5. CONCLUSIONS

5.1 CONCLUSIONS

We have studied various existing steganographic techniques to hide information like Hide & Seek, JSteg, OutGuess 0.1, OutGuess 0.2, F3. The limitations prevailing in those techniques were found. Hide & Seek and JSteg algorithm follows the sequential least significant bit for embedding. While, OutGuess 0.1 & OutGuess 0.2 are better as compared to Hide & Seek and JSteg because it scatters the locations for embedding by using a PRNG to shuffle the ordering. Moreover, F3 is advanced compared to all other techniques as it is embedded in DCT coefficients equal to 1 and avoids embedding in 0. The algorithm still embeds the message data sequentially. Further, F4 is enhanced but it results in shrinkage mechanism. But, in F5 disturbance is minimized by using the matrix encoding scheme. While Davern Scott, Barnsley use fractal image compression technique in which self similarity of structure in image is found through fractal compression for data hiding.

Thereafter, the objectives of the study were set that the embedding process of using sequential least significant bit was meant to be replaced by innovative approach of using fractals to hide information. Implementation of this approach was made in three different algorithms i.e. Steganography of Text and Images using Mandelbrot Fractal, Steganography of Text and Images using Hilbert Curve and Steganography of text and Images using RGB channel of an image. In these algorithms we use Mandelbrot and Hilbert Curve fractal for the purpose of steganography.

We experiment the algorithm on the basis of comparisons of images and histograms. For Steganography of Text and Images using Mandelbrot fractal we analyzed the mean and standard deviation of images between cover image, embedded image and cover image (post extraction) to find the variance between them. After analysis of twenty five different images to check the intensity of pixels for both grey scale and in RGB. We found
that, the mean difference between original image and embedded image is 0.0023, mean difference between embedded and cover image (post extraction) is 0.0013 and mean difference between original image and cover image (post extraction) is 0.001. Further standard deviation difference between original image and embedded image is 0.0084, standard deviation difference between embedded and cover image (post extraction) is 0.001 and standard deviation difference between original image and cover image (post extraction) is 0.0094.

For RGB, we found that, the mean difference between original image and embedded image is 0.02, mean difference between embedded and cover image (post extraction) is 1.25 and mean difference between original image and cover image (post extraction) is 1.27. Further standard deviation difference between original image and embedded image is 2.31, standard deviation difference between embedded and cover image (post extraction) is 0.56 and standard deviation difference between original image and cover image (post extraction) is 2.88.

For Steganography of Text and Images using Hilbert Curve we analyze the mean and standard deviation of image in grey scale we found that, the mean difference between original image and embedded image is 0.0166, mean difference between embedded and cover image (post extraction) is 0.0085 and mean difference between original image and cover image (post extraction) is 0.0081. Further standard deviation difference between original image and embedded image is 0.0063, standard deviation difference between embedded and cover image (post extraction) is 0.0089 and standard deviation difference between original image and cover image (post extraction) is 0.0152.

For RGB, we found that, the mean difference between original image and embedded image is 0.2964, mean difference between embedded and cover image (post extraction) is 0.7988 and mean difference between original image and cover image (post extraction) is 1.0952. Further, standard deviation difference between original image and embedded image is...
image is 0.468, standard deviation difference between embedded and cover image (post extraction) is 0.5732 and standard deviation difference between original image and cover image (post extraction) is 1.0412.

For Steganography of Text and Images using RGB channel of an image we analyzed the mean and standard deviation of image in grey scale and we found that, the mean difference between original image and embedded image is 0.0024, mean difference between embedded and cover image (post extraction) is 0.0106 and mean difference between original image and cover image (post extraction) is 0.0082.Further, standard deviation difference between original image and embedded image is 0.002, standard deviation difference between embedded and cover image (post extraction) is 0.0072 and standard deviation difference between original image and cover image (post extraction) is 0.0101.

For RGB, we found that, the mean difference between original image and embedded image is 0.56, mean difference between embedded and cover image (post extraction) is 2.36 and mean difference between original image and cover image (post extraction) is 1.79.Further standard deviation difference between original image and embedded image is 1.14, standard deviation difference between embedded and cover image (post extraction) is 2.74 and standard deviation difference between original image and cover image (post extraction) is 3.89.

Furthermore, we compare mean and standard deviation of same images for two different algorithms i.e Steganography of Text and Images using Mandelbrot Fractal and Steganography of Text and Images using RGB channel of an image because in both algorithms Mandelbrot fractal is used but while using it with RGB channel, the image is split in three channels and merged again.
In Steganography of Text and Images using Mandelbrot fractal, for grey scale we found that, the mean difference between original image and embedded images is 0.01, mean difference between embedded and cover image (post extraction) is 0.013 and mean difference between original image and cover image (post extraction) is 0.01. Further, standard deviation difference between original image and embedded image is 0.004, standard deviation difference between embedded and cover image (post extraction) is 0.010 and standard deviation difference between original image and cover image (post extraction) is 0.0065.

For RGB, we found that, the mean difference between original image and embedded images is 1.99, mean difference between embedded and cover image (post extraction) is 1.79 and mean difference between original image and cover image (post extraction) is 0.2. Further, standard deviation difference between original image and embedded image is 4.63, standard deviation difference between embedded and cover image (post extraction) is 4.36 and standard deviation difference between original image and cover image (post extraction) is 0.28.

In Steganography of Text and Images using RGB channel of an image for grey scale we found that, the mean difference between original image and embedded images is 0.0167, mean difference between embedded and cover image (post extraction) is 0.0332 and mean difference between original image and cover image (post extraction) is 0.0499. Further, standard deviation difference between original image and embedded image is 0.0176, standard deviation difference between embedded and cover image (post extraction) is 0.0381 and standard deviation difference between original image and cover image (post extraction) is 0.0557.

For RGB, we found that the mean difference between original image and embedded images is 0.39, mean difference between embedded and cover image (post extraction) is
0.64 and mean difference between original image and cover image (post extraction) is 0.25. Further, standard deviation difference between original image and embedded image is 0.48, standard deviation difference between embedded and cover image (post extraction) is 1.9, and standard deviation difference between original image and cover image (post extraction) is 1.42.

It was found that in the Steganography of Text and Images using RGB channel of image algorithm, nominal difference is noticed in original (cover) image and cover image (post extraction) because of the image being split in three channels and merge again.

Further, it was concluded that the image containing stegogramme is not recognized by the naked eye detection there is not much difference between cover, embedded and cover (post-extraction) image. In the analysis we find mean and standard deviation and concluded that there is not much difference between cover, embedded and cover (post extraction) images. That means the embedded, cover (post extraction) and cover image remains almost as it is.

5.2 The Path Ahead

The research provides an opportunity to go ahead in the field of Information Hiding. The research can be extended by using other fractals for the purpose of steganography.

The limitation of our technique is that the size of image to hide should be equal to the size of the fractal used. It may be attempted to overcome.

Moreover, the research may be extended by using different carriers (covers) like audio and video. One of the methods for audio steganography is to substitute the least significant bit of each sample of the cover speech signal with the secret data. While this method is easy to implement and can be used to hide larger secret messages, it cannot
protect the hidden message from small modifications that can happen as a result of format conversion or compression, so further advancement is needed. Moreover, in the video steganography generally video is separated into audio and images. Therefore any of them is selected as cover/carrier and data are embedded within them using LSB or any other technique.

The research can be furthered by using cryptography with steganography to enhance the security because by using cryptography, we can convert our plain text message to cipher text by using the secret key and embed the cipher text into any cover medium using steganographic techniques.