IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 6, June 2020

Only-Red Steganography using Reversible Texture Synthesis

Manish Y M[1], Kavya K[2]

BE, Department of ISE, BNMIT, Bangalore, India[1,2]

Abstract: Image Steganography is the technique of hiding data / information of interest within an image. Image Steganography is critical in hiding the information to prevent the intruders from stealing and is intended to be read or processed only by the intended receiver. In our assignment we use JPEG or JPG images for Steganography regardless of whether it is digital or analog. Efforts have been put to create a unique GUI dashboard to distinguishably allow admin, user and new registrations to communicate using the same. An effort is made to upload images that carry different pixel intensities to avoid repetition of stego images that may occur due to use of same image and repetitive text / data. The user is given enough freedom to select or edit a key of his own. We have followed diagonal pixel selection technique. SHA algorithm is used to check the integrity of the system. The ever increasing network transmission rate accelerates this technique which is versatile approach having attained increased payload capacity.

Keywords: Image Steganography, JPEG or JPG images, create a unique GUI dashboard, stego images, diagonal pixel selection technique, SHA algorithm, integrity, and LSB algorithm.

I. INTRODUCTION

Two or three decades ago, cryptography meant random shuffling of given data or information to be transmitted. With the advancement in technology and processing techniques steganography methods have gained popularity. Figure 1 shows the types of steganography methods (based on hiding of info) in existence. Image steganography is a technique of hiding important information within an image and can only be understood by a receiver to whom the message was intended to be sent, eliminating intruders from extracting the SECRET / PRIVATE information. With the very increasing dataflow speed, a technique once an expensive affair has open up and with new techniques with accuracies near to triple digit. Least significant bit (LSB) method suits well for our assignment. In LSB substitution method, secret data is hidden in the least bit of each byte of the container data. LSB embedding can even be used for embedding a hidden message into the color values of RGB bit map data and into the frequency coefficients of a JPEG image. It can also be applied to a variety of data formats or types. Steganography hides the very existence of a message so that it attracts no suspicion at all. The cover image may not be of any significance and would be very confusing to an intruder.

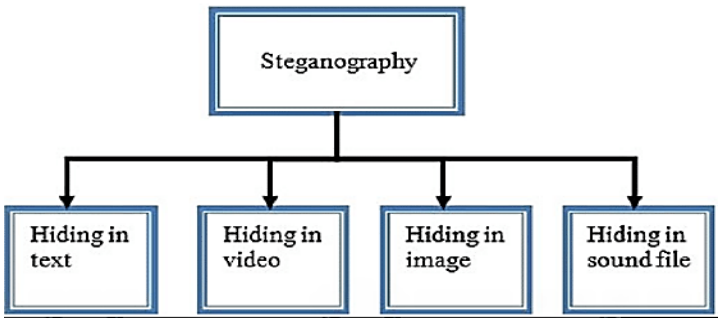

Figure 1 shows the types of steganography methods in existence.

II. MOTIVATION

Steganography hides the very existence of information / given message so that if successful it generally attracts no suspicion at all. Using steganography technique, information can be hidden in carriers such as audio files, images, text files and videos. Major advantages of Image Steganography have motivated us to take up this assignment. Firstly, since the texture synthesis can synthesize an arbitrary size of texture images, the embedding capacity which our scheme offers is proportional to the size of the stego texture image. Secondly, a steganalytic algorithm is not likely to defeat this steganographic approach since the stego texture image is composed of a source texture rather than by modifying the existing image contents. Third, the reversible capability inherited from our scheme provides functionality to recover

the source texture. Since the recovered source texture is exactly the same as the original source texture, it can be employed to proceed onto the second round of secret messages for steganography if needed.

III. PROBLEM STATEMENT

In this paper, we propose a novel approach for steganography using reversible texture synthesis. A texture synthesis process re-samples a small texture image with a similar local appearance and arbitrary size. We weave the texture synthesis process into steganography concealing secret messages as well as the source texture. In particular, in contrast to using an existing cover image to hide messages, our algorithm conceals the source texture image and embeds secret messages through the process of textures synthesis. This allows us to extract the secret messages and the source texture from a stego synthetic texture. A GUI to be created to easily interact with the machine and privileges to be considered (admin, user and new registrations). Provision to be made for selecting the cover image or uploading the same and the key.

IV. SOFTWARE REQUIREMENTS SPECIFICATION

A. Functional Requirements

A functional requirement defines a function of a system or its components, where a function is described as a specification of behaviour between outputs and inputs. It involves technical details, data manipulation and processing and other specific functionality that define what a system is supposed to accomplish.

- Image file in the form of JPEG.
- The text to be transmitted securely in digital format.
- The bit stream to be embedded onto a cover image or a stego object along with a stego key (known by both sender and receiver)
- Decryption of the information at the receiver end to obtain original data.

B. Non-Functional Requirements

Non-functional requirements define certain parameters such as usability, reliability, performance, scalability, portability, reusability and flexibility of the system even at its critical stages of functioning.

- Usability-Simple is the key here. The system must be simple that people like to use it, but not to complex that people avoid using it. The user must be familiar with the user interfaces and should not have problems in migrating to a new system with a new environment. The menus, buttons and dialog boxes should be named in a manner that they provide clear understanding of the functionality. Several users are going to use the system simultaneously, so the usability of the system should not get affected with respect to individual users.
- Reliability- The system should be trustworthy and reliable in providing the functionalities. Once a user has made changes, the changes must be made visible by the systems. The changes made by the programmer should be visible both to the project leader as well as the test engineer.
- Performance- The system is going to be used by many employees simultaneously. Since the system will be hosted on a single web server with a single database server in the background, performance becomes a major concern. The system should not succumb when many users would be using it simultaneously. It should allow fast accessibility to all of its users. For example, if two engineers are simultaneously trying to report the presence of a bug, then there should not be any inconsistency while doing so.
- Scalability- The system should be scalable enough to add new functionalities at a later stage. There should be a common channel, which can accommodate the new functionalities.
- Reusability- The system should be divided into such modules that it could be used as part of another system without requiring much of work.

V. SYSTEM DESIGN

A. The Encoding Process- The steganography technique used is LSB coding. The offset of the image is retrieved from its header. That offset is left as it is to preserve the integrity of the header, and from the next byte, we start our encoding process. For encoding, we first take the input carrier file i.e. an image file and then direct the user to the selection of the text file.

B. Creation of User Space- User Space is created for preserving the original file, so that all the modifications are done in the user space. In the object of Buffered Image, using ImageIO.read method we take the original image. Using create Graphics and draw Rendered Image method of Graphics class, we create our user space in Buffered Image object. The text file is taken as input and separated in stream of bytes. Now, each bit of these bytes is encoded in the LSB of each next pixel. And, finally we get the final image that contains the encoded message and it is saved.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 9, Issue 6, June 2020

C. The Decoding Process The offset of the image is retrieved from its header. Create the user space using the same process as in the Encoding. Using getRaster() and getDataBuffer() methods of Writable Raster and DataBufferByte classes.

As shown in this figure 1 we first consider the source image and the secret key. After selecting the diagonal pixel parity matrix, we apply the secret key to this diagonal. Later we embed the secret message in the red region of the image matrix diagonal using a embedding algorithm and thus a stego image is produced. The extraction process at the receiver end requires the stego image to be taken as input as well as the hash file, which basically consists of hash of the secret message computed beforehand and the secret key. This hash file is obtained, from which the hash of the message is extracted. According to figure 2 an extraction algorithm is applied on the image which reverses the encryption process thus retrieving the secret message. If the hash of this secret message matches to that of the hash extracted, then the data integrity is maintained and the secret message is successfully obtained.

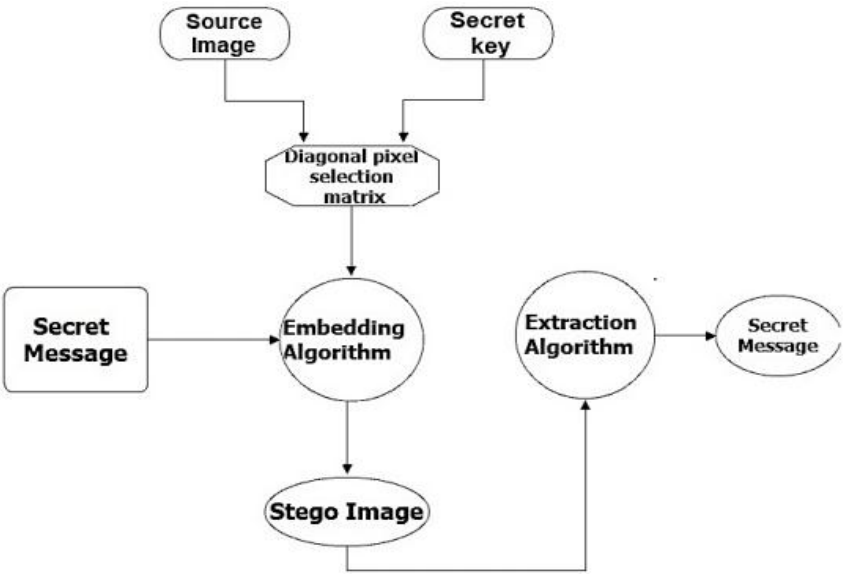

Figure 1 shows the Architectural design of Image steganography.

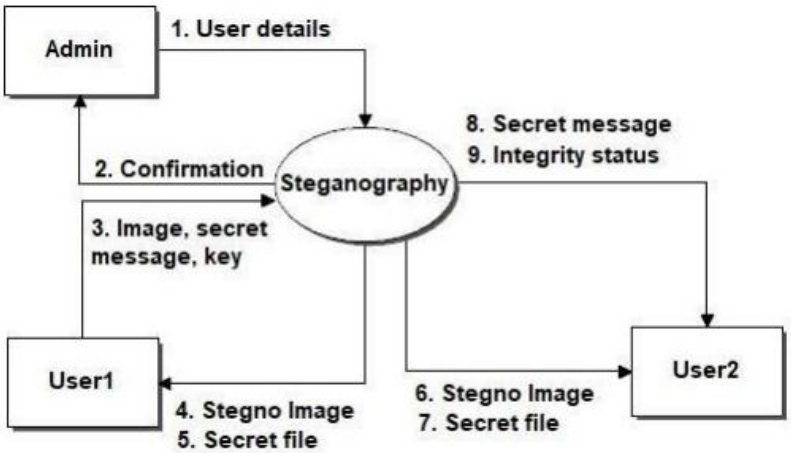

Figure 2 shows the detailed flow diagram of the system.

VI. METHODOLOGY AND RESULTS

The entire project is divided into 5 modules as shown below.

1. Data Hiding Space Reservation
2. Binary key mapping on reserved space
3. Secret Data Hiding process
4. Intranet Mail system
5. Secret Data Extraction process

A. Data hiding space reservation

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 9, Issue 6, June 2020

With the help of this method, we will be able to reserve the space on the cover image where we are going to hide the data. Here, we are planning for the diagonal parity matrix concept. That means from the image, image is matrix of pixel. In the matrix pixel, starting from the left hand top side to right hand bottom. Diagonally, we are selecting the set of pixel. Those selected set of pixels is called parity pixels. That space only we are going to damage only one colour layer.

B. Binary Key Mapping on Reserved space

As shown in the figure 3 before hiding the data, we have to get the secret key from the data owner. Once the data owner has given the secret key. That secret key will be converted into ASCII code. Then it will be converted into binary codes. Those binary codes are mapped on the reserved pixels. Once it is mapped on the reserved pixels where ever one is output, in that area only we will hide the data.

C. Secret Data Hiding Process

In this methodology, we will use LSB technique. LSB means Least significant bit. We are using colour image in this system. In the colour image, there are 3 channels: red, green and blue. We are going to hide the data only in the red channel only. In that red channel, we are damaging last 4 bit only. So, it will not give big impact on colour. Totally, image will not have any damage. With human eyes, it can't be identified.

D. Intranet Mail System

This module is used to transfer the stegno image from one person to another person. This is the reason intranet mail system is used.

E. Secret Data Extraction Process

Once a user received a stegno image, he needs to extract the content from stegno image. From that hidden key is needed. Once the user has downloaded the stegno image from the intranet mail system. With the help of this methodology, the user will be able to provide the stegno message and the key that is the hidden key. Then with this methodology, we can extract the binary data. Binary data will be converted into text and showed to the user.

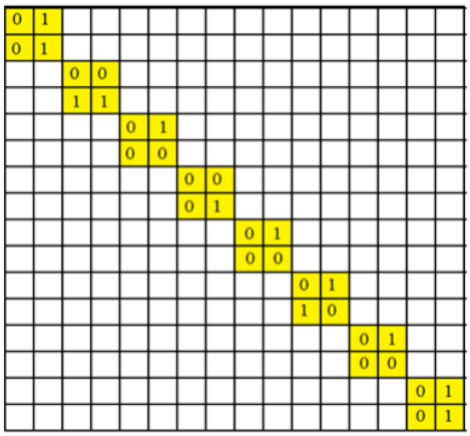

Figure 3: Binary Key Mapping on the reserved space.

Figure 4 shows the screenshot of the cover page of the proposed Image Steganography system. Using this GUI any user can navigate to the admin login or can register with proper credentials and set passwords in case of new registration. Three privilege levels have been created.

- User
- Admin
- New Registrations

An admin has the highest privilege and can alter the initial settings or update the system. User lacks such privilege but can use the system to transmit his secret information through a channel by choosing cover image of his/ her choice. New registrations are allowed to increase the scalability and reusability of the proposed system. Figure 5 shows the new registration, user login and admin login window. For any new registrations, one needs to mention

- User_id
- User name
- Password
- Email Address
- Gender
- City
- Contact number

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319-5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 9, Issue 6, June 2020

User login can be done with user_id, password and other credentials would be saved in the database. Similarly, admin can login with his admin_id and password. Figure 6 shows the window of the hiding process. Once a user is logged in, he can traverse following paths.

- Hiding process
- Receiving process
- Send mail
- Show profile
- Sign out

During the hiding process one can choose the image to be used as the cover to send the information by browsing. Once successfully uploaded, a message stating "Image uploaded successfully" is displayed as shown in figure 7. The data to be hidden is entered as shown in figure 8 and a key is chosen. We have chosen 'Steganography' as the data and 'project' as the key. The data to be hidden can be of any length and the cover image of his choice. Figure 9 shows the screen with the send mail option. A mail to be sent to an intended receiver. The fields to be entered are

- ToName
- ToMail
- Subject
- Attach file
- Message

Figure 10 shows the GUI of the key file. This contains the hash of the message and the key. LSB substitution method is used as explained in the system design and SHA algorithm is used for integrity check. Figure 11 shows the GUI of the receiving process. Any intended receiver can easily read the data which was embedded on to a cover image using a key which is only known to the sender of the image. By this method any intrusion can be blocked or prevented. Figure 12 shows a success message on receiving the information and completion of data movement securely across the channel.

Figure 4 shows the screenshot of the cover page of the proposed Image Steganography system.

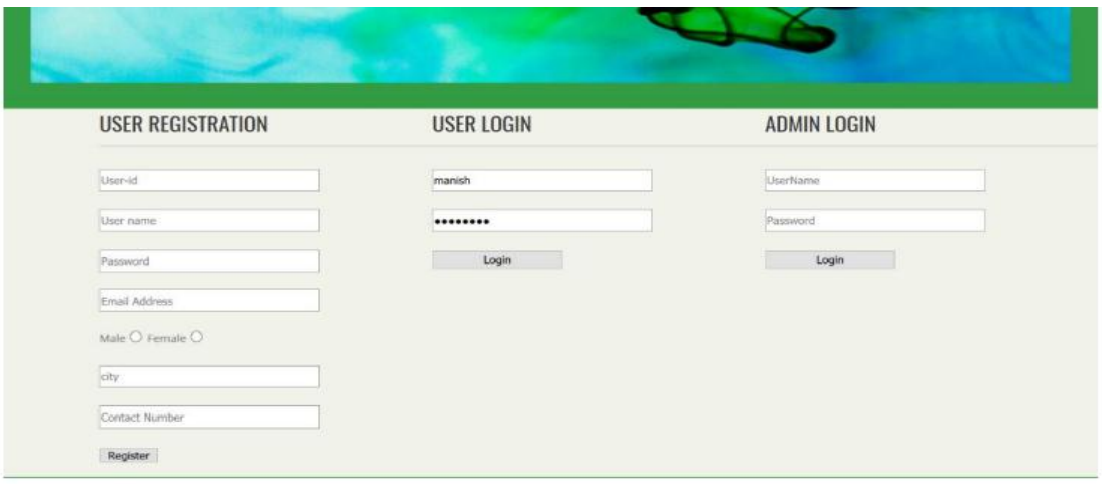

Figure 5 shows the new registration, user login and admin login window.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 6, June 2020

Figure 6 shows the window of the hiding process.

Figure 7 shows the status of the uploading process.

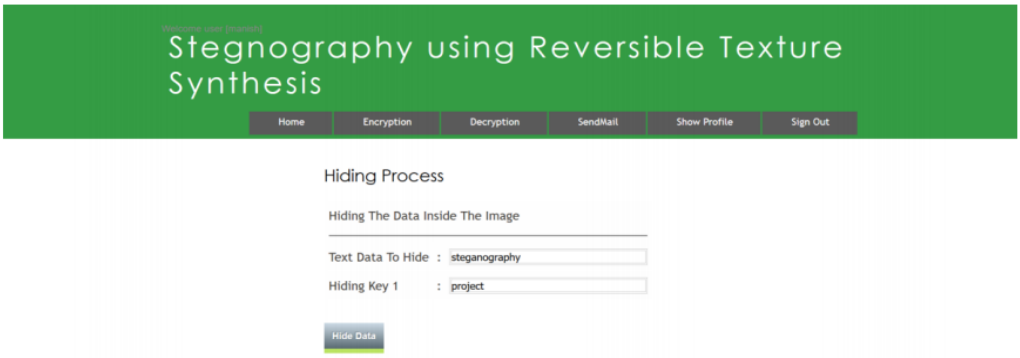

Figure 8 shows the screen in which an user can enter his/ her info and key.

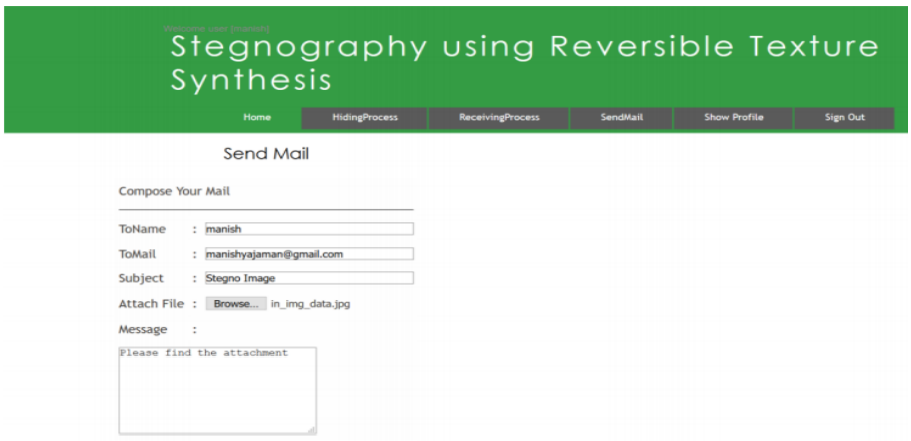

Figure 9 shows the screen with the send mail option.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 6, June 2020

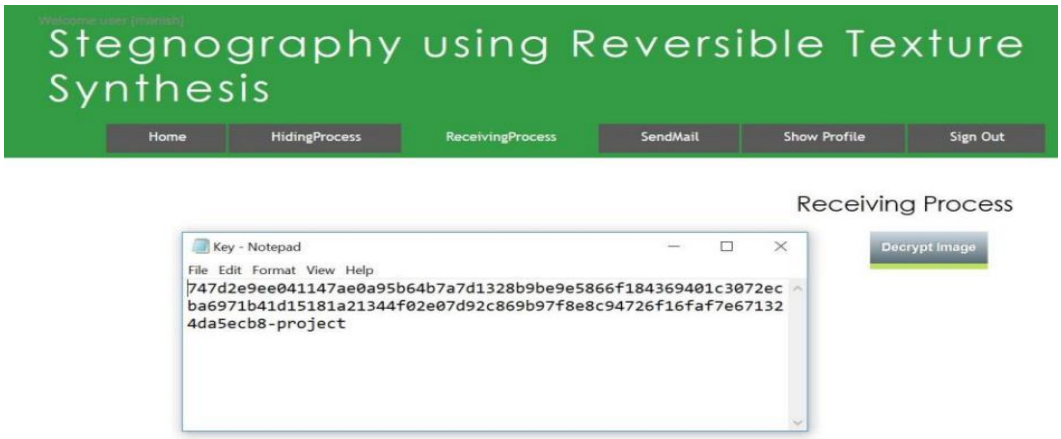

Figure 10 shows the GUI of the key file.

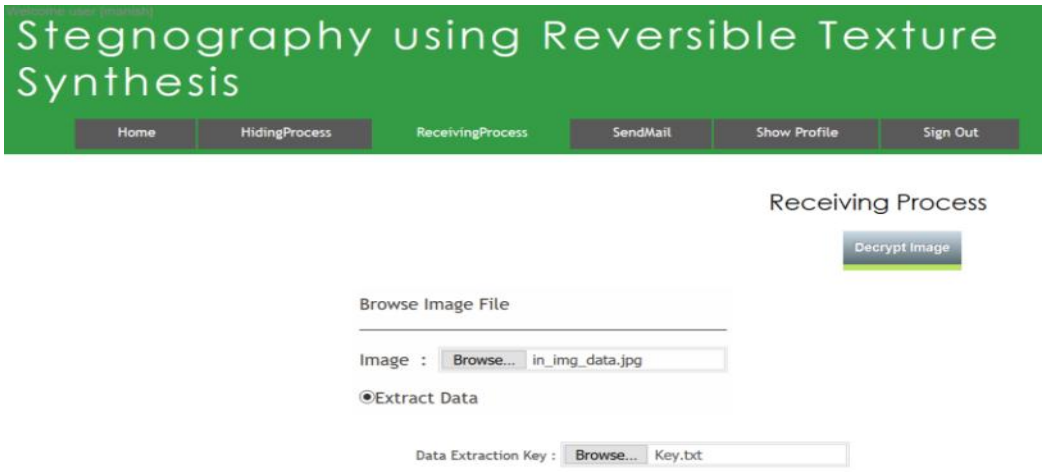

Figure 11 shows the GUI of the receiving process.

Fig.12 shows a success message on receiving the information & completion of data movement securely across channel.

VII.CONCLUSION

After transmitting the information or the SECRET data over the channel, other users (intruders or a person to whom the message is not intended to be) had no clue of the hidden message. Image Steganography is the technique of hiding the data within the image in such a way that prevents the unintended user from the detection of the hidden messages or data. To hide a message inside an image without changing its visible properties, the cover source can be altered in noisy areas with many colour variations, so less attention will be drawn to the modifications. The most common method to make these alterations involve the usage of the Least Significant Bit or LSB, masking, filtering and transformations on the cover image. These techniques can be used with varying degrees of success on different types of image files. Only the intended receiver could easily extract the message from the image thereby increasing the security of the channel against malicious attacks and intruders.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 9, Issue 6, June 2020

REFERENCES

[1] Steganography using reversible texture synthesis, Kuo-Chen Wu; Chung-Ming Wang Year-2018
[2] Comparison of LSB image image steganography technique in different color spaces, Ozcan Cataltas; Kemal Tutunc, 2017 International Artificial Intelligence and Data Processing Symposium (IDAP)
[3] LSB Based Image Steganography Using Dynamic Key Cryptography, Nikhil Patel, Dept. of Electronics & Communication Engineering, De Rosal Ignatius Moses Setiadi Heru Agus Santoso ; Eko Hari Rachmawanto ; Christy Atika Sari .2018 International Conference on Information and Communications Technology (ICOIACT)
[4] A new approach for LSB based image steganography using secret key ,S. M. Masud Karim, Md. Saifur Rahman ; Md. Ismail Hossain , 14th International Conference on Computer and Information Technology (ICCIT 2011)
[5] Mritha Ramalingam, Stego Machine Video Steganography using Modified LSB Algorithm, in World Academy of Science, Engineering and Technology 50 2011, pp. 497-500, 2011.
[6] Anil Kumar, Rohini Sharma, A Secure Image Steganography Based On RSA Algorithm And Hash LSB Technique, International Journal Of Advanced Research In Computer Science And Software Engineering, Volume 3, Issue 7, July 2013.
[7] Satya Kumari, K.John Singh, A Robust And Secure Steganograph Approach Using Hash Algorithm, International Journal Of Latest Research In Science And Technology Volume 2,Issue 1 :Page No.573-576 , January-February (2013).