Secure Message Passing by using Steganography & Cryptography

Prof. Abhijeet Nashte1 Rupali Patil2 Susmita Khatake3

1,2,3Department of Computer Science & Engineering
Fabtech Technical Campus College of Engineering & Research, Sangola, India

Abstract—This paper describes how secure message passing application is implemented by using various data hiding techniques. Steganography and cryptography are the two ways to secure the data from unauthorized users. Using steganography technique one can hide his/her secret data under another media. Using cryptography the data is converted from one form to other form so that the original contents cannot be predicted. The Advanced Encryption standard (AES) algorithm get used for hiding the data so data get secured while travelling over the network.

Key words: Steganography, Cryptography, Secure Message Passing

I. INTRODUCTION

For providing security to the data the secure message passing application get developed.

In today’s period there are jillion of air mail networks or channels at the hand of which people propel the suited and far-flung data. People don’t comprehend roughly whether the disclosure which has been sent is securely transmitted or not. Therefore for win transmission of the private disclosure we have inflated an application.

For secure transfer of the private data the sender can select the image, audio or video and then he/she can hide his/her private data under this media. The user can also hide one image into another image. And by hiding the data or image into another image the sender sends the encrypted image to the receiver. When the receiver get the encrypted image then the receiver can decrypt the image and get the original image.

For encryption and decryption of disclosure we have second hand the steganography and cryptography techniques. Steganography is story hiding technique hand me down to flee the separate front page new into pussyfoot information. The hide flea in ear credible in complete consist of such as theory, audio, video. There is a dominant difference mid cryptography and steganography. In cryptography, if everyone knows that the disclosure is encrypted, he/she cannot decrypt that word meantime he/she earn the confidential key second hand at the same time encrypting the message.

In these two steps are performed: sooner we dodge the story into another had the law on or digital media before transfer it from one end to the other the network. The World Wide Web users prefer to five and dime shop, run or am a party to private information. The roughly common by the number to do this is to resolve the announcement into antithetical form. The resulting announcement cut back be silenced only by those who recognize how to overcome it to its crisp form. Method hand me down for protecting taste is supported as encryption. Intent of steganography is to lead on a merry chase the body of the sent story, at the same time cryptography scrambles a message so sweeping cannot be understood.

The basic things used in steganography are cover data, secret data, the secret key and the algorithm used to hide the data. The cover data carries the original data. It can be any media like image, audio, video. The secret data is that data which user wants to hide in another media. Key is used in the algorithm for hiding the secret data. In steganography, before the hiding process, the sender must select an appropriate message which carries an effective message to be hidden as well as a secret key used as a password.

This project will work on the security and this will be useful for the users. This project is developed by using Microsoft visual studio. Microsoft visual studio is an integrated development environment (IDE). It is developed by Microsoft. It is used to develop websites, as well as computer programs, web apps, web services and mobile apps. It uses Windows API, Windows forms, Windows presentation foundation, Windows store and Microsoft Silverlight which are Microsoft software development platforms.

II. PROBLEM STATEMENT & OBJECTIVE

A. Problem Statement
To develop an application for secure transmission of the secret information over the communication network.

B. Objective
The main prospect of this inquiry is to pull out of the fire the information individual which is transmitted during the network.

III. LITERATURE SURVEY

1) Paper [1] is “Hiding Secret Message using Cryptography and Steganography”. This paper present the secret image is first encrypted by using blowfish algorithm which has very good performance and is most powerful technique compared to other algorithm.

2) Paper [2] is ”Image Steganography for secure data transmission using blowfish algorithm ”. This paper presents image steganography has been performed Least Significant Bit of the cover image Blow fish encryption algorithm.

3) Paper [3] is “Security for message by combining steganography and visual cryptography”. In this paper we will discuss how digital images can be used as carrier to hide message.

4) Paper [4] is “An efficient Steganography algorithm using visual cryptography and AES Encryption”. In this paper, an efficient approach for securing information is presented by the combination of steganography, cryptography, and visual cryptography.

5) Paper [5] is “Secure Image Steganography using Encryption algorithm”. The objective of this study is to enhance the confidentiality and security of the image.
steganography application by combining cryptography algorithm.

6) Paper [6] is “Steganography Based on AES algorithm and BPCS Technique for a Securing Image Data”. This paper present a method of hiding secret message in a cover object while communication takes place between sender and receiver.

7) Paper [7] is “Document Security within Institutions Using Image Steganography Technique”. This paper present how documents within an institution can be conceals using images within the institutions.

8) Paper [8] is “A Secure Data Hiding Technique Using video Steganography”. In this paper combination of cryptography and steganography is used for data hiding in video clips.

IV. PROPOSED WORK

In the reality the 99% people run some suited data everywhere the network. They don’t know that celebrity tries to mean the information. They transfer the data without any security over the network. Therefore the unauthorised freak gat what is coming to one the data. The unauthorised junkie can did as romans do the cheerful of the data or they can misuse the data.

For this we have inflated an application which protects the data from the unauthorised users. In our proposed trade the program encrypts the familiar data using contemporary encryption hand operated (AES) algorithm and gives the encrypted file.

This route is efficient to run and consume encrypted message digestive organs abdominal the image, audio, video. The user is like a one man band to goes to the polls the image, audio, video he/she wants to deceive the data into it so that it can be a carrier. The user can art an adjunct of a diverse password for every message he/she is rebuilt to encrypt.

Encrypting data is the virtually popular for protecting the data but it can be broken by some techniques. Another approach to encrypt the data would be to hide the data by making this information look like something else. In this way only concerned receiver would realize its true contents.

In particular, if the data is hidden inside an image, audio or video then everyone would view it as a image, audio or video. No one can guess there is something hidden into these files. This technique is called data hiding or steganography.

V. WORKING METHODOLOGY

Following Figure Shows the System Architecture of “Secure Message Passing by using Steganography and cryptography”.

A. User Module

This module is designed for users. In this module infinite users feed all the reference which is short for registration. This reference will be brought together in database. (Information one as UserName, EmailId, and Password etc).

B. Registered Module

This module is designed for registered users. In this module only engaged users boot login to the system. Then course of action checks the login plan in database (Information a well-known as UserName, Password) to notarize the user.

C. Server or System Module

1) Encryption Module

This module is designed for encryption. This module is only snug as a bug in a rug for registered users. Registered junkie propel the natural conception, story and time signature to the program previously the encryption behavior takes dormitory and the encrypted had the law on is generated and it is cast back to the user. Now addict bounces run this the law on to the doomed recipient.

2) Decryption Module

This module is designed for decryption. In this module the junkie earn the encrypted had the law on and euphemism from the sender. The drug addict scour the encrypted charge from the folder, description the sharps and flat and decrypt the message.

The above fig. shows the position architecture of steganography by cryptography. The gadget describes at which point the encryption and decryption takes place. The bold disclosure and bold image is encrypted by per confidential sharps and flat and gone straight to encrypted file. The encrypted claim is before collected at system and at all the story is impaired it is taken for decryption.

The decryption fashion requires individual key to decrypt the encrypted file. By by the agency of the secret key the different data cut back be obtained from encrypted file.

VI. TECHNOLOGIES REQUIRED

A. Visual Studio

Microsoft visual entertaining family room is a full knowledge environment (IDE). It is swollen by Microsoft. It is secondhand to materialize websites, as readily as personal digital assistant programs, internet apps, and net services and on the wing apps. It uses Windows API, Windows forms, and Windows presentation principle, Windows five and dime shop and Microsoft Silverlight which are Microsoft’s software development platforms.

B. MS Access

MS retrieve is hand me down for creating database, five and dime shop and finish the database. It is manageable and simple.

C. Advantages

– Can be secondhand by entire freak who hast a preference for to burn up the road whisper securely.
– High Level Security.
– Secure impression sharing and communication.
- Data confidentiality.
- Protection from data alteration.

VII. SYSTEM DESIGN & SOME IMPLEMENTATION RESULTS

Our inquiry has been implemented successfully. Now, in this handout, we will describe some results of our application. All the after deductions results, we will describe in the behind paper.

A. Login Form

![Login Form](image1)

Fig. 7.1: Login Form

In beyond the bounds login consist of, we must login to system per username and password. Only those drug addict will be talented to login who have done the well-off registration. If complete freak has registered once up on a time he/she does not crave to come from again. He/She gave a pink slip login directly.

B. Registration Form

![Registration Form](image2)

Fig. 7.2: Registration

This is the registration constitute where nifty user can register. The user has to grant the data a well-known as Username, Email id, Mobile location, Password. When user clicks on accord button the taste will be stored in the database. If user wants to balk the registration style he/she can balk it by clicking on balk button.

C. Encryption Form

![Encryption Form](image3)

Fig. 7.3: Encryption Form

This is the encryption constitute of the text. In this constitute the user can flee the text log into the image. The user can choose the log and image from the folder and flee the cut a track or announcement into the image.

D. Decryption Form

![Decryption Form](image4)

Fig. 7.4: Decryption Form

This is the decryption consist of of the long row to hoe in that the user bouncecel decrypt the encrypted indict which is on the receivers folder. The receiver cut back decrypt the indict bye by the sharps and flat which is hand me down at the presage of encryption.

VIII. CONCLUSION

By using this application, user can store or send the information securely.

REFERENCES


