Hybrid Security Approach for Multilevel Security in Data Communication

Padmashri Ramesh
USN: 1BM13IS04, Dept. of ISE, BMS College of Engineering, Bangalore, India

ABSTRACT

In the age of multiple, growing connections and online transfers of data across networks, it has become increasingly necessary to secure sensitive data. To ensure that the access to information is private and only by authorized persons, it must be secured over the transmissions. A Hybrid Security Approach for multi-level data security will be beneficial in solving the existing problems of keeping data safe and secure over its transfers across networks - involving countless computer systems and users, a basic achievement of which is the deliverable of this project. By combining the functionalities of encryption from Cryptography and concealing of the information from Steganography, powerful security can be established for the data. A strong Cryptographic algorithm - AES (Advanced Encryption Standard) and an appropriate Stenographic method – LSB (Least Significant Bit) are identified and they are implemented to work together to raise the potent of the information security setup. The confidential information required to be secure is encrypted by the AES algorithm, and this encrypted data is concealed in an image by the Least Significant Bit algorithm of Steganography. This project proposes multi-level data security, which can be integrated into networks and online transactions in the world of Net Banking for tighter security and safer transactions and transmissions of sensitive data. It can also prove to be helpful in advancing crypto-economics and cryptocurrencies through other forms of Information Hiding as well.

Keywords— *Security in data communication, secure and safe transfers over network, Stenographic method for data communication*

---

1. INTRODUCTION

Information is can be perceived as a stimuli that has meaning in some context for its receiver when communicated from the sender. When information is submitted and stored in a system, such as a computer, it is generally referred to as "data". After processing (like, formatting and printing), output data is considered as information. The challenge with Data Security is securing sensitive data over transfers. This is crucial for the protection of the data from malicious third parties. Cryptography is the methodology most often used to tackle this.

Cryptography is used to try to keep information safe by converting it via encoding. It can be of two types – Symmetric Key and Asymmetric Key Cryptography.

Symmetric/Shared Key Cryptography: The same key is used for both encryption and decryption.

Asymmetric/Public Key Cryptography: Different keys are used for encryption and decryption.

The important functions of Cryptography are:

Privacy/confidentiality- Ensuring that no one can read/access the message except the intended receiver.

Authentication - The process of proving one's identity, including sender, receiver and the communication channel.

Integrity- Assuring the destination user that the received message has not been altered in any way from the original transmitted message.

Non-repudiation- A mechanism to prove that the sender only really sent the transmitted message.

Key exchange- The mechanism by which crypto keys are shared between the sender and the receiver. This is like the protection guarantee that ensures that the sender and receiver can access the intended secret message for updating, modifying and transferring purposes.

There are 2 types of Cryptography :

- Symmetric Key Cryptography
- Asymmetric Key Cryptography

When describing Cryptographic mechanisms and their explanations with their working, the two communicating entities will be called Alice and Bob as this is the usual nomenclature in the field of Cryptography. This eases the task of identifying the sender and receiver. If there is a third and fourth party to the communication, they will be referred to as Carol and Dave, respectively. An eavesdropper, Eve is included, who has attacked the channel and has read-only access to data. She cannot modify it during its transfer or affect its transfer.
Cryptography, in normal usage, is most closely associated with the development and the creation of the mathematical algorithms that will be applied to encrypt and decrypt messages. Cryptanalysis, or also, crypto-analysis is the science of analysing and breaking the Cryptographic encryption schemes. It comes from the Greek word kryptós for hidden, and analýein, that means to loosen or to untie. It is the science of analysing information systems for a study of the hidden aspects of the systems. It is used to breach/hijack cryptographic security systems and gain access to the contents of encrypted messages, even and especially when the cryptographic key or code is unknown.
Steganography is the art and science of hiding information by embedding messages within other, seemingly harmless messages. Steganography works by replacing bits of useless or unused detain regular computer files (such as graphics, sound, text, HTML, or even floppy disks) with bits of different, invisible information. This hidden information can be plain text, cipher text, or even images.
One use of steganography includes watermarking which hides copyright information within a watermark by overlaying files not easily detected by the naked eye. This prevents fraudulent actions and gives copyright protected media extra protection.
Uses also include authentication of content, helping to solve ownership disputes and preventing illegal copying, modification or distribution of sensitive content. Also, it can be used along with other methods and tools to provide explanatory information in images like a doctor's notes in a patient's X-Ray image, tiny yellow dots in a printer's output with the date and time stamp and basically, to also hide the existence of sensitive files on storage media.

2. LITERATURE SURVEY

A few of the research papers, reference texts and other material consulted along with the conclusions in line with the scope of the work of this project are described with their analysis and understanding as follows:
Firstly, it is important to understand the basic working of Cryptography. Encryption and decryption schemes, how the keys are created, saved and sent and in what form the message is ultimately sent and received between the users. This text is a reliable source of information in this regard and explains all that there is to know about Cryptographic schemes. Uses, applications in varied fields, working and importance are all in rich detail. It also describes numerous Cryptographic techniques with algorithms and design. Key distribution algorithms and stream and block ciphers are written about adequately. However, these are found to be slightly beyond the scope of this project and not found to be necessary for in-depth understanding.

The Steganographic method used here is the Least Significant Bit substitution method. This has been found to be the most commonly used technique to hide data in images. The hardware part of this paper proposal is not necessary in view of the Hybrid Security Model as a software implementation is desired.

But, this algorithm has been proven to be weak against security attacks and eavesdropping instances. It is one of the oldest Cryptographic algorithms and was developed by the acclaimed security expert, Bruce Schenier. It is different from AES in the sense that it works on data blocks of 64 bits. It is found to work faster than AES of 256-bit keys, but the security achieved is not significant in comparison.

The usage of the Least Significant Bit Algorithm can be used to hide textual data into an image cover file. It specifies the Peak Signal Noise Ratio encountered as a result of this information hiding and compares the Stego image with the original and shows no visible difference. The Mean Square Error is another parameter that is used to check if the Stegano media, in this case- Stego image, is significantly different from the Cover Image. It is found that raw Least Significant Bit algorithm is a relatively common technique to embed data bits like, text, into cover media, like images and send the Stego image produced to the intended recipient. The receiver must

first analyse the data received and understand it to be a stego image. Then, the bits of text must be extracted from the last/ least significant bits of the image pixels and thus, the plaintext of the secret message is obtained.
This paper proposes a C+S method that uses Blowfish algorithm for encryption. Therein lays its con as this Cryptographic algorithm is weak in today's times and does not live up to the security requirements. It can be broken quite easily and quickly without much computational difficulty. LSB method is used for data hiding. Further, Discrete Haar Wavelet Transform is used to split the Stegano image into frequency bands and sent. Inverse Haar Wavelet Transform is used at the receiver's end to reconstruct the Stego image and retrieve and decrypt cipher text. This is a very complex method and does not enhance security significantly for its computational complexity.

3. DESIGN

Before the necessary figures of System Architecture, Sequence Diagram and Use case diagrams are specified, it is important to understand the uniqueness of this project.

This project aims to provide a Hybrid Security Model for Multilevel Security in Data Communication and delivers. The custom made security solution, as discussed previously is built on a strong C+S model.

Along with the Rjindael algorithm for encryption and the Least Significant Bit technique for hiding the ciphertext in the cover image, there is an added security feature. It is Pixel Value Histogram analysis for determining where to embed the ciphertext in the image. Existing methods use Pixel Value Differencing or Image Edge estimation or grayscale analysis. However, they are only moderately secure.

The proposal of this project that it ultimately implements is an enhancement of the security feature in the form of Custom Histogram Pixel Analysis, which works on the cover image chosen to embed the ciphertext bits into it by LSB method and produce the Stegano image. The working is as follows:

Figuring out which pixels have highest intensity average of their Red, Green and Blue bytes and taking that count of pixels and hiding the ciphertext in order by replacing the last 2 or the 2 least significant bits of these pixel bytes in the cover image to produce the Stegano image which is transferred.

4. SYSTEM ARCHITECTURE

System architecture is a discipline followed to represent and control objects that exist or are to be created, called "systems", in a manner that supports reasoning and understanding about the structural and functional properties of these objects or systems.

In this project, cover image and secret text are the inputs. The process of data hiding produces the necessary Stegano image. It is used with the Original cover image for the extraction and decryption process, after which the plaintext of secret data is obtained.

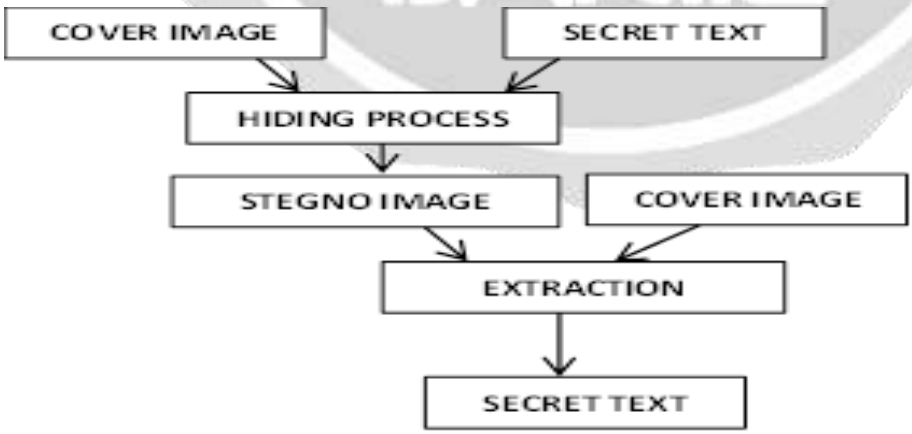


Fig-1 : System Architecture

A. Data Flow Diagram

A Data Flow Diagram (DFD) is a diagrammatical representation of the way in which the data flows through an information system. It models the processing aspects as well.

Above Level 0 DFD shows the contextual analysis of the project. It gives an overview of the security solution's working and gives a bird's eye view of the manner in which the data flows through the project system.
This shows the flow of data between user and user, admin and user and also the various processing inputs and outputs at each stage. The major process occurring here is that of Data hiding, i.e., how the data is handled between users and the admin.\

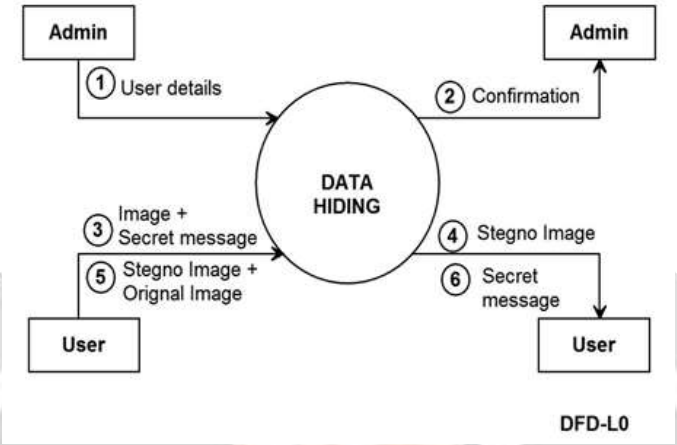


Fig-2: Data Flow Diagram Level 0

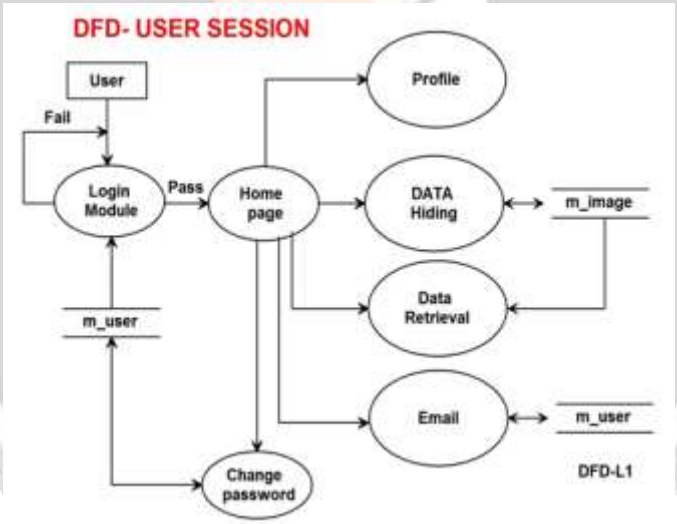


Fig.-3: User Session DFD Level 1

This diagram of Data Flow is at Level 1. It shows the basic users, components in use and the process underway. The way data flows through is determined by the condition checked at modules where necessary. Interacting entities here are the m_image which may be the cover image or the Stegano image, the m_user who may be admin or user and some of the processes like login, data hiding, data retrieval and sending/receiving email.

The user may attempt to login and if failed, try again. On successful login, the homepage of the security setup is shown. This is a private group and only authorised users may access it. User may choose to check profile and edit. Data hiding involves choosing an image and entering the secret text to be hidden into it after some alterations. User can email the Stegano image to another user via email. User may choose to retrieve data from previously received image by selecting the received Stegano image. User then logs out after desired operations are completed.

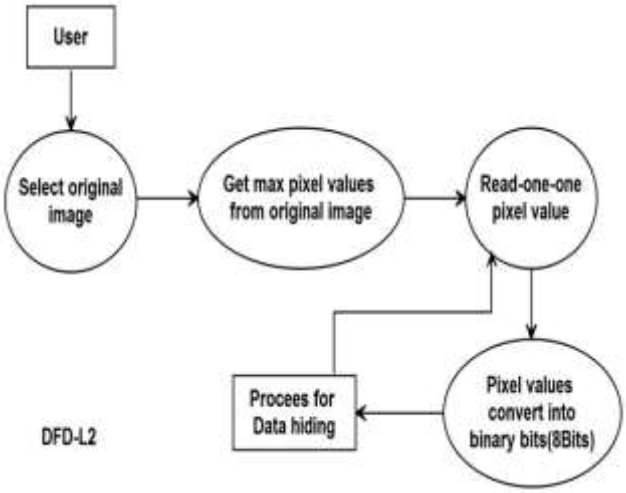


Fig.-4: Count and Pixel Selection DFD Level 2

This is a Level 2 Data Flow Diagram. It shows the way in which the Pixel Analysis is done for the images before embedding the ciphertext bits in the Cover Image in case of user being sender of information. It is for before the extraction of ciphertext from the Stegano image if the user is the receiver.

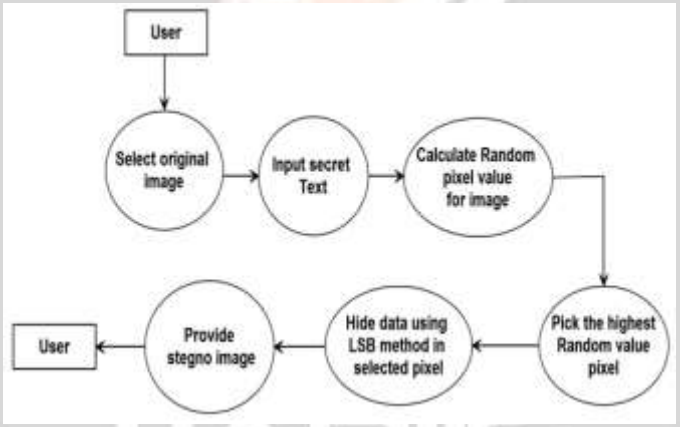


Fig.- 5: Data Hiding DFD Level 3

This is the most detailed Data Flow Diagram and is at Level 3. The first one is for the Data Hiding process. It shows how a user selects a cover image and inputs the secret text that is to be sent securely and confidentially. The Histogram is automatically drawn up and the highest intensity average along with the count of the pixels is determined. These are the pixels where the ciphertext bits will be embedded into. The LSB method is altered for usage and the ciphertext is stored in the last two bits of the pixels chosen in the order by 2 bits. Stego image is obtained and displayed to the user (sender) who may choose to send it via email after downloading the Stegano image.

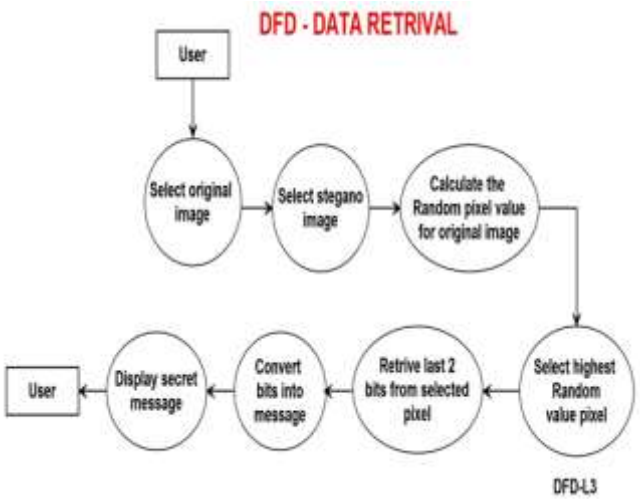


Fig.-6: Data Retrieval Process

This is the next part of the Level 3 DFD. It shows how a user who has received the Stegano image obtains the original secret text embedded in it. First, the original cover image and the received Stegano image are selected. The Pixel Value Histogram analysis is done for the original image to determine how many pixels and the position of these pixels that have the ciphertext embedded in them. Next, these are chosen correspondingly in the Stegano image. Compared and extracted the last two bits of the pixel bits. These are taken in order for the length of the embedded ciphertext and then decrypted using the Inverse AES cipher algorithm. After successful extraction and decrypting, the secret text is obtained.

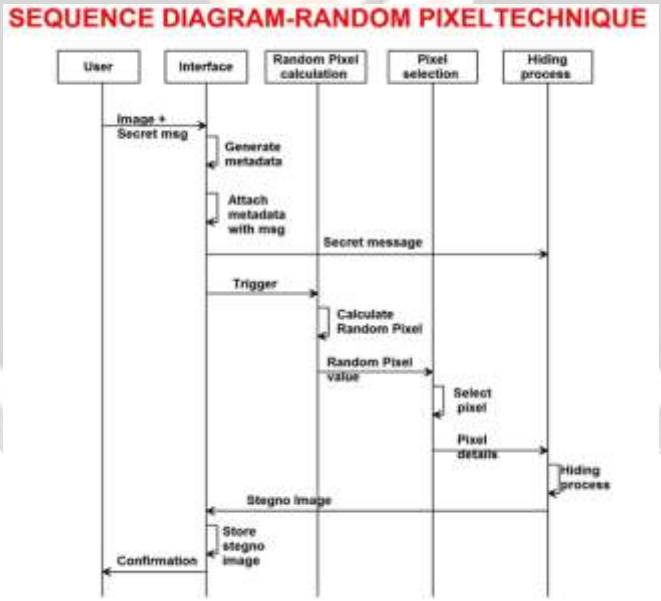


Fig.-7 : Sequence Diagram

A sequence diagram is an aspect of the Unified Modelling Language (UML) and is a notation of operations with lifetimes and durations. It shows the way different processes operate and communicate with each other via objects. Their lifetimes and durations are represented by the straight line and boxes on the line respectively. Here, the project is entirely denoted by this sequence diagram that shows the interactions between the user, who may be admin/ member user, the Hybrid Security System interface along with the hiding and retrieval processes.

5. IMPLEMENTATION

The implementation of this project includes a few of the following modules:

- Validating the usage of AES because of its supremacy over other existing Cryptographic algorithms.
- The analysis of different Steganographic tools to find one that works best with AES to determine a Steganographic module.
- Running the code in JavaScript and finding the feasibility of the methods.
- If found to be compatible, the C+S model of Rjindael + LSB is finalised for use.
- Enhancement in the form of Pixel Value Histogram analysis is added.
- Integration of the C+S modules with the security enhancement feature.
- Testing of different cases.
- Modifications and enhancements, if necessary, based on challenges encountered.

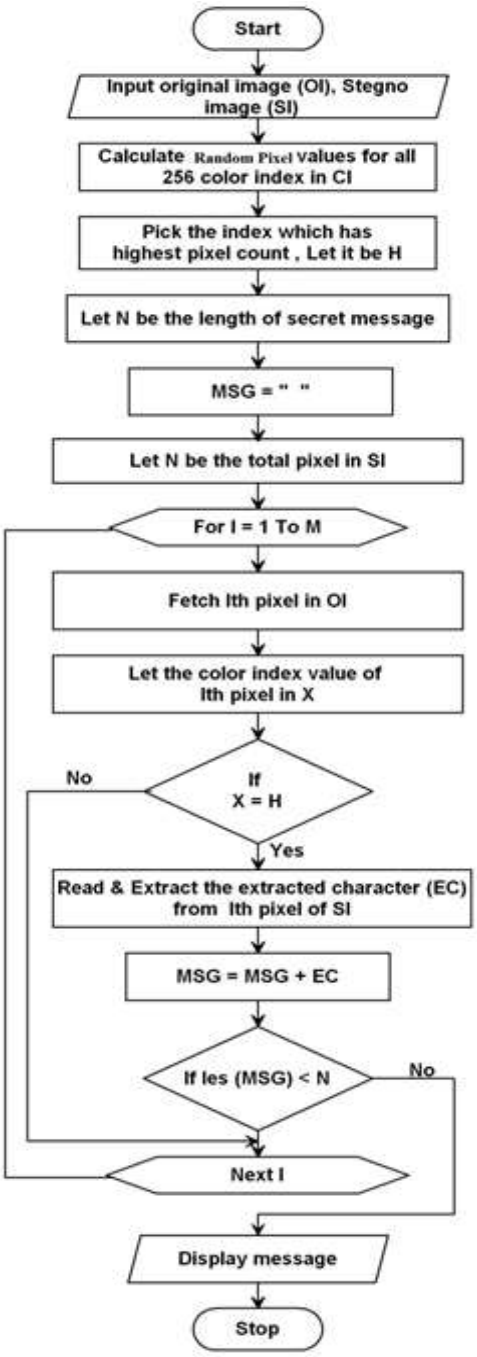


Fig-8: System Flow Chart

6. RESULTS

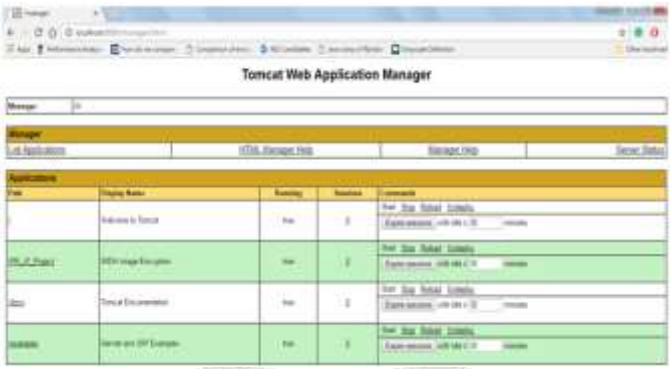


Fig.-9: System Flow Chart

Fig.-10: User Login

Fig-11: Home Page

Fig-12: User details

Fig-13: Edit User details

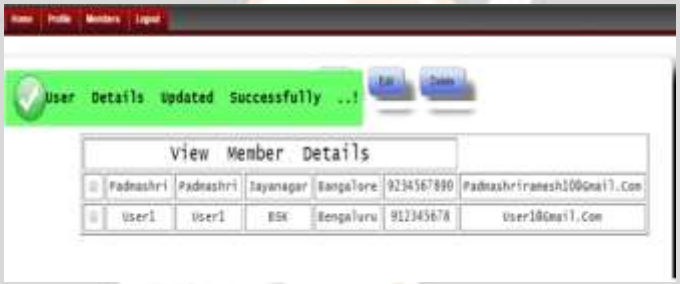
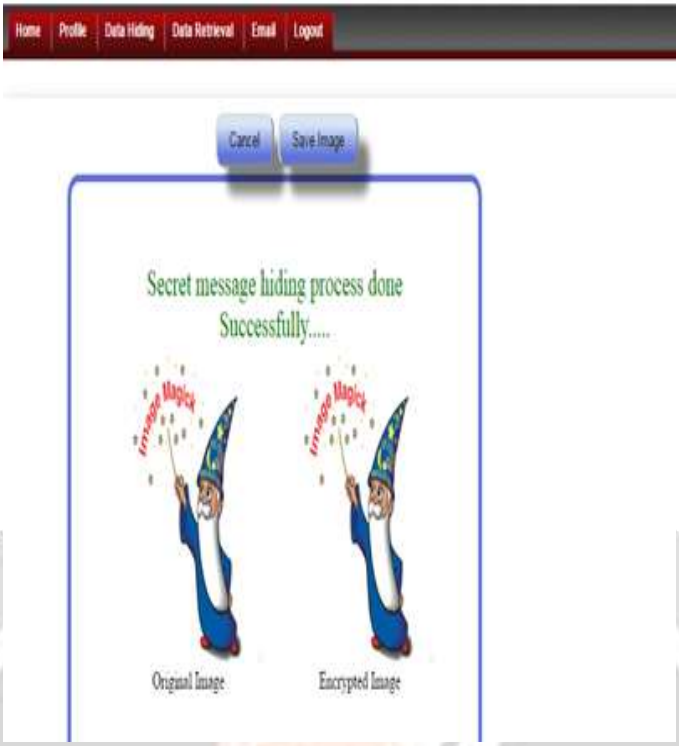
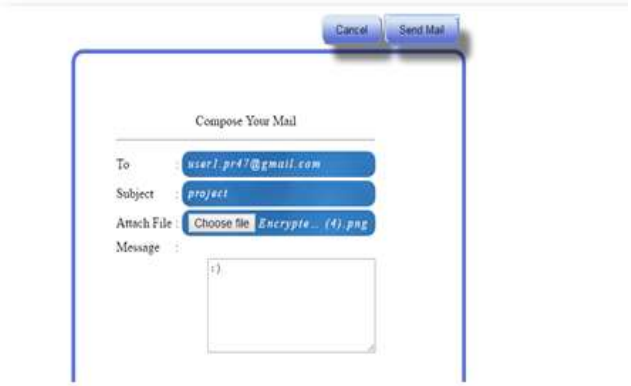


Fig-14 : Update Successful

Fig-15: Unauthorized login is prevented

Fig-16: Unauthorized login is prevented


Home
Profile
Data Hiding
Data Retrieval
Email
Logout
Cancel
Save Image
Secret message hiding process done Successfully.....
Original Image
Encrypted Image



Sending email can be seen in the console-

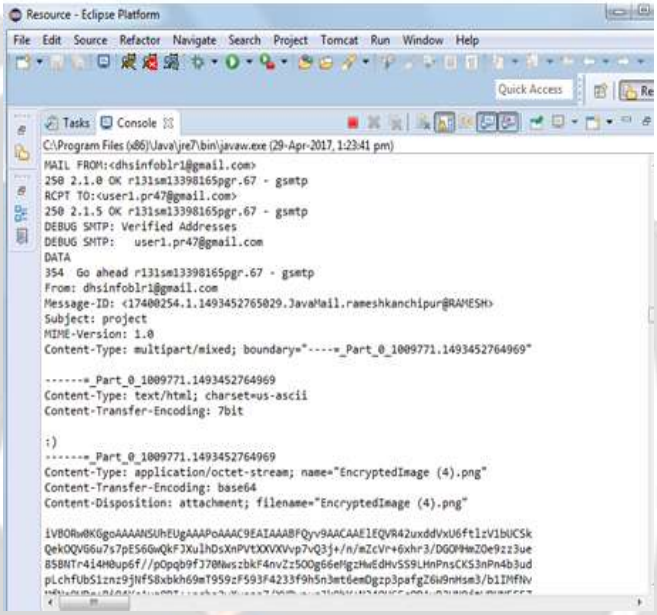


Fig. 17 Process Successful

Fig. 18 Email to the user

ACKNOWLEDGEMENT

I am grateful to Prof. Preetha S , Assistant Professor , Dept. of Information Science & Engineering , BMSCE for giving her constant support to complete the project.

REFERENCES

[1] William Stallings, “Cryptography and Network Security: Principles and Practice”, edn. 6

[2] Pallavi H. Dixit, Kamalesh B. Waskar, and Uttam L. Bombale, “Multilevel Network Security Combining Cryptography and Steganography on ARM Platform.” Journal of Embedded Systems, vol. 3, no. 1 (2015): 11-15. doi: 10.12691/jes-3-1-2..

[3] Chi-Kwong Chan, “Hiding data in images by simple LSB substitution”, L.M. Cheng Department of Computer Engineering and Information Technology, City University of Hong Kong, Hong Kong.

[4] Nani Koduri, “Information Security through Image Steganography using Least Significant Bit Algorithm”, Department of Information Technology, University of East London.

[5] Rashmi. J, Bharati. G, "A Wavelet Transform Based Secure Data Transfer Using Blowfish Algorithm", IJCSMC, Vol. 3, Issue. 2, February 2014, pg.794 – 803.

[6] Md. Khalid Imam Rahmani, Kamiya Arora and Naina Pal, "A Crypto-Steganography: A Survey", IJACSA, International Journal of Advanced Computer Science and Applications, Vol. 5, No. 7, 2014.

[7] Shraddha Dulera, Devesh Jinwala and Aroop Dasgupta, "Experimenting with the Novel Approaches in Text Steganography", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011.

[8] P Sumathi, G. Umamaheshwari and T. Santanam, "A Study of Various Steganographic Techniques Used for Information Hiding", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.4, No.6, December 2013, 10.5121/ijcses.2013.46029.

[9] H. Motameni, M. Norouzi, M. Jahandar, and A. Hatami, "Labeling Method in Steganography", International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol:1, No:6, 2007.

[10] Mr. Falesh M. Shelke, Miss. Ashwini A. Dongre and Mr. Pravin D. Soni, "Comparison of different techniques for Steganography in images", International Journal of Application or Innovation in Engineering & Management (IJAIEM), Vol. 3, Issue 2, February 2014, ISSN 2319 – 4847.

[11] N. Provos and P. Honeyman, "Hide and seek: An introduction to Steganography", IEEE Security Privacy, May/June 2013, vol. 1, no. 3, pp. 32-44.