Efficient Digital Image Authentication and Tamper Localization Technique Using 3Lsb Watermarking

Sajjad Dadkhah[1], Azizah Abd Manaf [2] and Somayeh Sadeghi[3]

[1,3] Faculty of Computer Science and Information System, University Technology Malaysia
54100 Kuala Lumpur, Malaysia

[2] Advanced Informatics School , University Technology Malaysia
54100 Kuala Lumpur, Malaysia

Abstract

The authentications of digital images have become the center of attentions for certain group of companies since the number of doctored images increased. Tampering the digital images in a way that it's impossible to be detected by naked eyes has become easier with development of image editing tools. Digital watermarking can preserve the authentication of digital images. In this paper we proposed an efficient image tamper detection method using 3 LSB (last significant bit) watermarking technique which is able to authenticate the digital image and detect the tamper locations accurately. In the proposed algorithm a 12-bit watermark key will be created from each block of host image which will be embed to last three significant bit of each block. Our proposed method improved tamper detection technique proposed by Prasad's in sense of tamper detection rate by 40 percent. The experimental result clearly proved the efficiency of our proposed method.

Keywords: *Image Authentication, Tamper Detection, 3Lsb watermarking, watermarking for tamper detection.*

1. Introduction

With tremendous growths of digital image technology, and low-cost distribution of digital image processing tools among professionals and armature users, preserving the authenticity and integrity of digital images became as a considerable aspect for several organizations [1, 2]. The best way to certify the integrity and authenticity of the digital image is by using digital watermarking. For any kind of watermarking to happen a digital signature will be created to be embedded into particular host image, there are two kind of digital signature visible and invisible. Visible watermarking usually use for the logo of the specific institute or some explanation message of the whole original image which can be a part of the image. Invisible digital signature or watermarked is hidden in original image [3]. The imperceptible watermarking or invisible watermarking has 3 categories which are fragile watermarking, semi-fragile and robust watermark. Fragile watermarking can be broken easily which means it's not totally immune from blind attacks. Fragile watermarking methods are very weak in functional sense. However because fragile watermarking is very sensitive to any kind of manipulation it can be very valuable for authentication purposes [4, 5]. Moreover Semi-fragile watermarking techniques are very suitable for tamper localization. This method of watermarking can be used to locate any alternation and extra modification that occurred inside an image [6]. Authentication or tamper detection for digital image is to perceive any sort of manipulation inside the particular image and distinguish the original image from the fake one [7, 8]. The digital watermarking can be divided into block-wise and pixel-wise techniques. Block-wise watermarking is dividing the host image into specified non overlapping blocks for the purpose of tamper detection [9].

Furthermore researchers started to pay more attention to digital watermarking area. Fridrich [10] proposed a fragile watermarking method which could protect against Vector Quantization attack (VQ attack). Quantization attack target independent block-wise approaches by using the host image information. Wong [11] proposed a public-key fragile watermark which divides the image into non-overlapping blocks, then embeds a digital signature into last significant bit of each block. Chang et al. [12] conducted series of attacks to examine a hierarchical digital watermarking method for image tamper detection proposed by Lin et al. [13]. The experimental result of

their scan illustrated that parity check and intensity-relation of the image blocks cannot help to detect all types of tampering attacks.

However Lee and Shinfeng [14] proposed a Dual watermarking method for image tamper detection and recovery that solved some basic problem like no second chance for watermarked information, in case watermarked information destroyed by tampering in. One year later Chaluvadi and Prasad [15] highlighted very important flaw in Lee and Shinfeng's method. They proved that lee and Shinfengs method cannot detect any tampering attacks in 5 MSB (most significant bit) of watermarked image.

To evaluate tamper detection method, various attacks can be performed. In order to achieve robustness, particular tamper detection methods have to be capable to detect collusion attacks [16]. Collusion attack can be deleting some portion of the watermark image or copy some part of the watermark image and paste it anywhere inside the same image. Performing bit tampering attack which is modifying a specific bit in specific position, can illustrate the consistency of any tamper detection. Tamper detection rate can be calculated in order to evaluate the capability of proposed authentication method. The tamper detection rate in our case is the number of tampered blocks detected by proposed method which will be explained in following sections.

The remaining of paper is organized as follows. An overall analysis of Chaluvadi and Prasad's dual tamper detection will be conducted in section 2. In section 3 the methodology of our proposed image authentication using 3 LSB) will be explained. Section 4 illustrated the examination result of the proposed method along with the comparison of result with two current methods. Finally we conclude our proposed method in section 5 and explain the contribution of proposed method.

2. Prasad's Tamper Detection Method

They used 3-level hierarchical tamper detection proposed by Lin [17] which is block-based tamper detection method. Their system has both tamper detection and recovery capability. The system starts with grayscale image with MxM size, where M assumed to be multiple of 2. First they divide the whole image to non-overlapping blocks of size 2x2. Their approaches consist of two parts, first embedding the watermark and second the 3-level tamper detection technique.

The watermarking approach starts with constructing a 12-bit watermark that is going to be embedded in last three significant bit of each block. Their method divides the image horizontally into two equal parts and select two blocks from same position. The 12-bit watermark is consisting of representative block information and average intensity of each block which is simply the average of 4 pixels inside each block. The last 2-bit of their watermark is the parity check of the average intensity which is number of one's inside the binary form of particular bit, if the number of ones were even the parity check value will be 0 and if the number of ones were odd the parity check will be 1.

$$r = \begin{cases} 0 & \text{if count is even} \\ 1 & \text{otherwise} \end{cases} \quad (1)$$

Their proposed method included a smoothing function which improve the quality of the watermark and recovered image. To evaluate their tamper detection, they have conducted two bit tampering attacks. We conducted exactly the same attacks as illustrated in [15] to be able to compare results. The experiment results are illustrated in section 4.

3. Proposed approach

The proposed algorithm of the system includes 3LSB watermarking which is same as [1] and proposed 2-level tamper detection method. The overall procedure of the proposed system is illustrated in Fig. 2.

However as figure 1 illustrated after dividing the image into blocks of 2x2 and generating the 12-bit watermark, the 12-bit watermark will be embedded into 3LSB of each block. The proposed tamper detection method is consist of two parts which both are the comparison of the content of the 12-bit that has been watermarked to host image .In the first level the average intensity bits will be compared which is the last 2 bits of the 12-bit, second level is the comparison of the remaining 10 bit which all has to be identical otherwise tampered has happened. The 2-Level of our tamper detection method will make sure of the efficiency and accuracy of tamper detection and localization. The procedure of proposed 3LSB watermarking and 2-Level tamper detection will be explained in section A and B.

2.1 Watermarking Procedure

In this phase, we identified and generated a 12-bit watermark for embedding into last three significant bit 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, our method can detect and localize the tampered blocks. The first step in watermarking procedure is constructing the 12-bit watermark. The procedure of constructing the 12-bit watermark for our proposed system is same as [15] in primary steps but the contents of the watermark is different, which improved the tamper detection rate as illustrated in experiment results.

First we pad the 3 last significant bit of each pixel to zero. It will produce a new value obviously, thus we calculate the average intensity of the new value which is simply the average of the 4 pixels inside the block followed by calculating the parity check with (1).

So far, one bit of 12-bits has been generated and 11 bits remain. The main purpose of generating these 12-bits watermark is to make a digital signature for each block of size 2x2. Thus for generating the 12-bit watermark as figure 2 illustrated the 5MSB (most significant bit) of watermark is 5MSBof the first pixel inside the block and the second 5MSB is selected from the second pixel of the block.

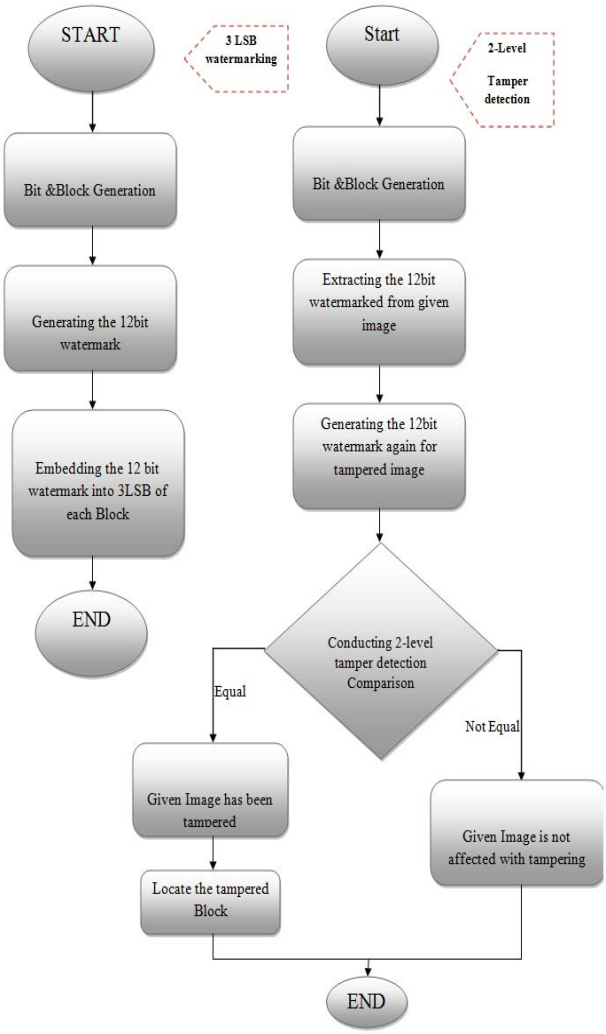


Fig. 1 General Structure of Proposed algorithm

After generating the 11 bits of watermark the best constant value that can be useful for tamper detection is parity check of the 10-bit that we just constructed in the previous section. As illustrated in figure 2 the parity check of the 10 bit calculated by (1) name as Cr. The last bit of the watermark is r which is the parity check of average intensity of the whole block.

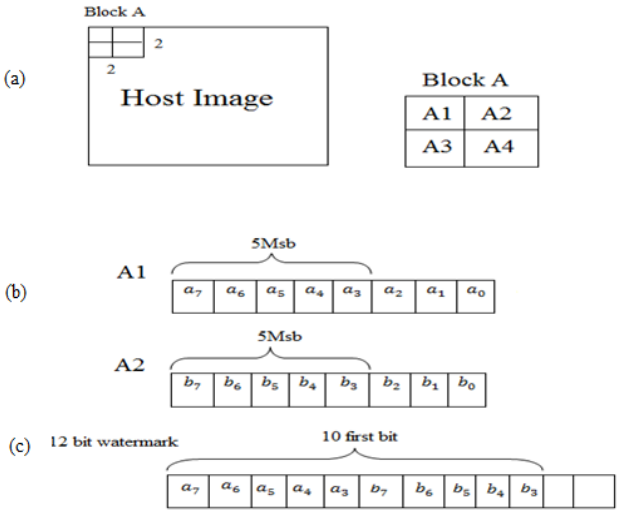


Fig. 2 Generation 10 MSB of watermark :(a)the block of size 2x2, (b) 5MSB of the first and second pixel of the block, (c) 10 bit of 12-bit watermark

As illustrated in figure 3 the first 5 bit of 12-bit of watermark will be embed to first two pixels inside each block, and the next 5 bit of watermark will be embedded into pixel three and pixel four. The last 2 significant bit of the watermark pixel will be embedded to 2nd LSB of the pixel number four inside each block. This embedding will be done for entire blocks inside the host image.

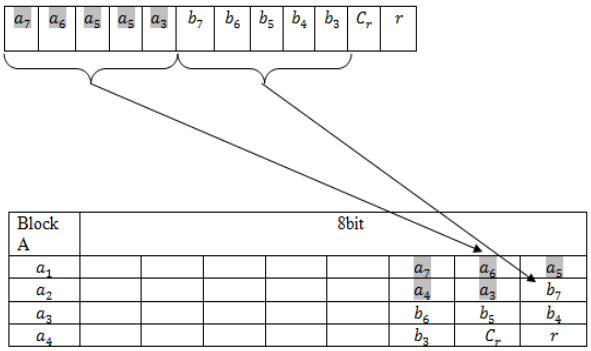


Fig. 3 Proposed watermarking process

2.2 Proposed Authentication Procedure

As figure 1 illustrated, the main concept of proposed tamper detection method is two important comparisons. So two level of tamper detection will be perform. If the tampered is not detected in fist level of tamper detection, the second level makes sure to detect the tampered blocks. After dividing the watermarked image to blocks of size 2x2, the last three significant bit of each pixel within the image will be padded to zero. The average intensity and parity check of new pixel value will be calculated and will be compared to last significant bit of the extracted watermark. This comparison will be done for each block of size 2x2 separately if the both value were equal then there has not been any tamper occurrence inside the image otherwise the tamper has happened and the method will mark that block as invalid to localize the tampered area. The first level of our tamper detection technique continues with calculating the parity check of the first 10 bits of the extracted watermark and compares the value to the second LSB of the same extracted watermark, If both values were equal to each other no tamper has happened, otherwise the block that method is doing comparison concurrently will be marked as invalid for purpose of tamper localization.
The efficiency of proposed tamper detection method will be guarantee with second level of tamper detection technique. After the first level if the method detects any tamper it would mark the tampered block as invalid and go on to second level. In this level a bit by bit comparison will be conduct between the 5MSB of the first two pixels and first 10 bit of the extracted watermark as illustrated in figure 1.

3. Experimental result

The first tampering attack that will be performed on proposed system is one type of collage attack. The collage attack that is going to be performed is made by copying one region from the watermarked image and pasting the region somewhere inside the same watermarked image. The second type of tampering attack is deletion attack which is simply deleting some part of watermarked image, however this attack will be performed in different scales to evaluate the proposed system ability in detecting the tampered areas.
The next tampering attack that is going to be performed is tampering with watermarked pixels bits. In order to compare the result of proposed system with recent tamper detection methods, attacks that are going to be perform in this phase of system, have to be same attacks as conducted in Chaluvadi and Prasad's tamper detection method [15]. The gray scale Lena image with size of 256x256 will be used for this experiment. According to size of testing image, total number of blocks with size 2x2 will be 16384. For conducting the same experiment as Chaluvadi and Prasad's method 10 % of total blocks with difference of 10 blocks between each selected block have to be selected.
The first type of bit tampering attack is Attack-1 which is made by changing the 4th LSB of selected blocks to value 1. It means if the value of the 4th LSB is 0, will be changed to 1 and if the value of the 4th LSB is already 1, no change will be performed. So in this attack number of selected blocks for tampering and number of actual tampered blocks will be different.
The second type of bit tampering attack that has been performed is Attack-2 which is made by modifying the 4th LSB of pixels inside the selected blocks by replacing 0 with 1 and 1 with 0 for all the 4th LSB inside the blocks. Thus the number of selected blocks and actual number of tampered blocks in this attack will be equal to each other, which make this attack a perfect experiment for evaluating the proposed tamper detection system. However tamper detection rate will be calculated by (2).

$$Dt = \frac{number\ of\ detected\ blocks}{Number\ of\ tampered} X\ 100 \qquad (2)$$

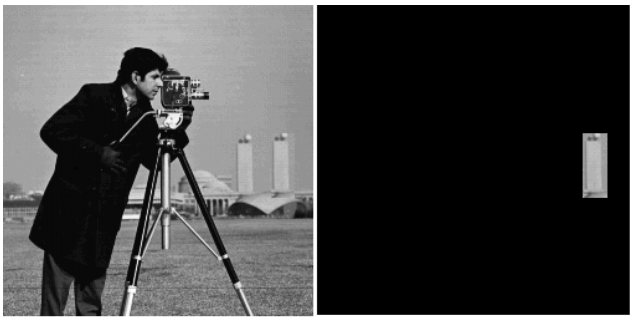
3.1 Collage Attack experimental result

The following figures illustrating the collage attack on gray scale images. The attack is copy and pastes some part of the image inside the image. As illustrated in following Figures the proposed method accurately detected the tampered areas.

(a) (b)

Fig. 4 Collage Attack: (a) tampered room, (b) Tamper detected

To achieve a good set of experiment, deletion attack is going to be performed in small and large size with different set of images. Fig. 9, Fig. 10 and Fig. 11 clearly illustrated the power of our proposed tamper detection method in detecting collage tampers in any size and scale. These images illustrate deletions in different size which all have been detected by system tamper detection method. Moreover, the localization of tampered blocks also has been calculated by proposed system.



(a) (b)

Fig. 5 Collage Attack2: (a) tampered camera man, (b) Tamper detected

(a) (b)

Fig. 6 Collage Attack3: (a) tampered house, (b) Tamper detected

As figure 5 and figure 6 illustrated the proposed authentication method is capable to detect the copy-move collage attack accurately.

3.2 Experiments Results of Deletion Attack

To achieve a good set of experiment, deletion attack is going to be performed in small and large size with different set of images. Figure 7, figure 8 and figure 9 clearly illustrated the power of our proposed tamper detection method in detecting collage tampers in any size and scale. These images illustrate deletions in different size which all have been detected by system tamper detection method. Moreover, the localization of tampered blocks also has been calculated by proposed system.

3.3 Experimenting result of Attack-1and Attack-2

In this section tampering on the 4th LSB of 10 % of selected block will be performed, the result will be used in comparison with [15] and [14]. The selected blocks are chosen from different position within the host image. Figure 10 illustrates performing of attack-1 on gray scale Lena image with size of 256x256. As figure 10 illustrated, proposed tamper detection method were able to detect 1187 of 1458 modified blocks. The total number of tampered blocks in this attack supposes to be 1639 blocks, but because Attack-1 attempted to replace all 4th LSB of watermarked image with 1 the bits that already have value 1 won't be changed.

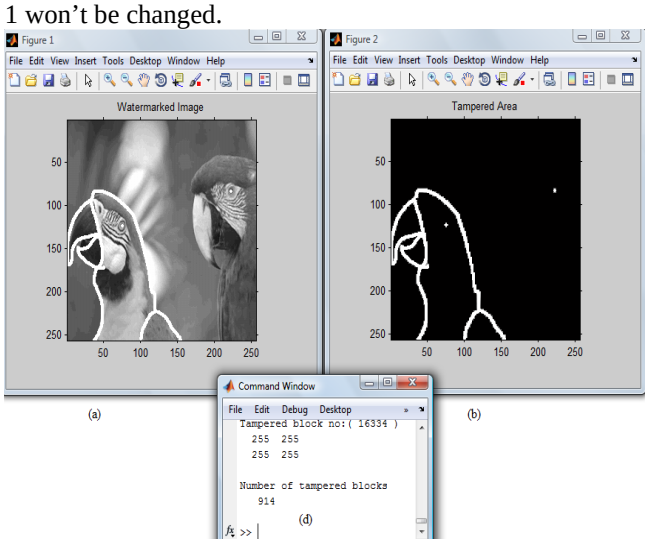


Fig. 7 DeletionAttack1: (a) tampered parrot, (b) Tamper detected, (d) number of tampered blocks

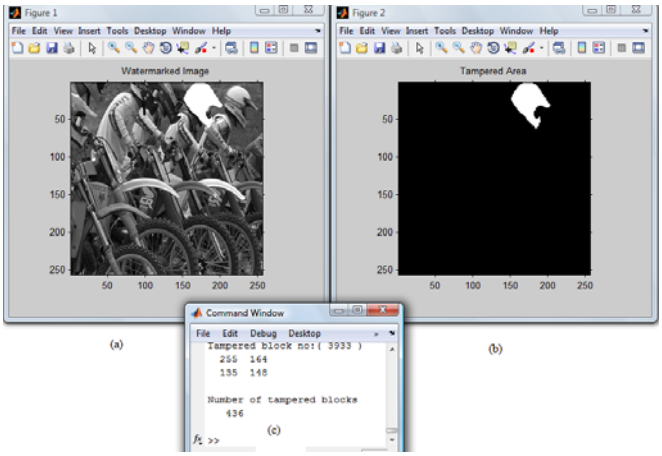


Fig. 8, DeletionAttack2: (a) tampered bike, (b) Tamper detected, (d) number of tampered blocks

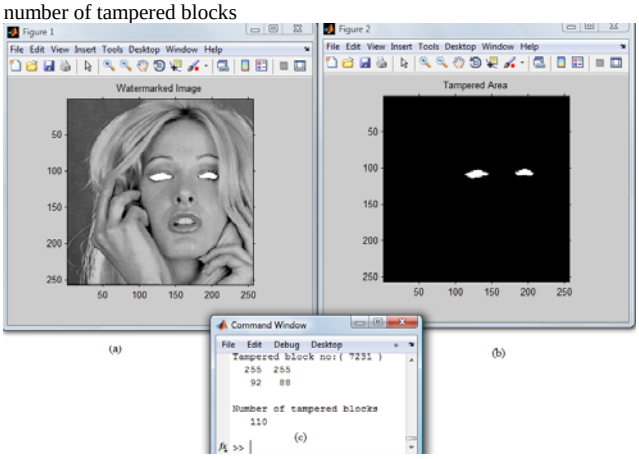


Fig. 9, DeletionAttack3: (a) tampered face, (b) Tamper detected, (d) number of tampered blocks

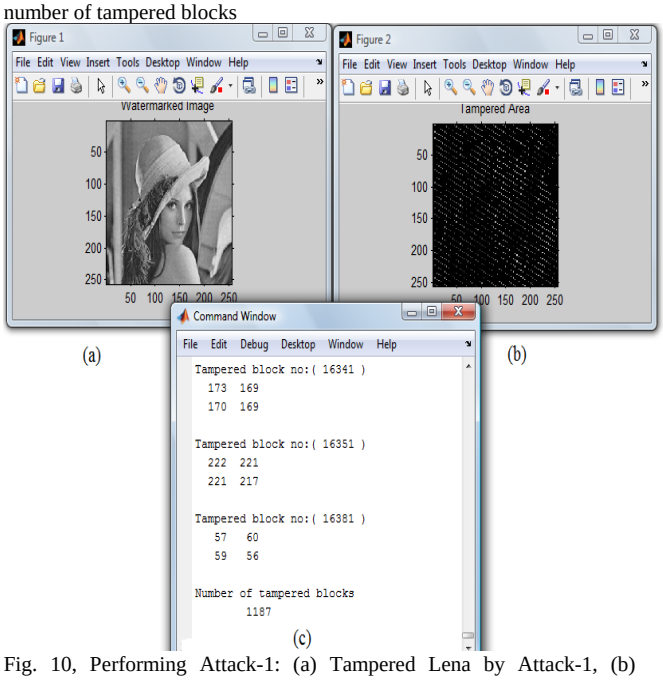


Fig. 10, Performing Attack-1: (a) Tampered Lena by Attack-1, (b) Tampered area detected, (c) Number of tampered blocks detected

Attack-2 has been performed on 10% of selected blocks. As explained previously, this tampering attack modifies the 4th LSB of the watermarked image. So if the value of the 4th LSB were 1, attack will change it to 0 and if the value were already 0 it will be changed to value 1. Attack-2 is perfect experiment to evaluate tamper detection rate, because number of modified blocks is equal to the number of actual tampered blocks which in this case is 1639 blocks.

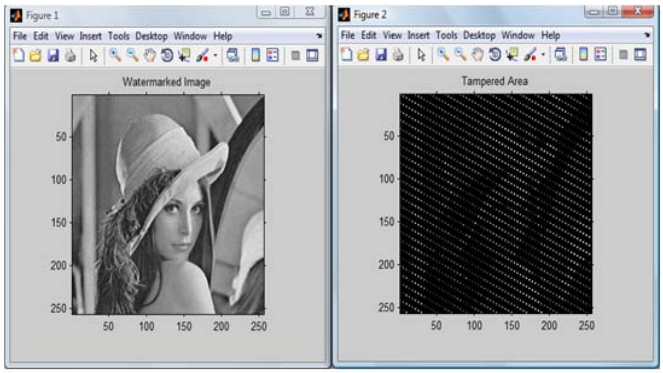


Fig. 11, Performing Attack-2: (a) Tampered Lena by Attack-2, (b) Tampered area detected

Figure 11 illustrates performing attack-2 on gray scale Lena image with 256x256 pixel size. As the figures illustrated our proposed tamper detection method was able to detect all the tampered blocks successfully which is 1639 blocks. Moreover, the system presents the tampered areas graphically and localizes all the tampered blocks with the corresponding blocks numbers.

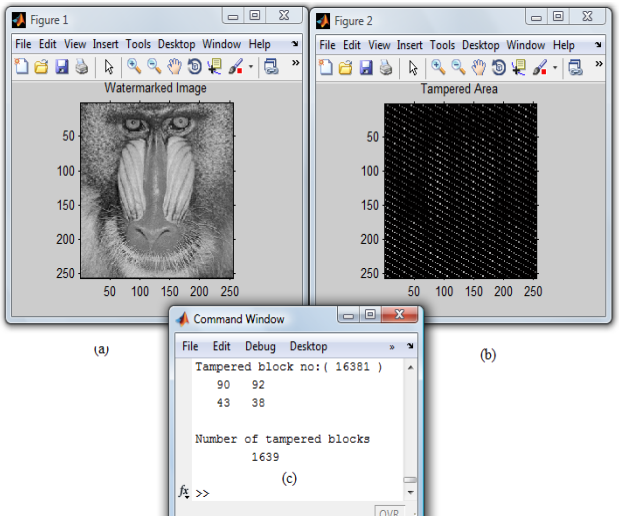


Fig. 12, Performing Attack-2 on Baboon: (a) Tampered Baboon by Attack-2, (b) Tampered area detected

Figure 12 illustrates performing attack-2 on watermarked Baboon image. As it is shown in figure 12 all the tampered blocks has been detected by the proposed authentication system. The number of tampered blocks is 1639 block which is exactly the same as number of detected blocks by the proposed system.

4. Evaluating the proposed tamper detection

A dual tamper detection method proposed by Lee and Shinfeng's [14] have been improved by Chaluvadi and Parsad's [15] tamper detection method and our proposed 2-Level tamper detection has improved the tamper detection percentage of [15]. The comparison of Attack-1 and Attack-2 experiment result is illustrated in Table 1.

Table 1: Comparison of tamper detection percentage

#	***Attack-1***	***Attack-2***
10% of Blocks selected in watermarking	**1639**	**1639**
Modified blocks in Watermark Image (%)	1458(1458/ 1639 = **88.96%)**	1639 (**100%)**
No of Detected blocks by Lee and Shinfeng's method [14] (%)	NIL (**0%**)	NIL (**0%**)
No of Detected blocks by Chaluvadi and Parsad's method [15] (%)	649 (649/1458 = **47.59%**)	849 (849/1639= **51.79%**)
No of Detected blocks by system's proposed method	1187(1187/1458 = **81.41%)**	1639 (1639/1639= **100 %**)

After conducting the Attack-1 on Lena watermarked image, Lee and Shinfeng's method were not able to detect even one single tampered block, Chaluvadi and Parsad's method [15] were able to detect 649 blocks which is 47.59 % of tampered blocks, but our proposed 2-Level tamper detection method detected 1187 of tampered blocks which is 81.41 % of tamper detection percentage which prove the efficiency of propos system. The number of selected blocks for Attack-2 is 1639 which is exactly equal to number of actual modified blocks. Lee and Shinfeng's method still were not able to detect one single block for this specific attack and Chaluvadi and Parsad's method [15] were able to detect 849 tampered blocks which is 51.79 % tamper detection rate. Finally our proposed tamper detection method had 100% detection rate for this high level attack which proved the high efficiency and accuracy of our proposed method.

5. Conclusions

In this paper, we illustrated an efficient method for image authentication and tamper localization. Different types of tampering attacks have been experimented in order to evaluate the proposed method. The examination results of our proposed authentication obtained high tamper detection rate result. However the evaluation result of proposed system proved the efficiency and accuracy of the proposed authentication method in detecting and locating the tampered area.

Acknowledgments

The authors would like to thank University Teknologi Malaysia for their educational and financial support.

References

[1] W. Lin et al, "Multimedia Analysis, Processing & Communications", Springer-Verlag Berlin Heidelberg, 2011 SCI 346, pp. 139–183.
[2] G. Friedman, "The trustworthy digital camera: restoring credibility to the photographic image ", Proceedings of the IEEE International Conference on Image Processing. Chicago, IL, USA. October 1998. pp. 409–413.
[3] Y. Tien, and D.Shinfeng, "Dual watermark for image tamper detection and recovery, Pattern Recognition", 2008. pp.3497–3506.
[4] D. Kundur,. and D. Hatzinakos, "Digital watermarking for telltale tamper proofing and authentication", Proceedings of the IEEE, 1999, Vol. 87, pp. 1167–1180.
[5] G.Yu, and H. Liao, "Mean quantization-based fragile watermarking for image authentication", 2001, pp. 1396–1408.

[6] C.Y Lin, .and C. Chang, "Semi-fragile watermarking for authenticating JPEG visual content", SPIE International Conference on Security and Watermarking of Multimedia Contents II.San Jose, USA, January 2000.
[7] S.H. Liu, H.X. Yao, W. Gao, and Y.L. Liu, "An image fragile watermark scheme based on chaotic image pattern and pixel-pairs", Applied Mathematics and Computation, 2007, vol. 185, no. 2, pp. 869-882.
[8] C. Vleeschouwer, J.F. Delaigle, and B. Macq, "Invisibility and application functionalities in perceptual watermarking-an overview", Proceeding of the IEEE, 2002, vol. 90, pp. 64–77.
[9] H. H, N. Zhang, and H.M. Tai, "Awavelet-based fragilewatermarking scheme for secure image authentication", Proceeding of 5th International Workshop on Digital Watermarking.
[10] J. Fridrich, "Security of fragile authentication watermarks with localization", Proceeding of SPIE Security and Watermarking of Multimedia Contents IV, San Jose, CA, 2002, vol. 4675, pp. 691–700.
[11] P.W. Wong, "A public key watermark for image verification and authentication", Proceedings of the IEEE International Conference on Image Processing, 1998, vol.1, pp.455-459.
[12] C. Chang, Y. Fan, and W. Tai, "Four scanning attack on hierarchical digital watermarking method for image tamper detection and recovery", Pattern Recognition, 2008, vol. 41, pp. 654-661.
[13] S.D. Lin, Y. Kuo, and M, Yao, "An image watermarking scheme with tamper detection and recovery", International Journal of Innovative Computing, Information and Control, 2007, vol. 3, no. 6(A), pp.1379-1387.
[14] T. Lee and S. D. Lin, "Dual watermark for image tamper detection and recovery,"Pattern Recognition", 2008, vol. 41, pp.3497–3506.
[15] S.B. Chaluvadi, M.V.N. Prasad, "Efficient Image Tamper Detection and Recovery Technique using Dual Watermark", Proc. IEEE. World Congress on Nature & Biologically Inspired Computing (NaBIC09), IEEE Press, Dec. 2009, pp.993, doi:10.1109/NABIC.2009.5393888.
[16] D. Kirovski, H.S. Malvar, and Y. Yacobi, "A dual watermarking and fingerprinting system", IEEE Multimedia, 2004, vol. 11, no. 3, pp. 59–73.
[17] P.L. Lin, C.K. Hsieh, and P.W. Huang, "A hierarchical digital watermarking method for image tamper detection and recovery", Pattern Recognition, 2005, vol. 38, pp. 2519–2529.