A New Data Hiding Approach in Images for Secret Data Communication with Steganography

Irfan Khan
Student, M.Tech
Technocrats Institution of Technology, Bhopal

Sudesh Gupta
Associate Professor, HOD
Technocrats Institution of Technology Science, Bhopal

Shivendra Singh
Associate Professor, HOD
Technocrats Institution of Technology, Bhopal

ABSTRACT
In this paper, a new secret data hiding and communication is proposed for natural images.in this proposed methodology. The aim of steganography is to hide an information message within harmless cover medium in such way that it's not possible even to observe that secrete message. It doesn't replace cryptography however rather boosts the security using its obscurity options. In the projected its obscurity features. In the proposed algorithm we have used second order differential equation to hide the data which improve the security level of hidden data. In encryption, information is transformed in such a way that it cannot be detect by hacker. But during encryption, message is changed so it become distorted and intruder may suspect about the presence of important information. For this skin tone detection is performed using HSV (Hue, Saturation and Value) color space. Additionally secret data embedding is performed victimization frequency domain approach – DWT (Discrete wavelet Transform), DWT outperforms than DCT (Discrete cosine Transform). Secret information is hidden in one of the high frequency sub-band of DWT by tracing skin pixels therein sub-band. Totally different steps of data hiding are applied by cropping a picture interactively. The output of our technique provides higher results because with the assistance of cropping an increased security than hiding data while not cropping i.e. in whole image, thus cropped region works as a key at decryption aspect. thus with this object destined steganography we have a tendency to track skin tone objects in image with the higher security and satisfactory PSNR (Peak-Signal-to-Noise Ratio).Modern steganography's goal is to stay its more presence undetectable.

Keywords
Steganography, DWT, Data Hiding. RGB, Second order differential equation

1. INTRODUCTION
In today's world use of computer and internet and transfer of important information through it increasing day by day. For the transferring of such important information, security of information is also necessary. Many security problem may occur during transmission of important information through internet any time, and they are becoming more critical than ever. The main problem of publicity is that unwanted people can attack in to personal data easily. It has been noticed since past few years that hacker's attacks are growing commonly. Which shows that there is still a demands for better and secure communication. Steganography is one possible technique to hide our important information and to achieve better data protection by hiding information in to a media carrier to form a media file. For example in steganography we can choose an image file and embedded our secret data inside. It .after embedded our image is converted in to a secret image called stego image. Steganography word comes from two greek words, steganos and graptos which means covered and writing respectively. Steganography deals with security of informa-tion.it is a distinctive technique of data hiding in some medium (cover file), so that it doesn't suspected by the hackers. Here we explain about working of steganography and the important terms used in steganography also we focus on some important terms which are generally used in steganography are:

1.1 Cover file
It is a medium in which hide our information. For hidden.it may be image, audio file, text and video file. There are many type of cover file as per requirement in our steganography technique. Different type steganography technique use different type of cover files.

1.2 Stego-file
It is a cover file that contains message bits (information which has to be sent) inside it. This file is communicated over the channel between sender and receiver.

1.3 Message
The data or important information to be hidden or extracted. Message is also some time says a secret data. This secret message or data is embedded with the base image.

1.4 Key
It is a secret number or value by which encryption and decryption is done. If the receiver does not know about the decryption key he cannot extract the hidden information.

2. STEGANOGRAPHY
2.1 Text Based Steganography
In text-based steganography, the message to be sent is embedded in a text file. a text steganography can used html documents as the cover medium to hide secret messages. The main disadvantage of text base steganography is that reformatting of the text destroys the embedded content so this technique is not robust.

2.2 Audio Steganography
It is the technique of hiding of secret information by concealing it into another medium such as audio file. The various audio steganographic methods are: LSB coding, parity coding, phase coding, spread spectrum, echo hiding etc.

2.3 Video Steganography
In this technique we can hide any kind of file or information into a digital video format. Video is a combination of pictures which is used as a carrier for hidden information to video steganography additional information is recognizable by human eyes because the change of pixel color is negligible.

Video steganography uses H.264, mp4, mpeg, AVI or other video format.

3. LITRATURE REVIEW

Image steganography is a branch of steganography in which there are many different carrier file formats can be used in steganography but digital images are most popular. In today's time because of their frequency on internet. For hiding secret information in images there are large number of techniques .two basic techniques of image steganography are: Spatial domain image steganography and transform domain image steganography. Most popular technique of spatial domain image steganography is least significant bit (LSB) insertion method.in LSB technique information are hidden in least significant bit .the right most bit is called the LSB because changing it has the least effect on the value of the number. There are three basic parameters for the evolution of different steganography techniques.

3.1 Spatial Domain Image Steganography

There are many versions of spatial steganography. The technique behind the all is, direct change some bits in the pixel values into hidden data. Least significant bit steganography is the most popular and simpler approach that hides a secret message in the LSB of pixel value without introducing many perceptible distortions. Changing on the value of the LSB are unpredictable to human eyes. There are many approaches of data hiding which use LSB technique. Broadly classification of spatial domain image steganography techniques shown below:

3.1.1 LSB Technique

It is the most popular and simpler technique which a secret message in to LSB of pixel value.in order to hide data inside an image different images i.e. cover file can be used there is no restriction on type of data to be hidden, it may be image file, text file etc. The main disadvantage of LSB technique is that it has less robustness, the hidden data can be lost with image manipulation.

3.1.2 Pixel value differencing (PVD)

In this technique the size of hidden data bits can be estimated by the difference between two consecutive pixels in cover image. This technique provides better imperceptibility by calculating the difference of two consecutive pixels.

3.1.3 Random pixel embedding (RPE)

It is an image steganography technique based on LSB calculation and selection of random pixel of required image are in this technique password is added with LSB of pixels which improve security.it generates the random number and select the area in image where the secret data has to be hidden.

3.1.4 Edge based data embedding (EBE)

In this approach data is hidden in the region like edges.it is a novel technique of hiding data in the edges of the image by extending the LSB embedding. The edge based steganography is to embedded secret data in the position of edge pixels which meets the requirement both perception and robustness.

3.1.5 Mapping pixel to hidden data technique

It is an image steganographic technique of mapping pixels to alphabetic letters.it maps 32 letters (26 for English alphabetic and other for special character) with the pixel value.

3.1.6 Texture based technique

In this approach the texture is divided in to two groups, simple texture area complex texture area. Simple texture area is used to hide the 3-3-2 LSB (3 bits for red, 3 bits for green and 2 bits for blue channel), and in the complex texture area 4 LSB embedding technique is apply for information hiding.

3.2 Transform Domain Techniques

This is a more complex steganographic approach of hiding data in image. Transform domain can be termed as a domain of embedding techniques for which we can use number of algorithms.in this technique the secret message is embedded in the transform domain of the cover. Embedding data in frequency domain is much stronger than in time domain. Most of the steganographic system today operating with the transform domain. This technique have more robustness than spatial domain technique.it hide information in areas of the image which are less exposed to compression, cropping and image processing. The transform domain technique can be broadly classified as:

3.2.1 Discrete Fourier transform technique

This technique works in the frequency domain. The frequency domain is the domain where the analog pictures of continuous signal resides.in this technique we change an N point input signal in to two port output signals. The input signal contains the N/2-1, the signal being decomposed while the two output signals contain the amplitude of the component sine and cosine waves.

3.2.2 Discrete Cosine transform technique

In DCT based data hiding technique we hide the color information in a compress gray scale-level. it follows the color quantization. The main purpose of this technique is to give free access to grey-level image to everyone but restricted access of same color images to those who have its key.

3.2.3 Discrete Wavelet transform technique

it is a process of hiding information in image steganography for authentication which is use to verify the integrity of the secret message from the stego image.in this technique the secret information is first transform from spatial domain to discrete wallet transform, then the coefficient of DWT are permuted with the verification code and then embedded in special domain of cover image.

4. PROPOSED METHOD

The proposed algorithm is made up of three important sections which are transmitter end, channel (medium) and receiver end. In transmitter end the content owner first select the image in which data has to be hidden this step is called image selection, then identify the area of the image (skin mask image) this step is known as area identification. Then select the part of the skin where the data has to be embedded this step is called selection of part or cropping of image. Then set the contrast of the image through histogram modification. After this the image is encrypted using an encryption key to produce an encrypted image. Then, the data hider construct the image using 2-D transform to create a space to accommodate the additional data. Then data is hided through OPA (second order differential equation). After hiding the data, we applying inverse haar transform to re-construct the image, now we get the secret image which look like the original image with secret data. This image is called stego image. Now we send this stego image to the receiver trough a channel or medium this is the most important part of our algorithm because at the transmitter and receiver end the user has control of all the data such as image, secret data or secret key. But once the image has transmitted to the receiver user does not have any control on it.

Most of the error and distortion as well as hacking may occur in our image when it travelled through the channel which is a radio channel. For the protection of our data from the hackers here we are using a second order mathematical differential equation.at the receiver side the user first get the stego image, it is a cover file that contains message bits (information which has to be sent) inside it. This file is communicated over the channel between sender and receiver. Then we select the area where our data is hidden this step is known as hidden area selection, then we transform or construct the image, After this we extract our data through a secret key and view the output which is same as our secret data.

Apply transform to construct the image, here we are using 2D haar transform, we convert our image in second level and four parts which are:

Second level HH, Second level HL, Second level LH

Second level LL

Here we also convert image in to one even dimension and one odd dimension. Figure shows the 2-D Haar transform of image of the image. In this figure two figure are over their first one is base image and the second is 2D Haar transform of the image. Figure 2 shows the Haar transform of Lena image. Here clearly see that base image and his haar transformed image in this figure 2.

Fig.1 - Shows the 2D Transform

4.1 Secret Key Adding

Generate a secret key which is used for hiding and extracting of data. If the user at the receiver does not have secret key, he can only get the image but he cannot extract the secret data embedded in it.so secret key is necessary for user to read the secret message. So therefore in this part of the proposed method adding a secret key with image.

4.2. Secret Data Hiding

For embedding purpose, select a text file in which our secret message is inbuilt. Add this text file in to our image. Now we have embedded image. Embedded image is a combination of cover image and secret data. Now we use OPA algorithm for hiding our data, here we are using second order differential equation. Embedded image is shown in figure 3(b).

4.3 Stego Image

After completing the data hiding process, retransform the image in to original form here we are using 2-D haar transform because it provide perfect reconstruction of image. Now our image is ready to send with our secret data embedded in it. This image is called stego image. Now we transmit this stego image to the receiver through radio channel. Stego image shown in figure 3(c)

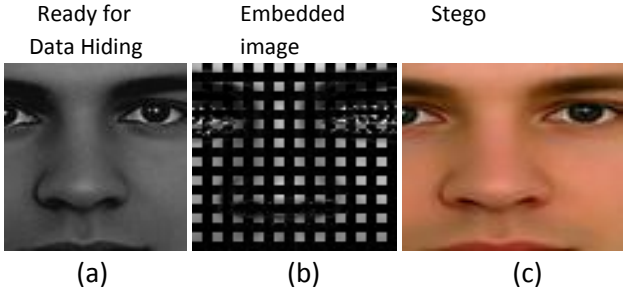

Fig.2 - (a) Shows Cropping image (b) Embedding (c) Reconstructed image or Stego image

Now our image is ready to send to the receiver. The image is sent to the receiver through a communication channel (radio channel), during the transmission of image through this channel hacker may attack on the image, that's why we hide our data using second order mathematical differential equation to protect our data by the hacker. In the figure 4 show the complete process of transmitter end of information hiding process in image. The complete process done in transmitter end by step A to step F. Now discuss about the receiving end.

4.4 Area Identification

At the receiver end we first get the secret image which is known as stego image. It is a cover file that contains message bits (information which has to be sent) inside it. This file is communicated over the channel between sender and receiver. After getting stego image we select the area of the image where our data is hidden, this step is called hidden area selection. The particular part of the image where we hide our data has already define in transmitter end algorithm. Transform in this step we again transform our image using 2-D haar transform. Here we are using 2-D haar transform because it has the property of real and orthogonal.

4.5. Information Extraction

After transform we get our secret message from the image by using same secret key which is used at the receiver to hide the data. Now we check our data which is same as the secret data which is hidden at the transmitter.

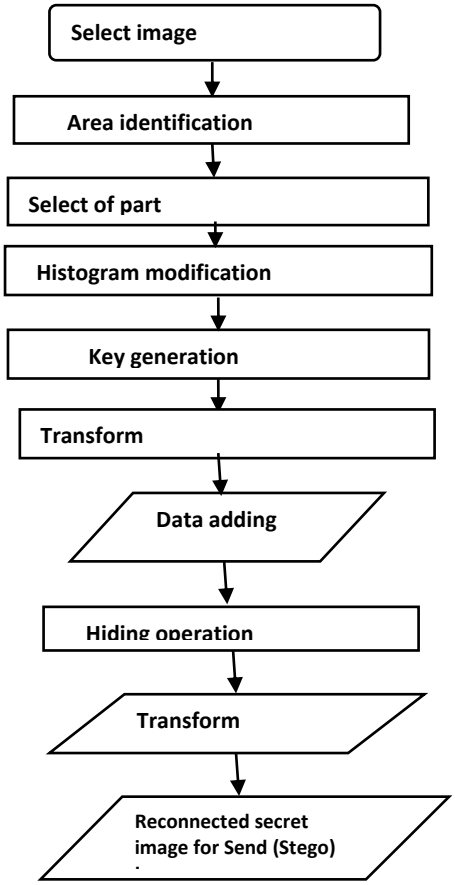

Fig. 3 - Flow chart of Data Embedding

4.6. Validation

Validation: here we validated the received secret image to calculate the peak signal to noise ratio (PSNR), and mean square error (MSE), to check the quality of the image

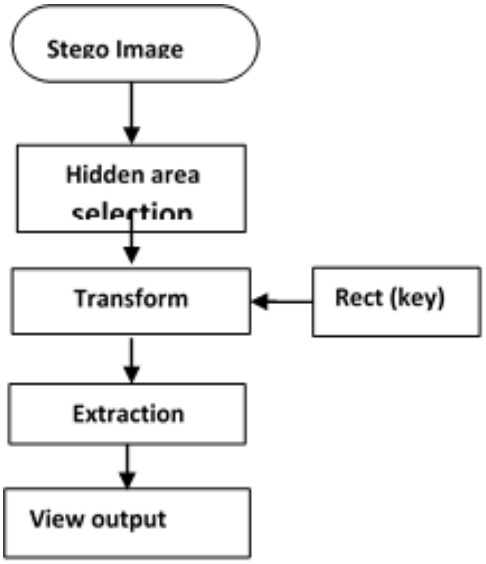

Fig. 4 - Flow chart of Reviver End

Received end process is shown in the above figure 4. It shows the complete flow chart of receiver end of proposed method.

5. RESULTS

The result of our proposed method for data hiding with contrast enhancement in natural images shown in this section, simulation of our proposed method and result calculation. We have done our proposed work with the help the MATLAB R-2013b (8.0.0.783) software and simulate our whole proposed methodology in graphical user interface (GUI). The performance of the proposed algorithm is tested for different color natural face images that is shown in figure 7. Basic configuration of our system is: Dell 4540s Processor: Intel (R) Quad Core (VM) i3 – 3110 Central Processing unit @, 2.40 GHz with 4GB RAM: System type: 64-bit Operating System. MATLAB based simulation result shows good PSNR value for stego image and better quality of stego image as compare to other method that is shown in table II. In the field of image data hiding, people normally have anxiety about the stego image, the capacity of the embedded secret information or data, and BR of the output that is distributed in a communication channel. These criteria can be evaluated by PSNR in dB, Capacity in bits, BR in Bits/pixel (b/p) respectively. Performance of our proposed method are quantitatively measured by PSNR, MSE and BR values defined by:

$$PSNR = 10\log_{10} \frac{(\mathrm{M \times N})^2}{\mathrm{MSE}} \quad (1)$$

Where MSE (Mean square error), is

$$MSE = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\sum_{k=1}^{S}(Y_{i,j,k} - \hat{Y}_{i,j,k})^2}{m \times n \times s} \quad (2)$$

Where M and N are width and length of the image for gray scale image but color image contain three frames of these are red, green and blue that why in color image take respectively.

TABLE IComparison of PSNR, MSE, Entropy and Time values of different NATURAL IMAGE

IMAGE	PSNR	MSE	Entropy(E)	Timing
Image 1	27.3194	33.7661dB	5.3288	9.71
Image 2	35.8336	32.5879dB	6.398	11.22
Image 3	33.1967	32.9199dB	6.741	10.486
Image 4	23.6465	34.3931dB	7.5692	12.481
image 5	33.1862	32.9212dB	5.3527	11.438
image 6	34.7146	30.1642 dB	7.1745	12.683

(a) (b) (c)

6. CONCLUSION

The secure data hiding is a very important and challenging task in the field of data communication.in this research article a new steganography algorithm has been proposed with property of contrast modification. This new methodology describes how we can maintain the image quality by histogram modification, and protect the image during transmission by using second order mathematical differential equation.so after studying this new technique it has been concluded that we can hide our data in image, without compromising security as well as image quality.in this algorithm ,image quality has minimum degradation after performing all the operations such as encryption, decryption, data hiding, data extraction etc. we has also concluded that high peak signal to noise ratio (PSNR) also of the decrypted image is observed after performing all the operation. In the research article we also focused on some basic improvement of stego image because when data hiding operation perform maximum times image pixel disturb so that why in proposed method we also improve the quality of the image in terms contrast and histogram enhancement of stego image. In future we will implement this method in a hardware through one of the famous technique in VLSI that is FPGA simulation and also improve the data capacity in stego image.

7. REFERENCES

[1] J. A.Stark “Adaptive image contrast enhancement using generalizations of histogram equalization, “IEEE Trans Image process, vol.9, no.5, pp.889-896, May 2000.

[2] Manu devi and Nidhi sharma, “Improved detection of least significant bit steganography algorithms in color and gray scale images” Proceedings of 2014 RAECS UIET Punjab university chandigarh, pp 6-8, March, 2014.

[3] Morkel. T, J.H.P. Eloff, M.S. Olivier “An overview of image steganography”, Proceedings of the Fifth annual information security South Africa conference (ISSAC), Sandton, South Africa, (2005).

[4] Sudhir goswami, Jyoti goswami and Rajesh mehra, “An efficient algorithm of steganography using JPEG colored image” IEEE International conference on recent advances and innovations in engineering (ICRAIE-2014), May 2014.

[5] Khalid A. Darabkh, Iyad F. Jafar,Raed T.Al Zulbi, And Mohammad Hawa "An improved image least significant bit replacement method” MIPRO , 26-30 May 2014, Opatija, Croatia.

[6] H.-C.Wu, N.-I. Wu, C.-S. Tsai, and M.-S. Hwang, “Image steganography scheme based on pixel-value differencing and LSB replacement methods,”IEEE proceddings on Vision, image and signal processing, Vol. 152, no. 5, pp.611-615, 2005.

[7] Reena M. Patel and D J Shah "Multiple LSB data hiding based on pixel value and MSB value”2013 nirma university international conference on engineering,NUiCONE , November 2013.

[8] Jawad M.J., “Hiding audio using wavelet transform”,M.Sc thesis, college of science,Al-Nahrain university,Iraq, 2005.

[9] Deepali singla and Mamta juneja,”An analysis of edge based iamge steganography techniques in spatial domain” Proceedings of RAECS UIET Punjab university chandigarh, March, 2014.

[10] Anderson R.J., “Streching the limits of steganography”springer lecture notes in computer science,vol.1174, pp.39-48, 1996. computer based system, pp.159-168, 2008.

[11] T. Zhang and X Ping,”Reliable detection of LSB steganography based on the difference histogram,”IEEE international conference on acoustics, speech and signal processing, vol.3, pp.545-548, april,2003.

[12] Kathryn Hempstalk, "Hiding behind corners:Using edges in image for better steganography”,proceddings of the computing women’s congress, 2006.

[13] M.M. Amin, M. Salleh, S. Ibrahim, M.R.K. Atmin and M.Z.I. Shamsuddin, “Information hiding using steganography”4th national conference on telecommunication technology. NCTT,pp. 21-25, Jan. 2003.

[14] Shahzad alam, vipin kumar, waseem A .siddiqui and musheer ahmed,, “Key dependent image steganography using edge detection” fourth international conference on advance computing and communication technologies,IEEE-ICACCT , 2014.

[15] Wei-jen wang, Cheng-ta huang and shiuh-jeng wang,– “VQ Applications in steganographic data hiding upon multimedia images,”IEEE system journal , vol.5,no.4, December 2011.

[16] Ashwin,s.;Ramesh,j.;Kumar,s.a.;gunavathi,k.”Novel and secure encoding and hiding techniques using image steganography:A survey,”Emerging trends in electrical engineering and energy management(ICETEEEM), pp. 171-177. 2012..

[17] Banoci,v.;Bugar,G.;Levicky,D.”A novel method of image steganography in DWT domain,”RADIOELEKTRONICS, 2011 21st international conference, pp.1-4, 2011.

[18] Babu,K.S.;Raja,K.B.;Kiran,K.K.;Manjuladevi,T.H;venugopal,K.R.,patnaik,L.M.,”Authentication of secret information in image steganography,” TENCON, pp.1-6, 2008.

[19] J.X. Wang and Z,M. Lu , "A path optional losssless data hiding scheme based on VQ joint neighboring coding", Inform.SCI. , VOL. 179, no. 19, pp. 3332-3348, 2009

[20] Z.H. Wang, C.C.. Chang , K.N. Chen , and M.C. Li , "An Encoding method for both image compression and data loss less information hiding " J.syst. softw. Vol 83, no.11, pp. 2073-2082. 2010.

[21] S.C. Shie and S,D. Lin , "Data hiding based on compressed VQ indices of images", Comput. Standrds interfaces, vol. 31 , no.6 pp. 1143-1149, 2009.

[22] C.C. Lee , W.H. KU and S.Y. huang, "A New Steganographic scheme based on vctor quantization and serch order coding ", IET image process,. Vol . 3 no. 4 pp. 243-248, Augest 2009 .

[23] C..C. Chang and W.C. Wu, "Hiding secret data adaptively in vector quantization index table" IEEE proc. Vision, image signal process., vol. 153, no. 5, pp. 589 – 597,2006

[24] C.C. Chang and C.Y .Lin, "Reversible stegnography for VQ –Compressed images using site matching and relocetion" IEEE Tans.inform forensics SEC. vol.1, no. 4 , pp. 493-501, December 2006.

[25] C.C. Chan and C.C. Chang, "High Capcity SMVQ – Based hiding scheme using adaptive index", Signal process. Vol . 90 no. 7. pp. 2141 – 2149, 2010.