



International Journal of Control Theory and Applications

ISSN : 0974-5572

© International Science Press

Volume 10 • Number 11 • 2017

Pseudo Random Sequential Watermarking with Pattern Match based Pixel Selection

Parveen Banga¹ and Damandeep Kaur²

¹ M.Tech Scholar, Department of computer science engineering, Chandigarh University, Mohali, India

E-mail: bangaparveen47@gmail.com

² Associate Professor, Department of Computer Science Engineering, Chandigarh University, Mohali, India

E-mail: @gmail.com

Abstract: The new edge directed interpolation (NEDI) has been utilized for the adaptive edge pixel selection for the robust embedding with minimum grade change in the cover image set. The proposed model is expected to produce the improved results than the existing algorithm while embedding the data into the cover image. The proposed algorithm has been obtained peak signal to noise ratio (PSNR) value along with the improved capacity of image. This proposed model has signified the high resilience against the histogram, chi-square and RS based steganalysis attacks for detection of various image manipulations like cropping, compression. The research work has been implemented on 24 bit RGB BMP images. The performance evaluation has been performed in the form of payload capacity, elapsed time and PSNR and MSE. The payload capacity has been recorded 11.28 bpp with the larger RGB cover images of size 1.43 MB to 2 MB for hidden image of size 400KB to 900 KB. The PSNR value of 52 to 55 Db and MSE value of 0.00554 has been recorded during Embedding process which improves the better quality of the results of the proposed model. The proposed model has been outperformed the existing model on the basis of the defend performance parameters.

Keywords: Watermarking, LSB, XOR encryption, secret key embedding, image watermarking, invisible watermarking.

INTRODUCTION

In recent decades, the increasing use of powerful internet has made the contemporary society digitized and enables us to easily share enormous multimedia data by ubiquitous channels [1]. It helps us for downloading, uploading, manipulating and exchanging information. Thousands of pieces of information are frequently transmitted in our daily life [2][3]. However, it reveals a potential problem that may result in exposures of our privacy to the public, if the security of network multimedia data is not well protected. Therefore, there is an urgent requirement for a secure communication way to protect transmitted confidential data via the Internet. Information hiding plays an important role in today's world. It has caught a ton of consideration by specialists because of the headway in the present day correspondence innovation. In the today's present day world, everybody goes over the computerized data. Significant worry about this computerized data is the security of the data as exchanging information over the web is not protected and it experiences eavesdropping[3].

Initially, Cryptology was used for a reliable and safe transmission. However, the encrypted data which has meaningless message may actually evoke suspicion from illegal attackers. But now, watermarking [4][5] is invented to overcome the drawback by embedding confidential data into a cover media without attracting any special attention from hackers. So, watermarking is such technique which is used to provide more security to the confidential information.

Now a days internet is widely used and information/data is transferred through the network regularly, so while sending the data through network is required information security. Encryption is also used to provide the security to the information and to encrypt the data in such a way so that intruder cannot decrypt the data on network.

LITERATURE SURVEY

Da-Chun Wu et.al [43], in 2003 proposed a technique for embedding secret data into a grayscale cover image. A cover image was split into non-overlapping blocks. Then two successive pixels in each block were selected to compute the difference in their values so as to embed data in the block when gray value falls off of the range of 0 through 255. In this, if value comes out to zero then it is marked as smooth block and if it is 255 then it would be shapely edge block. The range intervals of the selection were based on the behavior of human visual system (HVS) for grayscale value variations from smoothness to contrast. It provides good quality of stego image, but does not provide any security against various types of attacks [43]. H. C. Wu et.al [44], in 2005 proposed a method to use the combination of LSB and PVD approaches of watermarking to improve embedding capacity and the PSNR. This method used difference between two consecutive pixel values to hide data. It utilizes an LSB substitution technique for hiding data at the smooth area and PVD to hide data at edges of image. The splitting between smooth area and edge areas of range width table used at sender and receiver end to increase security level, which made it hard to figure the territory at which the information covering up was finished. In this, two pixels were embedded using LSB if difference falls into smooth area of range width table whereas few pixels were embedded by PVD if difference fall into higher level. This method has shown increase in imperceptibility and embedding capacity at image edge pixels as compared to the smooth area of image [44].

Manglem Singh et.al [46], in 2007 put forward a technique for hiding encrypted data in the feature of the image rather than embedding the secret data into smooth area of cover image. In this approach, message encryption was performed followed by edge detection and LSB embedding algorithm for hiding the encrypted message in non-adjacent and random pixel locations on edges of the image. The intruder did not have any suspicion that secret message bits were concealed in the cover image. This approach ensures the security. Blind LSB detection technique was not able to estimate the length of the secure message bits accurately [46].

Cheng-Hsing Yang [47], in 2008 the proposed watermarking strategy in view of the new versatile implanting calculation LSB information covering up in the non ceaseless zone (edge zone) of the picture with spatial space. Embedding the data into the grayscale image without any distortion and PVD was used to distinguish between continuous and non continuous area in the image [47].

IMPLEMENTATION PROCEDURE

Extraction of secret image using NEDI (New Edge Directed Interpolation) and DFM (Dynamic Fuzzifier Module) for RGB image

Pseudo Code 1: Extraction algorithm

1. Input Image: Stego Image
2. select Secret Image then perform watermarking_extraction
3. Read(stego image)

- 4.Bitstream=Extraction
 - 5.Then apply the NEDI to detect the edges and then apply defuzzifier to extract the original image form stego image.
 - 6.Reversed Embedding Procedure
 7. Secret File =XOR encrption
 8. End
-

Proposed Work Architecture

We have proposed the dynamic fuzzifier for the robust image embedding. The dynamic fuzzifier module (DFM) is responsible for the segmentation, selection and fuzzy weight calculation among the input cover and secret image.

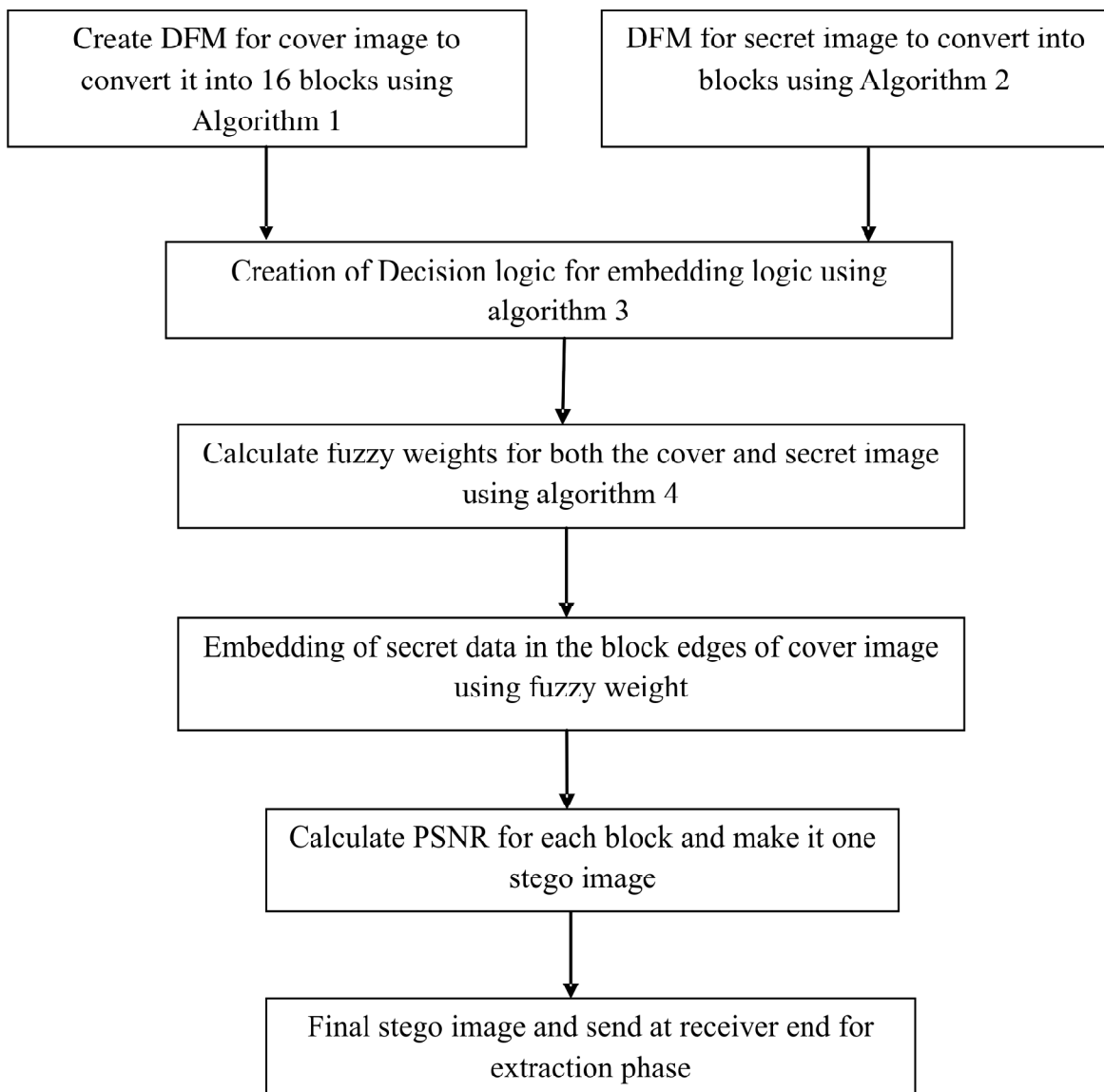


Figure 2: Approach used embedding at sender end

Dynamic Fuzzy rule set Determination for cover and secret image

Dynamic fuzzy rule set determination is used for robust image embedding. The dynamic Fuzzyfier module used for segmentation of cover and secret image into block and then selection of block of cover image for embedding it with secret image block using the calculation of fuzzy weight. Decision of Fuzzy weight is for embedding the block of cover image into secret image. The embedding algorithm has been designed with the spatiotemporal ability to embed the secret data in the block edges of the cover image, while utilizing the non-overlapping block-based division. In this we used four algorithms for embedding the block of the cover image with the secret image using the decision of fuzzy weight. It calculates the fuzzy weights of the blocks of cover image and fuzzy weights of the secret image then according to fuzzy weight embedding of cover and secret image done is :

Dynamic Fuzzy rule set Determination for cover image (DFRSD)

Algorithm 1: Dynamic Fuzzy Rule Set Determination for Cover (DFRSD-Cover)

1. Input cover image matrix (IC_m)
2. Calculate the image size in number of rows (C_r) and columns (C_c)
3. Evaluate the number of rows and columns and return the estimated number of blocks
 - a. Return the horizontal dividend (CH_d) and vertical dividend (CV_d)
 - b. Return the horizontal pad value (CH_p) and vertical pad value (CV_p)
4. Apply the padding pattern over the input image matrix according to CH_p and CV_p
5. Initialize the 2-Level iteration counters
6. Initialize the rotation counter and Input the round key value
7. Calculate the vertical seed value
 - a. $vSeed=(diffV*(imx-1))+1$
8. Calculate the vertical cap value
 - a. value $vCap=diffV*(imx)$
9. Calculate the horizontal seed value
 - i. $hSeed=(diffH*(imy-1))+1$
10. Calculate the horizontal cap value
 - i. $hCap=diffH*(imy)$
11. Segment the smaller chunk from the cover image according the the $vSeed$, $vCap$, $hSeed$ and $hCap$
 - i. $CoverChunk=IC_m(vSeed:vCap,hSeed:hCap);$

Algorithm 2: Dynamic Fuzzy Rule Set Determination for Secret (DFRSD-Secret)

1. Input secret image matrix (SC_m)
2. Calculate the image size in number of rows (SC_r) and columns (SC_c)
3. Evaluate the number of rows and columns and return the estimated number of blocks
 - a. Return the horizontal dividend (SH_d) and vertical dividend (SV_d)
 - b. Return the horizontal pad value (SH_p) and vertical pad value (SV_p)
4. Apply the padding pattern over the input image matrix according to SH_p and SV_p
5. Initialize the 2-Level iteration counters
6. Initialize the rotation counter and Input the round key value
7. Calculate the vertical seed value
 - a. $seeds=(diffV*(imx-1))+1$
8. Calculate the vertical cap value
 - a. value $vCap=diffV*(imx)$
9. Calculate the horizontal seed value
 - i. $hSeed=(diffH*(imy-1))+1$
10. Calculate the horizontal cap value
 - i. $hCap=diffH*(imy)$
11. Segment the smaller chunk from the secret image according the $vSeed$, $vCap$, $hSeed$ and $hCap$
 - i. $secretChunk= SC_m(vSeed:vCap,hSeed:hCap,1);$

After selecting the secret object, it is converted into the encrypted form using XOR encryption key. After that the data that is hidden is compared against each data blocks of cover image and will return the most similar matrix.

RESULTS AND DISCUSSION

The main advantage of this proposed work is that it is more secure and has high capacity as compared to the method proposed by Hsien-Wen Tseng[54] and Deepali [55] as seen from table 4.14 and table 4.15. The PSNR and MSE values calculated are better than those obtained by Hsien-Wen Tseng's method and Deepali's method using Dynamic fuzzifier Model and NEDI algorithm. This utilizes more edges areas rather than smooth area for embedding. The graphical analysis of PSNR, capacity has been shown in figure 4.22-4.23.

Tabel 4.14
Comparison of PSNR values

Cover Image	PSNR (Hsien-Wen Tseng's Method)	PSNR (Deepali's method)	PSNR (by Proposed Method)
Lena.bmp	50.79	52.39	55.67
Pepper.bmp	50.23	51.93	55.05
Mandril.bmp	49.11	51.11	54.44

The above table shows that the proposed method has been achieved the better results as compared to the previously introduced methods.

Similarly the comparison of the various methods with the proposed method on the basis of PSNR achieved is represented in graphical form that is shown in the following figure 4.22.

From figure 4.22 it can be seen that the proposed method has been achieved a PSNR value of 55.08 on an average whereas Hsien-Wen Tseng's method has achieved PSNR value of 50.79 and deepali's method has been achieved PSNR value of 52.39 on an average. From these results it can be seen that the proposed method has been achieved better performance.

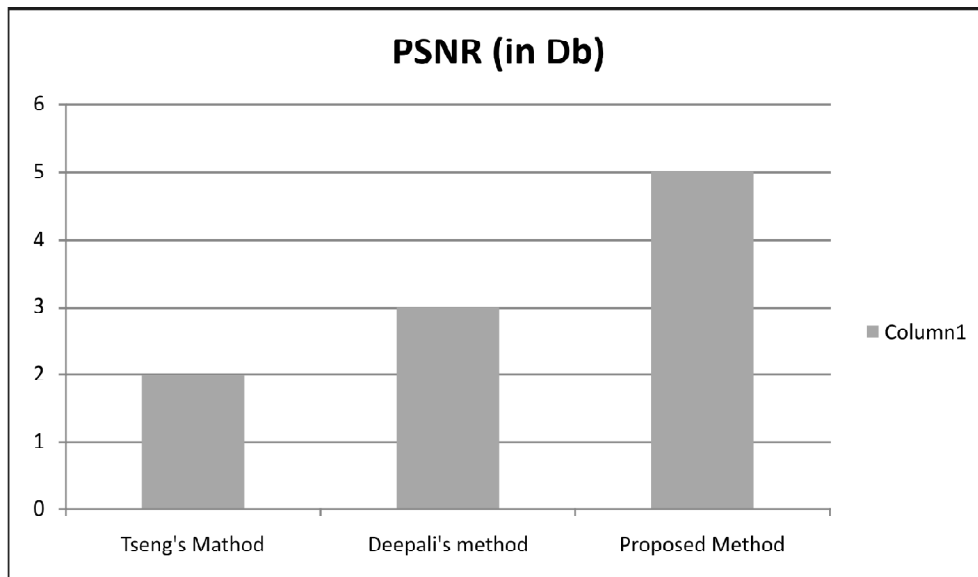


Figure 4.22: PSNR (in Db)

Tabel 4.15
Comparison of Payload Capacity

Cover Image	PSNR (Hsien-Wen Tseng's Method)	PSNR (Deepali's method)	PSNR (by Proposed Method)
Lena.bmp	7.53	10.09	11.11
Pepper.bmp	7.46	9.49	11.28
Mandril.bmp	8.63	10.24	10.24

Table 4.15 is showing the values of capacity achieved (calculated in bpp by proposed method, Tseng's method and deepali's method. Form these values it can be concluded that the proposed method has achieved a better capacity as compared to previous methods.

Similarly the comparison of the various methods with the proposed method on the basis of embedding capacity is represented graphical form the is shown in the following figure 4.23.

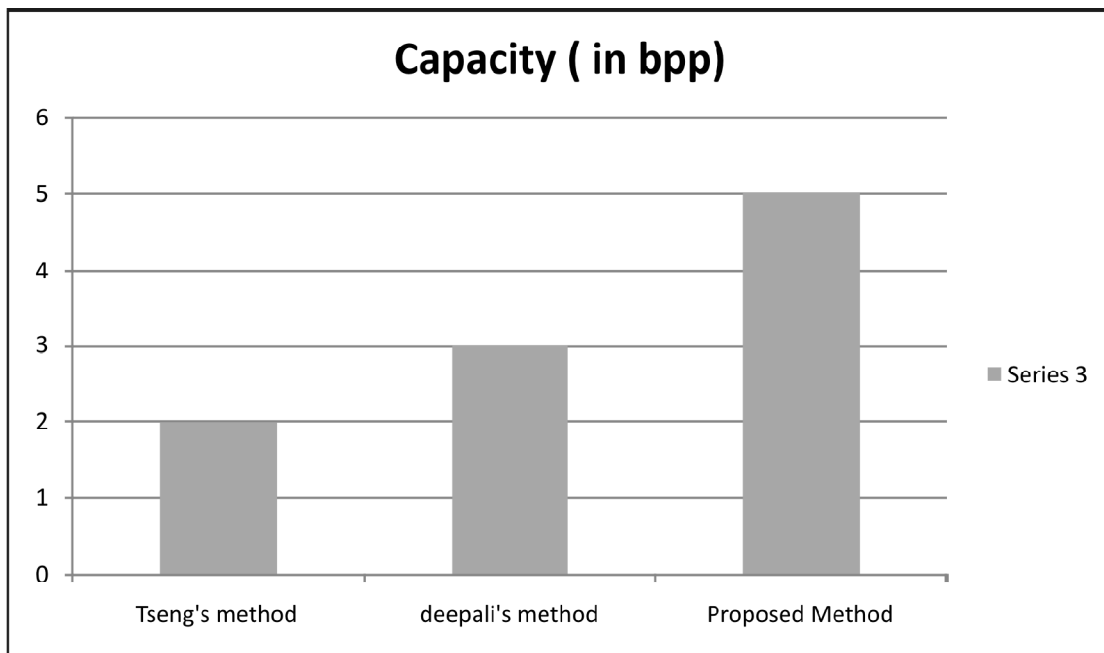


Figure 4.23: Capacity (in bpp)

Form figure 4.23 it can be seen that the proposed method has been achieved a capacity value of 11.11 bpp on an average whereas tseng's method has been achieved 9 bpp and deepali's method has achieved capacity value of 10.24 on an average. Form these results it can be seen that the proposed method has been achieved better performance.

CONCLUSION AND FUTURE SCOPE

The embedding algorithm has been designed with the spatio-temporal ability to embed the secret data in the block edges of the cover image, while utilizing the non-overlapping block-based division. After selecting the secret object, it is converted into the encrypted form using XOR encryption key. The new edge directed interpolation (NEDI) has been utilized for the adaptive edge pixel selection for the robust embedding with minimum grade change in the cover image set. The proposed algorithm has been obtained peak signal to noise

ratio (PSNR) value along with the improved capacity of image. This algorithm has been also obtained high resistance against different steganalysis attacks like Histogram attack, Chi-Square attack and RS attack and various image manipulations like cropping, compression. The performance evaluation has been performed in the form of payload capacity, elapsed time and PSNR and MSE. The payload capacity has been recorded 11.28 bpp with the larger RGB cover images of size 1.43 MB to 2 MB for hidden image of size 400KB to 900 KB. The PSNR value of 52 to 55 Db and MSE value of 0.00554 has been recorded during Embedding process which improvise the better quality of the results of the proposed model. The various steganalysis attacks have been performed on the stego image to prove the robustness of the algorithm. The result obtained after implementing the proposed system show the efficiency of the proposed system. In the future, the proposed model can be enhanced with the swarm intelligence algorithm for the dynamic selection of the pixels from the cover object in accordance with the secret image. Also, the proposed model can be enhanced by using the dual encryption mechanism by combining the public cryptosystem with symmetric encryption along with the image quality optimization method.

REFERENCES

- [1] Artz, D.: 'Digital watermarking: hiding data within data', IEEE Int. Comput., 2001, 5, (3), pp. 75–80.
- [2] T. Jamil, "Watermarking: The art of hiding information in plain sight", IEEE Potentials, Vol. 18, No. 1, pp. 10-12. 2011.
- [3] F. Petitcolas, R. Anderson and M. Kuhn, "Information Hiding – A Survey", Proceedings of the IEEE, Vol. 87, 1999.
- [4] R. Popa, "An analysis of watermarking techniques" The Politehnica University of Timisoara, Department of Computer Science and Software Engineering, 1998.
- [5] Provos and N. Honeyman, "Hide and seek: An introduction to watermarking", IEEE Security & Privacy Magazine Vol. 1, pp. 32-44, 2003.
- [6] Benlcouiri, Y., Ismaili, M., Azizi, A., and Benabdellah, M., "Securing images by secret key watermarking," Applied Mathematical Sciences, vol. 6, no. 111, pp. 5513–5523, 2012.
- [7] www. Google.com\ A Brief History of Watermarking.html.
- [8] Lee, Y.K., Chen, L.H.: 'High capacity image watermarking model', Proc. of IEEE on Vision, Image and Signal Process., vol. 147, no. 3, pp. 288–294, 2000.
- [9] T Morkel, JHP Eloff and MS Olivier, "An Overview of Image Watermarking," in Proceedings of the Fifth Annual Information Security South Africa Conference (ISSA2005), Sandton, South Africa, June/July 2005
- [10] K. Hempstalk, "Hiding Behind Corners: Using Edges in Images for Better Watermarking", Proceedings of the Computing Women's Congress, 2006.
- [11] B.Schneier, "A self-study course in block cipher cryptanalysis", Cryptologia, vol.24, No.1, pp.18-33, 2000.
- [12] Biham, Eli, A. Shamir, "Differential cryptanalysis of the data encryption standard", Springer-Verlag, Vol. 28, 1993.
- [13] H. O. Alanazi, B. B. Zaidan, A. A. Zaiden, H. A. Jalab, M. Shabbir and Y. A. Nabhani, " New comparative study between DES, 3DES and ASE within Nine factor", Journal of computing, vol.2, No.3,pp. 152-157, 2010.
- [14] Specification for the advanced Encryption Standard (AES), Federal Information processing Standards Publication 197, 2001.
- [15] H. V. Desai, "watermarking, Cryptography, Watermarking: A comparative study", Journal of Global Research in Computing science, Vol. 3, No.12, pp. 33-35, 2012.
- [16] M. Agarwal, "Text watermarking Approaches: A comparison", International Journal of Network Security & Its Application (IJNSA), Vol. 5, No. 1, pp. 91-103, 2013.
- [17] S.Malviya, M Saxena and A.khare, " Audio Watermarking by different methods", International Journal of Emerging Technology and Advanced Engineering, Vol. 2, No. 7, pp. 371-375, July 2012.
- [18] R. Doshi, P. Jain and L. Gupta, "Watermarking and Its Applications in Security", International Journal of Modern Engineering Research, Vol. 2, No. 6, pp. 4634-4638,2012.

- [19] Jankowski, B. W. Mazurczyk and K. Szczepiorski, "padsteg: Introduction interprotocol watermarking", *Telecommunications System*, Vol. 52, No. 2, pp. 1101-1111, 2013.
- [20] Abbas Cheddad, "Digital image watermarking: Survey and analysis of current methods", *Signal Processing*, Volume 90, Issue 3, pp. 727-752, Elsevier, March, 2010.
- [21] A. Shadded, j. Condell, K. Curran, and P. Mckevtt, "Biometric inspired digital image steganography", *Proceedings of the 15th Annual IEEE International Conference and workshop on the Engineering of Computer based system*, pp. 159-168, 2008.
- [22] P. Kruus, C. Scace, M Heyman, and M. Mundy, "A survey of watermarking techniques for image files", *advanced security Research Journal*, Vol. 5, No. 1, pp. 41-52, 2003.
- [23] M. S. Sutaone and M. V. Khandare, "Image based watermarking using LSB Insertion Techniques, *Wireless Mobile and Multimedia networks*", IET international Conference, pp. 146-151, 2008.
- [24] N.F. Johnson and S. Jajodia, "Exploring watermarking: Seeing the unseen", *IEEE Computer journal*, Vol. 31, No. 2, pp. 26-34, 1998.
- [25] B. C. Nguyen, S. M. Yoon and H. K. Lee, "Multi bit plane image watermarking", *5th International workshop IWDW, Lecture Notes in computer science springer*, Vol. 4283, pp. 61-77, 2006
- [26] X. Zhang and S. Wang, "watermarking using multiple base notational system and human vision sensitivity", *IEEE Signal Processing letters*, Vol. 12, No. 1, pp. 67-70, 2005.
- [27] B. Chen and G. W. Worwell, "Quantization index modulation: A class of proveably good methods for digital watermarking and information embedding", *IEEE Transaction Information Theory*, Vol. 47, No.4, pp. 1423-1443, 2001.
- [28] N.F. Johnson and S. Katzenbeisser, "A survey of watermarking techniques", *Information Hiding*, pp. 43-78, 2000.
- [29] A. Cheddad J. Condeed, K. Curran and P.M. Kevitt, "Digital image watermarking: survey and analysis of current methods", *Signal Processing Journal*, Vol. 90, No. 3, pp. 727-752, 2011.
- [30] A. Westfeld, "F5-A watermarking algorithm: high capacity despite better steganalysis", *Proceedings of the 4th Information Hiding workshop, Lecture Notes in Computer Science Springer*, pp.289-302, 2001.
- [31] P. Sallee, "Model based watermarking", *proceeding of the 2nd International Workshop on Digital watermarking, lecture Notes in Computer science springer*, pp. 254-260, 2004.
- [32] K. Solanki and B. S. Manjunath, "Yass: yet another Watermarking scheme that resists blind steganalysis", *Proceeding of the 9th Information Hiding Workshop, Lecture Notes in Computer Science Springer*, pp. 1-16,2007.
- [33] N. Hamid, A. Yahya, R. B. Ahmad and O. M. Qershi, "Image watermarking Techniques: An Overview", *International Journal of Computer Science and security*, Vol. 6, No. 3, pp. 168-187, 2012.
- [34] J. Fridrich and M. Goljan, "Practical Steganalysis – State of the Art", *proceedings of SPIE*, Vol. 4675, pp. 1-13, 2002.
- [35] A. Kumar and S. Khurana, "Steganalysis techniques on Gray scale Image by Varying message length using Adaptive Histogram Equalization Attack", *International Journal of Computer Application*, Vol. 90, No. 14, pp. 33-36, 2014.
- [36] A. Westfeld and A. Pfitzmann, "Attacks on Watermarking System", *Lecture Notes in Computing Science Springer-Verlag*, Vol.1768, pp. 61-78, 2014.
- [37] C. Stanley, "Pairs of Values and Chi-squared Attack", *Master's Thesis, Department of mathematics, Iowa State University*, 2005.
- [38] J. Fridrich, M. Goljan and R. Du, "Reliable detection of LSB watermarking in grayscale and color images", *Proceedings ACM Workshop on Multimedia and Security*, pp. 27-30, 2001.
- [39] J. Fridrich, "Application of data hiding in digital images", *tutorial for the ISPACS Conference*, 1998.
- [40] M. Juneja and P. Sidhu, "A Survey of Image Watermarking techniques", *International Journal of Advanced Science and Technology*, Vol. 5, No. 2, 2013.
- [41] M. Juneja and P. Sidhu, "Implementation of Improved Watermarking Techniques for 24-bit Bitmap Images in Communications", *Journal of American Science*, Vol. 2, No. 2, pp. 36-42, 2009.

- [42] Eltyeb E. A bed Elgabar, "Comparison of LSB Watermarking in BMP and JPEG Images", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-5, November 2013.
- [43] Wu, D.C., and Tsai, W.H.: 'A watermarking method for images by pixel-value differencing', Pattern Recognit. Lett. 2003, 24, (9-10), pp. 1613–1626.
- [44] H. C. Wu, N. I. Wu, C. S. Tsai, and M. S. Hwang, "Image watermarking scheme based on pixel-value differencing and LSB replacement methods," Proceedings of 2005 Instrument Electric Engineering, Vis. Images Signal Process, vol. 152, no. 5pp . 611–615, 2005.
- [45] Santosh Arjun, N. and Atul Negi, "A Filtering Based Approach to Adaptive Watermarking," 10th Conference, TENCON 2006, IEEE, pp. 1-4, Nov 2006.
- [46] Manglem Singh, Birendra Singh, Shyam Sundar Singh, "Hiding Encrypted Message in the Features of Images", IJCSNS, VOL. 7, No.4. April, 2007.
- [47] Cheng-Hsing Yang, Chi-Yao Weng, Shih-Jeng Wang, Hung-Min Sun, "Adaptive Data Hiding in Edge Areas of Images with Spatial LSB Domain Systems". IEEE Transactions on Information Forensics and Security, Vol. 3, No. 3,pp. 488-497, 2008.
- [48] C.-H. Yang and M.-H. Tsai, "Improving Histogram-based Reversible Data Hiding by Interleaving Predictions", IET Image Processing, Vol.4. Iss. 4 pp. 223-234, 2010.
- [49] Weiqi lu, member, IEEE, fangjun huang, member, IEEE et al., "edge adaptive image watermarking based on LSB matching revisited", IEEE transactions on information forensics and security, vol. 5, no. 2, June 2010.
- [50] Chen, W.-J., Chang, C.-C., and Le, T., "High payload watermarking mechanism using hybrid edge detector," Expert Systems with Applications, vol. 37, no. 4, pp. 3292–3301, 2010.
- [51] Anastasia Ioannidou, Spyros T. Halkidis, George Stephanides, "A novel technique for image watermarking based on a high payload method and edge detection", Expert Systems with Applications, Vol. 39, pp. 11517–11524, 2012.
- [52] Hussain, M. and Hussain, "Embedding data in edge boundaries with high PSNR", Proceedings of 7th International Conference on Emerging Technologies (ICET 2011), pp.1-6, Sept 2011.
- [53] Mamta Juneja and Parvinder S. Sandhu, "A New Approach for Information Security using an Improved Watermarking Technique," J Inf Process Syst, vol. 9, no. 4, 2013.
- [54] Hsien-Wen Tseng, Hui-Shih Leng, "high-payload block-based data hiding scheme using hybrid edge detector with minimal distortion" , IET Image Process, Vol. 8, Iss. 11, pp. 647–654, 2014.
- [55] Deepali Singla and Mamta Juneja, "Hybrid Edge Detection-Based Image Watermarking Technique for Color Images", Intelligent Computing, Communication and Devices, Advances in Intelligent Systems and Computing, Springer India, 2015.
- [56] Youssef Bassil, "Image Watermarking Based on a Parameterized Canny Edge Detection Algorithm," International Journal of Computer Applications (0975 – 8887), vol. 60, no. 4, 2012.
- [57] Cheddad, A., Condell, J., Curran, K., and Mc Kevitt, P., "Digital image watermarking: Survey and analysis of current methods," Signal Processing, vol. 90, no. 3, pp. 727–752, 2010.
- [58] Ran-Zan Wang, Chi-Fang Lin, Ja-Chen Lin (2000), "Hiding Data in Images by Optimal Moderately Significant Bit Replacement" IET Electronics Letters, vol. 36, no. 25, pp. 2069-2070.
- [59] J. Canny, "A Computatinal Approach to Edge Detection," IEEE Tranaction on Pattern Analysis and Machine Intelligence, vol. 8, pp. 679-687,1986.
- [60] TALAI Zoubir, TALAI Abdelouaheb , "A Fast Edge Detection Using Fuzzy Rules," International conference on CCCA, pp. 1-5, 2011.
- [61] T. Chaira and A.K. Ray, "A new measure using intuitionistic fuzzy set theory and its application to edge detection", Applied Soft Computing, Vol. 8, No. 2, pp. 919-927, 2008.