ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2014

Enhanced Tamper Localization Using Block Average Intensity

Anandita Bose[1], Medhashri B K[2], Ronica Jethwa[3], Sanjana Murthy[4]

B.E., Dept. of Telecommunication Engg., R.V.College of Engg., Karnataka, India[1]

B.E., Dept. of Telecommunication Engg., R.V.College of Engg., Karnataka, India[2]

B.E., Dept. of Electronics and Comm. Engg., R.V.College of Engg., Karnataka, India[3]

B.E., Dept. of Telecommunication Engg., R.V.College of Engg., Karnataka, India[4]

ABSTRACT: Tamper localization capable image watermarking scheme is able to detect the location of manipulated areas, and validate other areas as authentic. The usage of block average intensity in the tamper localization process is one of the popular techniques due to its easy implementation. The effectiveness of using existing and proposed average intensity techniques for tamper localization is tested. The results show that the existing tamper localization process will fail in certain conditions and cause some tampering to be left undetected. However the proposed tamper localization algorithm successfully identifies the region that has been manipulated when the image is received. The accuracy of 8 pixels is achieved by proposed algorithm.

KEYWORDS: ROI (Region of Interest), Block Average Intensity, Tamper Localization, Watermark, LSB (Least Significant Bit.)

I.INTRODUCTION

In recent times, the amount of digital images on the internet has seen an overwhelming increase. Image editing softwares are easily available to the users. In many situations, the changes made to the image maybe with bona fide purposes whereas tampering in a few situations maybe intentional. Multimedia authentication is a technology to check authenticity and integrity of multimedia signals [1-3]. It is often desirable to localize tampered pixels so that the unmodified parts can still be used if it lies within the region of interest [4,5]. Various applications in military and medical fields [6-8] require distortion free reception of images. Hence the images are watermarked to prevent unauthorized modification by authenticating the content of the image using reversible watermarking techniques. Watermarking scheme with tamper localization can detect and locate modification of pixels in an image and also verify rest of the areas of the image as authentic. Tampering can be localized by identifying the damage to the watermark.

The usage of Block Average Intensity in the Tamper Localization process is one of the popular techniques due to its easy implementation. The effectiveness of the existing Tamper Localization using Block Average Intensity proposed by Liew and Jasni [9] has been tested. The results show that the Tamper Localization process will fail in certain conditions causing some tampering to be left undetected. In the existing Tamper Localization scheme, validity and parity bits are used as authentication bits. These two bits, along with the Block Average Intensity, are used to verify whether a particular region is tampered or not. The usage of average intensity significantly reduces the watermark payload because the authentication information is generated for a group of pixels rather than each pixel in an image.

This method has proven to be ineffective in certain situations where the authentication bits are not enough for the verification process. As an example, the average intensity of a block is 85. The average intensities for its sub-blocks are 99, 84, 80 and 77. The values of v and p were computed based on the average intensities and embedded as part of the watermark. The four sub-blocks were tampered where the average intensities had been changed to 101, 82, 81 and 76 respectively. The value of the block average remains unchanged. During the tamper detection process, the authentication bit and parity check bit is computed, denoted as v’ and p’. The values of v’ and p’ for all the sub-blocks remained unchanged. In this situation, the tampered block will pass the detection process. Thus in this case the tampered region can only be localised to an accuracy of more than 16 pixels.

This drawback has been overcome in the modified Tamper Localization scheme. This scheme reduces the block size and thereby the number of pixels for which the average is computed. The embedded average is retrieved and compared with the recomputed average to verify the integrity of the region of interest. This algorithm has the same computational simplicity as the existing algorithm with increased accuracy. This algorithm can localise a tampered region to an accuracy of 8 pixels.

II.RELATED WORKS

Tamper localization capable watermarking scheme can detect and locate modification of pixel values on the image. Existing tamper localisation algorithms were analysed [1-15]. In pixel-wise fragile watermarking technique, watermark is embedded into LSBs of each pixels of host image [4,5]. This technique is useful when the accurate location of altered pixels is to be determined with a high precision.Some tamper localization schemes are proposed in wavelet domain [10,16]. The embedded watermark is generated using the Discrete Wavelet Transform (DWT). The improved security watermark is then embedded into the LSB of the image by scrambling encryption. This provides good tamper localization properties as well as greater security against attacks. Tamper localization using CRC (Cyclic Redundancy Code) was proposed by Tan et. al.[7]. The image is divided into 16X16 blocks and CRC is computed for each block. Each CRC is embedded into the same block. The watermarked image is verified by extracting the watermarking and comparing the CRC of each block. A mismatch indicates tampering. The disadvantage of this scheme is the computational overhead. In the digital image authentication and tamper detection scheme, suggested in [12], the last three bits of every pixel is modified in order to embed the authentication key. This scheme has a high computational overhead and results in greater distortion than the 1LSB watermarking approach.

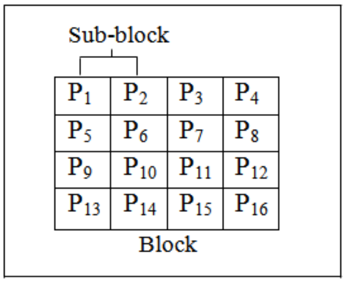
III. OVERVIEW OF ALGORITHM

This scheme divides an image into blocks of size 4 X 4 pixels and each block is further divided into sub blocks of size 2 X 2 pixels, as shown in Figure 2.1. Average intensity of the block and its sub-blocks will be used in the authentication and recovery process. The average intensity of a block is calculated based on equation 2.1.,

$$\text{Block average intensity}=\frac{(P_1+P_2+P_3\ldots+P_{15}+P_{16})}{16} \qquad (2.1)$$

where P1 to P16 are the pixel intensities in a block. The average intensity of a sub-block is calculated based on equation 2.2.,

$$\text{Sub block average intensity}=\frac{(P_1+P_2+P_5+P_6)}{4} \qquad (2.2)$$



P_1	P_2	P_3	P_4
P_5	P_6	P_7	P_8
P_9	P_{10}	P_{11}	P_{12}
P_{13}	P_{14}	P_{15}	P_{16}

Fig 2.1 A block divided into four sub-blocks

The authentication information for each block consists of two bits- one authentication bit and one parity check bit which are generated with the following algorithm:

1. The average intensity for block denoted as x1 and its sub-blocks, x1s will be computed, denoted by avg_x1 and avg_x1s respectively.
2. Generate the authentication bit, v, of each sub-block as:

$$V=\begin{cases}1, & \text{avg\_x1s} > \text{avg\_x1}\\ 0, & \text{otherwise}\end{cases} \qquad (2.3)$$

3. Generate the parity check bit p, of each sub-block as:

$$P=\begin{cases}1, & \text{if num is odd}\\ 0, & \text{otherwise}\end{cases} \qquad (2.4)$$

where num is the total number of 1s in the seven most significant bits of avg_x1s.

The authentication information generated is embedded as the watermark together with the Block Average Intensity that will be used for recovery purposes.

IV . PROPOSED TAMPER LOCALIZATION USING BLOCK AVERAGE INTENSITY

The image is divided into blocks of size 2 X 4 pixels, as shown in Fig 3.1. The Block Average Intensity is calculated by taking an average of all the pixels in the block. The seven most significant bits of each pixel are considered to calculate the average as shown in equation 3.1.,

$$\text{Block average intensity}=\frac{(P_1+P_2+P_3\ldots+P_7+P_8)}{8} \qquad (3.1)$$

where P_1 to P_8 are the pixel intensities in a block.

The average intensity of each block is embedded, as the watermark, in the LSB of each pixel in that block. This information is used to identify the tampered regions in the image.

If the tampered region coincides with the region of interest, the image should be rejected as unusable. The first step in verifying the integrity of the region of interest is to identify the sub blocks in that region. The sub block averages are recomputed and compared with the average embedded in the LSBs of the pixels. Any disparity in the sub block average intensities results in the image getting rejected. If the intensities match then that image is retained. In this manner the picture is resolved to size of 8 pixels and the tamper identification is thus localized to a smaller area than the previous algorithm.

P_1	P_2	P_3	P_4
P_5	P_6	P_7	P_8

Fig 3.1. A block containing 8 pixels

V. COMPARATIVE RESULTS OF TAMPER LOCALIZATION ALGORITHMS

The drawback of the existing tamper localisation algorithm using block average intensity is illustrated in Figures 5.1 to 5.4. and in Tables 4.1 to 4.4.

Table 4.1 gives the average intensities of all the sub-blocks in the region of size 16 x 16, before the image was tampered.

Table 4.1. Average intensities of all sub-blocks in the region of interest before image was tampered.

Block	1		2		3		4	
1	58 v=1 p=0	40 v=1 p=0	21 v=0 p=0	43 v=1 p=1	60 v=1 p=0	50 v=0 p=1	50 v=0 p=1	49 v=0 p=0
	30 v=0 p=0	29 v=0 p=1	32 v=1 p=1	33 v=1 p=1	50 v=0 p=1	54 v=1 p=0	50 v=0 p=1	62 v=1 p=1
2	44 v=1 p=1	37 v=0 p=0	40 v=1 p=0	38 v=0 p=1	60 v=1 p=0	61 v=1 p=0	66 v=1 p=0	54 v=0 p=0
	38 v=0	45 v=1	45 v=1	36 v=0	57 v=0	59 v=1	54 v=0	49 v=0

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2014

	p=1	p=1	p=1	p=0	p=1	p=0	p=0	p=0
3	25 v=0 p=0	52 v=1 p=1	52 v=1 p=1	37 v=0 p=0	57 v=1 p=1	46 v=0 p=0	63 v=1 p=1	63 v=1 p=1
	31 v=0 p=0	40 v=1 p=0	64 v=1 p=1	35 v=0 p=0	49 v=0 p=0	64 v=1 p=1	64 v=1 p=1	56 v=0 p=1
4	47 v=1 p=0	39 v=0 p=1	41 v=0 p=0	32 v=0 p=1	64 v=1 p=1	64 v=1 p=1	51 v=0 p=1	58 v=1 p=0
	45 v=0 p=1	57 v=1 p=1	51 v=1 p=1	51 v=1 p=1	71 v=1 p=1	59 v=0 p=0	58 v=1 p=0	62 v=1 p=1

It can be seen from Tables 4.2 and 4.3 that the sub-block averages have changed in a way such that the block averages remain unchanged. Since the authentication bits and the block average intensity is the only information used in the tamper detection process, the tampered region goes undetected.

Table 4.2. Average intensities of all blocks in the region of interest before image was tampered

Block	**1**	**2**	**3**	**4**
1	39	32	53	52
2	41	39	59	55
3	37	47	54	61
4	47	43	64	57

Table 4.3. Average intensities of all blocks in the region of interest after image was tampered

Block	**1**	**2**	**3**	**4**
1	**39**	**32**	**53**	**52**
2	**41**	**39**	**59**	**55**
3	**37**	**47**	**54**	**61**
4	**47**	**43**	**64**	**57**

Table 4.4 gives the sub-block average intensities of the same region, computed after the image was tampered. The highlighted values indicate a change in the sub-block average intensities as a result of tampering. A change in the sub-block average intensity is a direct consequence of changed grey levels of the pixels in the sub-block. The validity and parity bits computed from these changed sub-blocks match those computed from the original image

ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2014

Table 4.4. Average intensities of all sub-blocks in the region of interest after image was tampered

Block	1		2		3		4	
1	54 v=1 p=0	40 v=1 p=0	25 v=0 p=0	39 v=1 p=1	59 v=1 p=0	51 v=0 p=1	50 v=0 p=1	48 v=0 p=0
	34 v=0 p=0	29 v=0 p=1	32 v=1 p=1	33 v=1 p=1	50 v=0 p=1	54 v=1 p=0	50 v=0 p=1	63 v=1 p=1
2	44 v=1 p=1	40 v=0 p=0	40 v=1 p=0	38 v=0 p=1	60 v=1 p=0	66 v=1 p=0	61 v=1 p=0	54 v=0 p=0
	38 v=0 p=1	42 v=1 p=1	44 v=1 p=1	37 v=0 p=0	52 v=0 p=1	59 v=1 p=0	54 v=0 p=0	54 v=0 p=0
3	30 v=0 p=0	52 v=1 p=1	52 v=1 p=1	37 v=0 p=0	57 v=1 p=1	47 v=0 p=0	63 v=1 p=1	63 v=1 p=1
	31 v=0 p=0	35 v=1 p=0	63 v=1 p=1	36 v=0 p=0	49 v=0 p=0	63 v=1 p=1	63 v=1 p=1	57 v=0 p=1
4	47 v=1 p=0	43 v=0 p=1	41 v=0 p=0	33 v=0 p=1	63 v=1 p=1	64 v=1 p=1	56 v=0 p=1	58 v=1 p=0
	45 v=0 p=1	53 v=1 p=1	50 v=1 p=1	51 v=1 p=1	71 v=1 p=1	60 v=0 p=0	58 v=1 p=0	57 v=1 p=1

VI. SIMULATION ON MATLAB AND RESULTS

The experiment was carried out on MATLAB by watermarking a grey scale image of size 256 X 256 pixels. A region of this watermarked image was tampered. The Region of Interest (ROI) of size 32 x 32 is highlighted in red and the tampered region of size 16 x16 in blue, in Figure 5.1. Since the tampered region lies within the ROI the image should be rejected. The existing tamper localization algorithm was tested on the image. The old algorithm was unable to detect the tampering as shown in Figure 5.2

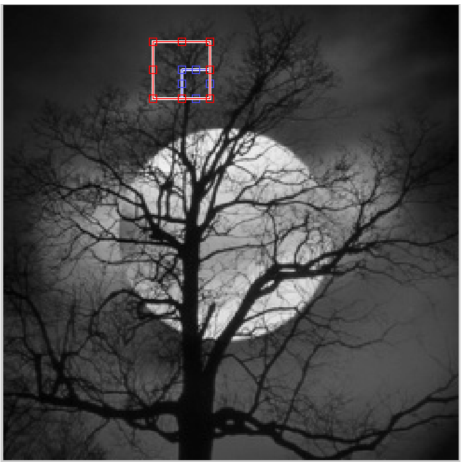
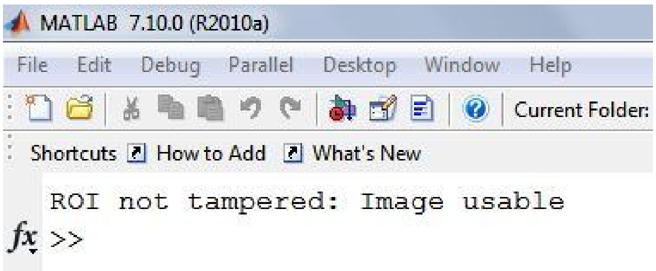


Figure 5.1. Tampered image. Region of interest is highlighted in red and tampered area in blue.



MATLAB 7.10.0 (R2010a)
File Edit Debug Parallel Desktop Window Help
Current Folder:
Shortcuts How to Add What's New

```
ROI not tampered: Image usable
fx >>
```

Figure 5.2. Image passed the detection process

The drawback of the existing tamper localisation algorithm has been overcome by the proposed algorithm as shown in Figures 5.3 and 5.4. The same tampered image was used in the proposed algorithm. For the same ROI the algorithm correctly rejected the image as tampered.

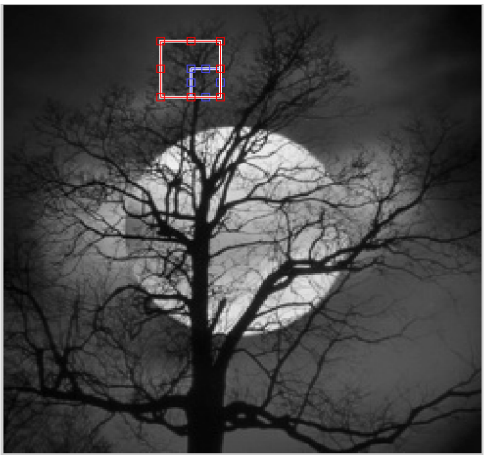
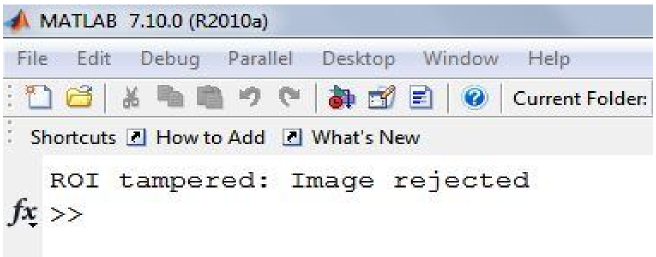


Figure 5.3. Tampered image. Region of interest is highlighted in red and tampered area in blue


MATLAB 7.10.0 (R2010a)
File Edit Debug Parallel Desktop Window Help
Current Folder:
Shortcuts How to Add What's New
fx

```
ROI tampered: Image rejected
>>
```

Figure 5.4. Image is rejected by the tamper detection process

Another example is considered by selecting a different ROI, as shown by the region highlighted in red as shown in Figure 5.4. In the first case the region of interest (ROI) highlighted in blue, overlaps with the tampered region, causing the image to be rejected as unusable, as shown in Figure 5.5.

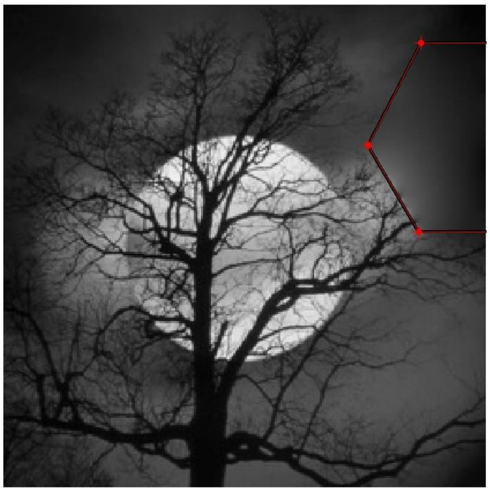
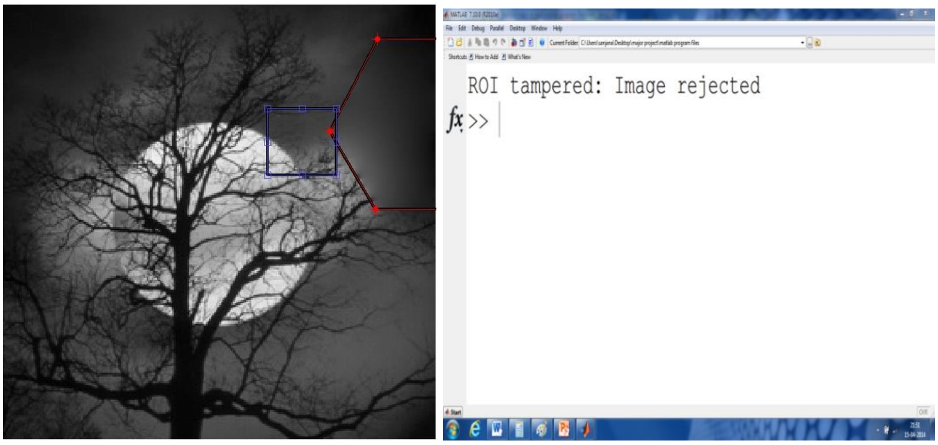


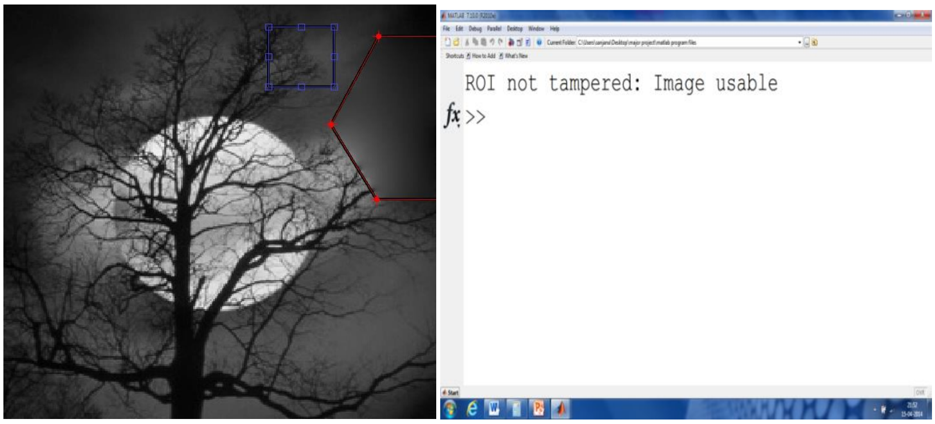
Fig 5.4. Watermarked cover image after tampering (highlighted in red).



```
ROI tampered: Image rejected
>>
```

Fig 5.5. Tampered part inside ROI (highlighted in blue).

In the second case the region of interest (ROI) lies outside the tampered region and this is successfully verified as shown in Figure 5.6.



```
ROI not tampered: Image usable
fx >>
```

Fig 5.6. Tampered part outside ROI

The tampered region can be any irregular region containing more than eight pixels, for this tamper detection and localization algorithm.

VII. CONCLUSIONS

Tamper Localization algorithm was implemented to determine whether the ROI has been tampered with or not. The smallest tampered region that can be localised by the algorithm was found to be a block of 2x4 pixels. The proposed algorithm rejected the ROI which coincided with the tampered region, whereas the existing algorithm did not.

Tamper Localization algorithm successfully identifies the region that has been manipulated when the image is received. The accuracy of 8 pixels is achieved by our proposed algorithm. However, for extreme magnification applications, the algorithm can be extended to provide greater accuracy.

REFERENCES

[1] Celik, M.U., Sharma, G., Tekalp, A.M., and Saber, E., “Localized lossless authentication watermark (LAW)", International Society for Optical Engineering, vol. 5020, pp. 689-698, California, USA, Jan. 2003.

[2] Liu Tong, and Qiu, Zheng-ding, “The survey of digital watermarking-based image authentication techniques,” *Proc. 6th International Conference on Signal Processing*, Aug 2002, pp. 1556- 1559.

[3] Utku Celik, M., Sharma, G., Saber, E., and Murat, Tekalp A., “Hierarchical watermarking for secure image authentication with localization,” *IEEE Pattern Recognition Transactions on Image Processing*, vol. 11, no. 6, pp. 585 –595, June 2002.

[4] Xinpeng Zhang and Shuozhong Wang, “Statistical fragile watermarking capable of locating individual tampered pixels,” *IEEE Signal Processing Letters*, vol. 14, no. 10, pp. 727 –730, Oct. 2007.

[5] Liu, S., Yao, H., Gao, W., and Liu, Y.,” An image fragile watermark scheme based on chaotic image pattern and pixel-pairs,” *Proc. Applied Mathematics and Computation*, 2007, 185(2), pp.869-882.

[6] Chiang, K., Chang, R., and Yen, H., “Tamper Detection and Restoring System for Medical Images Using Wavelet-Based Reversible Data Embedding,” *Journal of Digital Imaging*, vol. 21, no.1, pp.77-90, Mar. 2008.

[7] Tan, C.K., Ng, C., Xu, X., Poh, C.L., Yong, L. G. and Sheah, K., “Security protection of DICOM medical images using dual-layer reversible watermarking with tamper detection capability,” *Journal of Digital Imaging*, vol. 24, no.3, pp. 528-540, June 2011.

[8] Osamah, M., and Khoo, B. E., “Authentication and Data Hiding Using a Hybrid ROI-Based Watermarking Scheme for DICOM Images,” *Journal of Digital Imaging*, vol. 24, no.1, pp.114-125, Feb 2011.

[9] Siau-Chuin Liew, and Jasni Mohamad Zain, “The Usage of Block Average Intensity in Tamper Localization for Image Watermarking”, *2011 4th International Congress on Image and Signal Processing* ,IEEE,2011, pp.1044-1048.

[10] Dadkhah, S., Manaf, A.A., and Sadeghi, S., “Efficient Two Level Image Tamper Detection Using Three LSB Watermarking,” *IJCSI International Journal of Computer Science Issues*, Vol. 9, Issue 1, No 2, pp.300-305, January 2012.

[11] Siau-Chuin Liew, and Jasni Mohamad Zain, “The Usage of Block Average Intensity in Tamper Localization for Image Watermarking”, *2011 4th International Congress on Image and Signal Processing* ,IEEE,2011, pp.1044-1048.

[12] Motoi Iwata, Tomoki Hori, Akira Shiozaki and Akio Ogihara, “Digital Watermarking Method for Tamper Detection and Recovery of JPEG Images,” *ISITA 2010, IEEE, Taichung, Taiwan*, 2010, pp. 309-314.

[13] Baotian Cheng, Rongrong Ni, and Yao Zhao, “A Refining Localization Watermarking for Image Tamper detection and Recovery,” *ICSP2012 Proceedings*, 2004, pp.123-145.

[14] Hongjie He, Fan Chen, Heng-Ming Tai, Kalker T., and Jiashu Zhang, “Performance analysis of a block neighbourhood-based self-recovery fragile watermarking scheme,” *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 1, pp. 185 –196, Feb. 2012.

[15] Chao-Ming Wu, “Multi-Level Tamper Detection and Recovery with Tamper Type Identification”, *ICIP 2013 proceedings*, Dec. 2002, pp. 19-22.

[16] HongJie He, JiaShu Zhang, and Heng-Ming Tai, “A Wavelet-Based Fragile Watermarking Scheme for Secure Image Authentication,” In 5th *International Workshop, IWDW 2006, Jeju Island, Korea Proceedings*, 2006, pp 422 - 432.