Authenticating Images using Blind Fragile Watermarking Scheme based on LSB Technique

Mamta Baghel
GLNAIT, Mathura
INDIA

Rashmi Bhardwaj
GLNAIT, Mathura
INDIA

Shivendra Shivani
MNNIT, Allahabad
INDIA

ABSTRACT

This paper proposes blind fragile watermarking scheme along with the pixel-wise technique. Proposed scheme is capable enough in detecting tampered pixels and also able to provide security. For inserting watermark, 3-LSB substitution technique is used. As scheme is focus on blind watermarking technique that's why, embed self-watermark into the image. Self-watermark is generated by applying some set of operations on the pixel value of host image. For the generation of watermark: Firstly, generate secret matrix from the secret key .Secondly, generate pixel matrix from 5MSBs of pixel. Then, generate image matrix from pixel and secret matrices. Finally, generate final matrix consisting 3 rows and 1 column and this matrix gives 3LSBs which will be embedded into the host image to generate watermarked image. Security is provided by secret key and by using the concept of RSA algorithm.

General Terms

Algorithms, Watermarking, host image.

Keywords

Fragile watermarking, Temporization, Detection, Blind approach, LSB substitution, Pixel-wise technique

1. INTRODUCTION

In today's digital world, transferring of data is integral part of communication [13]. Data includes videos, images, audios etc. Securing these data is the big challenge. Digital watermarking technique provides copyright protection for the digital data [10] [12]. For securing these data, the concept of watermarking came into existence. With watermarking scheme, additional information is attached that provides security to these data [1] [2]. Watermarks are classified into two categories: Visible and Invisible watermarks [2] [9] [10]. Watermarking schemes are broadly divided into three categories: Fragile, semi-fragile, and robust. A fragile watermark is a mark that is readily altered or destroyed when the host image is modified through a linear or non-linear transformation. As fragile watermark are sensible to modification in an image even at slighter change in the pixel value, it leads to their use in image authentication [3]. Semi-fragile watermarks are those marks that designed in such a way that they break under the changes that exceed a user-specified threshold [2] [4] .Robust watermarks are designed to withstand moderate to severe signal processing attacks.Robust watermarks are used for copyright protection [2] [5] . For embedding and extracting watermarks, there are two techniques: Block-wise technique and Pixel-wise technique [6] [7]. In bock-wise technique, if any pixel is tampered in block, then it will show temporization in whole block. So it is very difficult to identifying exact location of tampered pixel but it is very good technique for securing images [6]. In pixel-wise technique, it will detect pixels which are tampered. So detection of tampered pixels is very difficult. Scheme proposed by Zhang and Wang [8] is one of the standard scheme on pixel-wise fragile watermarking.

In this paper, we propose image authentication techniques by using blind fragile watermarking scheme based on pixel-wise approach for accurately locating temporization in images. This paper provides authenticity to images and also there is no requirement of original image at the time of verification. For the insertion of watermark, this scheme uses 3LSB substitution technique [11]. This paper provides two algorithms, one for embedding watermark and another for the extraction of watermark along with the security mechanism. All details of these algorithms are provided in section 2. Scheme proposed by Yin Ke-xin, Zhu Jian-qi, Liu Bing and Zhong Guan-qun [14] use Hash function in order to achieve precise tamper localization and probability for detecting tampered pixels is about 95% whereas proposed approach provides probability up to 100% based on different types of temporization.

2. WATERMARKING SCHEME

Proposed watermarking algorithms are based on LSB substitution technique. This watermarking scheme uses pixel-wise approach as its base. Consider a host image I of size r*c then resize it to size of 255*255 and then set 3 LSBs to zero. After that apply security mechanisms and then apply embedding and extracting procedures. Block diagrams for embedding and extracting watermarks are shown by Fig 1 and Fig 2 simultaneously.

2.1 Watermarking embedding process

1. Input a Grayscale Image I of size r*c, such that r, c>=0.
2. Resize Grayscale Image I, such that $1 \geq r, c \leq 255$.
3. Randomly Provide a Secret Key.
4. Call RSA Embedding Algorithm.
5. Generate Secret matrix Sm, by Applying Pseudo-random function on randomly selected Secret Key scrt_key.
6. In an Image I , do
   - i) For every Pixel p of an image,
     - a) Represent pixel p in 8-bit binary format from decimal format.
     - b) Set 3 LSB of pixel p to zero.
     - c) From 8-bit binary pixel p, Generate 3*3 pixel matrix Pm.
   - ii) Generate 3*3 Image matrix Im, applying X-OR on pixel and secret matrix, such that

Im=XOR (Pm, Sm)

iii) Generate Final matrix F_k, such that r=3 and c=1.

a) F_k=Im ,here k=0

b) For k, where k=1, 2, 3………

For i→1 to r do

For j→1 to c-1 do

F_k (i, j) =XOR (F_{k-1}(i, j),F_{k-1}(i, j+1))

End

End

Decrement c by 1

End

c) Repeat step (b), until c=0.

iv) Thus, 3LSBs has been generated from Final matrix F_k of size 3*1.

v) Now, Replace 3 LSB of Pixel p with these newly generated 3 LSBs.

7. By applying this process to whole image, Watermarked Image W has been generated.

2.2 Watermarking extracting process

1. Input Tampered Watermarked Image T of size r*c, such that r=255 and c=255.
2. Input a Secret Key scrt_key, which is previously used in insertion process
3. Call RSA Extraction Algorithm.
4. Generate Secret matrix Sm, by Applying Pseudo-random function on randomly selected Secret Key scrt_key.
5. Generate 255*255 Tampered Pixel Localization Image TPL_img for locating tampered pixels, Such that every pixel p has value equal to zero.
6. In Tampered Watermarked Image T , do

i) For every Pixel p of an image,

a) Represent pixel p in 8-bit binary format from decimal format.

b) Store 3 LSB of pixel p in a vector, named as LSB_ORG.

c) Now, Set 3 LSB of pixel p to zero.

d) From 8-bit binary pixel p, Generate 3*3 pixel matrix Pm.

ii) Generate 3*3 Image matrix Im, applying X-OR on pixel and secret matrix, such that

Im=XOR (Pm, Sm)

iii) Generate Final matrix F_k, such that r=3 and c=1.

a) $F_{k=}$Im ,here k=0

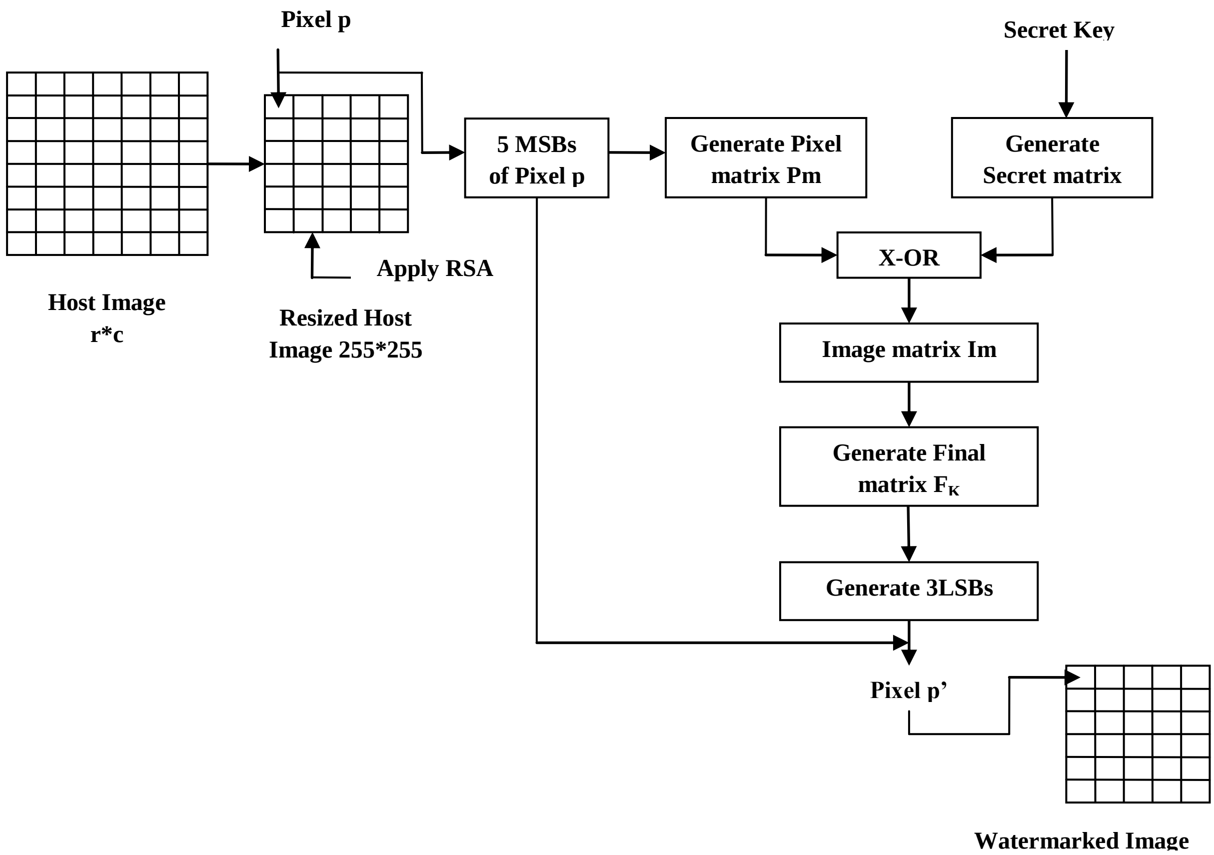


Fig 1: Block Diagram of Watermarking Embedding Procedure

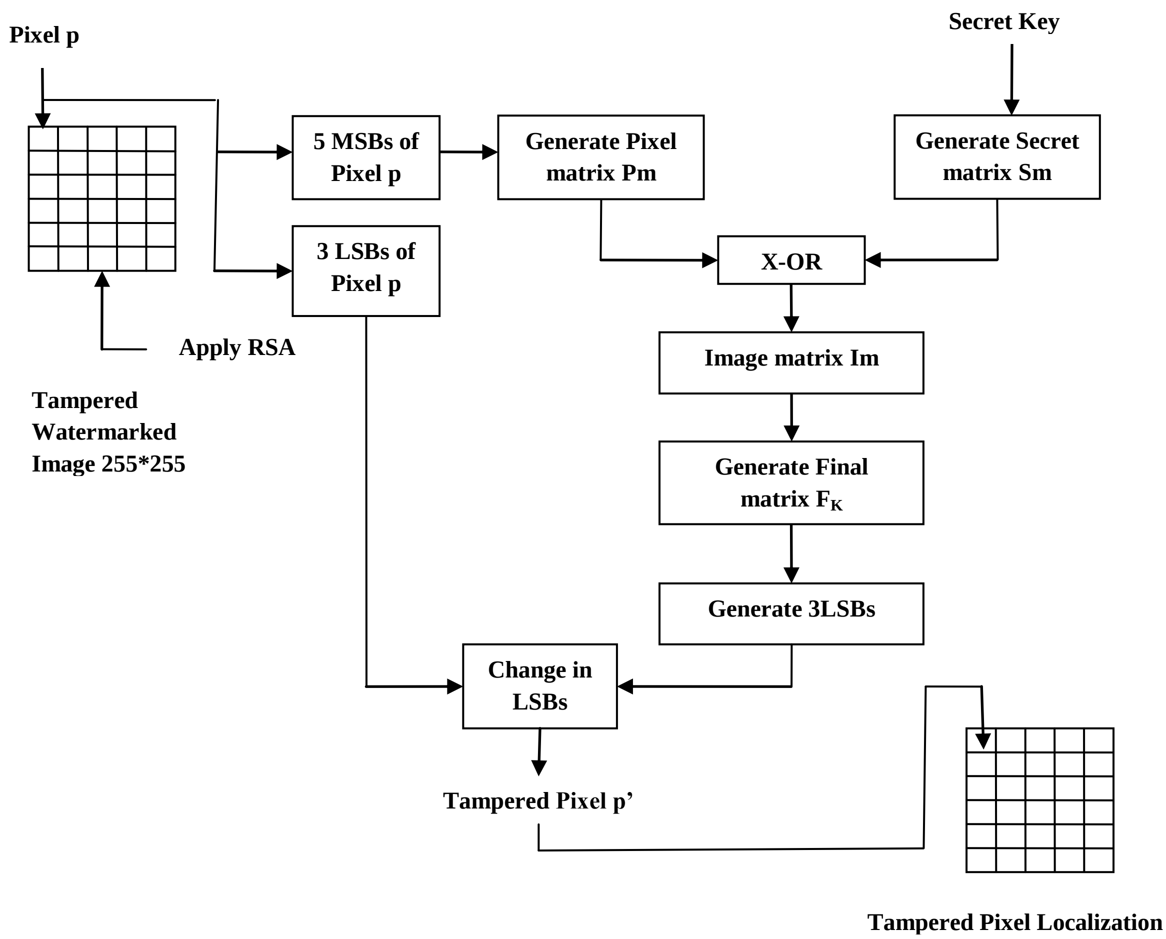


Fig 2: Block Diagram of Watermarking Extracting Procedure

b) For k, where k=1, 2, 3………
  For i→1 to r do
   For j→1 to c-1 do
    F_k (i, j) =XOR (F_{k-1}(i, j),F_{k-1}(i, j+1))
   End
  End
 Decrement c by 1
 End

c) Repeat step (b), until c=0.

iv) Thus, 3LSBs has been generated from Final matrix F_k of size 3*1.

v) Now, Compare these newly generated 3 LSB's with previously stored 3 LSB's, i.e.,
  if (LSB=LSB_ORG),then
   No Temporization is done to pixel value.
   So, there is no change in pixel p of TPL_img.
  Else
   Temporization is done to pixel value.
   So, set pixel p of TPL_img to 1.
  End

7. By applying this process to whole image, tampered pixels of Image T would be localized.

3. EXPERIMENTAL RESULTS

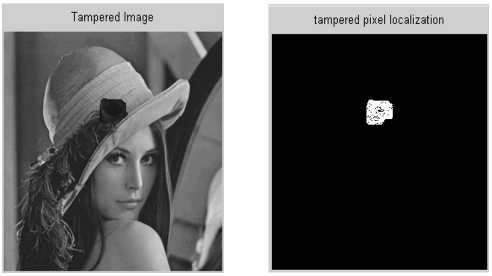
Experimental results show different types of temporization like addition of some object or text, deletion of some object or text etc. Different grayscale images show how watermarks are embedded and extracted. Here, experimental results show that this scheme is able to achieve PSNR value equal to 44.09 and efficiency up to 100%. PSNR value varies on basis of secret key used. These procedures can also be applied on color images. In color images, detection of tampered pixels will be showed in all three planes i.e., on RGB planes.

Fig.1 (a) and (b) shows the results after applying watermarking embedding procedure. Fig.1(c) and (d) shows the results after applying watermarking extracting procedure. Section 3.1 show different types of result on grayscale images and section 3.2 show result on various color images.

3.1 Result on grayscale images:

3.1.1 On Lena image

(a) (b)

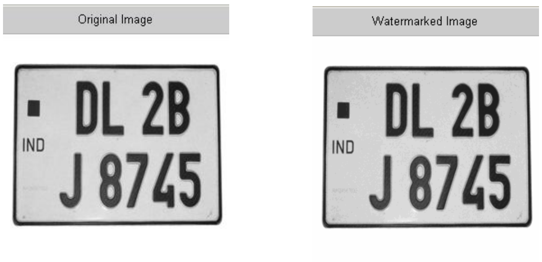


(c) (d)

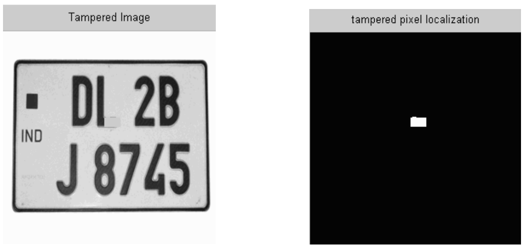
Fig.3

In Fig.3, temporization is done by adding a small rose flower on the hat of Lena by tampering 720 pixels. Then, by applying watermarking extracting procedure, 656 pixels are detected. Thus, this gives efficiency equal to 91.1% and PSNR value equal to 44.09 dB.

3.1.2 On number plate image:



(a) (b)



(c) (d)

Fig 4

In Fig.4, temporization is done by changing ‘L’ of number plate to ‘I’ by tampering 214 pixels then; this approach is able to detect 214 pixels. Thus, this approach is able to achieve 100% efficiency and PSNR value for this image is 40.59 dB.

3.1.3 On flower image

(a) (b)

(b) (d)

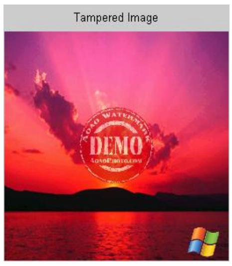
Fig.5

In Fig.5, temporization is done by adding text on image by tampering 246 pixels and by using watermarking extracting procedure; it is able to localize all 246 tampered pixels. PSNR value for this image is 39.41 dB.

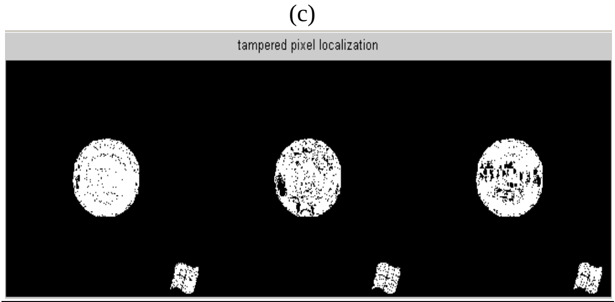
3.2 Result on color images:

3.2.1 On sunset image:

(a) (b)



(c)



(d)

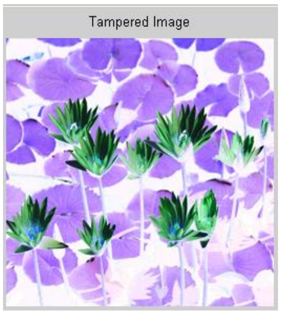
Fig.6

In Fig.6, temporization in sunset image is done by adding some logos by tampering 6339 pixels and by applying watermarking extracting procedure on tampered image; this is able to detect 6045 pixels. Thus, efficiency achieved is 95.36%.

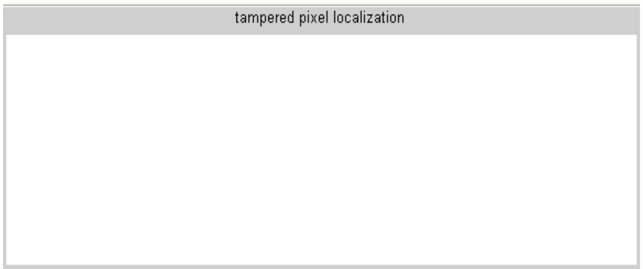
3.2.2 On water lilies image:

(a)

(b)



(c)



(d)

Fig 7

In Fig.7, temporization is done to whole image by inverting color of the image which tampers 65025 pixels. After applying watermarking extracting procedure, this scheme is able to detect all 65025 pixels of the image. Thus, 100% efficiency is achieved.

4. CONCLUSION

This paper proposes watermarking embedding and extraction algorithm in spatial domain by which one can easily identify changes in every pixel of the images accurately and also there is good security mechanism for securing images. Proposed watermarking algorithms are able to increase PSNR value and also have low complexity of algorithms. These algorithms also work on color images efficiently, but show temporization results in all three RGB planes. Proposed scheme achieve PSNR value up to 44.09 dB and also able to achieve 100% efficiency in some cases, which is good enough. Thus, these watermarking algorithms give significant responses in finding various types of temporization attacks.

5. REFERENCES

[1] S. Radharani and Dr. M.L. Valarmathi, Ph.D." A Study on Watermarking Schemes for Image Authentication" IJCA (0975 – 8887) Volume 2 – No.4, June 2010.

[2] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, "Information hiding—A survey," Proc. IEEE, vol. 87, no.7, pp. 1062–1078, Jul.1999.

[3] Eugene T. Lin and Edward J. Delp. "A review of fragile watermarking, Center for Education and Research in Information Assurance and Security" ,Purdue University, West Lafayette, IN 47907-2086.

[4] 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.

[5] C. Y. Lin and S. F. Chang, "A robust image authentication method surviving JPEG lossy compression," Proc. SPIE, vol. 3312, pp. 296-307, 1998.

[6] B. B. Zhu, M. D. Swanson, and A. H. Tewfik, "When Seeing Is n't Believing," IEEE Signal Processing, vol. 21, no. 2, pp. 40-49, March 2004.

[7] B. B. Zhu and M. D. Swanson, "Multimedia Authentication and Watermarking," Multimedia Information Retrieval and Management, D. Feng, W. C. Siu, and H. Zhang, Eds. Springer-Verlag, Berlin, Heidelberg, New York, 2003 chap. 7, pp. 148-177.

[8] Xinpeng Zhang and Shuozhong Wang, "Statistical Fragile Watermarking Capable of Locating Individual Tampered Pixels" IEEE Signal processing letters, VOL.14, NO.10, October 2007.

[9] K.Ganesan and Tarun Kumar Guptha, "Multiple Binary Images Watermarking in Spatial and Frequency Domains", Signal & Image Processing : An International Journal(SIPIJ), Vol.1, No.2, December 2010.

[10] Jaseena K.U., Anita John, "An Invisible Zero Watermarking Algorithm using Combined Image and Text for Protecting Text Documents", International Journal on Computer Science and Engineering (IJCSE), Vol. 3, No. 6 , June 2011.

[11] Sajjad Dadkhah, Azizah Abd Manaf and Somayeh Sadeghi, "Efficient Digital Image Authentication and Tamper Localization Technique Using 3Lsb Watermarking", IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 1, No 2, January 2012.

[12] Rosline Nesa Kumari, Vijaya Kumar, Sumalatha and Krishna, "Secure and Robust Digital Watermarking on Grey Level Images", International Journal of Advanced Science and Technology, Vol. 11, October, 2009.

[13] W. Lin et al, "Multimedia Analysis, Processing & Communications", Springer-Verlag Berlin Heidelberg, 2011 SCI 346, pp. 139–183.

[14] Yin Ke-xin, Zhu Jian-qi, Liu Bing, Zhong Guan-qun, "Pixel-based fragile image watermarking algorithm", 2010 Second International Workshop on Education Technology and Computer Science.