Review of Digital Watermarking and Different Methods for Temper Detection and Recovery

Rajneet Kaur, Er. Rana Gill

Chandigarh University of Engineering, Gharuan, Punjab, India

Abstract - In the aspect of tamper detection and recovery there are some methods to embed the feature information in host image for recovery. When the host image has been tampered with, the feature information can be used to restore the original image. However, it does not have the ability to describe the ownership of the copyright. In this article, an image watermarking scheme with tamper detection and recovery is proposed. The main goal is to detect and recover the tampered region accurately. And for this some basic methods have been discussed and properties of watermarking has also been discussed in this paper.

Keywords - *Digital Watermarking, Tamper Detection and Recovery.*

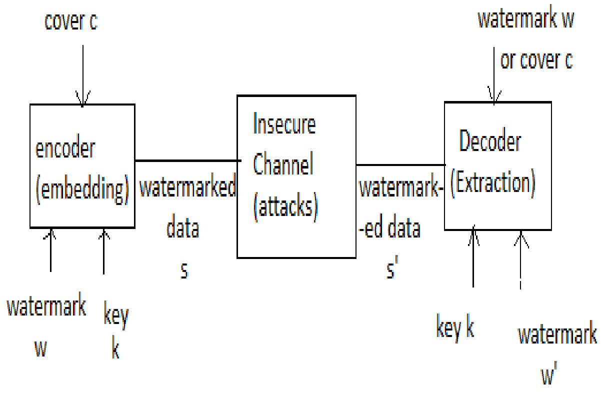
I. INTRODUCTION

With the use of multimedia data is being distributed over the internet. Someone download it, make some modifications and redistribute it as their own. In such kind of situation, digital watermarking technique can be used to prove ownership rights, verify authorized access, preventing illegal reapplication and enabling content authentication.

So digital watermarking is the process of embedding information into a digital carrier signal such that it becomes difficult to remove [9].And the signal may be audio, video or any image. Digital watermarking is used for various purposes such as copyright protection, proof of ownership, authentication, and content control [6]. The main requirements of digital watermarking is robustness and imperceptibility. It is hazardous to deliver the digital medium on public network because people can perfectly copy or tamper the media which leads to large illegal distribution of digital data [8]

II. WATERMARKING LIFE CYCLE

The authenticity represents that information in the signal has not been modified [3].The authenticity of images can be achieved by using such a watermarking method that has ability for image tamper proofing



Tamper proofing means to recover the tampered region which get affected or destroyed after attacks. For tamper proofing and authentication of the image, various watermarking methods were developed to recover the tempered region which has been discussed below.

III. PROPERTIES OF WATERMARKING

A. ROBUSTNESS

A robust watermarking is that which outlasts the common operations such as DAC, ADC, compression, rotation, resizing etc. In many application, robustness to all processing operations is unnecessary, watermark must survive common signal processing only between the time of embedding and extraction [10].

B. TAMPER RESISTANCE

Any watermarking algorithm is said to be tamper resistance if it is resistance to malicious attacks. Depending on the application, there are several types of attacks:-

1. ACTIVE ATTACK

In which attackers tries to detach the watermark or make it un-extractable. This is critical for some application like owner identification, copy control.

2. PASSIVE ATTACK

In which, attackers not trying to remove the watermark but simply trying to determine whether a watermark exist or not.

3. COLLISION ATTACKS

This is a special case of active attacks, in which attackers use several copies of one piece of media each with different watermark to build a copy with no watermark.

4. FORGERY ATTACKS

In which attackers tries to embed a valid watermark rather removing the already existed watermark.

C. FIDELITY

Fidelity means that the watermark embedded in an image must not be noticeable to the viewers and should maintain the quality of content [7].

D. COMPUTATIONAL COST

Different application requires different number of embedders and detectors like broadcast monitoring application requires a few embedders but several decoders at different locations and copy control application may need few embedders but several of detectors. So, the computing cost depends on the application.

E. FALSE POSITIVE RATE

It is a detection of watermark in a piece of media which actually does not contain that watermark.

IV. DIFFERENT METHODS TO RECOVER/ DETECTION OF TAMPERED REGION

A. Moment Preserving Techniques

Moment preserving technique is a image thresh holding method which arrange the pixels of a image into many groups and each group assigned with a gray values [1] so that moment of thresholded image can be preserved. In this technique there are 2 types of methods:-

1. Multi-level thresholding method

In which various thresholds are used to classify the pixels into several range of grey values.

2. Bi-level thresholding methods

In which one threshold is used to classify the pixels with grey values above the threshold and pixels with grey value equal to or below the threshold. In bi-level moment preserving technique, moment of an input image is computed as [6]:

$$m_b = \frac{\sum_{i=1}^{N} G^b(i)}{N}$$

Where b=order of the moment
G (I) = grey value of the pixel i
N = total number of pixels in the image G, or we can write it as:-

$$m_b = \sum_k p_k\,(g_k)^b, k = 1,2,3..$$

where p_k is the number of fractions.

B. ENTROPY METHOD

Entropy is a statistical measure of randomness that can be used to signalize the texture of the input image [2,4].

E=-Sum (p.*log2(p))

where P contains the histogram counts.

STEPS OF ENTROPY METHOD

- Convert the color image into grey
- Break the image into blocks
- Find entropy for each block and find the threshold value.
- Select the entropy blocks with higher entropy value than threshold value.
- Embed watermark.
- Re arrange the blocks.

C. HYBRID WATERMARK

It is a mixture of fragile and robust watermark. The fragile watermark has good security properties but cannot distinguish malicious changes such as feature adding or removal [11]. So, the hybrid watermark can be used which consist of 2 watermark pattern embedded in an image. First, the robust watermark is embedded and then the fragile watermark is embedded on the top of the robust one. Since the fragile watermark constitute a small distortion, the robust watermark should be affect only insignificantly.

D. TAMPER DETECTION USING RS CODE

The watermark used in this method consist of the check symbols of a Red-Solomon Code(RS Code).This method embeds the check symbols into the LSB of an image directly[5].

V. CONCLUSION

In this article, tamper detection and recovery of an image has been discussed. For Tamper detection and recovery different methods have been listed which helps for further research. Along with the methods properties of watermarking has been also written in this article.

VI. REFERENCES

[1] Liu, Kuo-Cheng. "Self-embedding watermarking scheme for colour images by bi-level moment-preserving technique." IET Image Processing 8.6 (2014): 363-372.

[2] Idrissi, Nadia, and Ahmed Roukhe. "Robust watermarking method based on contourlet transform, maximum entropy, and SVD decomposition."Multimedia Computing and Systems (ICMCS), 2014 International Conference on. IEEE, 2014

[3] Liu, K-C. "Colour image watermarking for tamper proofing and pattern-based recovery." Image Processing, IET 6.5 (2012): 445-454.

[4] Franklin, Rajkumar V., Manekandan GRS, and V. Santhi. "Entropy based robust watermarking scheme using Hadamard transformation technique."International Journal of Computer Applications 12.9 (2011): 14-21.

[5] Iwata, Motoi, et al. "Digital watermarking method for tamper detection and recovery of JPEG images." Information Theory and its Applications (ISITA), 2010 International Symposium on. IEEE, 2010:309-314.

[6] Mehdi Boroumand and Afshin Ebrahimi "An Improved Quantization Based Watermarking Scheme Using Local Entropy in Wavelet Domain”. Proceeding of International Conference on Signal and Image Processing Applications IEEE:2009:268-272.

[7] Ghazy , R. A., et al. "An efficient block-by block SVD-based image watermarking scheme." Radio Science Conference, 2007. NRSC 2007. National. IEEE, 2007:1-9.

[8] Lin, Shinfeng D., Yu-Chan Kuo, and Yu-Hsun Huang. "An image watermarking scheme with tamper detection and recovery." Innovative Computing, Information and Control, 2006. ICICIC'06. First International Conference on. Vol. 3. IEEE, 2006.

[9] Liu, Jian, and Xiangjian He. "A review study on digital watermarking."Information and Communication Technologies, 2005. ICICT 2005. First International Conference on. IEEE, 2005:337-341.

[10] Cox, Ingemar J., Matt L. Miller, and Jeffrey A. Bloom. "Watermarking applications and their properties." Information Technology: Coding and Computing, International Conference on. IEEE Computer Society, 2000.

[11] Fridrich, Jiri. "A hybrid watermark for tamper detection in digital images."Signal Processing and Its Applications, 1999. ISSPA'99. Proceedings of the Fifth International Symposium on. Vol. 1. IEEE, 1999.