iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** IV **Month of publication:** April 2017

DOI: http://doi.org/10.22214/ijraset.2017.4244

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 5 Issue IV, April 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Image Steganography and Cryptography Using Three Level Password Security

Sahil Lotlikar[1], Ashish Gupta[2], Jayesh Thorat[3], Sandhya Kadam[4]
Computer Engineering, University of Mumbai

Abstract: ***Image steganography and cryptography using three level password security is used for transferring sensitive data from one user to other user. The main aim of the project is to provide the users a secure way that helps the users to send and receive sensitive and important data from one user to other user in the form of image .The sensitive data is in the form of text. There is an authentication system that validates user for accessing the system only when they have input correct password. The project involves three levels of user authentication. In this sender will have to first go through all the three stages of authentication. After going through all the stages the senders text will be encrypted using the cryptography algorithm .These encrypted text will be hidden inside the image. After getting this image he can transfer/send this image by using email or simple message to the receiver. The receiver also has to go through all the three stages of authentication and use decrypt to decrypt the image and get the message or information hidden inside the image .***
Keywords: Cryptography , Steganography , Security, Data hiding and Image Processing.

I. INTRODUCTION

Let's start our discussion with security first. As all of us know that during the recent years due to fast growth of internet security is becoming an issue for internet users. Cryptography , steganography are two favorite techniques used by developers for security reasons As cryptography is the process of encrypting and decrypting the data. Here data gets encrypted which sender wants to send to the receiving party and decrypted on the other side. Steganography is another technique which totally denies the existence of information in an image so there is no knowledge of existence of any message in image. Authentication is a process in which the credentials provided are compared to those on file in a database of authorized users' information on a local operating system or within an authentication server. If the credentials match, the process is completed and the user is granted authorization for access. Three level password authentication helps for securing the data from any attacker. The sender and receiver has to go to all the three stages of authentication for encrypting or decrypting the data.

II. PURPOSES

In this paper we are working on these objectives which will provide better results than the previous techniques.

A. To propose a new algorithm for transmitting the secret image over a network by combining the cryptography steganography techniques.
B. To implement the above algorithm on various picture format like (jpeg, png , gif, bmp).
C. Three level password authentication is used to provide the authentication to the sender and the receiver.

III. PROPOSED WORK

A. *Cryptography*
The Sender will enter the text that the sender wants to send to the Receiver. The text will be encrypted by using a set of algorithms. This Text will be further hide by using Steganography.

B. Image steganography
1) Sender's Part
a) Sender loads an image which he wants to send Then he enters the text
b) He sets the password for text and finally encrypts it
c) He saves the image and sends it across to receiver (Through email or any other way).

C. Receiver's Part

1) Receiver opens the image in the application.
2) Enter password which was used for encrypting (Password can be pre-decided or shared).
3) After typing the password press Decrypt.

Text will be shown as it was sent by the Sender

D. Authentication Levels in the System

1) *First Level:* The first level is a conventional password system i.e. text based password or a passphrase. Users would have to set a text password initially based on some specifications.
2) *Second Level:* The second level is a graphical password method where users have to set password based on some color combinations through RGB button combinations.
3) *Third Level:* The third level is a otp (one time password).The user has to press a button .After pressing the button he will receive a password on his e-mail .Than by using this password the user can log into third level.

IV. REVIEW OF EXISTING TECHNIQUES FOR INFORMATION HIDING

Several techniques have been proposed by researchers for securing electronic communication. In the research work of, the researchers proposed cryptography and steganography for securing data transfer using images as cover objects for steganography and key for the cryptography[1]. The performance of the proposed ISC (Image-Based Steganography and Cryptography) system was presented and the system was compared with F5 algorithm. Also, proposed method that described two steps for hiding secret information by using the public steganography based on matching method. The first step, finds the shared stegno-key between the two communication parties (Alice and Bob) over the networks by applying Diffie Hellman Key exchange protocol. The second step in the method is that, the sender uses the secret stegno-key to select pixels that it will be used to hide. Each selected pixel is then used to hide 8 bits binary information in their research proposed two approaches for secured image steganography using cryptographic techniques and type conversions. One of the methods shows how to secure the image by converting it into cipher text through s-DES algorithm using a secret key and conceal this text in another image using steganographic method. The second method shows a new way of hiding an image in another image by encrypting the image directly through S-DES algorithm using a key image and the data obtained is concealed in another image[2].

V. COMBINATION OF CRYPTOGRAPHY AND STEGANOGRAPHY

Steganography must not be confused with cryptography that involves transforming the message so as to make its meaning obscure to malicious people who intercept it. In this context, the definition of breaking the system is different. In cryptography, the system is broken when the attacker can read the secret message. Breaking a steganographic system needs the attacker to detect that steganography has been used and he is able to read the embedded message. steganography provides a means of secret communication, which cannot be removed without significantly altering the data in which it is embedded. In addition, the security of classical steganography system relies on secrecy of the data encoding system. Once the encoding system is known, the steganography system is defeated. However, it is always a good practice to use Cryptography and Steganography together for adding multiple layers of security. By combining, the data encryption can be done by a software and then embed the cipher text in an audio or any other media with the help of stegano key. The combination of these two methods will enhance the security of the data embedded. This combined chemistry will satisfy the requirements such as capacity, security and robustness for secure data transmission over an open channel. The figure below depicts the combination of cryptography and steganography.

VI. METHODOLOGY

A. Least Significant Bit (LSB)

A very popular methodology is the LSB (Least Significant Bit) algorithm, which replaces the least significant bit in some bytes of the cover file to hide a sequence of bytes containing the hidden data . LSB coding is the simplest way to embed information in a digital audio file by substituting the least significant bit of each sampling points with a binary message. In computing, the least significant bit (LSB) is the bit position in a binary integer giving the units value, that is, determining whether the number is even or odd. The LSB is sometimes referred to as the right-most bit, due to the convention in positional notation of writing less significant digit further to the right. It is analogous to the least significant digit of a decimal integer, which is the digit in the right-most position. In referencing specific bits within a binary number, it is common to assign each bit a bit number, ranging from zero

upwards to one less than the number of bits in the number. The least significant bits have the useful property of changing rapidly if the number changes even slightly. For example, if 1 (binary 00000001) is added to 3 (binary 00000011), the result will be 4 (binary 00000100) and three of the least significant bits will change (011 to 100). By contrast, the three most significant bits stay unchanged (000 to 000). Least significant bits are frequently employed in pseudorandom number generators checksums [3][4].

B. Encryption

During encryption, the user is allowed to enter a password/key in any combination of numbers, symbols and characters. The key contains set of characters, which are used to encrypt the message before encoding. The processes of encryption is handled by the algorithms ceaser-cipher, Transposition cipher and play-fair cipher algorithm.

C. Decryption

The user's password/key is supplied to decrypt the encrypted message in order to get the original message. The processes of decryption is handled by the algorithms ceaser-cipher, Transposition cipher and play-fair cipher algorithm.

VI. OUR SOLUTION

As mentioned in the introduction of this paper, it is essential that a data bearing image be statistically and visually identical to the original image in order to avoid detection by an attacker .This was the goal we kept in mind while designing our data hiding application.

VII. COMPARATIVE STUDY

The following table represents the comparative study for various algorithms.

A. Comparative Study of the Encryption Algorithms

Algorithms	Resources Consumption	Security	Throughput	Cryptanalysis Resistance	Tunability
Caesar Cipher	Low	Low	Low	Vulnerable as Caesar cipher can be easily broken	No
Transpositio n Cipher	Requires more Cpu cycles and memory	Medium	Low	Vulnerable as transposition can be easily detected by the cryptanalyst by doing a frequency count	No
Play Fair Cipher	Requires effective resource consumption	Medium	Medium	Vulnerable as Obtaining the key is relatively straightforward if both plaintext and cipher text are known	No
Proposed Algorithm	Very High	Very High	Very High	Very High as it is difficult to guess the text	Yes

B. Comparative study for Different images used in Steganography.

	PNG	JPEG	GIF	BMP
Efficiency on reasonable data	High	Medium	Medium	High
Data Capacity	Medium	Low	Low	High
Detection (Steganalysis)	Medium	Medium	Low	Low
Resultant Image Distortion	Medium	Medium	Medium	High
Robustness against Image Manipulation	Medium	Medium	Low	Low
Robustness against statistical attack	Medium	High	Low	Low
Payload Capacity	Medium	Medium	Medium	High
Independent File Format	Low	Low	Low	Low
Suspicion on the basis of File created	Low	Low	Low	Low
Invisibility	Medium	High	Medium	High

Volume 5 Issue IV, April 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

VIII. IMPLEMENTATION

Fig 1. Login

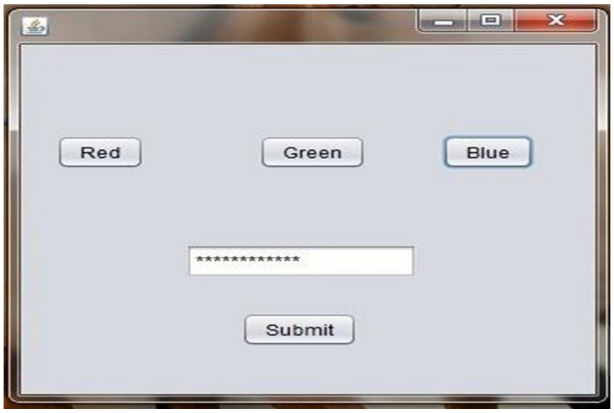


Fig 2. RGB password

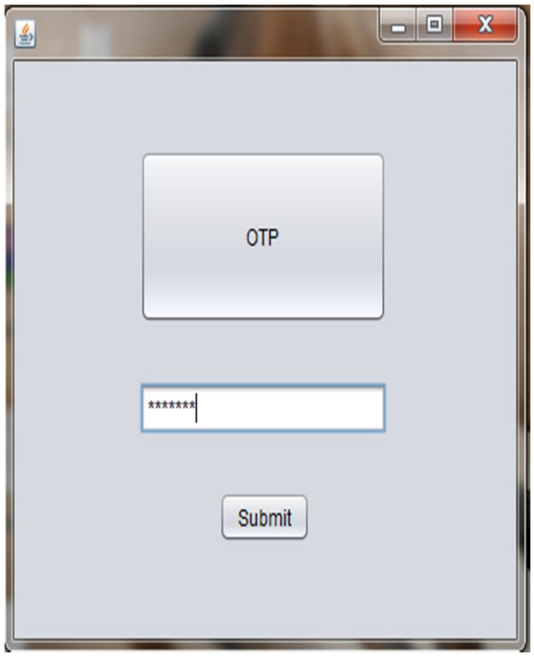


Fig 3. Otp password

Volume 5 Issue IV, April 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

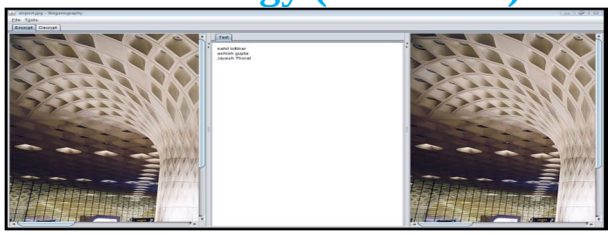


Fig 4.1. Steganography Encryption

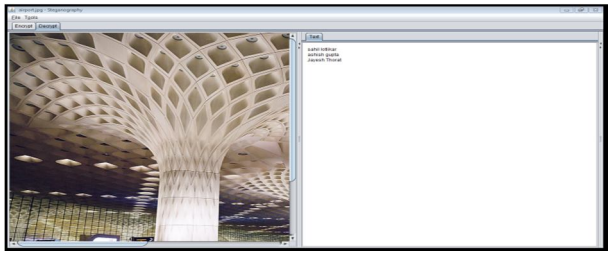


Fig 4.2. Steganography Decryption

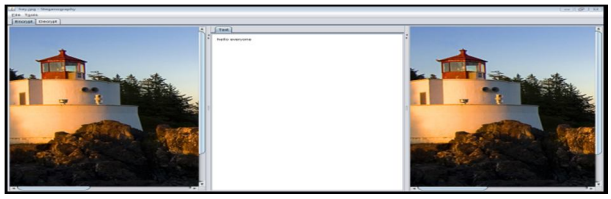


Fig 5.1. Steganography Encryption

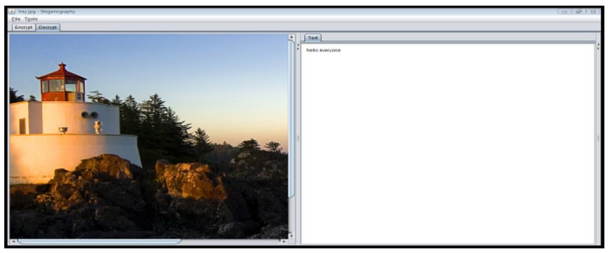


Fig 5.2. Steganography Decryption

IX. CONCLUSION

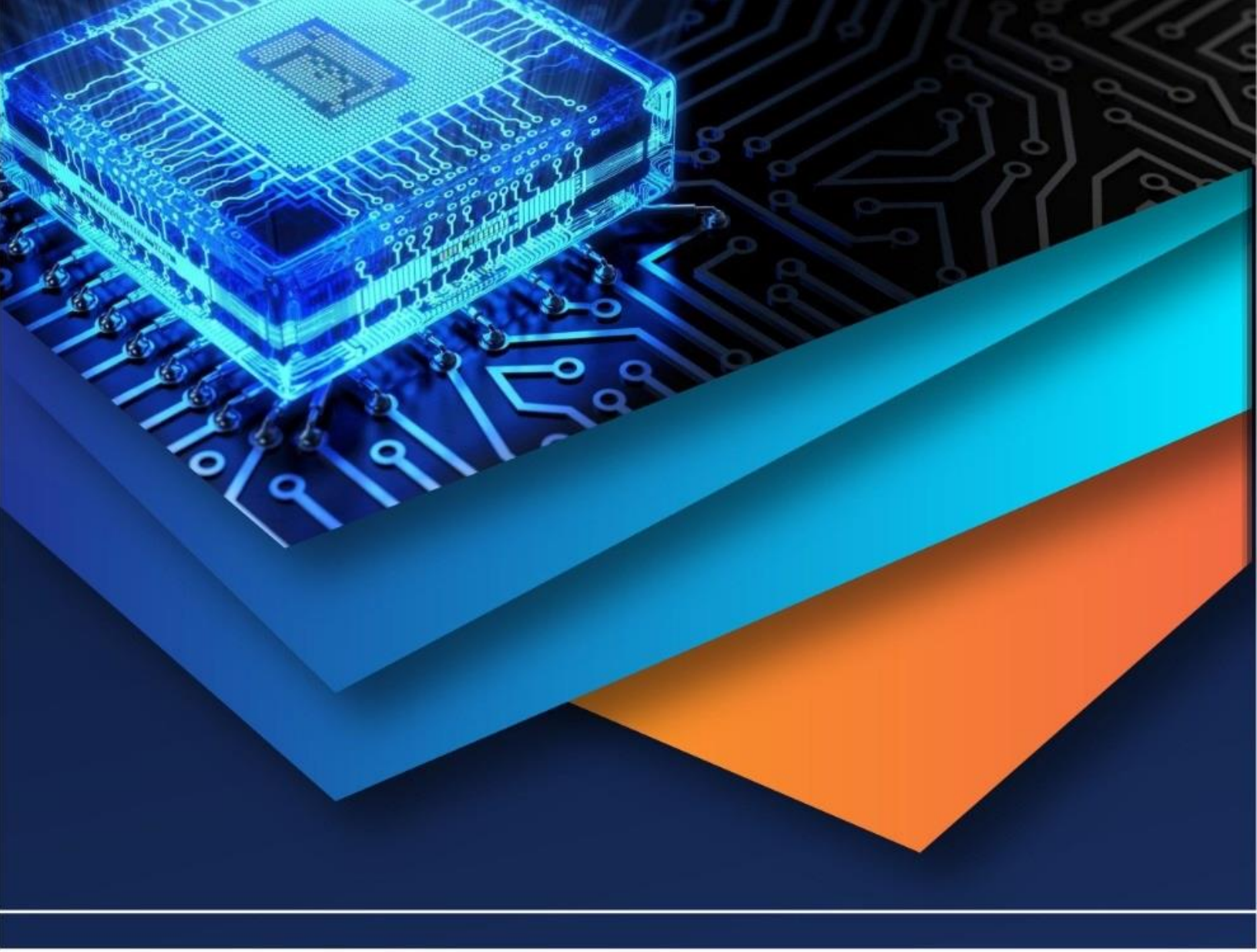
We believe that steganography when combined with encryption provides a secure means of secret communication between two parties. Our application, with its image analysis and security capabilities is a significant improvement on current steganography tools.

X. ACKNOWLEDGEMENT

The project has been supported by Department of Computer Engineering, K.J.Somaiya Institute of Engineering and Information Technology and the authors would like to thank our guide Prof. Sandhya Kadam, Dept. of Computer Engineering, K.J. Somaiya Institute of Engineering and Information Technology for helping in this project.

REFERENCES

[1] Rupesh Gupta , Dr .Tanu Preet Singh"New Proposed Practice for Secure Image Combing Cryptography Steganography and Watermarking based on Various Parameters" 2014 International Conference on Contemporary Computing and Informatics (IC3I).
[2] Mamta Juneja, Parvinder Singh Sandhu"Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption" 2009 International Conference on Advances in Recent Technologies in Communication and Computing.
[3] International Journal of Applied Information Systems "Efficient Data Hiding System using Cryptography and Steganography".
[4] ICTACT JOURNAL ON IMAGE AND VIDEO PROCESSING, FEBRUARY 2015 "Pixel pattern based steganography on images".
[5] S.Lyu and H. Farid, "Steganography using higher order image statistics, "IEEE Trans. Inf. Forens. Secure. 2006.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY