IJCSE International Journal of Computer Sciences and Engineering Open Access

Research Paper Volume-3, Issue-1 E-ISSN: 2347-2693

Secure Data Transform in Encrypted Image Using Steganography Technique

Malatesh M[1*], Anitha G[2] and Ujjini Venkatesh[3]

[1*]*Department of CS&E, UBDTCE, VTU, India*

www.ijcaonline.org

Received: Dec/22/2014 Revised: Jan/12/2015 Accepted: Jan/19/2015 Published: Jan/31/2015

***Abstract*—**the mean of the paper is to apply computer vision technique to transmit secret messages from sender to receiver. Cryptography and steganography are the two techniques to transform secret messages. In this paper steganography technique is used. Steganography is the hiding and transmitting secret data to the authorised user. One of the hiding techniques utilised here is LSB manipulation. System generate 3 keys using AES 128 bit algorithm based on these keys ,sender and receiver can encrypt and decrypt secret messages respectively. MySQL server, net beans IDE tool is used to obtain results.

Keywords*—Cryptography, LSB, AES, Steganography*

I. INTRODUCTION

In the present fashionable world, most of the individual prefer internet as a medium to transform data from one end to another across the world. There are many ways to send the data using internet via e-mail, chat etc. however, one of the main difficult situation with sending data using internet is the security threat. Here personal data can hack in many ways. Therefore security plays a very important role for secret data transform. In this paper steganography technique is used to secure data transform. The steganography is the hiding and transmitting secret messages to authorised user. The hiding technique used here is the LSB manipulation. Steganography can be implemented on various file formats such as audio (.mpg, .wave), video (.dat, .mpeg), image (.jpeg, .bmp).however in this paper images are most preferred format. The condition while using the steganography technique is the originality of the image should not be altered. If the originality of the image is altered, then it became easier to hack the information from unauthorised user.

Existing system: in existing system, user must have all the keys to get the original data and it provide less security for secret data.

Principal content of the data is exposed before data extraction.to overcome these issues steganography technique is applied. Provide secure data transform by hiding the secret data against unauthorised user.to hide the secret data LSB technique is used.

II. RELATED WORK

In related work, some of the research fellow's work to transform secret message to authorised user is explained below

X. Zhang *et al.* proposed Separable Reversible Data Hiding in Encrypted Image [1]. This method suggests a novel scheme for data hiding in encrypted images.

Akash Kumar Mandal, Chandra Parakash, Mrs.Archana Tiwari *et al.* proposed Performance Evaluation of Cryptographic Algorithms: DES and AES [2]**.** The fast progression of digital data exchange in electronic way, information security is becoming much more important in data storage and transmission.

X. Zhang *et al.* proposed a Lossy compression and iterative reconstruction for encrypted image [3].work suggest when higher is the compression ratio, reconstruction image can be obtain better quality.

MazharTayel, HamedShawky, Alaa El-Din Sayed Hafez *et al.* proposed A New Chaos Steganography Algorithm for Hiding Multimedia Data [4]. This is devoted to propose a new chaos steganography algorithm for hiding the multimedia data, image, text, or sound. The proposed algorithm based on coordinate the data in the image dimensions using chaos distribution arrangement. The data is embedded with the original image in the pixels least significant bits, so can't appears within the image.

W. Liu, W. Zeng, L. Dong, and Q. Yao *et al.* proposed an efficient compression of encrypted grayscale images [5].

III. PROPOSED METHOD

The proposed method of secret message passing consisting of image encryption, data embedding and data extraction. Below steps illustrate the proposed method

1. The sender will browse the image from computer. Sender will encrypt the image and system will generate encryption key.
2. The sender will browse the data that he wanted to encrypt. Sender will encrypt the original data and system will generate the encryption key.
3. The sender will hide the encrypted data in encrypted image and system will auto generate data hiding key and system will generate file extension as per user defined.
4. The sender will send the file with any extension (user defined) using LAN/WAN connection.

Corresponding Author: *Malatesh M[1*]*,
malateshm315@gmail.com

5. After receiving file from sender If receiver have only Image Encryption key then he will only decrypt the image and he will only able to get original data.

6. If receiver has data hiding key then he will able to extract hidden data. He will get data in encrypted form.

7. After getting encrypted data if receiver has data encryption key, then he will able to decrypt data. After decryption of data he will get the original data. If receiver have all three keys then he will able to perform all three operation i.e. Image decryption, Data extraction, Data decryption.

The proposed system architecture can be as shown in the fig .1 this figure explains about an overview of the system architecture.

Fig. 1 explains the general architecture, how secret text is transformed to authorized user

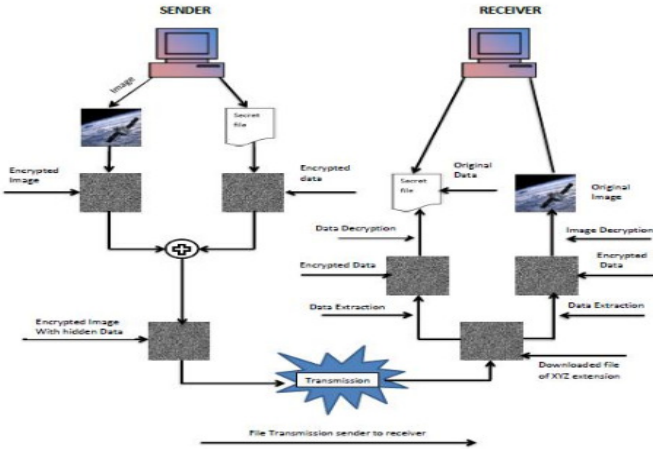


Fig. 1 PROPOSED SYSTEM ARCHITECTURE

A. *Activity Diagram*

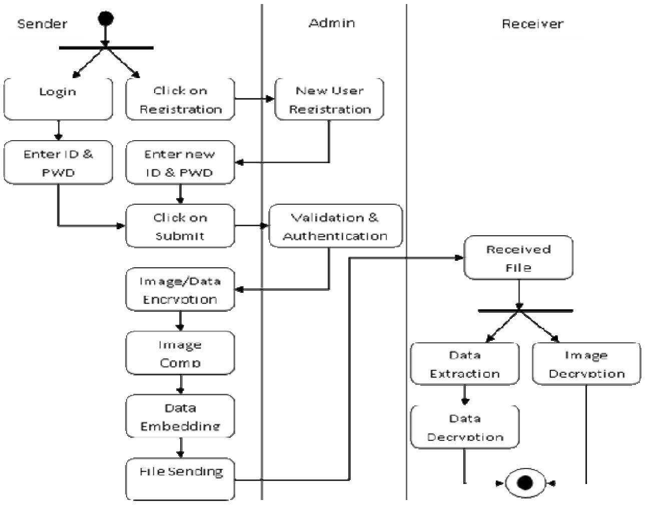


Fig. 2 The Activity diagram

An activity diagram shows the sequence of steps that make up a complex process, such as an algorithm or workflow. An activity diagram shows flow control, similar to a sequence diagram, but focuses on operations rather than on objects.

Activity diagram illustrate entire process of steganography technique of secret message transforming from sender to authorised user.it explain data embedding, data extraction and validation and authentication.

B. *The AES(Advanced Encryption Standard) Algorithm*

The AES Algorithm is a symmetric-key cipher, in which both the sender and the receiver use a single key for both encryption and decryption. The data block length is fixed to be 128 bits, while the length can be 128, 192, or 256 bits. In addition to this, the AES algorithm is an iterative algorithm. The each iteration can be called as a round, and the total number of rounds is 10, 12, or 14, when key length is 128, 192, or 256 bits respectively. The 128 bit data block is divided into 16 bytes. These bytes are mapped to array called the 4x4 State array, during encryption or decryption each stage is modified at last stage state is copied to output matrix, in the same way 128 bits key is characterised as a square matrix of bytes. Next key is widened into array of keywords; here each words consisting of four bytes. So for the 128-bit key the total key schedule is 44 words. Within a matrix ordering of bytes is done by column. example, the first four bytes of a 128-bit plaintext occupy the first column of the matrix, the second four bytes occupy the second column, and so on. Similarly, the first four bytes of the expanded key, which form a word, occupy the first column of the w matrix.

Step 1**:** AES algorithm is a symmetric block cipher with a block size of 128 bits.

Step 2**:** The key that is provided as input is expanded into an array of forty-four 32-bit words; w[i] four distinct words (128 bits) serve as a round key for each round.

Step 3**:** four distinctive phases are used, three for substitution and one for permutation:

Substitute bytes**:** it uses S-box table, where byte-by-byte substitution of block is formed

Shift rows**:** A simple permutation that is performed row-by-row.

Mix columns: here each byte is changed by substitution in a column, which acts as a function for all the bytes in the column.

Add round key: A easy XOR operation is applied for current block with part of the expanded key.

Step 4: SubBytes() adds confusion by processing each byte through an S-Box. An S-Box is a substitution table, where one byte is substituted for another, based on a substitution algorithm.

Step 5: ShiftRows() provides diffusion by mixing data within rows. Row zero of the State is not shifted, row 1 is shifted 1 byte, row 2 is shifted 2 bytes, and row 3 is shifted 3 bytes.

Step 6: MixColumns() also provides diffusion by mixing data within columns. The 4 bytes of each column in the State are treated as a 4-byte number and transformed to another 4- byte number via finite field mathematics.

step 7: The actual encryption is performed in the AddRoundKey() function, when each byte in the State is XORed with the subkey.

C. *Data Embedding Algorithm*

The Steps are as follows:

Step 1: 'Np' encrypted pixels were randomly selected by data-hider pseudo.

Step 2: some (N- Np) left out encrypted pixels are permuted pseudo-randomly and divided into groups, each which contains 'L' pixels.

Step 3: here, pixel-group gather the 'M' least significant bits of the 'L' Pixels and 'M' value less than 5.
Step 4: a matrix 'G' of size (M.L - S)* M.L is generated by the data-hider

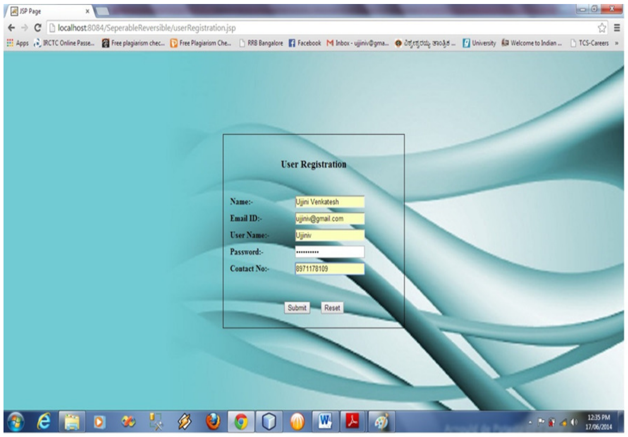
Step 5: Embed the values of the parameters M, L and S into the LSB of Np selected encrypted pixels.

Step 6: Then replace the LSB of selected encrypted pixels with the 20 bits.
Step 7: A total of (N-Np).S/L bits made of 'Np' original LSB of selected encrypted pixels and (N-Np).S/L – Np additional bits will be embedded into the pixel group.
Step 8: [B(k, 1), B(k, 2)……… B(k, M*L)] are compressed as (M.L - S) bits.
Step 9: Then replace [B(k,1), B(k,2)……… B(k, M*L)] with the [B'(k,1),B'(k,2)……… B'(k, M*L)] put them in the original position.
Step 10: (8-M) most significant bits (MSB) of encrypted pixels are kept unchanged.

IV. RESULTS AND TESTING

The proposed method is implemented using tool net beans IDE. Results are analysed. Following snapshot illustrate the result of this paper.

fig. 3 shows the user login page. Here the existing user has to enter his username and password to access his page. If he enter invalid username and password, the error message will display. If he is an authorized user, the system will allow him to access

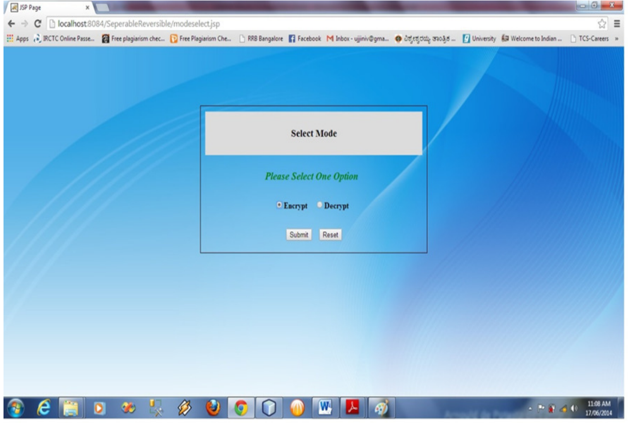

localhost:8084/SeperableReversible/userRegistration.jsp

User Registration

Name:- Ujjini Venkatesh
Email ID:- ujjiniv@gmail.com
User Name:- Ujjiniv
Password:- ••••••••••
Contact No:- 8971178109

Fig. 3: New User registration form.

The fig.4 shows the mode of operation to be select i.e., either Encryption or Decryption option


localhost:8084/SeperableReversible/modeselect.jsp

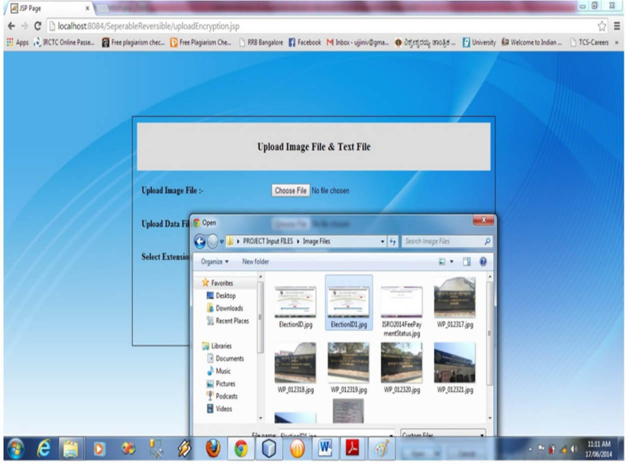
Select Mode

Please Select One Option

● Encrypt ○ Decrypt

Fig. 4: Select mode of operation

The fig.5 shows the browse an inpute image to perform an encryption using symmetric key. When click on the browse button the window has to open to select the image for encryption


localhost:8084/SeperableReversible/uploadEncryption.jsp

Upload Image File & Text File

Upload Image File :- Choose File No file chosen

Upload Data Fil

Select Extensio

Fig. 5: Browse Image file to be encrypted

The fig.6 shows the decrypted original image file. This be the original image file what the receiver actually wants from the sender.

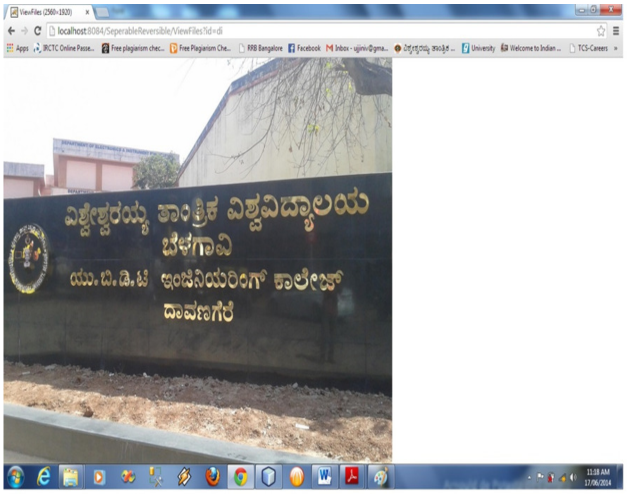

localhost:8084/SeperableReversible/ViewFiles?id=di
ವಿಶ್ವೇಶ್ವರಯ್ಯ ತಾಂತ್ರಿಕ ವಿಶ್ವವಿದ್ಯಾಲಯ
ಬೆಳಗಾವಿ
ಯು.ಬಿ.ಡಿ.ಟಿ ಇಂಜಿನಿಯರಿಂಗ್ ಕಾಲೇಜ್
ದಾವಣಗೆರೆ

Fig. 6: Decrypted image file

All of the applications need to run without any error and provide a quality service to the user of the application. In this regard the software has to be tested for its accurate and correct working. Following table illustrates some test cases

Sl. No.	*Name of the Test Case*	*Feature is being tested*	*Sample Input*	*Expected Output*	*Actual Output*	*Remarks*
1.	Check user is Unauthorized.	Username and the Password is Invalid.	Enter Wrong Username and Password.	Msg “Username and Password is wrong”.	Msg “Invalid Username and Pwd”.	Pass, User is Invalid.
2.	Check user is Authorized.	Username and the Password is Valid.	Enter Correct Username and Password.	Msg “Username and Password is Correct”.	Msg “User is Authorized”.	Pass, User is Valid.
3.	Block User	Wrong Entry of Username and Password for 3 times.	Wrong Entry of Username and Password.	Msg “Username and Password is Wrong, Block user”.	Msg“ Username and Password is Invalid, Block User”.	Pass, Username and Pwd is Invalid for 3 times. So, User is Blocked.
4.	Allow User to Access the Service.	Check whether User is Authorized or not?	Input -Correct Username & Pwd.	Msg “ User is Authorized to Access the Service”.	Msg “ User is Authorized to Access the Service”.	Pass, Allow User.
5.	Upload Encryption Page	Select on browse option.	Click on Browse Option.	Select window should get opened.	Window opened.	Pass, Window opened.
6.	Start process Button.	Click on start process button (keeping all field correct)	Click on the Start Process Button.	Encryption result page should get displayed.	Results Page Displayed.	Pass, Results of Encryption should display.

Sl. No.	***Name of the Test Case***	***Feature is being tested***	***Sample Input***	***Expected Output***	***Actual Output***	***Remarks***
7.	Decrypt option.	Select on decrypt option (keeping all field correct).	Click on the Decrypt Process Button.	Decryption Results page should get displayed.	Appropriate Results page should displayed.	Pass, Results Page displayed.
8.	Log Out	User Session has to Close.	Click on Log Out Button.	Msg"You Logged out Successfully".	It should not back to the previous page.	Pass, Log out Successfully.

V. CONCLUSION

This method helps for transmitting secured information by having more security level to data. A Separable Reversible Encrypted data hiding in Encrypted image will prevent third party access during transmission by providing user define extension to final generated file.

future work, make use of audio, video in case of image as cover for hiding the data, and hide any type of data like video and audio up to certain limit.

The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay). This data integrity can be achieved through the Message Authentication Code (MAC) algorithm.

ACKNOWLEDGEMENT

The author would like to thank Smt. Anitha G Associate professor, UBDTCE VTU University for her valuable suggestion and support. Also thank my friend Arvind Belure for his continuous support in throughout the paper.

REFERENCES

[1] X. Zhang, "Separable Reversible Data Hiding in Encrypted Image" *IEEE Trans. Inform. Forensics Security*, vol. 7, no. 2, pp. 826-832, April 2012.

[2] Akash Kumar Mandal, Chandra Parakash, Mrs.Archana Tiwari "Performance Evaluation of Cryptographic Algorithms: DES and AES", IEEE Trans. on Electrical, Electronics and Computer Science, 2012.

[3] X. Zhang, "Lossy compression and iterative reconstruction for encrypted image," *IEEE Trans. Inform. Forensics Security*, vol. 6, no. 1, pp. 53–58, Feb. 2011.

[4] MazharTayel, HamedShawky, Alaa El-Din Sayed Hafez, "A New Chaos Steganography Algorithm for Hiding Multimedia Data" Feb. 19~22, 2012 ICACT2012.

[5] T. Bianchi, A. Piva, and M. Barni, "On the implementation of the discrete Fourier transform in the encrypted domain," *IEEE Trans. Inform. Forensics Security*, vol. 4, no. 1, pp. 86–97, Feb. 2009.