Figure 4: Stego Image

This stego image under goes AES encryption in parallel to give the final encrypted image as in Fig 5.

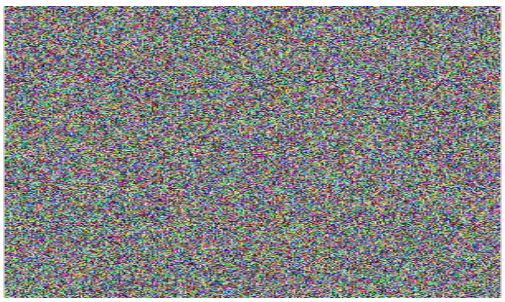

Figure 5:.Encrypted Image

This encrypted image is then sent at the receiver's end and who in turn uses the key k2 to get back the stego image from encrypted image as in Fig 6.

Figure 6: Decrypted Stego Image

From the stego image the user has to extract data to get back the original data using the key k1,thus user having both the correct keys will be able to get back the original image and data. Fig 7.

Figure 7: Image after data extraction

If in case the size of the data is small and the image has more capacity, then the remaining pixels of the image are embedded with random data so as to avoid steganalysis. The statistical analysis show that the PSNR ratio decreases as we go on hiding more data into the carrier image as more number of bits are needed to be altered for storing it. This can be easily studied from the comparison shown in the Table 1.

Table 1: PSNR and QIUI values for Decrypted Image

Image	*Available space (bytes)*	*Data to be hidden(bytes)*	*Actual bit loss %*	*PSNR without data padding*	*PSNR with data padding*	*UIQI*
Image	294912	0	0.0000	97.2298	49.0432	0.9742
	294912	147456	12.5002	54.1401	51.1413	0.8919
	294912	294912	25.0005	51.1372	51.1447	0.8835

Table 2 shows the bits loss for each key in the unique key set. Depending on the total bit loss percentage the key is selected for embedding and hiding the data. The key which gives minimum bit loss is used. In this case while embedding full data into image the key used is key no.2 which gives minimum bit loss of only 25.0005%.

Table 2: Bit loss calculation for each LFSR key

Key No	*Total Bit loss %*	*Key No*	*Total Bit loss %*	*Key No*	*Total Bit loss %*
0	49.981	11	37.5006	22	50.0002
1	25.0006	12	50.0006	23	50.0005
2	25.0005	13	50.0019	24	50.0006
3	25.0009	14	37.5008	25	37.5008
4	37.5009	15	37.5008	26	25.0009
5	37.5008	16	50.0006	27	37.5007
6	37.5008	17	62.5004	28	37.5008
7	50.0006	18	75.0003	29	37.5009
8	50.0005	19	75.0001	30	50.0008
9	50.0003	20	62.5003	31	37.5008
10	37.5006	21	50.0004		

Table 3 shows the percent time saved by applying the AES encryption algorithm in parallel as compared to normal AES algorithm.

Table 3: Percent time saved by applying AES in parallel

Image	*Image Size (kb)*	*Encryption time(ms)*	*Parallel Encryption time(ms)*	*% time saved*
Image 1	4122	2590	890	65.64
Image 2	2224	1780	630	64.61
Image 3	827	360	130	63.89

10. Conclusion

Steganography is an effective way of hiding the sensitive information. In this paper we have used the LSB technique on images to get the secure stego-image which is encrypted and then sent to the receivers. As we are altering the last bit of each channel of every pixel so there is non-significant change in the image and also we check and use the key that makes minimum changes in the bit pattern for every pixel. This paper focused on hiding more data while increasing the PSNR and reducing the distortion rate. It also focuses in getting the QIUI to close to 1 so that we get minimum distortion in the decrypted Image.

As a future scope we can work on using audio, video instead of cover image for hiding the data. Also an addition of integrity check after the image is ready to be sent is considerable. This will make sure that the receiver is decrypting an original i.e. an unaltered Image. This will make sure that the data thus obtained from the image is 100 % correct.

11. Acknowledgement

I would like to thank project guide Prof. Todmal S., Prof. Phursule R., Prof. Wadane V. and our Principal Dr. Admane S. for their valuable comments and suggestions.

References

[1] Announcing the ADVANCED ENCRYPTION STANDARD (AES), csrc.nist.gov/publications/fips/fips197/fips-197.pdf.
[2] A Secure Image Steganography Using LSB Technique and Pseudo Random Encoding Technique.
[3] Linear feedback shift register ,from Wikipedia, the free encyclopedia.
[4] Separable Reversible Encrypted Data Hiding in Encrypted Image Using AES algorithm and Lossy Technique.
[5] Separable Reversible Data Hiding Using Rc4 IEEE 2013.pdf.
[6] Separable Reversible Data Hiding in Encrypted Image, Xinpeng Zhang, IEEE Transactions on Information Forensics and Security, VOL. 7, NO. 2, APRIL 2012.
[7] A Universal Quality Index,Zhou Wang,Student Member IEEE and Alan C.Bovik,Fellow,IEEE