ISSN: 0975-8585

Research Journal of Pharmaceutical, Biological and Chemical Sciences

Secured Data Transmission Through Image on Optical Steganography Based on Noise.

M Anto Bennet*, S Mekala, MS Sugapriya, K Vijayabharathi, J Jenitta, and J Dhanalakshmi.

Department of ECE, VEL TECH, Avadi, Chennai 600 062, Tamil Nadu, India.

ABSTRACT

The enhancement of security system for secret data communication through secured data hiding in images on optical communication has been demonstrated experimentally and studied theoretically. The tolerance to the dispersion of Optical steganography has been studied. In recent years, the rapid growth of optical communication has become very important to secure information transmission between the sender and receiver. Therefore steganography is introduced, which is used to hide information and to communicate a secret data in an histogram enhanced image through an optical channel. The dispersion effect is deployed in order to improve the security of the stealth data. In this work, an algorithm for optical steganography has been proposed called LSB replacement algorithm to conceal a large amount of secret data presented by secret image into the pixels of gray scale image. The dispersion effect due to the larger length of the optical channel used is reduced by increasing the PSNR. The extra dispersion at the transmitter and the receiver functions as a key pair for the optical communication. Finally the enhanced performance of this proposal in image through an optical channel will be based on the parameters such as Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR).

Keywords: Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR).

**Corresponding author*

INTRODUCTION

Optical steganography aims to transmit stealth data in public fibre optic communication system without being detected. Amplified spontaneous emission (ase) noise is generated in optical fibre. Optical Steganography is the practice of concealing message or information within other non-secret text or data. Steganography is the art and science of writing hidden messages in such a way that no one, apart from the sender and intended recipient, suspects the existence of the message, a form of security through obscurity. The word steganography is of Greek origin and means "concealed writing" from the Greek word Stegano's (meaning "covered or protected", and graphy meaning "writing". The first recorded use of the term was in 1499 by Johannes Trithemius in his Steganographia, a treatise on cryptography and steganography disguised as a book on magic. Generally, messages will appear to be something else: images, articles, shopping lists, or some other cover text and, classically, the hidden message may be in invisible link between the visible lines of a private letter[1,2]. The advantage of steganography over cryptography alone is that messages do not attract attention to themselves. Plainly visible encrypted messages no matter how unbreakable will arouse suspicion, and may in themselves be incriminating in countries where encryption is illegal. Therefore, whereas cryptography protects the contents of a message, steganography can be said to protect both messages and communicating parties.

Steganography includes the concealment of information within computer files[3,4]. In digital steganography, electronic communications may include steganographic coding inside of a transport layer, such as a document file, image file, program or protocol. Media files are ideal for steganographic transmission because of their large size. As a simple example, a sender might start with an innocuous image file and adjust the color of every 100th pixel to correspond to a letter in the alphabet, a change so subtle that someone not specifically looking for it is unlikely to notice it.Steganography is the art of communication that does not let a third party know that the communication channel exists. It has always been influenced by the way people communicate and with the explosion of social networking websites; it is likely that these will be used as channels to cover the very existence of communication between different entities. The art of covered writing or steganography has a long history and has always been influenced by the way people communicate. It is often understood as the prisoners' problem where two inmates Alice and Bob, imprisoned in two different cells are trying to formulate a plan for escape. The only way to communicate with each other is through a channel that is monitored by the Warden. Alice and Bob should then find a way for communicating under monitoring without raising the Warden`s suspicion. The expansion of the virtual world has created a wide range of possibilities in the world of secret communication.

Although, cryptography is enough to keep the content of a given information unreadable from praying eyes. If the Warden (also referred as person in the middle) who monitors the communication is not favorable to encrypted data, and whenever he knows that something encrypted and suspicious is within the channel, he might decide to stop and interrupt the communication[5,6,7]..

PROPOSED SYSTEM

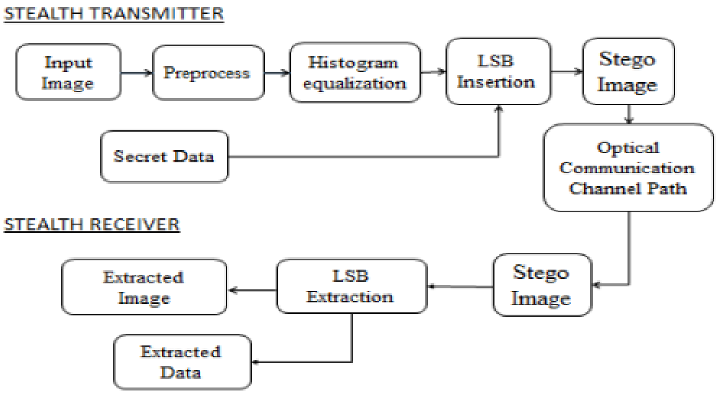


Fig 1: Block Diagram Of Stealth Transmitter and Receiver

The main challenge in steganographic technique is to maintain the approximate pixel values same as the original cover image and to reduce PSNR by increasing the Mean square error (MSE).In this work, the input image is enhanced using histogram. equalization and the data is concieved and retrieved using LSB techniqueis shown in fig 1.

INPUT IMAGE

Consider a 8-bit image consisting m × n pixels which in the form of RGB.The data to be transmitted securely is hidden into this image after the preprocessing stage.

PREPROCESSING

The RGB input image is converted into a gray scale image.Gray scale images are rendered in black, white, and all the shades of gray in between.The RGB encoding of any gray values is a set of three equal numbers, i.e., (x, x, x), where x is some integer between 0 and 255.For instance, white is (255,255,255), black is (0,0,0) and medium gray is (127,127,127).The higher the numbers, the lighter the gray.

x=0.299r+0.587g+0.114b--(1)

Adaptive LSB Embedding

A 8-bit gray scale image matrix consisting m × n pixels and a secret message consisting of k bits. The first bit of message is embedded into the LSB of the first pixel and the second bit of message is embedded into the second pixel and so on. The resultant Stego-image which holds the secret message is also a 8-bit gray scale image and difference between the cover image and the Stego-image is not visually perceptible. The quality of the image, however degrades with the increase in number of LSBs. This hiding process will introduce the error between input and output image and it is determined by mean square error and Peak signal to noise ratio determines the image quality.

Information to be hidden + cover image= STEGO image-------------------(2)

Optical Communication Channel Path

We consider the communication channel given by a fiber optical transmission line. We develop a method to perturbatively calculate the information capacity of a nonlinear channel, given the corresponding evolution equation. Using this technique, we compute the decrease of the channel capacity to the leading order in the perturbative parameter for fiber optics communication systems.

$$\sigma^2 = \frac{N_0}{2}\int_{-\infty}^{+\infty} |H_{RX}(f)|^2 \, \mathrm{d}f \qquad \text{--(3)}$$

Adaptive LSBs Extraction

A 8-bit gray scale image matrix consisting m × n pixels and a secret message consisting of k bits. The first bit of message is extracted from the LSB of the first high frequency coefficients and the second some bits of message is extracted from the second reserves coefficients and so on. This process is repeated upto all secret message bits are retrieved and these bits are grouped into 8bits to form a character values. The extraction of desired payload number of bits will be performed by using logical bitwise operators called ‘bitand’ and ‘bitor’. Finally all extracted message characters are applied to RSA decryption module to decrypt the data with private keys.

QUALITY MEASURES

The Quality of the reconstructed image is measured interms of mean square error (MSE) and peak signal to noise ratio (PSNR) ratio. The MSE is often called reconstruction error variance σ_q^2. The MSE between the original image f and the reconstructed image g at decoder is defined as:

$$\text{MSE} = \sigma_q^2 = \frac{1}{N}\sum_{j,k}(f[j,k]-g[j,k])^2 \text{--(4)}$$

Where the sum over j, k denotes the sum over all pixels in the image and N is the number of pixels in each image. From that the peak signal-to-noise ratio is defined as the ratio between signal variance and reconstruction error variance. The PSNR between two images having 8 bits per pixel in terms of decibels (dBs) is given by:

$$\text{PSNR} = 10\log_{10}\left(\frac{255^2}{MSE}\right) \text{---(5)}$$

Generally when PSNR is 40 dB or greater, then the original and the reconstructed images are virtually indistinguishable by human eyes.

EXPERIMENTAL RESULTS

STEPS INVOLVED

The following steps are involved in the data transmission through image in optical steganography:

Step 1: Image Acquisition: The first step in the data transmission process is the acquisition of image. Images are collected from the online shown in fig 2.

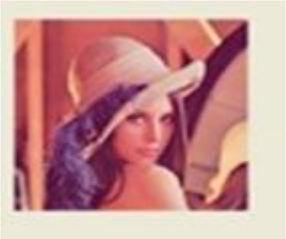


Fig 2: Example of input image

Step 2: RGB to gray scale Conversion

The next step is the conversion of the input image in RGB color space to gray scale image. Fig 3 (a,b) shows the images of a and b components obtained.

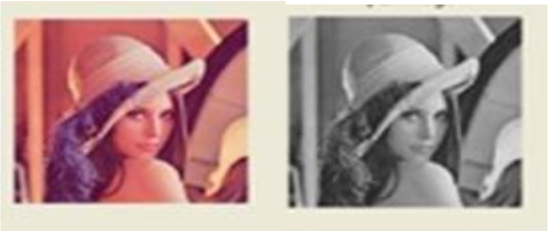


Fig 3: (a) Input ImageFig 3(b) Gray Scale Image

The input image is converted into the gray scale by conversion algorithm in preprocessing shown in fig 4.

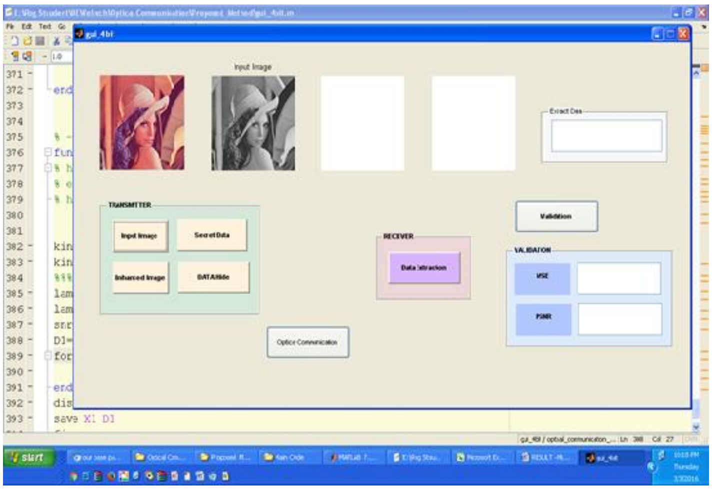


Fig 4: RGB to gray scale conversion

Step 3: Data embedding and histogram equalization

The gray scale image is converted in to high contrast image using histogram equalisation.Then the data is embedded in high contrast image through LSB algorithm. Fig 5(a,b) shows the images of a and b components obtained.

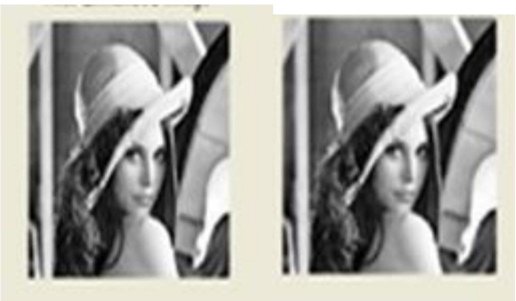


Fig 5(a): Histogram Enhanced fig 5(b): Scret Data Hidden Image

The histogram equalization is applied to the gray scale image which enhance the quality of the image to high contrastshown in fig6.

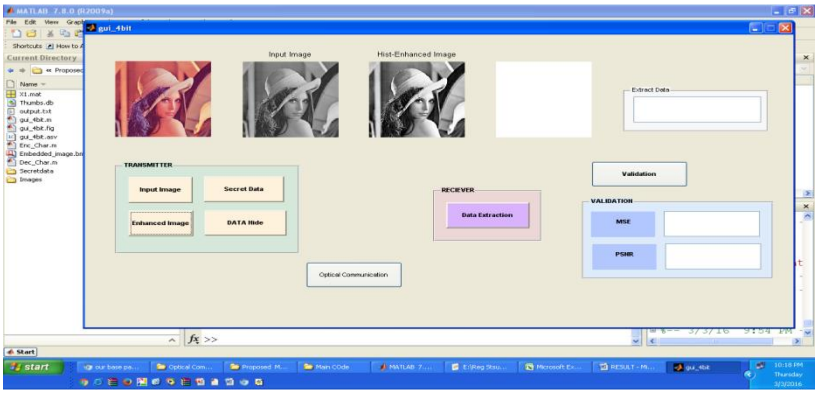
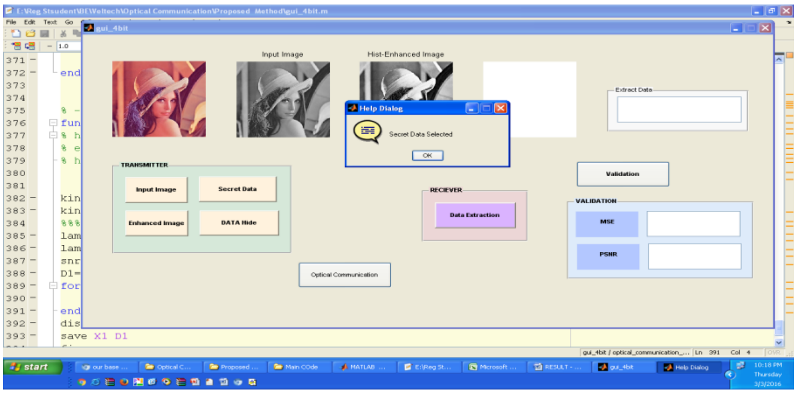


Fig 6: Conversion Of Gray Scale Image to Enhanced High Contrast Image



Secret Data Selected

Fig 7: Data Hiding In Enhanced image Through LSB insertion algorithm

The data is hidden in high enchanced image using LSB insertion algorithm to ensure secure transmission shown in fig7&8.

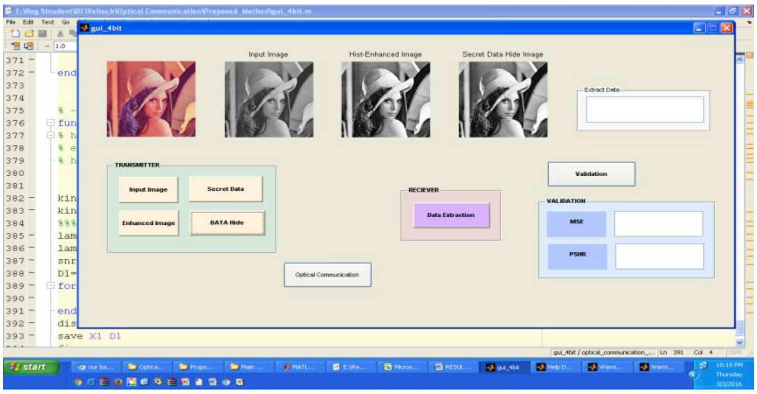


Fig 8: Data Hidden in a Enhanced Image

Step 4: optical channel path

The tolerance to dispersion to the data rate is described in the optical communication channel path.

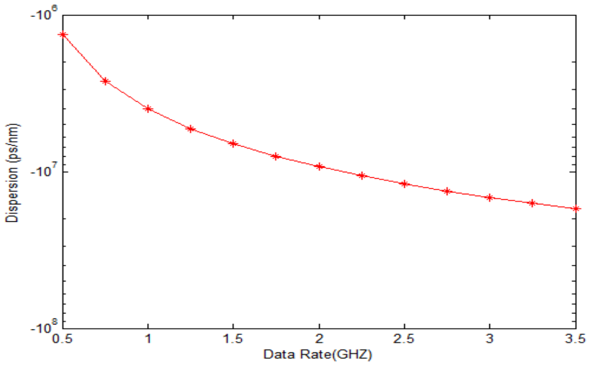


Fig 9: Dependence of Dispersion limit on the Data Rate - proposed method

The data transmission in optical communication path is described in the following figures 9 &10..

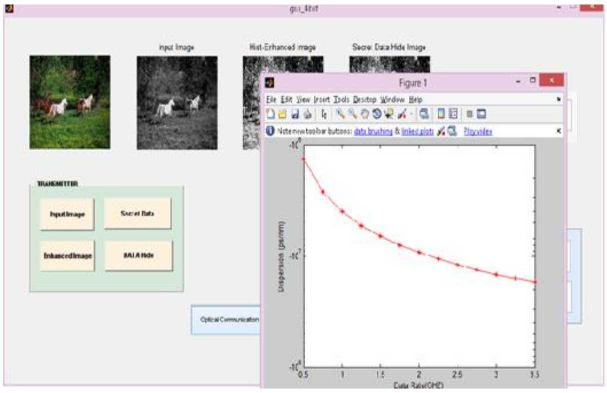


Fig 10: Data Transmission through the Optical Communication Channel Path

Step 5: Data extraction: The hidden data is extracted from the image using the LSB extraction algorithmshown in fig 11.

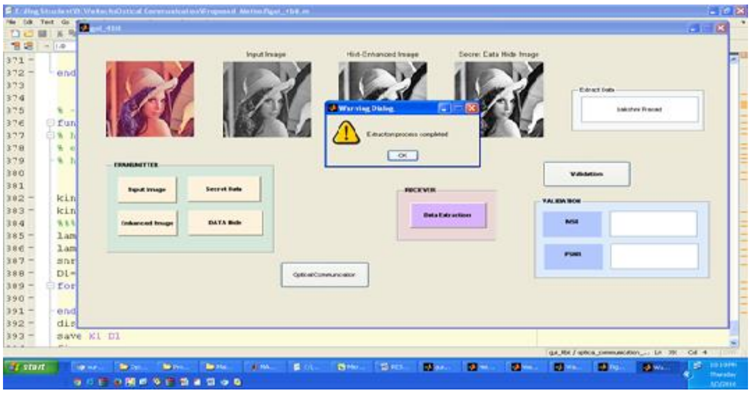
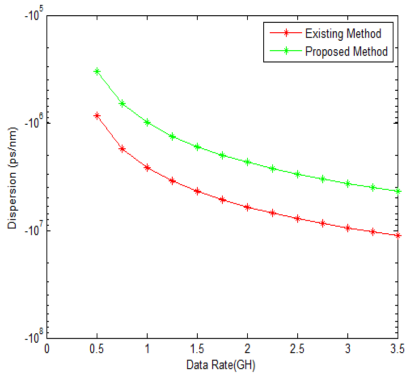


Fig 11: Data Extraction using LSB Algorithm

EXPERIMENTAL ANALYSIS

Comparision of dispersion vs data rate

Comparison between existing and proposed method analysis on stego image communicating through optical path shown in fig 12.



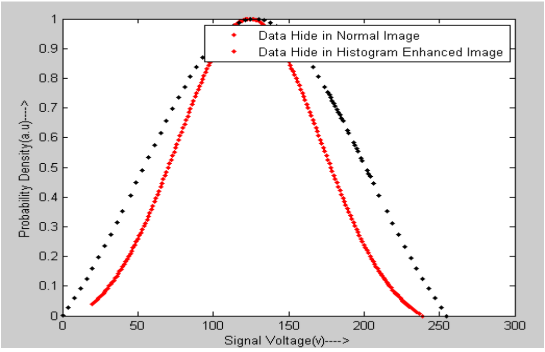


Fig 12: Dependence of Dispersion limit on the Data Rate Probability Density

Fig 13: Performance Measure

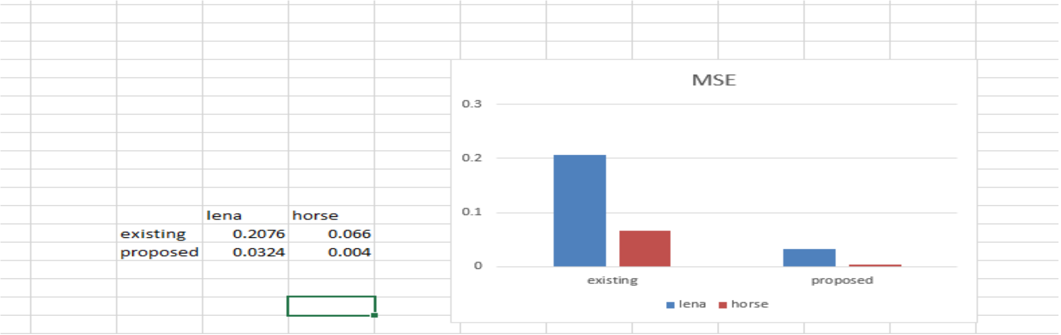
The performance of the data transmission through optical steganography(Fig 13) was analyzed using the following measures:

- Mean Square Error(MSE)
- Peak Signal to Noise Ratio(PSNR)

Table 1.a shows **the performance measures of the data transmission** in **optical steganography** with **the impact of MSE**and the corresponding wavefom is shown below in fig 14.

Table 1: Performance analysis based on MSE

	LENA	HORSE
EXISTING METHOD	0.207672	0.0660706
PROPOSED METHOD	0.0324	0.00403



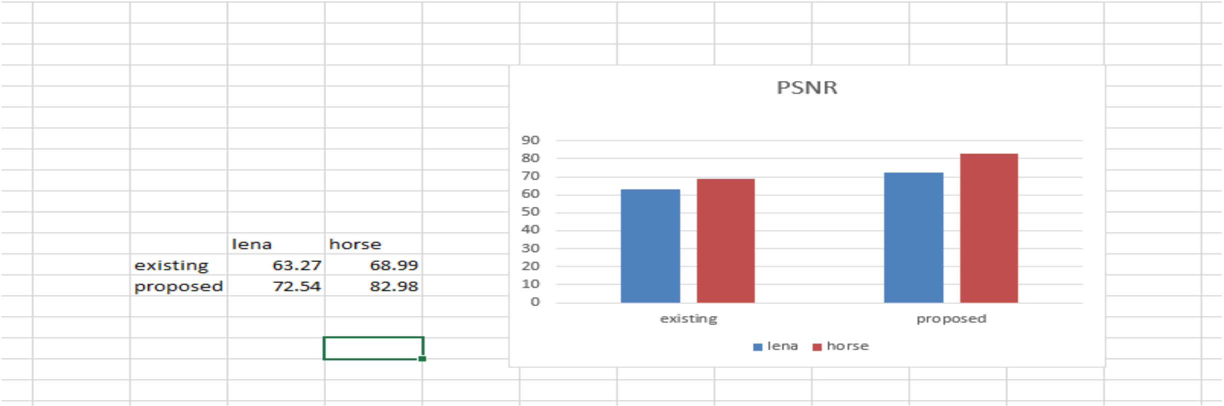
	lena	horse
existing	0.2076	0.066
proposed	0.0324	0.004

Fig 14: Performance analysis based on MSE

Table 2 shows the **performance measures of the datatransmission** in **optical steganography** with the **impact of PSNR**and the corresponding wavefom is shown below in fig 15.

	LENA	HORSE
EXISTING METHOD	63.27	68.99
PROPOSED METHOD	72.54	82.98

Table 2: Impact of PSNR



	lena	horse
existing	63.27	68.99
proposed	72.54	82.98

Fig 15: Performance analysis based on PSNR

CONCLUSION

The work explains about the enhancement of secure data transmission through image based on optical steganography and the effect of dispersion on optical steganography based on ASE noise. Deployment of dispersion effect is used to improve the security of the channel. If the data rate is increased, the error rate will decrease and thus the Dispersion effect is compensated. The optical encryption ,which encrypts the stealth data as a noisy signaL, while optical steganography region hides the stealth data enhances secure transmission. **EASVESDROPPING** is completely prevented by this method.This work is implemented in hardware it can used in military and defense purpose for secure retrival of important messages.

REFERENCES

[1] Siti Dhalila mohd satar et al.,2015 "A new model for hiding text in an image using logical connective" International journal of multimedia and ubiquitous engineering vol.10 no.6 pp.195-202 .

[2] S.A.Khandekar et al.,2015 "Steganography for text messages using images"vol 4 pp125.

[3] Dr. AntoBennet, M, Srinath R,Raisha Banu A,"Development of Deblocking Architectures for block artifact reduction in videos", International Journal of Applied Engineering Research,Volume 10, Number 09 (2015) pp. 6985-6991, April 2015.

[4] AntoBennet, M & JacobRaglend, "Performance Analysis Of Filtering Schedule Using Deblocking Filter For The Reduction Of Block Artifacts From MPEQ Compressed Document Images", Journal of Computer Science, vol. 8, no. 9, pp. 1447-1454, 2012.

[5] AntoBennet, M & JacobRaglend, "Performance Analysis of Block Artifact Reduction Scheme Using Pseudo Random Noise Mask Filtering", European Journal of Scientific Research, vol. 66 no.1, pp.120-129, 2011.

[6] Anto Bennet, M, Mohan babu, G, Rajasekar, C & Prakash, P, "Performance and Analysis of Hybrid Algorithm for Blocking and Ringing Artifact Reduction", Journal of Computational and Theoretical nanoscience vol.12,no.1,pp.141-149,2015

[7] AntoBennet, M & JacobRaglend, "Performance and Analysis of Compression Artifacts Reduction for MPEQ-4 Moving Pictures Using TV Regularization Method", Life Science Journal vol. 10, no. 2, pp. 102-110, 2013