Image Steganography using Pseudo Random Number Generator

Huma Jabeen, Professor Abdul Wahid

***Abstract*—For communication of secret information from one place to another two techniques are used i.e. Cryptography and Steganography. Steganography involves hiding secret data in an appropriate digital carrier e.g. image, audio and video files whereas Cryptography converts the message into an illegible format. Recently Rajput et al. proposed a Steganography algorithm that uses the angular transformation concept and the secret data was hidden using 3-3-2 approach in an RGB image. Here we take advantage of both Steganography and Cryptography. The Steganography method helps in hiding the fact that a secret message is hidden inside an image whereas Cryptography method further converts the secret message into a form that could not be understood so that even if the observer finds out that something is hidden inside the image s/he is unable to extract it. The proposed method modifies the Rajput et al.'s algorithm by encrypting the secret message and thus making it secure. Encryption is done using a pseudo random number generated key and a two level XOR operation. A pseudo random number is generated for each character of the secret message which after being folded to a single digit key is further XORed with the secret message and the length of the secret message. The result of this encryption is a stego image with no significant visual differences.**

***Index Terms*—Steganography, Encryption, Angular transformation, Pseudo random number generator.**

I. INTRODUCTION

For the last many years the Internet has been extensively used as a medium for transferring information such as digital data and multimedia from one place to another. Internet is so popular because it is accessible to almost everyone and also data gets received within seconds. But where there is ease, there are difficulties too. The wide popularity of internet has attracted the unauthorized parties towards it. They can monitor our data and extract useful information from it [1, 13]. Thus cryptography and steganography are the two major methods of attaining security and preventing those unauthorized users from stealing our private data [2, 14, 9]. Steganography is a term derived from two Greek words'Steganos' and 'graphie'where 'Steganos' means 'covered' and 'graphie' means 'writing'. It is a technique in which the secret message is hidden inside a carrier which can be any multimedia object e.g. text, image, audio, video etc.
The message is hidden in such a way that only the sender and the receiver knows about the presence of the message inside the cover. Steganography is considered both as an art and science. It is considered as an art because in ancient time secret message was written with invisible ink. Also message was tattooed on the shaved head of slaves and then the hair was left to grow. At the receiving end, the head was shaved again to read that secret message. It is considered as science because today we can hide our digital information e.g. text, image, audio, video etc. inside another digital information in bit format. Steganography works on the fact that if an attacker has the knowledge of presence of any secret data in a file then he/she tries to decrypt it anyhow. But if no one has the knowledge of presence of any secret data, then an attacker can't apply any decryption algorithm [3]. Steganography uses a medium like an image, video, audio or text file to hide some information inside it in such a way that it does not attract any attention and looks like an innocent medium. Recently, images have been a very popular choice as a cover medium primarily because of its redundancy in representation and pervasiveness in applications in daily life [15, 12].

All image steganography systems, irrespective of the algorithms by which they are implemented adhere to the following terms -:

.

(i) Image: An image C is a discrete function assigning a color vector c(x, y) to every pixel (x, y).

(ii) Cover Image: The cover image is the carrier inside which the secret message is hidden. A cover is generally chosen in such a manner that it appears most ordinary and innocuous and does not attract any suspicion as such.

(iii) Stego Image: The cover image with a secret message concealed within it is known as the Stego image. It is used at the recipient site for extracting the hidden message.

(iv) Stego Key: Stego key is a key used to embed data in a cover and extract data from the stego medium. It may be a number generated via a pseudo-random number generator orcan just be a password for decoding the embedding location. This key is optional.

(v) Embedding Domain: The Embedding domain refers to the characteristics of the cover medium that are exploited to embed message into it. The two types of embedding domain are spatial domain and transform domain. In spatial domain the constituent elements of the cover is directly modified (e.g. pixels in an image) whereas in transform or frequency domain some mathematical transformations are carried on the cover medium before embedding [4].

A good image steganography technique aims at three aspects: First one is capacity (the maximum amount of data that can be embedded inside the cover image). Second one is the imperceptibility (the visual quality of stego-image after

Manuscript received March, 2019.
***Huma Jabeen**, School of CS & IT, MANUU, (e-mail: humajabeen202@gmail.com). Hyderabad, India.*
***Professor Abdul Wahid**, School of CS & IT, MANUU, Hyderabad, India,, (e-mail: wahidabdul76@yahoo.com).*

hiding the data inside it) and the last one is robustness [5, 16]. In the image steganography, several algorithms are proposed [17, 18, 19], all of which can be grouped in either spatial or frequency domains. In the spatial domain algorithms, the "Message" is hidden in the "Cover-Image" by changing pixels' values, such as LSB (Least Significant Bit), OPAP and PVD (Pixel Value Differencing). Frequency domain algorithms hide the "Message" by changing the frequency coefficient of the "Cover-Images", such as Outguess, F5 and YASS (Yet Another Steganographic Scheme that resists blind steganalysis) [6].

The aim of this paper is to add encryption to the algorithm discussed by G. G. Rajput and Ramesh Chauvan [7]. The result of this encryption will be a more secure algorithm [2, 8].

II. Objective

Following are the objectives of this research work:

- To collect data and create an algorithm.
- To provide encryption to the secret message.

III. Research Methodology

The proposed research methodology is a modification to the algorithm presented by G.G. Rajput et al. First the 90^0 angular transformation of image is performed. Then the encrypted secret data is hidden into the LSBs of Red, Green and Blue planes of the image. Encryption is performed using a pseudo random number generator. The number generated by the pseudo random number generator is folded to a single digit key which is further XORed with each character of the secret message and the length of the message iteratively.

Cipher Text = (ASCII value of secret text XOR key) XOR word length.

The embedding algorithm is described below.

Embedding Algorithm

Input- Secret text data and onion.png RGB image from Matlab2017b

Output- onion.png image with hidden text

1. Read image.
2. Perform rotation of 90 degrees.
3. Get LSBs of all the 3 channels.
4. Read secret message.
5. Convert it into ASCII format.
6. Generate a random number e.g. of 3 digits and produce a single digit key by folding method.
7. Cipher text = (ASCII value of secret message XOR key) XOR word length.
8. Insert the cipher text in the RGB components of the pixel.
9. Repeat steps 6-8 for every letter of secret message.
10. Perform reverse angular transformation.

The block diagram representation of encryption algorithm is shown in fig.1.

Secret data retrieval is done using the following algorithm:

Extraction Algorithm

Input- Secret data embedded onion.png image

Output- Secret data extracted

1. Read stego image.
2. Perform rotation of 90 degrees.
3. Extract the hidden binary value from the LSBs of all the three channels.
4. Divide the hidden value into 8 bit sections.
5. Extracted text = (Word length XOR key) XOR extracted binary value.

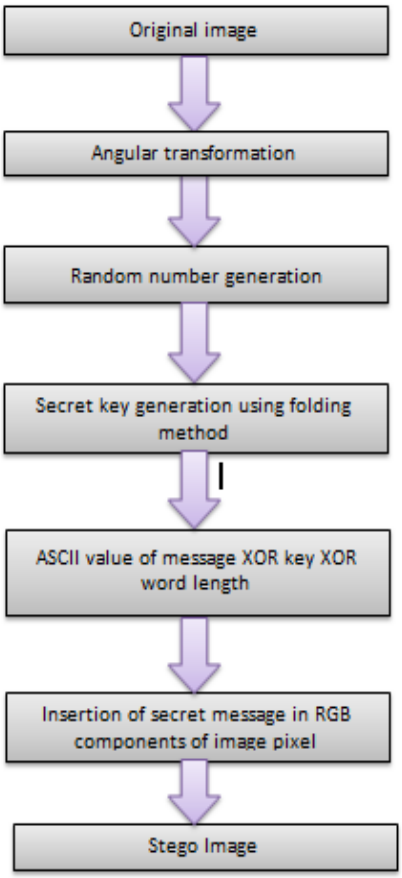


Fig.1.Block diagram representation of Encryption Algorithm

Fig. 2 is the block diagram representation of decryption algorithm:

IV. Data Analysis

The proposed technique is implemented to hide the same secret message in cover image, e.g.Onion.png of Matlab18a trial version.

The *MSE* and *PSNR* are obtained by Equation (1) and (2), respectively [9, 10, 11, 12].

MSE and *PSNR* are used to determine the quality of stego-image and the imperceptibility of hidden data.

PSNR is Peak Signal to Noise Ratio. It is utilized as a performance measurement for the distortion of the image. It

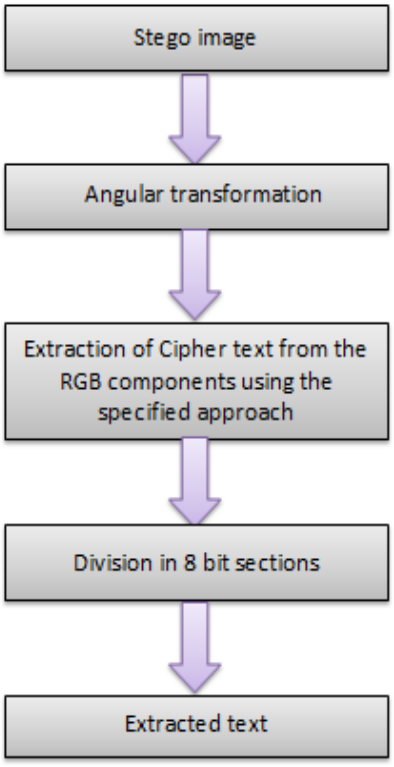


Fig.2.Block diagram of Decryption Algorithm

measures the image quality through a comparison between the cover image *C* and the stego-image *S*. It is defined as:

$$PSNR(C, S) = 10\log_{10}(2^d\text{-}1)^2/MSE \quad (1)$$

Where, *d* denotes the bit depth of the cover image, and is equal to 8 for gray-scale images.
MSE represents the cumulative mean square error between the cover image and the stego-image. It is defined as:

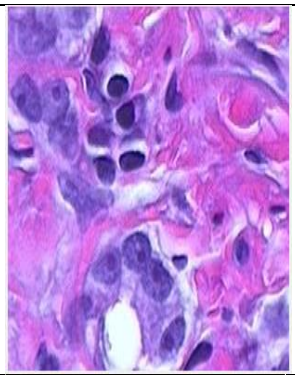
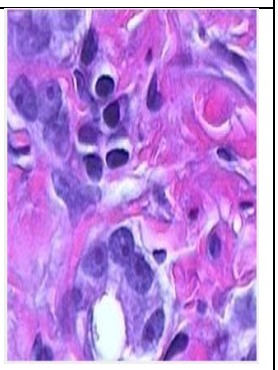
$$MSE(C, S) = 1/MN \sum_{i=1}^{M} \sum_{j=1}^{N} (S_{ij}.C_{ij}) \quad (2)$$

Where, *Sij*and *Cij*denote the pixel values of the cover image and the stego-image, respectively. *M* and *N* represent the dimensions of the cover image.

The result of the performance evaluation of the stego image is as follows:
The Mean Square Error generated is 0.0003.
The SNR value is 76.3630.
The PSNR value is 83.3699.

V. Experimental Results

The performance evaluation result is very high. The stego image obtained shows no visual difference.
The comparison between original image and stego image is shown in the following table.

Name	Original Image	Stego Image
onion.png		
hestain.png		
tape.png		

.

The MSE, SNR and PSNR values of the stego images discussed above are shown in the table below:

Name	**Size**	**MSE**	**SNR**	**PSNR**
onion.png	43.5KB	0.0003	76.3630	83.3699
hestain.png	128KB	0.0001	86.1351	88.9722
tape.png	277KB	0.0000	83.3906	93.0505

VI. Conclusion

Steganography is an effective way to hide sensitive information. In this paper, the researcher has used the LSB Technique and Pseudo-Random Number Generation Technique on images to obtain secure stego-image. The security has been further increased by XORing the secret message on two levels. The resultant Stego images show no visual difference in comparison to original images. The image resolution doesn't change much and is negligible when

we embed the message into the image and the image is protected with the personal key. So, it is not possible to damage the data by unauthorized personnel.
On the basis of the results obtained from the proposed algorithm, it can be concluded that the proposed algorithm provides better capacity and has no visual difference.

ACKNOWLEDGMENT

This research was supported by my Supervisor Prof. Abdul Wahid, Dean, School of CS&IT, Department of CS&IT, MANUU, Hyderabad. I thank him for consistently providing me with the required guidance to help me in the timely and successful completion of this research work.

REFERENCES

[1]. Osama S. Faragallah, Ahmed ELmhalawy, Gh. M. El-Banby Khalid A. Al-Afandy El-Sayed M. EL-Rabaie, "High Security Data Hiding Using Image Cropping and LSB Least Significant Bit Steganography," in *IEEE*, 2016.

[2]. K.S. Subalakshmi,Anishin Raj M M,V.Vaithiyanathan, B.Karthikeyan, A. Deepak, "A Combined Approach of Steganography with LSB Encoding technique and DES Algorithm ," in *3rd International Conference on Advances in Electrical, Electronics, Information, Communications and Bio-Informatics*, Kerala,India, 2017.

[3]. Sunny Dagar, "Highly Randomized Image Steganography using Secret Keys," in *IEEE International Conference on Recent Advances and Innovations in Engineering*, Jaipur, India, 2014.

[4]. Anirban Sarkar, Narayan C Debnath, Ratnakirti Roy Suvamoy Changder, "Evaluating Image Steganography Techniques: Future Research Challenges," in *IEEE*, 2013.

[5]. Shahbaaz Khan, Nadeem Akhtar, Pragati Johri, "Enhancing the Security and Quality of LSB based Image Steganography," in *5th International Conference on Computational Intelligence and Communication Networks,IEEE*, 2013.

[6]. Ahmad Reza Naghsh Nilchi, Amirfarhad Nilizadeh, "A Novel Steganography Method Based on Matrix Pattern and LSB Algorithms in RGB Images," in *1st Conference on Swarm Intelligence and Evolutionary Computation, IEEE*, Iran, 2016.

[7]. Ramesh Chavan, G. G. Rajput, "A Novel Approach for Image Steganography based on LSB Technique," in *ICCDA,ACM*, 2017.

[8]. Md. Ismail Hossain, S. M. Masud Karim, Md. Saifur Rahman, "A New Approach for LSB Based Image Steganography using Secret Key," in *14th International Conference on Computer and Information Technology*, Dhaka, Bangladesh, 2011.

[9]. Shuhua Lai, Shuting XuAn, "Optimal Least Significant Bit Based Image Steganography Algorithm," in *ICIMCS, ACM*, 2014.

[10]. Madhupama Chakraborty, Pallavi Das, Satish Chandra Kushwaha, "Data Hiding Using Randomization and Multiple Encrypted Secret Images," in *ICCSP, IEEE*, 2015.

[11]. May H.Abood, "An Efficient Image Cryptography using Hash-LSB Steganography with RC4 and Pixel Shuffling Encryption Algorithms," in *Annual Conference on New Trends in Information & Communications Technology Applications, IEEE*, 2017.

[12]. Muhmmad Ismail, Nasru Minallah, Tawab Khan Sahib Khan, Nasir Ahmad, "A Secure True Edge based 4 Least Significant Bits Steganography," in *IEEE*, 2015.

[13]. Vijay Anand J and Dharaneetharan G.D, "New Approach in Steganography by Integrating Different LSB Algorithms and Applying Randomization Concept to Enhance Security," in *ICCCS, ACM*, Rourkela, Odisha, India, 2011.

[14]. Kamaldeep Joshi, Rajkumar Yadav, "New Approach toward Data Hiding Using XOR for Image Steganography," in *IEEE*, 2016.

[15]. Mohanjeet Kaur, Mamta Juneja, "A New LSB embedding for 24-bit pixel using Multi-Layered Bitwise XOR," in *IEEE*, 2016.

[16]. Unik Lokhande, A. K. Gulve, "Steganography using Cryptography and Pseudo Random Numbers," in *International Journal of Computer Applications, Volume 96*, June,2014.

[17]. Prateek Thakral, Naveen Jarwal, Aman Arora, Manish Pratap Singh, "Image Steganography using Enhanced LSB Substitution Technique," in *Fourth International Conference on Parallel, Distributed and Grid Computing, IEEE*, 2016.

[18]. Rupali Bhardwaj, "Multimedia Security through LSB Matching," in *ICTCS, ACM*, Udaipur, India, 2016.

[19]. Chi-Kwong Chan, L.M. Cheng, "Hiding data in images by simple LSB substitution," in *Pattern Recognition Society, Elsevier Ltd.*, 2003.

[20]. R M Samant, S Agrawal, "Data Hiding In Gray-scale Images Using Pixel Value Differencing," in *International Conference and Workshop on Emerging Trends in Technology, ACM*, Mumbai, Maharashtra, India, 2011.