INTERNATIONAL RESEARCH JOURNAL IN ADVANCED ENGINEERING AND TECHNOLOGY (IRJAET) www.irjaet.com

ISSN (PRINT) : 2454-4744 | ISSN (ONLINE): 2454-4752

Vol. 1, Issue 4, pp.235 - 239, November, 2015

DATA HIDING AND RETRIEVAL IN DATA CLUSTERING IN IMAGE WITH NOISE DISCRIMINATION

K.Jancirani[1] | M.Vijayasuresh[2]

PG student, Bharathidasan Engineering college, Natrampalli

Asst professor, Bharathidasan Engineering college, Natrampalli

ARTICLE INFO

Article History:

Received 21st Nov, 2015

Received in revised form 23rd Nov,2015

Accepted 25th Nov, 2015

Published online 29th Nov, 2015

Keywords:

Digital watermarking, k- means clustering, Tamper detection

ABSTRACT

In this paper, we focus K-mean clustering based fragile watermarking scheme for image authentication and tamper detection. Tamper detection and localization accuracy are two important aspects of the authentication watermarking scheme. . The image retrieval is an interesting and rapidly growing methodology in all fields. It is an effective and well organized approach for retrieving the image. Clustering values of the watermarked image used as the secret key in our scheme. It can detect any modification is made to image and also indicate the specific location that have been modified. Important aspect of the schemes are time complexity reduction and PSNR value improvement, with stand attacks. It does not require original image for verification.

1. INTRODUCTION

As computer technologies become worldwide, besides numerical and categorical data, various digitalized images, sounds, voices, and videos have become part of daily life. Plenty of knowledge can be hidden in these data, it is since1970th people devoted themselves into image retrieval research, and then text based image retrieval technology and context web retrieval technology were proposed, which in a certain extent solved some image retrieval and resource discovery problems. With the fast development of Internet, digital images are used as evidences in the news and court reports in digital media. However, using powerful image processing software tools, digital images can be simply modified without any limit. Generally these modified 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.

Digital watermarking is a technology for embedding digital data in digital content (audio, images, video…). It has introduced as a tool to increase the security. Watermarking techniques are classified as follows: Spatial Domain: The watermarking system directly alters the main data elements (like pixels in an image) to hide the watermark data. Frequency Domain: The watermarking system alters the frequency transforms of data elements to hide the watermark data. 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 manipulation 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. In this paper we propose K-mean clustering based watermarking technique. The K-mean clustering algorithm is applied to the watermarked image to calculate the number of one's and number of zero'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 suitable for transmission in open network as Internet and location of the tempered area accurately. The performance evaluation shows that our proposed scheme can provide less computational complexity and better security than the traditional watermarking based tamper detection schemes.

2. K-MEANS ALGORITHM

The K- means algorithm have been found to be extremely useful in digital watermarking. It has a growing impact in data mining and image processing .It is an evolutionary algorithm that gains its name from its method of operation. The algorithm clusters observations into k groups, where k is provided as an input parameter. It then assigns each observation to clusters based upon the observation's proximity to the mean of the cluster. The cluster's mean is then recomputed and the process begins again. Here's how the algorithm works:

1. The algorithm arbitrarily selects k points as the initial cluster centers ("means").
2. Each point 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 recomputed as the average of the points in that cluster.
4. Steps 2 and 3 repeat until the clusters converge. Convergence may be defined differently depending upon the implementation, but it normally means that either no observations 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.

In our watermarking algorithm, we form two clustering values for each layer of RGB image.

3. PROPOSED SCHEME

In this section, we explain the proposed k-mean clustering based watermarking scheme. The system contains two procedures: watermark embedding procedure and tamper detection procedure.

A. Watermark Embedding

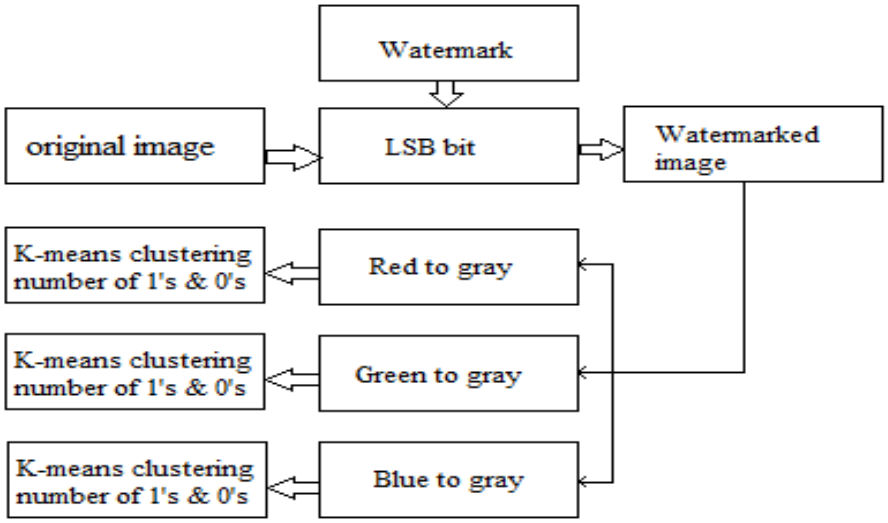

Fig.1.Block diagram of embedding process.

1. Let us consider, I is the original image(color image) of size MxN, W is the watermark image(color image) of size mxn.
2. The original image I is divided into blocks. Each blocks converted into 8-bit planes.
3. Each block in original image is converted into 8 bit planes.
4. Replace the least significant bit plane of I by W to get a watermarked imageI'.
5. Apply K-means clustering to the LSB bits of watermarked image I'.In this scheme we take a true color image, it has three layer such as red, green, blue. These layers are converted into grays scale form.
6. Calculate the number of 1's and number of 0's in each layer separately with the help of K- means clustering, which form a six clusters for three layer. These cluster value is used as a secret key in our scheme.

B. Tamper Detection

1. Take the tamper watermarked image I''. The tamper image is divided into blocks.
2. Each block in the image is divided into 8 bit planes.
3. Apply K-means clustering to the LSB bits of the tamper watermarked image.Image I'' of the red ,green and blue layer in LSB bits of the watermarked image is converted into gray scale form seperately.
4. Calulate the number of 1's and number of 0's in the gray scale of each layer of the tamper watermarked image with the help of K-means clustering.
5. Take the original watermarked image I'.Obtain same the K- means clusters of image I' as in step 6 of embedding algorithm.
6. Compare the clustering values of the tamper watermarked image $I''$and original watermarked imageI',thenlocate the tampered areas of the watermarked image.

4. EXPRIMENTAL RESULTS

A. Performance under copy and paste attack

Various experiments are carried out in this section, to assess the performance of the proposed algorithm. A boy image

is used as watermark in all the experiments. The parameters of K-means algorithm used in our scheme is K=6. PSNR (peak signal-to-noise ratio), is used in this paper to analyze the visual quality of the watermarked image I' in comparison with the original image I.

Fig. 2 .(a) Host image, (b) Watermark image and (c) watermarked image

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

where MSE is the mean squared error between the original image

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

B. Performance under text addition

In this experiment, the watermarked image, shown in Fig. 5(b) is modified by adding the text 'FRUITS' at the bottom of the image.

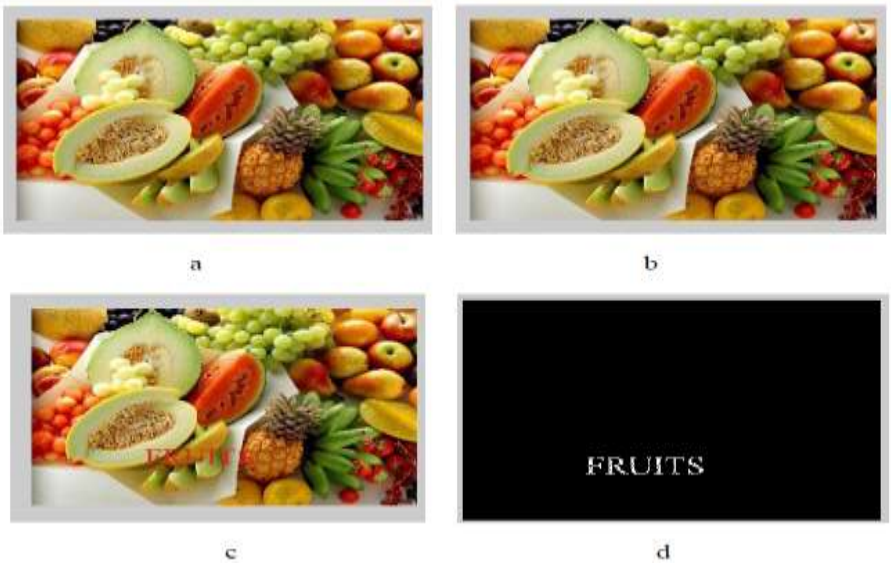

Fig.3. (a) Original Tropical Fruits image, (b) watermarked image, (c) tampered image, (d) detected tampered region

CONCLUSION

In this paper we proposed a K-means clustering watermarking scheme for image tamper detection In this paper we proposed 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 .The main application of the above scheme is widely used in court evidence. Also the count of RGB is used to identify the difference between the original image & the tampered image. Though time complexity is reduced, security is one of the important concerns which are yet to be fulfilled. Experimental results show that our scheme has high fidelity and is capable of localizing modified regions in water marked image. Future work will be done to enhance the security issues.

REFERENCES

1. Jose Antonio Mendoza-Noriega, Mariko Nakano-Miyatake.,"Halftoning-based Self-embedding Watermarking for Image Authentication and Recovery", IEEE Transaction 2010.
2. Rawat S., and Raman B., "A chaotic system based fragile watermarkingapproach for image tamper detection", International Journal of Electronicsand Communications (AE), vol. 16, pp. 1-8, 2011.
3. Walton S. "Information authentication for a slippery new age",Dr Dobb's Journal1995;20(4):18–26.
4. Yeung M, Mintzer F. "An invisible watermarking technique for image verification",In: Proceedings of IEEE international conference on image processing.1997. p. 680–3.
5. Fridrich J, Goljan M, Baldoza AC. "New fragile authentication watermark forimages",In: Proceeding of IEEE international conference on image processing,vol. 1. 2000. p. 446–9.
6. Memon N, Shende S, Wong P."On the security of the Yeung–Mintzer authentication watermark",In: Proceedings of the IS&T PICS symposium. 1999. p. 301–6.
7. Fridrich J, Goljan M, Memon N. "Further attacks on Yeung–Mintzer watermarking scheme", In: Proceedings of SPIE electronic imaging, vol. 3971. 2000. p.428–37.
8. Wong PW. "A public Key watermark for image verification and authentication", In: Proceedings of IEEE international conference on image processing. 1998. p.455–9.
9. Holliman M, Memon N." Counterfeiting attacks on oblivious block-wiseindependent invisible watermarking schemes", IEEE Transactions on Image Processing2000;9(3):432–41.
10. Wong PW, Memon N. "Secret and public key image watermarking schemes forimage authentication and ownership verification", IEEE Transactions on ImageProcessing 2001;10(10):1593–601.
11. Celik MU, Sharma G, Saber E, Tekalp AM. "Hierarchical watermarking for secure image authentication with localization", IEEE Transactions on Image Processing 2002;11(6):585–95.
12. Suthaharan S."Fragile image watermarking using a gradient image for improved localization and security".
13. Pattern Recognition Letters 2004;25(16):1893–903.Chang CC, Hu YS, Lu TC." A watermarking-based image ownership andtampering authentication scheme". Pattern Recognition Letters 2006.
14. Chen WC, Wang MS. A fuzzy c-means clustering-based fragile watermarking scheme for image authentication. Expert Systems with Applications 2009.