IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

An Invisible Robust Image Watermarking Technique based on Pseudo Random Numbers with Attacks

Shatha Ghazal[1], Raina S Alkhlailah[2]

Al – Balqa Applied University (BAU) [1, 2]

Abstract: In this paper an invisible robust image watermarking scheme based on pseudo random numbers with various attacks is proposed. This algorithm works on spatial domain. In this paper cover image partitioned into 3*3 blocks and random blocks are chosen for the watermark embedding. Watermark is pseudo random binary sequence and protected by the secrete key. At the receiver effectiveness is checked by the correlation between sender data and received data. This paper comprises various attacks such as noise attack, low pass filtering attack, median filtering attack on the watermarked image for checking robustness of the scheme.

Keywords: Watermarking, Robust, Pseudo random, invisible.

I. INTRODUCTION

In the recent time, the rapid and extensive growth in Internet technology is creating a pressing need to develop several newer techniques to protect copyright, ownership and content integrity of digital media. This necessity arises because the digital representation of media possesses inherent advantages of portability, efficiency and accuracy of information content in one hand, but on the other hand, this representation also puts a serious threat of easy, accurate and illegal perfect copies of unlimited number.

Unfortunately the currently available formats for image, audio and video in digital form do not allow any type of copyright protection. A potential solution to this kind of problem is an electronic stamp or digital watermarking which is intended to complement cryptographic process [1]. While the later technique facilitates access of the encrypted data only for valid key holders but fails to track any reproduction or retransmission of data after decryption. On the other hand, in digital watermarking, an identification code (symbol) is embedded permanently inside a cover image which remains within that cover invisibly even after decryption process. This requirement of watermarking technique, in general, needs to possess the following characteristics: (a) imperceptibility for hidden information, (b) redundancy in distribution of the hidden information inside the cover image to satisfy robustness in watermark extraction process even from the truncated (cropped) watermarked image and (c) possible use of one or more keys to achieve cryptographic security of hidden content [2]. Besides these general properties, an ideal watermarking system should also be resilient to insertion of additional watermarks to retain the rightful ownership. The perceptually invisible data hiding needs insertion of watermark in higher spatial frequency of the cover image since human eye is less sensitive to this frequency component. But in most of the natural images majority of visual information are concentrated on the lower end of the frequency band. So the information hidden in the higher frequency components might be lost after quantization operation of lossy compression [3]. This motivates researchers in recent times to realize the importance of perceptual modeling of human visual system and the need to embed a signal in perceptually significant regions of an image, especially if the watermark is to survive lossy compression [4].

In spatial domain block based approach, this perceptually significant region is synonymous to low variance blocks of the cover image. It is found in the literature that the robust watermarking systems proposed so far can only withstand some of the possible external attacks but not all. While spatial domain watermarking, in general, is easy to implement on computational point of view but too fragile to withstand large varieties of external attacks.

On the other hand, frequency or transformed domain approach offers robust watermarking but in most cases implementation need higher computational complexity. Moreover the transform domain technique is global in nature (global within the block in block based approach) and cannot restrict visual degradation of the cover image. But in the spatial domain scheme, degradation in image quality due to watermarking could be controlled locally leaving the region of interest unaffected. The present paper describes a computationally efficient block based spatial domain watermarking technique for a two level watermark symbol. The selection of the required block is based on variance of the block and watermark insertion exploits average brightness of the blocks. The Watermark recovery process does not require either the cover/watermarked image or the watermark symbol only except the secret image.

DOI 10.17148/IJARCCE.2016.5897

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

The paper is organized as follows: section 2 describes the watermark embedding and extraction process. Section 3 describes Result analysis and quality parameters. Section 4 consists of conclusion and then references.

II. METHODOLOGY

Following block diagram shows the basic watermarking sender and receiver side.

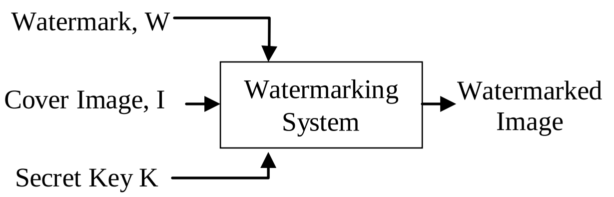

Fig. 1. Watermark embedding basic block diagram

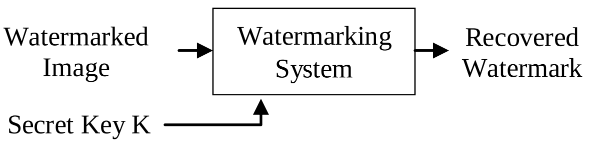

Fig. 2. Watermark Extraction basic block diagram

A. Proposed Embedding Process

Following block diagram shows the block diagram of embedding process.

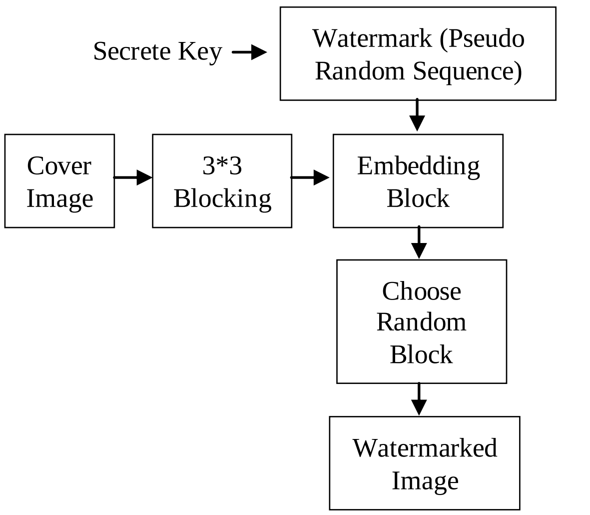

Fig. 3. Watermark Embedding Proposed block diagram

Cover Image: Cover image is either grayscale or colour. Let I be the cover image and having size $m*n*p$ presented as

$$I = \left\{ I(i,j,k) \middle| \begin{matrix} 0 \le i < m, 0 \le j < n \;\; 0 \le k < p \\ I(i,j,k) \epsilon \{0,1,2,3,4, \dots \dots .., 255\} \end{matrix} \right\}$$

Where m is number of rows, n is number of columns & p is number of planes.

Blocking: Cover image is divided into 3*3 blocks. Suppose we have image having size 510 rows 510 col. After dividing image into 3*3 size we get total 28900 blocks. So we able to embed almost 28900 bits of watermark in cover image.

Watermark: Watermark is a binary pseudo random sequence. Can be represented as below.

$$\text{Watermark} = \left\{ w(1,j) \middle| \begin{matrix} 0 \le j \le (row * col) \\ w(1,j) \, \epsilon \, \{0,1\} \end{matrix} \right\}$$

Length of the watermark sequence should less than number of blocks in cover image.

Secrete Key: Secrete key is a binary array having size equal to length of the pseudo random numbers. Can be represented as below.

$$\text{sec\_key} = \left\{ S(1,j) \middle| \begin{matrix} 0 \le j \le \text{len}(\text{Watermark}) \\ x(1,j) \, \epsilon \, \{0,1\} \end{matrix} \right\}$$

Encryption: In this pseudo random numbers are x-ored with secrete key.

$$\text{Enc\_sec\_msg} = \{\text{Watermark} \oplus \text{sec\_key}\}$$

Embedding Block: This block consist of embedding process. Random blocks chosen for embedding encrypted secrete message & embedded into the middle pixel of the 3*3 block. It has bit as an input parameter,

If (bits =3)
(Embed 3 bits of Enc_sec_msg into middle pixel of the block till message it not finished)
end

Following blocking diagram of the pixel shows the middle pixel is selected for embedding process.

10	20	60
40	**30**	50
77	66	55

Fig.4. Blocking of the cover image & selecting centre pixel for embedding

After embedding all the encrypted secrete bits in the blocking of the image at last we get watermarked image.

B. Proposed Extraction process

Following block diagram shows the Extraction process and it is exactly reverse to that of embedding process.

This technique checked for various attacks. Some of them are listed below.

Salt & Pepper noise Attack, Gaussian Noise Attack, Low pass filtering attack and median filtering attack.

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

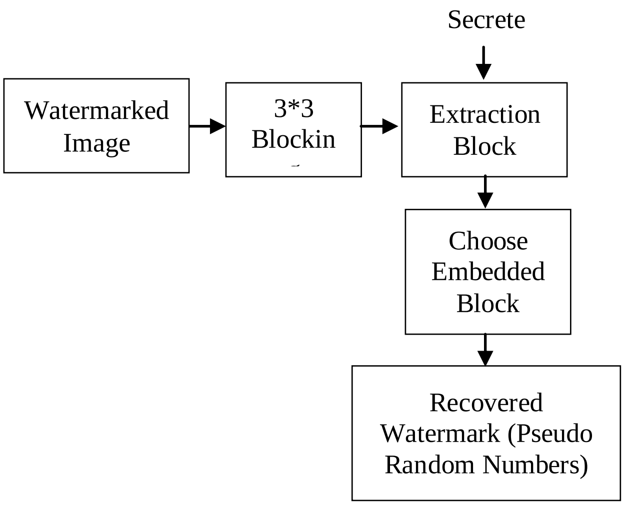

Fig. 5. Watermark Extraction Proposed block diagram

III.RESULT ANALYSIS & DISCUSSION

This method has various quality parameters & these are listed below.

A. Quality Parameters

PSNR (Peak Signal to Noise ratio):
This term is mainly used to measure the quality of watermarked Image. It is mostly defined through MSE (mean square error). PSNR is basically expressed in the logarithmic decibel scale.

$$\mathrm{PSNR} = 10 * \log_{10}\left(\frac{\mathrm{Max}(I)^2}{\mathrm{MSE}}\right)$$

MSE (Mean Square Error):
The MSE is cumulative squared error between the watermarked and the original image whereas PSNR is a measure of the peak error.

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

EC (Embedding Capacity):
This term is a measure for how much bits user able to embed in a cover image.

$$\mathrm{EC} = \sum_{i=1}^{bits}(\mathrm{No.of\ Blocks})$$

Correlation:
This term used for finding correlation between original secrete data and received data.

$$r = \frac{\sum_m \sum_n (A_{mn} - \bar{A})(B_{mn} - \bar{B})}{\sqrt{(\sum_m \sum_n (A_{mn} - \bar{A}))^2)(\sum_m \sum_n (B_{mn} - \bar{B})^2}}$$

B. Results

Following results are obtained for above quality parameters.

TABLE I BIT PER PIXEL AND PSNR FOR LENA IMAGE OF SIZE 510*510

Bit/pixel	PSNR in db	EC in bits	NBE in bits
1 bit	74.8272	28900	1024
2 bits	68.4841		
3 bits	62.7509		
4 bits	56.4757		
5 bits	50.8248		
6 bits	44.6197		
7 bits	38.7567		
8 bits	32.4264		

(a) (b)
Fig. 6. (a) Cover image, (b) watermarked Image

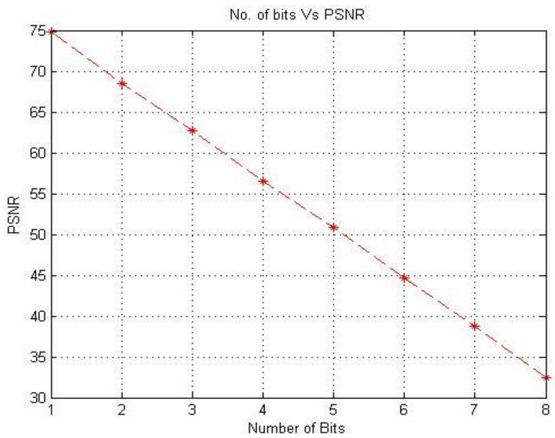

Fig. 7. Graph of Number of bits Vs. PSNR

Following Correlation Results are obtained at the receiver after attack.

TABLE II ATTACKS AND ITS CORRELATION VALUE

Bit	Attack	Correlation value
1	No Attack	1
	Salt & Pepper Noise	0.95314
	Gaussian Noise	0.931628
	Low Pass Filtering	0.929674
	Median Filtering	0.947256
2	No Attack	1
	Salt & Pepper Noise	0.949314

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 5, Issue 8, August 2016

	Gaussian Noise	0.945312
	Low Pass Filtering	0.95315
	Median Filtering	0.92971

C. **Graphical User Interface**

Following are the GUIs for sender and Receiver side

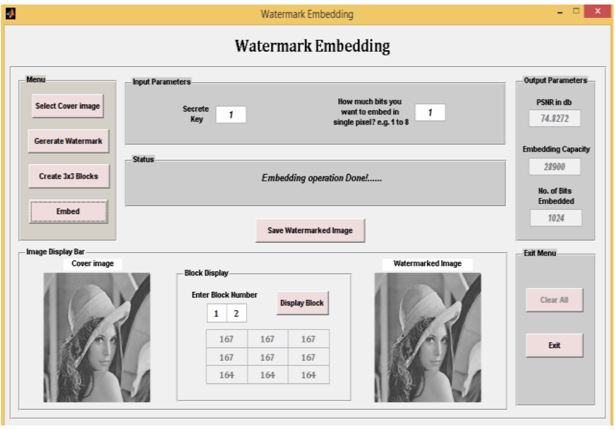

Fig. 8. GUI of sender side

Above GUI is created with the help of MATLAB. All coding and algorithms are done with the MATLAB.

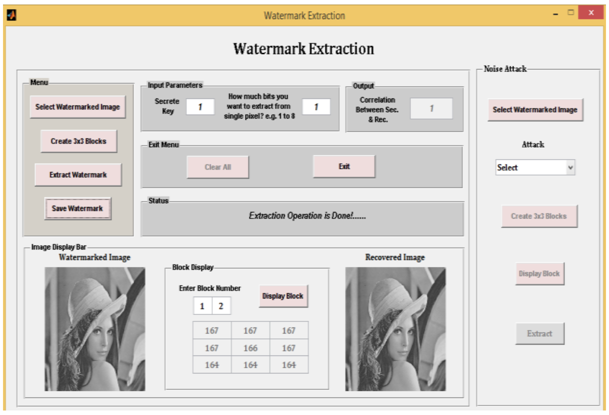

Fig. 9. GUI of Receiver side

IV. CONCLUSION

The Proposed technique describes robust and invisible digital image watermarking in spatial domain, which is computationally efficient. Embedded watermark is a sequence of real numbers that are normally distributed or a Pseudo-Noise sequence. Proposed technique has been tested over large number of benchmark images as suggested by watermarking community and the results of robustness to different signal processing operations are found to be satisfactory. Robustness is tested by various attacks. Correlation value shows the proposed technique withstand with all external attacks.

REFERENCES

[1] Santi Prasad Maity "Robust and Blind Spatial Watermarking in Digital Image"
[2] Anastasios L. Kesidis and Basilios Gatos "A Robust Image Watermarking Technique Based On Spectrum Analysis And Pseudorandom Sequences" International Conference on Computer Vision Theory and Applications in 2007
[3] R. Anderson.Information Hiding. Proceedings of the First Workshop on Information Hiding, LNCS-1174, Springer Verlag, New York, 1996.
[4] S.Katzenbesser and F.A.P Petitcolas.Information Hiding Techniques for Steganography and Digital Watermarking. Artech House, Boston, MA, 2000.
[5] Chiou-Ting Hsu and Ja-Ling Wu. Hidden Digital Watermarks in Images. IEEE Transaction on Image Processing, 8,pp. 58-68, 1999 .
[6] I.J. Cox, J. Kilian, T. Leighton and T. Shammon. Secure Spread Spectrum Watermarking for Multimedia. IEEE Transaction on Image Processing, 6, pp. 1673-1687, 1997.
[7] A. R. Nichal. A Novel Steganography Scheme via the use of Alpha channel as a carrier in International Journal of Innovative Research In Electrical, Electronics, Instrumentation And Control Engineering in 2015
[8] Nidhi S Kulkarni, IndraGupta, and S. N. Kulkarni, "A Robust Image Encryption Technique based on Random Vector," Proc. of IEEE 1st International conference on Emerging Trends in Engineering and Technology, pp.15-19, 2008.
[9] D. Samanta, A. Basu, T. S. Das, V. H. Mankar, Ankush Ghosh, Manish Das and Subir K Sarkar, " SET Based Logic Realization of a Robust Spatial Domain Image Watermarking," Proc. in 5th International Conference on Electrical and Computer Engineering-ICECE 2008, Dhaka, Bangladesh, pp. 986-993, Dec. 2008.
[10] Jeng-Shyang Pan, H. C. Huang, and L. C. Jain: Intelligent Watermarking Techniques. World Scientific, 2004.
[11] Mustafa Osman Ali and Rameshwar Rao. "An Overview of Hardware Implementation for Digital Image Watermarking," Proc. of International Conference on Signal, Image Processing and Applications (SIA 2011), Chennai, India, pp. 19-24, Dec. 2011.
[12] Saraju P. Mohanty, "A Secure Digital Camera Architecture for Integrated Real-Time Digital Rights Management," Elsevier, 2009
[13] Ingemar J. Cox, MatthewL. Miller, Jeffrey A. Bloom, Jessica Fridrich, and Ton Kalker, "Digital Watermarking and Steganography," 2nd edition, Elsevier, 2008.
[14] O. B. Adamo, Saraju P. Mohanty, E. Kougianos, and M. Varanasi, "VLSI Architecture for Encryption and Watermarking Units Towards the Making of a Secure Camera," Proc. In IEEE International Conference SOC, pp. 141-144, 2006.