniques that are independent of the underlying steganography algorithm used to hide the message and produces good results for detecting thepresence of a secrete message hidden using new and/or unconventional steganographic algorithms. The image steganalysis techniques under both the specific and generic categories are often designed to detect the presence of a secret message and the decoding of the same is considered complementary not mandatory.

Specific image steganalysis algorithms:

Image steganography algorithms are more often basedon an embedding mechanism called Least Significant Bit(LSB) embedding. Each pixel in an image is represented as a 24-bitmap value, composed of 3 bytes representing the R, G and B values for the three primary colors Red, Green and Blue respectively. A higher RGB value fora pixel implies larger intensity. For instance, a pixel p represented as FFFFFF16is composed of all of these three primary colors at their maximum intensity and hence the color represented by this pixel is “white”. LSB embedding exploits the fact that changing the leastsignificant bit of each of the three bytes of a pixel would produce only a minor change in the intensity of the color represented by the pixel and this change is not perceptible to the human eye. For example, changing the color values of pixel pto FEFEFE16would make the color darker by a factor of 1/256. Steganography algorithms based on LSB embedding differ on the pattern of modification – a modification of randomly chosen pixels or modification restricted to pixels located in certain areas of the image. Images can be represented in different formats, thethree more commonly used formats are: GIF (Graphics Interchange Format), BMP (Bit Map) and JPEG (Joint Photographic Exchange Group). Each of these image formats behaves differently when a message is embedded in it. Accordingly, there exist different image steganalysis algorithms for each of these three image formats. We now discuss the algorithms for each of these formats.

Encryption:

Encryption includes a message or a file encrypting. Hiding message is the most important module of steganography. It involves embedding the message intothe cover text. Each pixel typically has three numbers associated with it, one eachfor red, green, and blue intensities, and these values often range from 0-255.Inorder to hide the message, data is first converted into byte format and stored in a byte array. The message is then encrypted and then embedded each bits into the LSBposition of each pixel position. The least significant (rightmost) bit of each 8-bitbyte has been co-opted to hide a text message.

Decryption:

It involves retrieving the embed message from the file independent of the fileformat. Once the message has been retrieved it has to be converted into originalmessage or file.This can be done by reading the embedded data from the master file. The readdata will be in the bytes format. This message has to be converted into the suitableoutput file format.

Advantages of the proposed work:

The advantage of steganography chat is that messages do not attract attention to themselves. Plainly visibleencrypted messages-no matter how unbreakable-will arouse suspicion. Therefore, whereas cryptographyprotects the contents of a

message, steganography can be said to protect both messages and communicatingparties.

Experimental results:

The following are the screenshots of our proposed work,

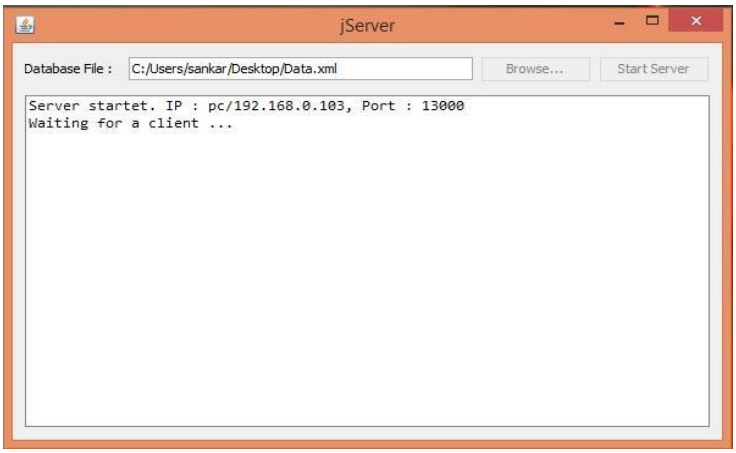

Fig. 3: Server Start

The Figure 3 gives the starting of the server. The server is accessed by the clients also knows as the service requesters who request the server. The clients are authenticated by the server which has the login information inthe data file.

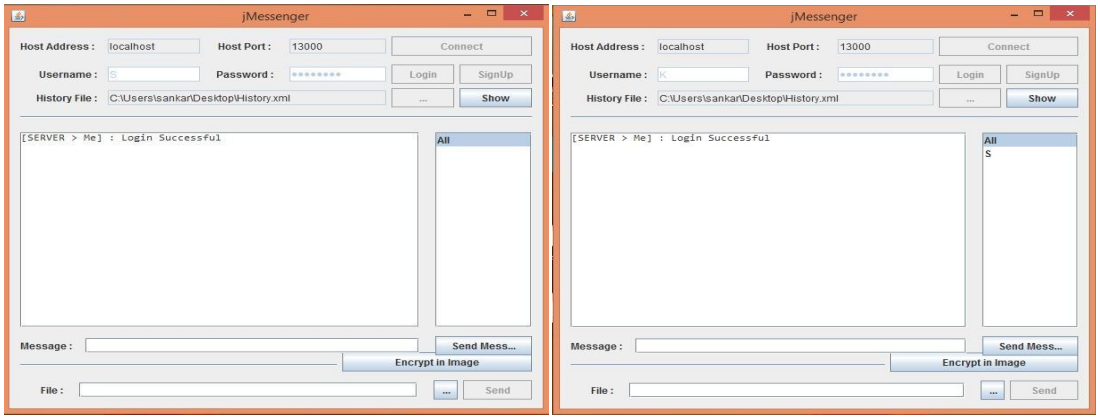

Fig. 4: Client1 and 2 Login.

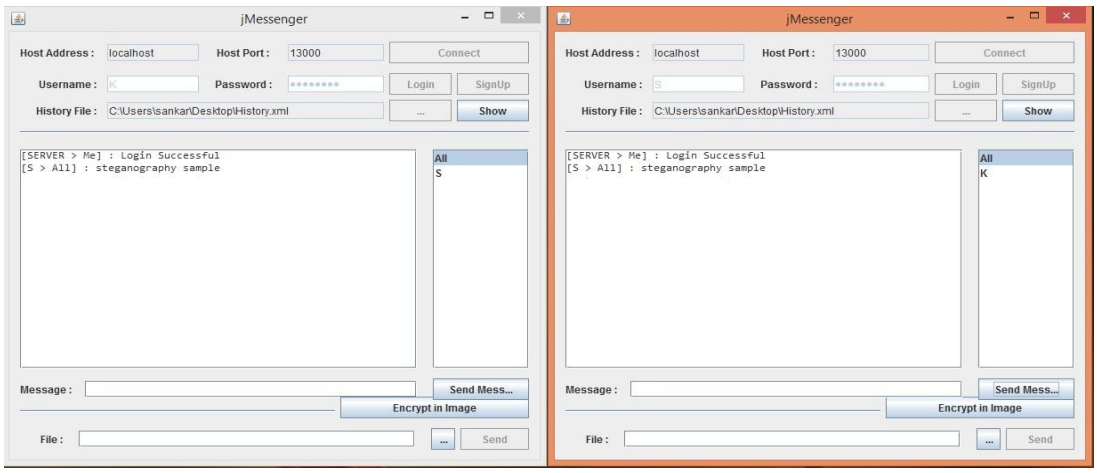

Fig. 5: Chat between clients.

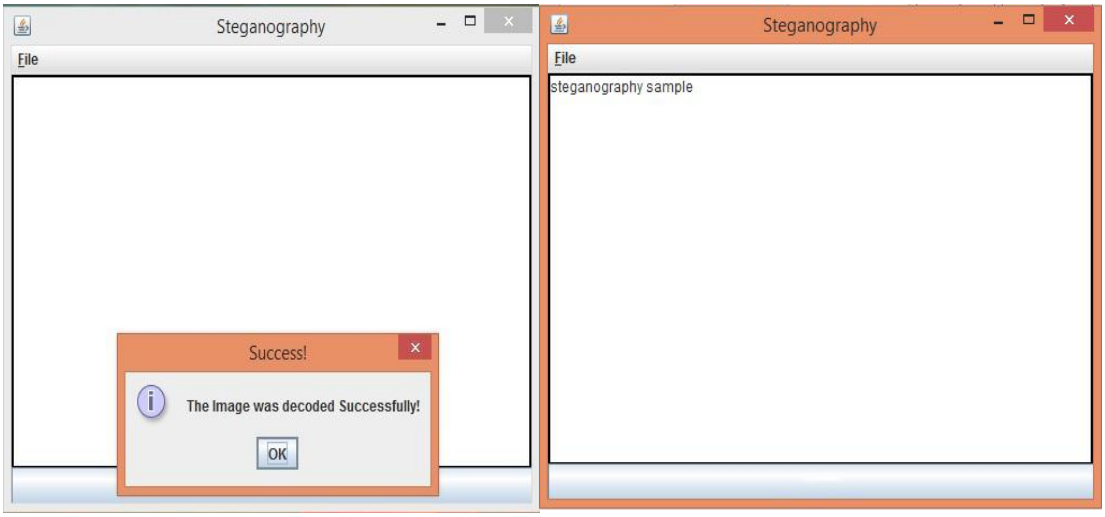

Fig. 7: Message Decode.

The Figure 4 gives the first client that logins into the chat application. The user logins giving the IP address andthe port number to connect to the server. The server accepts and connects if the id and password matches with thedata stored. Clients can also signup for a new account. The clients can chat and send messages through thewindow. Then the second client login into the chat application. The user logins giving the IP addressand the port number to connect to the server. The server accepts and connects if the id and password matches withthe data stored. The clients can view other clients who are logged in the application. Clients can also signup fora new account. The clients can chat and send messages through the window.

The Figure 5 gives the chat between the clients. The clients chat and send message to all the clients who arelogged into the application. When a client sends a message it is sent by encrypting it into an image file. Theimage file is decrypted at the end of the other client to retrieve the message.

The Figure 7 gives the decoding phase at the receiver side of the application. The receiver decodes the image to get the message sent by the sender and the message that was sent by the sender is decoded form the image file and the receiver canview the message. This process is done to explain the steganography process that is done.

Conclusion:

In this work, we have proposed a new system to communicate securely in a network using the concept of imagesteganography to hide data into an image for hidden communication. We printed out the enhancement of theimage steganography system using LSB approach to provide a means of secure communication. A steganography-key hasbeen applied to the system during embedment of the message into the cover image. The application proposedencodes the message at the sender side and transmits the steganography image to the receiver and at the receiver sidedecrypting to get back the message. By this way the message is sending in the image hidden and hencecommunicating in a secure manner. In future the work can be extended to support audio files and video files.

REFERENCES

Karthigai Seivi, G., Leon Mariadhasan and K.L. Shunmuganathan, 2012. ”Steganography Using Edge AdaptiveImage”, International Conference on Computing, Electronics and Electrical Technologies [ICCEET], pp: 1023-1027.

Monica Adriana D˘ag˘adit¸˘a,EmilIoan Slus¸anschi and R˘azvan Dobre, 2013. “Data Hiding UsingSteganography”, IEEE 12th International Symposium on Parallel and Distributed Computing, pp: 159-166.

Nadeem Akhtar, Shahbaaz Khan and Pragati Johri, 2014. “An Improved Inverted LSB Image Steganography”,International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT), pp: 49755.

Sudhir Goswami, Jyoti Goswami and Rajesh Mehra, 2014. “An Efficient Algorithm of Steganography Using PEGColored Image”, IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE2014),May09-11.

Sullivan, K., U. Madhow, S. Chandrasekaran and B.S. Manjunath, 2006. “Steganalysis for Markov Cover Data with Applications to Images,” IEEE Transactions on Information Forensics and Security, 1(2): 275 – 287.

Thangadurai, K. and G. Sudha Devi, 2014. “An analysis of LSB Based Image Steganography Techniques”,International Conference on Computer Communication and Informatics (*ICCCI* -2014), Jan. 03 – 05.