International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 5, Issue 4, ISSN No. 2455-2143, Pages 533-538
Published Online August 2020 in IJEAST (http://www.ijeast.com)

ADAPTIVE STEGANOGRAPHY SCHEME USING LOSSLESS TECHNIQUE

Gaurav Gupta
SPPU Computer Engineering,
Dr. D. Y. Patil Institute of Engineering Management and Research, Akurdi, Pune, India.

Shruti Patil
SPPU Computer Engineering,
Dr. D. Y. Patil Institute of Engineering Management and Research, Akurdi, Pune, India.

Piyush Varma
SPPU Computer Engineering,
Dr. D. Y. Patil Institute of Engineering Management and Research, Akurdi, Pune, India.

Ankita Raikwade
SPPU Computer Engineering,
Dr. D. Y. Patil Institute of Engineering Management and Research, Akurdi, Pune, India.

Yogita Sawant Yogita Sawant
SPPU Computer Engineering,
Dr. D. Y. Patil Institute of Engineering Management and Research, Akurdi, Pune, India.

Abstract: Steganography is the art and study of composing covered up and private messages so that nobody separated from the sender and proposed beneficiary even acknowledges there are shrouded messages. There are frequently situations when it is absurd to expect to send messages transparently or in scrambled structure. Steganography is the propelled rendition of cryptography where cryptography gives protection, steganography is planned to give mystery information. So no one beside the authorized sender and collector are fixed on the presence of the key data. This paper expects to give an outline of the picture steganography and its uses for concealing the information. In this paper the steganography is actualized utilizing the information room stowing away and a reversible information room covering up in which the messages is put away in the particular portion of the picture. Because of the offer covering up the third individual won't be ready to see the current data.

Keywords - **Steganography, secrecy, Cryptography, privacy, room hiding, reversible room hiding.**

I. INTRODUCTION

Steganography is that the method of concealing mystery data during a direct in such a style, that the very presence of information is covered. It is the study of "imperceptible" correspondence and keeps an unintended beneficiary from suspecting that the information exists. Information stowing away in picture arrangements is performed for the most part in two different ways: bit stream-level and information level. In bit stream-level, the redundancies inside the current pressure measures are misused. Nonetheless, these techniques exceptionally accept the structure of the bit stream; thus, they're very delicate, inside the feeling that much of the time they can't endure any arrangement change or transcoding, even with no huge loss of perceptual quality. Therefore, this kind of information concealing technique is typically proposed for delicate applications, similar to confirmation. On the contrary hand, information level techniques are increasingly powerful to assault. Along these lines, they are reasonable for a more extensive scope of uses. In spite of their delicacy, the bit stream-based ways are as yet appealing for information concealing applications.

II. LITERATURE SURVEY

This is a progressively perplexing method of concealing data in an image. Different calculations and changes are utilized on the picture to cover data in it. Change space installing is frequently named as a site of implantation procedures that assortment of calculations are recommended [3].

The encoder adds a succession of changes to the duvet picture. Along these lines, data is portrayed as being put away by signal twisting [4].

Utilizing this framework, a stego object is made by applying an arrangement of alterations to the duvet picture. This arrangement of adjustments is used to coordinate the mystery message required to transmit [5].

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 5, Issue 4, ISSN No. 2455-2143, Pages 533-538
Published Online August 2020 in IJEAST (http://www.ijeast.com)

The message is encoded at pseudo-haphazardly picked pixels. In the event that the stego-picture is not quite the same as the duvet picture at the given message pixel, the message bit might be a "1." In any case, the message bit might be a "0." The encoder can alter the "1" esteem pixels in such a way that the measurable properties of the picture are not influenced. [6].

A ton of Research has been completed on Steganography: Rajkumar Yadav et al. [7] proposed a swap picture steganography procedure for installing messages into dark level Images.The picture is part into squares of equivalent sizes and subsequently the message is then embedded into the focal pixel of the square utilizing cyclic blend of sixth, seventh and eighth piece Dr. Ekta Walia et al. [8] gives examination of Least Significant Bit (LSB) based steganography and Discrete Cosine Transform (DCT) based steganography.

LSB based steganography insets the instant message in lsb of computerized information. Changing over an image from an arrangement like BMP or GIF which remakes the principal message precisely to a JPEG which doesn't then back could demolish the information covered up in the LSBs. DCT based steganography install the instant message in lsb bits of the discrete cosine (DC) coefficient of computerized picture..[9]

Rajkumar Yadav [10] proposed a swap technique for the chief LSB for concealing information in computerized pictures. Another strategy for concealing information in computerized pictures is GLM procedure [6]. Fundamental disadvantage of above strategies is that in the event that the interloper changes least huge piece (LSB) of all picture pixels at that point shrouded message can be destroyed their strategy expels the two downsides related with LSB and GLM method and give us better outcomes. [5].

M.Sivaram et al.[11] in their proposed framework they have chosen an irregular pixel during a spread picture and in that they took the last two bits for encoding the information . In this way, the information length of the key message are frequently broadened. In the proposed strategy they need implanted a character with the help of just 2 pixels as opposed to utilizing the three pixels. So we will embed more characters during a solitary picture by utilizing this framework .

Nitin Jain et al.[12] they need to indicate how the sides of the photos are frequently wont to conceal instant messages in steganography. It gives the profundity perspective on picture steganography and edge identification channel procedures. The strategy computes parallel estimation of each character of instant message at that point and attempts to search out dull spots of dim picture (dark) by changing over the main picture to double picture. At that point these pictures are changed over to RGB pictures in order to search out dull places. In thus each succession of dim shading transforms into RGB shading and dim degree of dim picture is found along these lines. At long last every 8 pixels of dull spots has been considered as a byte and paired estimation of each character has been placed in low smidgen of every byte that was made physically by dim spots pixels for expanding security of the most method of lsb bit steganography. Steganalysis then wants to assess the concealing procedure to ensure the data are frequently covered up in the most ideal manner. This methodology shrouds the content in chosen dull places yet the information isn't put straightforwardly in those pixels and put in low bits of each eight piece pixel.

Steganography can be utilized for computerized watermarking, web based business, and the vehicle of sensitive data [13]. Computerized watermarking includes installing shrouded pictures or records to bring up proprietorship. This is helpful for ensuring copyright of the proprietor. In current online business exchanges, most clients are secured by a username and secret key. In any case, there's no genuine strategy for checking that the client is the real card holder. Biometric finger impression checking which is joined with remarkable meeting IDs installed into the unique mark pictures by means of steganography, leave a truly secure decision to open web based business exchange confirmation.

III. IMPLEMENTATION

1) Generation of Encrypted Image:

First we scramble the first picture into the encoded picture to build the encoded picture, first the encoded picture can be separated into three stages: picture segment, and oneself installing followed by picture encryption. From the start, the first picture is separating into two sections A and B and this is finished by the picture segment. At that point, By utilizing the standard DATA HIDING calculation the LSB's of section An are reversibly inserted into the part B so that LSBs of section A can be utilized for possessing messages; and the last, scramble the modified picture to produce its last encoded picture.

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 5, Issue 4, ISSN No. 2455-2143, Pages 533-538
Published Online August 2020 in IJEAST (http://www.ijeast.com)

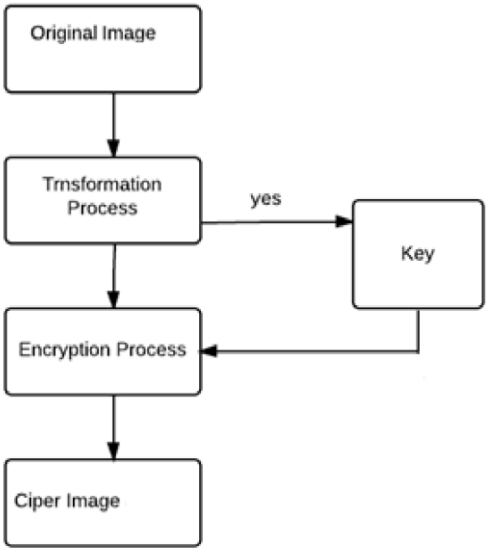


Figure 1: Architecture diagram of Encryption

2) Data hiding in Encrypted Image-

When the encoded picture will frame the information hider get that scrambled picture E, he can install some extra information into the encoded picture, in spite of the fact that information hider doesn't gain admittance to the unique picture. The information concealing procedure begins with finding the encoded variant of the section and that is meant by AE. At the highest point of scrambled picture E, AE has been reworked; it is easy for the information hider to peruse 10 bits information in LSBs of initial 10 encoded pixels. Subsequent to distinguishing what number of lines of pixel and bit-planes he can change, the information hider essentially embraces LSB substitution to put the accessible piece planes with extra information m . in the wake of inserting the extra information m into the encoded picture E by utilizing the information concealing key we get the stamped scrambled picture E'. any individual who needs to extricate the extra information m he/she doesn't remove that information without the information concealing key.

Data hiding algorithm (for image)(edited)

Input : Original image.

Output : Stego image.

Step 1 : Read the original (input) image.

Step 2 : Perform frame outline separation.

Step 3 : Apply Integer DCT on each of 8*8 block of the image.

Step 4 : Perform the Zigzag scanning on each of 8*8 block of the image.

Step 5 : Apply Huffman coding to compress the frame outliers.

Step 6 : Apply a mystery key to conceal the information.

Step 7 : Apply LSB algorithm to implant information.

Step 8 : Generate stego (output) image.

3) Data Extraction and Image Recovery-
Data extraction is a completely independent process from image decryption. So the order of implementing them are two different practical applications.

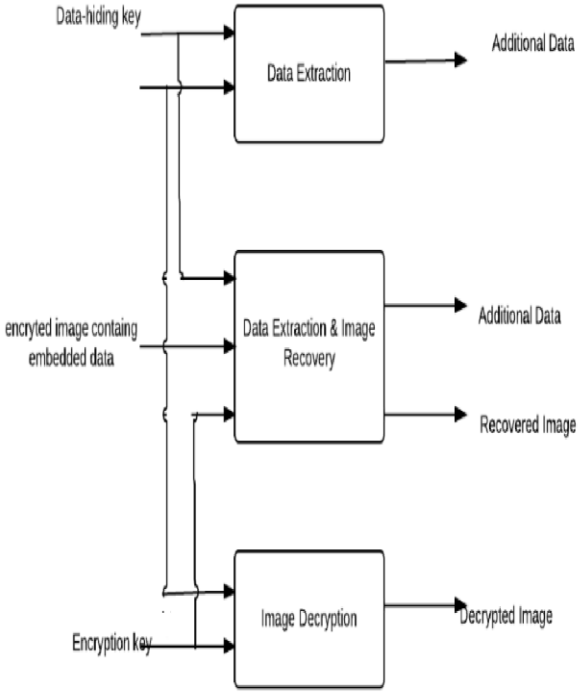


Figure 2: Architecture diagram of Decryption

Data Extraction algorithm (for image)

Input : Stego image.

Output : Secret (hidden) data.

Step 1 : Read the stego (input) image.

Step 2 : Perform decoding using IDCT and Inverse Huffman coding on the stego (input) image.

International Journal of Engineering Applied Sciences and Technology, 2020
Vol. 5, Issue 4, ISSN No. 2455-2143, Pages 533-538
Published Online August 2020 in IJEAST (http://www.ijeast.com)

Step 3 : Extract the hidden or secret data using ILSB and secret key.

Secret key generation algorithm-

Step 1 : Take a key which is the prime number.

Step 2 : Now generate two prime numbers p,q nearer to the given key.

Step 3 : Calculate n=p*q;

Step 4 : then calculate m=(p-1)(q-1).

Step 5 : Generate the e.

Now assume e=1 , x=1; while (mod(m,e)==0) e=e+1;

Step 6 : Generate e.

Take s=1+x*m.

While (mod(s,e)~=0)

x=x+1;

s=1+x*m;

d=s/e;

IV. ACCURACY OF THE SYSTEM

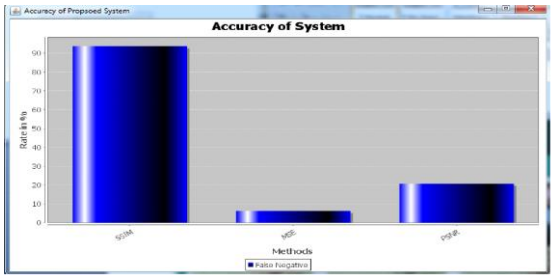


Figure 3: System performance with watermark image 512*512 image

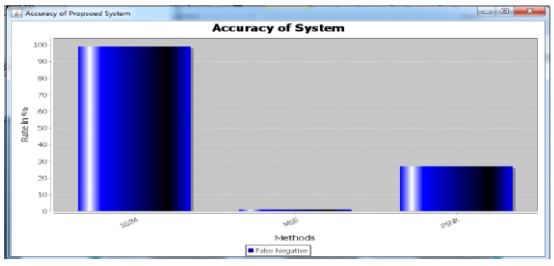


Figure 4: System performance with watermark image 1024*1024 image

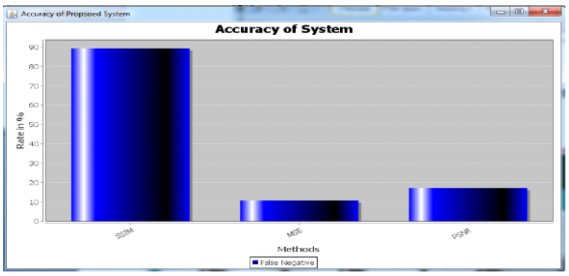
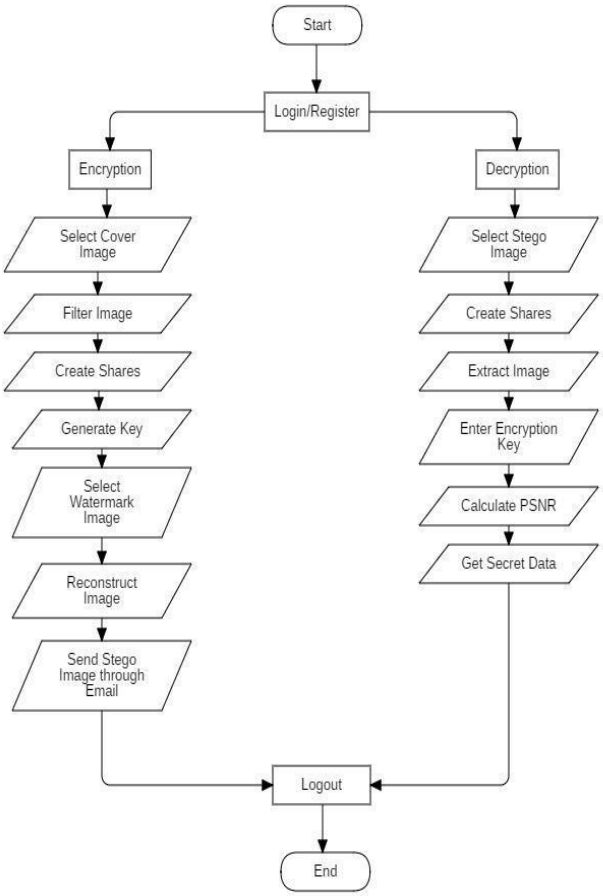


Figure 5: System performance with watermark image 2048*2048 image

V. FLOWCHART



VI. FUTURE WORK

We propose a novel strategy by holding room before encryption with a customary DATA HIDING calculation, and along these lines it is simple for the information hider to reversibly insert information in the scrambled picture. The proposed technique can accomplish genuine reversibility, that is, information extraction and picture recuperation are

liberated from any error. In this task we can conceal the information into the picture. What's more, by utilizing the encryption key and the information concealing key we can isolate out the picture and concentrate the messages.

VII. CONCLUSION

After finishing the proposed technique separate information extraction from picture unscrambling yet in addition accomplishes incredible execution in two distinct possibilities: Real reversibility is comprehended, that is, information extraction and picture recuperation are liberated from any mistake. For given installing rates, the PSNRs of decoded picture or picture containing the inserted information are significantly improved; and for the satisfactory PSNR, the scope of implanting rates is actually enlarged. Basically the information covering up in scrambled pictures is an inventive subject drawing consideration on account of the protection saving necessities from cloud information management. Going before techniques actualize DATA HIDING in scrambled pictures or pictures by clearing room behind encryption, as inverse to which we proposed by saving room past to encryption. In this manner the information hider can profit by the additional room discharged out in the past stage to make information concealing procedure easy.

VIII. ACKNOWLEDGMENTS

We are grateful to our Department of Computer Science for their support and also for providing us an opportunity to review and work on such an interesting topic in image processing. While reading and searching concerning this subject we tend to *learn concerning varied vital and interesting facts about it.*

IX. REFERENCES

[1]] Nagham Hamid, Abid Yahya, R. Badlishah Ahmad, Osamah M. Al-Qershi (2017). Image Steganography Techniques: An Overview.International Journal of Computer Science and Security (IJCSS), Volume (6) : Issue (3) : (2017,p168-187).

[2] Ritesh D. Yelane, Dr. Nitiket N. Mhala, Prof. B. J. Chilke (2018). Security Approach by Using Visual Cryptographic Technique. International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue (1, January 2018).

[3] Ms. Deepti Chaudhary, Mrs. Rashmi Welekar (2015). A Secure Authentication Using Visual Cryptography & Steganography. International Journal of Engineering Trends and Technology (IJETT) – Volume 21 (Number 6 – March 2015).

[4] J. Ida Christy and V. Seenivasagam (2018) . Feed forward network in color extended visual cryptography to generate meaningful shares. International Journal of Security and Its Applications Vol.9, No.1 (2018).

[5] Miss. Alfiya Saiyyad, Miss. Asma Khan, Prof. Madhuri Badole (2015). Secure authentication by image processing and visual cryptography for banking applications. International Journal of Advance Foundation and Research in Computer (IJAFRC) Volume 2, Special Issue(NCRIT 2015) ,ISSN 2348–4853 (January 2015).

[6] P.G. Haritha, Mrs. M. Mathina Kani (2017). A new visual cryptography technique for color images. International journal for trends in engineering & technology, volume 4 issue 2, (ISSN: 2349 – 9303) (April 2017).

[7] Shruti Sekra, Samta Balpande, Karishma Mulani (2017). Steganography using genetic encryption along with visual cryptography. SSRG International Journal of Computer Science and Engineering(SSRG-IJCSE) – volume 2 issue (1 January 2017).

[8] Prof. Sujit Ahirrao, Tusharkumar Sakariya, Abhijeet Bhokare, Rahul Thube (2015). Visual cryptography scheme for color image using K-N secret sharing algorithm. International Journal of Advanced Technology in Engineering and Science Volume No.03, Issue No. 02, (February 2015 ISSN (online): 2348 – 7550).

[9] Sankar Das, Sandipan Chowdhury, Dibya Chakraborty, Arijit Das, Asoke Nath(2016). Visual Cryptography using Three Independent Shares in Color Images. International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163 ,Issue 4, Volume 2 (April 2016).

[10] Fersna S, Athira V(2016). Progressive visual cryptography scheme without pixel expansion for color images. International Journal of Advanced Research in Computer and Communication Engineering, Vol. 4, Issue 6 (June 2016).

[11] M. Sivaram , B. Durga Devi J. Anne Steffi (2012). Steganography of two LSB bits. International Journal of Communications and Engineering Volume 01– No.1 (01 March2012, p82-87).

[12]Nitin Jain, Sachin Meshram, Shikha Dubey (2015). Image Steganography Using LSB and Edge – Detection Technique . International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-3 (July 2015 ,p217-222).

[13] Xuehu Yan , Shen Wang , Xiaomu Niu , Ching-Nung Yang (2015). Halftone visual cryptography with minimum

auxiliary black pixels and uniform image quality , Digital Signal Processing 38 (2015) 53–65.

[14] József LENTI (2017). Steganographic methods in periodica polytechnica ser. el. eng. vol. 44, no. 3– 4, PP. 249–258 (2017).