International Journal for Modern Trends in Science and Technology
Volume: 02, Issue No: 11, November 2016
ISSN: 2455-3778
http://www.ijmtst.com

Tamper Detection using Watermarking Scheme and K-Mean Clustering for Bio Medical Images

R. Suganya[1] | Dr. R Kanagavalli[2]

[1,2] ISE, The Oxford College of Engineering, Bangalore, Karnataka, India.

To Cite this Article
R. Suganya, Dr.R Kanagavalli, "Tamper Detection using Watermarking Scheme and K-Mean Clustering for Bio Medical Images", *International Journal for Modern Trends in Science and Technology*, Vol. 02, Issue 11, 2016, pp. 180-185.

ABSTRACT

In this paper, we focus image authentication and tamper detection using K-mean clustering based on fragile watermarking scheme. The two important aspects of the authentication watermarking scheme are Tamper detection and localization accuracy. In our scheme, clustering values of the watermarked image used as secret key. It can be detect any amendment is made to image and also point out the exact location that have been modified. Significant features of the schemes are reducing the time complexity and improving the PSNR value , with stand attacks. Original image is not required for verification.

KEYWORDS: *Watermarking, k- means clustering, Tamper detection.*

I. INTRODUCTION

In digital media, with the fast development of the Internet, digital images are used as evidences in the news and court reports. However, using dominant image processing software tools, digital images can be simply modified without any limit. Normally these customized images can cause financial and public damages to the concerned persons. Hence the development of a reliable digital image authentication scheme is a critical problem [1]. This problem can be solved by various authentication schemes that verify the integrity and authenticity of the image content.

The authentication schemes may classify in to two categories: as digital signature based schemes and digital watermark based schemes [2]. A digital signature can be either an encrypted or a signed hash value of image contents and/or image characteristics. The foremost problem of signature based schemes is that they can identify if an image has been modified, but they cannot find the regions where the image has been modified. To solve this problem, many researchers have proposed watermarking based schemes for image authentication.

Digital watermarking is a technology for embedding digital data in digital content (audio, images, video…). It has initiated as a tool to enhance the security. Watermarking techniques are classified into *Spatial Domain* and *Frequency Domain.* In *Spatial Domain* the watermarking system directly alters the main data elements (like pixels in an image) to hide the watermark data. In *Frequency Domain* the watermarking system alters the frequency transforms of data elements to hide the watermark data.

The watermarking properties are listed as robustness, data payload, capacity, security, computational cost.

- *Robustness* of the watermark refers to its ability to withstand non- maliciousdistortions,
- *Data payload* is the encoded message size of a watermarked in an image,
- C*apacity* is the amount of watermark information in an image,

- *Imperceptibility* is the characteristic of hiding a watermark so that it does not degrade the visual quality of an image,
- *Security* of a watermark is the ability of the watermark to resist malicious attack,
- *Computational cost* is the measure of computing resources required to perform watermark embedding or detection process. Depending on the application, the properties, which are used essentially in the evaluation process, varies.

Nowadays, digital watermarking appears as an efficient mean to ensure integrity and authenticity verification. Robust watermarks are designed to be hard to remove and to resist to common image operation procedures. They are useful for copyright and ownership assertion purposes. Unlike robust watermark, fragile watermarks are designed to be easily destroyed if the watermarked image is manipulated in the slightest manner. This property is investigated for tamper detection.

Watermarking is also critical for the exchange of data through internet. Significant progress has been achieved in using communication technologies to store and distribute data under digital formats in the last ten years. Conversely, the use of these technologies is not always secure as the court records are freely moved in open networks and thus focused to alterations and misuses. Here we propose K-mean clustering based watermarking technique. The K-mean clustering algorithm is applied to the watermarked image to compute the number of 1's and number of 0's in each layer (red, green, blue) separately. When comparing the clustering values of original and tamper watermarked image, we get a tamper region precisely. This will allow adding an additional security level, which is appropriate for transmission in open network as Internet and location of the tempered area exactly. The performance evaluation shows that our proposed scheme can provide less computational complexity and better security than the traditional watermarking based tamper detection schemes.

The rest of the paper is organized as follows. In Section II describes related work. In section III, K-mean clustering algorithm is briefly illustrated. In Section IV, the proposed watermarking scheme is enlightened. Experimental results are given in Section IV. Conclusions are drawn in Section V.

II. Related Work

A first watermarking was proposed by Walton-based on authentication scheme [1], which alienated the image into 8×8 blocks and each block of LSB embed the checksum . The main setback of the Walton‟s scheme is that there is a chance of exchanging the blocks in two different authenticated images with the same location without disturbing the checksum of the image. Fridrich et al. [5] analyzed the security problems in the scheme proposed by Yeung and Mintzer [4] and proposed a improved scheme with localization capacity, where a block cipher defined on a local region rather than on a single pixel is used to change the binary look-up tables. Minter [4] proposed a image authentication based watermarking. They use a pseudo random sequence and a modified error diffusion method to embed a binary watermark into an image, so that any alteration in pixel values of the image can be detected. Hence, attacker could not deduce the binary look-up table. Simultaneously, authors embedded an image index into all non-overlapping sub-blocks of each image to avoid the collage attack proposed in [6, 7].

Wong [8] proposed an image authentication scheme for Public key fragile watermarking. He separated the image into non- overlapping blocks and inserted a digital signature for authentication. In Wong scheme, using the seven most significant bits of the pixel a key is used to generate a signature sin each image block together with a logo to form a watermark, and embed the watermark into the least significant bits of the consequent blocks. The block wise independence of the authentication schemes, proposed in the literature was exploited by Holliman and [9]. They proved that vector quantization attack are vulnerable to these schemes. According to them, a imitation image can be constructed using a vector quantization codebook generated from a set of watermarked images. From the time when each block is authenticated by itself, the counterfeit image appears authentic to the watermarking scheme. A number of schemes has been proposed. to withstand the vector quantization attack, . [11] proposed a hierarchically structured watermarking scheme based on scheme [8] which provides a block wise authentication with highly overlapping blocks.Wong [10] proposed an improved block wise authentication scheme by adding an image index and a block index to the inputs of the hash function. However, this will works at the expense of requiring the verifier to have a priori knowledge about the image index, which limits its applicability to some extent. et al In et al.‟s scheme, the original image is partitioned into blocks in a multi-level hierarchy and then block

signatures in this hierarchy are calculated. Based on this hierarchy structure, the scheme can effectively thwart vector quantization attack.

Chang et al. [13] proposed a block- based image authentication scheme which can withstand counterfeiting attacks by combining the local and global features to obtain the authentication data. Chen et al. Suthaharan[12] proposed a fragile watermarking scheme in which the security against vector quantization attack is achieved using a gradient image and its bits distribution properties to generate large key space. A disordered image pattern is generated by using logistic map. A jumbled watermark is obtained by using exclusive-or (XOR) operation between chaotic image pattern obtained by using logistic map and the binary watermark. The scrambled watermark is then embedded in the least significant bit (LSB) plane of the image. In our scheme, we compare the clustering values of the original and tamper watermarked images. We detect any modification is made to image and also indicate specific location that have been modified.

[14] proposed a fuzzy c-means clustering based watermarking scheme to resist counter feting attacks. To break the block wise independency,they applied the fuzzy c means clustering technique to cluster all the image blocks, so that the relationship between blocks can be created. The authentication data is embedded into two least significant bits of each image block. The major drawback of fuzzy c-means clustering based scheme is that they use too many extra information including weighting exponent, clustering centers, secret key. Raman proposed [15], a novel watermarking scheme based on chaotic maps is proposed. The pixels of the cover image are disturbed with the help of Arnold‟s cat map. The image is further divided into 8-bitplanes and the least significant bit (LSB) plane is used for watermark embedding. A binary logo is used as watermark in our scheme.

III. K-Means Algorithm

In data mining and image processing the digital watermarking the K- means algorithm has a growing impact .It is an evolutionary algorithm that gains its name from its method of operation. The algorithm group the observations into k groups, where k is provided as an input parameter. Based upon the observation‟s proximity to the mean of the cluster it assigns each observation to clusters. The process begins again by recompute cluster‟s mean. Here is how the algorithm works:

1. The algorithm randomly selects k points as mean of the preliminary cluster centers .
2. Each spot in the dataset is assigned to the closed cluster, based upon the Euclidean distance between each point and each cluster center.
3. Each cluster center is recalculated as the average of the points in that cluster.
4. Continue the Steps 2 and 3 until the clusters congregate. Convergence may be defined differently depending upon the performance, but it normally means that either no interpretation change clusters when steps 2 and 3 are repeated or that the changes do not make a material difference in the definition of the clusters. We form two clustering values for each layer of RGB image in our watermarking algorithm.

IV. Proposed Scheme

In this section, we explain the proposed k - mean clustering based water marking scheme. The system contain two procedures such as water mark embedding procedure and tamper detection procedure.

A. Watermark Embedding

1. Assume that I is the original image(color image) of size MxN and the watermark image(color image) of size mxn is marked as W
2. The I image is divided into blocks and converted into 8-bit planes.
3. Each block has 8 bit planes of original image.
4. To get a watermarked image *I* replace the least significant bit plane of I by W & Apply K-means clustering to the LSB bits of watermarked image *I*. In this method we take a true color image of red, green, blue and converted into grays scale form.
5. With the help of K- means clustering compute the number of 1‟s and number of 0‟s in each layer separately , which form a six clusters for the above mentioned three layers. These cluster value is used as a secret key in our scheme.

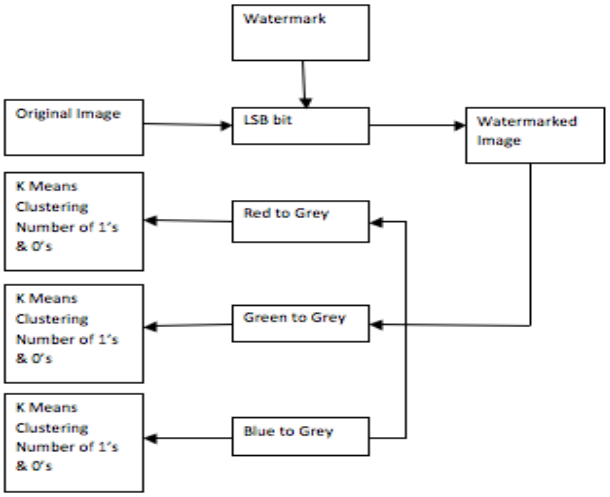

Fig.1.Block diagram of embedding process.

B. Tamper Detection

1. The tamper watermarked image is divided into blocks.
2. Each block in the image is separated into 8 bit planes.
3. Apply K-means clustering to the LSB bits of the tamper watermarked image. Image of the three layers in LSB bits of the watermarked image is converted into gray scale form seperately.
4. With the help of K-means clustering compute the number of 1"s and number of 0"s in the gray scale of each layer of the tamper watermarked image.
5. Take the original watermarked image *I'*.Obtain the same K- means clusters of image *I'* as in step 6 of embedding algorithm.
6. Then locate the tampered areas of the watermarked image by comparing the clustering values of the tamper watermarked image *I"* and original watermarked image *I'*.

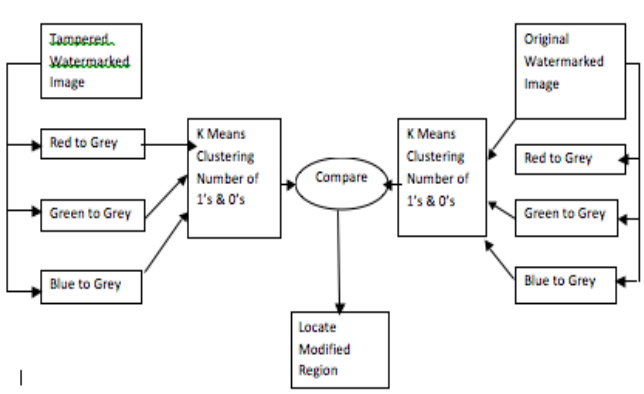

Fig.2.Block diagram of tamper detection process.

V. EXPERIMENTAL RESULTS

To evaluate the performance of the proposed algorithm. various experiments are carried out in this section. A boy image is used as watermark in all the experiments. The K-means algorithm used in our scheme is using the parameter value as K=6. To analyze the visual quality of the watermarked image *I'* in comparison with the original image I, PSNR (peak signal-to- noise ratio), is used in this paper

$$\text{PSNR} = 10log_{10}\left(\frac{255^2}{\text{MSE}}\right)dB$$

where MSE is the mean squared error between the original image

$$\text{MSE} = \frac{1}{\text{MN}}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}[I(i,j) - I'(i,j)]^2$$

A. Performance Evaluation

1. Copy and paste attack Performance:

Fig. 3. (a) Host image, (b) Watermark imageand (c) watermarked image.

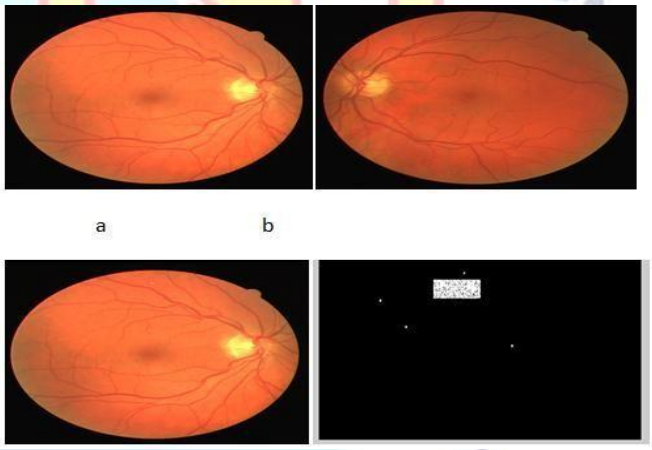

Fig.4. (a) Original image, (b) watermarked image, (c) tampered image, (d) detected tampered region

In this trial, host image is used as a " retinal funds" image and a watermark is used as a "Boy" image. Fig. 3 shows the host image, watermark image and corresponding watermarked image. One kind of copy and paste attack is performed in our scheme. The PSNR value of watermarked image is 51.7363 dB. The retinal image is modified by adding distortion in the image. The tamper image is shown in Fig.4(c). The tamper detection result is shown in Fig. 4(d).

2. Text addition Performance: In this experiment, the watermarked image, shown in Fig. 5(b) is modified by adding the text "FRUITS" at the bottom

of the image. Fig shows the tampered image. Detected tamper region is shown in Fig. 5(d).

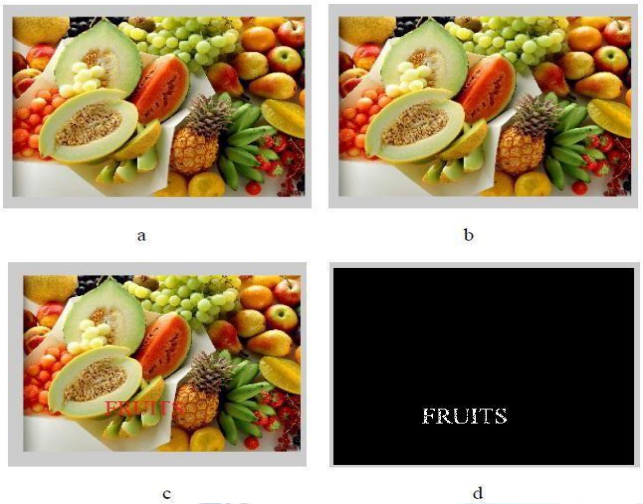

Fig.5. (a) Original Tropical Fruits image, (b)watermarked image, (c) tampered image, (d) detected tampered region

3. Collage attack Performance: To evaluate the performance under collage attack, a counterfeit image is formed by combining the portions of multiple watermarked image while preserving their relative spatial locations within the target image. We have performed this attack for two set of images. The simulation results are shown in Fig.6.*Harbor ships and aero plane:* The original harbor ships and aero plane images are shown in Fig.6 (a) and (b). The corresponding watermarked images are shown in Fig. 6(c) and (d), where the PSNR values are 52.1552 and52.0992 dB, respectively. The counterfeit image, as shown in Fig. 6(e) was constructed by copying the aero plane from Fig. 6(d) and pasting it in Fig. 6(c).

Fig. 6.(a) Original harbor ships, *(b) original aero plane, (c) watermarked harbor ship image, (d) watermarked aero plane image, (e) tampered harbor ship image, (f) detected tampered region*

VI. Conclusion

In this paper, for image tamper detection we proposed a K-means clustering watermarking scheme. In this process, it is easy to embed a watermark in a digital image and in the extraction phase it does not require the original image for reference purpose. This watermarking scheme is used to reduce time complexity when compared with the existing methods like fuzzy based tamper detection .The main application of the above scheme is widely used in court evidence. Also to identify the difference between the original image & the tampered image the count of RGB is used. Though time complexity is reduced, security is one of the important concerns which is yet to be fulfilled. Experimental results show that this scheme has high fidelity and is capable of localizing modified regions in watermarked image. Future work will be done to enhance the security issues.

References

[1] Walton. S, Information authentication for a slippery new age, *Dr Dobb's Journal,* 20(4), 1995, pp.18–26. Watermarking for Image Authentication and Recovery, *IEEE Transaction*, 2010.

[2] Rawat. S and Raman. B, A chaotic system based fragile watermarking approach for image tamper detection, *International Journal of Electronics and Communications (AE)*, 16, 2011, pp.1-8.

[3] Yeung. M and Mintzer. F, An invisible watermarking technique for image verification, *Proceedings of IEEE International Conference on Image Processing*, 1997, pp.680–683. *ce, Engineering & Technology, 1 (1), 2015, 23-27*

[4] Memon. N, Shende. S, Wong. P, On the security of the Yeung–Mintzer authentication

watermark, *Proceedings of the IS&T PICS symposium*, 1999, pp.301–306.

[5] Fridrich. J, Goljan. M, Memon. N, Further attacks on Yeung–Mintzer watermarking scheme, *Proceedings of SPIE electronic imaging*, 3971, 2000, pp.428–37.

[6] Fridrich. J, Goljan. M, Baldoza. A.C, New fragile authentication watermark forimages, *Proceeding of IEEE International Conference on Image Processing*, 1,2000, pp.446–9.

[7] Wong P.W, A public Key watermark for image verification and authentication, *Proceedings of IEEE International Conference on Image Processing*, 1998, pp.4559.

[8] Holliman. M, Memon. N, Counterfeiting attacks on oblivious block-wise independent invisible watermarking schemes, *IEEE Transactions on Image Processing*, 9(3), 2000, pp.432–441.

[9] Wong. P.W, Memon. N, Secret and public key image watermarking schemes for image authentication and ownership verification, *IEEE Transactions on Image Processing*, 10 (10), pp.1593–1601.

[10] Celik. M.U, Sharma. G, Saber. E, Tekalp. A.M, Hierarchical watermarking for secure image authentication with localization, *IEEE Transactions on Image Processing*, 11(6), 2002, pp.585–595.

[11] Suthaharan. S, Fragile image watermarking using a gradient image for improved localization and security, *Pattern Recognition Letters*, 25(16), 2004, pp.1893– 1903.

[12] Chang. C.C, Hu. Y.S, Lu. T.C, A watermarking-based image ownership andtampering authentication scheme, *Pattern Recognition Letters*, 2006.

[13] Chen. W.C, Wang. M.S, A fuzzy c-means clustering- based fragile watermarking scheme for image authentication, *Expert Systems with Applications*, 2009.