International Journal of Modern Trends in Engineering and Research
www.ijmter.com
e-ISSN No.:2349-9745, Date: 2-4 July, 2015

Digital image watermarking scheme for tamper detection & peak signal noise ratio

Priyanka Patil[1], Prof. Ms. J.V.Shinde[2]
[1]*Department of Computer Engineering, Late G.N.Sapkal College of Engineering, Anjaneri, Nasik*
[2]*Department of Computer Engineering, Late G.N.Sapkal College of Engineering, Anjaneri, Nasik*

Abstract*:* Digital image fragile watermarking is an information hiding technique which adds the watermark into the host image for authentication .while achieving the high integrity one should not compromise with quality distortion of images. numbers of watermarking schemes exist today for balancing between the tamper detection rate and quality of reconstructed images in propose scheme we aim at maintain high tamper detection rate as well as high Peak to Signal Noise Ratio (PSNR) of reconstructed images for their quality. For that we utilize Local Binary Pattern (LBP) for this purpose to obtain the optimum solution.In the proposes scheme we used a fragile image watermarking scheme with recover ability based on local binary pattern (LBP). The local binary pattern operator is used to extract localized spatial features .a local binary pattern is used to represent the localized relations of a pixel with its neighborhood pixels. Every pixel measured by the LBP operator and obtained its own local binary pattern as representation of local spatial relations. We utilizes the LBP operator to generate authentication data which are embedded into each image block with 3 × 3 pixels size for tamper detection and recovery. The recovery information is obtained by calculating the mean value of each image block, and then the mean value is converted into a binary string which is embedded into eight neighboring pixels' LSBs of each image block for image recovering
Keywords*:* LBP, tamper image, digital image, noise, watermark

I. INTRODUCTION:

digital images are in use in most of the applications. They also important in storage and transfer information specific the secret ones. With this wide use of digital images, in addition to the increasing number of tools and software of digital images editing, it has become easy to manipulate and change the actual information of the image. Therefore, it has become necessary to check the authenticity and the integrity of the image by using modern and digital techniques, which contribute to analysis and understanding of the images' content, and then make sure of their integrity**.**The local binary pattern (LBP) operator is utilizes a binary representation on gray-level local texture patterns. And is defined as a circular symmetric pattern on local image area which describes the relationships between the current pixel and it neighboring pixels. the LBP operator can be utilized as the representative information of the local structure for developing digital image watermarking for copyright protection and image authentication.In the proposed scheme an LBP-based fragile watermarking scheme for image tamper detection and recovery is used and also utilizes the LBP operator to generate the authentication information for self-embedding. The local binary pattern of each image block is considered as authentication data for tamper detection

II. PROPOSED SCHEME

In the proposed scheme we focuses on the ability of the LBP operator to improve the performance on image tamper detection and watermarking scheme for image tamper detection and recovery is proposed in this paper Also proposed scheme utilizes the LBP operator to generate the authentication information for self-embedding.

The proposed scheme uses the different module to process, th flow of the process is as shown in the architecture.

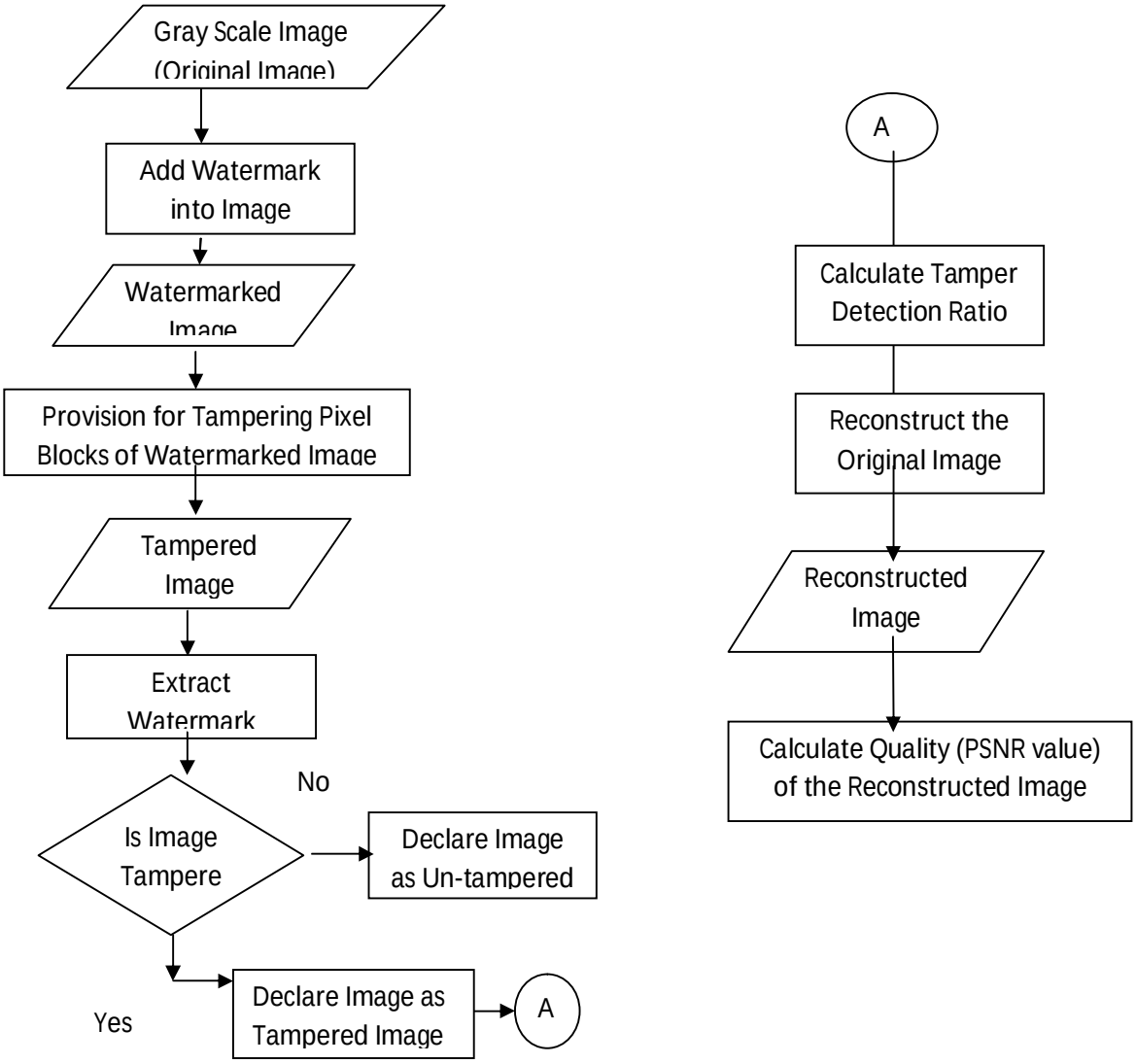

Figure: Architecture diagram

The authentication data and recovery information are embedded into 2-LSBs of each pixel of image blocks. The proposed scheme can achieve locating and recovering tampered areas on the watermarked image with better image quality. The proposed scheme embeds the watermark and authentication in the following different section:

2.1.Authentication & Read Image

At the starting section we validate the user by input the username and password. Validating the same in the database will allow using the system. Also read the input image which is gray scale image pixel by pixel. The read pixels will be temporarily saved in respective original image matrix of pixels.

2.2. Add Watermark and image tamper

In this section we apply the watermark in the original image and will save the pixel values of newly formed watermarked image in another respective matrix of pixels. It will generate watermarked image.

Step 1: Set the 2-LSBs of each pixel value of the original image *I* to (00)2.

Step 2: the LBP of the current image block is generated by Eq. (2),

$$s_x = \begin{cases} 1 \; if \; p_x \geq p_c \\ 0 \; if \; p_x < p_c \end{cases} \qquad (2)$$

Where,

Pc is center pixel value,

Px is each neighboring pixel value

Sx is the sign of each neighboring pixel.

Step 3: watermark bits *w*1 and *w*2 is generated by Eq. (3),

$$w_1 = s_0 + s_2 + s_4 + s_6 \qquad (3)$$
$$w_2 = s_1 + s_3 + s_5 + s_7$$

Step 4: add watermark bits *w*1 and *w*2 into 2-LSBs of the center pixel value *Pc*.

Step 5: Calculate pixel mean of the current image block then convert it into the binary format as *M* vector.

Step 6: Embed the both vector S vector and *M* vector into the 2-LSBs of the image block but the mapping sequence is same, then the watermarked image *I* is read

2.3. Extraction and tamper detection section:

Extracting the watermark form the possibly tampered image for checking weather intruder has tampered our image or not and then we will compare extracted watermark with the original watermark added previously. If the matching fails then the image will be confirmed as tampered image otherwise not.

If the section is found to be tampered then recover the original image from the tampered image by using extracted watermark. It will generate the reconstructed image. During the image transmission over the Internet, the watermarked image could be tampered. In this situation, the received image should be authenticated by the proposed scheme for image tamper detection and recovery. The detailed procedures are described as follows:

Step 1: get 2-LSBs of indivisual pixel value for each image block and insert it to (00)2 into 2-LSBs of each pixel value.

Step 2: obtained the LBP of the current image block by Eq. (2) as *S* vector and calculate the watermark bits *w1* and *w2* by Eq. (3).

Step 3: Compare *w1* and *w2* with extracted watermark bits *w*1 and *w*2. If they are not the same, then the current image block is denoted as "tampered block".

Step 4: Compare *S* vector with the extracted *S* vector. If they are not the same, then the current block is denoted as "tampered block".

Step 5: If Step 3 and Step 4 occur, the current block is judged as "tampered block", and then recover it by the extracted pixel mean with *M* vector

2.4. Performance Measurement section:
This module will measure the performance of our system by applying the two metrics namely, tamper detection ratio and Peak to Signal Noise Ratio (PSNR)

III. MODELING

In order to represent proposed system in mathematical form, we used set theory along with the functions and relationship, because it's easy to use and understand the system thoroughly.
System problem definition can be framed in the form of a set theory. Let S be a
automatic semantic content extraction system

S = {**I, F, O, C**} where,
I represents set of inputs;
I = {**II, TB**}
II = input image
TB=tamper block
F is the set of functions;
F = {**F1, F2, F3,F4,F5**}
F1 = add watermark
F2 = generate LBP
F3 = tamper detection
F4= extract watermark
F5=reconstruct image
C is the set of constraints applied to functions;
C = {**C1, C2**}
C1 = Calculate LBP
C2 = relations between pixel
O is the set of outputs;
O = {**E, C, O1, O2**}
E = Event
C = Concept
Functions:
F1: (add watermark)
X: LBP
C1 = Calculate LBP
F1(x): watermark is add with LBP
F2 :(generate LBP**)**
X: Given input II and F1(x)
C2 = relations between pixel
If (input is II and LBP)
Calculate relationship between pixels
If Similarity =1
Set representation using Venn diagram:

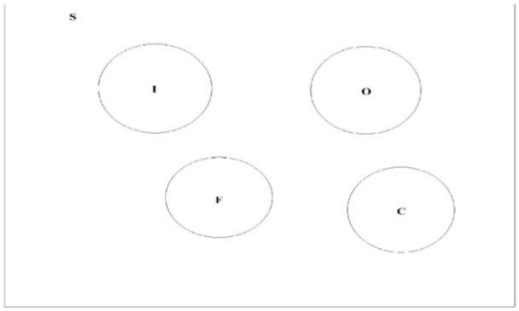

Figure 1: Venn diagram

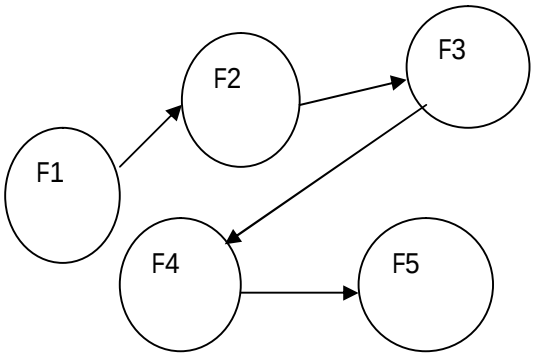

Figure 2: Functions Dependency

IV. RESULT ANALYSIS

gray-level images with 512 × 512 pixels are used in experiments, which are "Airplane", "Lena", "Sailboat" and "Peppers" Experimental results are compared with proposed system

1. The comparison result of PSNR of the watermarked image is shown in Table I, the proposed scheme embeds the information into 2-LSBs of each pixel value. The PSNR of watermarked image can achieve better tamper detection performance with low distortion image quality

Table 1: PSNR of Watermark image

Image	Existing system	Proposed system
LENA	42.6453	44.09695
AIRPLANE	41.2847	43.2156
PEPPERS	42.5264	45.4627

2. The comparison of tamper detection rates between the proposed scheme and existing scheme. The tamper detection rate of their scheme is over 40% .The tamper detection rate of the proposed scheme is over 90%, which means the proposed scheme can easily detect the tampering on digital images. In the proposed scheme, there is no technique is available to achieve the performance of tamper detection. The authentication data is generated by the content of digital images without extra information. Also, the complexity of the LBP operator is lower than any other signature-based fragile watermarking scheme. It can be widely used in hardware level or cloud computing in mass image database

Table 2: Tamper Detection Rate

Image	**Existing system**	**Proposed system**
LENA	**3688/3872**	**3260/3218**
AIRPLANE	**1347/1428**	**1280/1150**
PEPPERS	**631/652**	**630/620**

The following images of jpg show the experimental analysis of the proposed scheme. the lena image is used for the experiment analysis :

(a)_ (b)

Figure3: lena image (a) before experiment (b) after the experiment

CONLUSION AND FUTURE SCOPE

In the proposed scheme we utilize the relation among maintain high tamper detection rate so that the integrity check will be more successful, also maintaining high Peak to Signal Noise Ratio (PSNR) which will ensure high quality of reconstructed image. We also try to keep more flexibility to obtain required balance between the tamper detection rate and PSNR by introducing some user controllable parameters. The proposed scheme improves Zhang and Shih's watermarking scheme on ability of image tamper detection and image recovering. As a result of the texture analysis ability of the LBP operator, so future work consist of the spatial based fragile watermarking scheme can be further improved with LBP features on image tamper detection recovery with lossless for future works

REFRENCES

[1] T. Ojala, M. Pietikainen, and D. Harwood (1994), "Performance evaluation of texture measures with classification based on Kullback discrimination of distributions", Proceedings of the 12th IAPR International Conference on Pattern Recognition (ICPR 1994), vol. 1, pp. 582 – 585

[2] T. Ojala, N Pietikainen, and D. Harwood (1996), "A Comparative Study of Texture Measures with Classification Based on Feature Distributions", Pattern Recognition, vol. 29, pp. 51-59.

[3] Z. Wenyin and Frank Y. Shih, "Semi-fragile Spatial Watermarking Based on Local Binary Pattern Operators," *Optics Communications*, Vol. 284, Issues 16–17, 2011, pp. 3904-3912

[4] G. Voyatzis and I. Pitas, "Chaotic Mixing of Digital Images and Applications to Watermarking," *Proceedings of European Conference on Multimedia Applications, Services and Techniques (ECMAST '96)*, Vol. 2, May 1996, pp. 687-695

[5] G. Voyatzis and I. Pitas, "Applications of Toral Automorphisms in Image Watermarking," *Proceedings of the International Conference on Image Processing*, Vol. 2, 1996, pp. 237-240

[6] Chun-Shien Lu, Hong-Yuan Mark Liao," MultipurposeWatermarking for Image Authentication and Protection", *IEEE Transactions On Image Processing*, Vol. 10, No. 10, October 2001

[7] Ismail Avcıbas¸, *Member*, Nasir Memon,, and Bülent Sankur, "Steganalysis Using Image Quality Metrics", IEEE *Trans. On Image Processing*, Vol. 12, No. 2, February 2003.

[8] Chih-Wei Tang and Hsueh-Ming Hang," A Feature-Based Robust Digital Image Watermarking Scheme", IEEE *Trans. On Signal Processing*, Vol. 51, No. 4, April 2003

[9] Mohammad Ali Akhaee, S. Mohammad Ebrahim Sahraeian,Bulent Sankur, and Farokh Marvasti, ,"Robust Scaling-Based Image Watermarking Using Maximum-Likelihood Decoder With Optimum Strength Factor", *IEEE Trans.On Multimedia, Vol. 11, No. 5, August 200*

[10] Manickam. L,Dr.S.A.K.Jilani and ,Dr.M.N.Giri Prasad," A Novel Fragile Watermarking Scheme For Image Tamper Detection Using K Mean Clustering", *International Journal of Computer Trends and Technology (IJCTT) – volume 4 Issue10 – Oct 2013*

[11] Anil K. Jain, Fellow,Umut Uludag,"Hiding Biometric Data", *IEEE Transactions On Pattern Analysis And Machine Intelligence, Vol. 25, No. 11, November 2003*
[12] Yonghong Chen, Jiancong Chen," Digital Image Watermarking Based on Mixed Error Correcting Code", *Journal of Information Security*, 2012, 3, 156-161
[13] Darko Kirovski and Henrique S. Malvar," Spread-Spectrum Watermarking of Audio Signals", *IEEE Transactions On Signal Processing, Vol. 51, No. 4, April 2003*
[14] Ning Bi, Qiyu Sun, Daren Huang, Zhihua Yang, and Jiwu Huang," Robust Image Watermarking Based on Multiband Wavelets and Empirical Mode Decomposition", *IEEE Transactions On Image Processing, Vol. 16, No. 8, August 2007*
[15] Chao-Ming Wu, Yan-Shuo Shih," A Simple Image Tamper Detection and Recovery Based on Fragile Watermark with One Parity Section and Two Restoration Sections", *Optics and Photonics Journal*, 2013, 3, 103-107
[16] Arvind Kumar Parthasarathy and Subhash Kak," An Improved Method of Content Based Image Watermarking", *IEEE Transactions On Broadcasting, Vol. 53, No. 2, June 2007*
[17] Mauro Barni, Franco Bartolini,and Alessandro Piva," Improved Wavelet-Based Watermarking Through xel-Wise Masking", *IEEE Transactions On Image Processing, Vol. 10, No. 5, May 2001*

