International Journal of Current Trends in Engineering & Technology
ISSN: 2395-3152
Volume: 02, Issue: 02 (MAR-APR, 2016)

CECIMG: an STE-Cryptographic Approach for Data Security in Image

Naveen Jain[1], Jitendra Rai[2], Kailash Patidar[3]
[1]naveen.jain01@gmail.com, [2]rai.jitendra42@gmail.com, [3]kailashpatidar123@gmail.com
SSSIST, Sehore, India

***Abstract:* - Data security and its mechanism found an importance role while data storage and sharing in any media. Intruder activity is often occurring in case of some authentic area such as military or government project. Thus to obtain a security of data via image is performed via securing the data first using encryption technique and further the LSB steganography is performed by previous authors. Thus the LSB make use of least significant bit to store the data and further image to be transferred and further via de-steganography approach data can be retrieve. Still the traditional algorithm is well known and understands today to decode, also the encryption technique utilized is not much strengthful. Thus to avoid these drawback and limitations, our work present CECIMG (Canny edge encryption image steganography) algorithm which present the effective storage of data in series way storage and retrieval. The algorithm found to be more secure than the existing LSB and other steganography approach. Our approach also follows canny edge along with blowfish encryption approach for data security. Our approach is implemented via JDK8.0 API and experiment is performed, thus the proposed algorithm is found best as compare with existing technique.**

***Keywords:* - data authenticity, encryption over data, data hiding, multi-level approach.**

I. INTRODUCTION

Information hiding is a science which dates back to 1499, and it has long history. It has been used in various forms for 2500 years. It has found use in military, diplomatic, personal, spies, ruler, governments etc. Steganography has been widely used, including in recent historical times and the present day. Some known examples include: Past Early steganography was messy. Before phones, before mail, before horses, messages were sent on Foot. If you wanted to hide a message, you had two choices: have the messenger memorize it, or hide it on the messenger. While information hiding techniques have received a tremendous attention recently, its application goes back to Greek times. - according to Greek historian Herodotus, the famous Greek tyrant Histiaeus while in prison, used unusual method to send message to his son in- law. He shaved the head of a slave to tattoo a message on his scalp. Histiaeus then waited until the hair grew back on slave's head prior to sending him off to his son-in-law. Herodotus provides the first records of steganography in Greece [13]. - To communicate Greeks would etch the message they wished to send into the wax. - Coating of a wooden tablet. The tablet would then be transported to the recipient who would read the message, then re-melt the wax to etch their reply. In order to communicate in secret, the army would remove the wax completely, carve thesecret message into the wood, and re-coat the tablet with wax [13]. - Messages were also written on envelopes in the area covered by postage stamps to avoid the possible detection of the message. Present In today's generation, as most of the people often transmit images, audio over the internet, so most of the Steganography systems uses multimedia objects like image, audio and video as cover sources to hide the confidential data [14]. So, on the basis of this, steganography is divided into four categories: Text Steganography, Image Steganography, and Audio/Video Steganography Protocol Steganography. Future Strength analysis can be defined as process to crack the cover object in order to get the hidden data. In general terms, it is known as hacking i.e. unauthorized access of data during transmission. Future perspective of steganography lies on combining steganography with cryptography to achieve a higher level of security such that even if intruder detects the hidden message, no one can be able to decode it. LSB (Least Significant Bit) method is a standout amongst the most well-known and least demanding techniques for message covering up. In this system, message is covered up at all critical bits of picture pixels .Changing the LSB of the pixels does not present much distinction in the picture and in this way the steno picture appears to be like the first picture. In the event of 24- bit pictures three bits of pixel can be utilized for LSB substitution as every pixel have separate parts for red, green and blue [8].

II. RELATED WORK

The recent work in the field of secure image and data hiding approach in image is performed by authors [2]. In this work author performed LSB steganography using DES with S box strength as encryption model before hiding data in the image. They have been worked with three criteria operation work as capacity, robustness and the security of data. Where these entire three models is been done by three different modules such as LSB steganography where the least significant bits were used to further define the pixels where data is going to get store. Also before storing the data first a security cryptographic algorithm is performed this is DES (Data encryption system) for changing plaintext original data into the cipher text data. Upon selecting and data conversion into cipher text, the pixels are converted to decimal and further the least significant bits were calculated and then steganography is performed on those LSB positions. The two S –box s0 and s1 is used in the encoding model as well as decoding model from the complete flow. Finally a formation of steno image is done at user conversion end. The reverse process is applied for the decoding approach and to obtain the original input from the user. The experiment performed by them in 64*64 dimension image and PSNR is computed for the data. The average PSNR in DB value is found to be approx. 55.

III. PROPOSED WORK

The work discussed in literature contains the different approach for data security which increase the key length and provide the data security, the further approach can apply to enhance LSB to E LSB technique for the proposed work along with the symmetric key encryption technique which provide the high resolution with low computation time for the encryption and decryption as compare to other approach. Thus a symmetric key encryption and E-LSB approach can be further develop to maximize the security. In ELSB, we use all the edge pixels in an image. Here, we first calculate the masked image by masking the two LSB bits in the cover image. Then we identify the edge pixels by using the Canny Edge detection method. After obtaining the edge pixels we hide the data in the LSB bits of the edge pixels only and send the stego object to the receiver. At the receiver, the stego object is again masked at the two LSB bits. Then the canny edge detector is used to identify the edge pixels. We will get same edge pixels at the sender and receiver since we used the same masked image to calculate the edge pixels. Thus we identify the bits where data is hidden. Our approach use the following phases to compute the experiment using proposed technique: Computing Blowfish Encryption: a blowfish encryption algorithm is used for cipher text generation from plaintext, which are symmetric key encryption technique claims the secure encryption compare with DES. E-LSB: by using canny edge detection the edges pixel chosen for the cipher text data hiding in the edges been performed at this stage.

Algorithm CECIMG:

```
    Input: plaintext, key, base image.
    Output: Stenographic image, key.
    Steps: Begin
    Encoding model {
    Select base image as b-img;
    Select output image name o-img;
    Choose the algorithm to perform encryption and stenographic approach;
    Performing data encryption by providing the key from the user;
    Choosing edges for message hiding;
    Performing Embed function and generate the output image o-img;
    }
    Decoding model {
    Select output image name o-img;
    Choose the algorithm to perform reverse process;
    Performing data decryption by providing the key from the user;
    Obtain the original data and showing to the user;
    }
    End;
```

The complete algorithm for the encoding model and decoding model is performed using which the data security can be obtain via cryptography and steganography approach. The complete flow of the system is mentioned in figure 1. This diagram illustrate the mechanism is performed in our approach.

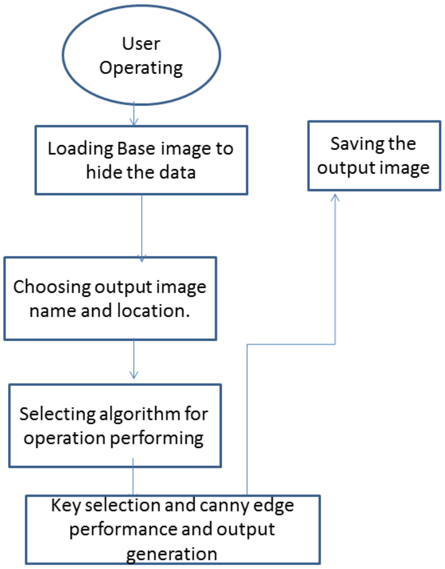
User Operating
Loading Base image to hide the data
Saving the output image
Choosing output image name and location.
Selecting algorithm for operation performing
Key selection and canny edge performance and output generation

Figure 1: proposed algorithm flow.

IV. EXPERIMENTAL & RESULT ANALYSIS

Our proposed algorithm is performed using JDK 8.0 API, where the Utilized system configurations as Windows 10 OS, 4 GB RAM, 750 GB hard disk, i3 processor. The experiment performed on net beans IDE and algorithm is executed on different images. Upon performing the result analysis on algorithm with LSB and Canny edge detection and steganography on it. The following results were obtained by performing experiment using DES-LSB and CECIMG algorithm.

Image Name	Capacity	PSNR in DB
Baboon	25%	55.5
Lena	25%	59.2
Pirate	25%	51.6
Living room	25%	50.1

Table 1: results obtain using Existing algorithm model.

The given tables represent the result from the existing approach where the capacity of the image and computed PSNR in DB is stated which is further compared with proposed algorithm.

Image Name	Capacity	PSNR in DB
Baboon	25-35%	59.6
Lena	25-35%	62.8
Pirate	25-35%	51.9
Living room	25-35%	58.2

Table 2: results obtain using proposed algorithm.

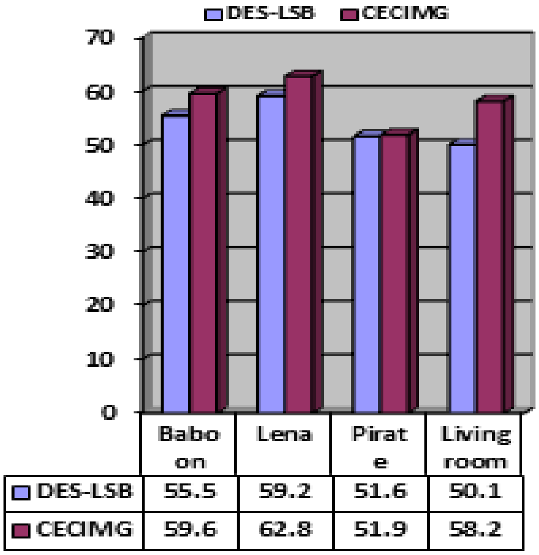

Figure 2: comparison analysis bar graph between existing & proposed technique.

V. CONCLUSION

Data security and its usage at different secure sector is an important task in every area. In this paper proposed algorithm CECIMG is introduced where the algorithm aims to produce an effective output image where data with high security and in best way it can be store and utilized. The algorithm makes use of blowfish encryption technique along with canny edge detection for hiding data over image. Upon performing simulation using java platform the result computed shows the efficiency of the proposed algorithm over the existing scenario, the work can be implemented in real time for computing high security. The proposed work can be further implement with cloud service where the data can be outsource to cloud in image form via CECIMG algorithm.

REFERENCES

[1]. Md. Rashedul Islam1, Ayesha Siddiqa2, Md. Palash Uddin3, Ashis Kumar Mandal4 and Md. Delowar Hossain "An Efficient Filtering Based Approach Improving LSB Image Steganography using Status Bit along with AES Cryptography" IEEE 2014.

[2]. Manoj Kumar Ramaiya, Naveen Hemrajani, Anil Kishore Saxena, "Security Improvisation in Image Steganography using DES", IEEE 2014.

[3]. H. Yang, X. Sun and G. Sun, "A High-Capacity Image Data Hiding Scheme Using Adaptive LSB Substitution", Journal: Radio engineering, vol. 18, no. 4, (2009), pp. 509-516.

[4]. S. Channalli and A. Jadhav, "Steganography an Art of Hiding Data", International Journal on Computer Science and Engineering, IJCSE, vol. 1, no. 3, (2009).

[5]. C.-H. Yang, C.-Y. Weng, S.-J. Wang, Member, IEEE and H.-M. Sun, "Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems", IEEE Transactions on Information Forensics and Security, vol. 3, no. (2008) September 3, pp. 488-497.

[6]. K.-H. Jung, K.-J. Ha and K.-Y. Yoo, "Image data hiding method based on multi-pixel differencing and LSB substitution methods", Proc. 2008 International Conference on Convergence and Hybrid Information Technology (ICHIT '08), Daejeon (Korea), (2008) August 28-30, pp. 355-358.

[7]. H. Zhang, G. Geng and C. Xiong, "Image Steganography Using Pixel-Value Differencing", Electronic Commerce and Security, ISECS '09. Second International Symposium on (2009) May.

[8]. W. J. Chen, C. C. Chang and T. H. N. Le, "High Payload Steganography Mechanism Using Hybrid Edge Detector", Expert Systems with Applications (ESWA 2010), vol. 37, pp. 3292-3301, April 4, 2010.

[9]. V. Madhu Viswanatham and J. Manikonda, “A Novel Technique for Embedding Data in Spatial Domain”, International Journal on Computer Science and Engineering, IJCSE, vol. 2, (2010).

[10]. M. A. Al-Husainy, “Image Steganography by Mapping Pixels to Letters”, Journal of Computer Science, vol. 5, no. 1, (2009), pp. 33-38.

[11]. H. Motameni, M. Norouzi, M. Jahandar and A. Hatami, “Labeling Method in Steganography”, World Academy of Science, Engineering and Technology, France, (2007).

[12]. B. Ahuja, M. Kaur and M. Rachna, “High Capacity Filter Based Steganography”, International Journal of Recent Trends in Engineering, vol. 1, no. 1, 2009.

[13]. M. Tanvir Parvez and A. Abdul-Aziz Gutub, “RGB Intensity Based Variable-Bits Image Steganography”, IEEE Asia-Pacific Services Computing Conference, (2008), pp. 1322-1327.

[14]. A. M. Hamid and M. L. M. Kiah, “Novel Approach for High Secure and High Rate Data Hidden in the Image Using Image Texture Analysis”, International Journal of Engineering and Technology (IJET): 0975-4042, (2009).

[15]. Awsnaserjaber, mohamadfadli bin zolkipli, 2013, “use of cryptography in cloud computing”.

[16]. Vijay .g.r, a. Rama Mohan reddy, 2012, “an efficient security model in cloud computing based on soft computing techniques.

[17]. Tamimi A. Al., "Execution Analysis of Data Encryption Algorithms", Oct 2008.