Transmission of Hidden Cipher Text over a Binary Symmetric Channel

Arun Rana
N.C. College of Engineering
Israna, Panipat

Nitin Sharma
N.C. College of Engineering
Israna, Panipat

Parveen Malik
N.C. College of Engineering
Israna, Panipat

ABSTRACT
A new high capacity and robust image steganography method based on human vision sensitivity is introduced. Kohonen Neural network is trained according to the contrast sensitivity of pixels present in cover image. Trained network classify the pixels of cover image in different levels of sensitivity. Data embedding is performed by LSB substitution method, which replaces the least significant bits of cover image with secret information that would be embedded. But prior to embedding, cryptography is applied on text. We used Optimal Pixel Adjustment Process (OPAP) to obtain an optimal mapping function to reduce the difference error between the original image and the stego-image, therefore improving the hiding capacity with low distortions. On the destination side, the original image is not needed for extracting the embedded data. Convolution Code are also used to improve performance of existing algorithm over binary symmetric channel (BSC). It is observed that the capacity and security is increased with acceptable PSNR in the proposed algorithm compared to the existing algorithm.

General Terms
Image Steganography, Authenticated Communication.

Keywords
OPAP, BSC, Convolution Codes,

1. INTRODUCTION
Steganography is the art of hiding the message in such a way that no one except the intended recipient is aware of its existence. Secrets can be hidden inside all types of cover information: text, images, audio, video and other executable files. Generally, a data hiding technique is considered to be good if it provide good visual imperceptibility and a sufficient capacity of hidden secret data. The most commonly used steganographic method is LSB (least significant bit) substitution, which replaces the least significant bits of cover image with secret information that would be embedded. LSB methods typically achieve high capacity [1]. Although LSB maintains a good visual quality of stego-image, it can hide litter information. Considering the limitation of LSB, some methods begin to take account of the visual identity that human eyes are insensitive to edged and dark areas when embedding secret information, such as BPCS(bit-plane complexity segmentation [2], DWT(Discrete Wavelet Embedding) and DCT (Discrete Cosine Transform) embedding [3] . With these methods, less secret payload is embedded into smooth areas, more in violent changed areas. The capacity of embedded information is thereby greatly improved while the quality of visual imperceptibility is maintained.
This paper is organized as follows. In the second sections, we give a brief literature survey. Then in section 3, we give a review of OPAP process. In section 4 we illustrate the algorithm proposed in detail, where after the experimental results are given in section 5.Section 6 concludes all aspect of proposed method. The last section of this paper is the future scope.

2. LITERATURE SURVEY
1. In 2007, Anil et.al proposed the secret and robust data transmission over the noisy channel. The secret data is encrypted by AES cryptographic algorithm, further encoded data using concatenated code is embedded into cover image. Experiments show the good quality of the stego-image and high resistant against the Salt and Pepper noise attacks [4].

2. In 2008, Zhang Jiaiia proposed a novel image steganography method based on self organizing map and HVS. According to contrast and texture sensitivity of human vision system, self-organizing map based on unsupervised learning is trained. So NNs trained is the stego key of the embedded and extracted secret data. The method evaluate neighboring pixels(left, right, upper, bottom) to estimate the degree of sensitivity of pixels with NNs trained so that pixels in less sensitive smooth areas can potentially carry more hidden payload as compared to dark area. This method can hide a much larger information and maintains a better visual quality of stego-image [5].

3. In 2011 B. Raja et.al proposed Performance Comparison of Robust Steganography Based on Multiple Transformation Techniques (PCRSMT). The cover image intensity values are evaluated to accommodate payload properly and segmented into blocks of 4*4 each. Discrete Wavelet Transform (DWT) is applied on each block and in the resulting DWT coefficients, blocks of vertical band of 2*2 each are considered and Integer Wavelet Transform (IWT) is applied to get locks of 1*1 each. The IWT is applied on the DWT vertical band of payload and then embedded into the IWT coefficients of the cover image. The concept of Error Detection and Correction Coding (EDCC) technique is used to ensure highly robust communication. It is observed that this algorithm has high PSNR, provides high level security and more robust compared to individual transform techniques [6].

3. OPTIMAL PIXEL ADJUSTMENTPROCESS

In this section, an Optimal Pixel Adjustment process (OPAP) is proposed to enhance the visual quality of the stego-image obtained by the simple LSB substitution method. The basic concept of this process is based on the technique proposed in Ref. [7].

Let P_1, P_2 and P_3 be the pixel values of the i^{th} pixel in the cover-image CI, the stego-image S obtained by the simple LSB substitution method and the refined stego-image obtained after the OPAP respectively. Let err $=P_2–P_1$ be the embedding error between P_1 and P_2. P_2 is obtained by the direct replacement of the k least significant bits of P1 with k message bits, therefore:

$$2^k<err<2^k$$

The value of err can be further segmented into following three intervals, such that

Interval 1 : $2^{k-1}< err <2^k$;

Interval 2 : $-2^{k-1}< err <2^{k-1}$;

Interval 3 : $-2^{k-1}< err <-2^{k-1}$;

Based on the three intervals, the OPAP, which modifies P_1 to form the stego-pixel P_2, can be described as

follows:

Case 1: ($2^{k-1}< err <2^k$): If $P_i \leq 2^k$, then $P_3 =P_2 -2^k$; otherwise $P_3 = P_1$.

Case 2: ($-2^{k-1}< err <2^{k-1}$):$P_3= P_2$.

Case 3 ;($-2^{k-1}< err <-2^{k-1}$): If $P_2<256 - 2^k$, then

$P_3 = P_3 + 2^k$, otherwise $P_3 = P_2$.

4. PROPOSED METHOD

According to contrast value of pixels present in cover image, Neural network is trained. This method exploits all pixels present in cover image to estimate the degree of sensitivity of pixels with trained neural network so that pixels can be classified into different classes of sensitivity. Pixels in less sensitive areas can carry more hidden data as compare to those which are in high sensitive area of human vision. We have used Kohonen neural network for classification [8].

4.1 Data Hiding Method

The steps for secret data hiding are as follows.

(1) Divide the cover image into 8*8 blocks. Apply Discrete wavelet transform to decompose each block of the cover image.

(2) Calculate the absolute sum of wavelet contrast coefficients C. The smaller the value of C is, the lesser the secret information will be embedded in that block.

(3) Train the neural network according to the calculated contrast C. Use trained network to classify the blocks into 3 categories. Blocks with largest C is a class Q_1, while that with smallest is a class Q_2, and rest is Q_3. Imbed secret information into image.. According the result of NN, Imbed secret information with *mi* ($m_1>m_2>m_3$). Imbed $floor(\log_2(m^{r*l-1}))$ secret data into the block.

(4) Unlikely traditional steganography algorithms, we have changed plain text into cipher text before embedding into image.

(5) Embed the cipher text into image by LSB substitution method.

(6) Apply the Optimal Pixel Adjustment Process over stego Image.

(7) Use Error detecting code to encode the stego image to improve its robustness over a binary symmetric channel. In proposed method Convolution codes with generator matrix [1 1 1 0; 1 0 0 1; 0 1 0 1; 1 0 0 1] is used.

4.2 Extraction of Data

The extraction of embedding data is easy. The The steps for data extracting are as follows.

(1) Apply Viterbi Decoding procedure over the received corrupted Image.

(2) Divide image and decomposed by wavelet. Divide image into 8*8 blocks, then decomposed each blocks by Extract the number of block.

(3) Use steganography based on module extract secret The pixel noting the number is not used for extraction.

(4) Provide the cipher key to recover plain text from received cipher text.

Here it should be noted that we do not need decoding procedure of OPAP process and also we do not need original image at receiver side to extract data. Actually, by using OPAP and codes we are improving capacity and robustness of wavelet contrast based Steganography method [5].

We have used error correcting codes on our stego image, however we can also use encode the text by same convolution codes before embedding .This Procedure of embedding encoded text with parity bits may also be used to tackle erroneous channel and noise present in image.

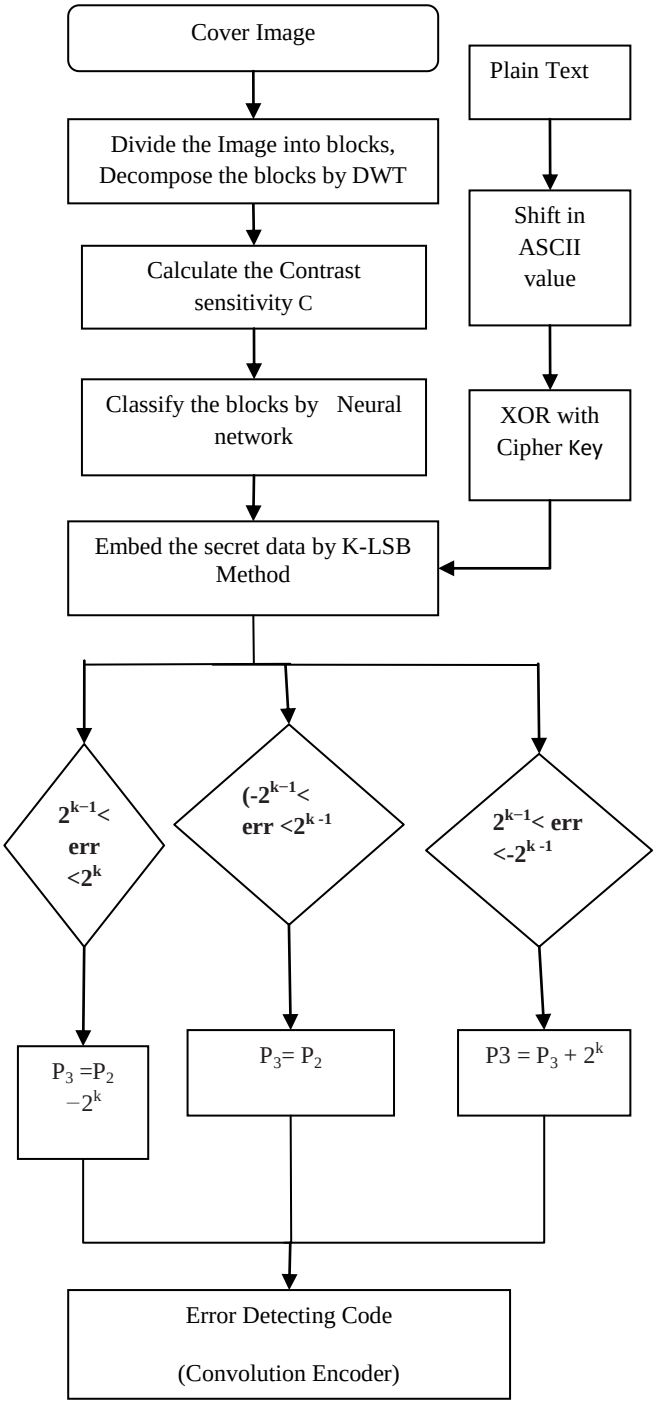

Fig.3.1 Flow Chart of proposed Algorithm

5. RESULTS

It is important to evaluate an image Steganography algorithm on different images. We have the Data Base as a standard evaluation for Steganography Algorithms. Figure 4.1 presents some of the sample images that have been used in the experiments. They are three images: "LENA" (151875 bytes), "GOLD-HILL" (151875 bytes), "ARUN" (1440000 bytes). We read the host image file on which we are going to implement our algorithm to MATLAB workspace and do the needful changes on that like if the image is in RGB format we convert it into grayscale and if the size of the image is too big then convert it to the nominal size. A comparison between our proposed and image steganography method given by Jiajia et.al [5] using LSB data embedding is shown below.

Fig.4.1 Images used for evaluation of proposed Algorithm

Lena Arun Gold-Hill

Table 4.1 Performance Evalutation of Propsed method with 4 bit LSB substitution

Images	Capacity (Bytes)	PSNR(dB)	
		Proposed Method	Jiajia [5]
Arun.jpg (256*256)	100	67.108	63.6145
	200	59.13	56.409
	400	55.88	53.45
	800	52.665	50.1015
	1600	49.877	47.36
Lena.tif (256*256)	100	64.15	62.05
	200	61.15	59.42
	400	57.3	55.19
	800	53.64	51.4
	1600	50.6	48.41

Table 4.2 Performance Evalutation of Propsed method with 3-bit LSB substitution

Images	Capacity (Bytes)	PSNR(dB)	
		Proposed Method	Jiajia[5]
Arun.jpg (256*256)	100	69.34	68.35
	200	63.89	61.88
	400	60.56	58.41
	800	56.96	54.77
	1600	54.67	52.6185
Gold-Hill (256*256)	100	70.10	69.86
	200	66.87	66.42
	400	63.77	63.1
	800	60.58	59.85
	1600	57.44	56.54

Subjective Results can also be shown for explaining the significance of cryptography used in proposed method. Let "**abcdefghijklmno**" is our plain text then after applying shift in ASCII value this may be changed in "**fghijklmnopqrst**".By xoring with private key we can get more randomness in cipher text. Let assume we have used 17(key) for exoring with cipher text then results will be "**wvyx{z}|□~a`cbe**".

Table 4.3 Robustness Evalutation of Propsed method over a Binary Symmetric Channel

Binary Symmetric Channel	**Data Recovered in Percentage (Cipher data =100 bytes)**	
Error Probability	**Proposed Method**	**Arun et.al [9]**
0.01	100	60
0.02	100	30
0.03	100	24
0.04	100	22
0.05	100	19
0.06	100	12
0.07	100	10
0.08	90	6

6. CONCLUSION

In this paper, we present an improved steganographic method based on Neural Network, OPAP and Convolution Codes. The proposed method adopts the character that human eyes are not sensible to the dark and texture area of image. More secret information is embedded into the dark and texture areas, less in smooth areas according to wavelet contrast. Compared with Jiajia's method [5], the proposed method can hide more information and maintains a better visual quality of stego-image. The amount of information carried by individual pixels is decided by trained Neural Network, which act as a secret key. Therefore, any third unauthorized party will be unable to detect or extract the embedded data when he or she does not know the secret key. Use of codes improved data recovery to a greater extent over binary symmetric channel. Conversion of plain text into cipher text provide one more level of security to data.

7. FUTURE SCOPE

1. In our proposed work, the image is first to be converted into gray image. This limitation can be eliminated and algorithm can be applied directly to color images, and the detection would then become significantly more complex.

2. Applying error correcting codes on stego image is a time consuming method so in future, prior to embedding, text can be encoded by Concatenated codes to attain same level of robustness.

3. Proposed algorithm need to be tested against AWGN channel also.

REFERENCES

[1] Li Zhi,Sui Ai Fen and Yang Yi Xian,2003, " A LSB Steganography Detection algorithm" in Proceeding of 14th International Symposium on Personal Indoor and Mobile Radio Communication, pp. 2780-2783.

[2] M. Niimi, H.Noda and B.Segee.2005.A Robust BPCS-Steganography against Visual Attacks: 5th International Conference on Information Communication and Signal Processing (IICSP), pp. 1116-1120 .

[3] Dr. Fadhil Salman Abed, Nada Abdul Aziz Mustafa,"A proposed Technique for Information Hiding Based on DCT" International Journal of Advancements in Computing Technology Vol. 2, Number 5, 201, pp.184-188.

[4] Anil et. al. 2007, Robust and Secret Data Transmission Over the Noisy Channel in proceeding of International conference on signal processing and Networking, IEEE, pp.199-203

[5] Zhang Jiajia et.al, 2009, "A Steganographic Method based on SOM and Wavelet Contrast" in proceeding of International Conference on Artificial Intelligence and Computational Intelligence, pp. 481-484.

[6] K B Raja et.al, "Performance Comparison of Robust Steganography Based on Multiple Transformation Techniques" International Journal of Computer Technology and Applications, 2011. pp. 1035-1048.

[7] Chi-Kwong Chan, L.M. Cheng.2001, "Improved hiding data in images by optimal moderately significant-bit replacement" IEEE Electron. Letter 37 (16)) 1017–1018.

[8] H.Ritter, K.Schulten.1988.Kohonen's Self Organizing maps: exploring their Computational Capabilities in proceeding of IEEE International Conference on Neural Networks, ICNN, pp. 109-116.

[9] Arun Rana et.al,"Image Steganography Method Based on Kohonen Neural Network" International Journal of Engineering Research, 2012, pp.2234-2237.

.