Abstract—Confidentiality calls for substantial research and development in network security and data communication. Several techniques have been proposed for the past decades to ensure secure and confidential transmission of data. Steganography is a significant method of hiding data in another media, such that it is physically and virtually invisible. It is used primarily to ensure secure communication in an indiscernible fashion so that the hidden information is not discovered at any stage. The goal is to hide the presence of secret information rather than the contents of information to avoid breaching of data confidentiality. This paper is an effort to bring about a comparison of some of the recent techniques used for steganography on the basis of embedding capacity and Peak signal to noise ratio (PSNR), Universal image quality index (UIQI), Number of pixel change rate (NPCR) and correlation. The performance metrics undertaken are robustness, security analysis and perceptual quality. The techniques were implemented in MATLAB 2013a v 8.1.0.604.

Index Terms—Steganography, BPCS, PSNR, Entropy.

I. INTRODUCTION

Good quality network security is an integral part of data communication infrastructure. With the growth in intelligent transmission and communication networks, a breach in security is a matter of concern [1, 2, 3]. The ITRC report gives the number of data breaches which demonstrates that the numbers have taken a great hike over the years. This is shown as in the figure 1:

One primary clause that ensures secure data communication is data confidentiality. Steganography produces an efficient mechanism for secure transmission of sensitive data [3, 4, 5]. The data is embedded in a cover media in a fashion such that its existence is not detected by an intruder. The most basic steganography technique uses an image to hide the secretive information. This is demonstrated as in figure 2.

This paper compares most of the popular steganography techniques which have good embedding capacity and robustness. The rest of the paper is organized as follows: Section II explains the techniques implemented. Section III gives simulation set-up parameters. Section IV gives the snapshots. Section V provides the performance metrics on the basis of which results and conclusion are formulated in section VI and VII respectively.

II. TECHNIQUES IMPLEMENTED

The implemented steganography techniques are described in this section.
A. Implementation using BPCS

BPCS stands for Bit Plane Complexity segmentation [14]. The last plane of the cover image is a complex noisy plane which is used for embedding. The first step in BPCS is to segment the cover image into 8 planes. Blocks of 8x8 are formulated of each plane. After block segmentation, canonical gray code conversion is applied on pure binary codes present in each block.

The next step is to divide the data into 8x8 blocks. Complexity is calculated for each data that is to be embedded. The complexity ($\alpha$) is given by

$$\alpha = \frac{K}{M}$$  \hspace{1cm} (1)

Where, $\alpha$ should lie from 0 to 1.

$M$ is the total number of blocks and $k$ is total no. transition changing from white to black or vice versa.

Threshold value is computed by:

$$th = \alpha \times C_{max}$$  \hspace{1cm} (2)

Where, $C_{max}$ is maximum complexity of Block. This threshold value acts as cut-off for block selection i.e. the blocks having complexity value greater than the threshold value are opted for embedding. Also complexity for data blocks is calculated to check whether it should be embedded without modifications or some needs to be done. If the complexity of the data block is greater than the threshold it is embedded into the image blocks directly. Otherwise, the conjugate of the block is taken to be embedded into the image block as shown in figure 3.

B. Implementation using Status Bit

The first step in Status bit Steganography involves the extraction of the R, G and B planes from the cover media. The most significant bits of each plane are taken and their decimal equivalent is computed [10, 11, 12, 13, 14, 15] then, the binary values of the pixels in the blue plane are computed. Embedding Decision would be taken on the basis of darker and lighter pixels.

If the MSB bits contains at least two “1” bits, then the pixel is called as lighter pixel. If the MSB bits contains at least two “0” bits, then the pixel is called as lighter pixel.

The decimal equivalent ($Z_n$) of the three MSB bits of each RGB pixels is used to decide the position of embedding in blue plane.

**Embedding in lighter pixels**: If the bit position ‘$Z_n$’ and message bit is same, then change the LSB bit of the pixels of blue plane into 1 otherwise make it 0.

**Embedding in darker pixels**: If the bit position ‘$Z_n$’ and message bit is same, then change the LSB bit of the pixels of blue plane into 1 otherwise make it 0. Here, there is one more condition that if all the MSB bits of
pixels are 0, then directly inserts the message in blue plane.

![Fig.4. LSB Status Steganography](image)

**Algorithm: compute the lighter and darker pixels**

**Input:** Plain image $I_{MN}$ where $M$, $N$ are height and width of the image, data.

**Output:** Stego image

**Step 1:** Take plain image

**Step 2:** Make 3x3 windows of plain image.

**Step 3:** Collect the MSB bits from a pixel {R, G, B} color space.

**Step 4:** For darker pixels - if the MSB bits contain at least two bit 1, then the pixels is used for data hiding.

**Step 5:** For lighter pixels - if the MSB bits contain at least two bit 0, then the pixels is used for data hiding.

**Algorithm: Embedding data in darker pixels**

**Input:** Darker pixels of Blue planes

**Output:** Stego image

**Step 1:** The decimal representation $Z_n$ of three MSB bits of RGB pixels are used for determining the position in blue plane. Now if bit position $Z_n$ and message bit is same then change the LSB bits of the pixels of blue plane into 1 otherwise 0.

**Step 2:** If all three MSB bits of pixels are 0 then in this situation directly insert the message bit in blue plain.

**Algorithm: Embedding data in lighter pixels**

**Input:** lighter pixels of Blue planes

**Output:** stego image

**Step 1:** The decimal representation $Z_n$ of three MSB bits of RGB pixels is used for determining the position in blue planes. If the bit position $Z_n$ and message bit is same then change the LSB bits of the pixels of blue plane into 1 otherwise 0.

**Step 2:** If LSB(pixels of plain image)=1, LSB(msg bit)=0, decrement LSB(pixels) by 1.

**Step 3:** If LSB(pixels of plain image)=0, LSB(msg bit)=1, increment LSB(pixels) by 0.

**Step 6:** Transmit the stego Image.
D. Implementation using LSB based Image Steganography using Secret Key

To hide the secret information, the cover image is divided into three planes (Red, Green and Blue). After dividing each plane, the secret key is chosen on the basis of user. The secret key is converted into one-dimension array of bit stream [16, 17, 18, 19, 20].

Secret key and red plane are used only for decision making to hide the information into either Green plane or Blue plane. Each bit of secret key is ex-ored with the LSB of red plane. The obtained ex-or results decide that the information will be embedded in either Green plane or Blue plane.

![Fig. 6. LSB based Image Steganography using Secret Key](image)

**Algorithm: Stego Image**

**Input:** Plain image Im_{MN} where M, N are height and width of the image, secret key data.

**Output:** Stego image

**Step 1:** Take plain image
**Step 2:** Divide image into three planes (R, G, and B).
**Step 3:** Convert the secret key into binary, if it is then keep it as such.
**Step 4:** Convert the secret key into one dimension array.
**Step 5:** Ex-or each bit of secret key with LSB of Red plane.
**Step 6:** Change the LSB of Green plane pixel if Ex-or result is 1 else, embed the data in LSB of Blue plane pixel.
**Step 7:** Transmit the stego image.

**NOTE:** Decryption process of each technique is just reverse as like encryption.

III. SIMULATION SETUP PARAMETERS

Hardware and software requirement for simulation and implementation of intended steganography techniques are given in table 1.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data size</td>
<td>16X16 (color image)</td>
</tr>
<tr>
<td>Image size</td>
<td>256 x 256, 512 x 512, 1024 x 1024</td>
</tr>
<tr>
<td>Image category</td>
<td>Color image (.bmp format)</td>
</tr>
<tr>
<td>Programming language</td>
<td>MATLAB 2013a v 8.1.064</td>
</tr>
<tr>
<td>Simulation implemented</td>
<td>64 bit MATLAB</td>
</tr>
<tr>
<td>Processor</td>
<td>1.4 GHz dual core Intel i5</td>
</tr>
<tr>
<td>Memory size</td>
<td>4 GB/1TB of1600 Mhz LPDDR3</td>
</tr>
</tbody>
</table>

IV. SNAPSHOTS

Relationship of original image and stego image obtained by implementation of steganography techniques is described in table 2.

<table>
<thead>
<tr>
<th>Size of Image</th>
<th>Original Image</th>
<th>BPCS</th>
<th>LSB Steg.</th>
<th>Status bit</th>
<th>LSB Secret Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>256</td>
<td><img src="image" alt="Image" /></td>
<td><img src="image" alt="Image" /></td>
<td><img src="image" alt="Image" /></td>
<td><img src="image" alt="Image" /></td>
<td><img src="image" alt="Image" /></td>
</tr>
<tr>
<td>512</td>
<td><img src="image" alt="Image" /></td>
<td><img src="image" alt="Image" /></td>
<td><img src="image" alt="Image" /></td>
<td><img src="image" alt="Image" /></td>
<td><img src="image" alt="Image" /></td>
</tr>
<tr>
<td>1024</td>
<td><img src="image" alt="Image" /></td>
<td><img src="image" alt="Image" /></td>
<td><img src="image" alt="Image" /></td>
<td><img src="image" alt="Image" /></td>
<td><img src="image" alt="Image" /></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Technique</th>
<th>Red Plane.:1</th>
<th>Green Plane.:2</th>
<th>Blue Plane.:3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Original Image</td>
<td><img src="image" alt="Image" /></td>
<td><img src="image" alt="Image" /></td>
<td><img src="image" alt="Image" /></td>
</tr>
<tr>
<td>BPCS</td>
<td><img src="image" alt="Image" /></td>
<td><img src="image" alt="Image" /></td>
<td><img src="image" alt="Image" /></td>
</tr>
<tr>
<td>LSB Steg.</td>
<td><img src="image" alt="Image" /></td>
<td><img src="image" alt="Image" /></td>
<td><img src="image" alt="Image" /></td>
</tr>
<tr>
<td>Status bit</td>
<td><img src="image" alt="Image" /></td>
<td><img src="image" alt="Image" /></td>
<td><img src="image" alt="Image" /></td>
</tr>
<tr>
<td>LSB Secret Key</td>
<td><img src="image" alt="Image" /></td>
<td><img src="image" alt="Image" /></td>
<td><img src="image" alt="Image" /></td>
</tr>
</tbody>
</table>
A. Histogram Analysis for 256 x 256 Image

Relationship of original image and stego image histogram analysis found by implementation of steganography techniques is described in table 3.

B. Histogram Analysis for 512 x 512 Image

Table 4. Comparison of Histogram for 512 x 512 Images

<table>
<thead>
<tr>
<th>Technique</th>
<th>Red Plane(:,:,1)</th>
<th>Green Plane(:,:,2)</th>
<th>Blue Plane(:,:,3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Original Image</td>
<td><img src="image" alt="Histogram" /></td>
<td><img src="image" alt="Histogram" /></td>
<td><img src="image" alt="Histogram" /></td>
</tr>
<tr>
<td>BPCS</td>
<td><img src="image" alt="Histogram" /></td>
<td><img src="image" alt="Histogram" /></td>
<td><img src="image" alt="Histogram" /></td>
</tr>
<tr>
<td>LSB Steg.</td>
<td><img src="image" alt="Histogram" /></td>
<td><img src="image" alt="Histogram" /></td>
<td><img src="image" alt="Histogram" /></td>
</tr>
<tr>
<td>Status bit</td>
<td><img src="image" alt="Histogram" /></td>
<td><img src="image" alt="Histogram" /></td>
<td><img src="image" alt="Histogram" /></td>
</tr>
</tbody>
</table>

C. Histogram Analysis for 1024 x 1024 Image

Table 5. Comparison of Histogram for 1024 x 1024 Images

<table>
<thead>
<tr>
<th>Technique</th>
<th>Red Plane(:,:,1)</th>
<th>Green Plane(:,:,2)</th>
<th>Blue Plane(:,:,3)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Original Image</td>
<td><img src="image" alt="Histogram" /></td>
<td><img src="image" alt="Histogram" /></td>
<td><img src="image" alt="Histogram" /></td>
</tr>
<tr>
<td>BPCS</td>
<td><img src="image" alt="Histogram" /></td>
<td><img src="image" alt="Histogram" /></td>
<td><img src="image" alt="Histogram" /></td>
</tr>
<tr>
<td>LSB Steg.</td>
<td><img src="image" alt="Histogram" /></td>
<td><img src="image" alt="Histogram" /></td>
<td><img src="image" alt="Histogram" /></td>
</tr>
<tr>
<td>Status bit</td>
<td><img src="image" alt="Histogram" /></td>
<td><img src="image" alt="Histogram" /></td>
<td><img src="image" alt="Histogram" /></td>
</tr>
<tr>
<td>LSB Secret Key</td>
<td><img src="image" alt="Histogram" /></td>
<td><img src="image" alt="Histogram" /></td>
<td><img src="image" alt="Histogram" /></td>
</tr>
</tbody>
</table>

V. PERFORMANCE METRICS

For thorough exploration of the techniques, three analyses were performed that are explained in the subsequent section.

A. Security Analysis

For security analysis, histograms of original image and encrypted-image are matched. A technique is said to be secure when the difference in the histograms is negligible which means the parameter values lie close to its ideal values. The parameters which are used for security analysis are listed below:

- **Jaccard Index**:
  
  The Jaccard index, also known as the Jaccard similarity coefficient is used for comparing similarity between the original image and the encrypted-image. The jaccard index is mathematically given by the formula
  
  \[ J(X, Y) = \frac{X \cap Y}{X \cup Y} \]

  Where, \( X \) is the original image and \( Y \) is the encrypted-image

  \( J(X, Y) \) is the jaccard index between image matrices \( X \) and \( Y \)

  \( X \cap Y \) is the intersection of matrices \( X \) and \( Y \)

  \( X \cup Y \) is the union of matrices \( X \) and \( Y \)

  The value of Jaccard index lies between 0 and 1. 1 signifies perfect matching and 0 signifies total mismatch.

- **Correlation Coefficient**:

  The correlation coefficient is a measure of the linear correlation (dependence) between two images \( X \) and \( Y \), giving a value between +1 and −1 inclusive, where 1 signifies perfect match and −1 signifies total mismatch.

  The correlation coefficient is given by the formula

  \[ \rho(X, Y) = \frac{\text{cov}(X, Y)}{\sigma_X \sigma_Y} \]

  Where, \( X \) is the original image and \( Y \) is the stego-image.
\( p(X,Y) \) is the correlation coefficient between image matrices \( X \) and \( Y \)
\[ \text{cov}(X,Y) \] is the covariance between matrices \( X \) and \( Y \)
\( \sigma_X \) is the standard deviation of \( X \)
\( \sigma_Y \) is the standard deviation of \( Y \)

- **Intersection Coefficient:**

Intersection coefficient of histograms counts the common number of pixels of same value between two histograms (histograms of cover image and stego-image). The intersection coefficient is given by the formula:

\[
I(X,Y) = \sum_{i=1}^{N} \min(X(i), Y(i))
\]

Where, \( X \) is the original image and \( Y \) is the stego-image

\( I(X,Y) \) is the intersection coefficient between image matrices \( X \) and \( Y \)

\( X \) and \( Y \) are the probability distributions of images \( A \) and \( B \) respectively

If value of intersection coefficient is 1 it signifies perfect match and if the value is 0 it signifies total mismatch.

- **Bhattacharyya Coefficient:**

The Bhattacharyya coefficient measures the similarity between two images by using their probability distributions. The formula for Bhattacharyya coefficient is given by:

\[
BC(X,Y) = \sum_{i=1}^{N} \sqrt{X(i)Y(i)}
\]

Where, \( A \) is the original image and \( B \) is the stego-image

\( BC(A, B) \) is the Bhattacharyya coefficient between image matrices \( A \) and \( B \)

\( X \) and \( Y \) are the probability distributions of images \( A \) and \( B \) respectively

If value of Bhattacharyya coefficient is 1 it signifies perfect match and if the value is 0 it signifies total mismatch.

- **Universal Image Quality Index (UIQI):**

UIQI is used to measure the changes in stego-image with respect to the cover-image. In this measure the comparison of the images is broken down into three comparisons: luminance (L), contrast (C) and structural comparison (S).

\[
L(X,Y) = \frac{2\mu_X\mu_Y}{\mu_X^2 + \mu_Y^2}
\]

\[
C(X,Y) = \frac{2\sigma_X\sigma_Y}{\sigma_X^2 + \sigma_Y^2}
\]

\[
S(X,Y) = \frac{\sigma_{XY}}{\sigma_X + \sigma_Y}
\]

\[
UIQI(X,Y) = L(X,Y) \times C(X,Y) \times S(X,Y)
\]

Where, \( X \) is the original image and \( Y \) is the stego-image

\( \mu_X \) is the mean of matrix \( X \)

\( \mu_Y \) is the mean of matrix \( Y \)

\( \sigma_X \) is the standard deviation of matrix \( X \)

\( \sigma_Y \) is the standard deviation of matrix \( Y \)

\( \sigma_{XY} \) is the covariance between matrices \( X \) and \( Y \)

B. **Robustness Analysis**

Robustness analysis is performed to measure the quality of image after implementation of particular technique. The parameters used for analysis of robustness are given below:

- **Mean Square Error (MSE):**

This parameter is a quantitative representation of the error that occurs in the final stego-image with respect to the original image. For a colour image MSE is given by:

\[
MSE = \frac{1}{M \times N} \sum_{c=1}^{3} \sum_{x=1}^{N} \sum_{y=1}^{M} (F^c(X,Y) - F^c (X, Y))^2
\]

Where, \( M \times N \) is the size of image (height and width respectively)

\( C=1 \) to \( 3 \) denotes the Red, Green and Blue colour plane respectively

\( F^c(X, Y) \) = value of pixel at position \((X, Y)\) in \( c \) colour plane of cover image

\( F^c (X, Y) \) = value of pixel at position \((X, Y)\) in \( c \) colour plane of stego-image

- **Mean Absolute Error (MAE):**

MAE is the average of absolute errors between the cover image and the stego-image. For a colour image the formula for MSE is given by:

\[
MAE = \frac{1}{M \times N} \sum_{c=1}^{3} \sum_{x=1}^{N} \sum_{y=1}^{M} |F^c(X,Y) - F^c (X, Y)|
\]

Where, \( M \times N \) is the size of image (height and width respectively)

\( C=1 \) to \( 3 \) denotes the Red, Green and Blue colour plane respectively

\( F^c(X, Y) \) = value of pixel at position \((X, Y)\) in \( c \) colour plane of cover image

\( F^c (X, Y) \) = value of pixel at position \((X, Y)\) in \( c \) colour plane of stego-image
• **Peak Signal to Noise Ratio (PSNR):**

PSNR is the most commonly used parameter to measure the quality of image after embedding. Higher the PSNR value, higher the robustness of the stego-image. PSNR value is most commonly defined in terms of MSE. The formula for PSNR is given as:

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

Where MAX is the maximum value of a pixel in the image. It is 255 for colour image of 8 bits.

VI. RESULTS

A. **Robustness**

Robustness of a steganography technique can be measured by calculating the PSNR, MSE and entropy of stego image with respect to original image.

• **PSNR**

Peak signal to noise ratio shows the changes of original message with respect to the stego Image. As per result observation the best results shows by LSB and LSB Secret Key Steganography Techniques. This is shown in figure 7.

![Fig.7. Comparison of PSNR](image)

• **MSE**

MSE shows the quantitative representation of the error that occurs in the final stego-image with respect to the original image. This is shown in figure 8.

• **Entropy**

Entropy is important factor in terms of robustness. It shows that the probability of occurrence of pixels in encrypted image should be equal to the original plain image. So the maximum value of entropy is provided by the Status bit. This is shown in figure 9.

![Fig.9. Comparison of Entropy](image)

• **Correlation Coefficient**

This parameter is used to find the linear correlation between two images. Its value must lie between (-1, 1). In this scheme the best results are shown by the LSB and Status bit Steganography technique. This is shown in figure 10.

![Fig.10. Comparison of Correlation Coefficient](image)

• **Intersection Coefficient**

Intersection coefficient of histogram of original and stego image is used to calculate the common number of pixels of same value between two images. The best results are shown by the BPCS and Status bit Steganography techniques. This is shown in figure 11.
Performance Comparison of Steganography Techniques

Fig. 11. Comparison of Intersection Coefficient

• Jaccard Index

This factor is used to find the similarity between cover image and Stego Image. Its value also must lie in between (-1, 1). So the best results are provided by the LSB and BPCS Steganography techniques. This is shown in figure 12.

Fig. 12. Comparison of Jaccard Index

• UIQI

This parameter is used to measure the modifications in stego image with respect to the cover image. The best results shown by the Bpcs steganography and status bit steganography as shown in below.

Fig. 13. Comparison of UIQI

VII. OVERALL COMPARISON

A. PSNR:

Table 6 shows the comparison of PSNR values of all techniques.

Table 6. Comparison of PSNR

<table>
<thead>
<tr>
<th>Image size</th>
<th>BPCS Steganography</th>
<th>Status bit Steganography</th>
<th>LSB Steganography</th>
<th>LSB Secret Key Steganography</th>
</tr>
</thead>
<tbody>
<tr>
<td>256 x 256</td>
<td>68.8033945</td>
<td>70.3607312</td>
<td>70.4184932</td>
<td>70.4297298</td>
</tr>
<tr>
<td>512 x 512</td>
<td>75.1284188</td>
<td>75.5753674</td>
<td>76.5797522</td>
<td>76.2956029</td>
</tr>
<tr>
<td>1024 x 1024</td>
<td>81.2582633</td>
<td>81.8087767</td>
<td>82.6508746</td>
<td>82.1633040</td>
</tr>
</tbody>
</table>

B. MSE:

Table 7 shows the comparison of MSE values of all techniques.

Table 7. Comparison of MSE

<table>
<thead>
<tr>
<th>Image size</th>
<th>BPCS Steganography</th>
<th>Status bit Steganography</th>
<th>LSB Steganography</th>
<th>LSB Secret Key Steganography</th>
</tr>
</thead>
<tbody>
<tr>
<td>256 x 256</td>
<td>0.85652669</td>
<td>0.59842156</td>
<td>0.59051513</td>
<td>0.58898925</td>
</tr>
<tr>
<td>512 x 512</td>
<td>0.19963582</td>
<td>0.18011239</td>
<td>0.14292399</td>
<td>0.15258789</td>
</tr>
<tr>
<td>1024 x 1024</td>
<td>0.48669197</td>
<td>0.42874857</td>
<td>0.35317738</td>
<td>0.39513905</td>
</tr>
</tbody>
</table>

C. Entropy:

Table 8 shows the comparison of Entropy values of all techniques.

Table 8. Comparison of Entropy

<table>
<thead>
<tr>
<th>Image size</th>
<th>BPCS Steganography</th>
<th>Status bit Steganography</th>
<th>LSB Steganography</th>
<th>LSB Secret Key Steganography</th>
</tr>
</thead>
<tbody>
<tr>
<td>256 x 256</td>
<td>5.6819561</td>
<td>5.70831778</td>
<td>5.684018599</td>
<td>5.6837178</td>
</tr>
<tr>
<td>512 x 512</td>
<td>5.7351863</td>
<td>5.74952317</td>
<td>5.736882404</td>
<td>5.7372235</td>
</tr>
<tr>
<td>1024 x 1024</td>
<td>5.7665946</td>
<td>5.78113672</td>
<td>5.767116194</td>
<td>5.7672020</td>
</tr>
</tbody>
</table>
D. Correlation Coefficient:-

Table 9 shows the comparison of Correlation Coefficient values of all techniques.

<table>
<thead>
<tr>
<th>Image size</th>
<th>BPCS Steganography</th>
<th>Status bit Steganography</th>
<th>LSB Steganography</th>
<th>LSB Secret Key Steganography</th>
</tr>
</thead>
<tbody>
<tr>
<td>256 X 256</td>
<td>0.99999810</td>
<td>0.99999831</td>
<td>0.99999819</td>
<td>0.99999813</td>
</tr>
<tr>
<td></td>
<td>116155885</td>
<td>85416594</td>
<td>285453964</td>
<td>0.4591908</td>
</tr>
<tr>
<td>512 X 512</td>
<td>0.99999951</td>
<td>0.99999952</td>
<td>0.99999955</td>
<td>0.99999953</td>
</tr>
<tr>
<td></td>
<td>298750989</td>
<td>35229688</td>
<td>973976529</td>
<td>53833081</td>
</tr>
<tr>
<td>1024 X 1024</td>
<td>0.99999987</td>
<td>0.99999848</td>
<td>0.99999988</td>
<td>0.99999987</td>
</tr>
<tr>
<td></td>
<td>80502577</td>
<td>73720525</td>
<td>509118853</td>
<td>16463776</td>
</tr>
</tbody>
</table>

E. Intersection Coefficient:-

Table 10 shows the comparison of Intersection Coefficient values of all techniques.

<table>
<thead>
<tr>
<th>Image size</th>
<th>BPCS Steganography</th>
<th>Status bit Steganography</th>
<th>LSB Steganography</th>
<th>LSB Secret Key Steganography</th>
</tr>
</thead>
<tbody>
<tr>
<td>256 X 256</td>
<td>0.24835840</td>
<td>0.23154428</td>
<td>0.24835603</td>
<td>0.24835348</td>
</tr>
<tr>
<td></td>
<td>680893925</td>
<td>19046689</td>
<td>49373784</td>
<td>60465022</td>
</tr>
<tr>
<td>512 X 512</td>
<td>0.99388411</td>
<td>0.97536470</td>
<td>0.99388273</td>
<td>0.99388165</td>
</tr>
<tr>
<td></td>
<td>257678549</td>
<td>775934314</td>
<td>850978004</td>
<td>80108865</td>
</tr>
<tr>
<td>1024 X 1024</td>
<td>0.39675645</td>
<td>0.38939569</td>
<td>0.39675627</td>
<td>0.39675606</td>
</tr>
<tr>
<td></td>
<td>302009649</td>
<td>632666965</td>
<td>452248408</td>
<td>75920393</td>
</tr>
</tbody>
</table>

F. Jaccard Index

Table 11 shows the comparison of Jaccard Index values of all techniques.

<table>
<thead>
<tr>
<th>Image size</th>
<th>BPCS Steganography</th>
<th>Status bit Steganography</th>
<th>LSB Steganography</th>
<th>LSB Secret Key Steganography</th>
</tr>
</thead>
<tbody>
<tr>
<td>256 X 256</td>
<td>0.99992834</td>
<td>0.99992787</td>
<td>0.99993178</td>
<td>0.99992940</td>
</tr>
<tr>
<td></td>
<td>898345062</td>
<td>38723726</td>
<td>394441506</td>
<td>831655184</td>
</tr>
<tr>
<td>512 X 512</td>
<td>0.99998164</td>
<td>0.99998158</td>
<td>0.99998340</td>
<td>0.99998248</td>
</tr>
<tr>
<td></td>
<td>163912162</td>
<td>79648375</td>
<td>156047349</td>
<td>33571332</td>
</tr>
<tr>
<td>1024 X 1024</td>
<td>0.99999537</td>
<td>0.99999543</td>
<td>0.99999564</td>
<td>0.99999513</td>
</tr>
<tr>
<td></td>
<td>926377824</td>
<td>16509651</td>
<td>578961153</td>
<td>630288095</td>
</tr>
</tbody>
</table>

G. UIQI

Table 12 shows the comparison of UIQI values of all techniques.

<table>
<thead>
<tr>
<th>Image size</th>
<th>BPCS Steganography</th>
<th>Status bit Steganography</th>
<th>LSB Steganography</th>
<th>LSB Secret Key Steganography</th>
</tr>
</thead>
<tbody>
<tr>
<td>256 X 256</td>
<td>0.99992834</td>
<td>0.99992787</td>
<td>0.99993178</td>
<td>0.99992940</td>
</tr>
<tr>
<td></td>
<td>898345062</td>
<td>38723726</td>
<td>394441506</td>
<td>831655184</td>
</tr>
<tr>
<td>512 X 512</td>
<td>0.99998164</td>
<td>0.99998158</td>
<td>0.99998340</td>
<td>0.99998248</td>
</tr>
<tr>
<td></td>
<td>163912162</td>
<td>79648375</td>
<td>156047349</td>
<td>33571332</td>
</tr>
<tr>
<td>1024 X 1024</td>
<td>0.99999537</td>
<td>0.99999543</td>
<td>0.99999564</td>
<td>0.99999513</td>
</tr>
<tr>
<td></td>
<td>926377824</td>
<td>16509651</td>
<td>578961153</td>
<td>630288095</td>
</tr>
</tbody>
</table>

VIII. CONCLUSIONS

In this paper various steganography techniques has been implemented for confidentiality and security purpose. The human perceptibility of blue plane is known to be very low as compared to any other plane. So, the data hidden in blue plane is considered to be much secure. Therefore, in BPCS technique all the data was embedded in complex noisy blue plane. The embedding capacity of BPCS techniques and LSB techniques is high. On comparison, it is found that the LSB steganography and LSB using secret key perform the best on the basis of PSNR. According to entropy and correlation point of view, the best results are shown by the status bit and BPCS steganography techniques.

REFERENCES

Performance Comparison of Steganography Techniques


Authors’ Profiles

Mr. Rinku Sharma is B.Tech (Electronics and Communication Engineering) and M.Tech (Electronics and Communication Engineering) from YMCA University of science & Technology, Faridabad, India. His academic interests include Image Processing, Encryption, Steganography and Artificial intelligence.

Ms. Reema Ganotra is B.tech (Electronics and Communication Engineering), M.tech (VLSI Design) and pursuing her PhD from YMCA University of Science and Technology, Faridabad, India. Her research interests are image processing and artificial intelligence.

Ms. Sangeeta Dhall is B.Tech (Instrumentation and Control Engineering), M.Tech (Electronics and Instrumentation) and pursuing her Ph. D in the area of network security. Her academic interests include network security, embedded systems and digital system design. Currently working as Assistant Professor in Electronics Engineering department at YMCA University of Science and Technology, Faridabad, India.

Dr. Shailender Gupta is B.Tech (Electronics Engineering), M.Tech (Computer Engineering) and received his Ph. D in the area of ad-hoc mobile network security. His academic interests include network security, Signal Processing, automata theory and fuzzy logic. Currently working as Assistant Professor in Electronics Engineering department at YMCA University of Science and Technology, Faridabad, India.