International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2020 IJSRCSEIT | Volume 6 | Issue 3 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/IJSRCSEIT

EDGE Based Algorithm for Encryption and Decryption Text into Images

Prof Manjunathraddi Bentur*, Prof. Shashidhar P K, Deepa Chakalabbi, Prabhavati Hosalli, Shridhar Kumbar, Kavya Megalgeri

Department of ECE, SKSVMACET, Lakshmeshwar, Karnataka, India

ABSTRACT

In this approach, we propose a new algorithm to hide the secrete data in the image by using the steganography technique. In this algorithm, we used the binary codes and pixels inside the image. Hiding the information and communicating a secret text or data in a proper multimedia camera is strongly introduced in steganography. For example. Text, image, audio & video files. The original steganography techniques are used in this approach, consider in the image edges have been used to insert the message or data in terms of text. The amount of information is fixed and plays an important part while selecting the edges of the image, i.e. the more amount of information is to be fixed, the longer we use and feebler edges for embedding.

Keywords : Steganography Procedure, Top-Secret Key, Information Retrieval

I. INTRODUCTION

A procedure is used to design hiding the information which is given as input inside the image, which will protect the secrecy of the information. At that time, based on the arrangement of steganography procedure is established. This future scheme offers an image policy for users to the input image and a text box to insert texts. Once the recommended system is reformed, one user can send stego image to another user of the computer so that receiver can user can send the stego image to other computer users so that the receiver can recover and recit the information which is buried in the stego image by using the same planned scheme.

In the steganography algorithm, there are many stages of levels to produce stego images with undetectable which are based on their performance. The image steganography method can be divided into two types: spatial domain and frequency domain. In the spatial domain, the secret data is injected straight to the image pixels, while in the latter case, cover images are transformed to the frequency domain and the secret information is inserted in the transform constants. Spatial and frequency domains are used to construct a steganography algorithm. The reason that challenges the security level is the number of lading capabilities in the stego image.

The selections of fixed pixels are used for the Security of any steganography method. For better choice pixels are nosy and textured area is used for embedding, because they are complicated to model. Pixels in edges can be seen as noisy pixels because their intensities are either higher or lower than their adjacent pixels due to sudden changes in the coefficient grade. Due to these sharp changes in the graphic and geometric properties, edges are difficult to model in comparison to pixels in Correspondence smoother area. Hence, the edges make a better option to cover secret information than any other area of an image where a small distortion is much morenoticeable.

II. LITERATUREREVIEW

S.No	Author	Algorithm	Conclusion
1.	Rosziati Ibrahim and TeohSuk Kuan.	To maintain the privacy, confidentiality, and accuracy of the message we have used two layers of security steganography algorithm and also used for hiding a secret message inside an image. For hiding the data, a username and password are required before use the system. Once the user has been login into the system, the user can use the information (data) together with the secret key to hide the data inside the chosen image.For retrieving the data, a secret key is required to retrieving back the data that have been embedded inside the image. Without the secret key, the data cannot be retrieved from the image.	A Steganography Imaging System has been developed using the proposed algorithm. We tested a few images with various sizes of data to be hidden. With the proposed algorithm, we found that the stego image does not have a noticeable distortion on it (as seen by the naked eyes). We also tested our stego images using PSNR value. Based on the PSNR value of each image, the stego image has a higher PSNR value. Hence this new steganography an algorithm is very efficient to hide the data inside theimage.
2.	Sanjeev Kumar, Amarphal Singh, Manoj Kumar.	In this algorithm, Inserting data in pixels areas recognized by existing conventional edge detection techniques like canny cannot ensure the recognition of the exact edge locations for the cover and stego images. The proposed algorithm ensures the exact edge location after embedding the message. In this algorithm, a fuzzy inference system to estimate the edge areas of the cover image is proposed. The proposed method correctly extracts the concealed information from the stego image.	The proposed technique effectively locates the sharper edges of cover images, utilized to embed secret information bits. The image edges after inserting the message are preserved so that it accurately retrieves the data at the intended receiver. Experimental results reveal that the proposed scheme achieves a better quality of stego images than other methods for the same embeddingcapacity rates.
3.	SaifulIslam, Mangat R Modiand Phalguni Gupta.	This algorithm involves Technique which hides secret messages in the edges of the carrier image. It is a delay of edge embedding in the color image. The canny edge detection technique has been used to get the exact edges. Inserting the choice edges is dependent on the length of the payload and the image. As the payload size increases, a weak threshold for the selection of edges is used so that more edges can be selected to accommodate the increased	Edges of the cover image data are to be hidden and based on the length of the message, select the random edges. The proposed technique can resist graphic, structural, and non- structural attacks better than the existing edge-based techniques. HBC is detected by structural detectors due to no males created by LSBsubstitution.

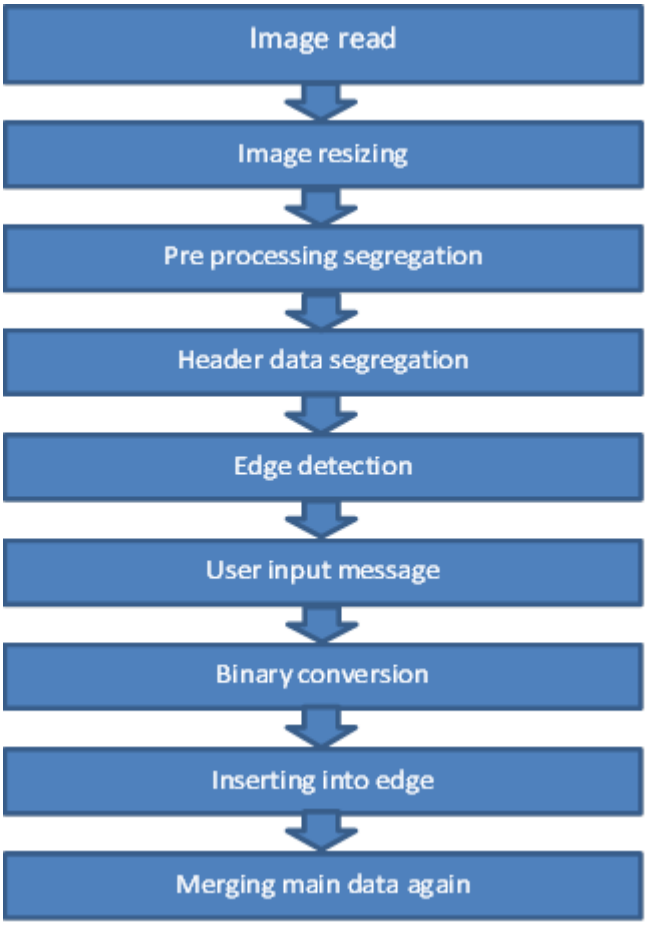
		amount of data. For a given payload, the sharpestpossible edgesare selected to embed the message.	
4.	Odai M. Al-Shatanawi and Nameer N. El. Emam.	In this algorithm, the image steganography has been proposed to hide a large amount of secret data obtained by a secret color image. It is based on different size image segmentation (DSIS) and modified least significant bits (MLSB), where the DSIS algorithm has been applied to embed a secret image randomly instead of sequentially; this approach has been applied before embedding process.	The algorithm is working effectively over an insecure channel and working against attacks by producing high undetectable stego images for both low and high payload. To make a secret image illegible by attackers for that here used (AES) advanced encryption standard. The aim of MLSBto increase the payloads and to improve security.

III. PROPOSEDALGORITHM

The proposed algorithm is based on two layers of security to maintain the privacy, confidentiality, and accuracy of the data. The system can hide the data inside the image as well as to retrieve the data from the image. Once the user has been login into the system, the user can use the data together with the secret key to hide the data inside the chosen image. Without the secret key, the data cannot be retrieved from the image. This makes sure the integrity and confidentiality of the data.

The secret key plays an essential role in this proposed algorithm where the key is acts as a locker that used to lock or unlock the secret message. For the data hiding method, each last two-bit is encoded into each pixel in an image. This will ensure the original image will not be moderated with too manychanges.

Sender part



To keep no changes in edges before and after embedding, the LSB of the cover image is masked, and edge detectors are applied on the masked cover images. Since LSB replacement does not modify any

bit other than LSB, a pixel of a cover image, the edges in cover and stego images remain identical as.It

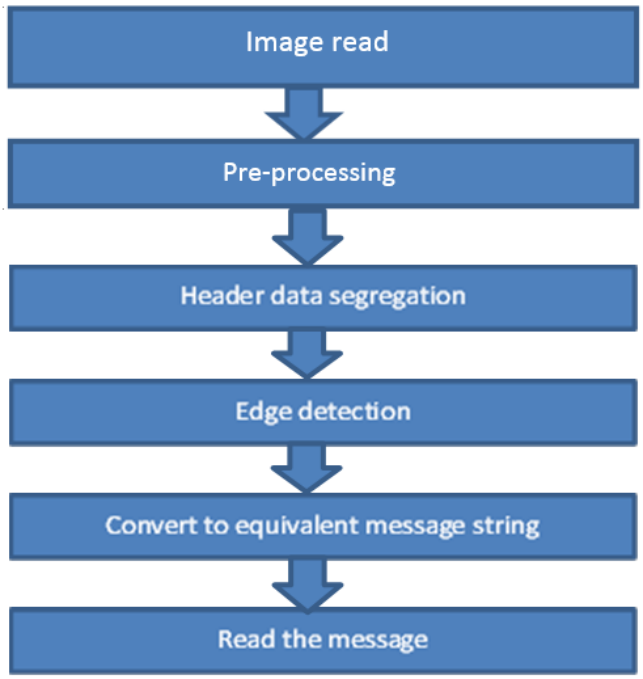
has been seen that the number of pixels belonging to edges does not change much by masking LSB or the least two significant bits. It can be noted that for both databases, the number of pixels belonging to edges is increased after masking 2LSB. Hence, masking at least two significant bits does not affect the edges in the cover image for most of the cases.

Most of the steganography techniques embed attain LSB of pixels in the cover image pixel. Embedding is done by either LSB replacement or LSB matching. LSB replacement is detected by most of the structural detectors, but LSB matching is reliably detected through non-structural detector SPAM and SRM. Hence, if one embeds in the LSB plane, then there is a high probability of detection of the presence of the message. To overcome these structural and non-structural detectors, inserting is done in the 2LSB plane of the cover image. Inserting in the 2LSB plane interrupts the basic assumption of structural detectors, and it has been observed that even SPAM and SRM areless.

Accurate in sensing the presence of the message for fewer amounts of data embedding in comparison to LSB replacement. It is shown in inserting in the 2LSB plane is better to embed in the LSB plane. A canny edge detection technique has been used. The selection of edges for embedding is dependent on the length of the payload and the image. As the payload size increases, a weak threshold for the selection of edges is used so that more edges can be selected to accommodate the increased amount of data, which consists of two primary tasks: threshold selection and embedding. The canny high threshold is founded by the threshold selection for that enough number of edges are nominated to insert the given payload in a cover image, while embedding is done by computing edge- map based onthe threshold.

Based on the stego key and the edge map, Inserted in a cover image in random order. The canny edge detector is randomly arranged using stego key P by calling random Permute (e, P). It makes sure that only the proposed users can extract data from the stego image. By using edge map e' we can modify the least two bits of pixels x, y to the corresponding, the secret message M is inserted in the casually permuted (S) in the order of two consecutive message bits are M index+1 and M index. The threshold and width are embedded in
non-edge pixels of the stego image. Non- edge pixel map e' is obtained by taking a complement of e for minimum values than bandwidth. The threshold bandwidth is embedded in the first 32 bits of S corresponding to e'. The image is reshuffled to get the stegoimage.

Receiver part



Extraction

It is the process to recover the amplified message from the given stego image. The threshold value and width are taken out from the non-edge pixels of the

stego image. Stego key has been used as the seed to modification the set of edge pixels.The embedding process is similar to the extraction. The least two significant bits of the stego image is covered, and edge map e is computed. The hidden image is altered using stego key P to restore them a message in the same order as it has been inserted. The value corresponding to the least. Message and few extra bits. Message size msg_size is pulling out from the first C bits of the payload which is used to restore the real message M [C+1:msg_size]. Further bits beyond msg_size are throwing away, and the secret message M is takenback.

The steganography system needs any type of image file and the information or message these are to be hidden. Steganography has two categories encrypt and decrypt. Microsoft.Net scheme prepares a vast amount of instrument and possibilities for programmers the sear simples programming. One of .Net instruments for pictures and images are auto-converting most types of pictures to BMP format.

This section offers a new Steganography technique that catches the secret messages in the edges of the conveyor image. The choice of edges forembedding is dependent on the length of the payload and the image. As the payload size increases, a weak threshold for the choice of edges is used so that more edges can be a choice to assist the higher amount of data. Threshold selection is to find a canny high threshold so that enough number of edges are choice to insert the given payload in a cover image while inserting is done by determining edge-map based on the threshold. The payload is embedded in a cover image in a random order based on the stego key and the edge map.

The implementation of the offered embedding algorithm has been applied in three colors to hide a secret image by using MLSB. One to four-bit(s) ofhiding depending on the value of NBTH, The value of NBTH is evaluated by proposed steganography algorithm for each color to reduce the distortion on stego image, it performs that the lowest value of NBTH of the blue color is equal to one due to small variance between TB and the surrounding NBs and the highest value of NBTH of the red color is equal to four due to large variance between TB and the surroundingNBs.

The distribution of edge detection is limited by the typical edge detection method in Steganography as cannot be seen the information would know some variations to the cover image. The typical edge detection techniques like canny are recognized areas of inserting data in the pixels that cannot make sure the recognition of the real edge locations for the cover and stego images. The offered method makes sure the real edge location after inserting the message, to estimate the edge areas of the cover image is proposed by a fuzzy inference system. The proposed method correctly extracts the hidden information from the stego image.

IV. RESULTS AND CONCLUSION

For implementing the proposed algorithm, we used PYTHON, which is one of the most suitable programming languages for image processing. Python is a popular high-level programming language and it is used for general-purpose programming.

Installing Python3.8, we have to check the installation properly by using the command prompt. For making this, we have to add python3.8 to PATH. Then set was successful, similarly, Pycharm is installed.

To run this, we should install: pip3 install openCV-python NumPy Try running script help:

Python steganography.py –help to encode some data to the image namedimage.PNG:

Python steganography.py -e image.PNG -t "This is some secret data."This will write another image named imaged_encoded.PNG with data encoded in it and outputs:
Maximum bytes to encode: 125028 Encoding data.
Saved encoded image.

To decode the data containing the image named encoded_image.PNG, use:

Python steganography.py -d encoded_image.PNG Decoding…

V. CONCLUSION

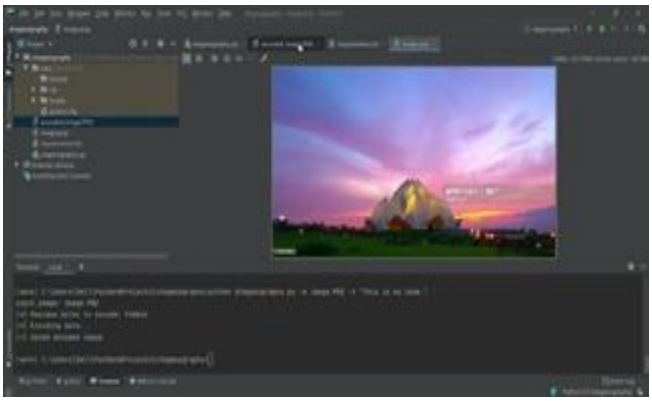


Figure.1: Originalimage

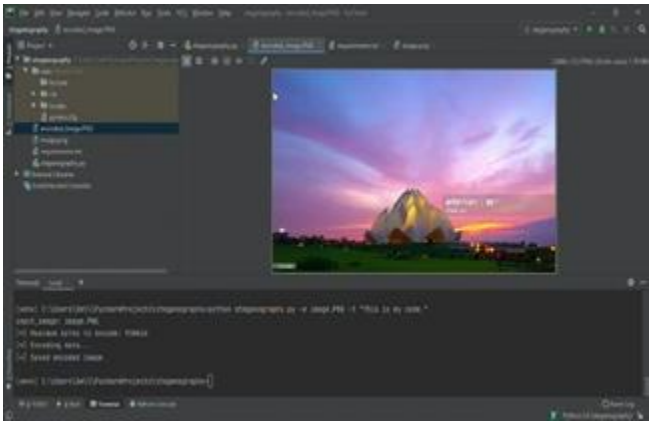


Figure.2: Encodedimage

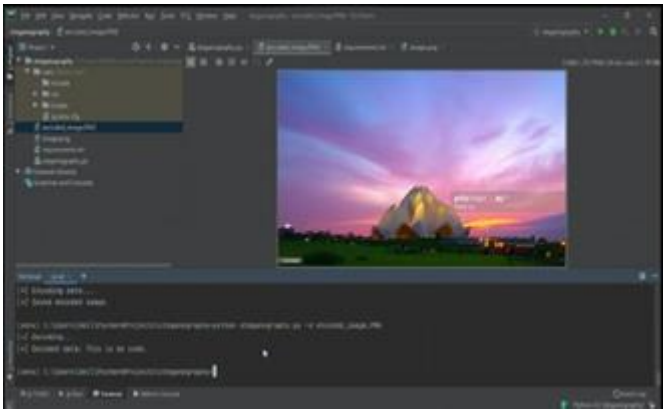


Figure.3: Decoded textimage

In this approach, Information in the form of text is hidden inside the images. The secret message is inserted in the selected cover image. Data are secretly hidden into edges that are randomly selected based the on text size. The proposed system of the LSB technique is free from structural attack.

VI. REFERENCES

[1]. Rosziati Ibrahim and Teoh Suk Kuan Faculty of Computer Science and Information Technology, University Tun Hussein Onn Malaysia (UTHM), BatuPahat 86400, Johor, Malaysia Received: November 25, 2010, / Accepted: January 10, 2011, / Published: February 25, 2011.

[2]. Saiful Islam, Mangat R Modi and PhalguniGuptaIslam et al. EURASIP Journal on Information Security 2014, 2014:8http://jis.eurasipjournals.com/content/2014/1/8.

[3]. Sanjeev Kumar a, Amarpal Singh b, Manoj Kumar c,Department of ECE, Beant College of Engineering & Technology, Gurdaspur, Punjab, India DAV Institute of Engineering & Technology, Jalandhar, Punjab,India.

[4]. Quist-aphetsiKester“Image Encryption based on the RGB PIXEL Traposition shuffling”july-2013.

[5]. Krishnan gupta “Different image encryption and decryption xor-techniques and kaimage cryptography”Dec-2013.
[6]. Monika Agarwal, Pradeep Mishra “A Comparative Survey on Symmetric Key Encryption Blowfish- Techniques”05May-2012.
[7]. Manishamankar,Dr.R.kshrisagar“Encryption and decryption using Rijndaelalgorithm”April-2015.

Cite this article as :

Prof Manjunathraddi Bentur, Prof. Shashidhar P K, Deepa Chakalabbi, Prabhavati Hosalli, Shridhar Kumbar, Kavya Megalgeri, "EDGE Based Algorithm for Encryption and Decryption Text into Images", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6, Issue 3, pp.865-869, May-June-2020.
Journal URL : http://ijsrcseit.com/CSEIT2063202