ISSN:2249-5789
Ranjan Kumar Arya et al , International Journal of Computer Science & Communication Networks,Vol 4(3),119-124

A Novel Digital Watermarking Algorithm using Dual Keys with RMI

Ranjan Kumar Arya
Computer Science and Engineering
Central University of Rajasthan
Email: ranjan2013_mtech@curaj.ac.in

Mr. Ravi Saharan
Computer Science and Engineering
Central University of Rajasthan
Email: ravisaharan@curaj.ac.in

Abstract-The availability of internet is sufficient to communicate digital docu ments. The digital documents are different types of threads. So we need protection mechanism to protect these digital documents. The most important protection mechanism for digital assets is to prevent the digital documents from unauthorized access .In modern time unauthorized access of digital assets are increasing rapidly. Unauthorized access is very big issue against the protection the digital assets. So a robust algorithm for copyright protection is required. The existing technique of watermarking protects the digital documents by embedding the watermarked image into host image. The imperceptibility is one of the most important properties of watermarking. When embed watermark image into host image, more distortions in the pixels value of host image may accrue, due to imperceptibility of watermarking is affected. In this paper protection of host image is base on the dual key. The first key is generating by the help of host image by using algorithm and second key generate from random matrix. We can also say that the random matrix image (RMI) [1] used for second key. In this paper the embedding and extraction algorithm both are different to each other. A histogram result shows the better impeccability of this new method.

Index Terms-Digital Watermarking, Dual Keys , Image processing, Embedding and Extraction.

1. Introduction

In modern time security is very important and effective, because we need security in each and every field. Without security we can't keep our things safe. In modern time everyone is using Internet because using internet we can do maximum work by paying low cost. Some time we need to send our documents through internet and we know very well that internet is not a secure way of transaction. So we need more security. Internet also provides facility to send digital data such as videos, audio and images for public. So we need security of these digital data in terms of authentication, security and copyright protection. For the copyright protection or ownership identification watermarking is one of the best solution. Now a day copyright protection is one of the big issues of digital documents, one that has made a lot of problems for the media [2]. Through the internet the data is transferred in many ways. There are different formats of data like image, audio and video. When data is being transmitted from one place to another then they travel long distance over the internet [3]. In this period illegal users try to access these data. If unauthorized user able to access these data then authorized user loss there data. Digital watermarking is an authentication of digital data with secret information that can be extracted [1]. The

image in which secret information embed is called cover image or host image. If the size of the secret information increases, the robustness of the watermark image will be decreases. Digital watermarking consider in three steps embed, attack and extraction. Digital watermarking may be classified into two groups according to its domains. They are spatial domain and frequency domain. Over spatial domain the watermark image embedded into host image by changing the pixels values of the host image [3]. There are so many algorithms in spatial domain like LSB (Least significant bit), ISB (Intermediate significant bit) and Patchwork etc [4]. In frequency domain embedding uses the transform coefficients to embed the watermark. Moreover, transform domain techniques are very robust against attacks, because the watermark is spread in whole image [4]. The technique which is use in frequency domain technique is discrete cosine transform (DCT), Discrete Wavelet Transform (DWT) and Discrete Fourier transform (DFT) [2]. There are so many types of watermarking attacks. The watermarked image is generally sent from one to another or may be store. If any person wants to change or change the documents then it is called attack in watermarking [7][8][9][10][11][12]. Noise and geometric attack is one of them. There are many types of noise attack such as Gaussian noise attack, and blurring noise attack [5].Geometric attack also a strong attack in watermarking. There are many types of geometric attacks such as rotation, cropping, and other transformations [6].

2. Proposed Work

In this paper we are using random matrix in place of watermark image [1]. For different image the watermark image will be different and each watermarked image need two key for extraction. The first key will be random matrix and second will be the master key. Watermarked image of original host image will be generated by the help of these keys. Generally in watermarking extraction process is just reverse of embedding process. In this paper extraction process is not a reverse process of embedding. For extraction we need to use two keys one random matrix and second master key.

2.1 Introduction of random matrix image

In this paper we are using random matrix image for key purpose. For each new image we are generating new watermark image. The second key is generated using random function which contains random number from given range. As for example if we want to generate matrix of size 5*5 and elements of matrix from 0 to 10. Then the generated matrix may contain any number from 0 to 10.

2.2 First key generation

The first key generate from the pixel value of host image (H). We generate the key on the basis of even and odd value of pixels of host image. If the pixel value is even number then the value of this particular pixel will be increase by one, if pixel value is odd number then increase the pixel value by two and if the value of pixel is zero (0) then decrease this particular value by one. After applying these operations we get a new matrix (H1). To get first key we do simple matrix subtraction between new matrix H1 and original host image H.

2.3 Second key generation

To generate second key we generate a random matrix having same size of host image, which contains the value from 1 to 10.

2.4 Master key generation

Master key is the combination of first key and second key. For master key we will do matrix subtraction. The key matrix one is substrate from the key matrix two by simple matrix operation.

2.5 Watermark embedding algorithm

Step1: Read the original image (H).

Step2: find new host image (H1) after the operation on pixel value of host image.

Step3: Generate K1 by subtract H from H1.

Step4: Generate Random matrix (K2) from 0 to 10 of same size of host image.

Step5: Add K1+K2 for Master key.

Step6: Add H1 + Master key and output image will be watermarked image.

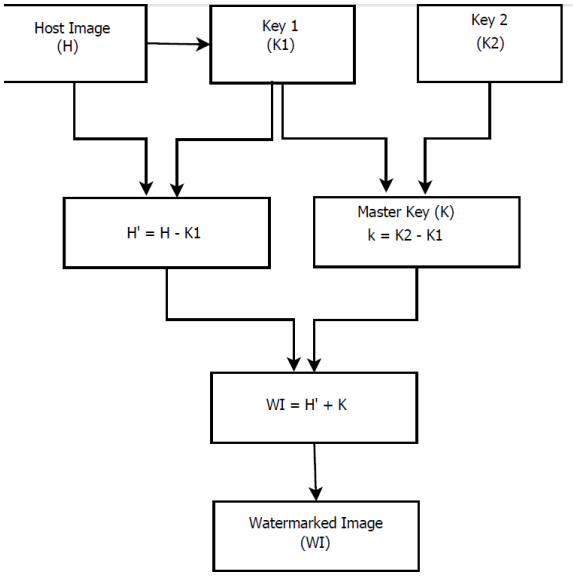

Fig. 1. Flow chart of Embedding of watermarking

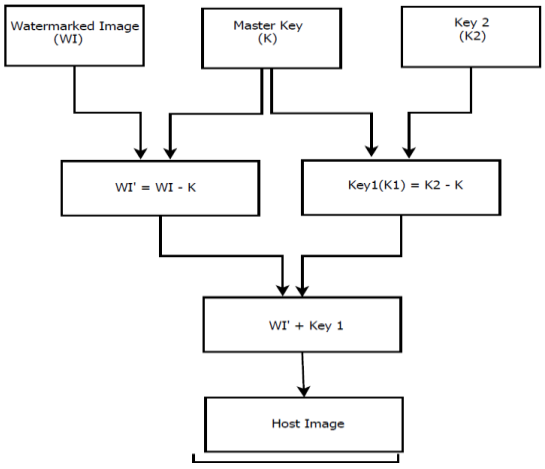

Fig. 2. Flow chart of Extraction of watermarking

2.6 Watermark extraction algorithm

Step1: Read watermarked image (WI)

Step2: Find WI from subtract Master key from watermarked image.

Step3: Again subtract Master key from key 2 (K2) to get key1 (K1).

Step4: Add key1 (K1) and WI.

Step5: Output image will be original host image.

3. Implementation and Results

The implementation are performed by using 256*256 pixels gray level host image and 8*8 pixels images.Fig.3 shows the gray level host image.Fig.4 is image which is generated from the pixels value of the host image. Fig.5 shows the pixels value of host image to identify the even and odd value of the host image pixels. Fig.6 is the pixels value of master key which is generated by the help of two keys. Fig.7 is watermarked image and the pixels value of watermarked image is shown in Fig.8. Now for proper identification histogram of host image, watermarked image and the extracted host image from watermarked image shown in Fig.9.

Fig. 3. Host Image

4. Conclusion

A novel algorithm of digital image watermarking based on random matrix and key generation. In place of watermark image we are using random matrix. Actually the random matrix which is explained in this

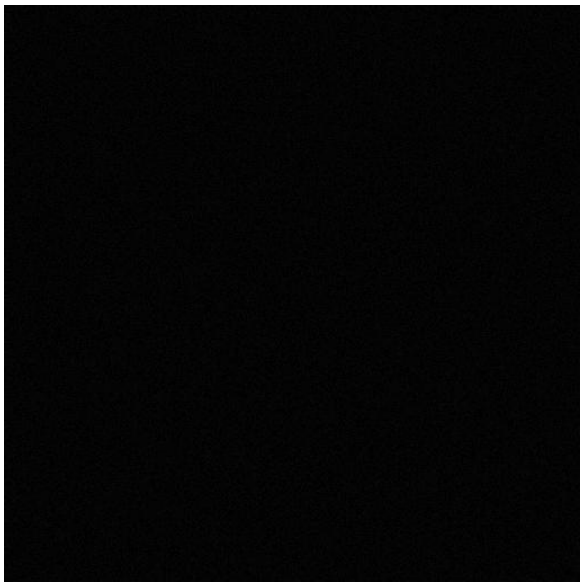

Fig. 4. Master key (K)

195	195	196	197	197	198	199	199
196	196	196	197	197	197	198	198
197	197	197	197	196	196	196	196
199	198	198	197	196	195	194	194
199	198	197	196	195	194	193	193
198	198	197	196	195	194	193	193
197	196	196	195	195	194	194	194
196	196	195	195	195	194	194	194

Odd pixels value

Even pixels value

Fig. 5. Pixel value of host image

2	2	9	8	2	6	3	6
7	2	0	0	0	0	8	3
9	1	3	0	4	0	1	1
2	6	3	0	7	2	4	2
9	3	0	6	3	6	7	2
5	5	3	7	7	0	5	2
5	1	0	7	5	8	0	5
2	0	5	5	9	7	6	6

Fig. 6. Pixel value of master key image [1]

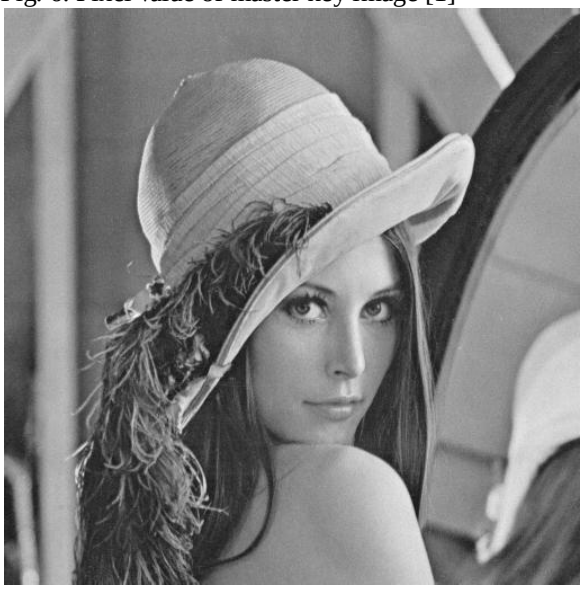

Fig. 7. Watermarked Image

197	197	205	205	199	204	202	205
203	198	196	197	197	197	206	201
206	198	200	197	200	196	197	197
201	204	201	197	203	197	198	196
208	201	197	202	198	200	200	195
203	203	200	203	202	194	198	195
202	197	196	202	200	202	194	199
198	196	200	200	204	201	200	200

Fig. 8. Pixel value of watermarked image [1]

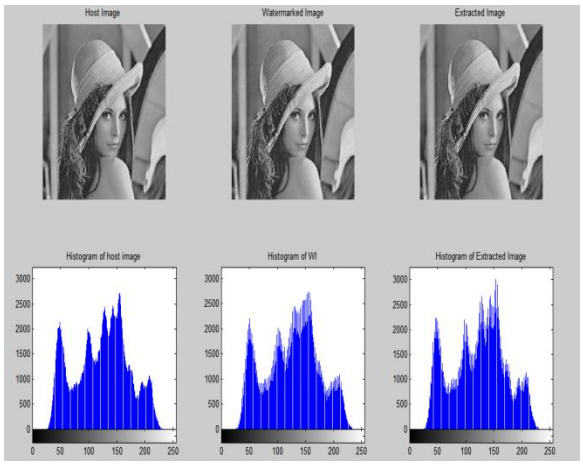

Fig. 9. Histogram of image

Paper is not only a random key it is a master key which is the combination of two keys. The interesting point is first key generate from the pixel value of the host image and further they used for watermark image. In place of using random matrix in this paper we are using master key for the authentication of user which is not easy to break. The most important in this algorithm is embedding and extraction process steps totally different. In proposed work if the attacker success to get any one key then attacker cannot find the original image because we are using two key to generate watermark image. The limitation of this paper is that the proposed technique of digital image watermarking is work on gray scale image not in colored image. The implementation performed on grayscale image having less than 245 grayscale pixel value. The future work of this work can use of this technique on colored images.

5. References

[1] Mahimn Pandya, Hiren Joshi,Ashish Jani, A Novel Digital Watermarking Algorithm using Random Matrix Image, International Journal of Computer Applications (0975 8887) Volume 61 No.2, January 2013

[2] Haohao Song; Zihua Qiu; Jian Gu, "A novel semi-fragile image watermarking scheme based on wavelet," Audio Language and Image Processing (ICALIP), 2010 International Conference on , vol., no., pp.1504,1510, 23-25 Nov. 2010 doi:10.1109/ICALIP.2010.5684538.

[3] Ali Sharifara, Mohd Shafry Mohd Rahim, Morteza Bashardoost, A Novel approach to Enhance Robustness in Digital Image Watermarking using Multiple Bit-planes of intermediate Significant Bits, 2013 International Conference on Informatics and Creative Multimedia, 978-0-7695-5133-3/13, 2013 IEEE DOI 10.1109/ICICM.2013.13

[4] Mohammad Abdullatif, Akram M. Zeki, Jalel Chebil, Teddy Surya Gunawan, Properties of Digital Image Watermarking, 2013 IEEE 9th International Colloquium on Signal Processing and its Applications, 8 - 10 Mac. 2013, Kuala Lumpur, Malaysia.

[5] O. O. Khalifa, Y. binti Yusof, A. H. Abdalla, and R. F. Olan rewaju, "State-of-the-art digital watermarking attacks," in Computer and Communication Engineering (ICCCE), 2012 International Conference on, 2012, pp. 744-750.

[6] V. Licks and R. Jordan, "Geometric attacks on image watermarking systems," Multimedia, IEEE, vol. 12, pp. 68-78, 2005.

[7] M. A. Suhail, M. S. Obaidat, S. S. Ipson, and B. Sadoun, A comparative study of digital watermarking in JPEG and JPEG 2000 environments, Information Sciences, Elsevier, vol. 151, pp. 93105, May 2003.

[8] M. Sreerama Murty, D. Veeraiah, and a Srinivas Rao, Digital Signature and Watermark Methods For Image Authentication using Cryptography Analysis, Signal Image Processing : An International Journal, vol. 2, no. 2, pp. 170179, Jun. 2011.

[9] D. Kirovski and F. a. P. Petitcolas, Blind pattern matching attack on watermarking systems, IEEE Transactions on Signal

Processing, vol. 51, no. 4, pp. 10451053, Apr. 2003.
[10] V. M. Potdar, S. Han, and E. Chang, A survey of digital image watermarking techniques, INDIN 05. 2005 3rd IEEE International Conference on Industrial Informatics, 2005. No. Indin, pp.709716, 2005.
[11] T. Furon and P. Duhamel, An asymmetric watermarking method, IEEE Transactions on Signal Processing, vol. 51, no.4, pp. 981995, Apr. 2003.
[12] M. Wu and B. Liu, Attacks on digital watermarks, Conference Record of the Thirty-Third Asilomar Conference on Signals, Systems, and Computers (Cat. No.CH37020), vol. 2, pp. 15081512.