ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

Integrity Verification of Images Using Fragile Watermarking

Rahul Kumar [1], Arun Kumar Shukla [2]

M.Tech [CSE] Student, Sam Higginbottom Institute of Agriculture, Technology and Sciences, Allahabad, India[1]

Asst. Professor, Department of Computer Science & Information Technology, Sam Higginbottom Institute of Agriculture, Technology and Sciences: Deemed University, Allahabad, India [2]

ABSTRACT: This paper proposes a novel pixel based fragile watermarking scheme in spatial domain by which one can easily identify the alteration in every pixel of the images accurately and scheme is also protected by user defined secret key. Proposed watermarking algorithms are able to increase PSNR value and also have low complexity of algorithms. These algorithms also work on color images efficiently, if all three RGB planes are treated as separate one. Proposed scheme achieves PSNR value up to 44.09 dB and also able to achieve 100% efficiency in some cases, which is good enough. Experimental results show that proposed watermarking algorithms give significant responses in finding various types of temporization attacks.

KEYWORDS: Integrity verification, Fragile watermarking, Authentication.

I. INTRODUCTION

Watermarking is the practice of imperceptibly altering a work to embed a message about that work. This technique contains two high level elements Embedder and Detector as shown in figure 1. The embedder takes two inputs. One is the payload we want to embed(e.g. either the watermark or secret message), other is the cover work in which we want to embed the payload. The output of embedder is presented as an input to the detector.

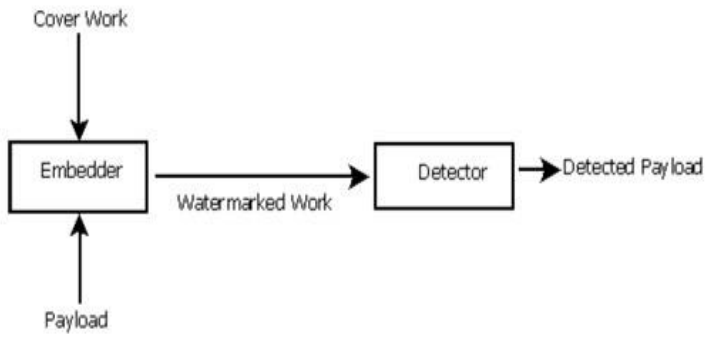

Figure 1: A Generic water making System

Watermarks are broadly classified into three categories viz. fragile, semi fragile and robust watermark.

- **Fragile watermark:** A watermark that becomes undetectable after even minor modification of the work in which it is embedded.
- **Robust watermark:** A watermark designed to survive on legitimate and everyday usage of content.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

- **Semi fragile watermarking:** A watermark that is unaffected by legitimate distortion but destroyed by illegitimate distortion.

For ensuring the legitimacy and data integrity the notion of fragile watermarking [1] [6] [8] [11]came in picture. A fragile watermark is a mark that is readily altered or destroyed when the host image is modified through a linear or nonlinear transformation [2] .The sensitivity of fragile watermark to alteration leads to their use in image authentication.

II. LITERATURE REVIEW

***P. wong et.al* (2008)** has proposed the fragile watermarking scheme [7].This approach is based on secret key and public key cryptography. Here a different image is used as watermark instead of self embedding technique.
Another fragile watermarking approach[5] is proposed by Hongjie is a standard technique to detect alteration. The embedded watermark is generated using the discrete wavelet transform (DWT), and then the improved security watermark by scrambling encryption is embedded into the least signicant bit (LSB) of the host image.

Fragile watermarking approach has restoration capability [12]. Here cover work is converted in to wavelet domain by DWT and higher bits of watermark is embedded in to lower subband of wavelet and the lower order bits are embedded into another wavelet subband. The stego image is obtained by an inverse transform from the wavelet domain into the spatial domain. To authenticate a test image which could have undergone changes, a DWT is performed and the watermark is extracted from the wavelet subbands.

The watermark is then compared with a down-scale version of the test image. If the similarity between them exceeds a threshold value, then the test image is classified as authentic. Otherwise, tampered regions will be highlighted and content recovery is carried out using the watermark information extracted.
Fragile watermarking can be divided into two major classes, block-wise fragile watermarking[2][4][5][6][8] and pixel-wise fragile watermarking[7][9][10][11][12]. The main concept behind the block-wise fragile watermarking is that the host image is divided into small blocks and each block has watermark information. This watermark may be any function based on principal content of host image. If image is altered intentionally or unintentionally, the tampered block and watermark contained in that block will mismatch. The fragile watermark scheme can identify these tampered blocks.

J Fridrich and M Goljan et al. (1999) have proposed the block-wise technique of self embedding in [4]. They have proposed two methods to protect the image content. The first technique is based on quantization of block-wise Discrete Cosine Transform (DCT) coefficient and represented as 64 or 128 bits. These bits are used to replace one or two Least Significant Bit (LSB) of another block. In the second method a new image is generated by reducing gray level of the original image. These reduced gray levels are cyclic shifted and embedded into pixel difference. If some modification is done on the watermarked image, then the quantized DCT coefficient and the new reduced gray level image can be used to recover the principal content of the tampered area.

Hongjie, et al. (2007) proposed block-wise fragile watermarking is standard technique, based on scramble encryption [5] in which the watermark calculated from a block, is arbitrarily distributed on the LSB of all pixels in the whole image. This technique is good enough to localize tampered block but lacks image restoration.

X Zhang and S Wan, et al. (2008) proposed fragile watermarking with error free restoration capability [8] which is based on tailor made watermark, consisting of reference bits and check bits. These bits are embedded into the host image using lossless data hiding method. On the receiver end, the check bits are calculated and compared with extracted check bits. This can detect the tampering of the image. After tamper detection the reference bit extracted from other blocks are used to exactly reconstruct the original image. In case of block-wise fragile watermarking, a single block will consist of many pixels. So within tampered block some pixels are really altered and some are unaltered which is undesirable when we need exact position of alteration with high precision. This negative aspect of block-wise fragile watermarking can be overcome by pixel-wise fragile watermarking. In pixel-wise fragile watermarking

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

technique, watermark information is obtained by gray scale value of each pixel of host image and then it is further embedded into LSBs of host image itself. This procedure is called self embedding. If gray scale value of any pixel is changed then embedded watermark corresponding to that pixel will also be changed hence one can easily localize the each altered pixel.

***Y Lim et al.* (2002)** has proposed a pixel-wise fragile [11]. According to this technique seven Most Significant Bits (MSB) of a pixel are given as an input to the hash function. Using a secret key and hash value, we calculate a single value either 0 or 1 for each pixel and this value is embedded in the LSB of corresponding pixel. If alteration is done with any pixel, on the receiver end, calculated hash value and extracted hash value from LSB will mismatch hence tampered pixel can be localized. The PSNR value of watermarked image is improved by this technique but, since the tamper detection completely depends on a single LSB value, the probability of altered pixel detection will be half.

X Zhang and S Wang et al. (2007) has proposed a standard technique for exactly localizing tampered pixel in [9] .They have calculated a set of tailor-made authentication data for every pixel with some additional test data and embedded into the host image. On the receiver side by examining the pixels and their respective authentication data, one can expose the correct pattern of the content alteration.

***Shengbing et al.* (2008) has proposed** another algorithm which is based on self embedding technique. They used the function of composite chaotic iterative dynamic system. According to the value of the specific position in chaotic iterative sequence and the seed value, one can get the watermarking information used for embedding in LSBs. Here only a single pixel value is used for self authentication. That authentication bit is embedded in the lowest significant bit of the pixel's gray scale value. This algorithm utilizes the sensitiveness and randomness of the composite chaotic iterative dynamic system and does not require any additional information for localizing the pixel.

Yong-Zhong He and Zhen Han et al. (2008) has given a proposal in [12] which is based on both, block-wise fragile watermarking as well as pixel-wise fragile watermarking. This scheme uses two LSB plane, one is for altered pixel detection and second is for block-wise authentication. Unlike self embedding, here the image is used as watermark information. Both the host image and watermark image are divided into equally sized blocks of m ×n pixels and also partitioning must assure the condition that the number of blocks should not be less than the number of pixels in one block. Now the hash value is calculated for all pixels within a block. The next computation is done for pixel-wise alteration detection in which hash function takes corresponding positioned pixel from other blocks as an input. On the receiver end, same procedure is repeated for getting hash value, so comparison mismatch shows the alteration in blocks and pixel of the blocks.

X Zhang and S Wang et al. (2008) has proposed a novel fragile watermarking scheme using hierarchical mechanism [10]. In this technique pixel-wise and block-wise watermark data, which are derived from MSBs are used to directly replace all the LSBs of a host image. On the receiver side, after identifying the blocks containing tampered content, the watermark data hidden in the rest blocks are exploited to exactly locate the tampered pixels.

III. PROPOSED MODEL

Proposed watermarking algorithms are based on LSB replacement technique. This watermarking scheme uses pixel-wise approach as its base. Consider a host image I of size r x c then resize it to size of 255x255 and then set 3 LSBs to zero. After that apply security mechanisms and then apply embedding and extracting procedures. Block diagrams for embedding and extracting watermarks are shown by Fig 2 and Fig 3 simultaneously.

3.1 Watermarking embedding process

1. Take a grayscale Image I of size r x c, such that r, c>=0 as input
2. Resize Grayscale Image I, such that 1≥r, c≤255.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

3. Generate Secret matrix Sm, by using a randomly selected Secret Key scrt_key.
6. In an Image I , do
i) For every Pixel p of an image,
a) Represent pixel p in 8-bit binary format from decimal format.
b) Set 3 LSB of pixel p to zero.
c) Applying bit wise X-OR on pixel and secret matrix, and resultant image is called Im.

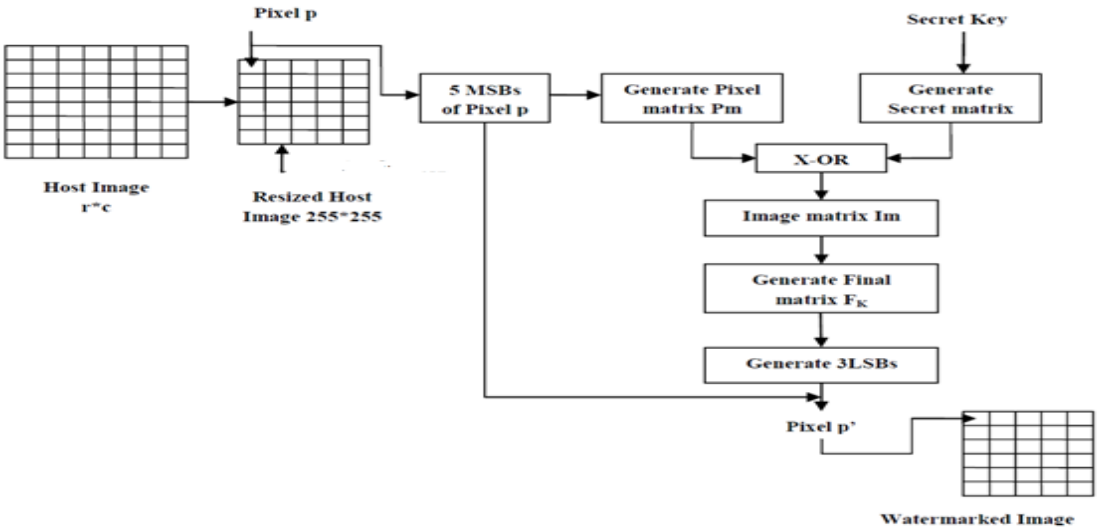

Figure 2: Watermark embedding procedure of proposed approach

Now generate 3 bits by only five MSBs of each pixel by following way:
For 1st bit generation-
Step 1- Take bit wise XOR of five bits of each pixel and calculate the modulo 2 of the sum of them.

$$1st\ bit = (\sum_{i=1}^{4} b_i \oplus b_{i+1}) mod\ 2 \qquad (1)$$

For 2nd bit generation-
Step 2- Generate a random matrix *Rm* of size r x c whose values ranges from 0 to 31. Do bit wise XOR between corresponding pixels of *Rm* and *Im.*

$$2nd\ bit = \left(\sum_{i=1}^{5} b_i(Im) \oplus b_i(Rm)\right) mod\ 2 \qquad (2)$$

For 3rd bit generation-
Step 3- Calculate the complement of the each pixels of Im and take the bit wise XOR with its original pixel.

$$3rd\ bit = \left(\sum_{i=1}^{5} b_i(Im) \oplus b_i(31 - Im)\right) mod\ 2 \qquad (3)$$

Step 4- Embed all generated three bits in to first three LSBs of its corresponding pixel. Now the resultant image will be called watermarked image.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

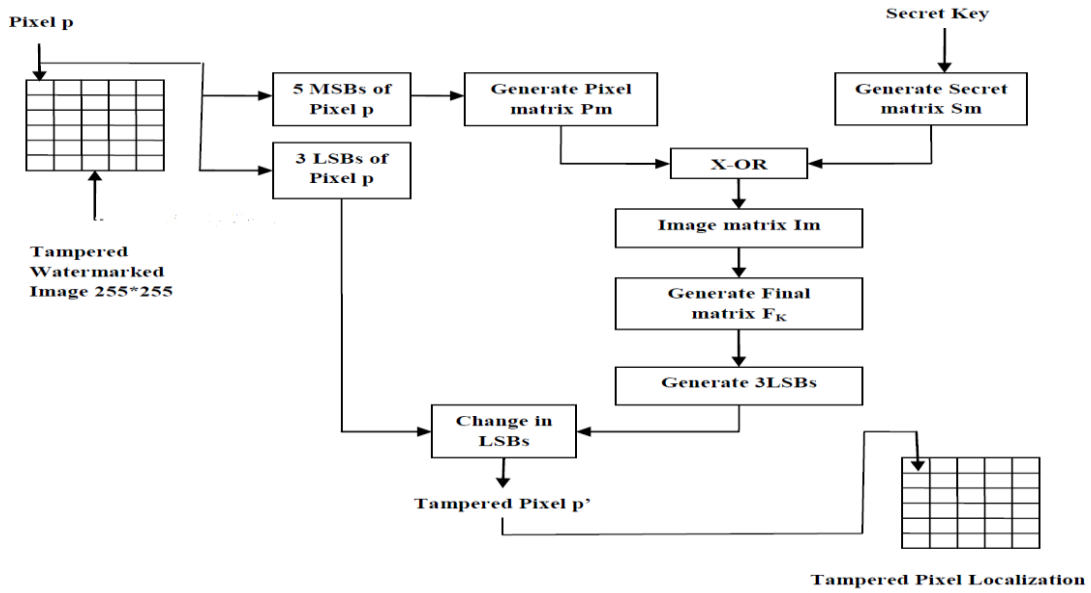

Figure 3: Watermark extraction procedure of proposed approach

3.2 Watermarking extracting process

1. Input Tampered Watermarked Image T of size r*c, such that r=255 and c=255.
2. Input a Secret Key scrt_key, which is previously used in insertion process
3. Generate Secret matrix Sm, by Applying Pseudo-random function on randomly selected Secret Key scrt_key.
4. Generate 255*255 Tampered Pixel Localization Image TPL_img for locating tampered pixels, Such that every pixel p has value equal to zero.
6. In Tampered Watermarked Image T , do
i) For every Pixel p of an image,
a) Represent pixel p in 8-bit binary format from decimal format.
b) Store 3 LSB of pixel p in a vector, named as LSB_ORG.
c) Now, Set 3 LSB of pixel p to zero.
7. Generate three bits by using eq. 1, 2 and 3. These are called recalculated bits. Now compare it by the corresponding three LSBs of vector LSB_ORG.
8. If any mismatch is found then mark the corresponding pixel of TPL by white pixels.

IV. EXPERIMENTAL RESULT & ANALYSIS

Experimental results show different types of temporization like addition of some object or text, deletion of some object or text etc. Different grayscale images show how watermarks are embedded and extracted. Here, experimental results show that this scheme is able to achieve PSNR value equal to 44.09 and efficiency up to 100%. PSNR value varies on basis of secret key used. These procedures can also be applied on color images. In color images, detection of tampered pixels will be showed in all three planes i.e., on RGB planes.
Fig.4 (a) and (b) shows the results after applying watermarking embedding procedure. Fig.4(c) and (d) shows the results after applying watermarking extracting procedure. Section 4.1 show different types of result on grayscale images and section 3.2 show result

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

4.1 Result on grayscale images:

***4.1.1 On Lena image* on.**

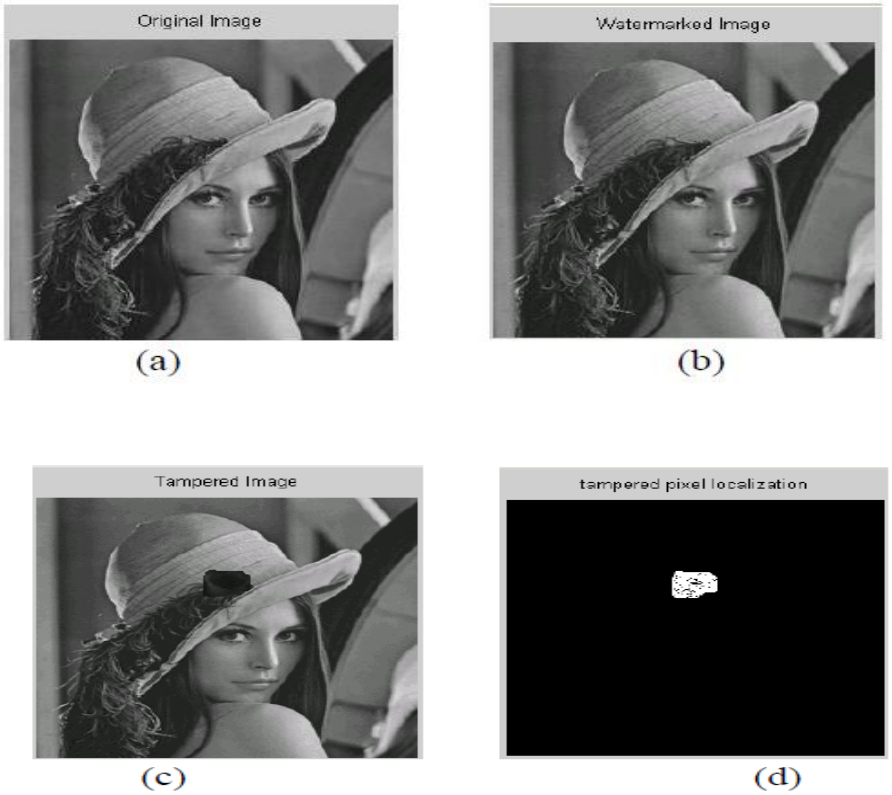

Figure 4: Tamper localization result for lena image.

In Fig.4, temporization is done by adding a small rose flower on the hat of Lena by tampering 720 pixels. Then, by applying watermarking extracting procedure, 656 pixels are detected. Thus, this gives efficiency equal to 91.1% and PSNR value equal to 44.09 dB.

4.1.2 On number plate image:

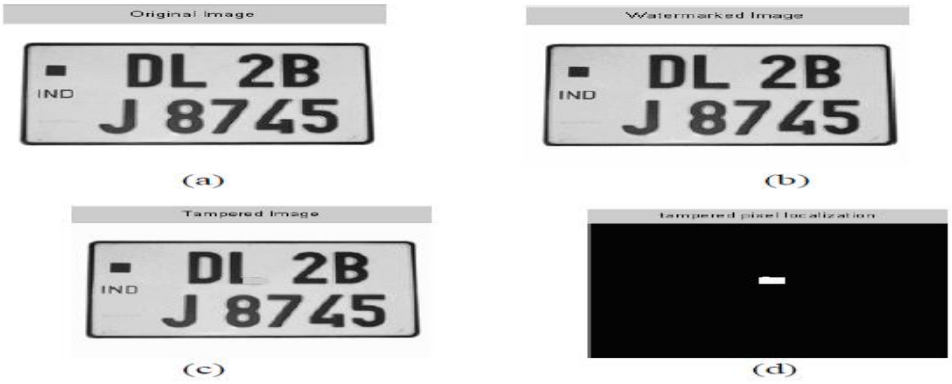

Figure 5: Tamper localization result for number plate image.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

In Fig.5, temporization is done by changing 'L' of number plate to 'I' by tampering 214 pixels then; this approach is able to detect 214 pixels. Thus, this approach is able to achieve 100% efficiency and PSNR value for this image is 40.59 dB

Table 1: Observations for various images

Host Image	PSNR Value	Altered Pixel	Detected Pixel	% of Accuracy	Detection Time (sec)
Baboon	41.14dB	1515	1421	93.79	147.3
Lena	40.98dB	1739	1656	95.22	140.5
Camera man	41.11dB	818	766	93.64	150.3
Number plate	40.79	859	841	97.7	148.8

From Table 1: Shows the effectiveness of the proposed approach. The Proposed scheme is able to detect tempered images with efficiency is about 100%.

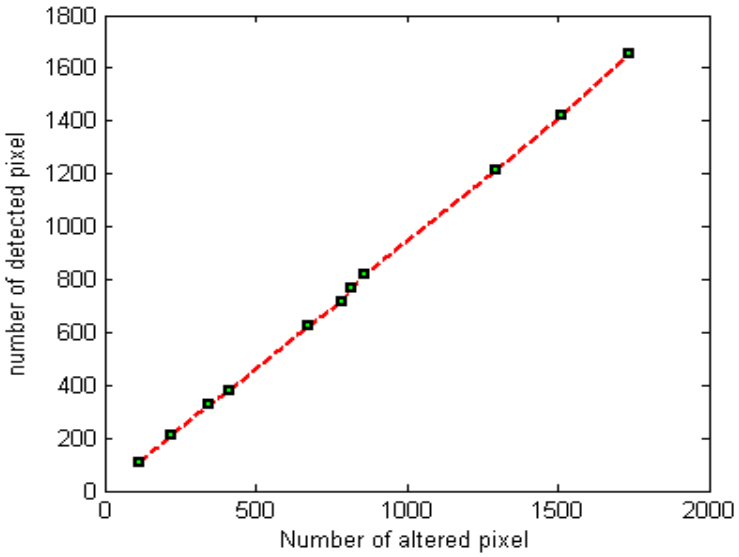

Figure 6: Plot between altered and detected pixels.

Figure 6: demonstrate the plot between number of altered pixel and detected pixels. Straight line shows the effectiveness of the proposed approach**.**

V. CONCLUSION

This paper proposes watermarking embedding and extraction algorithm in spatial domain by which one can easily identify changes in every pixel of the images accurately and also there is good security mechanism for securing images. Proposed watermarking algorithms are able to increase PSNR value and also have low complexity of algorithms. These algorithms also work on color images efficiently, but show temporization results in all three RGB planes. Proposed scheme achieve PSNR value up to 44.09 dB and also able to achieve 100% efficiency in some cases, which is good

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 5, May 2016

enough. Thus, these watermarking algorithms give significant responses in finding various types of temporization attacks.

REFERENCES

[1] A. Criminisi, P. Perez, and K. Toyama. Region filling and object removal by exemplar-based image inpainting. IEEE Trans. Image Process., vol. 13, no. 9, pp. 1200-1212, Sep. 2004.
[2] Anthony T. S. Ho, Xunzhan Zhu, Jun Shen, and Pina Marziliano. Fragile Watermarking Based on Encoding of the Zeros of the -Transform IEEE Transactions On Information Forensic and Security, VOL. 3, NO. 3, September 2008
[3] Eugene T. Lin and Edward J. Delp. A review of fragilewatermarking. Center for Education and Research in Information Assurance and Security,Purdue University, West Lafayette, IN 47907-2086.
[4] Jiri Fridrich and Miroslav Goljan. Images with Self-Correcting Capabilities. IEEE, 0-7803-5467-2/99, 1999.
[5] Hongjie He, Jiashu Zhang , Fan Chen. Block-wise Fragile Watermarking Scheme Based on Scramble Encryption. IEEE 978-1-4244-4105-1/07,2007.
[6] Mi-Ae Kim and Won-Hyung Lee. A Content-Based Fragile Watermarking Scheme for Image Authentication Springer-Verlag Berlin Heidelberg, AWCC 2004, LNCS 3309, pp. 258-265, 2004.
[7] Shengbing CHE, Bin MA, Zuguo CHE. An Adaptiveand Fragile Image Watermarking Algorithm Based on Composite Chaotic Iterative Dynamic System IEEE DOI 10.1109/IIH-MSP.2008.24,2008.
[8] Xinpeng Zhang and Shuozhong Wang. Fragile Watermarking With Error-Free Restoration Capability, IEEE transaction of multimedia, VOL. 10, NO. 8, December 2008.
[9] Xinpeng Zhang and Shuozhong Wang. Statistical Fragile Watermarking Capable of Locating Individual Tampered Pixels, IEEE Signal processing letters, VOL. 14, NO.10, October 2007.
[10] Xinpeng Zhang and Shuozhong Wang. Fragile watermarking scheme using a hierarchical mechanism Elsevier,doi:10.1016/j.sigpro.2008.10.001.
[11] Yusuk Lim, Changsheng Xu, David Dagan Feng. Web based Image Authentication Using Invisible Fragile Watermark, Australian Computer Society, Inc. 2002.
[12] Yong-Zhong He, Zhen Han, A Fragile Watermarking Scheme with Pixel-wise Alteration Localisation IEEE, 978-1-4244-2179-04/07, 2008.

BIOGRAPHY

Rahul Kumar was born in Uttar Pradesh, India, in 1992. He has received B.Tech degree in Computer Science & Engineering in 2012 and then worked as a Guest Speaker at Govt. I.T.I from 2012 to 2014. Currently perusing M.Tech degree in CSE from Sam Higginbottom Institute of Agriculture, Technology & Science, Technology & Science, Deemed-to-be- University in Allahabad (U.P).

Arun Kumar Shukla is currently working as Assistant professor in the Computer Science and IT Department in Sam Higginbottom Institute of Agriculture, Technology & Science, Deemed-to-be-University in Allahabad (U.P). He has done his bachelor of Engineering from Jawaharlal Institute of Technology from Khargone (M.P) in the year 2006 and Master of Engineering from I.E.T. - D.A.V.V., Indore in the year 2011.