

Tampering Detection Algorithms: A Comparative Study

Suresh Gulivindala¹, Ch.Srinivasa Rao²

¹Asst.Prof, Dept of ECE, GMR Institute of Technology, Rajam, A.P. INDIA.

²Professor & Head, Dept of ECE, JNTUK University College of Engineering, Vizianagaram, A.P. INDIA.

Abstract:- The reprehensible use of technology such as powerful editing software and sophisticated digital cameras leads to image tampering or manipulation. The tampered data is being illegally used and distributed through high-speed digital networks. Hence techniques to solve the problem of unauthorized copying, tampering, and multimedia data delivery through the internet are very much in demand. Information hiding, is the key issue, consists mainly of steganography and digital watermarking. Development of image tampering detection algorithms in active and passive methods became a significant research work. In this paper, comparative analysis on the performance of two algorithms such as 3LSB and DWT was reported. These two algorithms are designed in active method i.e. it uses digital watermarking in the background. Any tampering/modification on the watermarked image results in the change in the intensity levels, so in turn the coefficient values. The extraction procedure results in the watermark whose bit value reflects the respective changes. The 3LSB method proves to be superior to DWT method in terms of detection and localization.

Keywords:- Image Tampering, 3LSB method, DWT, Authentication, Image Forgery

I. INTRODUCTION

Sophisticated digital cameras and advanced photo-editing tools help in creating good quality images and on the other hand digital image forgeries. Further, the high-speed digital networks are the backbone of illegal distribution and manipulation. There is no scope to trust image media since (maliciously) tampered images are often found in the Internet even published in newspapers. If we take this issue for granted, it may eventually be harmful for our digital world, especially for the credibility of news coverage. Many researchers have worked on image forensics and a number of image tampering detection techniques have been proposed in recent years [1-12]. Generally speaking, there are two types of approaches of image tampering detection: active and passive approaches. Passive approaches [3] do not require extra information and they can be considered blind with respect to the original image. These approaches rely on the extraction of some features from the image under test and, based on pre-defined rule or statistical thresholds, make a decision. Unlike the watermark and signature-based methods, the passive technology does not need any digital signature to be generated or to embed any watermark in advance. Block matching techniques are employed in passive technology for detecting the forged regions. Active systems [3] are based on watermarking methodologies for tampering detection. They are based on the insertion of some features extracted from the image into the image itself. During the authentication control, the detection of modification in the hidden data can be used for assessing modification of the original image. In active approach, the digital image requires pre-processing of image such as watermark embedding or signature generation, which would limit their application in practice. In this paper, comparative analysis on the performance of two algorithms such as 3LSB and DWT was reported.

II. DISCRETE WAVELET TRANSFORM

The 2-D Discrete Wavelet Transform is used to provide multiresolution representation of the original image [4]. By applying 2-D DWT [5-7] on an image, obtained coefficients can be classified into 4 types and shown in Fig.1: 1.HH Coefficients: Obtained by high-pass filtering in both directions (represent the diagonal features), 2.HL Coefficients: Obtained by high-pass filtering of the columns followed by low-pass filtering of the rows (represent the horizontal structures), 3. LH Coefficients: Obtained by low-pass filtering of the columns followed by high-pass filtering of the rows (represent the vertical structures) and 4.LL Coefficients: Obtained by low-pass filtering in both directions (represents approximation image).

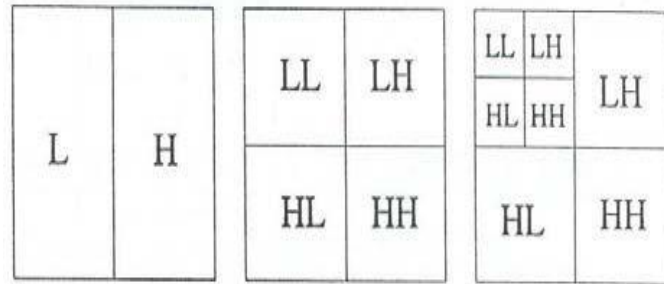


Fig.1 Representation of 2-D Wavelet Transform at different levels.

A. DWT METHOD

Image Tamper Identification Procedure consists of i) watermark embedding and ii) watermark extraction.

The embedding process can be described as follows:

- 1: Apply 1-Level DWT on an $N*N$ cover image.
- 2: Divide the binary watermark into non-overlapping blocks of size $2*2$.
- 3: Divide the HL sub band into non-overlapping blocks of size $4*4$ and embed four watermark bits into the LSBs of the four coefficients in the reverse diagonal of each block, as shown in Fig.2.
4. Perform IDWT on the embedded image to obtain an image.

The tampered watermarked image is processed to extract the binary watermark and is as follows:

- 1: Apply 1-Level DWT on an $N*N$ tampered watermarked image.
- 2: Divide the HL sub-band into non-overlapping blocks of size $4*4$ and extract four watermark bits from the LSBs of the four coefficients in the reverse diagonal of each block.
- 3: Construct the actual binary watermark image.

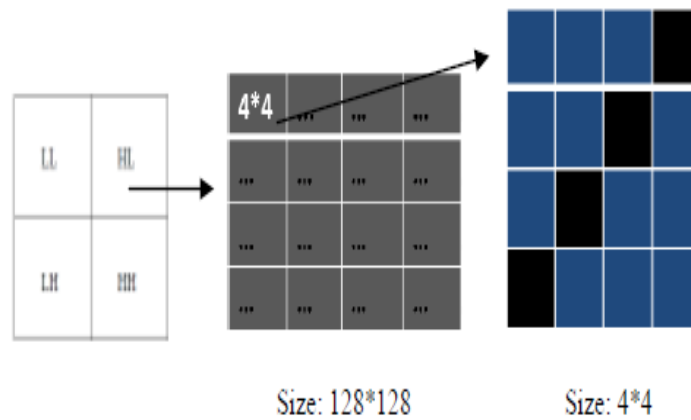


Fig.2 Partitioning of DWT HL Coefficients into 4x4 blocks

III. 3LSB METHOD

Here 3 LSB Method [10] proposed by Sajjad Dadkhah et al. is considered and is given in Section III. Fig.3 illustrates dividing the image into $2*2$ blocks and generating a 12-bit watermark for embedding into last three significant bits of each block. The watermark content which has 12-bit size have to be something that relate to each pixel of the block so in case of tampering in one of the pixels, this method can detect and localize the tampered blocks. In order to generate the 12bit watermark, first of all divide the cover image into non overlapping $2*2$ blocks, the first 10bits are obtained by taking 5MSB's of the 1st and 2nd pixel values of the block. The remaining two bits are odd &even parities of the 10bits. The 12-bit watermark will be embedded into 3LSB of each pixel of the block as shown in Fig.4. Now the watermarked image has generated. If the image is tampered, that is identified by using watermark extraction process. In this by comparing the 12 bit watermark of tampered image and 12 bit watermark of original cover image we got the tampering locations.

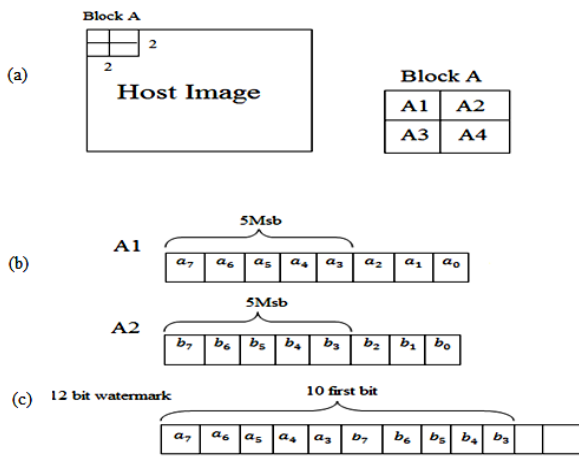


Fig.3 Generation of 12-Bit Watermark

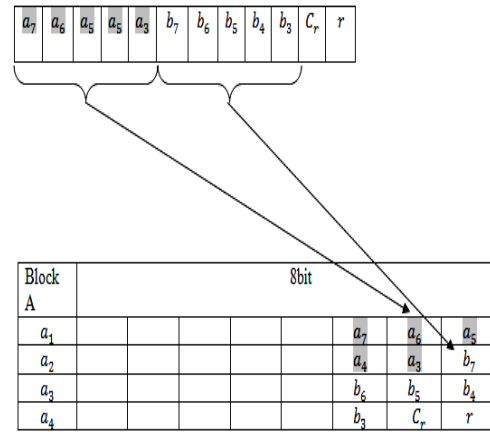


Fig.4 Embedding 12-bit watermark into 3LSBs

A. 3-LSB EMBEDDING ALGORITHM

- 1: Consider a cover image of size 512*512 and partition the image into 2*2 blocks. Each block contains four elements (A1, A2, A3, and A4).
- 2: Consider the first 5MSB's of the elements A1, A2 (10bits).
- 3: To obtain the 12bit watermark we consider the last two digits as odd & even parity of 10bits.
Even parity r=0 Cr=1
Odd parity r=1 Cr=0
- 4: Divide the 12bits into 4parts and replace each part in 3LSB's of the block Elements (A1, A2, A3, and A4).
- 5: Apply this procedure to all blocks of the image; the resultant image is watermarked image.

B. 3-LSB EXTRACTION ALGORITHM

- 1: Consider watermarked image and cover image & divide each image into 2*2 blocks.
- 2: Extract the 3LSB's of the block elements of the watermarked image.
- 3: Extract the 12bit watermark by taking 5MSB's of first two elements of 2*2 block of cover image and remaining 2bits are even and odd parities.
- 4: Compare 12bit watermarks of cover image and watermarked image, if those are not equal then we can say that there is a tamper.

C. 2-LEVEL TAMPER DETECTION ALGORITHM

If watermarked image is tampered, 2-level tamper detection is used to detect the tampering.

- 1: Consider tampered watermarked image and cover image & divide each image into 2*2 blocks.
- 2: Extract the 3LSB's of the block elements of the Tampered watermarked image.
- 3: Extract the 12bit watermark by taking 5MSB's of first two elements of 2*2 block of cover image and remaining 2bits are even and odd parities.
- 4: Compare 12bit watermarks of cover image and watermarked image, if those are not equal then we can say that there is a tamper.
- 5: If tampering is not detected in LSB's comparison go to next step.
- 6: Compare 5MSB's of each element in cover image with tampered watermarked image. If they are not equal then tampering is done in the MSB's of the watermarked image. This method is called 2-level tamper detection.





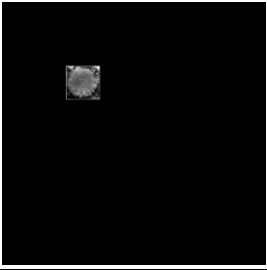


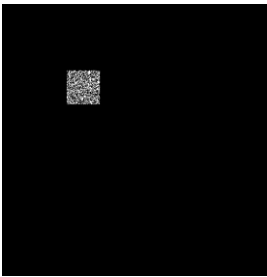





IV. RESULTS

The standard images Lena-512x512, Cameraman-256x256, are considered as Cover image and watermark respectively. The 3LSB Method does not require any watermark image separately; it generates the watermark from the cover image itself. The watermarked image is tampered with different attacks (copy-move forgery, deletion attack). The two detection algorithms are capable of tamper detection, its location and the number of pixels or blocks tampered. Here the two algorithms are compared in terms of tampered region and localisation. The results are tabulated in Table.1

V. CONCLUSION

Both the algorithms are capable of tamper detection and its localization as well gives the number of pixels that are being tampered. The experimental results demonstrate that 3-LSB method is superior to DWT based methods for collage type attacks. The 3-LSB method also detects exactly the image/portion which is being used to tamper the original. The 3-LSB method is basically a spatial approach but as the 12-bit watermark is self generated from the cover and embedded in the 2x2 blocks of the cover, the chances for intruder attacks are less.

Table I: Results of tampering algorithms

	Cover Image	Watermark	Watermarked Image	
				
	Tampered Watermarked Image	Extracted Watermark	Tamper Localisation	No. of Pixels Tampered
3 L S B		Self generating		4352
D W T				4347
3 L S B		Self generating		872
D W T				730

REFERENCES

- [1]. Hany farid, "Image Forgery Detection A Survey" IEEE Signal processing Magazine, March 2009, pp.16-25.
- [2]. D.Cozzolino, G.poggi, C.Sansone and Luisa Verdoliva, "A Comparative Analysis of Forgery Detection Algorithms" SSPR & SPR 2012, LNCS 7626, pp.693-700 2012.
- [3]. P.Deshpande, P.Kanikar, "Pixel Based Image Forgery Detection Techniques" International Journal of Engineering Research and Applications, VOL.2, Issue 3, May-June 2012, pp.539-543.
- [4]. R. Dugad, K. Ratakonda and N. Ahuja, A new wavelet-based scheme for watermarking images, Proc. IEEE Intl. Conf. on Image Processing, CIP'98, Chicago, IL, USA, Oct. 1998, 419-423.
- [5]. M.E.Hajji, H.ouaha, K.Afdel, H.Douzi, "Multiple Watermark Authentication and Tamper Detection using Mixed Scales DWT", International Journal of Computer Applications, Vol.28, No.6, August-2011.
- [6]. Saiqa Khan, Arun Kulkarni, "An Efficient Method for Detection of Copy-Move Forgery Using Discrete Wavelet Transform" International Journal on Computer Science and Engineering, Vol.2, No.5, 20120, 1801-1806.
- [7]. Yanjun Cao, T.Gao, Qunting Yang "A robust detection algorithm for copy-move forgery in digital images" Forensic International 214 (2012) 33-43.
- [8]. Anil Dada Warbhe, R.V.Dharaskar, "Blind Method for Image forgery detection: A tool for digital image forensics" NCIPET-2012, Proceedings published by International Journal of Computer Applications.
- [9]. Shuiming Ye, Qibin Sun and Ee-Chien Chang, "Detecting Digital Image Forgeries by Measuring Inconsistencies of Blocking Artifact", ICME 2007, pp.12-16.
- [10]. Sajjad Dadkhah, Azizah Abd Manaf and Somayeh Sadeghi, "Efficient Digital Image Authentication and Tamper Localisation Using 3LSB Watermarking" International Journal of Computer Science Issues, Vol.9, Issue.1, No.2, January 2012.
- [11]. Granty R.E.J, Aditya T.S, Madhu S.S, "Survey on Passive methods of image tampering detection" INCOCCI, 2010, E-ISBN : 978-81-8371-369-6.
- [12]. Pin Zhang, Xiangwei Kong, "Detecting Image Tampering using Feature fusion", International Conference on Availability, Reliability and Security, 2009, pp.335-340.