 ISSN: 2454-4248
08 – 12

Improved Performance of Image Steganography Technique using Quantum Scrambling and Pixel‘s Intensity Adjustment

Mani Rathore
Engineering College, Bikaner
rathoremani16@gmail.com

Mr. Narpat Singh Shekhawat
Assistant Professor
Engineering College, Bikaner

***Abstract*—** Steganography is the art for hidden communication. It provides the solution for secrete data communication. Trustworthy steganography techniques should provide the data protection when it is being transferred and fulfill the principles of security. This dissertation proposed a efficient steganography technique based on Quantum Hilbert image Scrambling (QHIS), alpha blending operation, and genetic algorithm based pixel's least significant bit swapping. Every steganography technique has two processes; encoding and decoding. In the encoding process of proposed steganography technique, initially secrete image is scrambled using QHIS then apply alpha blending (i.e type of mixing) operation on both the scrambled image and cover image, which results stego image. The stego image picture quality can be improved by allying GA based pixel's adjustment.

The strength of proposed steganography technique is shown in experimental results by testing it on different image quality parameters (i.e. Peak Signal to Noise Ratio, Normalized Cross Correlation, Average Difference, Maximum difference, Structural contents).

Keywords- *Steganography; communication; secrete data; Quantum Hilbert image Scrambling; stego.*

*****

I. INTRODUCTION

Today in the word of digitization sending the confidential information demands the security. So data transmission is the great concern when it is confidential so different secure information transfer techniques are used when the information is being transferred from one place to another place. Steganography is one of them. It is an art of hiding the information within the cover media. Any digital media may be chosen as a cove media like; image, text, audio, and video. The one big advantage of using steganography hare is; it hide the information within the carrier media or cover media so the inside secret information is not visible by outsider. So here is no chance to detect by the neck eyes. After applying the secret information embedding process the resultant image is known as stego media.

The steganography is one of the techniques for secure information transfer from other techniques like; cryptography, watermarking [6].

Steganography is the branch of information system security. Information system security can be classified in to three types, these are as follow;

1. Cryptography
2. Steganography
3. Watermarking

All the three techniques are used in data protection according to the application area. In steganography information is transferred by hiding it inside the carrier where as in cryptography information is transferred into encrypted form. In steganography the feature of secrete data is invisible to outsider where as in cryptography no cover media is used so information is shown in encrypted form or in other world we can say that the feature is visible to everyone.

There are many kids of cryptography techniques are available. These technique convert the meaning full information (plain text message) into the meaningless information know as cipher text.

For example; if we apply encryption at Hello message then we get some cipher text message as shown in following figure

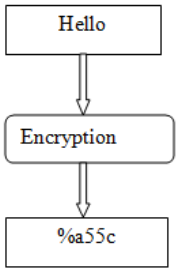


Figure 1: Encryption process

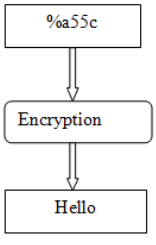


Figure 2: Decryption process

 ISSN: 2454-4248
08 – 12

II. LITERATURE REVIEW

The possibility of steganography was first introduced in [8] at 1983. It shows the situation of steganography framework [8]. Steganography situation can be outlined in two distinct stages: encoding (implanting) stage with the assistance of mystery key and translating (extricating) mystery information stage with the way of saving data undetectable.

In the time of 2013 Soni, A.; Jain, J.; Roshan, R., The Fractional Fourier change (FrFT), [1] Investigated on as a speculation of the traditional Fourier change, presented years prior in arithmetic writing. The upgraded calculation of fragmentary Fourier change, the discrete rendition of FrFT appeared DFrFT. This investigation of delineates the upside of discrete partial Fourier change (DFrFT) when contrasted with different changes for steganography in picture handling. The outcome indicates same PSNR in both area (time and recurrence) yet DFrFT gives a bit of leeway of extra stego key. The request parameter of this change.

In the time of 2013 Akhtar, N.; Johri, P.; Khan, S., [2] actualized a variety of plain LSB (Least Significant Bit) calculation. The stego-picture quality has been improved by utilizing bit-reversal method. LSB strategy improving the PSNR of stegoimage.

In the time of 2013 Prabakaran, G.; Bhavani, R. also, Rajeswari P.S. [3] Investigated on Medical records are amazingly delicate patient data a multi secure and heartiness of therapeutic picture based steganography plan is proposed. This procedure gives a productive and capacity security instrument for the insurance of computerized restorative pictures.

In the time of 2012 Thenmozhi, S. also, Chandrasekaran, M., [4] introduced the novel plan installs information in number wavelet change coefficients by utilizing an editing capacity in a 8×8 square on the spread picture. The ideal pixel change procedure has been connected in the wake of inserting the message.

V. Kumar and D. Kumar defined [5] the approach which based on Discrete Wavelet Transform (DWT) the wavelet coefficients of the cover image are modified to embed the secret message.

In may 2018 Vijay Kumar Sharma, Devesh Kumar Srivastava, Pratistha Mathur [7] proposed a graph wavelet transform-based steganography using graph signal processing (GSP). The research work defined better visual quality stego image as well as extracted secret image.

According to [9] Stego image visual quality is increased by using Daubechies wavelet.

III. PROPOSED WORK

A steganography technique for hiding secrete image inside the cove image using scrambling and pixel swapping operation is proposed in this section. The main aim here is to provide invisibility of secrete image inside the stego-image.

The proposed steganography technique has two processes:- 1). Secrete image embedding, 2). Retrieving the secrete image. in the embedding process, initially secrete image is scrambled by using QHIS scrambling, then apply alpha blending operation on every pixel of cover image and secret image which results the stego image. Here the stego image picture quality can be improved by using pixel swapping operation applied at stego image.

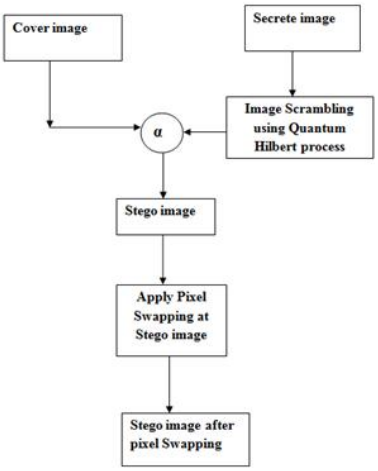


Figure 3: Block diagram for encoding the secrete image

The algorithmic steps of proposed steganographic encoding process are as follow:

Step1. Input the cover image (C).

Step2. Apply image Scrambling(QHIS image Scrambling.) on secrete image, and get SS (scramble secrete image) image

Step3. Perform Alpha operation at every pixels of cover image and scrambled secrete image and generate stego image.

Stego image= C + αSS

Here C represents the cove image and SS is the scrambled image, α represents mixing operation.

Step 4. Apply LSB based Pixel swapping operation at stego image (i.e. obtained in step 3) and get the stego image after LSB based pixel swapping operation.

The secrete image extraction process is just reverse of the embedding process.

a. Pixels LSB swapping process

To enhance the picture quality of stego image adjacent pixel pair's LSB bits are swapped and this process is applied on ever pixel pair of stego image. This applied pixel pair LSB bit swapping process is inspired by Genetic algorithm. The algorithmic steps the pixel pair intensity adjacent are as follow:

1. Initialization:

In the initialization process two adjacent pixels from a row are selected and generate two new pixel pairs form the adjacent pixel pair. The pixel pair generation process is shown in step2.

2. Generation of two new pixel pair:

The process for two Pixel pairs generation from the original pixel pair are shown in table 1.

 ISSN: 2454-4248
08 – 12

1st Pixel Value	2nd Pixel Value	Operation at first LSB		Newly Generated Pixel pair		
		1st Pixel	2nd Pixel			
64	91	No Swap	No Swap	C1=	64	91
		Swap	Swap	C2=	65	90

Table 1: Two Possible pixel pair

3. Selection of Pixel pair:

Out of two generated pixel pair, the one who minimize their difference value (intensity difference) is selected.

4. Intersection:

This pixel pair (i.e. 64 and 91 in original image) is shifted to one pixel right and applies the process on hall image pixels.

After applying this pixel adjustment process on stego image. the stego image visible quality will improved. It can be seen in result section.

B. Quantum Hilbert based secrete image scrambling

The scrambling process of the proposed steganography technique is based on quantum circuits. These recursive and progressively generates the scrambled version of the secrete image. by using QHIS scrambling the image can scrambled more efficiently.

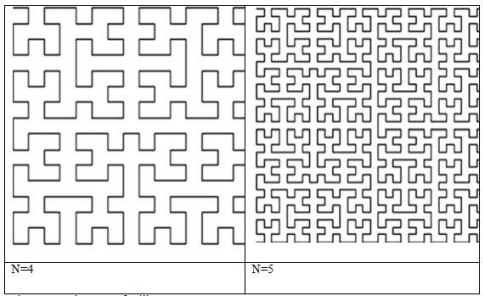


Figure 4: images of Hilbert curve

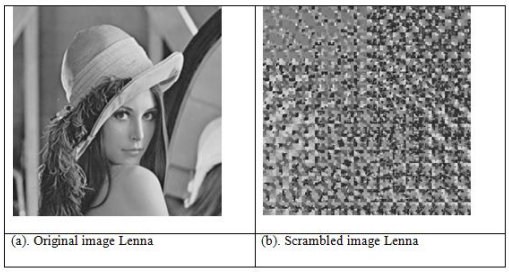


Figure 5: Image and its corresponding scrambled image

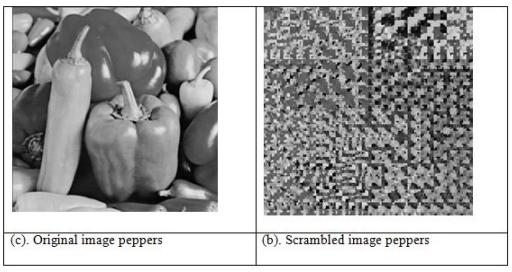


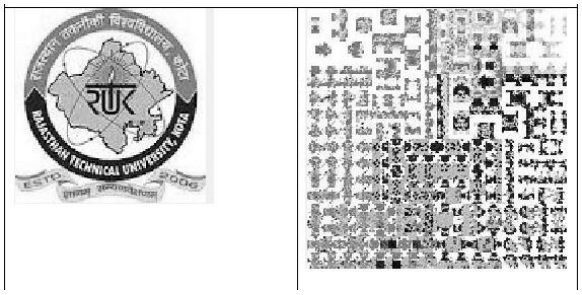
Figure 6: shows the image to be scramble and corresponding scrambled image

IV. RESULTS AND ANALYSIS

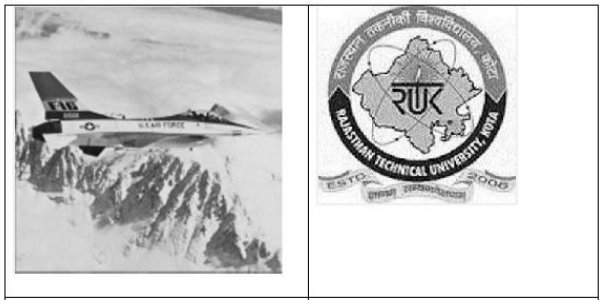
All the experimental results are generated using the MATLAB. It can be clearly seen in the results section that there is no visible difference in between two images (i.e. steo image and cover image). Different cover image and secrete image are used during the experiment.

The performance of the proposed method is evaluated by implementing it. By taking jet.tiff as the cover image, rtu.jpg as the secrete image.

(a). Original host image: Lenna.tiff



(b). secret image: rtu.jpg (c). Scrambled image



(d). Stego- image (e). Extracted image

Figure 7: Results for Encoding and Decoding of cover image (jet.tiff) and secrete image (rtu.jpg).

The performance of proposed method is tested on some of the image quality parameters these are as follow:

1). Peak Signal to Noise Ratio (PSNR),
2). Mean Square Error (MSE),
3). Normalized Cross Correlation (NCC)
4). Average difference (AD)
5). Structure Contents (SC)

The formula for PSNR is shown in equation

$$PSNR = 10 \log \frac{255^2}{MSE} DB$$

 ISSN: 2454-4248
08 – 12

Here, MSE represents the mean square error, which is defined for Mx N image size as follow.

$$MSE = \frac{1}{M*N}\sum_{j=1}^{M}\sum_{k=1}^{N}(x_{j,k} - x'_{j,k})^2$$

Here xj,k and x'j,k are the pixel position at jth row and kth column for cover image x and secrete image x' respectively.

Better PNSR represents less number of MSE errors.

NCC is correlation between two image, this is represented by follows equation

$$NCC = \sum_{j=1}^{M}\sum_{k=1}^{N} x_{j,k} \cdot x'_{j,k} / \sum_{j=1}^{M}\sum_{k=1}^{N} x_{j,k}^2$$

AD is the average difference between the cover image and stego image pixels; it is represented by equation

$$AD = \frac{\sum_{j=1}^{M}\sum_{k=1}^{N}(x_{j,k} - x'_{j,k})}{M * N}$$

SC denotes the structural contents, it is calculated by using following equation

$$SC = \frac{\sum_{j=1}^{M}\sum_{k=1}^{N}(x_{j,k})^2}{\sum_{j=1}^{M}\sum_{k=1}^{N}(x'_{j,k})^2}$$

The experimental results of the proposed techniques are tested on the different host image and the secrete image at the varying values of alpha. Table 1 shows the scrambling and descrambling results of a log of college of business and entrepreneurial technology.

The proposed steganography method is compared with the other existing technique. Our technique provides the better results in terms of PSNR and AD, as compared to the previously existing technique and our proposed method provides excellent results for NCC and SC values. Table 2 shows the results related to PSNR and NCC.

Cover image	Secret image	Proposed Technique before pixel adjustment		Proposed Technique after pixel adjustment		Existing Technique	
		PSNR	NCC	PSNR	NCC	PSNR	NCC
Lenna.Tiff	Message.jpg	42.1052	0.9861	43.7490	0.9891	41.6892	0.9969
Flower.jpg	Message.jpg	42.1052	0.9864	43.9392	0.9898	41.8758	0.9969
Peppers.Tiff	Message.jpg	42.1052	0.9866	43.6899	0.9894	41.4321	0.9969
Goldhill.jpg	Message.jpg	42.1052	0.9853	44.0611	0.9890	41.9740	0.9966

Table 2: Comparison of Proposed Technique with the Existing Technique In Terms Of PSNR and NCC

Cover image	Secret image	Proposed Technique before pixel adjustment		Proposed Technique after pixel adjustment		Existing Technique	
		AD	SC	AD	SC	AD	SC
Lenna.Tiff	Message.jpg	-1.9893	0.9724	-1.5655	0.9783	- 0.4215	0.9939
Flower.jpg	Message.jpg	-1.9893	0.9731	-1.5290	0.9798	-0. 4216	0.9940
Peppers.Tiff	Message.jpg	-1.9893	0.9733	-1.5779	0.9789	-0.4215	0.9940
Goldhill.jpg	Message.jpg	-1.9893	0.9708	-1.5008	0.9781	-0.4215	0.9935

Table 3: Comparison of Proposed Technique With The Existing Technique In Terms of AD And SC.

From the table 2 and 3 it can be clearly seen that the picture quality of stego image will be increases after applying the pixel adjustment operation at stego image. Results of all parameters are very good when we apply the pixel adjustment operation at stego image.

V. CONCLUSION

A new robust steganography technique has been proposed in this dissertation. The quality of extracted secret image is excellent as shown in results. The secret image is invisible or imperceptive inside the stego image because before embedding the secret image is scrambled which results the excellent invisibility of secret image inside the stego image.

It is concluded that the proposed technique provide good PSNR, NCC, AD, and MD values which are sufficient to prove the strength of proposed steganography technique. Our technique provides better results after applying the pixel adjustment operation at stego image.

It can be also concluded that our proposed technique gives the excellent results in NCC value means NCC value is obtained 99%.

The feature work will focus on other types of steganography techniques based on different wavelets like, DWT, counturlet and some advance wavelets such as Graph wavelet etc.

REFERENCES

[1] Soni, A.; Jain, J.; Roshan, R., "Image steganography using discrete fractional Fourier transform," Intelligent Systems and Signal Processing (ISSP), 2013 International Conference on , vol., no., pp.97,100, 1-2 March 2013.

[2] Akhtar, N.; Johri, P.; Khan, S., "Enhancing the Security and Quality of LSB Based Image Steganography," Computational Intelligence and Communication Networks (CICN), 2013 5th International Conference on , vol., no., pp.385,390, 27-29 Sept. 2013.

[3] Das, R.; Tuithung, T., "A novel steganography method for image based on Huffman Encoding," Emerging Trends and Applications in Computer Science (NCETACS), 2012 3rd National Conference on , vol., no., pp.14,18, 30-31 March 2012.

[4] Hemalatha, S.; Acharya, U.D.; Renuka, A.; Kamath, P.R., "A secure image steganography technique using Integer Wavelet Transform," Information and Communication Technologies (WICT), 2012 World Congress on , vol., no., pp.755,758, Oct. 30 2012-Nov. 2 2012.

[5] V. Kumar and D. Kumar, "Performance evaluation of DWT based image steganography," IEEE 2nd International Advance Computing Conference (IACC), Patiala, 2016, pp. 223-228.

[6] Thenmozhi, S.; Chandrasekaran, M., "Novel approach for image stenography based on integer wavelet transform," Computational Intelligence & Computing Research (ICCIC), 2012 IEEE International Conference on , vol., no., pp.1,5, 18-20 Dec. 2012.

[7] Vijay Kumar Sharma, Devesh Kumar Srivastava, Pratistha Mathur, "Efficient Image Steganography using graph signal processing", IET image processing Journa, Volume: 12 , issue 6, pp. 1065 - 1071 2018.

ISSN: 2454-4248
08 – 12

[8] G. J. Simmons, "The Prisoners' Problem and the Subliminal Channel," in Advances in Cryptology: Proceedings of CRYPTO '83, springer, 1983, pp. 51–67.

[9] Sharma V.K., Mathur P., Srivastava D.K. Highly Secure DWT Steganography Scheme for Encrypted Data Hiding. In: Satapathy S., Joshi A. (eds) Information and Communication Technology for Intelligent Systems. Smart I nnovation, Systems and Technologies, Vol 106, pp pp. 665-673, Springer, Singapore, 2019.