IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-5, Special Issue-1, Jun 2016 E-ISSN: 2347-2693

Image Steganography-Hiding Data within Image

Esha Deshmukh[1*], Juily Dangle[2], Sagar Ghadi[3], Shailesh Kewat[4] and Kalpana Shewale[5]

[1*] Department of Electronics and Telecommunication,
[2] A.C.Patil College of Engineering, Kharghar, Navi Mumbai
[3] Mumbai University, India

Corresponding Author: eshadeshmukh21@gmail.com

Available online at: www.ijcseonline.org

Abstract— Security of the data is of foremost important in today's world. Security has become a main important field in information and communication technology. For highly secure, hidden communication and sharing of information steganography is used. Steganography is a method of hiding the existence of communication, by hiding information data in other carriers. Different carrier mediums can be used for this, but digital images are the most famous because of their frequent use on the internet. There are several techniques of steganography, among them some are too complicated than others. Every technique have their strong and weak parameters. LSB, DES and AES algorithm is been used in this project. LSB technique is simple, high payload, low complexity and easy to detect. AES and DES are the complex technique but provide high security. The execution time of LSB is more, DES moderate and AES takes less time. Using these three methods we are going to design our project. This will enhance the security of the data which is being transferred.

Keywords—*Steganography, stego-key, AES, DES, LSB.*

I. INTRODUCTION

The main reason that attackers can successful is all of the information they acquire from a system is in the form that they can easily comprehend and read. The attackers may reveal the data to the others, misuse it, change it to misrepresent the information to an organization. To efficiently solve this security problem steganography is used. It is a method of successfully hiding the data in digital cover media. Steganography is so much different from the cryptography and watermarking method. In steganography, the existence of communication kept hidden whereas in cryptography existence of secret communication is easily identified.

The tremendous improvement in information hiding techniques has drawn a lot of attention now a day and becomes a dynamic topic in both private and government sectors. In order to protect the system integrity and prevent the exploitation of digital media from the criminal activities that have malicious intent. Steganography and cryptography methods are the two known sub-disciplines of information hiding in current years. It is a method of hiding textual information in carrier such way that it prevents the identification of hidden information from a third party [5]. Two individuals can secretly communicate using this message hiding technique.

As the ICT exponentially growing these days, almost all of the information is kept electronically. Therefore, security of this information is the main issue in ICT. Steganography is used to give high security to the information completely. In cryptography, the ASCII code of message or encrypted message is fully embedded in a digital carrier before transmitting it through the network, thus the existence of the message is unknown. Besides hiding data for confidentiality, this new approach of hiding information provides the best security among all media.

The network security is becoming more important as the number of data being exchanged on the internet increases [3]. Therefore, the data integrity and confidentiality are required to protect against unauthorized use.

Information hiding for security is a growing research field, which consists of applications such as copyright protection for digital media, watermarking, fingerprinting, and the technique mention in this paper.

In most of the watermarking applications, the message contains much information such as owner identification and a digital time stamp, which usually do apply for protection. Data is also kept locked using fingerprint security mechanism. An unauthorized user cannot access the information if the fingerprint is not matched with fingerprint security Steganography always hides the secret message within the data and it is reliably communicated to a receiver [8]. Basic flow chart of steganography via LSB is given in figure 1.

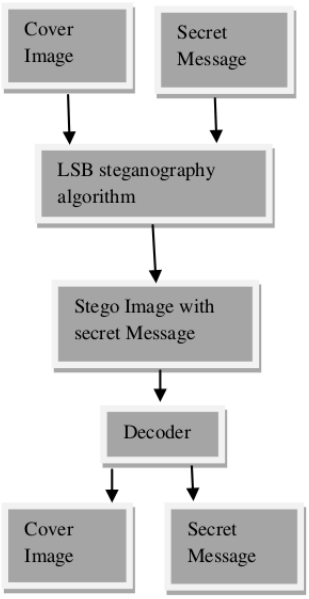

Figure-1 Basic flow chart of steganography using LSB

Steganography vs. Cryptography:

The ultimate purpose of both techniques is to provide secret sharing of information and data. Steganography is totally different than cryptography. Using algorithms like RSA, AES, DES and double DES cryptography can hide the contents of a secret message from other people by modifying it, whereas steganography hides the existence of the message [1]. In cryptography, the system is totally broken when the attacker can read the secret message even a little bit of it. For steganalysis system need the attacker to detect that type of steganography method has been used.

The combination of the both techniques results in better security. First, we convert the simple message into an encrypted message using cryptography then the hiding of this encrypted message is done in the carrier using steganography. The resulting image containing secret message will be transmitted on the network without revealing the existence of secret communication. Only authorized and the valid user can detect the stego carrier and read the message.

II. RELATED WORK

Bin Li, Jiwu Huang, Junhui He and Yun Qing Shi explain the main aspects of information hiding technique steganography and for detection technique steganalysis. Steganography is a method of hiding the existence of communication, by hiding information data in other carriers. Steganalysis is the method of finding the available steganographic content in carrier. In this document the basic concepts of steganography and the process of methods of steganography for digital images is discussed[5]. The summarization of methods of steganography is discussed.

Security of data has become the main concern nowadays with growing technologies of ICT. Varinder Kaur and Satwinder Singh proposes a dual security model for hiding Sensitive information with the help of LSB based steganography and AES encryption Technique. The proposed method is to hide the information behind some carrier image using LSB technique and then encrypt the image using AES algorithm.

Douglas selent discusses the detailed concept of AES in this paper[4]. AES algorithm is used for encrypting the data. In AES algorithm the same key is used for decryption and encryption of data. AES is block cipher which uses block sizes of 128, 192 and 256 bits. The paper also discusses announcing of AES and some drawbacks of triple DES (3DES) and DES. AES use EX–OR different operations like shift row, substitution and permutation and combination operations, column shifting.

In paper [6] they used AES-128 bit algorithm.In real time they have evaluated their implemented hardware design. In paper [9] they work with the same AES-128 bit algorithm for speed, power consumption and area. S. H. Kamali [11] used the modified encryption algorithm to give a high security and enhanced image encryption. The modified AES is made by adjusting the ShiftRow operation using s-box matrix. The difference aspects of old AES algorithm and modified AES algorithm are compared by the author.

III. PROPOSED SYSTEM

In recent years, many steganography methods that insert hidden messages in a text file, music file, image, and video have been proposed. There have been techniques for hiding information or secret message in images in a way that changes made to the image pixel is hardly recognizable. LSB, Transform techniques, filtering and masking are common approaches.

LSB is the simplest method of steganography. This inserts the message directly into the list significant bits of the carrier media in an organized manner. This change in the least bits didn't much affect the cover media. So just by seeing the cover media no one can recognize the difference in original cover image and stego image. This change in LSB is too small in amplitude. In LSB method, the inserting capacity can be increased by using two or more least significant bits. This use of two or more LSB results in more chance of detection and percentage of security becomes less compare to single LSB use. In LSB, the amount of payload depends on the number of pixels of the image. We can hide more data in an image having more number of pixels. The advantage of the LSB-based method is easy to employ and have a high payload.

LSB technique hides information such way that human being cannot recognize it with naked eyes. Only using some high-quality detection software it can be detected. An attacker can extract and read the message only if they suspicious that there is some hidden message is inserted in cover. Therefore, rather than sequentially inserting data in pixels of the cover image via LSB; some algorithms are used to specify random pixels to embed the data. These random pixels are scattered on every place from center to the edge of the cover image.

A method of masking and filtering is basically used on only 24 bits and grayscale image. It applied a special matrix modification on the image bits by marking it, similarly like paper watermark. The method practices analysis of the cover image by inserting the information in significant regions so that the hidden information looks more integral part of the cover image. Transform techniques insert the data by modulation of the coefficient in a transform domain.

Till now the basic idea of steganography is being introduced. Now further part is how the steganography process will be carried out. In steganography, there are three various techniques which we have used ideally or all together.

1) LSB Technique
2) DES Technique
3) AES Technique

A. *LSB (Least Significant Bit):*

There is no method for decreasing the file size of the bitmap images. Digital images are builds from pixels and these pixels of images are consists of three colors red, green and blue (RGB).each color of a pixel is one-byte information that shows the density of that color. Using combinations of the RGB colors other colors are formed digitally. Each byte of the pixel is consists of 8 bits. The first bit is termed as MSB(Most Significant Bit) and last bit of every byte is LSB(Least Significant Bit). The steganography is done on using LSB of the byte of pixels of the image. We use LSB bit for writing our ASCII code of data inside pictures [7]. We should change the last bit of pixels, in other hands, we have 3 bits in each pixel so we have 3*height*width bits memory to write our information. But before writing our data we must write the name of data (file), the size of the name of data & size of data [7]. We can do this by assigning some first bits of memory (8th layer).

This technique is the steganographic algorithm that is being used for embedding the text into the image. In the LSB method involves the mainly two steps:

(i) Convert the text into its ASCII code binary equivalent

(ii) Replace each bits of the cipher text with the last bit of selected pixels of the cover image.

Converting the Text into Binary: Each character is converted into its ASCII equivalent. The ASCII value is nothing but a number. This ASCII value is translated into its binary equivalent.

Replacing the bits: Only last bit is replaced because it contains very less information about the image properties. If we try to replace the other than the LSB bit then there is more distortion in the image. As more information is modified in the image. Each bit of ciphertext is replaced in the LSB position of the pixels in the image. As changes is done only in LSB so the difference between stego and original image will be minimum, that human naked eye cannot recognize it. The only software that particularly determines the patterns in the images can detect the irregularities in the patterns.

B. *DES (Data Encryption Standard):*

DES was originally developed by an IBM in 1970. Data encryption standard takes 64-bit plaintext as an input and creates 64-bit Ciphertext i.e. it encrypts data in blocks of size 64-bits per block. The given plaintext data is arranged into the size of 64-bits each and encrypted using 56-bits key at the initial level. Its key of 56-bit is short for high security. These 56 key bits can be easily known by brute force attack and then attacker can break down the encrypted data easily. Cascading two and three operations of DES with distinct keys advanced DES like double DES encryption is done. These advanced DES are not worked very fast, especially in software. DES was designed for efficient hardware implementation, but it properly not works in software [3].

The principal of the DES is very simple. Divide plaintext data into a block of size 64 bits each, which is an initial permutation. After initial permutation on the 64-bit block, the block is divided into two parts of 32 bit called left plaintext and right plaintext. The left plaintext and right plaintext goes through 16 rounds of encryption process along with 16 different keys for each round. 16 rounds of encryption process left plaintext and right plaintext gets combined and final permutation operation is performed on this combined block. The inverse of initial permutation is also called final permutation. This produces a 64-bit encrypted block. In this way, all the plaintext get encrypted by performing broad level steps on it in order to produce encrypted cipher text. This way block by block of the size of 64-bit is encrypted.

After the encryption is done by the DES algorithm, the encrypted message is converted to its ASCII code. This ASCII code then converted to their equivalent binary format.

Now, this binary data is inserted in the cover image of which is to be sent for communication purpose. For inserting of these binary data LSB method is used. This data is embedded bit by bit in the cover image pixels LSB. That is how the DES algorithm is used in steganography for better security of the hidden information.. Only authorized user can extract the encrypted data and access the message from the image as authorized user have the key given by sender.

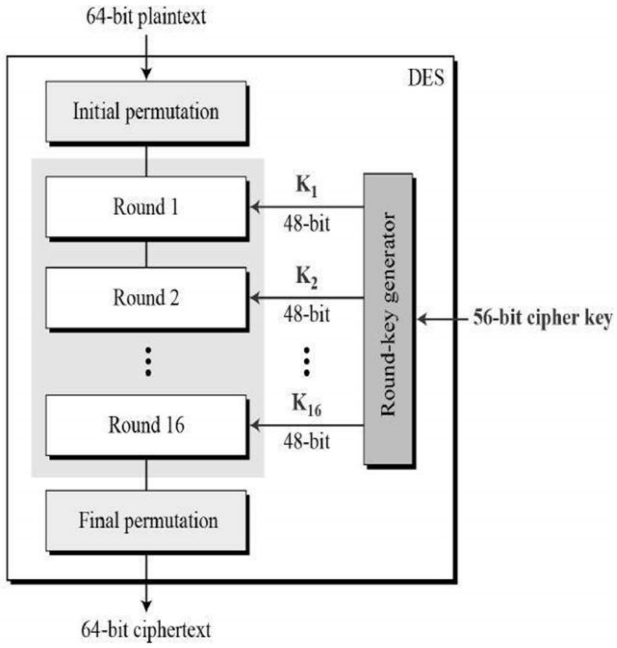

Figure-2 DES Structure

Decryption of DES encrypted data is the purely inverse procedure of encryption. All the operation applied on the data during encryption process will be applied in an inverse manner to do decryption. A minute change in the encrypted data will result in loss of information. So during LSB extraction correct key and method is must use by authorized person.

Strength/desirable properties of DES: A slight change in the plaintexts bit or character will drastically change the ciphertext. Each bit of ciphertext depends upon multiple bits of plaintext. It's not a group cipher, hence DES instances can be applied many times to a plaintext (2DES and 3DES). It makes brute force partially impractical as it uses 56-bit keys means 256 possible combinations of key.

Disadvantages of DES: New highly advanced cryptanalysis can break DES because during its design this attack wasn't invented. Now in the new age of parallel computing, breaking DES has become easy with the help of brute force attack which was impossible during that time.

C. *AES (Advanced Encryption Standard):*

The key used in AES is symmetric means for encryption and decryption same key is used. It is a cryptographic algorithm like DES, published in 2001. The algorithm was proposed by Rijndeal. It is a replacement of less secure encryption standard. In AES method block cipher is symmetric that works with data block which is of blocks size 128 bits. AES used three different sizes of key 128-bit, 192-bit and 256-bit According to the size of the key used for encryption and decryption the number of rounds of the AES operation differs[4]. The proposed system consists of the 128-bit of block size and 128 bit of key size. The algorithm is applied for both image encryption and decryption. As the key size is 128 bits it will take 10 rounds [3]. For 192-bit key, it takes 12 round and for 256-bit key size algorithm takes 14 round of operations to generate unbreakable cipher data.

1)AES Image Encryption

Conversion of original image i.e. plain image into encrypted image i.e. cipher image is known as image encryption. On 128bits of block size data below operation are done. The rounds have following stages in AES:

Substitute Bytes: It is a non-linear byte substitution, operation on each of the state bytes independently takes place [4]. Depending on its value state bytes of matrix is substituted from s-box lookup table. s-box look up table contains all the 256 combinations of 8-bit. If the state byte value is 25 then the combination present at 2^{nd} row and 5^{th} column will be replaced by it.

Shift Row: This operation includes, the rows are shifted to the left in a cyclic manner according to their row number. Row 0 remain unchanged. 1^{st} row does a shift of one byte to the left; row 2 does a shift of two bytes to the left and row 3 does a shift of three bytes to the left.

Mix Columns: In this step, the columns of the state are assumed as polynomials and multiplied by a special mathematical modulo + 1 with a fixed polynomial c(x), where, $c(x)=\{03\}x^3 + \{01\}x^2 + \{01\}x + \{02\}$. Every column is multiplied to this polynomial to generate new columns. In the last round of operation, the mix column transformation does not occur.

Add Round Key: In the Add Round Key transformation, the cipher key is added to the resultant states of the column transformation. The round key is simply EX-ORed with the output of the column transformation[6]. Added key in each round is different because AES also used key expansion algorithm. AES generate all these key from the single 128-bit key using key expansion algorithm. In AES first key is EX-ORed with plaintext then the round operations begins.

The output AES encryption embedded in the cover image using LSB steganography technique.

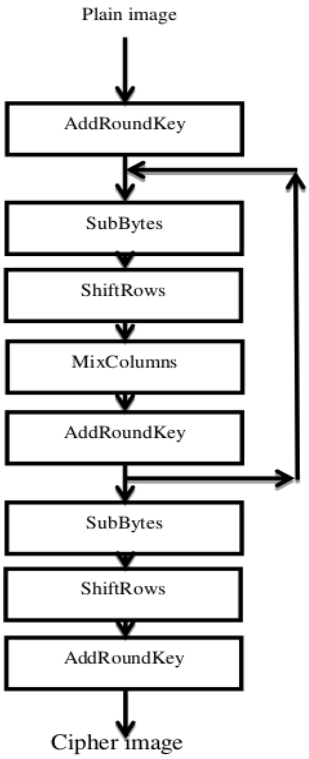

Figure-3 AES encryption

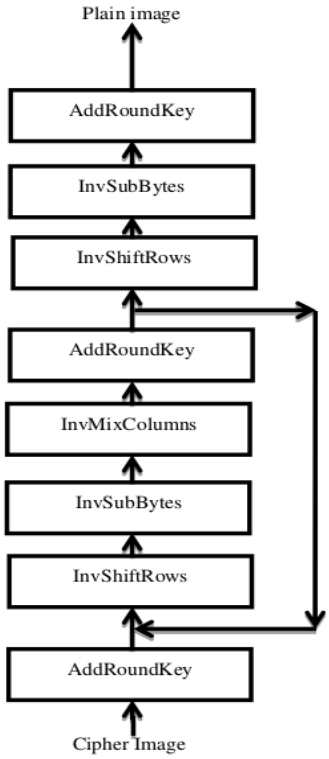

Figure-4 AES encryption

2)AES Image Decryption:

The reverse of encryption is called decryption. All the rounds of the encryption will be in a reverse manner in AES decryption. It will result in a conversion of cipher image into a plain image [6]. Today AES is used because DES was inherently weak.56- bit key is used in DES which means there are 256 combinations which are easy to crack in case of Brute Force attack. Alternatives to DES, like Triple DES (3DES) are available but 3DES is very slow. The round consists of the following stage for image decryption shown in figure 4.

Add Round Key: The round keys have to be selected in reverse order.

Inverse Shift Row: It is same as Shift Rows, only in the opposite direction.

Inverse Substitute Byte: Inverse s-box matrix is used. According to the present value of byte, it is substituted by inverse s-box bytes.

Inverse Mix Columns: In the Inverse Mix Columns transformation, the polynomials of degree less than 4 over GF(2^8), which coefficients are the elements in the columns of the state, are multiplied modulo (x^4 + 1) by a constant polynomial which is d(x) = {0B}x3 + {0D}x2 + {09}x + {0E}.

Table1. Comparison between AES and DES

PARAMETERS	AES	DES
Developed in Year	2000	1977
Cipher Type	Symmetric Block Cipher	Symmetric Block Cipher
Key Length	128,192,256 bit key	56-bit key
Possible keys combination	2128,2192,2256	256
Block size	128,192 or 256-bit key	64 bit
Security	Highly Secure	Not Secure, inadequate

This comparison is based on the research paper [3]. These encryption algorithms combine with LSB will result in highly secured method for secret data sharing.

IV. METHODOLOGY OF THE APPLICATION

- This project has two methods – Encode and Decode.
- In encryption, the secret information is hiding in with any type of image file.
- Decryption is getting the secret information from the image file.

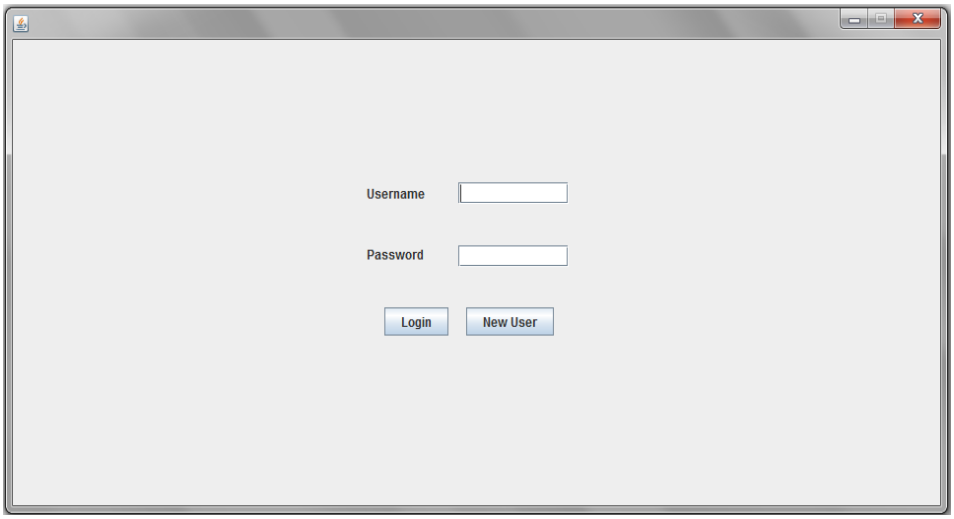

Figure-5 Login Window

The user needs to run the application. A login window will pop up as shown in figure 2. Here user will enter the username and the password. When the username and password matched as the information stored in the database then and then the only user can login for operations of steganography. For the registration of the new user in the system, there is an option as 'New User'. After clicking on it a new window will pop up as shown in figure 3. Here the newly unregistered user can register them. They have to enter a new username and password then the same password in the confirm password field then register.

After clicking on 'Register' the user can use same username and password to login into the system and can have secret communication with other users by using steganography techniques. This is simple but highly secure login as no one other than register user can use this application.

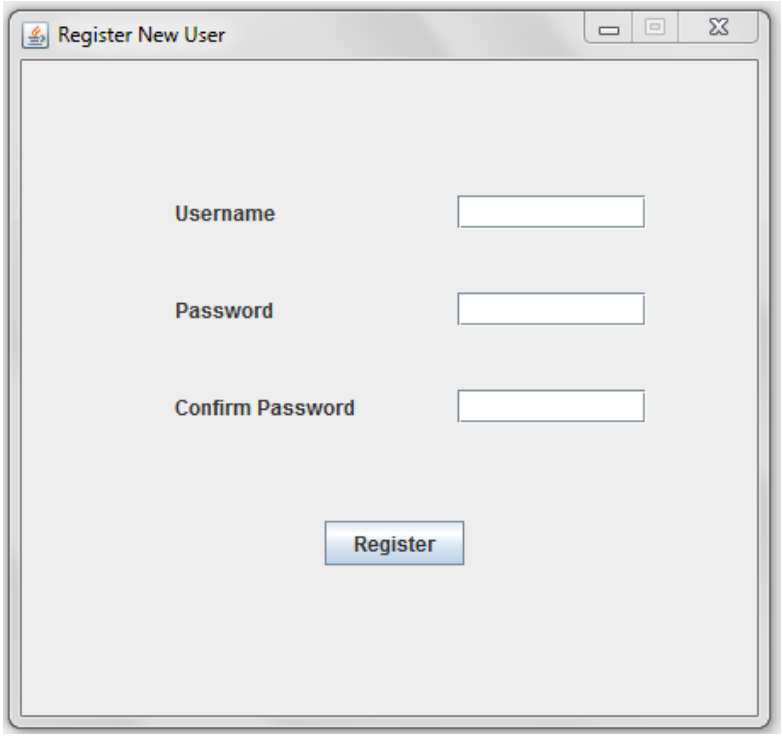

Figure-6 New User Register Window

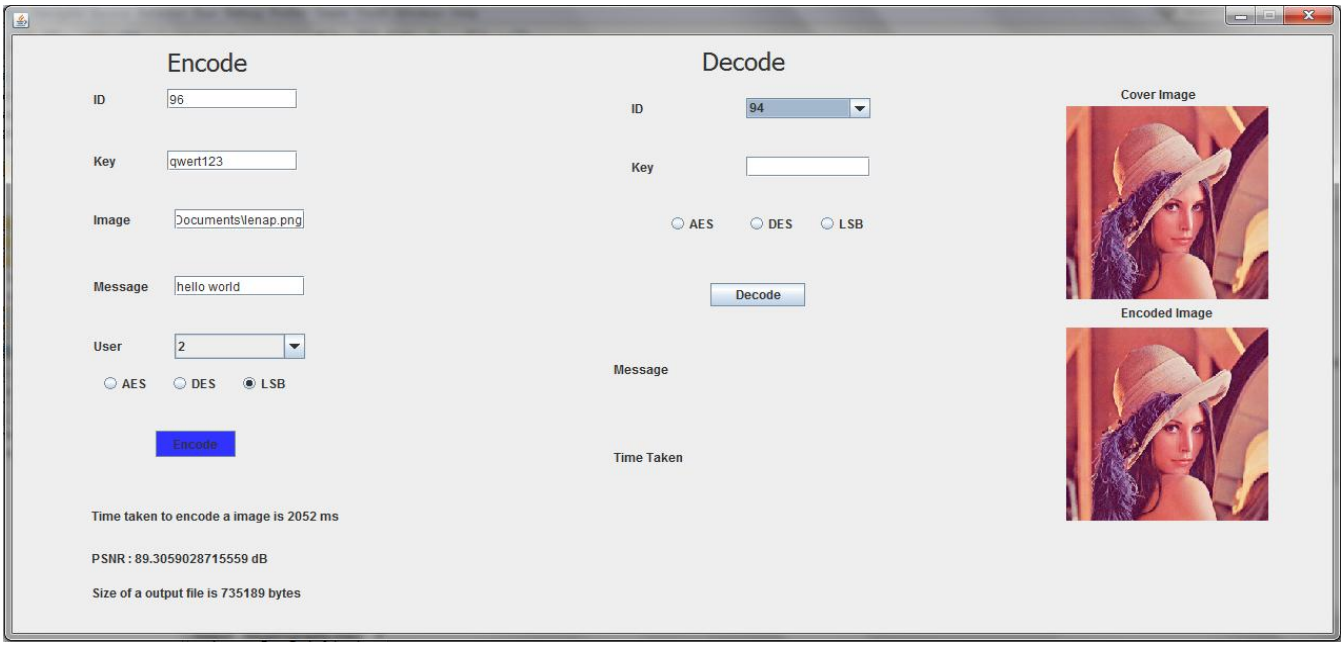

Figure-7 Encoding of lena.png

After successful login of the user. For encoding, the application gives the screen to select an image file, input secret text, selects the user to whom the user wants to send the image, option to the operation of the algorithm from LSB, DES and AES. Then locked image by user key and encode the image file. If user select decode, the application gives the screen to select image file ID, input key which was used to encrypt the image and method by which image is encoded. After encryption, the application shows time is taken for encoding, PSNR and size of the encrypted image with the cover image and the encoded image. As shown in fig 4. For decoding the other user will login and perform the decoding operation.

After decoding of image hidden message, decoding time with encoded and decoded image is given by application as shown in figure 5. The user must use the same key which was used during encryption and select the image id which was given during encryption.

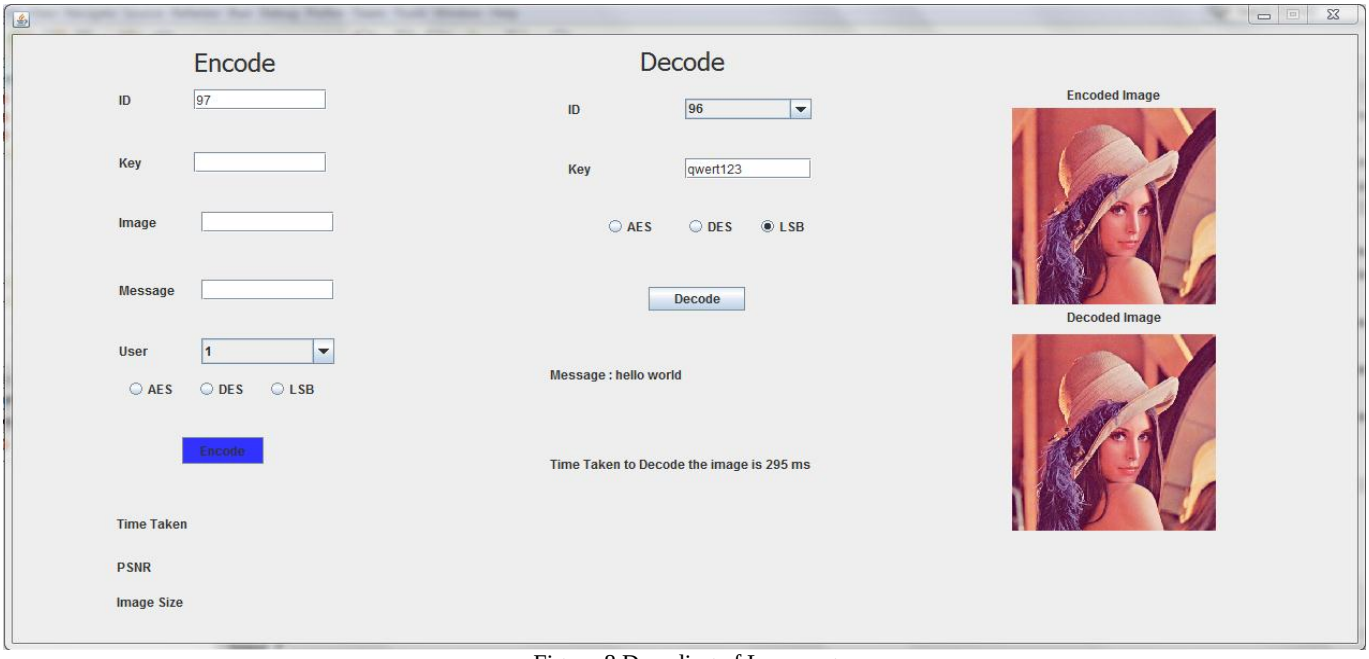

Figure-8 Decoding of Lena.png

V. PERFORMANCE ANALYSIS PARAMETERS

A. Peak Signal to Noise Ratio

PSNR value defines the image quality. Higher the PSNR value means image have high quality. The PSNR value shouldn't be less than 30dB. Here all encrypted images PSNR value is higher than 50 dB. Comparatively, LSB method gives the high PSNR encrypted image and AES and DES methods have little bit same PSNR value. Using this proposed system high quality and the less distorted image is getting. So with naked eyes, no one can detect that some message is hidden in the image which is encrypted one.

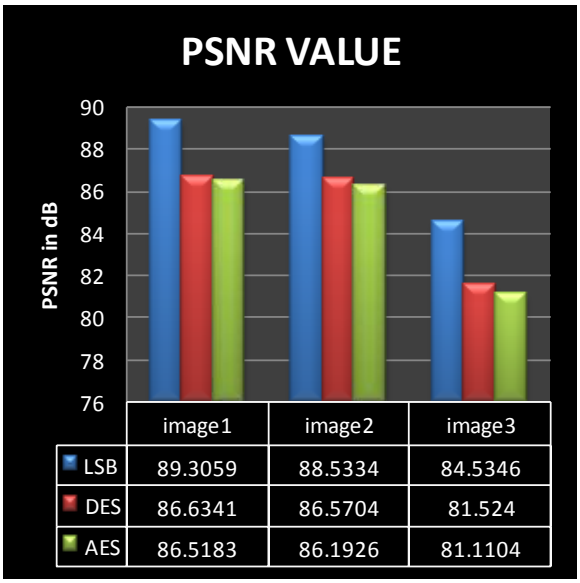

Figure-9 PSNR values

B. Encryption time

Encryption time for the images is in the range of milliseconds. For image1 LSB takes maximum time. AES and DES take almost same time but less than LSB. Approximately the encryption time is in the range of 200ms to 500ms. Which means that communication done by this proposed system of steganography is not too slow. Approximately real time hidden message within the image can be sent and received. So there is no time barrier using this method.

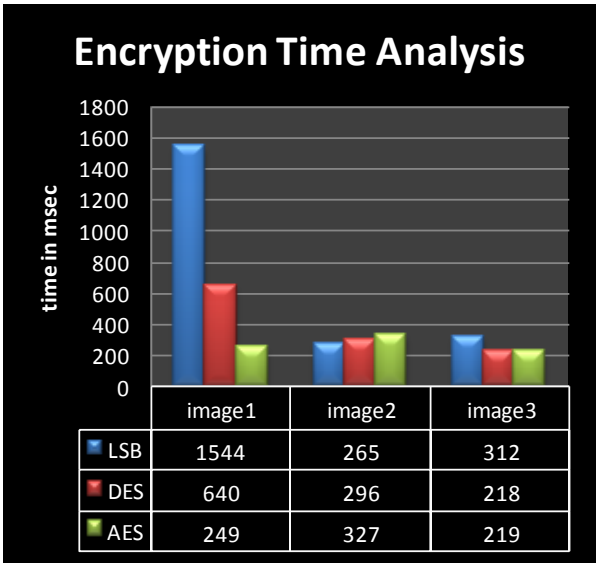

Figure-10 Encryption time

C. Size of Image file after encryption

The size of the encrypted image and the cover image is almost same for all the methods. There is a minute variation in the size of the encrypted image by LSB method. As the there is minute change the attacker can't detect the suspicious image by comparing original image size with encrypted one.

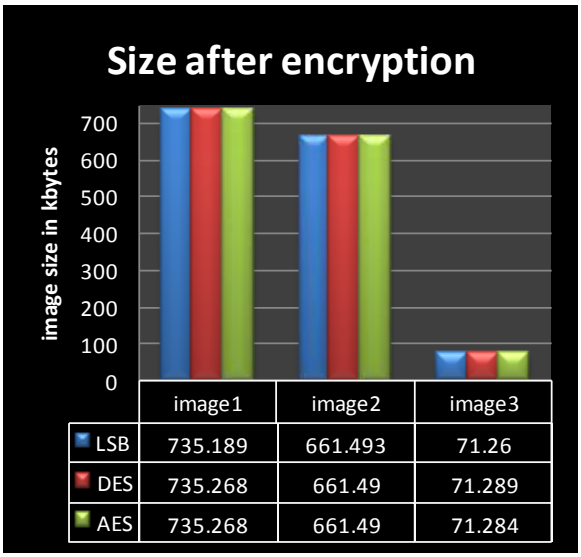

Figure-11 Size after encryption

VI. RESULT SUMMARY

Table2. Payload, Invisibility, PSNR and Security of proposed system

Parameter	LSB	DES	AES
Payload	High	Moderate	Less
Invisibility	Low	High	High
PSNR	89.3059	88.5334	84.5346
Security	Very low	Moderate	High

VII. APPLICATION AND ADVANTAGES

A. Application:

- Secure private files and Documents
- Hide passwords and Encryption keys
- Transport Highly Private Documents between International Governments.
- Confidential communication done and secret message can be stored.
- Our personal banking information, organization secrets can be stored in a cover source.

B. Advantages:

- In steganography, the message is not visible like cryptography in which the encrypted message is visible.
- To make information more secure steganography is used to hide cryptography.
- Steganalysis is hard and complex.

VIII. CONCLUSION AND FUTURE SCOPE

Steganography is a field of secret communication. People can secretly communicate using this technique. As the all the information and data these days becomes available electronically, the influence of steganography on everyone's lives will continue to grow. LSB steganographic technique with some advancement using AES and DES algorithm is presented in this article, based on the logical operation. Algorithm embedded data into LSB of the carrier image before that data is converted into ASCII code. Implementation of steganography is simple compared to the method to detect and attack on it because these methods are more complex than steganography technique itself. It is going to be reliable and secure. LSB technique is simple, high payload, low complexity and easy to detect. AES and DES are the complex technique but provide high security. The execution time of LSB is more, AES and DES take less time. Greater PSNR value indicates the quality of image is higher.

ACKNOWLEDGMENT

We are grateful to our Department of **Electronics and Telecommunication** for their support and providing us an opportunity to review on such an intriguing topic. We thank to the authors of references and reviewers.

REFERENCES

[1] X. Zhou, W. Gong, W. Fu, L. Jing "*An Improved Method for LSB based colour Image Steganography Combined with Cryptography*", Jin. Information Engineering School, Communication University of China,CUC. **15TH** International confrence on Computer and Information Science(ICIS), **2016**

[2] L. Randa and P. Saxena, "*Security Improvisation in Image Steganography using DES*", International Journal of Advanced Research in Computer Engineering and Technology (IJARCET). Volume **3** Issue **7**, July **2014**.

[3] S. Mewada, P. Sharma and S. S. Gautam, "Exploration of efficient symmetric algorithms," *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, 2016, pp. 663-666.

[4] D. Selent, "*Advanced Encryption Standard*", Rivier Academic Journal, Volume **6**, Number **2**, Fall **2010**.

[5] B. Li, J. He, J. Huang, Y.Qi. Shi. "*A survey on Image steganography and steganalysis*", Volume **2**, Number **2**, April **2011**.

[6] S. Mewada, P. Sharma and S. S. Gautam, "Exploration of efficient symmetric AES algorithm," *2016 Symposium on Colossal Data Analysis and Networking (CDAN)*, Indore, 2016, pp. 1-5. doi: 10.1109/CDAN.2016.7570921

[7] S. Nimje, A. Belkhede, G. Chaudhari, A. Pawar, K. Kharbikar, "*Hiding Existence of Communication Using Image Steganography*", International Journal of Computer Sciences and Engineering, Vol.2, Issue.3, pp.163-166, 2014.

[8] C.R. Gaidhani, V.M. Deshpande, V.N. Bora, "*Image Steganography for Message Hiding Using Genetic Algorithm*", International Journal of Computer Sciences and Engineering, Vol.2, Issue.3, pp.67-70, 2014.

[9] A. Sharma, RS Thakur, S. Jaloree, "*Investigation of Efficient Cryptic Algorithm for image files Encryption in Cloud*", International Journal of Scientific Research in Computer Science and Engineering, Vol.4, Issue.5, pp.5-11, 2016.

[10] S. Singh and V.K. Attri, "*Dual Layer Security of data using LSB Image Steganography Method and AES Encryption* ", ISSN: **2231-2307**, Volume-**2**, Issue-**3**, July **2015**.

[11] V. Kapoor, "*A New Cryptography Algorithm with an Integrated Scheme to Improve Data Security*", International Journal of Scientific Research in Network Security and Communication, Vol.1, Issue.2, pp.39-46, 2013.

[12] Rajesh Shah and Yashwant Singh Chouhan, "*Encoding of Hindi Text Using Steganography Technique*", International Journal of Scientific Research in Computer Science and Engineering, Vol.2, Issue.1, pp.22-28, 2014.

