Survey of different Steganography Techniques used in Digital Image Processing

Asutosh Tiwari , Prof. Y.S. Thakur

Department of Electronics and Communication Engineering, Ujjain Engineering College Ujjain

Abstract Typically, the data embedding is executed in communication corresponding to image, text, voice or multimedia content for copyright and also in military communication for validation and many new various purposes. latest image steganography, the secret hidden communication is obtained over embedding a message into a cover image which is used because the medium to embed messages toward the image and generate a stego image that is a most occasioned image that is carrying a secret invisible message. Within paper we have got analysed various steganography techniques and now have covered steganography overviews as well as its major types.

Keywords: Steganography , Data hiding , cover image.

I. INTRODUCTION

These days the communication systems happen to be turned into digital ones up to transmit data onto the networks. the advancement of networking as well as digital communication has presented grievous threats to reliable data transmission. The information security is crucial to various purposes, such as intimate data transfer, access control system for digital content distribution, secret data storing as well as protection of data alteration, along with media database systems. the information security is assessed toward information hiding and cryptography . the information hiding could be considered simultaneously of the most significant algorithms. it contains two fundamental techniques: steganography as well as watermarking techniques. The steganography technique is a approach the secret data communication, whereas the watermarking is used for the copyright protection for againes the electronic products. The main goal containing steganography commited to send data secretly through hiding the existence of a well known data onto another media. the content passed down as far as hide the data is known as cover objects, while the cover together with the hidden data is known as stego-object. cryptography is the learn about containing algorithms of sending messages in encrypted form (not understood) so that the most effective the authorized recipients take care of decrypt messages as well as read it. cryptography system is classified toward symmetric-key system and asymmetric-key system. symmetric-key system uses a special key that both the sender as well as the receiver has had, and asymmetric-key system uses two different keys(a public-key and a private-key), where the public key is known to everyone the term steganography refers that one may the art of hidden communications, encoding/embedding hidden information in cover media in such a way that it is a demanding task for any unauthorized individual to see thatthere is object hidden in the cover media. The output is an image called stego- image which is similar to the cover media . this stego image is then sent to the receiver where the receiver retrieves the hidden mesage through using the desteganography. a stego-key is used for embedding/encoding process as far as restrict decoding or extraction of the embedded data in cover media. the modern era steganography can also be implemented computationally, where multimedia files are used as cover media. an excellent steganographic mehods has three features, excellent hiding capacity, fine imperceptibility and the last is robustness.

II. SYSTEM MODEL

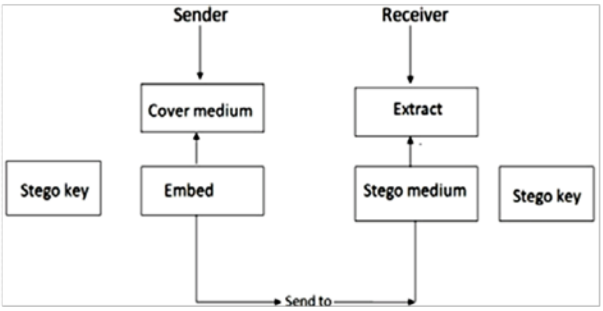

Fig Block diagram of Steganography.

III. LITERATURE SURVEY

Eshazly emad[1] this paper proposes a reliable steganography algorithm that hides a bitstream of the secret text toward the least significant bits (lsbs) from the approximation coefficients from the integer wavelet transform (iwt) containing grayscale images along with each one component of color images in order to establish stego-images. the embedding and extracting phases from the recommended steganography algorithms are performed using powerful matlab software. invisibility, payload capacity, and security in terms containing peak signal to noise ratio (psnr) and robustness are powerful key challenges to steganography. the analytical distortion between powerful cover images and the stego-images is restrained by using the mean square error (mse) and the psnr, whereas the degree consisting of closeness between them is appraised using the normalised cross correlation (ncc). the experimental results exhibit that, the proposed algorithms manage hide the secret text having a huge payload capacity with a high-level consisting of security and a higher invisibility. furthermore, the suggested technique is computationally efficient and better results for both psnr and ncc are executed compared with the previous algorithms.

Shiv prasad and arun Kumar pal [2] this paper presents a steganographic scheme according to the rgb colour cover image. the secret message bits are embedded into each colour pixel continuously by the pixel-value differencing (pvd) approach. pvd typically works on pair consecutive non-overlapping contents; consequently, the straightforward conventional pvd approach is not relevant up to embed the secret message bits within a colour pixel, therefore a colour pixel consists of three colour components, i.e. red, green and blue. hence, in the suggested strategy, at the start the three colour components are expressed toward two overlapping blocks like powerful combination containing red and green colour contents, while yet another one is the combination containing green and blue colour contents, respectively. thereafter, the pvd technique is employed toward each block individually to embed the, secret data. the two overlapping blocks are readjusted to attain powerful modified three colour contents. the suggestion of overlapping blocks has improved powerful embedding capacity of the cover image. powerful proposal has been tested toward a set consisting of colour images and satisfying results happen to be achieved in terms of embedding capacity and upholding powerful acceptable visual quality consisting of powerful stego-image."

Muhammad Arsal Usman [3] this paper proposes a improved image steganography approach in the interest of securing medical data. Swapped huffman tree coding is recognizable employ lossless compression along with manifold encryption up to powerful payload earlier than embedding toward the cover image. furthermore, most effective edge regions consisting of powerful cover image are used to embed the secret data whichever offers sharp imperceptibility. the results exhibit that one spectacular suggested method ensures confidentiality and secrecy of patient information whereas asserting imperceptibility.

jaspal kaur saini [4] this paper presents spectacular hybrid approach in the direction of image security that combines both encryption and steganography. first the image is encrypted using proposed new edition of aes algorithm, which is then hided directed toward cover image performing the steganography concept. experimental results and analysis is shown. that hybrid approach provides outstanding security toward attacks.

Rupali Bharadwaj [5] this paper is to provide two levels of security through a two step process, instead of hidden spectacular message bits directly in cover image, they are unarranged in a random order generated along 2D Arnold cat map after which encrypted message is hidden to conclude a cover image performing basic lsb approach. MSE(mean square error) and PSNR(peak signal to noise ratio) are two common quality measurements in order to measure the difference between the cover-image and the stego image. results showed that the recommended approach gives better impact than ordinary lsb with higher psnr and lower mseswarnjeet kaur [6] in the suggested method, a hybrid approach containing data hiding is used, in whichever a hybrid method containing data hiding performing optimal pixel adjustment process (opap) and identical matching has been used. further, to make the algorithm further undetectable data is split into segments along with image toward blocks and a data segment is embedded toward an image block where it effects the least image quality. the experimental results disclose that the quality containing stego image performing the suggested algorithm has been advanced over actual conventional methods of data hiding. in place of the verification of the results, peak signal-tonoise (psnr) and mean square error (mse) are calculated. The psnr quality for spectacular suggested method yields almost containing 14 db improvement.

marwa m. Imam [7] in this paper, a new image steganography approach based on spatial domain is suggested. according to the suggested approach, spectacular secret message is embedded randomly in the pixel location of the cover image using pseudo random number generator (prng) of every pixel value of spectacular cover image in place of embedding sequentially in the pixels of spectacular cover image. this randomization is anticipated to increase the security of the system. the suggested approach works with two layers (blue and green), as (2-1-2) layer, and the byte of the message can be embedded in three pixels only in this form (3- 2-3). from the experimental results, it has found that the proposed approach achieves a very sharp maximum hiding capacity (mhc), and better visual quality since indicated respectively peak signal-to- noise ratio (psnr)

prof dipto right , dubey swat [8] this paper includes 2lsb parity check and bit plane complexity segmentation (bpcs) steganography techniques to hide data within an image files which can be simple as well as very effective

R.S. Gutte, Y.D Chincholkar.[9] here, we proposed text steganography method together with cryptography in place of secret communication. it uses a straightforward method of steganography that is the data covering at lsb positions. we compared the data hiding at one lsb as well as two lsb positions and rated the performance parameters like standard deviation, mse and entropy and so on. the hiding of data at lsb positions is not fixed accordingly it is a well approach. the data is encrypted using extended square substitution algorithm. it covers all the alphabets, unique characters and mathematical symbols like µ, ß, þ, ø. Each pixel of the image is regarded as a byte. the encrypted text is embedded at lsb positions of each pixel and the carrier image after embedding the data is known as stego image. the stego image is transmitted and the secret data is successfully extracted at the receiver. the matlab outmoded used for implementation.

ritesh upadhyay Prof. y.s. thkur[10] this paper presents a comparison between unoptimized and optimized video steganography. in today's world containing internet communication, video is regarded as to be an effective as well as important tool for communication. Video steganography is a technique of hiding secret information in the video frames or the audio beats of the given cover video so that the existence of the secret information is concealed. The un-optimized base technique used during this paper for video steganography can be a 3-3-2 lsb based technique. the unoptimized video frames were after which optimized using modified genetic algorithm and that generated an optimum imperceptibility of invisible data. peak signal to noise ratio (psnr), mean square error (mse) and image fidelity (if) are the important mathematical measures for reviewing several steganographic technique. in this paper, we have compared all these three parameters for both un-optimized and optimized video steganography. experiential outcome exhibit a considerable improvement in these parameters for the optimized video steganographic technique.

IV. COMPARISION OF DIFFERENT METHOD

1- IWT-Least significant bit – In this method reliable steganography algorithm that hides a bitstream of the secret text toward the least significant bits (lsbs) from the approximation coefficients from the integer wavelet transform (iwt) containing grayscale images along with each one component ofcolor images in order to establish stego-images.The advantage of this method is high payload capacity and security.and limitation is less PNSR as compare to another method.

2- Block Based Pixel Value Differenciating – In this method the secret message bits are embedded into each colour pixel continuously by the pixel- value differencing (pvd) approach.The advantage of this method is easy to implement of RGB image and the limitation is PSNR ang capacity is less.

3- Swapped Huffman Coding with Edge Detection and LSB – In this method is improved image steganography approach in the interest of securing medical data. The advantage of this method capacity of the secreat is depend of the edge pixel and the limitation is Quality of inperceptibility of the hidden data is moderste.

4- MAES and LSB – In this method spectacular hybrid approach in the direction of image security that combines both encryption and steganography. The advantage of this method is better PSNR, greater security against attack and the limitation is low capacity.

5- 2D Arnald and LSB – In this method two levels of security through a two step process, instead of hidden spectacular message bits directly in cover image. The advantage of this method is high visual quality and high PSNR and the limitation is the generation of key is difficult.

6- Optimal Pixel Adjustment Process and LSB – In this method hybrid approach containing data hiding is used, in whichever a hybrid method containing data hiding performing optimal pixel adjustment process (opap). The advantage of this method is high PSNR and more efficient and the limitation is less secure.

7- Pseudo Random Number Generator – In this method spectacular secret message is embedded randomly in the pixel location of the cover image using pseudo random number generator (prng) of every pixel value of spectacular cover image. The advantage of this mehod is high PSNR and the limitation is not used for audio and vedio.

V. PSNR ANALYSIS

MSE (Mean Square Error) and PSNR (Peak Signal to Noise Ratio) are two common quality measurements to measure the difference between the cover-image and the stego-image. MSE is the averaged pixel-by-pixel squared difference between the cover-image and the stego image. Mathematically, MSE is expressed as:

$$MSE = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \left[C(i,j) - S(i,j)\right]^2$$

Where, M and N are the rows and columns of the cover image respectively, and C(i, j) and S(i, j) means the pixel value at position (i, j) in the coverimage and the corresponding stego-image, respectively.

The PSNR is expressed in dB's and can be calculated using MSE as

$$PSNR = 10 \times \log\left(\frac{P^2}{MSE}\right)$$

Where p is the peak signal value of cover image

$$P = \max\left(C(i,j), S(i,j)\right)$$

VI. CONCLUSION

it is also well defined as the learn about containing secret invisible communication that generally deals together with the alternative ways of concealing the presence of the communicated message. this paper gives an overview containing various steganography techniques. its dominant types as well as classification of steganography that has been suggested in the literature during the last several years.

REFERENCES

[1] E. Emad, A. Safey, A. Refaat, Z. Osama, E. Sayed and E. Mohamed, "A secure image steganography algorithm based on least significant bit and integer wavelet transform," in Journal of Systems Engineering and Electronics, vol. 29, no. 3, pp. 639-649, June 2018.

[2] Shiv Prasad and arun kumar pal “A rgb colour image steganography scheame using overlapping block based pixel value differencing” RSOS nov 18.

[3] Mohammad Arslan usman “using iamge steganography for providing enhanced medical data security” IEEE 2018.

[4] Jaspal K. Saini Harsh K. verma “A hybrid approach for image security by combining encryption and steganography” IEEE 2013.

[5] Rupali Bharadwaj , Divya Khanna “Enhanced the security of image steganography through image encryption” IEEE 2015.

[6] Swarnjeet Kuar, Navdeep Goel “Segmentation and block based image steganography using optical pixel adjustment process and identical approach” IEEE Dec. 2015.

[7] Marwa M. Emam “Improved image steganography method based on LSB technique with random pixel selection” IJACSA Vol. 7 No. 3 2016.

[8] L. jani Anbarasi, S. Kanna “ Secure secret color image sharing with steganography” IEEE 2012.

[9] Rosziati Ibrahim, Teoh Suk Kuan “PRIS: Iamge processing tool for dealing with criminal cases using steganography technique” IEEE 2011.

[10] Omend Khalind “Single mismatch 2LSB embedding method of steganography”

[11] Prof Dipti Dighe “Teganography using @LSB parity check and BPCS techniques”.

[12] R.S. Gutte comparison of steganography at one LSB and 2LSB position.

[13] Ritesh upadhyay Acomperison study of un optimize and optimize vedio steaganography.