3rd International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB17)

A Combined Approach of Steganography with LSB Encoding technique and DES Algorithm

B.Karthikeyan, Associate Professor - IT, Viswajyothi College of Engineering and Technology, Vazhakulam, Kerala-686670, India.
mbalakarthi@gmail.com

A. Deepak*, School of Computing, SASTRA University, Thanjavur-613401, India.
deepak.a.1996@gmail.com

K.S. Subalakshmi, School of Computing, SASTRA University, Thanjavur-613401, India.
subalakshmi26@gmail.com

Anishin Raj M M, Associate Professor - CSE, Viswajyothi College of Engineering and Technology, Vazhakulam, Kerala-686670, India.
anishinraj@gmail.com

V.Vaithiyanathan, School of Computing, SASTRA University, Thanjavur-613401, India.
vaithiya_nathan@hotmail.com

* Corresponding author

***Abstract*—Steganography has become one of the widely used tools in today's world for hiding information within another data or an image. It is a technique that takes cryptography to the next level by concealing the presence of a message itself. Data Encryption Standard algorithm is such a cryptographic key which is applied to a block of plain text to convert it into a cipher text and vice-versa. This paper presents an innovative idea to hide a message within an image of any dimension by encrypting the message through Data Encryption Standard algorithm and concealing the message by applying LSB encoding technique in a spiral manner thus enhancing the difficulty of the decoder. The main objective is that, securing of data becomes more potent and secretive than the previous ones.**

Keywords—Cipher, Cryptography, Data Encryption Standard, Spiral, Steganography, Transposition.

I. Introduction

Information is a very critical resource to all of us. Thus cryptography [3] and steganography are the two major methods of attaining it. Steganography is the technique of manipulating information to cipher texts and hiding their actuality and existence itself.

This is done by embedding the cipher texts into various other streams such as graphics, audios or other messages too. Cryptography is the art of shielding information by converting it into an illegible format known as cipher text. The basic difference between the steganography and cryptography is that while a cipher text could be deciphered in minutes steganography allows us to cover up the cipher text itself.

In this paper we are achieving this by DES algorithm that uses a 64-bit block of data every time and applies cipher key to modify the normal text into a code text. And then the code text is concealed into the image in a spiral manner.

II. Literature Review

Wu, H.-T et al. [1] proposed an algorithm in the field of steganography for JPEG images altering the block DCT coefficients. In this method the DCT coefficients are divided into four frequency bands by matrix encoding. A new method for selecting the coefficient is also used to make the concealed message less perceivable.

Gupta, R. et al. [2] proposed a new method for image security integrating cryptography stenography and watermarking techniques. It not only hides the message but also gives better results for MSE, PSNR and embedding power even after the noise attacks. It also provides security for watermarked video.

Baek, J et al. [3] presented a steganographic method for secret sharing of information using gray scale images. The relationship between the binary and gray code representation of a pixel is taken into consideration here. And an EX-OR operation is used upon N cover images accessible to sender and receiver.

Bajwa, I.S. et al. [4] proposed two methods for color image steganography. They have proceeded with a hashing approach for secure data hiding. Here secured images are transmitted at higher speed using gray scale images with this approach. Also various file formats such as bmp, JPEG, gif are supported in this technique of secured transmission.

Bouslimi, D. et al. [5] put forward an algorithm for concealing message in encrypted images using a predetermined watermark embedding before the process of encryption. Here the encryption/decryption has a unique key and watermark processing has a different key thus decryption of message is independent of extracting the image.

Zhang et al. [6] presented an approach for data concealing by reversible image transformation. Here RTI-based framework is used to convert the content of original image into another target image having same size. Traditional RDH scheme and unified embedding and scrambling scheme are used to insert watermark in the encrypted image.

978-1-5090-5434-3©2017 IEEE

Khodaei, M et al. [7] put forward a method for data hiding using pixel value differencing and LSB substitution. Here an image is split into blocks of two successive pixels .The difference of two pixels is calculated, and as per the difference, it will estimate the number of embedding bits into LSBs of two pixels.

Conci et al. [8] proposed an AES cryptography in color image by genetic algorithms and path re-linking. It presents a hybrid approach that replaces the LSB substitution methods thus increasing the usage of color images to hide a text.

Panda, S.S. et al. [9] presented a secured approach to spatial image steganography by changes in the neighbourhood pixels of the cover image. By this technique, the embedded area looks more regular and uniform.

Nilizadeh, A. et al. [10] presented a modern steganography technique grounded on matrix pattern and LSB algorithms proposed for RGB images. These methods utilize the spatial domain of image for concealing the data. The Matrix pattern divides the RGB image into various B*B blocks into non overlapping layers.

Karthikeyan.B. et al. [11] proposed an approach of cryptography and steganography by deploying rotor cipher for assured conveyance of data in an interrupted communication channel using 2-bit LSB steganography which helps in hiding the information from the intruder. They have also put forward [12] an advanced steganographic method by LSB substitution on a scanned image which increases the security level of the message. In addition to this they have presented [13] a LSB dependent steganography with multi-layered encryption by using caeser cipher technique to conceal the text in the image and encrypting it based on the chaos theory. Also they have put forth [14] a composite method for hiding information through random theory and reversible integer depiction in which DCT is applied to the image and is hidden by LSB substitution.

III. Proposed methodology

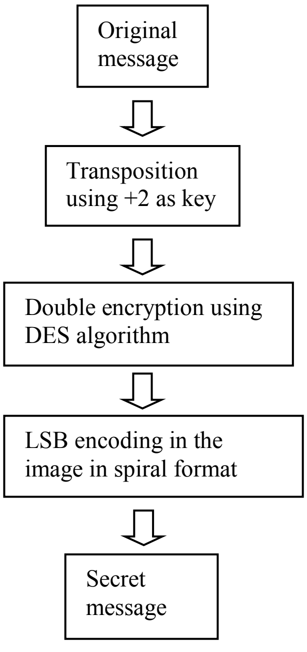
Original message
Transposition using +2 as key
Double encryption using DES algorithm
LSB encoding in the image in spiral format
Secret message

Fig. 1: Encryption process

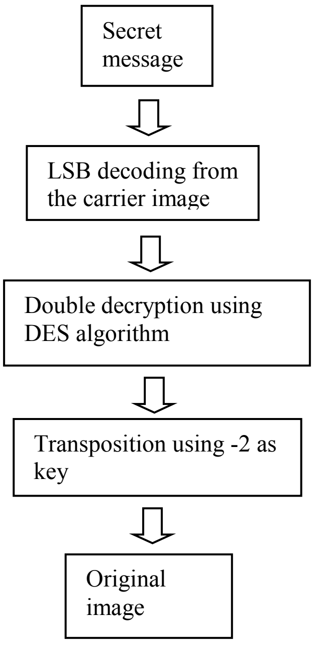
Secret message
LSB decoding from the carrier image
Double decryption using DES algorithm
Transposition using -2 as key
Original image

Fig. 2: Decryption process

A. Transposition using +2 as key

In Transposition [15], the ASCII value of each and every character is added with 2. This is done so as to make the encryption technique stronger. Example:

Input	Output
HELLO	JGNNQ

B. DES Algorithm

Data Encryption Standard algorithm is a block code, which means that the algorithm and the encryption key will be substituted to a block of data rather than to a single bit at an instance. DES categorizes the normal text into blocks of 64-bit in order to encrypt them. Each block of data will be encrypted with a help of a secret key through permutation and substitution. The entire process runs for 16 rounds in four different modes. The blocks may be encrypted individually or it can be made dependent on previous blocks. In our algorithm we encrypt the message with double DES encryption i.e. we use the DES algorithm twice.

C. LSB encoding in the carrier image

The information hiding is done with the help of encoding the bits at the LSB positions of the carrier image.

1. The information in converted into a string of 8 bits.
2. The string in divided into substrings of 2 bits.
3. These 2 bits are replaced with the last 2 bits of the pixels in the carrier image.

This is illustrated with an example:

Carrier image:

234	210
101	215

Information: “A”

ASCII equivalent of “A” is 65

Equivalent 8 bit binary of 65 is 01000001

After dividing into substrings we get 01, 00, 00, and 01.
The binary values of the carrier image are:

234 -> 111010**10**
210 -> 110100**10**
101 -> 011001**01**
215 -> 110101**11**

Replace the last 2 bits with the substrings of the information and convert back to decimal form:

111010**10** -> Replacing with ‘01’ -> 111010**01 ->** 233
110100**10** -> Replacing with ‘00’ -> 110100**00** -> 208
011001**01** -> Replacing with ‘00’ -> 011001**00** -> 100
110101**11** -> Replacing with ‘01’ -> 110101**01** -> 213

Carrier image:		Stego image:	
234	210	233	208
101	215	100	213

978-1-5090-5434-3©2017 IEEE

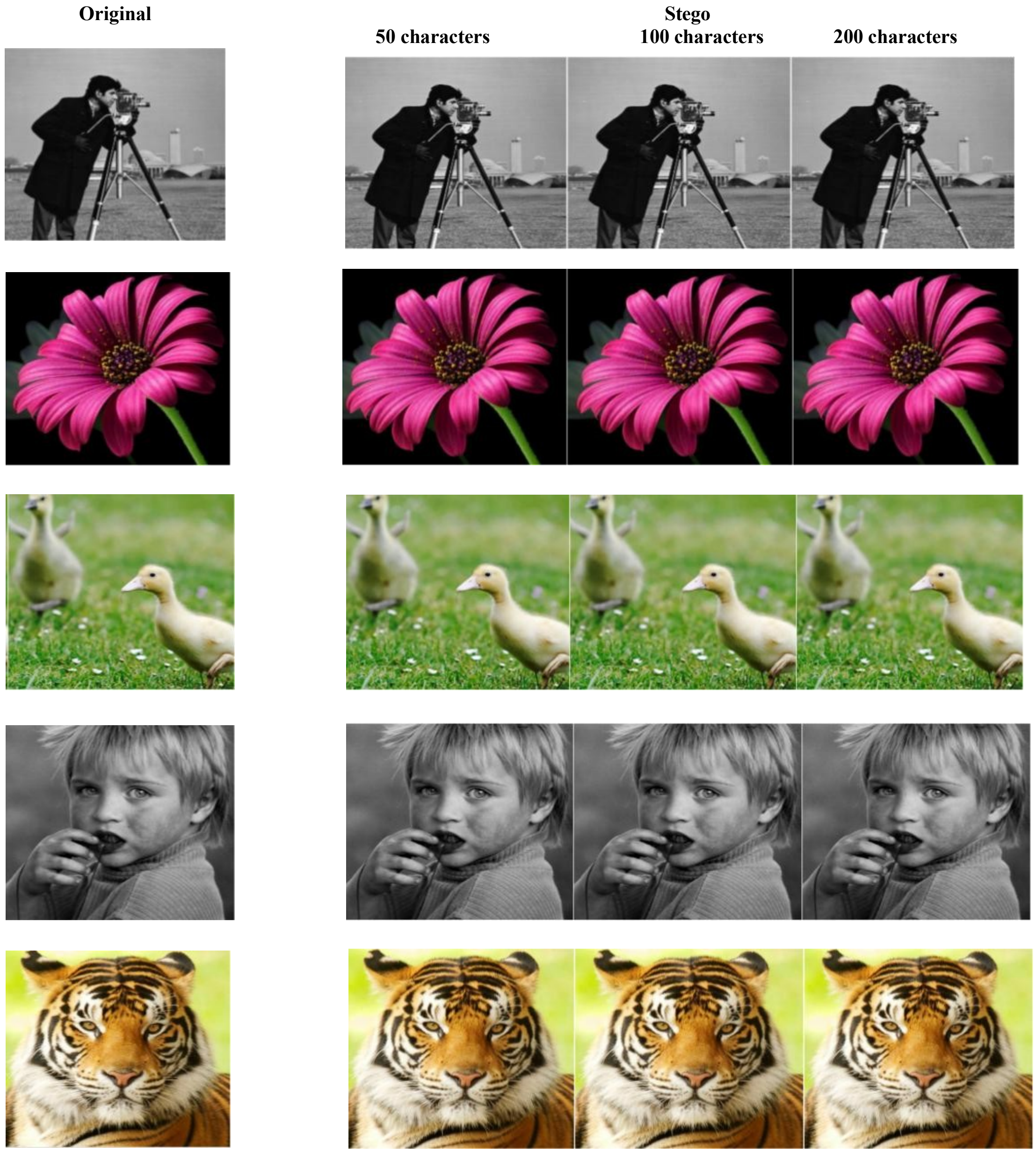

Fig. 3: Images (Cameraman, Birds, Flower, Baby, Tiger)

	50 characters		100 characters		200 characters	
Image name	MSE	PSNR	MSE	PSNR	MSE	PSNR
Cameraman	0.0017	51.7609	0.0033	48.8802	0.0052	46.9053
Flo	0.002	50.6411	0.0037	48.3833	0.0067	45.8046
Bi	0.00017	61.7354	0.00041	57.9008	0.0008	54.9354
Ba	0.00062	56.0734	0.0011	53.6514	0.0023	50.4481
Ti	0.00032	58.886	0.00056	56.5586	0.00097	54.1644

Table 1: MSE and PSNR value

978-1-5090-5434-3©2017 IEEE

D. LSB decoding in the carrier image

Decoding of the carrier image is just the reverse of the previous process.

1. Each index of the carrier image is converted to its binary equivalent.
2. The last 2 bits of these indexes are concatenated until the size becomes the size of original information.
3. Finally these are converted to decimal form which is then converted to equivalent character form.

This is illustrated with an example:

Stego image:

233	208
100	213

Binary values of the stego image are:

233 -> 111010**01**
208 -> 110100**00**
100 -> 011001**00**
213 -> 110101**01**

After concatenating the last 2 bits of the above values is: **01000001**

Decimal value of the above binary value is 65

Equivalent character of **65** is “A”

Thus the original data is retrieved.

The encoding and decoding of the information in the carrier image is in the form of a SPIRAL format. By this method the traversing of the image becomes complicated as compared to normal array traversing. Thus it increases the complexity of the encryption process and making it difficult for the intruder.

An example of SPIRAL traversing is given below: Matrix:

4	2	10
8	1	5
9	3	12

Spiral traverse:

4, 2, 10, 5, 12, 3, 9, 8, 1

IV. Results and Discussion

A comparison between the original image and the stego-image of 50, 100 and 200 characters is in Fig. 3 and Table 1.

V. Conclusion

Thus the security of data during its transmission has been taken care by converting it into a cipher text using cryptographic algorithm like DES and then it has been embedded into images with varying dimensions and tested with messages of different length. The required results of various tests have been obtained and tabulated.

Acknowledgment

We would like to thank SASTRA University for providing an effective environment to carry out our project by giving us necessary infrastructure facilities and thereby motivating us in every way possible.

References

[1] Wu HT “Secure JPEG steganography by LSB matching and multi-brand embedding”, IEEE International conference on image processing, November 2014, Article number 6116235, Pages 2737-2740.

[2] Gupta R “New proposed practice for secure image combining cryptography steganography and watermarking based on various parameters”, International Conference on Contemporary Computing and Informatics , November 2014, Article number 7019643, Pages 475-479 .

[3] Baek J “(N, 1) secret sharing approach based on steganography with gray digital images”, IEEE International Conference on Wireless Communications, Networking and Information Security,2010, Article number 5541793,Pages 325-329.

[4] Bajwa IS “A new perfect hashing based approach for secure steganograph”, 6th International Conference on Digital Information Management” September 2011, Article number 6093325, Pages 174-178.

[5] Bouslimi D “Data hiding in encrypted images based on predefined watermark embedding before encryption process”, MEDECOM, Plougastel Daoulas, France, Volume 47, 1 September 2016, Pages 263-270.

[6] Zhang W “Reversible data hiding in encrypted images by reversible image transformation”, University of Science and Technology of China, Hefei, China, Volume 18, Issue 8, August 2016, Article number 7470523, Pages 1469-1479.

[7] Khodaei M “Adaptive Data Hiding, Using Pixel-Value-Differencing and LSB Substitution”, Institute for Advanced Studies in Basic Sciences (IASBS), Zanjan, Iran, 14 August 2016, Pages 1-12.

[8] Conci A “AES cryptography in color image steganography by genetic algorithms”, 12th IEEE/ACS International Conference of Computer Systems and Applications, Volume 2016-July, 7 July 2016, Article number 7507100.

[9] Panda SS “A secure approach to spatial image Steganography” , VIT University, Vellore, India, Volume 8, Issue 2, June 2016, Pages 13384-13400.

[10] Nilizadeh A “A novel steganography method based on matrix pattern and LSB algorithms in RGB images” ,Dept. of Artificial Intelligence Engineering, University of Isfahan, Isfahan, Iran, 31 May 2016, Article number 7482107, Pages 154-159.

[11] Sriram S, Karthikeyan B, Vaithiyanathan V, Raj MMA ”An approach of cryptography and steganography using rotor cipher for secure transmission”2015 IEEE International Conference on Computational Intelligence and Computing Research, ICCIC 2015, 17 March 2016, Article number 7435669.

[12] Karthikeyan B, Ramakrishnan S, Vaithiyanathan V, Sruti S, Gomathymeenakshi M “An improved steganographic technique using LSB replacement on a scanned path image”, International Journal of Network Security, Volume 16, Issue 1, January 2014, Pages 14-18.

[13] Charan GS, NithinKumar SSV, Vaithiyanathan V, Divya Lakshmi, Karthikeyan B “A novel LSB based image steganography with multi-level encryption”, ICIIECS 2014-2015, IEEE International Conference on Innovations in Information, Embedded and Communication Systems, 12 August 2015, Article number 7192867.

[14] Nithin Kumar SSV, Charan GS, Karthikeyan B, Vaithiyanathan V, Rajasekhar Reddy M “A hybrid approach for data hiding through chaos theory and reversible integer mapping”, International Conference on Computational Intelligence, Cyber Security and Computational Models, ICC3 2015; Coimbatore; India, Volume 412, 2016, Pages 483-492.

978-1-5090-5434-3©2017 IEEE