ADVANCED LBP FRAGILE WATERMARKING SYSTEM FOR IMAGE TAMPER DETECTION AND RECOVERY

Shital Prabhakar Bagal¹, Prof. P. M. Mohite² and Prof. Sathya Praveen D.³
¹MECSE, SYCET, Aurangabad
²,³CSE Department, SYCET Aurangabad

Abstract—This paper describes how digital images are used in a wide range of applications and for multiple purposes. They also play an important role in the storage and transfer of visual information, especially the confidential ones. With the widespread usage 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 image content and then make sure of their integrity. 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 optimal solution. In this paper we used a fragile image watermarking scheme with recover ability based on local binary pattern (LBP). The local binary pattern operator 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. In the paper consider input as 256×256 as well as 512×512 dimension image, one of the advantage compare to other existing system is that it can also processed the color image. The quality is calculated by the PSNR but in the proposed scheme PSNR at peak point is also calculated to achieve better result.

General Terms—Digital image watermarking, fragile image watermarking, local binary pattern (LBP), PSNR (peak signal to noise ratio)

Keywords—Authentication, signal, noise, information hiding, integrity, Local Binary Pattern (LBP), PSNR (Peak Signal to Noise Ratio).

I. INTRODUCTION

Hence digital watermarking becomes very stunning research topic. Digital watermarking technology that detect and create invisible markings, which can be used to track down the origin, accuracy, and authorized usage of digital data. In future the major development of digital watermarking is like as: pirate tracking, image authentication, copying protection, copyright protection, and hide communication [1,3].

The meaning of robustness is in which watermark is capable to resist some changes in the watermark embedded signal. So a good algorithm should be robust. In terms of embedding field digital watermarking are classified into two category spatial domain and frequency domain watermarking. In spatial domain method watermark is embed by modifying the pixel values of novel
image and transform domain process which embeds the data by modulating the transform area coefficients. Semi fragile spatial domain technique is more robust than frequency domain technique.

II. LITERATURE SURVEY

2.1 History

Debotosh Bhattacharjee, Ayan Seal, Suranjan Ganguly, Mita Nasipuri, and Dipak Kumar Basu[1] proposed the study two local-matching techniques, one of it is wavelet and the other based on Local Binary Pattern, are analyzed. Human face images are processed first and cropped the face region only, from the entire face images. After the LBP features for dimensionality reduction, are used separately for recognition of the face.

Yaoran Huo, Hongjie He and Fan Chen[3] proposed a semi-fragile watermarking scheme with discriminating general tampering from college attack, which presents a new tamper proofing providing more information on who modified the image For each 8×8 image block. The proposed scheme has a superior performance of tamper detection and an ability of discriminating general tampering from college attack, but not able to recover the tampered region.

Chun-Shien [6] proposed a multipurpose watermarking scheme which can be applied to achieve both authentication and protection of multimedia data the proposed scheme has three special features:
1) The approximation information of a host image is kept in the hiding process by utilizing masking thresholds
2) Oblivious and robust watermarking is achieved for copyright protection.
3) Fragile watermarking is achieved for detection of malicious modifications and tolerance of incidental manipulations.

Ismail Avcıbas [7] proposed the problem of steganalysis of images, and he developed a technique for discriminating between cover-images and stego-images. This approach is based on the hypothesis that message-embedding schemes leave statistical evidence or structure in images that can be exploited for detection image quality metrics as the feature set. To identify good features (quality measures).

Chih-Wei Tang and Hsueh-Ming Hang [8] proposed a digital image watermarking scheme was designed to survive both geometric distortion and signal processing attacks. There are three key elements in our scheme:
1) Reliable image feature points
2) Image normalization
3) DFT domain bits embedding.
No reference images are needed at the detector.

Darko Kirovski and Henrique S. Malvar [13] proposed present several novel mechanisms for effective encoding and detection of direct-sequence spread-spectrum watermarks in audio signals. The developed techniques aim at
1) Improving detection convergence and robustness
2) Improving watermark imperceptiveness,
3) Preventing desynchronization attacks,
4) Alleviating estimation/removal attacks, and finally,
5) Establishing covert communication over a public audio channel.

Chao-Ming Wu, Yan-Shuo Shih [15] proposed a simple self-recovery fragile watermarking scheme that localizes tampering, the original image is partitioned into blocks of size 3×3. In this scheme, the watermark payload is composed of parity watermark section and two copies of restoration watermark section. All of the watermark sections are used for tamper detection.

III. PROPOSED SYSTEM

Local Binary Pattern (LBP) is a feature which is used for classification in digital images. LBP was first elaborated in 1994. Since then it is used as a powerful feature for texture classification.
Earlier LBP operator is widely used in texture classification and face recognition to measure the local contrast between pixels. Now a days it is also used to ensure the authenticity of digital image as it provide a comparatively robust watermark embedding technique for digital images. The main concept of LBP can be explained as:

### 3.1 Concept

In LBP technique, LBP operator is defined as, a local neighborhood surrounding a center pixel which is used as the threshold to define the local contrast of the surrounding pixels with respect to the center pixel. The surrounding pixels are labeled as 1 when the value of that pixel is greater than the center, or labeled as 0 when the value is smaller than the center. To obtain LBP code of the center pixel threshold values of neighboring pixels are multiplied with their corresponding weights and summing up them and watermark value is generated.

### 3.2 Watermark Embedding

In this method, three vectors are created namely gp, mp and sp. the first vector gp is used to hold the gray level values of pixels, second vector mp is used to hold the values of difference between each surrounding pixel and the center pixel, third vector sp is used to hold the binary information about each pixel based on the obtained difference between center pixel and the each surrounding pixel as 1 or 0 by comparing it with the value of center pixel.

In order to embed watermark, the XOR function is used to calculate the XOR value of the whole sp vector because has associative and commutative properties that is any circular shift of bits does not change the value of the function.

One bit of the watermark is embedded in a local region. In order to embed the watermark bit in the local region, the watermark bit and the XOR value of the region is compared if they are not same then only that bit is embedded in that local region. In this method author uses a $3 \times 3$ window to define local region. After successfully selecting the local region, the pixel whose value in the mp vector is minimum as choose to embed the watermark bit. If all the values of a local region are 0 or 1 then the value of the center pixel is modified in order to embed the watermark bit.

### 3.3 Watermark Extraction

To extract the watermark from the image simply the XOR value of each local region is judged if the value is 0 the corresponding watermark bit is 0 or if the value is 1 the corresponding watermark bit is 1. So the watermark embedding and the extraction phases are very simple but are robust against the post processing attacks like noise addition.
IV. PERFORMANCE ANALYSIS

Gray-level images with 512×512 pixels are used in experiments, which are “Lena”, “Airplane”, “Peppers” and “Sailboat”. Experimental results are compared with proposed system.

Figure 3
1. The comparison result of PSNR of the watermarked image is shown in Table 1, between the LBP and proposed system that embeds the information into 2-LSBs of each pixel value. The PSNR of proposed system can give the better performance as compare to LBP, the test is performed on the sample images as LENA, AIRPLANE, and PEPPERS & SAILBOAT.
Table 1: Comparison of PSNR of LBP based system and proposed system

| Image   | LBP Used System | Proposed System |
|---------|----------------|-----------------|
| LENA    | 44.0217        | 44.0897         |
| AIRPLANE| 44.0132        | 44.0643         |
| PEPPERS | 44.0561        | 44.0929         |
| SAILBOAT| 43.8853        | 44.0472         |

2. The comparison of tamper detection rates between the proposed scheme and LBP. The tamper detection rate of LBP 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. The tamper detection rate is calculated in terms of no of detected block from the total tamper blocks.

Table 2: Comparison of Tamper Detection Ratio of LBP based system and proposed system

| Image    | LBP used system (no. of tampered blocks/detected blocks) | Proposed system (no. of tampered blocks/detected blocks) |
|----------|---------------------------------------------------------|----------------------------------------------------------|
| LENA     | 1347/1428                                               | 1519/1530                                                |
| AIRPLANE | 3688/3872                                               | 370/1530                                                 |
| PEPPERS  | 631/652                                                 | 1272/1530                                                |
| SAILBOAT | 453/458                                                 | 1378/1530                                                |

3. The quality of the image is calculated on the basis of the watermark and the reconstructed image as follows quality of watermarked image and reconstructed image in terms of MSE (mean square error), SNR (signal to noise ratio), also one advantage that we can calculate the peak signal to noise ratio at peak point on the basis of these parameter we can calculate the quality of image.

Table 3: Calculated quality of GRAY SCALE LENA 512×512 Reconstructed and Watermarked image

| Parameters    | Watermarked Image | Reconstructed Image |
|---------------|-------------------|---------------------|
| MSE           | 2.53              | 1.94                |
| SNR           | 38.43             | 39.60               |
| PSNR          | 44.08             | 45.24               |
| PSNR at Peak Point | 43.95          | 45.06               |

Table 4: Calculated quality of COLOUR LENA 512×512 Reconstructed and Watermarked Image

| Parameters    | Watermarked Image | Reconstructed Image |
|---------------|-------------------|---------------------|
| MSE           | 2.58              | 3.74                |
| SNR           | 41.29             | 39.71               |
| PSNR          | 44.00             | 42.39               |
| PSNR at Peak Point | 44.00         | 42.39               |
4. In this section the “LENA”, ”AIRPLANE”, “PEPPERS” and ”SAIBOAT” are used for experiments images of (Table 2) as explained. The tamper detection rate of LBP scheme is over 40% and proposed scheme is over 90%, which means the proposed scheme is better and easily detects the tampering on digital images. In (Table 3 & 4) describes the quality of reconstructed image is better as compare to watermarked image so the result of all image is as shown below:

5. After the reconstruction of the image calculates the quality of image in terms of MSE, SNR, PSNR, PSNE at peak point, also in the proposed system we can extend the dimension as 512×512 also with 256×256 as of existing system as LBP with that in the proposed system calculate the tamper detection ratio as number of tampered blocks and its recovered blocks.

**Table 5: Tamper Detection Ratio of Gray Scale Images**

| Image   | Dimension | No. of Tampered Blocks | No. of Recovered Blocks | % Tamper Detection Ratio |
|---------|-----------|------------------------|-------------------------|--------------------------|
| Lena    | 256×256   | 765                    | 759                     | 99.21%                   |
| Sailboat| 512×512   | 1530                   | 1378                    | 90.06%                   |

**Table 6: Tamper Detection Ratio of Color Images**

| Image   | Dimension | No. of Tampered Blocks | No. of Recovered Blocks | % Tamper Detection Ratio |
|---------|-----------|------------------------|-------------------------|--------------------------|
| Mandrill| 512×512   | 1530                   | 1126                    | 73.59%                   |
| Lena    | 512×512   | 1530                   | 1178                    | 76.99%                   |
Figure 6: Test Images a) Lena Color 512×512 b) Lena Gray 256×256 c) Mandrill Color 512×512 d) Sailboat Gray 512×512

V. CONCLUSION

In this result analysis paper of watermarking technique describes a new development in the digital image watermarking for 256×256 which extends to 512×512 and 1024×1024 in which the watermarking technique is analyzed with the help algorithm LBP (local binary operate) and it is better than previous system also in the proposed system we can apply the watermarking on color image for tamper detection and recovery, the quality of the image is calculated in terms of MSE, SNR, PSNR, PSNR at peak point also the tamper detection ratio is calculated.

REFERENCES

[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 Pattern Recognition (ICPR1994), vol. 1, pp. 582-585.
[2] Jun-Dong Chang, Bo-Hung Chen and Chwei-Shyong Tsai, “LBP-based Fragile Watermarking Scheme for Image Tamper Detection and Recovery”, IEEE 2nd International Symposium on Next Generation Electronics (ISNE)-February 2015, Kaohsiung, Taiwan.
[3] 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.
[4] Z. Wenyin and Frank Y. Shih, “Semi-fragile Spatial Watermarking Based on Local Binary Pattern Operators”, Optics Communications, Vol. 284, Issues 1617, 2011, pp. 3904-3912.
[5] 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.
[6] 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.

[7] Chun-Shien Lu, Hong-Yuan Mark Liao, "Multipurpose Watermarking for Image Authentication and Protection", in Proc. IEEE Transactions On Image Processing. Vol. 10, No. 10, October 2001.

[8] Ismail Avchus, Member, Nasir Memon., and Blent Sankur,"Steganalysis Using Image Quality Metrics", in Proc. IEEE Trans. On Image Processing. Vol. 12, No. 2, February 2013.

[9] Chih-Wei Tang and Hsueh-Ming Hang," A Feature-Based Robust Digital Image Watermarking Scheme", in Proc. IEEE Trans. On Signal Processing. Vol. 51, No. 4, April 2013

[10] Mohammad Ali Akhaee, S. Mohammad Ebrahim Sahraeian,Bulent Sankur, and Farokh Marvasti, "Robust Scaling-Based Image Watermarking Using Maximum-Likelihood Decoder Withm Optimum Strength Factor", in Proc. IEEE Trans. On Multimedia, Vol. 11, No. 5, August 2009.

[11] Anil K. Jain, Fellow, Umut Uludag, "Hiding Biometric Data", in Proc. IEEE Transactions On Pattern Analysis and Machine Intelligence, Vol. 25, No. 11, November 2014.

[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", in Proc. IEEE Transactions On Signal Processing. Vol. 51, No. 4, April 2013.

[14] Ning Bi, Qiyu Sun, Daren Huang, Zhihua Yang, and Jiwu Huang, "Robust Image Watermarking Based on Multiband Wavelets and Empirical Mode Decomposition", in Proc. IEEE Transactions On Image Processing, Vol. 16, No. 8, August 2014.

[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", in Proc. IEEE Transactions On Broadcasting, Vol. 53, No. 2, June 2012.