International Journal of Latest Trends in Engineering and Technology
Vol.(9)Issue(3), pp.233-240
DOI: http://dx.doi.org/10.21172/1.93.39
e-ISSN:2278-621X

A COMPARATIVE PERFORMANCE ANALYSIS OF STEGANOGRAPHIC SCHEMES: SLSBS, VLSBS AND MSB-LSB

Indrajit Das[1], Avirup Chowdhury[2] & Avipsa Roy Chowdhury[3]

Abstract: Steganography is one of the most popular security mechanisms which is widely adopted in today's world for secure data communication in multiple domains. Steganography refers to 'concealed writing' where the goal is to veil the existence of data in transit in a cover medium (here image is considered) thereby ensuring data privacy. Three different steganographic schemes; namely Simple Least Significant Bit Substitution (SLSBS), Variable Least Significant Bit Substitution (VLSBS) and Most Significant Bit- Least Significant Bit (MSB-LSB) Substitution schemes are analyzed in this work. A detailed literature survey is rendered in the steganography domain, to investigate some of the widely adopted popular steganographic metrics employed nowadays. Some such metrics like Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) , Normalized Cross Correlation (NCC), Normalized Absolute Error (NAE), Average Difference (AD), Maximum Difference (MD), Structural Content (SC) etc have been computed and investigated for the above mentioned steganographic schemes for comparative performance analysis.
Keywords: Simple Least Significant Bit Substitution (SLSBS), Variable Least Significant Bit Substitution (VLSBS), Most Significant Bit- Least Significant Bit (MSB-LSB) Substitution, Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), Normalized Cross Correlation (NCC).

1. INTRODUCTION

In this era of internet, the transfer and exchange of data has increased tremendously and become a customary affair. Amidst these transfers, nowadays mostly confidential and secret data needs to be migrated from one place to the other. Such private data lure attackers and thus are highly susceptible to attacks. Therefore ensuring data privacy during data transit in internet is of paramount importance nowadays. Popular security schemes like Steganography can thus be adopted under such circumstances to offer higher data confidentiality.

1.1 Steganography

Steganography is the scheme of hiding a secret message that is intended to get dispatched to a communicating entity via a cover medium. The word Steganography has a Greek origin, where Steganos meaning 'covered' and graphie meaning 'writing'. The medium in which the message is incorporated is termed as the cover medium. The ultimate objective of this scheme is to conceal the very existence of the message/data in transit by embedding it within a cover medium.

In this paper we investigate the performance of three Steganographic algorithms; Simple Least Significant Bit Substitution (SLSBS), Variable Least Significant Bit Substitution (VLSBS) and Most Significant Bit- Least Significant Bit (MSB-LSB) Substitution schemes which are also analyzed on the basis of the surveyed image steganographic performance metrics.The rest of the paper is described as follows. In section II a thorough literature review has been conducted in the image steganographic domain. In section III the aforesaid three algorithms are discussed briefly. In section IV overview of image steganographic performance metrics is analyzed and section V puts forth the experimental result. Finally section VI discusses conclusion followed by the reference at the end.

2. LITERATURE SURVEY

Researchers worldwide have already worked in the domain of steganography and thus have employed and devised myriad metrics that evaluate the performance of their proposed methodologies and schemes. In this section, we have put forward some samples of such existent works along with their computed corresponding image steganographic performance metrics.

2.1 Comparative Analysis of Steganographic Algorithms Within Compressed Video Domain[3]

Researchers Tarik Faraj Idbeaa et al., have devised a scheme that can be administered by specifically substituting the host information with the measure of data and such kind of area names are termed as "spatial space." The process can also be alternatively computed by modifying transform co-efficients, this kind of domain is either referred to as "transform domain" or "compressed domain". Among the accessible video pressure gauges, MPEG-2 remains the most considered in light of its

[1] Department of Information Technology, Meghnad Saha Institute of Technology, Kolkata, India
[2] Department of Information Technology, Meghnad Saha Institute of Technology, Kolkata, India
[3] Department of Information Technology, Meghnad Saha Institute of Technology, Kolkata, India

high caliber and the accessibility of the equipment that has assisted this organization. The present examination researches and investigates the proficiency of the utilization of the ebb and flow steganographic calculations in the MPEG-2 packed area.
As far as intangibility is considered, LSB was superior to the BPCS or EPVD calculations. This outcome can thus be credited to the powerlessness of the human eye to recognize a little change; in this manner, both stego casing and reference outline (unique) would seem to be indistinguishable. The BPCS calculation showed higher inserting limit contrasted with the other two calculations. Further, the debasement of the perceptual quality ends up plainly observable due to the expanded number of bits inserted inside every coefficient of low-recurrence. Along these lines, the distinction in quality levels increments when the payload is little. With respect to security, the LSB scheme is secure since it cannot be identified due to the arbitrariness of the scrambling information bits everywhere throughout the host coefficients of the chosen outline.
The performance metrics that were considered here includes the follows:

- Compression Ratio (CR): It refers to the ratio of the number of bits employed to represent the original video to the number of bits used to represent the compressed video.
- Mean Square Error (MSE): The Mean Square Error is used to compute the difference between estimated values (employing an estimator) and the original value of the estimated quantity.
- Peak Signal to Noise Ratio (PSNR): It is quantified as the ratio of the peak signal to the unwanted noise signals that negatively affects the presentation accuracy of the stego image.
- Structural Content (SC): This analyzes the similar regions in both the cover and stego images.

2.2 Performance Analysis of Digital Image Steganographic Algorithm[4]

Researchers N.D. Jambhekar et.al. here have utilized the steganographic technique, the mystery message is embedded such that the message can be extricated without influencing the cover picture, to loose its permeability. The computed variations are calculated cautiously such that no noticeable change is visible in the picture. The scientific methods accessible in cryptography have constraints and thus are subject to mathematical cryptanalysis attacks. Though image steganography is more secure, yet the extraction of the message requires some additional processing time. In this, no steganalysis strategy can remove the message from the cover image without retrieving the best possible stego key.
Here the investigation of spatial-based strategies is completed by pixel picture base utilizing the systems, for example, LSB inclusion, SVD and spread range techniques. In frequency-based methods, DCT, DFT, DWT and IWT steganographic change based strategies are broken down to shroud the mystery message. The cover picture and stego picture are then contrasted thereby discovering the productivity of the steganographic calculations.
It has been discovered that the commotion is higher in utilizing spatial area techniques when contrasted with the recurrence space strategies. Having considered everything, the spatial area strategies are basic and more appropriate; however, the DWT strategy is distortion-less with less clamor and more noteworthy picture quality due to the Average Difference and Structural substance.
Some of the metrics used in this work have been already discussed above, such as Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE), Structural Content (SC). The additional ones are outlined below:

- Normalized Cross-Correlation (NCC): This specific correlation is employed as an effective similarity index to match tasks. This function returns the normalized cross correlation between the calling data series and the argument with the input data series.
- Average Difference (AD): It refers to the discrepancy between the selected pixel values of cover and stego images.
- Normalized Absolute Error (NAE): It effectively analyzes the statistical difference between the cover and stego images. High value implies low quality.
- Maximum Difference- It is the maximum difference between the original image and the produced stego image.

2.3 Steganography based information security with high embedding capacity[5]

In this work, researchers B. Lakshmi Sirishal et al. have embedded two secret images into a good quality cover image having identical sizes. The (t, n) threshold secret sharing scheme is one such popular method of implementing steganography, which has been adopted here. The secret image is distributed among n participants. It is interesting to note that though any t (or more) out of 'n' authorized participants can recover the secret image yet less than t participants cannot recover the secret image. This happens because the generated shadows are based on polynomial equation f(x) and are implanted in the cover images. The secret image is thus reconstructed without any loss in information. However, the LSB substitution scheme is unsuitable for embedding data in a smooth region.
An improvement over the aforesaid scheme can also be executed by embedding (t-1) secret digits. In this process 2*(t-1) digits get embedded. Given any t (t<= n) out of n stego images and key k from the authorized participants, the secret images and the cover image can be reconstructed with no loss of information by using Cramer's rule. The histograms of both cover and stego images are identical with small variations. Hence, the presence of secret image in the cover image will be secure and not easily detected by the unauthorized entities.
For the purpose of evaluation of the undertaken Steganography scheme, the considered metrics include PSNR (Peak Signal to Noise Ratio), MSE (Mean Square Error), NCC (Normalized Cross Correlation) which have been already discussed above and SSIM (Structural Similarity Index) that analyzes image degeneration as perceived pixel changes exhibit strong

interdependencies whenever images are spatially identical. Its magnitude varies in range of -1 to 1 (value is 1 for identical images).

2.4 Performance Evaluation Parameters of Image Steganography Technique[6]

Researchers Anita Pradhan et al., have illustrated certain performance evaluation parameters in this work for different steganographic techniques. Some of the performance evaluation parameters of a steganographic techniques comprises; (i) hiding capacity, (ii) distortion measure and (iii) security. One can evaluate the extent of security offered by their proposed steganographic techniques by evaluating the three above-mentioned parameters. The distortion however is quantified by using various metrics which are Peak Signal to Noise Ratio (PSNR),Mean Squared Error (MSE), Structural Similarity Index (SSIM) and Normalized Cross-Correlation which have been already highlighted above.

2.5 Enhanced Data Concealing Technique to Secure Medical Image in Telemedicine Applications[7]

In this work, researchers G.Vallathan et al. have proposed a model which refers to a hybrid of encryption and steganography schemes to hide patient's private data inside their biomedical images thereby allowing the information to be accessed only by authorized users. The proposed work carries out data embedding scheme in the contourlet coefficient of host image (i.e. CT, MRI, X-ray) in order to get perfect reconstruction in the receiver end. In wavelet based steganographic technique, it is ineffective to capture smooth contours in images and it works only at seizing point incoherence that is identified as one of the major shortcoming of this process. The contourlet transform is a two-dimensional allowance of the wavelet transform possessing a Laplacian pyramid followed by a directional filter bank. The LSB algorithm is used to conceal the data bits in the coefficients of each sub band. Experimental outcomes also designated that the proposed technique can recover the reconstructed image quality with SSIM=1.This method also ensures that diagnosis is possible with watermarked medical image and the concealed data can be retrieved successfully.

The evaluated performance metrics here comprises the Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) and Structural Similarity Index (SSIM).

2.6 A Cost Effective Approach for Securing Medical X-Ray Images using Chebyshev Map[8]

Researchers V. Praneeth Kumar Reddy et.al. in this work have employed an efficient and cost effective solution in order to securely transmit medical X-ray images utilizing the Chebyshev Map which intrinsically employs chaotic maps. In medical images, steganography and digital watermarking are primarily used for safety, which is efficient to hide the patient details within the medical image. However in addition there's a necessity for security within the medical images to nullify attacks. The security aspects in it are, random generator solely depends on seed value and hence key are thus relatively kept less secure. In place of random generator, chaotic maps are conventional to generate the random numbers, which have comparatively more key values to come up with random numbers thereby subsequently increasing the security. So Chebyshev chaotic maps can thus be employed for offering higher security in stego images. For selection of the location, Chebyshev map is utilized to generate the random pixels and the information bits of the character are embedded in the LSB of the selected pixel locations.

The information to be embedded in the cover image i.e. the medical X-ray image includes the patient details and the number of binary bits required to encode the details in ASCII. As the number of bits required for encoding the patient details varies, it becomes essential to mention the message length. Otherwise the random numbers will be generated unnecessarily or else it will be difficult to decode the complete information. It is experimentally concluded here that this approach provides better results than LSB algorithm.

The computed performance metrics in this work are Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR) and Correlation Coefficient

2.7 Stochastic Local Search Combined with LSB Technique for Image Steganography[9]

Researchers Dalila Boughaci et.al. have proposed here an unconventional steganographic methodology where an image is used as a cover file for hiding private information to ensure secret communication. LSB is mainly based on the modification of the least significant bits of each pixel in the image. It is the process of substituting the lower bits of the pixels of the cover image, where bits of secret message replace LSB i.e. eighth bit of some or all bytes inside cover image. The stochastic local Search (SLS) is a local search based meta-heuristic that adopts an initial random solution. Here certain diversification and intensification strategies are associated to locate good quality solutions. For all blocks, a fitness function is computed. If an image block is similar to block message, position search process is stopped for this block and continues for the remaining blocks. Steganography technique for JPEG images only with LSB is not effective as image size increases after inserting information, which facilitates discovery of hidden information. So to improve it, meta-heuristic is added to LSB. Local Search (LS) is thus hybridized with LSB then combining LSB with stochastic local search (SLS). In this work, in the three proposed methods: LSB, LSB+LS, LSB+SLS both image and secret message is decomposed in 4 bits block. Then by applying principle of each method, secret message is inserted in the image. The stego-key is a key generated and encrypted with the AES algorithm.

The evaluated performance metrics here comprises; Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) and the Encoding Time for all proposed schemes.

2.8 Objective Quality Metrics in Correlation with Subjective Quality Metrics for Steganography[10]

Researchers Raniyah Wazirali et.al. did acomparative study between objective quality metrics and subjective quality metrics of Steganography scheme . By employing Steganography scheme, data security can be enhanced in any application domain. Human Visual Evaluation (subjective) methodology is not considered good even though it can measure the imperceptibility of the stego file to determine visual quality. Thus, many objective evaluation metrics have been developed in the long run. Mean square Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) are effective quality assessment parameters. Objective Evaluation evaluates the image quality based mathematical algorithm whereas Subjective Evaluation assesses the image quality based on the human visual capability and characteristics. Objective Evaluation schemes can be classified into two Pixel Differences Measurements and Human Visual Based Measurements. The subjective quality of stego images has been assessed by evaluating Difference Mean Opinion Score (DMOS) which is calculated and normalized to one for comparison with the objective quality metrics. To analyze correlation between objective and subjective evaluation mainly "PSNR" experiment involves hiding same secret message into red, green and blue level of the images using LSB method. The evaluation based on the human vision sensitivity shows that human eyes are more sensitive to green color and less sensitive to blue color. So it is found that objective quality metrics that are driven from the HVS features have better correlation with the subjective assessment compared to standard MSE and PNSR.

The analyzed performance metrics here includes; Peak Signal to Noise Ratio (PSNR), Mean Square Error (MSE) and Structural Similarity Index (SSIM). The next section briefly outlines description and an overview of the image steganographic algorithms as adopted in papers [1-2].

3. OVERVIEW OF IMAGE STEGANOGRAPHIC ALGORITHMS UNDER ANALYSIS

This section furnishes a detailed overview of the proposed steganography algorithms under analysis i.e., Simple LSB, Variable LSB and MSB-LSB schemes undertaken in the research work from papers [1-2]. For implementing steganographic schemes, any cover image format (.jpg, .png etc) is considered which is always converted into.bmp format is since that yields lossless uncompressed version of image. The following section outlines the proposed steganographic schemes in brief.

3.1 Simple Least Significant Bit Substitution (SLSBS) Scheme

The Simple Least Significant Bit Substitution (SLSBS) strategy is an extremely recognizable and a standout amongst the most preparatory steganography schemes that performs substitution of the LSB of each cover picture pixel relative to the implanting message bit. This straightforward substitution state implies that if the message bit is 1 and the comparing LSB of the cover picture pixel where the message bit is to be installed is 0 or vice-versa i.e. at whatever point mismatch happens then only substitution is performed otherwise, the LSB of cover picture pixel stays unaltered. So each cover picture pixel experiences 50% probability of being modified. This scheme is highly popular owing to its simplicity, low computational overhead and its capacity to exchange information safely. Figure 1 represents the original cover image, converted image (.bmp format) and the stego image obtained by applying the SLSBS technique. Figure 2 shows the corresponding histogram representation of the original cover image, converted image (.bmp format) and the stego image.

Fig.1 Original and Stego Image (SLSBS)

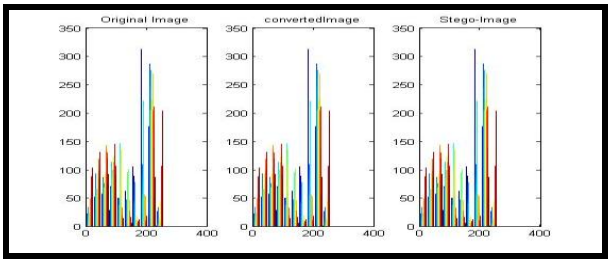

Fig.2 Histogram of Original and Stego Image (SLSBS)

3.2 Variable Least Significant Bit substitution (VLSBS) Scheme

In order to include haphazardness and variation in the embedding data positions in the cover medium, the Variable Least Significant Bit Substitution (VLSBS) scheme utilizes a hashing calculation that arbitrarily maps pixel estimations of cover picture to discrete hash mapped pixel locations every time whenever the message/information bit gets implanted. Thus this scheme offers better data confidentiality as compared to the former SLSBS scheme. Besides it also successfully resists replay attacks.

In the SLSBS scheme, the message bits were being implanted in the cover picture pixels consecutively (from 55th pixel onwards since initial 54 pixels contain fundamental data about picture header, thus needs to remain unaltered). However, in

the VLSBS scheme a hash calculation is utilized that haphazardly maps the cover picture pixels to discrete random locations, unevenly where the actual implanting of message bits is performed. Thus, this scheme consequently offers better security relative to SLSBS scheme. Figure 3 represents the original cover image, converted image (.bmp format) and the stego image obtained by applying the VLSBS technique. Figure 4 shows the corresponding histogram representation of original cover image, converted image (.bmp format) and the stego image.

Fig.3 Original and Stego Image (VLSBS)

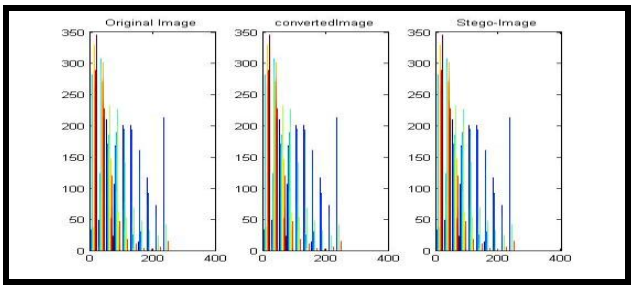

Fig.4 Histogram of Original and Stego Image (VLSBS)

3.3 Most Significant Bit-Least Significant Bit (MSB-LSB) Substitution Scheme

Though SLSBS substitution method is a simple and popular Steganography scheme, yet it can only implant one message/data bit. However, the designed MSB-LSB scheme intelligently utilizes both the MSB and LSB positions of cover picture pixel to substitute message/data, keeping the degree of distortion as 1. Thus this scheme works identical to SLSBS scheme but can implant 2 message bits with very little compromise of the cover picture quality. Figure 5 represents the original cover image, converted image (.bmp format) and the stego image obtained by applying the MSB - LSB technique. Figure 6 shows the corresponding histogram representation of original cover image, converted image (.bmp format) and the stego image respectively.

Fig.5 Original and Stego Image (MSB - LSB)

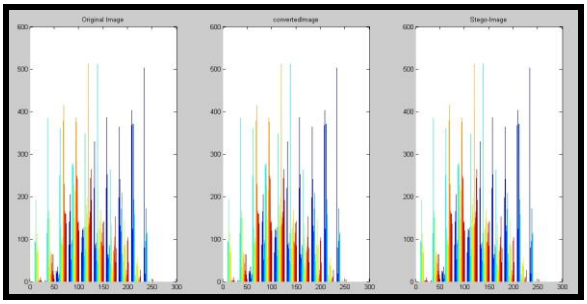

Fig.6 Histogram of Original and Stego Image (MSB - LSB)

The next section enumerates some of the popular image steganographic performance metrics that have been analyzed and computed in this work.

4. ANALYZED IMAGE STEGANOGRAPHIC PERFORMANCE METRICS

In this section, a brief outline and mathematical expressions of some popular image steganographic performance metrics have been highlighted that is being investigated in this paper to estimate the performance of the aforementioned proposed steganographic schemes; Simple Least Significant Bit Substitution (SLBS), Variable Least Significant Bit Substitution (VLSBS) and MSB – LSB Substitution schemes.

4.1 Outline of Computed Image Steganographic Performance Metrics

The image steganographic performance metrics that have been analyzed for comparison of the aforesaid mentioned three steganographic schemes are Mean Square Error, Peak Signal to Noise Ratio, Normalized Cross-Correlation, Average Difference, Structural Content, Normalized Absolute Error and Maximum Difference.

The formula for the aforementioned metrics is given below:

Table -1 Mathematical Expressions of Image Steganographic Metrics

Mean Square Error	$MSE = \frac{1}{MN}\sum_{j=1}^{M}\sum_{k=1}^{N}(x_{j,k} - x'_{j,k})$
Peak Signal to Noise Ratio	$PSNR = 10\log\frac{(2^n-1)^2}{MSE} = 10\log\frac{255^2}{MSE}$
Normalized Cross – Correlation	$NCC = 10\log\frac{(2^n-1)^2}{MSE} = 10\log\frac{255^2}{MSE}$
Average Difference	$AD = \frac{\sum_{j=1}^{M}\sum_{k=1}^{N}(x_{j,k}-x'_{j,k})}{MN}$
Structural Content	$SC = \frac{\sum_{j=1}^{M}\sum_{k=1}^{N}x_{j,k}^2}{\sum_{j=1}^{M}\sum_{k=1}^{N}x'^2_{j,k}}$
Maximum Difference	$MD = Max(\lvert x_{j,k} - x'_{j,k}\rvert)$
Normalized Absolute Error	$NAE = \frac{\sum_{j=1}^{M}\sum_{k=1}^{N}[O(x_{j,k})-O(x'_{j,k})]}{\sum_{j=1}^{M}\sum_{k=1}^{N}[O(x_{j,k})]^2}$

The following section next puts forth the experimental results.

5. EXPERIMENTAL RESULTS

As per the conducted literature survey in section II of this paper, some of the highlighted steganographic metrics (mathematical formulae of which are highlighted in Table 1 above) have been computed here to compare the performance of proposed schemes for analysis purpose. The hardware used is AMD A8, 500 GB Hard Disk and 8
GB RAM. The Software used is MATLAB R2013a (8.1.0.604). Accordingly, a varying data set is considered (Inputs: INDIA - 5 characters, AUSTRALIA - 9 characters, MIAMI -5 characters, MSIT - 4 characters and LONDON - 6 characters) have been simulated here and the corresponding obtained metrics have been enlisted below in Table. 2 and 3. For experiment purpose two different cover image sizes have been adopted here sunset.jpg (19.2 kb) and lenna.jpg (14.7 kb) .

Table -2. Steganographic Metric Computations (Image LENNA)

LENNA.jpg							
INDIA							
	MSE	**PNSR**	**NCC**	**AD**	**SC**	**MD**	**NAE**
SLSB	0.0000078213	102.3059	1	0.0000076294	1	1	0.0000000267
VLSB	0.000006837	99.3182	1	-0.000022231	1	1	0.0000001628
MSB- LSB	0.0000076294	99.3059	1	-0.000022231	1	1	0.0000001994
AUSTRALIA							
SLSB	0.000019127	98.8678	1	-0.000011444	1	1	0.0000007189
VLSB	0.000015259	99.2236	1	0.0000076294	1	1	0.0000001284
MSB- LSB	0.000015259	96.2956	1	0.0000076294	1	1	0.000000123
MIAMI							
SLSB	0.000078223	91.3189	1	0.0000076294	1	1	0.0000001538
VLSB	0.000019073	94.7822	1	-0.0000038147	1	1	0.0000002562
MSB- LSB	0.000019073	95.3265	1	-0.0000038147	1	1	0.00000015375
MSIT							
SLSB	0.00002638	97.5673	1	0.0000020345	1	1	0.0000006782
VLSB	0.000019073	99.3182	1	-0.000003847	1	1	0.0000007842
MSB- LSB	0.000019073	95.3265	1	-0.0000038147	1	1	0.00000015375
LONDON							
SLSB	0.000045776	100.2814	1	-0.000083231	1	1	0.0000003647
VLSB	0.000022888	99.7821	1	-0.000013762	1	1	0.0000002375
MSB- LSB	0.000022888	94.5347	1	-0.000015259	1	1	0.0000001845

Table -3. Steganographic Metric Computations (Image SUNSET)

SUNSET .jpg							
INDIA							
	MSE	**PNSR**	**NCC**	**AD**	**SC**	**MD**	**NAE**
SLSB	0.0000038147	102.3162	1	0.0000038147	1	1	0.00000005562
VLSB	0.000019073	95.3265	1	-0.000011444	1	1	0.0000078475
MSB- LSB	0.00000029769	113.3932	1	-0.000000099229	1	1	0.0000000026349
AUSTRALIA							
SLSB	0.000022888	94.5347	1	0.000022888	1	1	0.00000033375
VLSB	0.0000059537	110.3829	1	-0.000000927	1	1	0.00000782698
MSB- LSB	0.00000059537	110.3829	1	-0.00000039692	1	1	0.0000000052698
MIAMI							
SLSB	0.0000006946	99.3059	1	0	1	1	0.00000011125
VLSB	0.0000029615	111.1747	1	-0.00000078615	1	1	0.00000067915
MSB- LSB	0.00000049615	111.1747	1	-0.00000049615	1	1	0.0000000043915
MSIT							
SLSB	0.0000038147	102.3162	1	0.0000038147	1	1	0.00000055626
VLSB	0.000009625	112.8907	1	0.0000013976	1	1	0.00000080917
MSB- LSB	0.00000049615	111.1747	1	-0.00000029769	1	1	0.0000000043915
LONDON							
SLSB	0.0000038147	102.3162	1	0.0000038147	1	1	0.00000055626
VLSB	0.0000023946	109.7134	1	-0.000009769	1	1	0.00000000544
MSB- LSB	0.0000006946	109.7134	1	-0.00000029769	1	1	0.0000000061481

From the above tables it is clear that the Peak Signal to Noise Ratio (PNSR) value ranges between 90.5553 dB to 113.3932dB (high value implies good performance). The Normalized Cross Correlation (NCC), Structural Content (SC) is 1 for all experiments. This value 1 implies that the cover image and generated stego image are statistically identical to each other. Maximum Difference (MD) is used to measure the difference between cover and stego images which is 1 for all conducted experiments (low value implies high similarity and quality of the cover and stego images). Mean Square Value is low for all the experiments. Normalized Absolute Error (NAE) computes the statistical difference between the cover and stego image where small value implies a high quality (as illustrated in all the computed experimental results above).

On careful investigation of experimental results as presented in the aforesaid Table 2 and Table 3, it can be easily inferred that the image quality performance for both MSB-LSB and VLSBS schemes are almost identical to SLSBS scheme. The value of MSE for both MSB-LSB and VLSBS scheme(for MSB – LSB maximum value is 0.000022888 and minimum is 0.00000029769 and for VLSBS maximum value is 0.000022888 and minimum values is 0.000006837) is low which undoubtedly implies good performance. Further, it can also be concluded that the value of MSE obtained in both the above mentioned schemes are in close proximity to the MSE value as attained from the SLSBS scheme(as maximum value is 0.000078223 and minimum value is 0.0000006946). Also it can be easily analyzed that for MSB-LSB and VLSBS, the AD values are very low (ranging from -0.000022231 to 0.0000076294 for MSB-LSB and ranging -0.000022231 to 0.0000076294 for VLSBS). Even in this case, the AD values for MSB-LSB and VLSBS schemes are in close proximity with the AD of SLSBS (Values ranges from 0 to 0.000022888). Finally NAE values of MSB-LSB scheme (ranging from 0.0000000026349 to 0.0000001994) and VLSBS scheme (ranging from 0.00000000544 to 0.0000080917) are very low and in similar to SLSBS scheme (ranging from 0.0000000267 to 0.00000055626). For MSB-LSB, VLSBS and SLSBS, the values of NCC, SC and MD are same, i.e. 1.

Though experimentally, it can be inferred that the image quality performance of both VLSBS and MSB-LSB schemes is identical to SLSBS scheme, yet both the schemes are better as compared to SLSBS counterpart from two different perspectives as mentioned next. We have already discussed that VLSBS scheme offers better security as compared to SLSBS scheme since it randomly embeds and disperses data unevenly in the cover medium(here image). Besides in the MSB-LSB scheme, keeping the degree of distortion 1, we can embed 2 message/data bits in the cover medium (here image) in contrast to the SLSBS scheme which could only embed 1 message/data bit. The following section puts forth the conclusion.

6. CONCLUSION

In this paper, a comparative performance analysis is furnished among three adopted steganographic schemes namely; SLSBS, VLSBS and MSB-LSB as discussed in papers [1-2]. An extensive literature survey has been conducted in the Steganograhy domain to identify some of the widely adopted steganographic performance metrics. Here two different cover images (lenna. jpg and sunset.jpg) and a varying dataset (having different chracter lengths) has been considered for experimental purpose. Image Steganographic performance metrics such as PSNR, NCC,SC,AD,MD,MSE,NAE have been computed for each dataset and cover images and the corresponding results have been presented in a tabular fashion (as depicted in Tables 2 and 3). From the computed experimental analysis, it is obvious that though the image quality performance of both VLSBS and MSB-LSB schemes are relatively similar to that of SLSBS scheme (as seen from the attained values of performance metrics), yet both the schemes are better compared to SLSBS approach since firstly better security is furnished by VLSBS scheme and secondly more data can be transferred securely by MSB-LSB scheme (keeping the degree of distortion 1) as compared to its SLSBS counterpart.

7. REFERENCES

[1] Ria Das and Punyasha Chatterjee "Securing Data Transfer in IoT Employing an Integrated Approach of Cryptography & Steganography" in HP3C-2017 in Kuala Lumpur, Malaysia, March 22-24, 2017, published in ACM Digital Library,pp:17-22,ISBN: 978-1-4503-4868. https://dl.acm.org/citation.cfm?id=3069605

[2] Ria Das and Indrajit Das, "Secure Data Transfer in IoT environment: adopting both Cryptography and Steganography techniques" in 2nd IEEE International Conference on Research in Computational Intelligence and Communication Networks(ICRCICN), India, Sept. 23-25, 2016, Published in IEEE Xplore Digital Library, pp:296 -301,978-1-5090-1047-9. http://ieeexplore.ieee.org/document/7813674/

[3] Tarik Faraj Idbeaa, Salina Abdul Samad and Hafizah Husain, " Comparative Analysis of Steganographic Algorithms Within Compressed Video Domain" , Signal Processing and Communication Systems (ICSPCS), 2014 8th International Conference on, 15-17 Dec. 2014, 978-1-4799-5255-7, http://ieeexplore.ieee.org/document/7021067/ .

[4] N.D. Jambhekar, C.A. Dhawale and R. Hegadi, "Performance Analysis of Digital Image Steganographic Algorithm", ICTCS '14, Proceedings of the 2014 International Conference on Information and Communication Technology for Competitive Strategies, 14 – 16 Nov, 2014, ISBN: 978-1-4503-3216-3. https://dl.acm.org/citation.cfm?id=2677937&CFID=991879869&CFTOKEN=15691904

[5] B. Lakshmi Sirishal, S. Srinivas Kumarl and B. Chandra Mohan ," Steganography based information security with high embedding capacity", Recent Advances in Electronics & Computer Engineering (RAECE), 2015 National Conference On, 13-15 Feb. 2015, 978-1-5090-2146-8, http://ieeexplore.ieee.org/document/7510218/.

[6] Anita Pradhan, Aditya Kumar Sahu, Gandharba Swain and K. Raja Sekhar , "Performance Evaluation Parameters of Image Steganography Technique", Research Advances in Integrated Navigation Systems (RAINS), International Conference on, 6-7 May 2016, 978-1-5090-1111-7, http://ieeexplore.ieee.org/document/7764399/

[7] G.Vallathan, G.Gayathri Devi and A.Vinoth Kannan , "Enhanced Data Concealing Technique to Secure Medical Image in Telemedicine Applications", Wireless Communications, Signal Processing and Networking(WiSPNET), International Conference on, 23-25 March 2016, 978-1-4673-9338-6, http://ieeexplore.ieee.org/document/7566117/

[8] V. Praneeth Kumar Reddy and Annis Fathima A, "A Cost Effective Approach for Securing Medical X-ray Images using Chebyshev Map", 2016 International Conference on Recent Trends in Information Technology (ICRTIT), 8-9 April ,2016, ISBN : 978-1-4673-9802-2. http://ieeexplore.ieee.org/document/7569576/

[9] Dalila Boughaci, Abdelhafid Kemouche and Hocine Lachibi, "Stochastic Local Search Combined with LSB Technique for Image Steganography", 2016 13th Learning and Technology Conference (L&T), 10-11 April , 2016, pp:36-44, ISBN: 978-1-5090-3394-2. http://ieeexplore.ieee.org/document/7562863/

[10] Raniyah Wazirali, Shaher Slehat and Zenon Chaczko, Grzegorz Borowik and Lucia Carrion, "Objective Quality Metrics in Correlation with Subjective Quality Metrics for Steganography", 2015 Asia-Pacific Conference on Computer Aided System Engineering (APCASE), 14-16 July, 2015, pp: 238-245,ISBN: 978-1-4799-7588-4. http://ieeexplore.ieee.org/document/7287026/