A Novel Robust Watermarking Algorithm for Image Tamper Detection

Nashmin Afzali[†] **and Kooroush Manochehri**[††]

Department of Computer Engineering and IT, Parand Branch, Islamic Azad University, Parand, Iran

Summary
In recent years, various robust watermarking techniques have been proposed for image authentication and tamper detection. In this paper, a novel robust watermarking algorithm for image tamper detection is proposed. Tamper detection and integrity verification are two important aspects of the robust watermarking schemas. Our schema can detect any modification made to the gray image with acceptable accuracy and to improve the security of the proposed scheme two security layers with MD5 and key initial values are employed. The PSNR values of watermarked images are used as a measurement the efficiency of the proposed watermarking algorithm.

Key words:
Digital Watermarking, Tamper Detection, Image Security, Authentication.

1. Introduction

Nowadays, with grow of internet and multimedia technologies, it becomes very easy to create, duplicate, transmit and modify digital images [1]. Because of various development of multimedia editing tools, it's so difficult to guarantee the integrity verification of image contents [2]. These issues lead to unauthorized activities which bring copyright disputes in associate with lack of accurate information about real ownership of image. Therefore, researchers have looked for ways to ensure the accuracy of digital images. One of the available solution to address this concern is digital watermarking by using hidden information. The process of embedding watermark into a digital image is known as digital watermarking. Watermarking techniques can be classified to robust and fragile watermarking. The robust watermarking schemas are used to authentication of the digital image. The purpose of the fragile watermark is to identify and detect possible tamper and manipulation of the image. In fact, this scheme is used to verify the integrity of image [3].
In [4], a watermarking scheme based on DCT coefficients encoding is proposed so that more secure based on chaotic sequence is achieved. [5] use the hierarchical watermarking and LSB embedding schema to get a MSB sensitive approach. Their solution is based on a chaotic map. [6], to overcome the security and self-recovery issues, propose watermarking algorithm based on singular value decomposition for tamper localization and self-recovery. In [7], to improve quality of the watermarked and recovered images a fragile watermarking method for stereo image authentication with self-recovery capability is proposed. [8] proposed a watermarking scheme based on chaotic maps, where the security of the schema with two chaotic maps is improved.
In this paper, we proposed a novel robust watermarking algorithm with the security of BBS pseudorandom generation and hash function to improve the security and fast tampering detection of gray images. In this schema, a binary logo is used as watermark and extracting the correct hash code indicating lack of change in the image.
The rest of paper is organized as follow: In section 2, Blum-Blum-Shub pseudorandom generator is described. In section 3, the proposed schema is presented. In section 4, experimental results are explained and finally in section 5, the conclusions are presented.

2. Blum-Blum-Shub Pseudorandom Generator

Similar to the toss of cent, a pseudo random sequence generator should be unpredictable. These sequence of bits should quickly produce from short seeds. The seed is the input to the generator [9]. One of the characteristics of a pseudorandom generator is security level. This attribute shows that it's too hard to discover the difference between pseudorandom sequences and truly random sequences. This issue is most apparent in the Blum-Blum-Shub pseudorandom generator [10].
BBS is a random bit generator with the following form:

$$x_{n+1} = x_n^2 \bmod M \qquad (1)$$

Where M is the product of two large distinct primes (p, q=3mod4). Also, at each step of the algorithm, the output is derived from xn+1 or one or more of the least significant bits of xn+1. The seed x0 should be an integer that's not 1 or co-prime to M.

Manuscript received November 5, 2016
Manuscript revised November 20, 2016

3. The Proposed Scheme

In this section, we explain the proposed watermarking algorithm. Let us consider, I, is the host image of size M×N and w is the watermark image of size m×n.

3.1 Watermarking Embedding

Embedding process of watermark is as follow:

- Divide the binary image into 3×3 non-overlapping blocks;
- Scramble these blocks using rotation around central pixels of each block;
- Rearrange the blocks to obtain the basic scrambled image;
- The use of MD5 hash generator to generate the hash code;
- The definition of private key values, used as initial values of Blum-Blum-Shub pseudorandom generator;
- Determination of embedding criteria based on the output of BBS pseudorandom generator;
- Extracting the two values of embedding criteria; embedding location and embedding value;
- Obtain watermark using exclusive-or (XOR) operation between hash code (H_M) and embedding value extracted from the embedding criteria (C_V):

$$W = H_M \oplus C_V \quad (2)$$

- Replace C_L pixels in the host image by W to get the watermarked image (I_W).

The embedding process of watermark in the host image is shown in Fig. 1.

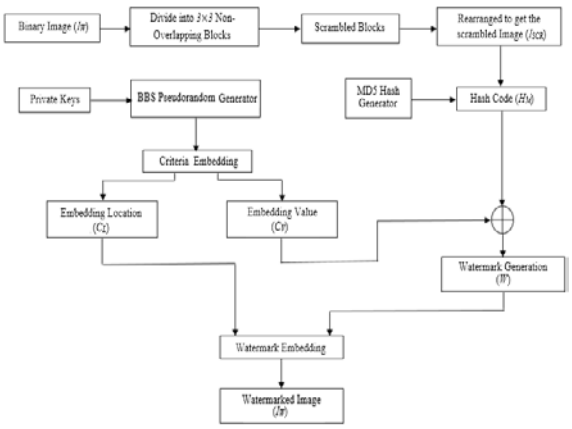

Fig. 1 Embedding of watermark in the host image.

3.2 Hash Code Extraction

Extraction process of hash code is as follow:

- Obtain the embedding criteria including embedding location and embedding value according to private key values provided in embedding algorithm;
- Extraction of embedding values in watermarked image by using the embedding location (C_L)
- Apply exclusive-or (XOR) operation between the embedding values in watermarked image and C_V, to get the hash code.

The extraction process of hash code from watermarked image is shown in Fig.2.

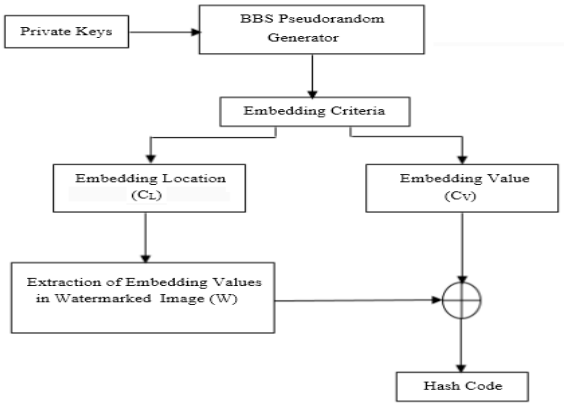

Fig. 2 Extraction of hash code from watermarked image.

As shown in Fig. 3 the hash code is extracted to check whether the image is tampered or not.

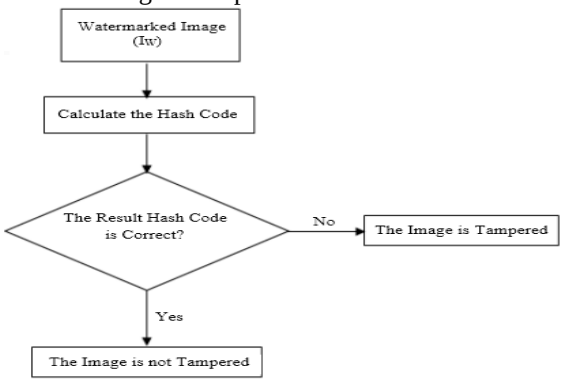

Fig. 3 Extraction of hash code to check if the image has tampered.

4. Experimental Results

To access the performance of the proposed algorithm, the approach is tested on two images. A binary logo of size 64×64 is considered as watermark which is to be embedded according to proposed method.

In this section, visual quality of the watermarked image is evaluated by PSNR parameter. Peak Signal-to-Noise Ratio (PSNR) represents the ratio between the maximum

possible value of a signal and the power of distorting noise that affects the quality of its representation. PSNR is defined as:

$$PSNR = 10log_{10}\left[\frac{b}{MSE}\right] \quad (3)$$

Where b, is the square of the largest value of the signal that in case of an 8-bit is 255. The Mean Square Error (MSE) is defined as:

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - K(i,j)]^2 \quad (4)$$

Fig. 4 shows the host image, binary watermark and the corresponding watermarked image. To original beach and mountain images are shown in Fig. 4(a) and (b). Binary logo is shown in Fig. 4(c) and the corresponding watermarked images are shown in Fig. 4(c) and (e).

The computed PSNR values are in order to 53.7574 and 60.5525 respectively. So, in this proposed scheme, the PSNR value is at an acceptable level.

Since change in the image results in change the value of MD5 hash, therefore this method can detect any manipulation caused by attacks as well.

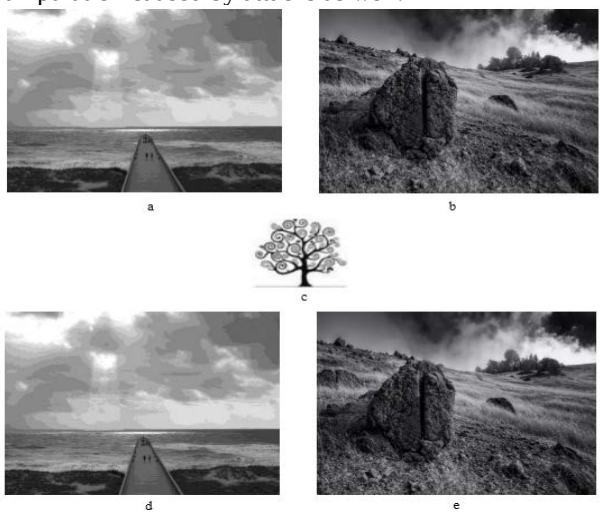

Fig. 4 (a) Original beach image, (b) Original mountain image, (c) Binary watermarked, (d) watermarked beach image, (e) watermarked mountain image.

3. Conclusion

In this paper, a novel robust watermarking algorithm for integrity verification and tamper detection of images is presented. Whereas this scheme is capable of detecting any modification to the gray image, can be useful for copyright protection. The security of proposed algorithm is provided by MD5 hash function and the initial values of Blum-Blum-Shub pseudorandom generator as private keys. So extracting the right sequence is not possible for everyone. Experimental results show that with the quite acceptable level of PSNR, our algorithm can detect any tampering attacks. Due to higher performance and more efficiency of hardware implementation in terms of increasing the image size, we can work on hardware implementation of robust watermarking algorithm for image tamper detection.

References

[1] Chen, Chun-Hung, Yuan-Liang Tang, and Wen-Shyong Hsieh. "An Image Authentication and Recovery Method Using Optimal Selection of Block Types." Multimedia (ISM), 2014 IEEE International Symposium on. IEEE, 2014.

[2] Liu, Fang, et al. "Enhanced perceptual image authentication with tamper localization and self-restoration." 2014 IEEE International Conference on Multimedia and Expo (ICME). IEEE, 2014.

[3] Saiyyad, Mohmmad Ali M., and Nitin N. Patil. "Authentication and tamper detection in images using dual watermarking approach." Reliability, Infocom Technologies and Optimization (ICRITO)(Trends and Future Directions), 2014 3rd International Conference on. IEEE, 2014.

[4] Zhang, Junpeng, Qingfan Zhang, and Hongli Lv. "A novel image tamper localization and recovery algorithm based on watermarking technology."Optik-International Journal for Light and Electron Optics 124.23 (2013): 6367-6371.

[5] Tong, Xiaojun, et al. "A novel chaos-based fragile watermarking for image tampering detection and self-recovery." Signal Processing: Image Communication 28.3 (2013): 301-308.

[6] Dadkhah, Sajjad, et al. "An effective SVD-based image tampering detection and self-recovery using active watermarking." Signal Processing: Image Communication 29.10 (2014): 1197-1210.

[7] Yu, Mei, et al. "New fragile watermarking method for stereo image authentication with localization and recovery." AEU-International Journal of Electronics and Communications 69.1 (2015): 361-370.

[8] Rawat, Sanjay, and Balasubramanian Raman. "A chaotic system based fragile watermarking scheme for image tamper detection." AEU-International Journal of Electronics and Communications 65.10 (2011): 840-847.

[9] Gawande, Kaustubh, and Maithily Mundle. "Various Implementations of Blum Blum Shub Pseudo-Random Sequence Generator."

[10] Sidorenko, Andrey, and Berry Schoenmakers. "Concrete security of the blum-blum-shub pseudorandom generator." IMA International Conference on Cryptography and Coding. Springer Berlin Heidelberg, 2005.

Nashmin Afzali received the B.Sc. degree in Software Engineeringfrom the Azad University (Central branch), Iran, in 2012 and the M.Sc. degrees in Computer Architecture from Azad University (Parand branch), Iran, in 2016. Her research interests include Computer Algorithms, Computer Security and Computer Networks.

Kooroush Manochehri is an assistant professor in Azad University (Parand Branch). He received his B.Sc. degree in Computer Engineering from the Azad University (Central branch), Iran, in 2001 and the M.Sc. degree in Computer Engineering (with honors) from the Department of Computer Engineering at the Amirkabir University of Technology, Iran, in 2005 and his PhD. In Computer Engineering from same university in 2011. His research interests are in the fields of Cryptography, Computer Arithmetic and Hardware Implementations.