IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

ISO 3297:2007 Certified

Vol. 3, Issue 11, November 2016

Image Steganography with LSB Algorithm using Median Filter

Reenu Jaswal[1], Munish Katoch[2], Jasdeep Malhotra[3]

Student, Dept of CSE, Sri Sai University[1]

Assistant Professor, Dept of CSE, Sri Sai University[2]

Reader, Bhatinda[3]

Abstract: Today's the rise of the internet has become the most important factor of information technology and communication but beside this the threat of information security increases. It's become very important to give security to the data so that no illegal person can access it. The two main techniques are used, first is cryptography and second is steganography. Both are used for data security purpose. Cryptography changes the form of the data and steganography fully conceals its presence from the users, except the intended receiver. The steganography is a powerful security method with which we can hide a secret message inside an object. Steganography is a technique used to protect the data by just hiding the data into data or information behind information. Currently, many types of steganography techniques are being used such as text, image, audio/video and protocol but digital images are the most widely used. There are many steganography procedures in which everyone has its own strength and weakness in terms of security and complexity. Some of which provides hiddenness of information while some provides a huge secret message to be hidden. This dissertation provides an overview of steganography specially image steganography and its uses. It attempts to design and develop the good steganography algorithm and briefly describes about the Least Significant Bit image steganography algorithm and also provides an improved version of LSB. In this dissertation, two parameters are used in order to measure the quality of image. First is PSNR and second is MSE.

Keywords: Steganography, Visual Cryptography, Steganography Techniques, Stego Image, PSNR, MSE.

I. INTRODUCTION

Many times, users on the internet have to send, share or receive confidential information. Due to rapid development in both computer technologies and Internet, the security of information is regarded as one of the most important factors of Information Technology and communication. Steganography has emerged as a powerful and efficient tool which provides high level for security particularly when it is combined with encryption. Steganography, hides the existence of message such that intruder can't even guess that communication is going on and thus provides a higher level of security.An electronic copy can be downloaded from the Journal website. For questions on paper guidelines, please contact the journal publications committee as indicated on the journal website. Information about final paper submission is available from the conference website.

A. STEGANOGRAPHY

The term Steganography was first introduced by Johannes Trithemiu in 1499. Steganography is a combination of two words Stegano + Graptos. Stegano means "Covered" and Graptos means "Writing" which exactly means "cover writing". So Steganography means covered writing. Steganography is a exclusive technique of hiding data in some medium so that it doesn't awaken doubt to the hackers. The key concept behind Steganography is that message to be transmitted is not detectable to the casual eye.

In this, the sender embedded its message into the text, image, video, or audio file so that hackers will not be aware of the message. This is not a new technique, it is very old. The most well-liked Steganographic methods used by spies contain invisible ink and microdots. People used design messages in wooden tablets and covered with wax. They used tattooing a shaved messenger's head, letting his hair grow back and then saving it again when he arrived at his contact point to reveal the message.

B. VISUAL CRYPTOGRAPHY

Visual Cryptography scheme was introduced by Naor & Shamir in 1994. Visual Cryptography is a technique which allows visual information (pictures, text, etc.) to be encrypted in the way that decryption becomes a mechanical operation. Visual Cryptography contains two transparent images.

- One image contains random or noisy pixels.
- Other image contains the secret data. It is almost impossible to retrieve the secret information from encrypted images.

Both transparent images and layers are essential to disclose the information. In order to implement a Visual Cryptography, the easiest way is to print the two layers onto one transparent sheet. The main advantage of visual cryptography scheme is:

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 3, Issue 11, November 2016

- It eliminates computation problem during decryption process, and the secret image can be restored by stack operation. This property makes the visual cryptography especially useful for the low computation method. It is a secret sharing scheme with good security for binary image.
- It decodes directly during human vision.

C. NEED OF STEGANOGRAPHY

Now a days, the use of internet increasing quickly. One of the most important areas which attracted by people is security is related to internet and also related to communication. At present, security for hiding data is most popular technique which receives more attention than cryptography. Various methods such as cryptography, coding Steganography, etc. are used for hidden communication. The major benefit of Steganography over other coding techniques is that it hiding the data inside other data in such a way that no other person recipient, even know the existence of it. Terms used in Steganography are**:**

- Cover Image: The medium in which information is to be hidden. It may be an audio, video, image or a text file.
- Key: It's a secret value which help in encoding or extraction of data, without which data cannot be encode and extract.
- Stego-image: A medium within which information is hidden.
- Messag**e**: The data to be hidden or to be extracted.

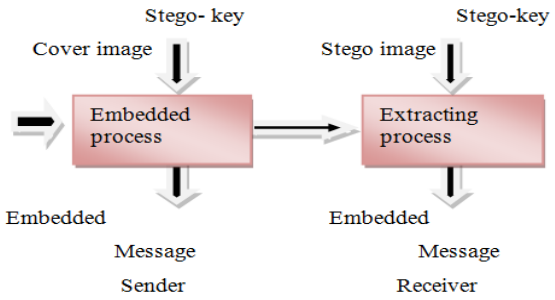


Figure 1: General Block Diagram of Steganography

For Steganography, the size of cover image can be of any size -8 bit, 24 bit, 32 bit, 36 bit. The image can be in any format either jpeg, gif, bmp, etc. we have a key which is used to select the random pixels in which data is to hide. Therefore Stego image is generated which is send to another person. Now on the receiver side the Stego image is processed and extraction of message can be done with the help of secret key. The key is the one by which receiver knows the position of the pixel on which message is rooted.

D. CLASSIFICATION OF STEGANOGRAPHY

- Text based Steganography.
- Image based Steganography.
- Audio based Steganography.
- Video based Steganography

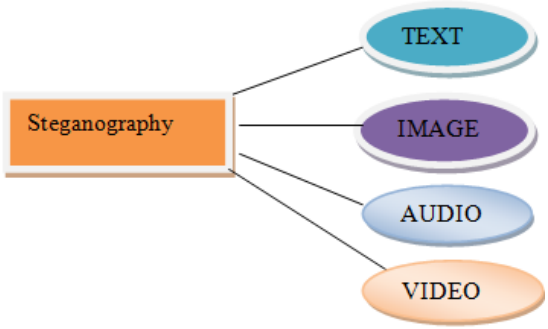


Figure 2: Types of Steganography Techniques

1) Text-based Steganography

In this, the message that is to be sent is rooted firstly in a text file by formatting. The format it based on line-shift coding, word-shift coding, feature coding etc. Reformatting of the text destroys the rooted content hence the technique is not robust.

2) Audio Steganography

This Alters audio files so that they contain hidden messages. The techniques are LSB manipulation, phase coding and echo hiding.

3) Image Steganography

This Steganography hides the message in the images. This is the most popular technique because of the fact that almost no perceivable changes occur. Some of the commonly used methods of embedding payload in cover image are least Significant Bits (LSB) substitution in which the LSBs of cover image pixel are altered to hide the payload and more data can be hidden in edges.

4) Video Steganography

Video Steganography is a technique to hide files or information into digital video format. Video is used as carrier for hidden information. Generally discrete cosine transforms (DCT which is used to hide the information in each of the images in the video, which is not visible by the human eye.

E. STEGANOGRAPHY TECHNIQUES

There are some approaches in classifying the Steganography techniques are given below:

1) Substitution Technique

These techniques try to encode secret data by substituting insignificant parts of the cover image by secret data bits. It consists of many techniques such as least significant bit substitution, pseudorandom permutation etc.

2) Transform Domain Technique

These techniques conceal message in a significant area of the cover image which makes them stronger to attack. It consists of DCT, DWT methods**.**

3) Spread Spectrum Technique

In this technique, it tries to extend a secret message over a cover, in order to make it impossible to recognize. By this

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 3, Issue 11, November 2016

technique, it is hard to remove the embedded message. It includes two types of methods: -one is direct sequence method and second is frequency hopping.

4) Distortion Technique
This technique requires the knowledge of original cover in the decoding process. Most text based hiding methods are of distortion type.

F. FACTORS AFFECTING ON STEGANOGRAPHY
Some factors that determine how efficient and Powerful a technique is are as follows:

1) Robustness
Robustness refers to the ability of embedded data to remain unbroken if the stego image undergoes transformations, such as linear and non-linear filtering, addition of random noise, sharpening or blurring, scaling and rotations.

2) Imperceptibility
The invisibility of a Stenographic algorithm is the first and foremost requirement, since the strength of Steganography lies in its ability to be unnoticed by the human eye. The moment that one can see that an image has been tampered with, the algorithm is compromised.

3) Payload Capacity
It refers to the amount of secret information that can be hidden in the cover source. Watermarking needs to embed only a small amount of copyright information, on the other side, Steganography aims at hidden communication and therefore requires sufficient embedding capacity.

4) PSNR (Peak Signal to Noise Ratio)
It is the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the reliability of its representation. This ratio is mainly used as a quality measurement between the original and compressed image. The higher the PSNR, the better the quality of the compressed image

5) MSE (Mean Square Error)
Mean Squared Error is the average squared difference between a reference image and a distorted image. An Image Steganography technique is able if it gives low MSE.

6) SNR (Signal to Noise Ratio)
It compares the level of a desired signal to the level of background noise. It is defined as the ratio of signal power to the noise power.

G. APPLICATION OF STEGANOGRAPHY

1) Secret Communication
By using Steganography, two parties can communicate secretly without anyone knowing about the communication and in Cryptography, only encode the message but its presence is not hidden. Thus draws unwanted attention. On the other hand, Steganography hides the existence of message in some cover media.

2) Copyright Protection
In this, secret message is embedded in the images which serves as the watermark and thus identify it as an intellectual property which belongs to a particular owner. This is basically related to watermarking.

3) Feature Tagging
Features such as captions, annotations, name of the individuals in a photo or location in a map can be embedded inside an image. Copying the stego image also copies all of the embedded features and only parties who possess the decoding stego key will be able to extract and view the features.

4) Use by terrorists
Steganography can also be used by terrorists in order to hide their secret messages in innocent, cover sources to spread terrorism across the country. Rumours were spread about terrorists using Steganography when the two articles titled “Terrorist instructions hidden online” and “Terror groups hide behind Web encryption” were published in newspaper.

5) Digital Watermarking
This is the most important applications of Steganography. It basically embeds a digital watermark inside an image. This Watermark is used to verify the authenticity or integrity of the carrier signal. It is highly used for tracing copyright infringements and for banknote authentication.

II. RELATED WORK

Authors have proposed a latest method designed for securing the online payment system using visual cryptography and text based Steganography. The planned text based Steganography is derived from Vedic Numeric Code which uses characters of English language. In this Paper, there are 3 users are considered Customer, Online merchant. The customer is provided by a unique authentication password related to the bank which is encrypted using text based steganography and visual cryptography. And one share obtained by this process is kept in CA‟s database and other by the customer. During online shopping the online merchant directs the customer to the certified authority portal. In this portal the customer submits his share and the merchant submit his account details. Then the CA combines the customer submitted share with its own share and obtains the original image. The CA forwards the cover text and the merchant bank details to the bank where the authentication password is recovered from the cover text. The CA then sent the customer authentication information to the merchant. When the bank receives the authentication password it will compared with the bank database and verify. If the verification is successful the fund is transferred from the customer account to the merchant account. Certified authority(C A). Nadeem Akhtar [3], planned the variation

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 3, Issue 11, November 2016

in plain LSB algorithm by using bit inversion technique. In this RC4 algorithm is used in order to achieve the randomization of message bits before hiding the message bits into the cover image. The result shows improvement in security as well as quality.

In 2013, Mamta Juneja et al.[3], introduced an approach to insert the text into gray scale image using RC4 stream cipher method and after that it stored the text in non sequential pixel in image by use of variable hop value power. In this approach, robustness increases due to multilevel security architecture along with faster embedding and extraction process. Zaidoon Kh. et al**.** [4], have given a general overview of Steganography types, general Steganography systems, and characterization of Steganography systems and categorization of Steganography techniques. A. M. Hamid and M. L. M. Kiah [5], authors have proposed a data hiding technique, this method used LSB technique in order to finds out the shady area of the image to hide the data. It converts the binary image and labels each object using 8 pixel connectivity schemes for hiding data bits. This method required high computation to find shady area. and has not tested on high texture type of image. Its hiding ability totally depends on texture of image.

Hamid et al.[6], have proposed a texture based image steganography. In this technique, the texture area is divided into two groups by texture analysis, Simple texture area and Complex texture area. In Simple texture, it is used to hide the 3-3-2 LSB (3 bits for Red, 3 bits for Green, 2 bits for Blue channels) method and in Complex texture area 4 LSB embedding technique is applied for information hiding. The above method used the both (2 to LSB for each channel) methods depending on texture classification for better visual quality. Proposed method has high hidden capacity with considering the perceptual transparency measures e.g. PSNR etc .H. Motameni [7] authors have proposed an adaptive least significant bit spatial domain embedding method. This method divides the image pixels ranges (0-255) and generates a Stego-key. This private Stego-key has 5 different gray level ranges of image and each range indicates to substitute fixed number of bits to embed in least significant bits of image. The strength of proposed method is its integrity of secret hidden information in Stego-image and high hidden capacity. The limitation is to hide extra bits of signature with hidden message for its integrity purpose. It also proposed a method for colour image just to modify the blue channel with this scheme for information hiding. This method is targeted to achieve high hidden capacity plus security of hidden message.

III. PROPOSED WORK

In Proposed work, Cryptography and Steganography differ to each other because cryptography is used to keep the contents of the message secret while steganography is used to hide the existence of secret message. Both techniques are used to protect information from the unauthorized use but sometime it is used in illegal means and neither cryptography is alone perfect nor steganography. Both approaches can be used with each other, to provide better security because cryptography makes the message secret and steganography make existence of message invisible. If someone try to find the existence of secret message and finds but that message would not be understood because it would be encrypted due to the use of cryptography. So, by combining these two approaches, information can be made more secure.

We use a LSB algorithm with median filter in order to hide the text behind the cover image. In this work, we use a median filter which enhances the image quality and removes the noise.

By using median filter, the PSNR and MSE values improved. Steps used in proposed work:

- Implement text based Steganography.
- Encode the text in the sentences in the form ASCII codes.
- Take a cover image in order to hide the data behind this cover image.
- Hide the message using LSB Algorithm.
- Use a Median filter in order to remove the Noise in stenographic image
- Calculate the PSNR and MSE of proposed Steganography technique.

In the proposed work we merge two techniques text steganography and image steganography. Proposed text based steganography uses characteristics of English language such as inflexion, fixed word order and use of periphrases for hiding data rather than using properties of a sentence construction.

H. Encoding

Steps:

- Representation of each letter in secret message by its equivalent ASCII code.
- Conversion of ASCII code to equivalent 8 bit binary number.
- Division of 8 bit binary number into two 4 bit parts.
- Choosing of suitable letters from table 1 corresponding to the 4 bit parts.
- Meaningful sentence construction by using letters obtained as the first letters of suitable words.
- Omission of articles, pronoun, preposition, adverb, was/were, is/am/are, has/have/had, will/shall, and would/should in coding process to give flexibility in sentence construction.
- Encoding is not case sensitive.

I. Decoding

Steps:

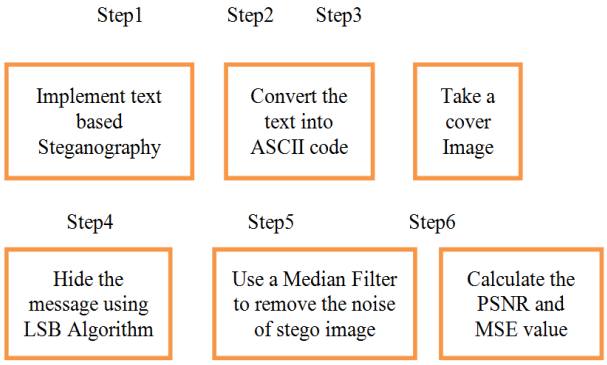
- First letter in each word of cover message is taken and represented by corresponding 4 bit number.
- 4 bit binary numbers of combined to obtain 8 bit number.
- ASCII codes are obtained from 8 bit numbers.
- Finally secret message is recovered from ASCII codes.

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 3, Issue 11, November 2016

Table No.1: Number Assignment

LETTER	CODE NO	LETTER	CODE NO. S
E	15	M	7
A	14	H	7
R	13	G	6
I	13	B	5
O	12	F	4
T	11	Y	4
N	11	W	3
S	10	K	3
L	10	V	3
C	9	X	2
U	8	Z	2
D	8	J	1
P	7	Q	0

J. Improved LSB algorithm with median filter



K. Image Filtering

Image filtering is used to

- Remove noise
- Sharpen contrast
- Highlight contour
- Detect edges
- Other uses?

Image filters can be classified as linear or nonlinear. Linear filters are also known as convolution filters as they can be represented using a matrix multiplication. Thresholding and image equalisation are examples of nonlinear operations, as is the median filter.

L. Median Filtering

Median filtering is a nonlinear method used to remove noise from images. It is widely used as it is very effective at removing noise while preserving edges. It is particularly effective at removing 'salt and pepper' type noise. The median filter works by moving through the image pixel by pixel, replacing each value with the median value of neighbouring pixels. The pattern of neighbours is called the "window", which slides, pixel by pixel over the entire image pixel, image. The median is calculated by first sorting all the pixel values from the window into numerical order, and then replacing the pixel being considered with the middle (median) pixel value.

On the left is an image containing a significant amount of salt and pepper noise. On the right is the same image after processing with a median filter.

Notice the well preserved edges in the image.

IV. CONCLUSION

Steganography is an effective way to hide sensitive information. In this paper we have used the LSB Technique on images to obtain secure stego-image. Our results indicate that the LSB insertion using simple LSB insertion is better than using random encoding technique. The image resolution doesn't change much and is negligible when we embed the message into the image and the image is protected with the personal key. The algorithm is usage for both 8 bit and 24 bit image of the same size of cover and secret image, so it is easy to be implementing in both gray scale and color image. This thesis focuses on the approach like increasing the security of the message and increasing PSNR and reducing the distortion rate.

Our main goal in this research work is to give new insights and directions on how to improve existing methods of hiding secret messages, possibly by combining Steganography and Cryptography. We start by describing the main existing methods and techniques in Steganography that allow us to hide the existence of a message. We then illustrate the different approaches that help us achieve a higher level of secrecy and security, together with their limitations. The first method is about combining Steganography and Cryptography in such a way to make it harder for a Stegoanalyst to retrieve the plaintext of a secret message from a stego-object if cryptanalysis were not used. In the proposed work we merge two techniques text Steganography and image steganography for secure information hiding. In this work,

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 3, Issue 11, November 2016

we provide two level securities to message. First we apply encoding and decoding based text steganography, secondly, using image steganography with LSB for higher level security and we increase the PSNR value of stego image.

V. FUTURE WORK

- As a future work we will implement and test this method for different number of cover images and apply different image Steganography techniques.
- We can use another filter in place of median filter in order to improve the MSE and PSNR value.

VI. RESULT

In this we have discussed about result of the proposed work. Firstly cover image is taken as shown. In figure 5.1 in which we have to hide the Stego_key. In figure5.2 stegano key have been hidden behind the cover image.

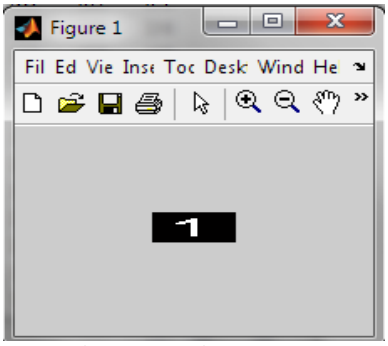


FIGURE5.1: Stegano Key

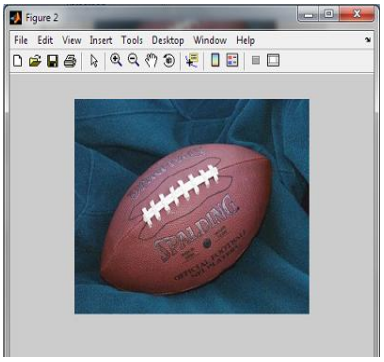


FIGURE5.2: Cover image

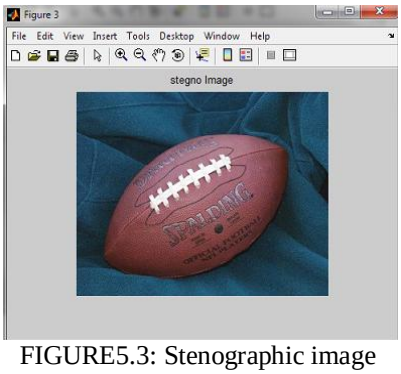


FIGURE5.3: Stenographic image

In the figure 5.3 the hidden message is covered behind this cover image as a result of which we will get a darker image and named it as a stenographic image and figure 5.4 it show the extracted message i.e. recovered stegano key which we have received.

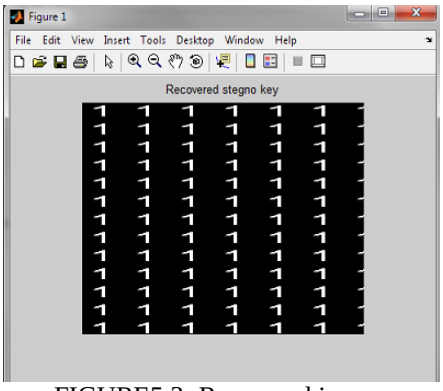


FIGURE5.3: Recovered image

Comparison between previous work and proposed work

1) PSNR (Peak Signal to Noise Ratio)
is an engineering term for the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representmnbvcxz741a/852tion, Because many signals have a very wide dynamic range, PSNR is usually expressed in terms of the logarithmic decibel scale. PSNR is most commonly used to measure the quality of reconstruction of lossy compression codec's. The PSNR block computes the peak signal-to-noise ratio, in decibels, between two images. This ratio is often used as a quality measurement between the original and a compressed image.

PSNR= 10log10 [255^2/MSE]

Comparison	Previous work	LSB Using Median Filter
PSNR value	69.35	74.3206

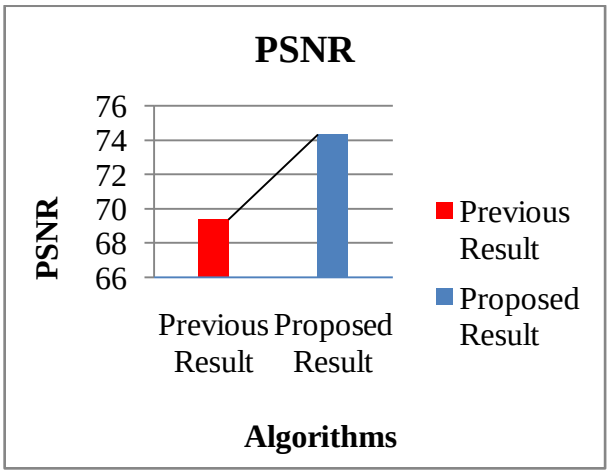


FIGURE5.5: Comparison of PSNR between Previous Work and Proposed Work

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
ISO 3297:2007 Certified
Vol. 3, Issue 11, November 2016

2) MSE (Mean Squared Error)

MSE of an estimator measures the average of the squares of the error or deviations, that is, the difference between the estimator and what is estimated. The MSE assesses the quality of an estimator or predictor. MSE is a risk function, corresponding to the Expected value of the squared error loss or quadratic loss. When we compared these results with the results shown in previous work, we found that the mean square error value in previous work is more as compared to our work. The MSE assesses the quality of an estimator or predictor.

Comparison	Previous work	LSB Using Median Filter
MSE value	0.012	0.0125

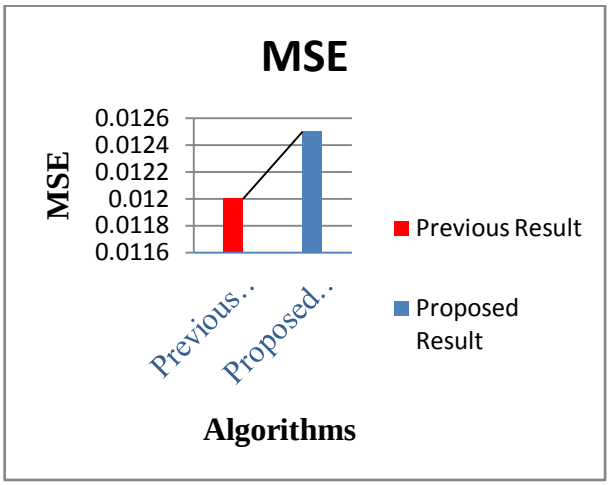


FIGURE: Comparison of MSE between Previous Work and Proposed Work

Table2. Comparison of PSNR and MSE values

Sr. no.	Algorithms	Cover image	Secret message	Stego image	PSNR	MSE
1	Simple LSB Algorithm	RGB image	Text file	Images	68.25	0.012
2	LSB with pseudorandom encoding technique	RGB image	Text file	Images	69.35	0.012
3	LSB with median filter	RGB image	Text file	Images	74.320	0.0125

REFERENCES

[1] Ramakrishna "Design and Implementation of Image Steganography by using LSB Replacement Algorithm and Pseudo Random Encoding Technique", International Journal on Recent and Innovation Trends in Computing and Communication July, 2015.
[2] Souvik Roy, P. Venkateswaran,"Online Payment System using Steganography and Visual Cryptography"IEEE Students' Conference on Electrical, Electronics and Computer Science 2014.
[3] Akhtar, N, "Enhancing the Security and Quality of LSB Based Image Steganography,"Computational Intelligence and Communication Networks (CICN), 2013 5thInternational Conference on , vol., no., pp.385,390, 27-29 Sept. 2013.
[4] MamtaJuneja and Parvinder Singh Sandhu"A New Approach for Information security using an Improved Steganography Technique", Journal of Info. Pro. Systems, Vol 9, No:3, pp.405-424 , (2013).
[5] Soni, A.; Jain, J.; Roshan, R., "Image Steganography using discrete fractional Fourier transform," Intelligent Systems and SignalProcessing (ISSP), 2013 International Conference on, vol., no., pp.97,100, 1-2 March 2013.
[6] Prabakaran, G.; Bhavani, R.; Rajeswari, P.S., "Multi secure and robustness for medical image based Steganography scheme,"Circuits, Power and Computing Technologies (ICCPCT), 2013International Conference on, vol., no., pp.1188, 1193, 20-21 March 2013.
[7] Saurabh V. Joshi, Ajinkya A. Bokil, Nikhil A. Jain, Deepali Koshti"Image Steganography Combination of Spatial and Frequency Domain" International Journal of Computer Applications (0975 – 8887) Volume 53– No.5, September 2012.
[8] Das, R.; Tuithung, T., "A novel Steganography method for image based on Huffman Encoding,"Emerging Trends and Applicationsin Computer Science (NCETACS), 2012 3rd National Conferenceon , vol., no., pp.14,18, 30-31 March 2012.
[9] 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.