To Develop an Image Based Steganography Framework to Enhance Quality of Payload Object

Monika
(Pursuing M. Tech, CSE)

Er. Mohinder Singh
(Assistant Professor, CSE)

Maharishi Ved Vyas Engineering College,
Kurukshetra University, India

Abstract- **The rising possibilities of current communications need the special way of security especially on computer networks. The security is becoming more important as the number of data being exchanged on the Internet increases. Therefore data integrity, the confidentiality is needed to protect against unauthorized access. This has resulted in an explosive development of the field of data hiding. The focus of our research is to present a new stenographic technique for embedding messages in BMP image. The main objective of this method is to hide a text of a secret message in the pixels of the image in such a way that the human visual system is not able to differentiate between the original and the stego image. Calculate the peak-signal-to-noise ratio (PSNR) stego image and maintain the size of the stego image.**

I. INTRODUCTION

The essential progress took place in the subject of facts era has generate many problems related to data certainty. The software regions which circulate around information certainty are: confidentiality of commercial enterprise transactions, payments in private conversation and password protection. For comfy communications cryptography is important. By using scrambling the records encryption makes the conversation uncertain. other third party can view the two events communicating in non-public and can really make a few strategy to kind out the cipher[3]. The approach used to conserve the contents of a message constrained is referred to as steganography. To maintain the reality of a message secret's purpose steganography.

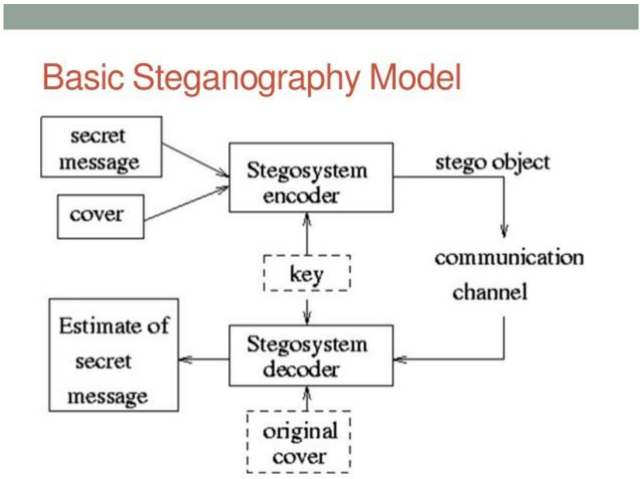


Figure 1: Steganography model

Different kinds of steganography:

Steganography may be widely categorized into four classes, and these are:

1) Text Steganography

2) Image Steganography

3) Audio Steganography

4) Video Steganography

(1) Text Steganography: A steganography method that makes use of text as the quilt media is known as a textual content steganography.

2) Audio Steganography: A steganography technique that uses audio as the quilt media is referred to as an audio steganography. it is the most tough project in steganography.

3) Video Steganography: A steganography approach that makes use of video as the duvet media is referred to as photo steganography.

4) Image Steganography: A steganography technique that makes use of photographs as the quilt media is called an picture steganography.

Algorithm

This set of rules is primarily based on wavelet remodel and bit aircraft complexity segmentation.

- **Wavelet transform:** The initiate strategy makes use of the wavelet remodel presentation of the quilt photo to conceal the secret message. In a four-band - dimensional wavelet remodel, the LL band consists of the low skip coefficients and Gowtham Dhanarasi et al. / global magazine of Engineering technological know-how and generation represents a smooth approximation to the photo. The HL, LH and HH bands constitute the vertical, horizontal, and diagonal features of the picture, respectively. Those three bands deliver the information of the image. we are able to do the identical decomposition at the LL quadrant up to log2 (min (peak, width))

- **Bit Plane Complexity Segmentation:** Typically, wavelet area permits for hiding data in areas that the HVS is less touchy. To try this, we adapt the amount of embedded statistics in each area of wavelet transform area with a degree of noisiness in that place. Here, we use the bit-aircraft complexity segmentation (BPCS) as the degree of noisiness. Every RGB component of a 24-bit bitmap photograph is an 8-bit price that modifications from zero to 255. In every color aircraft, the cost 0 represents the darkest shade of that color, in which the brightest shading corresponds to the 255 cost.

Image or Transform domain

A few steganographic algorithms can either be categorized as being in the image area or within the transform area depending on the execution.

- **Patchwork**

  Patchwork is a statistical technique that makes use of redundant sample encoding to embed a message in a photograph. The algorithm provides redundancy to the hidden statistics and then scatters it round the picture. And to select two sectors of the image (or patches) pseudorandom generator is used, patch A and patch B. All the pixels in patch A is lightened whilst the pixels in patch B is darkened. In different phrases the intensities of the pixels inside the one patch are elevated by means of a consistent price, whilst the pixels of the opposite patch are decreased with the identical regular price.
- **Spread Spectrum**

  In unfold spectrum techniques, hidden facts is unfold all through the cover image making it more difficult to detect. A gadget proposed via wonder et al. combines unfold spectrum communiqué, blunders manage coding and picture processing to hide facts in snap shots.

Some terminologies in Steganography:

- **Payload**: The records that's to be concealed.
- **Service report**: The media where payload must be hidden.
- **Stego-Medium**: it's miles the medium wherein the data is hidden
- **Redundant Bits**: Pieces of information interior a file which can be overwritten or altered without
- **Damaging the report Steganalysis**: The manner of detecting hidden information internal of a file.
- **Stego medium** = Payload file + service file.

The four basic techniques used for Steganography are:

- **LSB technique**: The LSB of service medium is directly inserted with the message bit. So LSB of the service medium carries the payload.
- **Injection:** Hiding statistics in sections of a document which are neglected with the aid of the processing software. Therefore keep away from enhancing the ones file bits which might be relevant to a quit perfectly usable.
- **Substitution:** Substitute of the least big bits of data that decide the meaningful content of the unique report with new data in a manner that causes the least amount of distortion.
- **Generation:** In contrast to injection and substitution, this does not require an current cowl document but generates a cowl record for the sole motive of hiding the message.

1.12 Challenges

The top provocations of steganography are:

1) Security of concealed communication: The concealed contents should be un-seeable both perceptually and statistically with a purpose to avoid the suspicions of eavesdroppers.
2) Area of Payload: Steganography calls for ample embedding ability. Necessity for higher payload and relaxed verbal exchange are often conflicting.

II. RELATED WORK

Gowtham Dhanarasi .et.al(2012) A block convolution research for regulate domain photo steganography is confirmed on this paper. The set of rules superior right here works at the wavelet transform coefficients which embedded the private information into the unique photograph. The approach carried out which are able to constructing a exclusive-embedded photograph this is alike from the original image to human eye. This will be attained with the aid of keeping integrity of the wavelet coefficients at high capability embedding. This refinement to potential-pleasant trading –off interrelation is tested in specified and experimentally illustrated inside the paper.

Inderjeet Kaur.et.al(2013) Personal communication and copyright defense are the two most important rely of modern-day conversation device. The studies achieved so far shows a version of techniques to speak confidentially. The approach executed in this paper is a merger of steganography and watermarking which produced copyright safety to the statistics being transmitted confidentiality. The proposed aptness is a rework domain primarily based device with the intervention of segmentation and watermarking (TDSSW). it is discovered that the superior technique comes up with top PSNR (height signal to Noise Ratio) and enhanced confidentiality.

Sneha Arora.et.al(2013) This paper superior a brand new method for photograph steganography that are using part detection for RGB photos. There are masses of algorithms to confidential information with exactness stage however they are additionally lowering the excellent of the picture. on this advanced examine, edges of an RGB image could be found by means of scanning approach which might be utilizing 3x3 window, and then textual content could be inserted in to the edges of the shade picture. Not only excessive placing quantity will be attained however additionally the quality of the stego image additionally magnifies from the HVS.

Rahna E.et.al(2013) Steganography is a system of dispatch dissemble transmission in such a technique that no one, aside from the sender and intentional recipient, thinks the existent of the message. There are triumphant many strategies for virtual picture steganography. But maximum of the existing techniques are based totally on lossy method and the essential provocation of steganography are certainty of hid transmission and in an image area of message can be embedded. So, this paper is intentional to increase an photograph steganography approach primarily based on contest between cover photo and personal records. This advanced technique retained the duvet photo as such and has endless extent of payload.

H.B.Kekre.et.al(2014) A number of strategies are manageable in literature to provide pledge to digital photographs, these ability provide their terminal to statistics beating, picture Scrambling and picture Encryption. In paper the writer have superior a hybrid method to confidential digital photos. The superior framework is a merger of information Hiding and photograph Encryption. In statistics beating there are 4 exceptional strategies of many LSB's algorithm are used and assessed. A number of parameters are also used to assess the superior framework. Experimental outcomes display a great performance.

Mamta Sharma.et.al(2010) Statistics compression is likewise known as as source coding. it is the procedure of encoding records the usage of fewer bits than an un-coded illustration is likewise creating a use of specific encoding schemes. Compression is a era for decreasing the amount of information used to symbolize any content material without excessively reducing the first-class of the photo. It also reduces the variety of bits required to keep and/or transmit virtual media. Compression is a technique that makes storing less difficult for huge amount of information. There are numerous strategies to be had for compression in my paper work, I've analyzed Huffman algorithm and evaluate it with other not unusual compression techniques like arithmetic, LZW and Run period Encoding.

Anushka Nagpal.et.al(2015) With the rise of net maximum of the conversation & facts sharing is accomplished over the net. The growing unauthorized get admission to of personal facts, facts security is most critical. Therefore a huge problem is to lessen the possibilities of statistics detection all through transmission. Steganography is a method that entails hiding message in an appropriate service as an instance an picture. The provider may be sent to receiver without anyone else understanding that it comprises a hidden message. The preliminary purpose of steganography is how it is carried out. The objective of this evaluation paper is to look at various steganography techniques for embedding the message and to talk secretly the use of open channel.

Tamanna Garg.et.al(2014) On this paper steganography and numerous steganographic strategies were included to fulfill the motive. The motive is to beautify the facts compression price the use of steganography. The paintings may be completed by way of introducing a brand new steganography method which will be used to cover big amount of textual content in pictures. The technique is based totally on the compression algorithm for you to enhance the compression rate. The compression algorithm to be used wills paintings in a number of 1 bit to eight bits per pixel ratio. With the aid of making use of this algorithm an application can be advanced which might enhance the garage ability of photo for the cause of hiding text.

Arun Sharma.et.al(2014) Steganography is a one of the technique for information hiding. With the help of steganography human beings can talk secretly. It entails speaking mystery information in the best multimedia service which include text, image, audio, and video files. the principle purpose of steganography is to make certain that the transmitted message is absolutely hidden within the cowl sign, and thereby making sure that the message is out there best through the supposed receiver and now not by way of any intruders or unauthorized parties. This evaluation paper discusses latest evaluate and analysis of the exclusive existing methods of steganography along with their strengths and weaknesses. This paper also affords a few common standards and suggestions drawn from the literature.

III. PROPOSED WORK.

Steganography is an excessive-stage type of encryption, and its use consequences in a mechanism to enforce two of the five key pillars of records security, specifically confidentiality and integrity. The confidentiality of the hidden message is included due to it being unrecognizable in its hidden and encrypted shape each within the vicinity of garage and throughout transmission. Any interceptor might not be privy to the secret message. Only legal humans might recognize of its lifestyles and could be capable of decrypt the name of the game message with the known password. The encrypting of the concealed message protects the integrity of the statistics. It has to be confused that the unique feature of steganography is largely to be attributed to the capacity for use in IT safety. no longer only is the name of the game message encrypted, but it is also hidden at the back of an photograph, textual content or tune record, making it invisible to normal interceptors. Increase the capability for the hidden statistics the use of the coloration transformation technique (RGB)

1. Convert the image into picture matrix.

2. Carry out the coloration transformation and convert the picture into RGB area

3 Read every pixel , Insert the records given by using the system:

Allow R represents the primary channel within the picture

R_1 (0), R2 (0), R3 (0) ………………………… R_n (0) be total first channels in all pixels

G_1(0),G_2(0),G3(0) …………………………G_n(0) be total Second channels in all pixels

B_1(0),B_2(0),B3(0) ………………………… B_n (0) be total third channels in all pixels

Let ch_1,ch_2,ch_3………………………………ch_m be total character that has to be inserted in the image.

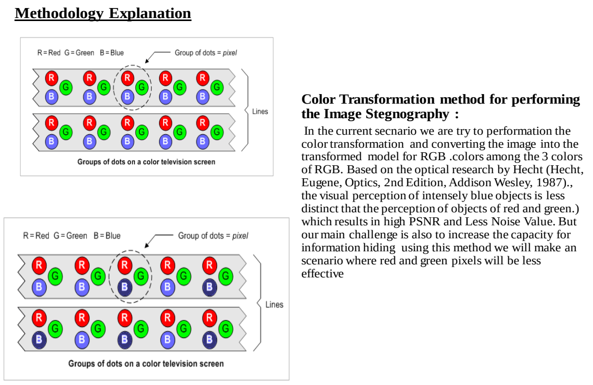
Therefore total character that has to be inserted is given by:-

Dividing Characters into three format

for blue Chi = Chi-16; and Bi= Chi;

for Red Ri | Chi

for Green Gi | Chi Where i = 0,1,2…….n (total character to be hidden)



Methodology Explanation

R = Red G = Green B = Blue
Group of dots = *pixel*
R
G
B
Lines
Groups of dots on a color television screen
R = Red G = Green B = Blue
Group of dots = *pixel*
R
G
B
Lines
Groups of dots on a color television screen

Color Transformation method for performing the Image Stegnography :

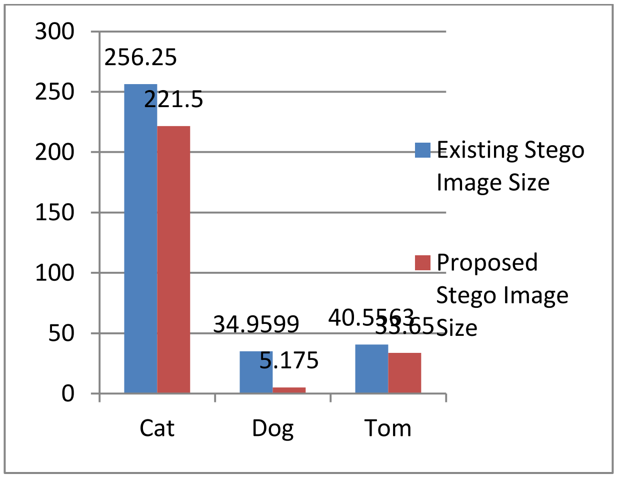
In the current secnario we are try to performation the color transformation and converting the image into the transformed model for RGB .colors among the 3 colors of RGB. Based on the optical research by Hecht (Hecht, Eugene, Optics, 2nd Edition, Addison Wesley, 1987)., the visual perception of intensely blue objects is less distinct that the perception of objects of red and green.) which results in high PSNR and Less Noise Value. But our main challenge is also to increase the capacity for information hiding using this method we will make an scenario where red and green pixels will be less effective

Figure 2: Pixels of an image

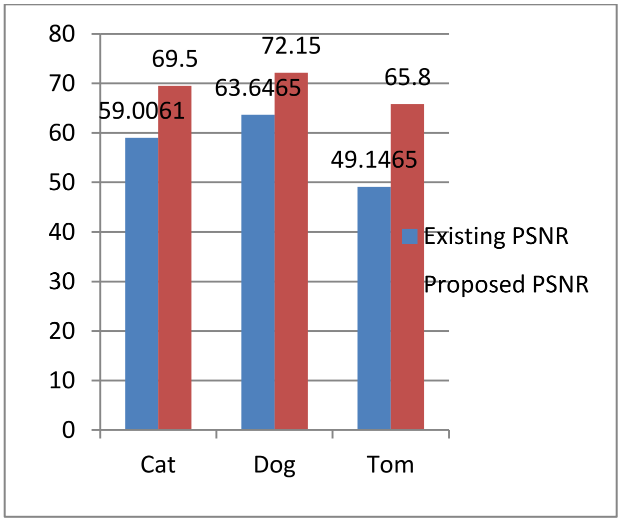
IV. SIMULATION RESULTS

Table: Results of image stenography

Name of Images	Size	Existing Stego-Image Size	Proposed Stego-Image Size	Existing PSNR	Proposed PSNR
Cat	221	256.25	221.50	59.0061	69.50
Dog	5.17	34.9599	5.175	63.6465	72.150
Tom	33.6	40.5563	33.65	49.1465	65.8



Graph1: Comparison of Existing Stego image size and Proposed Stego image size.



Graph2: Comparison of Existing PSNR and Proposed PSNR.

V. CONCLUSION AND FUTURE WORK

Steganography is widely used in computing there are certain issues that need to be resolved. There are many different techniques with their own merits and demerits. Color transformation technique not only maintains the same size of the image but also maintains the quality of the image. Proposed framework is based on steganography that uses Color transformation technique. Proposed approach gives satisfactory PSNR value to establish the robustness of the work. Existing technique can be pushed in video steganography this will be the future work for further research.

REFERENCES

[1] Ventriculograms H.B.Kekre, Tanuja Sarode and Pallavi Halarnkar "A Hybrid Approach for Information Hiding and

Encryption using Multiple LSB's Algorithms" International Journal of Application or Innovation in Engineering & Management (IJAIEM) Volume 3, Issue 6, June 2014 ISSN 2319 – 4847.

[2] Mridul Kumar Mathur, Seema Loonker, Dr. Dheeraj Saxena " LOSSLESS HUFFMAN CODING TECHNIQUE FOR IMAGE COMPRESSION AND RECONSTRUCTION USING BINARY TREES" IJCTA | JAN-FEB 2012 ISSN:2229-6093.

[3] Gowtham Dhanarasi,,Dr.A. Mallikarjuna Prasad "IMAGE STEGANOGRAPHY USING BLOCK COMPLEXITY ANALYSIS" International Journal of Engineering Science and Technology (IJEST).

[4] Inderjeet Kaur, Rohini Sharma, Deepak Sharma" TRANSFORM DOMAIN BASED STEGANOGRAPHY USING SEGMENTATION AND WATERMARKING" ISSN (Online) : 2229-6166 Volume 4 Issue 1 January 2013.

[5] Sneha Arora, Sanyam Anand" A New Approach for Image Steganography using Edge Detection Method" International Journal of Innovative Research in Computer and Communication Engineering Vol. 1, Issue 3, May 2013.

[6] Pallavi Hemant Dixit, Uttam L. Bombale "Arm Implementation of LSB Algorithm of Steganography" International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-3, February 2013.

[7] Rahna E. and V. K. Govindan" A Novel Technique for Secure, Lossless Steganography with Unlimited Payload" International Journal of Future Computer and Communication, Vol. 2, No. 6, December 2013.

[8] Saleh Saraireh "A SECURE DATA COMMUNICATION SYSTEM USING CRYPTOGRAPHY AND STEGANOGRAPHY" International Journal of Computer Networks & Communications (IJCNC) Vol.5, No.3, May 2013

[9] S.Shanmugasundaram " A Highly Secure Skin Tone Based Optimal ParityAssignment Steganographic Scheme Using DoubleDensity Discrete Wavelet Transform" International Journal of Scientific and Research Publications, Volume 4, Issue 3, March 2014 1 ISSN 2250-3153

[10] Mazhar Tayel, Hamed Shawky "A Proposed Assessment Metrics for Image Steganography" International Journal on Cryptography and Information Security (IJCIS), Vol. 4, No. 1, March 2014

[11] Inderjeet Kaur, Rohini Sharma and Deepak Sharma "TRANSFORM DOMAIN BASED STEGANOGRAPHY USING SEGMENTATION AND WATERMARKING" International Journal of Computing and Business Research (IJCBR) ISSN (Online) : 2229-6166 Volume 4 Issue 1 January 2013.

[12] Nan-I Wu and Min-Shiang Hwang "Data Hiding: Current Status and Key Issues" International Journal of Network Security, Vol.4, No.1, PP.1–9, Jan. 2007.