ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 2, April 2013

Comparative study of Steganography on Gray, Indexed, Colour and Black & White images by Equal / Near Equal Value Pixel Replacement Point Operations

H. Faheem Ahmed[1], Dr.U. Rizwan[2]

[1]Department of Computer Science, Islamiah College, Vaniyambadi, India

[2]Department of Mathematics, Islamiah College, Vaniyambadi, India

ABSTRACT: In this paper, we consider four types of images namely gray scale, indexed, colour and black & white images and apply steganogrphic techniques by embedding text of 512 bytes in each of these images. Three simple pixel replacement techniques like equal or nearly equal pixel replacement in each column, equal or nearly equal in pixel replacement in entire image, random pixel replacement and natural number increment pixel replacement methods are adopted. The actual, stego and the extracted images are shown explicitly. The Mean Square Error (MSE) and Peak to Signal Noise Ratio (PSNR) indices have been computed in each case. The histograms for the computed values of MSE and PSNR indices are drawn. At the end, we have given an introduction to steganography in an audio file.

Keywords: Pixel Replacement, Gray scale, indexed, RGB, Stego image, MSE, PSNR

I. INTRODUCTION

Steganography is the art of hiding information imperceptibly in a cover medium. The word *Steganography* is of Greek origin and means *covered* or *hidden writing*. The main aim in steganography is to hide the very existence of the message in the cover medium. Steganography and Cryptography are counter parts in digital security. The obvious advantage of steganography over cryptography is that messages do not attract attention to themselves, to messengers, or to recipients. During the last decade, an exponential growth in the use of multimedia data over the Internet is seen. These include Digital Images, Audio and Video files. This rise of digital content on the internet has further accelerated the research effort devoted to steganography. The various applications of steganography include secure military communications, multimedia watermarking and fingerprinting applications for authentication purposed to curb the problem of digital piracy. Although these are not perfect applications of steganography, many steganographic algorithms can be employed for these purposes as well.

Faheem Ahmed and Rizwan [2] have introduced a new concept in data embedding. The authors have embedded text message and digital image in audio files. They have also presented a technique for embedding text message and/or digital image in another image. A lot of examples have been presented. Fridrich etal. [3] have studied quantitative stegnanalysis of digital images. They have estimated the length of the secret message. Rizwan and Faheem Ahmed [5] have made a comprehensive study on various types of steganographic schemes. Faheem Ahmed and Rizwan [6] have introduced and studied seven different steganographic techniques applying randomization concept. They have also computed the MSE and PSNR indices for these techniques. Structural similarity indices have also been determined..

II. TYPES OF DIGITAL IMAGES

There are four basic types of images.

Binary Image : Each pixel is either black or white. Since there are only two possible values for each pixel, we only need one bit per pixel. Such images can therefore be very efficient in terms of storage. Images for which a binary representation may be suitable include text (printed or handwriting), fingerprints, or architectural plans. Figure 1 shows a black & white image and the contents of a section.

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 2, April 2013

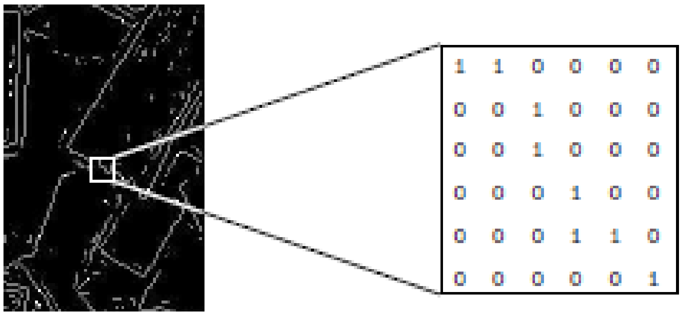


Fig. 1 Black & White (Logical) Image

Grayscale Image : Each pixel is a shade of gray, normally from 0 (black) to 255(white). This range means that each pixel can be represented by eight bits, or exactly one byte. This is a very natural range for image file handling. Other grayscale ranges are used, but generally they are a power of 2. Such images arise in medicine (X-rays), images of printed works, and indeed 256 gray levels is sufficient for the recognition of most natural objects. Figure 2 shows a gray level image and the contents of a section.

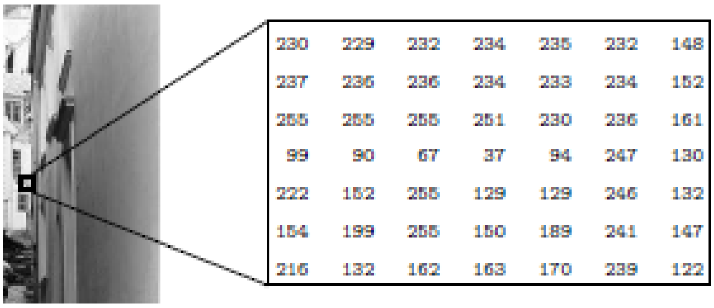


Fig. 2 Gray scale Image

Indexed Image : Most colour images only have a small subset of the more than sixteen million possible colours. For convenience of storage and file handling, the image has an associated colour map or colour palette, which is simply a list of all the colours used in that image. Each pixel has a value which does not give its colour (as for an RGB image), but an index to the colour in the map. It is convenient if an image has 256 colours or less, for then the index values will only require one byte each to store. Some image file formats (for example, Compuserve GIF), allow only 256 colours or fewer in each image, for precisely this reason. An indexed image and its contents are given in figure 3.

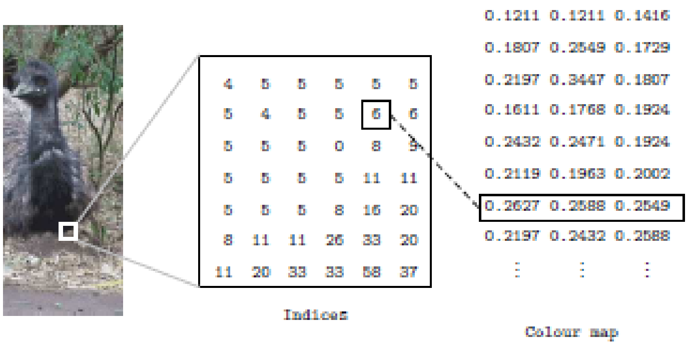


Fig. 3 An Indexed Image

True colour or RGB Image : Here each pixel has a particular colour; that colour being described by the amount of red, green and blue in it. If each of these components has a range 0 - 255, this gives a total of 255^3 = 16, 777, 216 different possible colours in the image. This is enough colours for any image. Since the total number of bits required for each pixel is 24, such images are also called 24-bit colour images. Such an image may be considered as consisting

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 2, April 2013

of a *stack* of three matrices; representing the red, green and blue values for each pixel. This means that for every pixel there correspond three values. Figure 4 shows a colour image and part of its contents.

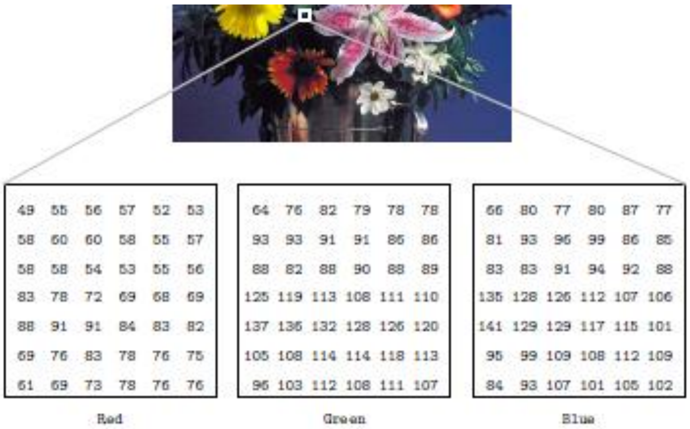


Fig. 4 True Color / RGB Image

III. . EMBEDDING TEXT IN AN IMAGE USING NATURAL NUMBER INCREMENTS

In this technique, we consider the usual natural sequence of numbers 1,2,3,4,5,6,…. and generate a sequence 1, 3, 6, 10, 15, 21, 28, 26, 45, 55, . . . by adding 2, 3, 4, 5, 6, 7, 8, . . . to each generated nuber. Then, hide each character of secret message in the above pixel locations. The resulting original image and the stego image after hiding 512 bytes of secret text are shown in figures 5, 6, 7 and 8.

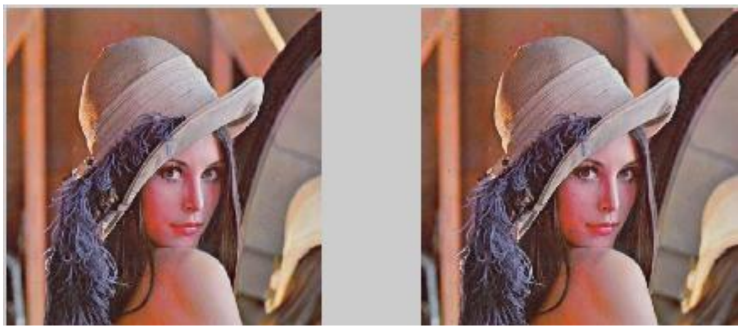


Fig. 5 `lena.jpg` 512x512 color image and stego image

Fig. 6. `lena.tif` 512x512 grayscale and stego image

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 2, April 2013

Fig. 7. `lena.gif` 512x512 indexed image and stego image

Fig. 8. `lena.png` 512x512 Black & White image and stego image

IV. EQUAL / NEAREST VALUE PIXEL REPLACEMENT POINT OPERATIONS IN EACH COLUMN

In this method, we find gray level that is equal or closest to each text value in each column, and replace that gray level with the text value.

For Example let the cover image be

10	8	6	4	1
2	5	8	9	4
6	0	9	9	8
5	8	7	4	0
9	4	2	9	1

and let the text to be embedded is

4 9 3 6 2

The above text is then embedded in the cover image as follows: The first text is 4 which is near equal to 5 in first column of image, the second text 9 is near equal to 8 in second column, the third text 3 is near equal to 2 in third column, and so on. So the cover image becomes

10	9	6	6	2
2	5	8	9	4
6	0	9	9	8
4	8	7	4	0
9	4	3	9	1

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 2, April 2013

The above technique is applied on `lena.tif` 512x512 grayscale image, `lena.gif` 512x512 indexed image and `lena.jpg` 512x512 color image and the orginal, stego image embedded with 512 bytes of text are shown in the figures 9, 10 and 11.

Fig. 9 `lena.tif` 512x512 grayscale and stego image

Fig. 10 `lena.gif` 512x512 indexed image and stego image

Fig. 11 `lena.jpg` 512x512 color image and stego image

V. EQUAL / NEAREST VALUE PIXEL REPLACEMENT POINT OPERATIONS IN ENTIRE IMAGE

Let cover be the image and message be the text to be embedded. The embedding is done as follows. The first character of message 72 is embedded at the nearest gray level 58 which is near equal in the entire image, the second character 101 is embedded at 103 which is near equal in the entire image and so on as shown in the following example.

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 2, April 2013

cover =

242	194	156	103	14
58	116	201	238	89
154	4	235	233	207
123	209	188	104	2
227	113	44	227	35

message = 72 101 108 108 111

The image with embedded text is

242	194	156	101	14
72	111	201	238	89
154	4	235	233	207
123	209	188	108	2
227	108	44	227	35

The above technique is applied on `lena.tif` 512x512 grayscale image, lena.gif 512x512 indexed image and `lena.jpg` 512 x 512 color image and the orginal, stego image embedded with 512 bytes of text are shown in the figures 12, 13 and 14.

Fig. 12. `lena.tif` 512x512 grayscale and stego image

Fig. 13 `lena.gif` 512x512 indexed image and stego image

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 2, April 2013

Fig. 14 `lena.jpg` 512x512 color image and stego image

VI. . EMBEDDING TEXT AT RANDOM LOCATIONS IN IMAGE

The embedding is done as follows. First 512 (number of text characters to be embedded) random numbers are generated. The first character of message 72 is embedded at the first random number 4th location in image, the second character of message 101 is embedded at the second random number 1st location in image, the third character of message 108 is embedded at the third random number 3rd location in image and so on as shown in the following example.

cover =

129	84	90	159	72
24	154	97	175	169
145	163	116	38	191
157	44	78	234	27
180	94	181	161	87

message = 'Hello'= [72 101 108 108 111]

random numbers generated = 4 1 3 2 2

Inserting the above text values at the memory locations of random numbers, we obtain

cover1 =

129	84	90	72	72
101	154	97	175	169
145	163	108	38	191
157	108	78	234	27
180	111	181	161	87

The above technique is applied on lena.tif 512x512 grayscale image, lena.gif 512x512 indexed image and lena.jpg 512x512 color image and the orginal, stego image embedded with 512 bytes of text are shown in the figures 15, 16 and 17.

Fig. 15 `lena.tif` 512x512 grayscale and stego image

ISSN (Print) : 2320 – 9798
ISSN (Online): 2320 – 9801

International Journal of Innovative Research in Computer and Communication Engineering
Vol. 1, Issue 2, April 2013

Fig.16 `lena.gif` 512x512 indexed image and stego image

Fig. 17 `lena.jpg` 512x512 color image and stego image

VII. PERFORMANCE ANALYSIS

The Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) are performance parameters to measure the quality of image.

- MSE: It is defined as square of error between cover stego-image. The error indicates the distortion in an image.MSE can be calculated by using two dimensional mathematical equation described as follows:

$$MSE = \left(\frac{1}{N}\right)^2 \sum_{i=1}^{M}\sum_{j=1}^{N}(X_{ij} - \bar{X}_{ij})^2$$

  where Xij = the value of pixel in cover image and $\bar{X}_{ij}$ =the value of pixel in stego-image and N is the size of image.
- PSNR: It is a measure of quality of image. PSNR can be calculated by using the mathematical formula given below:

$$PSNR = 10 \,\mathrm{x} \log \frac{255^2}{MSE} \mathrm{db}$$

The computed values of the PSNR and MSE indices, by considering the three different types of images and using four distinct methods introduced in this article are presented in table 1.

Table 1. The computed values of PSNR and MSE

S.No.	Pixel Replacement	Computed Values	Gray Scale Image	Indexed Image	Color Image
1	Natural numbers incremental values in image	PSNR	55.91397	53.55732	57.65658
		MSE	0.16660	0.28665	0.11154
2.	Equal/Nearest Value Pixel Replacement in each column	PSNR	57.97339	54.04704	59.16483
		MSE	0.10369	0.25608	0.07881
3.	Equal/Nearest Value Pixel Replacement in entire image	PSNR	53.83246	51.96843	57.71575
		MSE	0.26905	0.41327	0.11003
4.	Embedding text at random locations in image	PSNR	57.19043	53.73950	57.80407
		MSE	0.12418	0.27487	0.10781

The histograms of the computed values of PSNR and MSE indices for each of the above techniques for all three types of images are presented in figures 18 and 19.

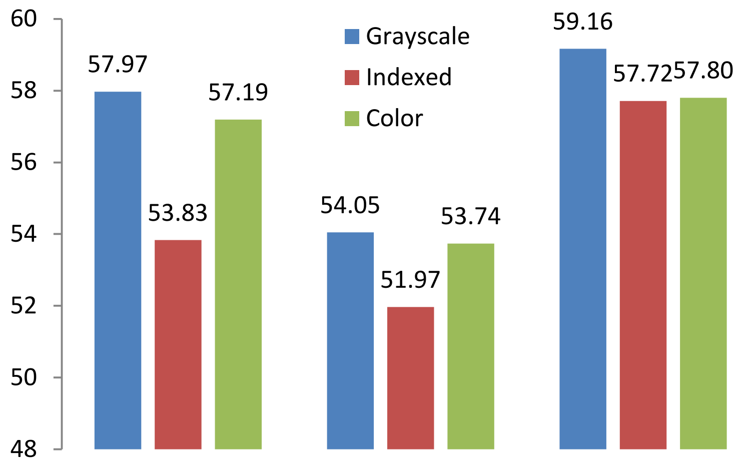


Fig. 18: Histogram of PSNR Values

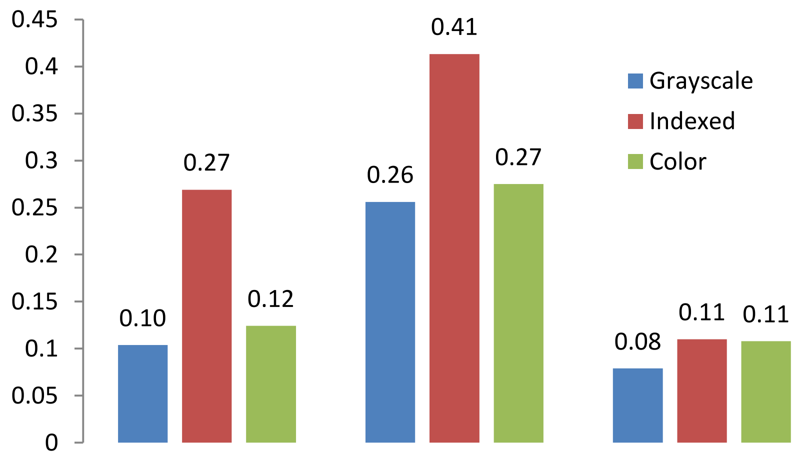


Fig. 19: Histogram of MSE Values

VIII. HIDING A SECRET MESSAGE IN AN AUDIO FILE

To do this, we require two software (i) coagula and (ii) Sonic visualizer.

In MS Paint, create a secret text message and save it as bmp file, say `mytext.bmp` as shown below.

Fig. 20. Secret text message saved as `.bmp` format

Next open the mytext.bmp file in coagula and render the image without blue/noise. Then select File/Save sound as and give a file name say `mysound.wav`. Lastly, open this mysound.wav file in sonic visualizer which looks like an ordinary sound file as shown in figure 21.

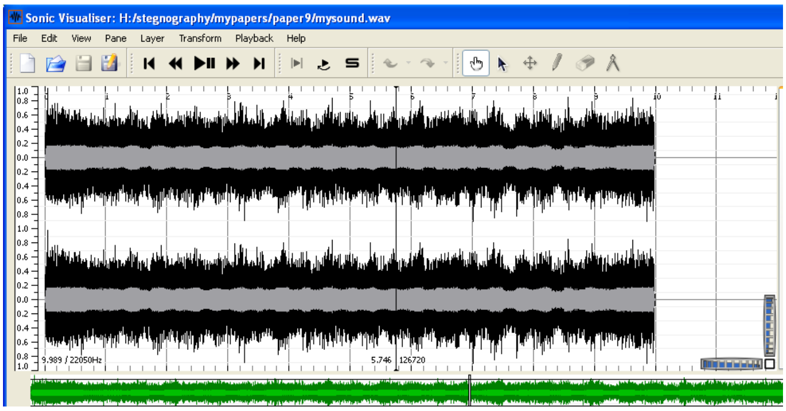


Fig. 21. Sonic visualizer `mysound.wav` file

Select Layer Menu/ Add spectrogram / All Channels mixed to reveal the secret message inside the audio file as shown.

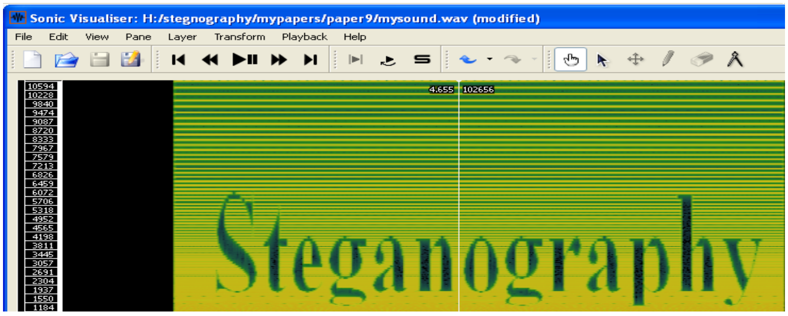


Fig. 22. Hidden secret text inside `mysound.wav`

IX. CONCLUSION

Steganographic techniques have been used with success for centuries already. However, since secret information usually has a value to the ones who are not allowed to know it, there will be people or organizations who will try to decode encrypted information or find information that is hidden in them. Governments want to know what civilians or other governments are doing, Companies want to be sure that trade secrets will not be sold to competitors and most persons are naturally curious. Many different motives exist to detect the use of steganography, so techniques to do so continue to be developed while the hiding algorithms become more advanced. Secrets can be hidden inside all, hide information inside images, as this is relatively easy to implement. However, there are tools available to store secrets inside almost any type of cover source.

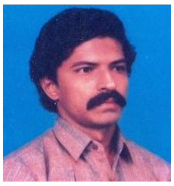
Many different carrier file formats can be used, but digital images are the most popular because of their frequency on the Internet. For hiding secret information in images, there exist a large variety of steganographic techniques; some are more complex than others and all of them have their own merits and demerits. Distinct applications have different requirements of the steganographic technique used. For example, some applications may require absolute invisibility of the secret information, while others require a larger quantity of secret message to be hidden. After giving an overview of image steganography, its uses and techniques are presented in this article. Some new techniques of embedding a text message in various types of digital images are introduced.

This paper has given a brief comparison on applying steganography on various types of images like black & white, gray level, indexed and RGB. Instead of hiding text in least significant bits, steganography is applied on direct pixel values itself and the actual and stego images in each type are given for comparison. Further, hiding of text in an audio file is also discussed.

REFERENCES

[1] Cachin. C., An information-theoretic model for steganography, *Information and Computation*, Ed. Academic, USA, Vol. **192** (1), pp. 41 – 56, 2004.
[2] Faheem Ahmed, H and Rizwan. U, *An Alternative Technique in Data Embedding*, Advanced Materials in Physics, pp 233 – 242, 2012.
[3] Fridrich, J and M. Goljan and D. Hogea and D. Soukal, Quantitative steganalysis of digital images: estimating the secret message length, *Multimedia Systems Journal* - Special issue on Multimedia Security, Vol. **9 (**3), pp. 288 – 302, 2003.
[4] Rafael Gonzalez and Richard E. Woods, *Digital Image Processing*, Addison-Wesley, second edition, 2002.
[5] Rizwan. U and Faheem Ahmed. H, Comprehensive study on various types of steganographic schemes and possible steganalysis methods for various cover carrier like image, text, audio and video, *International Journal of Scientific and Engineering Research*, Vol **3** (11)**,** pp 151 – 154, 2012.
[6] Rizwan. U and Faheem Ahmed. H, A New Approach in Steganography using different Algorithms and Applying Randomization Concept, *International Journal of Advanced Research in Computer and Communication Engineering*, Vol.**1** (9), pp 233 – 242, 2012.

BIOGRAPHY



H. Faheem Ahmed earned his M.Tech. degree in Information Technology from Punjabi University and M.Phil. degree in Computer Science from Manonmaniam Sundaranar University. He is pursuing Ph.D. in Computer Science. He has guided 50 M.Phil. research scholars in Computer Science. He is currently the Head of the Department of Computer Science and Applications, Islamiah College, Vaniyambadi and is serving the institution for the past 28 years. His research interest includes Steganography and Image processing. He has published 8 research articles and authored one book.

U. Rizwan earned his Ph.D. degree in Mathematics from the University of Madras. He is currently the Head of the Department of Mathematics, Islamiah College, Vaniyambadi and is serving the Institution for the past 26 years. He has published 43 research articles in journals of international repute. He has authored 7 books and is also the editor of two international journals. He has guided 30 M.Phil. Mathematics research scholars and one M. Tech. (IT) candidate. He is guiding Ph. D. research scholars in Mathematics and Computer Science. His research interest includes Image Processing, Hacking algorithms, Stochastic Processes, Fuzzy Logic, etc. He is the member of the board of studies in PG Mathematics of Thiruvalluvar University, Vellore. He is also an academic auditor.