International Journal of Security and Its Applications
Vol.9, No.8 (2015), pp.67-94
http://dx.doi.org/10.14257/ijsia.2015.9.8.07

An In-depth Analysis of Various Steganography Techniques

Sangeeta Dhall, Bharat Bhushan and Shailender Gupta

YMCA University of Science and Technology
Sangeeta_dhall@yahoo.co.in, bhrts@yahoo.co.in, Shailender81@gmail.com

Abstract

The Steganography is an art and technique of hiding secret data in some carrier i.e. image, audio or video file. For hiding data in an image file various steganography techniques are available with their respective pros and cons. Broadly these techniques are classified as Spatial domain techniques, Transform domain techniques, Distortion techniques and Visual cryptography. Each technique is further classified into different types depending on their actual implementation. This paper is an effort to provide comprehensive comparison of these steganography techniques based on different Performance Metrics such as PSNR, MSE, MAE, Intersection coefficient, Bhattacharyya coefficient, UIQI, NCD, Time Complexity and Qualitative analysis. For this purpose a simulator is designed in MATLAB to implement above said techniques. The techniques are compared based on performance metrics.

Keywords: *Steganography, Classification of Steganography Techniques, Performance Metrics and MATLAB*

1. Introduction

"Steganography is the art and science of communicating in a way which hides the existence of the communication. In contrast to Cryptography, where the enemy is allowed to detect, intercept and modify messages without being able to violate certain security premises guaranteed by the cover message with the embedded cryptosystem. The goal of Steganography is to hide messages inside other harmless messages in a way that does not allow any enemy to even detect that there is a second message present"[1]. That means steganography technique embed the secret message into a cover media that can be image, text, audio or video in such a way that attackers don't have any idea about the original message that the media may contain and also which algorithm is used to embed or retrieve it [6]. In a steganography system there are two entities i.e. cover image and message. The hidden message is called the embedded message. At transmitter side these two are combined using one the algorithms, thus presence of secret message cannot be recognized. This combination thus obtained is termed as stego-message or stego-image. Data type of cover message and stego message must be of the same; however the data type of embedded message may be different. At receiver side reverse steganography algorithm is used to extract the embedded message or secret message [4].

2. Classification of Steganography Technique

Steganography Techniques are classified into many categories based on embedding method used and are described as follows:

2.1. Spatial Domain Technique

In spatial domain steganography techniques image pixels values are converted in binary values and some of the bits are changed for hiding secret data. There are many categories of Spatial domain Techniques which differ mainly on the basis of manipulation

ISSN: 1738-9976 IJSIA
Copyright ⓒ 2015 SERSC

of different bits in pixel values. Least significant bit (LSB)-based technique is one of the simplest and most widely used techniques that inserts or hides the secret message in the LSBs of pixel values without much visual distortion in the cover image. Another technique employs embedding of message bits at randomly chosen pixels [4]. This technique is Pseudorandom LSB [7] in which random pixels are chosen using algorithm where bits of secret data are embed.

2.2 Transform Domain Technique

In transform domain the message is embedded in cover image which is transformed in frequency domain. The message bits are inserted into transformed coefficients of image. Many different transformations can be used for cover image before hiding the secret data [3]. This method of steganography gives more robustness against attacks, as the secret data is stored in image at those areas which are not directly exposed and will remain unchanged after cropping or resizing of image.

2.3 Distortion Technique

In this technique, information is stored by changing value of the pixel that is termed as distortion. The signal distortion is provided by introducing deviation in the pixel value for embedding secret data. At the receiver side the same deviation is used for retrieving hidden data from the image. The original image is the fundamental requirement at the receiver side to retrieve the secret data. The deviation between original image and stego image is used to recover data [8][9].To implement this method certain modifications are applied to the cover image. The secret message bits are inserted in pixels in cover image which are chosen pseudo-randomly. During retrieval process the original image and stego-image are compared. If the value of pseudo-randomly chosen pixel is different the message bit is logic 1 otherwise it is logic 0.

2.4 Visual Cryptography (VC) Technique

Instead of using image directly to embed data, it is broken into two or more parts called shares. Message is broken into bits and inserted into shares which in turn are transmitted via different paths. An intruder can't recover complete until data all the shares are received and combined in particular order. At the intended receiver side all the shares are received and stacked to recover the original data. Thus this technique provides a simple and robust method to embed data.

3. Algorithms

In this section algorithms to evaluate performance of above techniques based on different performance metrics are given:

3.1 Spatial Domain Technique

3.1.1 Least Significant Bit Substitution Technique (LSB): In this technique, the LSBs of the pixel values of cover image are modified according to bits of message. The simplest of LSB steganography techniques is LSB replacement for all pixels of image. Since only LSB is changed, difference between the cover (i.e. original) image and the stego-image is hardly noticeable.

Advantages:

- The picture quality of cover image is hardly affected.
- Hiding capacity is good.
- Very simple in implementation.

 Copyright ⓒ 2015 SERSC

Disadvantages:

- Robustness is less; the hidden data is subject to alternation due image manipulation.
- Detection of secret data is easy because of easy algorithm.
- More information storage requires large image size thus requires high transmission rate due to large size of stego image.

Embedding Algorithm:

Step 1: Read the cover image and secret message.
Step 2: Break message in bits called secret bits. The message to be written can be available in either text message or binary data. Text message is required to be converted to binary value first and then it can be embedded into cover image.
Step 3: Image is converted to matrix of pixels where each pixel value can be accessed. Each pixel value in decimal form is converted to binary and then its LSB is accessed.
Step 4: Each secret bit is checked sequentially. As per the value of bit, LSB of pixel will be modified. LSB of pixel of cover image is modified by each bit of secret message in sequence.
Step 5: This modified pixel value is fed back to its respective position. As per the size of message data LSBs of image pixels are modified.
Step 6: Write stego image.
Step 7: Performance evaluation of the stego-image is carried out.

Algorithm to Retrieve Text Message:

Step 1: Obtain the stego image in matrix of pixels values.
Step 2: Access the LSB of pixel of stego image containing data. These bits are combined to form bytes and bytes are combined to form the complete message data. For this step each pixel value of stego image is converted to binary and then its LSB is accessed which is secret bit.
Step 3: Retrieve bits and convert each set of 8-bits into character i.e. text message. This is required secret information.

3.1.2 Pseudo-Random LSB Encoding Technique: In this technique, a random-key is used to choose the pixels randomly where message bits will be stored. This will make the message bits more difficult to find for an intruder. Moreover the coloured image has three planes (RGB). The data can be hidden in the LSB of any colour plane of the randomly selected pixels [10]. With the use of this technique it will be difficult for the attacker to identify the pattern in which message bits are hidden, as no particular pattern is followed for embedding subsequent message bits. At transmitter side a random key is used to randomized the cover image and embed the message bits into the LSB of the pixels. The transmitting and receiving end share the random-key. This random-key is used as a seed for pseudo-random number generator for selecting pixel locations in an image for hiding the secret message bits.

Advantages:

- Degradation of cover image will be very low as the pixels identified are at distant from one another.
- Embedding capacity is good.
- Simple to implement.

Copyright ⓒ 2015 SERSC

Disadvantages:

- Access to key *i.e.* seed, can easily detect the location of pixels in cover image, and thus easily reveal the secret message.
- More information storage requires large image size thus requires high transmission rate due to large size of stego image.

Embedding Algorithm:

Step 1: Get the cover image and secret message.
Step 2: Break the message into bits. The message to be written can be available in either text message or binary data. Text message is required to be broken in bits before embedding it in cover image, but the binary data can be directly embedded.
Step 3: Initialize the random key and randomly identify the pixels of cover image. This random key is basically a seed which is used to generate same set of random values every time that random number generator command is used.
Step 4: LSB of randomly located pixels will be modified as per the values of message bits. First of all the message are inserted at the LSB of the Red plane's pixels. Later on process is repeated in green and blue planes.
Step 5: This modified pixel value is fed back to its respective position. As per the size of message data LSBs of image pixels are modified.
Step 6: Write stego image.
Step 7: Performance evaluation of the stego-image is carried out.

Algorithm to Retrieve Text Message:

Step 1: Input the stego image.
Step 2: Initialize the random key and randomly identify the pixels of cover image. This random key is basically a seed which is used to generate a same set of random variables, every time that random number generator command is used. This random key is same at both ends.
Step 3: Read the LSB of each identified pixel of stego image. These bits are combined to form bytes and bytes combined subsequently to form complete message.
Step 4: Convert each 8 bits into character *i.e.* text message. This is required secret message.

3.2 Transform Technique

3.2.1 DCT Based Steganography: In Discrete Cosine Transform steganography technique, image is converted into frequency domain [12]. This transformation process is divided into four distinct and independent phases.
Phase 1: In this phase, the image is divided into blocks of pixel size of 8 x 8.
Phase 2: Each block is subjected to DCT transformation to convert the information into frequency domain.
Phase 3: The information from step 1 is quantized to remove unnecessary information in frequency domain.
Phase 4: Standard compression technique sare applied to bit pattern [13].
This transformation is mainly used when the stego-image is prone to image modification processes like compression, cropping etc. This explains the reason for storing data in the areas of the image which are not much affected after application of these processes.

Advantages:

- Highly robust, as cover image is subjected to transformation before storing data. Thus data is safe even after application of image modification processes.

 Copyright ⓒ 2015 SERSC

- Less bandwidth requirement for stego-image transmission because its size can be reduced.

Disadvantages:

- As data is to be stored in transformed image so only few secret messages can be embedded in cover image.
- Picture quality is very much deteriorated which gives information regarding presence of message in cover image.

Embedding Aalgorithm:

Step 1: Get the cover image and secret message.
Step 2: Convert the pixel values of text data in bits. The binary data can be directly embedded.
Step 3: The cover image is broken into blocks of size 8×8 pixels. In case the block of pixels is undersized (less than 8 x 8) it is padded with extra pixels to make it a block of standard size.
Step 4: All the block of image are converted to frequency domain using DCT technique. The top left value in the block is the DC value which is average of the entire block. It is the lowest frequency cosine coefficient.
Step 5: Each block is subjected to quantization using standard quantization table. For carrying out this compression each coefficient is divided by predefined constant in Quantization table, and then rounding off the value.
Step 6: LSB of each DC coefficient modified as per value of message bits.
Step 7: Calculate inverse DCT of modified blocks and multiply with quantization table and reconstruct the image *i.e.* stego image.
Step 8: Performance evaluation of the stego-image is carried out.

Algorithm to Retrieve Text Message:

Step 1: Get the stego image.
Step 2: The image is broken into blocks of size 8×8 pixels. In case the block of pixels is undersized (less than 8 x 8) it is padded with extra pixels to make it a block of standard size.
Step 3: All the block of image are converted to frequency domain using DCT technique. The top left value in the block is the DC value which is average of the entire block. It is the lowest frequency cosine coefficient.
Step 4: Each 8x8 sized block is compressed using quantization table.
Step 5: Read the LSB of each DC coefficient. These bits are combined to form complete message.

3.2.2 DWT Based Steganography: Discrete Wavelet Transform (DWT) steganography is another frequency domain transformation proposed by Haar [15].This technique is divided into two operations i.e. horizontal operation and vertical operation. Various step of the procedure are as follows:
Step1: The pixels in a row are scanned in from left to right and addition &subtraction operations are performed on neighbouring pixels. On left hand side summation of the pixels is stored and on the right hand side difference value is stored. This process is repeated for all the rows. The addition of pixels gives the low frequency component and the difference of pixels gives the high frequency component of the original-image.
Step2: The pixels are scanned in column in vertical direction from top to bottom. The sum and difference is calculated on neighbouring pixels. The summation of pixels in

Copyright ⓒ 2015 SERSC

column is stored at top and difference value is stored at the bottom. This process is repeated for all the columns. The information is converted into four sub-bands termed as LL, HL, LH, and HH. The LL sub-band looks very similar to the original image as it is the low frequency portion [15].

Advantages:

- Highly robust, as cover image is subjected to transformation before storing data. Thus data is safe even after application of some signal processing and noises.
- Embedding capacity is very high.

Disadvantages:

- Complexity of this technique is high
- Speed is slower due to long process.

Embedding Algorithm:

Step 1: Read the cover image and secret message.
Step 2: Convert the text message into bits. The binary data can be directly embedded.
Step 3: Convert the coloured image into gray scale image and apply Haar-transform.
Step 4: Obtain the horizontal and vertical filtering coefficients of the cover image. Data bits are embedded in LL region of cover image. Randomly chosen pixels are identified for embedding of data bits.
Step 5: Stego image is obtained from after application of inverse DWT transform on the cover image.
Step 6: Performance evaluation of stego image is carried out.

Algorithm to Retrieve Text Message:

Step 1: Get the stego image.
Step 2: Calculate the horizontal and vertical filtering coefficients of the cover image. Retrieve the secret message bits are from the cover image bit by bit.
Step 3: These secret data bits are converted into message vector and then compared with original message.

3.3 Distortion Technique

This technique is modification of LSB substituting technique. In this technique modification in LSB of pixel value is done if value of secret bit is 1 else pixel value will remain unchanged which is unlike LSB technique in which every pixel value irrespective of 0 or 1 will modify pixel value[14]. It uses an approach similar to Pseudorandom LSB in which different cover-pixels are used for information hiding. A Pseudorandom number generator is used to make this selection. To embed bit 1, a random value x is added or subtracted from pixel's value. The value of x is so chosen that minimum change in cover image occurs. On receiver side the stego-image is compared with the original cover image. If the pixel differs, the corresponding message bit is 1, otherwise bit is 0**.**

Advantages:

- Cover image will be very little modified thus shows no visual difference from stego-image.
- Embedding capacity is good.
- Simple to implement and involves very little complexity.

 Copyright ⓒ 2015 SERSC

Disadvantages:

- Original image is required at receiver side for retrieving the stored information, thus needs to be sent with stego-image.
- In case attacker retrieves original cover image also, retrieval of message is easily detected.
- Requirement of high transmission rate due to large size of images.

Embedding Algorithm:

Step 1: Get the cover image and message.
Step 2: Convert the text message into bits. The binary data can be directly embedded.
Step 3: Initialize the random key and randomly identify the pixels of cover image. This random key is basically a seed which is used to generate same set of random values every time that random number generator command is used.
Step 4: Each message bit is checked sequentially. As per the status of it i.e. 0 or 1, LSB of randomly located pixel will be modified as per given scheme:
(i) If secret bit=1 then;
(ii) Pixel value is checked, if pixel value < 128;
(iii) Increase pixel value by x where x=1.
(iv) If pixel overflows (value>=128), decrease pixel value by x.

Insert the message bits in the LSB of the Red plane's pixels. The process is repeated for in green and blue planes.

Step 5: This modified pixel value is fed back to its respective position. As per the size of message data LSBs of image pixels are modified.
Step 6: Write stego image.
Step 7: Performance evaluation of stego image is carried out

Algorithm to Retrieve Text Message:

Step 1: Get the stego image.
Step 2: Initialize the random key and randomly identify the pixels of cover image. This random key is basically a seed which is used to generate same set of random values, every time that random number generator command is used. This random key is same at both ends.
Step 3: Calculate difference of pixel value of each identified pixel of stego image and cover image. The secret message bit is retrieved as per following scheme:
(i) If difference=0, then secret bit=0;
(ii) Otherwise if difference=1, then secret bit=1;
Step 4: Retrieve bits and convert set of 8 bits into character i.e. text message. This is required secret information.

3.4 Visual Cryptography Technique

This technique is applicable to binary images. It creates two shares of image i.e. share 1 and share 2, so that secret message cannot be retrieved with the help of single share. In this paper firstly the cover image is broken into two shares and then secret message is stored inside both shares of the image.

Advantages:

- Secret message cannot be retrieved unless all the shares are available.
- Very simple to implement.

Copyright ⓒ 2015 SERSC

Disadvantages:

- Complete deterioration of the cover image due to division into shares.
- Applicable only on binary images.

Embedding Algorithm:

Step 1: Procure the cover image and message.
Step 2: Convert the pixel values of text data in bits. The binary data can be directly embedded.
Step 3: The cover image is converted into binary image, so that it can be split in two shares.
Step 4: A random matrix of same size as cover image is generated, which is considered as share 1.
Step 5: As per the value of bit of cover image i.e. 0 or 1, second random matrix is formed and is termed as share2. If pixel value is 1, pixel value of new matrix is same as share1, if pixel value is 0; the pixel value of new matrix is compliment of share 1.
Step 6: The secret data bits are embedded in both shares using LSB substitution technique. Alternate message bits are stored in both shares for example (2*p) numbered bits in one share and (2*p-1) numbered bits in second share where p=0,1,2,…..length/2. As per size of message data image pixels are modified.
Step 7: Both the shares are sent as stego image.
Step 8: Performance evaluation of stego image is carried out.

Algorithm to Retrieve Text Message:

Step 1: Get the stego image.
Step 2: Both shares are converted to binary images.
Step 3: All the secret message bits are retrieved back from LSB of pixel values of both shares.
Step 4: Now both the share matrices are combined using xor operation to get back the binary cover image.
Step 5: Retrieved bits thus converted into character i.e. text message. This is required secret information.

4. Simulation Set Up

A simulator is designed in MATLAB Version 7.8.0.347 (R2009b) to implement and simulate above mentioned steganography techniques. MATLAB is used because of large number of advanced inbuilt functions for image processing.

4.1. Performance Metrics [6][12]

The performance of the various techniques is evaluated based on various performance metrics which are defined as follows:

4.1.1 Mean Absolute Error (MAE): The MAE represents the mean absolute error between the stego Image and the original image**.**

$$\mathrm{MAE} = \frac{1}{\mathrm{nm}} \sum_{\mathrm{i}=1}^{\mathrm{n}} \sum_{\mathrm{j}=1}^{\mathrm{m}} |\mathrm{f}(\mathrm{i},\mathrm{j}) - \mathrm{y}(\mathrm{i},\mathrm{j})|$$

In the above formula, the mean absolute error is an mean value of the absolute errors,. where f is the pixel value of original image and y is the true value of stego image. Size of image is mxn monochrome image. For coloured images size of image will be mxnx3.

 Copyright ⓒ 2015 SERSC

4.1.2 Mean Square Error (MSE): The MSE stands for cumulative squared error between the stego image and the original image. Lower the value of MSE means lower error. It is defined by the relation given below any m x n monochrome image.

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2$$

For coloured image size of image will be m x n x 3.

4.1.3 Peak Signal Noise Ratio (PSNR): It is defined as the ratio of peak square value of pixels by MSE. It is expressed in decibel. The PSNR is defined as:

$$PSNR = 10.\log_{10}(\frac{{MAX_I}^2}{MSE})$$

Where, MAX_I represents maximum value of pixel of the image. In the images with pixel having 8 bits per sample, its value is 255.

4.1.4 Time Complexity: It is defined as the total processing time on receiver side and transmitter side. In this paper comparison of time consumption by all receiver side processes is taken.

4.1.5 Qualitative Analysis: The cover image may undergo change in pixel values during embedding operation as a result of which the difference may observe in both the images. Thus qualitative visual analysis helps to observe any change in visual quality.

4.1.6 Normalized Color Deviation (NCD): This method is applicable for color images only and is used to measure the degradation in color quality in images.

4.1.7 Normalized Histogram Intersection Coefficient: This performance metric gives count of the same value of pixels between two histograms. If the probability distribution of two images is taken as P and Q respectively, then Normalize Histogram Intersection coefficient is given by

$$I(A,B) = \sum_{i=1}^{N}\min\big(P(i),Q(i)\big)$$

Where A is cover image and B is stego image. The range of value for this coefficient is between 0 to1. Where 0 represents mismatch and 1 represents exactly match

.

4.1.8 Bhattacharyya Coefficient: This performance metric gives approximate measure of amount of overlapping between two statistical samples which are two images in this paper. In other words it measure the relative closeness between two images i.e. cover image and stego image. Bhattacharyya Coefficient is given as

$$BC(A,B) = \sum_{i=1}^{N}\sqrt{P(i)Q(i)}$$

Where P and Q are probability distributions of two images respectively i.e. cover image and stego image.

4.1.9 Universal Image Quality Index (UIQI): In an image, pixels values available at different positions shows different effect on Human Visual System (HVS). If some distortion or changes is introduced in the image, such distortion in image is calculated as a

Copyright ⓒ 2015 SERSC

combination of three factors loss of correlation, contrast distortion and luminance distortion.

Luminance distortion, $L(A,B) = \frac{2\,\mu_A\mu_B}{{\mu_A}^2+{\mu_B}^2}$

Contrast distortion, $C(A,B) = \frac{2\sigma_A\sigma_B}{{\sigma_A}^2+{\sigma_B}^2}$

Loss of correlation, $S(A,B) = \frac{2\sigma_{AB}}{\sigma_A+\sigma_B}$

$$UIQI(A,B) = L(A,B) * C(A,B) * S(A,B)$$

Where A is cover image, μ_A and σ_A are mean and standard deviation, respectively of A.
B is stego image, μ_B and σ_B is mean and standard deviation, respectively of B.
σ_{AB} is covariance between A and B.

4.2 Simulation Setup Parameters: The simulation setup parameters are as given in Table 4.1. A secret message file is common among various steganography techniques.

Table 4.1. Simulation Setup Parameters

Cover image pixel size (N x N x3)	N=64, 128, 192, 256, 320
Secret text file size (kb)	One(1kb)
Image type	Bmp
Simulation Tool	MATLAB 7.8.0.347
Pseudo Random Number Generator	MATLAB rng with seed= 256
Secret data for Steganography	Alphabets A to Z (26)

5. Simulation Results

5.1. Impact on Image Quality

The following results are taken for evaluation of these techniques. The stego-image produced by all the techniques on different cover images given in Figure 5.1 to Figure 5.3. The following inferences can be drawn from the results:

- Visual quality of stego-image produced by spatial domain techniques is better than that of produced by transform domain techniques.
- Distortion, LSB substitution and pseudo-random LSB changes the value of pixel by a small factor, so there is no so much change in perceptual quality of image to detect visual changes i.e. quality of embedded image is not degraded by these techniques.
- DCT has highest effect on the image quality as it changes the pixel by large value.
- DWT applies on the gray scale images. Due to this fact conversion of colour image into gray scale introduces a lot of visual difference in the stego-image.
- Visual Cryptography divides the image into shares after converting the image into binary form, thus visually alters the image completely.

 Copyright ⓒ 2015 SERSC

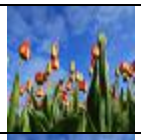
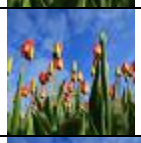
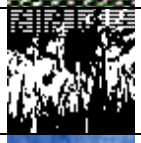
Steganography Technique	Resultant Image
Original Cover Image (without message)	
LSB	
Pseudo-random LSB	
DCT	
DWT	
Distortion	
Visual Cryptography	

Figure 5.1. Image 1 (size = 64x64x3)

Steganography Technique	Resultant Image
Original Cover Image (without message)	
LSB	
Pseudo-random LSB	

Copyright ⓒ 2015 SERSC

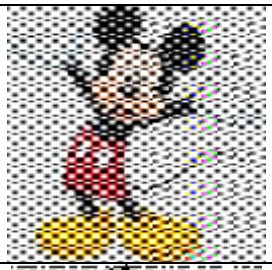
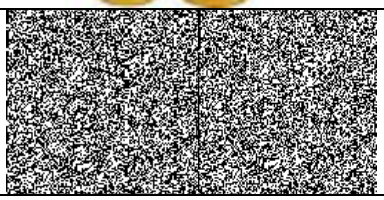
DCT	
DWT	
Distortion	
Visual Cryptography	

Figure 5.2. Image 2 (size = 128x128x3)

Steganography Technique	Resultant Image
Original Cover Image (without message)	
LSB	

Copyright ⓒ 2015 SERSC

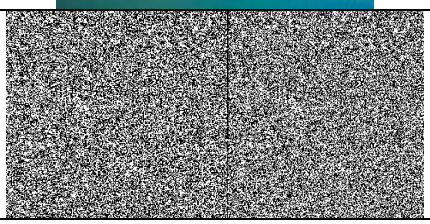
Pseudo-random LSB	
DCT	
DWT	
Distortion	
Visual Cryptography	

Figure 5.3. Image 3 (size = 256x256x3)

5.2 Impact on PSNR

The result of applying various techniques and image size on PSNR are given in Table 5.1 to Table 5.3 and Figures 5.4 to 5.6. The following inferences can be drawn from the results:

- PSNR is highest for distortion technique and minimum for DCT technique.
- Spatial domain techniques have high signal to noise ratio in comparison to DCT transform technique but lower than DWT transform technique.
- VC technique have PSNR value lower than spatial and DWT Technique but higher than DCT transform technique.

Copyright ⓒ 2015 SERSC

Table 5.1. PSNR v/s Image Size for Image 1

Image Size	LSB Technique	Pseudo-Random LSB	DCT Technique	Distortion Technique	DWT Technique	Visual cryptography Technique	
						Share1	Share2
64x64	62.72	63.36	27.30	79.03	67.17	55.60	55.60
128x128	68.80	69.09	27.30	81.60	71.58	55.70	55.70
192x192	72.28	72.93	30.35	85.78	75.16	55.80	55.80
256x256	74.89	75.62	32.80	87.08	78.70	55.80	55.80
320x320	76.76	77.24	34.68	90.96	80.00	55.80	55.80

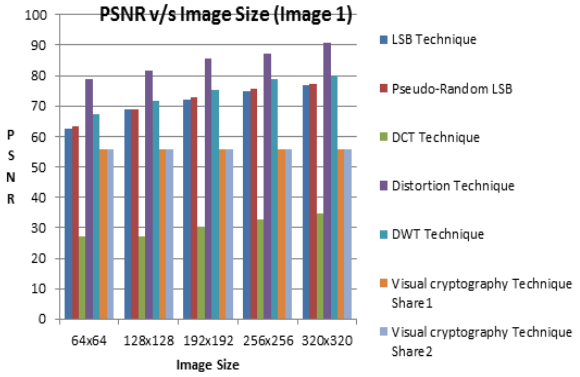


Figure 5.4. PSNR v/s Image1

Table 5.2. PSNR v/s Image Size for Image 2

Image Size	LSB Technique	Pseudo-Random LSB	DCT Technique	Distortion Technique	DWT Technique	Visual cryptography Technique	
						Share1	Share2
64x64	61.34	61.85	27.40	69.68	61.37	51.60	51.50
128x128	66.83	67.75	27.35	75.80	67.14	51.80	51.80
192x192	70.48	70.75	30.50	79.22	70.39	51.90	51.90
256x256	72.87	73.09	33.02	81.72	72.72	51.90	51.90
320x320	74.76	74.98	35.09	83.60	74.60	51.90	51.90

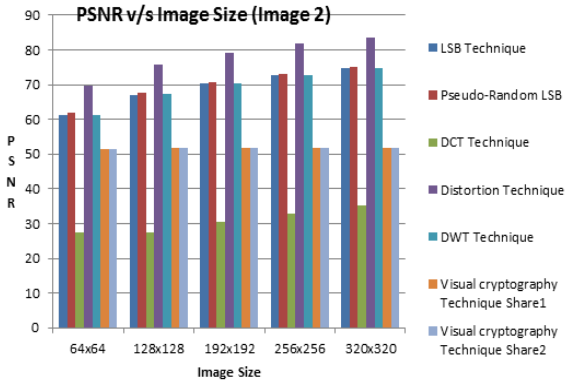


Figure 5.5. PSNR v/s Image 2

Copyright ⓒ 2015 SERSC

Table 5.3. PSNR v/s Image Size for Image 3

Image Size	LSB Technique	Pseudo-Random LSB	DCT Technique	Distortion Technique	DWT Technique	Visual cryptography Technique	
						Share1	Share2
64x64	63.10	63.15	27.22	73.11	62.27	52.70	52.70
128x128	69.51	69.67	27.20	81.20	71.94	52.90	52.90
192x192	72.30	72.87	30.50	83.79	76.31	52.90	52.90
256x256	74.68	75.16	33.02	88.05	81.52	53.00	53.00
320x320	76.99	77.12	35.10	89.00	82.21	52.90	52.90

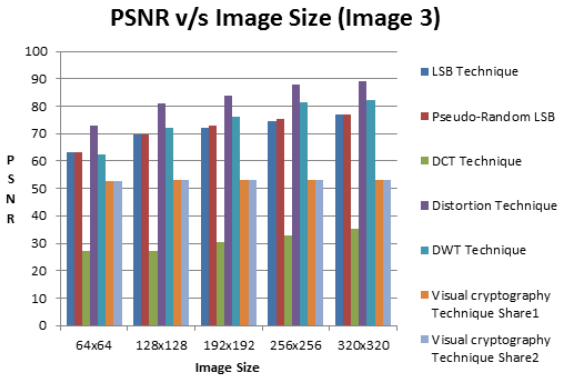


Figure 5.6. PSNR v/s Image 3

5.3 Impact on MSE

The results of applying various techniques and image sizes on MSE are given in Table 5.4 to Table 5.6 and Figure 5.7 to 5.9. From the results the following inferences can be drawn:

- MSE is highest for DCT transform technique. In comparison to this technique MSE for other techniques is very small (negligible).

Table 5.4. MSE v/s Image Size for Image 1

Image Size	LSB Technique	Pseudo-Random LSB	DCT Technique	Distortion Technique	DWT Technique	Visual cryptography Technique	
						Share1	Share2
64x64	0.035	0.029	121.00	8.1e-004	0.013	0.18	0.18
128x128	0.009	0.008	122.00	4.5e-004	0.004	0.17	0.17
192x192	0.004	0.003	59.90	1.7e-004	0.002	0.17	0.17
256x256	0.002	0.002	34.08	1.3e-004	8.7e-004	0.17	0.17
320x320	0.001	0.001	22.12	5.2e-005	6.5e-004	0.17	0.17

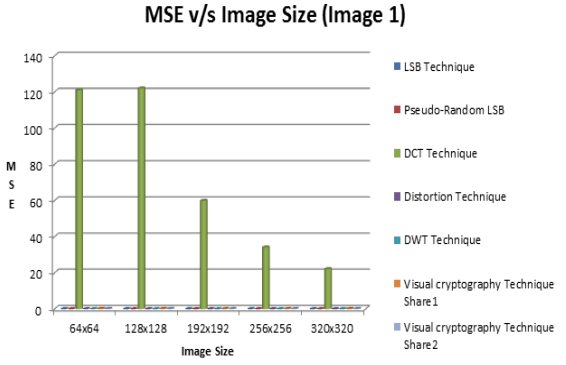


Figure 5.7. MSE v/s Image 1

Table 5.5. MSE v/s Image Size for Image 2

Image Size	LSB Technique	Pseudo-Random LSB	DCT Technique	Distortion Technique	DWT Technique	Visual cryptography Technique	
						Share1	Share2
64x64	0.048	0.042	117.80	0.007	0.050	0.45	0.46
128x128	0.014	0.011	119.40	0.002	0.013	0.43	0.43
192x192	0.006	0.006	57.15	7.7e-004	0.006	0.42	0.42
256x256	0.003	0.003	32.39	4.4e-004	0.004	0.42	0.42
320x320	0.002	0.002	20.12	2.8e-004	0.002	0.42	0.42

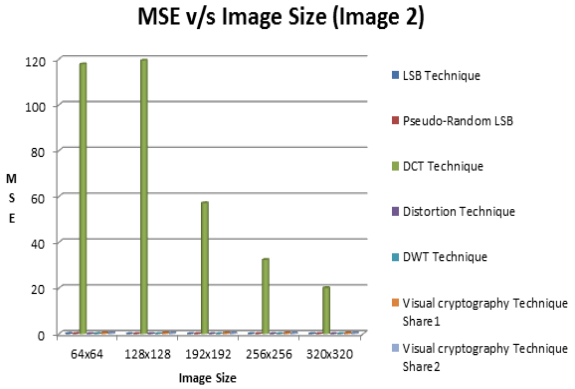


Figure 5.8. MSE v/s Image 2

Table 5.6. MSE v/s Image Size for Image 3

Image Size	LSB Technique	Pseudo-Random LSB	DCT Technique	Distortion Technique	DWT Technique	Visual cryptography Technique	
						Share1	Share2
64x64	0.032	0.035	123.20	0.003	0.039	0.35	0.35
128x128	0.007	0.007	123.10	4.8e-004	0.004	0.33	0.33
192x192	0.004	0.004	57.40	2.8e-004	0.002	0.33	0.33
256x256	0.002	0.002	32.40	1.0e-004	4.6e-004	0.32	0.32
320x320	0.001	0.001	20.08	8.1e-005	3.9e-004	0.32	0.32

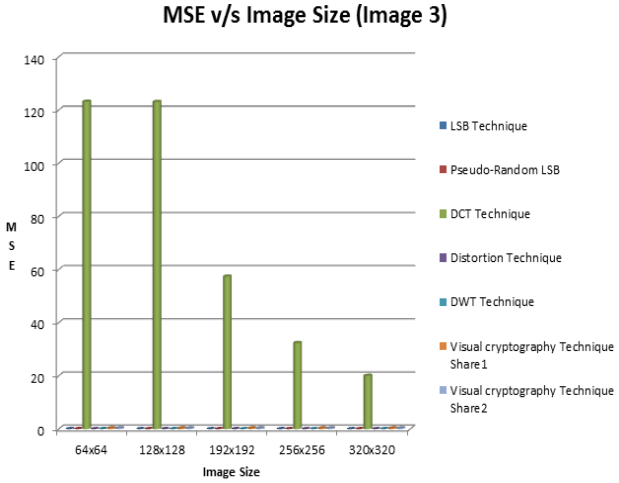


Figure 5.9. MSE v/s Image 3

5.4 Impact on MAE

The results of applying various techniques and image sizes on MAE are given in Table 5.7 to 5.9 and Figure 5.10 to 5.12. From the results the following inference can be drawn:

Copyright ⓒ 2015 SERSC

- MAE is highest for DCT transform technique. In comparison to this technique MAE for other techniques is very small (negligible).

Table 5.7. MAE v/s Image Size for Image 1

Image Size	LSB Technique	Pseudo-Random LSB	DCT Technique	Distortion Technique	DWT Technique	Visual cryptography Technique	
						Share1	Share2
64x64	0.012	0.011	9.80	2.7e-004	.004	0.06	0.06
128x128	0.003	0.003	9.78	1.5e-004	.002	0.06	0.06
192x192	0.001	0.001	5.40	5.7e-005	6.6e-004	0.06	0.06
256x256	7.0e-004	5.9e-004	3.03	4.2e-005	2.9e-004	0.06	0.06
320x320	4.6e-004	4.1e-004	1.88	1.7e-005	2.2e-004	0.06	0.06

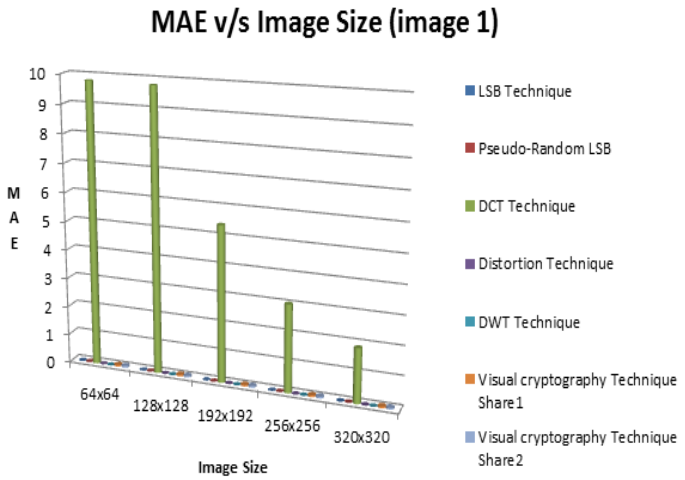


Figure 5.10. MAE v/s Image 1

Table 5.8. MAE v/s Image Size for Image 2

Image Size	LSB Technique	Pseudo-Random LSB	DCT Technique	Distortion Technique	DWT Technique	Visual cryptography Technique	
						Share1	Share2
64x64	0.016	0.013	10.36	0.002	0.150	0.15	0.16
128x128	0.005	0.004	10.43	5.7e-004	0.004	0.14	0.14
192x192	0.002	0.002	6.70	2.6e-004	0.002	0.14	0.14
256x256	0.001	.001	4.20	1.5e-004	0.001	0.14	0.14
320x320	7.2e-004	6.8e-004	2.56	9.3e-005	7.5e-004	0.14	0.14

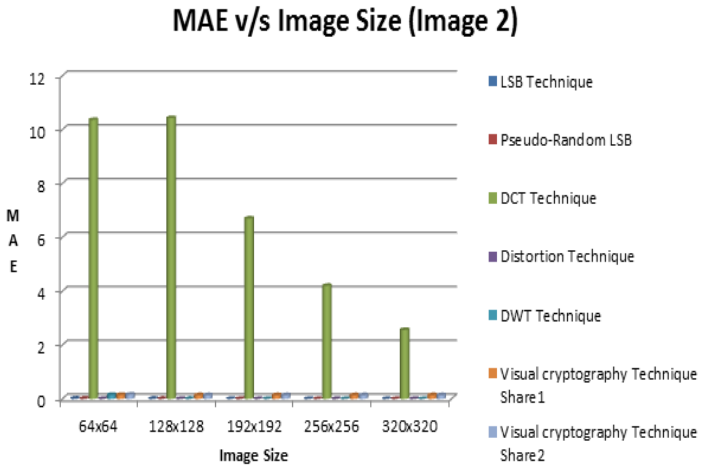


Figure 5.11. MAE v/s Image 2

Copyright ⓒ 2015 SERSC

Table 5.9. MAE v/s Image Size for Image 3

Image Size	LSB Technique	Pseudo-Random LSB	DCT Technique	Distortion Technique	DWT Technique	Visual cryptography Technique	
						Share1	Share2
64x64	0.011	0.011	10.90	0.001	0.012	0.17	0.17
128x128	0.002	0.002	11.01	1.6e-004	0.001	0.11	0.11
192x192	0.001	0.001	5.70	9.0e-005	4.8e-004	0.11	0.11
256x256	7.4e-004	6.5e-004	3.49	3.4e-005	1.5e-004	0.11	0.11
320x320	4.3e-004	4.2e-004	2.29	2.7e-005	1.2e-004	0.11	0.11

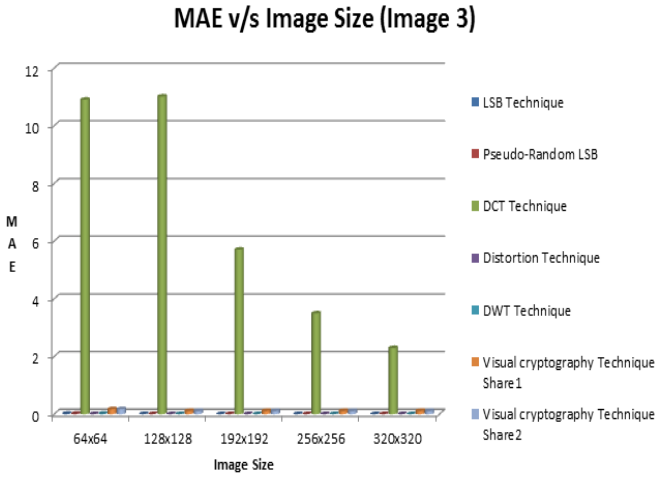


Figure 5.12. MAE v/s Image 3

5.5 Impact on NCD

The results of applying various techniques and image sizes on NCD are given in Table 5.10 to 5.12 and Figure 5.13 to 5.15. From the results the following inference can be drawn:

- Normalized Color deviation is highest in DCT techniques amongst all techniques which works on color Images.
- DWT and VC techniques are used for gray scale, binary images respectively.

Table 5.10. NCD v/s Image Size for Image 1

Image Size	LSB Technique	Pseudo-Random LSB	DCT Technique	Distortion Technique
64x64	2.3e-004	2.5e-004	0.389	5.1e-005
128x128	5.8e-005	6.6e-005	0.387	1.6e-005
192x192	2.37e-005	2.6e-005	0.259	5.9e-006
256x256	1.3e-005	1.2e-005	0.108	2.6e-006
320x320	8.3e-006	9.5e-006	0.063	1.9e-006

Copyright ⓒ 2015 SERSC

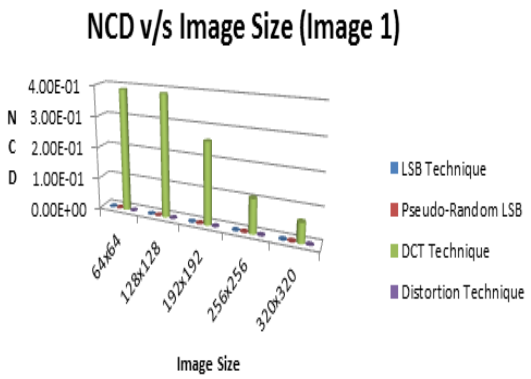


Figure 5.13. NCD v/s Image 1

Table 5.11. NCD v/s Image Size for Image 2

Image Size	LSB Technique	Pseudo-Random LSB	DCT Technique	Distortion Technique
64x64	1.5e-004	1.8e-004	0.232	2.8e-005
128x128	2.9e-005	3.5e-005	0.237	5.1e-006
192x192	1.3e-005	1.0e-005	0.163	2.2e-006
256x256	7.4e-006	7.3e-005	0.078	1.1e-006
320x320	4.3e-006	5.2e-006	0.050	8.7e-007

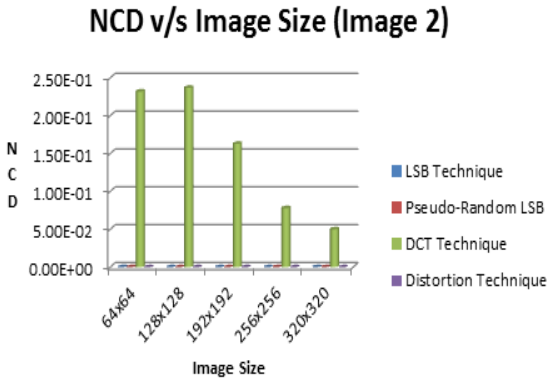


Figure 5.14. NCD v/s Image 2

Table 5.12. NCD v/s Image Size for Image 3

Image Size	LSB Technique	Pseudo-Random LSB	DCT Technique	Distortion Technique
64x64	1.8e-004	1.9e-004	0.350	3.5e-005
128x128	5.3e-005	4.6e-005	0.350	1.2e-005
192x192	2.3e-005	1.9e-005	0.210	3.9e-006
256x256	1.4e-005	1.3e-005	0.087	2.9e-006
320x320	8.6e-006	8.9e-006	0.054	1.8e-006

Copyright ⓒ 2015 SERSC

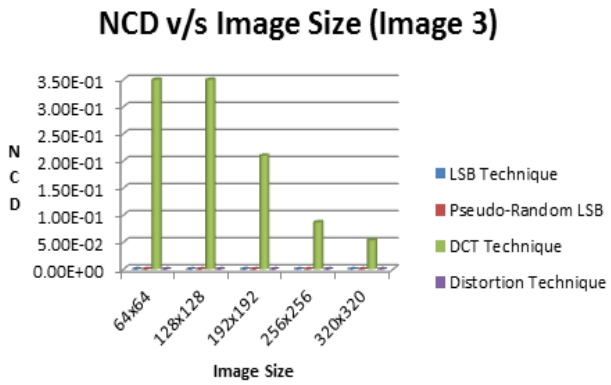


Figure 5.15. NCD v/s Image 3

5.6 Time Complexity

The results of applying various techniques and image sizes on Time Complexity are given in Table 5.13 to 5.15 and Figure 5.16 to 5.18. From the results the following inference can be drawn:

- The time complexity value of VC and DCT techniques increases with increase in image size.
- Time taken by spatial domain techniques remain same for different image sizes.
- For DWT also time taken for embedding information is independent of image size.

Table 5.13. Time Complexity (seconds) v/s Image Size for Image 1

Image Size	LSB Technique	Pseudo-Random LSB	DCT Technique	Distortion Technique	DWT Technique	Visual cryptography Technique
64x64	2.76	3.40	0.55	3.09	1.97	1.68
128x128	2.89	3.49	2.56	3.03	1.87	2.31
192x192	3.22	3.68	5.20	3.12	1.87	2.98
256x256	3.55	3.96	9.20	3.45	1.95	4.08
320x320	3.71	4.27	15.00	3.78	1.94	5.54

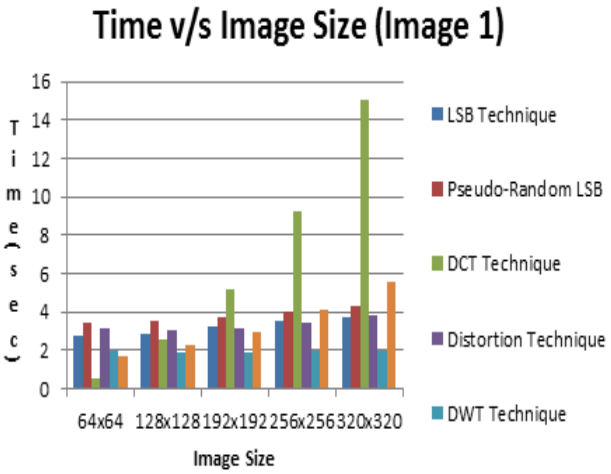


Figure 5.16. Time (sec) v/s Image 1

Copyright ⓒ 2015 SERSC

Table 5.14. Time Complexity (seconds) v/s Image Size for Image 2

Image Size	LSB Technique	Pseudo-Random LSB	DCT Technique	Distortion Technique	DWT Technique	Visual cryptography Technique
64x64	2.84	3.37	0.89	2.97	1.88	1.54
128x128	3.65	3.50	2.60	3.17	2.02	2.03
192x192	3.35	3.60	5.40	3.15	1.90	2.91
256x256	3.78	3.88	9.08	3.38	1.91	3.98
320x320	3.78	4.35	14.00	4.01	1.99	5.98

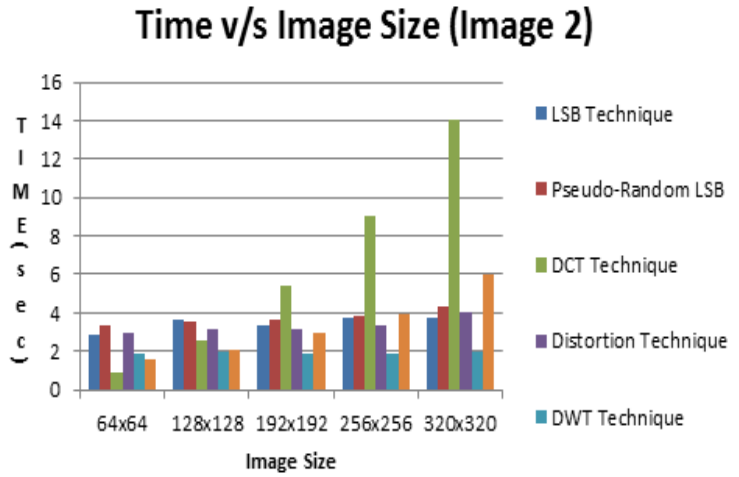


Figure 5.17. Time (sec) v/s Image 2

Table 5.15. Time Complexity (seconds) v/s Image Size for Image 3

Image Size	LSB Technique	Pseudo-Random LSB	DCT Technique	Distortion Technique	DWT Technique	Visual cryptography Technique
64x64	2.87	3.32	0.96	2.85	1.82	1.59
128x128	3.05	2.97	2.55	3.01	1.90	2.07
192x192	3.48	3.75	5.30	3.24	1.92	2.90
256x256	3.80	3.89	9.12	3.45	1.99	4.35
320x320	4.30	4.20	14.03	3.73	2.01	5.64

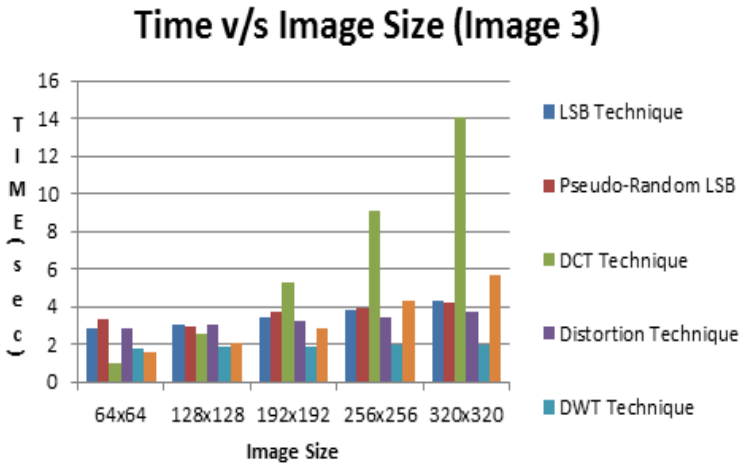


Figure 5.18. Time (sec) v/s Image 3

Copyright ⓒ 2015 SERSC

5.7 Intersection Coefficient

The results of applying various techniques and image sizes on Intersection Coefficient are given in Table 5.16 to 5.18 and Figures 5.19 to 5.21. From the results the following inference can be drawn

- As per the results LSB, Pseudo-random and distortion techniques have highest number of common pixels in both images.
- DWT gives lowest count for the number of common pixels in both images.
- DCT and visual cryptography have almost same number of common pixels.

Table 5.16 Intersection Coefficient V/s Image1

Image Size	LSB Technique	Pseudo-Random LSB	DCT Technique	Distortion Technique	DWT Technique	Visual cryptography Technique	
						Share1	Share2
64x64	0.970134	0.973145	0.569824	0.995524	0.558594	0.859131	0.880615
128x128	0.993184	0.992818	0.57076	0.998922	0.630249	0.851013	0.844849
192x192	0.996917	0.996971	0.745841	0.999439	0.641954	0.844293	0.844374
256x256	0.998332	0.998393	0.85967	0.999725	0.64856	0.838516	0.838547
320x320	0.998877	0.998903	0.884746	0.999827	0.651055	0.839727	0.842012

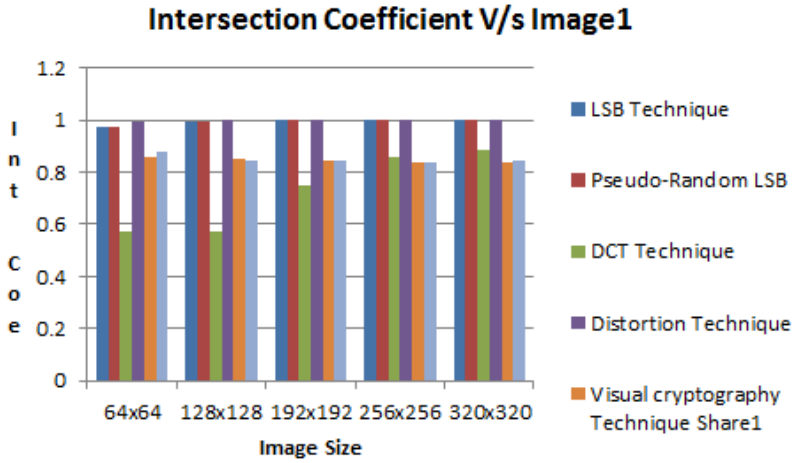


Figure 5.19. Intersection Coefficient V/s Image Size for Image1

Table 5.17 Intersection Coefficient V/s Image2

Image Size	LSB Technique	Pseudo-Random LSB	DCT Technique	Distortion Technique	DWT Technique	Visual cryptography Technique	
						Share1	Share2
64x64	.9553222	.9615071	.6761067	.9951171	.1535764	.6342773	.6306152
128x128	.9873250	.9893798	.6058349	.9985758	.1618652	.6525268	.6557600
192x192	.9943757	.9946017	.7964952	.9993851	.1643066	.6657986	.6632486
256x256	.9968363	.9968668	.8918863	.9996134	.1657867	.6671600	.6671600
320x320	.9979459	.9979752	.9232812	.9997591	.1657226	.6669531	.6664941

Copyright ⓒ 2015 SERSC

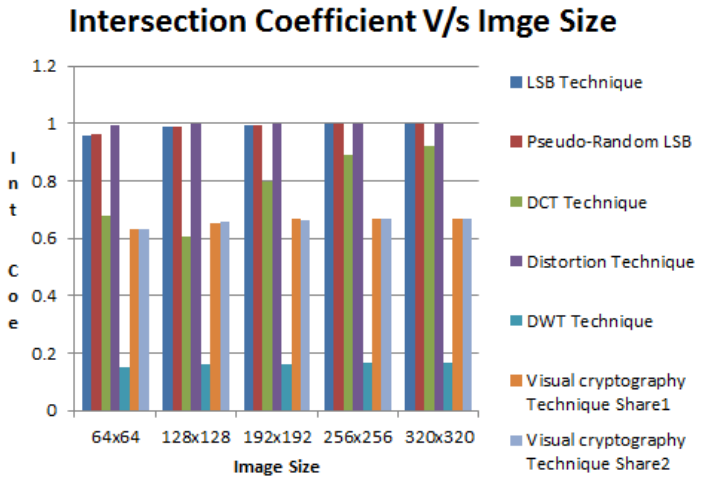


Figure 5.20. Intersection Coefficient V/s Image Size for Image2

Table 5.18 Intersection Coefficient V/s Image3

Image Size	LSB Technique	Pseudo-Random LSB	DCT Technique	Distortion Technique	DWT Technique	Visual cryptography Technique	
						Share1	Share2
64x64	.9709472	.9714355	.5415852	.9952799	.2968750	.8098144	.7978515
128x128	.9932861	.9934692	.5426432	.9989217	.3253784	.8479003	.8380126
192x192	.9969708	.9969437	.7777235	.9994845	.3421418	.8414170	.8421223
256x256	.9982045	.9981943	.8698527	.9996846	.3454323	.8471527	.8445892
320x320	.9989876	.9988574	.9139941	.9998437	.3442285	.8499902	.8512500

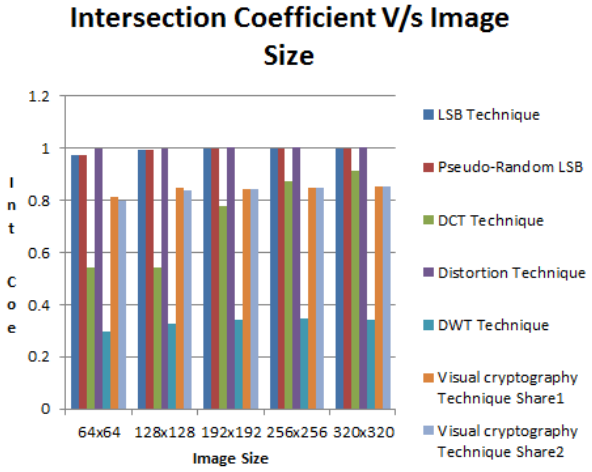


Figure 5.21. Intersection Coefficient V/s Image Size for Image 3

5.8 Bhattacharyya Coefficient.

The results of applying various techniques and image sizes on Bhattacharyya Coefficient are given in Table 5.19 to 5.21 and figures 5.22 to 5.24. From the results the following inference can be drawn

- As per results highest value shows perfect matching which is 1. The values of different techniques tell that in LSB, pseudo-random, distortion, the cover image and stego image are very similar.
- DWT has highest mismatching between two images.
- Coefficient values of visual and DCT are higher than DWT but less than other techniques.

Copyright ⓒ 2015 SERSC

Table 5.19 Bhattacharyya Coefficient V/s Image 1

Image Size	LSB Technique	Pseudo-Random LSB	DCT Technique	Distortion Technique	DWT Technique	Visual cryptography Technique	
						Share1	Share2
64x64	.9988612	.9989540	.8188376	.9999434	.6116189	.9896080	.9924771
128x128	.9999481	.9999450	.8208520	.9999980	.6469348	.9884579	.9875049
192x192	.9999883	.9999895	.9281123	.9999995	.6521008	.9874323	.9874451
256x256	.9999967	.9999971	.9630866	.9999998	.6557749	.9864966	.9866387
320x320	.9999986	.9999986	.9630085	.9999999	.6558708	.9867159	.9870845

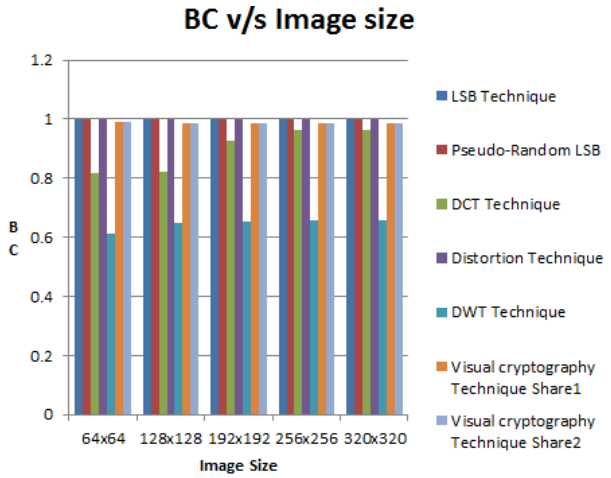


Figure 5.22 BC V/s Image Size for Image 1

Table 5.20 Bhattacharyya Coefficient V/s Image 2

Image Size	LSB Technique	Pseudo-Random LSB	DCT Technique	Distortion Technique	DWT Technique	Visual cryptography Technique	
						Share1	Share2
64x64	.9973912	.9984214	.8666607	.9999573	.1394042	.9224454	.9210213
128x128	.9997081	.9998569	.8321165	.9999971	.1654569	.9293398	.9305290
192x192	.9999415	.9999486	.9659689	.9999993	.1662616	.9340529	.9331392
256x256	.9999802	.9999821	.9888853	.9999997	.1670711	.9345533	.9344446
320x320	.9999911	.9999920	.9944487	.9999998	.1667303	.9344050	.9342414

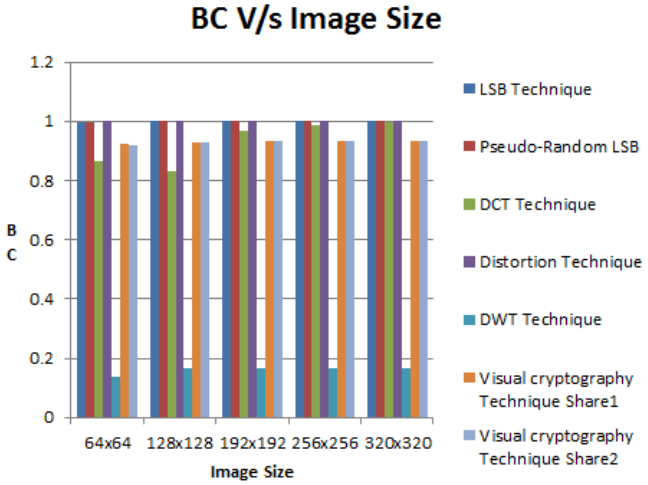


Figure 5.23 BC V/s Image Size for Image 2

Copyright ⓒ 2015 SERSC

Table 5.21 Bhattacharyya Coefficient V/s Image 3

Image Size	LSB Technique	Pseudo-Random LSB	DCT Technique	Distortion Technique	DWT Technique	Visual cryptography Technique	
						Share1	Share2
64x64	.9986174	.9990372	.7812859	.9999501	.3213766	.9814961	.9791250
128x128	.9999301	.9999304	.7906600	.9999966	.3386279	.9881145	.9865460
192x192	.9999828	.9999844	.9163700	.9999992	.3356933	.9870687	.9871815
256x256	.9999936	.9999938	.9615459	.9999997	.3411712	.9879797	.9875801
320x320	.9999978	.9999977	.9776190	.9999999	.3470635	.9884156	.9886060

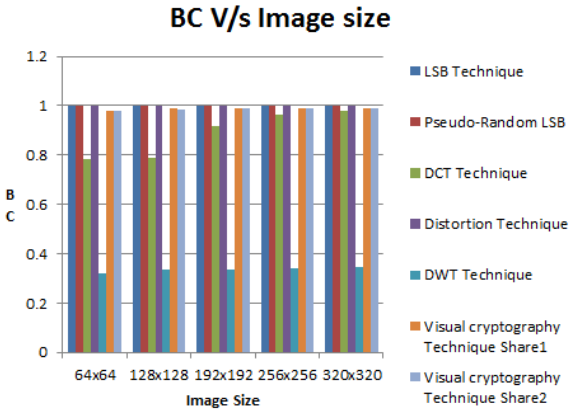


Figure 5.24 BC V/s Image Size for Image 3

5.9 Universal Image Quality Index (UIQI): The results of applying various techniques and image sizes on UIQI are given in Table 5.22 to 5.24 and Figures 5.25 to 5.27. From the results the following inference can be drawn

- As per results image quality index of spatial techniques is highest.
- Image quality index of transform technique DWT is lowest.
- But DCT has index higher than visual cryptography.

Table 5.22 UIQI V/s Image 1

Image Size	LSB Technique	Pseudo-Random LSB	DCT Technique	Distortion Technique	DWT Technique	Visual cryptography Technique	
						Share1	Share2
64x64	.9999979	.9999980	.6487928	.99999958	3.18e-006	.4635831	.4791187
128x128	.9999995	.9999994	.6593037	.99999990	6.47e-006	.4669965	.4582819
192x192	.9999997	.9999998	.8185376	.99999995	1.02e-005	.4621427	.4611564
256x256	.9999998	.9999998	.8874674	.99999997	1.53e-005	.4641268	.4638585
320x320	.9999999	.9999999	.9202664	.99999999	1.85e-005	.4633535	.4655026

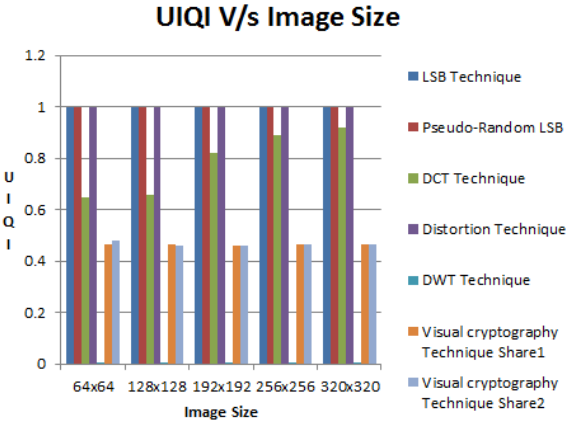


Figure 5.25 UIQI V/s Image Size for Image 1

Copyright ⓒ 2015 SERSC

Table 5.23 UIQI V/s Image 2

Image Size	LSB Technique	Pseudo-Random LSB	DCT Technique	Distortion Technique	DWT Technique	Visual cryptography Technique	
						Share1	Share2
64x64	.9999984	.9999985	.7601711	.99999976	2.39e-006	.4026496	.3874327
128x128	.9999995	.9999996	.7537316	.99999993	5.06e-006	.4172347	.4073946
192x192	.9999997	.9999998	.8759934	.99999997	8.92e-006	.4199942	.4214323
256x256	.9999998	.9999998	.9279633	.99999998	1.23e-005	.4230498	.4221908
320x320	.9999999	.9999999	.9520567	.99999999	1.43e-005	.4226383	.4224801

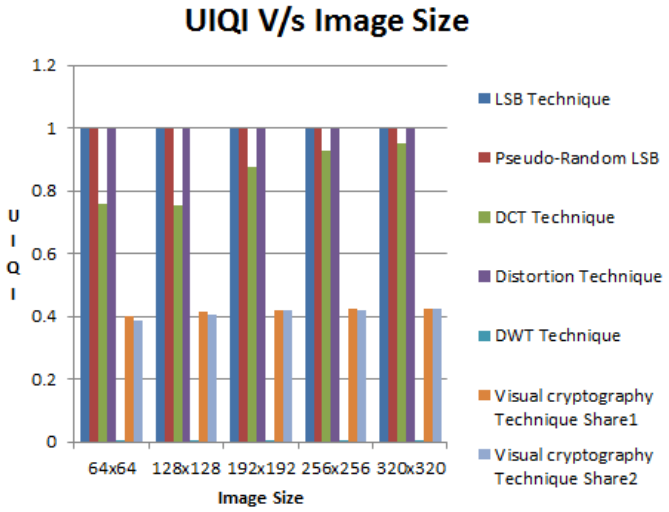


Figure 5.26 UIQI V/s Image size for Image 2

Table 5.24 UIQI V/s Image 3

Image Size	LSB Technique	Pseudo-Random LSB	DCT Technique	Distortion Technique	DWT Technique	Visual cryptography Technique	
						Share1	Share2
64x64	.9999979	.9999979	.6578805	.99999959	2.90e-006	.4674235	.4719051
128x128	.9999995	.9999995	.6585090	.99999989	7.15e-006	.4790128	.4871867
192x192	.9999997	.9999997	.8013528	.99999995	9.61e-006	.4810703	.4791255
256x256	.9999998	.9999998	.8801965	.99999997	1.42e-005	.4799667	.4818466
320x320	.9999999	.9999999	.9203912	.99999998	1.81e-005	.4857491	.4839870

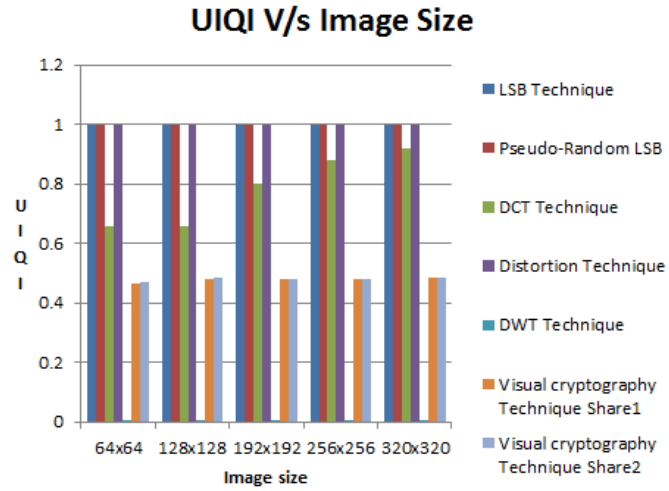


Figure 5.27 UIQI V/s Image Size for Image 3

6. Conclusion

- Spatial domain techniques are very simple to implement yet these are sensitive even small image changes.

Copyright ⓒ 2015 SERSC

- Applying signal processing techniques can entirely shuffle the secret information. This may result in total information loss.
- Transform domain methods hide messages in significant areas of the cover image and are therefore robust and less sensitive to small changes in the image.
- The spatial domain techniques provide high PSNR, high perceptual quality and low errors but not provide robustness. On the other hand transform domain provide robustness while providing low PSNR and low perceptual quality**.**
- As per the given graphs DCT has highest MSE, MAE and NCD and lowest PSNR.
- Amongst all technique Distortion steganography has highest PSNR and lowest MSE, MAE and NCD. LSB and Pseudo-LSB has almost same graphs.
- Amongst DWT and VC which are used for gray scale images, DWT has higher PSNR and lower MSE and MAE.
- As per results shown by different parameters it is clearly concluded that spatial techniques have highly matched stego image with respect to cover image.

References

[1] B. Saha and S. Sharma, "Steganographic Techniques of Data Hiding using Digital Images", in Defence Science Journal, vol. 62, no. 1, (**2012**) January, pp. 11-18.
[2] W. Bender, D. Gruhl and N. Morimoto, "Techniques for data hiding", IBM Systems Journal, vol. 35, no. 34, (**1996**), pp. 131-336.
[3] F. S. Abed, "A Proposed Method of Information Hiding Based on Hybrid Cryptography and Steganography", in International journal of application or innovative in Engineering and management, ISSN 2319 – 4847, vol. 2, no. 4, (**2013**) April, pp. 530-539.
[4] Z. Kh. AL-Ani, A. A. Zaidan, B. B. Zaidan and H. O. Alanazi, "Overview: Main Fundamentals of Steganography", in Journal of Computing, ISSN 2151-9617, vol. 2, no. 3, (**2010**) March, pp. 158-165.
[5] M. Pramanik and K. Sharma, "Analysis of Visual Cryptography, Steganography Schemes and its Hybrid Approach for Security of Images", in IJETAE, ISSN 2250-2459, vol. 4, no. 2, (**2014**) February, pp. 174-179.
[6] S. Singhania, S. Gupta, B. Bhushan and A. Nain, "A Noval Crypto-Stego Technique for Information Security in Communication Networks", in International Journal of Signal Processing, Image Processing and Pattern Recognition, vol. 6, no. 2, (**2013**) April, pp. 87-102.
[7] W. Bender, D. Gruhl and N. Morimoto, "Techniques for data hiding", IBM Systems Journal, vol. 35, no. 34, (**1996**), pp. 131-336.
[8] M. T. Sandford, J. N. Bradley, and T. G. Handel, "Data Embedding Method," in Proceedings of the SPIE 2615, Integration Issues in Large Commercial Media Delivery Systems, (**1996**), pp. 226-259
[9] Johnson, N. F., and S. Jajodia, "Exploring Steganography Seeing the Unseen, IEEE Computer , vol. 31, no. 2, (**1998**), pp. 26-34.
[10] J. Hossain, "Information-Hiding Using Image Steganography with Pseudorandom Permutation", Bangladesh Research Publications Journal, ISSN: 1998-2003, vol. 9, no. 3, pp. 215-225, (**2014**) January-February, pp. 215-225.
[11] S. Goel, A. Rana and M. Kaur, "A Review of Comparison Techniques of Image Steganography" IOSR Journal of Electrical and Electronics Engineering (IOSR-JEEE) e-ISSN: 2278-1676, p-ISSN: 2320-3331, vol. 6, no. 1, (**2013**) May-June, pp. 41-48.
[12] M. Taye and H. Shawky, "A Proposed Assessment Metrics for Image Steganography", International Journal on Cryptography and Information Security (IJCIS), vol. 4, no. 1, (**2014**) March, pp. 1-11.
[13] H. Sheisi, J. Mesgarian and M. Rahmani, "Steganography: Dct Coefficient Replacement Method and Compare with JSteg Algorithm", International Journal of Computer and Electrical Engineering, vol. 4, no. 4, (**2012**) August.
[14] C. P. Sumathi, T. Santanam and G. Umamaheswari, "A Study of Various Steganographic Techniques Used for Information Hiding", International Journal of Computer Science & Engineering Survey (IJCSES) vol. 4, no. 6, (**2013**) December, pp. 9-25.
[15] P.-Y. Chen and H.-J. Lin," A DWT Based Approach for Image Steganography" International Journal of Applied Science and Engineering, ISSN 1727-2394, vol. 4, no. 3, (**2006**), pp. 275-290.
[16] Z. Wang and A. C. Bovik, "A Universal Image Quality Index", IEEE Signal Processing Letters, vol. 9, no. 3, (**2002**) March, pp. 81-84.
[17] V. Asha, P. Nagabhushan and N. U. Bhajantri, "Similarity measures for Automatic defect detection on patterned textures", International Journal of Image processing and vision sciences (IJIPVS), vol. 1, no. 1.

Copyright ⓒ 2015 SERSC

Copyright ⓒ 2015 SERSC