International Journal of Engineering Research in Computer Science and Engineering Engineering (IJERCSE) Vol 2, Issue 3, March 2015

Secure storage and transferring file system

[1]Ramya Mala.P,[2]Petchiammal.M,[3]Anand.M
[1],[2]UG scholar,[3]Assistant Professor
[1],[2],[3]Department of Information Technology
[1],[2],[3]Sri Vidya College of Engineering & Technology, Virudhunagar
[1]p.ramyamalait@gmail.com,[2]m.petchiyammal@gmail.com,[3]msmileanand@gmail.com

Abstract — **In many organization, there is a lack of data security while transmission and storage. Because of the digital information and data are transmitted more often over the Internet, the technology of protecting and securing the secure messages requires to discovered and developed. And a web application involves communication among network between client and server. There is need for security of data between client and server involved in web applications. Digital steganography is the art and science of hiding information into covert channels so as to conceal the information and prevent the detection of the hidden message. In our proposed system an application is created. User login into the application and select the cover image. The selected image is splitted into 16 image slices. Image slice is key of the system. Secure file is encrypted using Inigma algorithm. The encrypted secure file is embedded into the selected image. Then the embedded image is transmitted through internet to the corresponding receiver. The receiver can extract the file from image and decrypt, if receiver knows key. Verify the file and store it.**

Index Terms --- **Steganography, cryptography, cover image, stego image, LSB technique, data hiding.**

I. INTRODUCTION

Steganography means "covered writing". Steganography is a technology that hides a message within an object. Steganography has an important role in information security. In general, steganography approaches hide a message in a cover e.g. audio, video, text, image etc. Cover file is defined as a original message or file in which hidden information will be stored inside of it. Stego medium is defined as the medium in which the information is hidden. Embedded or payload can be defined as the information which is to be hidden or concealed. The goal of the steganographyis to make the transmitted information invisible by embedding the information in a cover media.To enhance the security and roubstmess of the information against attacks and image processing techniques. Steganalysis is the detection of data that has been hidden. Detecting and decoding the hidden data within a given medium even if secret content is not revealed, modifying the cover medium changes the medium's statistical properties.Cryptography is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it. The term is most often associated with scrambling into cipher text , then back again. Encryption is the conversion of electronic data into another form, called cipher text, which cannot be easily understood by anyone except authorized parties. Cipher text is encrypted text. Plain text is what you have before encryption, and cipher text is the encrypted result. The term cipher is sometimes used as a synonym for cipher text, but it more properly means the method of encryption rather than the result. decryption is the reverse process to Encryption.

Frequently, the same Cipher is used for both Encryption and Decryption. While Encryption creates a Cipher text from a Plaintext, Decryption creates a Plaintext from a Cipher text. LSB substitution method is used to embed the secret message into an image. The secret message is inserted or replaced into the least significant bit of an image. In Jpeg (Joint Photographic Expert Group) images there is a three color component which are RGB(RED,GREEN,BLUE).Each pixel contains RGB values and each color has each value. User can embedded a secret message in least significance value of each values of a pixel. . LSB Insertion has some advantages which are given below: If message bit is same as the pixel's least significant bit then no chance is required for that pixel value .If pixel value is different from message bit then effective change in pixel value is still invisssible to human eye.

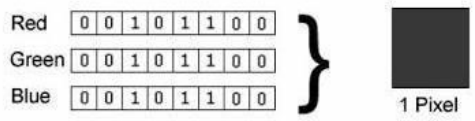


Fig1.1Jpeg pixel format

An example is used that explain LSB insertion of each color value of a jpeg images.

00100111 11101001 11001000

00100111 11001000 11101001

11001000 00100111 11101011

00100111 11101000 11001000

00100110 11001000 11101000
11001000 00100110 11101011

In this example A(10000001) is inserted into the pixel of an image by changing the least significance bit of an image

I. LITERATURE SURVEY:

It provides the small survey that produces some techniques have been used for compression-decompression, encryption-decryption, data embedding etc.

Debnath Bhattacharyya, Asmita Haveliya and Tai-hoon Kim, paper provides the text data hiding in text document such as DOC, PPT, TXT, MATLAB script file(.M) formats. There are various methods of information hiding but in text Steganography it is not easy to hide information as text data provides us less redundant space for concealing the secrets. In this paper it gets the input cover file and the secret file that is to be embedded. Then it checks if the secret file size is less than the 5% of the size of the cover file, it will be encrypted. Else an error message is displayed and selects another existing cover file with large size. To embed the secret file into the cover file , it is converted into binary file and each binary bits are taken right shift, XOR operation.

C.Anuradha, S.Lavanya paper[2] cover image is encrypted using an encryption key and then add secret message are embedded into the encrypted cover image using data-hiding key. With an encrypted image containing additional data, if the receivers only know the data-hiding key, then he can extract the secret message and receiver does not know the image. If receiver only know the encryption key, then he can decrypt the received message to obtain an image which is equal ant to the original one, but he cannot extract the embedded secret message.

Dipti Kapoor Sarmah, Neha Bajpai paper[3] develop a system in which Cryptography and Steganography are combined with enhanced security module. In Cryptography we are using AES algorithm to encrypt a message.In Steganography the message is hide in to an cover image using FCT, IFCT. The other part of the message is used to establish two secret keys to make the system highly secured[3].

Suresh Kumar, Ganesh Singh, Tarun Kumar, Maninder Singh Nehra [4] paper uses least significant bit (LSB) algorithms for hiding data into Jpeg (Joint Photographic Expert Group) images. The password is used for secret of encryption and decryption. In this paper, hide text file of different size into cover image file for authentication of login and logout the system for secure the systems. Only authorized persons can hide and disclose the message. The text files of different size are used to test the system and found that the system satisfies all requirements of Steganography and the system is more secure[4].

Obaida Mohammad Awad Al-Hazaimeh

[5] paper the secret message is inserted in the cover images in random manner by selecting any pixel of a cover image. However, LSB hides the message, still possible for the hacker to retrieve the message due to the simplicity of the method. To enhance the security, the message is not in the least significant bit, and the least significant bit of the pixel just a sign to extract data from the image. This can be held by matching the message bit and the pixel bit which is randomly chosen from second to the last bit. Using this comparison, 1 is inserted in the least significant bit if the message bit identical to that of the image, whereas, 0 is inserted if the message bit didn't match with the randomly chosen bit from the cover image. If the message bits and pixel pits are similar then the result is 1.Else the result is 0. Accurate of the Steganalysis bits positions cannot be negotiated [5].

Masoud Nosrati, Ronak Karimi, Mehdi

Hariri [6] paper embeds the message in cover image with a structure such as linked lists. Using linked list place the bits in the memory. Linked list is a data structure like an array,but linked lists get irregular addresses. Each item is called as node. Each item stores proposed data and the address of the next item in the memory.The address of first byte of secret message could be used as stego-key. In linked lists, the address of first node is stored in a pointer for accessing the linked list data. Advantage of this paper is, stegnoanalysis is harder because non sequence of message structure is provided[6].

Vikhyath K.B, Dr. M. Siddappa [7] paper secure the password in web application using Steganography. Sequence of characters provided by the client as password which is embedded to an cover image using Steganographic method. Embedded image containing password is transmitted over network to the server over network. Server retrieves the original password from the embedded image using steganographic decoding technique. Server verifies and authorizes the password for connection establishment of web application. Even if the hacker steals the image through network, hacker cannot be able to decrypt the password from the cover image.

FilterFirst algorithm: This algorithm filters the image and then hides in the highest filter values. **BattleSteg**: It hit the highest filter value from randomly selected pixel and hide the information.

T. Gomathi, B. L. Shivakumar [8] paper uses Enigma Intermix cube encryption for secure data transmission using LSB algorithm. Consider an image.Perform the sum of elements in all individual rows. If the sum of first row elements is even, carry out a right circular shift of that row. If the sum is odd then perform left circular shift. And carry out column wise sum of all elements. If the sums of first column elements are even, carry out a down circular shift of that column. If it is odd then carry out circular shift. Convert the obtained image matrix data into binary form with each pixel. Execute an XOR operation between binary value of one single key letter consume 'R' represented in the form of 8 bits and every element in the binary value matrix. After executing XOR operation, the matrix is again converted into integers form. Now obtain the encrypted image. To perform stegnoanalysis reverse the process which are performed in the above.

Frank Y.Shih, Scott Y.T.WU [9] paper designed the division of the watermark image into two planes (ie) one for spatial insertion and another for frequency insertion. This paper provides the comparison when various sized watermarks are added into the grayscale images. It has some advantages which are following: More watermark information is embedded in to the cover image. Capacity also increased. The divisions of two parts increased protection double. It leads complexity to be unable to compose. In this paper the combination of spatial and frequency watermark are used. The watermark image is splitted into two division. One for spatial insertion and another for frequency insertion. That two planes are called as w1, w2.Watermark image (w1) is processed into spatial domain insertion which is added into host image. Watermark image (w2) is processed into frequency domain insertion. Then it is added with spatial processed insertion watermarked image and take DCT. Obtain the marked image. To recover that host image use IDCT.

Diego De Luca Picione,Federica Battisti, Macro Carli,[10]paper provides the Least significant bit algorithm where the gray scale image wants 12 bit planes instead of 8 bit planes which is in the form of binary representation. It has some advantages which are following. It leads less perceptual distortion even if various planes are chosen for embedding. This scheme is compatible with classical LSB data hiding scheme. It leads low computational complexity. It posses high embedding capacity. It does not affect human perception of the overall image quality. It has some disadvantage which are robustness, tampering, geometric attacks, filtering and compression.

II. PROPOSED SYSTEM:

These papers propose secure storage and transffering file system. In this system aims at providing secured transmission of files sent by client over a network. Our system has four modules which are following as:

Login process and create database.

Image slicing and file encryption

Embedding file into an image

File Extraction and verify process. Now explain the each modules of the system.

1. Login process and create database.

Step1: To login the application first creates an account by registration. Only authorized person can create an account by registration process. If the user is not authorized person can't create an account.

Step2: User upload the cover image.

Step3: After uploading image, the selected image is splitted into 16 image slices.

Step4: User selects any one slice from 16 image slice which image slice is considered as a key.

Step5: After create an account user login the application and verify the password and userid.

2. Image slicing and file encryption

Step1: After getting access permission, the user selected image is display in the application.

Step2: Then splitted 16 image slice also shown to the user.

Step3: User click the image slice which is already selected during registration.

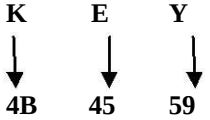
Step4: Now verify the authorized user by using selected key image.

3. Embedding file into an image

Step1: The selected file is encrypted using secret key value which is known by the sender and receiver.
Step2: Using LSB substitution method the secret file is encrypted.

Step3: The secret message is converted into the decimal value**.**

Ex: secret message is key



Step4: Then numbers and letters are separated to embedded in cover image.(ie)letters are embedded in first row of image then the numbers are embedded in second row of an image an so on.

Step5: The embedded file is transferred over the internet to the destination**.**

4. File Extraction and verify process

Step1: To extract the file the receiver knows the key image slice.

Step2: Receiver choose the key image slice from the
16 slice of image. If receiver select the correct key image slice then extract the encrypted file.

Step3: Now the encrypted file is extracted and receiver decrypt the file using secret key.

Step4: And finally stores the file. If the key is wrong then the encrypted file gets destroyed.

The below Fig2.1 shows the flow of the system. First the user creates an account to login that application. Only authorized persons can register the application. This can be done by testing of date of join. While the user registration, the application get date of join and designation of user. If the date of join and designation is valid data, then the user can only create an account. Else the user cannot complete the registration process and cannot create an account. Then the user selects the cover image and upload the secret file which wants to send. The user can upload only restricted height and width. Height is 400 and width is 400 which was predefined. And the user can select the restricted file size. It should be limited file size.

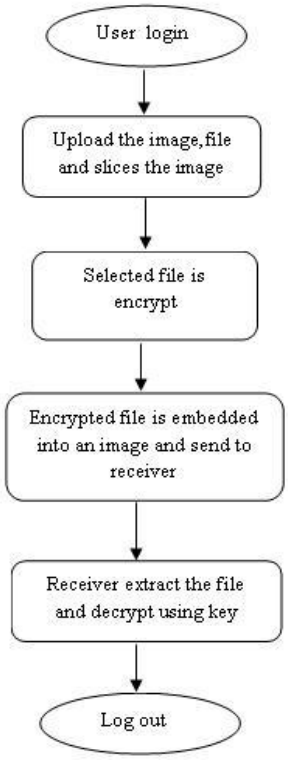


Fig2.1 flow diagram

After uploading the cover image that image is splitted into 16 slices. And user selects one key image from the slices. The secure file is encrypted. The encrypted secure file is embedded into the cover image. That embedded image is send to the destination. In the receiver side extract the encrypted file is extracted using key image. Now encrypt the file using key an verifies the file. If it is valid then store it else it is destroyed. The destroyed file is store in the separate folder. If the destroyed folder file is increased then system admin can alert that some unauthorized people access.

III. EXPERIMENTAL RESULT AND IMPLEMENTATION:

In this section the experimental result for the implementation of the secure storage and transferring file system are described. The below fig3.1 explain the login for the application for the purpose of secure and authentication.

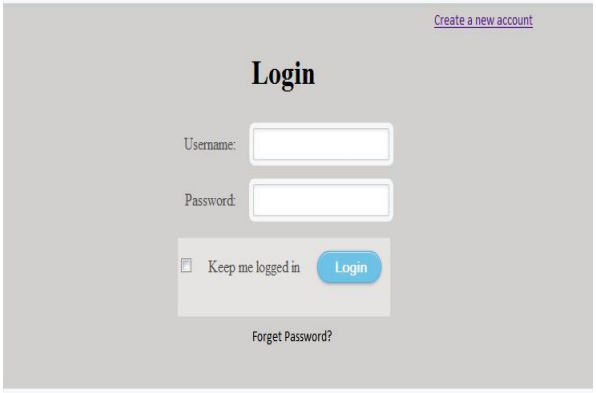


Fig3.1: snapshot for login

After completion of login process the user select the cover image to embedded the secure file and select the file. The selected cover image is displayed below Fig3.2.

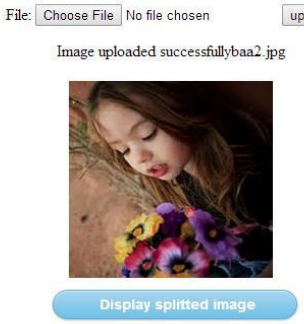


Fig3.3: upload a cover image

Then click the button display splitted image to slices the 16 image slices.

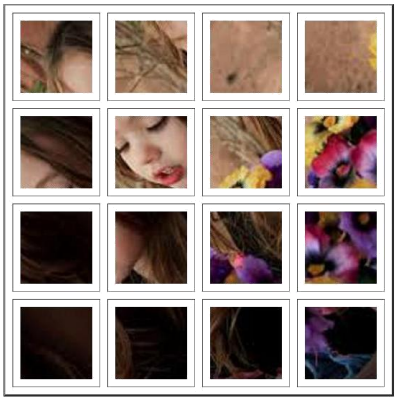


Fig3.4: Slices of cover image

When the button is clicked, the selected cover image is split up into 16 image slices. Then user selects any one slice which is key image of that user. The splitted image is randomly displayed. The selected file is encrypted and embedded to send. The embedded file is send over the internet. And the file is received by the receiver. The receivers select the key image to extract the encrypted file and enter the password to decrypt the file. If the file is verify then it will be store. Else it get destroyed.Fig3.5 shows original image and stego image.

Fig3.5 Original Image **Fig3.6** Stego-image

IV. FUTURE ENHANCEMENT:

The implemented Secure storage and transferring file system can be enhanced in future by the following supplies. This paper support only for jpg images. In future work should apply for all format of images such as jpg,png, tif etc. And this paper accept only limited or restricted file sizes. In future enhancement should apply for variable sized file future enhancement should apply for variable sized file.

CONCLUSION

The implemented secure storage and transferring file system has low computation complexity which consist of login process and create database, image slicing and file encryption, eaxbedding file into an image, file extraction and verify process. This paper provides set of hints to secure file storage and transferring between two ends.

REFERENCE:

[1] Debnath Bhattacharyya, Asmita Haveliya and Tai-hoon Kim, "Secure Data Hiding in Binary Text Document for Authentication" Appl. Math. Inf. Sci.

8, No. 1L, 371-378 (2014).

[2] C.Anuradha**,** S.Lavanya "Secure and Authenticated Reversible Data Hiding in Encrypted Image" Volume 3, Issue 4, April 2013.

[3] Dipti Kapoor Sarmah, Neha Bajpai "Proposed System for data hiding using Cryptography and

Steganography".

[4] Suresh Kumar, Ganesh Singh, Tarun Kumar, Maninder Singh Nehra, "Hiding the Text Message of

Variable Size using Encryption and Decryption

Algorithms in Image Steganography".

International Journal of Computer Applications (0975 – 8887) Volume 61– No.6, January 2013.

[5] Obaida Mohammad Awad Al-Hazaimeh "Hiding Data in Images Using New Random Technique" IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 4, No 2, July 2012.

[6] Masoud Nosrati, Ronak Karimi, Mehdi Hariri "Embedding Stego-Text in Cover Images Using linked List Concepts and LSB Technique" World Applied Programming, Vol (1), No (4), October 2011. 264-268 ISSN: 2222-2510

[7]Vikhyath K.B, Dr. M. Siddappa"Authenticated Connection establishment in Web Applications using Steganography" International Journal of Internet Computing, Volume-I, Issue-1, 2011

[8] T. Gomathi, B. L. Shivakumar"Suspection Less Steganographic Approach using Enigma Intermix Cube Encryption Technique" International Journal of Innovative Technology and Exploring Engineering (IJITEE)

ISSN: 2278-3075, Volume-4 Issue-4, September 2014

[9] FrankY. Shih, Scott Y.T. Wu "Combinational image watermarking in the spatialand frequency domains" Pattern Recognition 36 (2003) 969 – 975

[10] Diego De Luca Picione , Federica Battisti, Marco Carli ,Jaakko Astola, and Karen Egiazarian 14th European Signal Processing Conference (EUSIPCO 2006), Florence, Italy, September 4-8, 2006, copyright by EURASI.