Indian Journal of Science and Technology, Vol 9(44), DOI: 10.17485/ijst/2016/v9i44/105311, November 2016
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Recovery of Watermarked Image from Geometrics Attacks using Effective Histogram Shape based Index

M. Divya[1*] and Murari Devakannan Kamalesh[2]

[1]Department of Computer Science and Engineering, Sathyabama University
Chennai - 600119, Tamil Nadu, India; Divyamano2@gmail.com
[2]Faculty of Computing, Sathyabama University, Chennai - 600119, Tamil Nadu, India; kamal2gd@gmail.com

Abstract

Objective: The main objective of the paper is to provide security and proof of ownership to the watermarked image. **Methods:** Watermark is a transparent or an undetectable signature implanted inside an image to show uniqueness or proof of ownership. The illegally used images can undergo different kind of attacks namely signal processing attacks and geometric attacks. We have used Tree Based Parity Check (TBPC) algorithm to deal with these common attacks. We preprocess the host image using Gaussian filter. And using Fast Walsh-Hadamard method, we embed watermark inside an Image. **Findings:** We choose the Gray levels of the image by the means of secret key. Later we construct the histogram based on the gray level that is chosen. In these chosen pixels group's watermarks are embedded. Then a secret text or code is inserted into this filtered image. To encrypt this text we use Tree Based Parity Check algorithm. Based on the secret key that is available, in the decoding phase we identify watermark pixel group and then we extract the watermarks from them. **Application:** The proposed system can achieve strong robustness of the image and detailed view of Bone structure in X-ray images. It can also be used to find the duplicate currency notes.

Keywords: Fast Walsh-Hadamard and Tree Based Parity Check, Gaussian Filter, Image Water Marking

1. Introduction

In the modern communication networks data are transmitted at a very high speed. Simultaneously illegally altered copies of digital media files are replicated and distributed over the network. Due to this copyright protection has become a big issue in today's modern digital world. In order to avoid this problem digital water marking is introduced. Such digital marking is used in audio, video and images. This paper deals mainly on image watermarking. The watermarks are supposed to be self-effacing. Robustness specifies the capability of appropriately extracting watermarks from image after going through the diverse kinds of attacks. There are two types of common attacks; signal processing attacks and geometric attacked are a great threat to the authenticity of the information. Signal processing attacks refers to filtering, noise addition, compression and geometric attacks refer to scaling, random bending, cropping and rotation. Protection refers to the confrontation to illegal watermark decoding by not identifying the secret key.

In the recent years, many image-watermarking techniques are implemented. All these techniques are vigorous to signal processing threats but they could not manage well with geometric attacks. All these techniques are vigorous to signal processing threats but they could not manage well with geometric attacks. The techniques are insolent to the JPEG compression however it is very receptive to rotation[1,2]. In order to manage geometric attacks, many procedures are exploited in image water marking. These methods could be generally segregated into non-blind and blind water marking methods,

*Author for correspondence

respectively. Non-blind watermarking methods[3-10] will need the actual image to extract watermarks at the decoding phase. This limits the practical usage. However the blind watermarking procedures don't need the details of the actual image at the decoding end. By predicting the probable attacking parameters[11,12], thorough exploration is conceded out during the extraction process in order to find the implanted watermarks from the image that is received. Complete explore -based techniques are very costly at the other end. Additionally, the probability of false detection is high. The province or the domain that is generated by Fourier–Mellin transform is used to embed watermarks[13,14]. These are invariant to scaling and rotation. However this method is naturally helpless to cropping attack. The method[15] uses the combination of discrete Fourier transforms and discrete wavelet for image watermarking, however the major drawback is that it could not resist with Random Bending Attacks (RBA's). In[16] they developed uniform log-polar mapping to withstand geometric attacks, but the same is vulnerable to random bending attacks. The combination of decomposition of singular value and discrete cosine transform is used to deal cropping attacks; however the same is cannot cope up well with filtering, noise addition, compression and few geometric attacks[17].

While decoding, this template will provide details about the various geometric attacks that the image that is watermarked has underwent. In[18] 25 point templates are embedded in DFT domain by means of log-log-map to defend against scaling and rotation. However, this technique is helpless to the mixture of scaling and rotation. A common line structure can be implied to the template so that the general affine transformations can be resisted[19]. In order to get more precise and quicker template matching they used chirp-Z transform[20]. The main drawback is the attackers can easily predict the template and can remove the same, moreover for template-based techniques[21] it is difficult to guess the RBA's parameters used, thus it will degrade the robustness to a higher extent[22]. It cannot assure to extract the inserted watermarks due to cropping attacks as a result information of the image could be lost.

Moment invariant can betaken from an image using the properties of spatial statistics[23,24]. Affine attacks can be easily handled by this method; however cropping attacks are still highly vulnerable. The watermarks are implanted into some attribute areas in the spatial province[25-28], this technique is helpful in resisting cropping and affine attacks. In[29] a method is used in order to optimally select the attribute regions so that it could resist as many attacks. Thus, as a result the decoding method will be affected due to the shifting of pixel position, which could be caused by Random bending attacks. As a result, all the aforesaid watermarking methods could not cope up with Random bending attacks and few geometric attacks such as cropping. Some part of image can be cut in order to destroy the sync in-between the transmitter and receiver. This is automatically reduces the perceptual quality of an image. Such RBA can be determined by using high-quality printer[30], so that the watermarked image is filtered and after which high-quality scanner is used to scan the same. When a watermarked image is randomly modified, a resynchronization problem is caused due to the displacement of sample grid locations. Furthermore, with few image processing tools, the random bending and cropping attacks can be handled by the person who doesn't have much knowledge about the image watermarking.

They applied fractal coding in order to withstand random bending and cropping attacks however this method is helpless towards global transforms[31]. In recent times, they showed that histogram shape of water marked image is not variant to displacement of pixel location and the same is not sensitive towards cropping, which increases the stamina to resist cropping attacks and Random Bending attacks. But, the techniques implemented from do not clearly utilize the histogram shape of the image. As an alternative, they used signify of the histogram in order to select the gray values in a particular range or pixels with respect to these gray levels is used to figure out pixel groups while embedding watermark. A universal disadvantage of this[32] technique is that numerous probable pixel groups which enclose more pixels are not created and used while embedding watermark, which reduces the robustness of the watermarked image. Furthermore, the performance of histogram-based method is affected by interpolation errors and signal processing attacks that are caused by geometric attacks. The techniques do not consider these kinds of impacts; as a result it is insensitive to most of the attacks[33]. Low-pass pre-filtering process is applied in order to handle this difficulty however the depressing bang on decryption of watermark caused by pre-filtering is not efficiently handled.

The histogram and the spatial feature regions and combinedin[34],howeverthiscombinationbringsmanyother problems. Firstly, the non-stable volatility is persuaded due to lack of robustness. Secondly, the inadequate pixels in one particular feature region make the system more

vulnerable towards the attacks. In[35,36] they used histogram in reversible watermarking. In[37] they introduced many approaches for the software watermarking methods that are technical approaches to identify software copyright details. In[38] they used fragile watermarking method in order to deal with image tampers. The main offerings of our paper are that the proposal of a new histogram based shape related index to select the pixel group using secret key. The side effects of Gaussian filtering are controlled by the usage of Fast Walsh-Hadamard and Tree Based Parity Check techniques. Using the simulation example we illustrated the performance of the proposed image-watermarking technique.

This paper is composed in such a way that sections 2, 3 and 4 demonstrate the proposed image-water marking technique. Section 5 concludes this paper.

2. Watermark Embedding Process

The Figure 1 shows the architecture diagram of the watermark embedding process. Before inserting the watermark into the original image, it is necessary to preprocess the image.

Hence we use low pass filtering method to preprocess the image.

2.1 Gaussian Low Pass Filtering

Gaussian filtering g is used for the purpose of blurring the images and to remove its noise and detail. This method acts as a softening operator.

$$H_{(U,V)} = e^{-D^2(u,v)/2\,D_2^2}$$

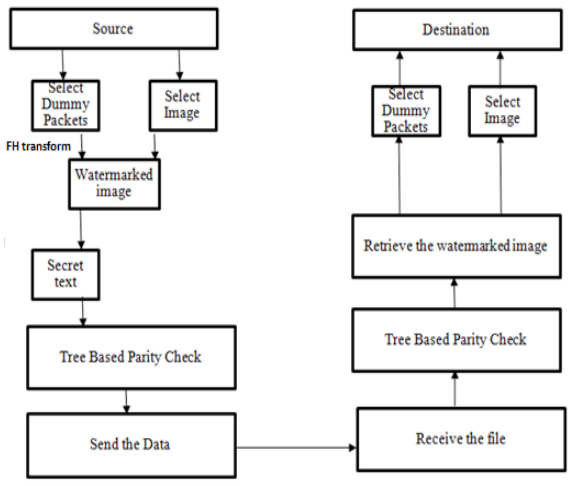

Figure 1. Block diagram of the proposed system.

Two dimensional Gaussian distribution function is mostly used while working with images. The robustness of the water marked image shall be attained by the process of embedding the watermarks into a low frequency module of an image. Thus the image is initially preprocessed by Gaussian low pass filtering method.

2.2 Fast Walsh–Hadamard Transform

The Fast Walsh–Hadamard transform is a proficient method in order to compute Walsh-Hadamard transform. The attribute values provide complete information for one particular grouping of input variables. The details regarding the other combinations are not available. Also some information regarding the behavior of function is provided at multiple points. However complete information about any single point is not provided.

Hadamard matrices

$$H_0 = +1$$

$$H1 = 1/\sqrt{2}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

H1 indicates precisely the size-2 of DFT.

To embed the watermark, we need to determine the largest square block which encircles the image. For an image with size (p; q) we select a block size c = max (p; q) and then we need to pad this image with 0's in order to create a square image during the watermark process. Then that particular padded portion is removed once the watermark is embedded. Thus the watermark is inserted into the DFT domain in between the radii r1 and r2. Later r1 and r2 are chosen to reside in a particular mid-frequency range. We see that the well-built components of DFT are in the core which holds the low frequencies. Although in the recovery stage the image signifies noise, these kinds of low frequencies are supposed to be avoided. We must also avoid high frequencies as these are the ones which are more significantly modified during lossy compression like JPEG. The frequencies r1 and r2 must be set since the process of decoding (in insensible watermarking) the block size c is unknown as the image might have been distorted by cropping or other geometric attacks. In order to embed the watermark among the chosen radii, we need to produce a series of spots pseudo-randomly as established by means of a secret key. The message we need to embed is inserted into the particular points of the DFT domain. The message is then inverted to get a spatial domain watermark that is straightly supplemented to the

image. The image fraction is well maintained as this leads to smaller amount of artifacts.

2.3 Histogram Construction and Pixel Group Selection

Consider that the image IL has K gray levels. A histogram of an image shows the number of pixels against the gray level values. Obviously, the figure of the histogram is directly associated to the image content. Once the histogram is constructed we consider each neighboring gray levels to form a bin.

We need to select the appropriate pixel groups that are suitable to hide watermarks

3. Template Embedding Algorithm

The template is a tool used in order to pull through probable alterations in the image, it usually contains no information. The template could be the employee ID or any unique information about the employee which is later used to detect the person through which the image was attacked.

- Step 1: Finding the location
  Edge regions of an image are more suitable for Hiding Secret data. As it is more secure, edge regions are preferred to hide secret data. The Edge Region represented as ER contains a pair of pixels like an embedding unit (xi, x i+1). The difference between these two pixels will be larger or equal to threshold T value which is known by the sender and receiver. The number of pixel pairs is determined based on the number of nodes existing in the master tree.
- Step 2: Tree Based Parity Check (TBPC) Method
  The TBPC technique is termed as the least significant bit stenography technique. This technique is used to generates ego code using the least significant bit of the selected pixels which has the below three steps.
- Step2.1: Master tree construction and generating master string and toggle string:
  This technique constructs a complete binary tree which is known to be master tree. The message length will be equal to the total number of leaf nodes of the tree. The master tree is filled with LSB's of the selected pixel level, from top to bottom and left to right. Aneven parity check is performed on master tree from its root to leaves in order to create master string. Exclusive-OR bit wise (XOR) function is applied between message and master string to get the toggle string.
- Step2.2: Toggle tree construction: Toggle tree is formed by loading the leaf nodes with toggle string and all the supplementary on-leaf nodes with Zero 0. Then, navigate through each level, starting from bottom towards the root. The non-leaf node and its resultant leaf nodes are spanned if both its children have bits as one.
- Step 2.3: Stego tree construction: This algorithm attains the stego tree by means of carrying out XOR among the master tree and the toggle tree. From the stego tree the stego code is obtained. The construction of the stego tree is shown n the Figure 2. The attained stego image hides secret bits in an extremely secure way.
- Step 3: The Least Significant Bit Matching Revisited (LSBMR) Algorithm: We apply the LSBMR algorithm to the stego code. Two consecutive bits of the stego code is embedded for each embedding region.

4. Template Extraction Algorithm

- Step 1: Finding the Location: Find the pixel pairs in the stego image where the template is embedded by the location finding technique used in step 1 of data embedding algorithm.
- Step 2: Extracting Stego code: Two stego code bits are extracted for each competent pixel pairs.
- Step 3: Stego tree construction: Complete binary tree can be constructed by filling its nodes by the stego codes. Later the original message can be extracted by performing parity check method.

Using the extracted template the owner of the image can identify the employee ID or the unique information that he provided to protect the water marked image.

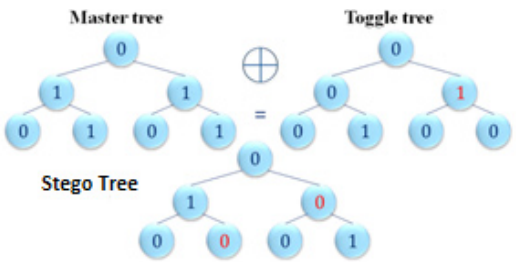

Figure 2. Stego tree construction.

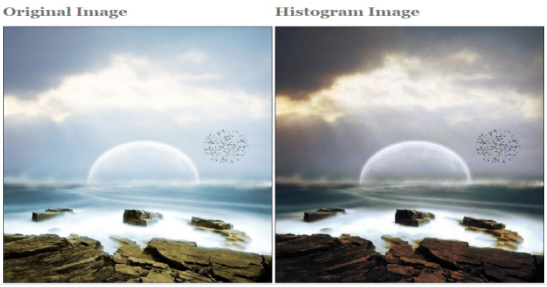

Figure 3. Histogram comparison.

5. Results

The original image and the preprocessed image are shown in Figure 3. The gray levels are randomly selected by means of secret key and in the randomly chosen pixels group watermarks are embedded.

6. Conclusion

In this paper, we have proposed a new image water marking method which is robust to signal processing attacks and geometric attacks. The host image is first processed by Gaussian filter in order to tackle the common geometric attacks i.e. cropping attacks and Random Bending Attacks. We choose the Gray levels of the image by the means of secret key. Later we construct the histogram based on the gray level that is chosen. In these chosen pixels group watermarks are embedded. Using Fast Walsh-Hadamard method, we embed watermark inside an Image. This Walsh-Hadamard method helps in compensating the side effects that is caused due to Gaussian filtering, which enhances more robustness. Due to the usage of secret key by means of tree based parity check algorithm, the proposed watermarking method will be more secure and the image can resist to the common geometric attacks.

This is will ensure to have proof of ownership of the water marked image and to determine the hackers who hacked the image. Thus, the proposed system can achieve a detailed view of Bone structure in X-ray images and better perspectives of photographs that are over or under exposed.

7. References

1. Xiang Y, Natgunanathan I, Peng D, Zhou YS. A dual channel time-spread echo method for audio watermarking. IEEE Transaction on Inf Forensics Security. 2012 Apr; 7(2):383-92.
2. Xiang Y, Peng D, Natgunanathan I, Zhou W. Effective pseudonoise sequence and decoding function for imperceptibility and robustness enhancement in time-spread echo-based audio watermarking. IEEE Transaction on Multimedia. 2011 Feb; 13(1):2-13.
3. Kalantari NK, Ahadi SM, Vafadust M. Robust image water marking in the ridge let domain using universally optimum decoder. IEEE Transaction on Circuits System Video Technology. 2010 Mar; 20(3):396-406.
4. Nezhadarya E, Wang ZJ, Ward RK. Robust image water marking based on multi-scale gradient direction quantization. IEEE Transaction on Information Forensics Security. 2011 Dec; 6(4):1200-13.
5. Wang L, Ling H, Zou F, Lu Z. Real-time compressed domain video water marking resistance to geometric distortions. IEEE Multi-Media. 2012; 19(1):70-9.
6. Lee M, Kim KS, Lee HK. Digital cinema water marking for estimating the position of the pirate. IEEE Transaction on Multimedia. 2010; 12(7):605-21.
7. Johnson NF, Duric Z, Jajodia S. Recovery of water marks from distorted images. Proceeding of 3rd International Workshop on Information Hiding; Germany. 2000. p. 318-32.
8. Davoine F. Triangular meshes: A solution to resist to geometric distortions based watermark-removal software's. Proceedings of EURASIP Signal Processing Conference; France. 2000.
9. Dong P, Brankov JG, Galatsanos N, Yang Y. Geometric robust water marking based on a new mesh model correction approach. Proceeding of IEEE International Conference on Image Process; USA. 2002 Jun 3. p. 493-6.
10. Zhang H. Affine Legendre moment invariants for image water marking robust to geometric distortions. IEEE Transaction on Image Process. 2011 Aug; 20(8):2189-99.
11. Lichtenauer JF, Setyawan I, Kalker T, Lagendijk RL. Exhaustive geometrical search and the false positive watermark detection probability. Proceeding of SPIE, Security Watermarking Multimedia Contents V; 2003 Jun. p. 203-14.
12. Barni M. Effectiveness of exhaustive search and template matching against watermark desynchronization. IEEE Signal Processing Letters. 2005 Feb; 12(2):158-61.
13. Ruanaidh JJKO, Pun T. Rotation, scale and translation invariant spread spectrum digital image water marking. Signal Process. 1998 May; 66(3):303-17.
14. Lin CY, Wu M, Bloom JA, Cox IJ, Miller ML, Lui YM. Rotation, scale and translation resilient watermarking for images. IEEE Transaction on Image Process. 2001 May; 10(5):767-82.
15. Kang X, Huang J, Shi YQ, Lin Y. A DWT-DFT composite water marking scheme robust to both affine transform and JPEG compression. IEEE Transaction on Circuits System Video Technology. 2003 Aug; 13(8):776–86.

16. Kang X, Huang J, Zeng W. Efficient general print-scanning resilient data hiding based on uniform log-polar mapping. IEEE Transaction on Information Forensics and Security. 2010 Mar; 5(1):1–12.
17. Rosiyadi D, Horng SJ, Fan P, Wang X, Khan MK, Pan Y. Copyright protection for e-government document images. IEEE Multi-Media. 2013 Jul/Sep; 19(3):62-73.
18. Pereira S, Ruanaidh JJKO, Deguillaume F, Csurka G, Pun T. Template based recovery of Fourier-based watermarks using log-polar and log-log maps. Proceeding of IEEE International Conference on Multimedia Computing and System; 1999 Jul. p. 9870.
19. Pereira S, Pun T. Robust template matching for affine resistant image water marks. IEEE Transaction on Image Process. 2000 Jun; 9(6):1123-9.
20. Pereira S, Pun T. An iterative template matching algorithm using the Chirp-Z transform for digital image watermarking. Pattern Recognition. 2000 Jan; 33(1):173-5.
21. Licks V, Jordan R. Geometric attacks on image watermarking systems. IEEE Multi-Media. 2005 Sep; 12(3):68-78.
22. Rodriguez MA, Gonzalez FP. Analysis of pilot-based synchronization algorithms for water marking of still images. Signal Process, Image Communication. 2002 Sep; 17(8):611-33.
23. Alghoniemy M, Tewfik AH. Geometric invariance in image water marking. IEEE Transaction on Image Process. 2004 Feb; 13(2):145–53.
24. Dong P, Brankov JG, Galatsanos Y, Yang Y, Davoine F. Digital water marking robust to geometric distortions. IEEE Transaction Image Process. 2005 Dec; 14(12):2140–50.
25. Seo JS, Yoo CD. Image watermarking based on invariant regions of scale-space representation. IEEE Transaction on Signal Process. 2006 Apr; 54(4):1537–49.
26. Tsai JS, Huang WB, Chen CL, Kuo YH. A feature based digital image water marking for copyright protection and content authentication. Proceeding of IEEE International Conference on Image Process; Taiwan. 2007 Sep/Oct. p. V-469–72.
27. Gao X, Deng C, Li X, Tao D. Geometric distortion insensitive image water marking in affine covariant regions. IEEE Transaction on System Man Cybernetics C, Application and Reviews. 2010 May; 40(3):278–86.
28. Lin YT, Huang CY, Lee GC. Rotation, scaling and translation resilient water marking for images. IEEE Transaction on Image Process. 2011 Jun; 5(4):328–40.
29. Tsai JS, Huang WB, Kuo YH. On the selection of optimal feature region set for robust digital image water marking. IEEE Trans Image Process. 2011 Mar; 20(3):735–43.
30. Petitcolas FAP, Anderson RJ, Kuhn MG. Attacks on copyright marking systems. Proceeding of 2nd International Workshop on Information Hiding; Portland. 1998. p. 218–38.
31. Dugelay J, Roche S, Rey C, Doerr G. Still-image water marking robust to local geometric distortions. IEEE Transaction on Image Processing. 2006 Sep; 15(9):2831–42.
32. Xiang S, Kim HJ, Huang J. Invariant image water marking based on statistical features in the low-frequency domain. IEEE Transaction on Circuits System for Video Technology. 2008 Jun; 18(6):777–90.
33. Wei LX, Long GB, Da LL, Xin SH. A new histogram based image water marking scheme resisting geometric attacks. Proceeding of 5th International Conference on Information Assurance and Security. Beijing. 2009 Aug. p. 239–42.
34. Deng C, Gao X, Li X, Tao D. Local histogram based geometric invariant image water marking. Signal Processing. 2010 Dec; 90(12):3256–64.
35. Jung SW, Ha LT, Ko SJ. A new histogram modification based reversible data hiding algorithm considering the human visual system. IEEE Signal Processing Letters. 2011 Feb; 18(2):95–8.
36. Coatrieux G, Pan W, Boulahia NC, Cuppens F, Roux C. Reversible water marking based on invariant image classification and dynamic histogram shifting. IEEE Transaction on Information Forensics Security. 2013 Jan; 8(1):111–20.
37. Lim HI. A performance comparison on characteristics of static and dynamic software water marking methods. Indian Journal of Science and Technology. 2015 Sept; 8(21):1-6.
38. Vaishnavi D, Subashini TS. Image tamper detection based on edge image and chaotic Arnold map. Indian Journal of Science and Technology. 2015 Mar; 8(6):548–55.