ISSN No: - 2456 – 2165

Digital Image Based Data Hiding By Using Steganography

Priyanka Gulab Gosavi
Information Technology, Siddhant College of Engineering Sudumbare,Pune,
priyankagosavi02@gmail.com

Rashmi Deshpande
Information Technology, Siddhant College of Engineering Sudumbare,Pune,
Rmn1780@gmail.com

Abstract—In this paper, a new facts of data hiding in images is proposed. The goal of steganography is to cover an statistics message inside a medium in such way that it is now not feasible even to take a look at that secrete message. It would not update cryptography however rather boosts the security using its obscurity alternatives. In the projected its obscurity capabilities. In the proposed algorithm we've used 2d order differential equation to hide the records which improve the security stage of hidden facts. In encryption, records is transformed in any such manner that it cannot be come across with the aid of hacker. But throughout encryption, message is modified so it grow to be distorted and intruder can also suspect about the presence of important statistics. For this pores and skin tone detection is executed using HSV (Hue, Saturation and Value) color space. Additionally mystery facts embedding is accomplished victimization frequency area approach – DWT (Discrete wavelet Transform), DWT outperforms than DCT (Discrete cosine Transform). Secret information is hidden in a single of the excessive frequency sub-band of DWT by tracing skin pixels therein sub-band. Totally one of a kind steps of statistics hiding are carried out by means of cropping a picture interactively. The output of our approach provides better effects due to the fact with the help of cropping an accelerated protection than hiding facts even as no longer cropping i.E. In complete photo, consequently cropped location works as a key at decryption thing. As a result with this object destined steganography we will be inclined to tune pores and skin tone gadgets in picture with the higher safety and high-quality PSNR (Peak-Signal-to-Noise Ratio).Modern steganography's aim is to live its extra presence undetectable.

Keywords: Steganography, Discrete Wavelet Transform, Data Hiding, Second Order Differential Equation .

I. INTRODUCTION

In these days's international use of laptop and internet and transfer of essential statistics through it growing day by using day. For the moving of such critical facts, protection of statistics is additionally essential. Many safety hassle can also arise during transmission of essential facts via internet any time, and they are turning into extra crucial than ever. The main trouble of exposure is that unwanted human beings can attack in to personal statistics effortlessly. It has been observed because beyond few years that hacker's attacks are growing rapidly. Which indicates that there's nevertheless a needs for higher data security. Steganography is one viable approach to hide our important statistics and to obtain better information safety by means of hiding information in to a media carrier to shape a media file. For example in steganography we will select an photograph file and embedded our mystery facts internal. It .After embedded our image is converted in to a secret photo referred to as stego photo. Steganography phrase comes from greek phrases, steganos and graptos because of this included and writing respectively. Steganography deals with safety of informa- tion.It is a different approach of facts hiding in a few medium (cover document), so that it doesn't suspected by the hackers. Here we explain approximately operating of steganography and the vital phrases used in steganography additionally we consciousness on some vital phrases which are usually used in steganography are.

- *File:* It is a medium in which cover our information. For hidden.It may be picture, audio file, textual content and video document. There are many kind of cover document as in step with requirement in our steganography technique. Different kind steganography method use exclusive type of cover documents.
- *Message:* The information or essential records to be hidden or extracted. Message is also some time says a mystery statistics. This mystery message or information is embedded with the bottom image.
- *Key:* A key with the aid of which encryption and decryption is executed. If the receiver does not realize approximately the decryption key he can't extract the hidden facts.

II. LITERATURE SURVEY

A. *"Image Steganography on Coloured Images Using Edge Based Data Hiding In DCT Domain"*

Author :: Sounak Lahiri, 1Malay Gangopadhyaya Year 2016

This paper show how the DTC (i.e Discrete cosine transform) is used for the Image compressions. In this method filters are

ISSN No: - 2456 – 2165

used to identify the image sharp edge in the is continuous location.. by using the filter on the image its helpful for a small array applied to each pixel and its neighbours within an image for find the edges. Edge-Detection using Filters Here the Laplacian, Sobel, Prewitt can be used to detect edges in an image. here used the 2 processed to data security like Encoding process for the data encryption and decoding process for the data Decryption to the Authorise users. The hiding of information in colour images is of much importance as it can be effective in providing large capacity for embedding data.

B. Data Hiding Using EDGE Based Steganography

Data can be of any of the format like Audio,Video ,Text and Images.So there are the multiplay ways for the detecting the eadge of the eact type of data format for each method which aregiven in this paper.here the Least Significant Bit embedding (LSB) method is used for the finding the LSB of the images In a gray scale image each pixel is represented in 8 bits. The last bit in a pixel is called as Least Significant bit as its value will affect the pixel value only by "1". So, this property is used to hide the data in the image. Here we have considered last two bits as LSB bits as they will affect the pixel value only by "3". This helps in storing extra data.

III. REALAED WORK

A. Image Steganography

Image steganography is a department of steganography in which there are many one of a kind carrier record codecs can be used in steganography however virtual pictures are maximum popular. In nowadays time because of their frequency on internet. For hiding mystery information in snap shots there are big range of strategies .Two fundamental techniques of image steganography are: Spatial domain photo steganography and remodel domain image steganography. Most popular approach of spatial domain photo steganography is least considerable bit (LSB) insertion method. In LSB technique data are hidden in least good sized bit .The right maximum bit is referred to as the LSB because converting it has the least impact on the price of the variety. There are three basic parameters for the evolution of various steganography techniques. .

B. Discrete Wavelet Transform Technique

It is a system of hiding facts in photograph steganography for authentication which is use to verify the integrity of the secret message from the stego photograph. In this method the name of the game information is first transform from spatial domain to discrete wallet rework, then the coefficient of DWT are permuted with the verification code and then embedded in unique domain of cover picture.

IV. PROPOSED METHODOLOGY

The proposed set of rules is made up of 4 crucial sections which are File, encryption, channel (medium) and receiver give up.

In transmitter stop the content material proprietor first pick the image in which information has to be hidden this step is called image selection, then discover the location of the image (skin masks photo) this step is acknowledged as area identification.

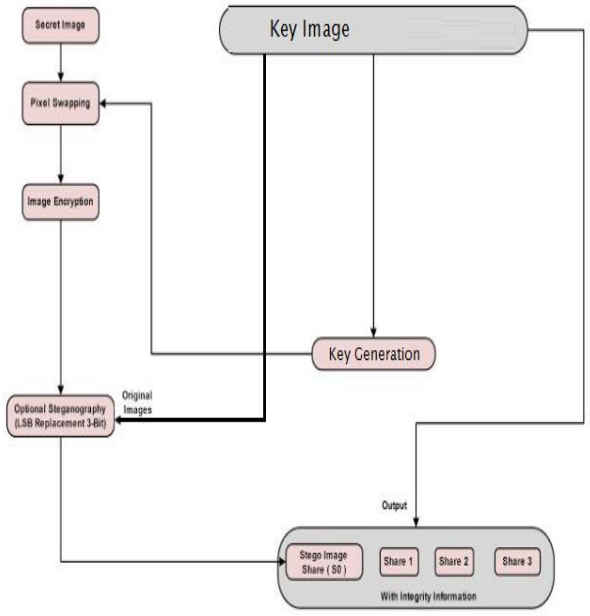
Then select the part of the skin wherein the data needs to be embedded this step is called selection of element or cropping of picture. Then set the contrast of the photograph through histogram change.

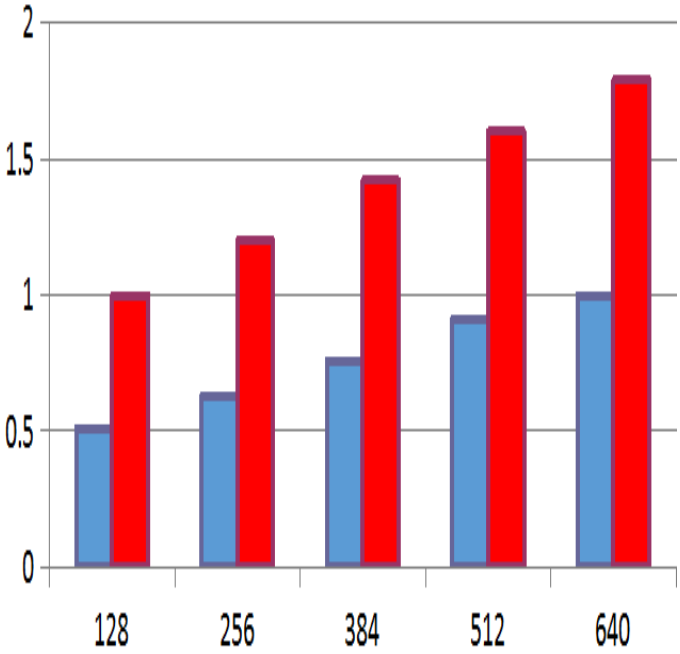
After this the photograph is encrypted using an encryption key to supply an encrypted photo. Then, the information hider assemble the image the usage to create a space to deal with the additional statistics. Then statistics is hided through DWT.

After hiding the statistics, now we get the secret photograph which appearance like the original image with mystery data. This photo is known as stego photo. Now we ship this stego photo to the receiver trough a channel or medium this is the most critical component of our set of rules because at the transmitter and receiver give up the user has manage of all of the information including photo, mystery statistics or mystery key.

But as soon as the picture has transmitted to the receiver consumer does now not have any manage on it. Most of the error and distortion in addition to hacking may additionally arise in our image while it travelled via the channel that's a radio channel. For the safety of our records from the hackers here we are the usage of a 2d order mathematical differential equation. On the receiver facet the consumer first get the stego picture, it is a cowl record that contains message bits (records which has to be sent) interior it. This document is communicated over the channel between sender and receiver. Then we pick the area wherein our facts is hidden this step is recognized as hidden area choice, then we rework or construct the image, After this we extract our information thru a secret key and view the output that's equal as our mystery information.

ISSN No: - 2456 – 2165





.

V. EXPECTED RESULT

Differentiate output results of enc-dec (Base 64, Hexadecimal) results are given in Fig. for Exisiting and Proposed System, Fig. shows the results at base 64 encoding while It gives the results of hexadecimal base encoding. We can notice that there is significant difference at both system. The same method is applied for encryption with multiple sample; we can recognize that the two bars given in image.

Data In KB	Time Complexity For Decrypt [Proposed System] In Second	Time Complexity For Decrypt [Exisitng System] In Second
128	0.51	1
256	0.63	1.2
384	0.76	1.42
512	0.91	1.6
640	1	1.79

VI. ACKNOWLEDGMENT

With immense pleasure, we are publishing this paper as a part of the curriculum of M.E. Computer Engineering. It gives us proud privilege to complete this paper work under the valuable guidance of Principal for providing all facilities and help for smooth progress of paper work. We would also like to thank all the Staff Members of Computer Engineering Department, Management, friends and family members, Who have directly or indirectly guided and helped us for the preparation of this paper and gives us an unending support right from the stage the idea was conceived.

REFERENCES

[1]. DeepikaBansal, Rita Chhikara, “An Improved DCT based Steganography Technique”, International Journal of Computer Applications (0975 – 8887) Volume 102– No.14, September 2014.

[2]. Syed Ali Khayam, 2003, “The Discrete Cosine Transform (DCT):Theory and Application” , ECE 802 – 602: Information Theory and Coding, Michigan State University.

[3]. DmitrijCsetverikov, “Basic Algorithms for Digital Image J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.Analysis: a course” , E¨otv¨osLor´and University Budapest.

[4]. ElifAybar, “Sobel Edge Detection Method ForMatlab”, Anadolu University, Porsuk Vocational School, Eskişehir.

[5]. SOBEL, I.,” An Isotropic 3×3 Gradient Operator, Machine Vision for Three – Dimensional Scenes”, Freeman, H., Academic Pres, NY, 376-379 , 1990.

[6]. SOBEL, I., “Camera Models and Perception, Ph.D. thesis” ,Stanford University, Stanford, CA, 1970.

[7]. B. Lipkin and A. Rosenfeld, Ed.. PREWITT, J., “Object Enhancemet And Extraction, Picture Processing and Psychopictorics” ,NY, Academic Pres,1970.

[8]. J. K. Mandal and Debashis Das,” Colour Image Steganography Based on Pixel Value Differencing in Spatial Domain”, International Journal of Information Sciences and Techniques (IJIST) Vol.2, No.4, July 2012.

[9]. Hemalatha S, U Dinesh Acharya, Renuka A, Priya R. Kamath, “ASecure Color Image Steganography In Transform Domain” (IJCIS)