Securing Image Using Enhanced Watermarking Technique

Swati Gupta, Raju Baraskar, Shikha Agrawal

Abstract: ***The image is significantly used in applications such as medical area, research area, image conferencing, a military image system, online transactions, digital signatures, passwords etc. But not everyone who uses this network is going to play by the rules or have the best interest at heart. Just as we have physical security like locks, fences and police officers to minimize crime in the real world. We need some security to minimize crime and harm in the virtual world. Three important factors form the security objectives of the digital content: they are Availability, Confidentiality, and Integrity. Watermarking techniques along with some Cryptography are used to protect the confidentiality of data. Watermarking is basically a process of injecting data into an image in such a way that it can depict the authenticity of those possessing it. The digital information hidden inside an image is imperceptible to the user but can be easily detected by a computer or various digital devices. Watermarking Technique has proved to be a powerful technique for image security and a lot of research has been made over the years to how to embed the watermarks and recover the watermarks effectively. These types of technique where watermark can be fully extracted from the image and along with the restoration of the cover are popularly known as Reversible Watermarking techniques. These techniques have significantly gained importance due to this excellent recovering property making them suitable for content authentication based applications. However, they are not able to identify any modifications or changes done in watermark making it susceptible to tamper location-based attacks. Due to the rapid development of watermarking techniques, a concluding review of recent research in this field is highly desirable. However, the major focus of this paper is on tamper localization based reversible watermarking techniques.***

Keywords: ***Watermarking Techniques, Reversible Watermarking, Histogram Modification, Tamper Localization, Image security***

I. INTRODUCTION

Reversible watermarking is the process where some data is embedded inside an image and later that data is extracted back from the image easily without any quality degradation in original image. This lossless recovery is useful in applications where security concern arises such as medical image analysis, forensics, military images, etc. Honsinger et al.[1] proposed one of the first reversible watermarking schemes. It was based on the addition of modulo 256. Macq[2] developed a new approach by combining the patchwork algorithm and modulo addition to achieve reversibility. Later Fridich et al. [3] proposed a reversible watermarking technique which doesn't use any modulo additions A significant amount of research is done over the years in this field [4, 5, 6, 7, 8, 9] and newly emerging watermarking techniques can be categorized into four types:

(i) Reversible Watermarking based on Compression,
(ii) Reversible Watermarking based on Histogram Modification,
(iii) Reversible Watermarking based on Difference Expansion, and
(iv) Reversible Watermarking based on Tamper Localization.

Tamper localization based reversible watermarking technique is able to identify any modifications or changes done in watermark making it susceptible to tamper location-based attacks. This field is new and recently some work is reported in tamper based reversible watermarking. It is suitable for content-based applications and is fragile. It means a system when suffering from any tamper based attacks would break indicating tampering of watermark image. The tamper based algorithms attempt to determine such locations and recover the original image. There are two fragile watermarking methods used for image tamper identification and localization: pixel-wise method and the block-wise based.

The objective of this project is to build an enhanced watermarking technique which can determine the tamper detection easily and increase the self-recovery rate and is best in terms of efficiency, security, and is suitable for fragile applications.

II. RESEARCH METHODOLOGY

The watermarking approach used in our dissertation work for tamper detection and self-recovery is dual in nature [10]. It is type of watermarking technique which is fragile and blind in nature. In this process, two image digests are created for each non-overlapping. These copies use lifting wavelet transform (LWT) [11] and half-toning technique [12, 13], and LSB-Matching technique is used for embedding. It is clear from the experimental results that the above technique generates image digest which have better quality in comparison with earlier image digests which are calculated by averaging of pixel values.

Manuscript published on 30 September 2019.
*****Correspondence Author(s)

Swati Gupta, Student, Department of Computer Science and Engineering, University Institute of Technology, RGPV, Bhopal(M.P), India.
Raju Baraskar, Assistant Professor, Department of Computer Science and Engineering, University Institute of Technology, RGPV, Bhopal(M.P), India.
Shikha Agrawal, Assistant Professor, Department of Computer Science and Engineering, University Institute of Technology, RGPV, Bhopal(M.P), India.

The LSB Rounding method is used to increase the quality of image digest. Arnold Cat Map (ACM) [14] is employed to increase the security and Shift-aside technique to enhance rate of recovery.

By combining the properties and advantages of other tamper based watermarking techniques we get an efficient and enhanced watermarking techniques which provides greater security. There are mainly three phases in the method we have used to implement the watermarking technique:

(A) **Watermark Creation and Embedding**- The host image is used to create image digests which are obtained using the Lifting Wavelet Transform and Stucki kernel. The image digest bits are used to create authentication bits. The permutation is applied to the coefficients to increase security. Then all the bits are shuffled and encrypted with the help of ACM. Eventually, the LSB matching technique embeds the image digests bit and authentication bits into the image. It is explained in Fig.1.

(B) **Tamper Detection and Authentication**- The watermark contains image digests and authentication bits. Therefore the first step is to extract these bits for authentication purposes. Then the image is checked against any tampering attacks. The actual content can be recovered using the recovery phase explained in the next step in case any tampering occurs.

(C) **Recovery and Reconstruction**-The regions which contain tampering are recovered with the help of image digests which are already embedded in the host image as illustrated in Fig.2.

III. RESULTS AND DISCUSSION

The algorithm used for implementation is found to have better performance than the existing algorithms. The standard metrics known as Peak Signal to Noise Ratio (PSNR) is employed to determine the quality of watermarked images in the below experiments. More is the value of metrics, better is the image quality and imperceptibility.

The PSNR evaluates the quality of the recovered image in comparison to the original. It is measured in decibels (dB). It is defined using MSE for two monochrome images p_1 and p_2 where one image is the noise approximation of the other images as in (1):

$$PSNR = 10\log_{10}\left(\frac{MAX_{p_1}^2}{MSE}\right) = 20\log_{10}\left(\frac{MAX_{p_1}}{\sqrt{MSE}}\right) \ldots\ldots\ldots\ldots\ldots\ldots (1)$$

Here, MAX_{p1} denotes the maximum pixel value of the image. If the pixels are represented using 8 bits, the value is 255.

Fig.3 shows 6 grayscale images used in proposed work for testing. The image size is 512 ×512 pixels and is in bitmap format.

The quality metric based on PSNR values prove that the proposed method has outstanding tamper detection accuracy and good recovery and quality rate.

Also, a comparative analysis is done by calculating the average PSNR value of all the results obtained in each work. It is obtained using (2):

$$PSNR_{avg} = \frac{1}{n}\sum_{i=0}^{n-1} PSNR_i \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

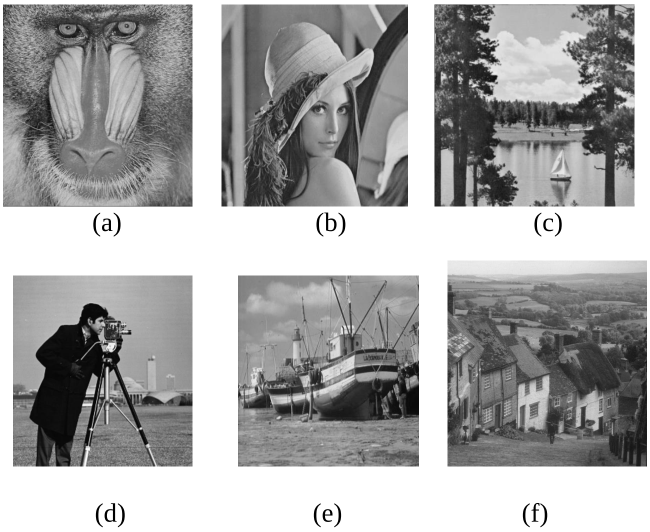


Fig.3. Standard test images (512×512) used in proposed work: (a) Baboon (b) Lena (c) Lake (d) Boat (e) Camera (f) Goldhill

To evaluate the proposed work, a few experiments are done to demonstrate the performance of tamper identification and recovering capability by analyzing and comparing previous work. General tampering for example addition of objects, swapping the parts of the image and various attacks is applied after watermarking the image to analyze the efficiency of the proposed method.The PSNR based results of watermarked images for some previous fragile methods and the proposed work are showed in Table I. It is clear from the results that the PSNR reached a quite high value of 46 dB by applying LSB-matching technique and 44 dB without it. Thus, the proposed method based on LWT and half-toning retains better image quality compared to other methods.

Briefly, we have proved remarkable results of the proposed method. It is clear from the PSNR metrics that the method used in implementing our work has high accuracy of tampering detection, high recovery and quality rate. The PSNR Graphs of each data set is plotted against them as shown in Fig.4.Also, an average value of PSNR in Fig.5 for each work is obtained and it is found that average PSNR value of our algorithm reached to the highest value as compared to existing works.

Also, to demonstrate the successful implementation of this watermarking technique we have used two standard metrics PSNR and SSIM to determine the image quality of the watermarked image and the recovered image. General tampering such as the addition of object is done to test the recovering capability of our work. Our results are tabularized in Table II.

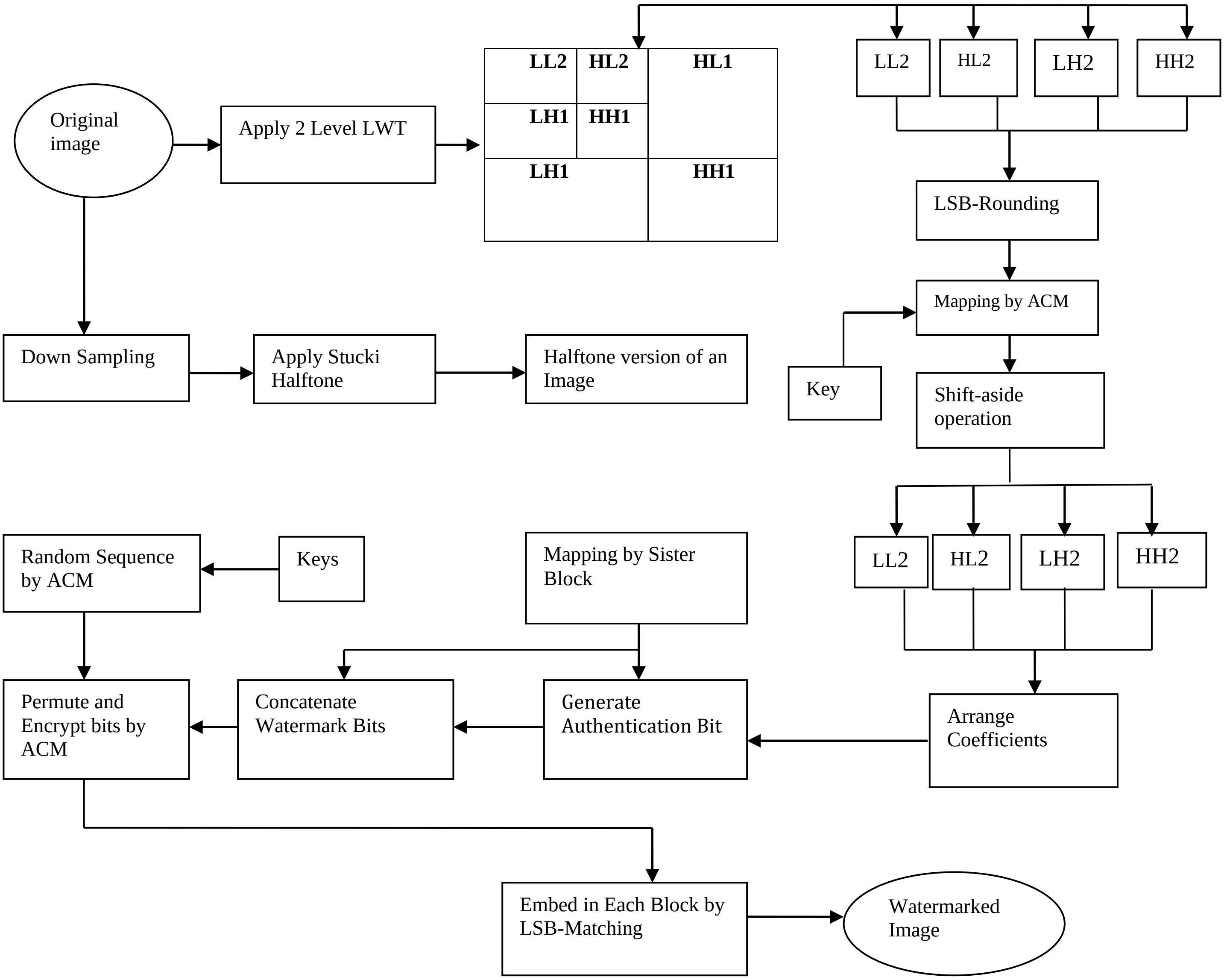


Fig.1. Block diagram for Generating and Embedding Watermark

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)
© Copyright: All rights reserved.

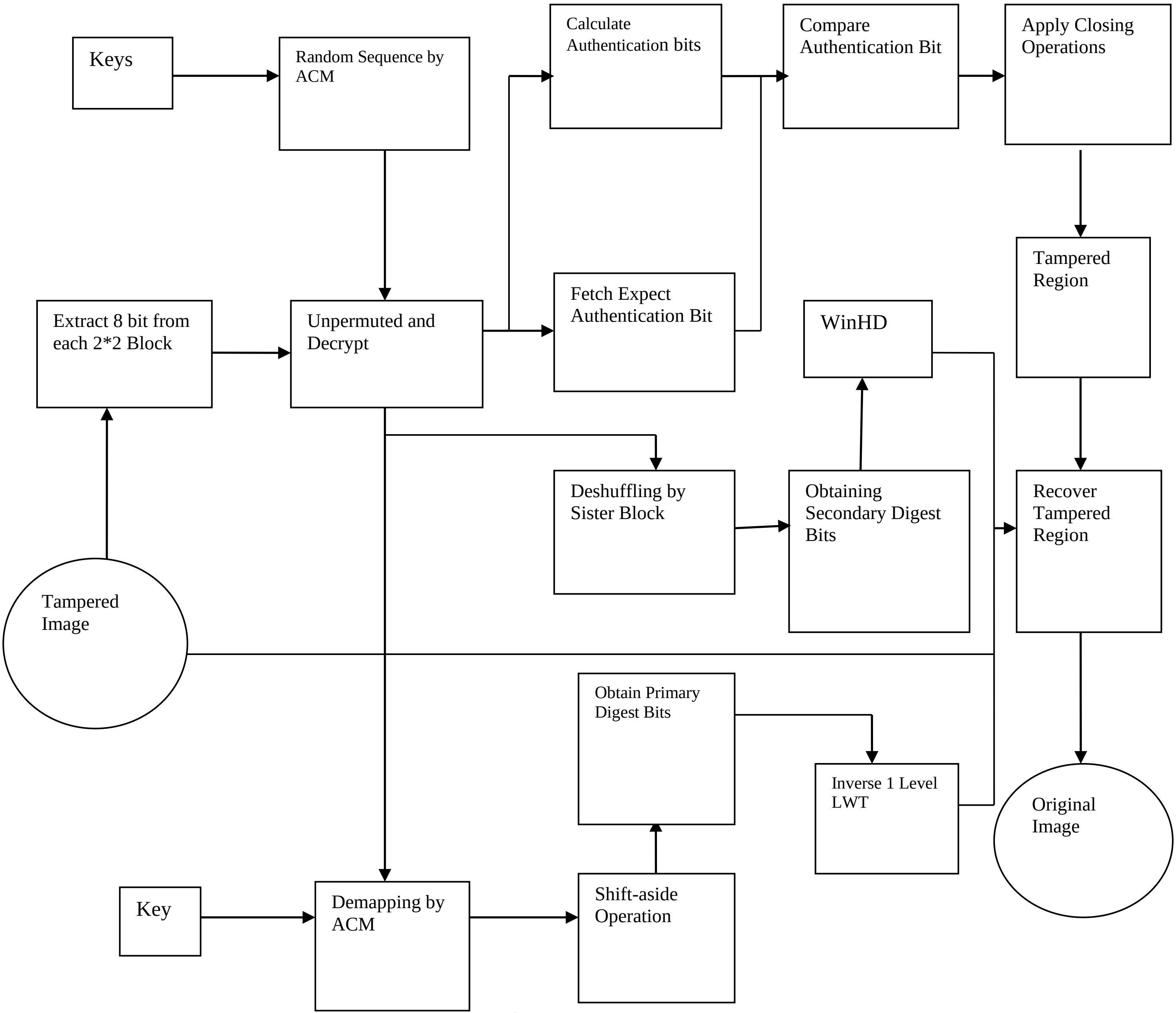

Keys
Random Sequence by ACM
Calculate Authentication bits
Compare Authentication Bit
Apply Closing Operations
Tampered Region
Extract 8 bit from each 2*2 Block
Unpermuted and Decrypt
Fetch Expect Authentication Bit
WinHD
Deshuffling by Sister Block
Obtaining Secondary Digest Bits
Recover Tampered Region
Tampered Image
Obtain Primary Digest Bits
Inverse 1 Level LWT
Original Image
Key
Demapping by ACM
Shift-aside Operation

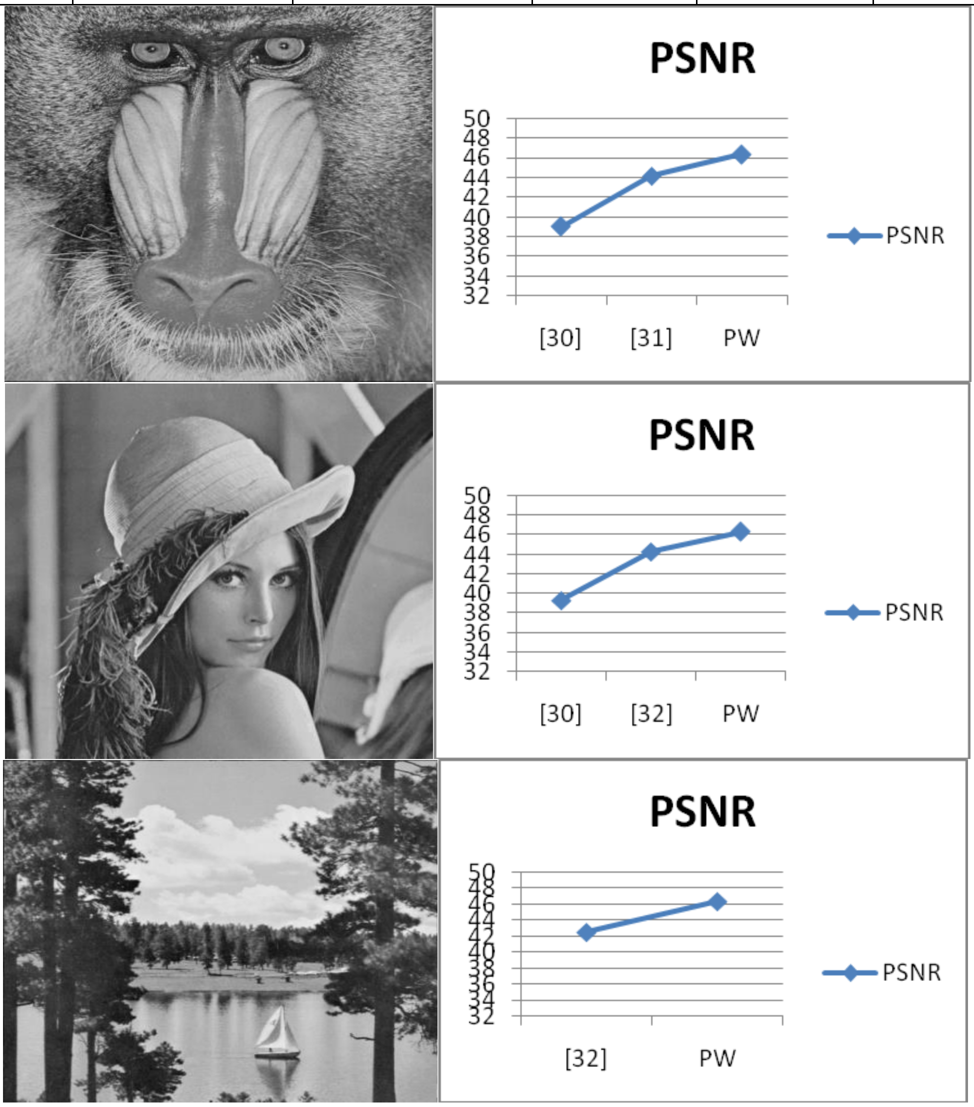
Fig.2. Block Diagram for recovering tampered regions and authentication

Retrieval Number: J99490881019/19©BEIESP
DOI: 10.35940/ijitee.J9949.0981119
Journal Website: www.ijitee.org

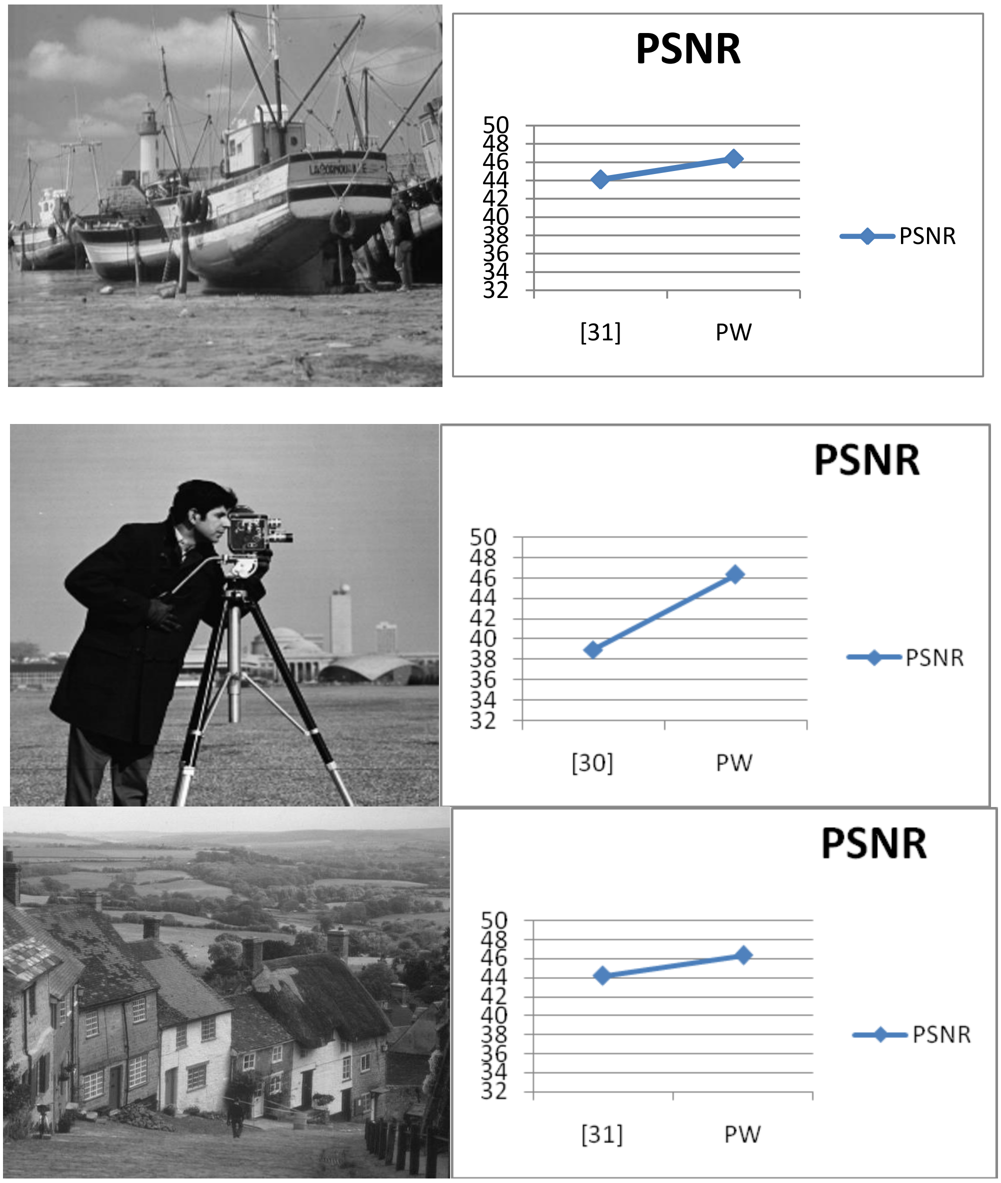
Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

Table-I: The PSNR values of watermarked images for proposed work and related works.

Image	Proposed Work		D.Singh[15]	F.Chao[16]	Zhang[17]
	Without LSB-matching	By LSB-matching			
Baboon	44.1502	46.3805	39.03	44.17	-
Lena	44.1669	46.3491	39.31	-	44.27
Lake	44.1558	46.3695	-	-	42.49
Boat	44.0289	46.3635	-	44.11	-
Camera	44.1552	46.3628	39.00	-	-
Goldhill	42.6835	46.3764	-	44.16	-



(a)



(b)

Fig.4. (a) & (b) PSNR Value Graph for proposed work and existing works.

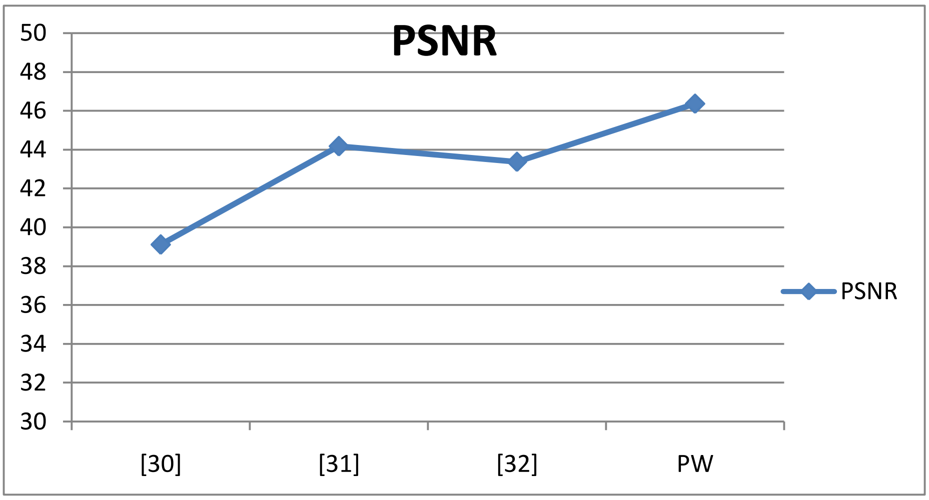


Fig.5.Comparative Analysis of proposed work with existing work (Singh et al. [30], Chao et al. [31], Zhang et al. [32])

Table-II: Result Calculation for proposed work

Image	Watermarked Image		Recovered Image	
	PSNR	SSIM	PSNR	SSIM
Baboon	46.3805	0.99684	29.7704	0.90881
Lena	46.3491	0.99068	32.9943	0.93774
Lake	46.3695	0.99296	32.4409	0.94146
Boat	46.3628	0.99297	32.0066	0.93396
Camera	46.3635	0.98737	33.7735	0.96553
Goldhill	46.3764	0.99393	32.228	0.90946

IV. CONCLUSION

With the emergence of the Internet, Computers have become interconnected allowing us to communicate easily and instantly across the globe. The image is widely used in many applications like government scanned documents, in medical diagnosis where any loss in confidential data can lead to serious copyright issues or can put the name of an organization at stake. Therefore it is necessary to keep the confidential information out of reach of malicious users who intend to break the security of the system. By use of certain algorithm, these issues can be solved and can be made secure by means of watermarking algorithms. Watermarking is basically a process of injecting data into an image in such a way that it can depict the authenticity of those possessing it. The digital information hidden inside an image is imperceptible to the user but can be easily detected by a computer or various digital devices. Watermarking Technique has proved to be a powerful technique for image security and a lot of research has been made over the years to how to embed and recover the watermarks more efficiently. However, they are not able to identify any modifications or changes done in watermark making it susceptible to tamper location-based attacks. In order to overcome these limitations, tamper detection and self-recovery is done using an enhanced watermarking technique. The proposed algorithm that is the enhanced watermarking algorithm provides better security, high rate of recovery and increased quality of the watermarked image.

REFERENCES

1. C.W. Honsinger, P.W. Jones, M. Rabbani, J.C. Stoffel, “Lossless recovery of an original image containing embedded data”, U.S. Patent No. 6,278,791, 2001.
2. Macq, “Lossless multiresolution transform for image authenticating watermarking”, in Proc. EUSIPCO, 2000, pp. 533–536.
3. J. Fridrich, M. Goljan, R. Du, Lossless data embedding — “A new paradigm in digital watermarking”, EURASIP J. Appl. Signal Process. 2002 (2) (2002) 185–196.
4. D. Zheng, Y. Liu, J. Zhao, A. El Saddik, “A survey of RST invariant image watermarking algorithms”, ACM Comput. Surv. 39 (2) (2007).
5. J.-M. Guo, “Watermarking in dithered halftone images with embeddable cells selection and inverse halftoning”, Signal Process. 88 (6) (2008) 1496–1510.
6. R. Caldelli, F. Filippini, R. Becarelli, “Reversible watermarking techniques: an overview and a classification”, EURASIP J. Inform. Security 2010 (2010) 1–19.
7. I.J. Cox, M.L. Miller, J.A. Bloom, J. Fridrich, T. Kalker, “Digital Watermarking and Steganography”, 2nd ed., Morgan Kaufmann, 2008.
8. J. Feng, I. Lin, C. Tsai, Y. Chu, “Reversible watermarking: current status and key issues”, Int. J. 2 (3) (2006) 161–170.
9. J. Fridrich, M. Goljan, R. Du, “Lossless data embedding — a new paradigm in digital watermarking”, EURASIP J. Appl. Signal Process. 2002 (2) (2002) 185–196.
10.Behrouz Bolourian Haghighi, Amir Hossein Taherinia, Ahad Harati, “TRLH: Fragile and blind dual watermarking for image tamper detection and self-recovery based on lifting wavelet transform and half toning technique”, Journal of Visual Communication and Image Representation (2018)
11.W. Sweldens, The lifting scheme: A construction of second generation wavelets, SIAM Journal on Mathematical Analysis29 (2) (1998) 511{546.
12.P.-E. Axelson, Quality measures of halftoned images (a review)(2003) 81
13.J. F. Jarvis, C. N. Judice, W. Ninke, “A survey of techniques for the display of continuous tone pictures on bilevel displays”, Computer Graphics and Image Processing 5 (1) (1976) 13{40.
14. V. I. Arnold, A. Avez, Ergodic problems of classical mechanics, Vol. 9, Benjamin, 1968.
15.D. Singh, S. K. Singh, “Dct based efficient fragile watermarking scheme for image authentication and restoration”, Multimedia Tools and Applications 76 (1) (2017) 953{977.doi:10.1007/s11042-015-3010-x.URL http://dx.doi.org/10.1007/s11042-015-3010-x
16. F. Cao, B. An, J. Wang, D. Ye, H. Wang, “Hierarchical recovery for tampered images based on watermark self-embedding, Displays 46(2017)52{60,doi:https://doi.org/10.1016/j.displa.2017.01.001
17.C. Qin, P. Ji, X. Zhang, J. Dong, J. Wang, “Fragile image watermarking with pixel-wise recovery based on overlapping embedding strategy”, Signal Processing 138 (2017) 280 { 293.doi:https://doi.org/10.1016/j.sigpro.2017.03.033.

AUTHORS PROFILE

Swati Gupta, pursuing Dual Degree Integrated Course in Computer Science and Engineering from University Institute of Technology, Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal (MP) India. She is currently a student in final year doing research on Reversible Watermarking Techniques. Her research areas include Image Processing and Image Security.

Dr Raju Baraskar is an Assistant Professor in Department of Computer Science & Engineering at University Institute of Technology, Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal (MP) India. He obtained B.E. from SATI Vidisha(M.P.), then M.Tech. and Ph.D in Computer Science & Engineering from Maulana Azad National Institute of Technology, Bhopal. He has more than twelve years of teaching experience. His area of interest is Network Security, Vehicular Ad hoc networks, Image Processing, Parallel, Algorithm Pattern matching algorithm and Data Mining etc. He has published more than 20 research papers in different reputed international journals and 02 chapters. He is also member of various academic societies such as IEEE etc.

Dr Shikha Agrawal is an Assistant Professor in Department of Computer Science & Engineering at University Institute of Technology, Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal (MP) India. She obtained B.E., M.Tech and Ph.D in Computer Science and Engineering from Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal. She has more than fifteen years of teaching experience. Her area of interest is Artificial Intelligence, Soft Computing and Particle Swarm Optimization and Database. She has published more than 40 research papers in different reputed international journals and 10 chapters. For her outstanding research work in Information Technology, she has been rewarded as “Young Scientist” by Madhya Pradesh Council of Science and Technology, Bhopal. Her other extraordinary achievements include “ICT Rising Star of the Year Award 2015” in International Conference on Information and Communication Technology for Sustainable Development(ICT4SD-2015), Ahemedabad, India and Young ICON Award 2015 in Educational category by Dainik News Paper Patrika, Bhopal, India. She got recognition of IEEE as a senior member. She is also a member of various academic societies such as IEEE, ISTE, CSI, ACM & CSTA.