A REVIEW ON ADVANCED LBP WATERMARKING SCHEME FOR IMAGE TAMPER DETECTION AND RECOVERY

Shital Prabhakar Bagal¹, Prof. P. M. Mohite² and Prof. P. D. Sathya³
¹MECSE, SYCET, Aurangabad
²³CSE Department, SYCET Aurangabad

Abstract—Now a days, digital images are in use 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 secret ones. With this 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 images 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 optimum solution. In the proposed scheme 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 proposed scheme we can take the 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 get better result.

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

I. INTRODUCTION

The success of Internet and digital consumer devices such as mobile, laptop, tablet etc. which are used by individuals profoundly changes our daily lives and society by making the transmission, capture and storage of digital data easily and conveniently. However, this raises a big issue is how to protect these data and avert from unauthorized use. These concerns have become issues in many regions such as video and music industry etc. So as a solution digital watermarking is mainly used. 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 embed 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

The idea to communicate secretly is as old as communication itself. Paper watermarks appeared in the art of handmade papermaking nearly 700 years ago. The oldest watermarked paper found in archives dates back to 1292 and has its origin in Fabriano, Italy, which is considered the birthplace of watermarks. At the end of the thirteenth century, about 40 paper mills were sharing the paper marked in Fabriano and producing paper with different format, quality and price. They produced raw, coarse paper which was smoothed and post processed by artisans and sold by merchants. Competition not only among the paper mills but also among the artisans and merchants was very high, and it was difficult to keep track of paper provenance and thus format and quality identification. The introduction of watermarks helped avoiding any possibility of confusion. After their invention, watermarks quickly spread over Italy and then over Europe, and although originally used to indicate the paper brand or paper mill, they later served as indication for paper format, quality, and strength and were also used to date and authenticate paper.

2.2 Watermarking Schemes

2.2.1 The Local Binary Pattern (LBP)

The local binary pattern (LBP) operator is a kind of texture descriptors proposed by Ojala et al [1,2]. It utilizes a binary representation on gray-level local texture patterns. Basically, this local texture pattern is defined as a circular symmetric pattern on local image area which describes the relationships between the current pixel and its neighboring pixels. The main purpose of texture analysis is to extract the characteristics of the local structure for pattern recognition. Therefore, the characteristic of 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. The proposed scheme 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.

2.2.2 Semi-Fragile Watermarking Scheme

Zhang and Shih proposed a semi-fragile watermarking scheme based on the LBP operators [3]. Their scheme utilizes the characteristic of the LBP operator on localized spatial relations of an image to adjust the local pixel contrast for the embedding and extraction of watermarks. The performances on copyright protection can effectively against image processing operation and geometric attacks. However, it cannot effectively achieve the performances of tamper detection and location with recover ability. Thus, the proposed scheme focuses on the ability of the LBP operator on texture analysis to improve the performance on image tamper detection.

2.2.3 Self-Recovery Fragile Watermarking

A simple self-recovery fragile watermarking scheme is proposed paper. To localize tampering, the original image is partitioned into blocks of size 3x3. In this scheme, the watermark payload is composed of parity watermark section and two copies of restoration watermark section [15]. All of the watermark sections are used for tamper detection. Thus, with the same size of watermark payload, the tamper detection performance of the proposed scheme is better. only the two LSBs of each pixel are used for watermark embedding.
2.2.4 K-Means Clustering Watermarking Scheme

A K-means clustering watermarking scheme for image tamper detection. In this method, it is easy to embed a watermark in a digital image and in the extraction phase it doesn’t require the original image for reference purpose. This scheme is used to reduce time complexity when compared with the existing methods like fuzzy based tamper detection [10]. The two applications of watermarking to secure that data are presented. In addition to watermarking, encryption can also be used to further increase the security of biometric data. The first application is related to increasing the security of biometric data exchange, which is based on steganography the proposed method utilizes several properties of the human visual system to keep the visibility of the changes made to the host image low. The future research is to investigate how different (e.g., robust and fragile) watermarking schemes can be combined [11].

2.2.5 Content Based Watermarking Scheme By Analyzing The Cover Object In Both Frequency And Spatial Domains

A comprehensive evaluation and implementation of a content based watermarking scheme By analyzing the cover object in both frequency and spatial domains, a distortion sensitivity of the image content is determined. Local information that is derived from properties such as texture, corner, edge and luminance is used to determine a mask of just noticeable difference values the proposed watermarking. a novel algorithm for image watermarking has been presented. The algorithm embeds the watermark code by modifying the DWT coefficients of the image, and exploits a model derived from image compression techniques for adapting the watermark strength to the characteristics of the HVS The performances of the novel algorithm are very good [13]. Experimental results, in fact, supported the suitability of DWT watermarking schemes for robustly hiding watermarks into images. In particular, the behavior of the watermark detector with respect to image cropping was surprisingly good. The watermarking energy can be kept so high that even a small portion of the image is sufficient to correctly guess the embedded code [11].

2.2.6 Texture Analysis Methods

The various texture analysis methods have been studied for the automatic defect inspection of textile fabrics and it also shown that one-method based systems are unreliable due to the different nature of fabrics. A more specific study has been carried out on five classes of textiles in order to determine the best methods. The results show that there is not a winner between the Algorithms and test of algorithm complexity has been carried out by estimating the computation time in the analysis of standard images the results give a real point of view of the real-time possibilities of every method with the actual technology [2]. A chaotic transformation of image which is based on the mixing property of total automorphism and method for embedding watermark in digital image such a tration scan create hidden pattern [4] and the watermark detection from the signed image is done by applying the same system and by using a specific set of parameters which characterizes the watermark embedding. A more complex mixing, possessing more independent parameters, can miser if we use different automorphisms on sub lattices having different sizes. By using signal detection methods we can get a reliable answer about the existence or not of a watermark even if the watermarked image has been affected quite strongly by filtering and JPEG compression beater than 10: l [5]. A multipurpose watermarking scheme which can be applied to achieve both authentication and protection of multimedia. This is the first method that combines both robust watermarking and fragile watermarking into a single one for image/audio authentication and protection. But having the issues like how to eliminate the need of storing and retrieving the mapping file and the hidden watermarks and considered as secret keys [6].

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 grey 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*3 window to define local region. After successfully selecting the local region, the pixel whose value in the mp vector is minimum is 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.
Figure 2. Watermark embedding and extraction process

IV. CONCLUSION

In this review paper of watermarking techniques describes a new development in the digital image watermarking for 256x256 which will extend to 512x512 in which the watermarking technique will be analyzed with the help algorithm LBP(local binary operate) and it will be better than existing system also in the proposed scheme we can apply the watermarking on color image for tamper detection and recovery, the quality of the image will be calculated in terms of MSE, SNR, PSNR, PSNR at peak point also the tamper detection ratio will be 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] T. Ojala, M. 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, "Multipurpose Watermarking for Image Authentication and Protection", in Proc. IEEE Transactions On Image Processing, Vol. 10, No. 10, October 2001.
[7] Ismail Avcibas, Member, Nasir Memon., and Blent Sankur, "Steganalysis Using Image Quality Metrics", in Proc. IEEE Trans. On Image Processing, Vol. 12, No. 2, February 2013.
[8] 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
[9] 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.
[10] 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.
[11] Yonghong Chen, Jiancong Chen,"Digital Image Watermarking Based on Mixed Error Correcting Code", Journal of Information Security, 2012, 3, 156-161.
[12] 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.
[13] 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.
[14] 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.

[15] 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.

[16] https://en.wikipedia.org/wiki/Imageprocessing.