

Multiple layer Text security using Variable block size Cryptography and Image Steganography

Shivani Chauhan

Dept. of Computer
Science & Engineering,
National Institute of
Technical Teachers'
Training and Research,
Sector-26, Chandigarh-
160019, India
shivnichauhan.1953@gmail.com

Jyotsna

Dept. of Computer Science
& Engineering, National
Institute of Technical
Teachers' Training and
Research,
Sector-26, Chandigarh-
160019, India
jyotsnabhumbila@gmail.com

Janmejai Kumar

Lecturer, Department of
Computer, Government
Polytechnic Saharanpur
janmejai_kumar9@yahoo.co.in

Amit Doegar

Assistant Professor, Dept. of
Computer Science &
Engineering,
National Institute of
Technical Teachers'
Training and Research,
Sector-26, Chandigarh
160019, India
amit@nitttrchd.ac.in

Abstract- Information security is the major concern now a day since number of internet users is increasing and secret information is getting shared every second. This has also hiked the cyber crime and threat of malicious access. The two main techniques that are used for information security are steganography and cryptography. Cryptography is basically secret writing; on the other hand Steganography is data hiding. In this paper, a hybrid technique is introduced by combining the cryptography and Steganography properties. Also for data encryption vary the block size in place of fixed block. The proposed image steganography algorithm works on spatial domain. LSB method is used for data hiding in different ways. The aim of this work is to design an algorithm for text security as well as improve MSE and PSNR value. The data hiding capacity is also considered. The technique has been designed and simulated in MATLAB 2013a using different format images. Also Qualitative and Quantitative analysis is done and compared with the existing results.

Keywords- Steganography, Cover image, Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), block size.

I. INTRODUCTION

In the last several years information security has become one of the major issues in communication system. With the passage of time, security requirements have been changing rapidly. Before the emergence of computer and network communications facilities, information security was primarily provided by physical and administrative means. But with the introduction of computer, distributed systems and the use of internet, automated tools are needed to protect information stored on the computer and measures are also needed to protect the data during their transmission also. There are various forms of security attacks which demands high level of security [1].

Steganography is the scientific discipline of inconspicuous communication by concealing information in some another media. It refers to the process of hiding the presence of the secret message. It is an art of covert writing. It does not keep the message secret but it provides the secrecy of the message.

Steganography hides a secret message from the third party. It does not arouse an eavesdropper's attention. According to Dictionary.com- "Steganography is hiding a secret message within a larger one in such a way that others cannot discern the presence or contents of the hidden message". The Steganography term is deduced from the Greek words "stegos" implying "cover" and "grafia" implying "writing" and literally means "Cover writing" [2].

Any steganography technique must satisfy a no. of requirements- the integrity of the secret message which is embedded in stego-object must be accurate; the alteration in the stego-object should not be detected by the naked eye; choice of stego-object must be dependent on the size of secret message to be hidden and last but not the least we must always presume that malicious person knows that steganography is being used (that the stego-object is carrying some secret message).

The Steganography systems consist of following elements:

1. Cover Object
2. The Secret Message
3. The Stego Object

1) Cover Object

In Steganography, the cover objects are those in which we hide secret message. The cover object can be images, audio, videos, text. The most used cover object for hide information is image.

2) Secret Message

In Steganography, the secret message is the message to be hidden in cover object. The secret message can be images, text messages etc.

3) Stego Object

The stego object is generated after hiding the secret message in cover image. After that stego object is transmitted and then at receiver side processing is done on stego object to retrieve message from it.

Secret message is embedded into cover object using some embedding algorithms and it is extracted at the receiver side by reversing that procedure as shown in Fig.1. –

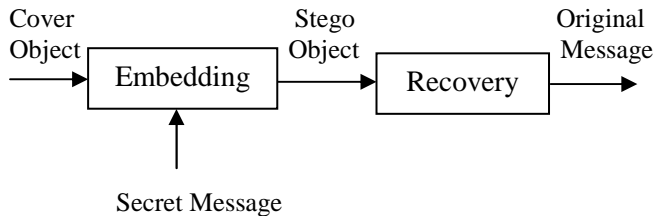


Fig.1 Block Diagram of Steganography

II. CATEGORIES OF STEGANOGRAPHY

Following are the various categories of steganography [3] [4] [5] -

A. Text Steganography

In text steganography, text is used as cover object. It hides secret message behind the other text file. It is done by modifying the text or by modifying some features of text components. Different methods used are line-shift coding, word-shift coding and feature coding. Text steganography was very much used in ancient times, but today these techniques have become obsolete. It is also known as linguistic steganography.

B. Image Steganography

In image steganography, images are used as cover object. It hides secret messages into digital images. It makes use of the weakness of HVS as it cannot detect any variation in luminance part of color pixels. There are different algorithms for different file formats of images. These are Least Significant bit (LSB) insertion, Masking and Filtering etc. JPEG, PNG, GIF (Graphics Interchange Format) etc. are the file formats for images which are used.

C. Audio Steganography - In this, digitized audio signal is used for embedding secret message which produce modification of binary sequence order of the corresponding audio file. By inserting non-hearable tones in audio signal used as cover object data is embedded. Audio steganography exploits the weaknesses of the human auditory system (HAS). It exploits psycho acoustical masking phenomenon (makes a weak tone unperceivable in the existence of a strong tone) of HAS. HAS cannot identify some variations in the sound waves. The methods used are LSB coding, Spread Spectrum, Echo hiding etc. MPEG, MP3 etc. are the file formats for audio which are used.

D. Video Steganography - In video steganography, video is used as cover object. Since videos are basically aggregation of images and sounds, that is why many of the techniques can be implemented on video files also. The advantage of concealing secret information in video is the fact that it is a moving flow

of images and sounds and a large amount of information can be concealed inside a video. Any noticeable change might remain unobserved by humans because it is an uninterrupted flow of information. AVI (Audio Video Interleave), MPEG, and MP4 etc. are the file formats for video which are used.

E. Protocol Steganography - It is the process of hiding information network control protocols that are used in network transmission. It is also known as network steganography. Steganography can be used on the covert channels which exist in the OSI network model layers. Network protocols used are TCP/IP (Transmission Control Protocol/Internet Protocol), UDP (User Datagram Protocol), and ICMP (Internet Control Message Protocol) etc.

The techniques including image steganography, audio steganography, video steganography and protocol steganography are collectively known as technical steganography.

III. RELATED WORK

A. Literature Survey

Many researchers have been done till now in the field of steganography. Many papers on the recent researches and developments in the field of steganography were studied. The literature survey basically provides a way to investigate for research and gives an idea of what has been done till date. A succinct review based on the study of these papers related to our work is as follows.

Dr. Diwedi Samidha et al. [6] described several image steganography techniques in spatial domain. Along with existing techniques like LSB, layout management schemes and replacing only 1's or only zero's, some more methods like replacing intermediate bit, raster scan principle, random scan principle, color based data hiding and shape based data hiding are also proposed. These new techniques are based on random selection of pixels for data hiding considering many parameters of an image like physical location and intensity value of pixel, etc.

Sourabh Chandra et al. [7] proposed a symmetric key cryptographic algorithm which is content based. This algorithm included binary addition operation for encrypting the plain text and circular shift operation and folding method for making the key secure. This algorithm posed a difficulty for opponent to decrypt the key and text.

Amrit Pal Singh et al. [8] developed an improved method for image steganography using LSB technique. This worked by slicing the three planes of RGB image and then hiding the data into each plane based on color sensitivity by using LSB technique. It resulted in high embedding capacity and better image quality. Its PSNR value was better than previous steganographic methods.

Yogita Birdi et al. [9] proposed a method in steganography for secure communication. First, data is encrypted and then embedded using raster scan technique. This method made use of the Raster Scan Principle of displaying an image on CRT (Cathode Ray Tube) display. In this pixels have been hidden in the cover image in left to right and right to left manner. This made data extraction difficult for the opponent.

B. Motivation

Due to advancement in technology the number of attacks increases on internet so data security required so in this paper proposed a hybrid technique for data security by using cryptography and steganography properties. We took the motivation from literature work papers they work on variable block size and data hiding in different ratios so it's difficult to Steganalysis of data.

IV. DATA ENCRYPTION AND STEGANOGRAPHY ALGORITHMS

In this section, the encryption and data hiding techniques are explained –

A. Variable Block Size data Encryption Algorithm

1. Read the plain text and their corresponding ASCII values.
2. Calculate the word length of message.
3. Enter the Three digits Random Key and produce single digit key (key encryption is done by circular bit shift operation).
4. Encrypted Value = ASCII value + word length + Random Key [7].

B. Steganography Algorithms

1) Modified LSB Technique: In Modified LSB technique in place of LSB bit, 2 or 3 bits from LSB side is replaced with data bits as shown in table 1 and 2.

TABLE I. COVER IMAGE PIXELS

| | | | |
|----------|----------|----------|----------|
| 10010101 | 11100011 | 01110010 | 01111111 |
| 10001001 | 01010101 | 10101110 | 00011001 |

Let suppose data want to hide: 10101100

TABLE II. STEGO IMAGE PIXELS

| | | | |
|------------------|------------------|------------------|------------------|
| 100101 00 | 111000 11 | 011100 10 | 011111 10 |
| 10001001 | 01010101 | 10101110 | 00011001 |

Modified LSB technique has high capacity as compared to LSB technique but variability increases as compared to LSB technique.

2) Raster Scan Technique: This concept is taken from displaying in the image on television. In television the electron beam scan the image from left to right then again come back to original position right to left for scan next line and so on.

So, in the same way in steganography data can be hidden left to right then right to left or can also take another pattern top to bottom or bottom to top for data hiding [9].

TABLE III. COVER IMAGE PIXELS FOR RASTER SCAN TECHNIQUE

| | | | |
|----------|----------|----------|----------|
| 10010101 | 11100011 | 01110010 | 01111111 |
| 10001001 | 01010101 | 10101110 | 00011001 |

Let suppose we want to hide: 10101100

TABLE IV. STEGO IMAGE PIXELS FOR RANDOM SCAN TECHNIQUE

| | | | |
|------------------|------------------|------------------|------------------|
| 100101 00 | 111000 10 | 011100 11 | 011111 11 |
| 100010 01 | 010101 00 | 101011 11 | 000110 00 |

V. PROPOSED HYBRID TECHNIQUE

In the proposed method, message bit is concealed in LSB of Red (R), Green (G), and Blue (B) color components of 24-bit RGB color image.

A. Embedding Process

The step-by-step methodology to be followed for hiding data is as follows-

- 1) The proposed approach will begin with taking a RGB image as cover image and a secret text to be hidden in that image.
- 2) The secret text will be first encrypted to convert it into cipher text using a symmetric key cryptography technique which is a content based and utilizes block cipher principle. But in this technique block size is not fixed, it depends upon the word length. The encryption algorithm is explained below-

Variable block size data encryption algorithm in proposed algorithm

- a. Read the plain text and their corresponding ASCII values.
- b. Calculate the length of the words of the message.
- c. Enter the three digits random key and produce the single digit key by folding method.
- d. Cipher Text = (ASCII value XOR key) XOR word length.

The whole process is explained with example below -

Let suppose enter the random key is: 969

1st Round = 9+6+9 = 24

2nd Round = 2+4 = 6,

So final key for encryption = 6

TABLE V. ENCRYPTION PROCESS

| Character Fetched | ASCII values of character | ASCII value after XOR with key (key value = 6) | First encrypted text | ASCII values after XOR with word length (= 5) | Final encrypted text |
|-------------------|---------------------------|--|----------------------|---|----------------------|
| P | 80 | 86 | V | 83 | S |
| E | 69 | 67 | C | 70 | F |
| A | 65 | 71 | G | 66 | B |
| C | 67 | 69 | E | 64 | @ |
| E | 69 | 67 | C | 70 | F |

- 3) The R, G, B planes of RGB image will be extracted from the cover image.
- 4) The cipher text will be hidden in R G B planes of cover image –
 - 2 bits will be embedded in 2 LSB of red plane using modified LSB substitution by XORing secret data bits with cover pixels' bits,
 - 2 bits will be embedded in 2 LSB of green plane using raster scan technique (in first scan hide from left to right and in next scan right to left and so on..) by XORing secret data bits with cover pixels' bits,
 - 4 bits will be embedded in 4 LSB of blue plane using raster scan technique (in first scan hide from top to bottom and in next scan bottom to top and so on..) by XORing secret data bits with cover pixels' bits.
 - This process will continue till the whole cipher text will be hidden in cover image.
- 5) Stego image will be obtained by combining the three embedded planes and the parameters MSE and PSNR will be evaluated.
- 6) Results achieved after the execution of algorithms will be analysed and compared with the existing techniques like LSB, Raster Scan technique etc.

B. Extracting Process

- 1) Bitxor operation is done between cover and stego image to return the data that is hidden in cover image (rgb plane).
- 2) Enter the key for decryption.
- 3) Bitxor operation is done between encrypted data, key, and their resultant with corresponding word length to extract the plain text.
- 4) Plain text return at output.

VI. RESULTS AND DISCUSSION







The simulation has been done in MATLAB 2013a using 12 images and the results of 6 images have been shown with

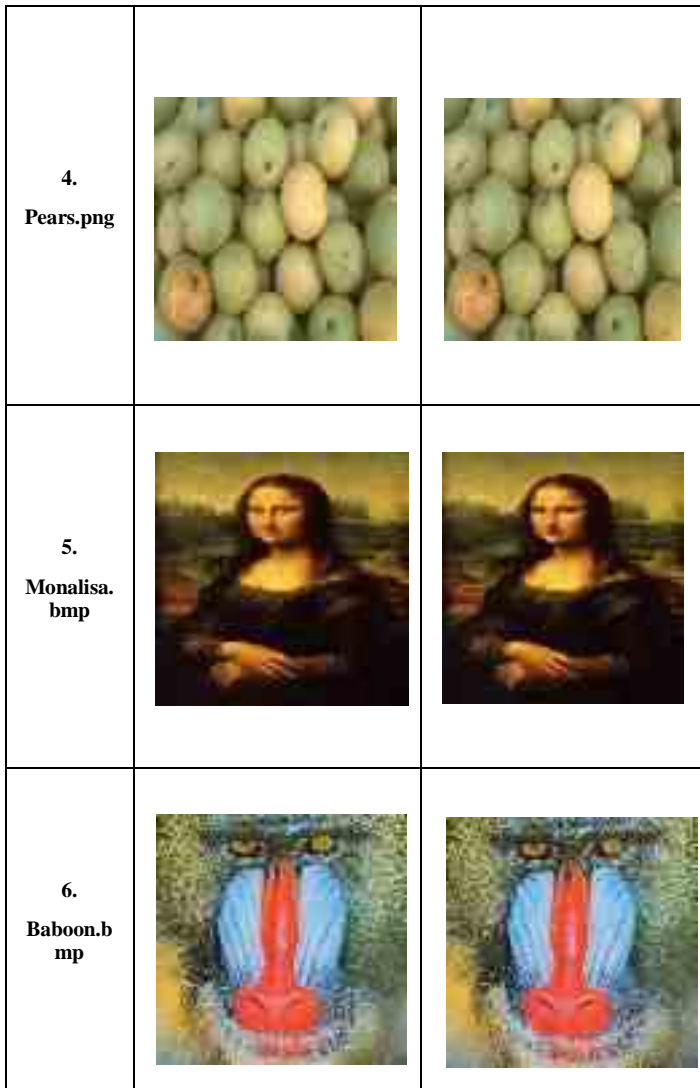
respect to its qualitative as well as quantitative analysis. The images are taken from SIPI database [11]. The qualitative as well as quantitative analysis has been shown in Table VI and Table VII respectively.

A. Qualitative Analysis

For Qualitative analysis, all images are taken from MATLAB database. In Table 6.1, 2 KB message is hidden in cover image of size 512×512 pixels.

TABLE VI. QUALITATIVE ANALYSIS

| Image Details (512×512) | Cover Image | Stego Image |
|-------------------------|--|---|
| 1. Lena.jpg |  |  |
| 2. Peppers.jpg |  |  |
| 3. Coloredchips.png |  |  |



2) Peak Signal to Noise Ratio

PSNR measures the maximum noise, the signal tolerate. PSNR is given as [10]

$$PSNR=10\log_{10} \frac{(2^t-1)^2}{MSE} \quad (2)$$

Here, 't' represents the bits per sample. In image processing, low MSE and High PSNR are preferred. In Steganography up to 30dB PSNR is acceptable.

3) Entropy

Entropy (Average information content) measures the proportions of the details of the image and it is usually measured in units as bits.

$$E(p)=-\sum_{i=0}^{G-1} P(i)\log P(i) \quad (3)$$

Where P(i) is probability density function of a given image at intensity level I and G is total number of grey levels in the image. An image having high entropy value is considered to be having high details and have better quality.

The Tables VII shows the quantitative analysis between cover image and stego image.

TABLE VII. QUANTITATIVE ANALYSIS

| Image (512x512) | MSE | | PSNR (in dB) | |
|---------------------|------------------------|--------------------|------------------------|--------------------|
| | Existing Technique [8] | Proposed Technique | Existing Technique [8] | Proposed Technique |
| 1. Lena. Jpg | 0.0743 | 0.0211 | 59.41 | 64.89 |
| 2. Peppers. Jpg | 0.0747 | 0.0212 | 59.50 | 64.88 |
| 3. Coloredchips.png | 0.0746 | 0.0218 | 59.40 | 64.94 |
| 4. Pears.png | 0.0744 | 0.0214 | 59.42 | 64.83 |
| 5. Monalisa.bmp | 0.0740 | 0.0219 | 59.43 | 64.73 |
| 6. Baboon.bmp | 0.0741 | 0.0214 | 59.44 | 64.83 |

B. Quantitative Analysis

The Mean Square Error, Peak Signal to Noise Ratio and Correlation are the parameters used for quantitative measure of proposed technique. These two parameters (MSE and PSNR) basically error matrices to compare the original cover image with the output Stego image. The third parameter entropy is used to measure the level of security of encrypted information.

1) Mean Square Error

MSE measured the error between original and Stego image [10].

$$MSE = \frac{1}{A \times B} \sum_{A,B} [f1(A, B) - f2(A, B)]^2 \quad (1)$$

Where f1(A,B) represent the Original image and f2(A,B) represents the Stego image. A X B denotes the size of the original image. In Steganography low value of MSE required so output image looks similar to input image.

The following figures Fig.1 and Fig.2 shows the comparison of Existing technique and proposed technique based on MSE and PSNR of Table VII.

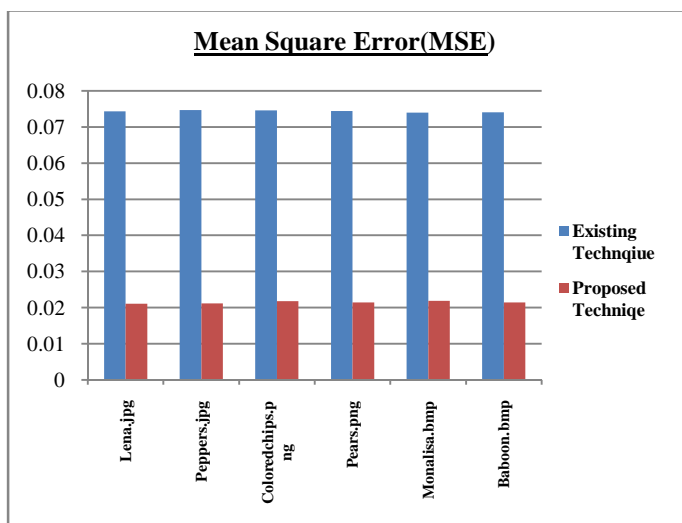


Fig.2 Histogram for MSE

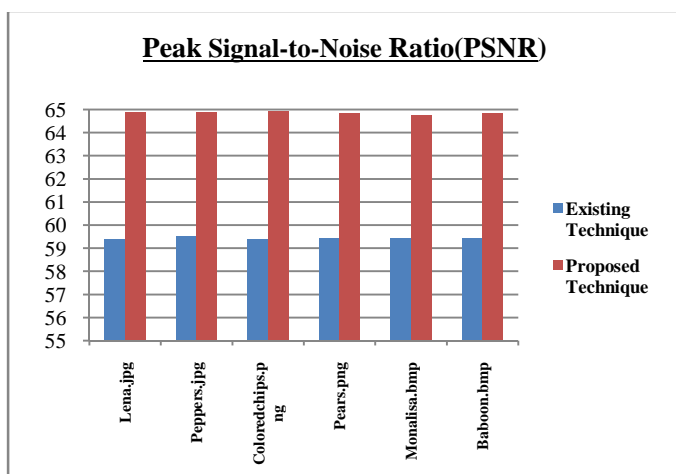


Fig.3 Histogram for PSNR

In hybrid algorithm, variable block size algorithm applies on data for encryption. The qualitative analysis shows that even after encryption of data the visualization of Cover image and Stego image is same.

In Quantitative analysis measure MSE and PSNR parameters and compare with existing results. The proposed work has variability in PSNR as compared to existing work and security level is also very high.

In existing technique [8], they have used only PSNR and MSE parameter for analysis of results. In proposed work, other parameter is also used that is Entropy for analysis of algorithm.

TABLE VIII. ENTROPIES OF COVER IMAGE AND STEGO IMAGE

| Images (512×512) | Entropy of cover image | Entropy of stego image |
|------------------|------------------------|------------------------|
| Lena.jpg | 7.7551 | 7.7553 |
| Peppers.jpg | 7.7361 | 7.7262 |
| Coloredchips.png | 7.4619 | 7.4620 |
| Pears.png | 7.5931 | 7.5932 |
| Monalisa.bmp | 7.0003 | 7.0004 |
| Baboon.bmp | 7.7624 | 7.7625 |

The results obtained for entropies shows that the entropy of stego image is slightly greater than that of cover image as more hidden information is added.

VIII. CONCLUSION AND FUTURE WORK

The proposed method uses combination of cryptography and image steganography. The cryptographic technique used for encrypting the secret message is content based encryption algorithm and the steganographic techniques used are LSB and raster scan technique. In this work, encrypted data is hiding using different ratio in RGB plane simultaneously. The proposed method can hide approximately 16 KB message in a cover image of size 128×128 pixels, 260 KB message in a cover image of size 512×512 pixels and 480 KB message in a cover image of size 800×600 pixels. The proposed algorithm as compared to existing algorithm [8] gives result in less MSE and more PSNR value. The computation time of proposed work is user dependent as value for key is input given by user at run time. The Qualitative and Quantitative Analysis is also done. Also conclude that MSE and PSNR depend on image size, data to be embedded and probability of pixel variation. The entropies for cover and stego image are also calculated and results show that entropy of stego image is slightly greater than that of cover image as more hidden information is added.

In future, video can be taken as cover media for increasing the data hiding capacity. Different ratio of data like 3:3:2 can be used for hiding and randomness can be increased between techniques by switching between the techniques randomly. Methods to reduce pixel variation can also be applied.

REFERENCES

- [1] W. Stallings, "Cryptography and Network Security: Principles and Practices, fourth edition", pp. 592, November 2005.
- [2] H. Gupta, Prof. R. Kumar, and Dr. S. Changlani, "Enhanced Data Hiding Capacity Using LSB-Based Image Steganography Method", International Journal of Emerging technology and Advanced Engineering(IJETAE), vol. 3, no. 6, pp. 212–214, June 2013.
- [3] S. Suri, H. Joshi, and V. Minocha and A. Tyagi, "Comparative Analysis of Steganography for Coloured Images", International Journal of Computer Sciences and Engineering(IJCSE), vol. 2, no. 4, pp. 180–184, 2014.
- [4] B. Madhuravani, Dr. D. S. R. Murthy, Dr. P. B. Reddy and Dr. K. V. S. N. R. Rao, "Strong Authentication Using Dynamic Hashing and Steganography", IEEE International Conference on Computing, Communication and Automation(ICCCA), pp. 735–738, 2015.

- [5] P. Joseph and Vishnukumar S., "A Study on Steganographic Techniques", Proceedings of IEEE Global Conference on Communication Technologies(GCCT), pp. 206–210, 2015.
- [6] D. Samidha and D. Agrawa, "Random Image Steganography in Spatial Domain", IEEE International Conference on Emerging Trends in VLSI, Embedded System, Nano Electronics and Telecommunication System(ICEVENT), pp. 1–3, 2013.
- [7] S. Chandra, B. Mandal, S. S. Alam, and S. Bhattacharyya, "Content Based Double Encryption Algorithm Using Symmetric Key Cryptography", Procedia computer Science International Conference on Recent Trends in Computing(ICRTC), vol. 57, pp. 1228–1234, 2015.
- [8] A. Singh and H. Singh, "An Improved LSB Based Image Steganography Technique for RGB Color Images", IEEE International Conference on Electrical, Computer and Communication technologies, pp. 1-4, 2015.
- [9] Y. Birdi and Harjinder Singh, "Raster Scan Technique for Secure Communication in Steganography", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, vol. 4, no. 6, pp. 5174–5179, 2015.
- [10] B. J. Mohd, S. Abed, T. Al-Hayajneh, and S. Alouneh, "FPGA hardware of the LSB Steganography Method", IEEE International Conference on Computer, Information and Telecommunication Systems(CITS), pp. 1–4, 2012.
- [11] <http://sipi.usc.edu/database/>.
- [12] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding - A Survey", Proceedings of the IEEE, Special issue on protection of multimedia content, vol. 87, no. 7, pp. 1062–1078, July 1999.
- [13] P. Bharti and R. Soni, "A New Approach of Data Hiding in Images using Cryptography and Steganography", International Journal of Computer Applications, vol. 58, no. 18, pp. 1–4, 2012.
- [14] M. R. Mani, V. Lalithya and P. S. Rekha, "An Innovative Approach for Pattern based Image Steganography", IEEE International Conference on Signal Processing, Informatics, Communication and Energy Systems(SPICES), pp. 1–4, 2015.
- [15] R. Nivedhitha and T. Meyyappan, "Image Security Using Steganography And Cryptographic Techniques", International Journal of Engineering Trends and Technology, vol. 3, pp. 366–371, 2012.
- [16] P. P. Aung and T. M. Naing, "A Novel Secure Combination Technique of Steganography and Cryptography", International Journal of Information Technology, Modeling and Computing(IJITMC), vol. 2, no. 1, pp. 55–62, February 2014.
- [17] N. Akhtar, S. Khan, and P. Johri, "An Improved Inverted LSB Image Steganography", IEEE International Conference on Issues and Challenges in Intelligent Computing Techniques(ICICT), pp. 749–755, 2014.
- [18] K. Joshi and R. Yadav, "A New LSB-S Image Steganography Method Blend with Cryptography for Secret Communication", IEEE Third International Conference on Image Information Processing(ICIIP), pp. 86–90, 2015.