International Journal of Current Engineering and Technology
ISSN 2277 - 4106

Available at http://inpressco.com/category/ijcet

Research Article

Fragile Pixel-Wise Watermarking using Neighborhood Location Based Technique

Raji Chacko[Å] and W.Jeberson[Å]

[Å]Department of Computer Science & IT, SHIATS, India

Accepted 25 November 2013, Available online 01 December 2013, **Vol.3, No.5 (December 2013)**

Abstract

As the exponential growth of computer users, huge data flows become a normal event around us. The aims of communication method increase, people begin to use digital media to transmit valuable data through public accessible network. Now a day's most important thing is to secure data while sending using a public network. Potential for exactly tracing maliciously altered pixels is currently desired in image authentication. This paper proposes a efficient novel approach as fragile pixel-wise watermarking using neighborhood location technique based on two bits (Binding & position) bits. In this scheme Binding & position bits are embedded as a watermark into the first two LSBs of each pixel of the host image. On the receiver end, by comparing the extracted LSBs and recalculated Binding & position bits, one can easily recognize the altered pixels of the host image .Improve the data security and integrity using two key at the time of embedding watermark as well as the same key is used for extraction and recalculated at the receiver end to recognize the altered pixels of the host image.

Keywords: *Fragile watermarking, Tamper detection, Pixel localization.*

1. Introduction

The enormous popularity of the World Wide Web and exponential growth of computer users, huge data flows become a normal event. The aims of communication method increase, people begin to use digital media to transmit valuable data through public accessible network. This development made unauthorized distribution of multimedia data. With the growing need of multimedia technology security concerns about digital data like audio, video, text and image have grown to be a vital issue in these few years. For the protection of multimedia data, a solution known as watermarking is used. Integrity of image information is important especially when this type of data is used for authentication purpose e.g. biometric, medical diagnosis or court evidence. In order to protect the copyright of multimedia information, lead to the attention of watermarking technique. These techniques are broadly classified into three categories viz. fragile, semi fragile and robust watermarking .For ensuring the legitimacy and data integrity the notion of fragile watermarking came in picture. The fragile watermarking scheme was proposed by *P. won* . This approach is based on secret key and public key cryptography. Here a different image is used as watermark instead of self-embedding technique. In a fragile marking system, a signal (watermark) is embedded within an image such that subsequent alterations to the watermarked image can be detected with high probability. *Eugene T. Lin* and *Edward J. Delp* defined fragile watermark as a mark that is readily altered or destroyed when the host image is modified through a linear or nonlinear transformation. The sensitivity of fragile watermark to alteration leads to use in image authentication. Fragile watermarking can be divided into two major classes, block-wise fragile watermarking and pixel-wise fragile watermarking. The major 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 basic 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. A block-wise fragile watermarking proposed by *Hongjie, et al* is a standard technique, based on scramble encryption in which the watermark calculated of all pixels in the whole image. This technique is good enough to localize tampered block but lacks image restoration. Hence *X Zhang and S Wang* have proposed fragile watermarking with error free restoration capability 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

*Corresponding author **Raji Chacko is a M.Tech Scholar** and **Dr. W.Jeberson is working as HOD.**

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 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.

A pixel-wise fragile watermarking scheme is proposed by *Y Lim et al.* 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* has proposed a standard technique for exactly localizing tampered pixel. .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. Another algorithm which is also based on self embedding technique is proposed by *Shengbing et al.* 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* have given a proposal 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 x 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. Similarly *X Zhang and S Wang* has proposed a novel fragile watermarking scheme using hierarchical mechanism. 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.

The motivation behind this is rapid expansion of the internet in the past years has rapidly increased the availability of digital data such as audio, images and videos to the public. As we have witnessed in any intentional modification of their data or work. Some serious work needs to be done in order to maintain the availability of multimedia information. This is an interesting challenge and this is probably past few years, the problem of protecting multimedia information becomes more and more important and a lot of copyright owners are concerned about protecting any illegal. The main goal is to provide a fragile watermarking technique which is effective enough to detect alteration with high precision in a image as well as able to improve the contras (higher quality) of an host image after watermarked.

Keeping in view the above challenges and applications of

Fragile Watermarking the main objectives is to study and analyze the performance of different existing watermarking technique. To design a new watermarking approach that improves the contrast (higher quality) and effective enough to detect alteration with high precision of a host image after it is watermarked. To evaluate and improve the Authentication, Data security and Integrity of an image from the existing system. The motive behind this newly proposed approach is to achieve the objective with less computational work. This approach can be done with help of experimental and simulation tools.

There are different approaches used for Authentication, data security and to find out the alteration done in an image. In the newly proposed approach it improved the contrast of image (higher quality), security and find out maximum altered pixel in an host image using less computation and less time from the existing system.

Rest of the paper is organized as: A detailed overview of our proposed algorithm is described in section 2. Section 3 provides experimental results and their analysis and Article is concluded in section 4.

2. Related Works

In the existing proposed system algorithm is bifurcated in to two major proposals. First proposal is Pixel-wise fragile watermarking scheme based on ARA bits which is only used for alteration detection whereas second proposal is based on block-wise fragile watermarking which detects the altered block as well as recover altered region with good approximation without changing the domain. They

Consider a gray scale host image I, having dimension m x n. is Then N represents the number of pixels, N= m x n.
The existing to detect alteration with high precision but still there approach good enough is some need is lagging that is restoration of altered pixels. This was limitation of the first proposal. Hence they proposed another technique which is based on block-wise fragile watermarking which will detect altered block as well as restore it with good approximation without changing the present working domain that is spatial domain 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.

3. Solution/Need/Importance of the study Problem Statement/Objectives

The above challenges and applications of Fragile Watermarking, using the new approach Fragile Pixel-Wise Watermarking Using Neighborhood Location Based Technique. A new watermarking approach that uses fragile pixel-wise self embedding technique improves the contrast (higher quality) of a host image an after it is watermarked known as watermarked image. It also detects exact position of alteration with high precision. It also improved the Authentication, Data security and Integrity using two keys during embedding and extraction of an image in order to increase the probability of tamper detection from the existing system. This provides a best approach achieve the objective with less computational work within less time.

4. Hypothesis

Most of the earlier proposed algorithm uses the same technique to calculate revised three LSBs which is used to replace the original LSBs of host image and treated as watermark. The main bottleneck of these algorithms is that the probability for detection of altered pixel will be less. In our proposed technique we are calculating two LSBs with a method in order to increase the probability of tamper detection. These bits are used to replace one or two Least Significant Bit (LSB) of another block

Here we are calling these two LSBs which stand for Binding and Position bits. These names are closely related to the method used for generation of these bits.

5. Methodology

Watermark Embedding Procedure

Consider a gray scale host image I which has dimension $\mathbf{m} \times \mathbf{n}$. Then N represents number of pixels $\boldsymbol{N = m \times n}$. So the gray scale value at each pixel of the image is denoted by $\boldsymbol{P_i}$ where $\boldsymbol{P_i} \in (0..255)$, $i = 1,2,3.....N$. $\boldsymbol{P_i}$ can be denoted by 8 bits. So each single bits of $\boldsymbol{P_i}$ is denoted by $b(\boldsymbol{P_i}, 7)$, $b(\boldsymbol{P_i}, 6)$, $b(\boldsymbol{P_i}, 5)$….. $b(\boldsymbol{P_i}, 0)$. Then the individual bit of any pixel $\boldsymbol{P_i}$ can be represented in binary form by following equation:

$$(\boldsymbol{P_i}, \boldsymbol{u}) = \left\lfloor \frac{P_i}{2^u} \right\rfloor \boldsymbol{mod\ 2 \text{ where } u = 0, 1, 2 \ldots . 7} \quad \textbf{(1)}$$

Where u=0,1,2...7
Calculated 8 bits for a particular pixel can be verified by-

$$\boldsymbol{P_i = \sum_{u=0}^{7} b(p_{i,u}).\, 2^u} \quad \textbf{(2)}$$

This algorithm will generate two bits which will be replaced by two original least significant bits (LSBs). There two different algorithm has been proposed to generate these bits. The first LSB is called Binding bit and second bit is called position bit. Here we have taken the benefit of neighbours of pixel $\boldsymbol{P_i}$. As we know there are two type of neighbours first one is diagonal neighbours $N_D(P_i)$ and second one is immediate neighbour $N_4(P_i)$.

Binding bit generation: The first LSB for a given pixel in host image I is called as binding bit. As a first step we are taking the position of all pixels with respect to their row and column value then associate it with corresponding pixel by following ways

Consider any pixel of I as P_i of block B. So we 8 MSBs of P_i represented as b_a where $a \in (0..7)$ for binding bit calculation. Similarly $b(N_D(P_i))$ is the binary value of corresponding diagonal row and column value in spatial image plane. First of all convert first two LSBs of all pixels P_i to zero.

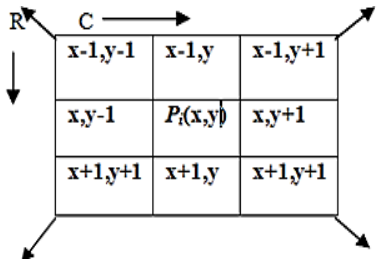

Figure 1: Fragile Pixel wise using Diagonal Neighbor location generating binding bit.

Let us consider that we are dealing with pixel P_i having coordinate value x and y now there will be four diagonal neighbor. Now we will calculate the following.

Step1- Calculate x=x-1 and y=y+1 repeat until x=0 or y= M (if M=N)
If x=0 then $P_{D1} = r$ else $P_{D1} = c$
Where r and c are the corresponding row and column value.

Step2- Calculate x=x-1 and y=y-1 repeat until x=0 or y= 0
If x=0 then $P_{D2} = c$ else $P_{D2} = r$

Step3- Calculate x=x+1 and y=y-1 repeat until x=M or y= 0
If x=M then $P_{D3} = c$ else $P_{D3} = r$

Step4- Calculate x=x+1 and y=y+1 repeat until x=M or y= M (if M=N)
If x=M then $P_{D4} = c$ else $P_{D4} = r$

Step5- Now convert the P_{D1}, P_{D2}, P_{D3} and P_{D4} into 6 bit binary format denoted by $b_i(P_{D1})$, $b_i(P_{D2})$, $b_i(P_{D3})$ and $b_i(P_{D4})$ respectively.

Step6- Take a Secret key K_1 and generate a pseudo random binary matrix I_{key1} of same size as image.

Step7- Now calculate the following:

B_1= Ex-Or($b_i(P_{D1}$),P_a) Where a={5,6,..0} and i=(0,1,2..5)
B_2= Ex-Or (b_i (P_{D2}),P_a)
B_3= Ex-Or (b_i (P_{D3}),P_a)
B_4= Ex-Or (b_i (P_{D4}), P_a)
B_{12}= Ex-Or (B_1,B_2)
$B34$= Ex-Or (B_3,B_4)

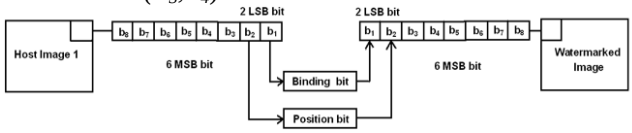

Figure 2: Block diagram for watermarking Embedding procedure

Where, B_1, B_2, B_3, B_4 represents bitwise Ex-OR operation between row value and pixel value where as B_{12}, B_{34} represents bitwise Ex-OR operation between column value and pixel value. Hence Binding bit can be calculated as
After getting these four values calculate B_{12} and B_{34}

$$\boldsymbol{Binding\ bit} = \{\sum_{j=0,1..5}(\boldsymbol{B_{12}} \wedge \boldsymbol{B_{34}})\}\ \boldsymbol{mod\ 2} \quad \textbf{(3)}$$

Finally this binding bit will be replaced by first LSB of the original pixel P_i.

Step8- Finally we take the xor operation in between the I_{key1} and matrix of binding bits.

Position bit generation: The second LSB of Pi is called as Position bit. The Second LSB of given pixel will be called Position bit is generated by the immediate neighbor $N_4(p_i)$ of pixel P_i. To generate it first of all b_i for each P_i will set to zero where i=(0,1,2).Now perform the following steps.

Step1- Calculate $b_a^r \bmod 64$ and $b_a^c mod\ 64$ for each $P_i mod\ 64$ where a={0-5} and i of P_i is also from 0 to 5.Step2- Perform decimal addition on every bit of b_a^r , b_a^c and P_i respectively. here, individual bit sum will must be greater or equal to two

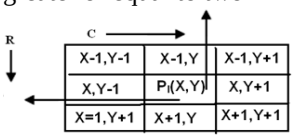

Figure 3: Fragile Pixel wise using immediate Neighbor location generating associate bit

Step2- Represent individual sum bit in 2-bit binary format so by this way we will have 12 bits.

Step3- Now, from these 12 bits, generate 4x3 pixel matrix P_m.

Step4- Generate 4x3 secret matrix Sm from secret key with the help of pseudo-random function. This is the symmetric key which must be known to authentic embedder and receiver.

Step5- Now, By XOR-ing P_m.with the S_m, we get destination matrix D_m .

$$\boldsymbol{D_m = Ex\text{-}or(P_m, S_m)} \quad \textbf{(4)}$$

Step6- Calculate the $D_{m(col)}$which a column vector by repeatedly applying the following formula by following way

$$\boldsymbol{D_{m(col)} = Ex - or_{i=1,2,3}(D_m^i \oplus D_m^{i+1})} \quad \textbf{(5)}$$

Step7- Now calculate the two position bit by using following formula

$$\boldsymbol{Position\ bit = Ex - or\ \ (D^1_{m(col)} \oplus D^2_{m(col)})} \quad \textbf{(6)}$$

Now this calculated position bit will be replaced by second and LSB of given pixel P_i .After all manipulation of matrix M_i whatever image we get that will be watermarked image. Assuming that the original distribution of 2 LSBs is uniform, the average energy of distribution caused by watermarking on each pixel can be calculated a

$$\boldsymbol{MSE} = \frac{1}{mn}\sum_{i=0}^{m-1}\ \sum_{j=0}^{n-1}\big(\boldsymbol{I(i,j) - K(i,j)}\big)^2 \quad \textbf{(7)}$$

Where MSE is mean square value which is for $m \times n$ two monochrome image I and K in which one of the image is original host image and another one is watermarked image.

The mean squared error (MSE) for our practical purposes allows us to compare the true pixel values of our original image to our degraded image. The MSE represents the average of the squares of the errors between our actual image and our noisy image. The error is the amount by which the values of the original image differ from the degraded image.

Now the PSNR is defined as:

$$\textbf{PSNR} = \boldsymbol{10\log_{10}\frac{(MAX)^2}{MSE}} \quad \textbf{(8)}$$

The proposal is that the higher the PSNR, the better degraded image has been reconstructed to match the original image and the better the reconstructive algorithm. This would occur because we wish to minimize the MSE between images with respect the maximum signal value of the image.

Effect of tampering: Suppose an attacker alters the gray scale value of pixel P_i then we see that at what probability three alteration bits namely Binding, Position1 and Position2 will alter.

Total number of possible alteration for any pixel P_i due to 8 Pixel is

$$\boldsymbol{\alpha_1 = \sum_{k=0,1..7} {}^8C_{\ k}} \quad \textbf{(9)}$$

Since alteration in P_i will not be detected by Binding bit if the $b_i(P_{D1})$ and $b_i(P_{D2})$ or $b_i(P_{D3})$ and $b_i(P_{D4})$,which are binary bits of corresponding diagonally row and column of altered pixels are even time similar. Hence the total number of set of MSBs which affects the Binding bit is

$$\boldsymbol{\alpha_2 = \sum_{1 \le w \le k} \binom{k}{w} . 2^{8-k}\ \ Where\ w\ is\ odd} \quad \textbf{(10)}$$

Above equation shows that combination also, for which $b_i(P_{D1})$ and $b_i(P_{D2})$ or $b_i(P_{D3})$ and $b_i(P_{D4})$ is not similar for any bit. So we calculate that factor for getting the number of actual altered pixels. Since the size of image M x N . Here we are considering the M=N=255. If either M ≥ 128 or N ≥ 128

Hence the probability for altering the Binding bit or both are satisfied then the multiplicative factor i

$$\boldsymbol{\Omega = 1 - \frac{\{(M-128)+(N-128)\}}{(M*N)}} \quad \textbf{(11)}$$

Hence the number of pixels which actually affects the Binding bit is given by

$$\boldsymbol{\alpha_3 = \Omega * \alpha_2} \quad \textbf{(12)}$$

So the probability of alteration in Binding bit due to any change in pixels is

$$\textbf{Pr}(\boldsymbol{b}) = \boldsymbol{\frac{\alpha_2}{\alpha_1}} \quad \textbf{(13)}$$

Effect on Position bits: Alteration in P_i will be detected by Position bits if and only if the number of change in the each row of Destination matrix D_m of altered pixel P_i odd. Hence the total number of pixels which actually affects the Position bit is

$$\boldsymbol{\beta} = \boldsymbol{\alpha_1} - \sum_{l=0,2,,4} {}^{4}\boldsymbol{C}_{l} \quad \textbf{(14)}$$

Therefore the probability of alteration in Position bit due to any change in P_i is

$$\boldsymbol{Pr(p)} = \frac{\boldsymbol{\beta}}{\boldsymbol{\alpha_1}} \quad \textbf{(15)}$$

Hence the total probability for a pixel to be detected as a altered one is

$$\boldsymbol{Pr_{(pix)} = Pr_{(b)} + Pr_{(p)}} \quad \textbf{(16)}$$

We have calculated total probability for a pixel to be detected; now we calculate probability for detection of all altered pixels for the host image. Let I be an image having dimension M × N .Suppose μ number of pixels are during any attack without changing the image size. Denote the ratio between μ and M × N as *Rp.* Since any alteration in the pixel may change the Binding and Position bits, so we can calculate the probability for detection of altered pixel in the host image as,

$$\boldsymbol{Pr_{(Image)} = R_p \, x P_{r(pix)}} \quad \textbf{(17)}$$

Watermark Extraction Procedures

At the receiver end we have to localize the entire tampered pixel which may be intentional or unintentional. So detection of tampered pixels needed extraction algorithm which is as follows:

Now at receiver end if the image is altered then it is desirable to detect the altered pixel. For proposed algorithm it is compulsory to have the knowledge of shared secret key by which watermark is embedded. The watermark extraction algorithm is as follows.

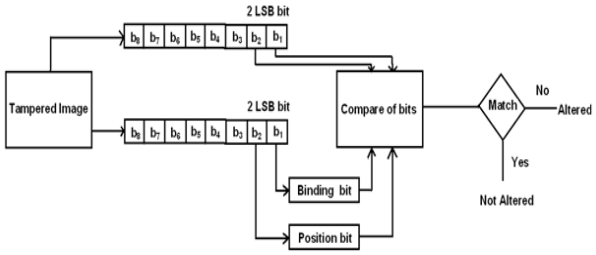

Figure.4 Block Diagram of watermark extraction Procedure to identify image pixel value

Step1- Suppose tampered image is denoted by I_T . Now first of all we have to calculate the binding bits for each pixel P_i . Same procedure will be followed as embedding and generated bit will be stored separately in other matrix M_r of same size M x N.

Step2- Now for each pixel P_i we will calculate two Position bits. For which first of all we have to generate the pseudo random matrix for by same secret key. Using same procedure as embedding we will calculate the both position bits and store it in M_r.

Step3- Now extract the two LSBs of each pixel P_i of altered image and compare the one to one three bit LSBs of M_r .If there is mismatch found then mark that pixel as altered one else mark as unaltered. There are two type of false decision may occur: False positive and false negative. It may be calculated as 0

$$\boldsymbol{\pi = \alpha_1 - (\Omega * \alpha_2 + \beta)} \quad \textbf{(18)}$$

$$\boldsymbol{Pr_{(false)} = \pi / \alpha_1} \quad \textbf{(19)}$$

6. Result & Discussion

Now, we demonstrate the effectiveness and accuracy of the proposed approach with experimental results and discuss the performance of our algorithm. The simulation has been implemented in Matlab 2010 environment. We have taken many gray level test images as a host image with size 256× 256 form a standard image database. First of all we do some major alteration in image which ensures the change in MSBs. Series (c) of all figure having black region shows the unaltered pixel whereas white region shows altered one.

(a) (b) (c)

(i) Lena

(a) (b) (c)

(ii) Baboon

(a) (b) (c)

(iii) Cameraman

(a) (b) (c)

(iv) Jennifer

Figure 5: (a) Watermarked Image, (b) tampered version, and (c) the tampered-pixel localization result

All the results which are generated during watermark embedding and watermark extraction procedure related to

each test image are shown in table [1]. All four alterations mentioned in figure (2) are standard type of tampering which are generally done by attackers. The first experiment shown in figure 5(i) in which Lena's image altered, her eyes has been darken additional on the image is addition of any object in the image. The main application of this attack is to impersonate like someone else using her face or whole image and add it to desired image. So for preventing this, fragile watermarking is used to prove integrity of image. Second tampering shown in figure 5(ii) in which baboon's image is altered, is a common way to write any additional text on the image. In this case it becomes a key task for owner of host image to provide evidence for his virtue. Here the owner can exploit the characteristics of fragile watermarking. Third type of attack on image shown in figure 5(iii) is cameraman image altered some object has been marked in rectangle and circle and added using many algorithms like region filling which is used to identify evidence from the host image.

Table.1. Essential information observed during watermark embedding and extraction by neighborhood location based technique algorithm

Host Image	Watermarking Embedding Time	PSNR Value Embedding	Altered Pixels	Detection Time (sec)
Lena	65	54.22 dB	15	51.9
Baboon	49.37	53.99 dB	890	49.7
Cameraman	45.93	53.69 dB	190	46.5
Jennifer	46.59	54.21 dB	613	48.1

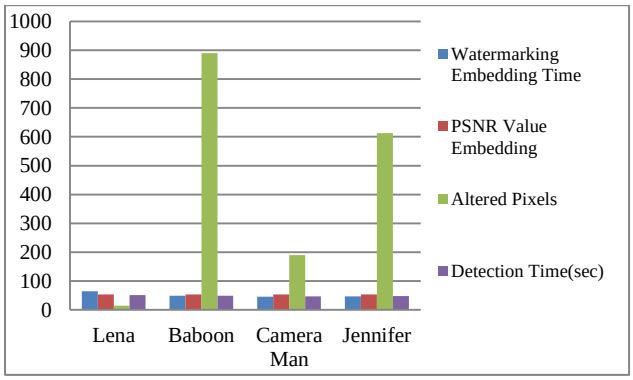

Figure 6 Test results for altered pixels, embedding and detection time.

Using the fragile watermarking it is very easy to detect the object added area. The fourth alteration shown in figure.5 (iv) is very precarious i.e. image of Jennifer alteration has been done as some text been added with a grey color rectangle box. So attacker may try to tamper the evidence .If the image is watermarked using fragile watermarks technique, one can easily reveal the intentionally tampered areas. If the image is watermarked using fragile watermarks technique, one can easily reveal the intentionally tampered areas. Experimental results which are shown in figure(5) ensure the alteration in MSBs, which are detectable up to a satisfactory level by proposed algorithm. There are some filters like mean filter, median filter which generally affects LSBs of most of the host image pixels.

Conclusion

Experimental results have shown the effectiveness of the proposed method for authenticating host images. The proposed approach may detect effective alterations for the watermarking of images and would provide better results than the existing method of fragile watermarking schemes. This paper suggests an efficient pixel-wise fragile watermarking scheme capable of exactly localizing the pixels that are tampered intentionally or unintentionally. In this scheme Binding and position bits are used for ensuring the image integrity. Unlike earlier proposed algorithm by *X Zhang and S Wang* this scheme uses two different techniques for recalculating first two LSBs of a pixel. The results show that this scheme not only detects altered MSBs with high precision but also can localize tampered LSBs with full accuracy

Scope for Further Research

This proposal can also be used for black & white and color images in component-wise manner by taking the all three planes of images as a gray scaled image. Some issues require further exploration in the future, as capability of pixel restoration. If MSBs of any pixel are tampered then it must be perfectly recovered as its original value. Ideas with high pixel-wise restoration capability are desired

References

CHE Shengbing, MA Bin and CHE Zuguo (2008), An Adaptive and Fragile Image Watermarking Algorithm Based on Composite Chaotic Iterative Dynamic System, IEEE DOI 10.1109/IIH-MSP,24.

Chen W. C and Wang M. S (2009),A fuzzy c-means clustering-based fragile watermarking approach for image authentication, *Expert Systems with Applications*, vol. 36, pp. 1300-1307.

Fridrich Jiri and Miroslav Goljan (1999), Images with Self-Correcting Capabilities, IEEE, 0-7803-5467-2/99.

Fridrich, J. Goljan and M. Baldoza, A.C (2000), Image Processing, 2000, Proceedings. 2000. *International Conference on* (Volume:1

He Hongjie, Zhang Jiashu and Chen Fan (2007), Block-wise Fragile Watermarking Scheme Based on Scramble Encryption, IEEE 978-1-4244-4105-1/07.

He Hongjie, Zhang JiaShu and Tai Heng-Ming (2000),A Wavelet-Based Fragile Watermarking Scheme for Secure Image Authentication, IWDW 2006 LNCS 4283, pp. 422432.

Ho.Anthony T. S, Zhu. Xunzhan, Shen Jun and Marziliano Pina (Sept. 2008), Fragile Watermarking Based on Encoding of the Zeros of the –Transform, *IEEE Transactions On Information Forensic and Security*, Vol. 3, NO. 3, Sept.

J.Fridrich (Jan 2002), Security of fragile authentication watermarks with localization, *Proc. SPIE, vol. 4675, Security and Watermarking of Multimedia Contents*, San Jose, CA.

Kim Mi-Ae and Lee Won-Hyung (2004) , A Content-Based Fragile Watermarking Scheme for Image Authentication,

Springer-Verlag Berlin Heidelberg, AWCC.

Lu H.T, Shen R.M and Chung F.L (2003), Fragile watermarking scheme for image authentication, *Electronics Letters* 39 (12).

Liu Shao-Hui, Yao Hong-Xun , Gao Wen and Liu Yong-Liang (2006), An image fragile watermark scheme based on chaotic image pattern and pixel-pairs, 0096-3003/$,. Elsevier.

Lim Yusuk, Xu Changsheng and Feng David Dagan (2002), Web based Image Authentication Using Invisible Fragile Watermark, Australian Computer Society..

Lin Eugene T and Delp Edward. J (2008),A review of fragile watermarking. Center for Education and Research in Information Assurance and Security, Purdue University, West Lafayette, Mechanism. Elsevier.

M.M. Yeung and F. Mintzer (1997), An invisible watermarking technique for image verification, *Proc. IEEE Int. Conf. Image Processing*, ,vol. 2.

P. Wong (1998), A public key watermark for image verification and authentication, *Proc. IEEE Int. Conf. Image Processing, Chicago*, IL.

Seng Woo Chaw, Du Jiang, and Pham Binh (2009) , exact position of alteration with high precision Watermark with Self Authentication and Self Recovery. *Malaysian Journal of Computer Science*, Vol. 22(1).

Shivani Shivendra, Patel Anoop, Kamble Sushila and Agarwal Suneeta (Feb 2011), Self Recoverable Block wise Fragile Watermarking Scheme based on Histogram Segmentation *ACM ICWET.*

Shivani Shivendra, Patel Anoop, Kamble Sushila and Agarwal Suneeta (Feb 2010), An Efficient Pixel wise Fragile Watermarking Scheme based on ARA bits, *ACM ICCCS*, Rourkela.

Shivani Shivendra, Patel Anoop, Kamble Sushila and Agarwal Suneetl (2012), Image Authentication and Recovery using Block wise Fragile Watermarking based on K-medoids Clustering Approach. *IJCA* Vol-15.

Wong Ping Wah and Memon Nasir (Oct 2001), Secret and Public Key Image Watermarking Schemes for Image Authentication and Ownership, *Verification IEEE Transactions On Image Processing.*

Xi Zhao**,** Robust and Semi-fragile Watermarking Techniques for Image Content Protection , M. Phil/PhD Transfer Report. Page (1-2)

Yang-Kuo Lee, Jen-Chun Chang, Hsin-Lung Wu and Rong-Jaye Chen (Dec 2012) An Efficient Fragile Watermarking Scheme for Pixel-wise Tamper Detection 2012, *Sixth International Conference on Genetic and Evolutionary Computing*.

Yong-Zhong He and Zhen Han (2008),A Fragile Watermarking Scheme with Pixel-wise Alteration Localisation, IEEE, 978-1-4244-2179-4/08.

Yusuk Lim, Changsheng Xu and David Dagan Feng, Web based Image Authentication Using Invisible Fragile Watermark, *Australian Computer Society, Inc*

Zhang Xinpeng and Wang Shuozhong , Fragile watermarking scheme using a hierarchical mechanism, Science Direct, Elsevier, Volume 89, Issue 4, Pages 675–679.

Zhang Xinpeng and Wang Shuozhong (2009), Fragile Watermarking Scheme with Extensive Content Restoration Capability Springer-Verlag Berlin Heidelberg, IWDW 2009, LNCS 5703, pp. 268278.

Zhang Xinpeng, Wang Shuozhong, Qian Zhenxing and Feng Guorui (Feb 2011) , Reference Sharing Mechanism for Watermark Self-Embedding, IEEE Transactions On Image Processing, Vol.20,NO.2.

Zhang Xinpeng and Wang Shuozhong (Dec 2008), Fragile Watermarking With Error-Free Restoration Capability, *IEEE transaction of multimedia*, VOL. 10, NO. 8.

Zhang Xinpeng and Wang Shuozhong, Statistical Fragile Watermarking Capable of Locating Individual Tampered Pixels, *IEEE Signal processing*

Zhao, X. , Univ. of Surrey, Guildford Ho, A.T.S. Treharne and H. ; Pankajakshan, V (2007). A Novel Semi-Fragile Image Watermarking, Authentication and Self-Restoration Technique Using the Slant Transform. Intelligent Information Hiding and Multimedia Signal Processing, 2007. IIHMSP 2007. Third International Conference on (Volume, 1), Page(s): 283 – 286, 26-28 Nov. 2007.