International Conference on Research Advances in Integrated Navigation Systems (RAINS - 2016),
April 06-07, 2016, R. L. Jalappa Institute of Technology, Doddaballapur, Bangalore, India

Performance Evaluation Parameters of Image Steganography Techniques

[1]Anita Pradhan, [2]Aditya Kumar Sahu, [3]Gandharba Swain, [4]K. Raja Sekhar
Department of Computer Science & Engineering, K L University
Vaddeswaram-522502, Guntur, Andhra Pradesh, India
[1]anita.pradhan15@gmail.com, [2]adityasahu.cse@gmail.com, [3]gswain1234@gmail.com, [4]raja.sekhar@owasp.org

Abstract - **This paper illustrates the various performance evaluation parameters of image steganography techniques. The performance of a steganographic technique can be rated by three parameters; (i) hiding capacity, (ii) distortion measure and (iii) security. The hiding capacity means the maximum amount of information that can be hidden in an image. It can also be represented as the number of bits per pixel. The distortion is measured by using various metrics like mean square error, root mean square error, PSNR, quality index, correlation, structural similarity index etc. Each of these metrics can be represented mathematically. The security can be evaluated by testing the steganography technique with the steganalysis schemes like pixel difference histogram analysis, RS analysis etc. All these metrics are illustrated with mathematical equations. Finally, some future directions are also highlighted at the end of the paper.**

Keywords - **steganography; hiding capacity; distortion measure; security; performance evaluation parameters**

I. INTRODUCTION

Steganography is an art of invisible communication, achieved by hiding secret message inside a carrier file like image. Mainly steganography techniques are of four types, (i) steganography in image, (ii) steganography in audio, (iii) steganography in video, and (iv) steganography in text [1, 20], as shown in Fig.1. Image steganography schemes are categorized into two major types, (i) spatial domain techniques, and (ii) transform domain techniques [2].

The spatial domain techniques perform direct manipulation over the pixels of the image. The transform domain techniques use some transformations to transform the image into transform domain and then hide the secret message. The image with secret message hidden inside it is called as the stego-image. There are various categories of techniques in spatial domain, (i) LSB substitution, (ii) pixel value differencing (PVD), (iii) exploiting modification direction (EMD), etc [20]. The transform domain techniques are based on various transforms like, (i) DCT, (ii) DWT, and (iii) FFT [2]. In a steganography technique if the host image can be recovered along with the data from the stego-image, then it is called reversible steganography. Reversible steganography techniques are available both in spatial domain and transform domain. In image steganography the unnatural message is hidden inside a natural image in such a way that the distortion is minimum so that the intruder cannot notice it [3]. The most familiar image steganography technique is the least significant bit (LSB) substitution. The LSB substitution can be extended upto 4 LSB planes to achieve higher embedding capacity. It is the simplest technique, but vulnerable to RS analysis [4]. The LSB substitution can be enhanced in the following ways. The LSB bits of all the pixels can be formed as LSB array. The secret binary words can be hidden at minimum distortion locations of LSB array, so that the security could be improved [5]. Similarly, the bits from four LSB planes can form four LSB arrays and the binary message can be partitioned into four parts and then one part of the message can be hidden in one LSB array at minimum distortion locations, so that security can be improved [6]. To increase the hiding capacity and security, the three LSB planes can be investigated, but only two bits can be embedded in two selected planes based on the secret data bits [7]. This is called data dependent embedding. Similarly, only two LSB bits can also be used to achieve data dependent embedding [8]. The pixel value differencing (PVD) steganography is another familiar image steganography technique. It was initially proposed by Wu & Tsai [9] in 2003. PVD techniques based on maximum pixel value differences are also proposed to achieve higher embedding capacity [10, 11]. Many other higher capacity PVD techniques [12, 13, 14] has been proposed in literature. There is a steganalysis scheme, called pixel difference histogram analysis to detect PVD steganography [15]. So Adaptive PVD techniques [16, 17] have been proposed to overcome this pixel difference histogram analysis. In adaptive PVD techniques the quantization ranges are made adaptive for different pixel blocks to improve upon the security. In non-adaptive PVD technique the range table is common to all the blocks, where as in adaptive PVD techniques the ranges for different pixel blocks are different being dependent on the pixel values of that block. Combination of PVD steganography with LSB substitution has been proposed in literature to increase embedding capacity and enhance security [18, 19]. Another direction in image steganography is exploiting modification directions (EMD) [20]. In this technique the main idea is, a secret digit in (2n+1)-ary system is hidden in a group of n pixels. Only one pixel value is increased or decreased by 1. Over the years a good number of improved EMD techniques has been proposed in literature [21, 22, 23]. Recently combination of

978-1-4673-8819-8/16/$31.00 ©2016 IEEE

EMD and PVD has also been proposed to improve upon the hiding capacity and security [24]. There are many other directions in image steganography like, palette based steganography, mapping based steganography, collage steganography, code based steganography, spread spectrum steganography etc [25]. The rest of the paper is described as follows. In section II the different evaluation parameters are discussed. In section III some notable highlights are shared and in section IV the paper is concluded.

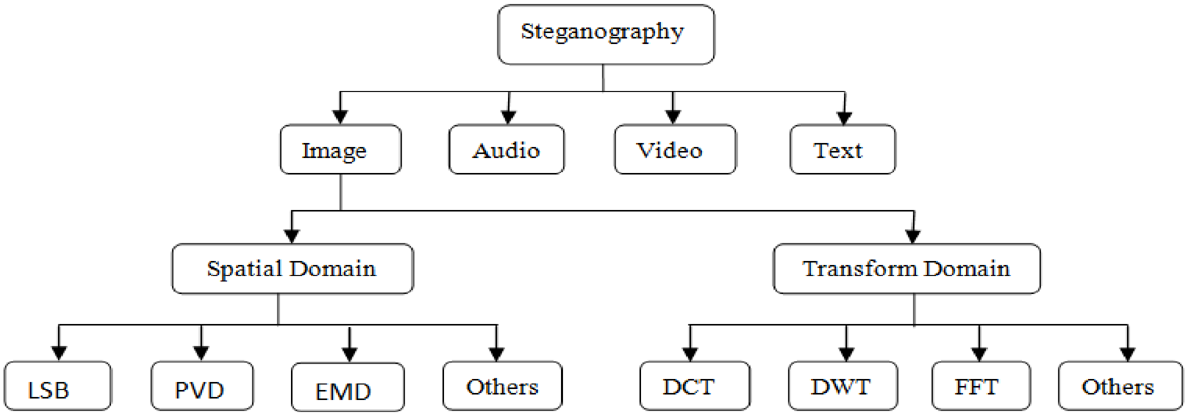


Fig.1 Classification of image steganography techniques

II. EVALUATION PARAMETERS

The image steganographic techniques can be evaluated by three main parameters; (i) hiding capacity, (ii) distortion measure, and (iii) security. The algorithm complexity may also be considered as the fourth parameter. In literature no researcher has considered the algorithm complexity as an evaluation parameter.

A. *Hiding Capacity*

The hiding capacity can be referred in two ways; (i) maximum hiding capacity, and (ii) bit-rate as shown in Fig.2. The maximum hiding capacity is the maximum amount of data that can be hidden in the image. It can be represented in bits or bytes or kilobytes. The bit-rate is the maximum number of bits that can be hidden per pixel; it is often termed as bits per pixel (bpp) or bits per byte (bpb). For example consider a 512×512 gray image. At most if it can hide 3,00,000 bits of data then the maximum hiding capacity is 3,00,000 bits. If represented in bpp it is 3,00,000 divided by 262144 (=512×512) which is equal to 1.14 bpp. If the hiding capacity is larger then the steganography technique is better.

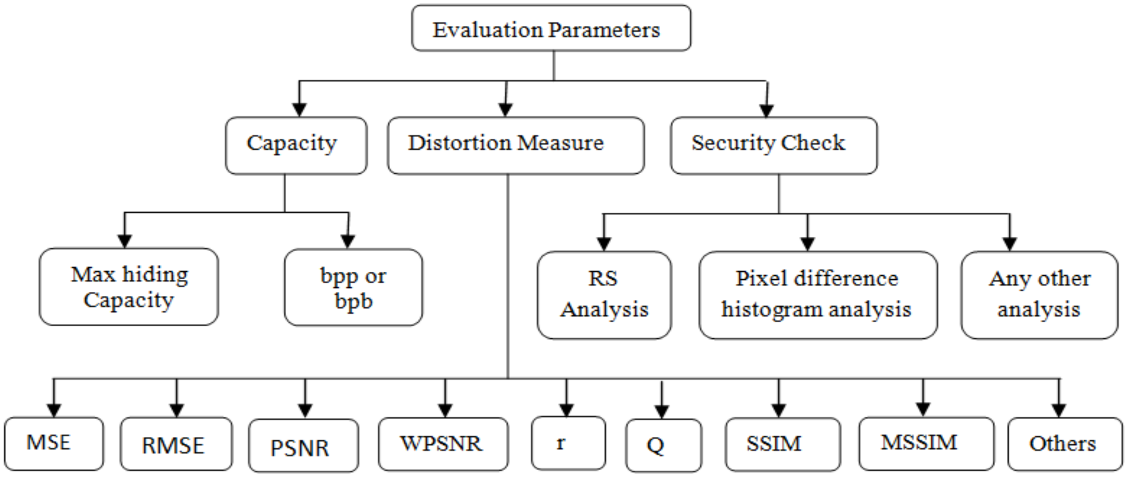


Fig.2 Evaluation parameters

978-1-4673-8819-8/16/$31.00 ©2016 IEEE

B. Distortion Measurement

The stego-images should be imperceptible, means the distortion should not be noticeable. As an example for the original images shown in Fig.3, the stego-images generated by a PVD steganography technique are shown in Fig.4. The stego-images are imperceptible; one cannot identify any distortion in them. The distortion can be measured by using many metrics such as; (i) Mean Square Error (MSE), (ii) Root Mean Square Error (RMSE), (iii) Peak signal-to-noise Ratio (PSNR), (iv) Weighted PSNR (WPSNR) (v) Correlation, (vi) Quality Index, (vii) Structural SIMilarity (SSIM) index (viii) Kullback-Leibler Divergence (K-L divergence), (ix) Manhattan Distance, and (x) Euclidean Distance. The MSE between the original image and the stego-image is computed by using (1) [25]. The p_{ij} and q_{ij} are the original image pixel value and the stego-image pixel value at i^{th} row and j^{th} column respectively. The m and n are the number of rows and columns in the digital image. The MSE should be as less as possible. If the original image and the stego-image are the same then MSE is zero. The RMSE is often used as a measure of distortion; it is computed using (2).

$$\mathrm{MSE} = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} \left(p_{ij} - q_{ij}\right)^2 \tag{1}$$

$$\mathrm{RMSE} = \sqrt{\frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} \left(p_{ij} - q_{ij}\right)^2} \tag{2}$$

The PSNR is a measure of distortion in the stego-image. It is computed using (3) [25]. Higher PSNR value means lesser distortion. A PSNR value is more than 40 decibels (dB) is very good. If it is in between 30 dB and 40 dB, can be acceptable, but a PSNR less than 30 dB is not acceptable because the distortion is very high. For color images a pixel comprises of 3 bytes. Each byte can be treated as a pixel; and then (1) and (3) be used to calculate the MSE and PSNR values.

$$\mathrm{PSNR} = 10 \times \log_{10} \frac{255 \times 255}{\mathrm{MSE}} \tag{3}$$

(a) Lena (b) Baboon (c) Tiffany (d) Peppers

Fig.3 Original Images

Fig.4 Stego-images of a particular PVD Technique

The WPSNR is another metric for image quality measurement [40, 41, 42]. It uses another parameter called Noise Visibility Function (NVF) along with MSE. The NVF value will be close to zero and maximum up to one. It is defined as in (4).

$$\mathrm{WPSNR} = 10 \times \log_{10} \left(\frac{255}{\sqrt{MSE} \times NVF}\right)^2 \tag{4}$$

The NVF is defined in (5)

$$\text{NVF}(i, j) = \frac{1}{1+\sigma^2_{I(i,j)}} \tag{5}$$

Where, $\sigma^2_{I(i,j)}$ is the local variance of an image in a window centered on a pixel whose coordinate is (i, j). The correlation, represented by the letter r, is a measure of the similarity between the original image and the stego-image. It is measured using (6) [25]. The $\bar{p}$ and $\bar{q}$ are the average pixel value in original image and stego-image respectively. The MATLAB function corr2(p, q) computes the correlation between the cover image, p and the stego-image, q. The maximum value of corr2(p, q) will be 1, if p and q are the same images. So if distortion is lesser, then the correlation can be higher.

$$r = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n}(p_{ij}-\bar{p}) \times (q_{ij}-\bar{q})}{\sqrt{\left(\sum_{i=1}^{m}\sum_{j=1}^{n}(p_{ij}-\bar{p})^2\right) \times \left(\sum_{i=1}^{m}\sum_{j=1}^{n}(q_{ij}-\bar{q})^2\right)}} \tag{6}$$

The qualities of the stego-images are evaluated by using the universal image quality index (Q) [26, 27]. It is computed by using (7). The maximum value of Q can be 1, if p and q are the same images.

$$Q = \frac{4\,\sigma_{xy}\,\bar{p}\,\bar{q}}{(\sigma_x^2+\sigma_y^2)[(\bar{p})^2+(\bar{q})^2]} \tag{7}$$

Where $\bar{p}$ is the mean pixel value in original image, $\bar{q}$ is the mean pixel value in stego-image, σ_x^2 is the standard deviation for original image, σ_y^2 is the standard deviation for stego-image, and σ_{xy} is the covariance. They are defined in (8), (9), (10), (11), and (12) respectively.

$$\bar{p} = \frac{1}{m\times n}\sum_{i=1}^{m}\sum_{j=1}^{n} p_{ij} \tag{8}$$

$$\bar{q} = \frac{1}{m\times n}\sum_{i=1}^{m}\sum_{j=1}^{n} q_{ij} \tag{9}$$

$$\sigma_x^2 = \frac{1}{m\times n-1}\sum_{i=1}^{m}\sum_{j=1}^{n}(p_{ij}-\bar{p})^2 \tag{10}$$

$$\sigma_y^2 = \frac{1}{m\times n-1}\sum_{i=1}^{m}\sum_{j=1}^{n}(q_{ij}-\bar{q})^2 \tag{11}$$

$$\sigma_{xy} = \frac{1}{m\times n-1}\sum_{i=1}^{m}\sum_{j=1}^{n}(p_{ij}-\bar{p})(q_{ij}-\bar{q}) \tag{12}$$

The SSIM index is another metric originally defined in [28] and has been used in [29, 30] for image quality measurement. The original image is divided into B blocks each of size 8×8 pixels. For the block mean pixel value ($\bar{p}$) and standard deviation (σ_x^2) is calculated. Then for stego-image also the mean pixel value ($\bar{q}$) and standard deviation (σ_y^2) is calculated. The covariance (σ_{xy}) between the original image and stego-image is calculated. Finally, SSIM is computed as in (13). Here c_1 is a constant used to avoid instability when$(\bar{p}^2+\bar{q}^2)$ is very close to zero. Similarly, c_2 is a constant used to avoid instability when $(\sigma_x^2+\sigma_y^2)$ is very close to zero. The $c_1$value may be chosen as $(K_1L)^2$, where L is 255 for gray image and $K_1 \ll 1$. Similarly, c_2 value may be chosen as $(K_2L)^2$, where $K_2 \ll 1$. Note that when $c_1 = 0$ and $c_2 = 0$, SSIM is equal to quality index Q. Thus Q is a special case of SSIM.

$$\text{SSIM}=\frac{(2\bar{p}\,\bar{q}+c_1)(2\sigma_{xy}+c_2)}{(\bar{p}^2+\bar{q}^2+c_1)(\sigma_x^2+\sigma_y^2+c_2)} \tag{13}$$

For all the B blocks of the image SSIM is computed and then the mean SSIM index is calculated to evaluate the overall quality of the image, as in (14).

$$\text{MSSIM}=\frac{1}{B}\sum_{i=1}^{B}\text{SSIM}_i \tag{14}$$

We can also use the K-L divergence to find the difference between the cover image and the stego-image histograms [31]. If h1 and h2 are the histograms of cover image and stego-images respectively, then K-L divergence from h1 to h2 (say d1) can be estimated as in (15) and from h2 to h1 (say d2) as in (16) [32, 39]. Then the average d=(d1+d2)/2 is taken into consideration. This K-L divergence value will be 0 if both the cover image and stego-image are the same.

$$d1 = \sum_{i=0}^{255} h1(i) * \log\frac{h1(i)}{h2(i)} \tag{15}$$

$$d2 = \sum_{i=0}^{255} h2(i) * \log\frac{h2(i)}{h1(i)} \tag{16}$$

The Manhattan distance [33] can also be used to find the differences between the histograms of original and stego-images. If h1 and h2 are the histograms of cover image and stego-images respectively, then the Manhattan distance can be estimated by using (17). It is the sum of the absolute differences of their corresponding components.

$$\text{MD(h1,h2)}= \sum_{i=0}^{255}|h1(i)-h2(i)| \tag{17}$$

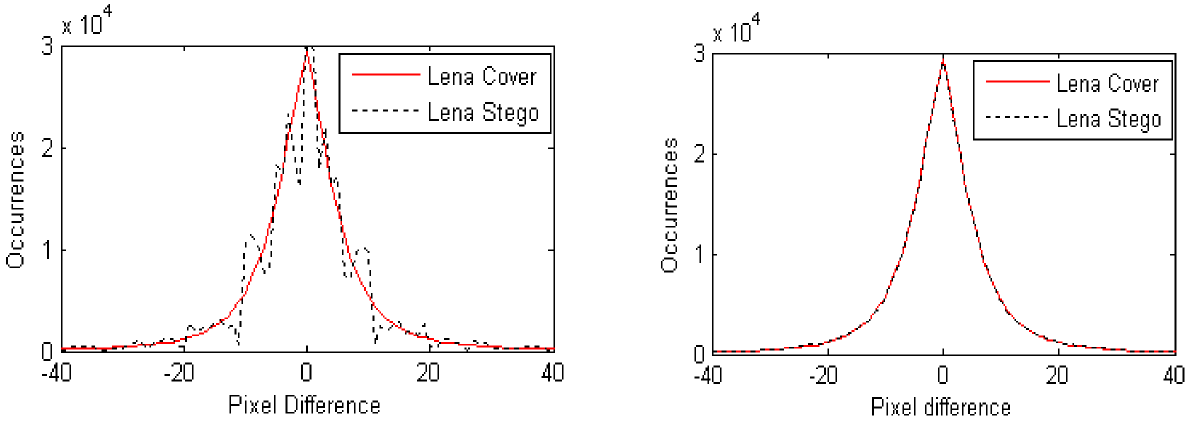
The Euclidian distance [33] can also be used to find the differences between the histograms of original and stego-images. It is the square root of the sum of the squared differences. If h1 and h2 are the histograms of cover image and stego-images respectively, then the Euclidian distance can be estimated by using (18).

$$\text{ED(h1,h2)}= \sqrt{\sum_{i=0}^{255}\{h1(i)-h2(i)\}^2} \tag{18}$$

C. *Security Analysis*

A steganographic technique is said to be secured if it is resistant to various steganalytic attacks. There are various steganalysis schemes to test the security of a steganographic technique. A LSB substitution based technique can be tested by RS analysis and a PVD based technique can be tested by pixel difference histogram analysis.

The pixel difference histogram is a graph [15], wherein the X-axis represents the pixel difference between every pair of two consecutive pixels and the Y-axis represents the number of occurrences. If there are undesired steps in the histogram, then steganography is detected. For example, Fig.5 represents two different pixel difference histograms for two different techniques. The curves represented by solid lines in each graph are the pixel difference histograms of the original images and those represented by dotted lines are the pixel difference histograms of the stego-images. In pixel difference histogram the step effect is clearly visible for technique 1. For technique 2 it is not visible. So technique 2 is not vulnerable to pixel difference histogram analysis. The pixel difference histogram is a graph [15], wherein the X-axis represents the pixel difference between every pair of two consecutive pixels and the Y-axis represents the number of occurrences. If there are undesired steps in the histogram, then steganography is detected. For example, Fig.5 represents two different pixel difference histograms for two different techniques. The curves represented by solid lines in each graph are the pixel difference histograms of the original images and those represented by dotted lines are the pixel difference histograms of the stego-images. In pixel difference histogram the step effect is clearly visible for technique 1. For technique 2 it is not visible. So technique 2 is not vulnerable to pixel difference histogram analysis.



(a) Technique-1

(b) Technique-2

Fig. 5 Pixel difference histograms of three different techniques

The RS analysis [4] investigates the dual statistics of the cover/stego-image. It is done as follows. Define functions F_1 : 2n ↔2n+1 and F_{-1} : 2n ↔2n -1. Divide the cover/stego-image M into many small parts of same size, say such a part is G. Then use the function $f\ (X_1, X_2, X_3, \dots, X_n) = \sum_{i=1}^{n-1} |X_{i+1} - X_i|$ to measure the smoothness of G. Where X_i, for i=1,2 …n are the pixels in G. Then apply F_1 to all the parts of M and define the parameters; $R_m = \frac{\sum G \mid f(F_1(G)) > f(G)}{\sum G}$ and $S_m = \frac{\sum G \mid f(F_1(G)) < f(G)}{\sum G}$, where $\sum G$ in the denominator represent the total number of groups and in the numerator it is the number of groups satisfying the said condition. Similarly define $R_{-m} = \frac{\sum G \mid f(F_{-}1(G)) > f(G)}{\sum G}$ and $S_{-m} = \frac{\sum G \mid f(F_{-1}(G)) < f(G)}{\sum G}$.

If M is the cover image, then by applying F_1 and F_{-1} equally increases the f value, so $R_m \approx R_{-m} > S_m \approx S_{-m}$. If M is the stego-image, then by applying F_1 and F_{-1} to this stego-image will decrease the difference between R_{-m} and S_{-m} , so R_{-m} - $S_{-m} > R_m$ - S_m .

The LSB embedding can be determined by observing these two relationships. The Fig.6 shows RS diagrams for two techniques. The X-axis represents the percentage of hiding capacity and Y-axis represents the percentage of regular or singular groups. The RS diagram of Technique-3 (shown in Fig.6.(a)), satisfies $R_m \approx R_{-m} > S_m \approx S_{-m}$, so it is not vulnerable to RS analysis, But the RS diagram of Technique-4 (shown in Fig.6.(b)) satisfies, R_{-m} - $S_{-m} > R_m$ - S_m , so vulnerable to RS analysis.

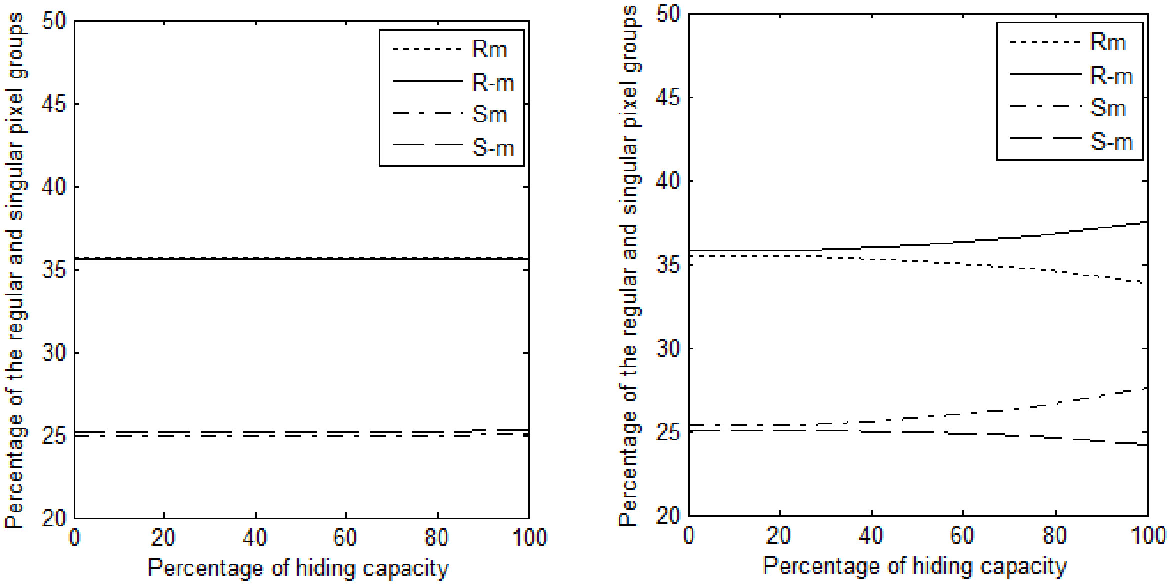
III. SOME FUTURE DIRECTIONS

The important directions, where some more investigations can be carried are, (i) use of adaptive range table in PVD, (ii) utilization of multi directional edges, (iii) suitable combination of LSB, PVD, and EMD approaches, and (iv) use of YCbCr color model.

The PVD techniques are detectable by pixel difference histogram analysis. The step effects in the pixel difference histogram are clearly identifiable. Furthermore the PVD techniques uses a fixed quantization range table, which is common for all the pixel blocks. The security can be improved if the quantization ranges can be different for different pixel blocks. Furthermore, the capacity as well as security can be improved by exploiting vertical, horizontal, and diagonal edges.

LSB substitution can be extended upto 4 LSB planes to get higher embedding capacity. PVD approaches exploit the smoothness of a block and hides desired number of bits, hence increases the security. The LSB and PVD approaches are combined to get both higher hiding capacity and higher security [34, 35]. A combined LSB and PVD approach proposed by Khodaei and Faez [27] performs very well in terms of capacity and PSNR. In the recent literature the PVD and EMD approaches are also combined to get better performance [24]. In the same direction, the LSB, PVD, and EMD can be suitably combined to achieve higher embedding capacity, lesser distortion and higher security.

The LSB steganography with RGB color images can be done in a different way by treating each R, G, or B components separately and substituting in their LSB planes [36, 37]. Similarly, the PVD steganography can be done with RGB images by treating each of the R, G, or B component as a different pixel. Watermarking is the process of embedding information in a carrier file in order to protect its ownership. The YCbCr model has been used in watermarking [38]. The YCbCr color model can also be used in steganography



(a) RS diagram for Technique-3

(b) RS diagram for Technique-4

Fig.6. RS diagrams of two techniques

IV. CONCLUSION

For any new proposed steganographic algorithm, one has to evaluate its performance using the three parameters like hiding capacity, distortion measure, and security. This paper narrates all the distortion measurement metrics using mathematical equations. It also illustrates two steganalysis tools like RS analysis and pixel difference histogram analysis for security testing. Furthermore, it also highlights some directions on which further investigations and experimentations can be conducted. The first important direction to be explored further is use of YCbCr model in steganography. The second important direction is combination of LSB, PVD, and EMD.

Acknowledgement

This work has been supported by the Department of Science and Technology, India through the fund sanctioned for improving Science & Technology infrastructure, at department of CSE, K.L University, by order number SR/FST/ESI-332/2013.

References

[1] A. Cheddad, J. Condell, K. Curran, P.M. Kevitt, “Digital image steganography: survey and analysis of current methods”, Signal Processing, vol. 90, pp.727-752, 2010.

[2] W.M. Abdullah, A.M.S. Rahma, A-S. K. Pathan, "Mix column transform based on irreducible polynomial mathematics for color image steganography: A novel approach", Computers and Electrical Engineering, vol.40, pp.1390-1404, 2014.

[3] A. Martin, G. Sapiro, G. Seroussi, "Is image steganography natural?", IEEE Transactions on Image Processing, vol.14, no.12,pp.2040-2050, 2005.

[4] J. Fridrich, M. Goljian, R Du, "Detecting LSB steganography in color and gray-scale images". Magazine of IEEE Multimedia Special Issue on Security, vol.8, no.4, pp.22–28, 2001.

[5] G. Swain, S.K. Lenka, "A novel steganography technique by mapping words with LSB array", International Journal of Signal and Imaging Systems Engineering, vol.8, no.1, pp.115-122, 2015.

[6] G. Swa*i*n, S. K. Lenka, "LSB array based image steganography technique by exploring the four least significant bits", Global Trends in Information Systems and Software Applications, Communications in Computer and Information Science, vol.270, pp.479-488, 2012.

[7] G. Swain, S. K. Lenka, "A technique for secret communication by using a new block cipher with dynamic steganography", International Journal of Security and Its Applications, vol.6, no.2, pp.1-12, 2012.

[8] G. Swain, S. K. Lenka, "A robust image steganography technique using dynamic embedding with two least significant bits", Advanced Materials Research, vols. 403-408, pp.835-841, 2012.

[9] D.C. Wu, W.H. Tsai, "A steganograhic method for images by pixel value differencing", Pattern Recognition Letters, vol.24, no.9-10, pp.1613-1626, 2003.

[10] A. Pradhan, D.S. Sharma, G. Swain, "Variable rate steganography in digital images using two, three and four neighbor pixels", Indian Journal of Computer Science and Engineering, vol.3. no.3, pp.457-463, 2012.

[11] G. Swain, "Steganography in Digital Images Using Maximum Difference of Neighboring Pixel values", International Journal of Security and Its Applications, vol.7, no.6, pp.285-294, 2013.

[12] Y.P. Lee, J.C. Lee, W.K. Chen, K.C. Chang, I.J. Su, C.P. Chang, "High-payload image hiding with quality recovery using tri-way pixel-value differencing", Information Sciences, vol.191, pp.214-225, 2012.

[13] G. Swain, S.K. Lenka, "Steganography using two sided, three sided, and four sided side match methods", CSI Transactions on ICT, vol.1, no.2, pp.127-133, 2013.

[14] G. Swain, S. K. Lenka, "Pixel value differencing steganography using correlation of target pixel with neighboring pixels", IEEE International Conference on Electrical, Computer and Communication Technologies, 2015, pp.599-604.

[15] X. Zhang, S.Wang, "Vulnerability of pixel-value differencing steganography to histogram analysis and modification for enhanced security", Pattern Recognition Letters, vol. 25, pp.331-339, 2004.

[16] W. Luo, F. Huang, J. Huang, "A more secure steganography based on adaptive pixel-value differencing scheme", Multimedia Tools and Applications, vol. 52, pp.407-430, 2011.

[17] G. Swain, "Adaptive pixel value differencing steganography using both vertical and horizontal edges", Multimedia Tools and Applications, 2015, doi: 10.1007/s11042-015-2937-2.

[18] X. Liao, Q.Y. Wen, J. Zhang, "A steganographic method for digital images with four-pixel differencing and modified LSB Substitution", Journal of Visual Communication and Image Representation, vol. 22, pp.1-8, 2011.

[19] G. Swain, "Digital image steganography using nine-pixel differencing and modified LSB Substitution", Indian Journal of Science and Technology, vol.7, no.9, pp.1444-1450, 2014.

[20] X. Zhang, S. Yang, "Efficient steganographic embedding by exploiting modification direction", IEEE Communication Letters, vol.10, no.11, pp.781-783, 2006.

[21] C.F. Lee, Y.R. Wang, C.C. Chang, "A steganographic method with high embedding capacity by improving exploiting modification direction", IIHMSP, pp. 497–500, 2007.

[22] C.F. Lee, C.C. Chang, K.H. Wang, "An improvement of EMD embedding method for large payloads by pixel segmentation strategy", Image and Vision Computing, vol.26, pp.1670-1676, 2008.

[23] T.D. Kieu, C.C. Chang, "A steganographic scheme by fully exploiting modification directions", Expert Systems with Applications, vol.38, pp.10648-10657, 2011.

[24] S.Y. Shen, L.H. Huang, "A data hiding scheme using pixel value differencing and improving exploiting modification directions", Computers & Security, vol.48, pp.131-141, 2015.

[25] G.Swain, S.K. Lenka, "Classification of spatial domain image steganography techniques: a study", International Journal of Computer Science & Engineering Technology, vol.5, no.3, pp.219-232, 2014.

[26] Z.Wang, A.C. Bovic, “A universal image quality index”, IEEE Signal Processing Letters, vol.9, no.3, pp. 81-84, 2002.

[27] M. Khodaei, K. Faez, “New adaptive steganographic method using least-significant-bit substitution and pixel-value differencing”, IET Image Processing, vol.6, no.6, pp.677-686, 2012.

[28] Z. Wang, H.R. Sheikh, E.P. Simoncelli, “Image quality assessment: from error visibility to structural similarity”, IEEE Transactions on Image Processing, vol.13,no.4, pp.1-14, 2004. [29] Y.A.Y Al-Najjar, D.C. Soong, “Comparison of image quality assessment: PSNR, HVS, SSIM, UIQI”, International Journal of Scientific & Engineering Research, vol.3, no.8, pp.1-5, 2012.

[30] I. Banerjee, S. Bhattacharyya, G. Sanyal, “Hiding & analyzing data in image using extended PMM”, Procedia Technology, vol.10, pp.157-166, 2013.

[31] J.C. Joo, H.Y. Lee, H.K. Lee, “Improved steganographic method preserving pixel-value differencing histogram with modulus function”, EURASIP Journal on Advances in Signal Processing, 2010, doi:10.1155/2010/249826.

[32] F. Nielsen, “On the Chi square and higher-order Chi distances for approximating –divergences”, IEEE Signal Processing Letters, 2013, doi: 10.1109/LSP.2013.2288355.

[33] A. Hasnat, S. Halder, D. Bhattacharjee, M. Nasipuri, D.K. Basu, “Comparative study of distance metrics for finding skin similarity of two color facial images”, CS & IT-CSCP, 2013, pp. 99–108, doi: 10.5121/csit.2013.3210.

[34] H.C. Wu, N.I. Wu, C.S. Tsai, M.S. Hwang, “Image steganographic scheme based on pixel-value differencing and LSB replacement methods”, IEEE Proceedings Vision, Image and Signal Processing, vol.152, no.5, pp.611-615, 2005.

[35] C. H. Yang, C.Y Weng, S. J. Wang, H.M. Sun, “Varied PVD+LSB evading programs to spatial domain in data embedding systems”, The Journal of Systems and Software, vol.83, pp.1635-1643, 2010.

[36] G. Swain, S. K. Lenka, “A better RGB channel based image steganography technique”, Communications in Computer and Information Science, vol.270, pp. 470-478, 2012.

[37] G. Swain, S. K. Lenka, “A novel approach to RGB channel based image steganography technique”, International Arab Journal of e-Technology, vol.2, no.4, pp.181-186, 2012.

[38] F. Lusson, K. Bailey, M. Leeney, K. Curran, “A novel approach to digital watermarking exploiting colour spaces”, Signal Processing, vol.93, pp.1268–1294, 2013.

[39] W. Zhao, Z. Jie, L. Xin, W. Qiaoyan, “Data embedding based on pixel value differencing and modulus function using indeterminate equation”, The Journal of China University of Posts and Telecommunications, vol.22, no.1, pp.95-100, 2015.

[40] K. Sau, R.K. Basak, A. Chanda, “Image compression based on block truncation coding using clifford algebra”, Procedia Technology,vol.10, pp.699-706, 2013.

[41] S. Sidhik, S.K. Sudheer, V.P.M. Pillai, “Performance and analysis of high capacity steganography of color images involving wavelet transform”, Optik, vol.128, pp.3755-3760, 2015.

[42] H. Al-Dmour, A. Al-Ani, “A steganography embedding method based on edge identification and XOR coding”, vol.46, pp.293-306.